Cisco Crosswork Network Controller 6.0.x Release Notes

First Published: 2023-12-19

This document provides information about Cisco Crosswork Network Controller 6.0.x, including product overview, solution components, new features and functionality, compatibility information, and known issues and limitations.

Overview

Cisco Crosswork Network Controller empowers customers to simplify and automate intent-based network service provisioning, monitoring and optimization in a multi-vendor network environment with a common GUI and API.

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. Using telemetry gathering and automated responses, Cisco Crosswork Network Controller delivers network optimization capabilities that would be nearly impossible to replicate even with a highly skilled and dedicated staff operating the network.

The fully integrated solution combines core capabilities from multiple innovative, industry-leading products including Cisco Network Services Orchestrator (NSO), Cisco Segment Routing Path Computation Element (SR-PCE), Cisco WAN Automation Engine (WAE), Cisco Crosswork Data Gateway, and an evolving suite of applications operating on the Cisco Crosswork Infrastructure. Its unified user interface allows real-time visualization of the network topology and services, as well as service and transport provisioning, via a single pane of glass. While its feature-rich API allows operators to seamlessly integrate the solution with other applications they use to operate, monitor, and provision services on the network.

Primary Use Cases:

- **Orchestrated service provisioning:** Provisioning of layer 2 VPN (L2VPN) and layer 3 VPN (L3VPN) services with underlay transport policies to define, meet, and maintain service-level agreements (SLA), using the UI or APIs. Using Segment Routing Flexible Algorithm (Flex-Algo) provisioning to customize and compute IGP shortest paths over a network according to specified constraints and visualizing the resulting path.
- **Real-time network and bandwidth optimization:** Intent-based closed-loop optimization, congestion mitigation, and dynamic bandwidth management based on Segment Routing and RSVP-TE. Optimization of bandwidth resource utilization by setting utilization thresholds on links and calculating tactical alternate paths when thresholds are exceeded.
- **Circuit Style Segment Routing Traffic Engineering (CS SR-TE) policy provisioning with network topology visualization:**
  - Straightforward verification of CS SR-TE policy configurations
  - Visualization of CS SR-TE details, bi-directional active and candidate paths

  - Operational status details
  - Failover behavior monitoring for individual CS SR-TE policies
  - A percentage of bandwidth reservation for each link in the network
  - Manually triggered recalculations of existing CS SR-TE policy paths that may no longer be optimized due to network topology changes

- **Local Congestion Management:** Local Congestion Mitigation (LCM) provides localized mitigation recommendations within surrounding interfaces, with the use of standard protocols. Data is gathered in real-time and when congestion is detected, solutions are suggested. LCM has a “human-in-the-loop” aspect which ensures that the control of making changes in the network is in the hands of the operator. Likewise, LCM also offers operators the option to automate changes – allowing the system to implement changes to the network on its own.
- **Visualization of network and service topology and inventory:** Visibility into device and service inventory and visualization of devices, links, and transport or VPN services and their health status on maps with logical or geographical contexts.
- **Performance-based closed-loop automation:** Automated discovery and remediation of problems in the network by allowing Key Performance Indicator (KPI) customization and monitoring of pre-defined remediation tasks when a KPI threshold is breached. For this use case, Health Insights and Change Automation functions must be installed.
- **Planning, scheduling, and automating network maintenance tasks:** Scheduling an appropriate maintenance window for a maintenance task after evaluating the potential impact of the task (using WAE Design). Automating the execution of maintenance tasks (such as throughput checks, software upgrades, SMU installs) using playbooks. For this use case, Health Insights and Change Automation functions must be installed.
- **Zero-touch provisioning (ZTP) and onboarding of devices:** Onboarding new IOS-XR and IOS-XE devices and automatically provisioning Day0 configuration, resulting in faster deployment of new hardware at lower operating costs. For this use case, the Zero Touch Provisioning function must be installed.
- **Visualization of native Segment Routing (SR) paths:** Visualizing the native path using the traceroute SR-MPLS multipath command to get the actual paths between the source and the destination can be achieved using Path Query. A traceroute command runs on the source device for the destination TE-Router ID and assists in retrieving the paths.
- **Provision, Visualize, and Analyze Tree Segment Identifier Policies in Multipath Networks:** Creating and visualizing static Tree-SID policies using the UI. Static mVPN Tree-SID policies, associated with existing or newly created L3VPN service models (SR MPLS point-to-multi-point), can be visualized and analyzed to assist in efficient management and troubleshooting of your multicast network.
- **Transport Slice Provisioning:** Cisco Crosswork Network Controller offers direct support for network slicing at the OSI transport layer. Using this solution, network engineering experts can design slices around customer intents and then add them to a catalog. Network line operators can then simply pick the slice that best meets the customer's needs, specify the slice endpoints, and (where needed) set any custom constraints or options built into the chosen slice. Once the slice is provisioned, the path chosen can be visualized. Customers wishing an even greater amount of insight can use Service Health to gather additional performance data about the service.

Solution Components

Cisco Crosswork Network Controller components hosted on the Crosswork cluster:

Table 1:

Component	Version	Description
Crosswork Infrastructure	6.0	A resilient and scalable platform on which all of the Cisco Crosswork applications can be deployed. The infrastructure is based on a cluster architecture for extensibility, scalability, and high availability. For installation, configuration and administration procedures, refer to the following documents: • Cisco Crosswork Network Controller 6.0 Installation Guide • Cisco Crosswork Network Controller 6.0 Administration Guide
Optimization Engine	6.0	Provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity. Provides traffic engineering visualization of SR-MPLS, SRv6, and RSVP-TE policies.
Active Topology	6.0	Enables VPN (L2VPN, L3VPN) service provisioning, service oriented transport (SR-MPLS, SRv6, CS-SR, RSVP-TE) provisioning and topology visualization of the provisioned services with the ability to customize the service provisioning and visualization through service model extensibility.
Service Health	6.0	Overlays a service level view of the environment and allows operators to monitor the health of services (for example, L2/L3 VPN) based on rules established by the operator.
Health Insights	6.0	Performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. It builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.
Change Automation	6.0	Automates the process of deploying changes to the network.

Component	Version	Description
Crosswork Data Gateway	6.0	A secure, common collection platform for gathering network data from multi-vendor devices that supports multiple data collection protocols including MDT, SNMP, CLI, standards-based gNMI (dial-in), and syslog.
Zero Touch Provisioning	6.0	Automatic onboarding of new IOS-XR and IOS-XE devices and provisioning of Day0 configuration, resulting in faster deployment of new hardware at a lower operating cost.

Some of Cisco Crosswork Network Controller's functionality is enabled by the following products:

Table 2:

Products	Version	Description
Cisco Network Services Orchestrator	6.1.4	An orchestration platform that makes use of pluggable function packs to translate network-wide service intent into device-specific configuration. Cisco NSO provides flexible service orchestration and lifecycle management across physical network elements and cloud-based virtual network functions (VNFs), fulfilling the role of the Network Orchestrator (NFVO) within the ETSI architecture. It provides complete support for physical and virtual network elements, with a consistent operational model across both. It can orchestrate across multi-vendor environments and support multiple technology stacks, enabling extension of end-to-end automation to virtually any use case or device. **Note** Function Packs are required to support compatibility with certain applications.
Cisco Segment Routing Path Computation Element (SR-PCE)	7.11.1	An IOS-XR multi-domain stateful PCE supporting both segment routing (SR) and Resource Reservation Protocol (RSVP). Cisco SR-PCE builds on the native Path Computation Engine (PCE) abilities within IOS-XR devices, and provides the ability to collect topology and segment routing IDs through BGP-LS, calculate paths that adhere to service SLAs, and program them into the source router as an ordered list of segments.

Cisco Crosswork Network Controller Packages

Cisco Crosswork Network Controller solution is distributed as two packages (Essentials and Advantage) with additional add-on services.

Table 3: Cisco Crosswork Network Controller Packages

Package	Contents	Version
Cisco Crosswork Network Controller Essentials	• Element Management Functions (EMF) • Provisioning • Visualization • Path Compute • Traffic Engineering • Optimization	6.0
Cisco Crosswork Network Controller Advantage	• Service Health Monitoring[1]	6.0

[1] To install Service Health, the Crosswork Network Controller Essentials package must be installed before you can install the Advantage package.

Table 4: Cisco Crosswork Network Controller Add-On Services

Contents	Description	Version
Change Automation	An application that automates the process of deploying changes to the network. Orchestration is defined via an embedded Ansible Playbook and then configuration changes are pushed to Cisco Network Services Orchestrator (NSO) to be deployed to the network.	6.0
Health Insights	An application that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. Cisco Crosswork Health Insights enables programmable monitoring and analytics, and builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.	6.0
Zero Touch Provisioning	An application that streamlines on-boarding and provisioning of Day 0 configuration resulting in faster deployment IOS-XR and IOS-XE devices at a lower operating cost.	6.0

What's New

The following tables list the primary new features and functionality introduced in Cisco Crosswork Network Controller 6.0:

• Table 5: Traffic Engineering

- Table 6: Service Health
- Table 7: Topology
- Table 8: Crosswork Data Gateway
- Table 9: Infrastructure
- Table 10: Documentation

Table 5: Traffic Engineering

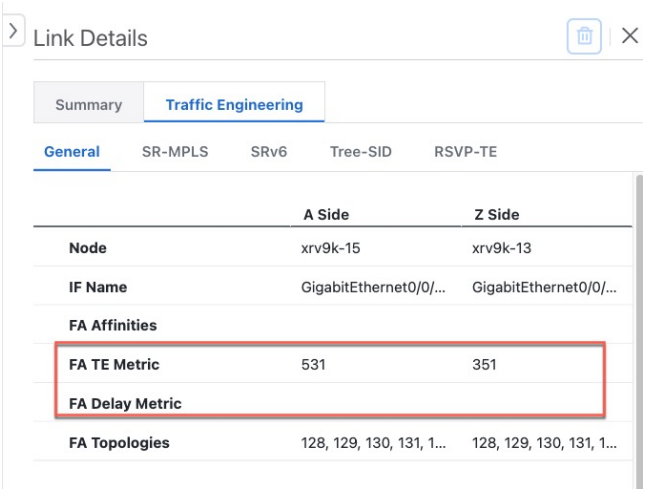
Feature	What's New?
Local Congestion Mitigation (LCM) feature pack	• Automated Mode—This option allows LCM to automatically deploy TE tunnel recommendations based on thresholds that you configure. **Note** Automated mode is accessible through Limited Availability. Engage your account team for further details. • Manual Mode (default)—This option, which was available in previous releases, requires a user to view the LCM Operational Dashboard and decide whether to commit TE tunnel recommendations. • Pause Mode—This option can pause LCM operations on a particular interface when LCM is in either Automated or Manual mode. Pausing operations in Automated mode are necessary in cases where deployed solutions do not result in the intended resolution, there is uneven ECMP traffic, there are policies that are not carrying traffic, or when an interface is continuously throttling between different solutions. **Note** Pausing LCM operations removes all existing TE policies that were deployed for that interface.

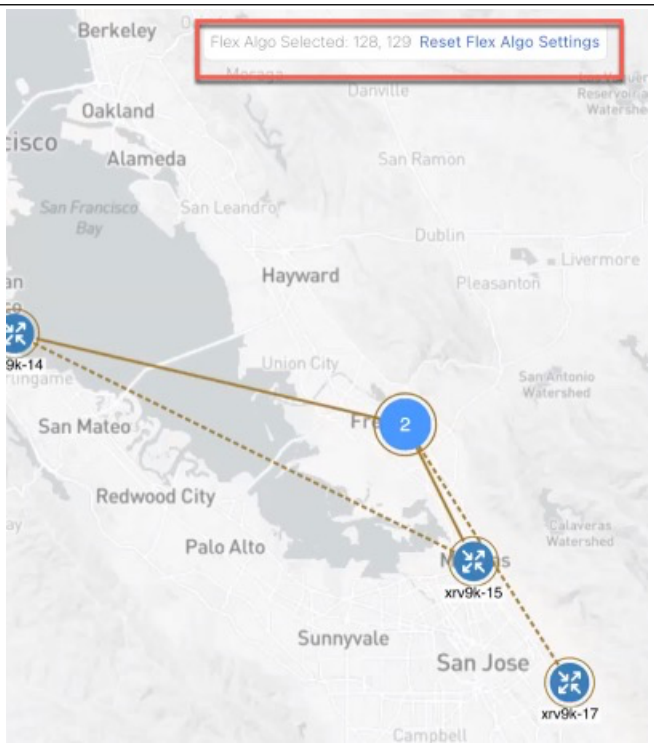
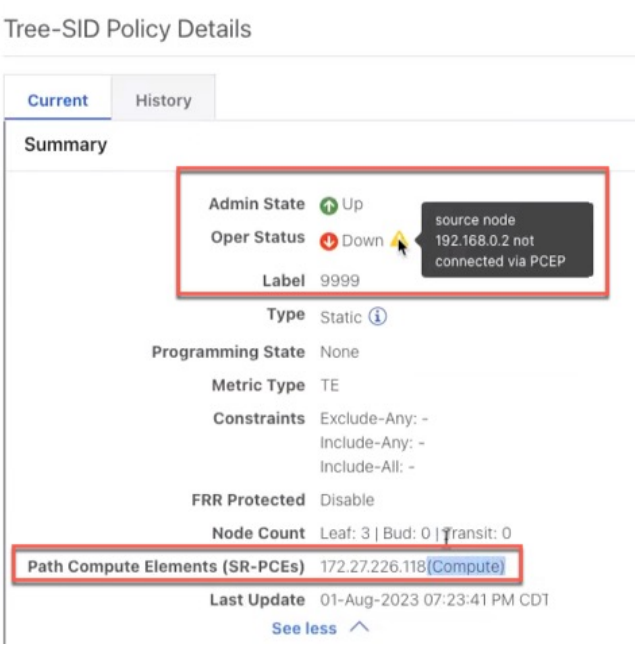
Feature	What's New?

SR Circuit Style Manager (CSM) feature pack	• Hop count is now available as a metric type when computing SR-TE Circuit Style policies.
	• In response to feedback from customers, we have changed some events to alarms. For example, an alarm is triggered when policy traffic exceeds the reserved bandwidth pool size or threshold.
	• APIs:
	  • RESTCONF APIs—Manually re-optimize (single or multiple) SR-TE Circuit Style policies. These APIs can be initiated after network topology changes.
	  • CSPolicyPathsOnLinks—Lists Circuit Style SR-TE policies on a specified link and filtered by its operational state (up,down,active, and unknown) of the specified policies.
	  • AllCSPolicyPaths—Lists Circuit Style SR-TE policies filtered by its operational state and if it has hops (segment lists).
	  • CSPolicyPathsonNode—Lists all Circuit Style SR-TE policies on specified nodes filtered by its operational state (up,down,active, and unknown).
	To view API documentation, see Cisco Devnet.

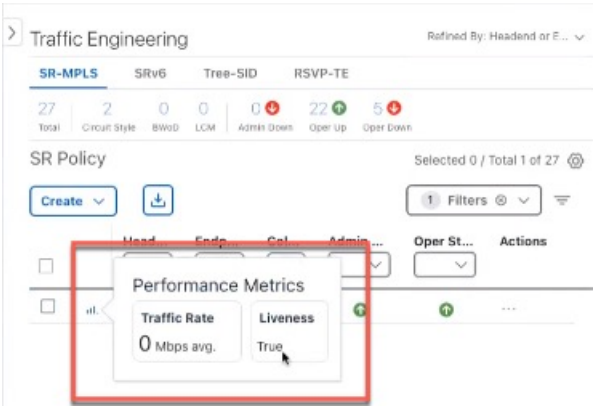
Bandwidth on Demand feature pack	• In previous releases, BWoD required protected adjacency SID constraints. Now user can elect BWoD to prefer to use protected (default option) or unprotected adjacency SIDs. • The Policy Violation now has two options: Strict or Loose. • The process of changing delegation from one PCE to another has been improved to guarantee a clean transfer of PCE roles. • Enhanced batch processing of queued BWoD policy computations. The queue is initially cleared prior to running a list of new pending delegations/undelegations instead of running each delegation one at a time.

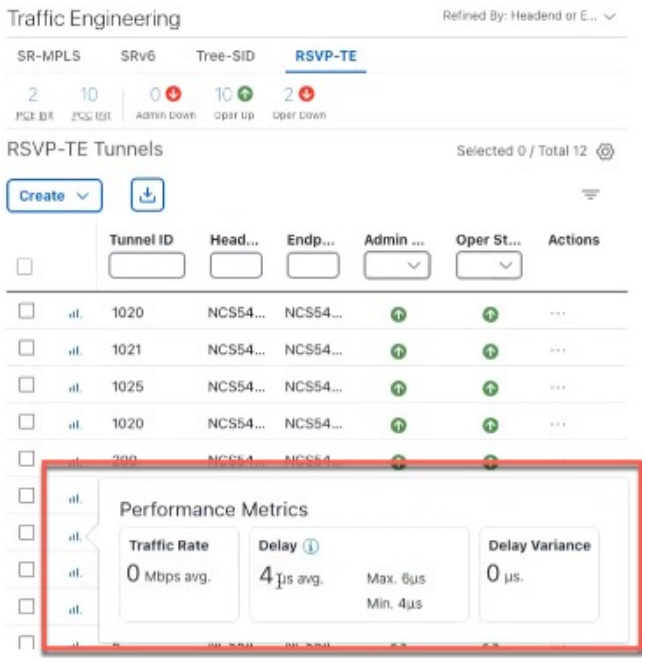
Feature	What's New?
Flexible Algorithm	

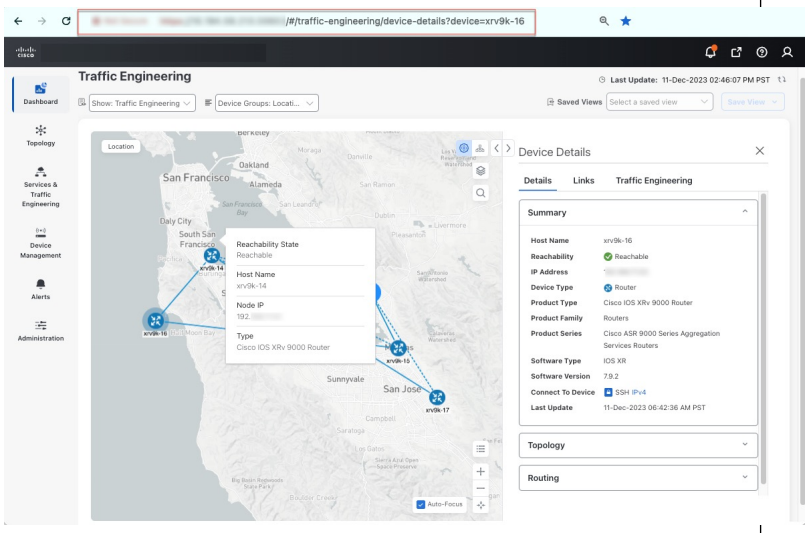
Feature	What's New?
	• You can now view Application-Specific Link Attribute ASLA Flexible Algorithm metrics (TE and Delay) in the link details: **Note** ASLA is supported on PCC and core routers that are Cisco IOS XR 7.4.1 or later versions. 1. From the Traffic Engineering topology map, click on a participating Flex Algorithm link. 2. From the Links page, click ***Link_Type_entry*** > **Traffic Engineering** tab > **General**. For example:  • An overlay on the topology map has been added when Flexible Algorithms are selected. This is to help identify which Flexible Algorithms are selected more easily. For example:

Feature	What's New?
	
Tree-SID	PCE warnings and path compute elements are displayed in Tree-SID policy details: 

Feature	What's New?
Performance Metrics of TE policies	

Feature	What's New?
	When Service Health is installed and SR-PM collection is enabled, you can view KPI metrics (Delay, Jitter, and Liveness) from the Traffic Engineering table or from the TE tunnel details. To view the KPI metrics for the policy: 1. Configure SR-PM on the device from the policy provisioning page (**Services & Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** or **RSVP** tab. Locate the policy you are interested in from the policy table and click > **performance metrics**). **Note** You can configure Delay or Liveness (not both) manually on the device. See the device platform documentation for information. For example: Segment Routing Configuration Guide for NCS 540 Series Routers. 2. Enable SR-PM collection in **Performance Metrics Settings** (**Administration** > **Settings** > **System Settings** tab > **Performance Metrics**). **SR-MPLS policies** KPI metrics contain Delay, Delay Variance (Jitter) or Liveness (Boolean value) along with traffic utilization. For example: ***Figure 1: SR-MPLS Policy Performance Metrics in the Traffic Engineering Table***  **RSVP-TE Tunnel** KPI metrics include Delay and Delay Variance (Jitter) along with Utilization. For example: ***Figure 2: RSVP TE Tunnel Performance Metrics in the Traffic Engineering Table***

Feature	What's New?
	
Asymmetric delay for links	In previous releases, only one side of the link delay value for an interface was considered during computation. When you configure delays on both remote and local nodes, the calculation of each delay on each interface is now taken into consideration when computing a path. **Note** To configure link delay over an interface, refer to the device platform configuration guide. For example, Segment Routing Configuration Guide for Cisco NCS 540 Series Routers.

Feature	What's New?
Unique TE tunnel and device detail URLs	TE tunnel or device details are now assigned unique URLs that can be shared. The URL sends the user to the Policy or Device Details page after logging in. • SR-MPLS, SRv6, Tree-SID, and RSVP-TE tunnels —From the Traffic Engineering table, click **Actions > View Details** for a particular row. • Devices—From the Traffic Engineering topology map, click on a device. 
Increased performance and memory footprint	Improvements made in topology discovery time, network model building, and processing cache, bandwidth, metric, and TE tunnel type information.

Feature	What's New?
Transport Slicing	

Feature	What's New?

	Cisco Crosswork Network Controller offers direct support for network slicing at the transport level. This slice “instance” is a unique slice provisioned in the network but with a set of Service Level Requirements chosen from a set of pre-created Network Slice Templates (NST). The Slice Management Function (SMF) in turn communicates with each sub-domain controller, called a Network Slice Subnet Management Function (NSSMF) which in turn provisions the corresponding domain specific slice instance across its own sub-domain boundaries (called a Network Slice Subnet Instance (NSSI)) using a similar set of domain specific Network Slice Subnet Templates (NSST).
	
	Cisco Crosswork Network Controller also offers:
	• Slice design and deployment from the perspective of two user persona: Slice Designer and Slice Instance Requester.
	• Deploying the Slice Catalog using the new slice template UI.
	  • Adding Service Assurance into the catalog using the NSO CLI.
	• Requesting a new Slice Instance by picking intent from the catalog using IETG Slice YANG model, select endpoints and submit.
	  • You can deploy a slice instance after providing information, in the UI, after following four easy steps.
	• Automated slice instance deployment:
	  • QoS: The Slicing CFP will apply input and output QoS policy maps on all slice endpoint interfaces (policy-maps pre-deployed). Both L2 & L3 QoS supported.
	  • Path Forwarding: The Slicing CFP will deploy SR-TE ODN templates on all head-ends (metrics= latency, igp, TE, BWoD, FA, etc). Additionally, it will set BGP color community accordingly on all slice advertised VPN prefixes.
	  • Service Assurance: The Slicing CFP will setup:
	  1. Cisco Crosswork Network Controller Heuristic packages for Cisco Crosswork Network Controller Automated Assurance/Service Health.
	  2. Configure Y1731 probing for P2P L2 slices.
	  3. Configure SR-PM probing for delay and liveness on all slice SR-TE tunnels.
	  • Connectivity: The Slicing CFP will use the L2/L3VPN IETF NM to setup L3 or L2 connectivity automatically across defined slice endpoints. All VPN parameters inferred and abstracted.

Feature	What's New?
	• Setup eVPN VPWS for P2P L2 slices. • Setup eVPN any-to-any or hub-spoke for L2 multipoint or L3 multipoint slices. • Setup up "extranet" connectivity between dedicated and shared slice types. (more on this later). • Setup PE-CE eBGP for L3 based slices. **Note** If you are creating an L2 point-to-point transport slice, prerequisites include the following: (a) The route-policy needs to be configured on the PE nodes (for example: L2-ATTACH). (b) In global-settings on NSO, configure this sample command: `set network-slice-services global-settings parent-rr-route-policy L2-ATTACH`. • Using the UI, visualize the slice components: VPN, Transport, Health: • Display a slice on the map. • View Slice and VPN view along with Shared Slices and CE (Neighbor) connected in Logical View. • Visualize Shared Slices associated to dedicated slice. • From the VPN list, display VPN details including Assurance data if monitoring is enabled. • From the Transport list, display SR TE details including SR-PM data if SR-PM is enabled. • Using Health details, view symptom details and any failed subexpressions and metrics (which will provide information on any active symptoms and root causes).

Table 6: Service Health

Feature	What's New?
Introduced a new monitoring status - Monitoring Error	Errors due to a component failures, operational errors or device errors are now displayed as **Monitoring Errors** on the UI. You can filter these errors using the mini-dashboard or the filters.

Feature	What's New?
Ability to rate-limit monitoring requests	To efficiently manage service monitoring requests, Service Health has implemented a rate-limiting process. This means that there may be a delay in publishing service monitoring requests if the number of requests raised per minute exceeds a specific threshold. The thresholds are defined as follows: • Basic monitoring requests – 50 services per minute • Advanced monitoring requests – 5 services per minute • Delete monitoring requests – 30 services per minute The rate-limiting process also extends to the monitoring data, that is metrics and Events of Significance (EOS), sent by Crosswork Data Gateways to the Crosswork Tracker component. For example, during a restore process, when all Crosswork Data Gateways send metrics again to the Crosswork Tracker component, the rate at which the Crosswork Tracker processes this data and forwards it to Assurance Graph Manager is regulated. This may lead to a delayed reporting of Events of Significance (EOS) following the restore. In the event of delays, an event is triggered with a severity level of 'Warning' and a corresponding description to notify you of the delay. The event is cleared once Service Health resumes normal publishing of monitoring requests.
Ability to monitor performance metrics of TE policies using SR-PM	To measure the performance metrics of VPN services using the SR-MPLS or RSVP-TE Traffic Engineering policies, Service Health leverages Segment Routing Performance Measurement (SR-PM). This feature enables measuring metrics on the underlay SR-TE policy to enforce Service Level Agreements in VPN services.
Monitor service health with external probes from Accedian Skylight	Crosswork Network Controller can leverage external probing, provided by Accedian Skylight, to measure metrics of the network services. The metrics are compared with the contracted SLA (defined in the Heuristic package), and the results are made available on the Crosswork Network Controller UI. After an L3VPN service is provisioned and service monitoring is enabled, the probe intent and probe topology are learned (from provisioned service) and a probe session to monitor the service starts automatically by invoking relevant RESTConf APIs. Service Health processes the metrics and raises symptoms as needed to be displayed on the UI. You can view historical data for upto 24 hours from the Probe Sessions. The maximum number of probe sessions per service are capped at 200 (for all connection types). **Note** Accedian Skylight integration is available as a limited-availability feature in this release. Engage with your account team for more information.

Table 7: Topology

Feature	What's New?
Simplified Topology Rebuild Tool	If the topology is not displaying status as expected, you can now place the system into maintenance mode and then choose to rebuild the topology. This will force the system to create a new topology model and avoid the complicated steps from previous versions. **Note** Only users with write permission can Rebuild Topology.

Table 8: Crosswork Data Gateway

Feature	What's New?
Ability to reattempt the import of Controller Certificate file	When Crosswork Infrastructure and Crosswork Data Gateway are deployed simultaneously, on the first reboot Data Gateway attempts to the download the Controller Certificate file from Crosswork Infrastructure. If the Infrastructure deployment is in-progress, Crosswork Data Gateway may not find the certificate. In the past, you had to wait for the Data Gateway VM to restart before downloading the certificate through the Interactive Console menu. With Crosswork Data Gateway's latest release, you can let Data Gateway retry the certificate download multiple times. If the file download fails, the Crosswork Data Gateway will now retry automatically. For information on importing the certificate, see the *Import Controller Signing Certificate File* section in Cisco Crosswork Network Controller 6.0 Installation Guide.
Parameter to configure the CLI session timeouts for devices	The **SSH Session Timeout** parameter is implemented to indicate the duration of the CLI connection on a device. For information on how to configure the **SSH Session Timeout** parameter, see the *Configure Crosswork Data Gateway Global Parameters* section in Cisco Crosswork Network Controller 6.0 Administration Guide.
Changes to the Crosswork Data Gateway APIs	The Crosswork Data Gateway APIs have been altered in the following ways: • The new dg-manager APIs are compatible with the OpenAPI v2/v3 specification. • The change logs include the deprecated APIs. In the subsequent release, the deprecated APIs are removed. • A change log is created for each modified API. The change log includes the APIs that have been deprecated, removed, or updated. For information on change logs, see Cisco Devnet.

Feature	What's New?
NETCONF Collector support is decommissioned	The NETCONF collector enabled data collection over the NETCONF protocol. Support for the NETCONF collector has been discontinued in configurations, such as the base VM, application layer, Docker, and dg-manager.

Table 9: Infrastructure

Feature	What's New?
Device Level RBAC	This release introduces role-based access control (RBAC) at a device granularity for provisioning and device configuration workflows. Each user must be assigned a role that determines what functions they can access along with a Device Group that determines on which devices they can manage or deploy services. For more information, see the *Manage Device Access Groups* section in the Cisco Crosswork Network Controller 6.0 Administration Guide.
Geo Redundancy	This release introduces the first phase of the geo redundancy solution for Crosswork Network Controller and its components in case of a region or data center failure. For more information, see the *Enable Geo Redundancy* section in the Cisco Crosswork Network Controller 6.0 Installation Guide. **Note** Geo Redundancy is accessible through Limited Availability. Engage your account team for further details.

Table 10: Documentation

Feature	What's New?
Documentation	• An Information Portal is now available for Crosswork Network Controller 6.0. Information is categorized per functional area, making it easy to find and easy to access. • Cisco Crosswork Network Controller 6.0 Service Health Monitoring is a new Crosswork Network Controller specific guide that provides information on monitoring the health of L2VPN and L3VPN services. It provides insights into analyzing and troubleshooting degraded services, as well as visualizing service health status and logical dependency trees. • Cisco Crosswork Network Controller 6.0 Traffic Engineering and Optimization is a new Crosswork Network Controller specific guide that provides information on how to visualize and configure traffic engineering in Crosswork Network Controller. • Cisco Crosswork Network Controller 6.0 Network Bandwidth Management is a new Crosswork Network Controller specific guide that provides information on how to use Crosswork Network Controller feature packs. Feature packs are tools that tackle congestion mitigation and the management of SR-TE policies to find and maintain intent based bandwidth requirements.

Compatibility Information

The following table lists hardware and software versions that have been tested and are known to be compatible with Cisco Crosswork.

Table 11: Cisco Crosswork Infrastructure Support

Software	Supported Version
Cisco Operating System **Note** This is an application-level compatibility.	• Cisco IOS XR: 6.7.2, 7.0.2, 7.1.2, 7.2.1, 7.3.1, 7.3.2, 7.4.1, 7.4.2, 7.5.2, 7.6.1, 7.7.1, 7.8.1, 7.8.2, 7.9.1, 7.9.2, 7.10.2, 7.11.1 • Cisco IOS XE: 17.6.3, 17.7.1, 17.8.1, 17.9.1, 17.12.1 • Cisco NX-OS: 9.2.1, 9.3.1, 10.2(3)
Hypervisor and vCenter	• VMware vSphere 6.7 or above. • VMware vCenter Server 7.0 and ESXi 7.0. • VMware vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 (Update 1 or later).

Software	Supported Version
Browsers	• Google Chrome—119 or later • Mozilla Firefox—120 or later
Cisco Crosswork Data Gateway	• 6.0
Cisco Network Services Orchestrator (Cisco NSO)	• 6.1.4

	Cisco Network Element Driver (NED)
	• Cisco IOS XR:
	  • CLI: 7.52.2
	  • NETCONF: 7.3.2, 7.4.2, 7.5.2, 7.6.2, 7.7.2, 7.8.2, 7.9.2, 7.10.1, 7.11.1.49I ENG
	• Cisco IOS XE:
	  • CLI: 6.100
	Note Additional function packs may be required based on the applications and features being used. See the Crosswork Network Controller 6.0 Installation Guide for details.

Cisco Segment Routing Path Computation Element (SR-PCE)	• Cisco IOS XR 7.11.1

Many features on Crosswork Network Controller depend on the underlying router XR/XE versions and the SR-PCE software. In the below table, you can review those that are supported and working in combination with software versions on router platforms and SR-PCE.

Table 12: Cisco IOS Software Version Support

Operating System	Version	PCE-Init	PCC-Init	NSO + CFP CLI	NSO + CFP NETCONF	Crosswork Infrastructure	Optimization Engine	ZTP (Secure)[2]	Service Health
IOS-XR	6.7.2	✓	✓	✓	✗	✓	✓	✗	✗
	7.0.2	✓	✓	✓	✗	✓	✓	✗	✓
	7.1.2	✓	✓	✓	✗	✓	✓	✗	✓
	7.2.1	✓	✓	✓	✗	✓	✓	✗	✓
	7.3.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.3.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.4.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.4.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.5.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.6.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.7.1[3]	✓	✓	✓	✓	✓	✓	✗	✓
	7.8.1	✓	✓	✓	✓	✓	✓	✓[4]	✓
	7.8.2	✓	✓	✓	✓	✓	✓	✓[5]	✓
	7.9.1[6]	✓	✓	✓	✓	✓	✓	✓[7]	✓
	7.9.2[8]	✓	✓	✓	✓	✓	✓	✓[9]	✓
	7.10.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.11.1	✓	✓	✓	✓	✓	✓	✓	✓
IOS-XE	17.6.3	✓	✓	✓	✗	✓	✓	✓	✗
	17.7.1	✓	✓	✓	✗	✓	✓	✗	✗
	17.8.1	✓	✓	✓	✗	✓	✗	✗	✗
	17.9.1	✓	✓	✓	✗	✓	✓	✓	✓
	17.12.1	✓	✓	✓	✗	✓	✓	✓	✓

[2] Classic ZTP supports all IOS-XR versions found in the table.
[3] Not supported on Cisco ASR 9000 (32-bit)
[4] Only Secure ZTP config download is supported.
[5] Only Secure ZTP config download is supported.
[6] As SMUs become available, this document will be updated.
[7] Only Secure ZTP config download is supported.
[8] As SMUs become available, this document will be updated.
[9] Only Secure ZTP config download is supported.

Note Software Maintenance Updates (SMUs) are required for both PCC/Headend and SR-PCE versions indicated in the table. To download the Cisco IOS XR versions and updates, see the IOS XR Software Maintenance Updates (SMUs) document.

Traffic Engineering Compatibility Information

The following table details Traffic Engineering and Network Bandwidth Management support for IOS Versions, SR-PCE, and Cisco devices.

Cisco IOS Support

We recommend that the SR-PCE version you use be equal to or higher than the PCC software version. PCC 7.11.1 is recommended and has been validated to work with Traffic Engineering 6.0 features. Other listed PCC versions are supported, but may not support all Traffic Engineering features because of PCC version limitations.

Note Software Maintenance Updates (SMUs) are required for both PCC/Headend and SR-PCE versions indicated in the table. To download the Cisco IOS XR versions and updates, see the IOS XR Software Maintenance Updates (SMUs) document. The correct SMUs to download will have "Optima" or the bug ID appended to the filename. For example: `asr9k-x64-7.3.2.Optima.tar` or `xrv9k-7.3.2.CSCvy63506.tar`.

Table 13: Traffic Engineering 6.0 Support for SR-PCE 7.11.1 (by Cisco IOS Version and Headend Router Type)

Cisco IOS XR	Cisco ASR 9901 (64-bit)	Cisco XRv 9000[10]	Cisco 8000 series	Cisco NCS 5500 series	Cisco NCS 540 series[11]	Cisco NCS 560 series
7.3.1	✓	✓	✗	✓	✓	✓
7.3.2	✓	✓	✗	✓	✓	✓
7.4.1	✓	✓	✗	✓	✓	✓
7.4.2	✓	✓	✗	✓	✓	✓

Cisco IOS XR	Cisco ASR 9901 (64-bit)	Cisco XRv 9000[10]	Cisco 8000 series	Cisco NCS 5500 series	Cisco NCS 540 series[11]	Cisco NCS 560 series
7.5.2	✓	✓	✓	✓	✓	✓
7.6.1	✓	✓	✗	✓	✓	✓
7.7.1	✓	✓	✓	✓	✓	✓
7.7.2	✓	✓	✓	✓	✓	✓
7.8.1 + SMU (CSCwc93705)	✓	✓	✓	✓	✓	✓
7.8.2	✓	✓	✓	✓	✓	✓
7.9.1	✓	✓	✓	✓	✓	✓
7.9.2	✓	✓	✓	✓	✓	✓
7.10.2	✓	✓	✓	✓	✓	✓
7.11.1	✓	✓	✓	✓	✓	✓

[10] The SR-PCE may be deployed on XRv9000 (VM or appliance).

[11] The SMU is available via the Cisco NCS 540-ACC-SYS Router or Cisco NCS 540x-ACC-SYS Router Software Download Center.

Cisco IOS XE Version	Cisco ASR 920	Cisco ASR 903 RSP 3
17.4.1[12]	✓	✗
17.5.1	✓	✓
17.6.3	✓	✗
17.7.1	✓	✓
17.8.1	✓	✓
17.9.1	✓	✓
17.12.1	✓	✓

[12] Supports only PCE- initiated SR-TE policy deployment.

Note

- Segment Routing Traffic Matrix (SRTM) is only available in Cisco ASR 9000 devices.
- SRv6 and Visualizing Native Path (Path Query) features are supported from PCC IOS XR 7.3.2 or later.
- Local Congestion Mitigation is supported from:
  - PCC IOS XR 7.3.2 and above for NCS 5500, NCS 560, and NCS 540
  - PCC IOS XR 7.4.1 (ASR 9000)
  - PCC IOS XR 7.5.2 and 7.7.1 for Cisco 8000
  - PCC IOS XE 17.05.1 or 17.05.1 (ASR 920/903 RSP 3)

Scale Support

To support large scale deployment, the applications that make up Cisco Crosswork Network Controller (Optimization Engine, Active Topology, and other applications) are built with workload and endpoint load balancing using the Crosswork infrastructure's cluster architecture.

Table 14: Scale Support

Feature	Scale Support
Devices	25,000
Total Interfaces[13]	500,000[14]
Provision of SR-TE policies and RSVP-TE tunnel (PCE-initiated)	150,000
IGP links	200,000
VPN Services (L2VPN, L3VPN)	300,000

[13] This is the total number of interfaces that Cisco Crosswork can receive and process.
[14] This number has been validated with a total collection load of 650,000 interface entries across 25,000 devices (with 150,000 entries filtered out in the CDGs based on interface type). The number of CDG VMs can be increased to support higher collection loads.

Note Scale numbers will reduce if Layer 2 collection is enabled (for example, when LLDP, CDP, or LAG collection is enabled).

Note The Crosswork Network Controller Essentials package requires a minimum of 3 Virtual Machines (VMs) and the Crosswork Network Controller Advantage package requires a minimum of 5 VMs. For more information, see the Crosswork Network Controller Installation Guide.

Networking Technology Support for Traffic Engineering

The following is the networking support information for SR-PCE 7.11.1.

Table 15: Supported Features

Category	Description	Notes / Details
SR	SR-MPLS PCE initiated policies	Policies that are provisioned or discovered by Cisco Crosswork.
SR	PCC initiated policies and ODN policies	Policies that are discovered by Cisco Crosswork.
SR	Explicit path SR-TE policies	Policies that are PCC initiated (SID list with labeled SID list with addresses), PCE reported, PCE initiated. Includes SRv6 TE discovery of PCC initiated policies.
SR	Dynamic path SR-TE policies	PCC computed, PCE reported, PCE delegated
SR	Single consistent Segment Routing Global Block (SRGB) configured on routers throughout domain covered by Cisco Crosswork	—

Category	Description	Notes / Details
SR	Egress Peer Engineering (EPE) PeerAdjacency SIDs, PeerNode SIDs	• EPE must be configured on both ends of the eBGP link to appear in Cisco Crosswork. • EPE PeerAdjacency SIDs and PeerNode SIDs are represented as individual links in the Crosswork UI between the corresponding Autonomous Systems border routers (ASBR). **Note** EPE PeerNode SIDs are identified by the Border Gateway Protocol Router ID (BGP RID) Loopbacks as the A and Z side link interfaces. • Labels for both types of EPE SIDs, are shown as adjacency SIDs in the Cisco Crosswork UI.
SR	Prefix SID	Regular/Strict Node SIDs + FA. Includes SRv6 Locators.
SR	Adjacency SID	B-flag (protected/unprotected), P-flag (Persistent). Includes SRv6 Locators.
SR	SR policy optimization objective min-metric (IGP, TE, and Latency)	PCE initiated provisioning and PCC initiated discovery

Category	Description	Notes / Details
SR	SR policy path constraints (affinity and disjointness, protected segments)	• Only 2 SR-MPLS policies per disjoint group or sub-id are supported. Disjoint Types: link, node, srlg, srlg-node. • Only 32-bit affinities supported. EAG (RFC 7308) is not reported by PCE and not visualized by Cisco Crosswork.
SR	Binding SID for explicit or dynamic policies	Discovered for PCC initiated and PCE initiated policies. It is configurable for PCE initiated policies.
SR	Profile ID (Discovered and configurable for PCE-init)	Parameter used for applying features on PCC to PCE initiated policies.
SR	Flexible Algorithm (Flex Algo) for SR-MPLS and SRv6 policies	• Discover and visualize node Flex Algo participation. • Discover and visualize Flex Algo definitions. • SR policy IGP path respecting Flex Algo associated with prefix SIDs. • Displays pruned topology participating in FlexAlgo. • Preview and provision PCE initiated SRTE policies with a SID-Algo constraint.
SR	Discovery and visualization of multiple candidate paths	—
SR	Binding SIDs as Segment List Hops for SR policies	Discovery and visualization of PCC initiated policies.
SR	Tree-SID	Visualization and provisioning of PCE initiated policies.
SR	SR policies with Loopback IPs (Prefixes) other than TE router ID for headend/endpoint and prefix SIDs in segment list	Prefix (node) SIDs associated with specific IGP domain / area.

Category	Description	Notes / Details
SR	Maximum SID Depth (MSD)	• Per-node Base MPLS imposition MSD discovered via IGP/BGP-LS. • Per-node MSD discovered via PCEP session info. • Per-policy MSD.
SR	Global Max Latency	Configured on PCE and applied to all PCE delegated SRTE policies with a latency metric.
SR	Inter-domain SRTE policies (inter-IGP domain, inter-AS)	PCE delegated and Bandwidth on Demand policies.
SR	Node SID reuse across different IGP domains	Recommended to not reuse node SIDs in adjacent IP domains. Inter domain explicit path policies with a label-only hop that is a node SID used in adjacent domains may be unresolvable if hop after ABR hop.
SR-IGP	Application-Specific Link Attribute (ASLA) Delay / TE metric	Crosswork collects and uses ASLA delay and TE metric in Flex Algo topology computations and SRTE policy IGP paths.
SR-IGP	Visualizing native SR-IGP path	Path Query OAM feature to use traceroute on device to report actual SR-IGP multi-paths to destination node ***(SR-MPLS only)***
SR	Dynamic Circuit Style	Path computation and bandwidth reservation through the Circuit Style feature pack.
RSVP	PCE initiated tunnels (provisioned by or discovered by Cisco Crosswork), PCC initiated tunnels discovered by Cisco Crosswork	—
RSVP	ERO strict hops, ERO loose hops (PCC initiated only)	—
RSVP	FRR protection on Cisco Crosswork provisioned tunnels	—
RSVP	Path optimization objective min-metric (IGP|TE|Latency)	—

Category	Description	Notes / Details
RSVP	Path constraints (affinity, disjointness)	Only 2 RSVP tunnels per disjoint group or sub-id
RSVP	Binding Label (explicit | dynamic)	—
RSVP	Signaled Bandwidth	—
RSVP	Setup and Hold Priority	—
RSVP	Path Protection (partial support)	Paths discovered as independent tunnels if multiple paths are up. Cisco XR only reports active path. Other vendors may report all active paths.
PCEP	PCEP Session discovery	Each PCEP session a PCC has with a PCE along with its details is displayed as part of node details
IPv4/IPv6	Dual Stack IPv4 or IPv6	Nodes can be IPv4, IPv6 or IPv4/IPv6 capable
IPv4	Unnumbered Interfaces (partial)	Topology discovery, SR policies with unnumbered IF hops discovery/provisioning, LCM policy support
IPv6	IPv6 Link Local Interfaces	Discovery of IPv6 link local interfaces as part of topology and as a hop in an SRv6 TE policy
IPv6	IPv6 Router ID	Nodes with IPv6 and IPv6 Router ID only with support for SRv6 only

Table 16: Unsupported Features and Limitations

Category	Description	Notes / Details
SR	Provisioning multiple candidate paths via Cisco Crosswork	—
SR	Per-Flow Policies (PFP)	PFP (ODN or manually configured) not supported in PCEP. This PFP is the mapping of forward class to PDP with matching color and EP. Underlying PDP is reported as normal.

Category	Description	Notes / Details
SR	Multiple segment lists per candidate path	This configuration is not supported in Crosswork. These segment lists will not be discovered if configured on a PCC. High level requirements: • Discover multiple segment lists (with weights) per policy (TopoSvc, PCE, PCC) • Provision multiple segment lists (with weights) per policy (UI, PCED, PCE, PCC) • Visualize including showing IGP paths (UI, OE) • Compute paths of policies with multiple segment lists for LCM (OE, LCM)
SR	Anycast SIDs	—
SR	SR policy provisioned (SR-PCE initiated) with IPv6 endpoints or hops	—
SR	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	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	Heterogeneous SRGBs	Different SRGBs configured on nodes are not supported. SRGB must be configured to ensure proper discovery and visualization of SR policy paths.
SR	Egress Peer Engineering (EPE) Peer Set SIDs	No discovery
SR	Routers that are not SR-capable	All nodes assumed SR capable when computing SR policy IGP paths. LCM and BWoD SR policy path computation will not exclude non-SR capable nodes in IGP path.

Category	Description	Notes / Details
SRv6	PCE initiated provisioning of SRv6 policies is not supported.	—
SRv6	Traffic collection on SRv6 policies is not currently supported.	Requires telemetry (gNMI) for policy counters (no SNMP support)
IGP	ISIS Overload bit	Affects IGP paths for all policies and PCE path computation (BWoD, LCM). PCE reports but does not process.
IGP	OSPF MADJ Interfaces	No support for discovering OSPF Multi-area adjacencies
IGP	Multiple IGP instances on same interface	Single interface that participates in multiple IGP instances are not supported.
IGP	Cisco Crosswork supports L1 or L2 adjacencies on links but not both on the same link.	—
RSVP	Configuring loose hop Explicit Route Object (ERO) in Crosswork	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 loopbacks, unexpected behavior may occur
RSVP	Named tunnels configured on PCCs	Required for Juniper RSVP HEs
RSVP	Tunnels with Loopback IPs other than TE router ID for headend/endpoint and path hops	—
RSVP	Display of active FRR protected path in UI	Cisco Crosswork will discover FRR tunnels which are displayed in UI but will not associate an actively protected tunnel with the FRR tunnel. Path in UI will not include FRR protected path when protection is active.
RSVP	P2MP tunnels	—
RSVP	Path protected RSVP LSPs	No association between paths discovered.

Category	Description	Notes / Details
LDP	Local Congestion Mitigation (LCM) in Mixed SR/LDP networks	LCM will not work in a mixed SR/LDP network with PEs that are LDP only. LDP traffic destined to the LDP-only egress PE attempted to be steered into Autoroute LCM tactical polices will be blackholed
IPv4	IPv4 Unnumbered Interfaces	BWoD, Circuit Style Support, and RSVP
IPv4/IPv6	Secondary IP addresses for interfaces	Not supported. Unpredictable behavior if discovered.
IPv4/IPv6	Overlapping IP addresses in different IGP domains	IP addresses for IGP interfaces and nodes (router-ids) are assumed to be unique across all domains
IPv6	IPv6 Router ID	SR and RSVP not supported (SRv6 only)

Important Notes

Take into consideration the following important information before starting to use Cisco Crosswork Network Controller 6.0.x:

- **Crosswork Infrastructure:**
  - It is recommended to deploy Crosswork on a highly available cluster with shared storage.
  - Managed devices, VM host, VMs, and all integrated components should use the same NTP source to avoid time synchronization issues.
  - Confirm that the DNS and NTP servers are properly configured and reachable on the network the Crosswork cluster will be using.
  - Cisco recommends using Terminal Access-Control System Plus (TACACS+), Lightweight Directory Access Protocol (LDAP) or Role-Based Access Control (RBAC) to track access and prevent unauthorized usage of Crosswork capabilities.
  - During configuration, note the Cisco Crosswork UI and CLI user names and passwords. Due to added security, the only way to recover the administrator password is to re-install the software.
  - In situations where it is expected to work with SR-PCE (for L3 topology discovery), we recommend the use of dual SR-PCEs in an HA configuration.
  - Use CSV files to quickly import and on-board device, credential, and provider information.
- **Obtaining Geomaps for topology map renditions:**

  Cisco Crosswork Network Controller allows users to obtain downloadable geographical maps (geomaps) based on their specific topology mapping needs. If your environment allows contact with the map provider website we specify in Crosswork, you do not need to download the map files. If your environment does

not allow outside access, you will need to download the map files for the areas where your network requires coverage.

- **VPN Service Provisioning:**

  The Cisco NSO sample function packs are provided as a starting point for VPN service and RSVP-TE provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found here and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.

Note For licensing and ordering information, work with your Cisco Partner or Cisco Sales representative to review the options described in the Cisco Crosswork Network Controller Ordering Guide.

Known Issues and Limitations

The table below shows known issues and limitations that should be taken into account before starting to work with Cisco Crosswork Network Controller 6.0.x.

- Table 17: Infrastructure
- Traffic Engineering
- Table 19: Service Health Monitoring
- Table 20: Crosswork Data Gateway

Table 17: Infrastructure

Feature	Limitation
Fault and Alarm Synchronization	While geo redundancy enables a switch-over to an active cluster, it's important to take into account the timing of backups. Given the interval between the last backup and the restoration process, there is a loss of some alarm data from the devices. This is due to the time lag since the last backup was completed and restored.
Geo redundancy (with astack functionality)	If switchover is performed on Crosswork cluster containing Service Health, the EOS data may contain partial metrics data (with intermittent gaps in the data metric sequence) for up to 24 hours.

Table 18: Traffic Engineering

Feature	Limitation
TE Dashboard	Traffic Utilization is not supported on Tree-SID and SRv6 policies.
	You cannot view the IGP path on the historical data when an event is selected.
	The metric type for BWoD policies are not visible on the TE Dashboard.
	Hop count metric and BWoD type are not shown in the TE Dashboard under metric/policy type.
	State and Path change events are not visible in the Historic tab of a policy until you zoom in by 5 to 6 clicks.
IPv4 Unnumbered Interfaces	Bandwidth on Demand and SR Circuit Style Manager feature packs will not factor in IPv4 unnumbered interfaces.
	Tree-SID policies are not supported.
	RSVP-TE PCE-initiated tunnels are not supported.

Feature	Limitation
Tree-SID	Only static Tree-SID policies can be created via the UI. Also, you can only update and delete static Tree-SID policies that have been created via the UI.
	Tree-SID policies are only supported on devices running Cisco IOS XR software.
	PCE HA is not supported if the static Tree-SID policy was configured manually on the device (not via the UI).
	Tree-SID policies are not deleted from the UI when the SR-PCE in HA mode is down.
	IPv4 Unnumbered interfaces are not supported.
	Tree-SID policies are not supported in Label Switch Multicast (LSM) routing. In cases where LSM is enabled, IGP updates and traffic utilization data are not supported.
	LCM will not operate in portions of the network carrying Tree-SID LSPs.
	On Cisco 8000 Series Routers, only static Tree-SID policies with leaf role are supported.
	The RestConf API is not supported.
	Tree-SID policy details do not show IPv6 router ID or SRv6 core information.
SR-MPLS	In the SR-MPLS provisioning screen and while previewing an SR-MPLS policy with an IPv6 address, a parsing error is displayed instead of correct error message: "Request Failed. Endpoint address is IPv6, IPv6 provisioning is not supported yet."
	Updating the SID constraint on an existing policy is not allowed by the SR-PCE. The modification screen gives a successful update message, instead of a warning message that it is not allowed.
APIs	The Topology API cannot discover and report IPv6 Link-Local style links.
	The Dashboard Export API cannot export CSV files to an external location. It can only export to /mnt/cw_glusterfs/bricks/rscoean/export.

Feature	Limitation
BWoD	BWoD gets disabled when SR Policy Traffic field has 'Measured' selected and Policy Violation field has 'Strict' selected.

Table 19: Service Health Monitoring

Feature	Limitation
Upgrade	The following limitations have been identified with Service Health on upgrading from Crosswork Network Controller 5.0 to Crosswork Network Controller 6.0: **1.** The **Monitoring** status for existing services from 5.0 is **Unknown** by default. **2.** After the upgrade, some of the services (including the sub-services - *device.health subservice* and *sr.policy.pcc.pm*), may have the monitoring status as **Monitoring Error**. This is on account of some of the components being restarted (ASTACK, Crosswork Data Gateway tracker for example) during the upgrade. To clear the error, stop and start the monitoring again for the service to clear the active symptom. However, if the monitoring error is on account of an issue with device health, then stop monitoring for all the services relating the device and start monitoring the services again to clear the error. This limitation is also observed after a patch upgrade when the lab environment is temporarily shut down and then restarted. **3.** Metric data is restored and available only after the Crosswork Data Gateway becomes active following an upgrade. There is no metrics data available for the duration that the Crosswork Data Gateway was inactive. For example, if the Crosswork Data Gateway was active from October 10, 9:00 AM to October 10, 9:00 PM and was active again after an upgrade from October 11, 3:00 AM, an Event-of-Significance (EoS) generated on October 11 at 8:03 AM will lack metrics data between October 10, 9:00 PM and October 11, 3:00 AM.

Table 20: Crosswork Data Gateway

Feature	Limitation
Upgrade	When Crosswork Network Controller 5.0 is upgraded to 6.0, critical alarms remain uncleared, despite the data gateway VMs being **UP** and operational.

Product Documentation

An Information Portal is now available for Crosswork Network Controller 6.0. Information is categorized per functional area, making it easy to find and easy to access.

You can also access documentation for all Cisco Crosswork products at https://www.cisco.com/c/en/us/support/cloud-systems-management/crosswork-network-automation/tsd-products-support-series-home.html

The following documents are provided for Cisco Crosswork Network Controller 6.0.x.

Table 21: Cisco Crosswork Network Controller 6.0.x Documentation

Document	What is Included
Cisco Crosswork Network Controller 6.0.x Release Notes	This document
Cisco Crosswork Network Controller 6.0 Installation Guide	Shared installation guide for all the Cisco Crosswork applications and their common infrastructure. Covers: • System requirements • Installation prerequisites • Installation instructions • Upgrade instructions
Cisco Crosswork Network Controller 6.0 Administration Guide	Shared administration guide for all the Cisco Crosswork applications and their common infrastructure. Covers: • Managing clusters and data gateway • Data collection • High availability • Backup and restore • Onboard and manage devices • Zero touch provisioning • Set up maps • Managing users, access and security • Maintain system health

Document	What is Included
Cisco Crosswork Network Controller 6.0 Solution Workflow Guide	• Solution overview • Supported use cases and their benefits. • Procedures for achieving the desired outcome for real-life usage scenarios using the Cisco Crosswork Network Controller UI.
Cisco Crosswork Network Controller 6.0 Closed-Loop Network Automation	Provides information on real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. It also provides information on the automated process of deploying changes to the network.
Cisco Crosswork Network Controller 6.0 Service Health Monitoring	Provides information on monitoring the health of L2VPN and L3VPN services. It provides insights into analyzing and troubleshooting degraded services, as well as visualizing service health status and logical dependency trees.
Cisco Crosswork Network Controller 6.0 Traffic Engineering and Optimization Guide	Provides information on how to visualize and configure traffic engineering in Crosswork Network Controller.
Cisco Crosswork Network Controller 6.0 Network Bandwidth Management Guide	Provides information on how to use Crosswork Network Controller feature packs. Feature packs are tools that tackle congestion mitigation and the management of SR-TE policies to find and maintain intent based bandwidth requirements.
Open Source Used in Cisco Crosswork Network Controller 6.0	Lists of licenses and notices for open source software used in Cisco Crosswork Network Controller 6.0.x.
API Documentation	Advanced users can extend the Cisco Crosswork functionality using the APIs. API documentation is available on Cisco Devnet.

Feature Pack Documentation

- Cisco Crosswork Change Automation NSO Function Pack 6.0.0 Installation Guide
- Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 6.0.0-62 Installation Guide
- Cisco Network Services Orchestrator DLM Service Pack 6.0.0 Installation Guide
- Cisco NSO Transport SDN Function Pack Bundle 6.0.0 Installation Guide
- Cisco NSO Transport SDN Function Pack Bundle 6.0.0 User Guide

Bugs

If you encounter problems while working with Cisco Crosswork, check this list of open bugs. Each bug ID in the list links to a more detailed description and workaround. You can use the Cisco Bug Search Tool to search for bugs.

1. Go to the Cisco Bug Search Tool.
2. Enter your registered Cisco.com username and password, and click **Log In**.

   The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register here.

3. To search for all Cisco Crosswork bugs, from the Product list select **Cloud and Systems Management** > **Routing and Switching Management** > **Cisco Crosswork Network Automation** and enter additional criteria (such as bug ID, problem description, a feature, or a product name) in the Search For field. Examples: "Optimization Engine" or "CSCwc62479"
4. When the search results are displayed, use the filter tools to narrow the results. You can filter the bugs by status, severity, and so on.

Note To export the results to a spreadsheet, click **Export Results to Excel**.

Security

Cisco takes great strides to ensure that all our products conform to the latest industry recommendations. We firmly believe that security is an end-to-end commitment and are here to help secure your entire environment. Please work with your Cisco account team to review the security profile of your network.

For details on how we validate our products, see Cisco Secure Products and Solutions and Cisco Security Advisories.

If you have questions or concerns regarding the security of any Cisco products, please open a case with the Cisco Customer Experience team and include details about the tool being used and any vulnerabilities it reports.

Accessibility Features

For a list of accessibility features in Cisco Crosswork Network Controller, visit https://www.cisco.com/c/en/us/about/accessibility/voluntary-product-accessibility-templates.html (VPAT) website, or contact accessibility@cisco.com.

All product documents except for some images, graphics, and charts are accessible. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Support & Downloads

The Cisco Support and Downloads website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies.

Access to most tools on the Cisco Support and Downloads website requires a Cisco.com user ID and password.

For more information:

https://www.cisco.com/c/en/us/support/index.html

Obtain Additional Information

Information about Cisco products, services, technologies, and networking solutions is available from various online sources.

- Sign up for Cisco email newsletters and other communications at:

  https://www.cisco.com/offer/subscribe

- Visit the Cisco Customer Experience website for the latest technical, advanced, and remote services to increase the operational reliability of your network. Go to:

  https://www.cisco.com/c/m/en_us/customer-experience

- Obtain general networking, training, and certification titles from Cisco Press publishers at:

  http://www.ciscopress.com