Solution Overview

This section explains the following topics:

- Description, on page 1
- What's New in This Release, on page 1
- Supported Use Cases , on page 7
- Solution Components Overview and Integrated Architecture, on page 9
- Multi-Vendor Capabilities, on page 14

Description

The exponential growth of network traffic and the pressures of efficiently running network operations pose huge challenges for network operators. Providing quick, intent-based service delivery and optimal network utilization, with the ability to react to bandwidth and latency demand fluctuations in real-time is vital to success. Migration to Software-Defined Networks (SDNs) and automation of operational tasks is the optimal way for operators to accomplish these goals.

Cisco Crosswork Network Controller is an integrated 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 costs. 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 with operator-selected manual or automated remediation. Cisco Crosswork Network Controller delivers network optimization capabilities that are nearly impossible to replicate even with a highly skilled and dedicated staff operating the network.

The fully integrated solution combines functionality from multiple Crosswork components installed upon a common Crosswork infrastructure, as well as industry-leading capabilities from Cisco® Network Services Orchestrator (NSO), Cisco Segment Routing Path Computation Element (SR-PCE), and Cisco Crosswork Planning. Its unified user interface provides a single pane of glass for real-time visualization of the network topology and services, provisioning, monitoring, and optimization.

What's New in This Release

The information below lists the primary new features and functionality introduced in Cisco Crosswork Network Controller 7.0.x.

Platform Infrastructure

- **AWS EC2 Support**: Support is available for deploying the following Cisco Crosswork Network Controller packages on the AWS EC2 platform.
    - Cisco Crosswork Network Controller Essentials package, excluding Zero Touch Provisioning
    - Cisco Crosswork Network Controller Advantage package, excluding Service Health
    - Cisco Crosswork Network Controller Add-on package: data export to 3rd party apps (CDG) & geo redundancy (new)

  New capabilities supported for AWS EC2 platform:
    - Element management enhancements
        - Software Image Management (SWIM) UI
        - Performance trends
        - Deeper inventory
        - Policy and service performance trend analysis
    - FlexAlgo aware BWoD
    - Support for RON 3.0 Optics
- **Crosswork Network Controller deployed as a single VM**: This release introduces support for deploying the Crosswork Network Controller solution on a single VM. The solution is deployed using a unified package that includes Crosswork Infrastructure, Embedded Collectors, and Element Management Functions, enabling you to leverage the device lifecycle functionalities of Crosswork. However, functionalities like service provisioning and overlay are only available on the cluster-based installation.
- **Geo Redundancy**: This release introduces the asynchronous data replication for geo redundancy clusters (on-premises L2 & L3 multi-site) for Crosswork Network Controller. It is no longer necessary to move the cluster into maintenance mode for data synchronization. For more information, see the *Enable Geo Redundancy* section in the Cisco Crosswork Network Controller 7.0 Installation Guide.
- **Dual stack support**: Support is available for deploying the Crosswork Network Controller with a dual stack (IPv4 and IPv6) configuration.
- **Installation enhancements**:
    - The auto-action feature has been added to automate application installation alongside cluster installation.
    - Support has been added to install Cisco Crosswork Network Controller 7.0 on VMware vCenter and ESXi version 8.0.
- **System access and security infrastructure**:
    - Support has been added to register Crosswork components using the Crosswork Network Controller solution license.
    - Support has been added to launch the Single Sign On (SSO) service provider page from the Crosswork UI.
    - Support has been added for the automatic renewal of internal Crosswork certificates.

Traffic Engineering

- **Bandwidth on Demand (BWoD) feature pack**: You now have the option to have BWoD find a path with a specified Flexible Algorithm SID. The acceptable SID values are 0, 1, and 128-255.
- **Alarms and Events**: Traffic engineering alarms and events have been added or updated to be more consistent with other Crosswork services.
- **Virtual Routing and Forwarding (VRF)**: Duplicate IP addresses on two interfaces in the same router are now supported when configured in a VRF table.
- **Interface Index (IfIndex)**: Crosswork Network Controller now supports multiple IP addresses on a single IfIndex.
- **IS-IS Layer 1 and Layer 2**: Crosswork Network Controller now discovers L1 and L2 links. They are displayed on the topology map as dotted lines between devices.
- **Cisco WAN Automation Engine (WAE) and Cisco Crosswork Planning plan file**: The plan file from Crosswork Network Controller now includes additional attributes: LSP MetricType, Dynamic, and applicable disjoint group information. A plan file is comprised of a series of tables that store information about a network, including topology, configuration information, traffic, failure state, and visual layout. For more information, see the Cisco Crosswork Solution Workflow Guide.
- **Interface Names**: When Element Management Functions (EMF) is installed, Crosswork Network Controller now abstracts any non-standardized interface name and populates the `interfaceName` value. As a result, only the `interfaceName` is used, which helps alleviate device telemetry, polling, and configuration problems.

  The Link Summary details page displays the following field changes:

  - Interface Name—Displays the `interfaceName` value.
  - Interface Description—If applicable, displays any user specified text on the actual interface.

Topology

- **Enhanced topology visualization of large VPNs**: Cisco Crosswork Network Controller 7.0 introduces enhanced navigation, provisioning, and visualization of the service overlay and details for large L3 VPNs containing up to 20,000 endpoints (UNI/PE-CE interface).

  When a user selects a VPN service in the UI that is too large to display in full (since a maximum of 50 endpoints can only be displayed once), they can click **Select endpoints** and choose from a list of endpoints to visualize the service overlay and details. The list shows only the endpoints on devices in the current selected device group. The list also includes filters to narrow down the list of endpoints, making it easier to select.

  Preconditions and limitations:

  - Visualization of large VPN support for L3VPN aligning with IETF L3 NM model.
  - Maximum number of vpn-node (PE) in the L3VPN: 4,000.
  - Maximum number of endpoints (UNI/PE-CE interface) in the L3VPN: 20,000.
  - Maximum number of policies or tunnels per large VPN: 5,000.
  - Maximum number of large VPN service instances in each deployment: 6.
  - Recommended provisioning of endpoints in a single request with a single L3VPN: 500.

- **Enhancements in the Topology UI - Links Visualization**: The Topology UI has been updated with a new **Links** tab to display all links on the map and a global links table in the **Devices** tab showing link details and metrics. Key metrics like bandwidth utilization, packet errors, packet drops, delay, and jitter are now visualized in both the map and details panels, with delay and jitter available when Crosswork Service Health is installed and SR-PM is enabled. You can also customize link color and metric thresholds in the Topology map and view historical data for collected metrics on the **Link Details** page.
- **Topology Dashboard**: A new **Topology** dashlet has been added to the **Dashboards** page, offering details on L2 and L3 links along with their associated metrics. When you click the L2 or L3 links in the dashboard, you will be directed to the Topology UI, where the corresponding map is displayed in the left pane. The **Devices** and **Links** tabs in the right pane offer detailed information about the devices and links on the map.

Change Automation

- **Support for check-sync action play**: Crosswork Network Controller 7.0 includes a new stock play, **Perform Check Sync on the device**, to achieve check-sync. You can use this Play as a pre-step to running other operations in the Playbook or as part of pre-maintenance. This Play checks the device sync status with NSO and performs a sync-from (pulling the present device config into NSO) only when needed, based on the Playbook's sync parameter value. It reduces the playbook execution time and ensures the NSO configuration matches the device configuration.
    - If the Playbook's sync parameter is set to True and the device is not in sync, it will sync the device with the NSO configuration, and the operation succeeds with an in-sync status.
    - If the sync parameter is set to False and the device is not in sync, the Playbook fails with a commit message.
    - If the device is already in sync, the operation succeeds.

Service Health

- **Monitor Service Health using Cisco Provider Connectivity Assurance**: Crosswork Network Controller can leverage external probes from Cisco Provider Connectivity Assurance (formerly Accedian Skylight) to provide additional insights into the health of the L3 VPN services in the network.

Note Cisco Provider Connectivity Assurance integration is available as a limited-availability feature in this release. Engage with your account team for more information. For more information, see the *Monitor Service Health* section in Cisco Crosswork Network Controller 7.0 Service Health Monitoring.

- **L3 VPN service monitoring enhancements**: Service Health supports large-scale VPN visualization by monitoring L3VPN services at the node level and creating an Assurance graph for each service at either the node or endpoint level. If the graph contains more than 50 endpoints, Service Health indicates that the graph is too large to view and prompts you to use the **Select Endpoints** option to select and view up to 50 endpoints.
- **Enhanced metrics and insights with SR-PM**: When Segment Routing Performance Measurement (SR-PM) is enabled on your devices, Service Health collects and processes additional metrics like Delay, Delay Variance, and Liveness to assess the performance of links and the health of TE policies. It also offers historical data and trends for these metrics, providing valuable insights into network performance and trends.

- **Service Health dashboard**: A new Service Health Dashboard displays a consolidated view of L2 VPN and L3 VPN services. In the event an SLA for a service is breached, the UI clearly indicates the break, making detection of problems easier.

Data Gateway

- **Support for dual-stack configurations**: Crosswork Network Controller introduces support for dual-stack configurations, enabling the system to establish connections using IPv4 and IPv6 protocols. With this enhancement, Crosswork can seamlessly communicate concurrently with various systems (such as NTP, DNS, and Syslog) and devices (SSH, SNMP, MDT) over IPv4 and IPv6. In dual-stack mode, Crosswork gives priority to IPv6 for all communication purposes.

  For information on configuring a dual stack when creating or editing a pool and adding destinations, see Cisco Crosswork Network Controller 7.0 Administration Guide.

- **New custom package to support different file formats**: Crosswork Network Controller has introduced a new feature that provides the flexibility in managing custom packages. This feature unifies the previously available different upload structures by standardizing the file structure for both system and custom packages. Crosswork Network Controller now supports multiple custom packages and allowing users to upload their specific packages more efficiently. The feature includes support for aggregate custom packages, which users can use for Embedded Collectors and Crosswork Data Gateway in a cluster deployment.

  The updated Crosswork Network Controller UI enables users to upload a common package type as well as the new aggregate package type, facilitating the combination and merging of various file formats into a single, unified package.

  For information on adding and downloading aggregate packages through the Crosswork UI, see Cisco Crosswork Network Controller 7.0 Administration Guide.

- **Deployable on VMware vCenter version 8.0**: Cisco Crosswork Network Controller 7.0 and Crosswork Data Gateway instances can be installed on VMware vCenter and ESXi version 8.0.

  For information on the installation of Crosswork Data Gateway on vCenter, see Cisco Crosswork Network Controller 7.0 Installation Guide.

- **Embedded Collectors**: With an intent to simplify deployment, the Crosswork Network Controller can be set up on a single VM, though this comes with a trade-off in terms of scale and availability. This deployment model minimizes the reliance on external components by incorporating an embedded collector, replacing the need for external Crosswork Data Gateway VMs. In this model, the data gateway is installed as a lightweight CAPP within the single VM, reducing the need for separate data gateway nodes and significantly decreasing the deployment footprint. The data gateway functions as embedded collectors within the Kubernetes pods.

  For information on installing embedded collectors, see Cisco Crosswork Network Controller 7.0 Installation Guide.

- **A new Interactive Console menu option to modify the controller's IP or FQDN for data gateway enrollment and geo redundancy features**: The interactive menu now has a new option that enables you to modify the controller's IP or FQDN in these scenarios:

  - A data gateway may fail to enroll with the Crosswork Network Controller if deployed with an invalid controller IP.

  - A data gateway is registered with a Crosswork Network Controller, and the controller's VIP IP or IP is changed to an FQDN. This change might be necessary for Geo Redundancy configuration.

For more information on using the new menu option, see the *Configure Controller IP for Crosswork Data Gateway* section in Cisco Crosswork Network Controller 7.0 Administration Guide.

Device Lifecycle Management

- Device management has been enhanced with new features allowing for customized monitoring and management of network devices. These include:
  - Tag Management window to manage the tags available for assignment to devices in your network. Tags can provide information such as the device's physical location and administrator's email ID, which can be used to group devices.
  - A comprehensive Network Inventory overview listing device names, types, hardware details, and operational statuses.
  - Manual inventory synchronization for up-to-date network device tracking.
  - Options for device groups and port groups are available, which can be utilized for performance monitoring data collection based on specific parameters.
- **Software Image Management**: All workflows related to image management are now handled through Software Image Management (SWIM). SWIM offers improved management of device software images, enabling seamless deployment, upgrades, and downgrades across a two-version range. Additionally, it supports specialized firmware upgrades for Field Programmable Devices (FPD) to maintain devices with unique firmware needs efficiently..
- **Monitoring Policies**:

  Monitoring policies help you control how Crosswork monitors your network. You can create and customize different monitoring policies to monitor network-wide device information and manage your network health. Monitoring policies are available for:
  - Device Health
  - Interface Health
  - LSP Traffic Policy
  - Optical SFP Interfaces
  - Optical ZR Pluggable Devices
- **Alert Management**:

  Crosswork's alert management has been improved to offer a more comprehensive system notification experience. Enhancements include:
  - Standardized alarms and events notifications integration and visibility.
  - Option to configure and customize your settings to receive alerts.
  - System-level event processing with throttling mechanisms to prevent system overload and maintain network stability and performance.
- **Zero Touch Provisioning**:
  - **ZTP is integrated with EMF**

ZTP is now integrated with Element Management Functions (EMF), enabling deployment directly through the CAPP file.

- **UI/UX workflow changes**

  The ZTP sub-menu is integrated under the "Device Management" section of the UI main menu, consolidating various individual sub-menus.

For more information, see the *Zero Touch Provisioning* section in Cisco Crosswork Network Controller 7.0 Device Lifecycle Management.

Documentation

- An Information Portal is now available for Crosswork Network Controller 7.0. The information is categorized by functional area, making it easy to find and access.
- Cisco Crosswork Network Controller 7.0 Installation Guide covers installing the cluster and Crosswork applications on top of the infrastructure. It also includes installing the Cisco Crosswork Data Gateway.
- Cisco Crosswork Network Controller 7.0 Administration Guide covers the setup and maintenance of the Crosswork system. This guide also includes information on Cisco Crosswork Data Gateway and the Single VM install.
- Cisco Crosswork Network Controller 7.0 Solution Workflow Guide provides an overview of the solution and its supported use cases. It walks users through various common usage scenarios to illustrate how they can work with the solution components to achieve the desired benefits.
- The Cisco Crosswork Network Controller 7.0 Device Lifecycle Management Guide details the steps for onboarding, managing, and monitoring network devices. It covers key aspects such as alarm management, monitoring policies, ZTP and software image management (SWIM).
- Cisco Crosswork Network Controller Getting Started Guide has been deprecated, and the topics in this guide are now covered in other guides.

Supported Use Cases

Crosswork Network Controller supports a wide range of use cases, allowing operators to manage many aspects of the network. The following use cases illustrate the most commonly used features and the applications needed to implement them. In addition, Crosswork Network Controller solution is highly adaptable and if the use case you are focused on is not covered, consult your Cisco Customer Experience representative for more information.

- **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 and visualizing to customize and compute IGP shortest paths over a network according to specified constraints.

  For this use case, Cisco Crosswork Advantage must be installed.

- **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

  For this use case, Cisco Crosswork Advantage must be installed.
- **Local Congestion Management:** Local Congestion Mitigation (LCM) provides localized mitigation recommendations within surrounding interfaces using standard protocols. Data is gathered in real-time, and solutions are suggested when congestion is detected. LCM supports deployment as either "human in the loop" or fully automated implementations, allowing operators to choose how to use the feature. See the Local Congestion Mitigation chapter in the Crosswork Network Controller 7.0 Network Bandwidth Management guide for more information. For this use case, Cisco Crosswork Advantage must be installed.
- **Visualization of network and service topology and inventory:** The topology UI, along with the various tables that can be accessed from it, allows you to easily assess the health of the network and drill down to see details about devices, links, and services.
- **Performance-based closed-loop automation:** Automated discovery and remediation of problems in the network by allowing Key Performance Indicator (KPI) customization and execution of pre-defined remediation tasks when a KPI threshold is breached. Health Insights and Change Automation functions must be installed for this use case.
- **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 Crosswork Planning Design). Automating the execution of maintenance tasks (such as throughput checks, software upgrades, and SMU installs) using playbooks. For this use case, Health Insights and Change Automation functions must be installed.
- **Secured zero-touch onboarding and provisioning of devices:** Onboarding new IOS-XR devices and automatically provisioning Day0 configuration resulting in faster deployment of new hardware at lower operating costs. For this use case, Cisco Crosswork Essentials must be installed.
- **Visualization of native SR paths:** Using the traceroute SR-MPLS multipath command to get the actual paths between the source and the destination can be achieved using Path Query. With the Cisco Crosswork Network Controller, a traceroute command runs on the source device for the destination TE-Router ID and assists in retrieving the paths. For this use case, Cisco Crosswork Advantage must be installed.
- **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) using the Crosswork Network Controller can be visualized and analyzed to assist in efficient management and troubleshooting of your multicast network. Configuring link affinities to specify the link attributes that determine which links are suitable to form a path for the Tree-SID policy and map each bit position or attribute with a color (making it easier to refer to specific link attributes). Modifying existing static Tree-SID policies

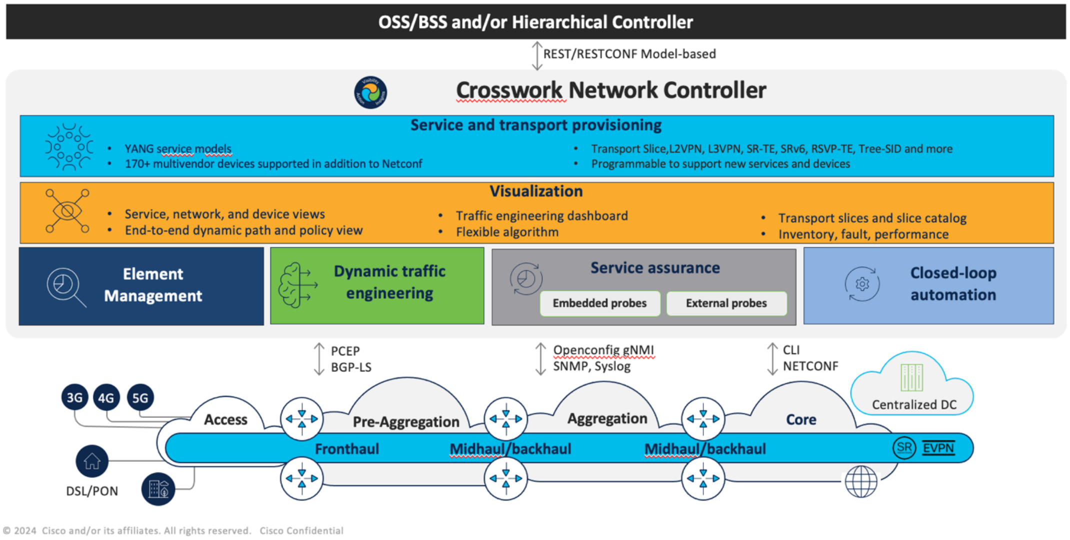
and mVPN Tree-SID policies associated with an L3VPN service model – both edit and delete – using the UI. For this use case, Cisco Crosswork Advantage must be installed.

- **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 slice profiles around customer intents and add them to a catalog. Network line operators can assign the profile identified for a given customer to their endpoints and adjust the constraints according to the customer's requirements. Using the UI, you can inspect the slice details for active symptoms, failures, and root causes. In addition, the slice can be visualized on a geographical map. For this use case, Cisco Crosswork Advantage must be installed.

Solution Components Overview and Integrated Architecture

The following diagram provides a high-level illustration of how the solution's components work together within a single pane of glass to execute the primary supported use cases.

Figure 1: Solution Components and Integrated Architecture


OSS/BSS and/or Hierarchical Controller
REST/RESTCONF Model-based
Crosswork Network Controller
Service and transport provisioning
• YANG service models
• 170+ multivendor devices supported in addition to Netconf
• Transport Slice,L2VPN, L3VPN, SR-TE, SRv6, RSVP-TE, Tree-SID and more
• Programmable to support new services and devices
Visualization
• Service, network, and device views
• End-to-end dynamic path and policy view
• Traffic engineering dashboard
• Flexible algorithm
• Transport slices and slice catalog
• Inventory, fault, performance
Element Management
Dynamic traffic engineering
Service assurance
Embedded probes
External probes
Closed-loop automation
PCEP
BGP-LS
Openconfig gNMI
SNMP, Syslog
CLI
NETCONF
Centralized DC
3G
4G
5G
Access
Pre-Aggregation
Aggregation
Core
Fronthaul
Midhaul/backhaul
Midhaul/backhaul
SR
EVPN
DSL/PON

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The following components make up the Cisco Crosswork Network Controller 7.0 solution:

Cisco Crosswork Active Topology

Cisco Crosswork Active Topology's logical and geographical maps provide real-time visibility into the physical and logical network topology, service inventory, SR-TE policies, and RSVP-TE tunnels, all within a single pane of glass. They enable operators to see the status and health of the devices, services, and policies at a glance. Services and transport policies can be visualized end-to-end as an overlay within the context of the topology map. Cisco Crosswork Active Topology provides device grouping functionality so that operators can set up their maps to monitor exactly the set of devices, services, and locations for which they are responsible. In addition, operators can save custom views for quick and easy access to the views and functionality they use on an ongoing basis.

Cisco Crosswork Optimization Engine

Cisco Crosswork Optimization Engine provides real-time network optimization, allowing operators to effectively maximize network capacity utilization, preserve network intent with proactive network monitoring and visualization, and increase service velocity. Leveraging real-time protocols, such as BGP-LS and Path Computation Element Communication Protocol (PCEP) and SR-PCE, Crosswork Optimization Engine enables near real-time tracking of the network, with the ability to react quickly (manually or through automation) to changes in network conditions to minimize disruptions or degradation in performance.

Cisco Service Health

Service Health substantially reduces the time required to detect and troubleshoot service quality issues. It monitors the health of provisioned L2 and L3 VPN services and lets operators pinpoint why and where a service is degraded. This is accomplished through a heuristic model that provides the following:

- Monitoring the health of:
    - Point-to-point L2VPN services
    - Multipoint L2VPN (EVPN E-LAN and E-Tree L2VPN EVPN) services
    - L3VPN services
- Analysis and troubleshooting of services with degraded health
- Visualize the health status of a service and view its logical health dependency tree to help operators troubleshoot cases of degradation by locating where the problem resides, indicating possible symptoms, and impacting metrics in case of degradation
- Performance metrics and health status of Traffic Engineering (TE) policies
- Historical view and trends of service health status
- Extensible to add service monitoring capabilities to address specific needs

Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is a secure, standard collection platform for collecting telemetry and other performance data from compatible non-Cisco and Cisco network devices. Several data-collecting protocols, including MDT, SNMP, CLI, standards-based gNMI (dial-in), and Syslog, are supported by Crosswork Data Gateway. By doing this, it can enable a wide range of use cases and modifications. Operators can add their collection jobs to acquire network performance data, which can subsequently be sent to suitable Kafka and gRPC message buses for consumption by other applications using APIs and the configuration examples provided by Cisco. Rather than requiring each data consumer to collect information directly from the source, Crosswork Data Gateway enables the operator to capture the data once and send it to numerous consumers.

With Cisco Crosswork Network Controller operating as the controller and consumer of data and Crosswork Data Gateway working as both a centralized shared collector and distributor of data, Cisco has established a mechanism for obtaining data from the network that is reliable, flexible, and efficient.

Several Crosswork Data Gateway VMs can be installed and scaled horizontally as a pool of devices capable of handling your network's data-gathering demands to provide high availability within the pool. The number of pools and Crosswork Data Gateways in the pool is determined by the number of devices in your network, the geographic distribution of those devices, the amount of data you collect, and the level of redundancy desired (1 to 1 or n to m). For more details on scaling your Crosswork Data Gateways to match your specific use case, please collaborate with Cisco Customer Experience (CX), the Cisco account team, or the partner from whom you purchase Cisco products.

Crosswork Common UI and API

All Cisco Crosswork Network Controller's functionality is provided within a common graphical user interface. This common UI brings together the features of all Crosswork Network Controller's components, including common inventory, network topology and service visualization, service and transport provisioning, and system administration and management functions. When optional add-on Crosswork components are installed, their functionalities are also fully integrated into the common UI. Having all functionality within a common UI instead of navigating individual application UIs separately enhances the operational experience and increases productivity.

A common API enables Crosswork Network Controller's programmability. The common APIs provide a single access point for all APIs exposed by various built-in components. The API provides a REST-based Northbound Interface to external systems (e.g., OSS systems) to integrate with Cisco Crosswork Network Controller. RESTCONF and YANG data models are made available for optimization and service provisioning use cases. For details about the APIs and examples of their usage, see the Cisco Crosswork Network Automation API Documentation on Cisco DevNet.

Crosswork Infrastructure and Shared Services

The Cisco Crosswork Infrastructure provides a resilient and scalable platform on which all Cisco Crosswork components can be deployed. This infrastructure and shared services provide:

- A single API endpoint for accessing all APIs of Crosswork applications
- A shared Kafka bus to pass data between applications
- Shared Databases
  - Stores all configuration data for each of the applications.
  - Stores all the time series (telemetry) data gathered from the network.
- A robust Kubernetes-based orchestration layer that gives process-level resiliency and elasticity to scale the environment when additional resources are needed.
- Tools for monitoring the health of the infrastructure.

Cisco Crosswork Health Insights and Cisco Crosswork Change Automation

Cisco Crosswork Health Insights and Cisco Crosswork Change Automation are components that can optionally be installed with Cisco Crosswork Network Controller.

Cisco Crosswork Health Insights performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. When used with Cisco Change Automation, or as part of a broader integration with your existing automation solutions, Health Insights plays a key role in both manual and automated response to network events.

Cisco Crosswork Change Automation 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.

These components within Cisco Crosswork Network Controller enable closed-loop discovery and remediation of network problems. Operators can match alarms to pre-defined remediation tasks, which are automatically performed when a defined Key Performance Indicator (KPI) threshold is breached. This reduces the time it takes to discover and repair a problem.

Element Management Functions

A library of functions that provides deep inventory collection, device management, alarm management, and software image management.

Zero Touch Provisioning with 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.

Cisco Network Services Orchestrator

Cisco Network Services Orchestrator (NSO) is an orchestration platform that leverages pluggable function packs to translate network-wide service intent into device-specific configuration. Cisco Network Services Orchestrator 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 European Telecommunications Standards Institute (ETSI) architecture. It provides complete support for physical and virtual network elements, with a consistent operational model across both. With the ability to orchestrate across multi-vendor environments and support multiple technology stacks, Cisco Network Services Orchestrator empowers the extension of end-to-end automation to virtually any use case or device.

Cisco Network Services Orchestrator has a rich set of APIs designed to allow developers to implement service applications. It provides the infrastructure for defining and executing the YANG data models that are needed to realize customer services. It is also responsible for providing the overall lifecycle management at the network service level.

Service and device models, written using YANG modeling language, enable Cisco Network Services Orchestrator to efficiently ‘map’ service intent to device capabilities and automatically generate the minimum required configuration to be deployed in the network. This feature, facilitated by Cisco Cisco Network Services Orchestrator's FASTMAP algorithm, can compare current configuration states with a service’s intent and then generate the minimum set of changes required to instantiate the service in the network.

All Crosswork components that are included in Cisco Crosswork Network Controller or are optional add-ons, require integration with Cisco Network Services Orchestrator.

Cisco Crosswork Network Controller requires the following Cisco Network Services Orchestrator function packs:

- SR-TE core function pack (CFP) enables the provisioning of explicit and dynamic segment routing policies, including SRv6, and on-demand SR-TE policy instantiation for prefixes with a specific color.
- The IETF-compliant L2VPN and L3VPN Core Function Packs provide baseline L2VPN and L3VPN provisioning capabilities, based on IETF NM models. Prior to customization, these sample function packs enable provisioning of the following VPN services:

Note The Service Health function pack should be independently installed apart from Cisco Crosswork Network Controller function packs.

- L2VPN:
  - Point-to-point VPWS using Targeted LDP
  - Point-to-point VPWS using EVPN
  - Multipoint VPLS using EVPN (with service topologies ELAN, ETREE, and Custom)
- L3VPN – both IPv4 and IPv6 address families are supported.
- Sample IETF-compliant RSVP-TE function pack intended as a reference implementation for RSVP-TE tunnel provisioning, to be customized as required.

Note By default, the IETF-compliant NM models are used. If your organization wishes to continue using the Flat models provided with the previous version, a manual setup process is required. Consult your Cisco Customer Experience representative for more information.

Note The Cisco Network Services Orchestrator sample function packs are provided as a starting point for service 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 on Cisco Devnet, and Cisco Customer Experience representatives can answer 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 Cisco Network Services Orchestrator currently does not support bundle ethernet (BE), route distinguisher (RD), or BGP route-target (RT) functions with L2VPN EVPN. Although it does support multihoming and L2VPN route policy, there is no option to specify an RD value in L2VPN for an EVPN ELAN/ETREE, nor is there an option to specify load balancing type. To perform these functions, contact your Cisco account team for a set of custom configuration templates and advice on configuring bundles manually.

Cisco Segment Routing Path Computation Element

Cisco Segment Routing Path Computation Element (SR-PCE) is an IOS-XR multi-domain stateful Path Computation Engine (PCE) supporting segment routing (SR), Resource Reservation Protocol (RSVP), and

SRv6-aware PCE. Cisco Segment Routing Path Computation Element builds on the native PCE abilities within IOS-XR devices and provides the ability to collect topology and segment routing IDs through IGP (OSPF or IS-IS) or BGP Link-State (BGP-LS), calculate paths that adhere to service SLAs, and program them into the source router as an ordered list of segments. A Path Computation Client (PCC) reports and delegates control of head-end tunnels sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that Segment Routing Path Computation Element uses to push updates to the network and re-optimize paths where necessary. PCEPv6 is also supported.

Cisco Segment Routing Path Computation Element can either reside on server resources using virtualized XRv9000 , or run as a converged application within IOS-XR Routers.

Multi-Vendor Capabilities

Crosswork Network Controller is multivendor capable, leveraging open industry standard mechanisms and protocols such as BGP-LS, SNMP, gNMI, PCEP, segment routing, and NETCONF/YANG to communicate with network devices in a multivendor environment. In order to deploy the product in a multivendor environment, Cisco professional services (CX) should be engaged to validate interoperability with third-party devices in your network environment. See the Cisco Crosswork Network Controller Data Sheet for supported use-cases and capabilities.

Today’s networks have typically been built over time and incorporate multiple vendors and generations of hardware and software. Furthermore, there is a lack of industry standardization, making support for these networks using a single tool challenging.

Service providers require an integrated solution to manage third-party devices that will reduce operational expenses and maintenance overhead, as well as eliminate the need to build custom applications to deploy and maintain different vendor products for a single network.

Using standards-based protocols, the Cisco Crosswork Network Controller has multi-vendor capabilities for:

- Network service orchestration via Cisco Network Services Orchestrator using CLI and Netconf/YANG. Cisco Network Services Orchestrator is a YANG model-driven platform for automating provisioning, monitoring, and managing applications and services across multi-vendor networks.
- The Cisco Crosswork Network Controller provisioning functionality can be extended using the application programming interfaces (APIs). Each product in the platform supports external integration, development, and customization by providing easy-to-use APIs that cover all or most of each product's functions, including functions created exclusively for access via APIs. For more information, see the Cisco Crosswork Network Automation API Documentation on Cisco DevNet.
- Telemetry data collection via the Cisco Crosswork Data Gateway using SNMP with standards-based MIBs, Syslog, gNMI, and CLI commands. Cisco Crosswork Data Gateway also supports Native YANG data models for external destinations and SNMP MIBs. Custom packages are available to use with Crosswork applications, such as Crosswork Health Insights, for device telemetry and network management automation.
- Topology and transport discovery via SR-PCE, using IGP and BGP-LS, with link utilization and throughput collected via SNMP using standard MIBs.
- Transport path computation using PCEP.

Building a custom package (or modifying the samples we provide) can get complicated. Refer to the Cisco DevNet guide to get details about the process. This documentation includes the steps to load custom packages and the basic steps needed to leverage them. Even with these extensive resources, operators may find it more productive to use the expertise from Cisco CX (Cisco Customer Experience) to perform this work. For more details, contact Cisco or the Cisco partner you work with to purchase products and services.