LiveNX 7

LiveAction™

Network Performance and Analytics Platform

LiveNX collects and analyzes data from multiple sources in an SD-WAN architecture to analyze and present insights to optimize design, policy verification and operations across the enterprise in order to deliver peak performance for an optimal customer experience.

Overview

End-to-end Flow Visualizations Across the Network

LiveNX's patented visualization technology simplifies network operations and troubleshooting. LiveNX correlates multiple data sets to provide views, graphs and maps to illustrate the current state of applications and network performance.

Application Visibility and Troubleshooting

Gain a deep understanding of application traffic with full visibility of protocol and application type including video, voice, instant messaging, file transfer, etc. Troubleshoot applications deployed in the data center, public cloud or SaaS. Understand how your network is being used, how applications are performing, and which sanctioned or unsanctioned applications are being used.

Intuitive Graphical Interface for QoS Control

Create, edit and apply QoS polices for Cisco routers and Layer 3 switches on live networks consistently and confidently. QoS wizard and built-in templates are available to apply policies based on Cisco best practices or use the QoS GUI editor to build custom policies. LiveNX generates a QoS audit report to show QoS policies in detail, including configuration settings, performance issues, drops, and policy errors.

Software-Defined WAN Management

Utilize application and path visualizations to effectively validate WAN Return-on-Investment (ROI) for traditional MPLS, hybrid, or Soft-ware-Defined WAN (SD-WAN). When a network element makes a path change to protect the applications due to an Out-of-Policy (OOP) condition, LiveNX renders the end-to-end path changes graphically. Visualize the network and overlay paths from the branch-office, through the service provider(s) to the data center where the applications reside, for meaningful and actionable information.

LiveNX gathers real-time data from both any multi-vendor network elements as well as Cisco-specific REST APIs (DNA Center, vManage BFD (Bidirectional Forward Detection) and AppId (Application Identification to provide accurate visual analytics.

What's New

SD-WAN policy verification: With site to site visual analytics, policy verification at scale is simplified. The performance of the service path between an application, SD-WAN tunnel and the service provider transport is analyzed and presented with overall service status to ensure policies are operating as expected.

SD-WAN Topology Filters: From the comprehensive summary view, NetOps can now filter to isolate and analyze individual layers of the service path for troubleshooting performance issues. The SD-WAN Topology view provides isolation of functional elements while placing it in context to the end to end. SD-WAN filters include: Site, SD-WAN tunnel, Application, DSCP, Service Provider and VPN

Catalyst 9000 and SD-Access: LiveNX presents SD-Access to visualize the performance of the service path. With Cisco DNA Center integration, Scalable Group Tags (SGT) and Virtual Network Identifiers (VNI) are resolved and with Cisco ISE (Identity Service Engine) integration, IP addresses are resolved to user names for a complete view of the SD-Access overlay and current status, and full concurrent visibility into the virtual overlay and physical underlay.

Extended Flow Reports: Extend visibility beyond the edge of the network with flow reporting to end point device, either physical or virtual, for complete visibility across your organization.

WAN Availability story: Empower the user to see the availability percentage of any WAN interface they have monitored by LiveNX. NetOps can filter by any combination of site name, device, interface, group, tag, service provider and see the availability percentage for that wan interface over a time range.

Operations Dashboard: Alert Widget Customization
LiveNX customized dashboard now supports Alert widget creation and display on the main dashboard for: Category, Site, Device or WAN interface

Flexible Deployment : LiveNX is available as a software package for on premises, public cloud or on a Cisco ENCS 5000 or Cisco CSR virtual router. In addition, LiveNX is now available on the LiveNX server appliance (hardware) for ease of installation and operations.

Key Features

SD-WAN Policy Verification:

With site to site visual analytics, policy verification at scale is simplified. The performance of the service path between an application, SD-WAN tunnel and the service provider transport is analyzed and presented with overall service status to ensure policies are operating as expected.
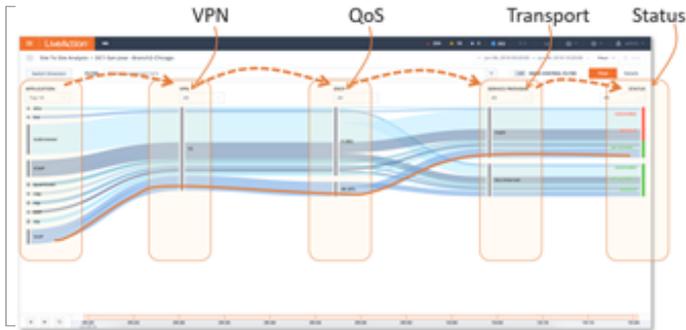
LiveNX Site to Site Policy Verification

Extended Flow Reports:

Extend visibility beyond the edge of the network with flow reporting to end point device, either physical or virtual, for complete visibility across your organization
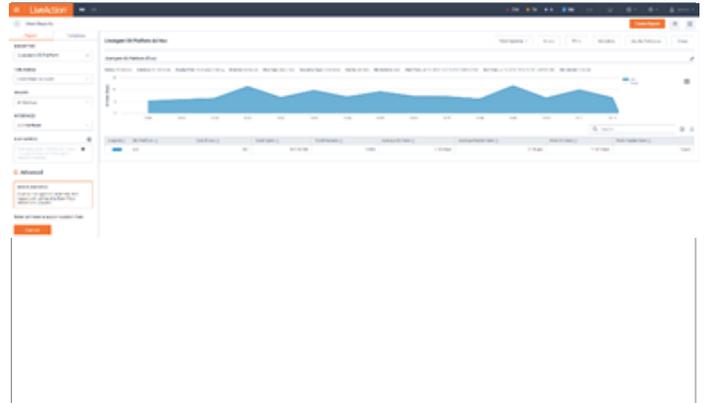

SD-WAN Topology Filters:

From the comprehensive summary view, NetOps can now filter to isolate and analyze individual layers of the service path for troubleshooting performance issues. The SD-WAN Topology view provides isolation of functional elements while placing it in context to the end to end
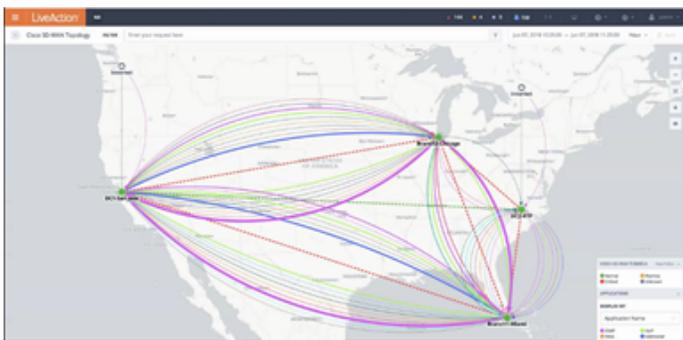
LiveNX Cisco SD-WAN Topology View Top Ten Application View

**Catalyst 9000 and SD-Access:**

LiveNX presents the SD-Access Traffic Assessment view to visualize the performance of the service path. With Cisco DNA Center integration, Scalable Group Tags (SGT) and Virtual Network Identifiers (VNI) are resolved and with Cisco ISE (Identity Service Engine) integration, IP addresses are resolved to user names for a complete view of the SD-Access overlay and current status.

LiveNX SD-Access Site-to-Site Analysis View

**Operations Dashboard – Custom Alert Summary by Sites:**

The LiveNX Operations Dashboard supports custom widgets to illustrate an aggregated alerting view. NetOps teams can now visualize the Dashboard Alerts in one location by Site, Device, or Interface for easier access with summarized views.
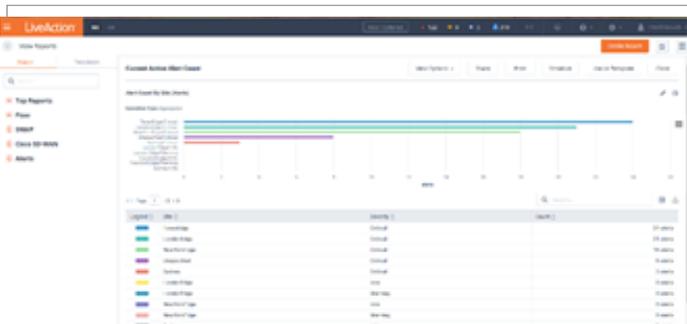
LiveNX Operations Dashboard: Current Alerts by Site

Operations Dashboard – WAN Interface Availability:

Availability is a benchmark that can be an indicator of issues. LiveNX provides customization for WAN interface availability widgets as well as flex search for targeted sites, devices or interfaces for reporting.
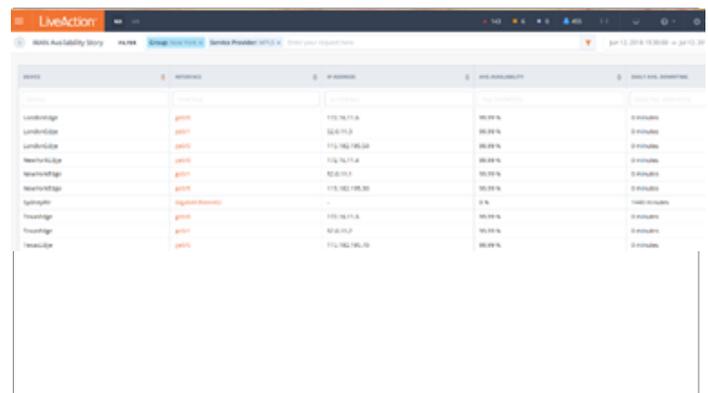
Key Capabilities

Flow Visualization for Network Troubleshooting

Visualization allows you to better understand network traffic so that you can identify trouble spots.

- Application and flow path analysis
- Multi-vendor support – NetFlow v5/v9, IPFIX, sFlow and J-Flow
- Jitter, delay, packet loss metrics for voice and video
- Application response times, round-trip time, server delay and client delay metrics
- NetFlow Secure Event Logging (NSEL)
- Wireless information including user identity
- Firewall high-speed logging
- End-system (device type, OS) and end-user information
- Integration with Network Packet Brokers
- Flow DVR for playback of historical data
- Built-in Domain Name System (DNS) name resolution
- Topology export to Visio

Software-Defined WAN Monitoring

GUI-based management for SD-WAN monitoring for path control and application performance optimization.

- Path control visualization
- SD-WAN dashboard and trending
- PfRv3 multiple data center support
- Shows what Out-of-Policy reason triggers path change(s)
- Reports on traffic class/application associated

Cisco IWAN Support

- PfR configuration of multiple Master Controllers
- Automatically learn semantic settings for PfRv3 monitoring to simplify setup
- PfRv3 multiple data center support

Cisco SD-WAN Support (Viptela)

LiveNX consolidates a unified reporting, inventory, and alert notification. For Cisco SD-WAN, LiveNX supports :

- Cisco SD-WAN Site to Site Topology View
  - Overlay visibility – VPN, tunnel
  - Service Provider transport
  - Performance Status
  - Filtering by application, DSCP, VPN or Service Provider
- Cisco SD-WAN Site to Site Analysis: Viptela device inventory, including vEdge routers and management devices like vManage, vBond and vSmart
- Add relevant interfaces for monitoring from each vEdge router.
- Device monitoring credentials, like SNMP settings
- Gather network semantic information per device and interface:
  - Site association per device
  - Site geo location
  - WAN interfaces per device
  - Service Provider associated with each WAN interface. Note: Viptela refers to the service provider information as "colors".
  - Capacity of WAN links (inbound and outbound)
  - Site IP mappings

  - Determine if a device is in the data center
  - Viptela VPN ID mapping to a VPN name. The VPN ID is synonymous to a VRF. Viptela may or may not associate VPN ID's to names, as is the case with Cisco.
  - vManage API: BFD (Bidirectional Forward Detection), AppId (for identification of over 4000 applications) and Alarms.

QoS Monitoring

Track QoS performance on a per-class basis. Monitoring and alerting of priority queue drops provides proactive notification of potential voice quality issues.

- NBAR2 application visualization
- Custom NBAR definitions
- Pre- and post-QoS graphs
- Detailed graphical display of interface and CBQoS statistics
- 95th/99th percentile, quarterly, yearly and collated reports

Alerting

LiveNX associates Events from devices (routers, switches, firewalls, etc.) to Alerts, which are generated upon meeting specific criteria, such as a threshold, and are displayed in the Operations Dashboard.

With the Event-to-Alert mapping concept, LiveNX is able to eliminate the common complaint that the number of alerts being created is too high, thereby displaying only the alerts that require immediate attention.

Alerts are categorized into three severity levels:

Critical:
The highest severity, e.g. for alerts that would cause the biggest problem to the network

Warning:
A high severity, e.g. for alerts that may indicate issues that are problem- atic or will become problematic

Info:
A low severity, e.g. an issue that is worth knowing about but may not be that detrimental to the network

Alerts can be configured to integrate into workflows within industry incident management systems such as ServiceNow and PagerDuty.

QoS Configuration

Create, edit, and apply QoS policies for Cisco routers and Layer 3 switches on live networks. Use the QoS wizard and built-in templates to apply policies across multiple devices based on Cisco best practices or use the QoS GUI editor to build policies.

- Full Modular QoS configuration support including WRED, CBWFQ, and Priority Queue
- Hierarchical policy creation for advanced configurations
- Custom NBAR2-based matches including high-level attributes, HTTP URL, MIME, HOST and RTP protocols
- Built-in ACL editor
- Built-in rules for QoS settings that highlight violations
- Configuration audit trail
- System-wide QoS audit
- LAN Service Policy

LAN

Visualize Spanning Tree Protocol. Provide real-time Layer 2 visualiza- tions for networks, including trunk interface, port channels, VLAN associations and bandwidth percentages. Run Layer 2 QoS reports.

Routing

Real-time routing visualizations for Cisco networks that can identify reachability problems, routing loops, and asymmetric paths affecting traffic quality. In addition, the policy-based routing viewer/editor pro- vides a high degree of control over traffic policy to route traffic easily and predictably over user-specified paths.

IP SLA

Cisco IOS IP SLA is easily accessible to generate and monitor synthetic network traffic to baseline network performance, test policy changes, or proactively monitor key network paths. Synthetic traffic types include data (HTTP, FTP, DNS, DHCP) and voice that can be used to measure latency, loss, jitter, and Mean Opinion Score (MOS) for VoIP. The highly interactive graphical interface delivers the functionality and flexibility of IP SLA features without the need to learn and use Cisco device command lines.

Test Types:
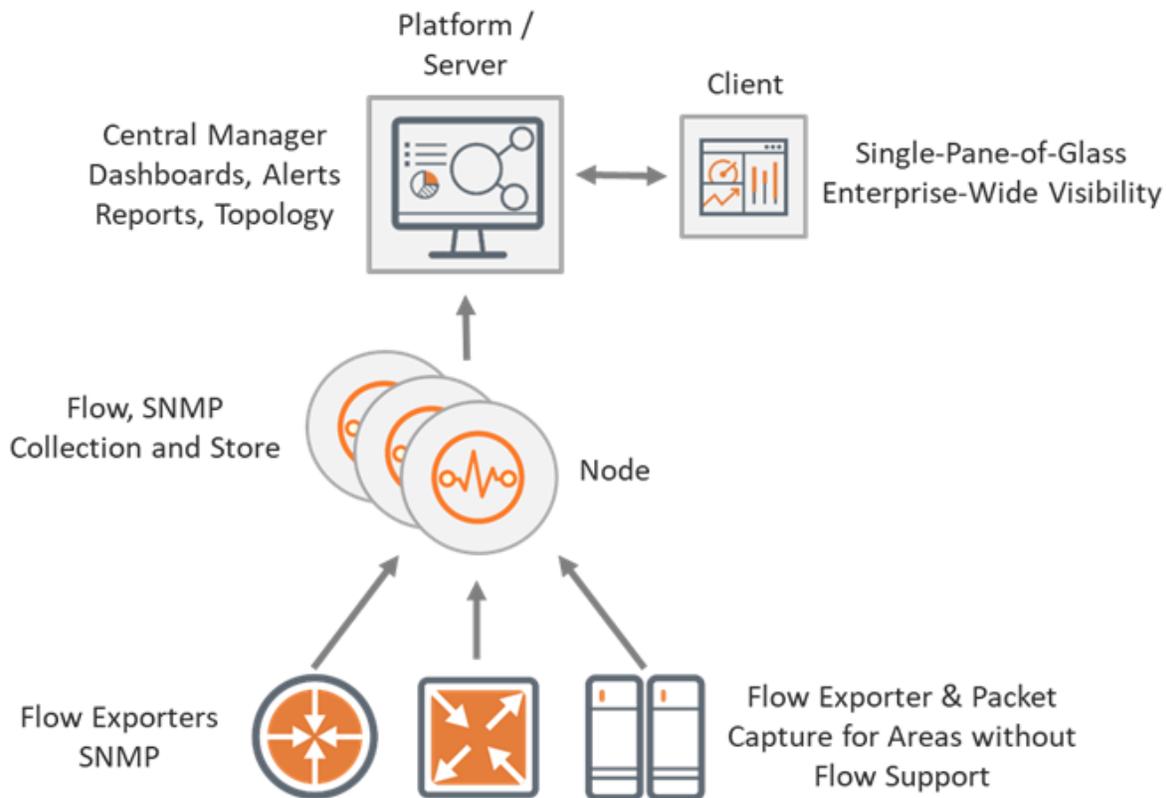DHCP, DNS, ICMP Echo, FTP, HTTP, Jitter, UDP Echo, Video Operations

Latency:
MOS performance measurements, loss, jitter

Large-scale:
Wizard-based IP SLA provisioning in full-mesh and hub/spoke configuration

Integrations and Component Architecture

Platform / Server

Central Manager
Dashboards, Alerts
Reports, Topology

Client

Single-Pane-of-Glass
Enterprise-Wide Visibility

Flow, SNMP
Collection and Store

Node

Flow Exporters
SNMP

Flow Exporter & Packet
Capture for Areas without
Flow Support

Deployment Models:

- Single Server/Node deployed as single system
- Multi-Server with nodes deployed anywhere there is IP connectivity
- Public cloud instance in AWS, Azure or Google Cloud
- Preloaded bundled appliance

LiveNX

LiveNX is a network performance analytics platform with patented end-to-end visualization for a global view of the network and the ability to drill-down to individual devices. Using LiveNX, enterprises gain real- time and continuous insight into network traffic based on application and user level activity. LiveNX offers the ability to gather and analyze volumes of network data at scale from every device, application and user to reduce mean time to repair, and it performs exploratory and explanatory analysis.

LiveInsight

LiveInsight is a cloud-based, add-on software module that integrates with the scalable, tiered architecture of LiveNX to collect, analyze, and generate insights that allows operators to manage the performance of the network, applications and user experience.

LiveNX

LiveUX monitors end-user experience of web applications. By combining the end-user experience metrics with the network performance monitoring information, you can quickly triage performance issues.

- Integrated LiveNX and LiveUX dashboard for instant visibility of site health, network devices, application usage, and application performance (incl. Unified Communications).

- Quickly identify the sites that are experiencing performance degradation and the applications impacted.

- From the site, drill down to examine network conditions including bandwidth utilization, link errors, QoS metrics and applications that are competing for the bandwidth.

LiveNX Monitor of Monitors

LiveNX Monitor of Monitors provides a single-pane-of-glass for server settings, system health, sites and configuration, aggregating multiple geographical or organizationally segmented LiveNX domains. Through an aggregation layer, each LiveNX server domain instance injects relevant data for summary dashboard views and management by way of a north-bound REST API.

System Requirements

Deployment Options

Component	Virtual Appliance (.ova)	Virtual Appliance (Hyper-V)	Amazon Web Services (AMI)	Microsoft Azure	LiveNX Server Appliance
Monitor of Monitors	x	x	x	x	x
LiveNX Server	x	x	x	x	x
LiveNX Node	x	x	x	x	x
LiveNX Analytics Node	x	x			
LiveAgent	x				
LiveSensor	x				

Engineering Console Client

- Windows 7, 8, 10 or Mac OSX 64-bit OS
- 4 Cores
- 8 GB RAM
- Web browser: IE9 and higher, Firefox, Chrome and Safari

Software Packaging: Server/Node Virtual Appliances

- Custom—Less than 25 devices or less than 25k flows/sec; target-ed at small laptop deployments or starter platform, customer able to configure additional data disks
  - 8 vCPU Xeon or i7
  - 16 GB RAM
  - 500 GB data disk
- Small—Less than 100 devices or less than 100k flows/sec
  - 8 vCPU Xeon or i7
  - 16 GB RAM
  - 2 TB data disk
- Medium—100 to 500 devices or less than 200k flows/sec
  - 16 vCPU Xeon or i7
  - 32 GB RAM
  - 4 TB data disk
- Large—500 to 1,000 devices or greater than 200k flows/sec
  - 32 vCPU Xeon or i7
  - 64 GB RAM
  - 8 TB data disk
- Cisco NFVIS Hosted with IOS XE 16

LiveNX Server Appliance (Optional)

- Pre-loaded, tested, and fully integrated LiveNX software
- Linux OS
- 2x Intel Xeon Gold 5118 processors - 24 cores total
- RAM - 96 GB DDR4
- Storage - 32 TB set up as Raid 10 with 16 TB being available for storage
- Two built-in 1GBASE-T ports
- Two built-in 10GBASE-T ports

Management Interface

- Supports remote power control, re-installation, BIOS access, and system management.

Bus

- Two PCI Express 3.0 slots

Environmental

- Operating temperature: 50° to 95° F (10° to 35° C)
- Non-operating temperature: -40° to 149° F (-40° to 65° C)
- Operating relative humidity: 10% to 80% (non condensing)
- Non-operating relative humidity: 5% to 95% (non condensing)
- Heat dissipation (maximum): 2559 BTU/Hour

Power and System Input Requirements:

- 550 W redundant power supply
- AC input voltage: 100–240 VAC
- Rated input current: 7.4 A – 3.7 A
- Rated input frequency: 50–60 Hz

Dimensions and Weight

- Rack-mount 1U appliance
- 17.08-by-1.68-by-27.26-inches (434-by-42.7-by-692.4 millimeters)
- 8.5 lbs (17.5 kg) maximum

Network Device Support

LiveNX : `ck

O   VŒ7

u

O   VŒ

Adtran NetVanta Series Routers	F5 BIG-IP Application Delivery Controller Platforms
Alcatel-Lucent Routers	Gigamon GigaSMART
Brocade Series Routers	Hewlett-Packard Enterprise Procurve Series Switches
Cisco Series Routers (ISR Series, CRS-1, ASR 1000 & ASR 9000 Series Routers, ENCS 5000)	Ixia's Network Visibility Solution
Cisco Catalyst Switches	Juniper MX Series Routers
Cisco Nexus Switches (Nexus 3000, 7000 & 9000 Series)	nTop nProbe
Cisco ASA 5500 Series Firewalls	Palo Alto Networks Firewalls
Cisco AnyConnect Network Visibility Module on Windows and Mac OS X Platforms	Riverbed SteelHead WAN Optimization Controllers
Cisco DNA Center, Cisco APIC-EM Cisco Meraki MX	Silver Peak WAN Optimization Controllers
Cisco NetFlow Generation Appliance	Cisco Viptela vEdge Routers Cisco Viptela VManage API
Extreme Network Switches	LiveAgent

LiveNX IP SLA

Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V are supported.

LiveNX LAN

Cisco Catalyst Series Switches: 2960, 2960-X, 3560, 3650, 3750, 3850, 4500, 6500 and 9000 are supported.

LiveNX Routing

- Cisco Series Routers: 800, 1700, 1800, 1900, 2600, 2600XM, 2800,
- 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR
- 1000V, ENCS are supported.

LiveNX QoS Monitor

- LiveNX QoS Monitor provides quality of service monitoring and trouble-shooting for Cisco router and switches.
- Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600,
- 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200,
- 7600, ASR1000, CSR 1000V
- Cisco ASR 1000 and 9000
  Recommend IOS versions 12.3 or higher or 15.0 or higher for use with the software (IOS XE 2.6.0 or higher for ASR 1000 series). Earlier IOS versions may also work but are not officially supported. General-release IOS versions are recommended, although early- and limited- release versions will also work with LiveNX.

- Cisco Catalyst Series Switches: 3650, 3850, 4500-X and 9000 Limited LiveNX QoS Monitor support on Layer 3-routable interfaces and VLANs depending upon Cisco hardware capabilities.

- Cisco 5000 Series Enterprise Network Compute System

- Cisco Nexus Series Switches: 7000

LiveNX QoS Configure

LiveNX QoS Configure provides for configuring and troubleshooting Quality of Service for Cisco routers and switches.

- Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600,
- 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200,
- 7600, ASR1000, CSR 1000V
  Recommend IOS versions 12.3 or higher or 15.0 or higher for use with the software (IOS XE 2.6.0 or higher for ASR 1000 series). Earlier IOS versions may also work but are not officially supported. General-release IOS versions are recommended, although early- and limited-release versions will also work with LiveNX.

- Cisco Catalyst Series Switches: 9000

- Cisco Catalyst Series Switches: 3850 & 4500-X

- Limited LiveNX QoS Monitor support on Layer 3-routable interfaces and VLANs depending upon Cisco hardware capabilities.

- Cisco Nexus Series Switches: 7000 Series are partially supported