Network and Application Performance Monitoring Platform

LiveNX collects and analyzes data directly from network devices to analyze and present insights to design, policy verification, and operations across the enterprise 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 policies 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 Software-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 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**

**Reporting/Dashboards**
- WebUI enhanced report drilldowns
- Availability dashboards widgets
- Enhanced report scheduling and sharing options
- Added recent report history management
- Business hours support for multi-interface SNMP reports
- Introduced “Situational Awareness” overview dashboard
- Application and voice/video performance reporting and dashboarding enhancements
- Enhanced IPv6 support
- DMVPN Per-Tunnel QoS monitoring
- Catalyst 9k: QoS monitoring via packet rate (CBQoS MIB)
- Added the following reports:
  - Multicast Audit Report
  - Interface Bandwidth and Utilization Summary Reports (SNMP)
  - Daily Interface Bandwidth Summary
  - Interface utilization above threshold overtime
  - Additional report templates

**Topology**
- Enhanced web Geo Topology for large-scale operations

**LiveWire**
- SNMP support
- Additional cross-launch to Omnipeek options

**WebUI Stories**
- WAN Capacity Planning Story
- WAN Interface Utilization Story
- Search by DN (call) Story
Device/System Management
- WebUI Geo-location grouping
- Custom application management (w/NBAR)
- Enhanced dashboard filtering
- Improved system backup and restore for non-snmp managed devices
- Updated Cisco WLC Netflow template support (Higher Visibility)
- Geo-Topology: current alerts status box
- Configurable device auto-refresh time
- Improved Cisco SD-WAN onboarding
- Single Sign-On (SSO) vis SAML (ADFS)

Alerting
- Web: Drilldown from Alert to relevant report
- QoS Class Drop catch-all threshold
- Multi-threshold alerting for:
  - Interface, Device, Site Reachability Alerts
  - Device CPU/Memory Alerts
  - WAN Utilization Alert
- Service Now: Incidents (urgency/sub-category fields)
- SD-WAN Enhancements: vManage alert and event visibility
- Maintenance Mode

LiveAction Network Analytics (LiveNA) (Preview)
- On-premise GPU based appliance(s)
- Anomaly detection of app behavior
- Advanced baselining and analytics

Cloud Monitoring for AWS/Azure (Preview)
- End to End Visibility – both cloud and on-premise
- Visibility across VPC and VNet traffic
- Native flow log visibility

Please contact support@liveaction.com if you are interested in seeing a demo of the Preview products—LiveNA and Cloud Monitoring.

Key Features

Rapid Incident Response with Flow to Packet Analysis
Workflow Optimization
Resolving complex incidents can be challenging when different systems, vendors, devices and software are involved. LiveNX optimizes a rapid incident response workflow with Alert notification or predictive insight where the event is identified for remediation. Within LiveNX’s Engineering Console, NetOps can easily isolate the issue with the visual analytics presented as topology, site or device views. LiveNX presents the time stamp from the Alert and problem isolation from the Flow data, should additional analysis be necessary the NetOps team can quickly cross launch Omnipeek for deep packet analysis for root cause.

LiveWire Integration For Monitoring WAN Edge Segments

The LiveWire Network Monitoring Appliance is optimized for WAN edge applications to provide packet capture and integrated IPFIX Export solution with LiveNX. LiveWire captures and converts real-time packet data which feeds directly into the visualization engine of LiveNX.

Together, LiveWire and LiveNX bring new visual insights and analytics to traditionally “dark” environments such as application classification and performance management for SD-WAN deployments or traditional legacy multi-vendor edge switch environments. LiveWire is extremely powerful for numerous use cases including branch wireless monitoring, point-of-sale transaction troubleshooting and VoIP troubleshooting.
Application Visibility and Control (AVC) Reports

LiveNX presents advanced network performance data with Cisco Application Control and Visibility (AVC) data. With this network data, LiveNX reports on Top Applications Performance and AVC Applications with latency, jitter, packet loss and advanced performance indicators for: sites, devices, users and service provider environments.

Alerting Enhancements – Site Availability

LiveNX offers the broadest suite of integration for Cisco environments. In LiveNX 8, Cisco DNA Center API integration is now available for General Availability, in addition to Cisco Identity Service Engine (ISE), vManage (SD-WAN), SD-Access and PxGrid connectors. These integrations provide rich datasets for LiveNX advanced visual analytics. Real-time Topology Flow Views and forensic playback and analysis are key NetOps elements.

Cisco Integrations

Key Capabilities

Flow and Packet Optimized Workflow for Network Troubleshooting

With both flow and packet level analysis NetOps can now isolate problem areas quickly and have a rapid response ready for any high severity incidents.

With Flow Topology Views and integrated Expert Packet Analysis, LiveNX optimizes the problem isolation to root cause incident management cycle. With integrated ServiceNow ITOM workflows, LiveNX is a key platform for NetOps to resolve incidents faster, and report on status and impact to the business.

Visual Analytics

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 SD-WAN Support (Viptela)
LiveNX consolidates a unified reporting, inventory, and alert notification. For Cisco SD-WAN, LiveNX supports:
• Cisco vEdge, cEdge and ENCS platform support
• Cisco IWAN support
• 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
  • Policy verification
  • Application – VPN – DSCP – Service Provider service status
• 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
• vManage API: BFD (Bidirectional Forward Detection), AppId and Alarms.

Cisco IWAN Support
• PfR configuration of multiple Master Controllers
• Automatically learn semantic settings for PfRv3 monitoring to simplify setup
• PfRv3 multiple data center support

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 problematic 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 visualizations 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 provides 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

LiveNX

LiveNX is a network and application performance monitoring 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.

Omnipeek

- Deep packet analysis
- Vast library of decoders
- Expert system – suggested causes

LiveUX

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 geographically 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

<table>
<thead>
<tr>
<th>Component</th>
<th>Virtual Appliance (OVA)</th>
<th>Virtual Appliance (Hyper-V)</th>
<th>Amazon Web Services (AMI)</th>
<th>Microsoft Azure</th>
<th>LiveNX Server Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUX Application Monitoring</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LiveNX Server</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LiveNX Node</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

LiveNX Deployment

Deployment Options
LiveNX components can be deployed via the following methods: Virtual, Physical, and Cloud. The Virtual Deployment Specifications, as well as the Cisco and Multi-Vendor Device Support lists are provided below.

If you are interested in deploying LiveNX in a Physical, Cloud (Azure, AWS, & Google Cloud), Hyper-V, or KVM environment, please contact LiveAction sales (sales@liveaction.com) for the specifications appropriate for those environments and your needs.

Virtual Deployment Specifications
The LiveNX Server is primarily deployed as a VMware .OVA appliance and is fully operational right out of the box. The server operating system runs on a Linux (TinyCore or Ubuntu) platform.

Server Platform Specifications
- VMware ESXi v5.0 or higher - VMware Hardware Version 8 (vmx-8)
- Network Hardware - At least two Physical NICS on ESXi
  - Support up to 10 Gbps
  - Virtual NICs on OVA are utilizing E1000

<table>
<thead>
<tr>
<th>Proof of Concept (POC)</th>
<th>Small Deployment</th>
<th>Medium Deployment</th>
<th>Large Deployment</th>
<th>Physical Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 25 devices or</td>
<td>&lt;= 100 devices or</td>
<td>100 to 500 devices or</td>
<td>500 to 1000 devices or</td>
<td>1000 or more devices, or &lt;= 350 k flows/sec.</td>
</tr>
<tr>
<td>&lt;= 25 k flows/sec.</td>
<td>&lt;= 50 k flows/sec.</td>
<td>&lt;= 100 k flows/sec.</td>
<td>&lt;= 150 k flows/sec.</td>
<td></td>
</tr>
</tbody>
</table>

Min. Requirements:
- 8 vCPU Xeon or i7
- 16 GB RAM
- LiveNX Server Max Heap Size
- 8 GB
- 500 GB Data Disk

Min. Requirements:
- 16 vCPU Xeon or i7
- 32 GB RAM
- LiveNX Server Max Heap Size 16 GB
- 2 TB Data Disks

Min. Requirements:
- 16 vCPU Xeon or i7
- 64 GB RAM
- LiveNX Server Max Heap Size 31 GB
- 4 TB Data Disks

Min. Requirements:
- 32 vCPU Xeon or i7
- 64 GB RAM
- LiveNX Server Max Heap Size 31 GB
- 8 TB Data Disks

Min. Requirements:
- 48 vCPU Intel Xeon Gold 5118
- Hyperthreading enabled
- 96 GB RAM
- LiveNX Server Max Heap Size 64 GB
- 32 TB Data Disks

Each LiveNX server/node supports up to 76 TB disk space. It is recommended to add each disk in 10 TB increments.
Server IOPS Recommendation LiveNX 8.0 - 1000 IOPS Read and 4500 IOPS Write.
Client Platform Specifications

- Windows or macOS
- 4 Cores
- 8 GB RAM
- Web browser: IE11 and higher, Firefox, Chrome, and Safari

### Network Device Support

**LiveNX Flow**
LiveNX Flow provides advanced end-to-end system-level flow visualizations for multi-vendor networks. The following devices have gone through flow-analysis testing with LiveNX.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Supported Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adtran NetVanta Series Routers</td>
<td>F5 BIG-IP Application Delivery Controller Platforms</td>
</tr>
<tr>
<td>Alcatel-Lucent Routers</td>
<td>Gigamon GigaSMART</td>
</tr>
<tr>
<td>Brocade Series Routers</td>
<td>Hewlett-Packard Enterprise Procurve Series Switches</td>
</tr>
<tr>
<td>Cisco Series Routers (ISR Series, CRS-1, ASR 1000 &amp; ASR 9000 Series Routers, ENCS5000)</td>
<td>Ixia’s Network Visibility Solution</td>
</tr>
<tr>
<td>Cisco Catalyst Switches</td>
<td>Juniper MX Series Routers</td>
</tr>
<tr>
<td>Cisco Nexus Switches (Nexus 3000, 7000 &amp; 9000 Series)</td>
<td>nTop nProbe</td>
</tr>
<tr>
<td>Cisco ASA 5500 Series Firewalls</td>
<td>Palo Alto Networks Firewalls</td>
</tr>
<tr>
<td>Cisco AnyConnect Network Visibility Module on Windows and macOS X Platforms</td>
<td>Riverbed SteelHead WAN Optimization Controllers</td>
</tr>
<tr>
<td>Cisco DNA Center, Cisco APIC-EM Cisco Meraki MX</td>
<td>Silver Peak WAN Optimization Controllers</td>
</tr>
<tr>
<td>Cisco NetFlow Generation Appliance</td>
<td>Cisco vEdge/vEdge Routers Viptela VManage API</td>
</tr>
<tr>
<td>Extreme Network Switches</td>
<td>Endpoint Agent</td>
</tr>
</tbody>
</table>

**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, ENCS 1000V 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 supported.

**LiveNX QoS Monitor**
LiveNX QoS Monitor provides quality of service monitoring and troubleshooting 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