LiveAction

LiveNX Technical Data Sheet

Technical Data Sheet

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, SNMP, API, and Packet Data Visualization 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

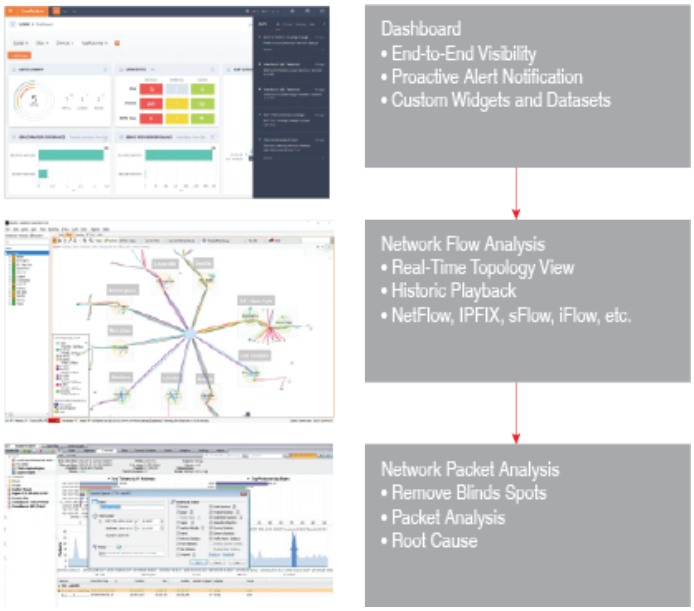
Utilize application and path visualizations to effectively validate WAN Return-on-Investment (ROI) for traditional MPLS, hybrid, or Software- Defined WAN (SD-WAN). When a network element makes a path change to protect the applications due to an Out-of-Policy (OOP) condition, LiveNX renders the end-to-end 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 (vManage BFD (Bidirectional Forward Detection) and AppId (Application Identification to provide accurate visual analytics)).

Key Features

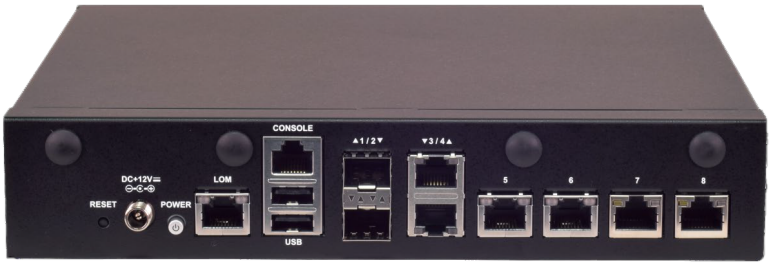
Rapid Incident Response with Flow to Packet Analysis Workflow Optimization

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.



Rapid Incident Response for Faster Incident Resolution

LiveWire Integration for Monitoring WAN Edge Segments



LiveWire Edge 1515 — WAN Edge Continual Monitoring

The LiveWire Network Monitoring Appliance is optimized for WAN edge applications to provide packet capture and integrated LiveFlow 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 traditioal legacy multi-vendor edge switch environments. In addition, there application performance dashboards and forensic cross link capability making it possible to filter and analyze data to uncover potential security threats below with the ability to seamlessly pivot back to the packets. LiveWire is extremely powerful for numerous use cases including branch wireless monitoring, point-of-sale transaction troubleshooting and VoIP troubleshooting.

LiveAssist

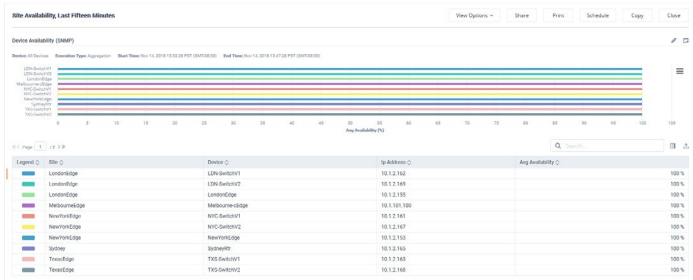
LiveAssist is a new generative AI product which allows correlation of alerts, anomalies, and security events. LiveAssist provides a natural language interface to quickly locate potential trouble areas on your network. Additionally, for certain alerts (when enabled), RCA recommendations are computed in the cloud and sent back to LiveNX for display within the UI.

Flow Reporting

LiveNX provides a wide range of advanced flow, SNMP, Cisco SDWAN report capabilities such as AVC reports, Application Reports, Site/Device/Interface Availability reports, Bandwidth Reports, etc.

Alerting

LiveNX provides a wide range of Alerting Capabilities such as Device reachability, site reachability, Flow Stop, Cisco SDwan alerts, IPSLA alerts, etc. LiveNX also provides the capability for root cause analysis of alerts.



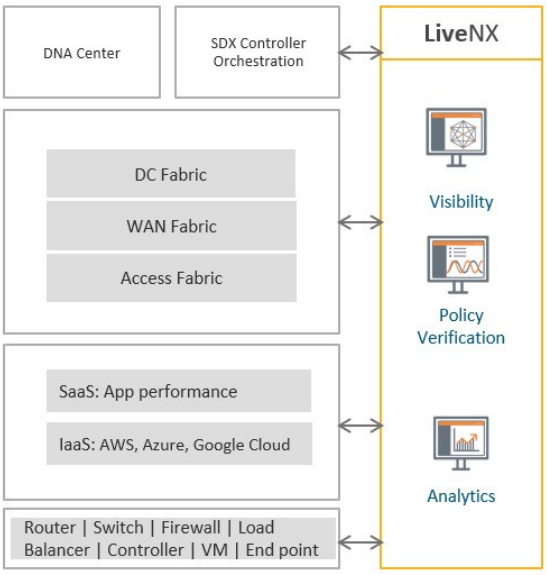
LiveNX Operations Dashboard — Current Alerts by Site

Dashboard

The LiveNX Dashboard provides quick navigation and exploration of the health and performance of the network and applications running on it. Dashboards are a collection of widgets that are can be customized and organized as desired. Each user can have up to 12 tabs of dashboards.

LiveNX also provides three different categories of Grafana dashboards such as Flow dashboard, Analytics Dashboard and Monitoring Dashboard.

Cisco Integrations



LiveNX Cisco DNA Center Integration

LiveNX offers the broadest suite of integration for Cisco environments, including 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.

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 integration capabilities of ServiceNow, Syslog and webhook servers, LiveNX is a key platform for NetOps to monitor and 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 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.

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.

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

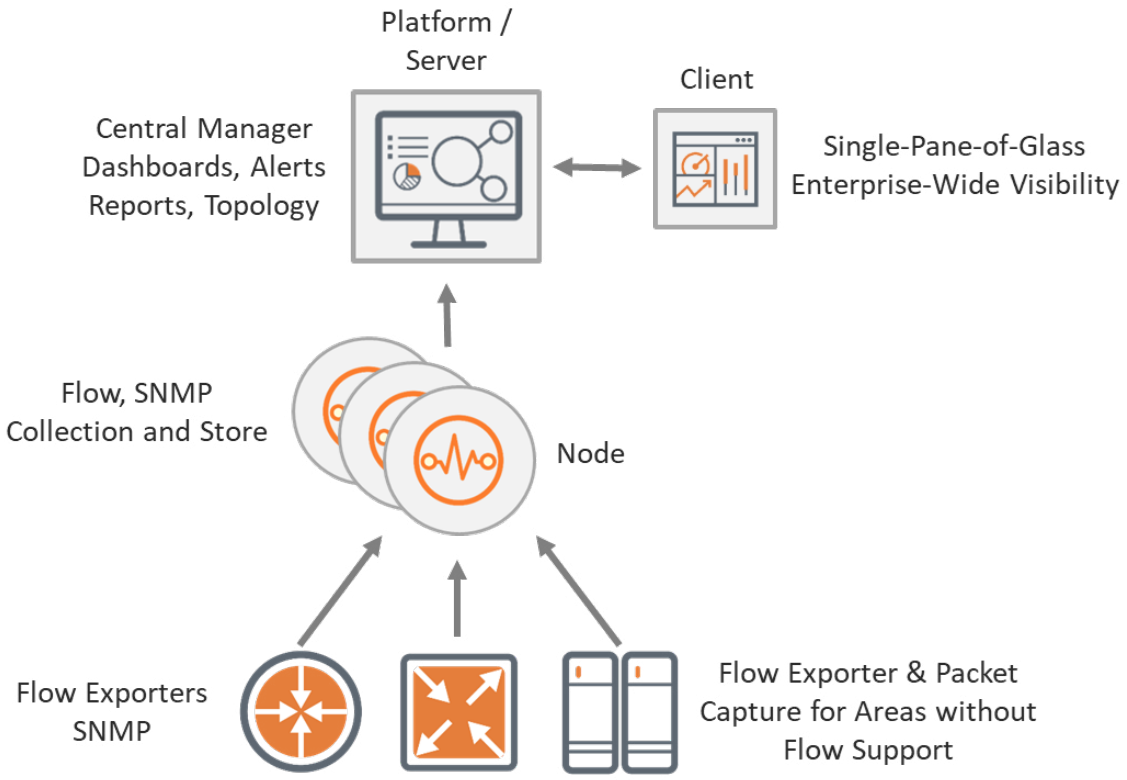
Latency:

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.

LiveWire

LiveWire is the only solution designed to collect and process the data that network engineers need – both network telemetry and network packets. LiveWire integrates with LiveNX to extend network monitoring and application troubleshooting to remote sites and branches, the WAN edge (including SD-WAN), data centers, and the cloud. When telemetry data is not enough to solve complex problems, easily transition from monitoring to packet-level forensics and back using LiveNX as your single pane of glass.

Deployment

LiveNX components can be deployed via the following methods: Virtual, Physical, and Cloud..

Component	Virtual Appliance (OVA)	Virtual Appliance (Hyper-V)	Amazon Web Services (AMI)	Microsoft Azure	Google Cloud (GCP)	Oracle Cloud (OCI)	LiveNX Server Appliance
LiveNX Server	✔	✔	✔	✔	✔	✔	✔
LiveNX Node	✔	✔	✔	✔	✔	✔	✔

System requirements

Below are the system requirements for LiveNX.

Items	Minimum Requirements for New Medium OVA	Minimum Requirements for New Large OVA
FPS (K)	100K	150K
CPU	32 vCPU Xeon	64 vCPU Xeon
RAM	128 GB	256 GB
Data Disk	8 TB	16 TB

New Flow Ingestion Scale Matrix.

Appliance	Ingestion FPS w/o CH Enabled for Flow	Ingestion FPS with ClickHouse Enabled for Flow
6200 Gen-2	500K	350K
6210 Gen-3	800K	600K
Legacy OVA Large	150K	100K
New OVA Large	250K	150K

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.

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, ENCS5000)	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 macOS 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 vEdge/cEdge Routers Cisco Viptela VManage API
Extreme Network Switches	Endpoint Agent

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, 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 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