Where Too Much Technology Would *Never* Be Enough

A Packet *Pushers* Whitepaper

LiveAction:

Insight and Service Assurance for Your Software-Defined Network

Software-defined networks are complex beasts. They're carrying more data at greater throughputs, across a broader suite of Internet and telecommunications services. They support an increasing variety of applications, including voice and video, that require network optimization for a positive user experience.

To deliver the application experience across the SD-WAN overlay, the mapping and managing of the 'what' and 'how' present challenges. Most network management tools extract configuration, and SDN controllers or intelligent network elements focus on policy enforcement by resolving a declarative, high-level policy into more detailed imperative network element configuration.

A declarative model focuses on the intent, or WHAT is to be accomplished, without describing HOW it is to be accomplished. For example, a network operator may express that an application such as voice is business-relevant – meaning that it is to be treated with the appropriate quality of service – but the details of how the QoS policies are to be configured across the underlay infrastructure is not defined.

It's the job of network operators and engineering to monitor and manage this growing complexity, tying applications and resource consumption to business policies (intent).

For network professionals to succeed as they adopt intent-based networking, they need visibility and insight into what's happening on the network to get the assurance that declarative policies have been successfully resolved. This service assurance is key to intent-based networking delivering on its promise.

Network professionals also need smart analysis of real-time and historical data to help them make sense of what's going on and to respond quickly and effectively to problems.

These demands have given rise to software-defined tools and platforms that aim to tackle this complexity and provide a better view of network and application performance.

In particular, SD-WAN is attracting enterprise attention for a variety of reasons. SD-WAN lets companies mix and match connectivity at branch offices, including MPLS, business broadband, and 3G/4G LTE, and to send applications over a specific link based on end-to-end application service requirements and business policies.

SD-WAN also helps companies cut WAN costs and shorten provisioning time by letting organizations replace expensive private circuits with lower-cost, more readily available broadband connections.

While those are compelling benefits, WAN visibility and service assurance becomes even more critical in SD-WAN environments. There are several reasons for this.

First, hybrid IT is the new normal. Users access applications that reside in the corporate data center and multiple cloud environments. And while some applications are business critical, others clearly are not.

And while IT might not own 100% of critical business apps (think Salesforce or Office 365, for example), it's still held responsible for the user experience. IT will be the first to get a call if an application is slow or the VoIP quality on a collaboration meeting or video session is poor.

To ensure that IT can respond to user experience issues, fix the problem, and report on root cause for governance or audits, you need deep visibility into the network. You need visibility that spans application performance from the data center all the way to the branch edge and across multiple cloud environments.

Second, organizations considering SD-WAN technology need to have visibility into their existing WAN deployments (current state). It doesn't make sense to roll out a new technology without understanding current conditions and usage. The baseline performance characteristics are critical to document before the migration, so you can audit and report on the positive business outcomes achieved from the SD-WAN investment (future state).

Third, even if organizations plan to roll out SD-WAN appliances or software to every single branch, they're still going to operate in a hybrid environment consisting of multiple generations of network routers, controllers, and possibly different vendor equipment

For example, during an SD-WAN rollout you can't expect an instantaneous cutover at every location. Hence, you'll be running parallel legacy routers and WAN devices alongside your SD-WAN gateway devices throughout the duration of the deployment project.

And many companies may continue to operate existing branch equipment, such as routers and firewalls, even with SD-WAN appliances or software in place, depending upon the financial depreciation cycle and operations plans.

Given this mixed environment, organizations need a mechanism to understand how links are currently performing, the kinds of applications and services in use, and whether branch and remote offices are saturating connections.

By having a clear picture of the differences in application usage, performance, and bandwidth requirements for individual sites, you can apply more impactful policies and architect the underlay WAN to best meet the requirements of each branch type.

Depending on the kind of organization, different types of branches will have different requirements. For instance, a manufacturer may have some branches dedicated to manufacturing, some to sales, and some to basic back-office functions such as billing and payroll.

Or, a sales office may prioritize real-time voice and video communications, while a back-office branch will emphasize both a fast connection to the organization's core data center applications as well as require strong performance for SaaS-based business apps.

The upshot of all this is that a software-defined environment requires a comprehensive view of the network that provides broad and deep insights on both network and application performance.

This is where LiveAction comes into play.

LiveAction and Continuous Insight

LiveAction uses NetFlow, IPFIX and other flow records, SNMP, and deep packet inspection (with NBAR2 [Network Based Application Recognition] and AVC [Application Visibility and Control] through a strategic relationship with Corvil) to build a detailed model of the real-time network topology, from the data center to the branch and to the end point.

The UI can show you every device a flow traverses from source to destination, including routers, switches, firewalls and any other network devices in between.

Operators can then drill down from a summary view to site, device, interface or application details to get the information they need. You can examine flows from source to destination based on application type (Web, voice, video, and so on) and examine individual conversations leveraging NBAR2, Medianet (PerfMon), or AVC to identify and debug over 1,000 unique applications.

You can also click on specific network devices to get detailed information, such as the interface that a flow traversed; and key performance metrics such as CPU utilization, QoS policies, DSCP markings, packet loss, jitter, and more.

The LiveNX platform can also integrate application metrics based on user experience to provide an even more comprehensive view of overall performance.

LiveAction's patented visualization capabilities are a competitive differentiator. That's because the platform takes real-time raw flow records and transforms them into intuitive, navigable network maps that cleanly and concisely illustrate where and how traffic moves across your network.


LiveNX – Operations Dashboard and Engineering Console

A color-coded classification system breaks out flow conversations into general categories such as Web traffic, enterprise applications, voice calls, video, and other core application types.

Operators can filter on a variety of metrics for deeper analysis, as well as get spreadsheet-style breakouts of elements such as source and destination addresses and ports, TCP flags, and other details.

LiveNX continuously collects and analyzes flow records so that you can get both real-time views and historical network performance information for forensic analysis to determine who did what when.
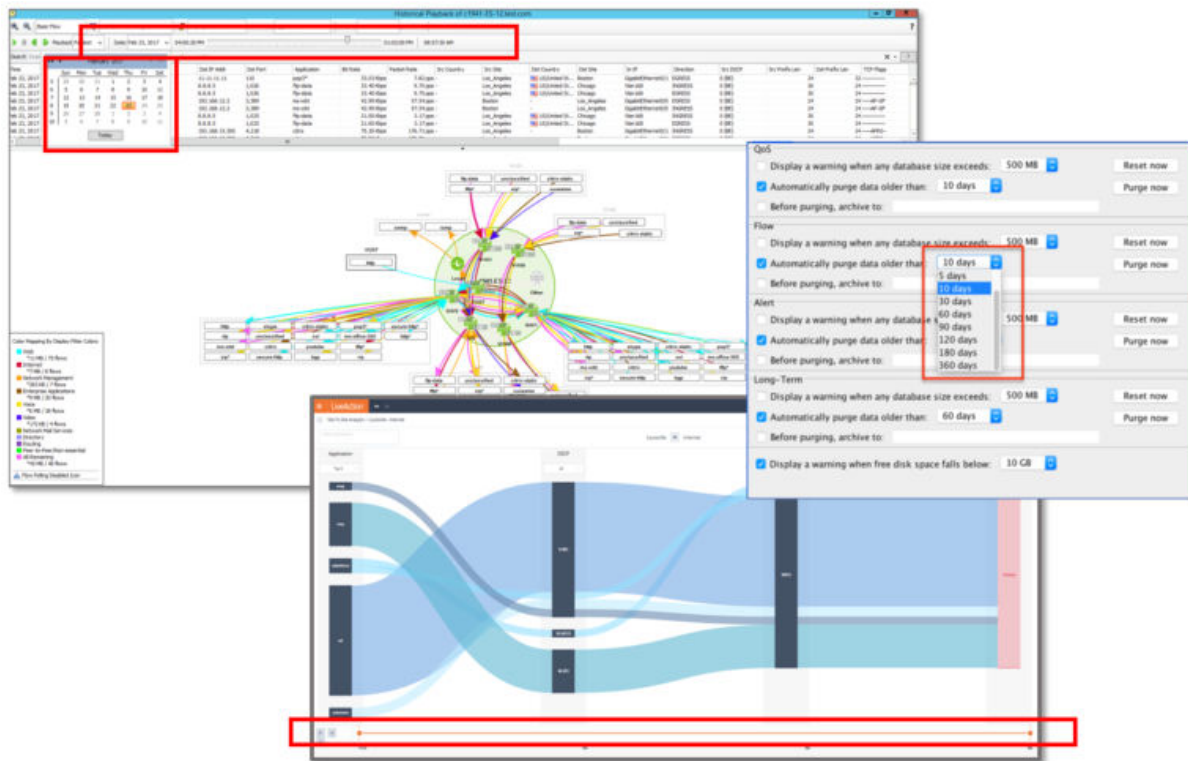

LiveNX – Historical play-back

LiveNX for Network Performance Management

LiveNX is the core platform for LiveAction's performance management solutions. It is architected for scale, consisting of a 3-tier structure including a management interface to applications such as LiveInsight, LiveUX, and LiveAgent; a server for

regional consolidation and management; as well as collection nodes that receive flow records from network devices.

All are software-based, packaged as OVAs for deployment in VMs or as an AMI image for Amazon Web Services.
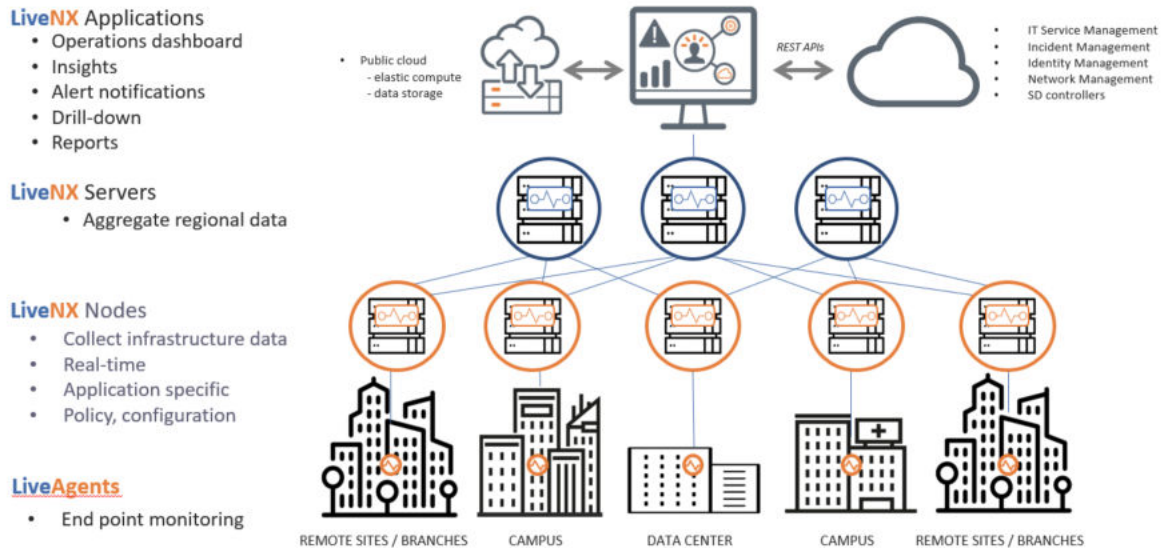
LiveNX Distributed Architecture

A collection node is essentially a server running a Linux-based virtual appliance. These nodes can be deployed directly in branch and remote offices as well as in the data center headquarters. If a branch or remote office is too small to support a collection node, administrators can configure flow records to be directed to a node in the data center.

Note that nodes must be properly sized based on the volume of flow records generated, as they can scale to 1 million flow records per second. Minimum requirements for a server that will handle fewer than 100,000 flow records per second include an 8 Core 2+ GHz CPU, 8 GB RAM, and 2-6 TB 7,200 RPM hard drive.

LiveNX supports NetFlow v5/v9, IPFIX, sFlow, Z-Flow, J-Flow, cFlow, and NetStream.

LiveUX for Application Performance Monitoring

In addition to network performance, LiveAction can also monitor users' experience of Web applications—both on premises and in the cloud—to provide a more comprehensive picture of performance.

LiveUX uses software agents for application monitoring. You can deploy private agents on premises near where your users reside, and global agents that are hosted by LiveAction all over the world.

These agents test Web and SaaS applications to measure load times for the full Web page as well as individual elements of page, as well as track metrics such as DNS response times and network latency.

Administrators can also use ping for basic up/down status and traceroute to show the network path.

These tests are useful for triage and to narrow the scope of a troubleshooting exercise. For instance, if a user says they can't reach a SaaS app, an administrator can run a test using an agent either on premises or a global agent hosted off site.

If the global agent cannot reach the SaaS app, this may indicate a local problem.

LiveAction integrates LiveNX and LiveUX such that if an administrator finds a problematic link within LiveUX that's being monitored by LiveNX, he or she can then examine flow data to get more details about network performance issues.

LiveUX can also show if a problematic node is operated by a third party such as a service provider or carrier.

The LiveAction Value Proposition

LiveAction positions its value to the enterprise in four broad areas: simplicity, visibility, analysis, and control. Let's look at each one in turn.

© Packet Pushers Interactive, LLC

Simplicity

LiveAction takes complex information about your traffic and the nodes that traffic traverses and presents it in a format that lets you grasp key details simply and clearly. A picture really is worth a thousand words.
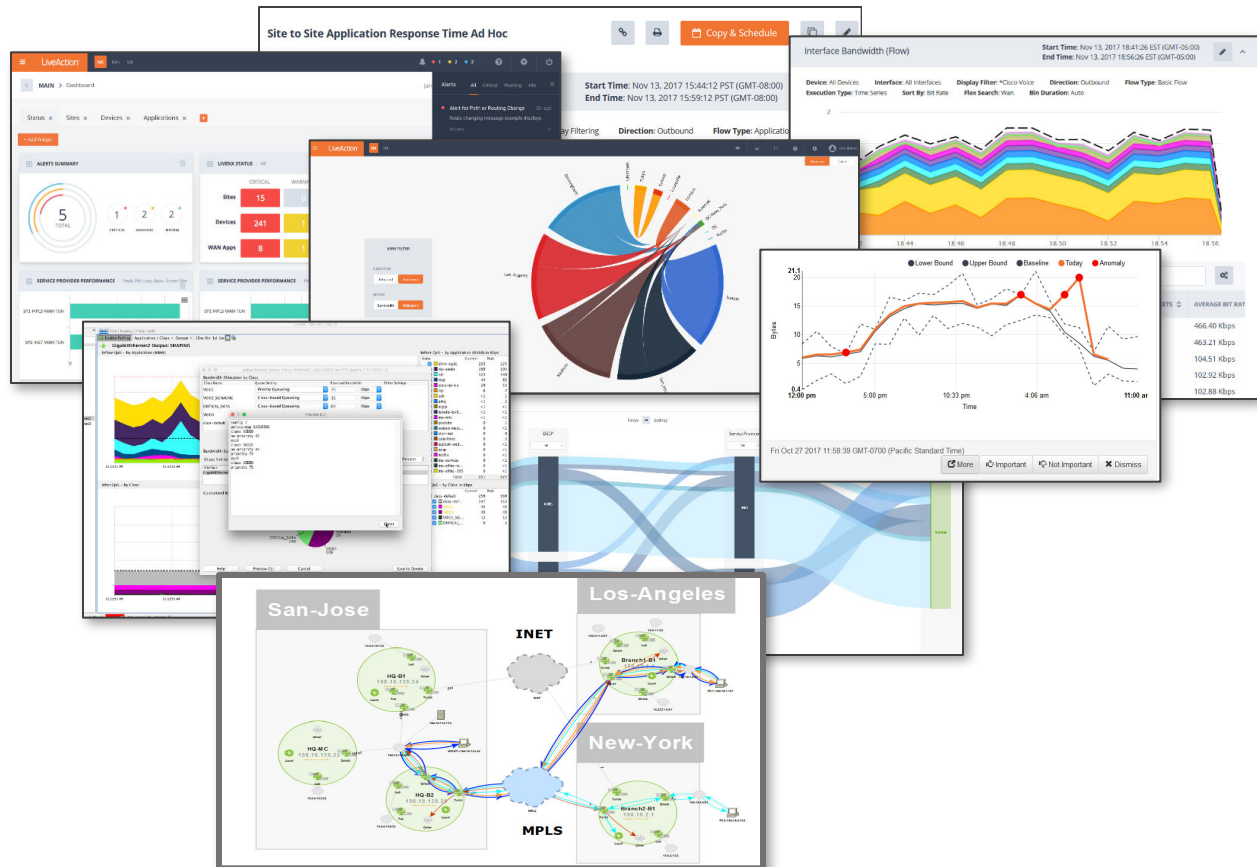
And because it can present a complete end-to-end picture, from source to destination with every site, device, and hop in between, operators don't have to hunt among dashboards, management consoles, and opaque carrier or service provider portals to understand what's happening in the WAN.

This simple view, which also enables operators and administrators to dig in for more detail, provides independent validation of network performance and service assurance. That's valuable information that can be used with providers, partners, and your counterparts on the business side of the house to report on SLAs, support audits, and work collaboratively with the application teams.

Visibility

SD-WAN lets you use multiple providers at a single branch or remote office, allowing you to mix and match pricing and capacity based on your requirements, and to get the benefits of having providers compete for your business.

At the same time, sending traffic across multiple providers also increases complexity. When a user, customer, or executive asks, "What's going on with the network?" you want to have a ready answer.

With LiveAction, you have a clear view into:

- What applications are running and are they performing within the target service levels
- The full end-to-end data path, including provider networks to validate QoS policies and ensure traffic is not being remarked
- Real-time and historical views for service assurance and root cause forensics
- Your data center and all branch and remote locations with summary alarms

LiveAction scales to thousands of nodes while still providing a single GUI to get a complete picture of your network.

Analysis

While visibility is key, administrators can also use LiveAction to proactively analyze network and application performance. Detailed reports can show top applications and conversations to help organizations understand where and how bandwidth is being consumed, in addition to threshold crossing events such as path reroutes or interface utilization.

If LiveAction is being used in an SD-WAN use case, this information can influence how policies are applied in SD-WAN gateways or controllers to enforce business priorities.

Administrators can also get details on individual network devices including CPU utilization, memory usage, interface statistics, and errors.

Administrators can also set thresholds or severity levels to trigger alerts for events such as changes in BGP peering or routing changes.

LiveAction also offers LiveNX Insight, which is an add-on software module that uses machine learning to analyze real-time and historical data to deliver proactive insights directly to IT Operations.

Using this analysis, LiveNX can identify patterns to spot anomalies, detect path changes, and identify new applications that appear on the network.

The machine learning software can then provide contextual alerts to help the human-in-the-loop respond to these issues. In addition, LiveInsight can incorporate feedback based on operator actions to help teach it about relevant events and issues.

Control

Besides visibility and performance monitoring, LiveAction allows you to manage QoS configurations and policies (assuming you have security privileges).

However, rather than using a command line to set service quality, which can lead to errors and misconfigurations, LiveAction provides a GUI that lets administrators generate the correct instructions based on Cisco best practice CVDs (Cisco Validated Designs), and then automate the implementation on the appropriate network devices.

LiveAction: A Cisco Insurance Policy

Many companies rely on Cisco for their network infrastructure in the campus, the data center, and the WAN. LiveAction is a Cisco Solutions Partner and part of the Cisco Investments' portfolio, making it well-suited to be deployed in Cisco environments.

But even if you're an all-Cisco shop, you can't get a unified network view from Cisco. For example, Meraki has its own management and monitoring interface, which is

separate from IWAN, which is separate from Viptela, Cisco's most recent SD-WAN acquisition.

This is where LiveAction can serve as an insurance policy for your Cisco investments, as technology migrations may well be in your future. In addition to providing a unified view of network visibility and performance assurance across the network, LiveAction also deeply integrates with key Cisco product instrumentation such as NBAR2, Medianet (PerfMon), AVC, NetFlow, and routing.

Cisco IWAN – Intelligent Wide Area Networking

Cisco's IWAN solution leverages the ISR and ASR router platforms with add-on software capabilities to provide feature-rich services for branch and remote offices, including application identification and performance-based path selection.

LiveAction integrates with Cisco IWAN to provide visibility into, and management of, the IWAN environment. In particular, LiveAction can:

- Visualize before-and-after path changes made by Cisco's PfR (Performance Routing) module
- Leverage NBAR2 to identify applications, map the interfaces they traverse, and tie them to performance metrics such as server and network response times to speed troubleshooting
- Track and control QoS settings on Cisco routers by application type

Cisco APIC-EM - Application Policy Infrastructure Controller - Enterprise Module

LiveAction also integrates with the EasyQoS app on APIC-EM, Cisco's Software Defined controller for enterprises. Using LiveNX REST-based APIs, LiveNX monitors instrumentation such as application bandwidth and traffic class, and can report the business relevance tags assigned to applications in APIC-EM.

Administrators can also adjust QoS settings from the LiveNX console, allowing APIC-EM to serve as the system of record, while using LiveNX as the system of change.

Viptela and Meraki SD-WAN

LiveNX delivers unified network performance management across the entire lifecycle of SD-WAN migrations including support for Cisco SD-WAN (based on Viptela), Cisco IWAN and Cisco Meraki technology. With LiveNX, you get complete visibility into the SD-WAN overlay and underlay network infrastructure.

LiveNX can also ingest flow records and other data from Viptela and Cisco Meraki to monitor end-to-end network and application performance, ensure services are meeting SLAs, identify application and bandwidth use, and use consumption metrics for capacity planning.

LiveNX consolidates a unified reporting, inventory, and alert notification for Cisco IWAN and Cisco SD-WAN which provides:
- Device monitoring credentials, including SNMP settings
- Viptela device inventory, including vEdge routers and management devices like vManage, vBond, and vSmart
- Visibility into relevant interfaces for monitoring from each vEdge router
- Network semantic information per device and interface:
    o Site association per device
    o Site geo location
    o WAN interfaces per device
    o Service Provider associated with each WAN interface. Note: Viptela refers to the service provider information as "colors"
    o Capacity of WAN links (inbound and outbound)
    o Site IP mappings
    o Determine if a device is in the datacenter
    o Viptela VPN ID mapping to a VPN name. The VPN ID is synonymous to a VRF. Viptela may or may not associate VPN IDs to names, as is the case with Cisco

A Comprehensive Ecosystem

While LiveAction has strong ties to Cisco infrastructure, the company can also integrate with routers, switches, load balancers, firewalls, ticketing systems, and SD-WAN gateways from a variety of companies, including

- Riverbed
- Silver Peak

- Juniper
- Palo Alto Networks
- ServiceNow

This broad support means organizations can get visibility, insight, and performance monitoring in heterogeneous network environments.

Conclusion

Networks are supporting more applications, pumping out more data, and doing it all faster than ever before.

All of this creates unprecedented complexity for IT Operations and Network Engineering teams who need to understand how data and apps move across the network, identify applications and bandwidth consumption, monitor and report on performance, and respond quickly to incidents.

LiveAction gathers and analyzes flows, SNMP, and other data such as NBAR2 to provide real-time and historic analysis of network and application performance and how it ties to business policies.

Its intuitive GUI and growing capabilities in machine learning provide more than just alarms and alerts. Operators get actual proactive insights they need to monitor and troubleshoot the networks they have, and to plan the networks they'll build.

Find Out More

Learn How to Future-Proof your SD-WAN Investment. Watch the on-demand webinar from Live Action and Packet Pushers.

For more information on SD-WAN visibility and assurance solutions, visit www.liveaction.com