1

Agenda – Day 1

- LiveNX Overview & Architecture
- The LiveNX WebUI
  - Dashboards
  - Sites/Devices/Interfaces
  - Reports Overview
    - Stories
    - Scheduling
    - Custom Reports
  - System Management
- LiveNX Engineering Client
  - Dashboard
  - Reports
- Visualizations & Troubleshooting
  - Voice, Video, Delays
- Flow Collection
- Custom Filters
- Add & Manage Devices
  - Adding Devices
  - Grouping & Objects
  - Device Semantics
- Topology Definition
- More Dashboards, Reports and Alerts
- QoS Monitoring and Configuration

LiveAction
2

2

Agenda - Day 2

- Implementation Best Practices
  - Installation Considerations
  - Netflow Best Practices
  - Other Best Practices
- Quality of Service
  - Concept Overview
  - Classification & Marking
  - Queueing & Shaping
  - Policing & WRED
  - Buffer Tuning
- Deployment Strategies
- LiveAction SD-WAN
  - Cisco/Viptela SDWAN Overview
  - LiveNX – SDWAN Integration Overview
  - Day 0: Cisco SD WAN Planning for Deployment
    - LiveNX - SDWAN Onboarding
  - Day 1: Cisco SD WAN Policy Validation and Intent
  - Day 2: Cisco SD WAN Operations

LiveAction
3

3

Class Logistics

- Daily Schedule
  - Start
  - Breaks
  - Finish
- Equipment
  - Laptops
  - Internet Access
  - eLab Access

LiveAction 4

4

Your Training Resource…

Dave Lau

Senior Technical Trainer

LiveAction 5

5

Prerequisites

- You already:
  - Have a basic knowledge of applications, networking, and protocols…
  - Understand TCP/IP, network addressing, and subnet masks
  - Know basic router & switching concepts
  - Manage NetFlow devices within your environment

LiveAction 6

6

And you are…

- Name ?
- What do you do at your company ?
- Have you used LiveAction Products?
- What Product Certs do you maintain? (Brag if you must;-)
- What was your first car?

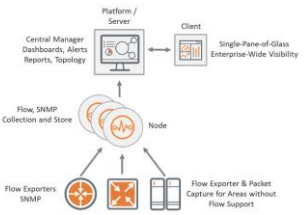
LiveAction 7

7

8

Architecture Overview

- **Distributed Computing Architecture**
  - High-performance database
  - Large-scale distributed analytics platform
  - Capable of handling 1M+ flows/sec
  - Monitor 40,000+ devices across distributed deployment
  - Visualize up to 1,000 active interfaces per device
  - 3-layer architecture – **client**, **server**, **node**
- **Client**
  - Single Pane of Glass (SPOG) over entire network
  - Limiting user data access by groups per node
  - Browser, Windows (32/64-bit), or Mac OSX
- **Server**
  - Central management of nodes
  - Virtual install - HyperVisor, Hyper-V, KVM
- **Collector Node**
  - Hold data store, automatic data management
  - Node management policy set at server
  - Virtual install - HyperVisor, Hyper-V, KVM



LiveAction 9

9

System Requirements

http://www.liveaction.com/support/specifications/

- 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 E100

Proof Of Concept (POC)	Small Deployment	Medium Deployment	Large Deployment	Physical Deployment
<= 25 Devices or <= 25k Flows/sec.	<= 100 Devices or <= 50k Flows/sec.	100-500 Devices or <= 100k Flows/sec.	500-1000 Devices or <= 150k Flows/sec.	Upto 1000 Devices or <= 500k Flows/sec.
Min Requirements: • 8 vCPU Xeon or i7 • 16 Gb RAM • Max Heap Size 8GB • 500GB Data Disk	Min Requirements: • 16 vCPU Xeon or i7 • 32 Gb RAM • Max Heap Size 16GB • 2TB Data Disk	Min Requirements: • 16 vCPU Xeon or i7 • 64 Gb RAM • Max Heap Size 31GB • 4TB Data Disk	Min Requirements: • 32 vCPU Xeon or i7 • 64 Gb RAM • Max Heap Size 31GB • 8TB Data Disk	Min Requirements: • 64 vCPU Xeon Gold 5218 • 768 Gb RAM • Max Heap Size 384GB • 32TB Data Disk (16TB usable with RAID 10)

LiveAction

10

Network Devices Supported

http://www.liveaction.com/specifications/

Cisco Device Support – SNMP & Flow
ASR 9000 Series Router
Cisco AnyConnect Network Visibility Module on Windows and Mac OS X Platforms
Cisco ASA 5500 Series Firewalls
Cisco Catalyst Series Switches 2900, 3650, 3850 & 4500-X 6500, 6800, 9000 are supported.** (Limited LiveNX QoS Monitor support on Layer 3-routable interfaces and VLANs depending upon Cisco hardware capabilities.)
Cisco ISR Series Routers: 800, 900, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4200, 4300, 4400, 4500, 7200, 7600**, ASR 1001x, 1002x Series Routers, CSR 1000V**
Cisco Meraki MX Security Appliance
Cisco Nexus Switches (Nexus 3000, 7000, 6000 & 9000 Series)
Cisco NetFlow Generation Appliance
Cisco SD-WAN vEdge, Cisco IOS XE SD-WAN Edge Devices

Multi-Vendor Device Support – Flow
Adtran NetVanta Series Routers
Alcatel-Lucent Routers
Barracuda Firewall
Brocade Series Routers
Checkpoint Firewall
Citrix NetScaler Load Balancer
Extreme Network Switches
F5 Load-Balancer
Gigamon GigaSMART
Hewlett-Packard Enterprise Procurve Series Switches
Ixia's Network Visibility Solution
Juniper MX Series Routers
Ntop nProbe
Palo Alto Networks Firewalls
Riverbed SteelHead WAN Optimization Controllers
Silver Peak WAN Optimization Controllers
Sophos Firewall
Ziften ZFlow

LiveAction

11

Bandwidth Overhead – Server/Node

- Data is stored on the **Collector Nodes**
- Server requests data from Node(s) on demand
  - In case of loss of communication, server may initiate to reestablish communications
- Minimal synchronization communication between the Server and Node(s).
  - "Keep-alive" (not really… more a "I have new data!")
- Bandwidth is proportional to the number of devices being monitored by each Node
- End-user actively monitoring LiveNX also increases bandwidth.

Examples of Node/Server Bandwidth

Devices Per Node	Node to Server Traffic (Avg./Peak)	Server to Node Traffic (Avg./Peak)
100	125Kbps/1.2Mbps	5Kbps-25Kbps
500	625Kbps/ 1.75Mbps	25Kbps-125Kbps
1000	1.25Mbps/ 2.25Mbps	50Kbps/ 250Kbps

Note: These are typical bandwidth estimates that LiveAction would expect to see. Each network is different so results may vary.

LiveAction

12

LiveNX Flow Capabilities

LiveNX is a *flow collector*

- Supports NetFlow V5/V9, FNF, sFlow, jFlow, IPFIX, and other multi-vendor flow types
- Provides unique end-to-end flow visualization for a holistic view of the network
- Provides hop-by-hop color-coded application and flow path analyses for network and application performance issues
- Visually shows mis-marked DSCPs for traffic priority
- Easily enables Cisco advanced flow technologies
- Topology can be exported to Visio
- Keep all raw data as long as there is sufficient disk space

LiveAction 13

13

LiveNX Communication with Devices

LiveNX uses SSH or Telnet access to read IOS configurations, as well as to make desired configuration changes to the device(s);

- QoS Configurations
- Netflow Configurations
- IP SLA Configurations
- Policy Based Routing

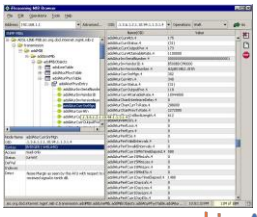
LiveNX does not save the router configuration in our database!

LiveAction 14

14

LiveNX Communication with Devices

- LiveNX uses SNMP v2 or v3 RO (Read Only) access to devices
- Polling for reading the MIB (Management Information Base)
  - CBQoS MIB
  - IP SLA MIB
  - LAN MIBs
  - Routing MIBs
- Updates statistics according to user configured polling intervals



LiveAction 15

15

LiveNX Network Protocol Requirements

Protocol	Port Number	Direction	Description
TCP	7000	Java Client to NX Server	Java Client Access to Platform
TCP	443	Web Browser to NX Server	User Access to Web UI of Platform
TCP	7026	Server to Node (Bidirectional)	Server <-> Node Communication
UDP	2055	Network devices to nodes	Netflow Export
UDP	161	NX Node/Server to Network Devices	SNMP Polling of Network Devices

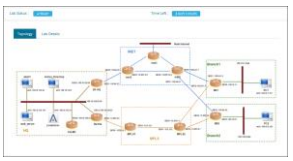
Required network protocols for normal operation of the LiveNX platform. This can be used as the basis for any firewall rules required.

LiveAction 16

16

Our Training Infrastructure

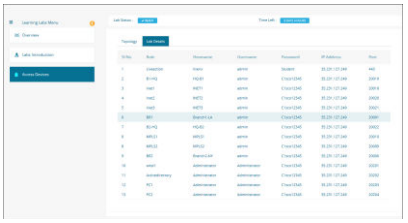
- Each attendee will connect to a dedicated "Training Pod"
- The Instructor will provide credentials for each attendee
- All Pods are monitoring similar traffic flows.
- We'll connect over the Internet and run a Browser and Client locally.
- Initial device configuration has been performed on all Training Pods.

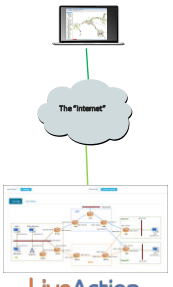


LiveAction 17

17

LiveNX Class Infrastructure





LiveAction 18

18

Sites Used in This Training Course

Course Component	Site	Description
Student Guide	https://www.liveaction.com/support/training-resources/	Your copy of the slides to follow the presentation/make notes
Lab Workbook Pt 1	https://www.liveaction.com/support/training-resources/	Day 1 Lab Workbook: Lab Exercises
Lab Workbook Pt 2	https://www.liveaction.com/support/training-resources/	Day 2 Lab Workbook: Lab Exercises
LiveNX Client (Mac or Windows)	https://www.liveaction.com/support/training-resources/	Client Access to be installed for some exercises
Website for Access to Hands-On Labs	https://portal.criterionnetworks.com/	You will be given your specific login information by the instructor

LiveAction 19

19

LAB 0: Setup and Get Connected

- Turn on / Plug-in, and verify network & internet connectivity.
- Note the addressing and credentials provided by your instructor.
- Install and run:
  - LiveNX Client
  - https://cloudkeys.liveaction.com/downloads
- You may now ping your LiveNX Server…

LiveAction 20

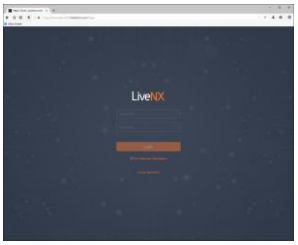
20

21

From Any Browser… from Anywhere!

https://<LiveNXserverIP>

- Create and View Dashboards
- Configure:
  - User Management
  - Devices
  - Alerts
- View:
  - Reports
  - Device Detail
  - Interface Detail

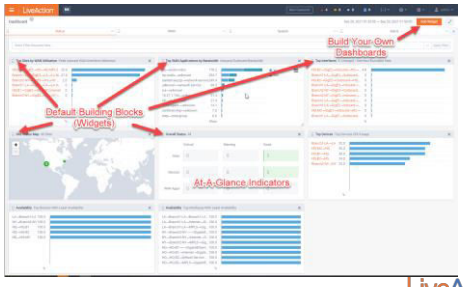


LiveAction

 22

22

Customizable Dashboards



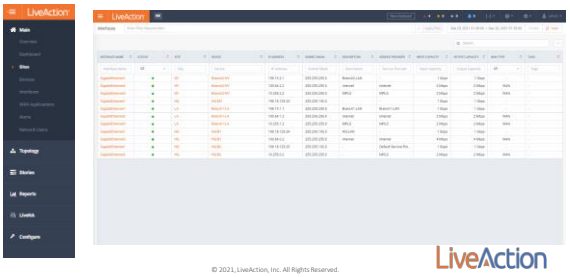
LiveAction

 23

23

Sites Details

Drill into Sites > Devices > Interfaces…

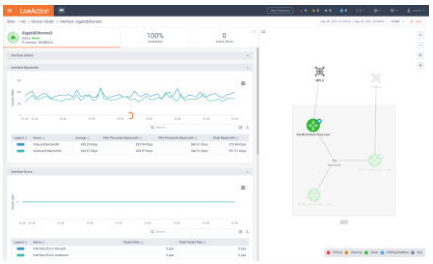


LiveAction

 24

24

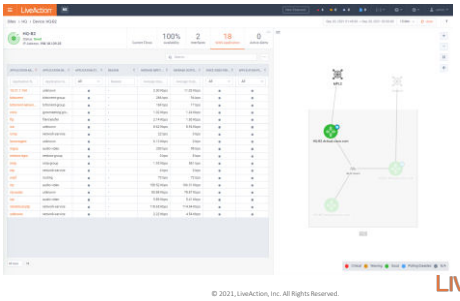
Interfaces



LiveAction
25

25

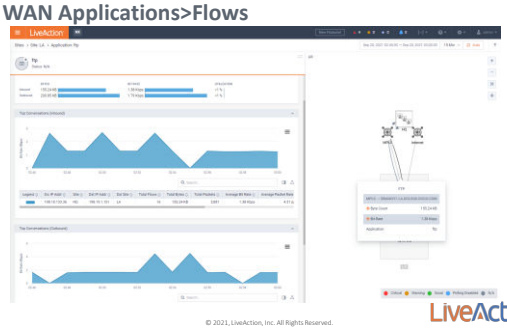
WAN Applications



LiveAction
26

26

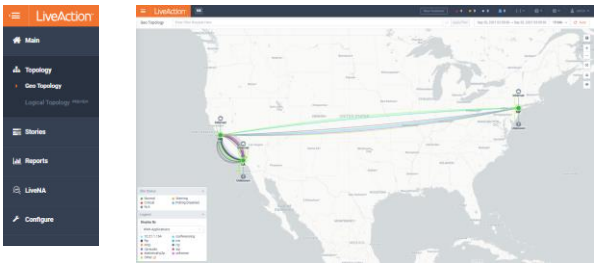
WAN Applications>Flows



LiveAction
27

27

Geo Topology

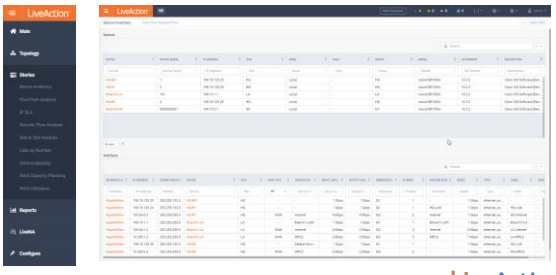


LiveAction

28

28

Stories

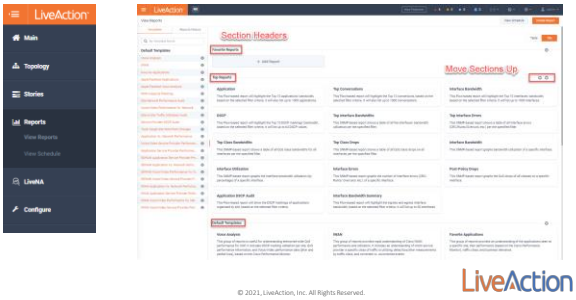


LiveAction

29

29

View ANY Report Defined in LiveNX

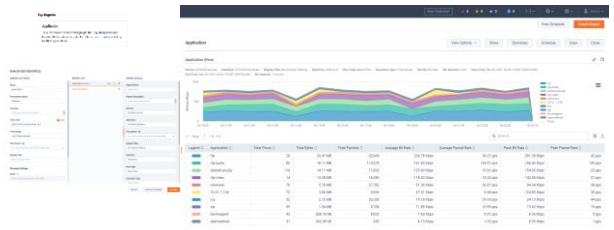


LiveAction

30

30

Run Reports…

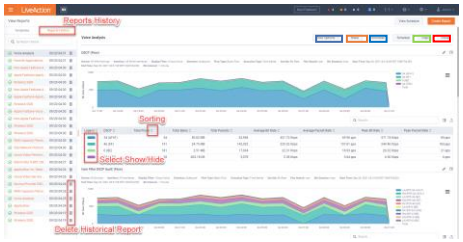


LiveAction

31

31

WebUI Reporting – Tools



Include Report Elements

Copy URL to Clipboard

Print/Download (opens new URL)

Re-open Run Report Dialog

Return to Reports Entry Page

LiveAction

32

32

Report Groups

LiveAction

33

33

WebUI Reporting – Create & Groups of Reports

Schedule Group to run Now, Hourly, Daily, Weekly, or Monthly

Advanced Report Group can be emailed to one or multiple users

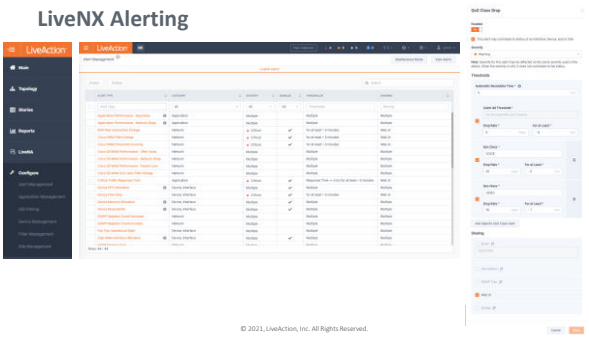
Advanced Reports allow the creation of groups of reports

LiveAction

34

34

LiveNX Alerting

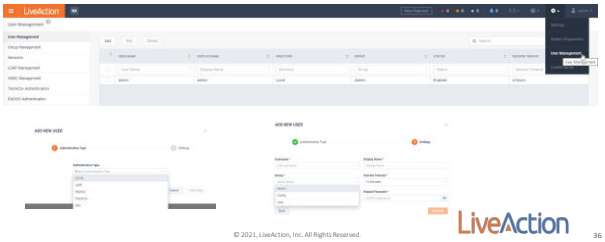


35

35

User Management

- Supports Local or AD-LDAP Authentication
- 3 Levels – Admin, Config, View



LiveAction

36

36

System Management

Using the WebUI to manage your LiveNX server and nodes

- User Management
- System Health
- System Support

LiveAction

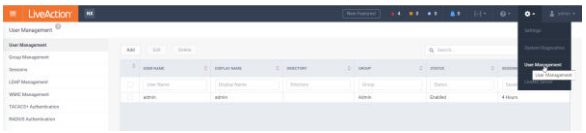
37

37

User Management

Local or LDAP

- Multiple Roles (privilege levels)
- LDAP Server configuration under LDAP Management tab
- See who is currently logged in and Active under the Sessions tab



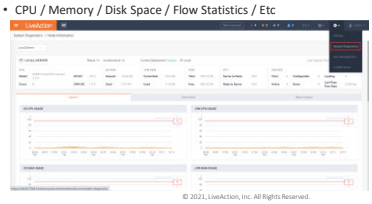
LiveAction

38

38

System Health

- Under the Settings gear choose System Diagnostics
- Here you can monitor many system health statistics for either the server or nodes:
  - CPU / Memory / Disk Space / Flow Statistics / Etc



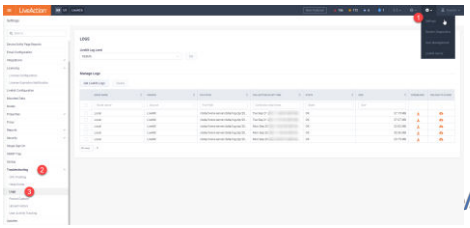
LiveAction

39

39

What to do when you need support

- Often the support team will ask for diagnostic information
- Under (1) Settings (top right), you will find (2)Troubleshooting in the Menu
- Here you can collect diagnostic information as well as (3) system logs



LiveAction 40

40

LAB 1: Using the Web UI

- View & Create Reports
- User Management
- View/Modify Alerts
- Create/Edit Dashboard

LiveAction 41

41

LiveAction 42

42

The LiveNX Client is… Your Engineering Console

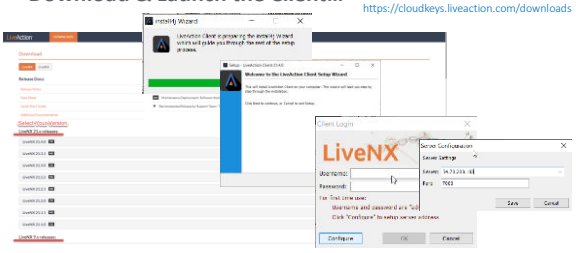
- A Java client application
- Runs on a standard Windows 32/64-bit PC
  - LiveAction's Mac client runs on OSX .9+.
- View & Configure:
  - Devices
  - Alerts
  - Reports
- Client interface to visualize and configure network topologies & traffic flows.

LiveAction
43

43

Download & Launch the Client…

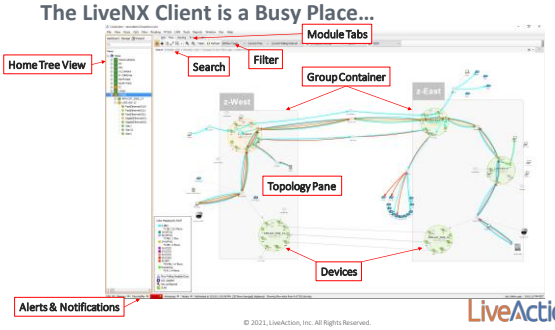
https://cloudkeys.liveaction.com/downloads



LiveAction
44

44

The LiveNX Client is a Busy Place…

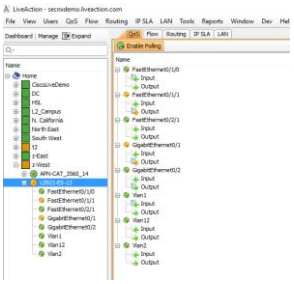


LiveAction
45

45

The Home Tree-view

- Groups
  - Devices
    - Interfaces
- Select Home to view all Groups/Devices in the Topology Pane
- Select & Modify Devices & Interfaces
- Right-click Zoom-to…



LiveAction

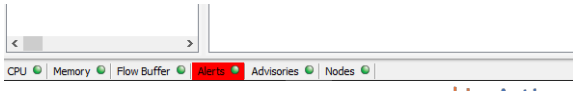
46

46

Immediate Feedback…

Look at the bottom of the screen for information about:

- CPU
- Memory
- Buffer
- Alerts
- Advisories
- Nodes



LiveAction

47

47

Immediate Results!

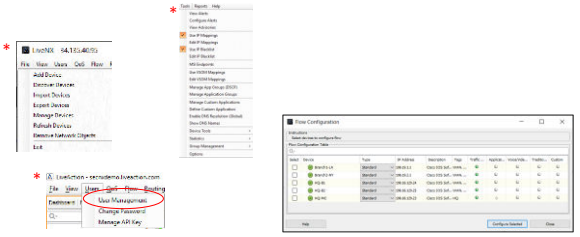
Select any Interface to generate real-time graphs

LiveAction

48

48

Manage, Create, View, Provision



* Configure in the WebUI!

LiveAction

49

49

LAB 2: LiveNX Client

- Launch the LiveNX Desktop Client
  - Connect from your Desktop…
- Explore Topology visualization

LiveAction

50

50

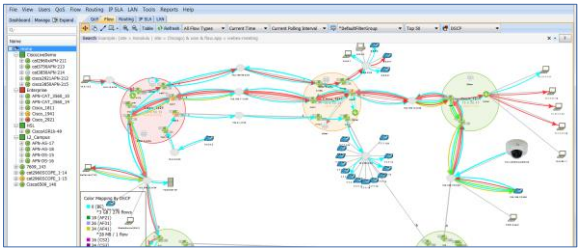
LiveAction

51

51

Flow Visualization

End-to-End Application Flows Through the Network



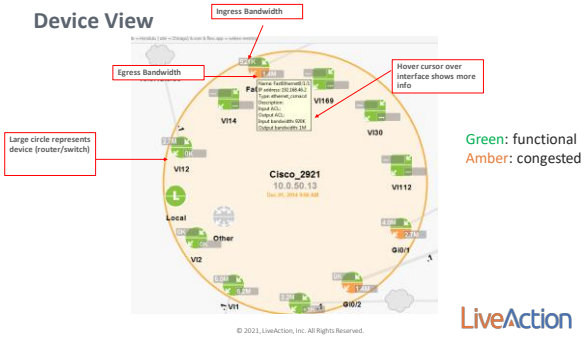
LiveNX discovers and draws topology based on SNMP
LiveNX imposes end-to-end flows on topology

LiveAction

 52

52

Device View

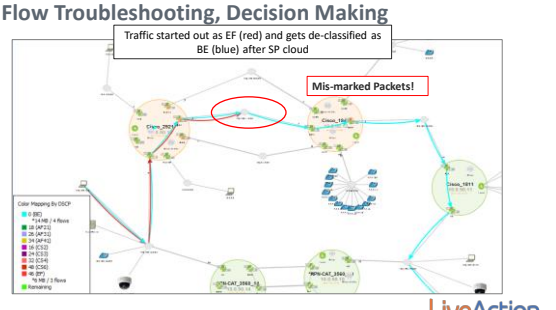


LiveAction

 53

53

Flow Troubleshooting, Decision Making

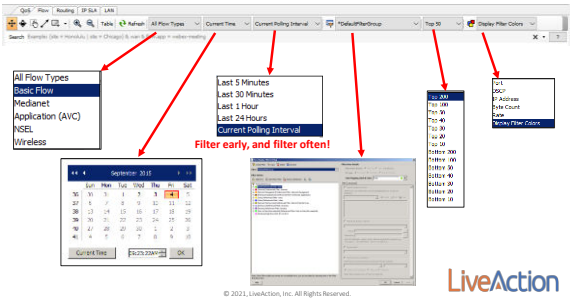


LiveAction

 54

54

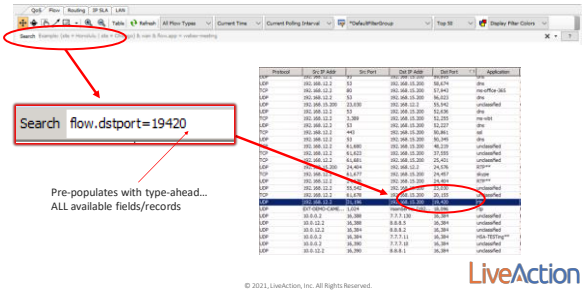
Eliminate the Detractors!



55

55

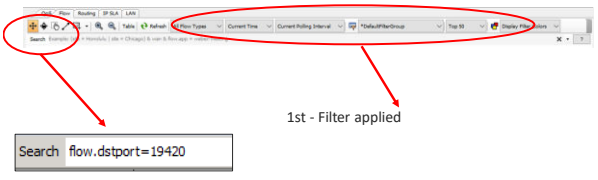
The Search Field



56

56

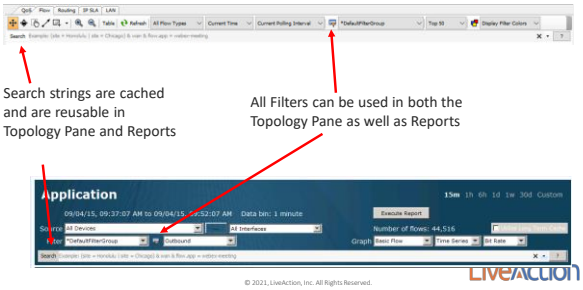
Search Functions – Order of Operation



57

57

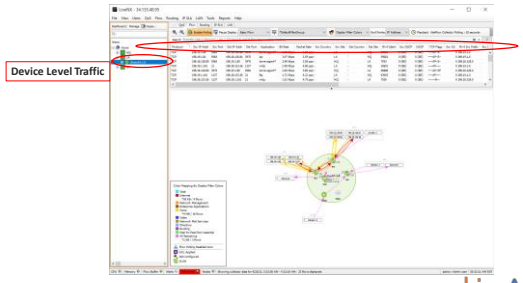
Filters & Search Retention



LiveAction
58

58

Flow Visualization



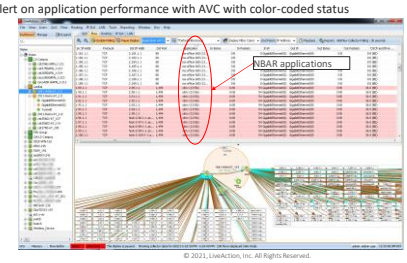
LiveAction
59

59

AVC Flow Visualization

Application Performance

- NBAR2 application recognition and performance metrics
- Alert on application performance with AVC with color-coded status

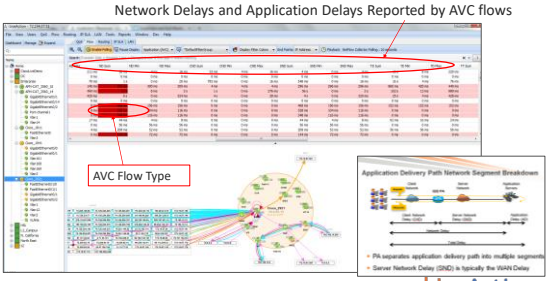


LiveAction
60

60

Flow Visualization

Network Delays and Application Delays Reported by AVC flows

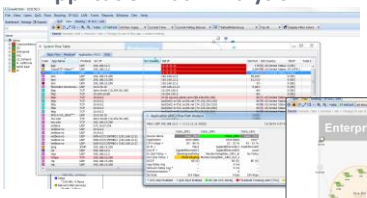


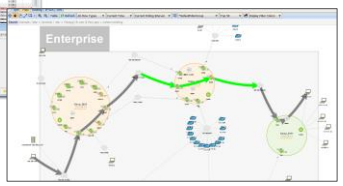
LiveAction

 61

61

Application Path Analysis





Path view based on AVC flows Drill down to reports

- DSCP along path
- Historical flows
- Gray arrows mean AVC flows not enabled

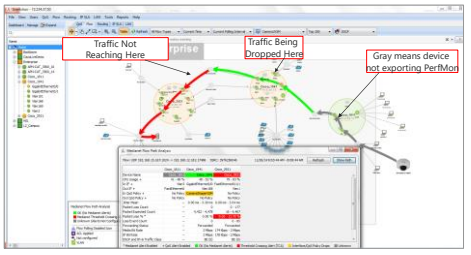
LiveAction

 62

62

Medianet Flow Path Analysis

Pinpoint Root Cause



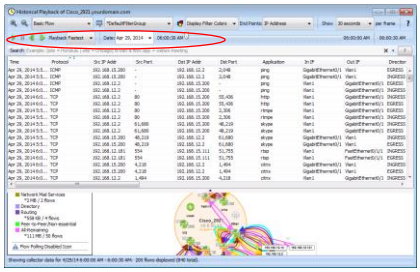
LiveAction

 63

63

Flow Visualization Over Time…

Flow Playback / DVR



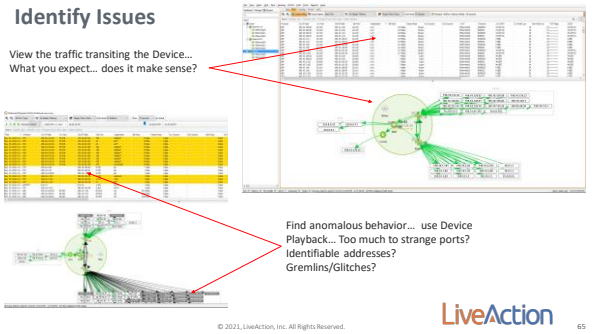
LiveAction

 64

64

Identify Issues

View the traffic transiting the Device…
What you expect… does it make sense?

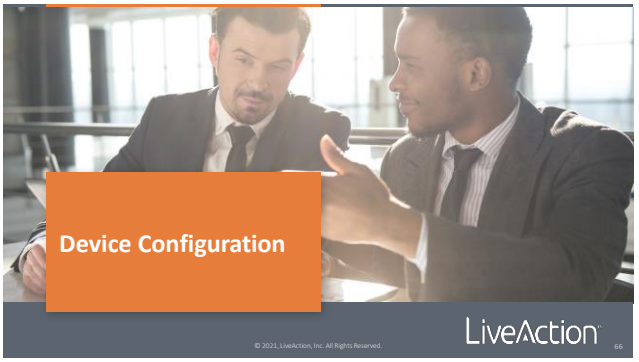


Find anomalous behavior… use Device Playback… Too much to strange ports?
Identifiable addresses?
Gremlins/Glitches?

LiveAction

 65

65

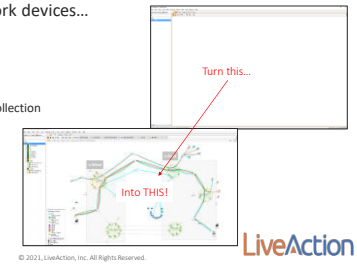


66

LiveNX Topology – A Blank Slate

LiveNX acts as a framework to help you visually manage and troubleshoot your network devices…

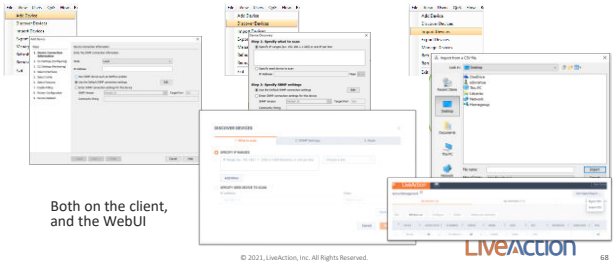
- Add devices
  - Routers & switches
- Configure interfaces
  - Enable SNMP & Flow collection
- Identify end-points
  - Various icons
- Create Groups
- Filter flows…



67

Adding Devices

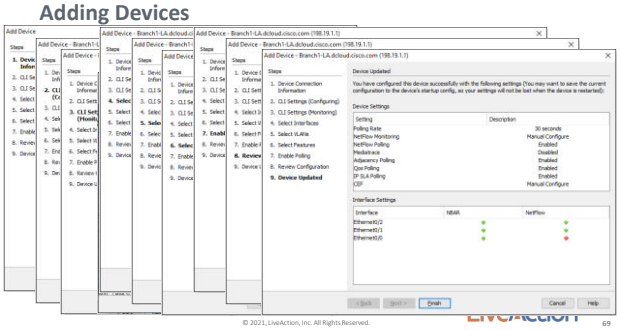
LiveNX contains many “wizards” to guide you through the process…



Both on the client, and the WebUI

68

Adding Devices



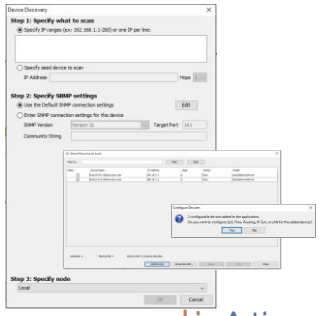
69

Device Discovery

Scan and find connected devices

- Use a "seed" device
- SNMP settings & Creds
- Is the collection Node Local or…

Returns a dialog with suggested devices to add.



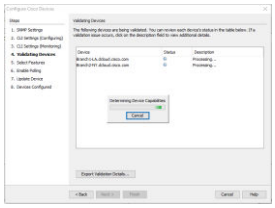
LiveAction

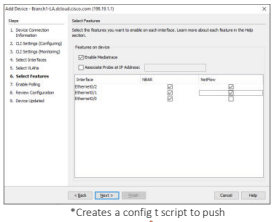
70

70

Device Discovery… Configure Cisco Devices

Allows you to pre-configure specific features on recognized devices.*





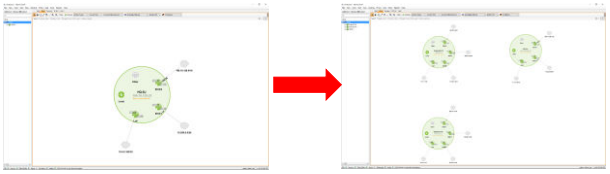
*Creates a config t script to push

LiveAction

71

71

Working Topology… Almost



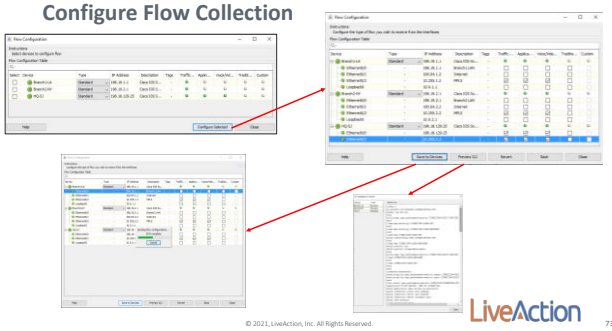
Devices installed… But no Flows?

LiveAction

72

72

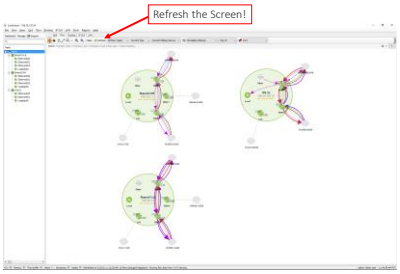
Configure Flow Collection



73

73

View Traffic Flows!



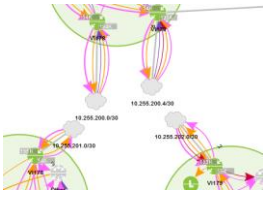
Pretty colors and lines/arrows… but still not connected!

74

74

Merge Clouds*

A “Merged” cloud is when you combine separate networks that logically form one cloud, i.e; MPLS



Once merged… flows will properly draw through the topology

*Merge Clouds only applied in LiveNX Client

75

75

LAB 3: Add & Configure Devices

We've already installed the Server, Client, and a single device (HQ SJ). It's up to you to:

- Add additional device(s) to the topology
- Enable / Configure Flow collection
- Merge Clouds…

LiveAction

76

76

77

Flow Collection

- Netflow is a brand name for Cisco Flow
  - Like Jaguar is a brand name for an automobile
- The industry standard for flow type is "IPFIX"
  - Cisco uses sflow for certain devices types, such as Nexus 5k Switch
- Juniper uses a flow type called "jflow"
- LiveNX can ingest most types of flow technology
- If a Flow Export is v5, v9, or IPFIX LiveNX can gather that information!

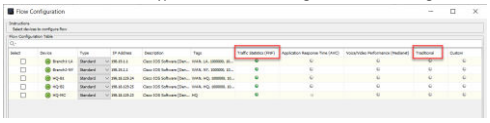
LiveAction

78

78

Configure NetFlow Monitoring (LiveNX Console)

- Two types of Cisco Netflow – Traditional and Flexible
  - Traditional - an older flow type that uses a set record that cannot be configured
  - Flexible - newer flow type that allows for more granular record configuration

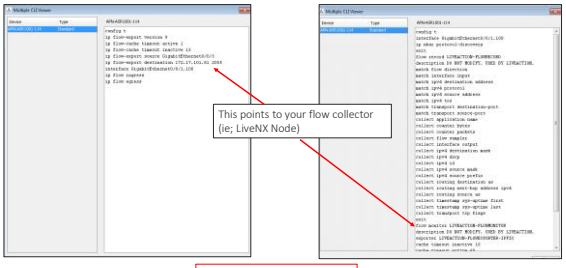


- Traditional Netflow should only be used if Flexible is not available!
  - LiveNX can discover what type of Netflow is supported and configure it for you!
    - LiveNX will not let you configure both Traditional and Flexible on the same interface

LiveAction
79

79

Traditional v. Flexible Netflow - Preview CLI

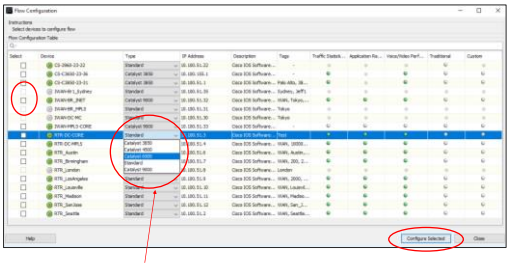


Cisco's Best-Practices Templates

LiveAction
80

80

Enable Flow Collection Within LiveNX Console

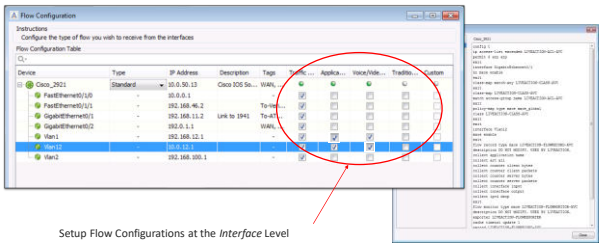


Easily Setup Flow Configurations at the *Device* Level

LiveAction
81

81

Enable Flow Collection on Interfaces



Setup Flow Configurations at the *Interface* Level

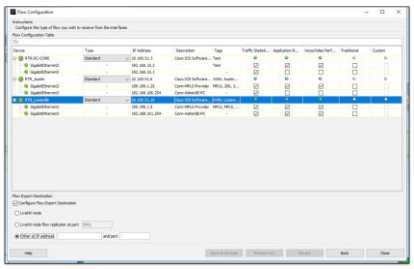
LiveAction

82

82

Re-Direct Collected Flows…

- Ability to specify alternate target for Flow Collectors
  - LiveNX Node
  - LiveNX Flow Replication on Port#
  - Other IP / Port (Gigamon, Samplicator, SolorWinds…)

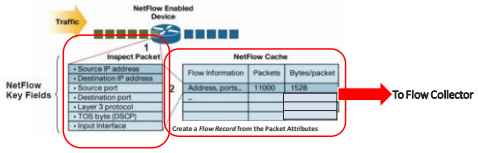


LiveAction

83

83

NetFlow Collects *Statistics* on Packets as they pass…



1. **A flow is unidirectional**
2. **Defined by inspecting a packet's key fields (common properties) and identifying the values**
3. **If the set of key field values is unique, create a flow record or cache entry**

LiveAction

84

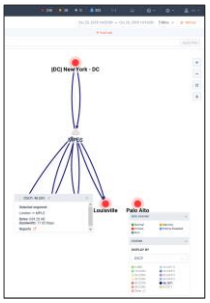
84

Netflow

By analyzing the data across interfaces and exporting the Netflow data to LiveAction, a network administrator can determine:

- Traffic source and destination
- Class of service
- Protocol
- Ports
- etc…

per device.

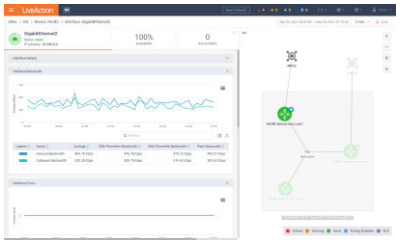


LiveAction

85

85

Netflow Interface View



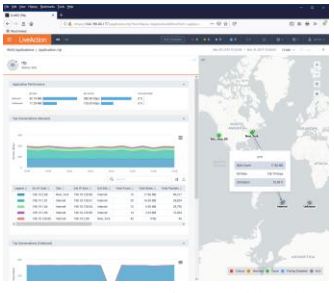
View quantity & type of traffic traversing a specific interface

LiveAction

86

86

Application Flow View



End-to-end quantity of traffic for selected applications

LiveAction

87

87

Other types of Flow in LiveNX

- LiveNXcan also ingest the following types of flows:
  - NSEL Flow (Network Security Event Logging)
    - Cisco ASA firewalls
    - Zone Based Firewalls (ASR, ISR4k)
  - Wireless Flow (SSID, Wireless Client, Access Point information)
    - Wireless Lan Controllers
    - Cisco 3850 Switches
  - "Unknown" (SFLOW, JFLOW, almost any flow technology using v5, v9, or IPFIX Export protocol)

LiveAction
88

88

Netflow Performance Monitors; AVC & Medianet

- AVC and Medianet use a Netflow Performance Engine that captures advanced metrics about a flow
- AVC (Application Visibility and Control) is Application Response Time (ART) for TCP applications
  - LiveNX leverages AVC to assist users with troubleshooting TCP performance in the network such as application delay, application response time, and network delay.
- Medianet is a Media Monitoring (MMON) engine that collects voice and video performance parameters, such as jitter and loss, in a network
  - LiveNX leverages Medianet to assist users with understanding RTP (Video, Teleconference, VOIP) Performance

LiveAction
89

89

Netflow Performance Monitors; AVC and Medianet

- AVC * and Medianet * are available on:
  - Cisco Integrated Services Routers Generation 2 (ISR G2)
  - Cisco ASR 1000 Series Aggregation Service Routers (ASR 1000s)
  - Cisco ISR 4k routers.
  - Cisco Wireless LAN Controllers
- LiveNX's AVC and Medianet Templates may be pushed to supported devices through its' GUI

LiveAction
90

90

Network Based Application Recognition (NBAR2)

- NBAR2 uses the Service Control Engine (SCE) with advanced classification techniques called PDLMs (Packet Description Language Modules). This engine inspects packets through the actual payload of the traffic.
  - Much more accurate classification of traffic rather than only based-upon IP and port number
- NBAR2 is Cisco's standard cross platform protocol classification mechanism.
  - supports <1400 application and sub-application definitions.
- Cisco updates NBAR2 protocol packs regularly to match new application definitions.
  - LiveNX recommends updating protocol packs as they come out.

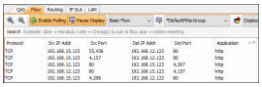
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/QoS_nbar/prot_lib/config_library/nbar-prot-pack-library.html

LiveAction
91

91

NBAR2

- How does Deep Packet Inspection help?
  - For example, Most web traffic is HTTP
  - IANA Port for HTTP is 80
  - NBAR2 can still define the Application



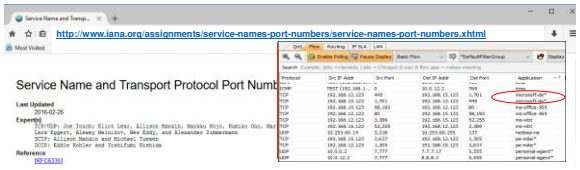
- LiveNX uses NBAR2 in Flow records for detailed application information
- You can use NBAR2 definitions for granular QoS configuration
- If your application is not known, you can set a NBAR application on the CLI
- If NBAR2 is supported, LiveNX will push the configuration to the devices during Netflow configuration

LiveAction
92

92

IANA.Org

- If LiveNX is *not* able to get the NBAR2 application definitions from the device:
  - Uses the IANA (Internet Assigned Numbers Authority) definitions for Applications.

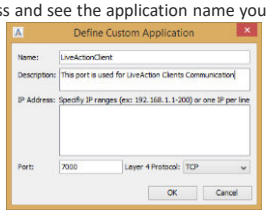


LiveAction
93

93

Custom Application Label

- What if you have your own custom applications in the Network?
- You can go into LiveNX and define applications based on Protocol, Ports or IP Address and see the application name you desire



LiveAction
94

94

Using Flows for QoS

- Quality of Service (QoS) refers to the capability of a network to prioritize provide better service to selected network traffic over various applications
- Without QoS policies, each packet is given equal access to network resources.
  - For example, Voice and Video applications are delay and jitter sensitive. If a FTP transfer and a Voice transfer are both being processed through the same interface at the same time, then the Voice transfer could have to wait until the FTP packets are processed. This could result in dropped voice packets and complaints by the those utilizing the voice application.
- Using QoS a network administrator could prioritize those Voice packets over the FTP packets, ensuring good quality for those utilizing the Voice application.

LiveAction
95

95

Differentiated Service Control Point (DSCP)

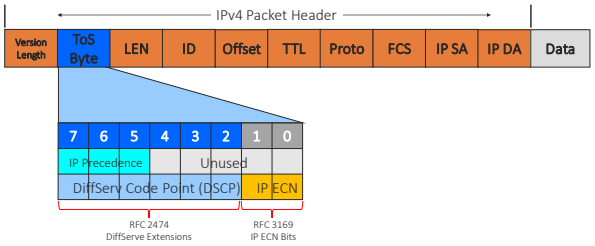
- Depending on your network, you would define which traffic needs priority, then mark the traffic with the correct DSCP values.
- These values may then be used to give priority to traffic throughout the network, specifying **Per-Hop-Behaviour.**

Application	L3 Classification PHB	DSCP	IETF RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency Data	AF21	18	RFC 2597
OAM	CS2	16	RFC 2474
High-Throughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

LiveAction
96

96

Packets & DSCP Markings



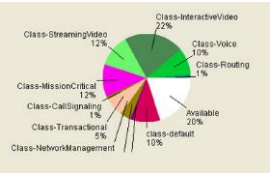
LiveAction

97

97

QoS Techniques

- After setting DSCP Markings in your network you can easily conform the traffic to your network needs with:
  - Queuing
  - Shaping
  - Policing



LiveAction

98

98

LAB 4 & 5: Working With Flow and Customizing Filters

- Discover Flows
- Identify Flows
- Create Custom Filters
- ACL Creation

LiveAction

99

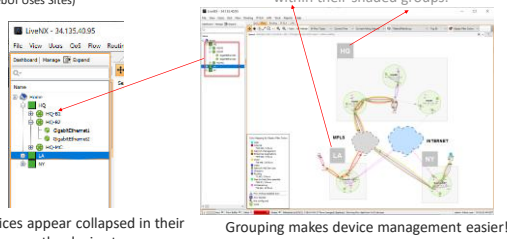
99

100

Topology Basics – Grouping*

*Grouping only applied in LiveNX Client (WebUI Uses Sites)

Devices appear on the topology within their shaded groups.



Devices appear collapsed in their groups on the device tree.

Grouping makes device management easier!

LiveAction

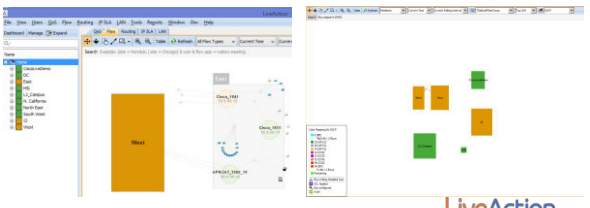
101

101

Topology Basics

Devices reporting issues will change colors to prompt for investigation.

Quickly identify many problem sites visually



LiveAction

102

102

Topology Basics – Add Network Object

Associate Network Objects with IP Addresses help to visualize devices such as PCs, Servers, IP Phones, Laptops…

Step 1
Right-Click and create Network Object

Step 2
Draw connection to cloud

Step 3
Flows now connect

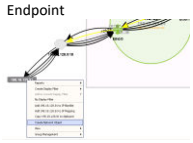
103

103

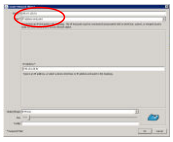
Topology Basics – Add Network Object

Do it the EASY way!

Step 1
Right-Click on Flow Endpoint



Step 2
Select the Object Shape



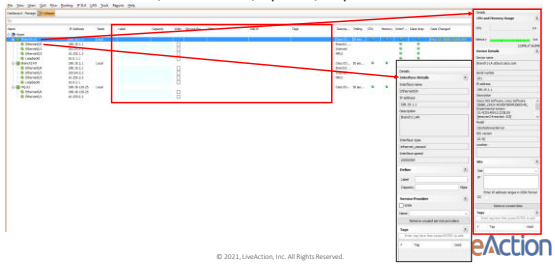
Step 3
Flows now connect

104

104

Device *Semantics*

Set Interface Labels, Destination, Speeds, Capacities…

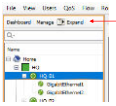


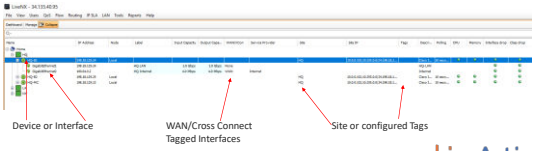
105

105

Managing Data Storage

LiveNX creates *pointers* as data is collected into the database.





LiveAction
106

106

LAB 6: Customize Topology

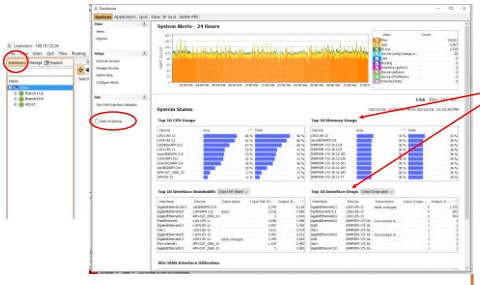
- Device Semantics
- Creating / Modify Groups
- Network Objects

LiveAction
107

107

108

System Dashboard At-A-Glance Flow Traffic Pattern

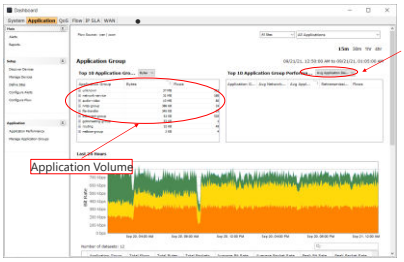


LiveAction
109

109

Application Dashboard

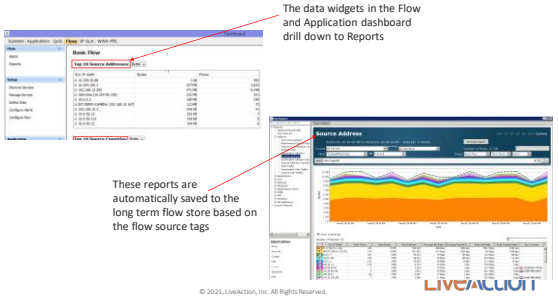
Instant Application
Performance
Visibility
Driven by AVC Flows



LiveAction
110

110

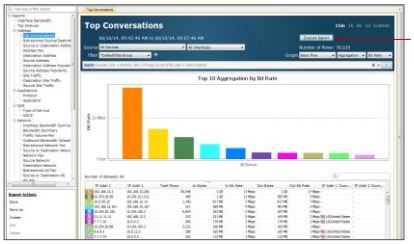
Report Drill-downs



LIVEACTION
111

111

Flow - Top Conversations (Top Talkers)



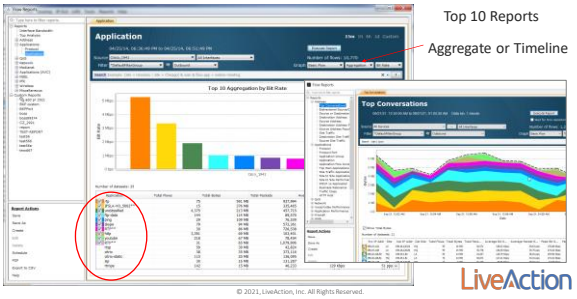
Don't forget to Execute

LiveAction

112

112

Top Applications & Most Visited Websites



Top 10 Reports

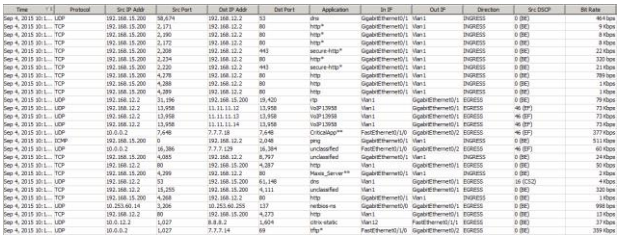
Aggregate or Timeline

LiveAction

113

113

Flow Reports – Raw Data

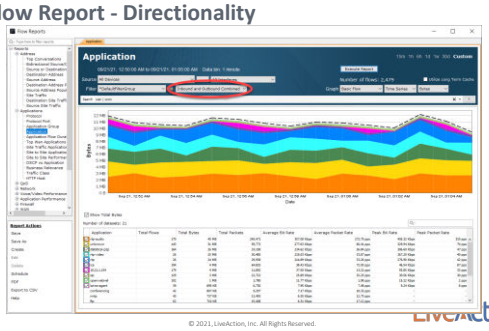


LiveAction

114

114

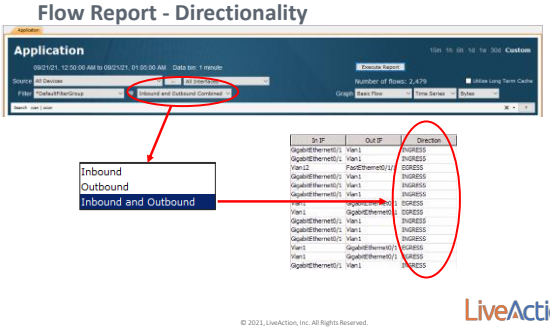
Flow Report - Directionality



LiveAction
115

115

Flow Report - Directionality

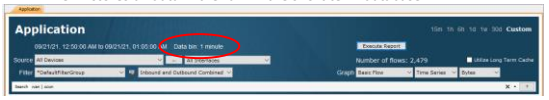


LiveAction
116

116

Automatic Granularity - Report Length / Data Bin

LiveNX stores all data *in the raw* in the short term database



15m to <1h = 1 Minute Bin
1h to 30d = 5 Minute Bin

If selected, the long term Flow store will be used for the report – If the data is available.

LiveAction
117

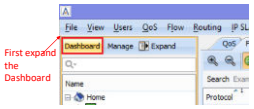
117

Long Term Data Storage (2)

How is data populated?

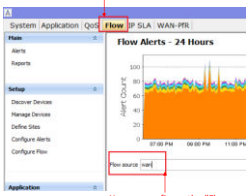
The Dashboard Flow Source alters what devices and interfaces are processed in Long Term Report Processing.

You can find the Flow source on the Flow tab of the Dashboard.



First expand the Dashboard

Then select the Flow Tab



You can configure the "Flow source" to use tags for either Device, Interface, WAN, Site, or Tag

LiveAction

118

118

Commonly Used Reports

- Top Applications
- Top Talkers/IP addresses
- Top DSCP
- WAN Bandwidth Utilization by application
- IPs and Ports

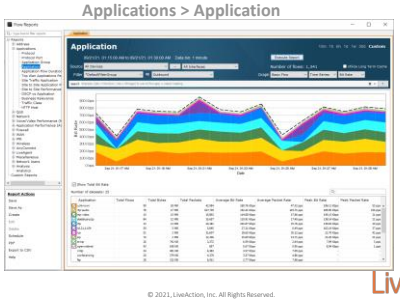
LiveAction

119

119

Use Case 1 – Top Applications

Applications > Application



LiveAction

120

120

Use Case 2 – Top Talkers

Address > Top Conversations

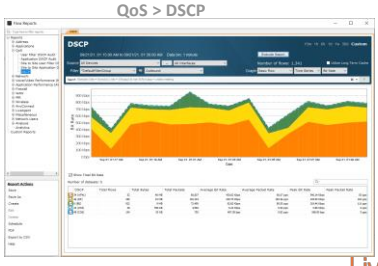
LiveAction

 121

121

Use Case 3 – Top DSCP

QoS > DSCP



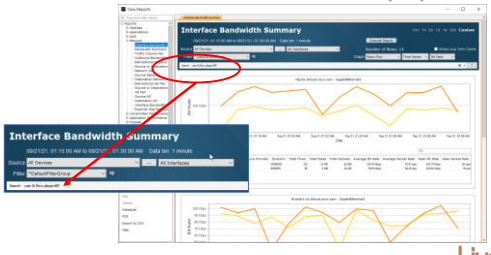
LiveAction

 122

122

Use Case 4 – Top DSCP

Network > Interface Bandwidth Summary Report



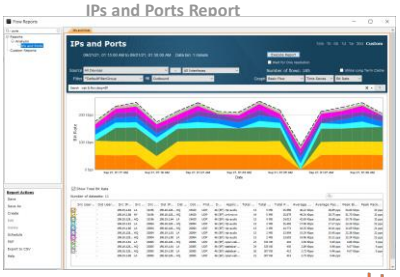
LiveAction

 123

123

Use Case 5 – IPs and Ports

IPs and Ports Report



LiveAction

124

124

LAB 7: Dashboards and Reporting

- Create & View Reports

LiveAction

125

125

LiveAction

126

126

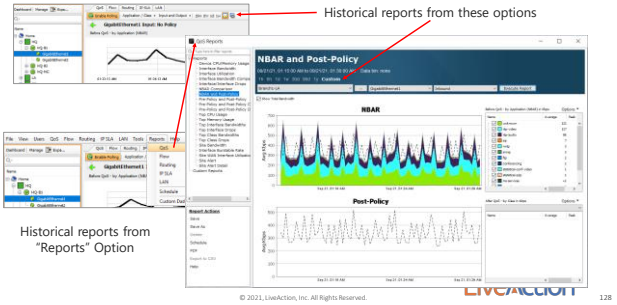
LiveNX QoS Baseline

- Configuring QoS Control on the network is very important, but if you do not have a good understanding of your current network traffic… implementing QoS *could* cause issues.
- You can baseline your network performance with NBAR2 reports or Netflow reports *before* implementing QoS Control
- Baselining allows you to see current traffic trends and understand if your policy will meet your network needs.

LiveAction
127

127

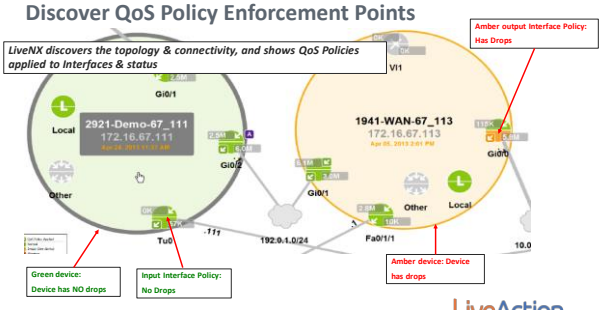
Historical QoS Class View/Reports



LiveAction
128

128

Discover QoS Policy Enforcement Points



LiveAction
129

129

QoS ACL

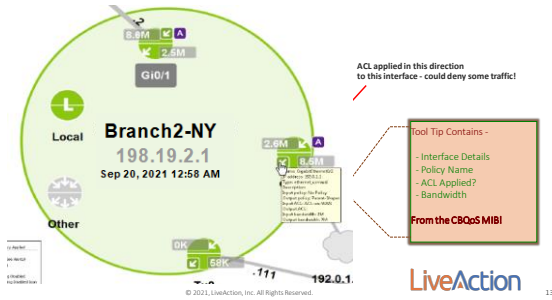
- What is an ACL (access control list)?
- In the Cisco IOS, an access control list is a record that can be used to identify traffic, which can even be used to manage traffic.
- After identifying that traffic, an administrator can specify various actions that can happen to that traffic.
- You can use an ACL as a packet sniffer to list packets that meet a certain requirement. For example, if there is specific traffic on your network that you want to match for a QoS policy, you can use an ACL to identify that traffic to better control it

LiveAction

130

130

QoS Policy Detail Display

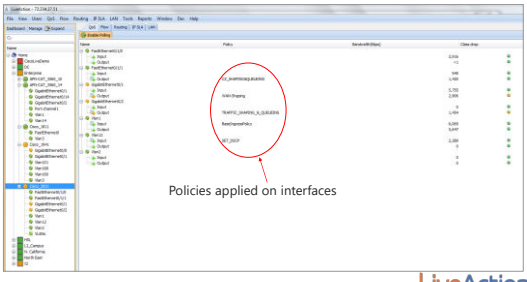


LiveAction

131

131

QoS Device View

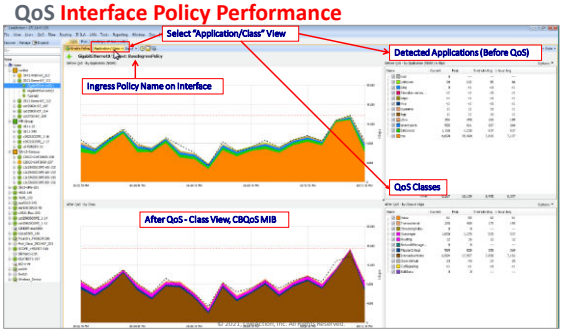


LiveAction

132

132

QoS Interface Policy Performance



133

133

QoS Troubleshooting

- Real-Time QoS Issues

Amber QoS class color shows class drops

LiveAction

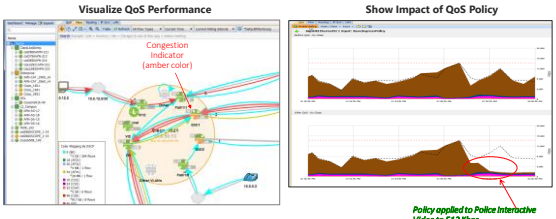
134

134

Track QoS Performance & Policy Validation

Visualize QoS Performance

Show Impact of QoS Policy

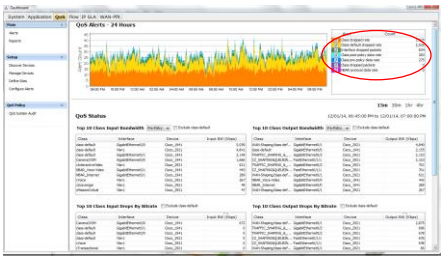


LiveAction

135

135

QoS Dashboard



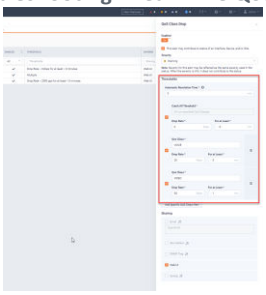
Driven from MIB-II, NBAR, and CBQoS MIBs

LiveAction

136

136

Troubleshooting - Real-Time QoS Alerts



User-defined thresholds can be configure to create QoS alerts when thresholds are exceeded

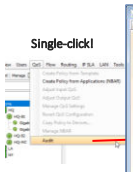
LiveAction

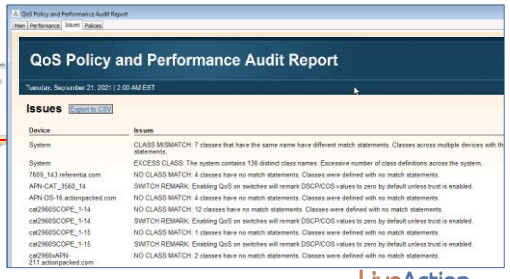
137

137

Troubleshooting – Auditing QoS Policies

Single-click!





LiveAction

138

138

LiveNX QoS Configure

- Full MQC (Modular QoS Configuration) support including WRED, CBWFQ, Priority Queuing, Shaping
- Read pre-existing QoS policies already configured on devices
- Take snapshots of current QoS configuration for future use
- Apply or remove QoS configurations quickly and easily across multiple interfaces
- Copy QoS policies across multiple devices, including associated ACLs (Access Lists)
- Hierarchical policy creation for advanced configurations
- CLI command preview before applying policy
- Rollback to previous policies at anytime*
- Built-in rules for QoS settings that highlight violations

LiveAction
139

139

LAB 8: Quality-of-Service

- QoS Marking Policy
- QoS Queueing Policy
- QoS Verification Policy

LiveAction
140

140

141

142

Agenda - Day 2

- Implementation Best Practices
  - Installation Considerations
- Deployment Strategies
- Quality of Service
  - Concept Overview
  - Classification & Marking
  - Shaping & Queueing
  - Policing & WRED
  - Buffer Tuning
- QoS Best Practices
- LiveAction SD-WAN
  - Concept Overview
  - SD-WAN Fundamentals
  - SD-WAN Deployment
  - SD-WAN Operations

LiveAction
143

143

144

System Requirements

http://www.liveaction.com/support/specifications/

- 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 E100

Proof Of Concept (POC)	Small Deployment	Medium Deployment	Large Deployment	Physical Deployment
<= 25 Devices or <= 25k Flows/sec.	<= 100 Devices or <= 50k Flows/sec.	100-500 Devices or <= 100k Flows/sec.	500-1000 Devices or <= 150k Flows/sec.	Upto 1000 Devices or <= 500k Flows/sec.
Min Requirements: • 8 vCPU Xeon or i7 • 16 Gb RAM • Max Heap Size 8GB • 500GB Data Disk	Min Requirements: • 16 vCPU Xeon or i7 • 32 Gb RAM • Max Heap Size 16GB • 2TB Data Disk	Min Requirements: • 16 vCPU Xeon or i7 • 64 Gb RAM • Max Heap Size 31GB • 4TB Data Disk	Min Requirements: • 32 vCPU Xeon or i7 • 64 Gb RAM • Max Heap Size 31GB • 8TB Data Disk	Min Requirements: • 64 vCPU Xeon Gold 5218 • 768 Gb RAM • Max Heap Size 384GB • 32TB Data Disk (16TB usable with RAID 10)

LiveAction

145

145

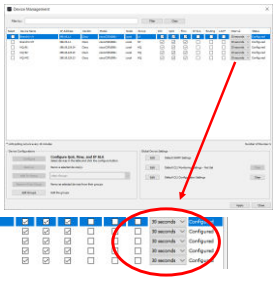
Disk Sizing- SNMP

SNMP

- QoS, IPSLA, Interface stats, etc.
- Raw data - never averaged on disk
- Poll rates and technology determines utilization

LiveAction Recommends

- Router polling = 30 seconds
- Switch polling = 1 minute or 5 minutes
- Poll fewest technologies required



LiveAction

146

146

Disk Sizing

SNMP

- QoS, IPSLA, Interface, etc. stats
- Raw data - never averaged on disk
- Poll rates and technology determines utilization

Short Term Flow **= 90% of storage**

- Raw data - never averaged on disk
- Flow/ Sec determines utilization

Long Term Flow

- 5 minute averaged on disk
- Capacity Planning data
- WAN data is default data sent here

Drive Recommendations
○ Local drive preferred
Minimum equivalent to SATA 6 Gb/s performance
7,200 RPM base or 10,000 RPM for better performance
RAID 10 for better performance
SSD for better performance
○ SAN and NAS
Meet performance and latency specification of local drive
Support sustained writes at high speed
Support sequential reads at high speed for sequential blocks

We typically see:
1 year SNMP + Long-Term Flow
<=
1 Month of Short-Term Flow

LiveAction

147

147

Disk Sizing

SNMP

Each LiveNX **node** supports ~76TB disk space. Recommended way is to add each disk of 10TB

Number of Devices	100	250	500	1000
SNMP/Month	22 - 45GB	56 - 112GB	112 - 225GB	225 -450GB

Poll rates and technology determines utilization - This is assuming 25% of devices are 30 Second Poll/ 75% 60 Second Poll

Short Term Flow

Avg Flow Rate (K flows sec)	< 25K/sec	< 100K/sec	< 200K/sec	< 300K/sec
Short Term Flow/Month	.75TB	3TB	6TB	9TB

Long Term Flow

Avg Flow Rate (K flows sec)	< 25K/sec	< 100K/sec	< 200K/sec	< 300K/sec
Long Term Flow/Month	7GB	30GB	60GB	90GB

LiveAction

148

148

NetFlow Bandwidth Overhead – Someone ALWAYS Asks!

Device Type	Flows/Sec	Full-Duplex User Bandwidth Avg.-Peak	NetFlow Bandwidth Average	NetFlow Bandwidth Peak
WAN Router	.61	158-309Kbps	2Kbps (1%)	14.8Kbps (4%)
WAN Router	34	505K-1.1Mbps	16Kbps (3%)	42.4Kbps (3%)
WAN Router	27	820K-2.6Mbps	22Kbps (2%)	36Kbps (1%)
WAN Router	197	~21-39Mbps	85Kbps (.04%)	117Kbps (.03%)
WAN Router	366	~37-72Mbps	161Kbps (.04%)	219Kbps (.03%)
WAN Router	474	~80-125Mbps	280Kbps (.03%)	396Kbps (.03%)
Internet Router	593	~75-115Mbps	317Kbps (.04%)	418Kbps (.03%)
Core Switch	633	~146-335Mbps	470Kbps (.03%)	578Kbps (.01%)
Core WAN Router	22,000	~4-4.2Gbps	11Mbps (.02%)	12Mbps (.02%)

Bandwidth	<768Kbps	1.544Mbps	3Mbps	10Mbps or higher
Overhead	3%	2%	1%	<.5%

Note: the percentages represent the percent of bandwidth utilized by Flow compared to rest of the end-user bandwidth. Each of these examples has Flow configured bi-directionally on only the WAN interface.

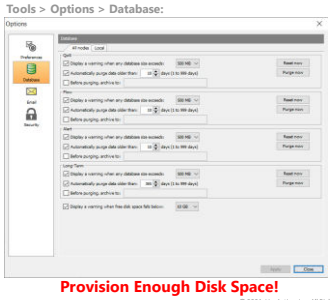
LiveAction

149

149

Disk Retention

Tools > Options > Database:



Admin can set:

- Data Retention policy
- Manual Purge
- Backup
- Mounting

Disk full = Automatic Purging

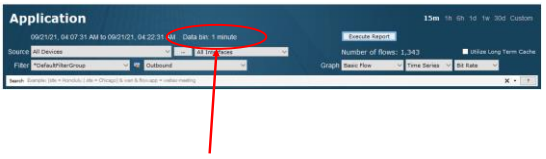
Provision Enough Disk Space!

LiveAction

150

150

Search – Data Bin



- LiveAction stores all data in the raw in the short term database
- LiveAction stores all data in the long term database with 5 minute average
- 1 minute bin < 1 hours search
- 5 minute bin >= 1 hours search

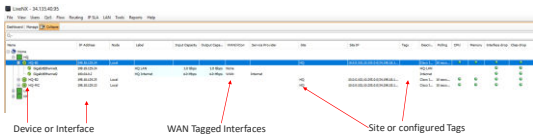
LiveAction
151

151

Device Semantics…

The Flow Source is a flex string that can only be set as only as Device, Interface, WAN, Site or Tags.

Expand to see device information



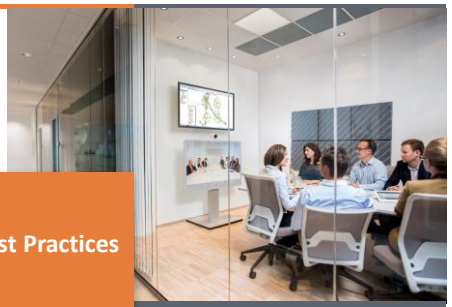
Device or Interface

WAN Tagged Interfaces

Site or configured Tags

LiveAction
152

152



NetFlow Best Practices

LiveAction
153

153

NetFlow Best Practices

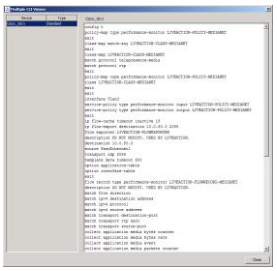
- Use LiveAction to deploy NetFlow
- Use Flexible NetFlow when possible*
- Use NBAR2 and standardized on Protocol Pack
- Use NetFlow v9 or IPFIX
- Enable Flow on the fewest interfaces possible
- Medianet and AVC on WAN interfaces only for routers
- Use good IOS for Medianet and AVC

*with good/modern IOS

LiveAction
154

154

NetFlow – Configuration Management



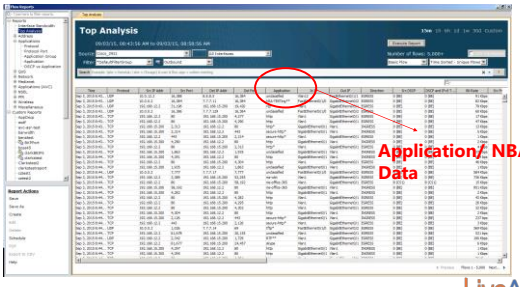
Use Best Practice NetFlow templates built into LiveAction

Note: LiveAction Support has configuration guides for enabling flow for platforms that may not be part of this configuration wizard.

LiveAction
155

155

NetFlow – Flexible NetFlow



LiveAction
156

156

NetFlow – NBAR2

audio-over-http
internet-audio-streaming
internet-video-streaming
skype
msn-messenger
netflix
linkedin
pandora
rhapsody
dropbox
call-of-duty
twitter
youtube
facebook
espn-browsing
espn-video
skydrive
salesforce
wikipedia
http
hulu
instagram
yahoo-mail

apple-app-store
apple-ios-updates
apple-services
mac-os-x-updates
itunes
itunes-audio
itunes-video
facetime

gmail
google-docs
google-earth
google-play
google-plus
google-services
gtalk
gtalk-video
gtalk-voip
gtalk-chat

cisco-jabber-audio
cisco-jabber-control
cisco-jabber-im
cisco-phone
cisco-phone-audio
h323
mgcp
ms-lync
ms-lync-audio
ms-lync-video
rtp
sip
skinny
telepresence-control
webex-media
webex-meeting
webex-app-sharing

This is a sample of the applications found on a LiveAction Customer's Network via NBAR2

LiveAction
157

157

NetFlow – NetFlow v9 or IPFIX

- IPFIX = IP Flow Information Export
- You can think of IPFIX as IETF Standard NetFlow v10
- NetFlow v9 and IPFIX are template based – Allows extensions for inserting extra data into the Flow records
- IPFIX allows for more fields and that can be variable in length
- IPFIX allows a vendor proprietary information

Example IPFIX variable fields:

URL	URI
thumbnails.huluim.com	827:2 ads:2 248:3 829:2 pixel;r=1608579339;fpan=0;fpa=P0-322201277-1287906563231;ns=0;url=http%3A%2F%2Fw:2 quant.swf:2 981:3 crossdomain.xml:3 913:2 914:2 461:2 cgi-bin:6 915:2 ad:2 462:2 adcedge:2 839:2 quant.js:2 api:3 761:2 notice.do:2 _vti_bin:2 jaction:2 images:10 pixel;r=1182204851;fpan=0;fpa=P0-322201277-1287906563231;ns=0;url=http%3A%2F%2Fw:2 features:4 shows:6 adServer:2 captions.xml:3 pagead:9 499:3 live-streams:2 b:3
us.bc.yahoo.com	B:1

NetFlow v9 - RFC3954
IPFIX – RFC5101

LiveAction
158

158

NetFlow – Where to Enable Flow?

The Fewest Interfaces Possible!

Why?
- Most Efficient
- Lowers CPU, bandwidth consumption, disk space

Routers
- Usually WAN Interfaces Only
- Usually Tunnel Interfaces Only for IWAN/DMVPN

Switches
- Watch CPU if lots of interfaces are enabled with Flow
- If switch only supports ingress Flow, use fewest interfaces that provides required visibility
- If switch support ingress/egress Flow, typically only uplinks required

LiveAction
159

159

NetFlow – AVC/Medianet

- AVC/Medianet enabled on fewest interfaces possible
  - Enable only on WAN interfaces for routers
  - L2/L3 uplinks only on switches
- Modify Interesting traffic class-maps where applicable

```
class-map match-any LIVEACTION-CLASS-AVC
 match access-group name LIVEACTION-ACL-AVC

class-map match-any LIVEACTION-CLASS-MEDIANET
 match protocol rtp
 match protocol telepresence-media
```

Note: LiveAction Support can provide additional details and IOS data.

LiveAction

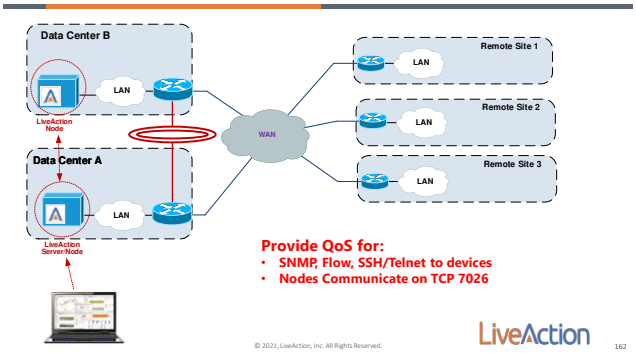
160

160

LiveAction

161

161

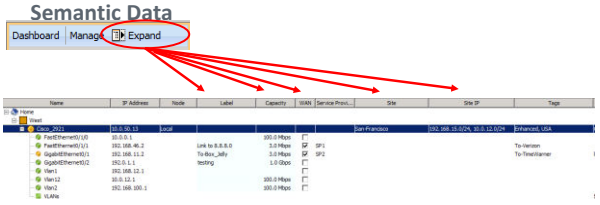


LiveAction

162

162

Semantic Data



Label, Capacity, WAN, Service Provider, Site, Site IP

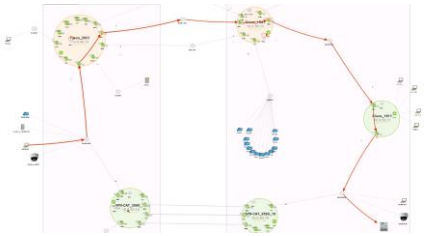
Semantic data makes LiveAction come “alive”!

LiveAction
163

163

Semantic Data – example 1

Search site=San-Francisco | site=Chicago | site= New_York & wan & flow.dstport=19420



LiveAction
164

164

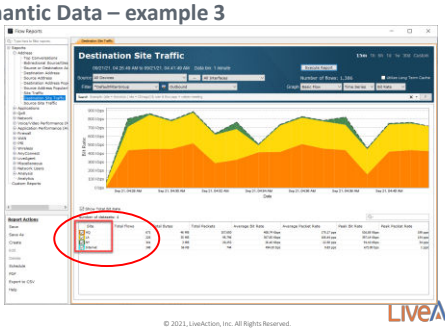
Semantic Data – example 2

Search wan & tag=Enhanced & flow.app=RTP

LiveAction
165

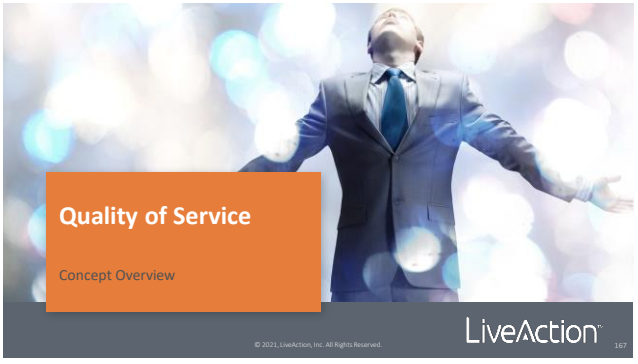
165

Semantic Data – example 3



LiveAction
166

166



167

How to Implement QoS

Step 1 - Recognize Application Traffic (Classification and Marking)

Step 2 - Prioritize (Queuing and Shaping)

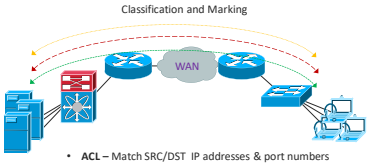
Step 3 - Throttle Traffic (Policing and WRED)

Step 4 - Buffer Tuning

LiveAction
168

168

Step 1 - Recognize Application Traffic

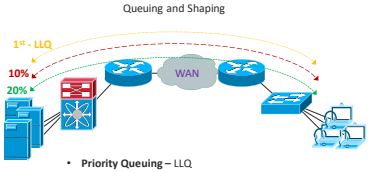


- **ACL –** Match SRC/DST IP addresses & port numbers
- **DSCP-** TOS byte QoS markings
- **NBAR–** Protocol discovery by Cisco devices

LiveAction
169

169

Step 2 – Prioritize

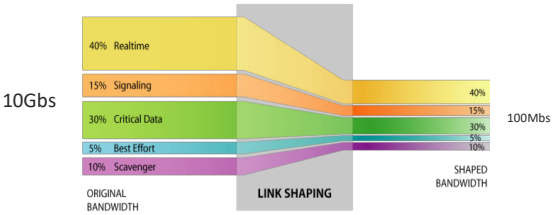


- **Priority Queuing –** LLQ
- **CBWFQ -** Guaranteed bandwidth
- **Shaping -** Transmit data to software set limit, buffer and queue overage

LiveAction
170

170

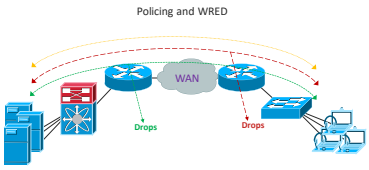
Shaping (or Scaling)



LiveAction
171

171

Step 3 –Throttle Traffic

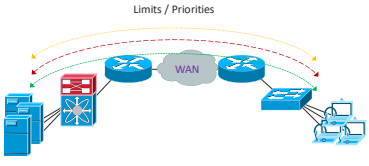


- **Policing -** Transmit data to software set limit, drop overage
- **WRED –** Selectively drop specific data before congestion occurs

LiveAction
172

172

Step 4–Buffer Tuning (advanced)



- **Queue-limit –** Buffer size that stores queue data during congestion
- **Priority queue BC –** Token bucket interval that schedules the releases data in priority

LiveAction
173

173

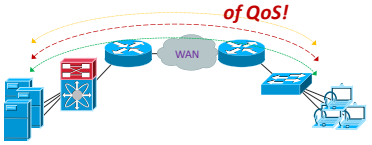
Classification & Marking

LiveAction
174

174

Recognize Application Traffic

This may be the hardest & most important part of QoS!



Step 1 – Day 0: Application Landscape
Step 2 - Use Filters/Search to identify traffic in LiveNX
Step 3 - Use visualization & reports to confirm traffic
Step 4 - Standardize on DSCP values
Step 5 - Use visualization & reports to validate DSCP
Step 6 - Update QoS policies on routers/switches/etc.
Step 7 - Confirm QoS policies via visualization & reports in LiveNX

LiveAction
175

175

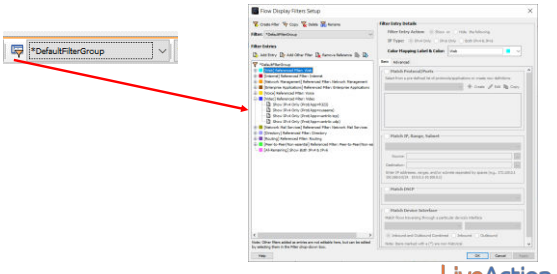
Classification: Day 0: Application Landscape

- Step 1: Review customer's critical applications
- Step 2: Review LiveNX Flow Reports to understand application usage:
  - Application Report
  - Interface Bandwidth Summary
  - IPs & Ports
  - Site Traffic
  - Destination Site Traffic
  - Source Site Traffic

LiveAction
176

176

Classification: Create Custom Filter

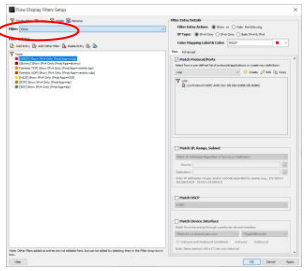


LiveAction
177

177

Classification: Copy Voice Filter

- Find pre-canned Voice filter
- Copy and rename it



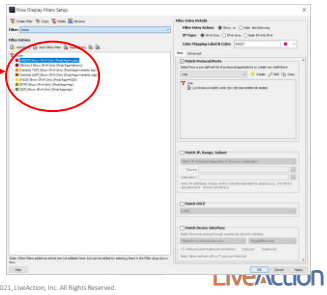
LiveAction

178

178

Classification: Delete Unused Entries

Delete unused Entries
- VoIP
- Ventrilo TCP
- Ventrilo UDP



LiveAction

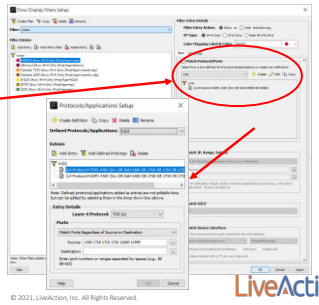
179

179

Classification: Add/Edit Entries

Edit Entries:
- h323
- RTP
- SIP

Add Entry:
- MGCP



LiveAction

180

180

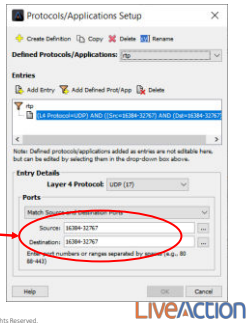
Classification: Edit Entries

MGCP
TCP/UDP = Src or Dst = 2427 2727
TCP = Src or Dst = 2428

H323
TCP/UDP = Src or Dst = 1718 1719 1720

SIP
TCP/UDP = Src or Dst = 5060 5061 5062

RTP
UDP = Src **AND** Dst = 16384-32767

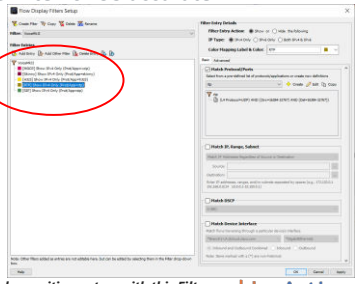


LiveAction
181

181

Classification: Voice Filter is ~95 accurate

- MGCP
- Skinny
- h323
- RTP
- SIP



Note: There will likely be a false positive or two with this Filter

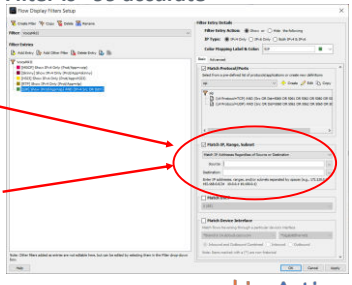
LiveAction
182

182

Classification: Voice Filter is ~99 accurate

Add CallManager Server(s) IP address to Filter For:
- MGCP
- Skinny
- h323
- SIP

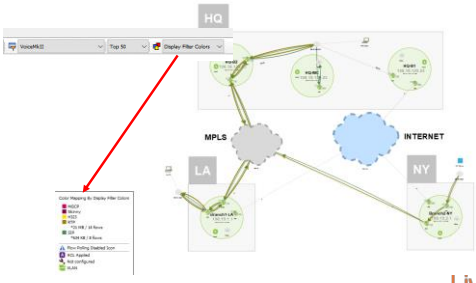
If feasible, add voice subnets to:
- RTP



LiveAction
183

183

Classification: Display Filter Colors



LiveAction

 184

184

Classification: IPs & Ports Report

Use this report to validate Filter's Accuracy.

NBAR2 is your Friend!

LiveAction

 185

185

Marking: Selecting DSCP Values

Class Type Cisco Name/ RFC4594 Name	4 Class	8 Class	12 Class
Voice / IP Telephony	EF (46)	EF (46)	EF (46)
Interactive Video / Multimedia Conferencing	CS5 (40) CS4 (32)	CS5 (40) CS4 (32)	AF41 (34) AF42 (36) AF43 (38)
Streaming Video	AF31 (26) AF32 (28) AF33 (30)	AF31 (26) AF32 (28) AF33 (30)	AF31 (26) AF32 (28) AF33 (30)
Real-Time Interactive			CS4 (32)
Broadcast Video			CS5(40)
Call Signaling	CS6 (48)	CS3 (24)	CS3 (24)
IP Routing / Network Control	CS3 (24)	CS2 (16)	CS6 (48)
Network Management	CS2 (16)	CS6 (48)	CS2 (16)
Transactional Data / Low-Latency Data	AF41 (34) AF42 (36) AF43 (38) AF31 (26) AF32 (28) AF33 (30) AF21 (18) AF22 (20) AF23 (22) AF11 (10) AF12 (12) AF13 (14)	AF41 (34) AF42 (36) AF43 (38) AF21 (18) AF22 (20) AF23 (22) AF11 (10) AF12 (12) AF13 (14)	AF21 (18) AF22 (20) AF23 (22)
Bulk Data / High Throughput Data			AF11 (10) AF12 (12) AF13 (14)
Scavenger / Low-Priority Data	BE (0)	CS1 (8)	CS1 (8)
Best Effort		BE (0)	BE (0)

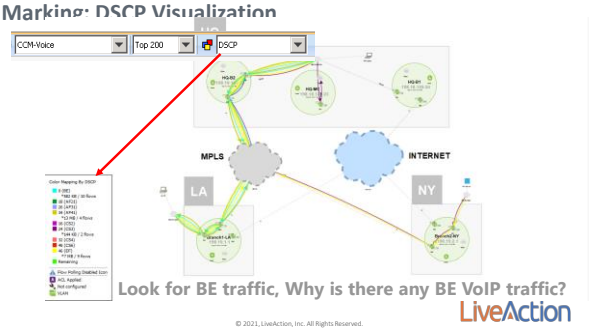
These are just Cisco's recommendations – all values are arbitrary!
You can use any of the 64 values, but you will see these most often.

LiveAction

 186

186

Marking: DSCP Visualization



Look for BE traffic, Why is there any BE VoIP traffic?

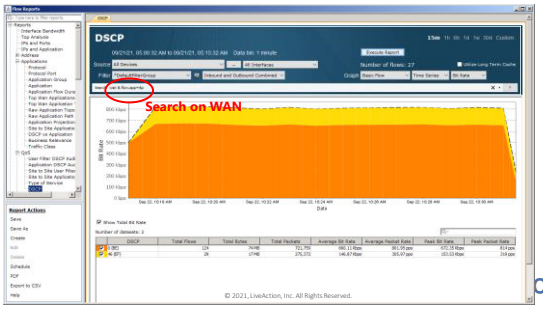
LiveAction

 187

187

Marking: DSCP Report

Is there any BE VoIP traffic?

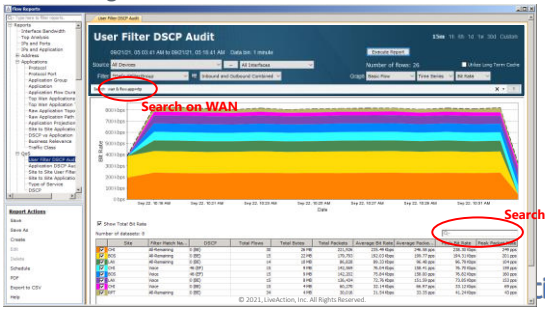


 188

188

Marking: User Filter DSCP Audit

Where is the BE VoIP traffic?

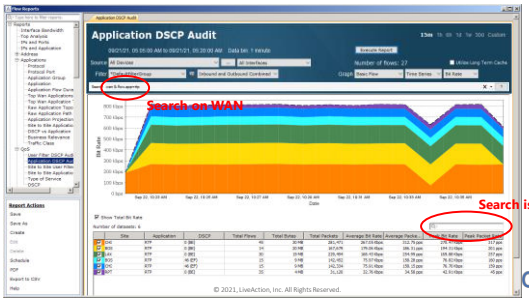


 189

189

Marking: Application DSCP Audit

Where is the BE VoIP traffic?

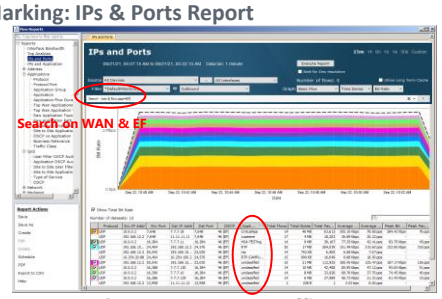


on

190

190

Marking: IPs & Ports Report



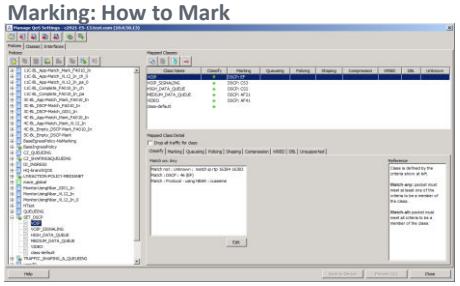
Is there any Rogue EF traffic?

LiveAction

191

191

Marking: How to Mark



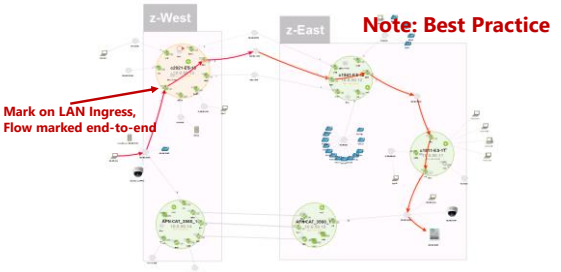
To Classify: Use ACLS, DSCP, & NBAR2. Then mark with appropriate DSCP.

LiveAction

192

192

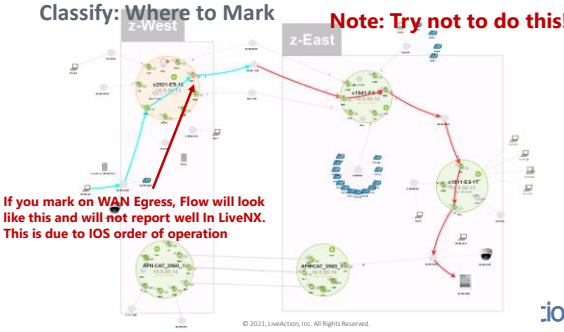
Classifv: Where to Mark



LiveAction
193

193

Classify: Where to Mark

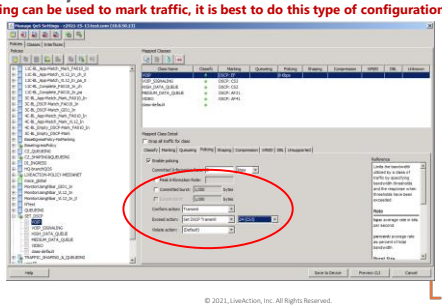


194

194

Classify: Where to Mark

Policing can be used to mark traffic, it is best to do this type of configuration on LAN ingress too



LiveAction
195

195

Classify: Next Steps?

1. **Use same visualization & reports to validate polices**
2. **Repeat these steps for all important applications**

LiveAction
196

196

Lab: Classify / Mark

- Run Reports
- Recognize application traffic
- Mark
- Validate DSCP values

LiveAction
197

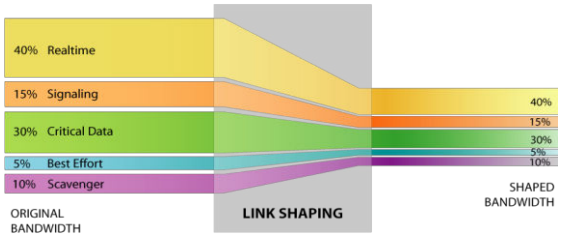
197

Queueing & Shaping

LiveAction
198

198

Shaping: Throttle Traffic via software & Queue

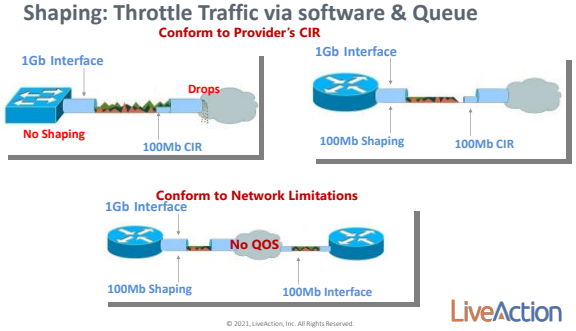


LiveAction

 199

199

Shaping: Throttle Traffic via software & Queue

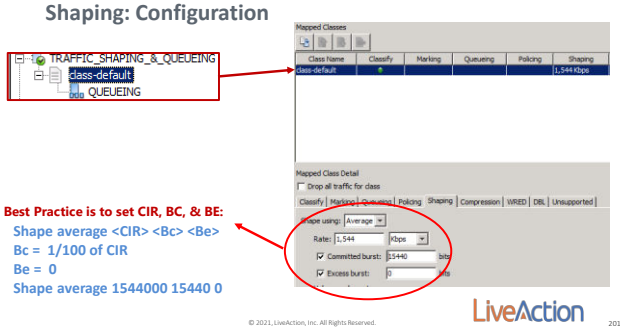


LiveAction

 200

200

Shaping: Configuration

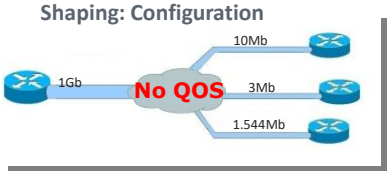


LiveAction

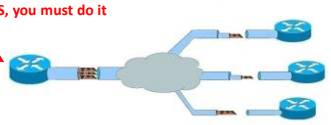
 201

201

Shaping: Configuration



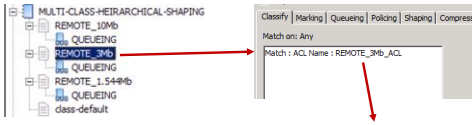
This design requires a Multi-Class Hierarchical Policy
Since the provider doesn't have QOS, you must do it

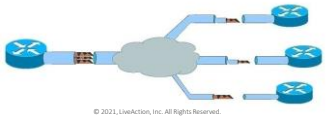


 202

202

Shaping: Configuration





veAction 203

203

Queueing: Selecting Bandwidth Allocations

Class Type Cisco Name/ RFC4594 Name	4 Class	8 Class	12 Class
Voice / IP Telephony	≥33%	10%	10%
Interactive Video / Multimedia Conferencing		23%	10%
Streaming Video		10%	10%
Real-Time Interactive			13%
Broadcast Video			10%
Call Signaling	Remaining	2%	2%
IP Routing / Network Control		5%	2%
Network Management / Operations,Administration,Management (OAM)			2%
Transactional Data / Low-Latency Data		24%	10%
Bulk Data / High Throughput Data	≤5%	1%	5%
Scavenger / Low-Priority Data			1%
Best Effort	≥25%	25%	25%

These are Cisco's SRND recommendations, these are good starting points. LiveNX is great at helping with this!

LiveAction 204

204

Queueing: Understanding Traffic

This is how one voice call looks:

1x G.711 Call is ~82 Kbps
1x G.729 call is ~ 24.6 Kbps

Consistent pps = no burst

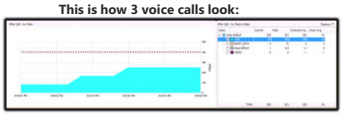
LiveAction

205

205

Queueing: Understanding Traffic

This is how 3 voice calls look:



1x G.711 Call is ~82 Kbps
2x G.711 Call is ~164 Kbps
3x G.711 Call is ~246 Kbps

Etc...

No Burst = No Buffer Tuning

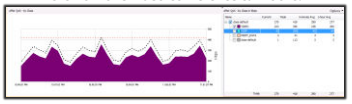
LiveAction

206

206

Queueing: Understanding Traffic

This is how one video conference call looks:



Resolution	1080p			720p		
Quality	Best	Better	Good	Best	Better	Good
Frame Rate	30	30	30	30	30	30
Bandwidth	4Mb	3.5Mb	3Mb	2.25Mb	1.5Mb	1Mp
Max Burst (IDR + AUX)	128K	128K	128K	128K	128K	128K

Overprovision Video Queues by 20% & Tune Buffers

LiveAction

207

207

Queueing: Understanding Traffic

Know critical apps SLA Targets!

Parameter	VOIP	Traditional Video	HD / Immersive Video
Bandwidth	8-90Kbps	384 -768 kbps + network overhead	1.5 - 12.6 Mbps + network overhead
Latency	150ms	400-450ms	150ms
Jitter	30ms	30-50ms	10ms
Loss	1%	1%	0.05%

Treat with Care!

LiveAction

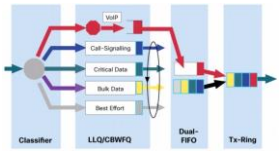
208

208

Queueing: Understanding Traffic

Voice = LLQ /Priority Queue

Video = ?



LiveAction

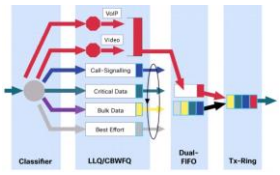
209

209

Queueing: Understanding Traffic

Voice = Priority Queue/LLQ

Video = Priority Queue/LLQ



****Always put Video in its own unique queue****

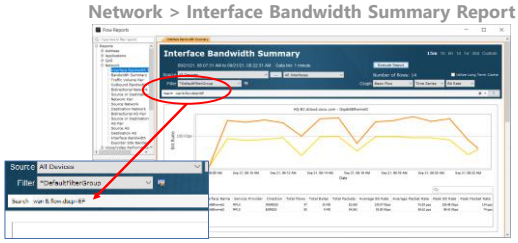
LiveAction

210

210

Queueing: Sizing/Capacity Planning

Network > Interface Bandwidth Summary Report



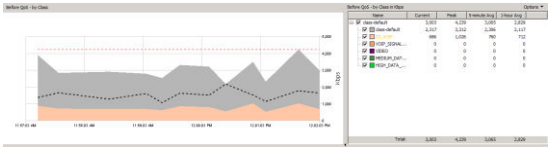
If Classification & Marking are in place, Flow is a great way to do queue sizing

LiveAction
211

211

Queueing: Sizing/Capacity Planning

Pre-Policy QoS Report is a Great QoS Sizing Report



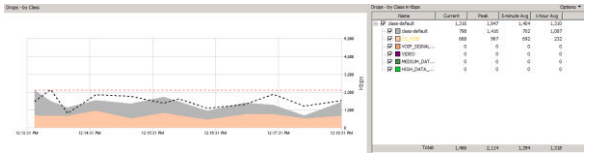
This report shows the volume of bandwidth of each queue before QoS is actually applied

LiveAction
212

212

Queueing: Capacity Planning

QoS Drop Report can also be a QoS Capacity Report



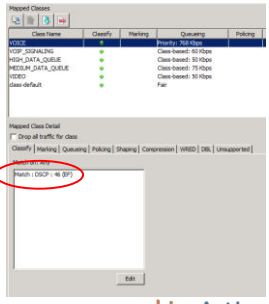
This report shows the volume of traffic dropped after QoS is applied. This can be good for finding gross sizing errors. But is not the whole story, fixing drops may also required buffer tuning too!

LiveAction
213

213

Queueing: Configuration

Match on DSCP



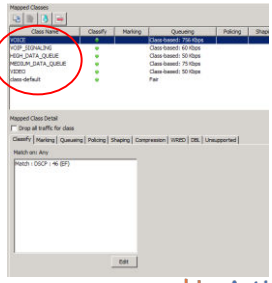
LiveAction

214

214

Queueing: Configuration

Order Queues based on priority. Queues are match in a top-down order, so this helps ensure priority traffic is matched by the appropriate queue if there are configuration mistakes. It does not change the priority of traffic transmission.



LiveAction

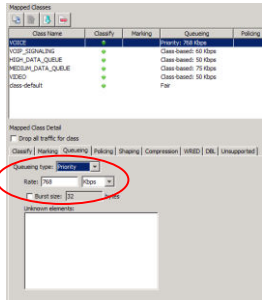
215

215

Queueing: Configuration

Voice = Priority Queue
Video = Priority Queue (usually)
Everything else = Class based
Default = Fair Queue (optional*)

**There will be more drops with fair-queue*



LiveAction

216

216

Lab

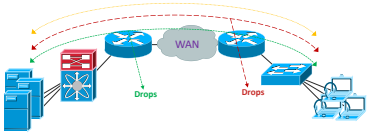
- Prioritization (Queueing & Shaping)
  - Capacity Planning Reports
  - Configure Queueing
  - Configure Shaping
  - Create Validating Policy

LiveAction
217

217

218

Step 3 –Throttle Traffic (Policing and WRED)

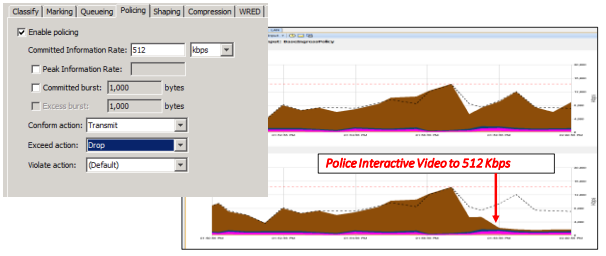


- **Policing** - Transmit data to software set limit, drop overage
- **WRED** – Selectively drop specific data before congestion occurs

LiveAction
219

219

Policing



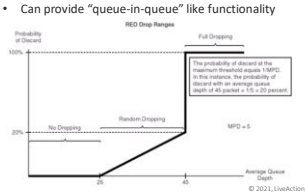
Best done on LAN ingress close to source

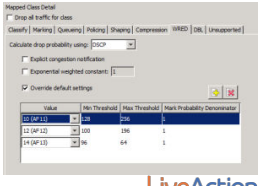
LiveAction
220

220

WRED – What It IS…

- WRED = Weighted Random Early Detection
- What is a Queue? It's a "holding tank" for when there is too much data to be sent
- Default queue depth is 64 packet. When queue is full, "tail drop" begins
- WRED allows you to randomly start dropping data before the queue is full, to try to avoid congestion (tail drop). Min Thresholds is when random drops begin. Max Threshold = Tail Drop.
- The "W" stands for weighted – allows a queue to reference DSCP values and assign each a different depth before the random drops begin.
- Can provide "queue-in-queue" like functionality



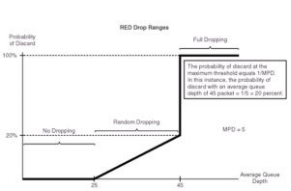


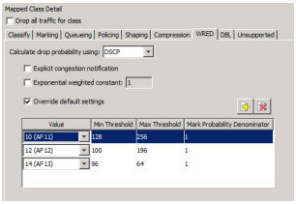
LiveAction
221

221

WRED - Warning!

- Will cause more drops (harm) than normal, if not tuned correctly
- Typically, only effective if multiple DSCP values are in a Queue





LiveAction
222

222

Lab

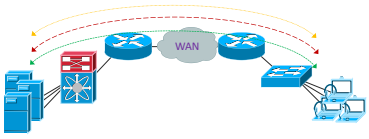
- Throttling Traffic (Policing & WRED)
  - Implement Scavenger Queue
  - Police Queue

LiveAction
223

223

224

Step 4–Buffer Tuning (Advanced)



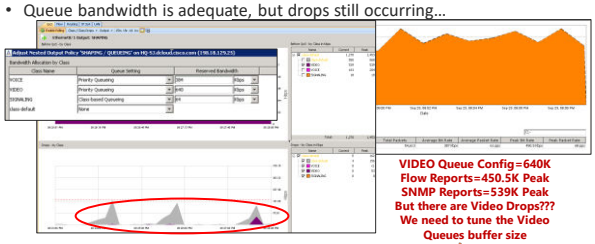
- **Queue-limit** – Buffer size that stores queue data during congestion
- **Priority queue BC** – Token bucket interval that schedules the releases data in priority

LiveAction
225

225

Buffer Tuning

- Only really needed for critical, but bursty queues – VIDEO, Citrix(VDI), etc.
- Queue bandwidth is adequate, but drops still occurring…



VIDEO Queue Config=640K
Flow Reports=450.5K Peak
SNMP Reports=539K Peak
But there are Video Drops???
We need to tune the Video Queues buffer size

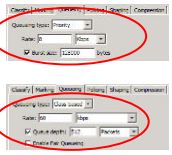
LiveAction

226

Buffer Tuning

Interface's hold-queue >= total of all queues queue-limit
Show interface shows the size of the hold-queue
Output queue: 72/***1000***/1732089236 (size/max total/drops)

```
policy-map CZ_QUEUEING
class CZ_VOIP
priority 8 128000
exit
class VOIP_SIGNALING
bandwidth 60
queue-limit 512
```



LiveAction

227

Lab

- Buffer Tuning
  - Video Queue Performance Tuning

LiveAction

228

229

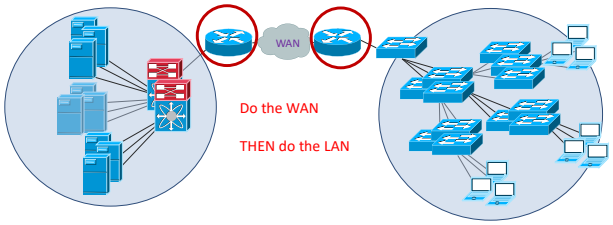
QoS Deployment Strategies

Step 1 - Deploy QoS in Phases
Step 2 - Use NetFlow Tools to Understand Bandwidth Usage
Step 3 - Understand Application Details
Step 4 - Get Business' Buy-In
Step 5 - Understand the Network
Step 6 - Have a Plan
Step 7 - Use QoS Management Tools
Step 8 - K.I.S.S.

LiveAction
230

230

Step 1 : Implement QoS in Phases!



LiveAction
231

231

Step 2 - Use NetFlow Tools to Understand Bandwidth Usage

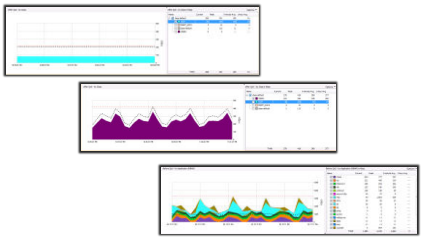
*Use minute by minute reporting (no Averaging)

LiveAction

232

232

Step 3 - Understand Applications Details



LiveAction

233

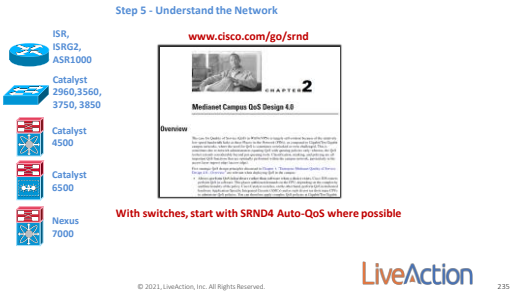
233

Step 4 - Get Business' Buy-In

LiveAction

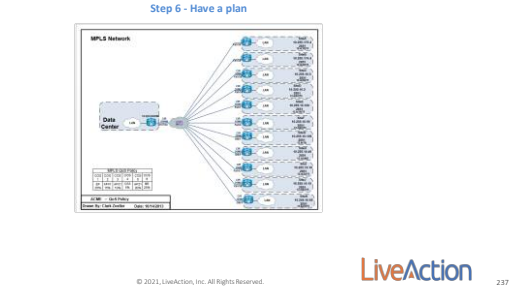
234

234



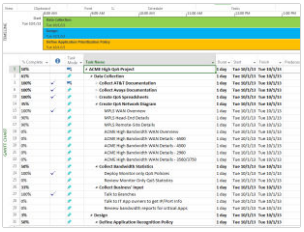
235

236



237

Step 6 - Have a plan

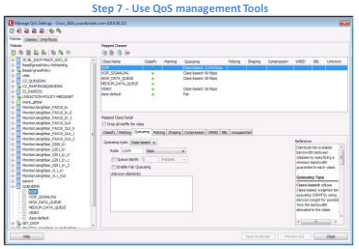


LiveAction

238

238

Step 7 - Use QoS management Tools

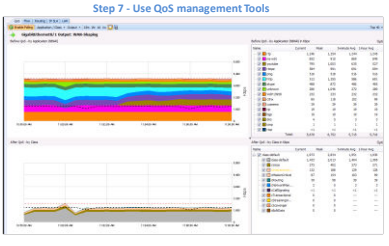


LiveAction

239

239

Step 7 - Use QoS management Tools

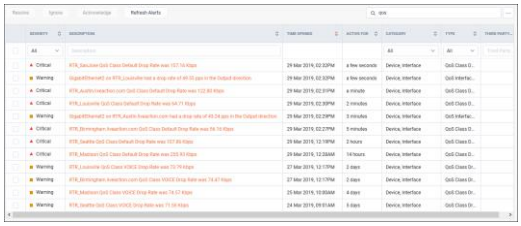


LiveAction

240

240

Step 7 - Use QoS management Tools



LiveAction

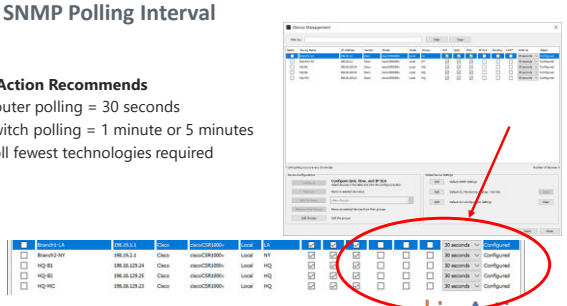
 241

241

SNMP Polling Interval

LiveAction Recommends

- Router polling = 30 seconds
- Switch polling = 1 minute or 5 minutes
- Poll fewest technologies required

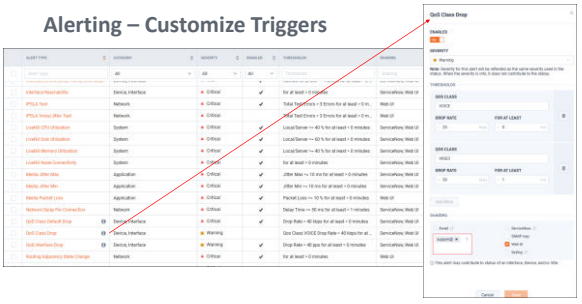


LiveAction

 242

242

Alerting – Customize Triggers



LiveAction

 243

243

Finish the Labs…

LiveAction

244

245

Agenda

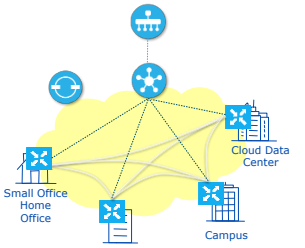
- Cisco/Viptela SDWAN Overview
- LiveNX – SDWAN Integration Overview
- Day 0: Cisco SD WAN Planning for Deployment
- LiveNX - SDWAN Onboarding
- Day 1: Cisco SD WAN Policy Validation and Intent
- Day 2: Cisco SD WAN Operations

LiveAction

246

247

SDWAN Basics



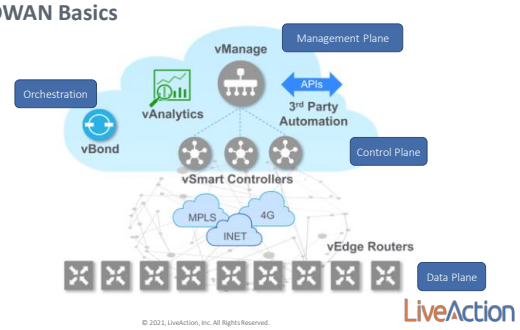
- vEdge – SDWAN Edge Router
- vManage – SDWAN Manager
- vBond – SDWAN Orchestrator
- vSmart – SDWAN Controller

LiveAction

248

248

SDWAN Basics

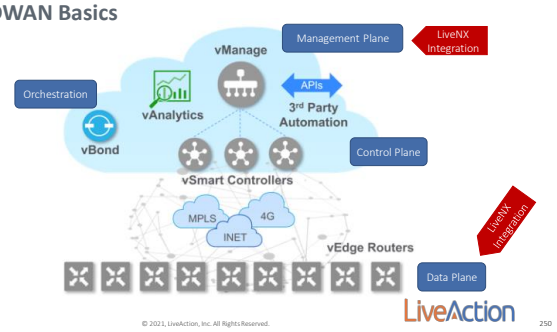


LiveAction

249

249

SDWAN Basics

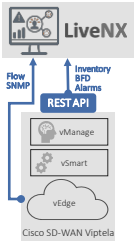


LiveAction
250

250

251

LiveNX and Cisco SD-WAN Viptela Overview



LiveNX receives data from the vEdges and vManage

- vManage
  - Inventory information is pulled to onboard the SDWAN devices
  - Other information like routing tables is used to populate site info
  - Tunnel health (BFD) loss, delay, and jitter measurements are pulled
  - vManage alarms are pulled every 5 minutes
- vEdge
  - LiveNX polls vEdges via SNMPv2 or v3 for device statistics (interface, cpu, memory, etc)
  - vEdges export cflowd to LiveNX collection nodes which includes:
    - source & destination address and port info for each flow
    - Byte and packet counts per flow
    - Each flow also includes an App ID which is the application identified by the deep packet inspection engine on the vEdge

[1] Bidirectional Forwarding Detection

LiveAction
252

252

Network Preparation - Summary

Required Tasks

- Collect management IP range for the Cisco SD-WAN (Viptela) vEdge routers
- Enable SNMP v2/v3 RO access for LiveNX monitoring
- Collect SNMP v2/v3 community/password
- Configure centralized data policy to enable Flow on LAN Interfaces
- Set Flow active timeout = 60 sec
- Set Flow inactive timeout = 15 sec
- Collect vManage hostname/IP address, username and password
  - Used for polling northbound API's from vManage (Inventory, BFD, Alarms, etc)

LiveAction
253

253

254

Day 0: Design Baseline performance for policy design

Site to site traffic performance	App group behavior	Service Provider analysis
		

• Site to site traffic type and paths
• Provides data for:
  • Selection of initial pilot sites
  • Usage patterns
  • Site to site traffic behaviors
	• App Group behavior
	• Policy design inputs:
	  • App consumption patterns – bandwidth, class
	  • Performance baseline – know targets for SLAs
		• Service Provider
		• Path design inputs:
		  • Which telco infrastructure path they should apps take, site by site.
		  • Picking application to include in app route policies
		  • How SD-WAN enabled vs non SD-WAN traffic maybe handled during deployment

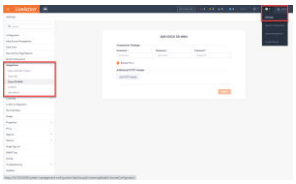
LiveAction
255

255

LiveNX SD-WAN On-Boarding

Required Tasks

- Onboard SD-WAN devices via LiveNX integration with vManage (via REST API). This simplifies:
  - vEdge router discovery
  - Monitoring of WAN and LAN interfaces
  - Automatically sets network semantics including sites, WAN links, service providers, site IP prefixes, etc
- Confirm reception of Flow on vEdge Routers
- Confirm BFD data from integration with vManage



LiveAction

256

256

257

Day 1: Verify

Policy verification at scale

Overlay performance	Policy performance	Application performance
		

• Transport view
• Geo map
  • Quickly verify site to site behavior during deployment
• Verify the overlay performance:
  • Verify service VPN topology matches the intent set via policy
  • Verify service provider performance
  • Traffic engineering / paths
	• Virtual overlay view
	• Site to Site diagram - Verify legacy and SD-WAN controlled traffic behavior
	• Verify policy enforcement:
	  • Verify application and user traffic is associated to correct service VPN
	  • Verify split handling of legacy traffic and SD-WAN traffic
		• Custom Reports
		• Verify vEdge or cEdge transport VPN connecting to SP network and performance
		• In/Out bound resource allocation
		  • Bandwidth
		  • Latency, jitter, packet drops

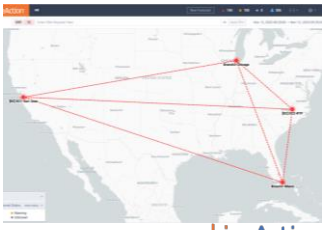
LiveAction

258

258

Verify that your control policy is working as intended

- Full Mesh or Hub&Spoke?
- Use the Geo Topology map to visualize your data plane topology
- Apply a VRF filter to see the data tunnels only for that VPN



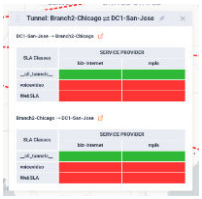
LiveAction

259

259

Verify Application Aware Routing Policy

- Use the Sankey Diagram to visualize which traffic is going over which WAN transport
- Launch from Site-toSite story or from the Geo Topology Map



LiveAction

260

260

Use the Playback feature to verify traffic steering

- Does critical traffic get steered to the alternate WAN transport when the preferred tunnel suffers an outage or brownout
- Set the time interval at the top of the diagram to capture the problem event
- Use the playback at the bottom to visualize the traffic moving between transports

LiveAction

261

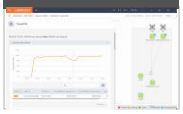
261

262

Day 2: Scale and Operate

Performance insights for optimization and rapid troubleshooting

Enterprise visibility



- Enterprise visibility - multi-vendor
- NOC Operation workflows
  - alerting, dashboards, reports, capacity planning, integrations
- Situational awareness:
  - Sites
  - Applications
  - Service Providers

Flow Path analysis

- Visual path analytics
- Verification of policy changes at scale
- Understand app path switching
  - site to site tunnel performance correlated to service provider and policy thresholds

Deep packet analysis

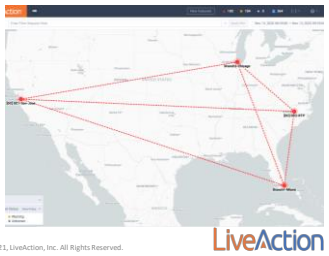
- LiveWire and Omnipliance packet capture and analysis appliance
- Packet drill down
- Delivers intuitive visualization and robust forensics for faster incident resolution of network issues
- application performance issues and security investigations. 2

LiveAction
263

263

Use the Geo Topology to monitor tunnel status

- Here we see all tunnels are red
- LiveNX is using the loss/latency/jitter statistics to show SLA violations

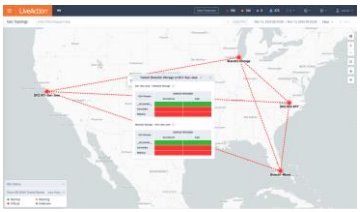


LiveAction
264

264

Use the Geo Topology to monitor tunnel status

- Here we see all tunnels are red
- LiveNX is using the loss/latency/jitter statistics to show SLA violations
- Click on a data tunnel to drill into the tunnel status for each SLA class



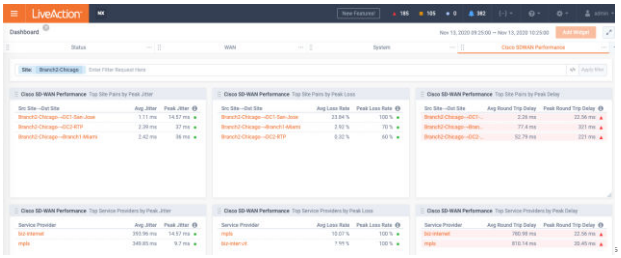
LiveAction

265

265

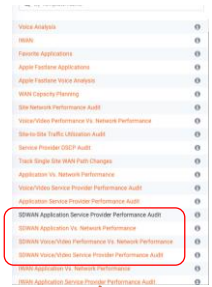
Cisco SDWAN Performance Dashboard

The SDWAN Dashboard has many widgets that put site health at your fingertips



266

There are also pre-configured SDWAN report templates



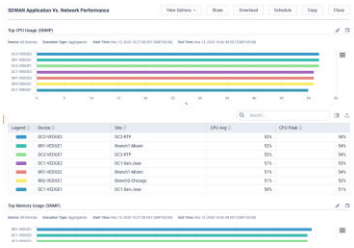
LiveAction

267

267

SDWAN Application Vs. Network Performance

- These reports will draw on all data sources:
  - vManage API
  - SNMP
  - Flow
- These reports put operational details at your fingertips



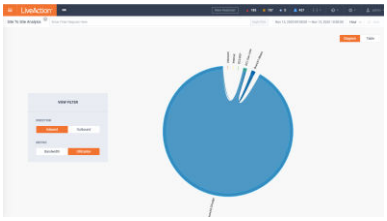
LiveAction

268

268

Site To Site Analysis Story

Quick view of traffic between sites



LiveAction

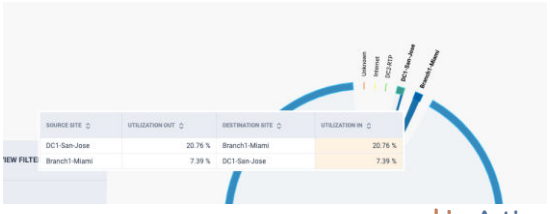
269

269

Site To Site Analysis Story

Mousing over any one of the sites allows to see site specific stats

Clicking on a site will launch the Sankey Diagram of all traffic for that site



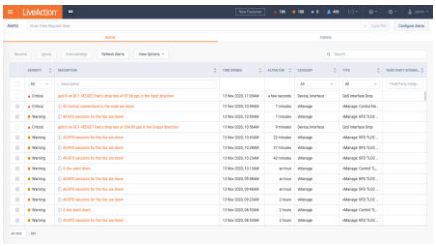
LiveAction

270

270

Alerting

- In addition to the standard LiveNX alerts there are specific SDWAN Alerts
- LiveNX imports vManage Alarms via the API



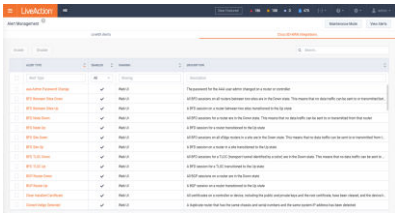
LiveAction

271

271

Alert Configuration

- All the Cisco SD-WAN Integrations alerts are the ones imported from the vManage alarms
- Any vManage alarms to be displayed must me enabled here
- It is recommended to only enable the vManage alarms that are of particular interest



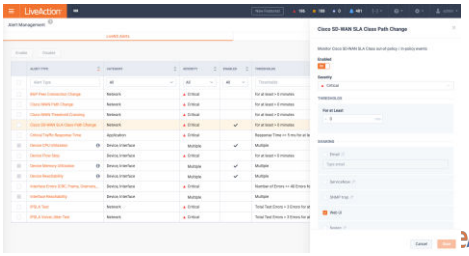
LiveAction

272

272

Cisco SD-WAN SLA Class Path Change Alert

- SDWAN specific alert generated by LiveNX based on the loss/latency/jitter measurements (NOT imported from vManage
- Should be fired when a tunnel has an SLA class change



LiveAction

273

273

Launch the SDWAN Learning Labs…

LiveAction

274

274

275

LiveAction Support

- Global support
  - Contact support@liveaction.com
  - Call: 408-217-6501
    - Monday-Friday 6am -7pm Pacific Time
  - 24x7 *Priority One* support
- "Resources" website
  - www.liveaction.com/support/resources/
    - Product Downloads - Release notes
    - Knowledge base
    - Documentation
    - Training Videos
- Professional Services has many offerings to assist you in your deployment and network maintenance
  - Contact sales@liveaction.com

LiveAction

276

276

Training Resources

You will get these resources in an email

- Videos: https://www.liveaction.com/resources/#category-video
- Tips and Tricks: https://www.liveaction.com/tips-and-tricks
- White Papers: https://www.liveaction.com/resources/#category-white-papers-solution-briefs
- Documentation: https://docs.liveaction.com/

LiveAction
277

277

Course Evaluation

We'll use this information to improve our courses and teaching methods. Please enter as much comment material as you'd like… the more info you add, the better we'll get!

Point your browser to: (This is also in the email!)

http://www.surveygizmo.com/s3/2657898/312e4e3f5212

Please select Instructor and Course info…

- **Course:** Intro to LiveNX
- **Instructor Name:** David Lau

Thank You in advance for your participation!

LiveAction
278

278

279