1

© Copyright 2019 LiveAction, Inc.

2019April01

2

Agenda – Day 1

- LiveNX Architecture Review
- The LiveNX WebUI
  - Dashboards
  - Sites/Devices/Interfaces
  - Reports
    - Stories
    - Scheduling
    - Custom Reports
  - System Management
- Visualizations & Troubleshooting
  - Voice, Video, Delays
- Flow Collection Overview
- LiveNX Client
  - Dashboard
  - Reports
- Topology Navigation
- Add & Manage Devices
  - Topology Navigation
  - Grouping & Objects
  - Device Semantics
- QoS Overview

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
- Troubleshooting
  - IWAN Cheat Sheet

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

2019Apr01 7

LiveAction

7

2019Apr01

LiveAction™

9

Live

Simplify the Network

History

2006

2014

7000+

2017
LivingObjects
Service Providers

2018
Packet Capture
& Analytics

Investors

2019Apr01 10

10

Complete Solution

LiveNX
For Enterprises

LiveSP
For Service Providers

LiveCapture Omnipeek
Packet Capture and Analytics

Insight
Predictive Analytics

LiveAgent
End Point Visibility

LiveUX
User Experience Monitoring

LiveNCA
Network Configuration and Automation

LiveAction

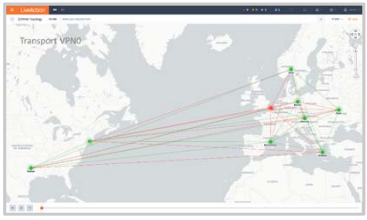
2019Apr01 11

11

Driven by our patented Visualization engine

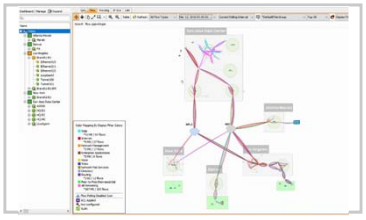
Enterprise Visibility

Transport View

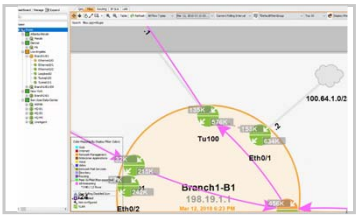


Virtual Overlay View

Visual Path Analytics



Site Specific Details

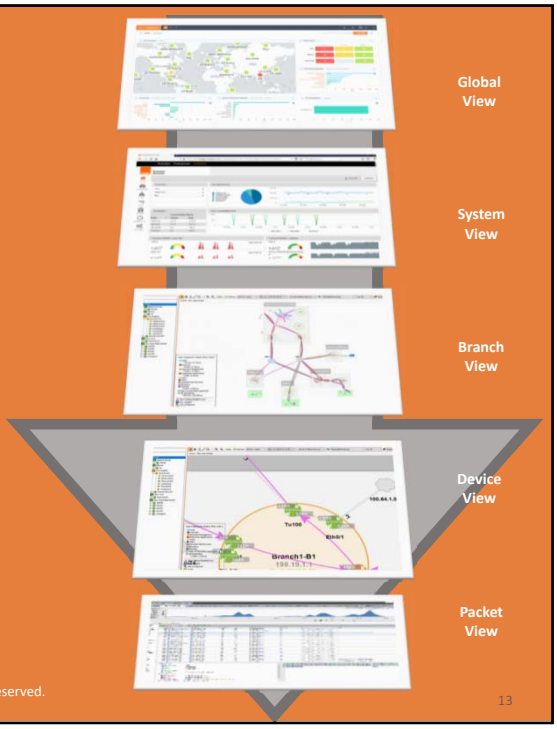


Packet Analytics

12

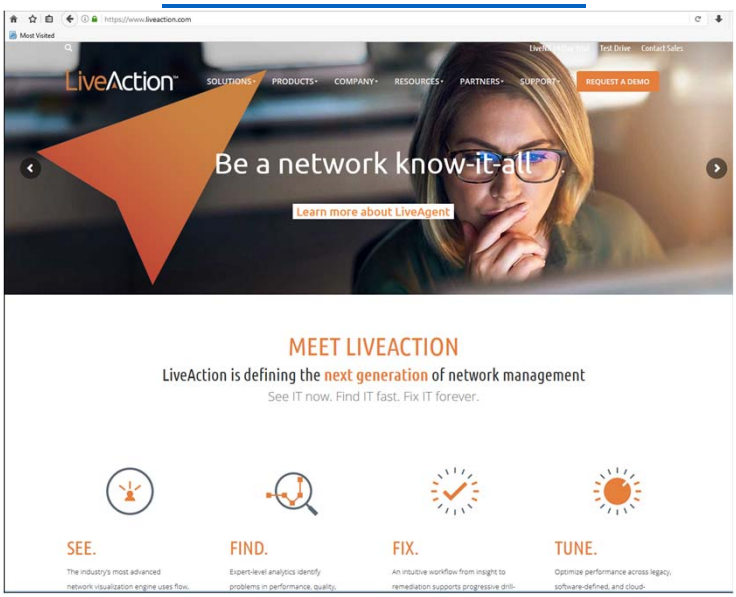
LiveAction Technology 2019

- Single Pane of Glass
- Tool consolidation
- Consistent Look and Feel
- Accessed via tabs on LiveNX or LiveSP
- All products connected via Single Sign On and delivered in common distribution



13

Browse to… www.LiveAction.com



2019Apr01 14

LiveAction

14

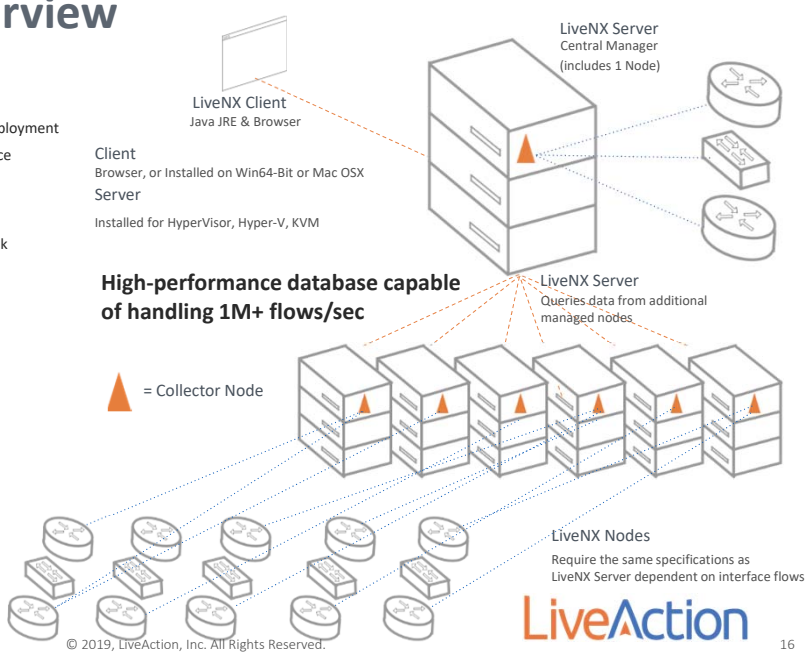
2019Apr01

LiveAction™

15

Architecture Overview

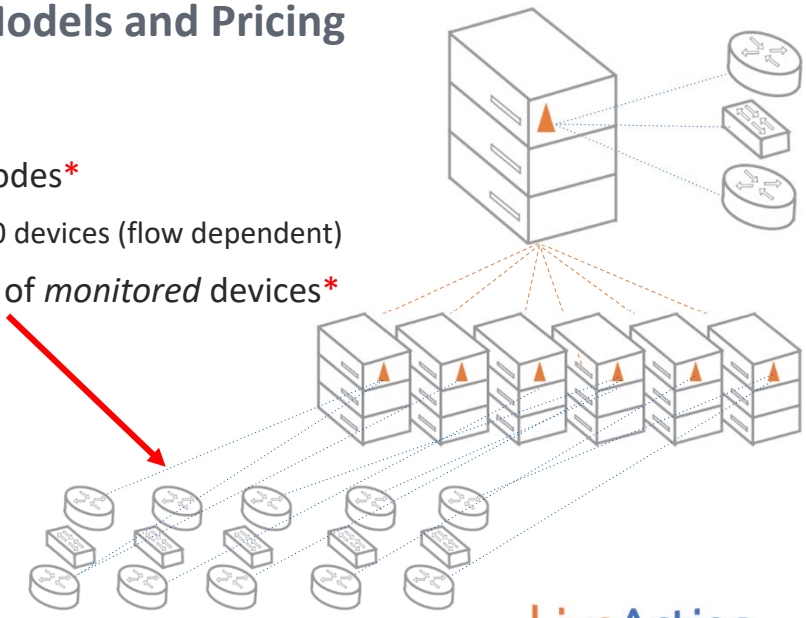
- **Distributed Computing Architecture**
  - Large scale distributed analytics platform
  - Monitor 40,000+ devices across distributed deployment
  - Visualize up to 1,000 active interfaces per device
  - 3-layer architecture – **client**, **server**, **node**
- **Client**
  - Single Pane of Glass (SPOG) 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



16

Simple License Models and Pricing

- Single-server
- Multiple Collector Nodes*
  - Collect from 200-500 devices (flow dependent)
- Based-upon number of *monitored* devices*

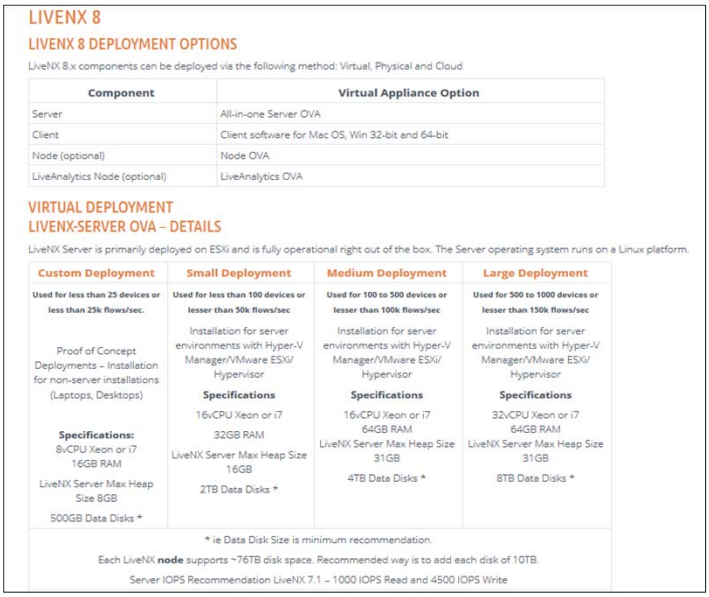


* Consumes a license

17

System Requirements

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



LIVENX 8

LIVENX 8 DEPLOYMENT OPTIONS

LiveNX 8.x components can be deployed via the following method: Virtual, Physical and Cloud

Component	Virtual Appliance Option
Server	All-in-one Server OVA
Client	Client software for Mac OS, Win 32-bit and 64-bit
Node (optional)	Node OVA
LiveAnalytics Node (optional)	LiveAnalytics OVA

VIRTUAL DEPLOYMENT
LIVENX-SERVER OVA – DETAILS

LiveNX Server is primarily deployed on ESXi and is fully operational right out of the box. The Server operating system runs on a Linux platform.

Custom Deployment	Small Deployment	Medium Deployment	Large Deployment
Used for less than 25 devices or less than 25k flows/sec.	**Used for less than 100 devices or lesser than 50k flows/sec**	**Used for 100 to 500 devices or lesser than 100k flows/sec**	**Used for 500 to 1000 devices or lesser than 150k flows/sec**
Proof of Concept Deployments – Installation for non-server installations (Laptops, Desktops)	Installation for server environments with Hyper-V Manager/VMware ESXi/ Hypervisor	Installation for server environments with Hyper-V Manager/VMware ESXi/ Hypervisor	Installation for server environments with Hyper-V Manager/VMware ESXi/ Hypervisor
Specifications: 8vCPU Xeon or i7 16GB RAM LiveNX Server Max Heap Size 8GB 500GB Data Disks *	**Specifications** 16vCPU Xeon or i7 32GB RAM LiveNX Server Max Heap Size 16GB 2TB Data Disks *	**Specifications** 16vCPU Xeon or i7 64GB RAM LiveNX Server Max Heap Size 31GB 4TB Data Disks *	**Specifications** 32vCPU Xeon or i7 64GB RAM LiveNX Server Max Heap Size 31GB 8TB Data Disks *

* ie Data Disk Size is minimum recommendation.

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

Server IOPS Recommendation LiveNX 7.1 – 1000 IOPS Read and 4500 IOPS Write

18

Network Devices Supported

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

CISCO DEVICE SUPPORT – SNMP & FLOW

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 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 Nexus Switches (Nexus 3000, 7000, 6000 & 9000 Series)
ASR 9000 Series Routers	Cisco NetFlow Generation Appliance	Cisco AnyConnect Network Visibility Module on Windows and Mac OS X Platforms
Cisco SD-WAN vEdge, Cisco IOS XE SD-WAN Edge Devices	Cisco ASA 5500 Series Firewalls	Cisco Meraki MX Security Appliance

*Recommend IOS versions 12.3 or higher or 15.0 or higher for use with the software (IOS XE 2.6.0 or higher for ASR 1000 series). Earlier IOS versions may also work but are not officially supported. General-release IOS versions are recommended, although early-and limited-release versions will also work with LiveNX.

MULTI-VENDOR DEVICE SUPPORT – FLOW

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

19

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.

20

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

21

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);

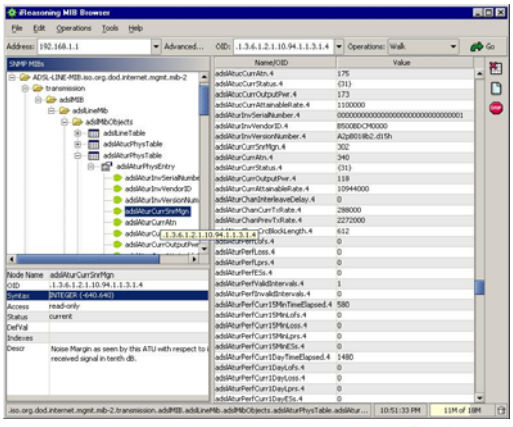
- QoS Configurations
- Netflow Configurations
- IP SLA Configurations
- Policy Based Routing
- Performance Routing

LiveNX does not save the router configuration in our database!

22

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



23

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
- You may now ping YOUR LiveNX Server…

2019Apr01 LiveAction 26

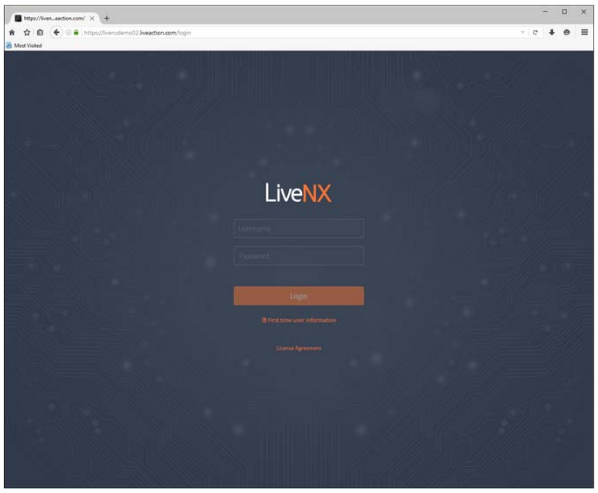
26

27

From Any Browser… from Anywhere!

https://<LiveNXserverIP>

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

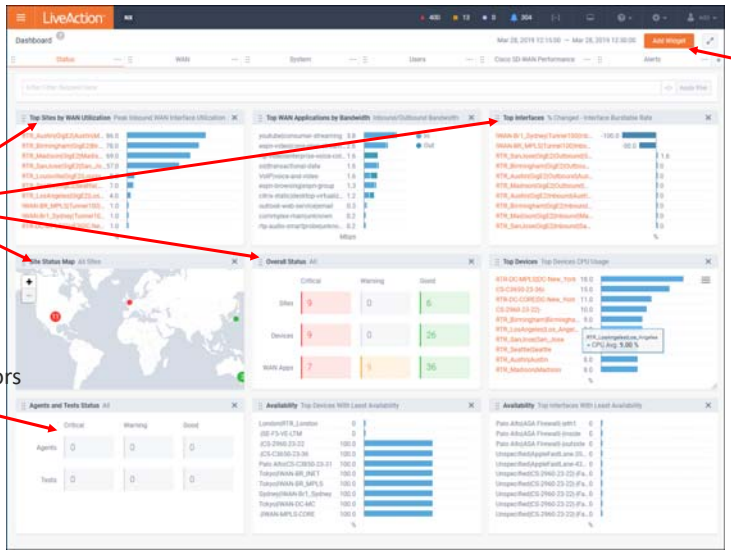


LiveAction

Customizable Dashboards

Lots of default building-block *widgets*

At-a-Glance indicators

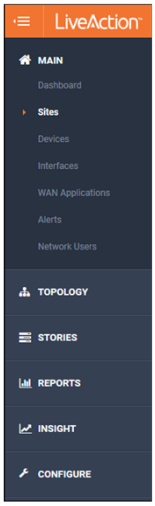


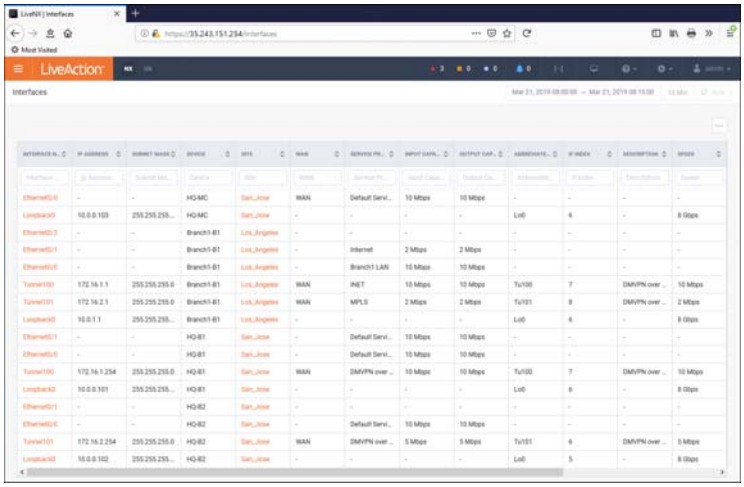
Build your own custom dashboard by adding widgets

LiveAction

Sites Details

Drill into Sites > Devices > Interfaces…

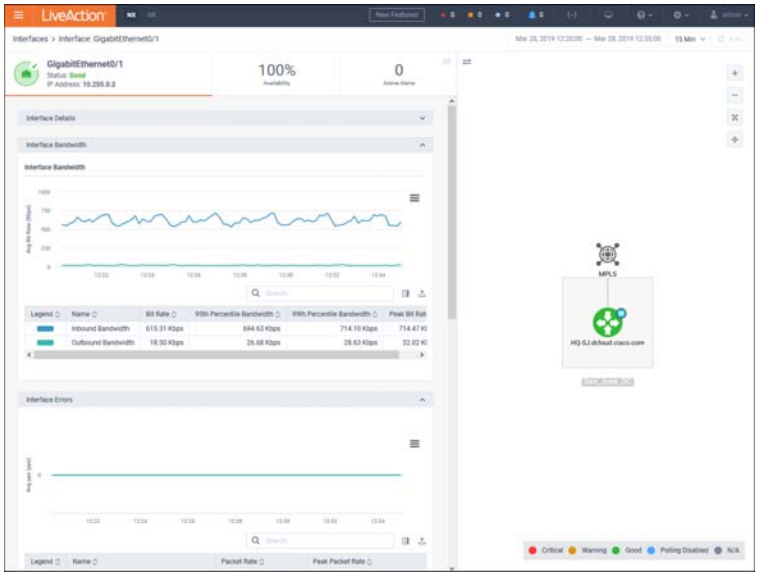




2019Apr01 30

30

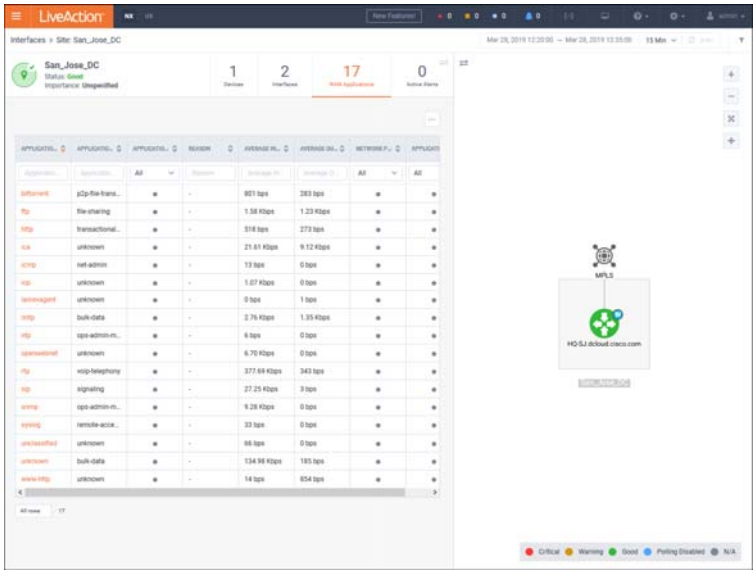
Interfaces



2019Apr01 31

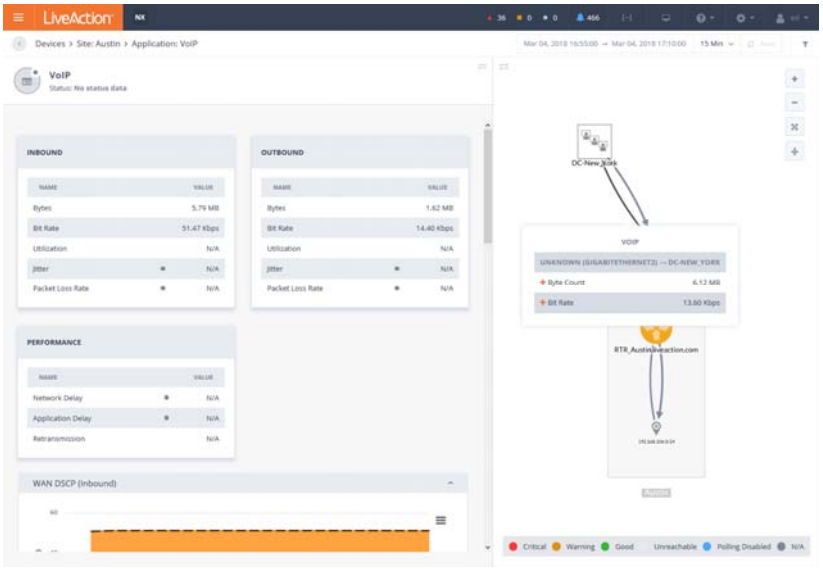
31

Wan Applications



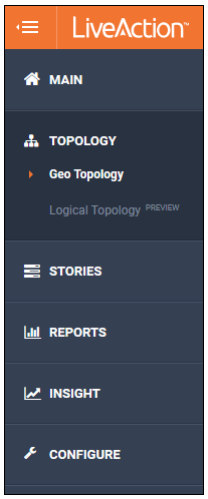
32

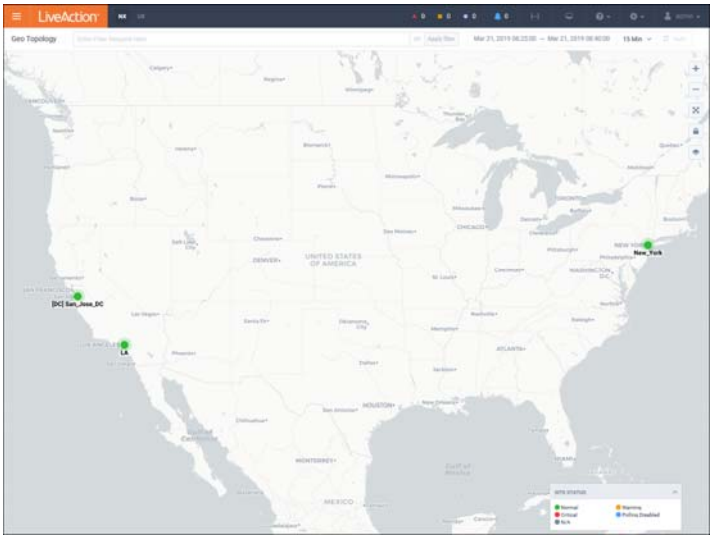
Wan Applications>Flows



33

Geo Topology

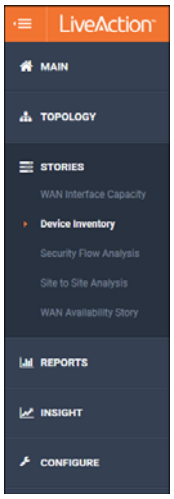


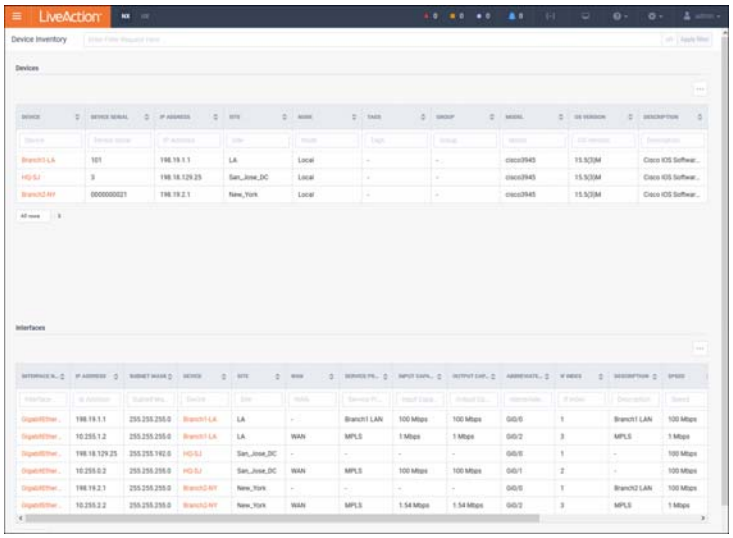


LiveAction

34

Stories

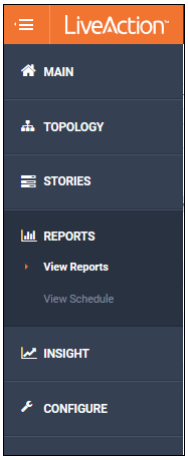


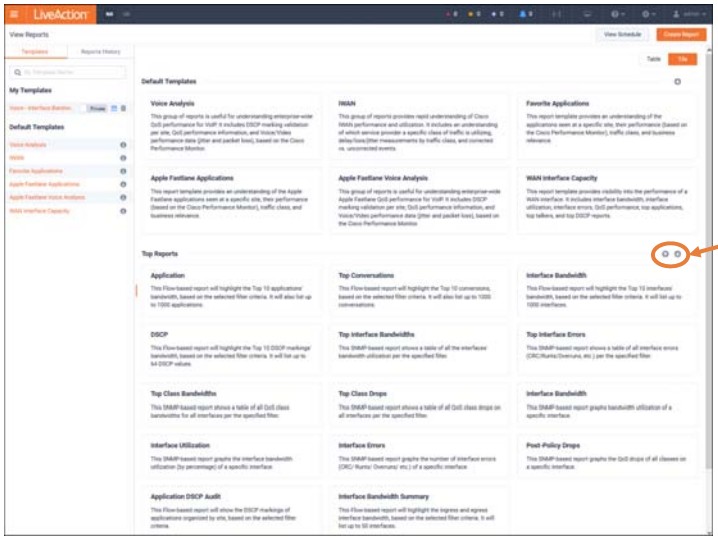


LiveAction

35

View ANY Report Defined in LiveNX

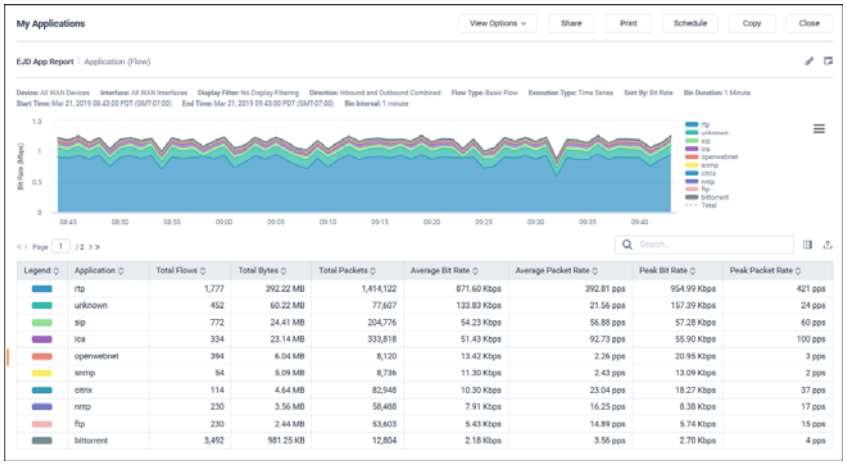




2019Apr01 36

36

Run Reports…

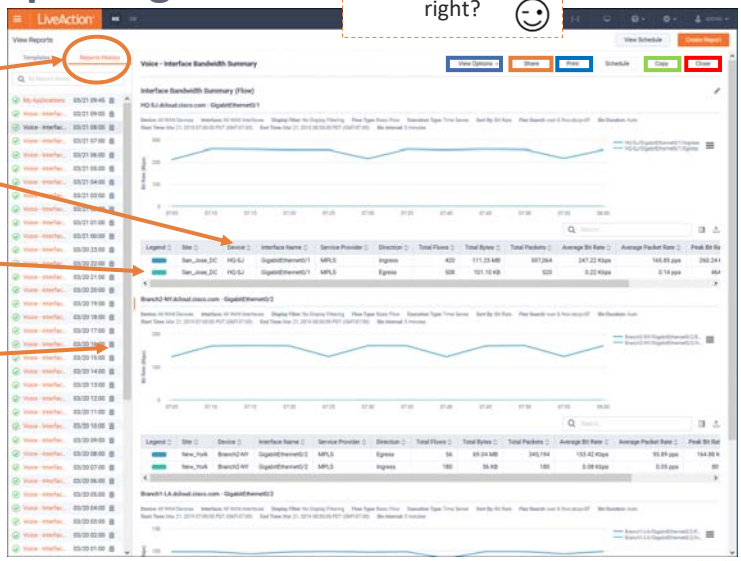


2019Apr01 37

37

WebUI Reporting – Tools

LOTS of stuff here… but, it's SO intuitive, right?



Include Report Elements

Copy URL to Clipboard

Print/Download (opens new URL)

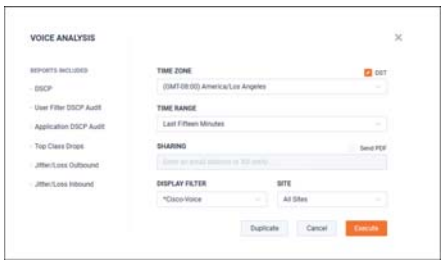
Re-open Run Report Dialog

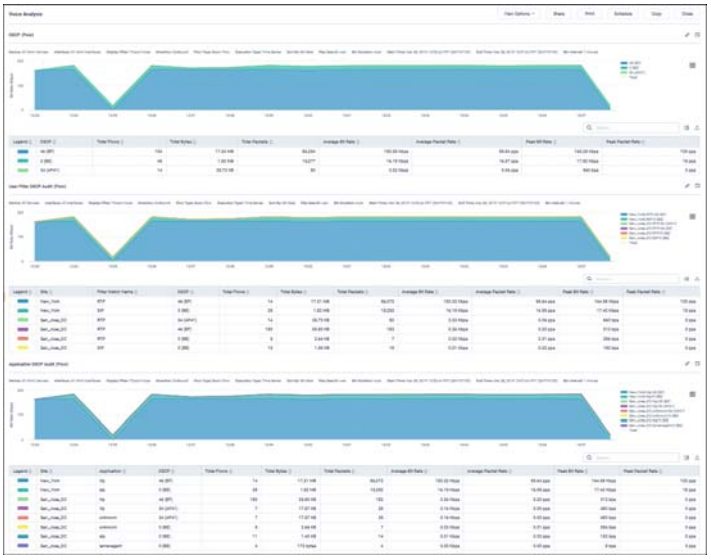
Return to Reports Entry Page

LiveAction

38

Report Groups





LiveAction

39

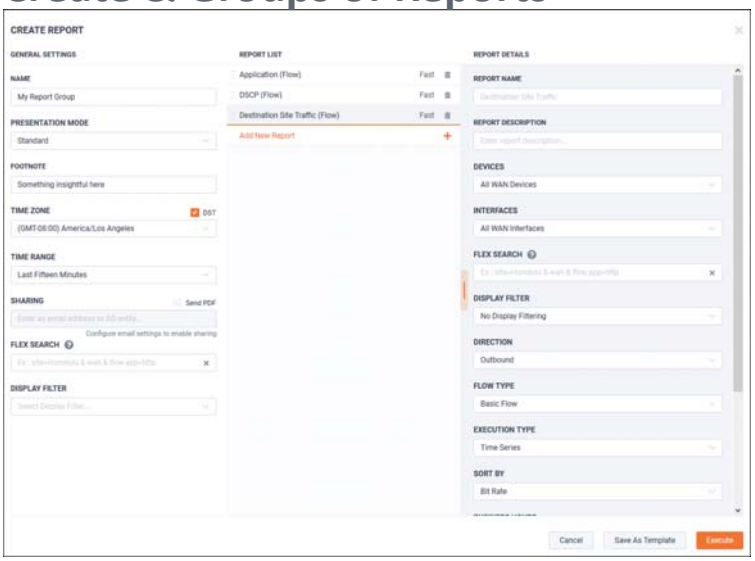
WebUI Reporting – Create & Groups of Reports

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

Advanced Report Group can be emailed to one or multiple users

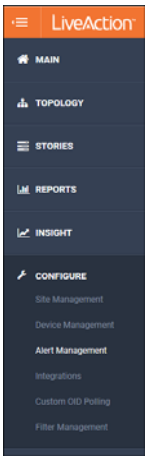
Note: Email server set up via Java Client

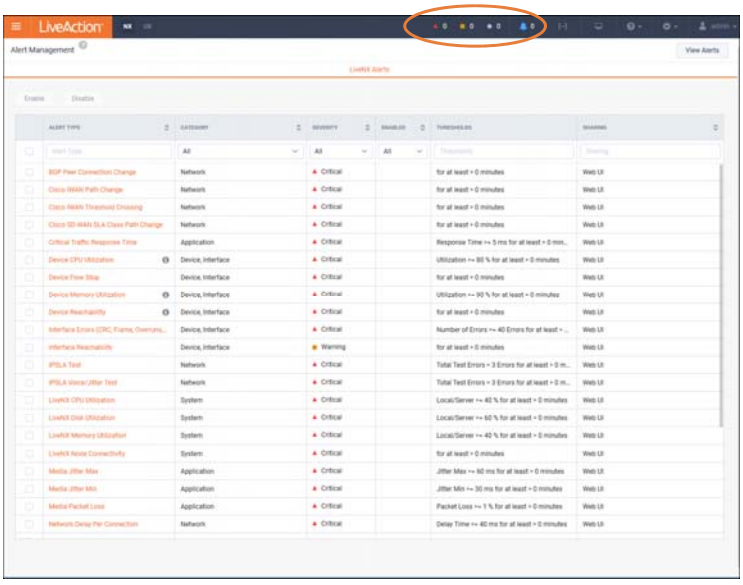
Advanced Reports allow the creation of groups of reports



40

LiveNX Alerting



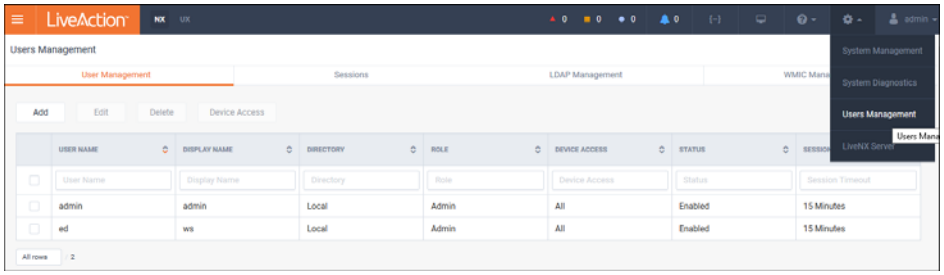


41

User Management

Why add more users?

- Because you need to provide different levels of User Privilege to different personnel.
- Supports Local or AD-LDAP Authentication



LAB: Using the Web UI

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

44

The LiveNX Client is… Your Engineering Console

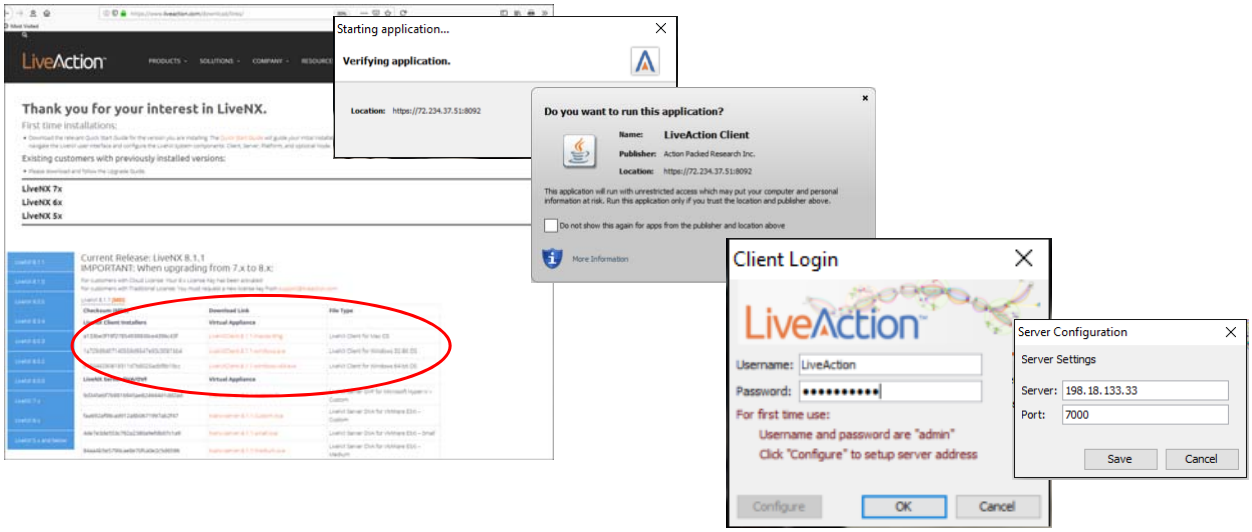
- A Java client application… REQUIRES Java JRE 1.8 or greater.
  - Runs on a standard Windows 32/64-bit PC with Webstart for Windows.
  - LiveAction's Mac client runs on OSX .9+.
- View & Configure:
  - Devices
  - Alerts
  - Reports
- The main interface to visualize network topologies & traffic flows.

2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. LiveAction 45

45

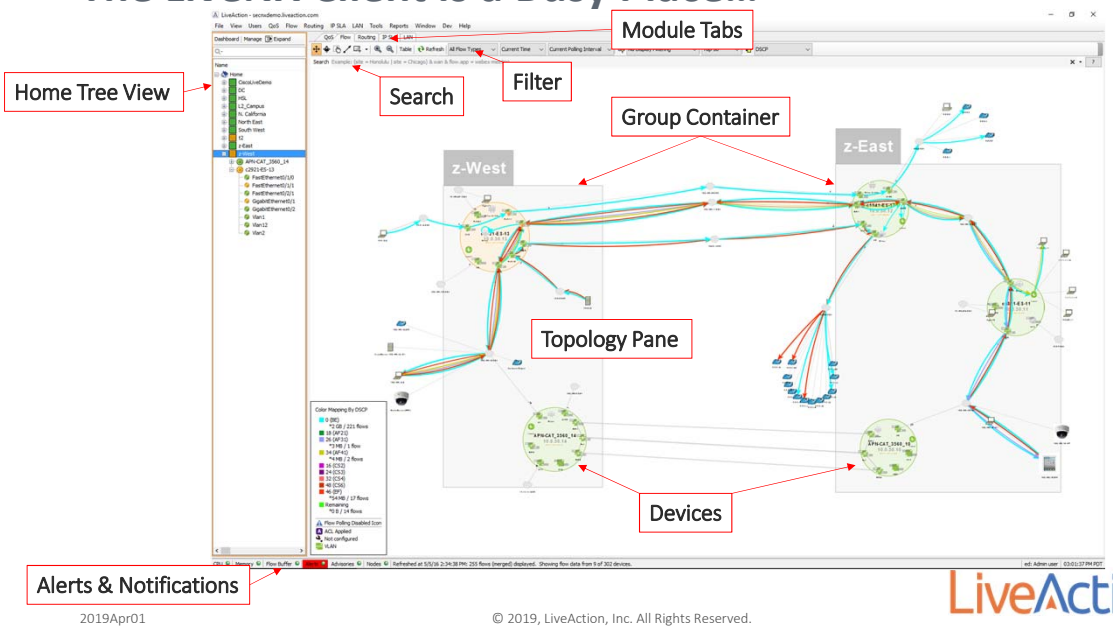
Download & Launch the Client…

https://www.liveaction.com/download/links/



46

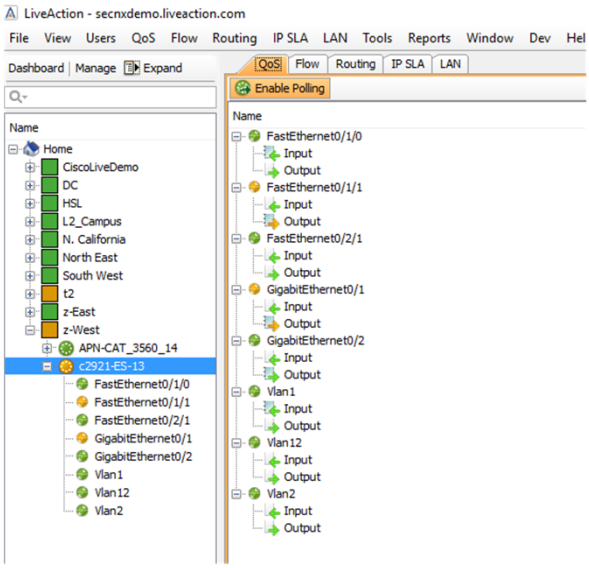
The LiveNX Client is a Busy Place…



47

The Home Tree-view

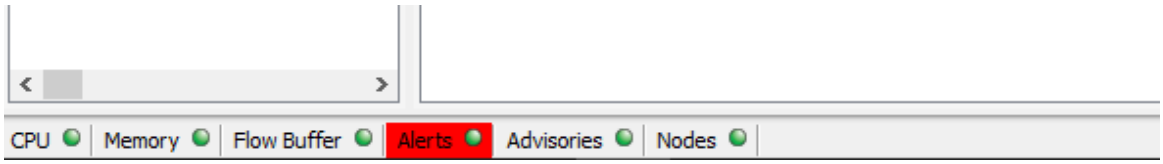
- Groups
  - Devices
    - Interfaces
- Select Home to view all Groups/Devices in the Topology Pane
- Select & Modify Devices & Interfaces
- Right-click Zoom-to…



Immediate Feedback…

Look at the bottom of the screen for information about:

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



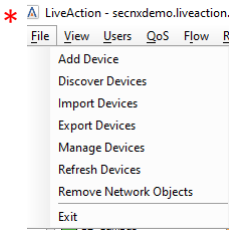
Immediate Results!

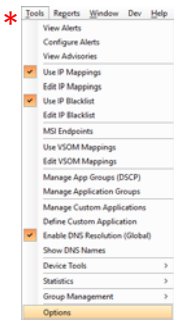
Select any Interface to generate real-time graphs

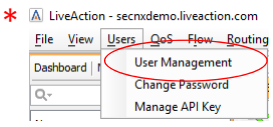
2019Apr01 50

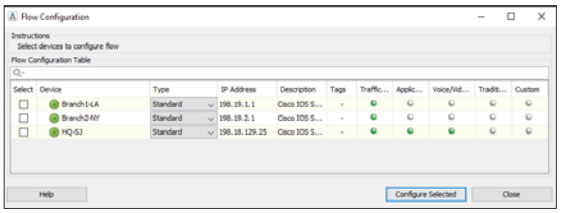
50

Manage, Create, View, Provision









* Configure in the WebUI!

2019Apr01 51

51

LAB: LiveNX Client

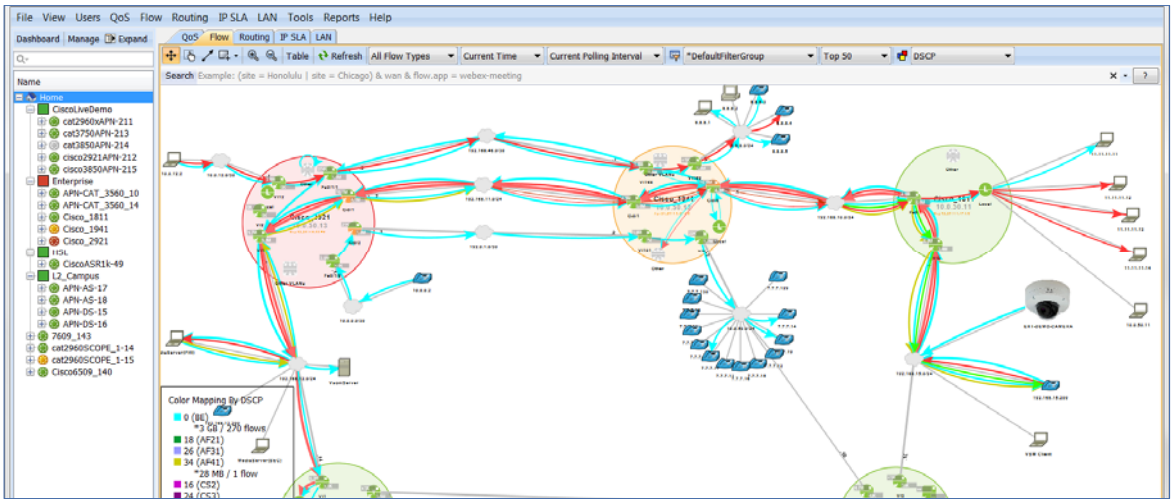
- Launch the LiveNX Desktop Client
  - Connect from YOUR Desktop…
- Explore Topology visualization

52

53

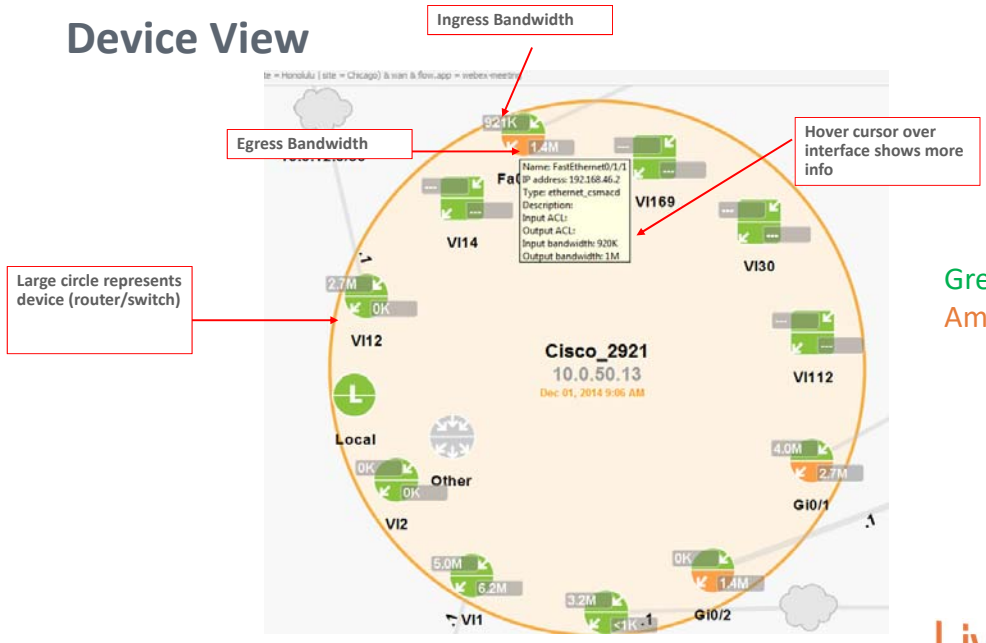
Flow Visualization

End-to-End Application Flows Through the Network



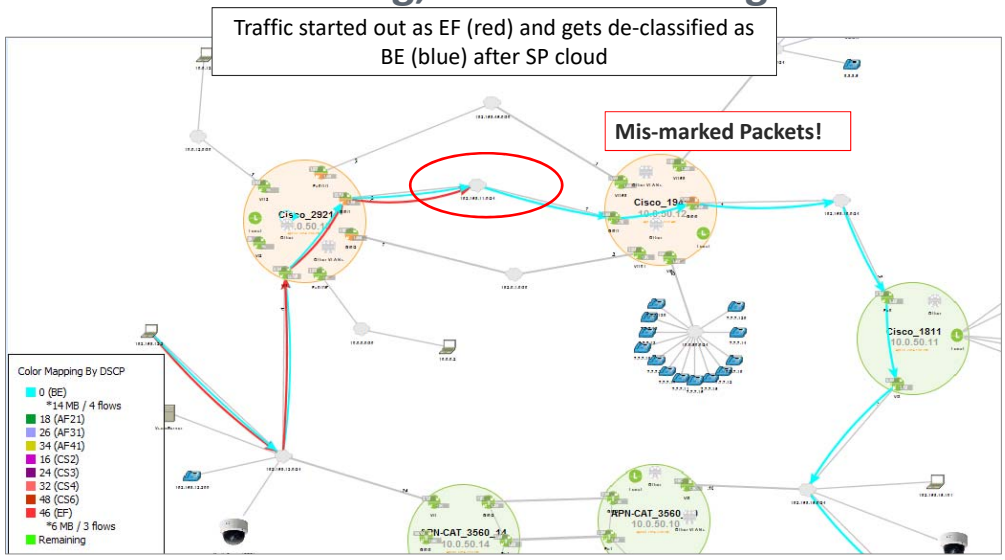
LiveNX discovers and draws topology based on SNMP
LiveNX imposes end-to-end flows on topology

Device View



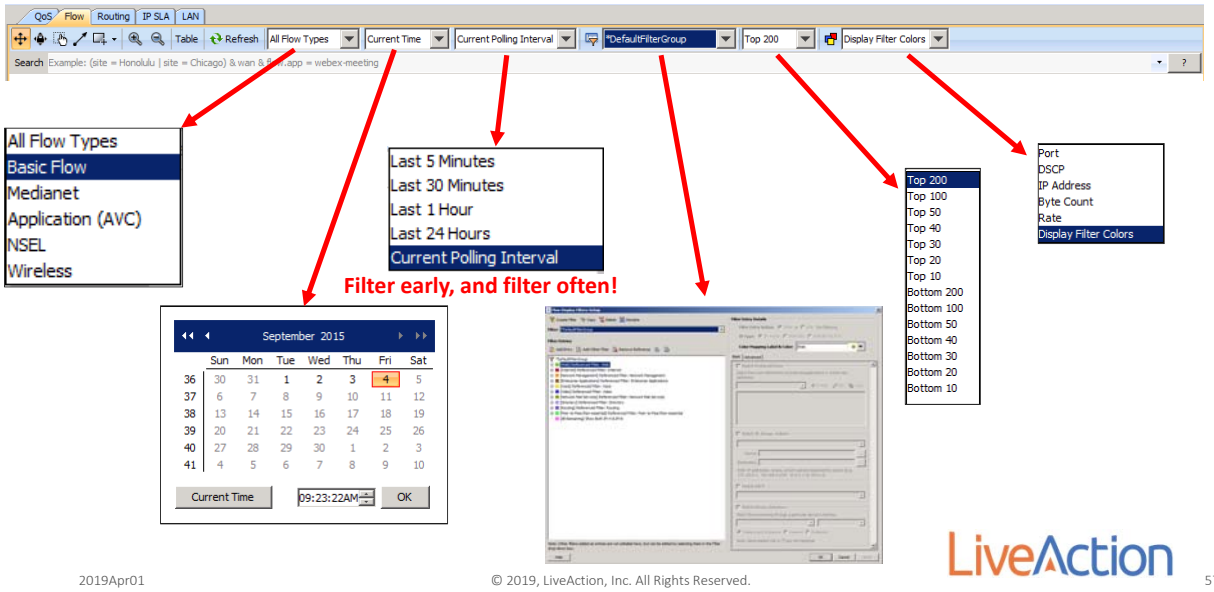
Green: functional
Amber: congested

Flow Troubleshooting, Decision Making



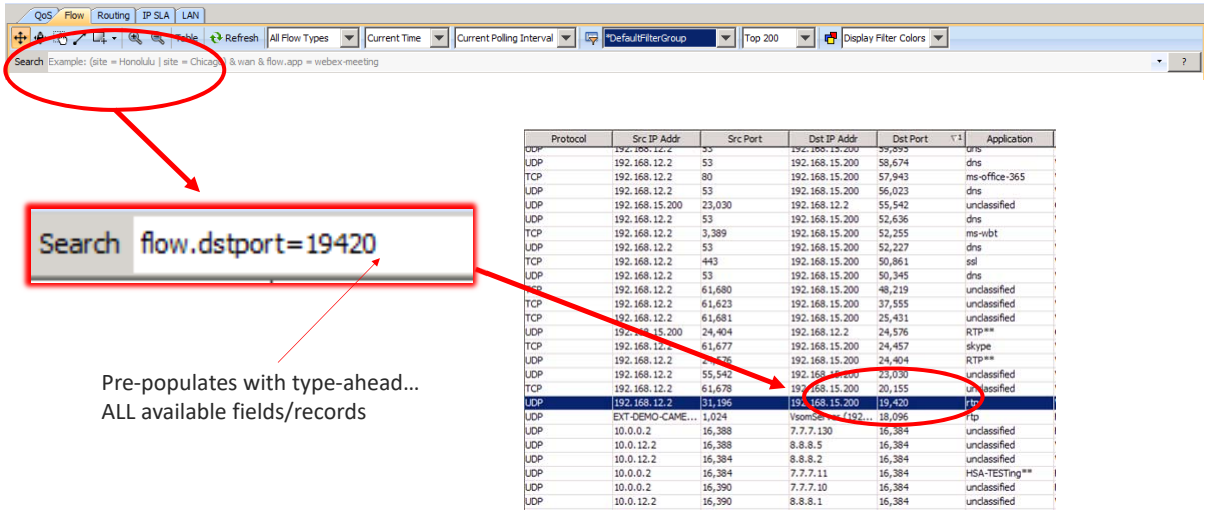
56

Eliminate the Detractors!



57

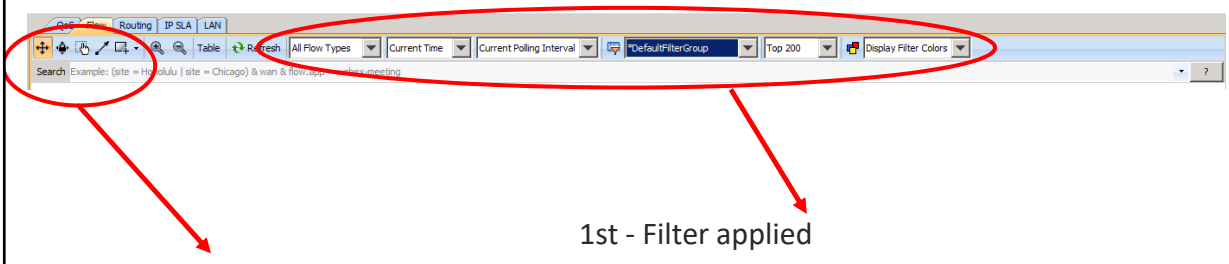
The Search Field



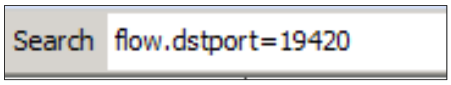
Pre-populates with type-ahead…
ALL available fields/records

58

Search Functions – Order of Operation



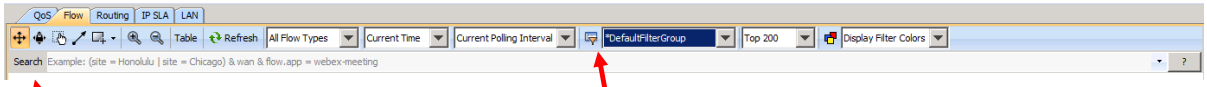
1st - Filter applied



2nd- Search applied to
pulldowns' results

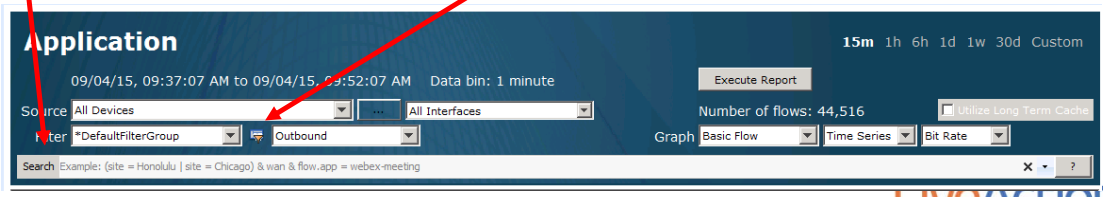
59

Filters & Search Retention



Search strings are cached and are reusable in Topology Pane and Reports

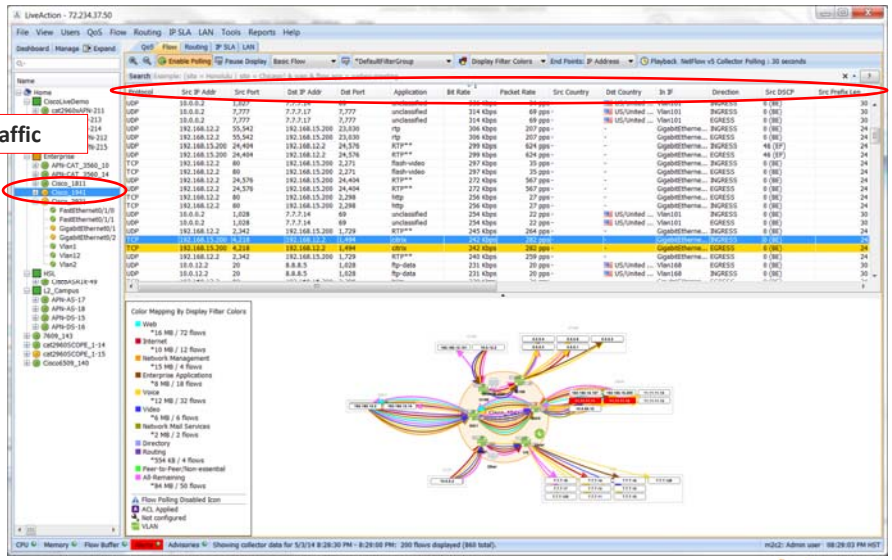
All Filters can be used in both the Topology Pane as well as Reports



60

Flow Visualization

Device Level Traffic

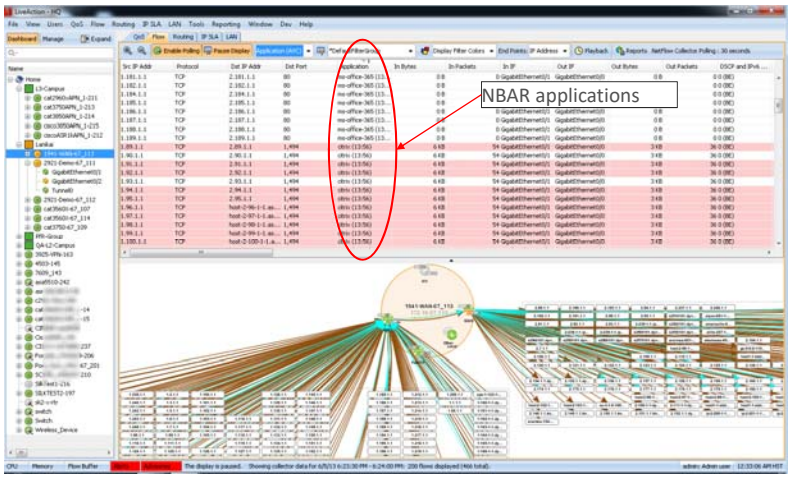


61

AVC Flow Visualization

Application Performance

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

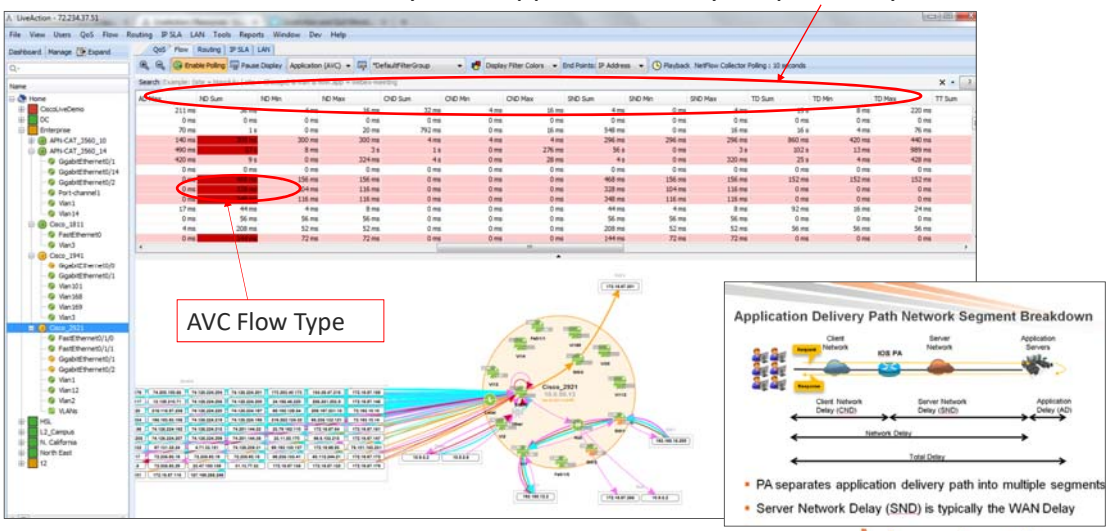


LiveAction

62

Flow Visualization

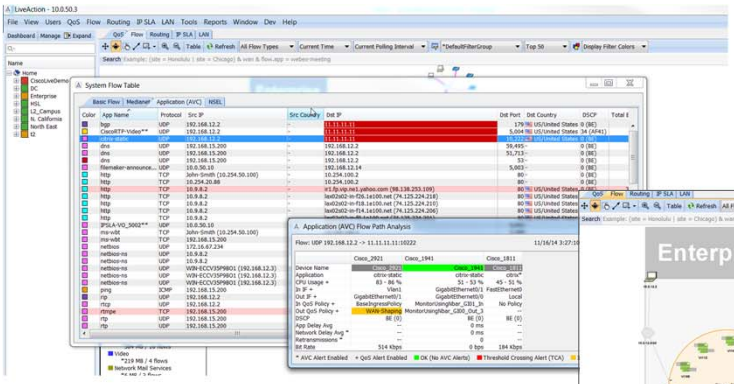
Network Delays and Application Delays Reported by AVC flows

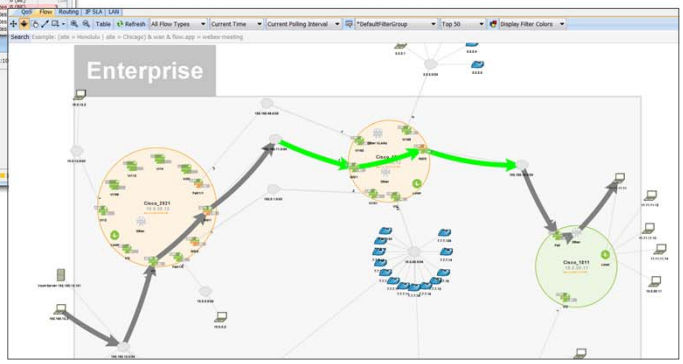


LiveAction

63

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

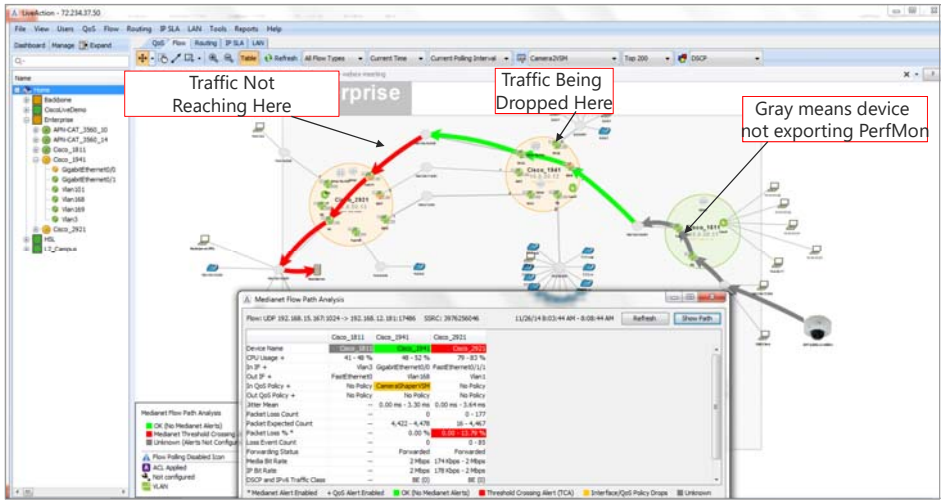
LiveAction

2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 64

64

Medianet Flow Path Analysis

Pinpoint Root Cause



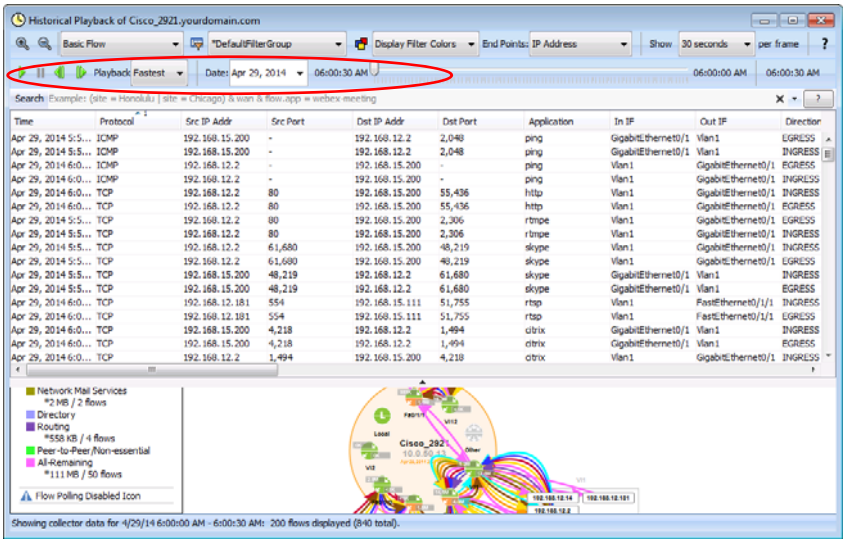
LiveAction

2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 65

65

Flow Visualization Over Time…

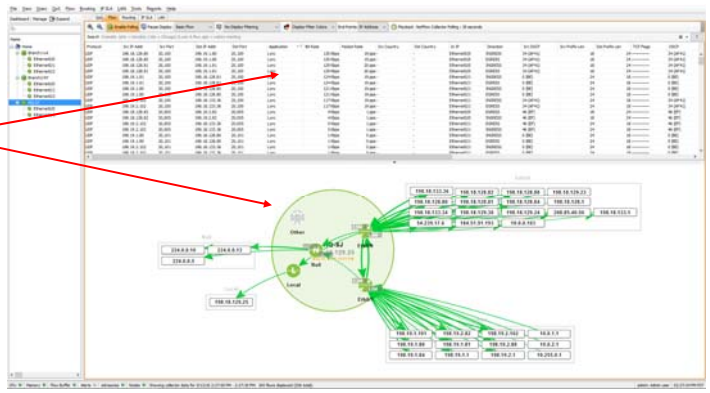
Flow Playback / DVR

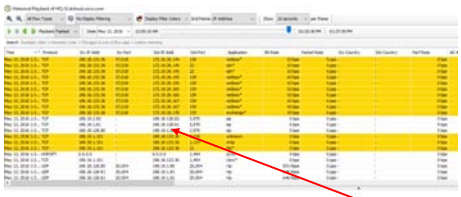


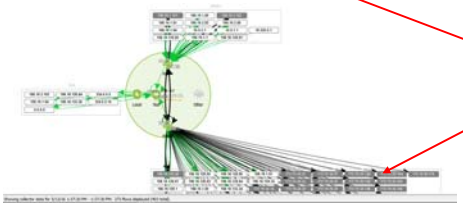
66

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?

67

LAB: Working with Flows

- Identify Flows
- Troubleshoot Performance issues

2019Apr01 68

68

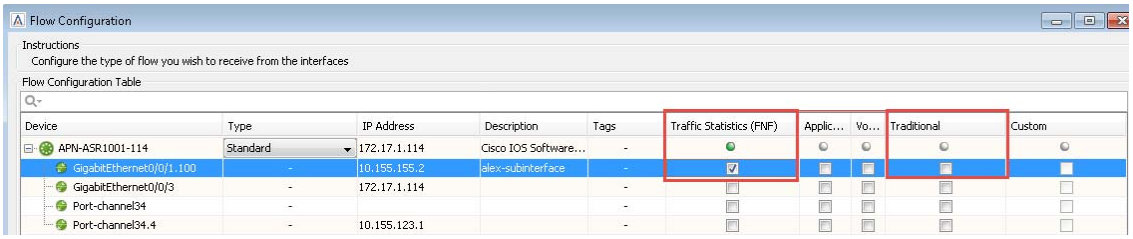
69

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!

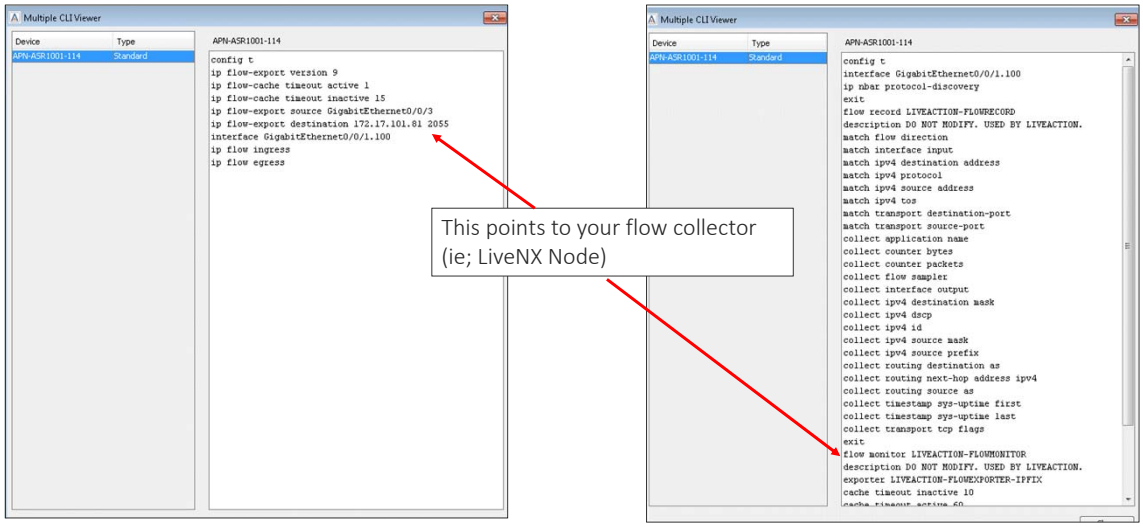
Configure NetFlow Monitoring (LiveNX Console)

- 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

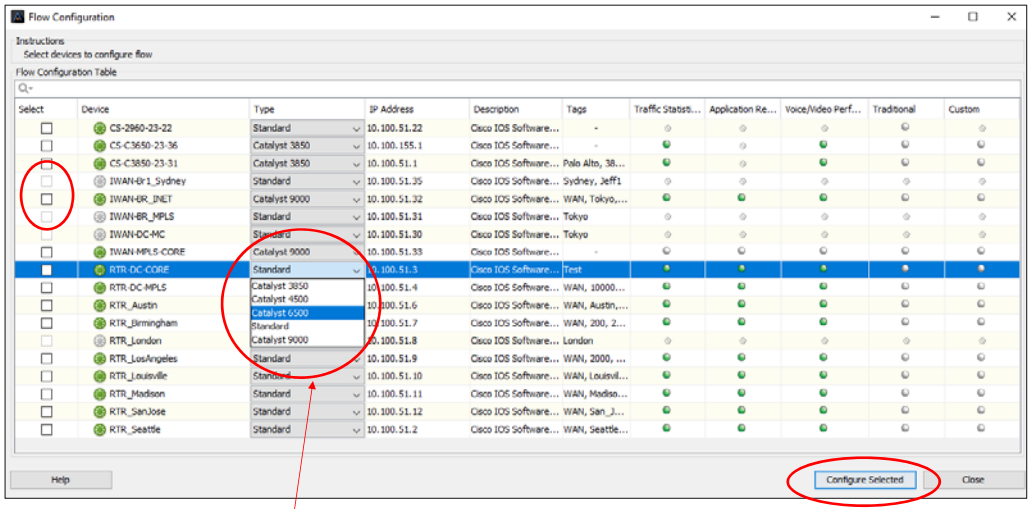
Traditional v. Flexible Netflow - Preview CLI



Cisco's Best-Practices Templates

72

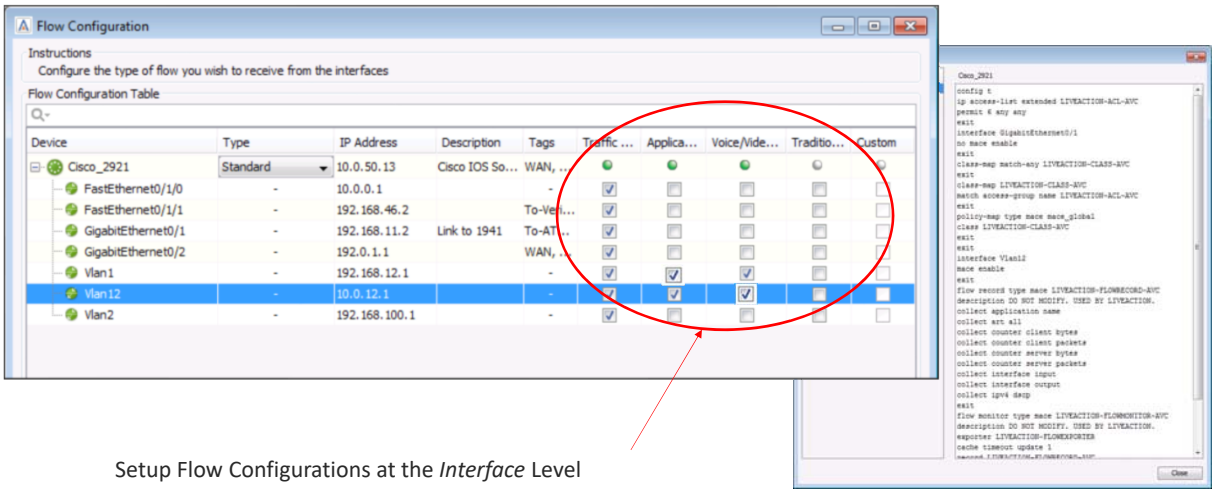
Enable Flow Collection Within LiveNX Console



Easily Setup Flow Configurations at the *Device* Level

73

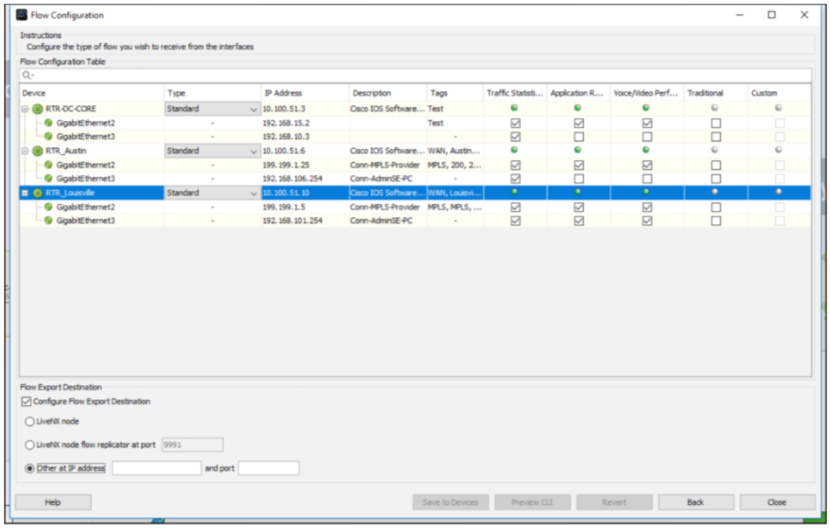
Enable Flow Collection on Interfaces



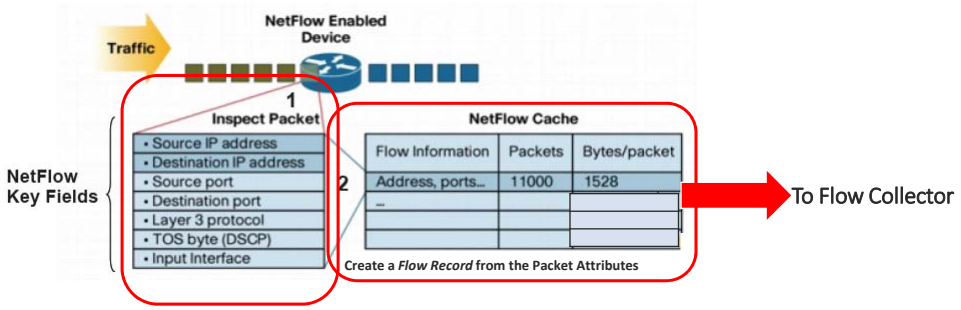
Setup Flow Configurations at the *Interface* Level

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…)



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**

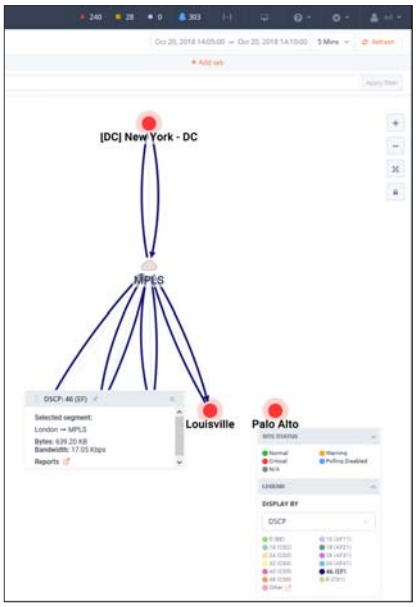
LiveAction

Netflow

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

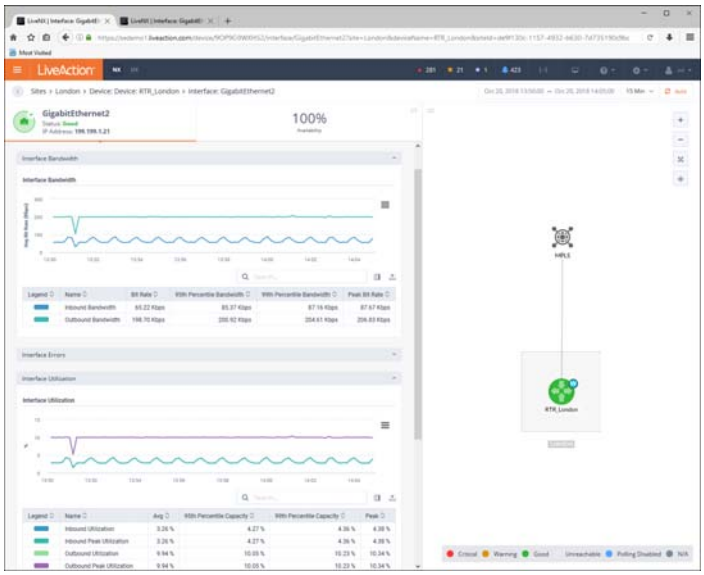
- Traffic source and destination
- Class of service
- Protocol
- Ports
- etc…

  per device.



LiveAction

Netflow Interface View

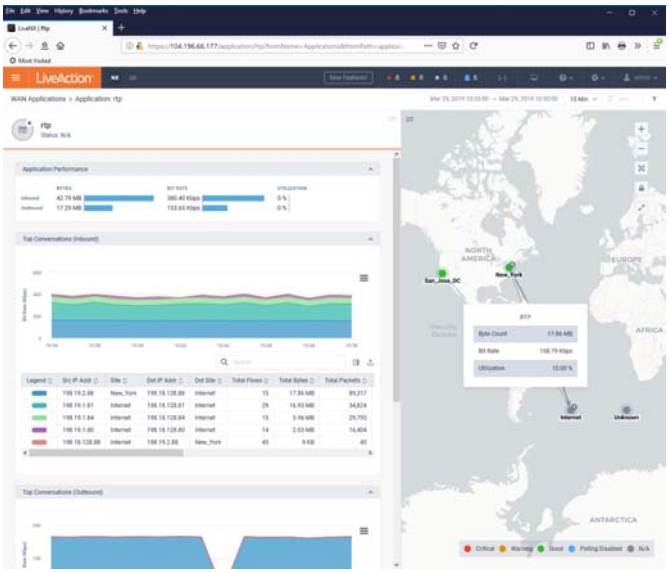


View quantity & type of traffic traversing a specific interface

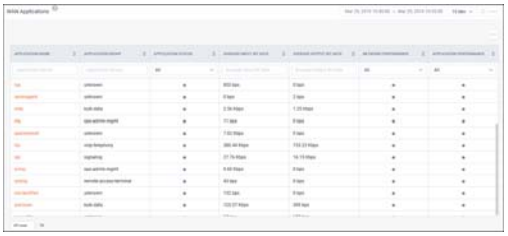
LiveAction

78

Application Flow View



End-to-end quantity of traffic for selected applications



LiveAction

79

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
  - PfR (Performance Routing Threshold Crossing Alerts)
  - "Unknown" (SFLOW, JFLOW, almost any flow technology using v5, v9, or IPFIX Export protocol)

80

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

81

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

82

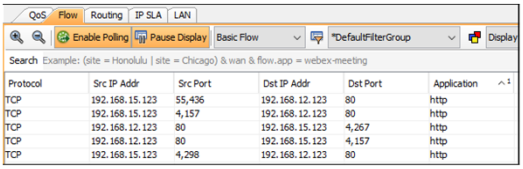
Network Based Application Recognition (NBAR2)

- 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

83

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

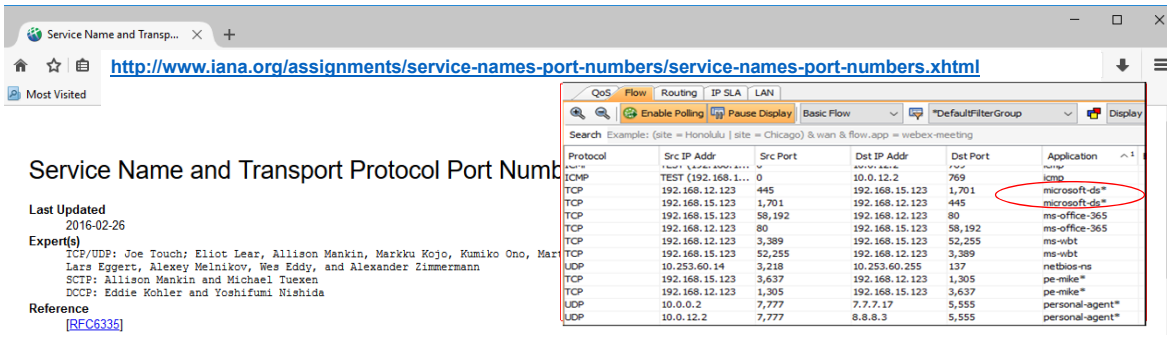


- LiveNX uses NBAR2 in Flow records for detailed application information
- You can use NBAR2 definitions for granular QoS configuration
- If your application is not known, you can set a NBAR application on the CLI
- If NBAR2 is supported, LiveNX will push the configuration to the devices during Netflow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

84

IANA.Org

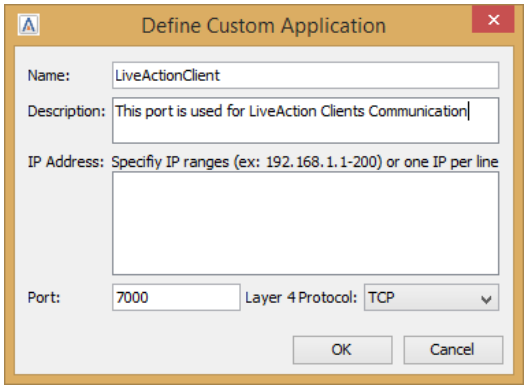
- If LiveNX is *not* able to get the NBAR2 application definitions from the device:
  - Uses the IANA (Internet Assigned Numbers Authority) definitions for Applications.



85

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



86

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.

87

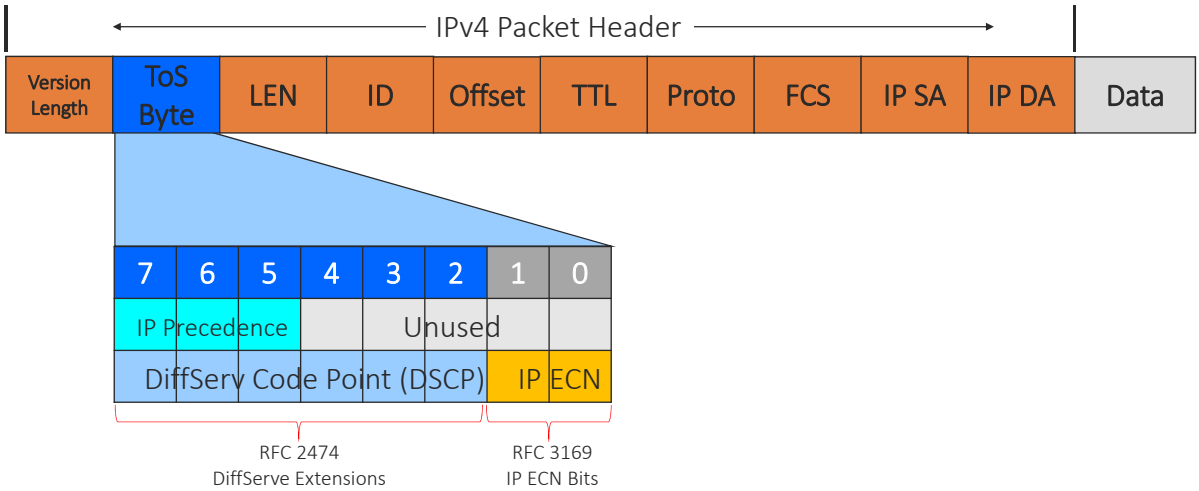
Differentiated Service Control Point (DSCP)

- 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		IETF
	PHB	DSCP	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-Troughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

88

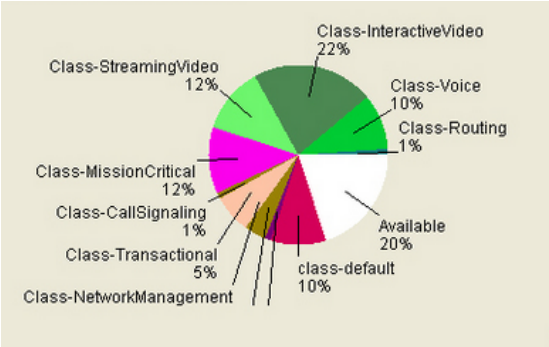
Packets & DSCP Markings



89

QoS Techniques

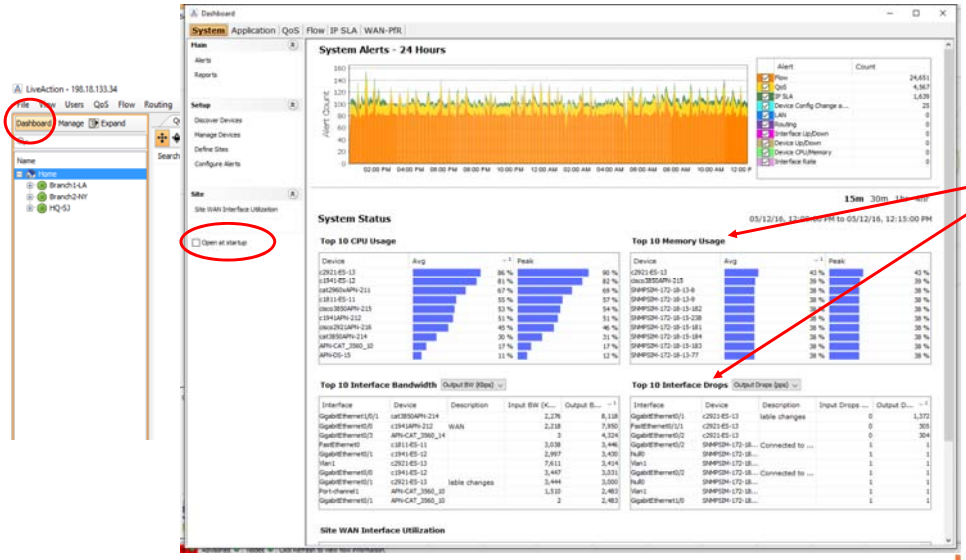
- After setting DSCP Markings in your network you can easily conform the traffic to your network needs with:
  - Queuing
  - Shaping
  - Policing



LAB: Marking, Shaping, Policing

92

System Dashboard At-A-Glance Flow Traffic Pattern



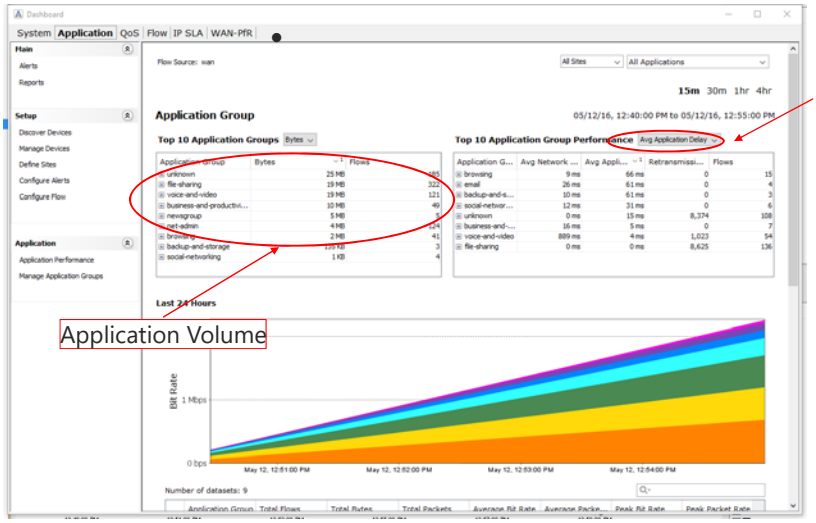
At-a-Click Report widget!

2019Apr01
© 2019, LiveAction, Inc. All Rights Reserved.
LiveAction
93

93

Application Dashboard

Instant Application
Performance
Visibility
Driven by AVC Flows

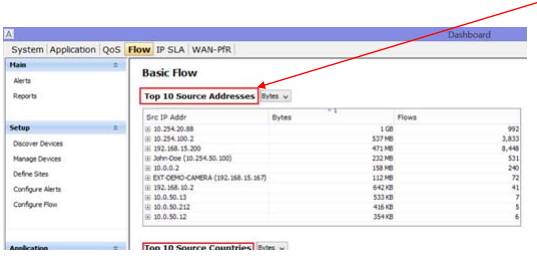


Network vs.
Application
Delay

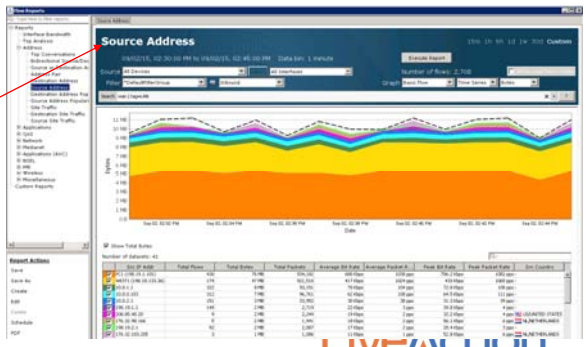
94

Report Drill-downs

The data widgets in the Flow
and Application dashboard
drill down to Reports

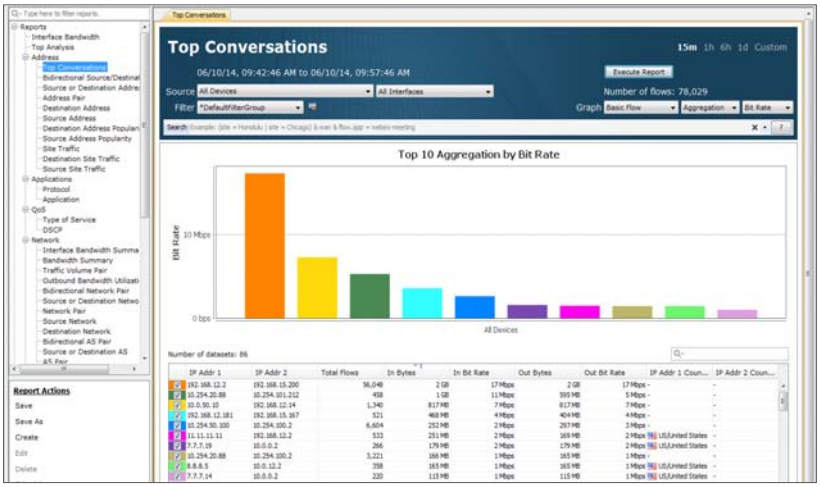


These reports are
automatically saved to the
long term flow store based on
the flow source tags



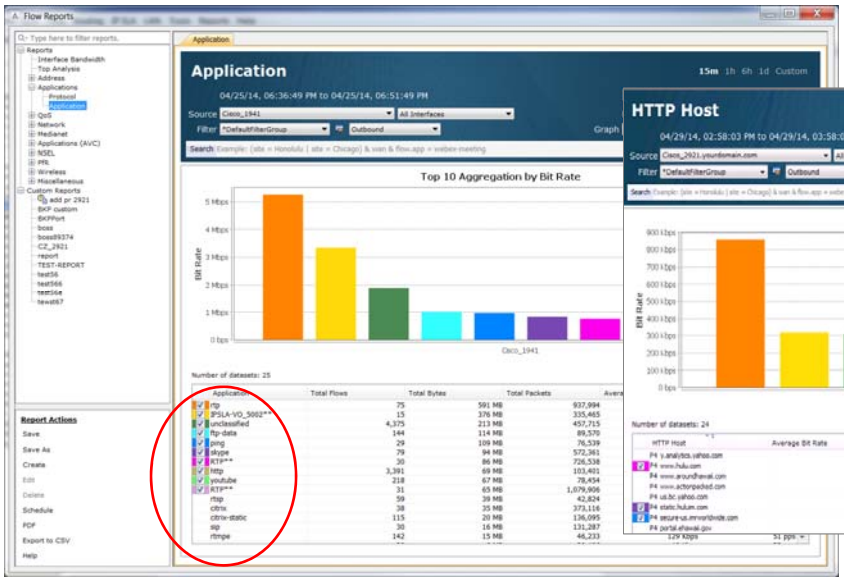
95

Flow - Top Conversations (Top Talkers)



96

Top Applications & Most Visited Websites



Top 10 Reports

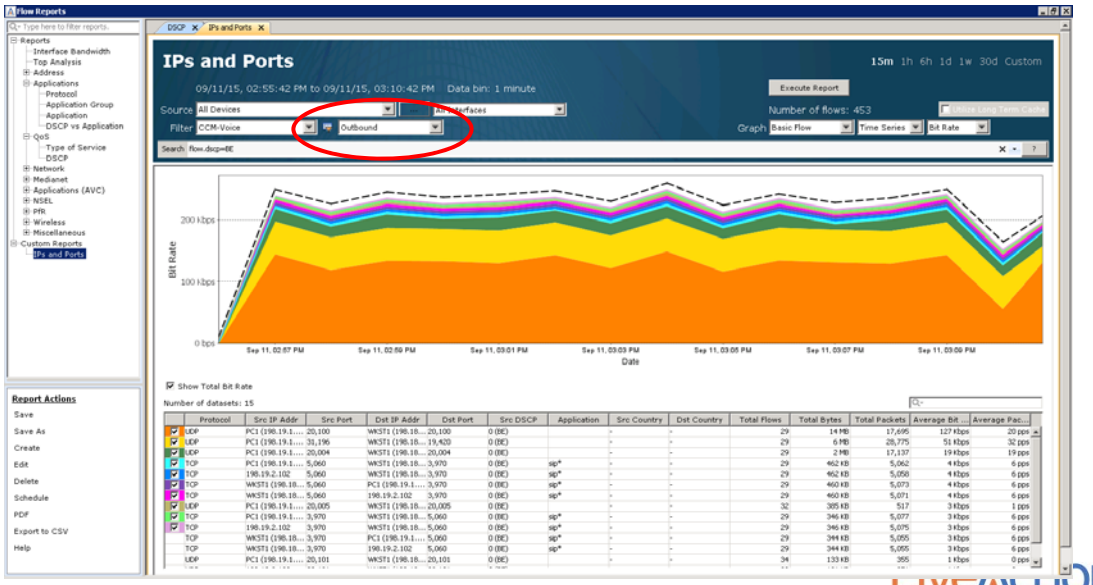
97

Flow Reports – Raw Data

Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	Direction	Src DSCP	Bit Rate
Sep 4, 2015 10:1...	UDP	192.168.15.200	58,674	192.168.12.2	53	dns	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	464 bps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,171	192.168.12.2	80	http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	9 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,190	192.168.12.2	80	http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	8 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,172	192.168.12.2	80	http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	8 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,208	192.168.12.2	443	secure-http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	22 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,234	192.168.12.2	80	http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	320 bps
Sep 4, 2015 10:1...	TCP	192.168.15.200	2,220	192.168.12.2	443	secure-http*	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	21 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,278	192.168.12.2	80	http	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	789 bps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,288	192.168.12.2	80	http	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	1 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,289	192.168.12.2	80	http	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	1 Kbps
Sep 4, 2015 10:1...	UDP	192.168.12.2	31,196	192.168.15.200	19,420	rtp	Vlan1	GigabitEthernet0/1	EGRESS	0 (BE)	79 Kbps
Sep 4, 2015 10:1...	UDP	192.168.12.2	13,958	11.11.11.12	13,958	VoIP13958	Vlan1	GigabitEthernet0/1	EGRESS	46 (EF)	73 Kbps
Sep 4, 2015 10:1...	UDP	192.168.12.2	13,958	11.11.11.13	13,958	VoIP13958	Vlan1	GigabitEthernet0/1	EGRESS	46 (EF)	73 Kbps
Sep 4, 2015 10:1...	UDP	192.168.12.2	13,958	11.11.11.14	13,958	VoIP13958	Vlan1	GigabitEthernet0/1	EGRESS	46 (EF)	73 Kbps
Sep 4, 2015 10:1...	UDP	10.0.0.2	7,648	7.7.7.18	7,648	CriticalApp**	FastEthernet0/1/0	GigabitEthernet0/2	EGRESS	46 (EF)	377 Kbps
Sep 4, 2015 10:1...	ICMP	192.168.15.200	0	192.168.12.2	2,048	ping	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	511 Kbps
Sep 4, 2015 10:1...	UDP	10.0.0.2	16,386	7.7.7.129	16,384	unclassified	FastEthernet0/1/0	GigabitEthernet0/2	EGRESS	46 (EF)	60 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,085	192.168.12.2	8,797	unclassified	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	24 Kbps
Sep 4, 2015 10:1...	TCP	192.168.12.2	80	192.168.15.200	4,287	http	Vlan1	GigabitEthernet0/1	EGRESS	0 (BE)	50 Kbps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,299	192.168.12.2	80	Maxis_Server**	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	2 Kbps
Sep 4, 2015 10:1...	UDP	192.168.12.2	53	192.168.15.200	61,148	dns	Vlan1	GigabitEthernet0/1	EGRESS	16 (CS2)	4 Kbps
Sep 4, 2015 10:1...	TCP	192.168.12.2	15,255	192.168.15.200	4,111	unclassified	Vlan1	GigabitEthernet0/1	EGRESS	0 (BE)	320 bps
Sep 4, 2015 10:1...	TCP	192.168.15.200	4,268	192.168.12.2	80	http	GigabitEthernet0/1	Vlan1	INGRESS	0 (BE)	1 Kbps
Sep 4, 2015 10:1...	UDP	10.253.60.14	3,206	10.253.60.255	137	netbios-ns	GigabitEthernet0/0	GigabitEthernet0/1	EGRESS	0 (BE)	998 bps
Sep 4, 2015 10:1...	TCP	192.168.12.2	80	192.168.15.200	4,273	http	Vlan1	GigabitEthernet0/1	EGRESS	0 (BE)	13 Kbps
Sep 4, 2015 10:1...	UDP	10.0.12.2	1,027	8.8.8.2	1,604	citrix-static	Vlan12	FastEthernet0/1/1	EGRESS	0 (BE)	37 Kbps
Sep 4, 2015 10:1...	UDP	10.0.0.2	1,027	7.7.7.14	69	tftp*	FastEthernet0/1/0	GigabitEthernet0/2	EGRESS	0 (BE)	359 Kbps

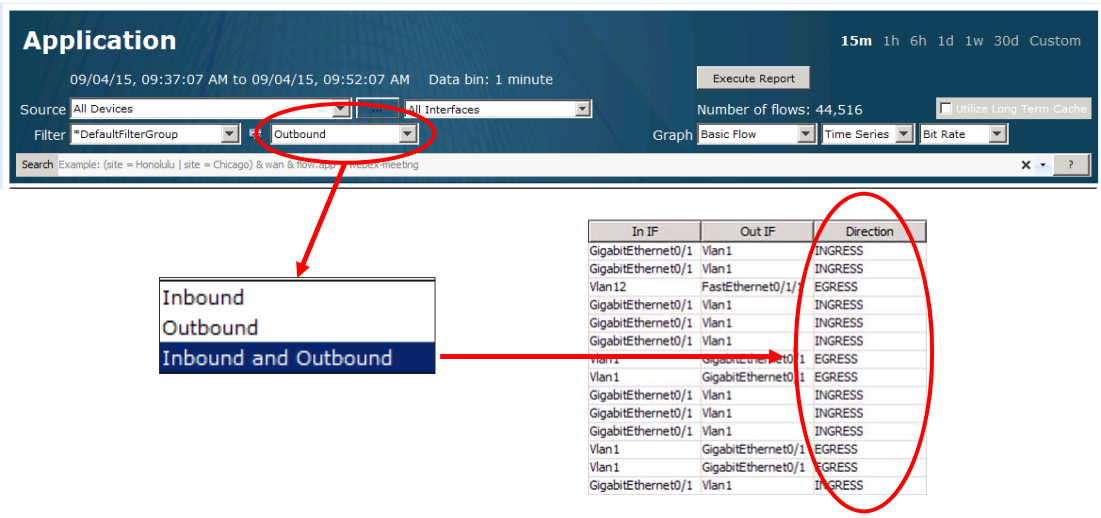
98

Flow Report - Directionality



99

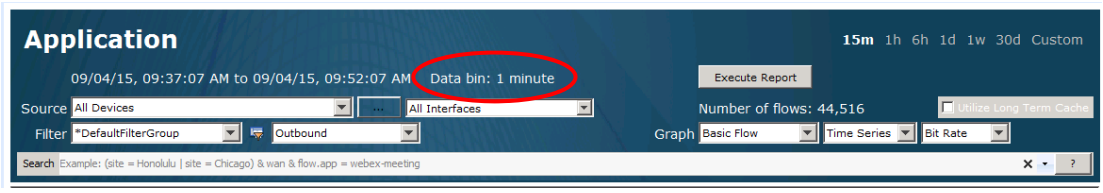
Flow Report - Directionality



100

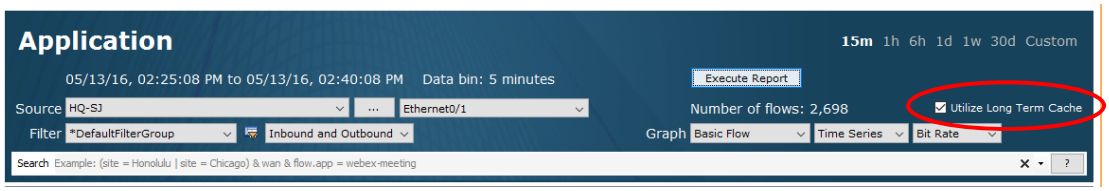
Automatic Granularity - Report Length / Data Bin

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.



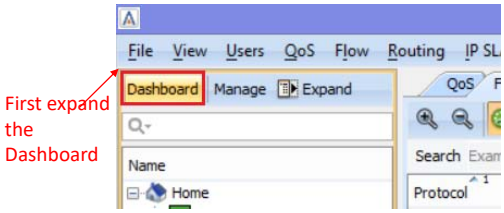
101

Long Term Data Storage (2)

How is data populated?

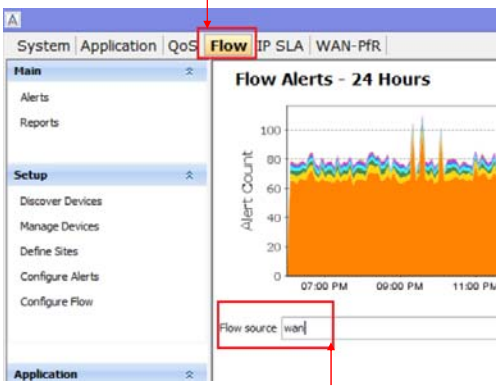
The Dashboard Flow Source alters what devices and interfaces are processed in Long Term Report Processing.

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

102

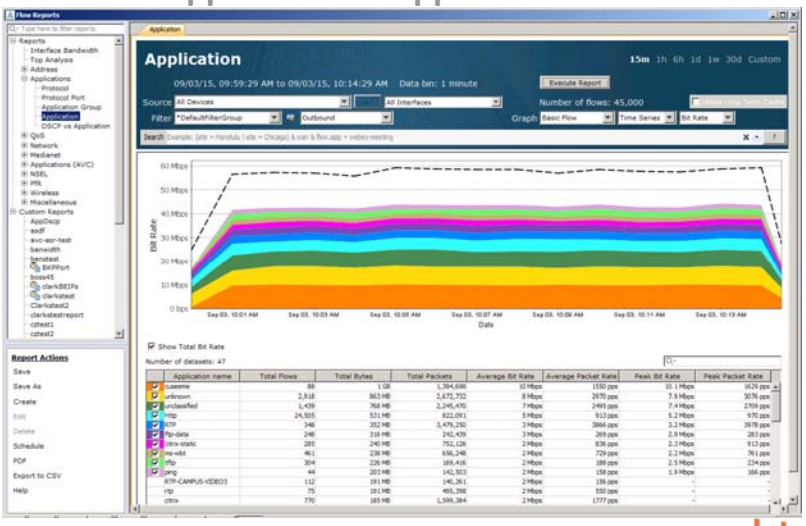
Commonly Used Reports

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

103

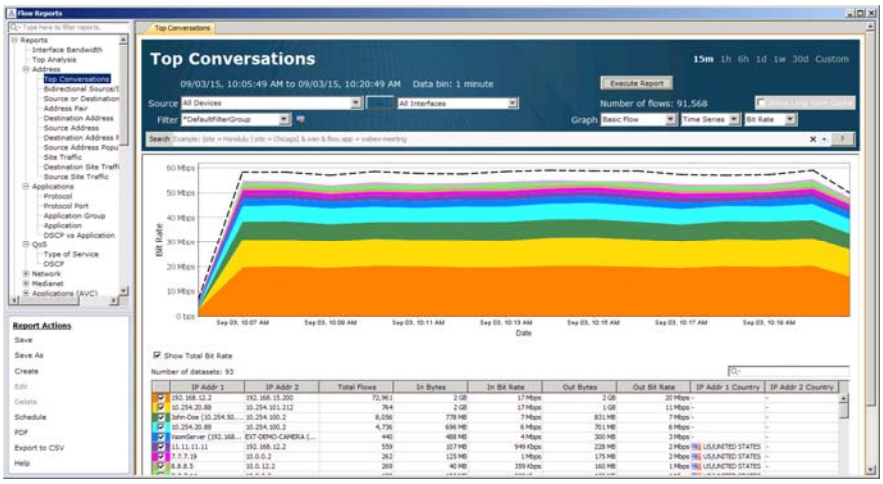
Use Case 1 – Top Applications

Applications > Application



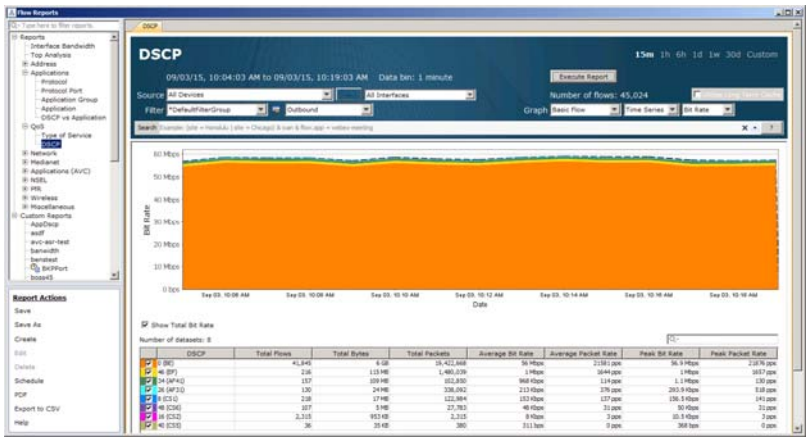
Use Case 2 – Top Talkers

Address > Top Conversations



Use Case 3 – Top DSCP

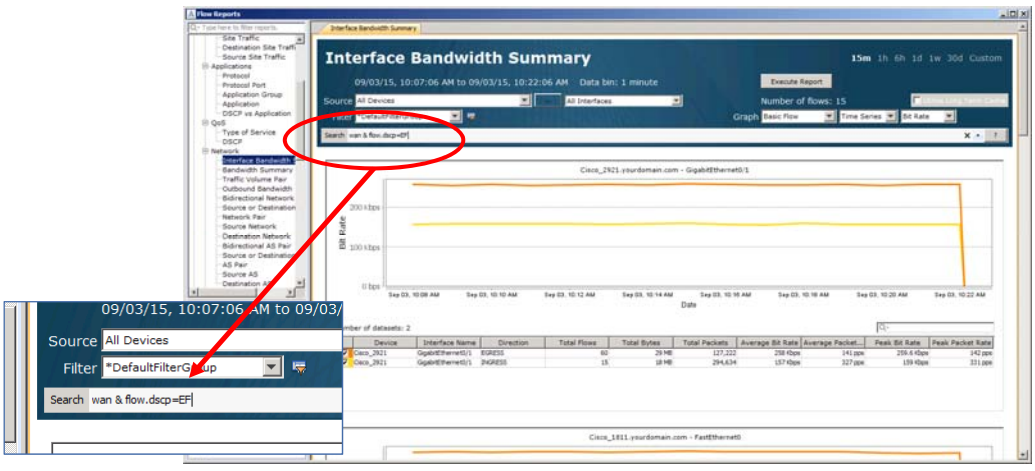
QoS > DSCP



106

Use Case 4 – Top DSCP

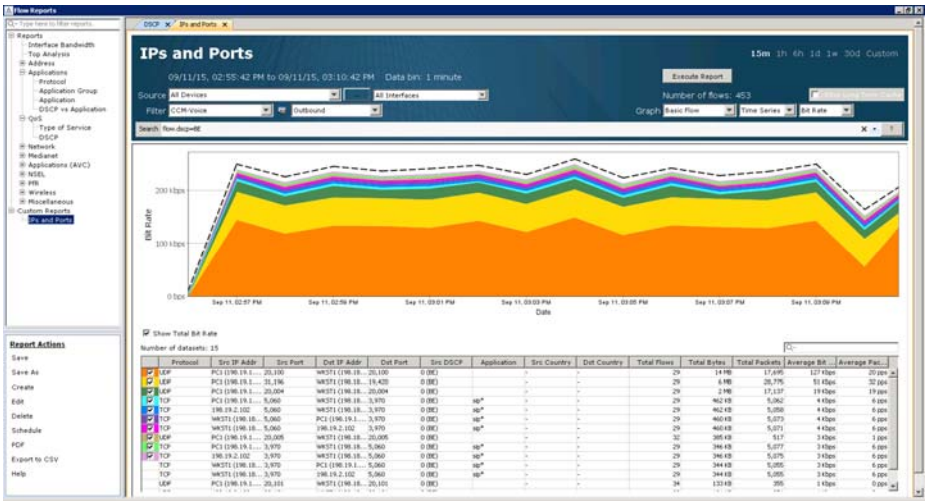
Network > Interface Bandwidth Summary Report



107

Use Case 5 – IPs and Ports

IPs and Ports Report



LAB: Reporting and Alerting

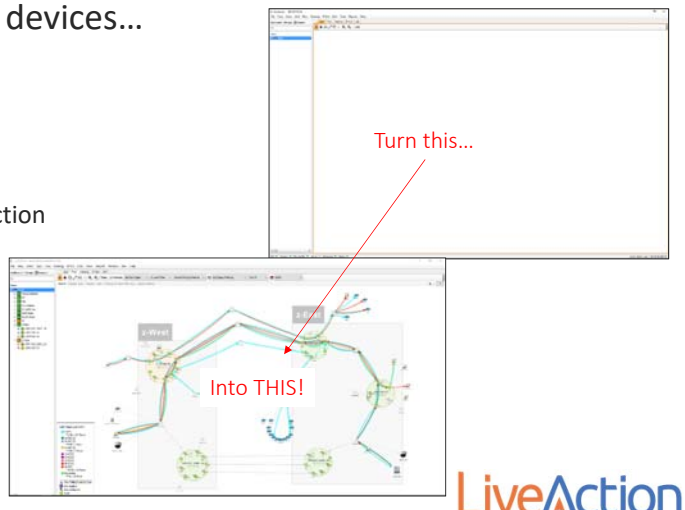
- View & Create Reports
- Configure Alerts

110

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…



2019Apr01

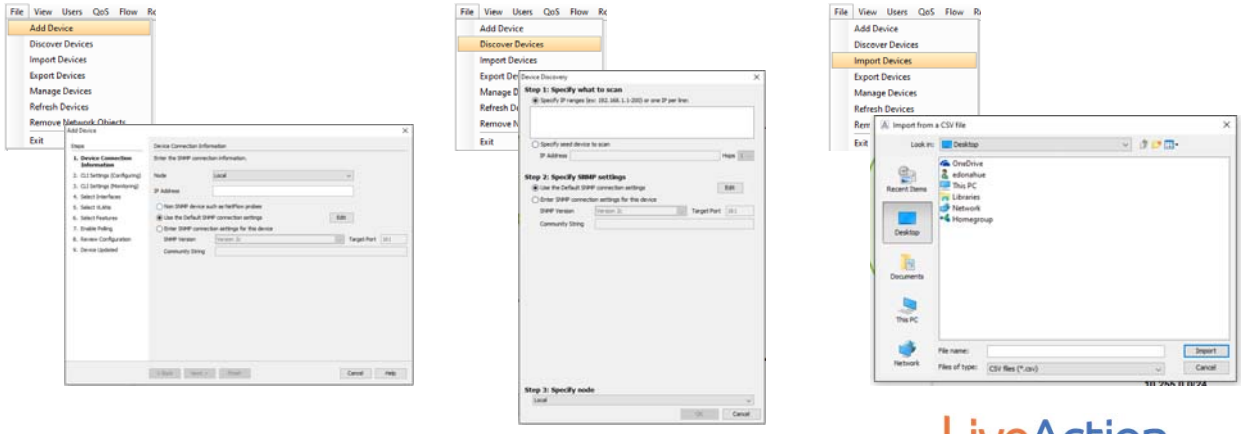
111

LiveAction

111

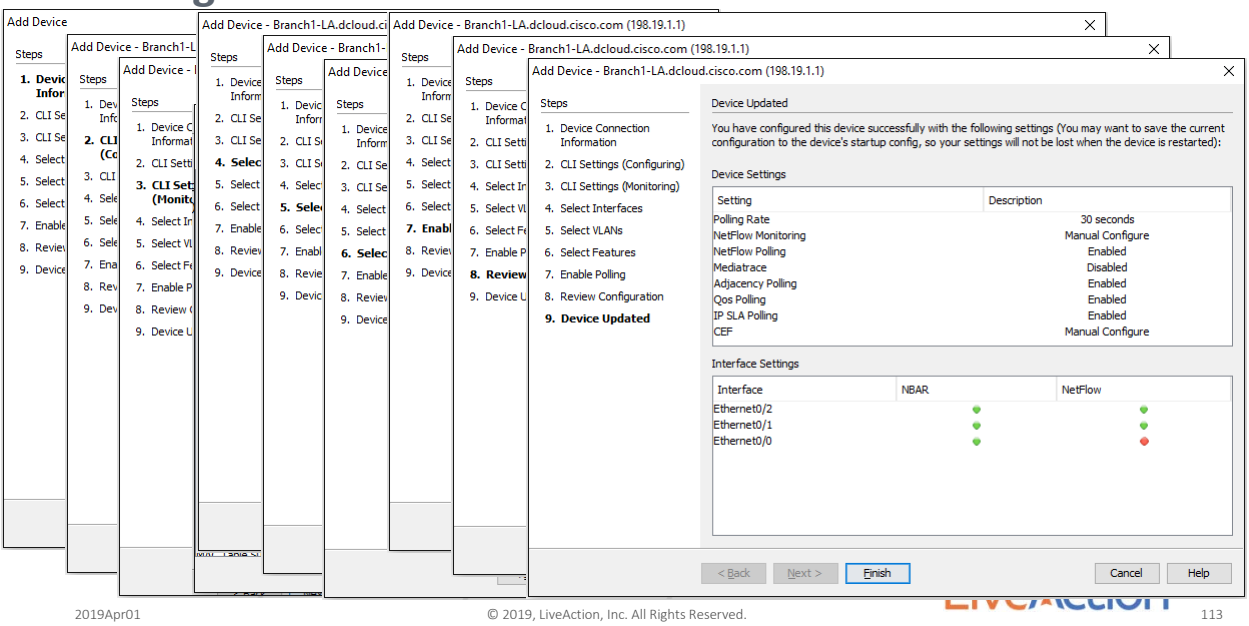
Adding Devices

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



112

Adding Devices



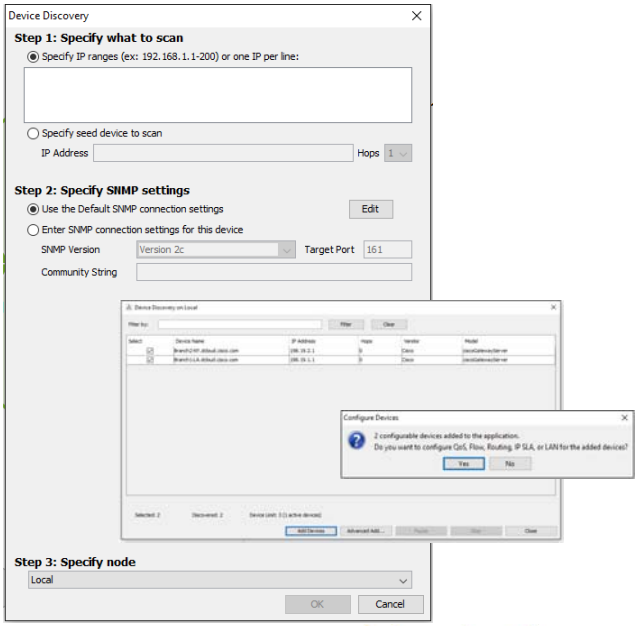
113

Device Discovery

Scan and find connected devices

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

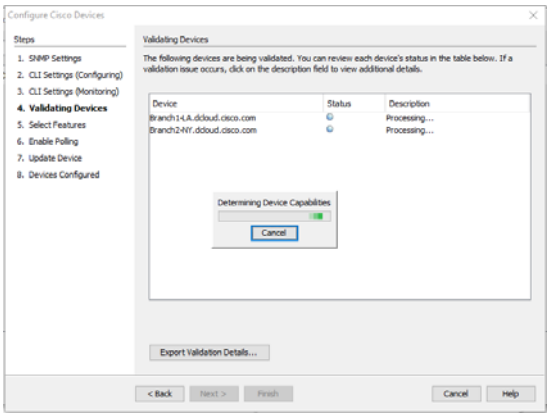
Returns a dialog with suggested devices to add.

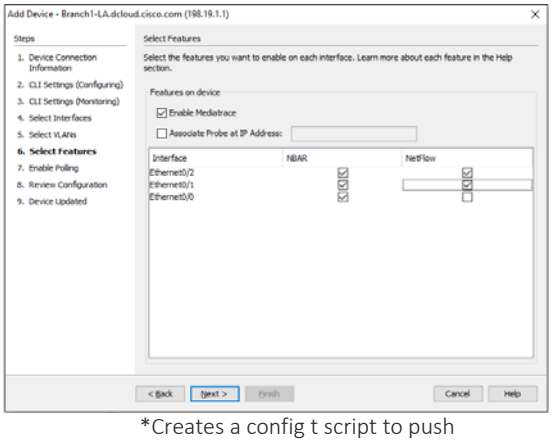


114

Device Discovery… Configure Cisco Devices

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

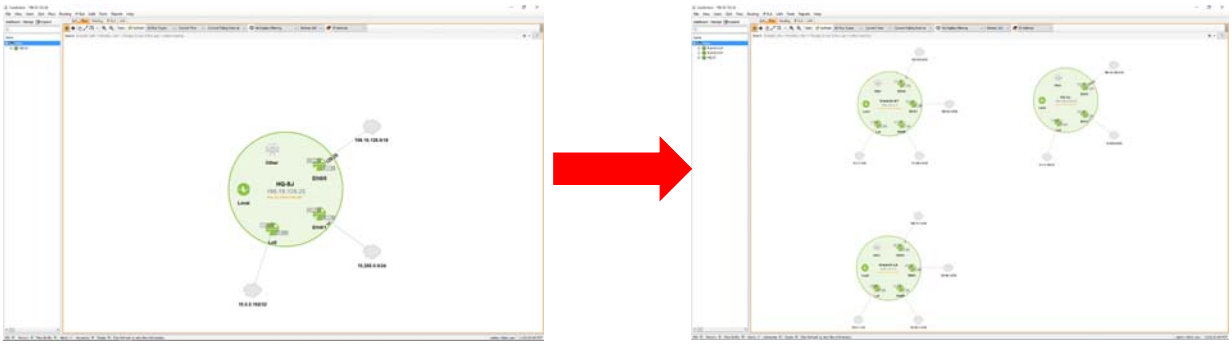




*Creates a config t script to push

115

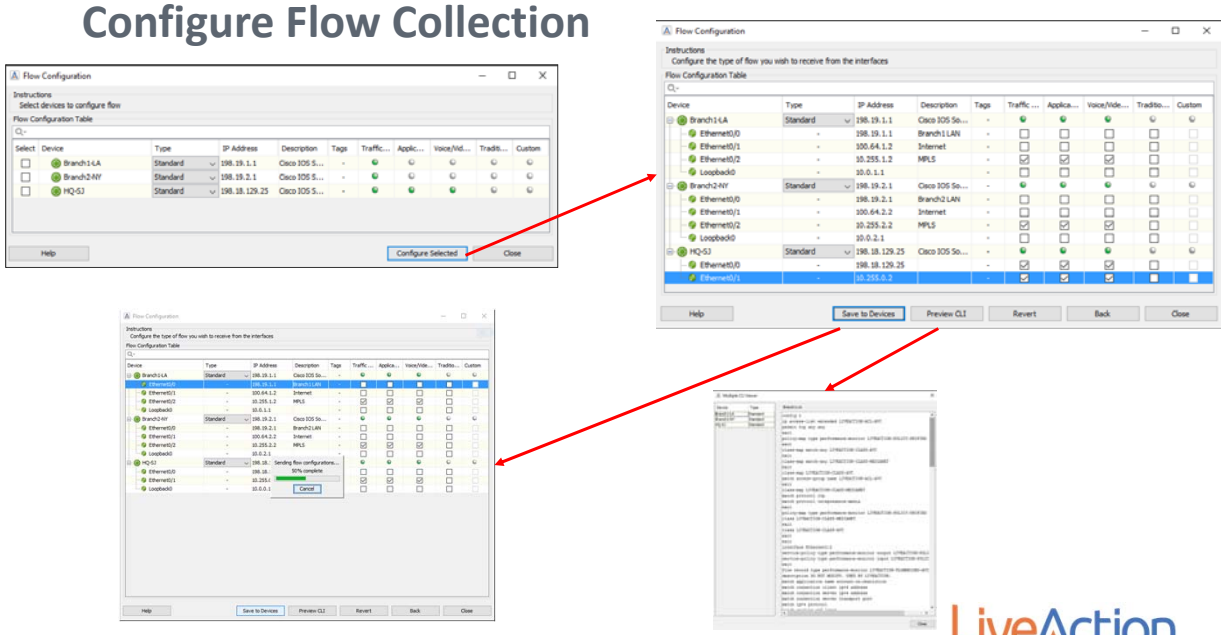
Working Topology… Almost



Devices installed… But no Flows?

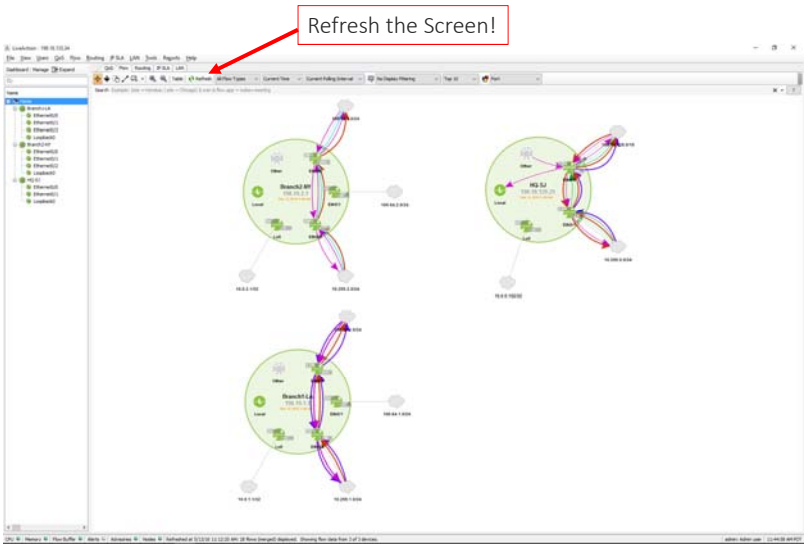
116

Configure Flow Collection



117

Vew Traffic Flows!

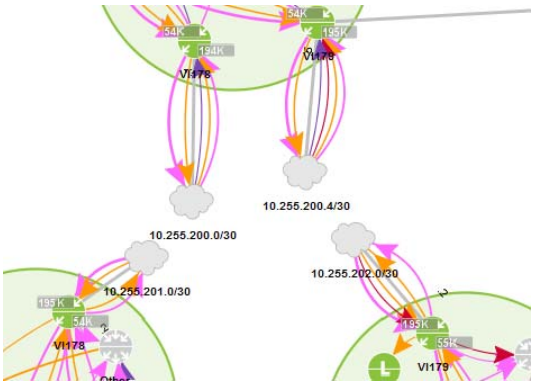


Pretty colors and lines/arrows… but still not connected!

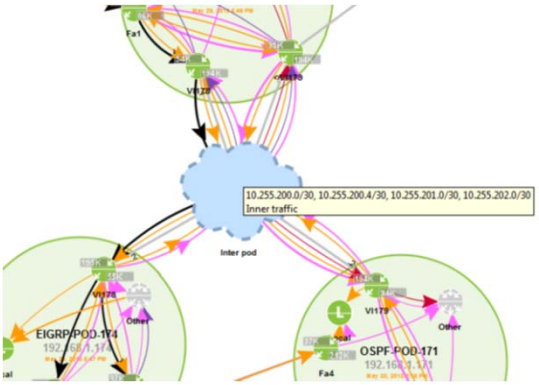
LiveAction

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



LiveAction

LAB: 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
- Delete unused interfaces
- Merge Clouds…

LiveAction

2019Apr01 120

120

Topology Definition

LiveAction™

2019Apr01

121

Topology Basics - Grouping

Devices appear on the topology within their shaded groups.

Devices appear collapsed in their groups on the device tree.

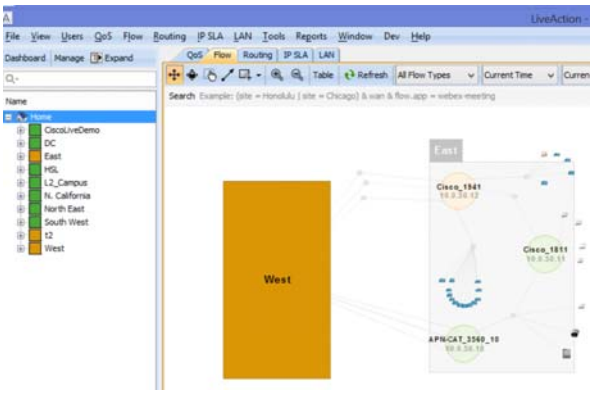
Grouping makes device management easier!

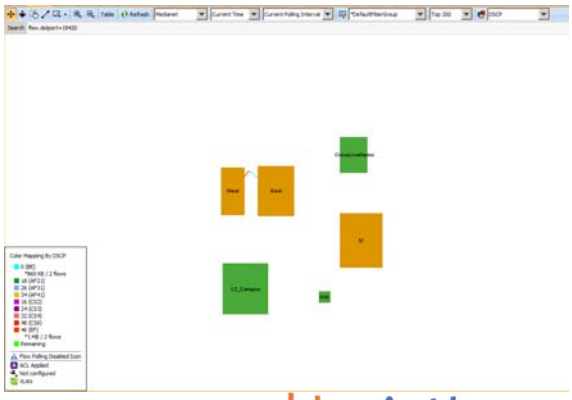
LiveAction

Topology Basics

Devices reporting issues will change colors to prompt for investigation.

Quickly identify many problem sites visually



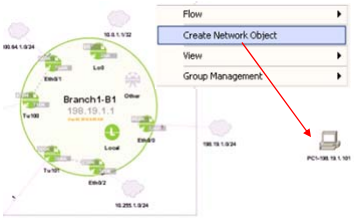


LiveAction

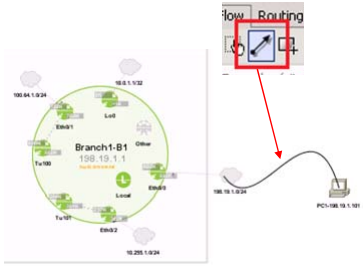
Topology Basics – Add Network Object

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

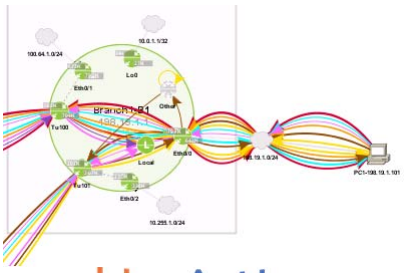
Step 1
Right-Click and create Network Object



Step 2
Draw connection to cloud



Step 3
Flows now connect

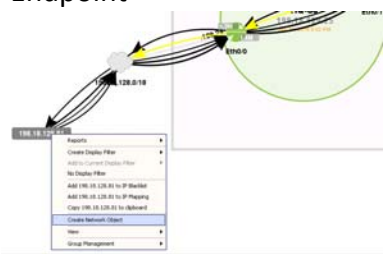


124

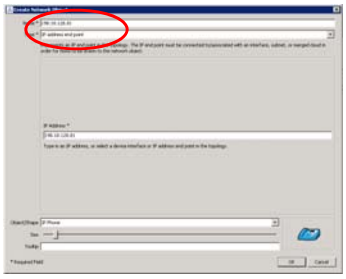
Topology Basics – Add Network Object

Do it the EASY way!

Step 1
Right-Click on Flow Endpoint



Step 2
Select the Object Shape

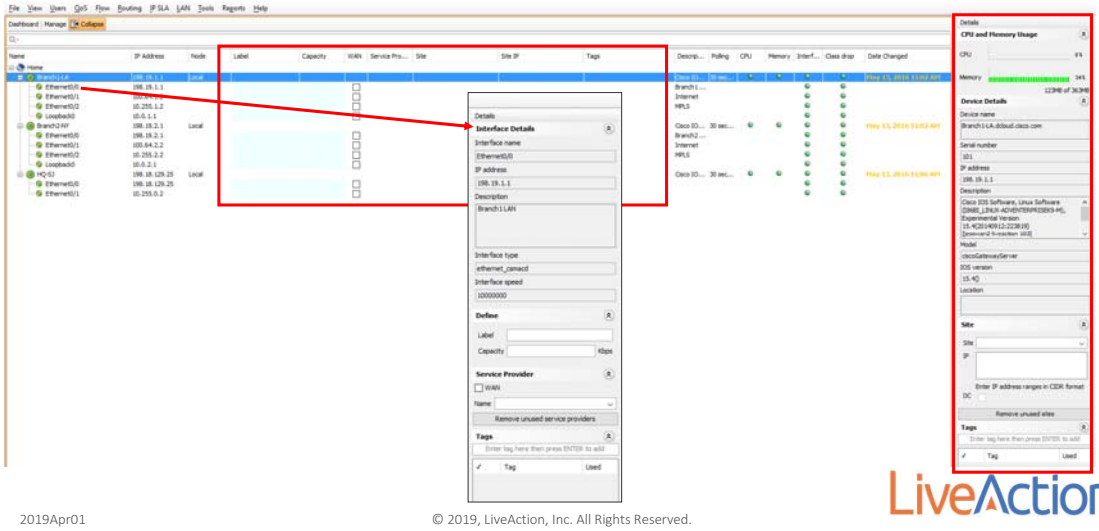


Step 3
Flows now connect

125

Device *Semantics*

Set Interface Labels, Destination, Speeds, Capacities…

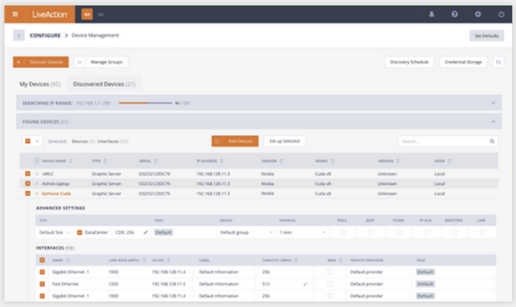


126

Auto-Semantic Discovery via WebUI

RAPID DEVICE DISCOVERY THROUGH AUTO-SEMANTIC DISCOVERY FOR FAST DEPLOYMENT TIMES

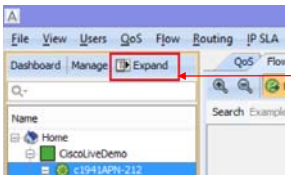
The legacy way of inputting device name, IP address, interface type, etc. into LiveNX manually was time consuming and labor intensive. LiveNX 6.2 introduces new Auto-Semantics capabilities that associate devices to sites, link capacity, site IP mapping, service provider, etc. and auto populates LiveNX so you can be up and using the platform faster.



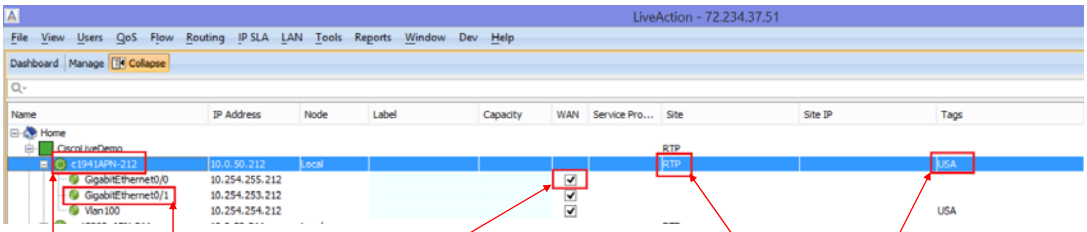
127

Managing Data Storage

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



Expand to see device *semantic* information



Device or Interface

WAN Tagged Interfaces

Site or configured Tags

128

LAB: Customize Topology

- Device Semantics
- Creating / Modify Groups
- Network Objects

129

130

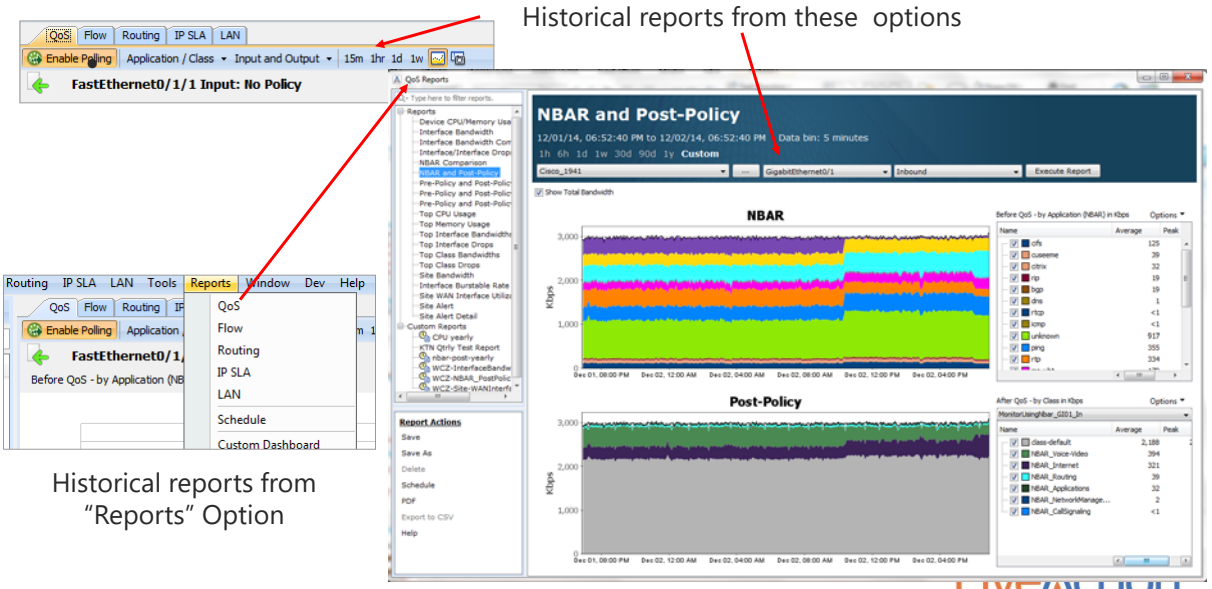
LiveNX QoS Baseline

- 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.

2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. LiveAction 131

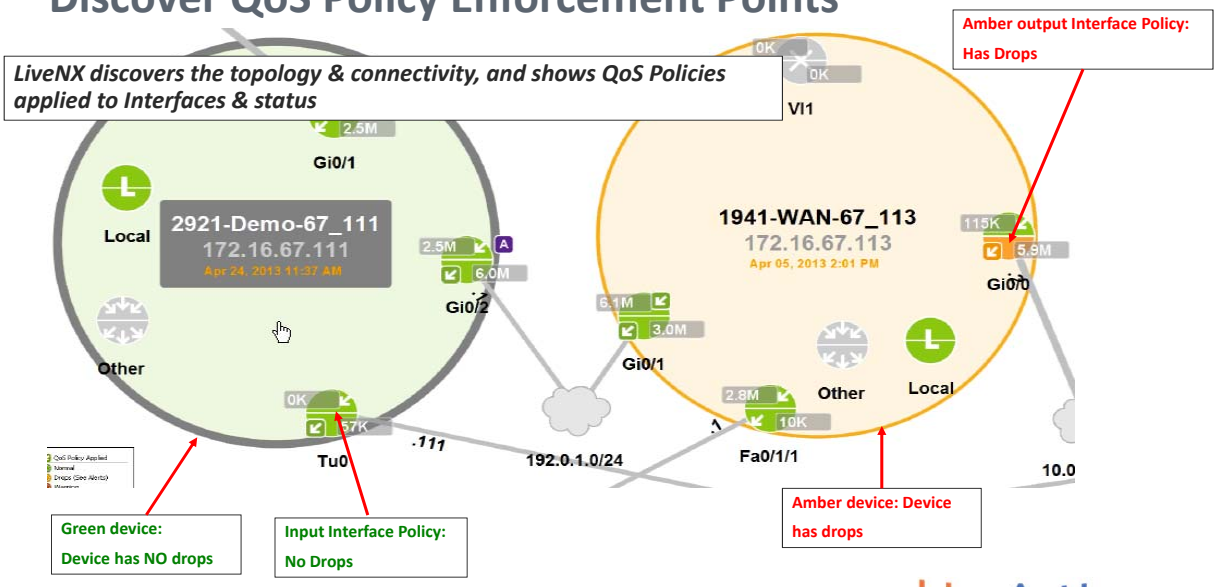
131

Historical QoS Class View/Reports



132

Discover QoS Policy Enforcement Points



133

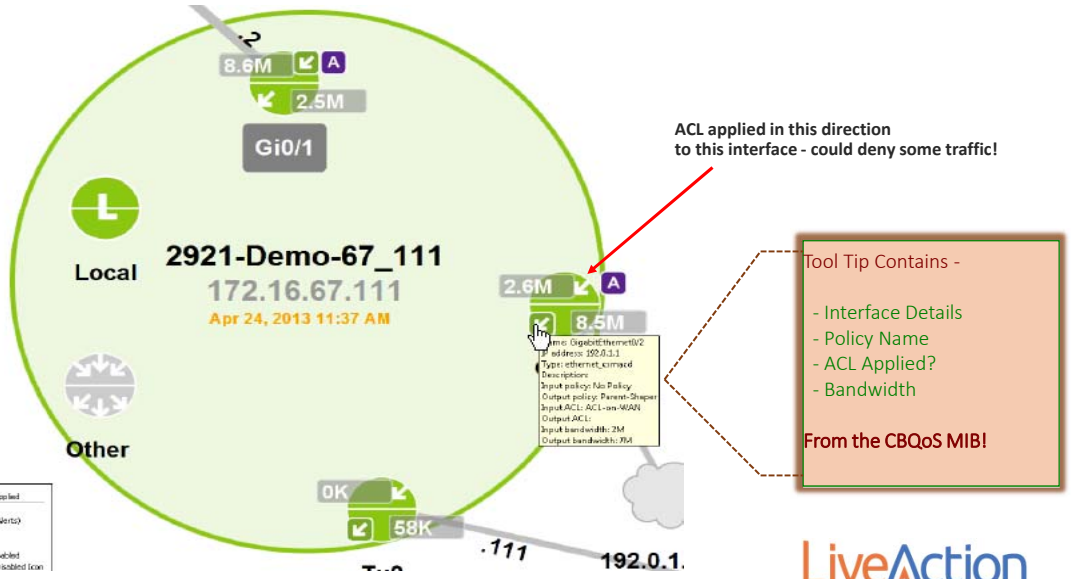
QoS ACL

- 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

2019Apr01 134

134

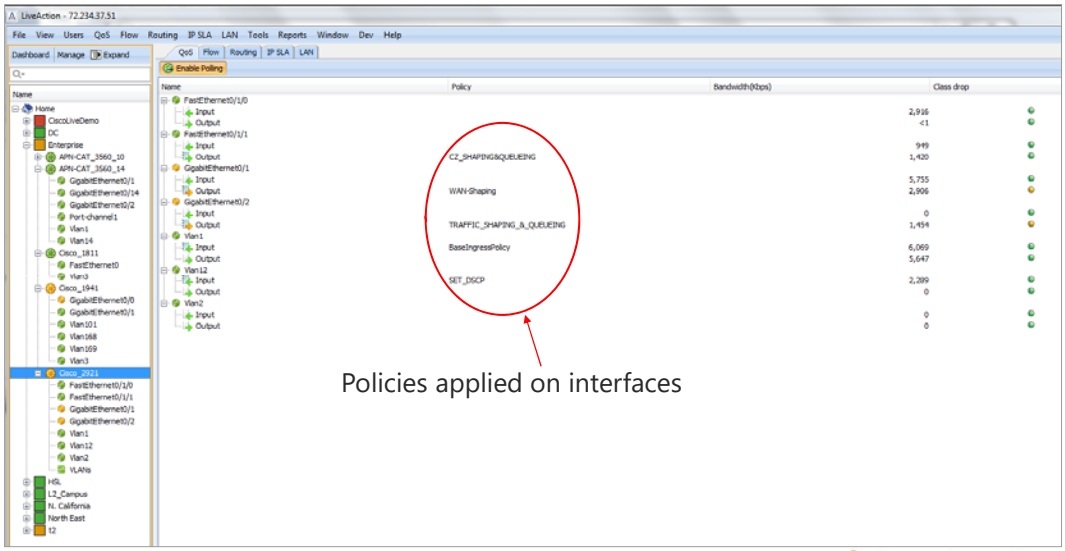
QoS Policy Detail Display



2019Apr01 135

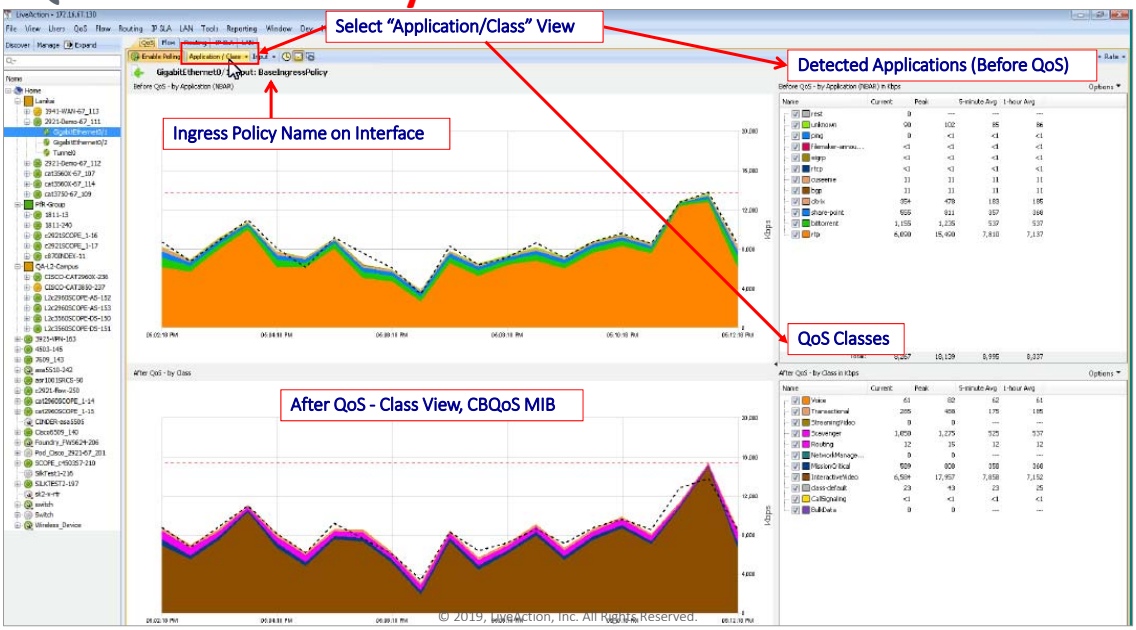
135

QoS Device View



136

QoS Interface Policy Performance

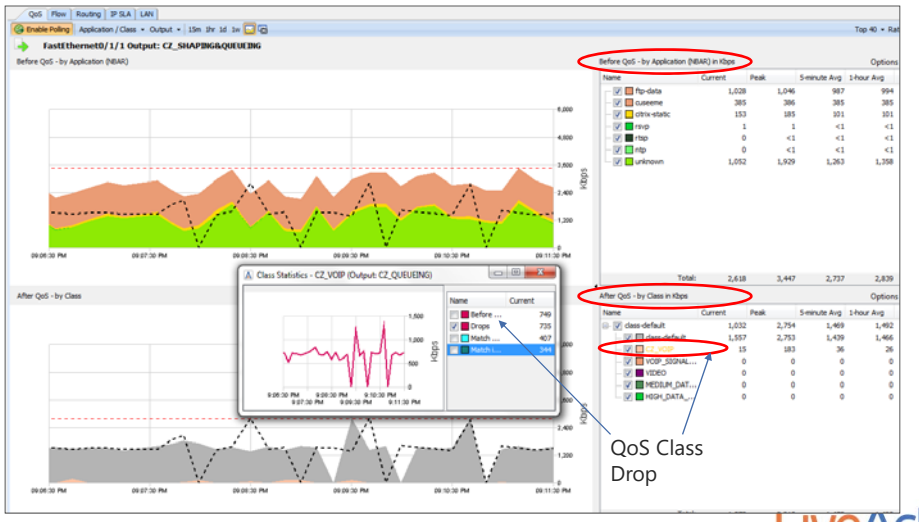


137

QoS Troubleshooting

- Real-Time QoS Issues

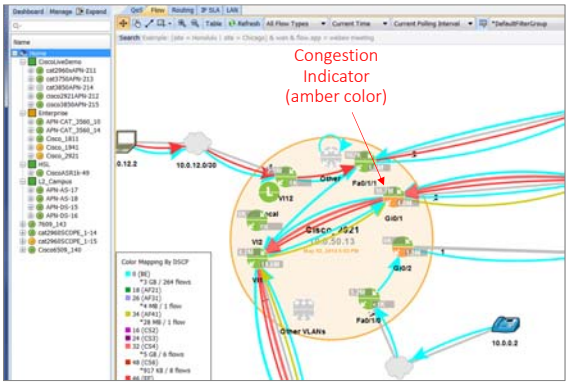
Amber QoS class color shows class drops



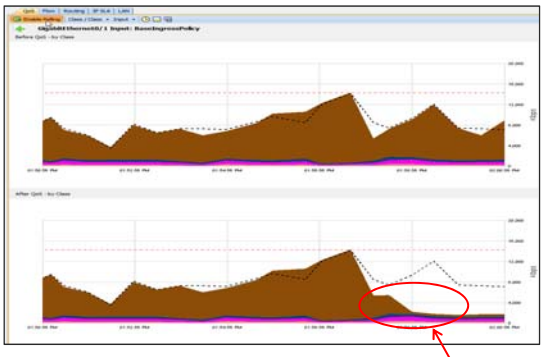
138

Track QoS Performance & Policy Validation

Visualize QoS Performance



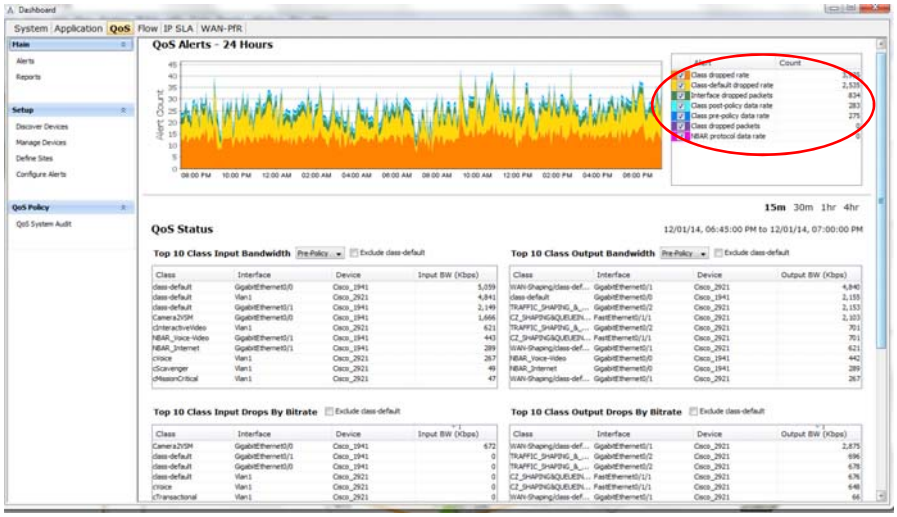
Show Impact of QoS Policy



Policy applied to Police Interactive Video to 512 Kbps

139

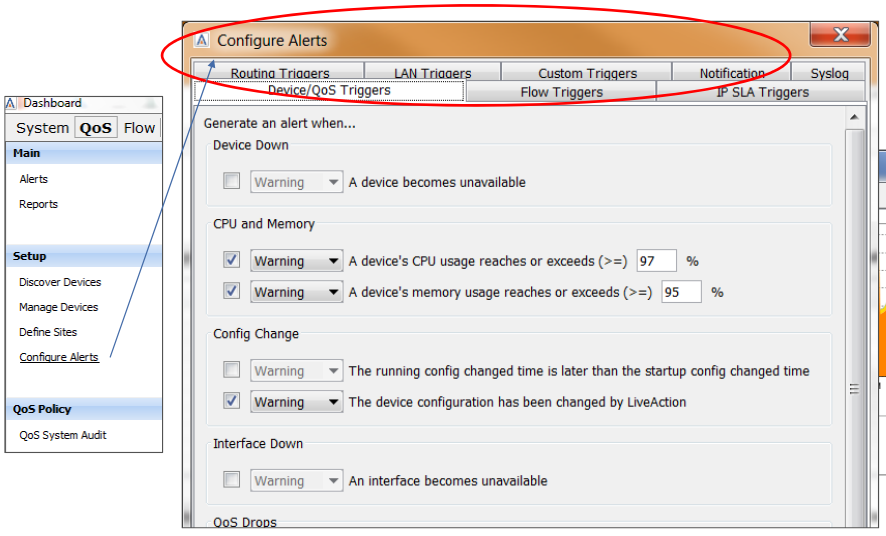
QoS Dashboard



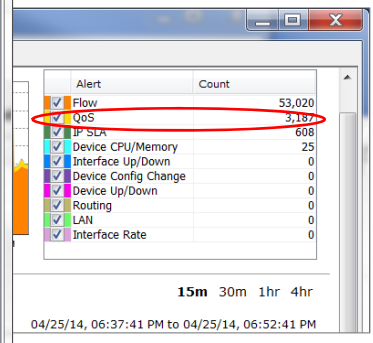
Driven from MIB-II, NBAR, and CBQoS MIBs

140

Troubleshooting - Real-Time QoS Alerts



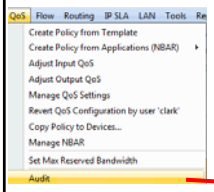
User-defined thresholds can be configure to create QoS alerts when thresholds are exceeded

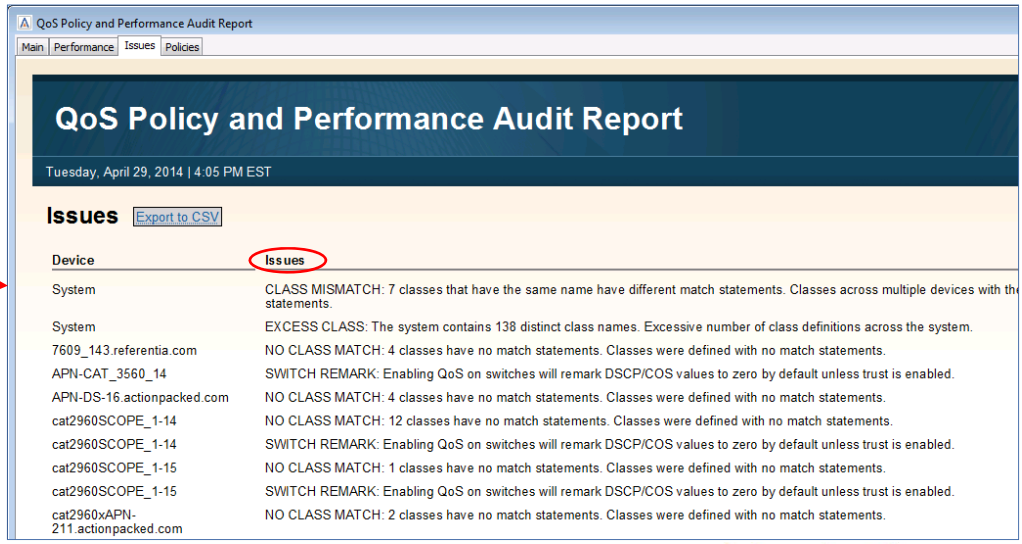


141

Troubleshooting – Auditing QoS Policies

Single-click!





142

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

143

LAB: Quality-of-Service

- Investigate ways QoS can help our gateways be more efficient!

144

151

Server / Collector Node Sizing

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

LiveNX 8 Specifications

LIVENX 8

LIVENX 8 DEPLOYMENT OPTIONS

LiveNX 8.x components can be deployed via the following method: Virtual, Physical and Cloud

Component	Virtual Appliance Option
Server	All-in-one Server OVA
Client	Client software for Mac OS, Win 32-bit and 64-bit
Node (optional)	Node OVA
LiveAnalytics Node (optional)	LiveAnalytics OVA

Custom Deployment	Small Deployment	Medium Deployment	Large Deployment
Used for less than 25 devices or less than 25k flows/sec.	**Used for less than 100 devices or lesser than 50k flows/sec**	**Used for 100 to 500 devices or lesser than 100k flows/sec**	**Used for 500 to 1000 devices or lesser than 150k flows/sec**
Proof of Concept Deployments – Installation for non-server installations (Laptops, Desktops)	Installation for server environments with Hyper-V Manager/VMware ESXI/ Hypervisor	Installation for server environments with Hyper-V Manager/VMware ESXI/ Hypervisor	Installation for server environments with Hyper-V Manager/VMware ESXI/ Hypervisor
Specifications: 8vCPU Xeon or i7 16GB RAM	**Specifications** 16vCPU Xeon or i7 32GB RAM	**Specifications** 16vCPU Xeon or i7 64GB RAM	**Specifications** 32vCPU Xeon or i7 64GB RAM
LiveNX Server Max Heap Size 8GB	LiveNX Server Max Heap Size 16GB	LiveNX Server Max Heap Size 31GB	LiveNX Server Max Heap Size 31GB
500GB Data Disks *	2TB Data Disks *	4TB Data Disks *	8TB Data Disks *

Virtual Platform

VMware ESXi v5.0+ – VMware Hardware Version 8 (vmx-8)

Network Hardware – At least 2 Physical NICS on ESXi

– Support up to 10Gbps

– Virtual NICs on OVA are utilizing E1000

LIVENX CLIENT SIZING – DETAILS

The client application can be launched via Web Start directly from the LiveNX Web Server or Mac. For large scale deployments, the client application installer is recommended as it can s

Operating System Specification

Windows 10 or Mac OSX 64-bit OS

4 Cores

8 GB RAM

Web browser: IE11 and higher, Firefox, Chrome and Safari

OTHER COMPONENTS

- Java JDK `1.8.0_181`
- NodeJS `v8.9.4`
- InfluxDB `1.6.1`
- MongoDB `3.6.3`

PHYSICAL DEPLOYMENT PLATFORM – DETAILS

Base Hardware Model – Dell R440 1U Chassis

Processors – 2 x Intel Xeon Gold 5118 (24 CPU Total)

RAM – 96 GB DDR3; Heap-Size – 64GB

Storage – 4 x 8 TB 7200-RPM disks in RAID 10

IDRAC support

152

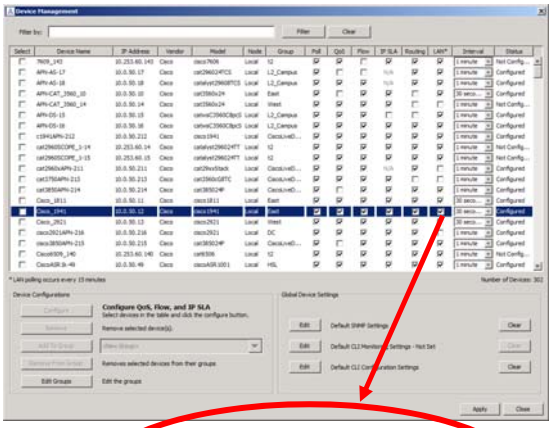
Disk Sizing- SNMP

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



153

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
o 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
o 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

154

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

155

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%)

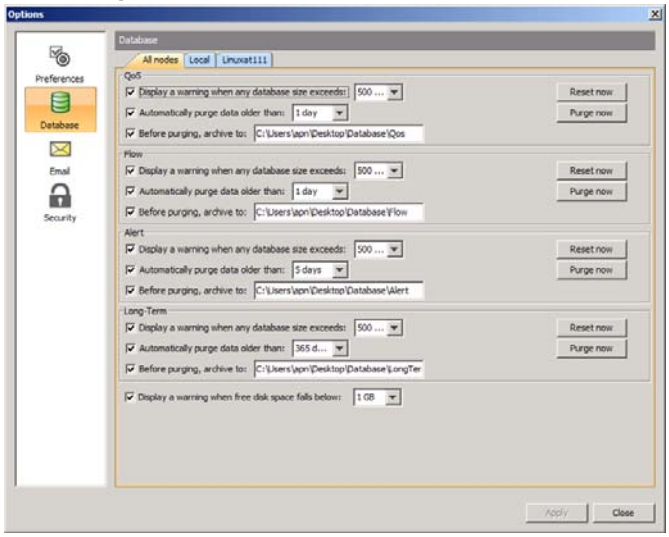
Bandwidth	<768Kbps	1.544Mbps	3Mbps	10Mbps or higher
Overhead	3%	2%	1%	<.5%

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.

156

Disk Retention

Tools > Options > Database:



Admin can set:

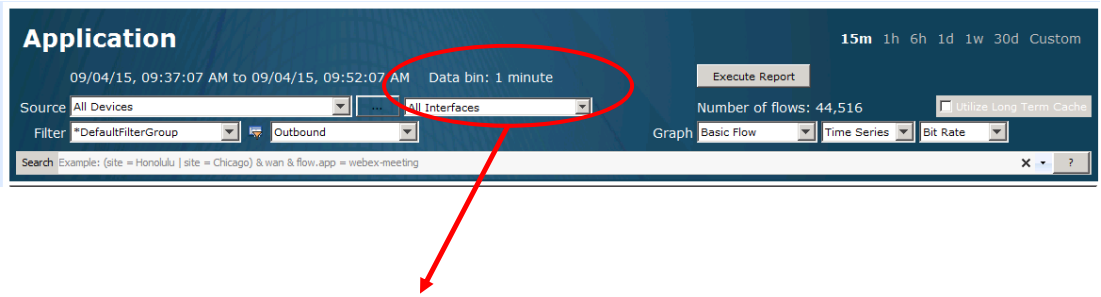
- Data Retention policy
- Manual Purge
- Backup
- Mounting

Disk full = Automatic Purging

Provision Enough Disk Space!

157

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

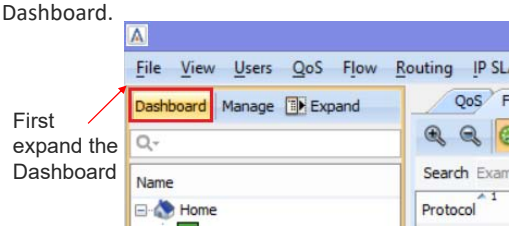
158

Long Term Report Management

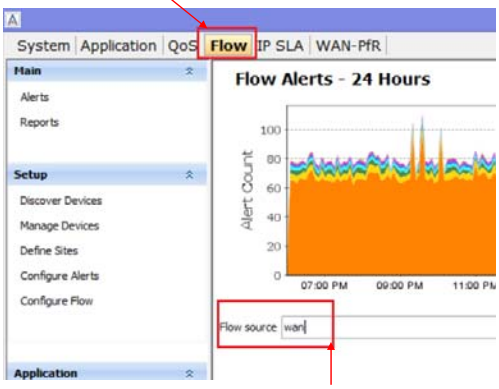
Populating data in the data store…

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

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



Then select the Flow Tab

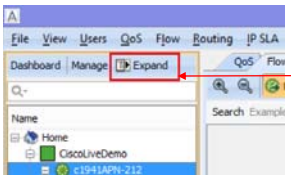


You can configure the "Flow source" to use tags for either Device, Interface, WAN, Site, or Tag

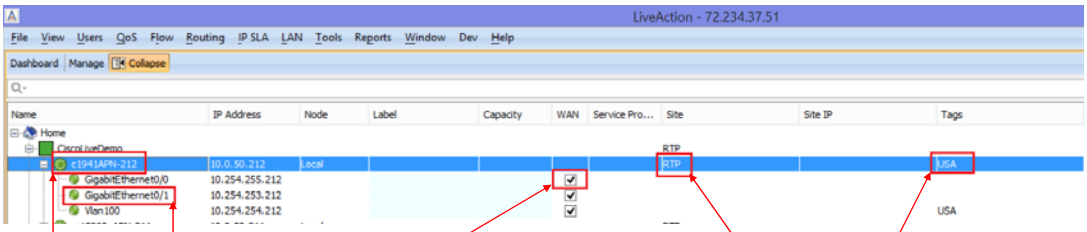
159

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

160

NetFlow Best Practices

LiveAction™

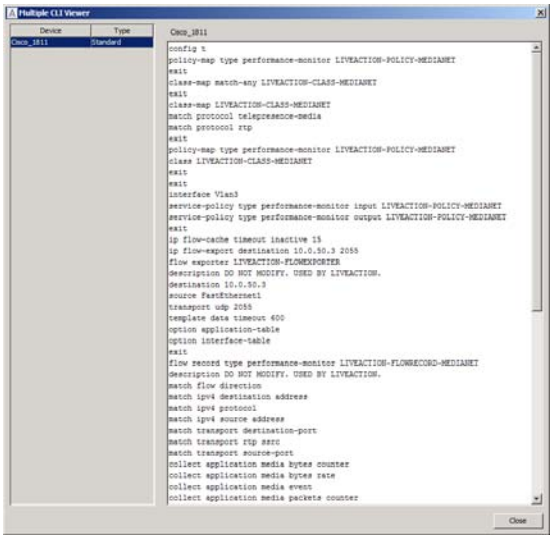
161

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

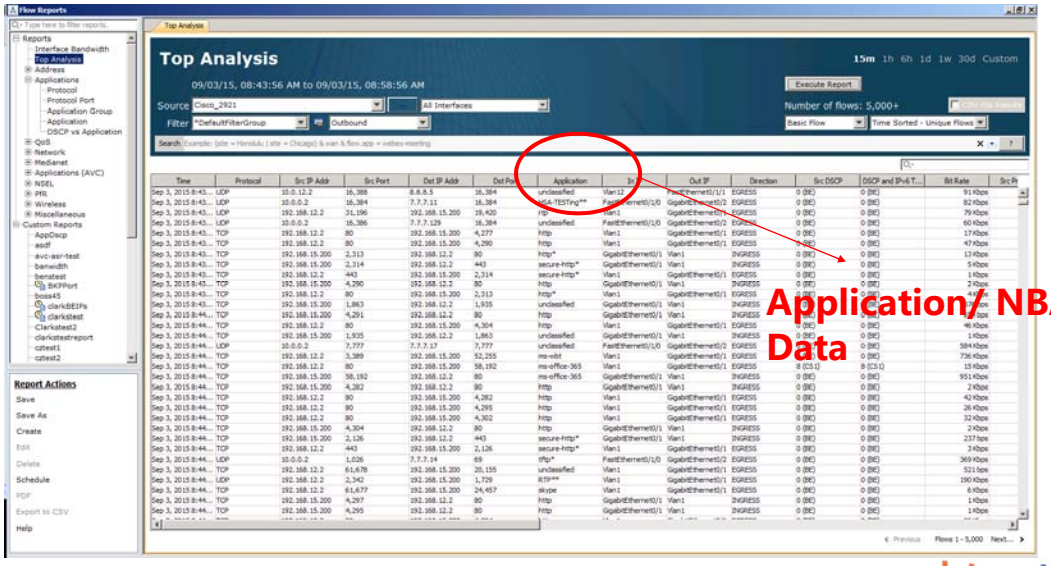
NetFlow – Configuration Management



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.

NetFlow – Flexible NetFlow



164

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

165

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

166

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

167

NetFlow – AVC/Medianet

Use solid versions of IOS for 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.

2019Apr01 168

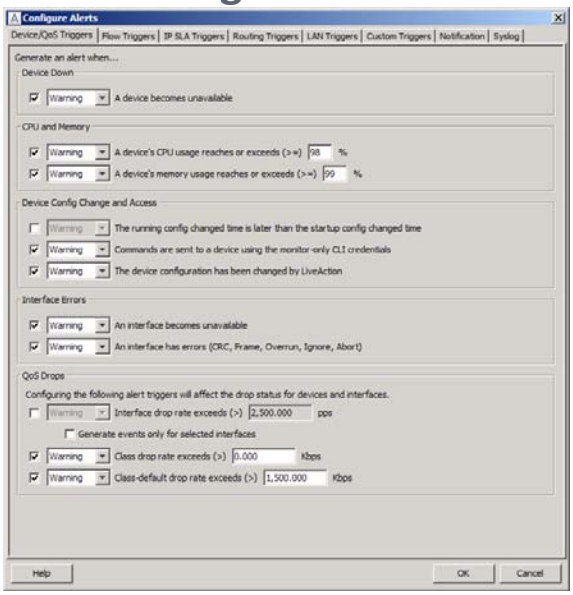
168

Other Best Practices

2019Apr01

169

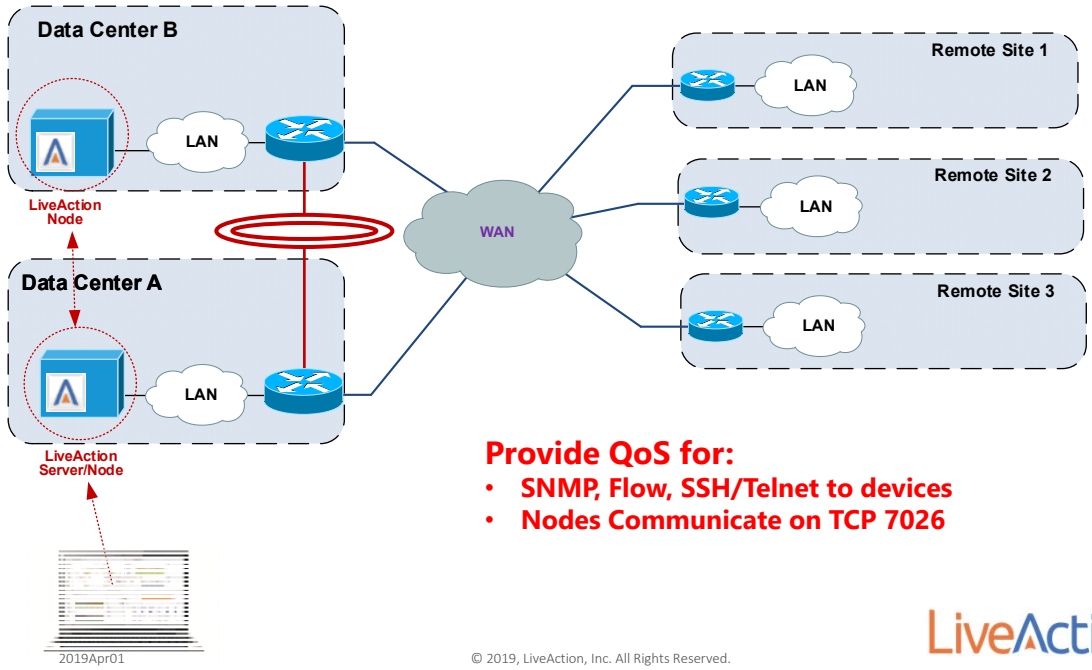
Alerting



LiveAction Prefers the following Defaults:

- Tick - A device becomes unavailable
- Tick - CPU Utilization
- Tick - Memory Utilization
- Tick - Commands sent for monitor-only
- Tick - Device config has been changed via LiveAction
- Tick - Interface becomes unavailable
- Tick - An interface has errors (CRC, Frame, etc)
- Un-Tick - Interface drop rate errors
- Tick - Class drop rate exceeds = 0Kbps
- Tick - Class-default drop exceeds = 1500Kbps

170

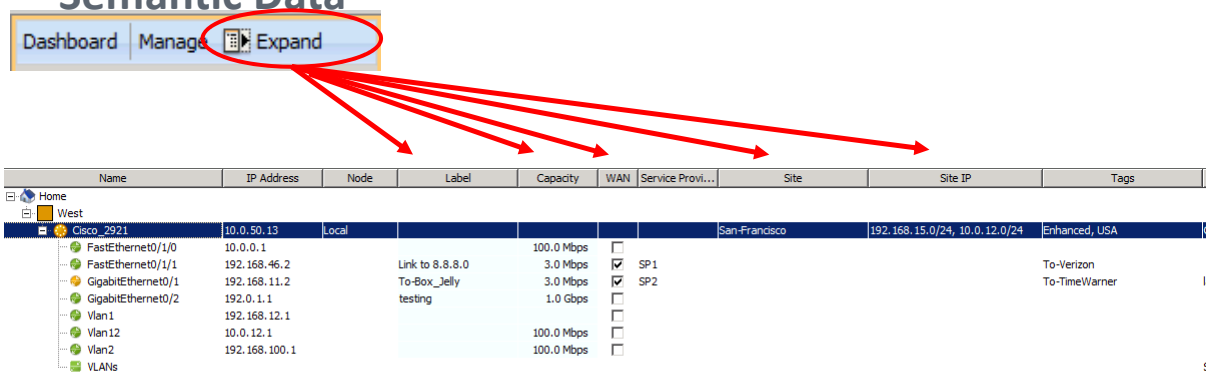


Provide QoS for:

- SNMP, Flow, SSH/Telnet to devices
- Nodes Communicate on TCP 7026

171

Semantic Data



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

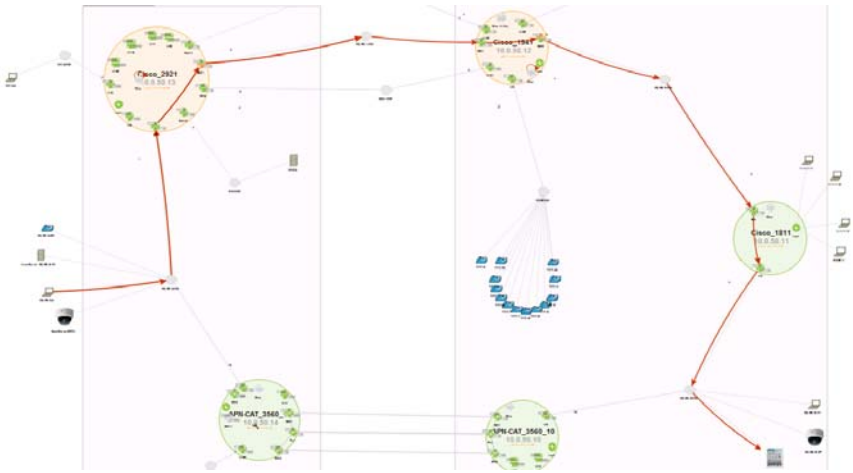
Semantic data makes LiveAction come "alive"!

LiveAction

172

Semantic Data – example 1

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

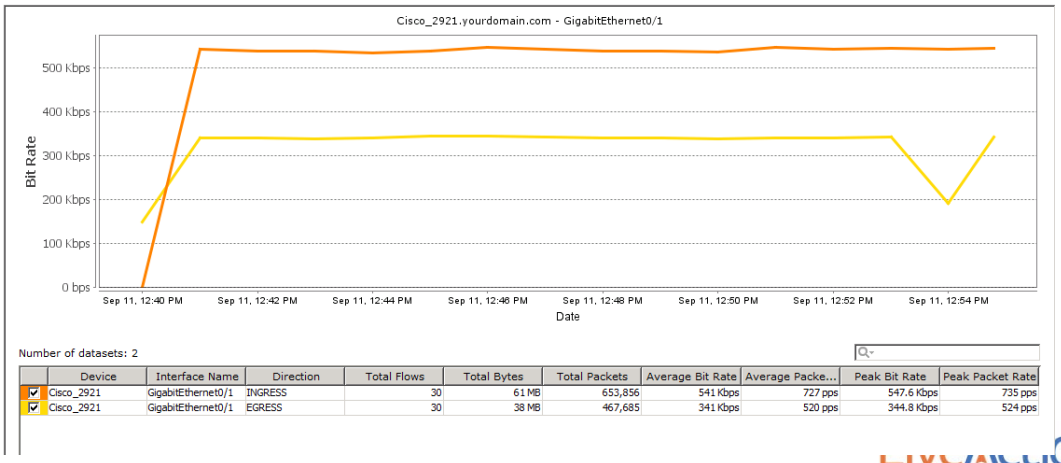


LiveAction

173

Semantic Data – example 2

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

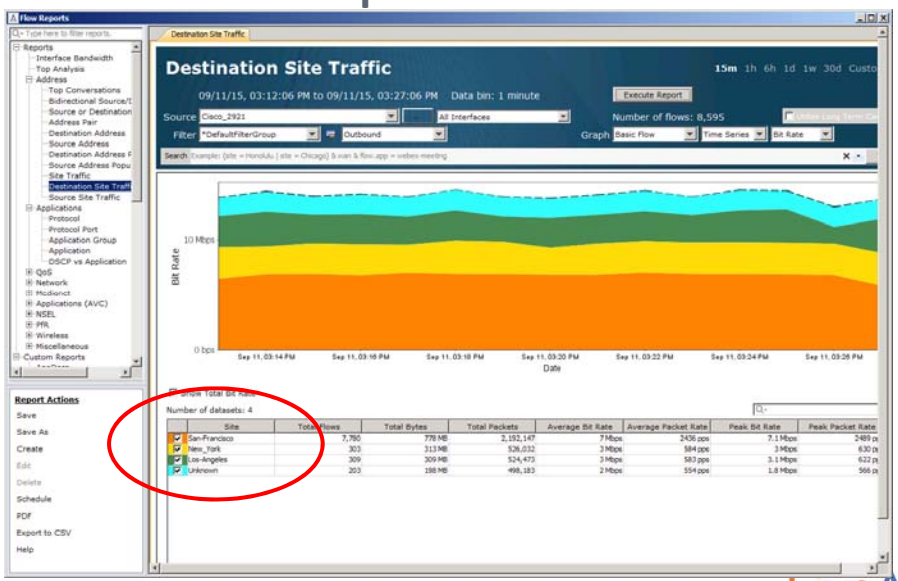


Number of datasets: 2

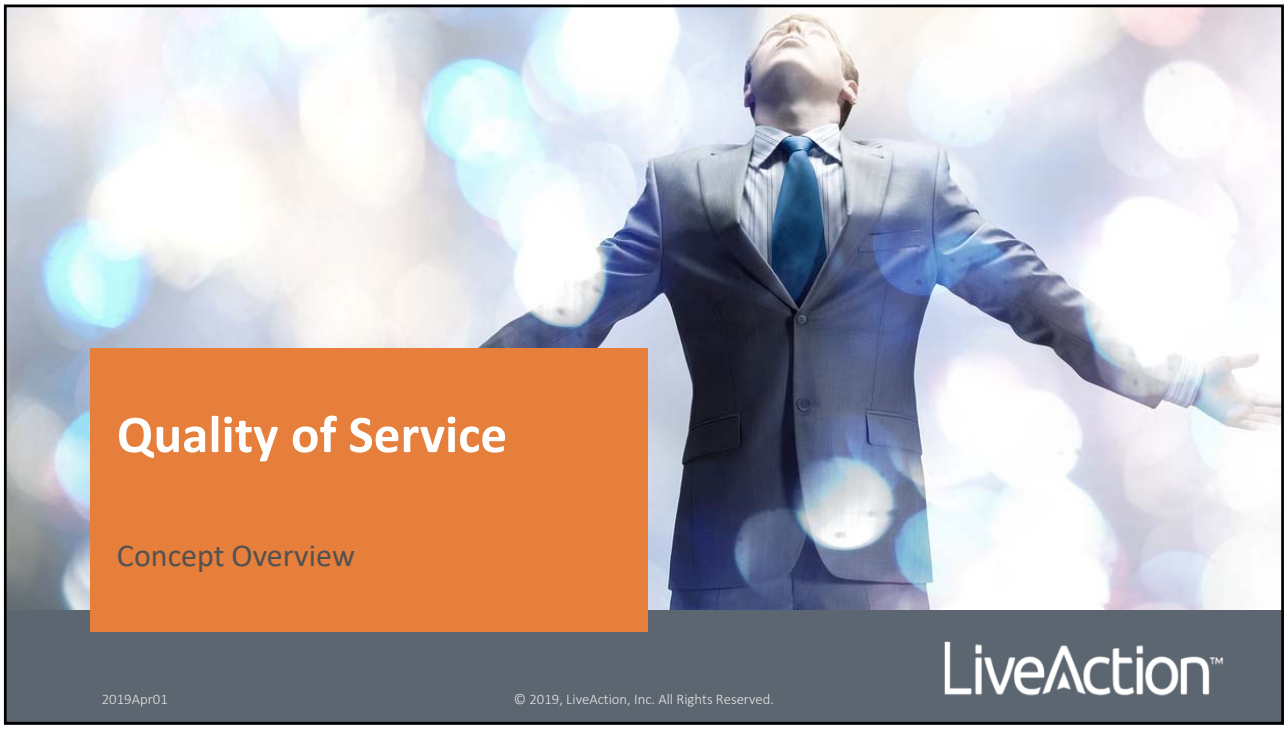
Device	Interface Name	Direction	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packe...	Peak Bit Rate	Peak Packet Rate
Cisco_2921	GigabitEthernet0/1	INGRESS	30	61 MB	653,856	541 Kbps	727 pps	547.6 Kbps	735 pps
Cisco_2921	GigabitEthernet0/1	EGRESS	30	38 MB	467,685	341 Kbps	520 pps	344.8 Kbps	524 pps

174

Semantic Data – example 3



175



176

How to Implement QoS

Step 1 - Recognize Application Traffic (Classification and Marking)

Step 2 - Prioritize (Queuing and Shaping)

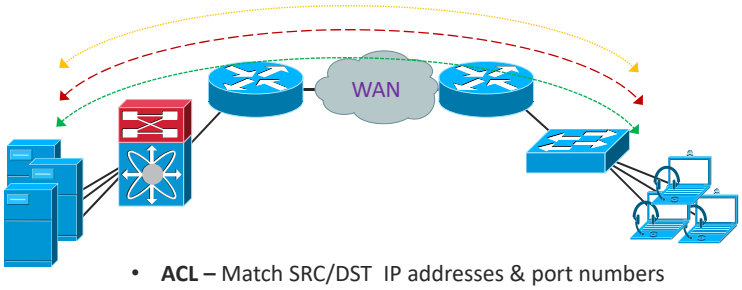
Step 3 - Throttle Traffic (Policing and WRED)

Step 4 - Buffer Tuning

177

Step 1 - Recognize Application Traffic

Classification and Marking



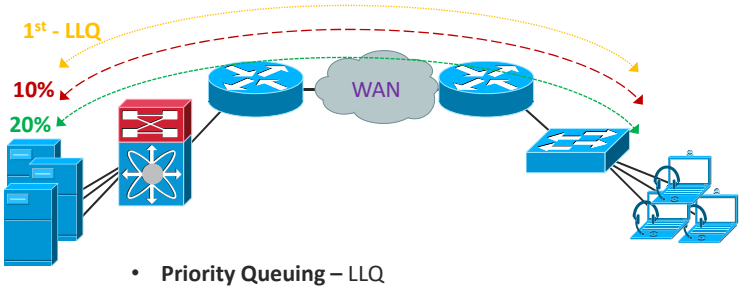
- **ACL –** Match SRC/DST IP addresses & port numbers
- **DSCP-** TOS byte QoS markings
- **NBAR –** Protocol discovery by Cisco devices

2019Apr01 178

178

Step 2 – Prioritize

Queuing and Shaping

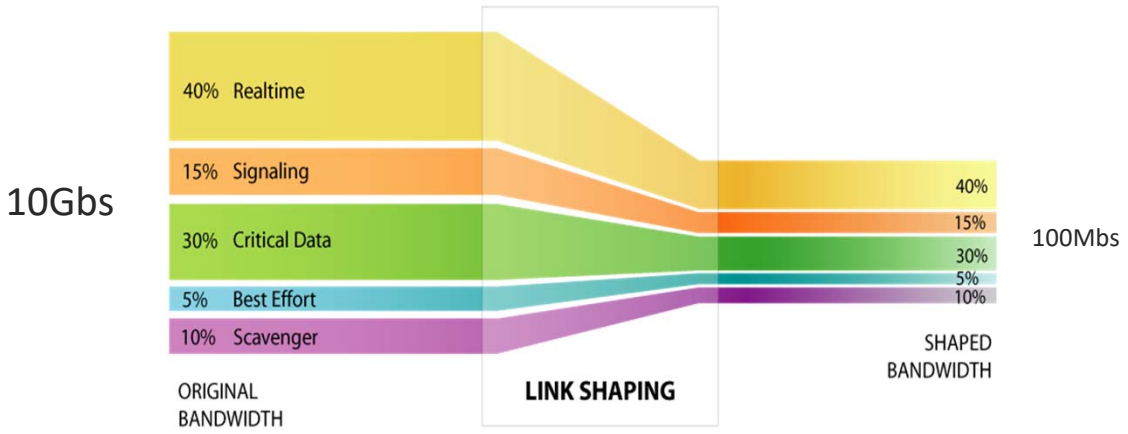


- **Priority Queuing –** LLQ
- **CBWFQ -** Guaranteed bandwidth
- **Shaping -** Transmit data to software set limit, buffer and queue overage

2019Apr01 179

179

Shaping (or Scaling)

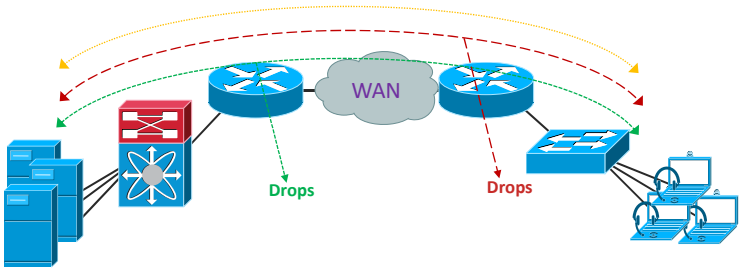


2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 180

180

Step 3 –Throttle Traffic

Policing and WRED

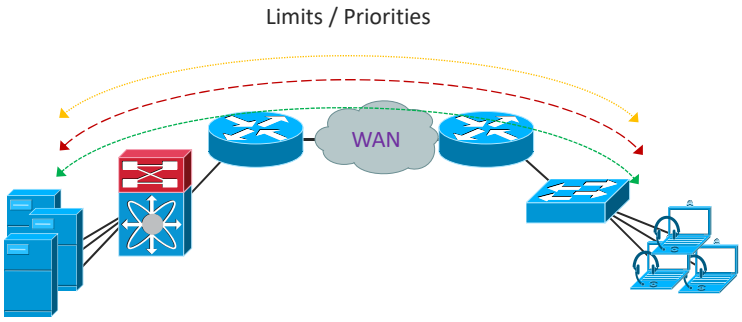


- **Policing -** Transmit data to software set limit, drop overage
- **WRED –** Selectively drop specific data before congestion occurs

2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 181

181

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

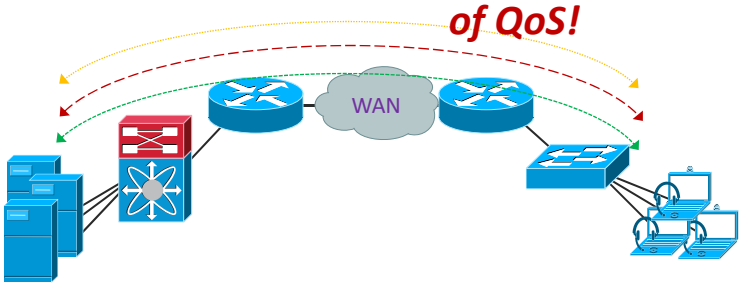
182

Classification & Marking

183

Recognize Application Traffic

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

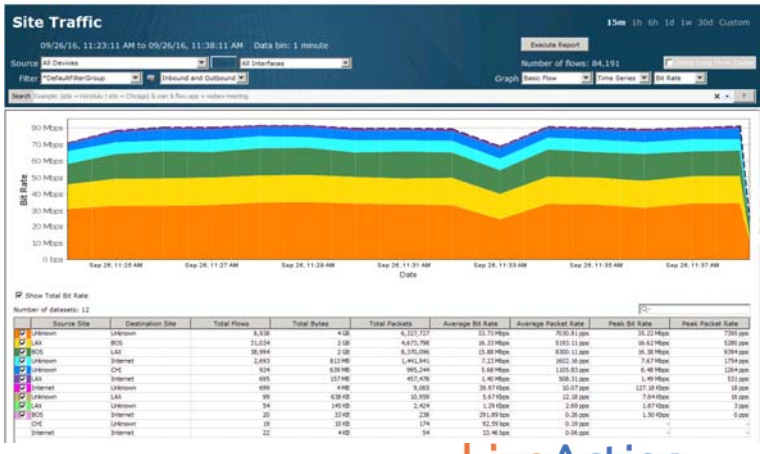


Step 1 – Day 0: Application Landscape
Step 2 - Use Filters/Search to identify traffic in LiveNX
Step 3 - Use visualization & reports to confirm traffic
Step 4 - Standardize on DSCP values
Step 5 - Use visualization & reports to validate DSCP
Step 6 - Update QoS policies on routers/switches/etc.
Step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

184

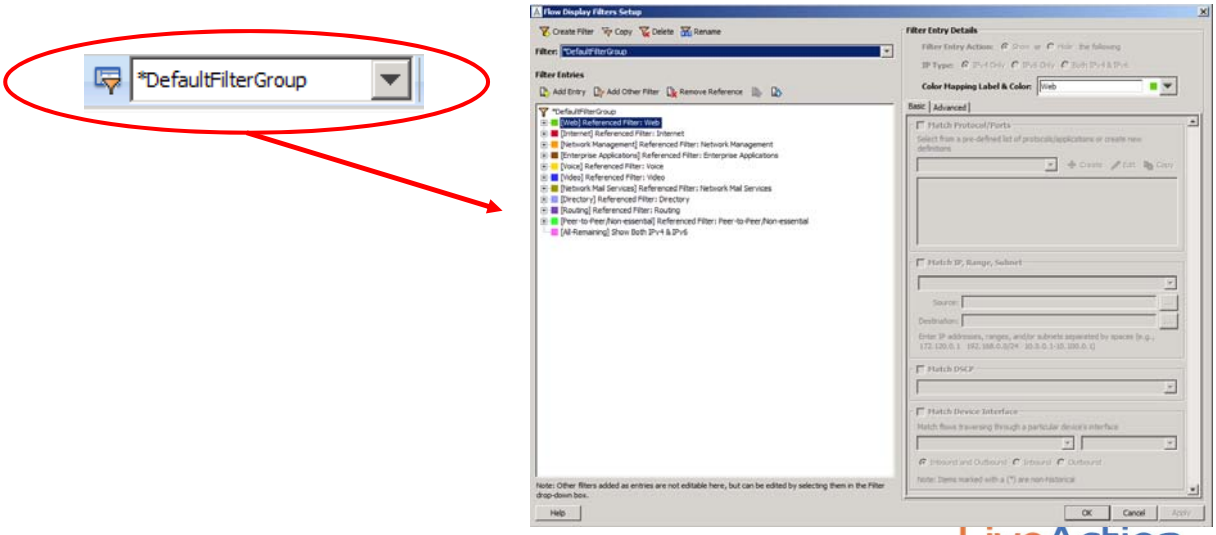
Classification: Day 0: Application Landscape

- 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



185

Classification: Create Custom Filter

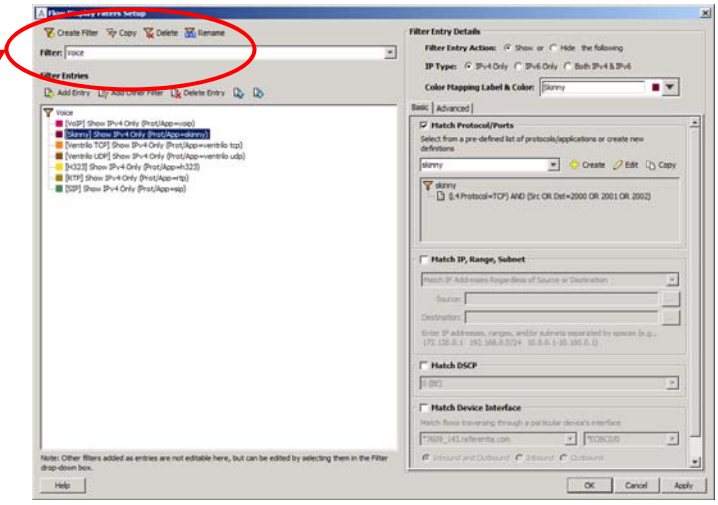


2019Apr01 186

186

Classification: Copy Voice Filter

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

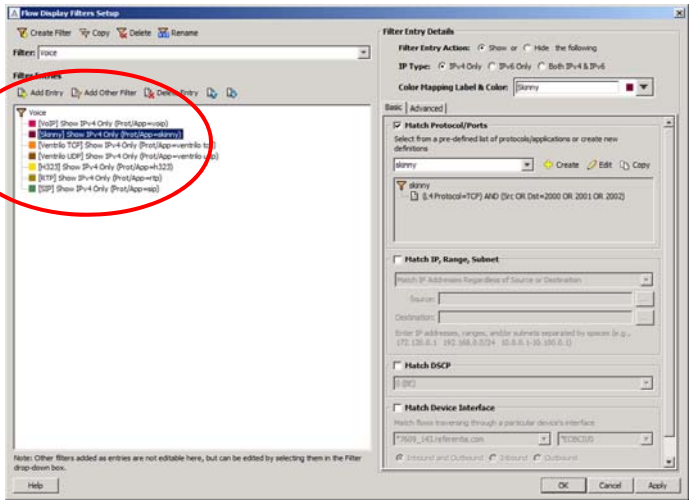


2019Apr01 187

187

Classification: Delete Unused Entries

Delete unused Entries
- VoIP
- Ventrilo TCP
- Ventrilo UDP

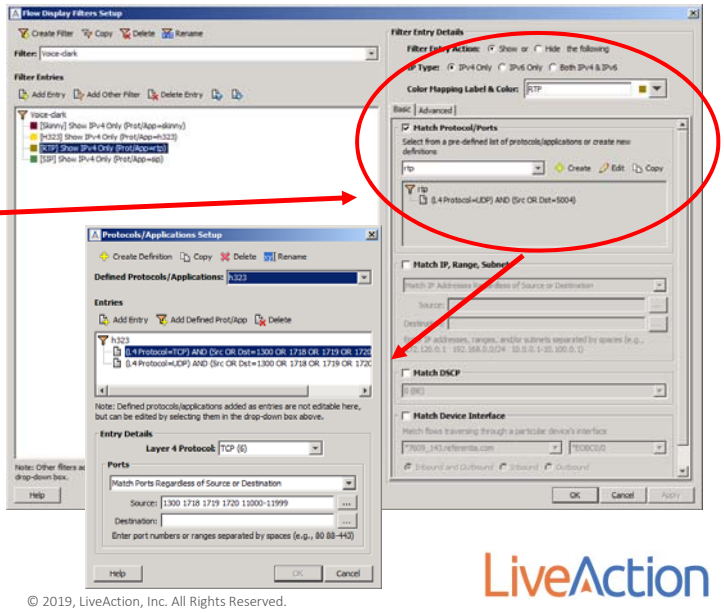


188

Classification: Add/Edit Entries

Edit Entries:
- h323
- RTP
- SIP

Add Entry:
- MGCP



189

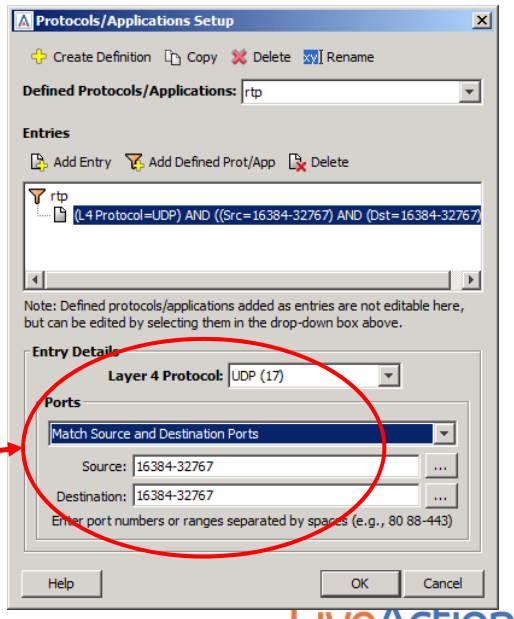
Classification: Edit Entries

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

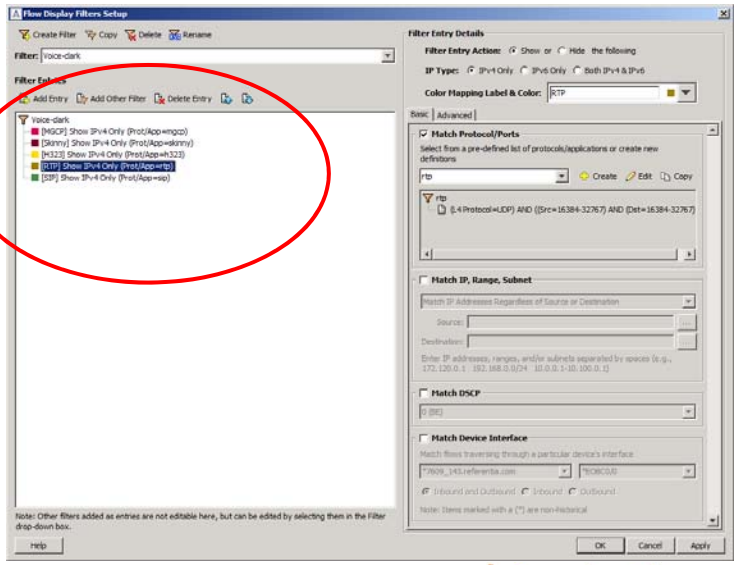
RTP
UDP = Src **AND** Dst = 16384-32767



190

Classification: Voice Filter is ~95 accurate

- MGCP
- Skinny
- h323
- RTP
- SIP



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

191

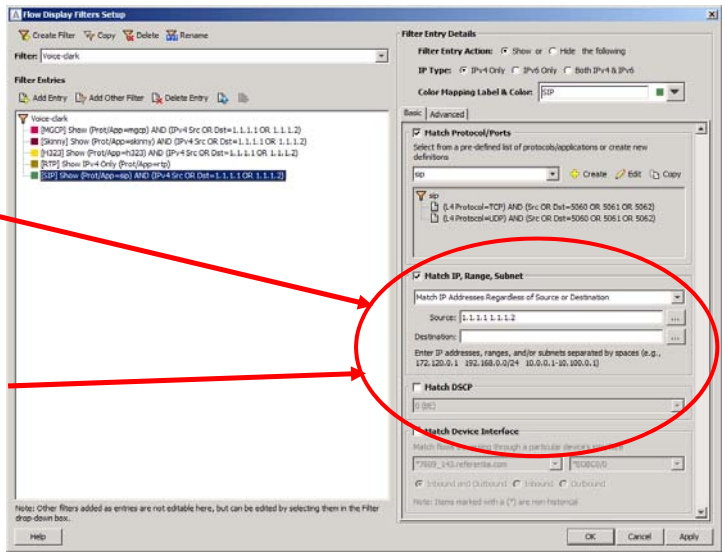
Classification: Voice Filter is ~99 accurate

Add CallManager Server(s) IP address to Filter For:

- MGCP
- Skinny
- h323
- SIP

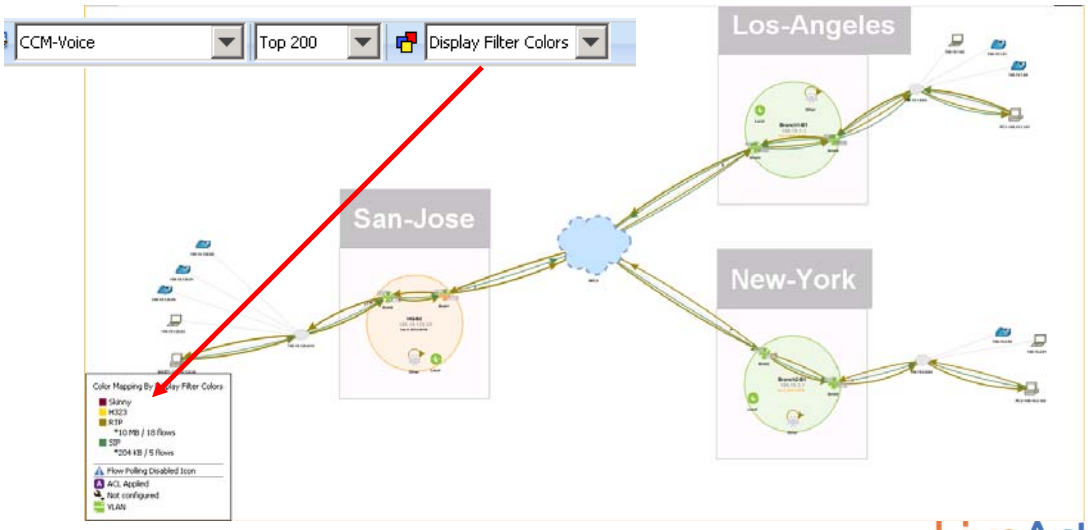
If feasible, add voice subnets to:

- RTP



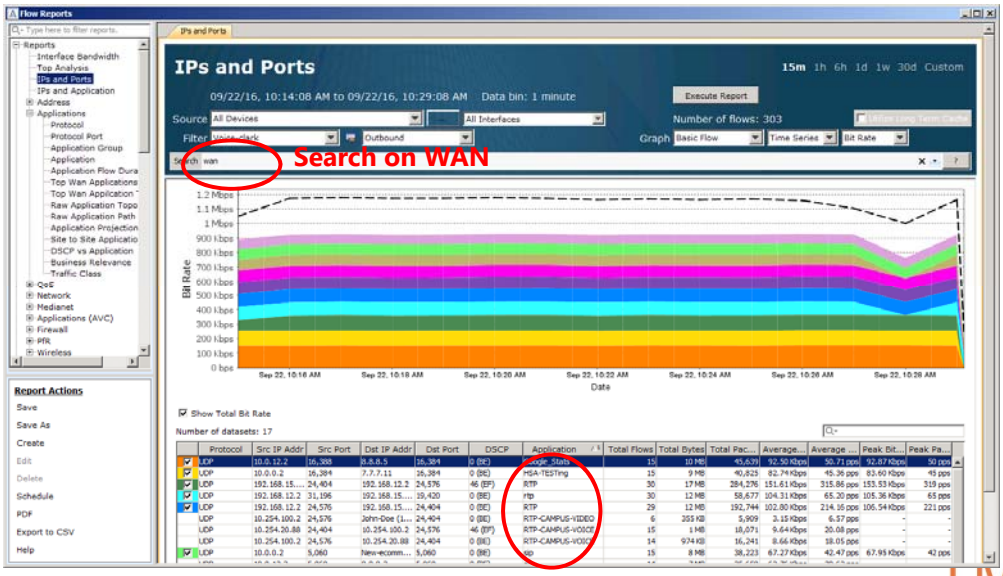
192

Classification: Display Filter Colors



193

Classification: IPs & Ports Report



Use this report to validate Filter's Accuracy.

NBAR2 is your Friend!

194

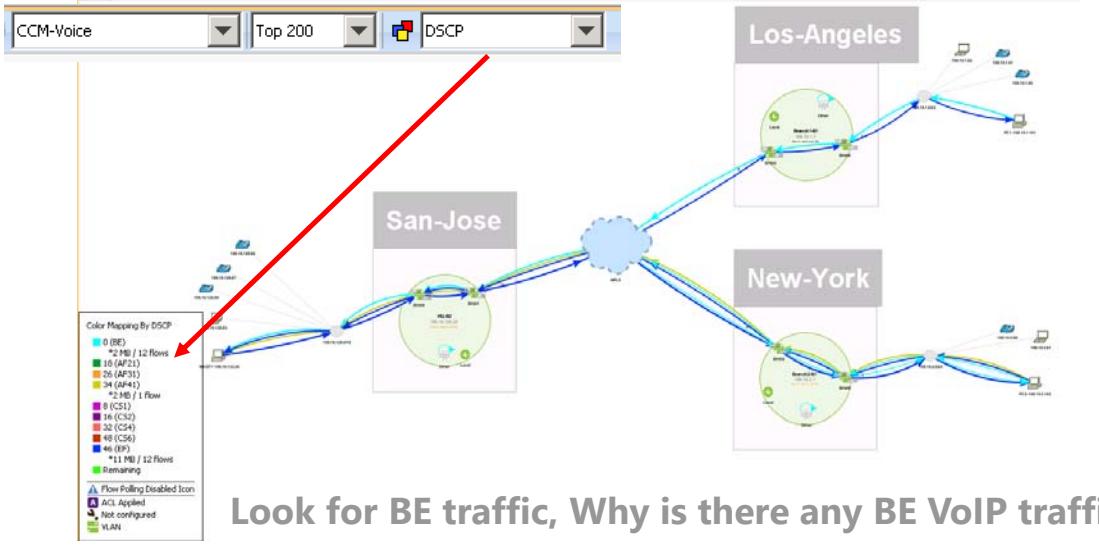
Marking: Selecting DSCP Values

Class Type Cisco Name/ RFC4594 Name	4 Class	8 Class	12 Class
Voice / IP Telephony	EF (46) CS5(40) CS4 (32)	EF (46)	EF (46)
Interactive Video / Multimedia Conferencing		CS5 (40) CS4 (32)	AF41 (34) AF42 (36) AF43 (38)
Streaming Video		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) CS2 (16)	CS3 (24)	CS3 (24)
IP Routing / Network Control		CS2 (16) CS6 (48)	CS6 (48)
Network Management			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.

195

Marking: DSCP Visualization



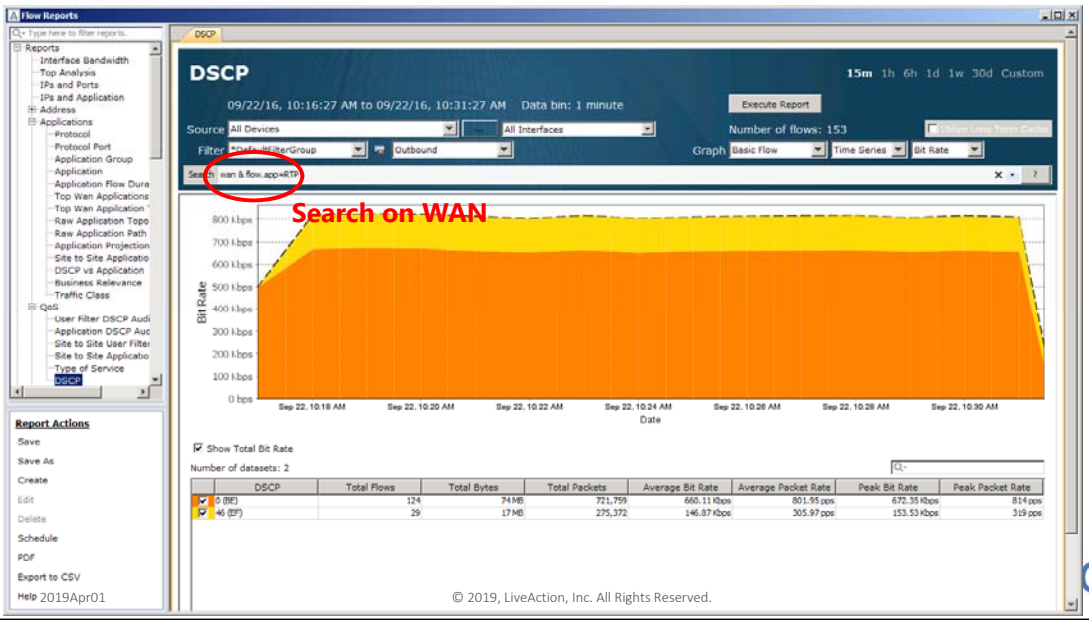
Look for BE traffic, Why is there any BE VoIP traffic?

LiveAction

196

Marking: DSCP Report

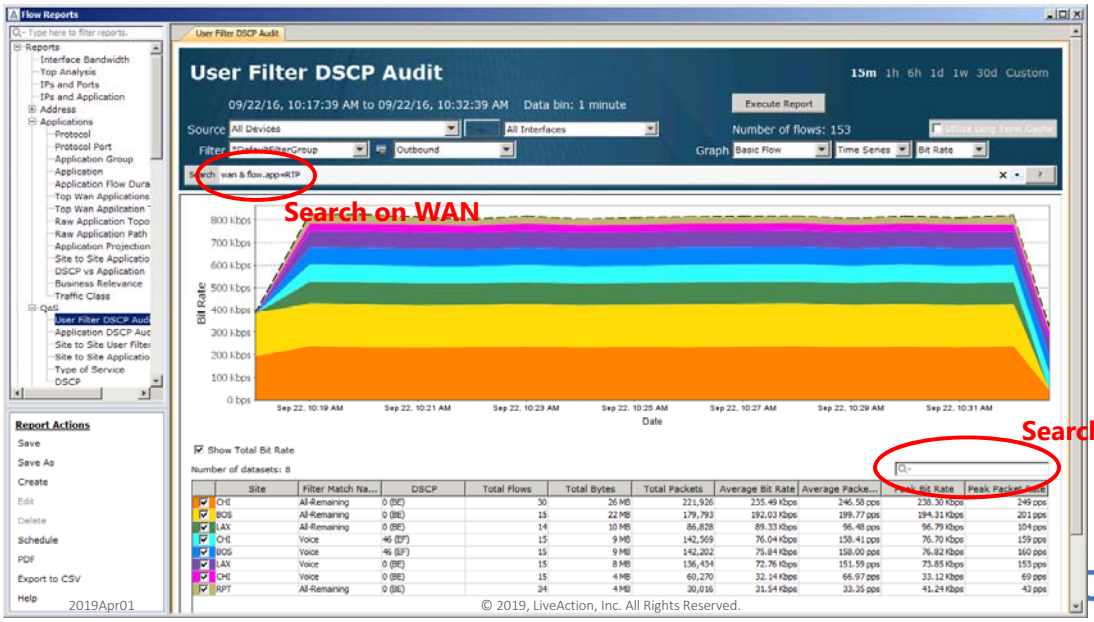
Is there any BE VoIP traffic?



197

Marking: User Filter DSCP Audit

Where is the BE VoIP traffic?



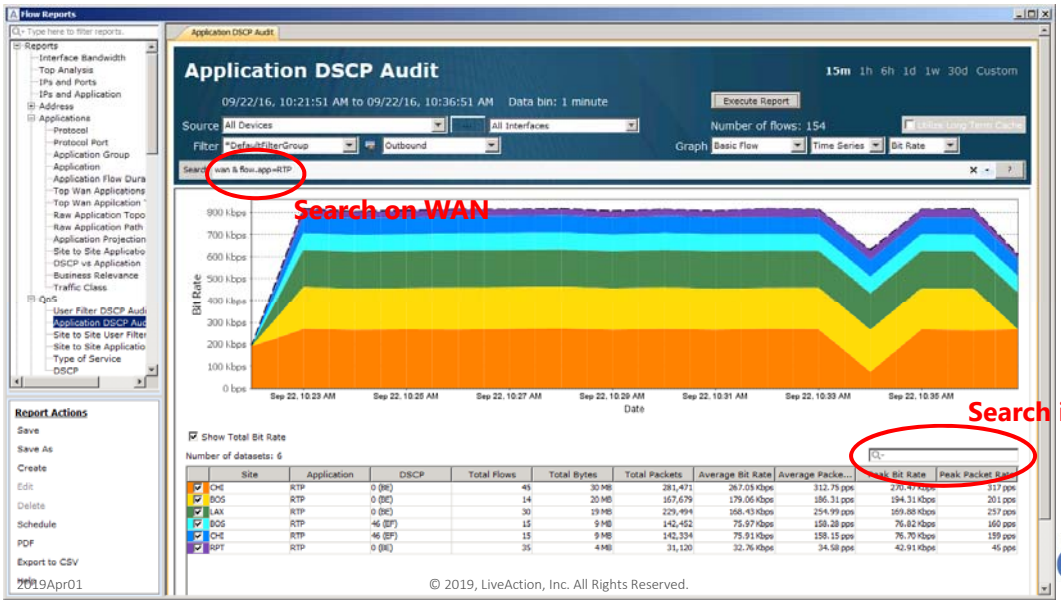
2019Apr01

198

198

Marking: Application DSCP Audit

Where is the BE VoIP traffic?

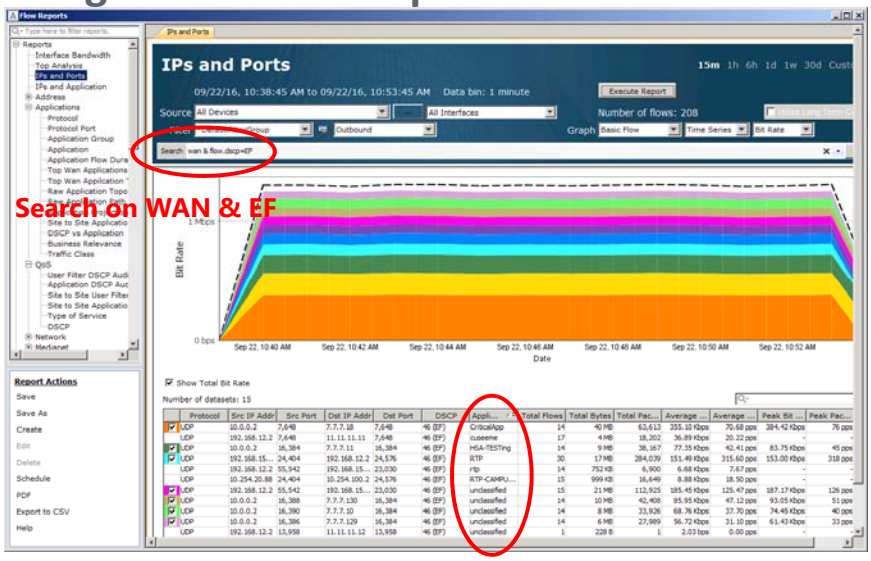


2019Apr01

199

199

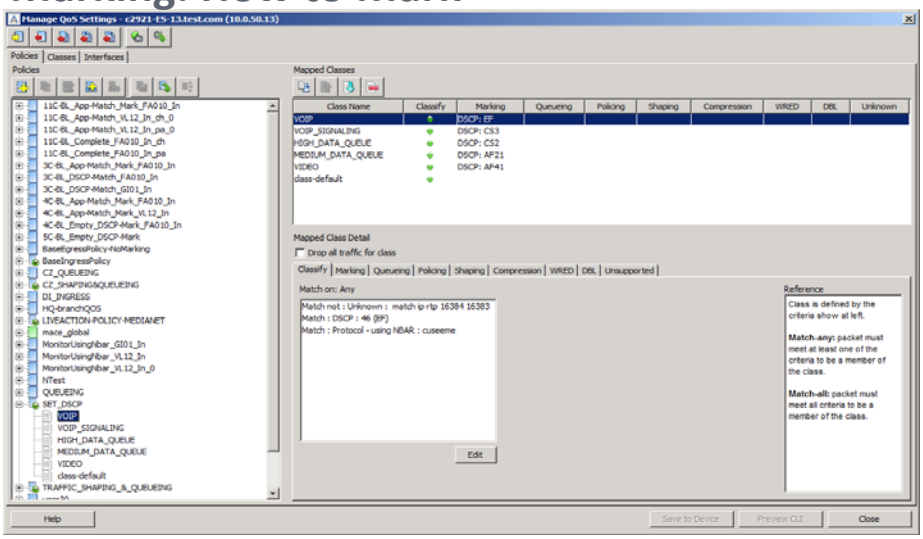
Marking: IPs & Ports Report



Is there any Rogue EF traffic?

200

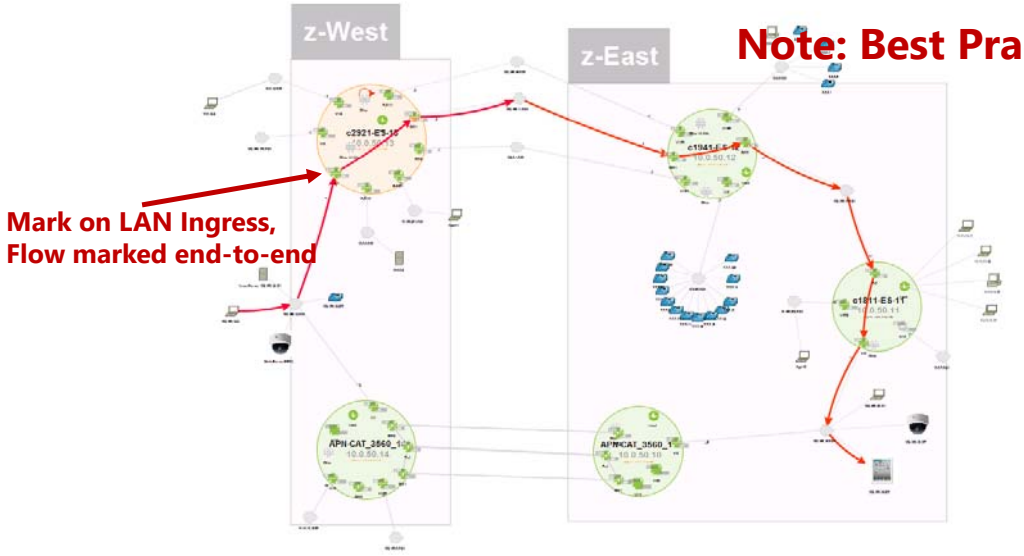
Marking: How to Mark



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

201

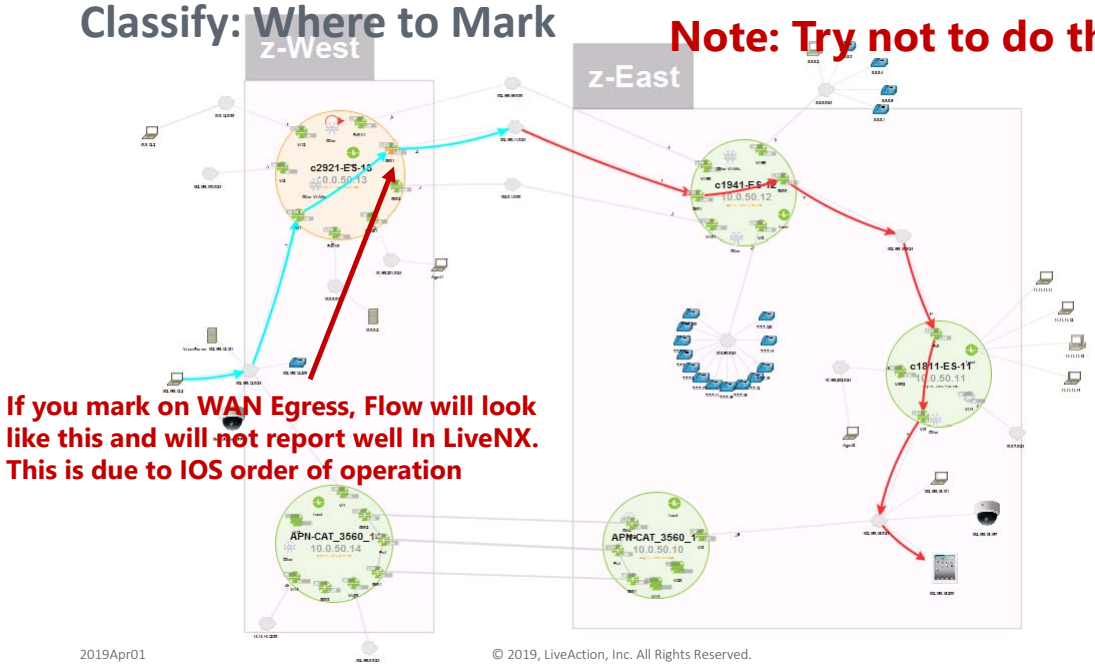
Classifv: Where to Mark



2019Apr01 202

202

Classify: Where to Mark

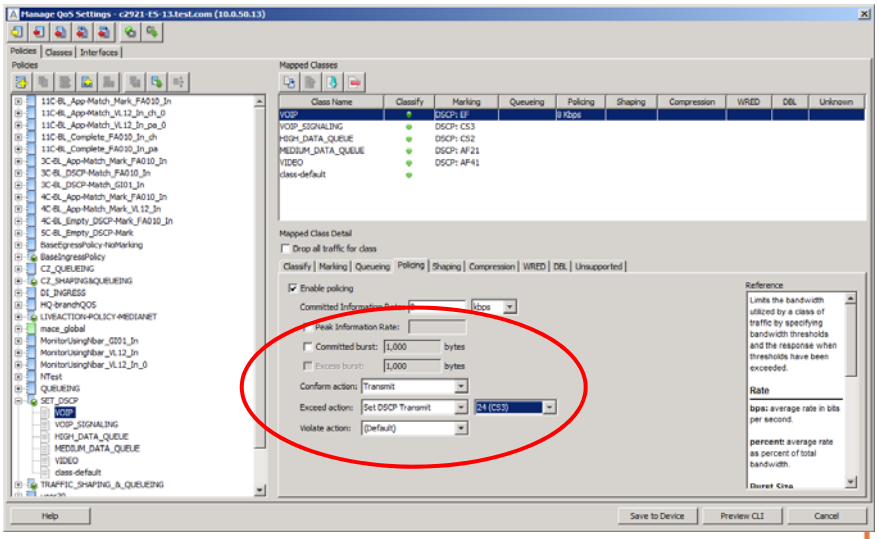


2019Apr01 203

203

Classify: Where to Mark

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



Classify: Next Steps?

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

Lab: Classify / Mark

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

2019Apr01 206

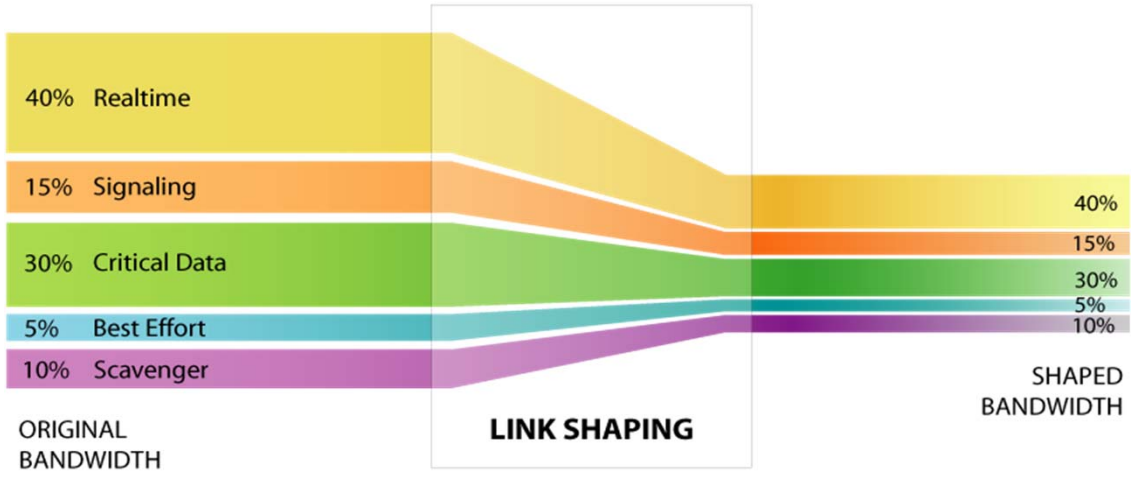
206

Queueing & Shaping

2019Apr01

207

Shaping: Throttle Traffic via software & Queue

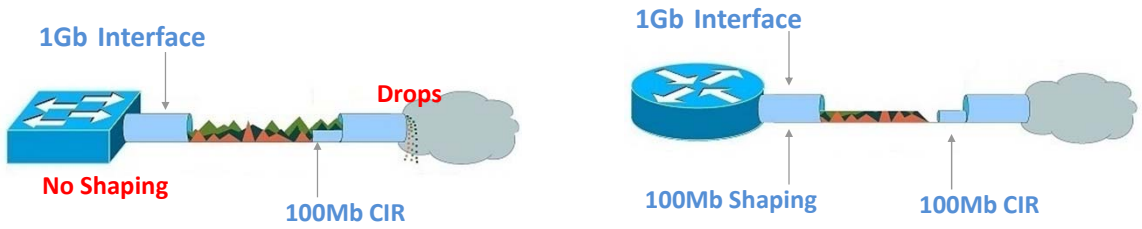


2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 208

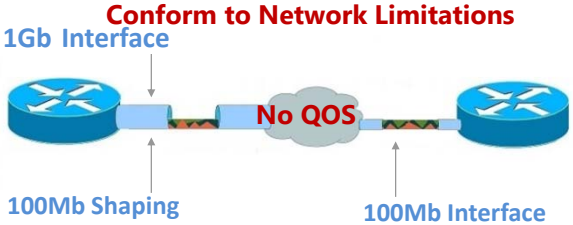
208

Shaping: Throttle Traffic via software & Queue

Conform to Provider's CIR



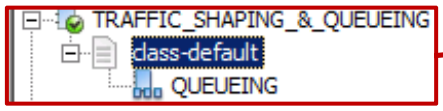
Conform to Network Limitations

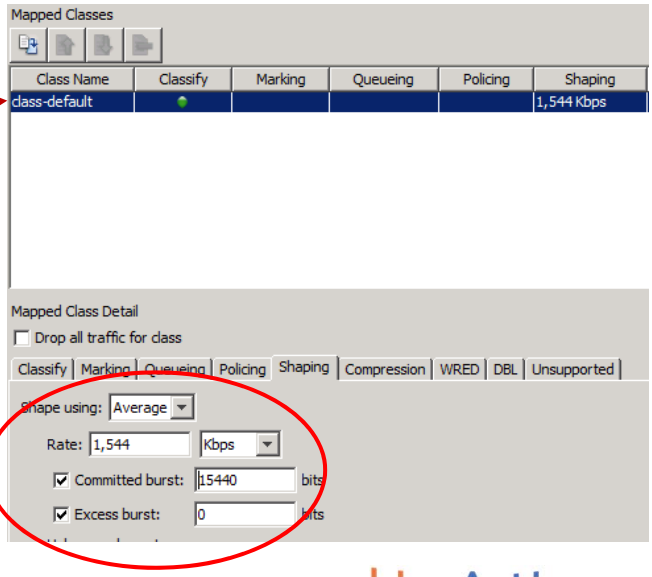


2019Apr01 © 2019, LiveAction, Inc. All Rights Reserved. 209

209

Shaping: Configuration





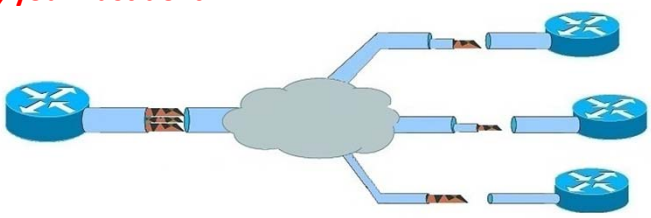
Best Practice is to set CIR, BC, & BE:

Shape average <CIR> <Bc> <Be>
Bc = 1/100 of CIR
Be = 0
Shape average 1544000 15440 0

210

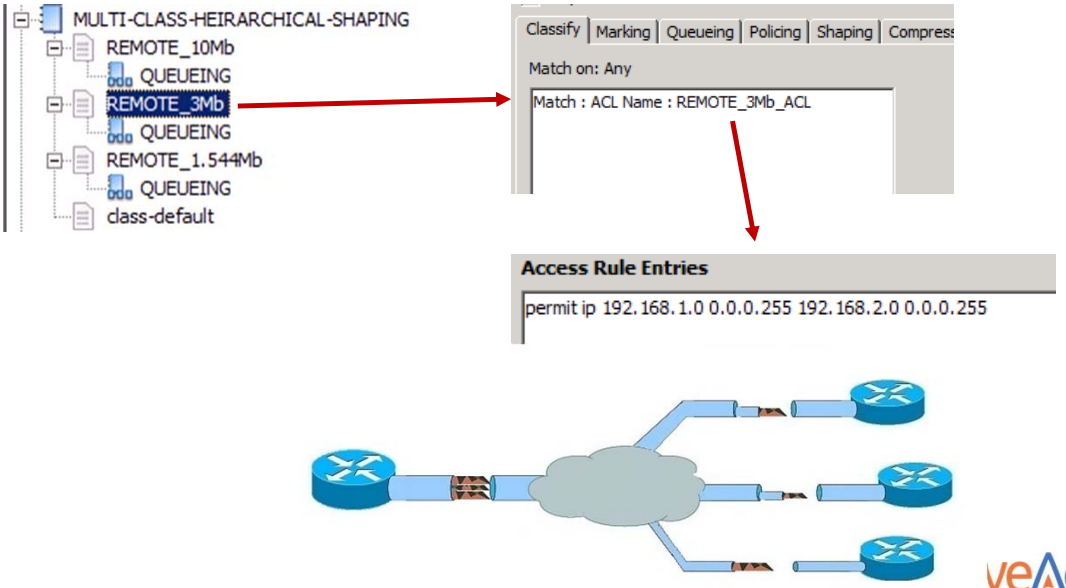
Shaping: Configuration

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



211

Shaping: Configuration



212

Queueing: Selecting Bandwidth Allocations

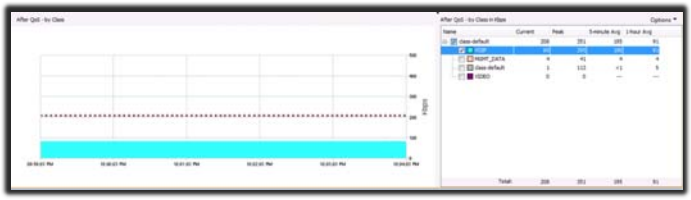
Class Type Cisco Name/ RFC4594 Name	4 Class	8 Class	12 Class
Voice / IP Telephony	≥33%	10%	10%
Interactive Video / Multimedia Conferencing		23%	10%
Streaming Video		10%	10%
Real-Time Interactive			13%
Broadcast Video			10%
Call Signaling	Remaining	2%	2%
IP Routing / Network Control		5%	2%
Network Management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

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

213

Queueing: Understanding Traffic

This is how one voice call looks:



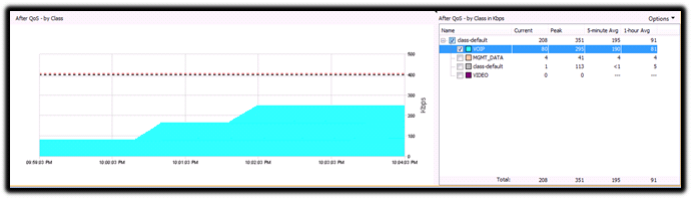
1x G.711 Call is ~82 Kbps
1x G.729 call is ~ 24.6 Kbps

Consistent pps = no burst

214

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

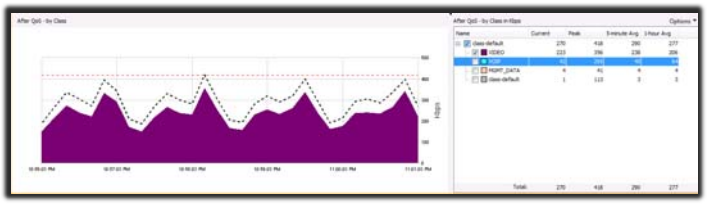
Etc…

No Burst = No Buffer Tuning

215

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	128K	128K	128K	128K	128K	128K

Overprovision Video Queues by 20% & Tune Buffers

Queueing: Understanding Traffic

Know critical apps SLA Targets!

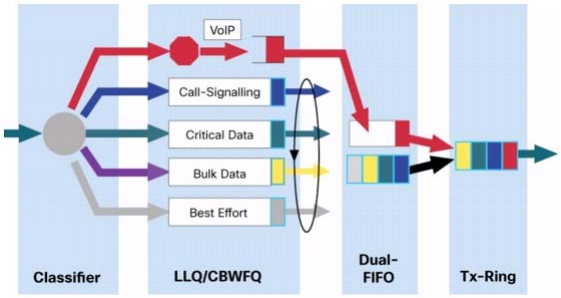
Parameter	VOIP	Traditional Video	HD / Immersive Video
Bandwidth	8-90Kbps	384 -768 kbps + network overhead	1.5 - 12.6 Mbps + network overhead
Latency	150ms	400-450ms	150ms
Jitter	30ms	30-50ms	10ms
Loss	1%	1%	0.05%

Treat with Care!

Queueing: Understanding Traffic

Voice = LLQ /Priority Queue

Video = ?

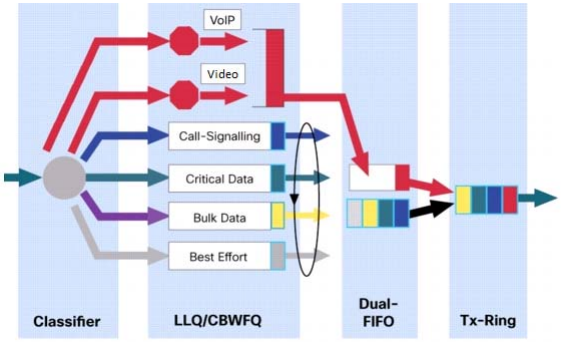


218

Queueing: Understanding Traffic

Voice = Priority Queue/LLQ

Video = Priority Queue/LLQ

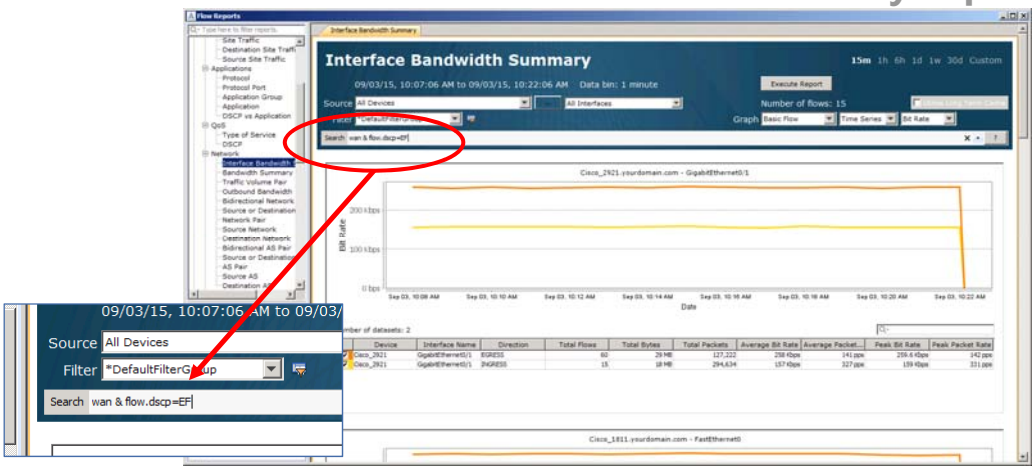


Always put Video in its own unique queue

219

Queueing: Sizing/Capacity Planning

Network > Interface Bandwidth Summary Report

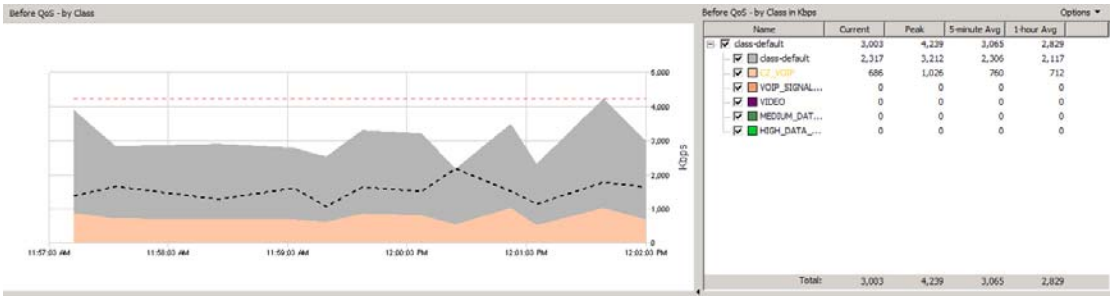


If Classification & Marking are in place, Flow is a great way to do queue sizing

220

Queueing: Sizing/Capacity Planning

Pre-Policy QoS Report is a Great QoS Sizing Report

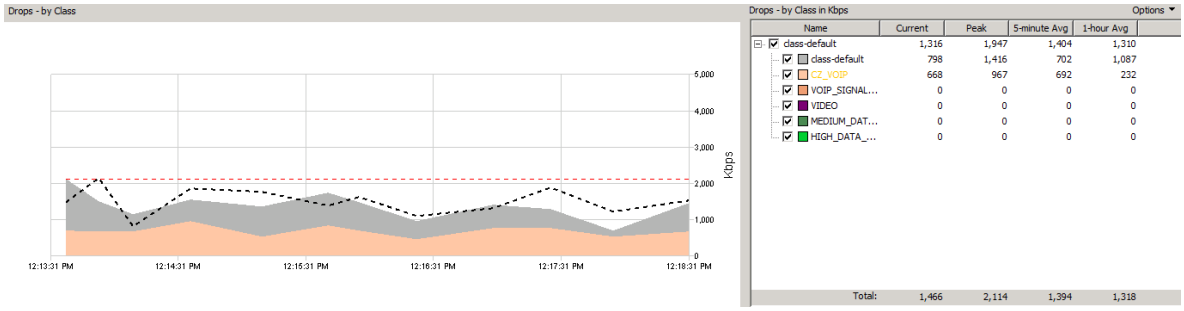


This report shows the volume of bandwidth of each queue before QoS is actually applied

221

Queueing: Capacity Planning

QoS Drop Report can also be a QoS Capacity Report

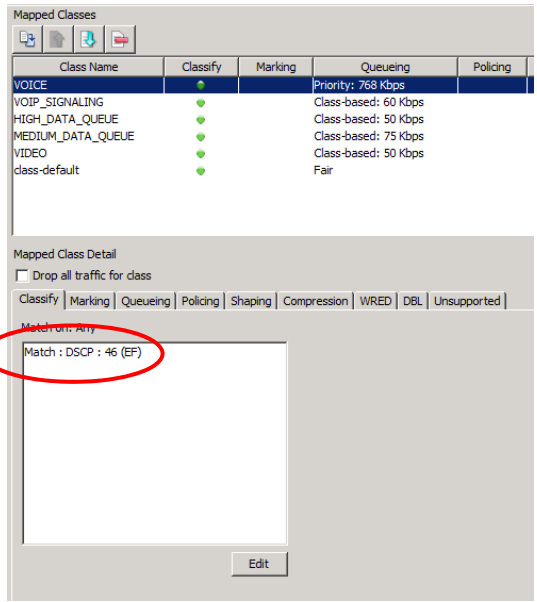


This report shows the volume of traffic dropped after QoS is applied. This can be good for finding gross sizing errors. But is not the whole story, fixing drops may also required buffer tuning too!

222

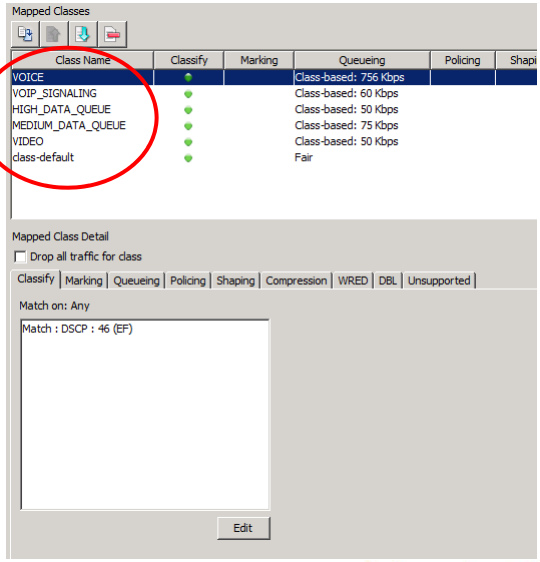
Queueing: Configuration

Match on DSCP



223

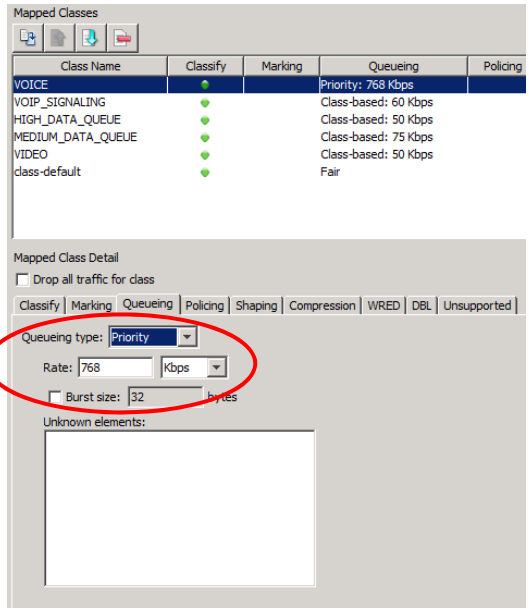
Queueing: Configuration



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.

224

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

225

Lab

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

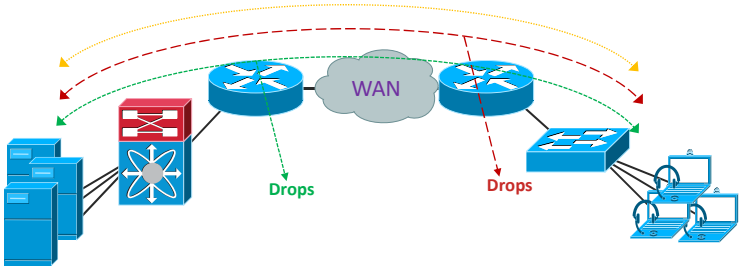
2019Apr01 LiveAction 226

226

2019Apr01 LiveAction™

227

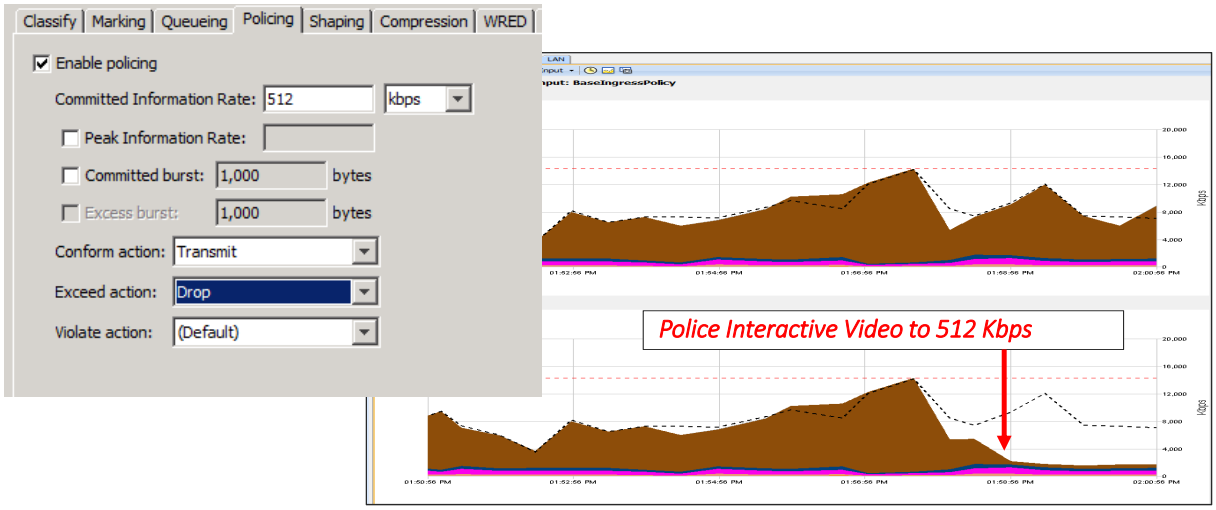
Step 3 –Throttle Traffic (Policing and WRED)



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

228

Policing

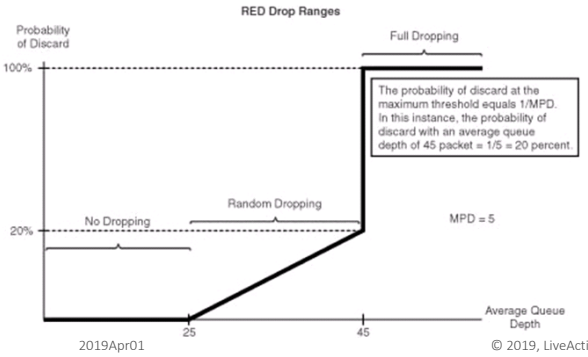


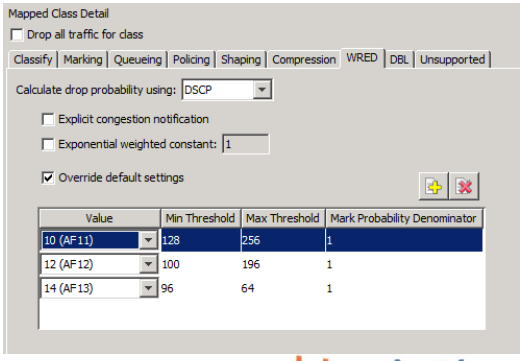
Best done on LAN ingress close to source

229

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

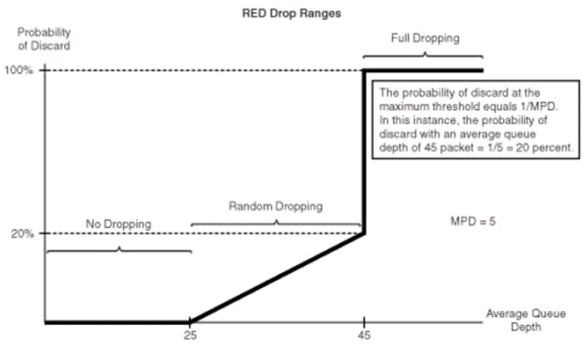


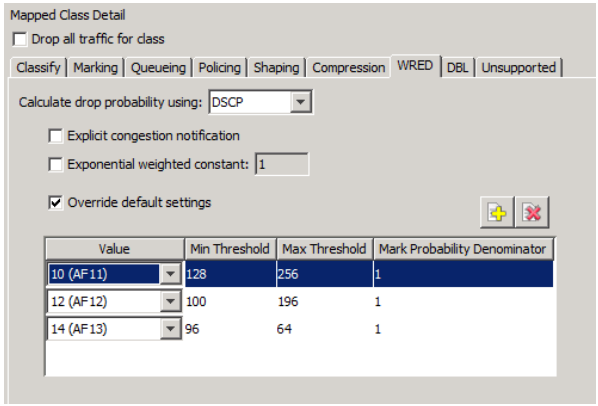


230

WRED - Warning!

- Will cause more drops (harm) than normal, if not tuned correctly
- Typically only effective if multiple DSCP values are in a Queue
- Only 1% of customers are sophisticated enough to use WRED effectively





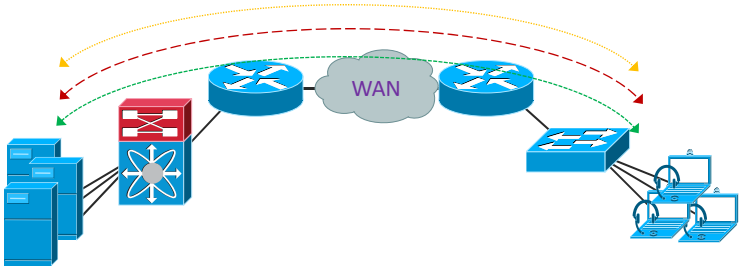
231

Lab

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

LiveAction

Step 4–Buffer Tuning (Advanced)

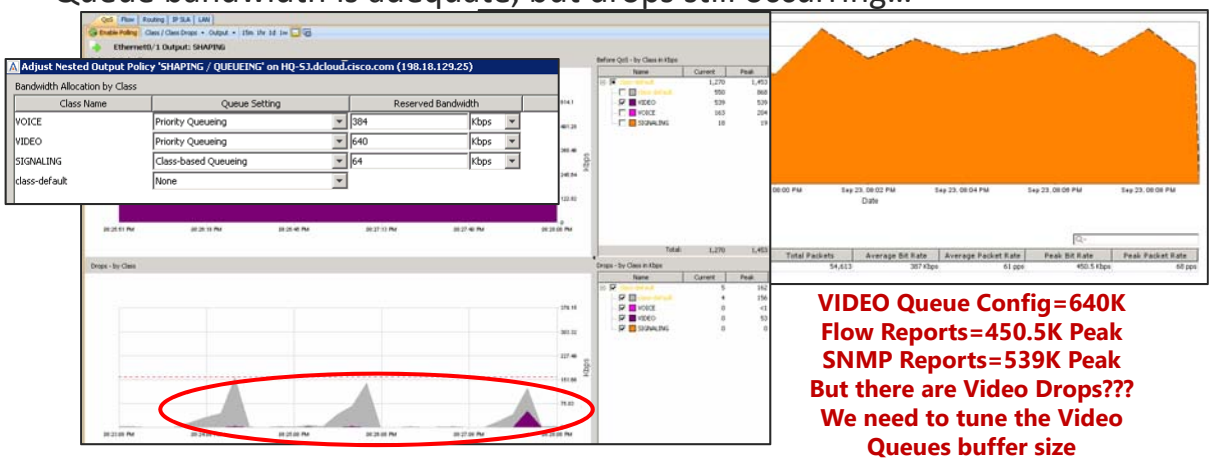


- **Queue-limit –** Buffer size that stores queue data during congestion
- **Priority queue BC –** Token bucket interval that schedules the releases data in priority

234

Buffer Tuning

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



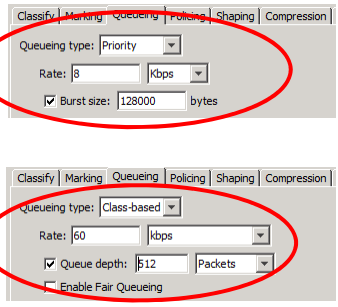
VIDEO Queue Config=640K
Flow Reports=450.5K Peak
SNMP Reports=539K Peak
But there are Video Drops???
We need to tune the Video Queues buffer size

235

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
```



Lab

- Buffer Tuning
  - Video Queue Performance Tuning

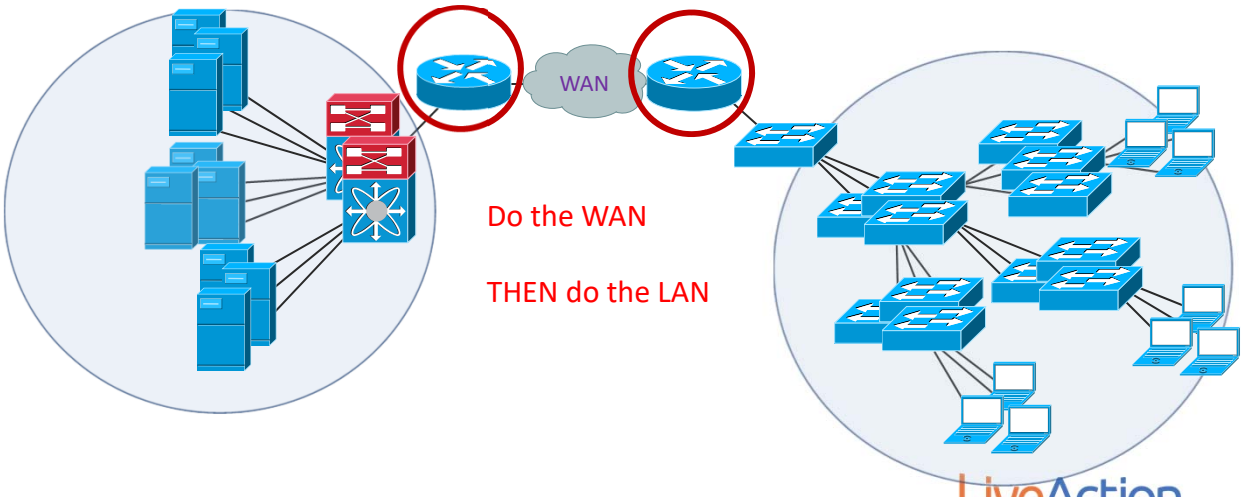
238

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.

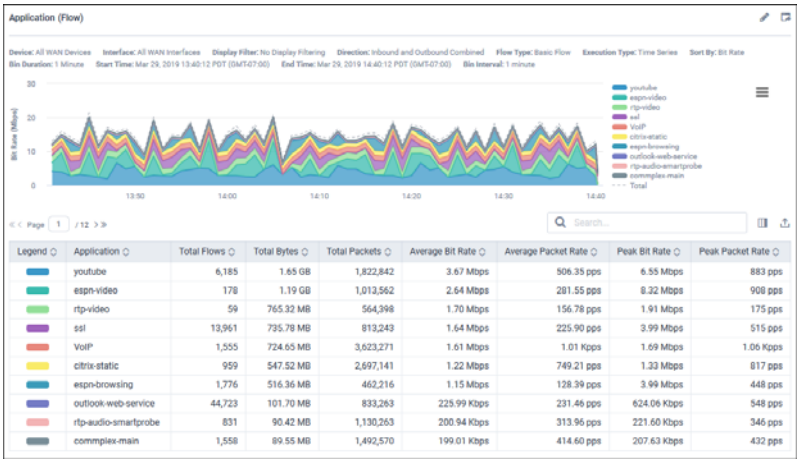
239

Step 1 : Implement QoS in Phases!



240

Step 2 - Use NetFlow Tools to Understand Bandwidth Usage

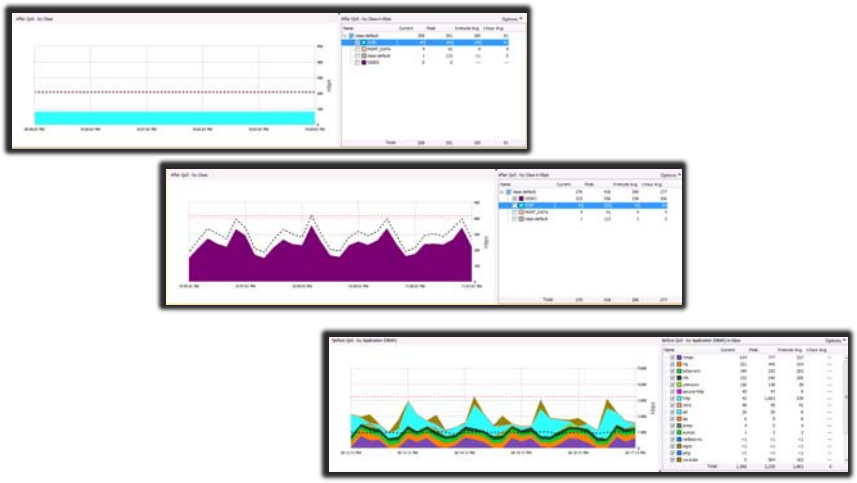


Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	youtube	6,185	1.65 GB	1,822,842	3.67 Mbps	506.35 pps	6.55 Mbps	883 pps
	espn-video	178	1.19 GB	1,013,562	2.64 Mbps	281.55 pps	8.32 Mbps	908 pps
	rtp-video	59	765.32 MB	564,398	1.70 Mbps	156.78 pps	1.91 Mbps	175 pps
	ssl	13,961	735.78 MB	813,243	1.64 Mbps	225.90 pps	3.99 Mbps	515 pps
	VoIP	1,555	724.65 MB	3,623,271	1.61 Mbps	1.01 Kpps	1.69 Mbps	1.06 Kpps
	citrix-static	959	547.52 MB	2,697,141	1.22 Mbps	749.21 pps	1.33 Mbps	817 pps
	espn-browsing	1,776	516.36 MB	462,216	1.15 Mbps	128.39 pps	3.99 Mbps	448 pps
	outlook-web-service	44,723	101.70 MB	833,263	225.99 Kbps	231.46 pps	624.06 Kbps	548 pps
	rtp-audio-smartprobe	831	90.42 MB	1,130,263	200.94 Kbps	313.96 pps	221.60 Kbps	346 pps
	commplex-main	1,558	89.55 MB	1,492,570	199.01 Kbps	414.60 pps	207.63 Kbps	432 pps

***Use minute by minute reporting (no Averaging)**

241

Step 3 - Understand Applications Details



242

Step 4 - Get Business' Buy-In

243

Step 5 - Understand the Network


ISR, ISRG2, ASR1000


Catalyst 2960,3560, 3750, 3850


Catalyst 4500


Catalyst 6500


Nexus 7000

www.cisco.com/go/srnd


CHAPTER 2

Medianet Campus QoS Design 4.0

Overview

With switches, start with SRND4 Auto-QoS where possible

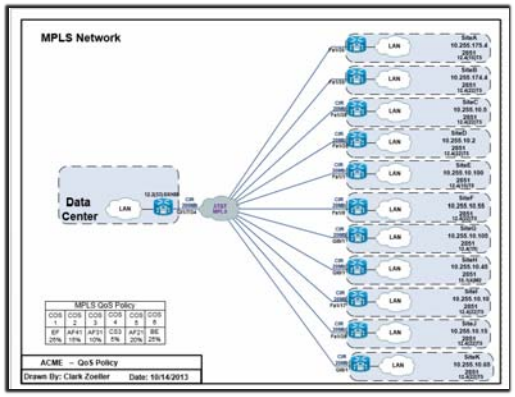
244

Step 6 - Have a plan

Site	Device Name	Device Type	IP Address	IOS Version	Line Card Model(s)	Interface	AT&T CIR	AT&T COS1 (Priority)	AT&T
Louisville	PGS-LOUISVILLE-RTR	CISCO2821	10.255.253.52	C2800NM-IPVOICE-MZ.124-8A	WIC-1DSU-T1-V2 WIC-1ADSL NM-HDV VWIC-1MFT-T1 PVDM-12 PVDM-12	1.5Mbps	1.5Mbps		
Louisville	PGS-LOUISVILLE-RTR	CISCO2921	10.255.253.52	C2900-UNIVERSALK9-MZ.SPA.152-4.M4	HWIC-4T1/E1	3Mbps	3Mbps	20% (600K)	60%
Lexington	PGS-LEXINGTON-RTR	CISCO2821	10.255.253.54	C2800NM-IPVOICE-MZ.124-8A	WIC-1DSU-T1-V2 WIC-1ADSL NM-HDV VWIC-1MFT-T1 PVDM-12 PVDM-12	1.5Mbps	1.5Mbps		
Lexington	PGS-Lexington-RTR	CISCO2921	10.255.253.54	C2900-UNIVERSALK9-MZ.SPA.152-4.M4	HWIC-4T1/E1	3Mbps	3Mbps	20% (600K)	60%
London	PGS-LONDON-RTR	CISCO2821	10.255.253.50	C2800NM-IPVOICE-MZ.124-8A	WIC-1DSU-T1-V2 WIC-1ADSL NM-HDV VWIC-1MFT-T1 PVDM-12 PVDM-12	1.5Mbps	1.5Mbps		
London	PGS-LONDON-RTR	CISCO2921	10.255.253.50	C2900-UNIVERSALK9-MZ.SPA.152-4.M4	HWIC-4T1/E1	3Mbps	3Mbps	20% (600K)	60%
Manchester	PGS-MANCHESTER-3825-R	CISCO3825	10.255.253.65	C3825-IPVOICE-MZ.124-8A	WIC-1DSU-T1-V2 WIC-1DSU-T1-V2 WIC-1DSU-T1-V2 NM-HDV VWIC-1MFT-T1 PVDM-12 PVDM-12 NM-HDV VWIC-1MFT-T1 PVDM-12 PVDM-12	3Mbps	3Mbps		
Manchester	PGS-MACHESTER-RTR	CISCO2921	10.255.253.65	C2900-UNIVERSALK9-MZ.SPA.152-4.M4	HWIC-4T1/E1	4.5Mbps	4.5Mbps	20% (600K)	60%
Jacksonville	PGS-JACKS-2821-RTR	CISCO2821	10.255.253.55	C2800NM-IPVOICE-MZ.124-8A	WIC-1DSU-T1-V2 WIC-1ADSL NM-HDV VWIC-1MFT-T1	1.5Mbps	1.5Mbps		

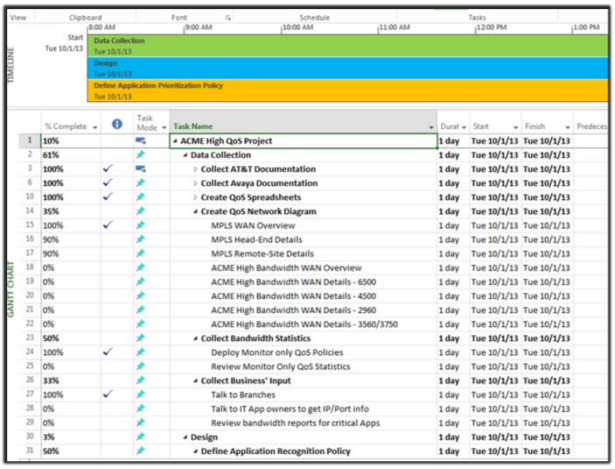
245

Step 6 - Have a plan



246

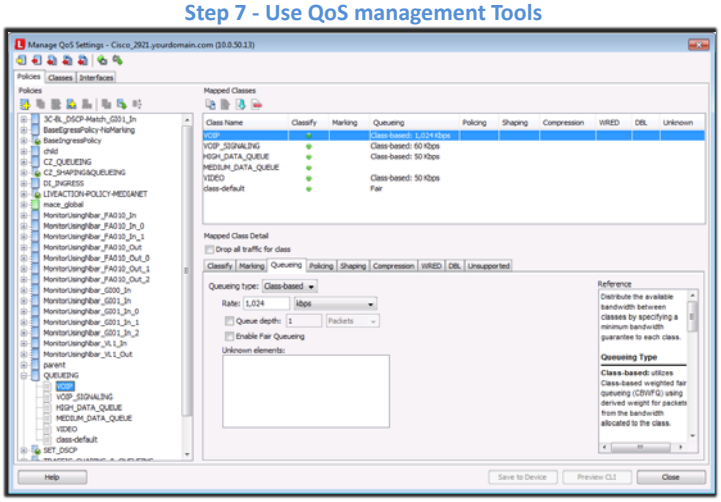
Step 6 - Have a plan



	% Complete	Task Name	Duration	Start	Finish
1	10%	ACME High QoS Project	1 day	Tue 10/1/13	Tue 10/1/13
2	61%	Data Collection	1 day	Tue 10/1/13	Tue 10/1/13
3	100%	Collect AT&T Documentation	1 day	Tue 10/1/13	Tue 10/1/13
6	100%	Collect Avaya Documentation	1 day	Tue 10/1/13	Tue 10/1/13
10	100%	Create QoS Spreadsheets	1 day	Tue 10/1/13	Tue 10/1/13
14	35%	Create QoS Network Diagram	1 day	Tue 10/1/13	Tue 10/1/13
15	100%	MPLS WAN Overview	1 day	Tue 10/1/13	Tue 10/1/13
16	90%	MPLS Head-End Details	1 day	Tue 10/1/13	Tue 10/1/13
17	90%	MPLS Remote-Site Details	1 day	Tue 10/1/13	Tue 10/1/13
18	0%	ACME High Bandwidth WAN Overview	1 day	Tue 10/1/13	Tue 10/1/13
19	0%	ACME High Bandwidth WAN Details - 6500	1 day	Tue 10/1/13	Tue 10/1/13
20	0%	ACME High Bandwidth WAN Details - 4500	1 day	Tue 10/1/13	Tue 10/1/13
21	0%	ACME High Bandwidth WAN Details - 2960	1 day	Tue 10/1/13	Tue 10/1/13
22	0%	ACME High Bandwidth WAN Details - 3560/3750	1 day	Tue 10/1/13	Tue 10/1/13
23	50%	Collect Bandwidth Statistics	1 day	Tue 10/1/13	Tue 10/1/13
24	100%	Deploy Monitor only QoS Policies	1 day	Tue 10/1/13	Tue 10/1/13
25	0%	Review Monitor Only QoS Statistics	1 day	Tue 10/1/13	Tue 10/1/13
26	33%	Collect Business' Input	1 day	Tue 10/1/13	Tue 10/1/13
27	100%	Talk to Branches	1 day	Tue 10/1/13	Tue 10/1/13
28	0%	Talk to IT App owners to get IP/Port info	1 day	Tue 10/1/13	Tue 10/1/13
29	0%	Review bandwidth reports for critical Apps	1 day	Tue 10/1/13	Tue 10/1/13
30	3%	Design	1 day	Tue 10/1/13	Tue 10/1/13
31	50%	Define Application Recognition Policy	1 day	Tue 10/1/13	Tue 10/1/13

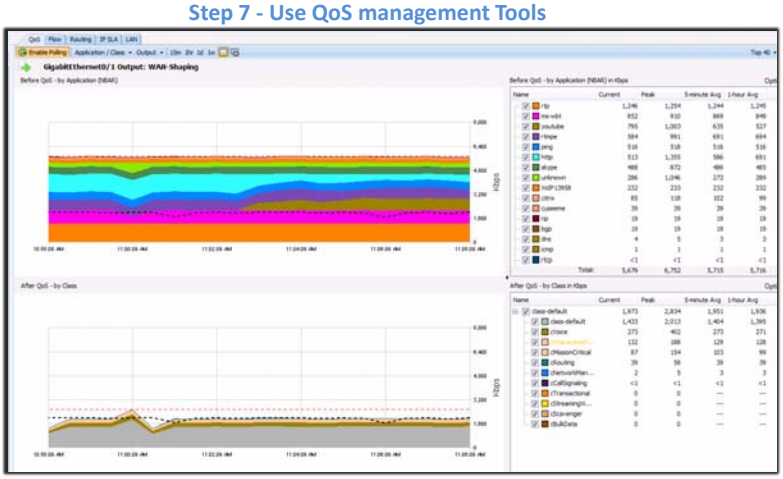
247

Step 7 - Use QoS management Tools



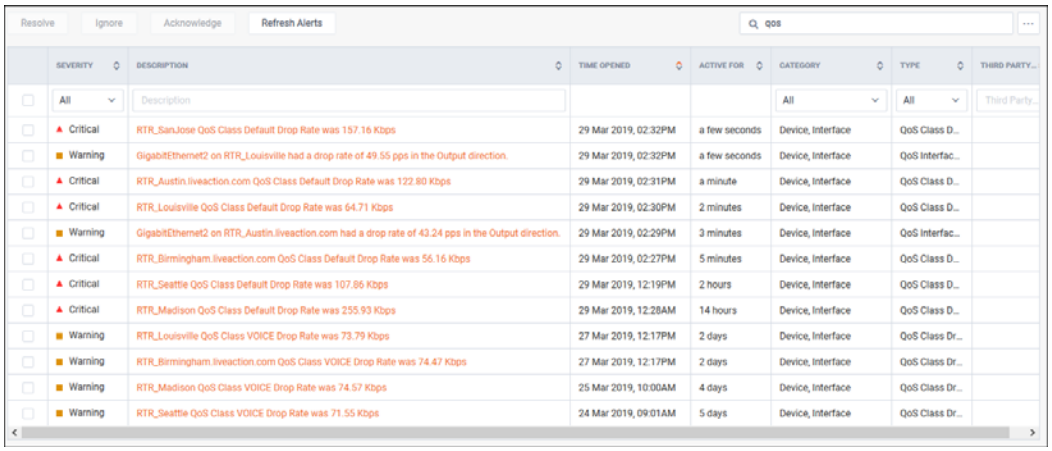
248

Step 7 - Use QoS management Tools



249

Step 7 - Use QoS management Tools

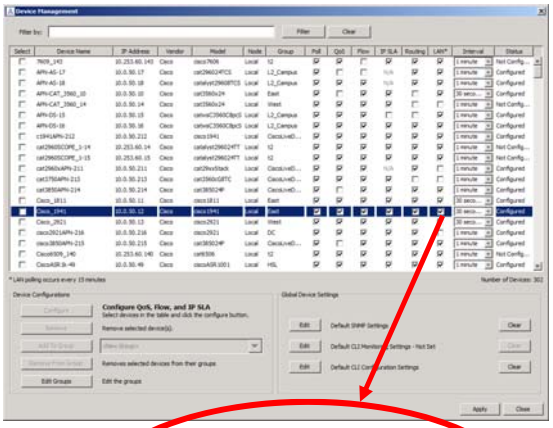


250

SNMP Polling Interval

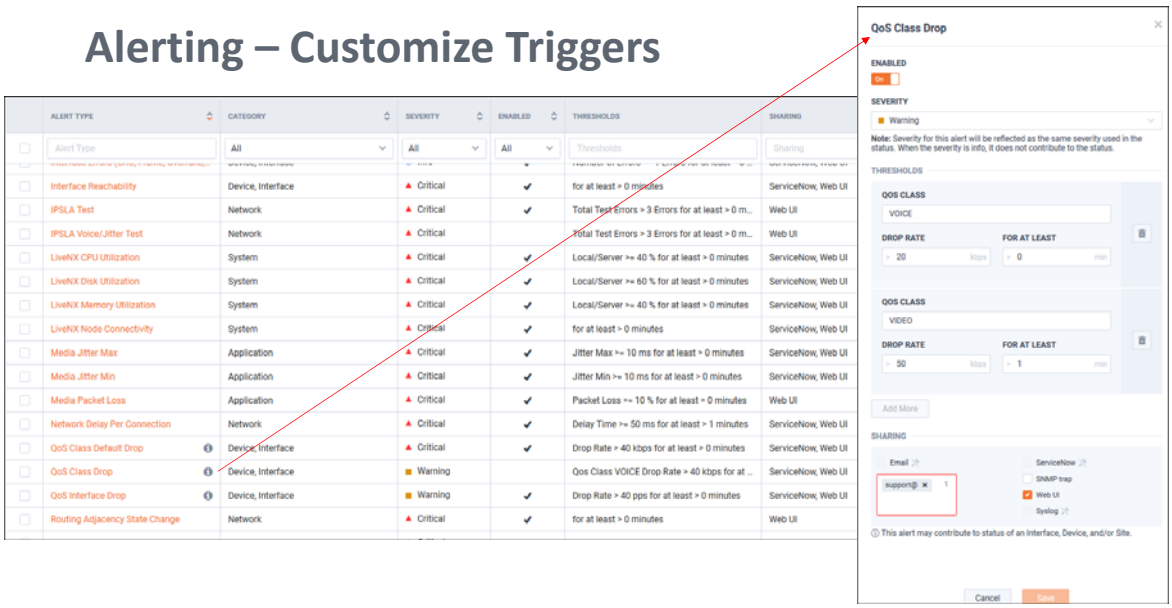
LiveAction Recommends

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



251

Alerting – Customize Triggers



252

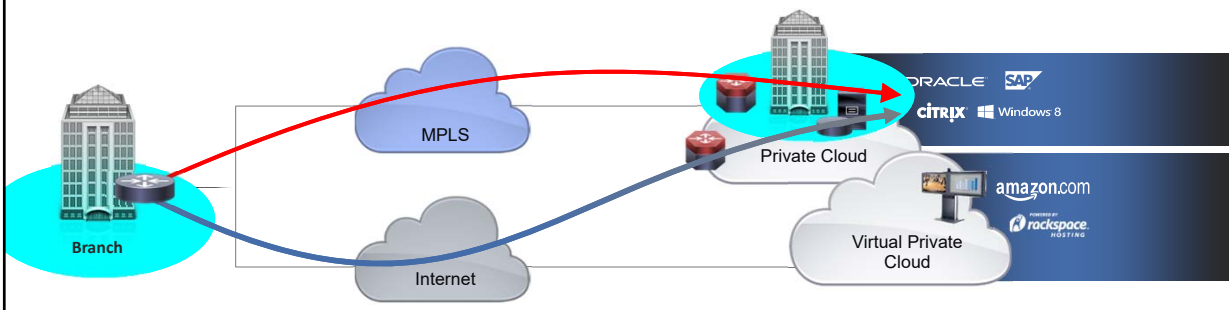
Finish the Labs…

253

254

255

WHY IWAN/SDWAN?



- Fully utilize WAN bandwidth – seamlessly load-balance traffic circuits on backup circuits
- Maximize application performance – routing based on network performance

2019Apr01 LiveAction 256

256

LiveAction LiveNX for IWAN/SDWAN Management

How Can LiveAction Help Manage the SD-WAN Environment?

- **Baseline network and application performance**
- **Monitor QoS performance**
- **Visualize and mitigate application issues with QoS graphical control (w/NBAR)**
- **Visualize PfR intelligent path control so network admin can visually validate how PfR works**
- **Accelerate troubleshooting of network brownouts**
  - What caused the brown-out?
  - How PfR reroutes traffic and protects application performance during the brown-out?
  - Which applications are affected by a brown-out?
  - Which service provider is having a brown-out issue?
  - What traffic is moved from one provider to another?
- **Graphically and easily define QoS policies so PfR can use them to load balance or protect application performance during a fail over**

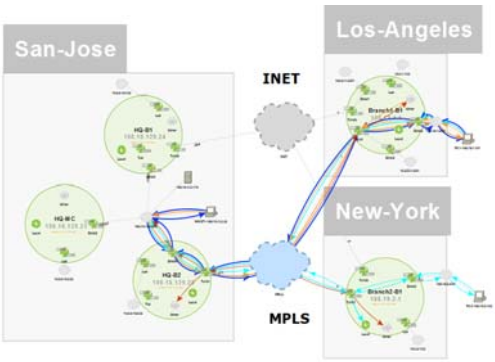
2019Apr01 LiveAction 257

257

IWAN Monitoring: CLI vs. LiveNX

CLI

LiveNX



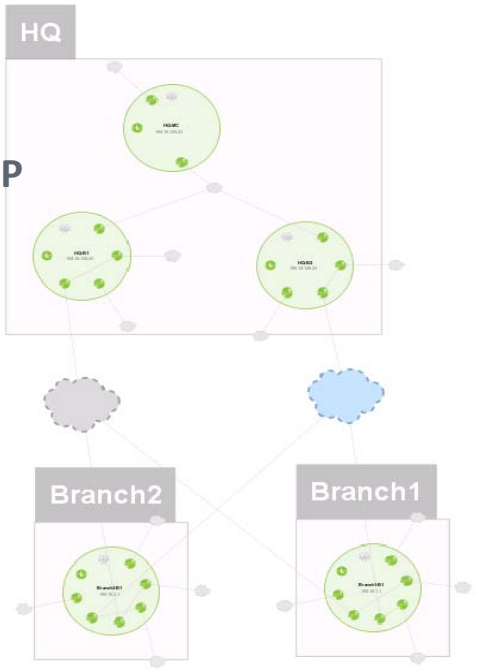
2019Apr01 258

258

259

Configure SD-WAN devices in LiveNX

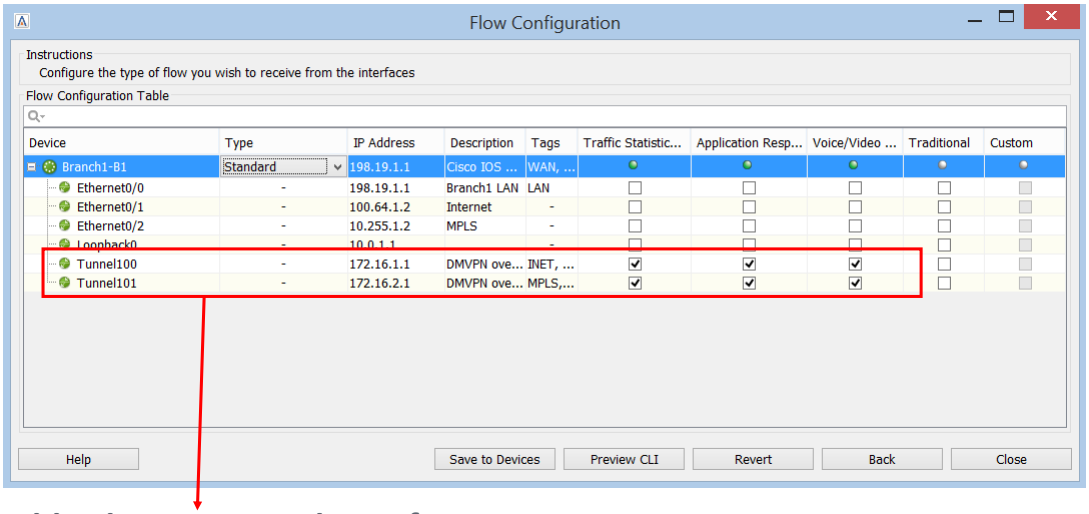
- Add all MCs and BRs routers
- Add routers using their PfR Loopback IP
- Add all user created Tunnel Interfaces
- Add PfR Loopback interfaces
- Add all physical WAN interfaces
- (optional) Add LAN interfaces



2019Apr01 260

260

Flow Configuration



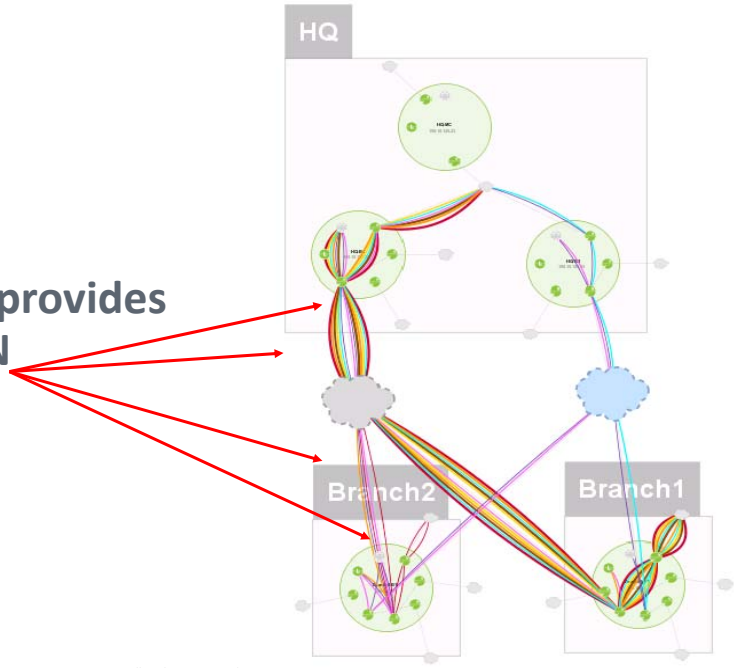
- Enable Flow on Tunnel Interfaces
- (optional) Enable Flow on DIA interfaces

2019Apr01 261

261

Flow Configuration

Flow on only Tunnels still provides complete visibility of WAN



2019Apr01 262

262

Ensure that PfRv3 NetFlow is Enabled

- Please ensure that PfRv3 NetFlow is enabled to send performance updates to LiveNX.
- Enabling the “collector” command at the Hub Master Controller will propagate the setting throughout the domain automatically.

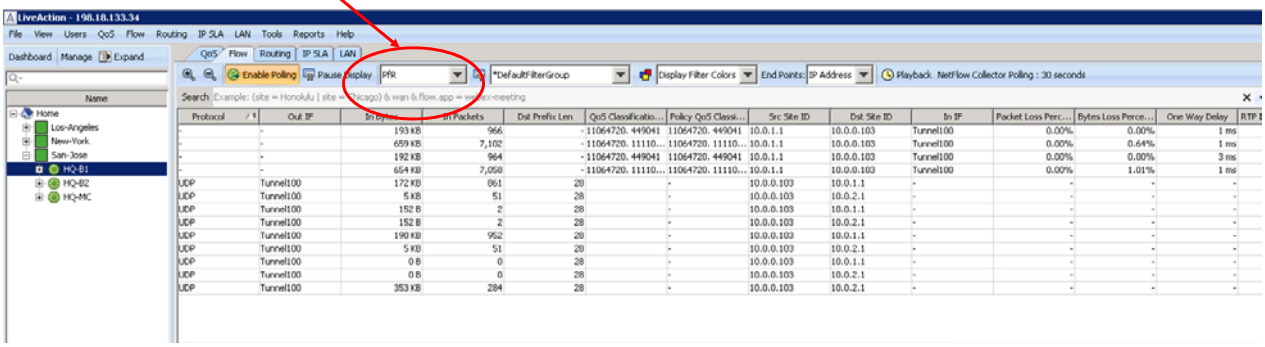
```
domain <DOMAIN>
 vrf default
  master hub
   source-interface Loopback0
   collector <LiveNX-IP-Address> port 2055
```

2019Apr01 263

263

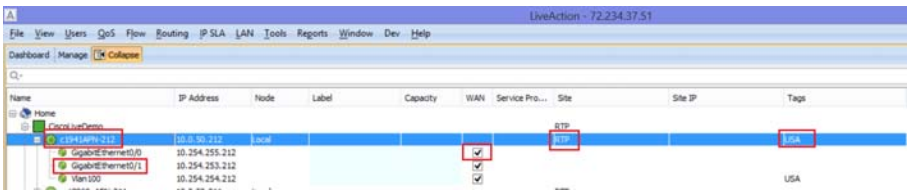
PfRv3 Flow

PfR log data is sent to LiveNX as Flow information



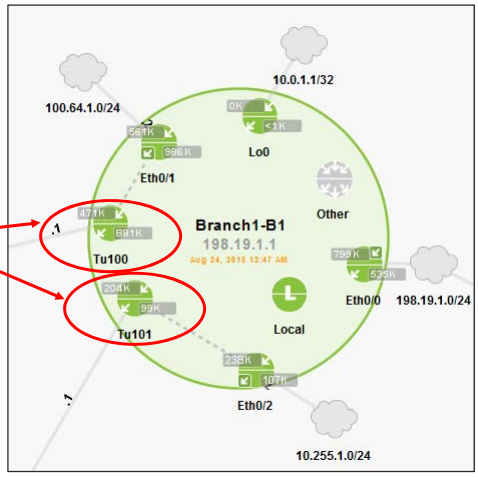
Network Semantics

- LiveNX network semantics to better understand and troubleshoot your network.
- Identify:
  - Group
  - WAN links
  - Label
  - Capacity
  - Service Providers
  - Sites and Site IP settings
  - Device and Interface Tags
- Usage: Search, Reporting, Dashboard



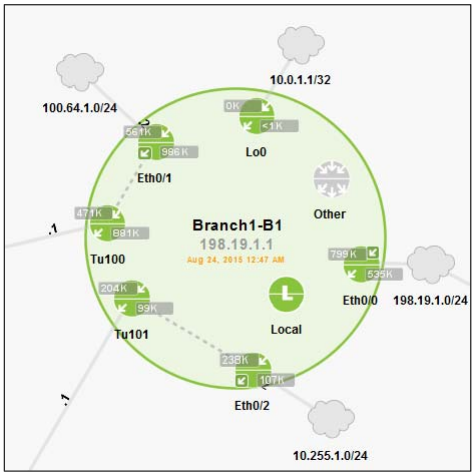
Interface Semantics

- Interface Semantics
  - WAN Tag
  - Label
  - Capacity of Link (Example: 10Mbps)
  - Service Provider (Example: Sprint or AT&T)
  - Interface Tags – User Defined

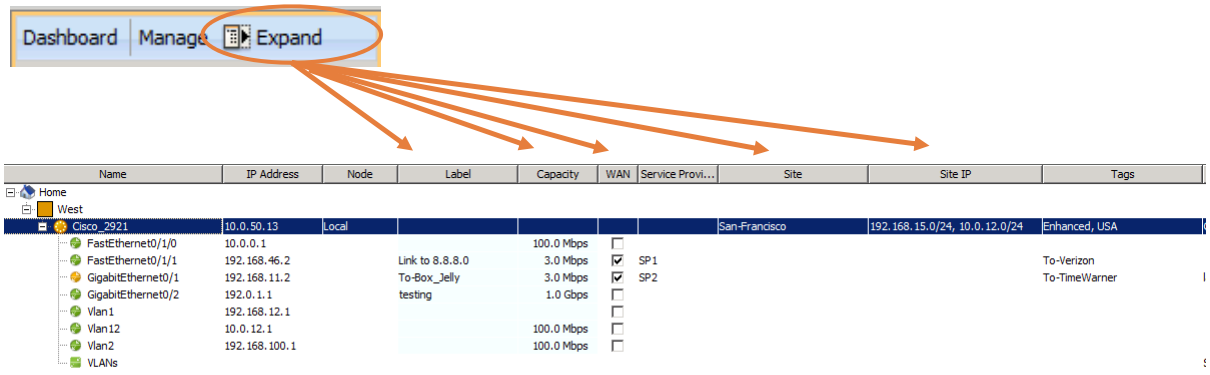


Device Semantics

- Group – to group devices together (Example: West)
- Site (Example: Los-Angeles)
  - Datacenter tag
- Site IP settings
  - Example: 198.19.1.0/24, 10.0.1.1/32
- Device Tags – User Defined



Network Semantics



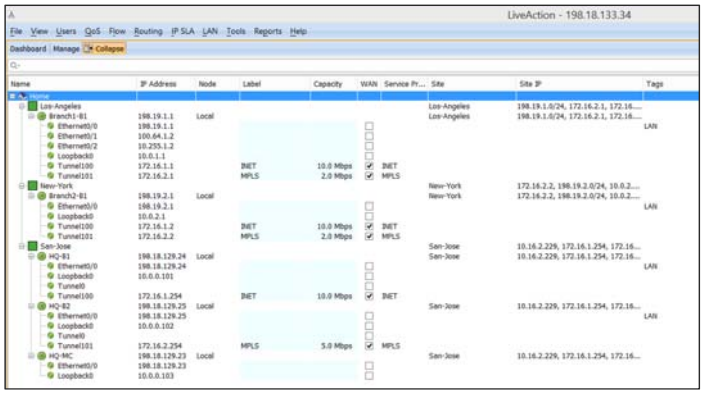
Label, Capacity, WAN, Service Provider, Site, Site IP

LiveAction

268

Network Semantics – AND!!!

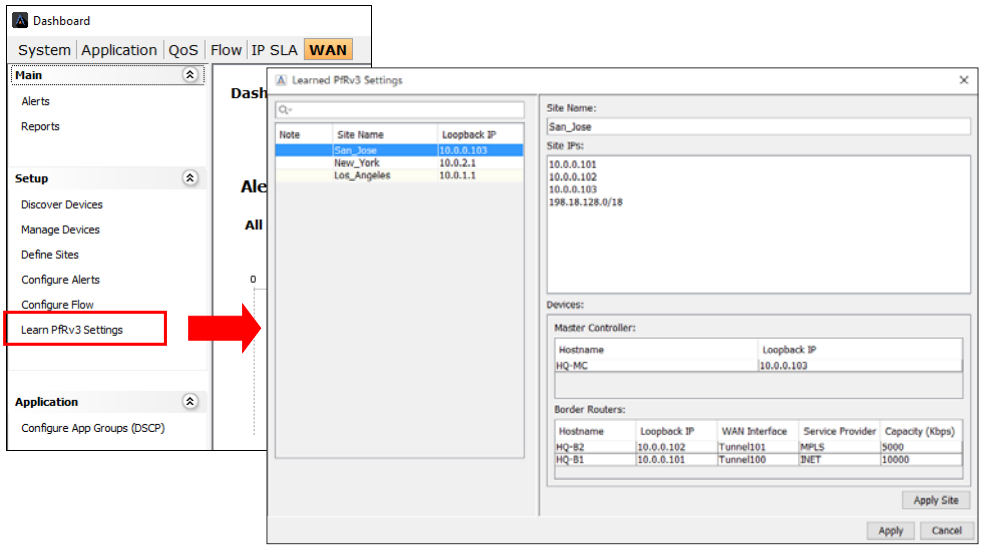
- LiveNX will automatically populate semantics values!!!
  - Rapid Device Discovery / Auto-Semantic Discovery
  - Associate devices to sites, link capacity, site IP mapping, service provider, etc. and auto populates LiveNX so you can be up and using the platform faster.



LiveAction

269

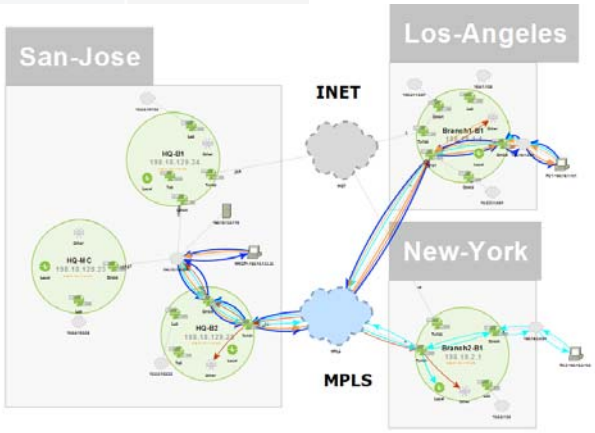
Another way to Setup the Semantics? PfRv3



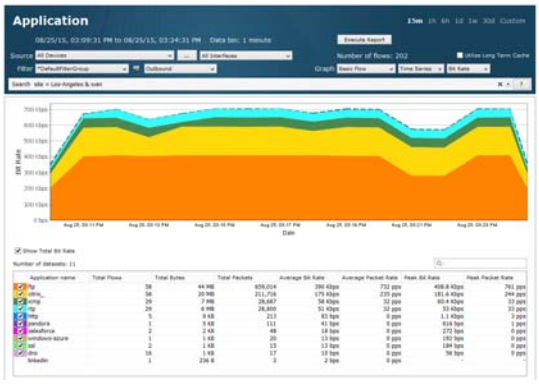
270

Network Semantic Usage Examples

Search sp = MPLS



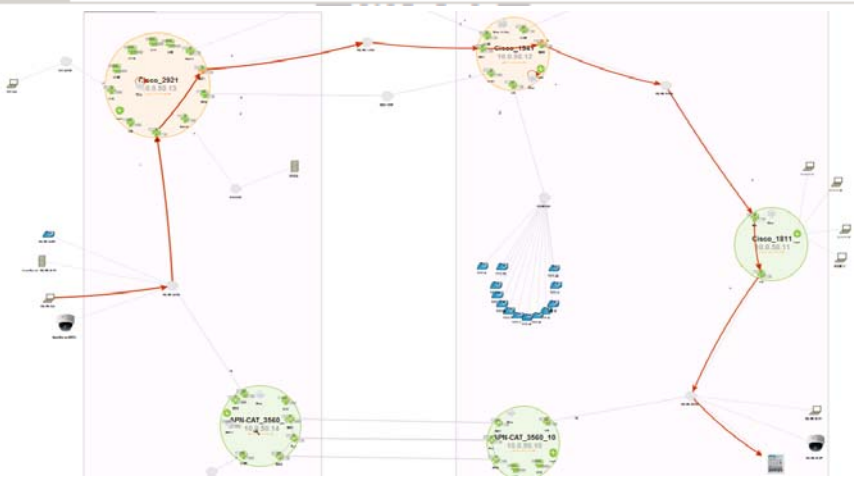
Search site = Los-Angeles & wan



271

Semantic Data – Example 1

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



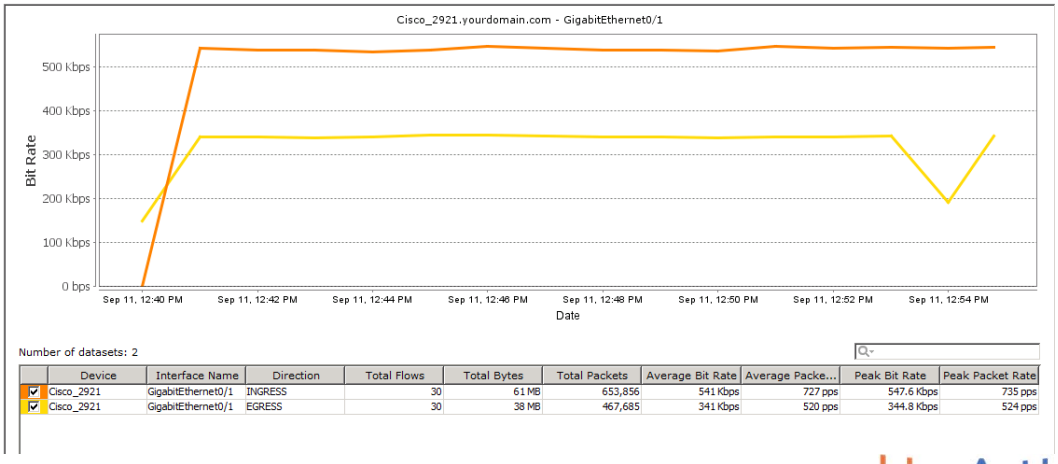
2019Apr01

LiveAction

272

Semantic Data – Example 2

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



Number of datasets: 2

Device	Interface Name	Direction	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packe...	Peak Bit Rate	Peak Packet Rate
Cisco_2921	GigabitEthernet0/1	INGRESS	30	61 MB	653,856	541 Kbps	727 pps	547.6 Kbps	735 pps
Cisco_2921	GigabitEthernet0/1	EGRESS	30	38 MB	467,685	341 Kbps	520 pps	344.8 Kbps	524 pps

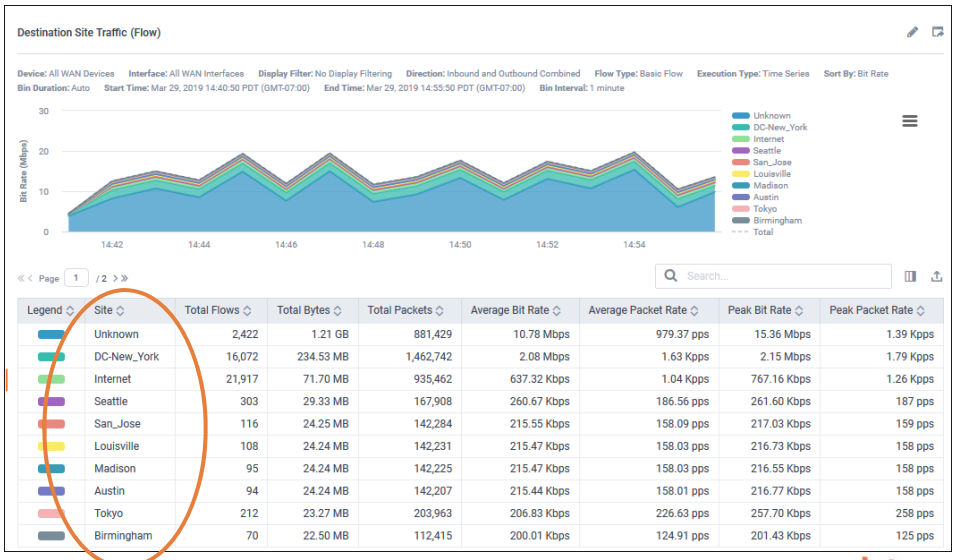
LiveAction

2019Apr01

273

273

Semantic Data – Example 3



Legend	Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	Unknown	2,422	1.21 GB	881,429	10.78 Mbps	979.37 pps	15.36 Mbps	1.39 Kpps
	DC-New_York	16,072	234.53 MB	1,462,742	2.08 Mbps	1.63 Kpps	2.15 Mbps	1.79 Kpps
	Internet	21,917	71.70 MB	935,462	637.32 Kbps	1.04 Kpps	767.16 Kbps	1.26 Kpps
	Seattle	303	29.33 MB	167,908	260.67 Kbps	186.56 pps	261.60 Kbps	187 pps
	San_Jose	116	24.25 MB	142,284	215.55 Kbps	158.09 pps	217.03 Kbps	159 pps
	Louisville	108	24.24 MB	142,231	215.47 Kbps	158.03 pps	216.73 Kbps	158 pps
	Madison	95	24.24 MB	142,225	215.47 Kbps	158.03 pps	216.55 Kbps	158 pps
	Austin	94	24.24 MB	142,207	215.44 Kbps	158.01 pps	216.77 Kbps	158 pps
	Tokyo	212	23.27 MB	203,963	206.83 Kbps	226.63 pps	257.70 Kbps	258 pps
	Birmingham	70	22.50 MB	112,415	200.01 Kbps	124.91 pps	201.43 Kbps	125 pps

274

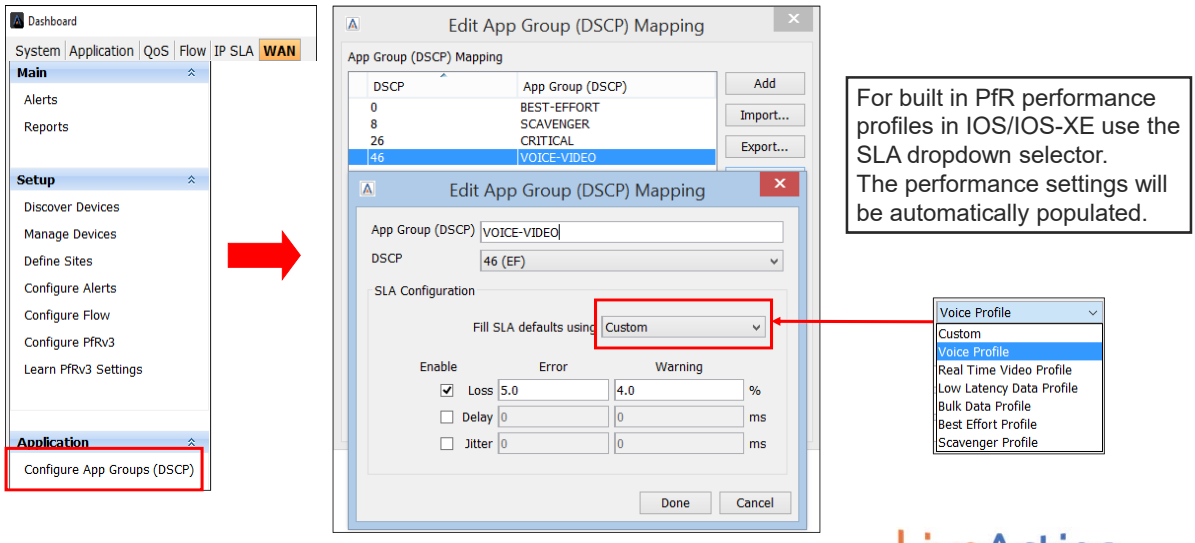
Semantic Data – Example 4

Define Application Groups (DSCP)

- LiveNX allows customers to define application groups to align with DSCP settings within their network so that the WAN-PfR dashboard or drill-down reports can show application names instead of DSCP values.
- This is done by selecting “Configure App Groups (DSCP)” off the WAN-PfR dashboard or under “Tools”, “Manage App Groups (DSCP)”.

276

Define Application Groups (DSCP)



For built in PfR performance profiles in IOS/IOS-XE use the SLA dropdown selector. The performance settings will be automatically populated.

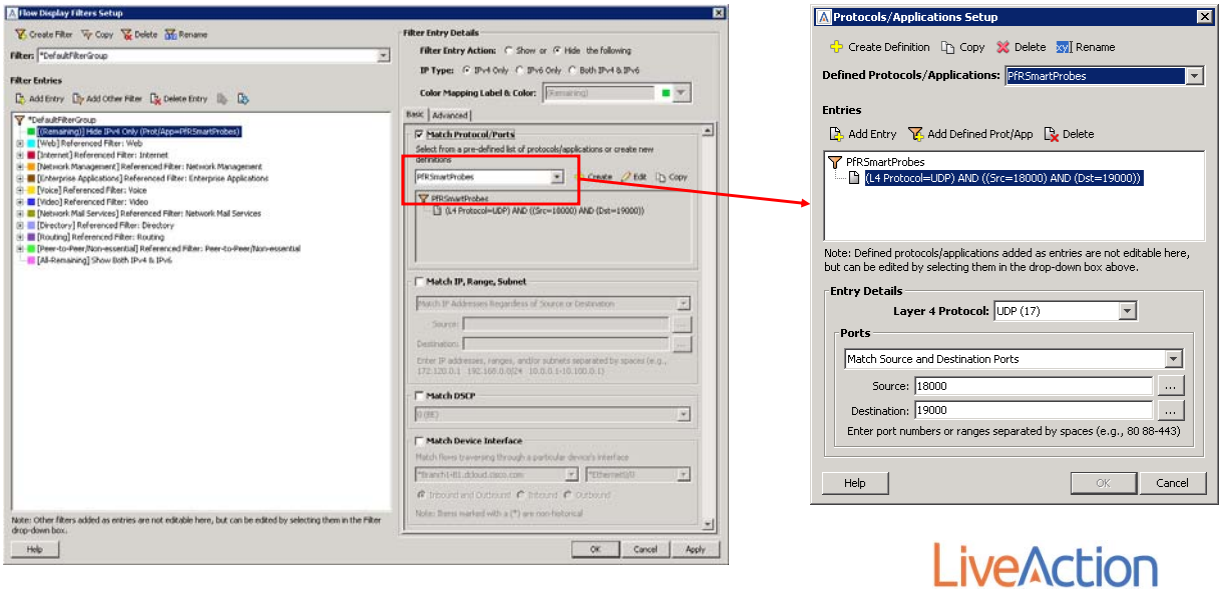
277

Filter Traffic to Visualize Path Changes

- PfRv3 uses smartprobes to determine the performance of various service provider links. These probes may add clutter on the LiveNX topology view, since PfR will create corresponding smartprobes for every traffic class learned.
- Smartprobes use the following ports by default:
  - Source port: 18000
  - Destination port: 19000
- Hiding the smartprobe traffic allows the network engineer to focus his/her attention on the user application traffic.

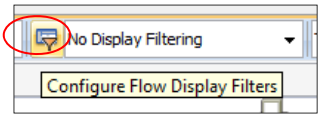
278

Filter PfR Smart Probe data

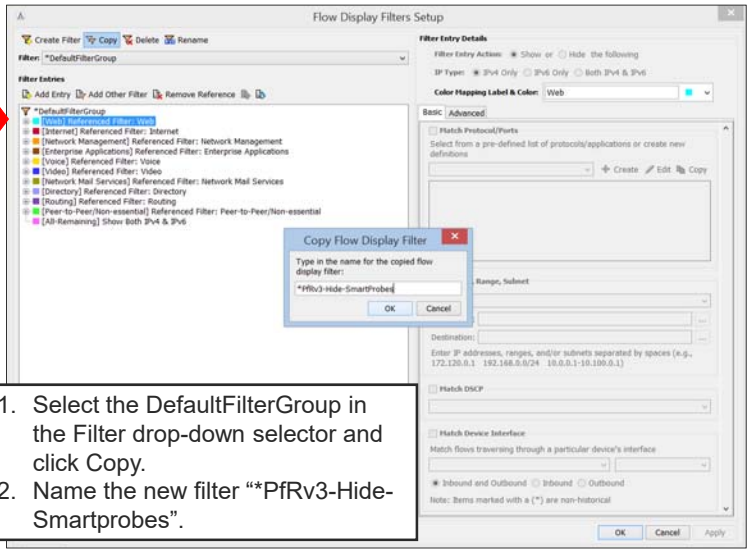


279

Create a Custom Filter to Hide Smartprobes



Click on the Configure Flow Display Filters button

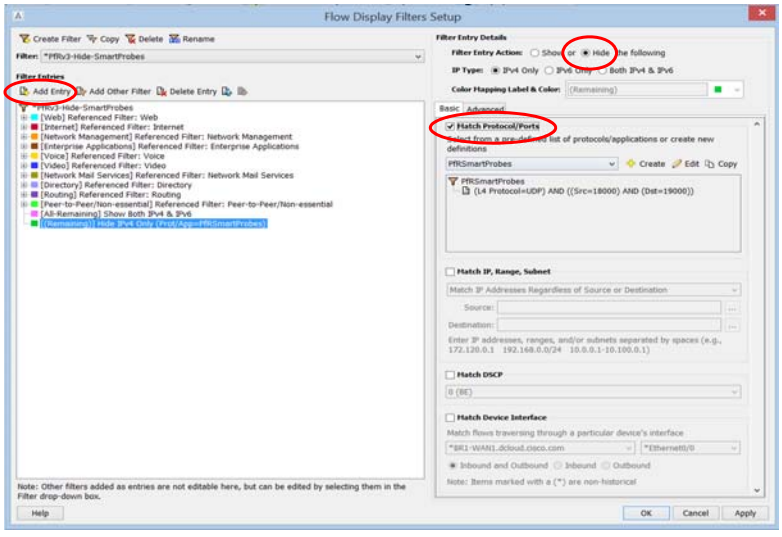


1. Select the DefaultFilterGroup in the Filter drop-down selector and click Copy.
2. Name the new filter "*PfRv3-Hide-Smartprobes".

280

Create a Custom Filter to Hide Smartprobes

1. Click "Add Entry".
2. In the upper right-hand corner of the dialog select "Hide" in the "Filter Entry Action:" section.
3. Click the checkbox to "Match Protocol/Ports" and click "Create" to add a definition.
4. Name the new definition "PfRSmartProbes" and click "OK".

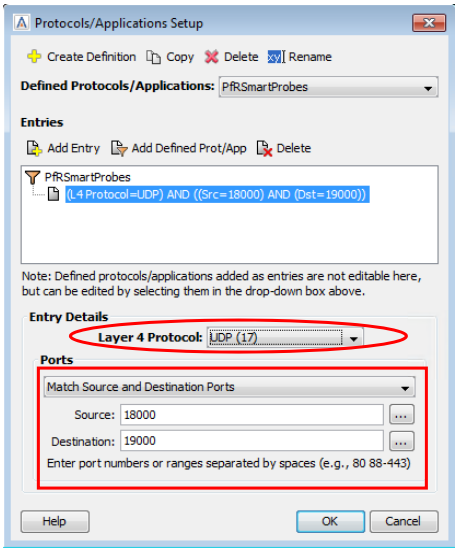


281

Create a Custom Filter to Hide Smart Probes

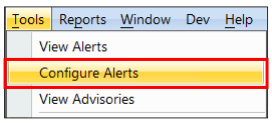
1. In the Protocols/Applications Setup dialog. Set the "Layer 4 Protocol" to "UDP (17)".
2. Under the "Ports" settings choose "Match Source and Destination Ports" from the drop-down menu.
3. Set the "Source" port to "18000" and the "Destination" port to "19000" and click "OK".

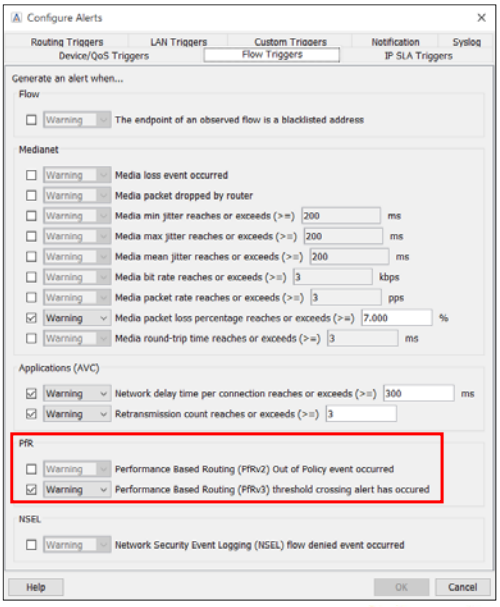
"Note: These are the default ports for the smartprobes. If you change the default settings, please set the port numbers accordingly."



282

Set PfRv3 Alerts





283

IWAN/SDWAN Cheat Sheet

- Validate they used the loopback interface for management on all IWAN routers and MC too (same loopback as PfR's Router ID)
- Manage the loopback, tunnels, physical wan interfaces minimally (easiest way in bulk is export/import the config via CSV)
- Do not manage Tunnel 0
- Check tunnel interfaces' MTU, if it is set to 1400, then set "snmp-server packetsize 1372"
- Enable FnF on Tunnel interfaces
- Set pollers to 30 seconds on routers (switches stay at 1 minute)
- Have them provide you a show run of the domain MC "show run | sec domain"
- Validate collector command is set up on the MC
- Validate that PfR flow is being received
- You set up the PfR application groups from the PfR dashboard
- Go to alerts and check the flow tab and make sure that PfRv3 is ticked, go to the notification tab and make sure in-application alerts are active
- Learn PfR semantics from the PfR dashboard
- Update *DefaultFilterGroup to hide Pfr Smartprobe

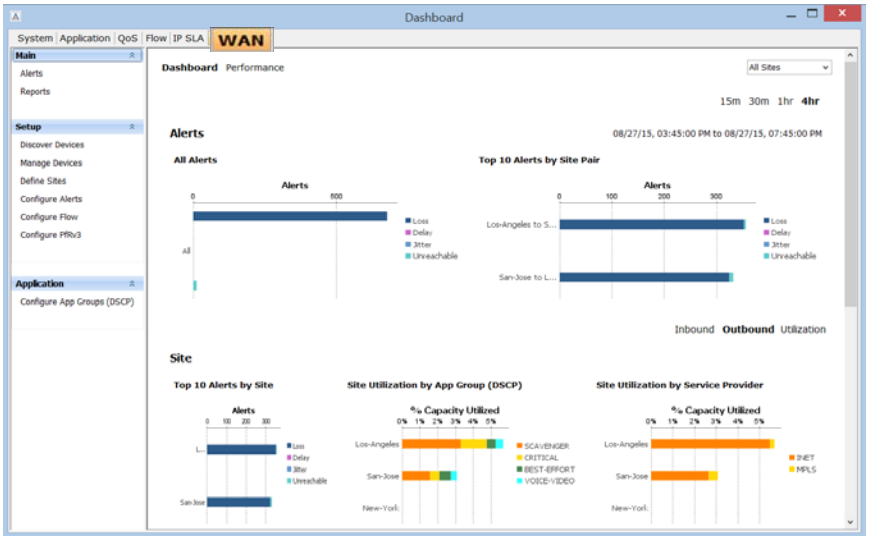
284

LAB: SD-WAN Deployment

285

286

LiveNX - SD-WAN Dashboard



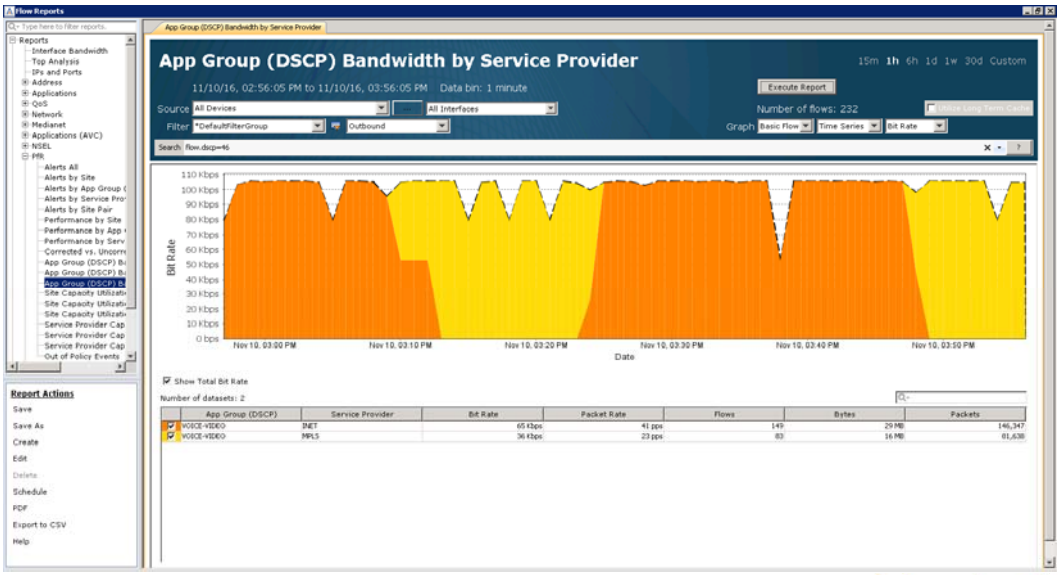
287

LiveNX - SD-WAN Dashboard - Performance

LiveAction

288

LiveNX - SD-WAN Reporting

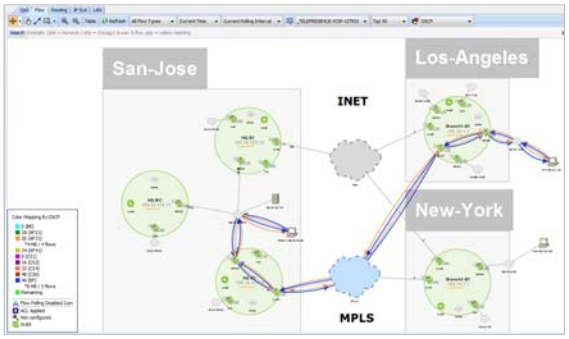


LiveAction

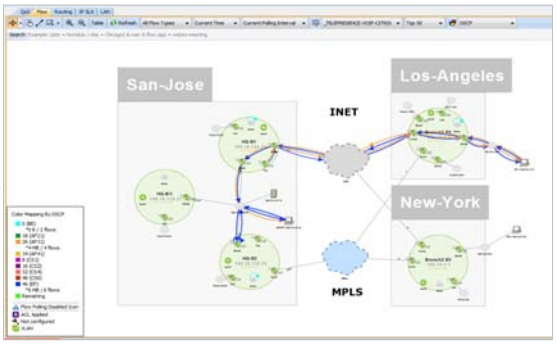
289

LiveNX - SD-WAN Visualization

Before Brown-Out
High Priority Traffic over MPLS Path



After Brown-Out
High Priority Traffic Over INET Path

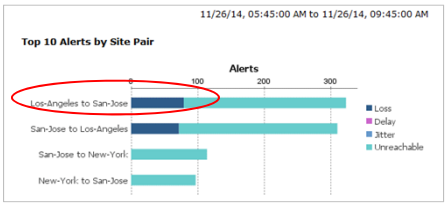


2019Apr01 290

290

LiveNX - Diagnosing a Brown-Out Issue

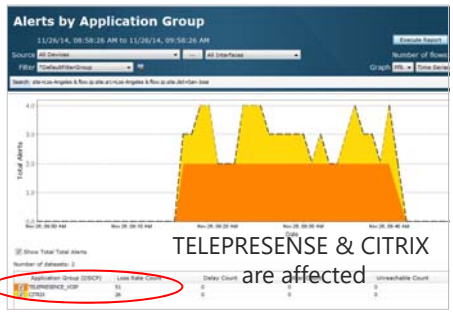
1



Dashboard Shows Loss From LA->SJC

2

3



4

2019Apr01 291

291

How can LiveNX Help Manage the SD-WAN Environment?

- Help select pilot sites before SD-WAN deployment
- Baseline network and application performance
- Monitor QoS performance
- Visualize SD-WAN intelligent path control so network admin can visually validate how SD-WAN works
- Accelerate troubleshooting of network brownouts
  - What caused the brown-out?
  - How SD-WAN reroutes traffic and protects application performance during the brown-out?
  - Which applications are affected by a brown-out?
  - Which service provider is having a brown-out issue?
  - What traffic is moved from one provider to another?

292

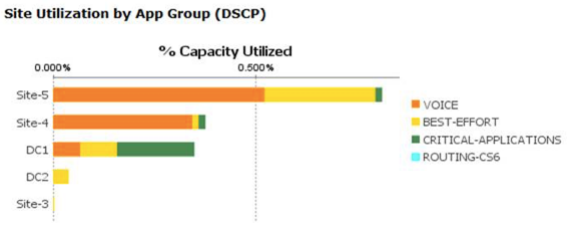
SD-WAN Pre-deployment

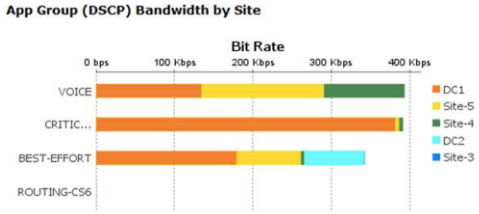
Pick Pilot Sites

- Based on Utilization
- Based on the type of applications

293

WAN Dashboard

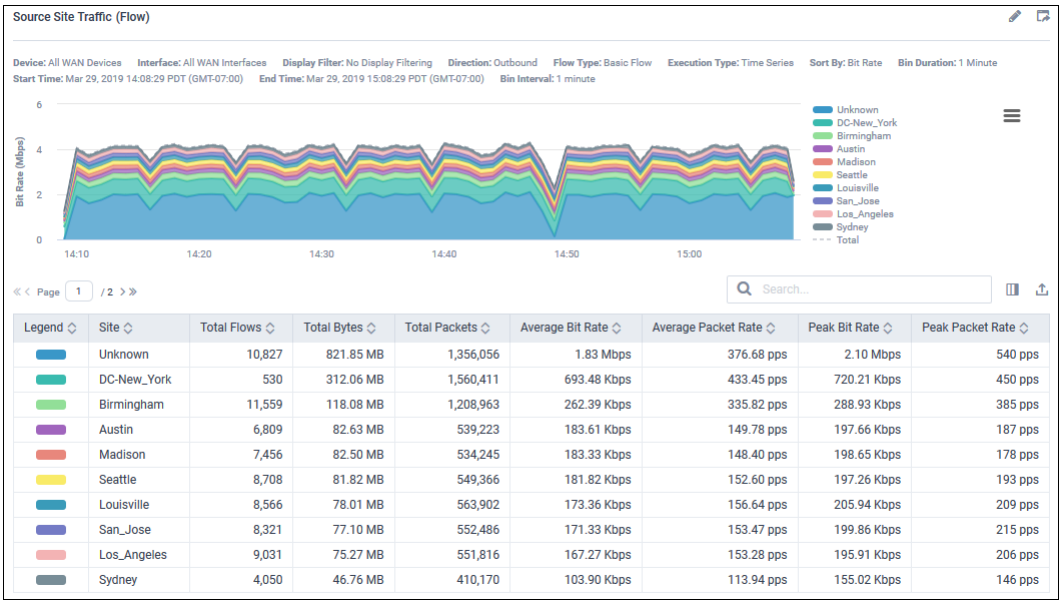




- Based off of utilization (% capacity), Site-5 is using the most resources
- Voice is also being utilized the most.

- Which applications are taking up the most bandwidth
- What is the site breakdown per application

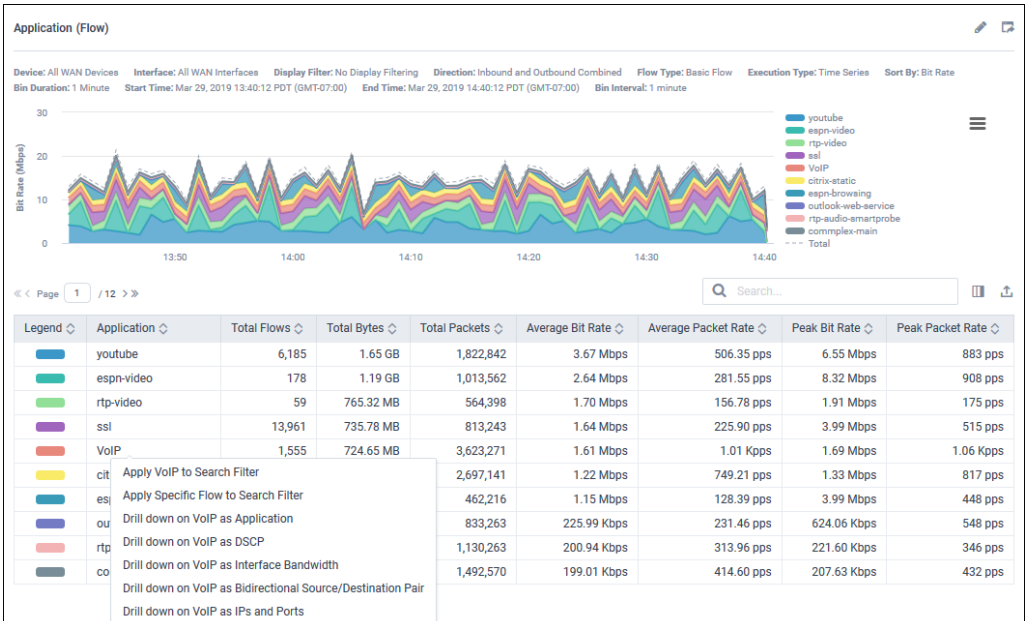
294



Legend	Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	Unknown	10,827	821.85 MB	1,356,056	1.83 Mbps	376.68 pps	2.10 Mbps	540 pps
	DC-New_York	530	312.06 MB	1,560,411	693.48 Kbps	433.45 pps	720.21 Kbps	450 pps
	Birmingham	11,559	118.08 MB	1,208,963	262.39 Kbps	335.82 pps	288.93 Kbps	385 pps
	Austin	6,809	82.63 MB	539,223	183.61 Kbps	149.78 pps	197.66 Kbps	187 pps
	Madison	7,456	82.50 MB	534,245	183.33 Kbps	148.40 pps	198.65 Kbps	178 pps
	Seattle	8,708	81.82 MB	549,366	181.82 Kbps	152.60 pps	197.26 Kbps	193 pps
	Louisville	8,566	78.01 MB	563,902	173.36 Kbps	156.64 pps	205.94 Kbps	209 pps
	San_Jose	8,321	77.10 MB	552,486	171.33 Kbps	153.47 pps	199.86 Kbps	215 pps
	Los_Angeles	9,031	75.27 MB	551,816	167.27 Kbps	153.28 pps	195.91 Kbps	206 pps
	Sydney	4,050	46.76 MB	410,170	103.90 Kbps	113.94 pps	155.02 Kbps	146 pps

Breakdown of the biggest Sites in terms of Usage

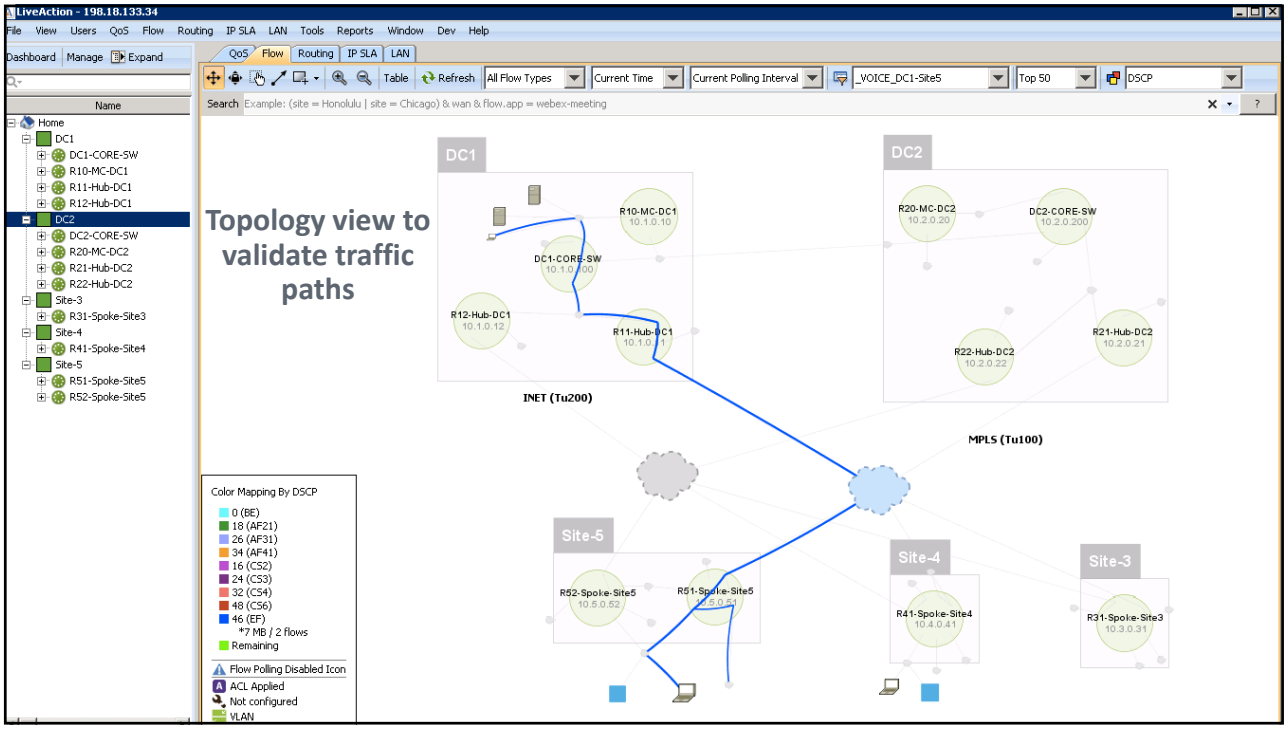
295



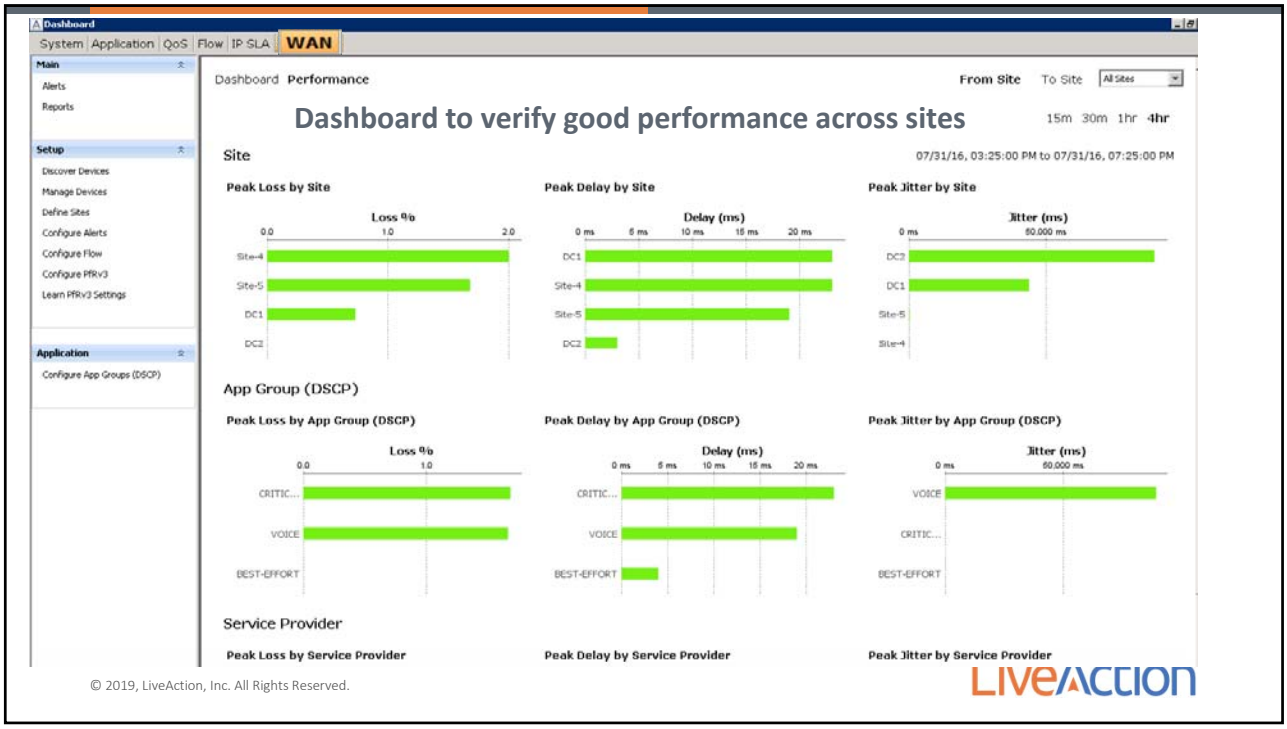
Drilldown to the applications on an interesting site

During SD-WAN Deployment

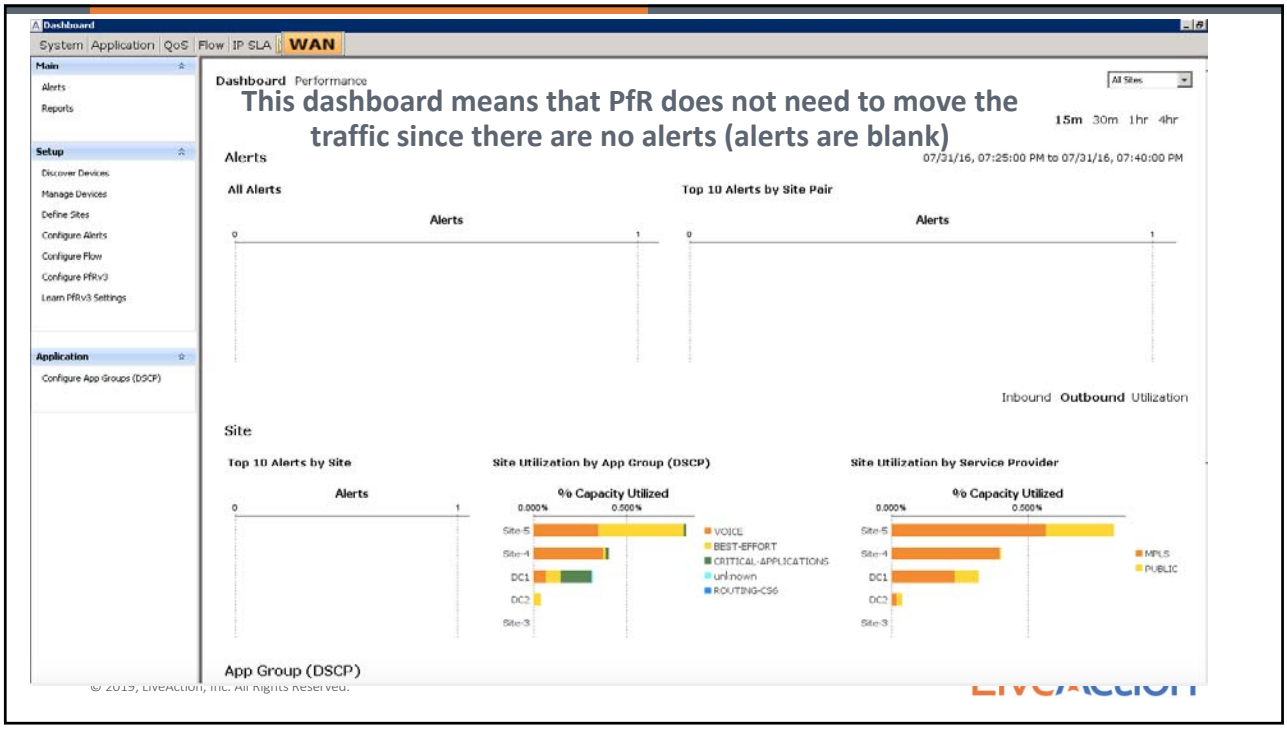
- Validate policies
  - Is traffic load balanced?
  - Where are my critical Applications going? (Either searching by appname or DSCP value)
- Verify Performance from the IWAN Dashboard
- Is PfR needing to move the traffic?



298



299

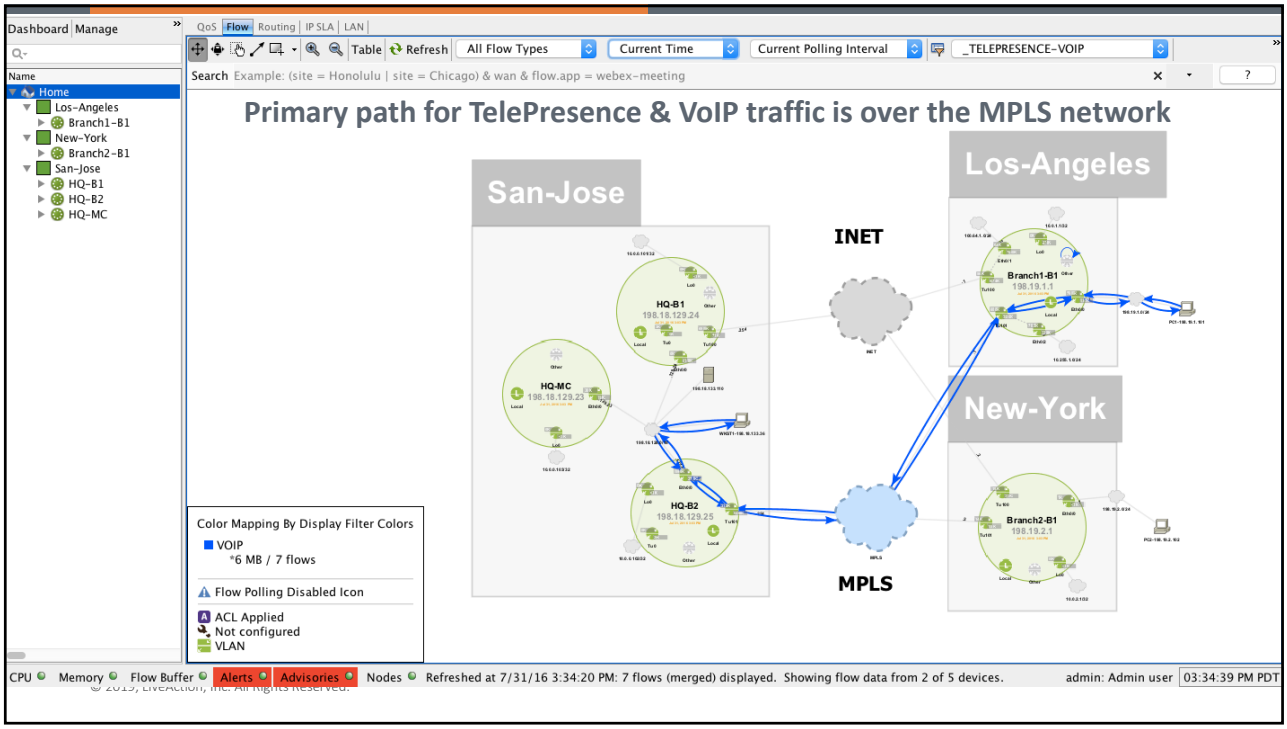


300

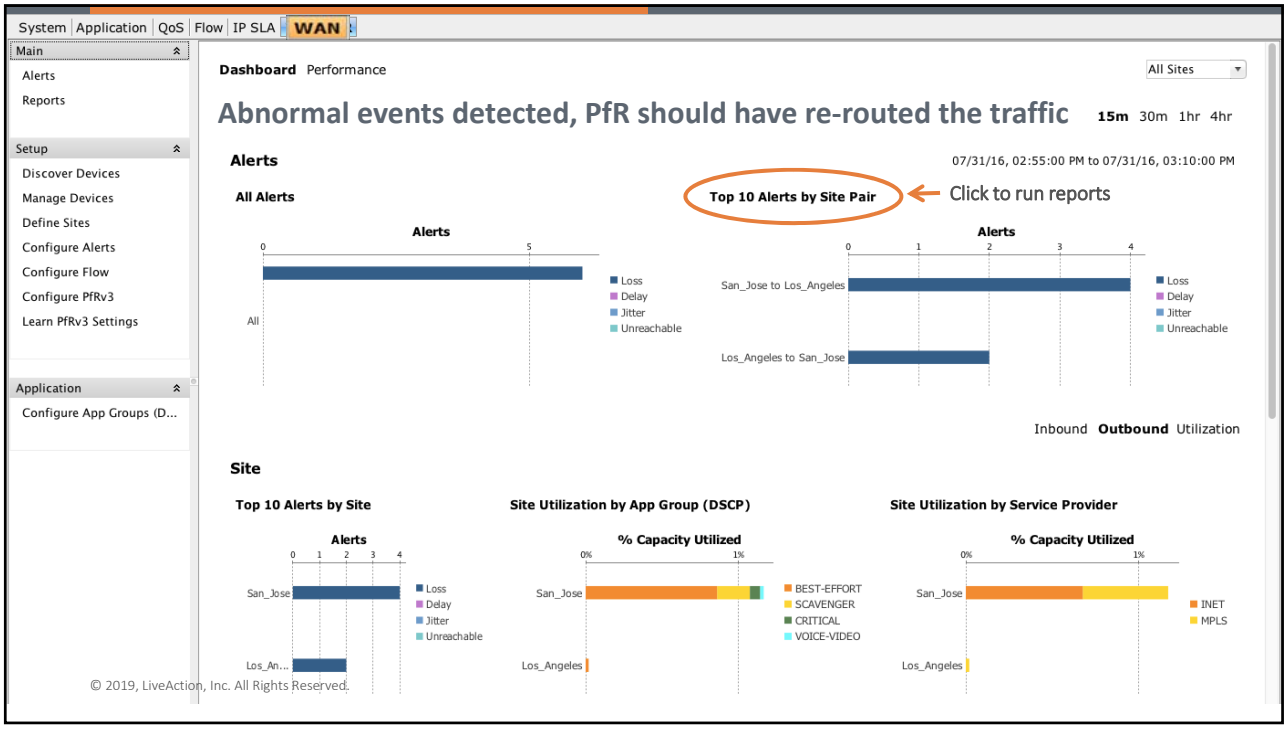
Abnormal Events Notification

- You want to be notified of any abnormal events that can potentially impact services
- When that happens, you want to quickly find out if sites and services are impacted – validate PfR is doing its job

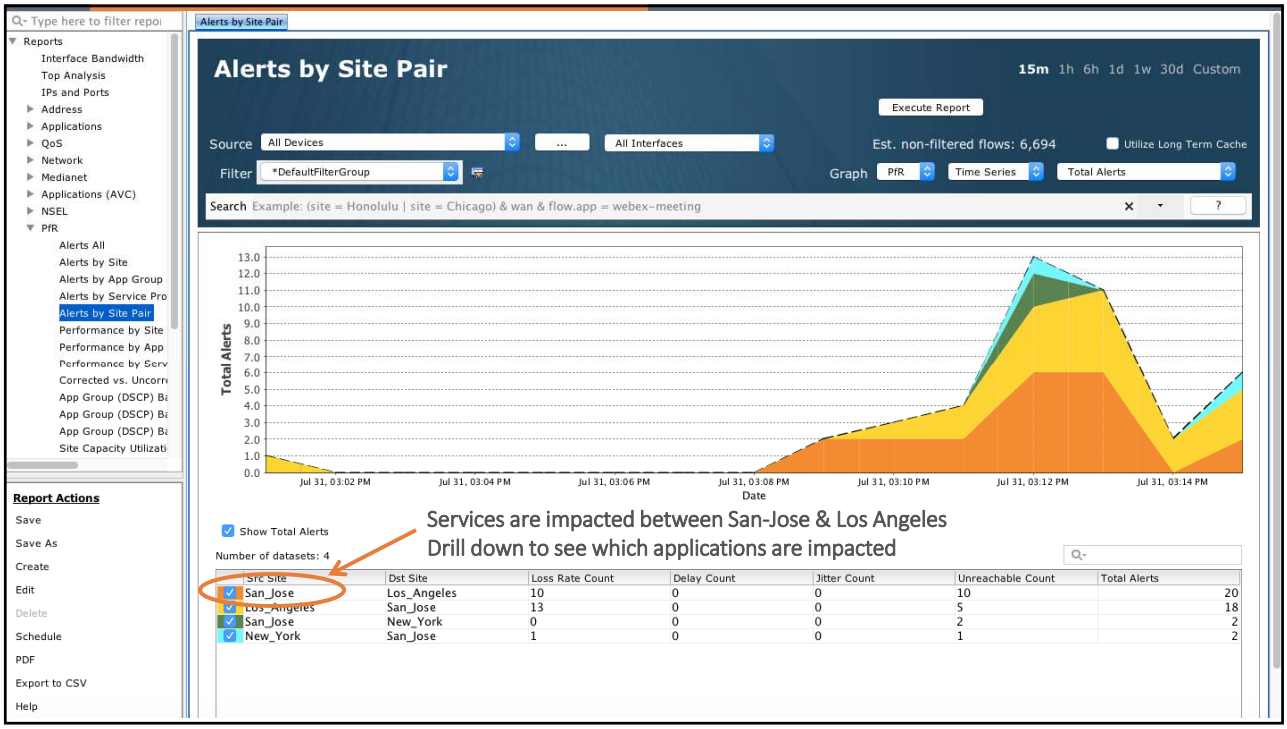
301



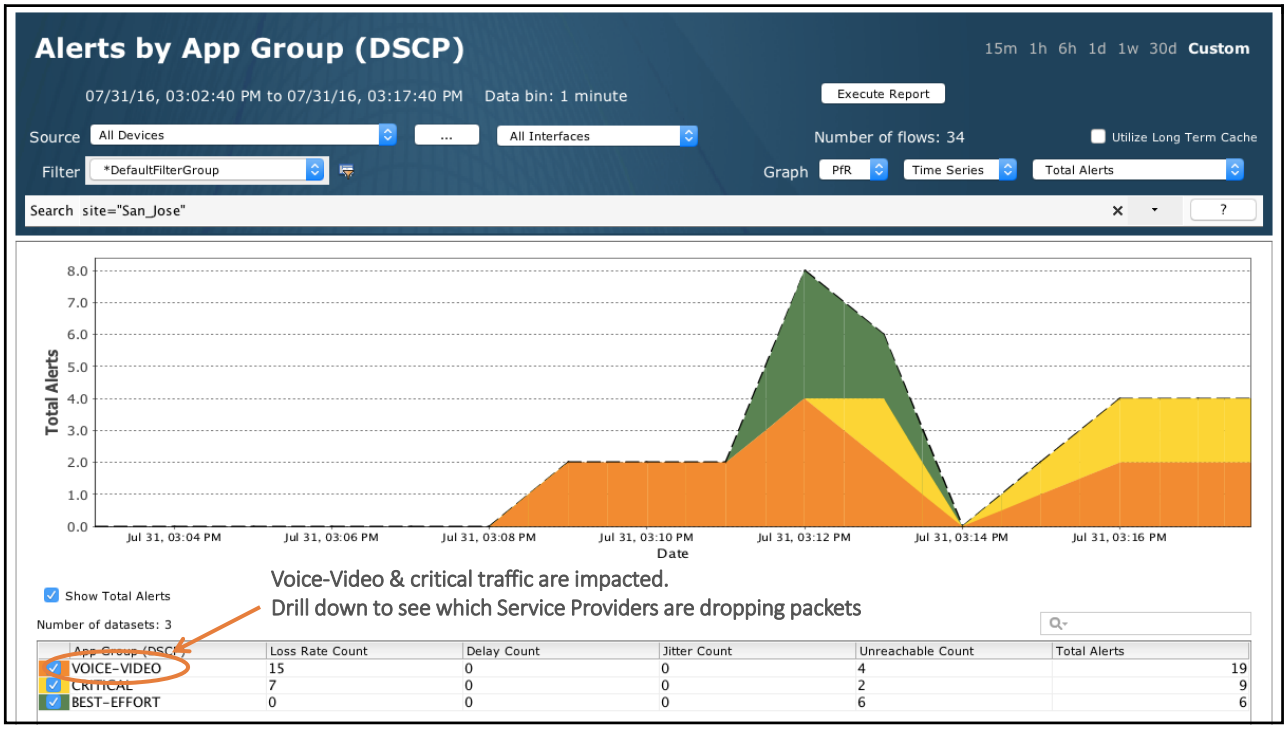
302



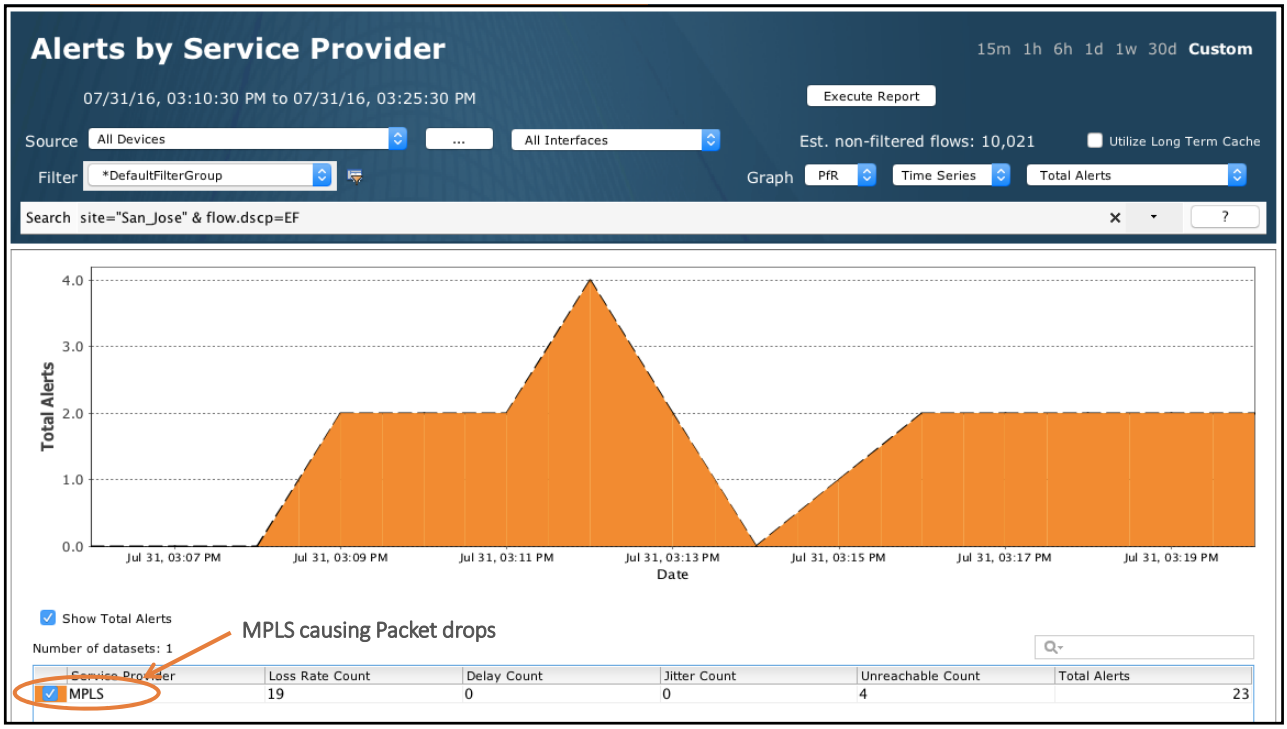
303



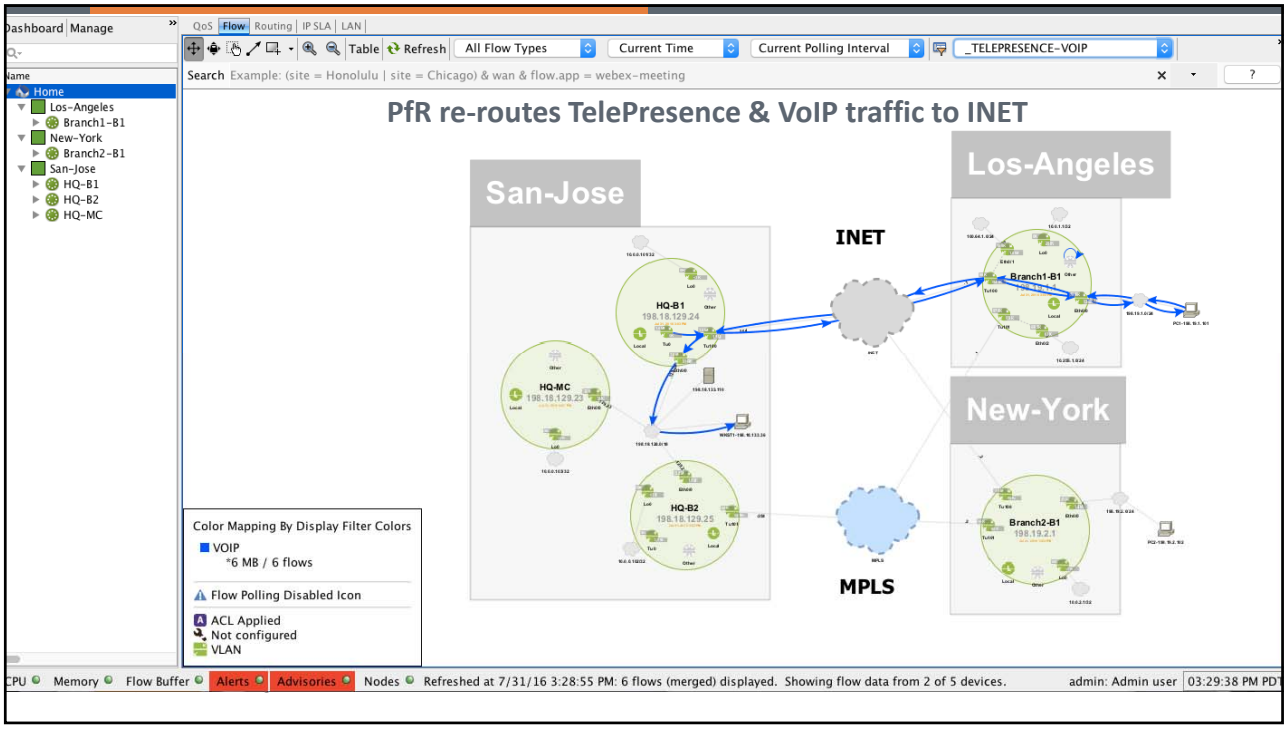
304



305



306



307

308

Lab: SD-WAN Troubleshooting

2019Apr01

309

309

310

SD-WAN QoS with DMVPN

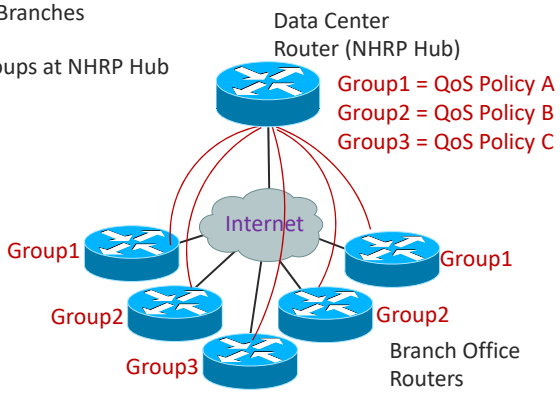
- LiveNX can be used to configure QoS in DMVPN environments
  - Per-Tunnel QoS at DMVPN Head-End
  - Branch Hierarchical QoS with point-to-multipoint DMVPN
- *Note: LiveNX's DMVPN Per-Tunnel QoS configuration and monitoring capabilities can be used with or without SD-WAN.*

311

Per-Tunnel QoS at DMVPN Head-End

Step 1 – Assign NHRP Groups to Branches

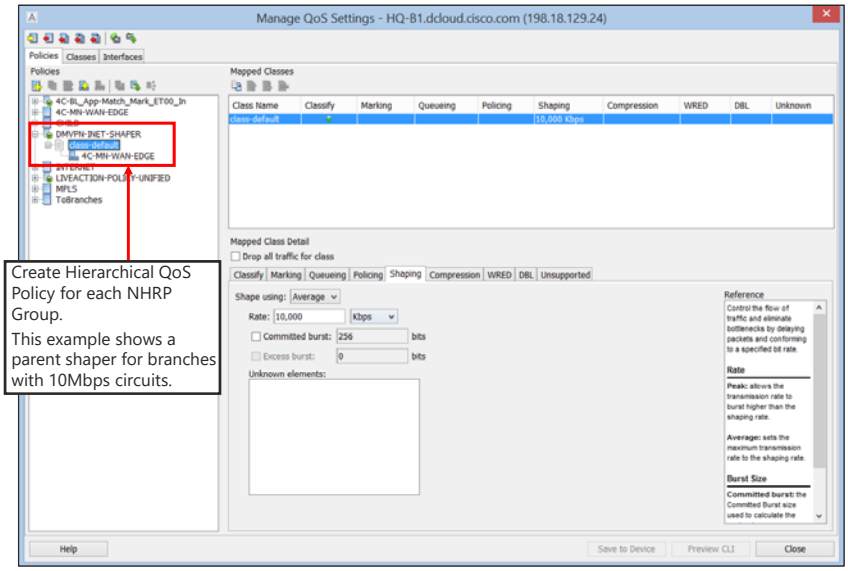
Step 2 – Map QoS policies to Groups at NHRP Hub



LiveAction

312

Configuring Per-Tunnel QoS



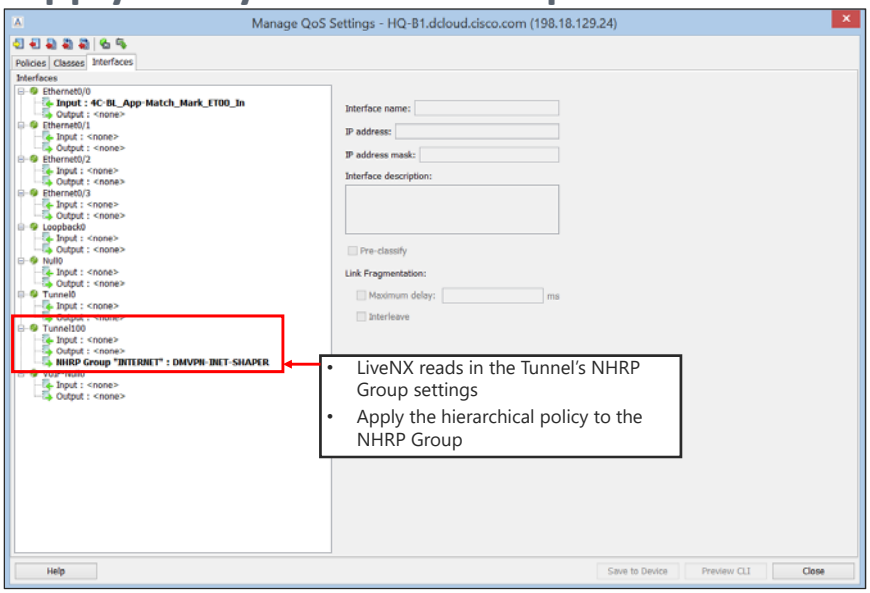
Create Hierarchical QoS Policy for each NHRP Group.

This example shows a parent shaper for branches with 10Mbps circuits.

LiveAction

313

Apply Policy to NHRP Group

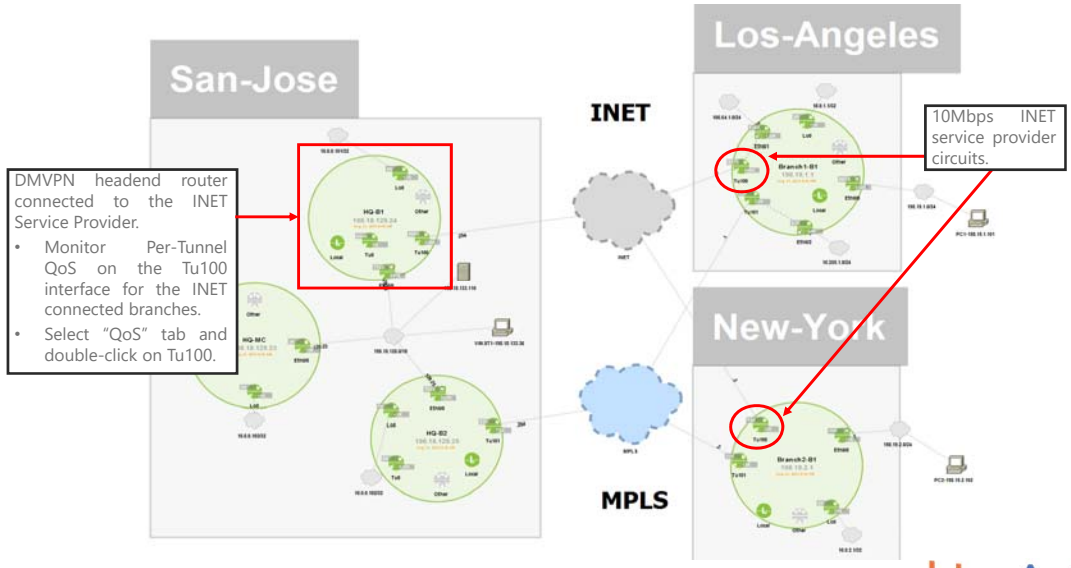


- LiveNX reads in the Tunnel's NHRP Group settings
- Apply the hierarchical policy to the NHRP Group

Per-Tunnel QoS Monitoring at the Head-End

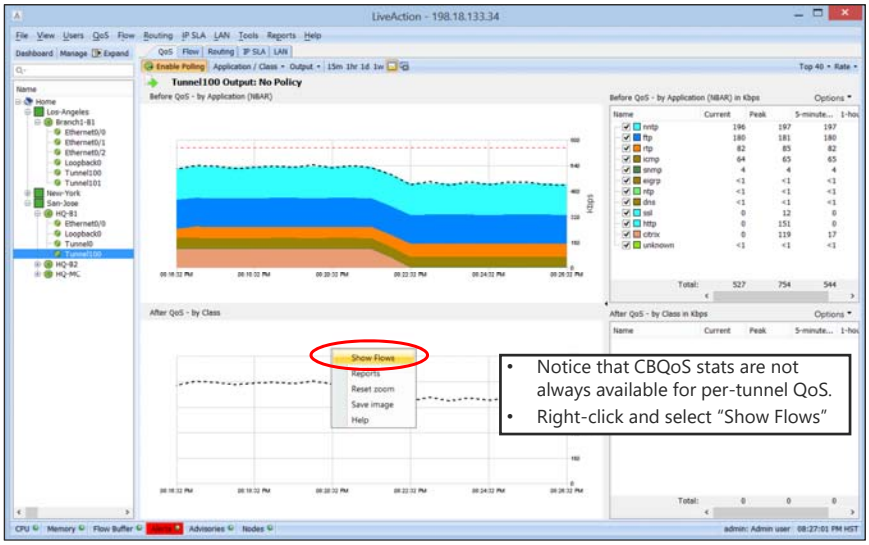
- Per-Tunnel QoS monitoring was not supported via the CBQoS MIB in the past
- Monitoring in LiveNX can be performed using NetFlow and network semantics

DMVPN Per-Tunnel QoS Topology Example



316

Per-Tunnel QoS Monitoring

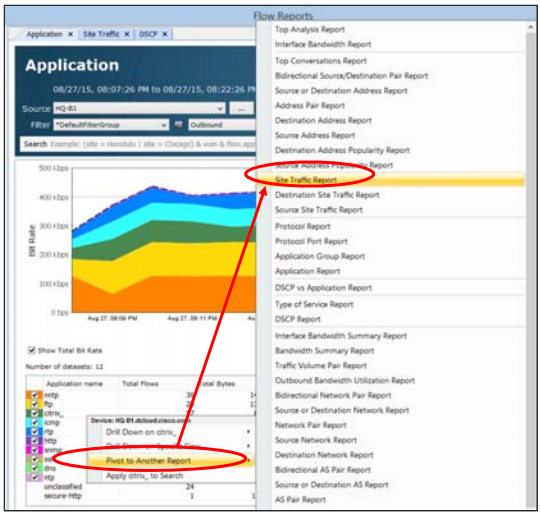


317

Per-Tunnel QoS Monitoring

- LiveNX will automatically run the Application report for the tunnel interface.
- Right-click in the table and select “Pivot to Another Report”.
- Select the “Site Traffic Report”.

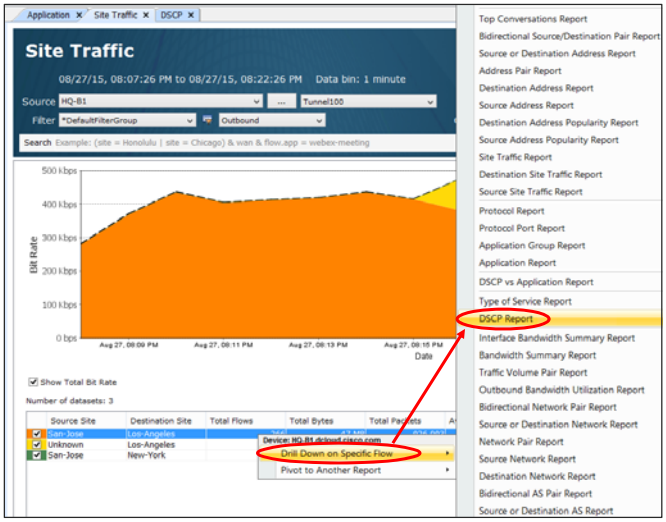
Note: Site and Site IP semantics are needed for this workflow.



318

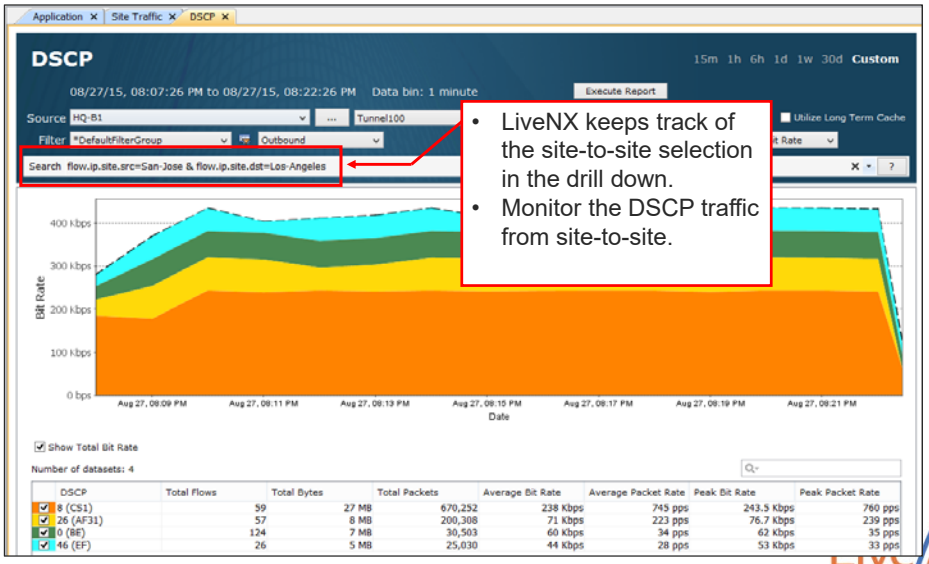
Per-Tunnel QoS Monitoring

- The “Site Traffic” report will show site-to-site traffic from the DMVPN head-end.
- Right-click on the site-to-site communication of interest and “Drill Down on Specific Flow”.
- Select the “DSCP Report”



319

Per-Tunnel QoS Monitoring

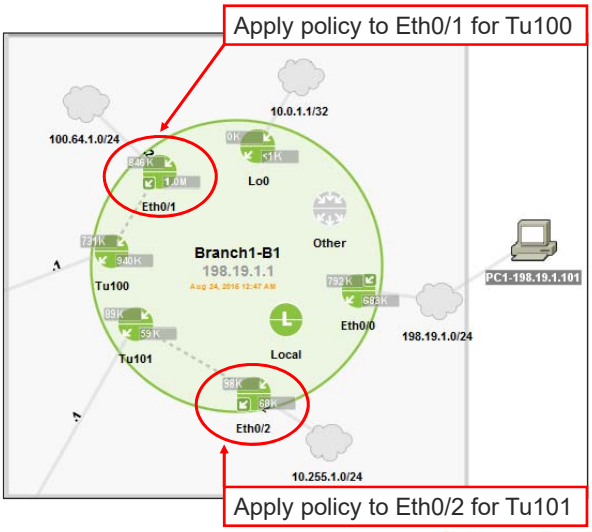


- LiveNX keeps track of the site-to-site selection in the drill down.
- Monitor the DSCP traffic from site-to-site.

320

Branch QoS Configuration for DMVPN

- DMVPN is a point-to-multipoint technology.
- Outbound QoS shaping policies must be applied to the physical interface of the tunnel at the branch.
- *Side note: Recall Remote Ingress Shaping can be applied to the LAN interface: Eth0/0 to protect critical apps inbound to the site.*



321

323

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 services@liveaction.com

324

327