LiveNX Training

Day 1

LiveAction™

Agenda – Day 1

- LiveNX Overview & Architecture
- The LiveNX WebUI
  - Dashboards
  - Sites/Devices/Interfaces
  - Reports Overview
  - System Management
- LiveNX Engineering Console
  - Dashboard
  - Reports
- Visualizations & Troubleshooting
  - Voice, Video, Delays
- Add & Manage Devices
  - Adding Devices
  - Grouping & Objects
  - Device Semantics
- Flow Collection
- Topology Definition
- More Dashboards, Reports and Alerts
- Custom Filters
- Implementation Best Practices
  - Installation Considerations
- Deployment Strategies

Agenda - Day 2

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

Class Logistics

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

Your Trainer…

Nate Richie

Senior Consulting Engineer, Advanced Services Team

Interim Manager, Advanced Services Team

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

And you are…

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

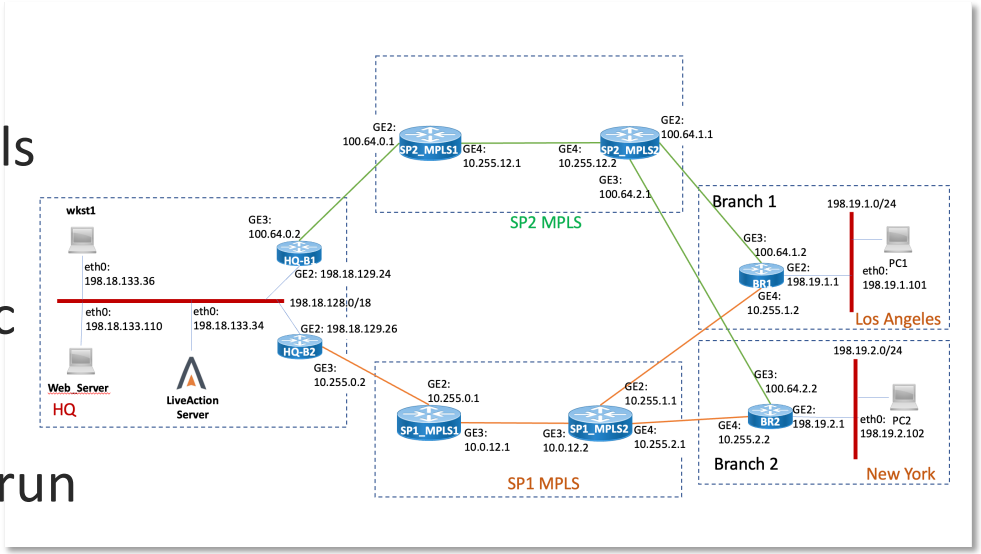
LiveNX

Lab Preparation

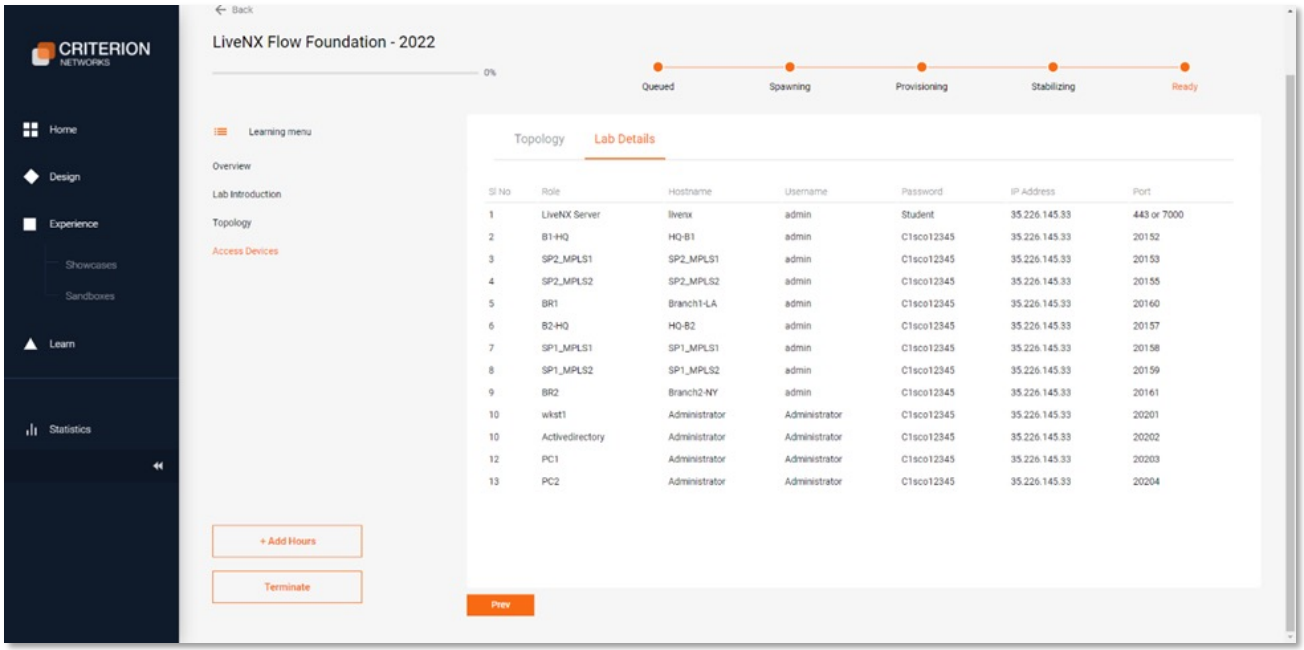
LiveAction™

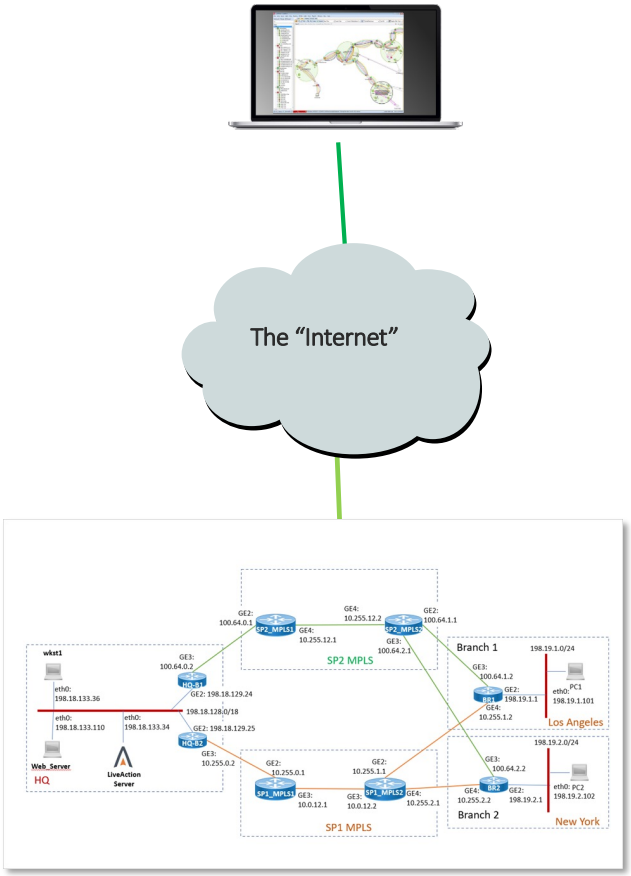
Our Training Infrastructure

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



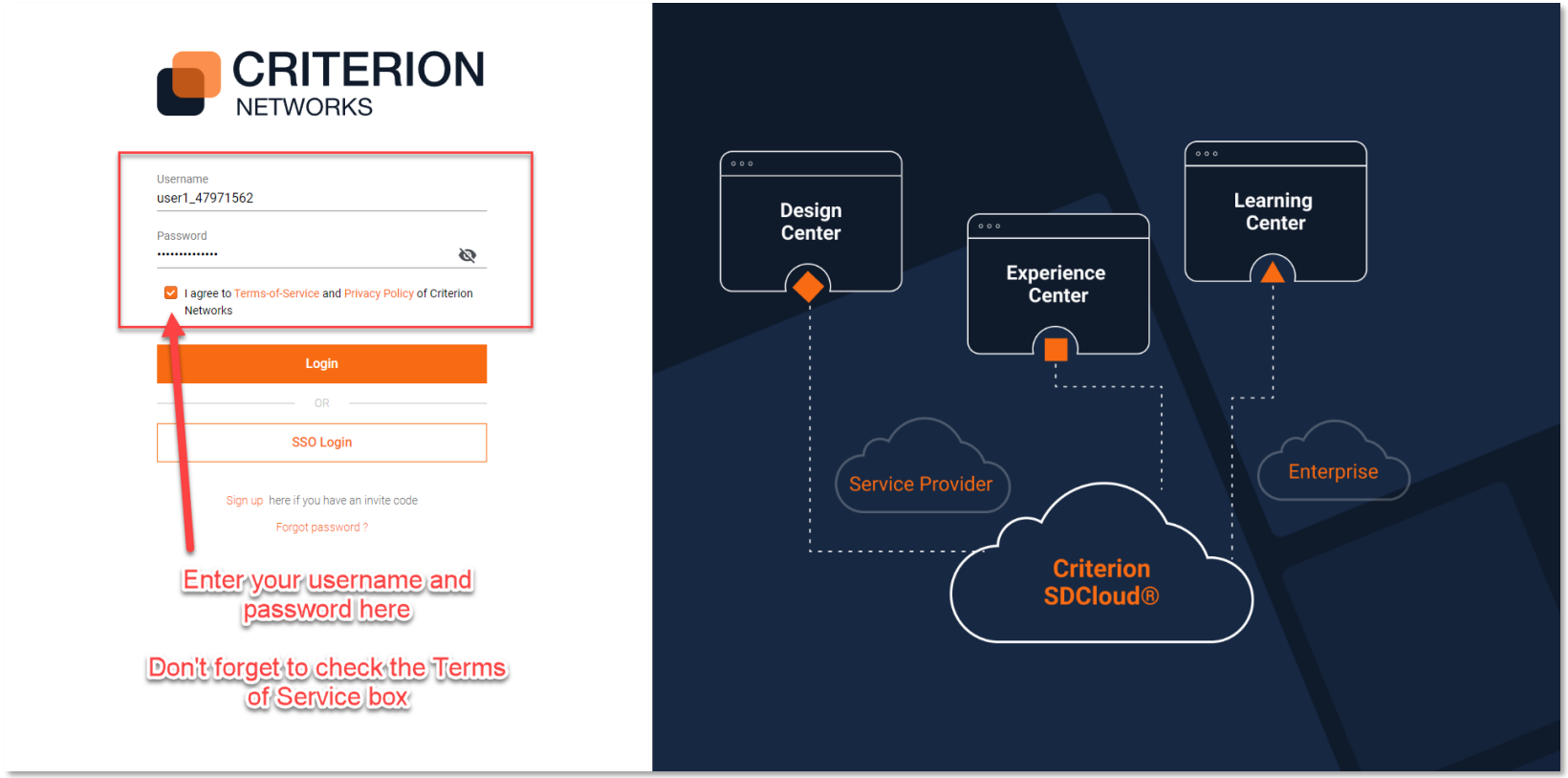
LiveNX Class Infrastructure



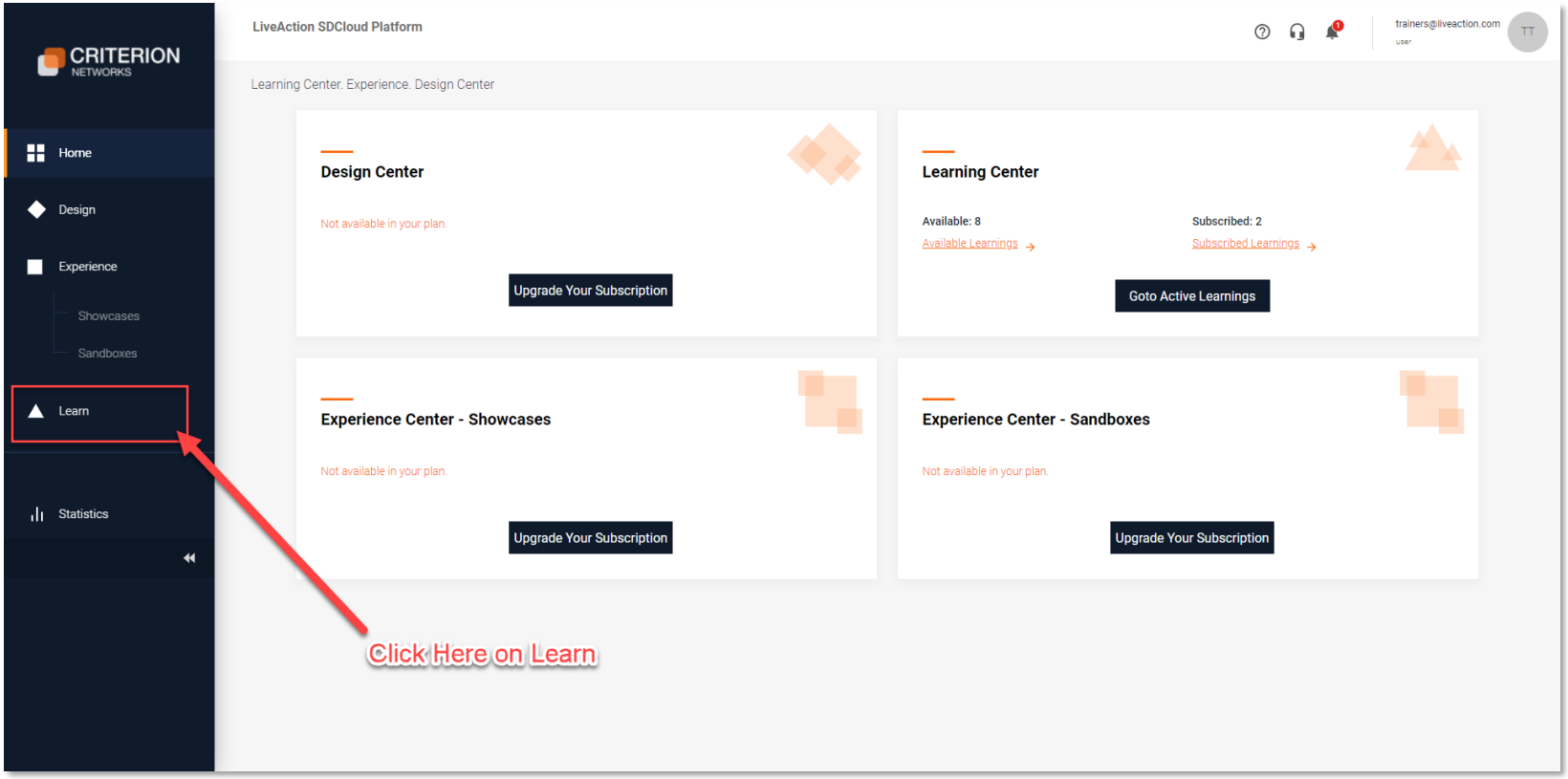


LiveAction®

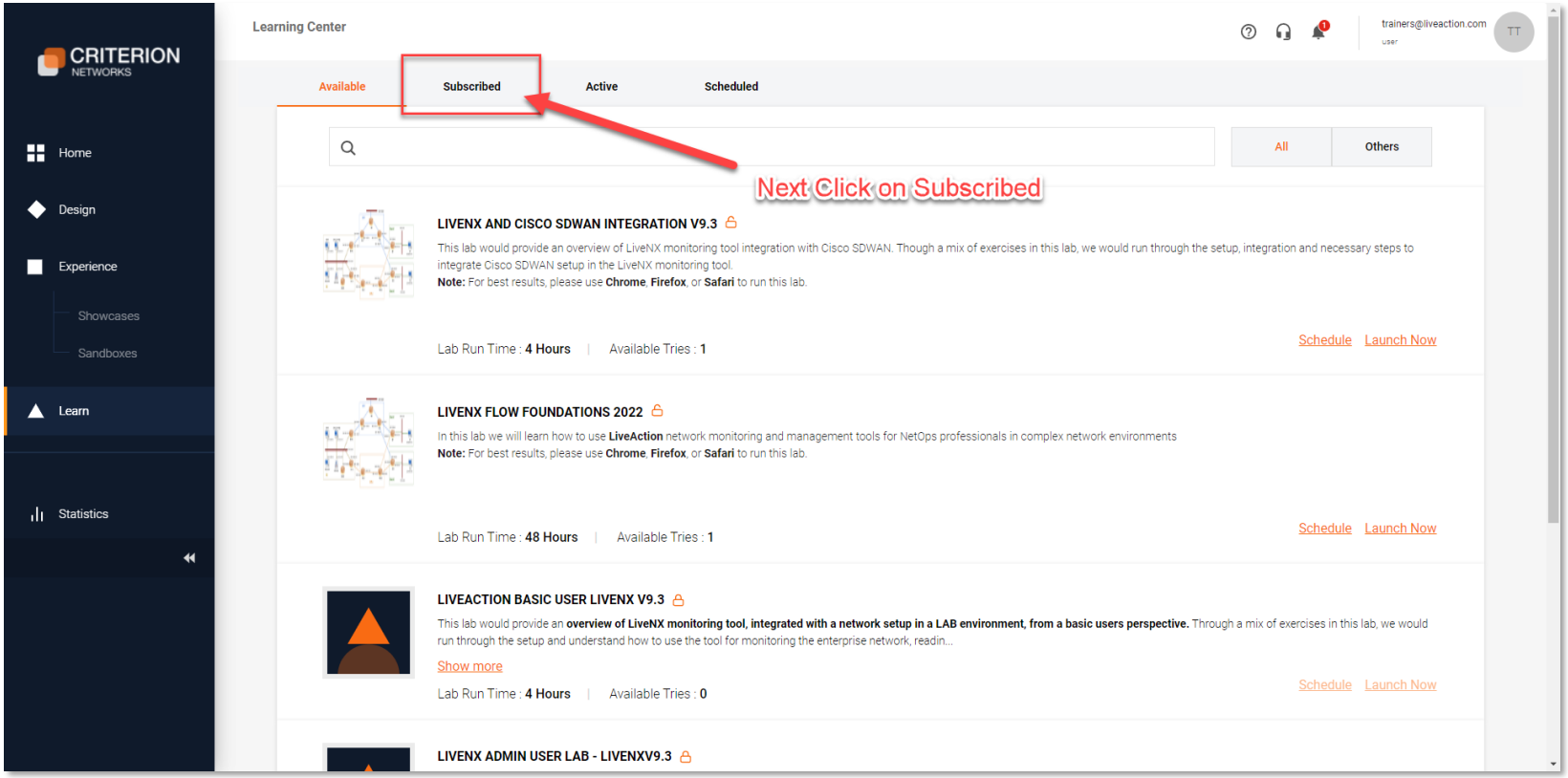
Criterion Labs Log On Screen



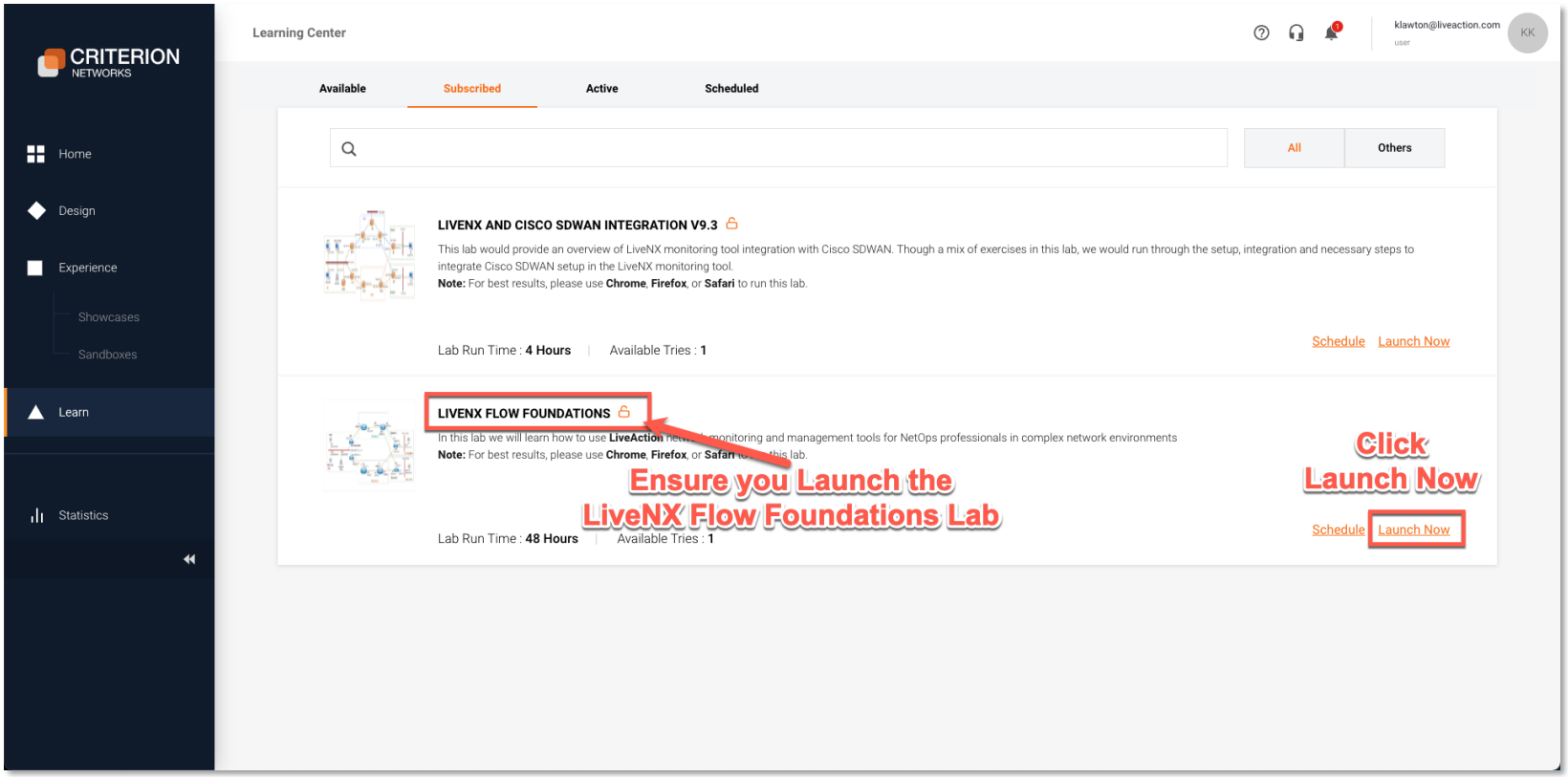
Click Learn



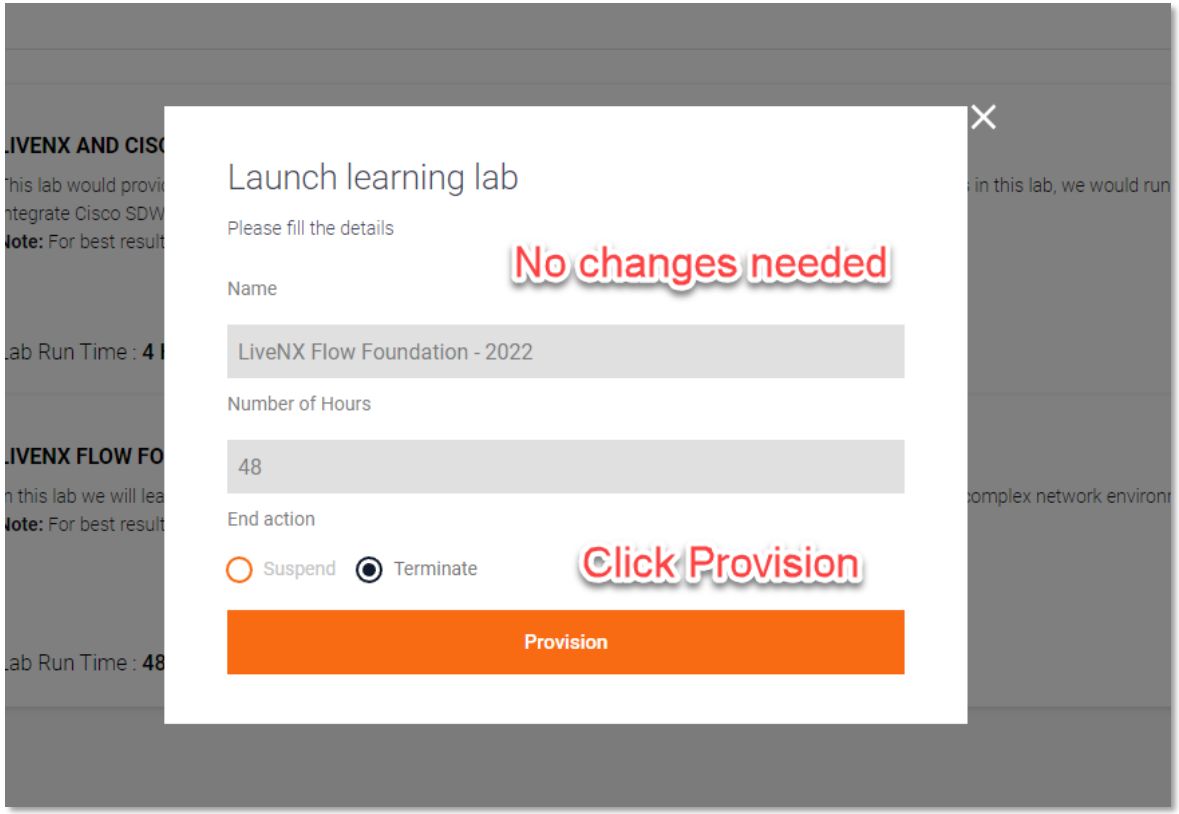
Click Subscribed



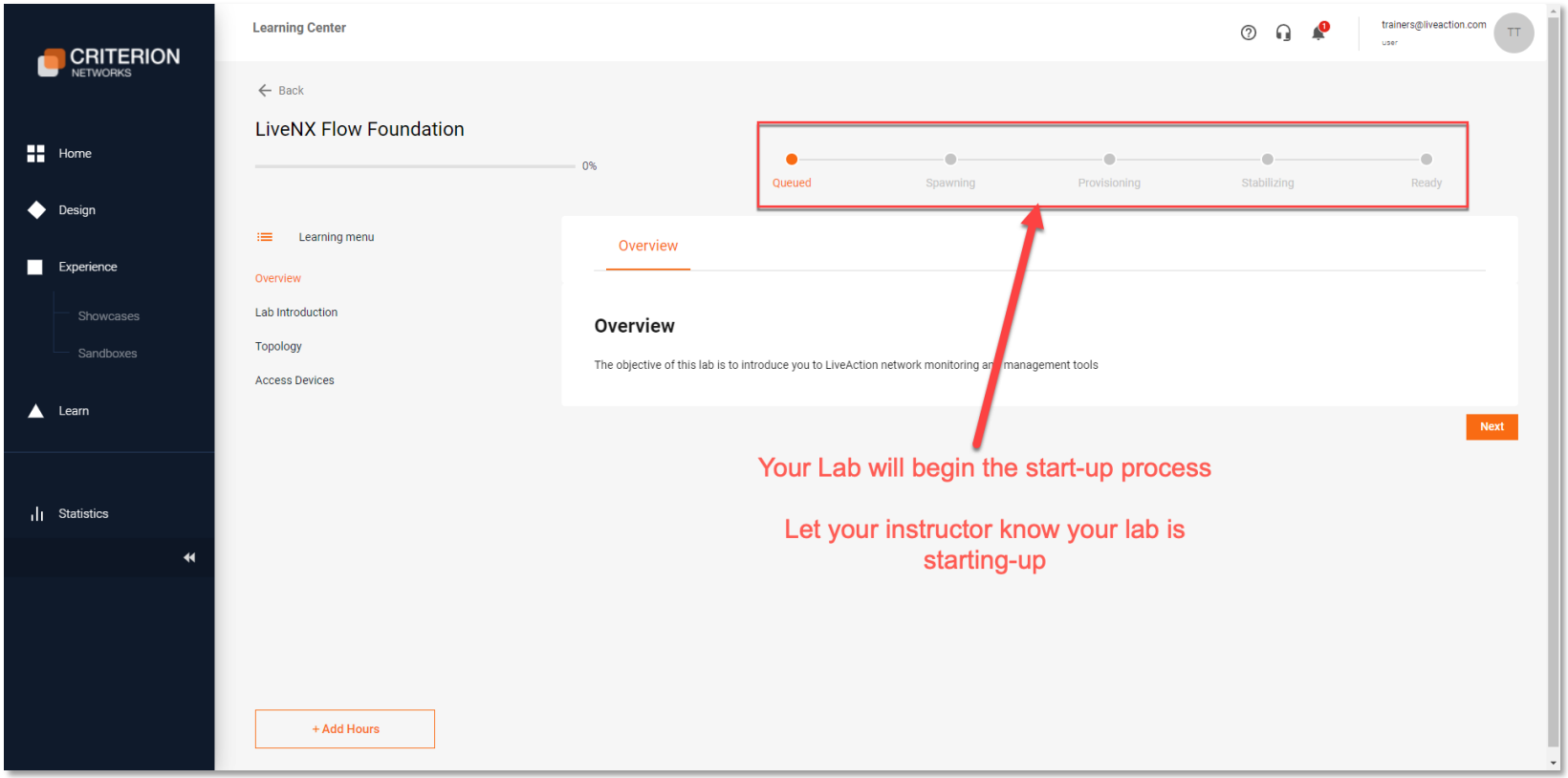
Select the Correct Lab and Click Launch Now



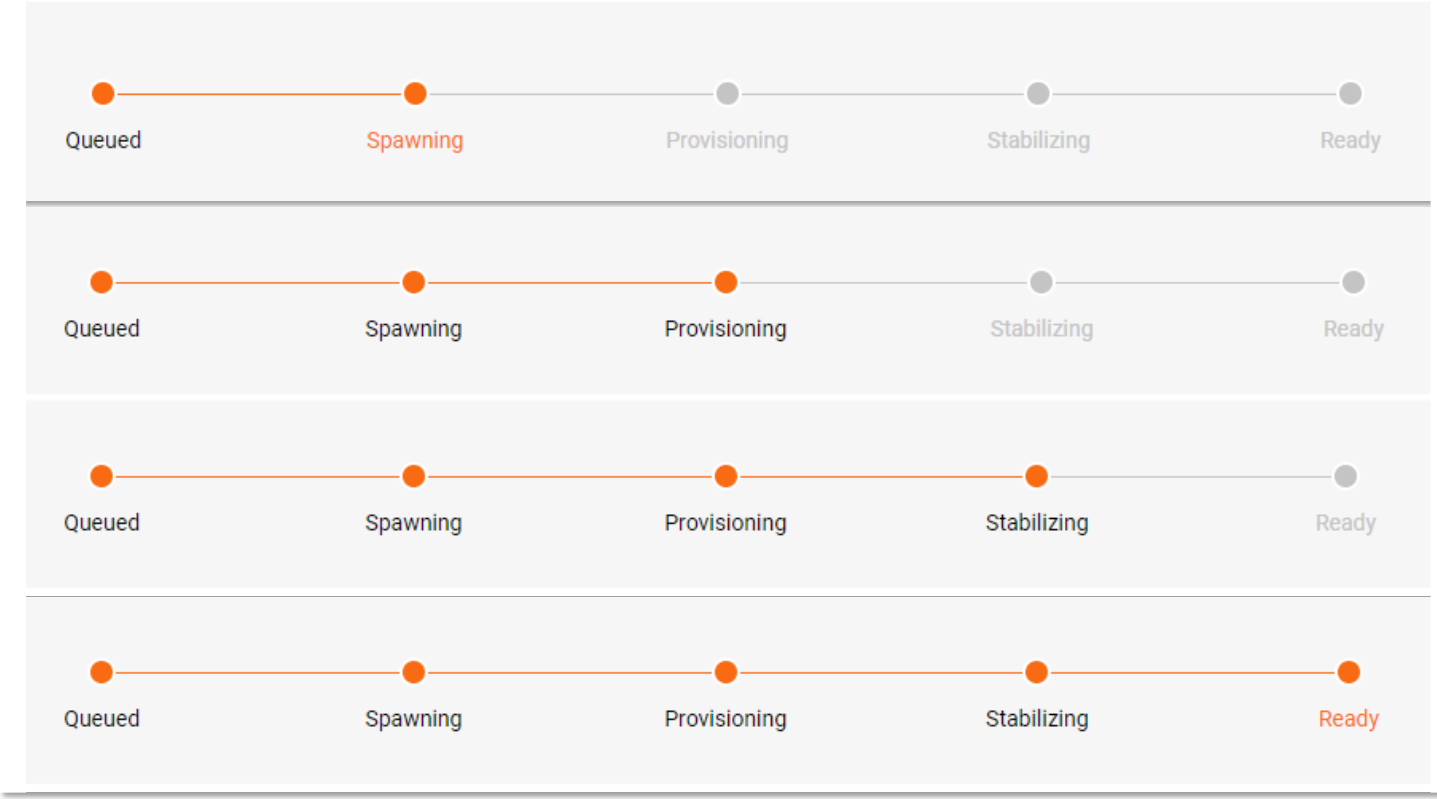
Click Provision



Your Lab Should Begin Start-Up



Start-up Takes Around 5 mins



Sites Used in This Training Course

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

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 Engineering Console
  - https://cloudkeys.liveaction.com/downloads
- You may now ping your LiveNX Server…

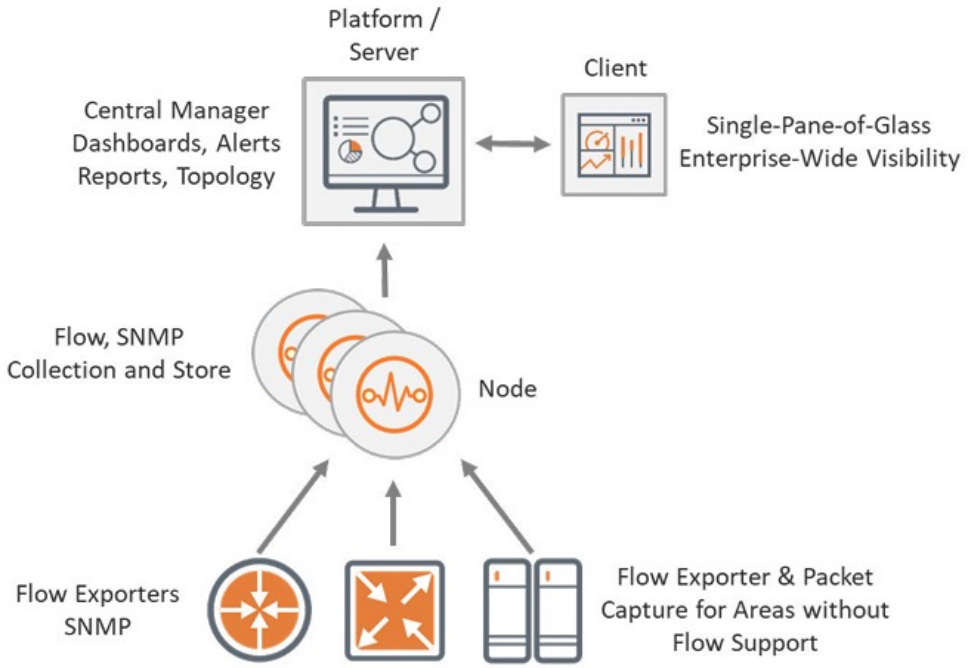
LiveNX

System Overview & Architecture

LiveAction™

Architecture Overview

- **Distributed Computing Architecture**
  - High-performance database
  - Large-scale distributed analytics platform
  - Capable of handling 1M+ flows/sec
  - Monitor 40,000+ devices across distributed deployment
  - Visualize up to 1,000 active interfaces per device
  - 3-layer architecture – **client**, **server**, **node**
- **Engineering Console**
  - 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



System Requirements

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

- Server Platform Specifications:
  - VMware ESXi v5.0 or higher – VMware Hardware Version 8 (vmx-8)
- Network Hardware – At least two Physical NICS on ESXi
  - Support up to 10 Gbps
  - Virtual NICs on OVA are utilizing E100

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

Network Devices Supported

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

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

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

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 NodeTraffic (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.

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

LiveNX Communication with Devices

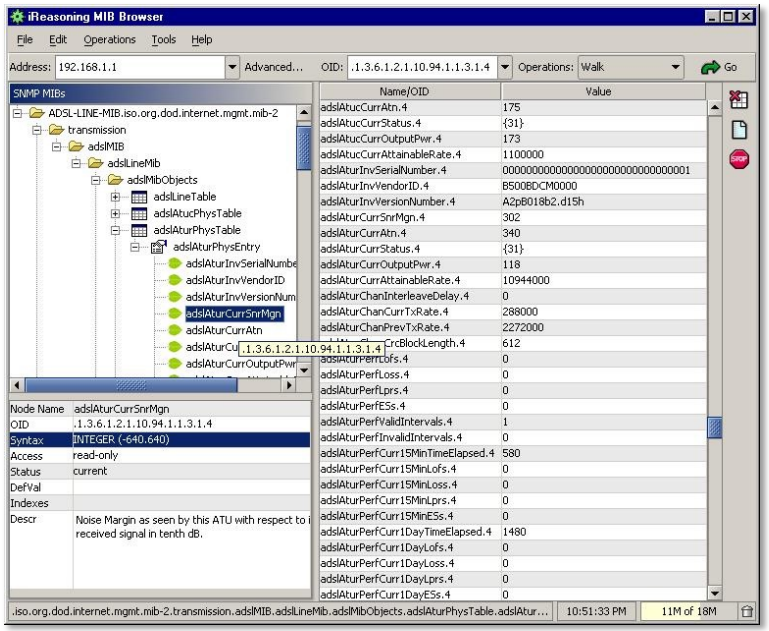
LiveNX uses SSH or Telnet access to read IOS configurations, as well as to make desired configuration changes to the device(s);

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

LiveNX does not save the router configuration in our database!

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



LiveNX Network Protocol Requirements

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

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

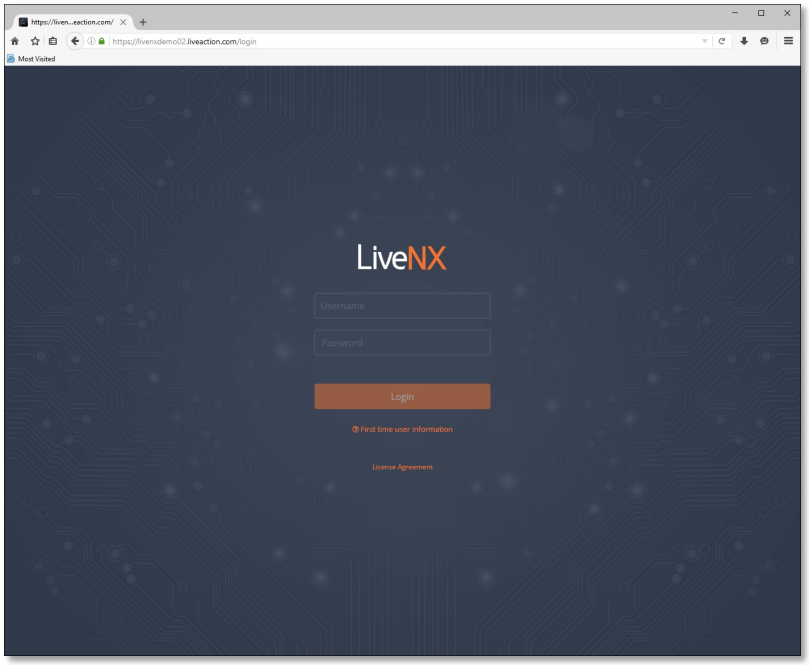
LiveNX Web UI

LiveAction™

From Any Browser… from Anywhere!

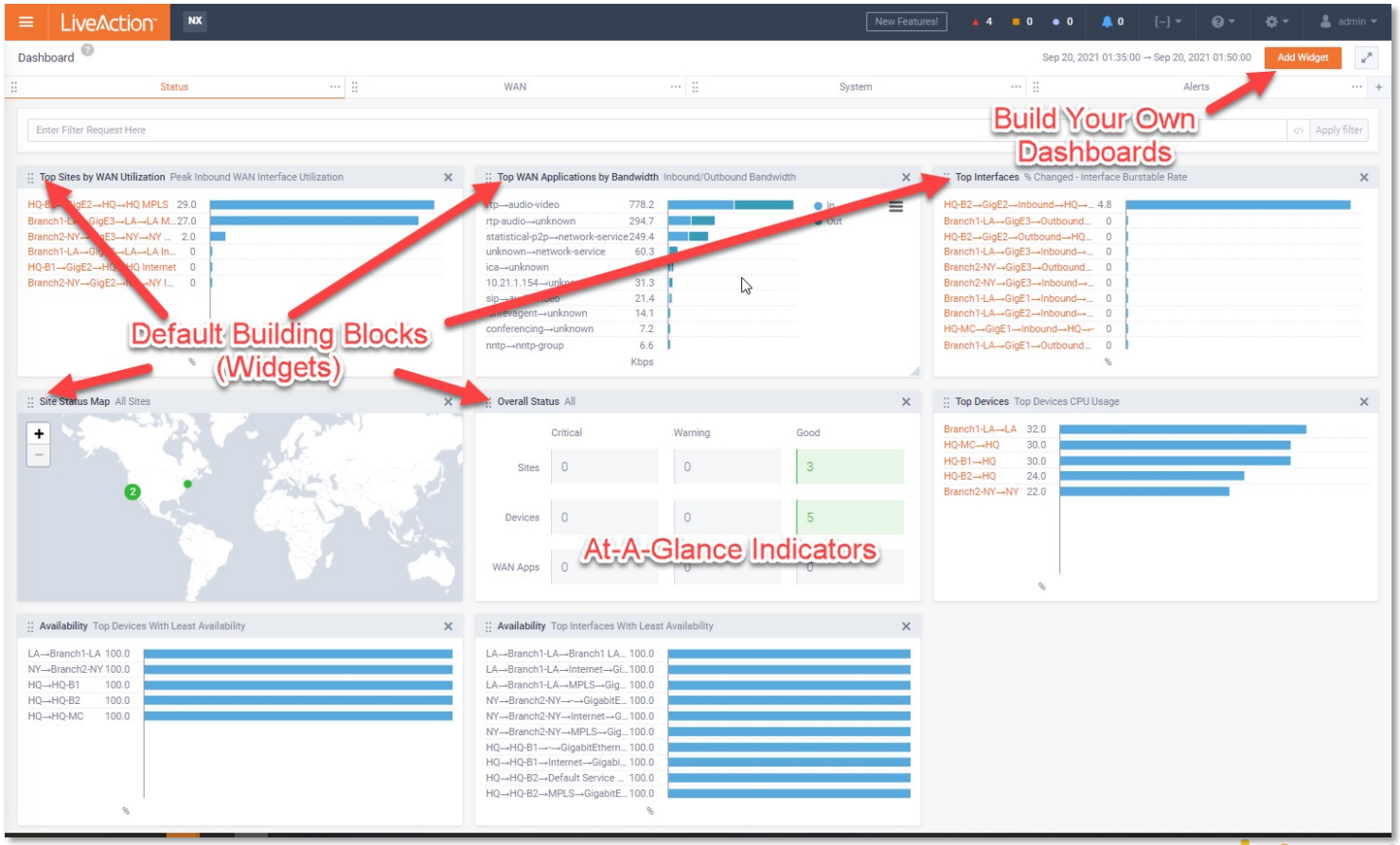
https://<LiveNXserverIP>

- Create and View Dashboards
- Manage and View:
  - User Management
  - Devices (accept or reject information from devices – cannot configure)
  - Alerts
  - Reports



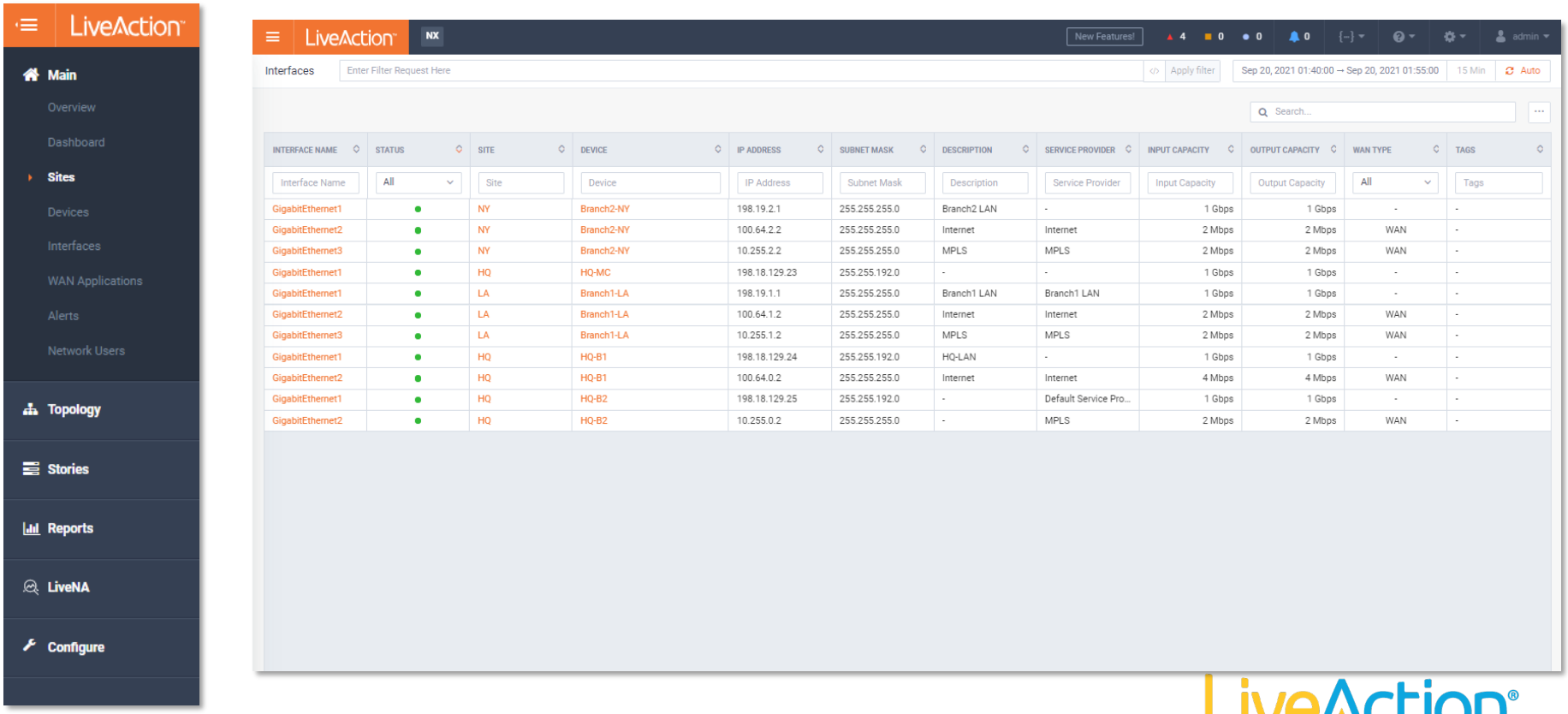
Visualization Philosophy: Shows what you ask it to show

Customizable Dashboards

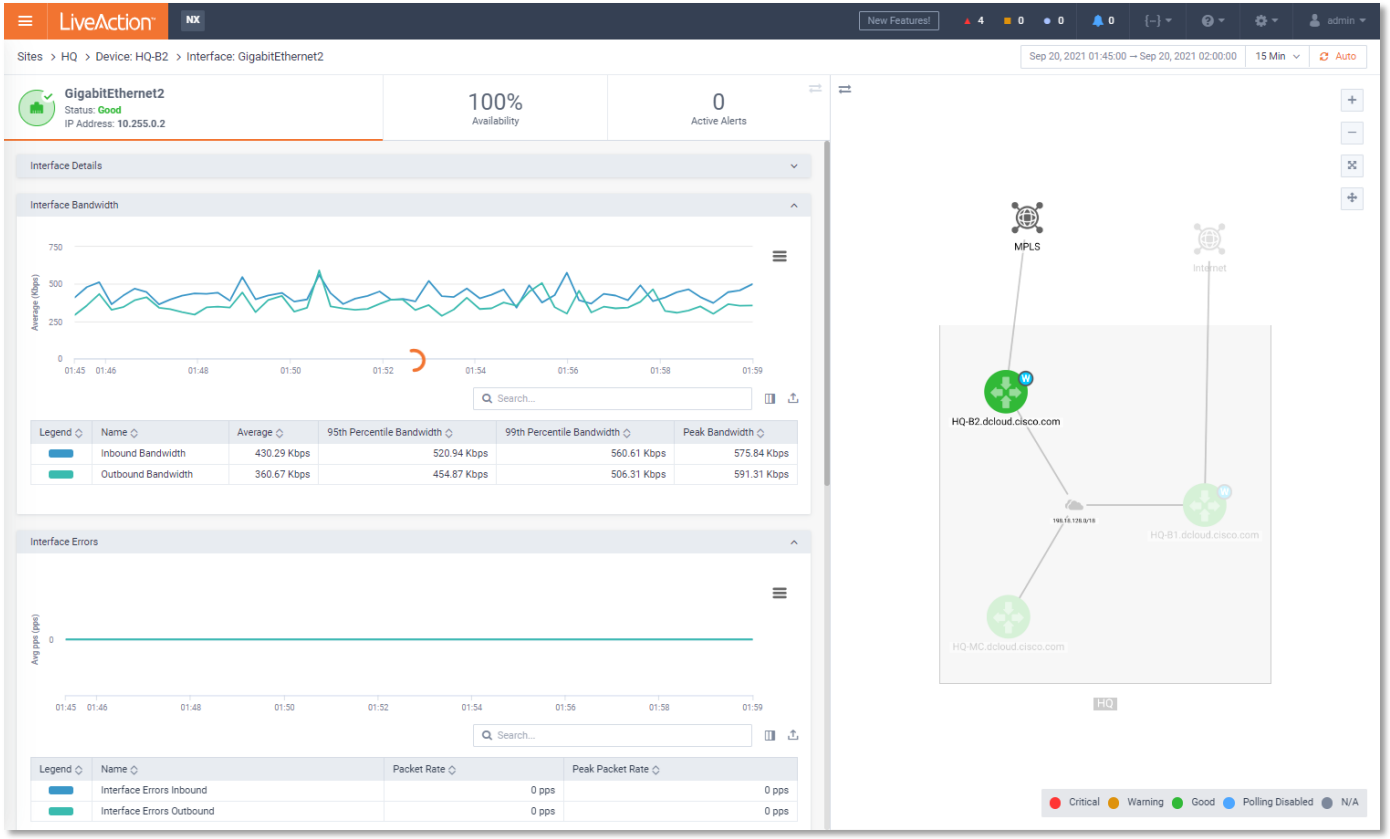


Sites Details

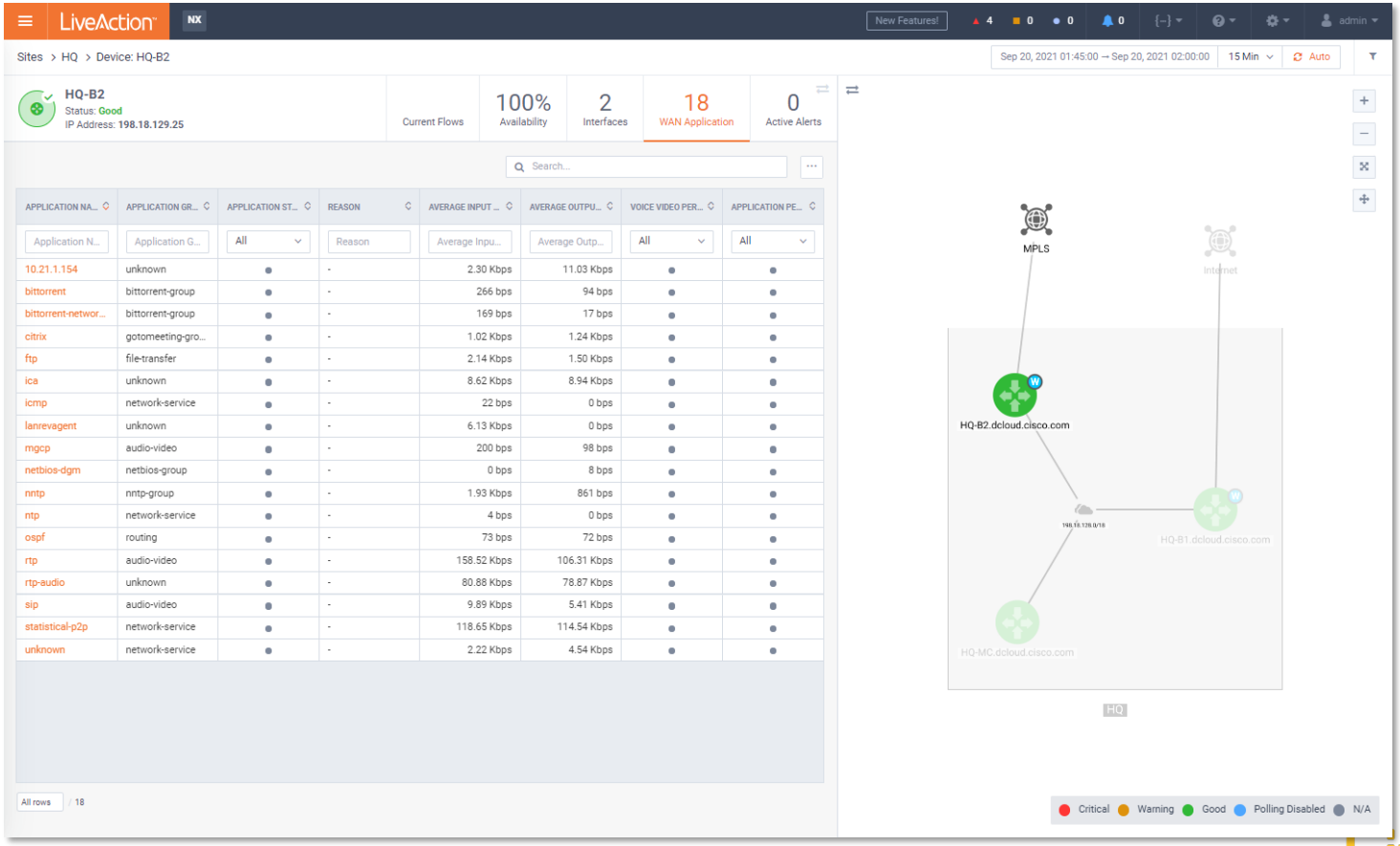
Drill into Sites > Devices > Interfaces…



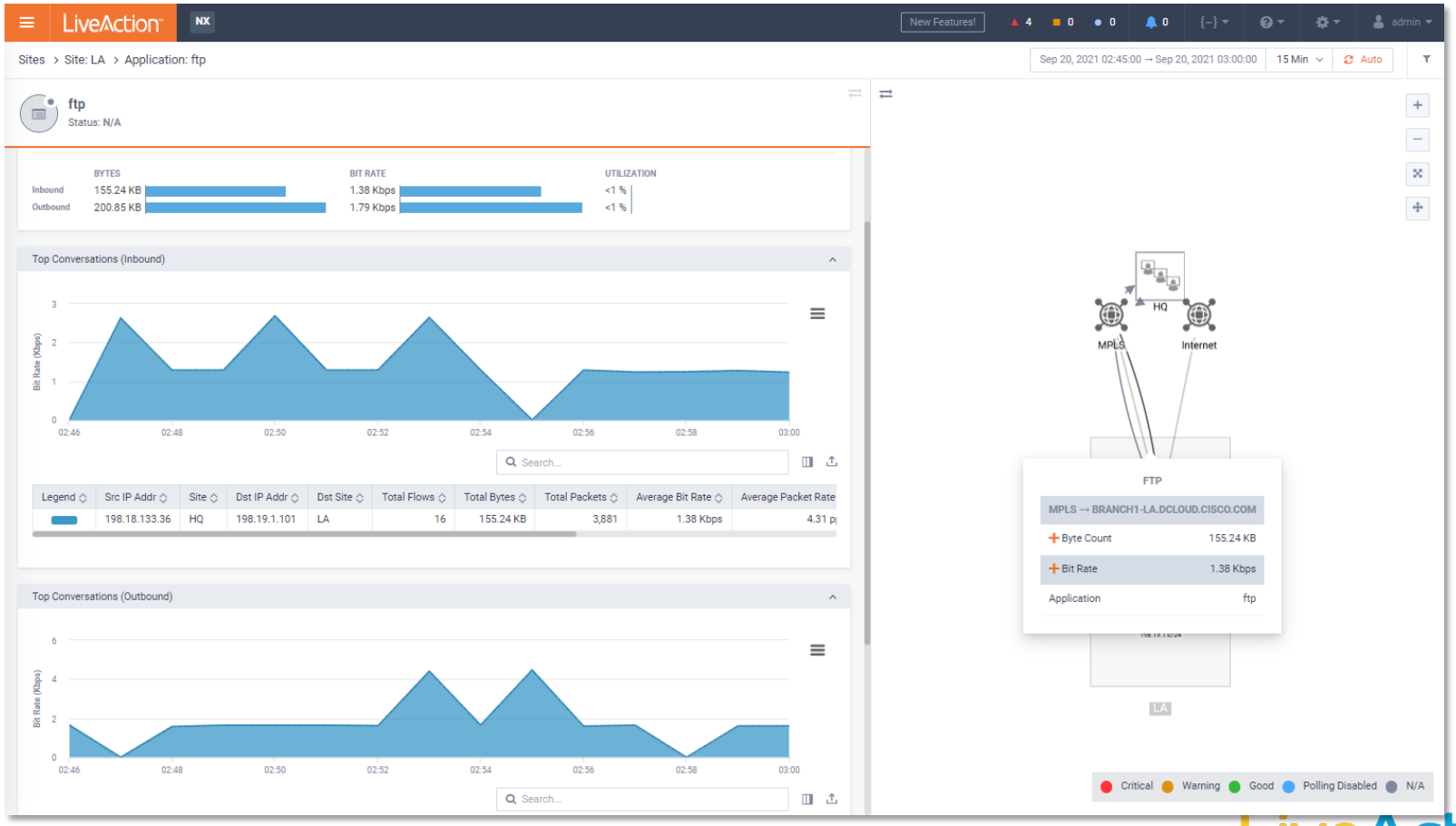
Interfaces



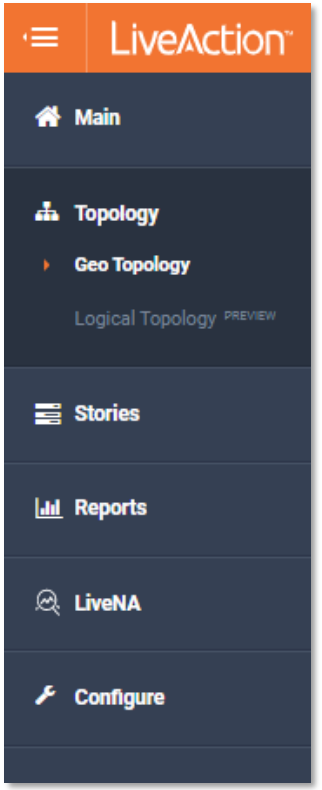
WAN Applications

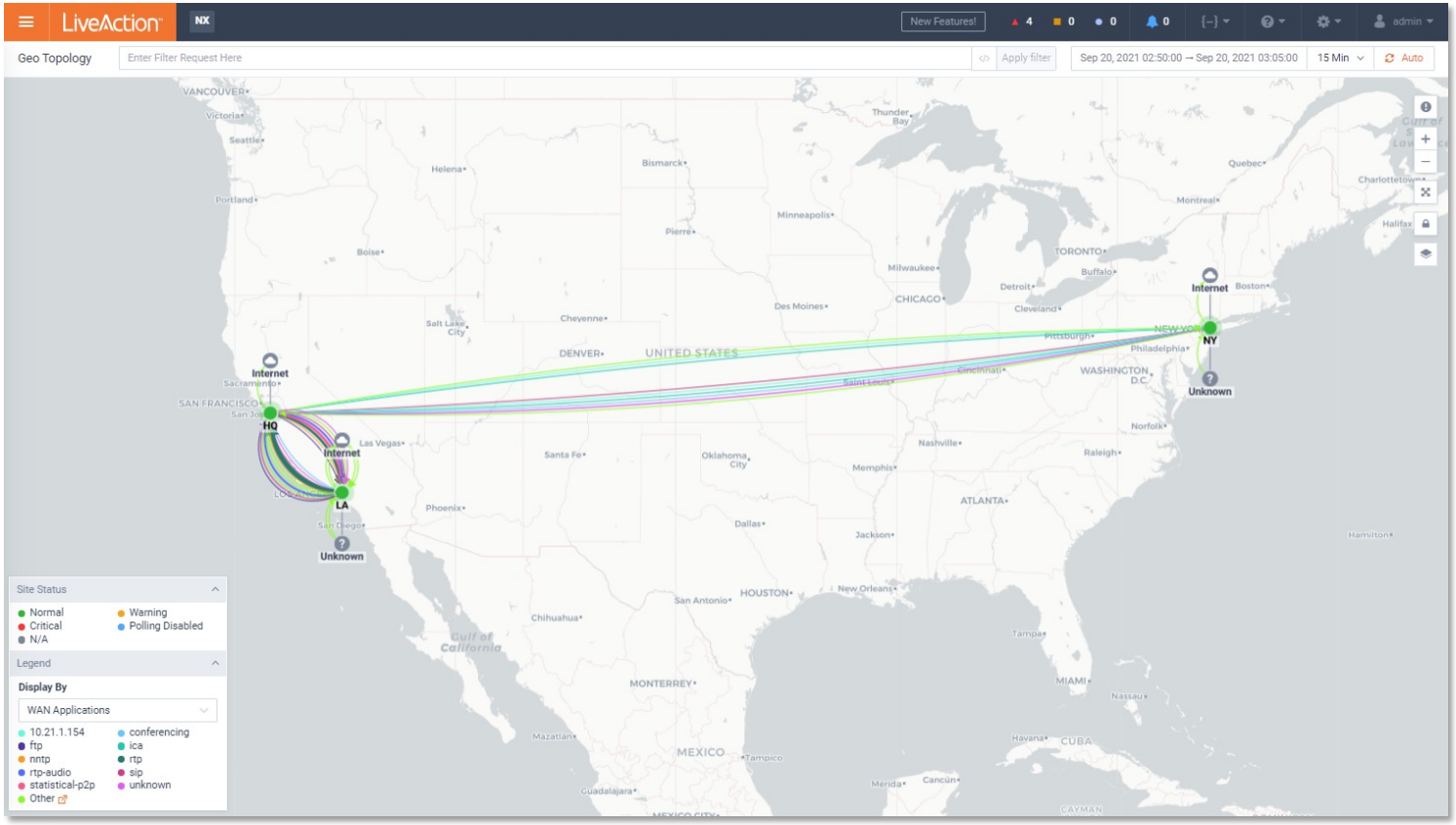


WAN Applications>Flows

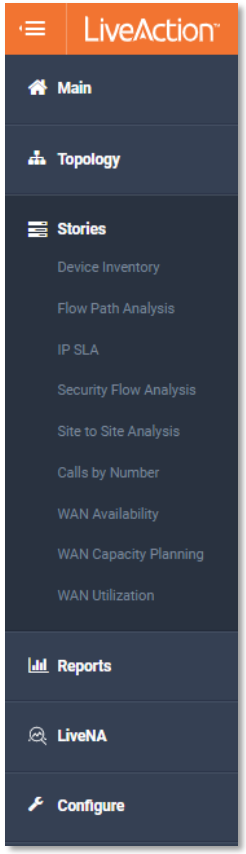


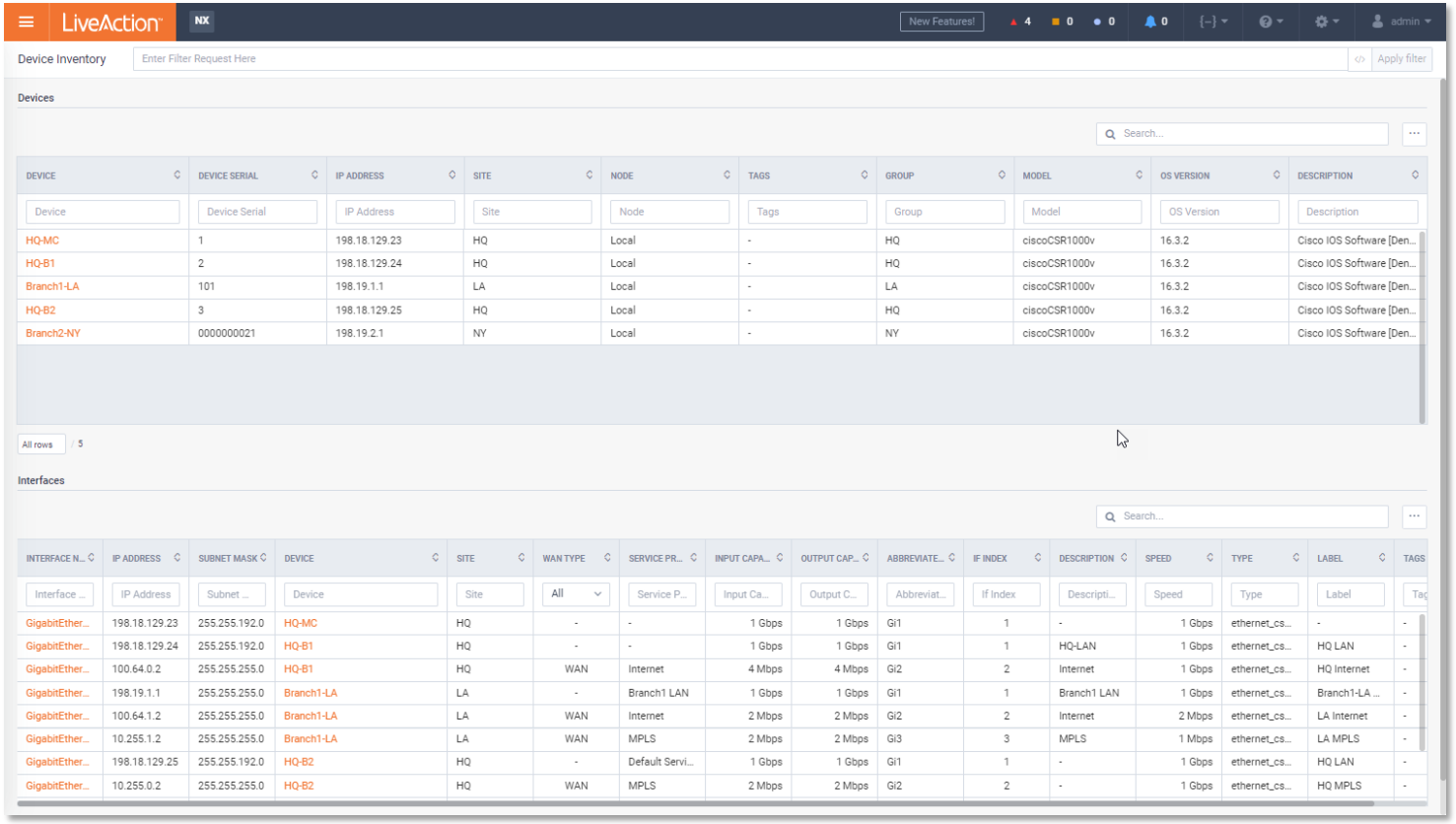
Geo Topology



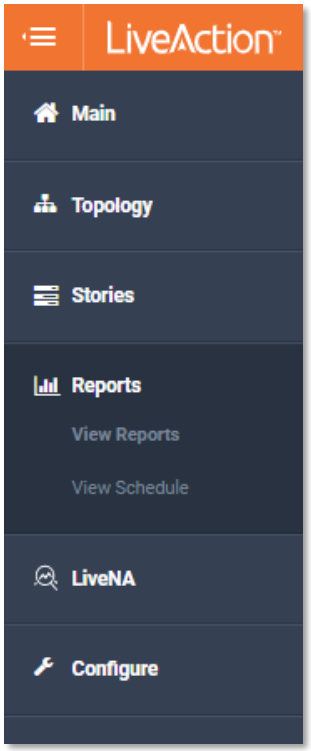


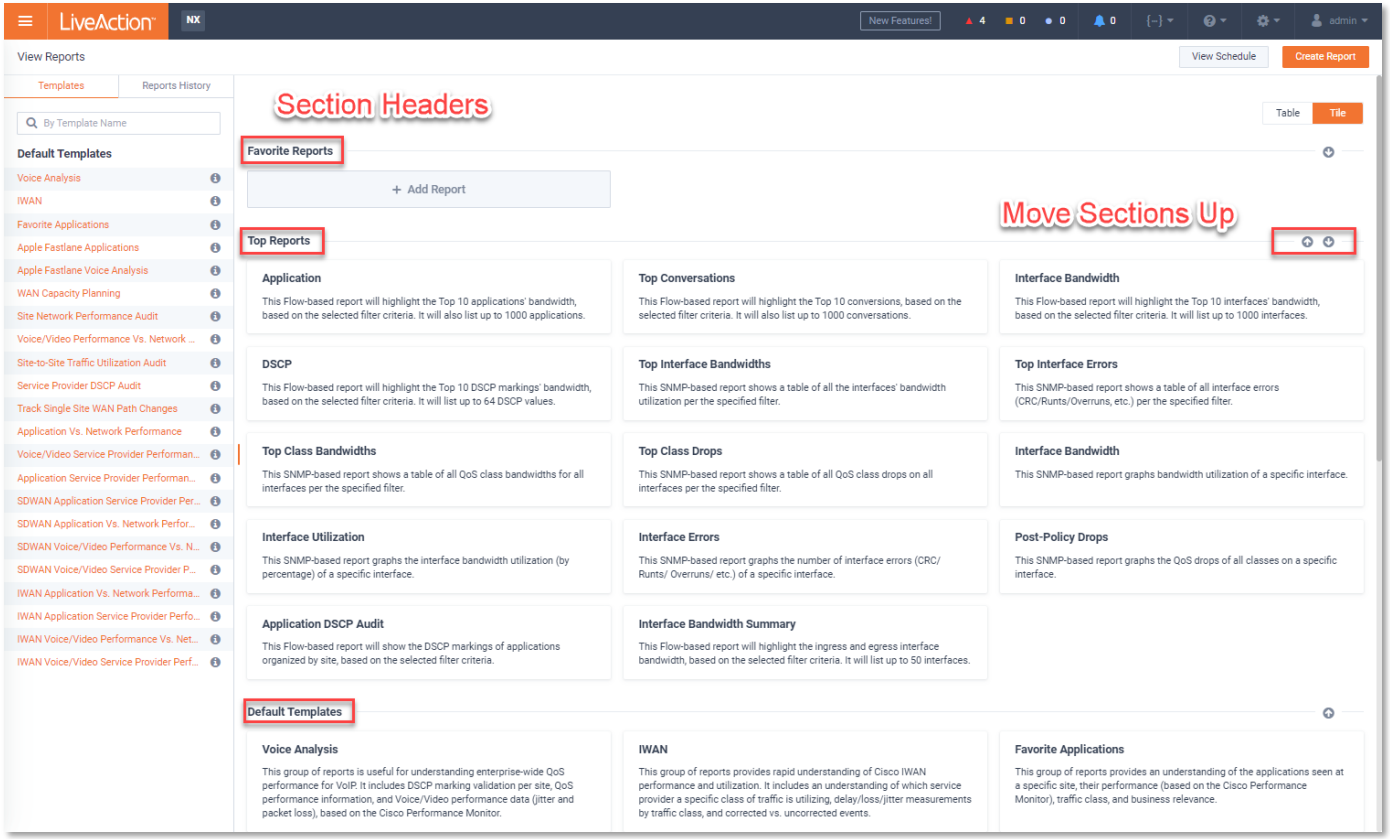
Stories



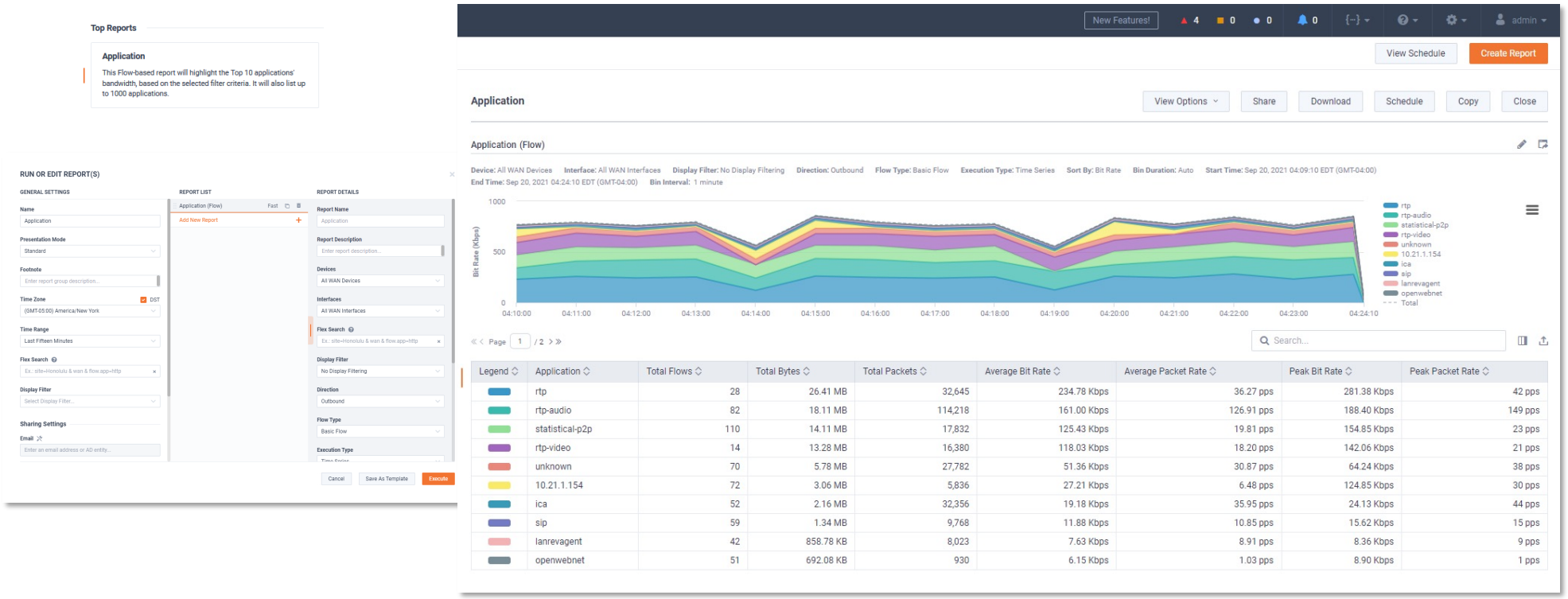


View ANY Report Defined in LiveNX



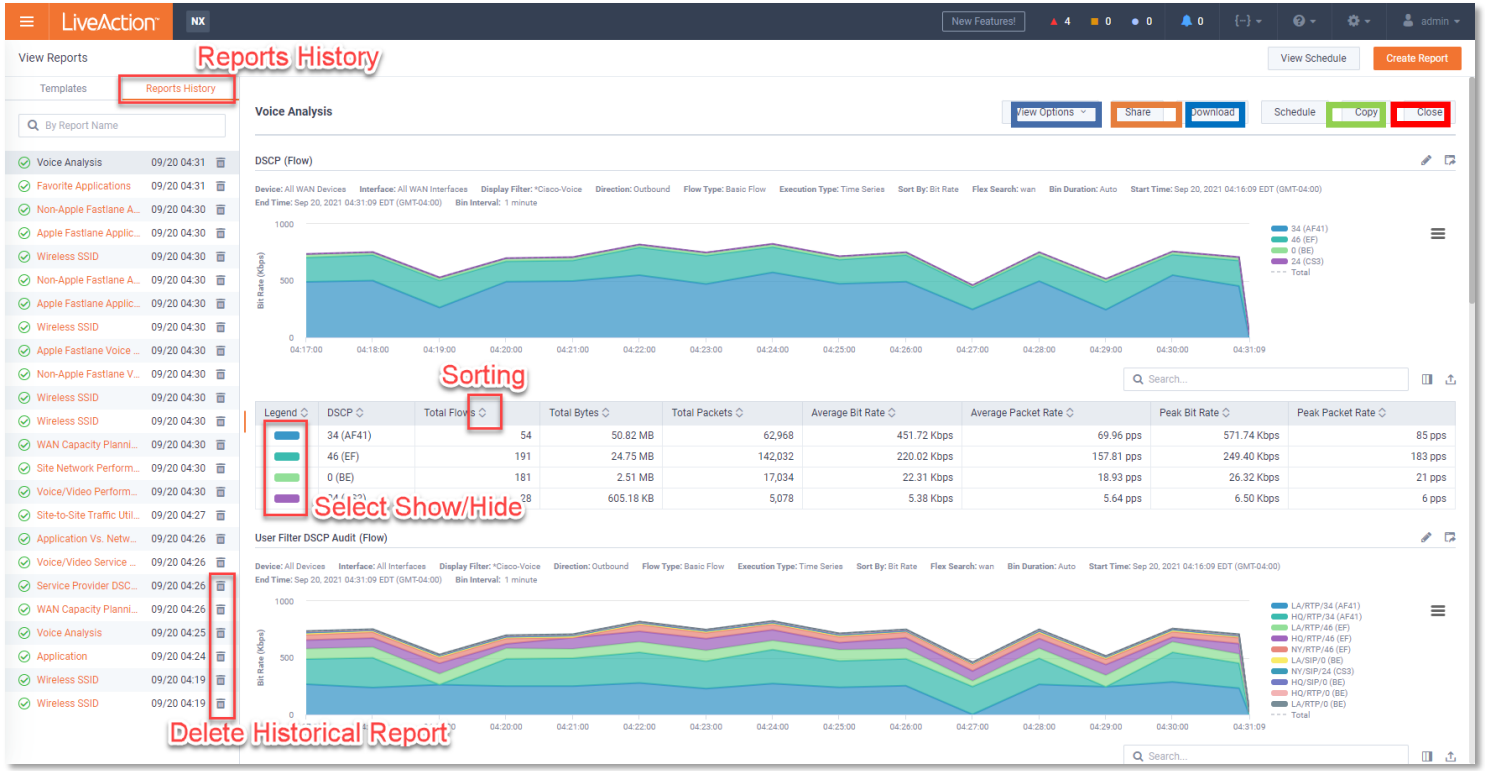


Run Reports…



Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	rtp	28	26.41 MB	32,645	234.78 Kbps	36.27 pps	281.38 Kbps	42 pps
	rtp-audio	82	18.11 MB	114,218	161.00 Kbps	126.91 pps	188.40 Kbps	149 pps
	statistical-p2p	110	14.11 MB	17,832	125.43 Kbps	19.81 pps	154.85 Kbps	23 pps
	rtp-video	14	13.28 MB	16,380	118.03 Kbps	18.20 pps	142.06 Kbps	21 pps
	unknown	70	5.78 MB	27,782	51.36 Kbps	30.87 pps	64.24 Kbps	38 pps
	10.21.1.154	72	3.06 MB	5,836	27.21 Kbps	6.48 pps	124.85 Kbps	30 pps
	ica	52	2.16 MB	32,356	19.18 Kbps	35.95 pps	24.13 Kbps	44 pps
	sip	59	1.34 MB	9,768	11.88 Kbps	10.85 pps	15.62 Kbps	15 pps
	lanrevagent	42	858.78 KB	8,023	7.63 Kbps	8.91 pps	8.36 Kbps	9 pps
	openwebnet	51	692.08 KB	930	6.15 Kbps	1.03 pps	8.90 Kbps	1 pps

WebUI Reporting – Tools



Include Report Elements

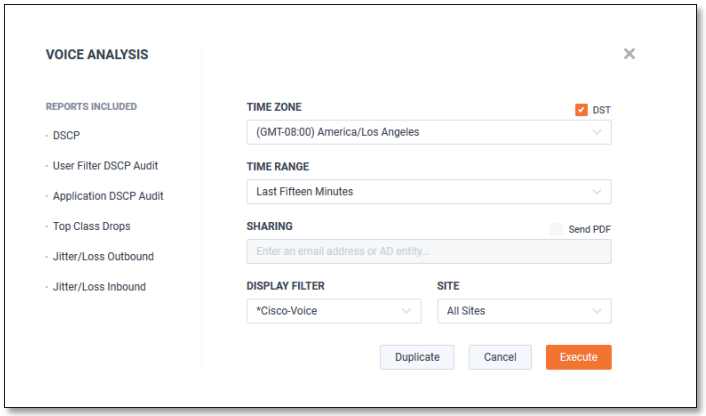
Copy URL to Clipboard

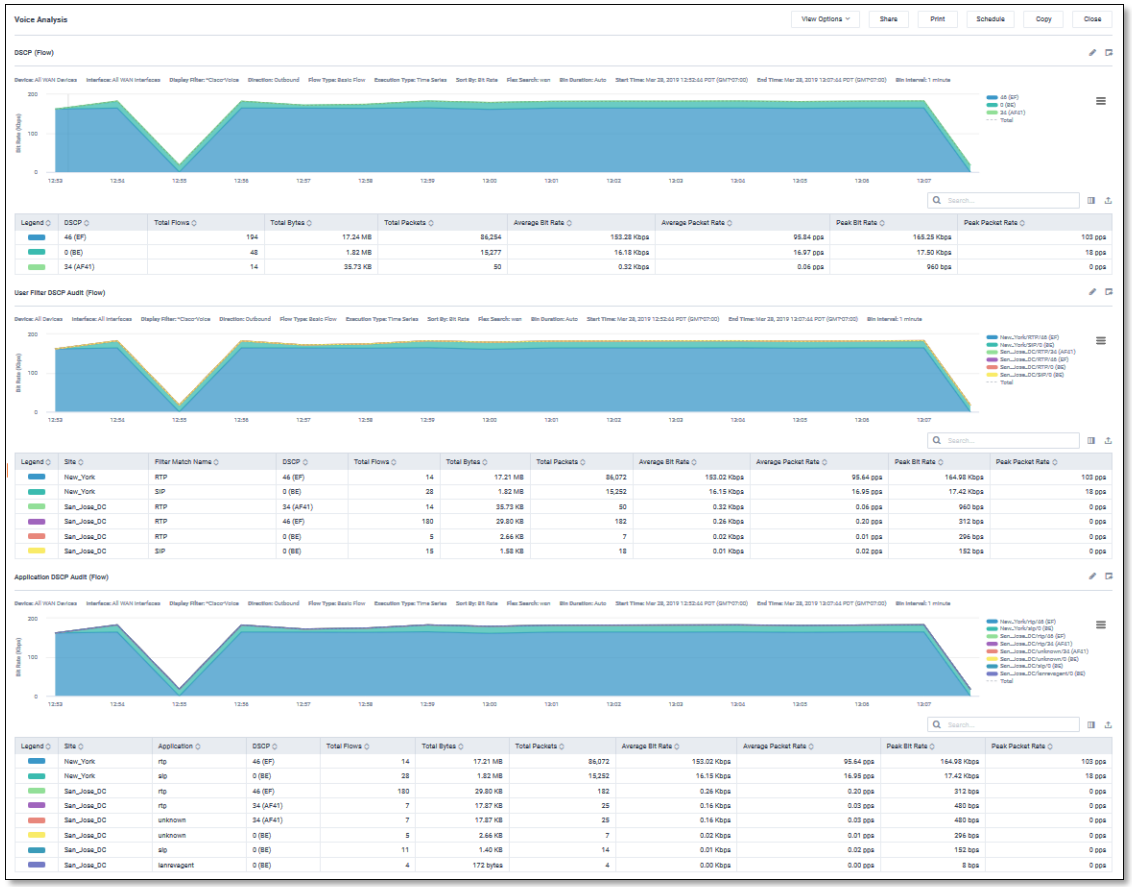
Print/Download (opens new URL)

Re-open Run Report Dialog

Return to Reports Entry Page

Report Groups



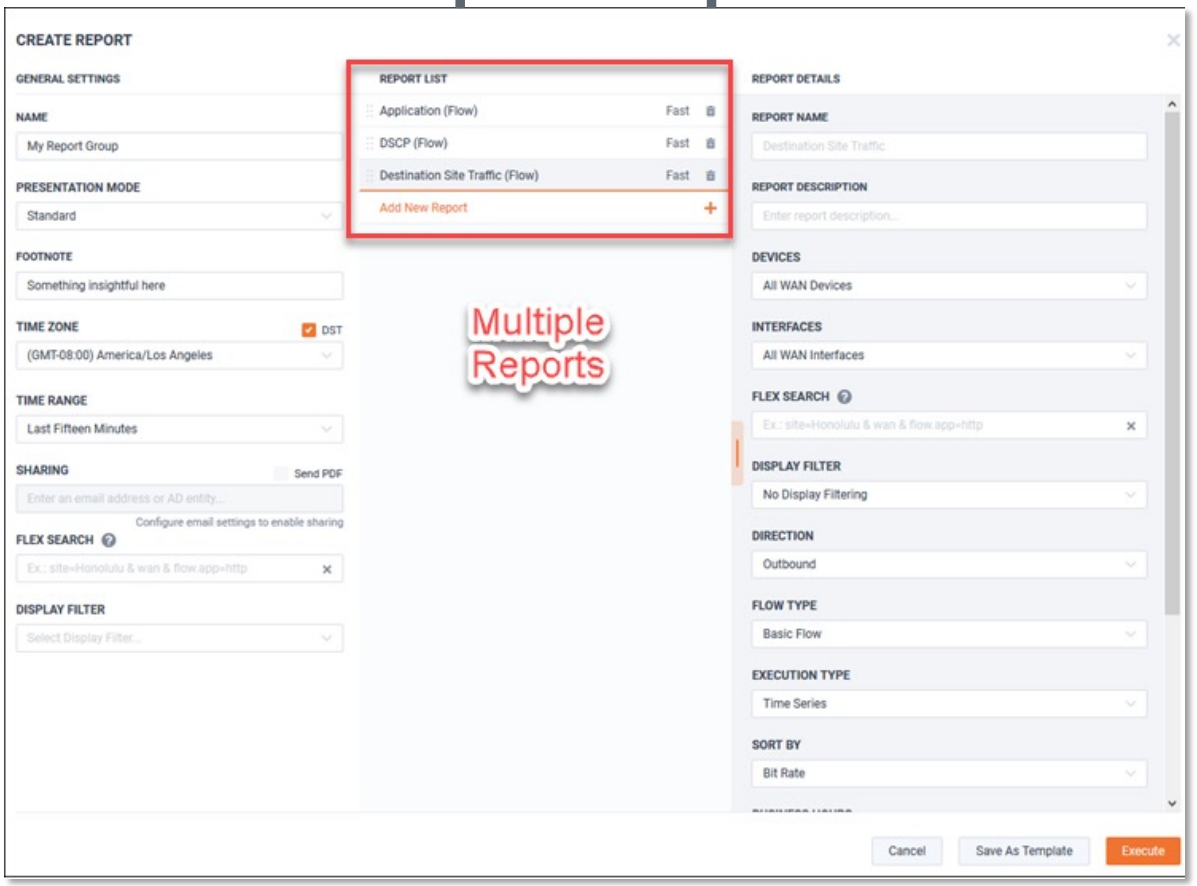


WebUI Reporting – Create & Groups of Reports

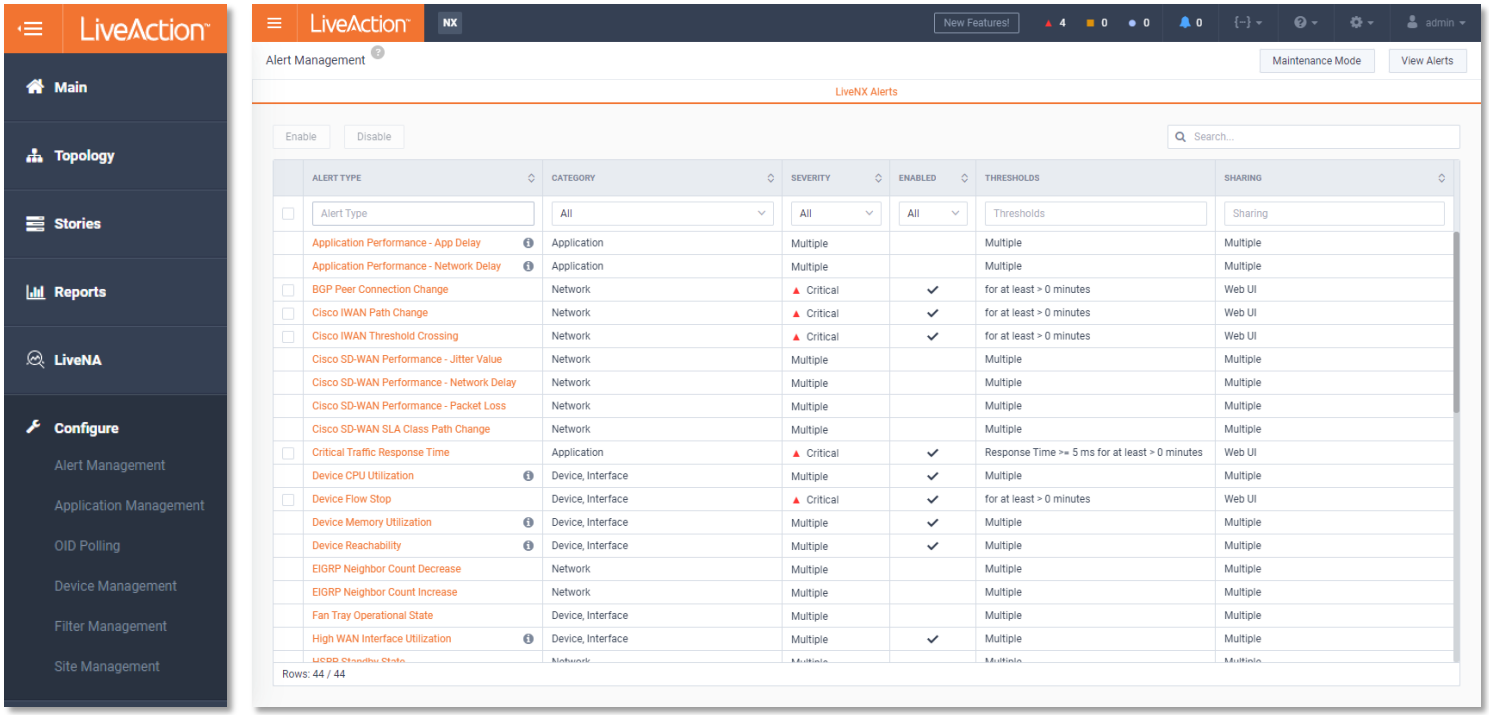
Schedule Group to run Now, Hourly, Daily, Weekly, or Monthly

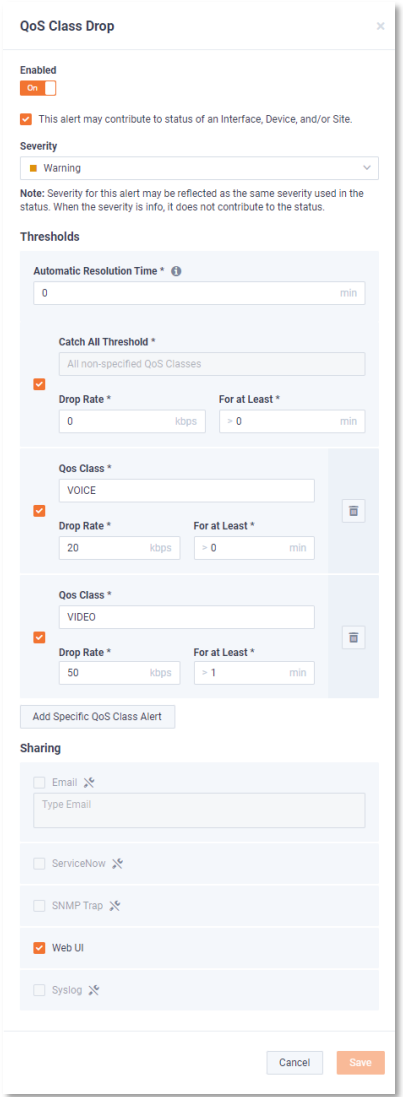
Advanced Report Group can be emailed to one or multiple users

Advanced Reports allow the creation of groups of reports



LiveNX Alerting





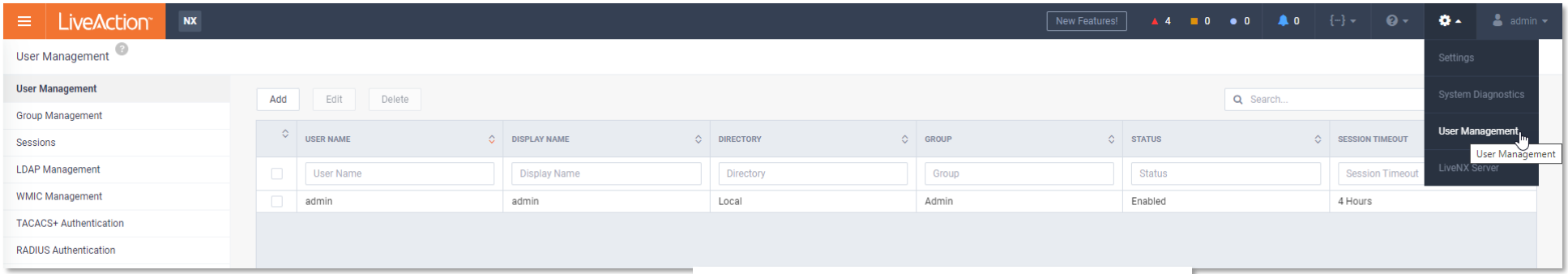
System Management

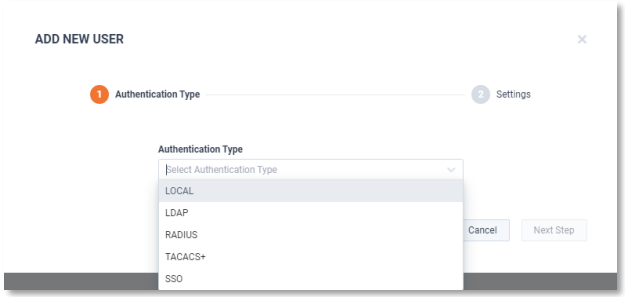
Using the WebUI to manage your LiveNX server and nodes

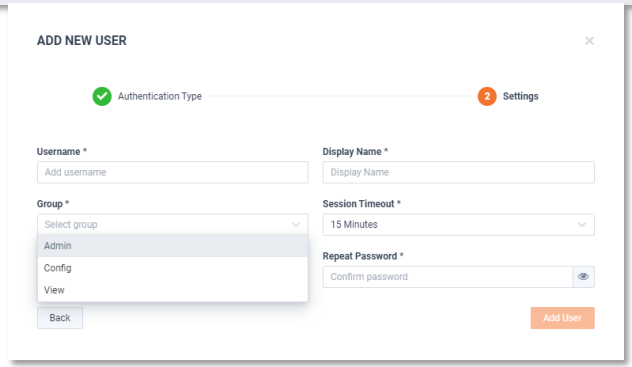
- User Management
- System Health
- System Support

User Management

- Supports Local, LDAP, SSO, TACACS+, and Radius Authentication
- 3 Levels – Admin, Config, View
- Current Logged In Users



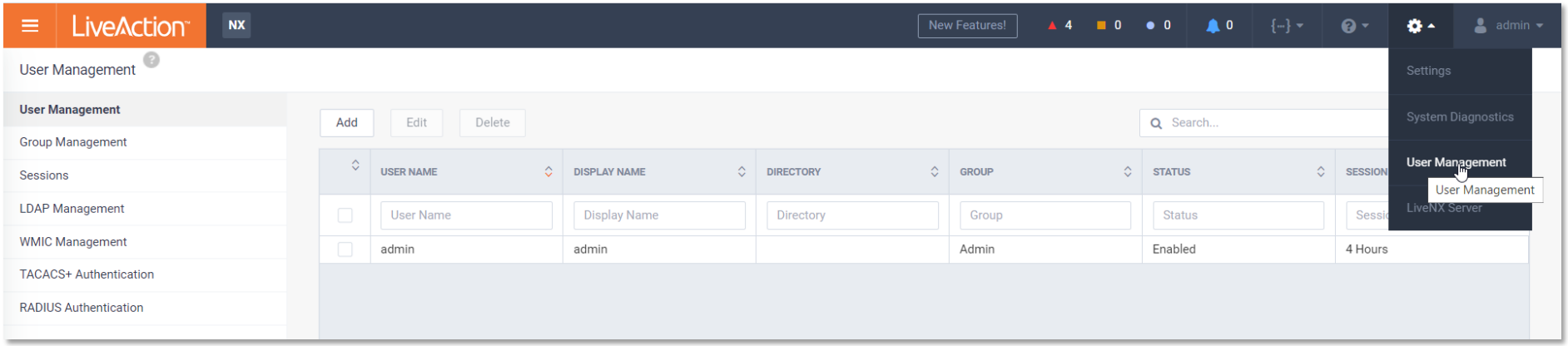




User Management

Local or LDAP

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

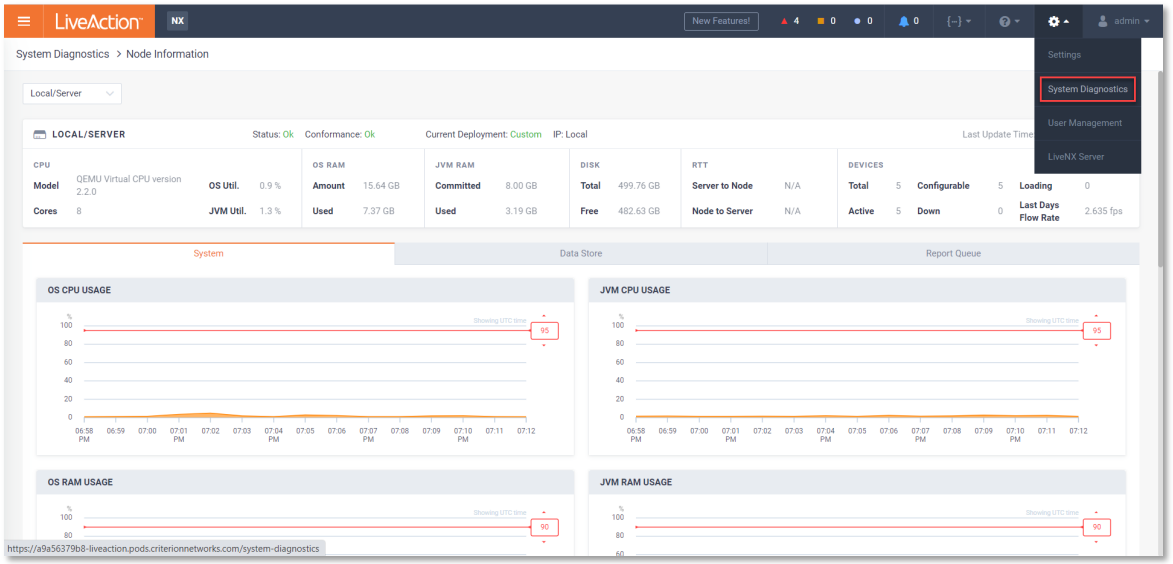


User Groups

- User Groups can be used to segment, or limit, the access of users in the group
  - Specific Sites
  - Specific Devices
  - Specific Regions
- Select entity pages can also allowed/omitted
- Select Reports can be allowed/omitted
- Users can be added from the Group Config page
- Users can only be in ONE group

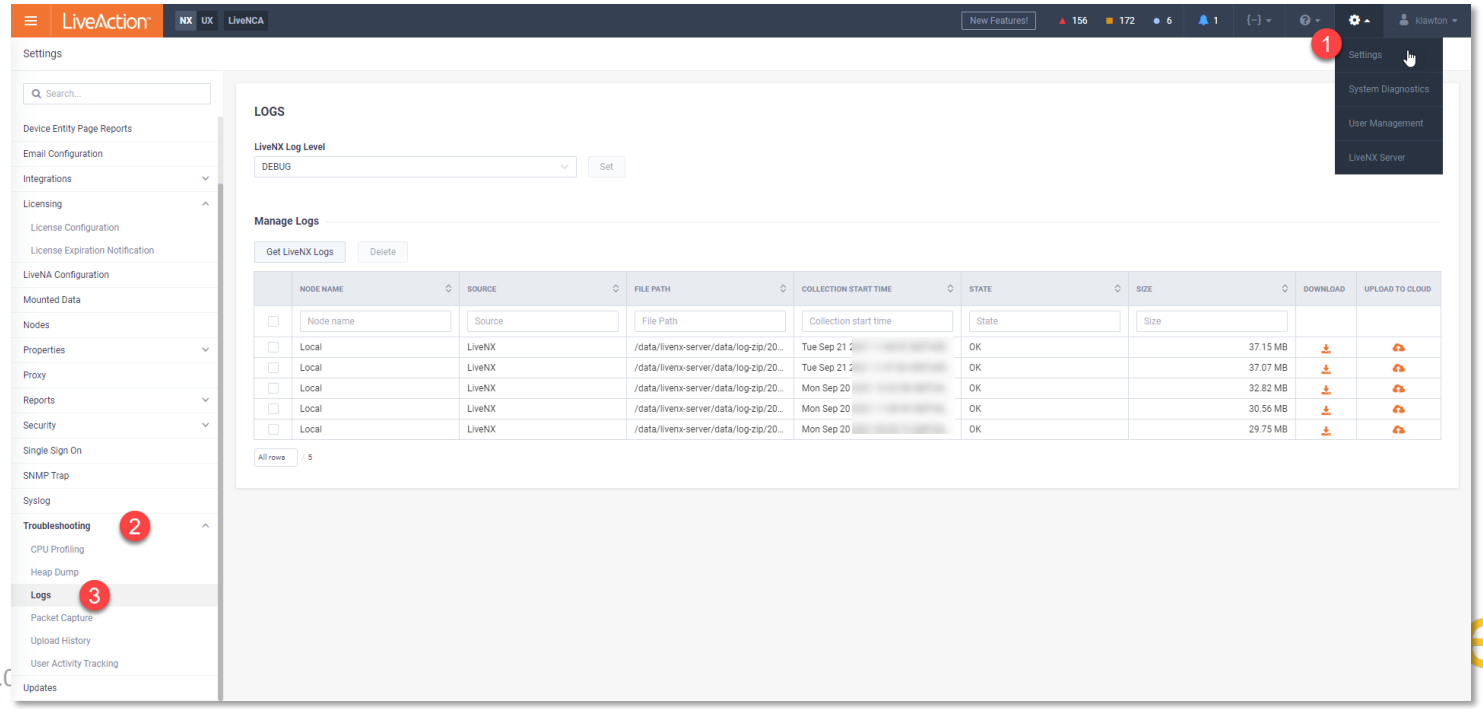
System Health

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



What to do when you need support

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



LAB 1: Using the Web UI

- View & Create Reports
- Look at Stories
- User Management
- View/Modify Alerts
- System Information

The LiveNX Engineering Console

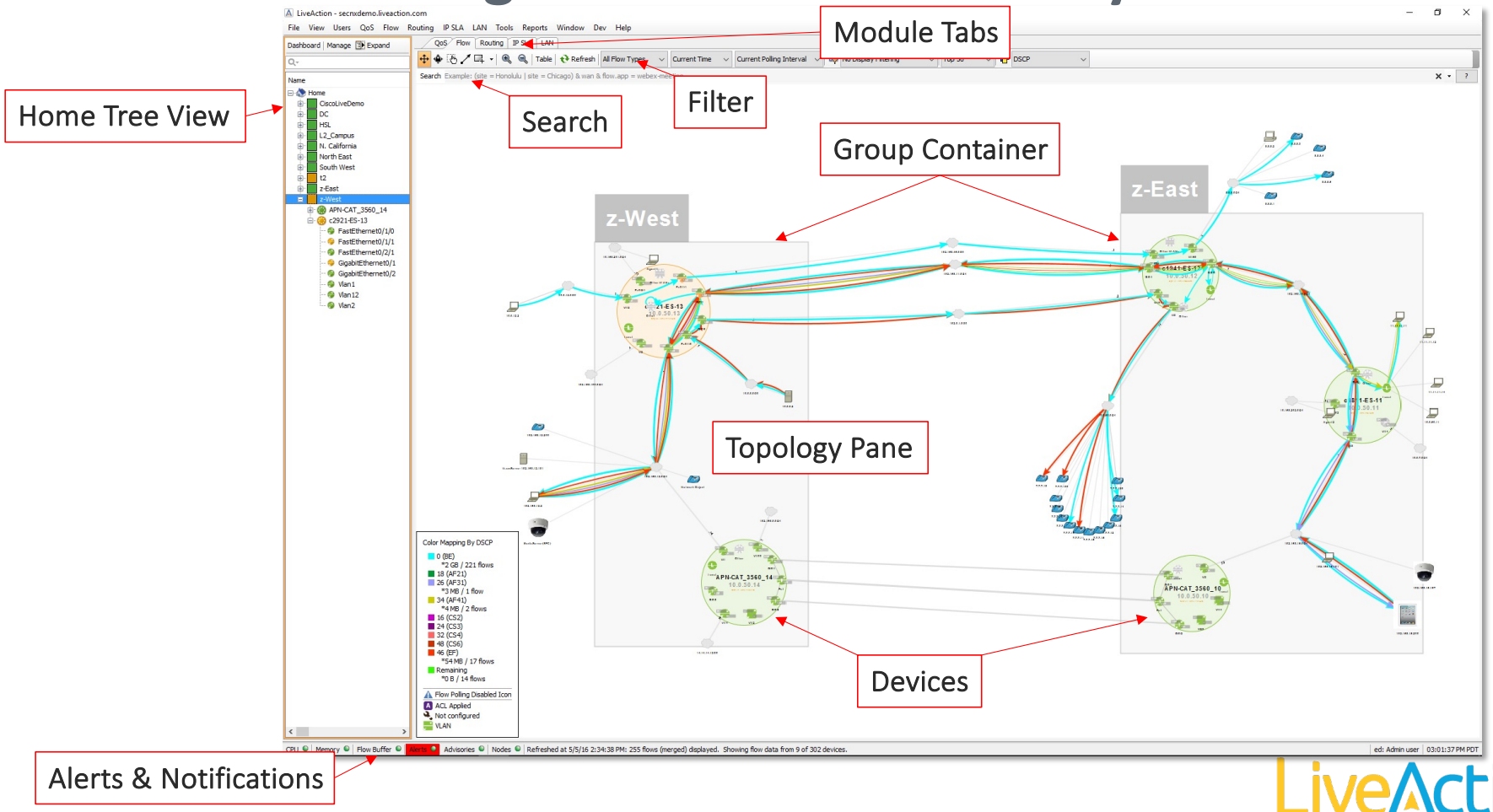
LiveAction™

The LiveNX Client is… Your Device Configuration Tool

- A Java client application
- Runs on a standard Windows 32/64-bit PC
  - LiveAction's Mac client runs on OSX .9+.
- View & Configure:
  - Devices (can access CLI and configure your devices)
  - Alerts
  - Reports

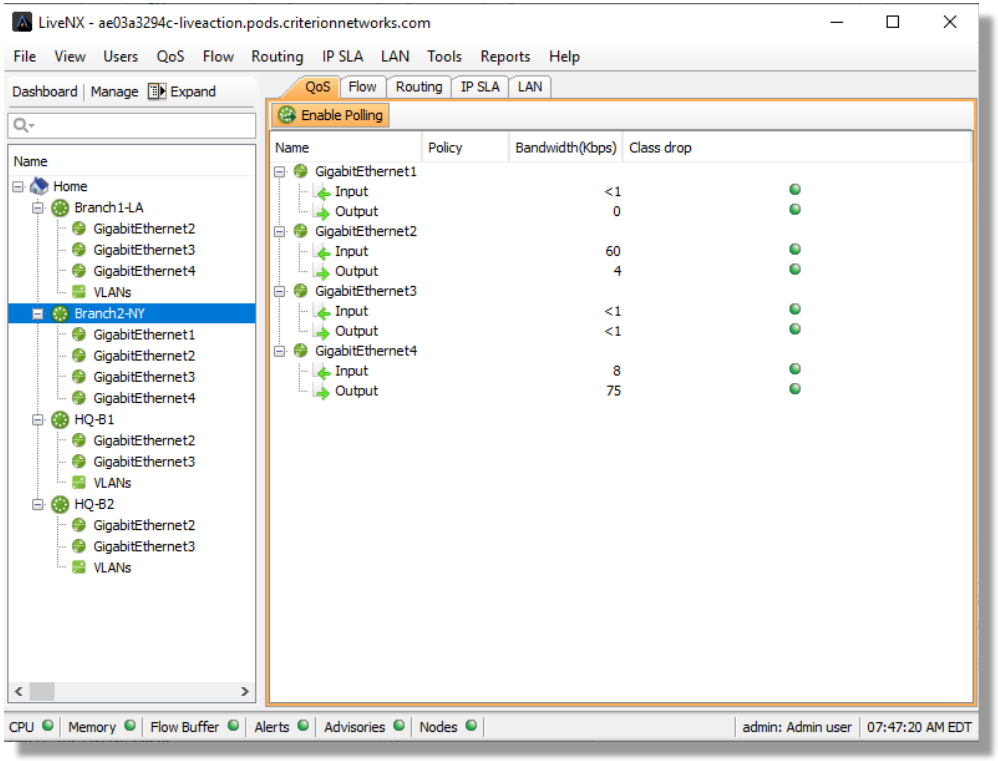
Visualization Philosophy: Shows all, remove what you don't need to see

The LiveNX Eng Console Can Be A Busy Place…



The Home Tree-view

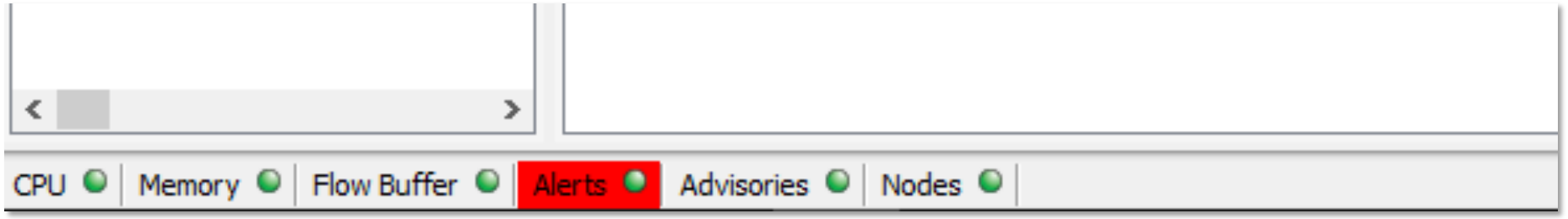
- Groups
  - Devices
    - Interfaces
- Select Home to view all Groups/Devices in the Topology Pane
- Select & Modify Devices & Interfaces
- Right-click Zoom-to…



Immediate Feedback…

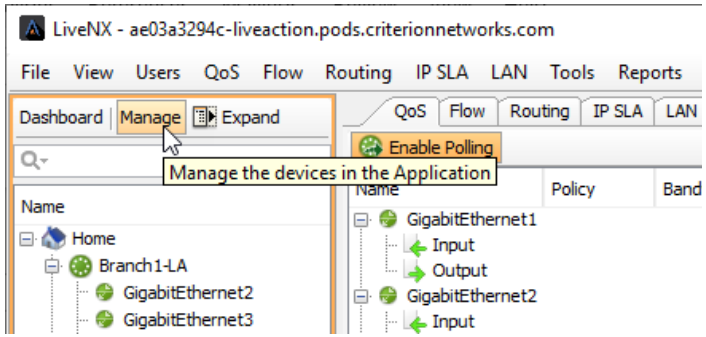
Look at the bottom of the screen for information about:

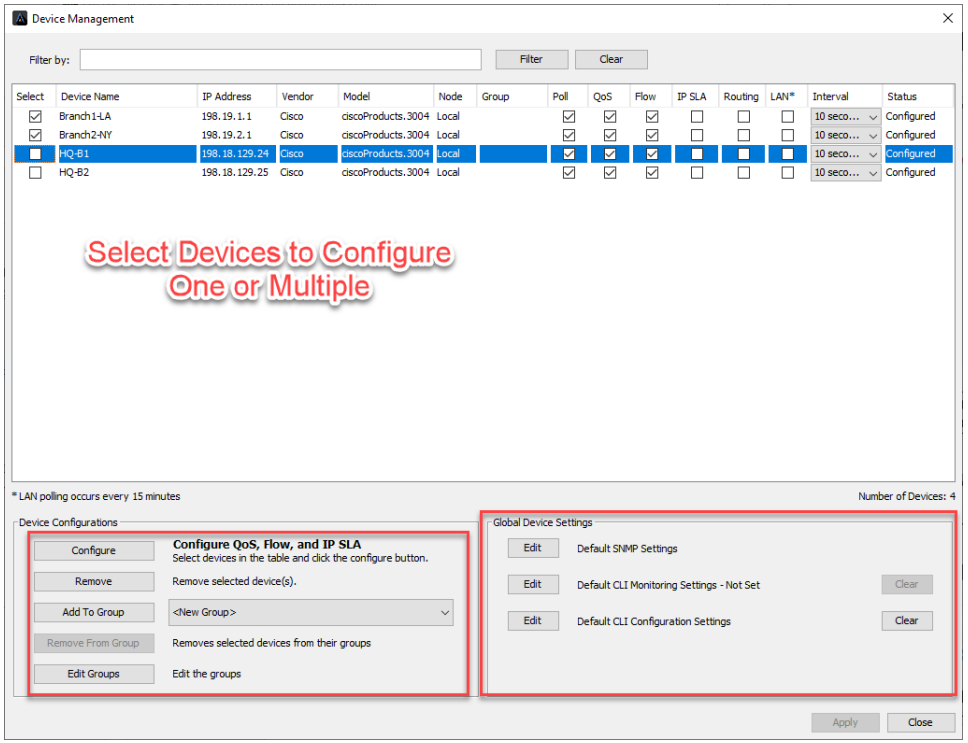
- CPU
- Memory
- Buffer
- Alerts
- Advisories
- Nodes



Main Configuration Tool

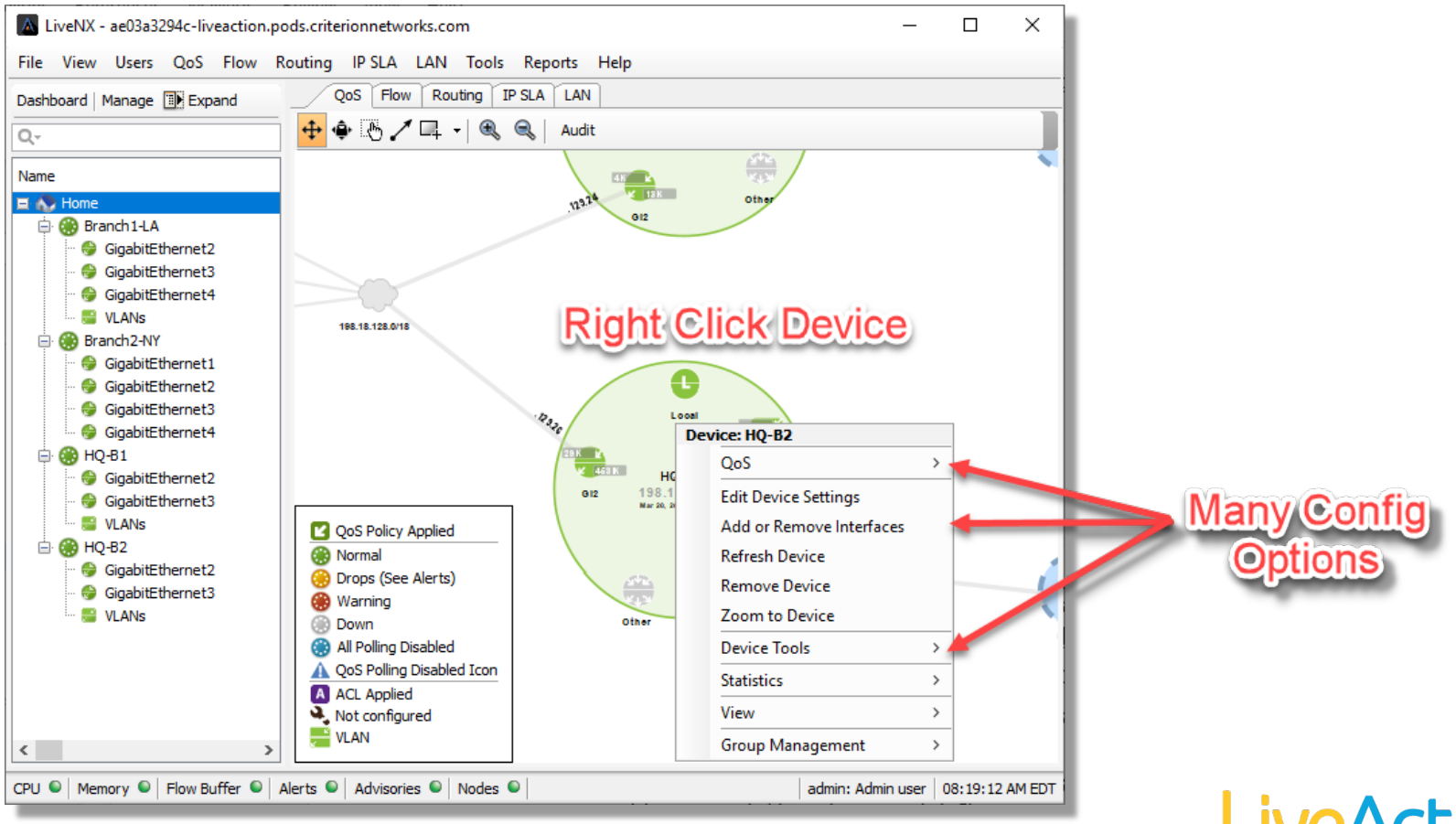
Click **Manage** to open **Device Management** window



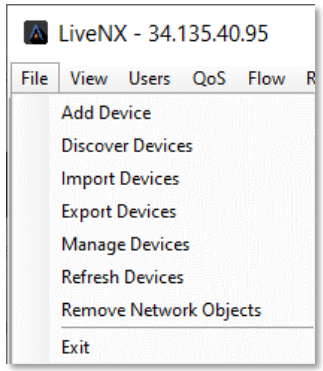


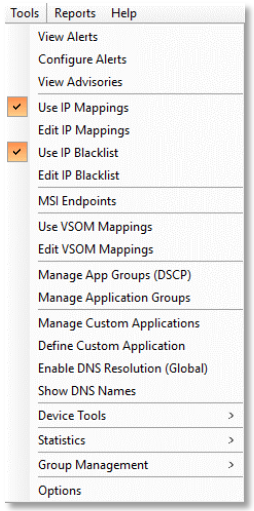
We will use the **Configuration** capabilities extensively in the class

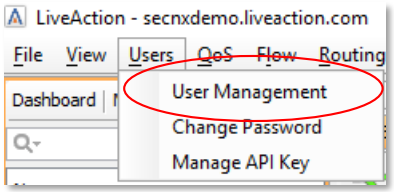
Configuration of Flow

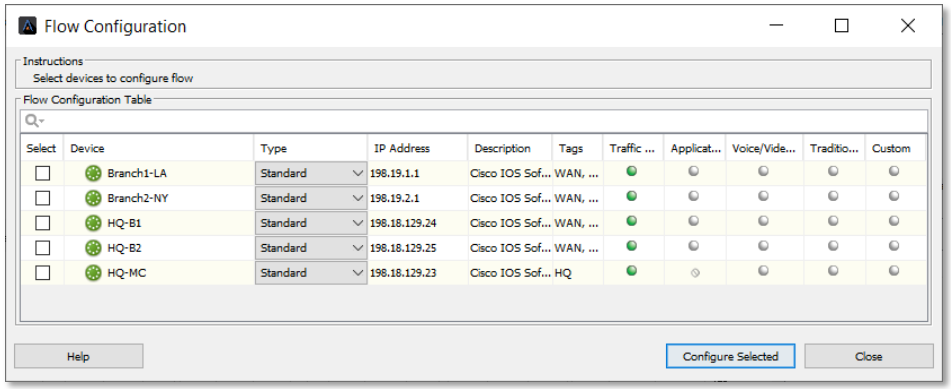


Manage, Create, View, Provision

* 

* 

* 



* Also Configurable in the WebUI!

LAB 2: LiveNX Engineering Console

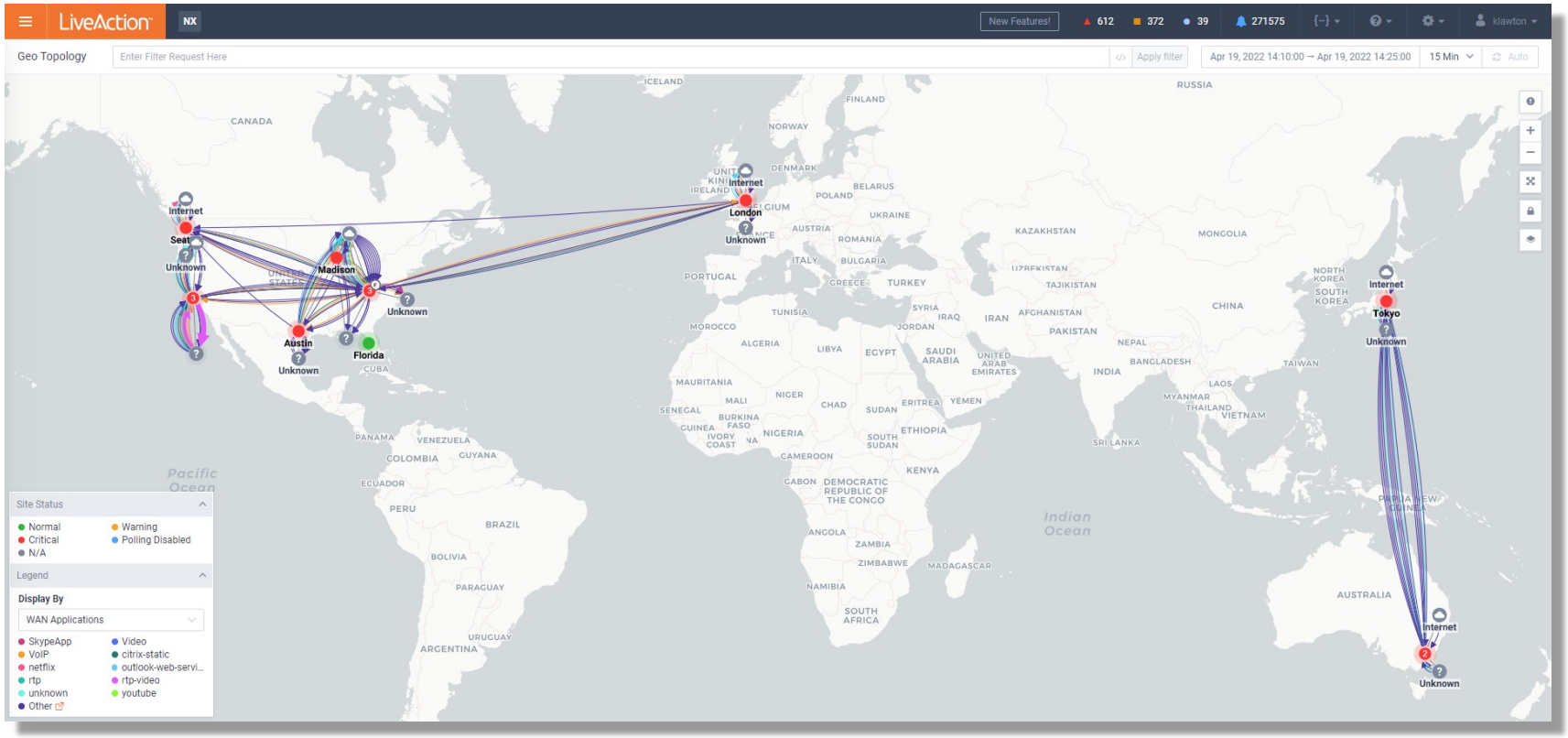
- Launch the LiveNX Engineering Console
  - Connect from your Desktop…
- Explore Engineering Console

Visualizations

LiveAction™

Flow Visualization

End-to-End Application Flows Through the Network

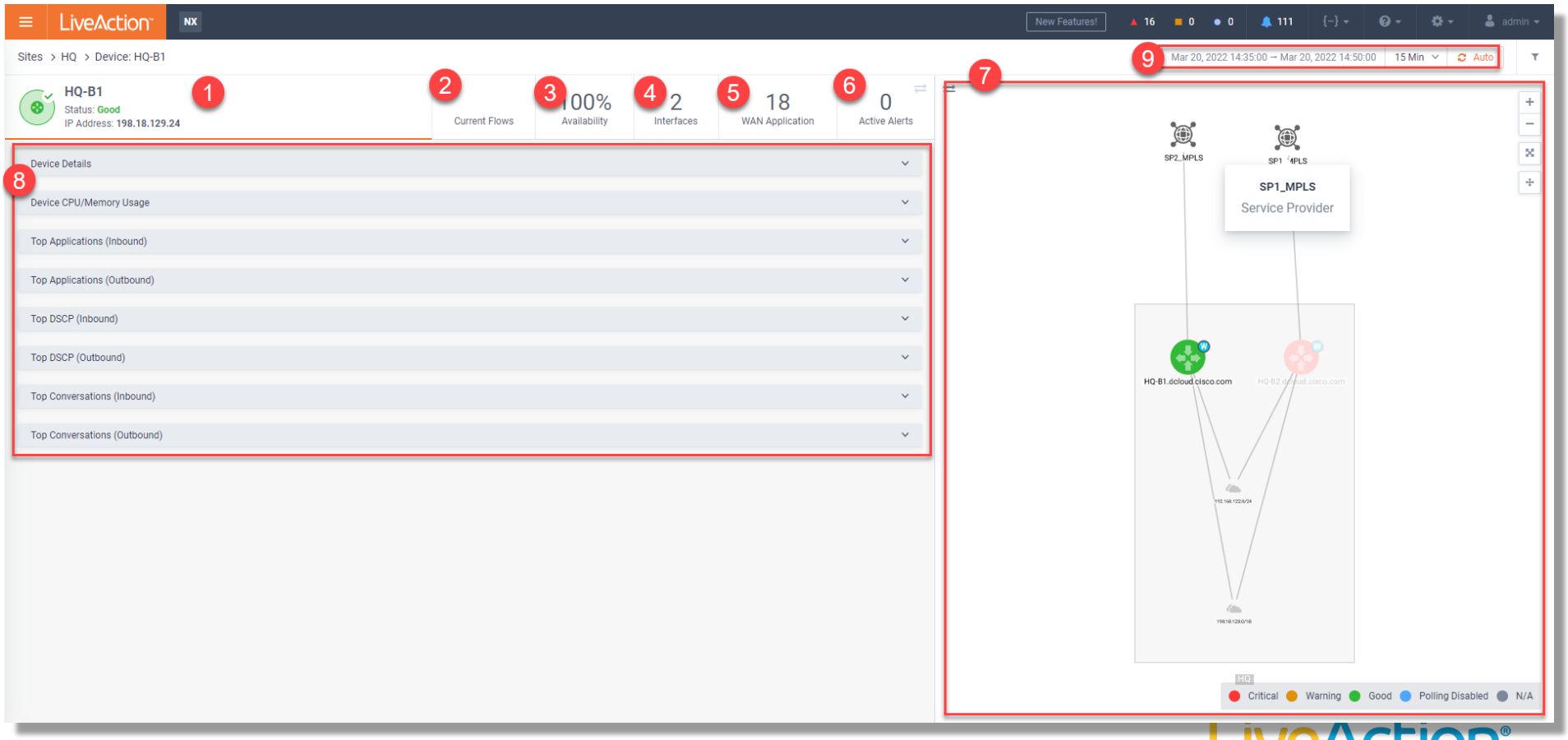


LiveNX discovers and draws topology based on SNMP

LiveNX imposes end-to-end flows on topology

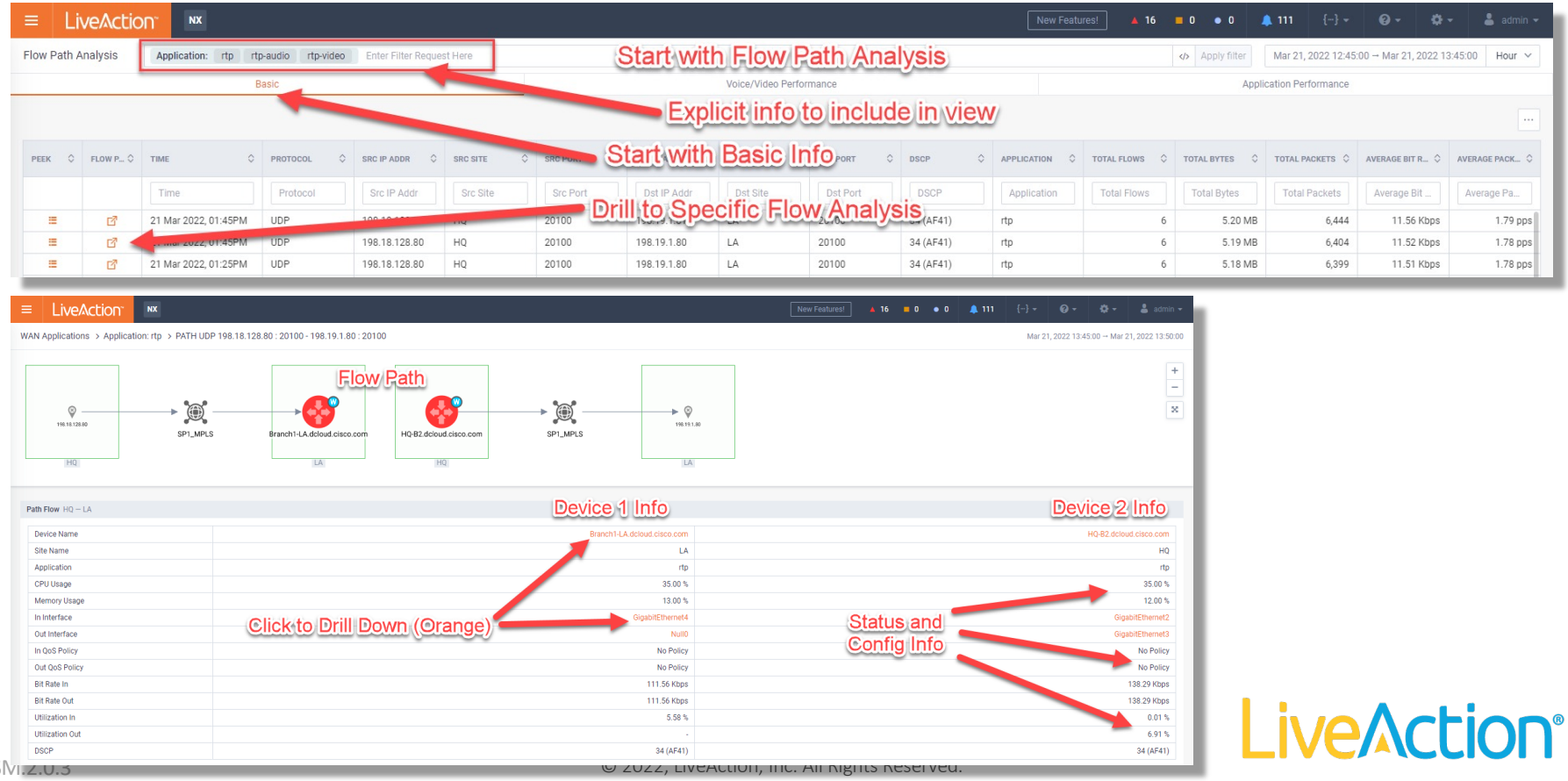
LiveAction®

Device Entity Pages

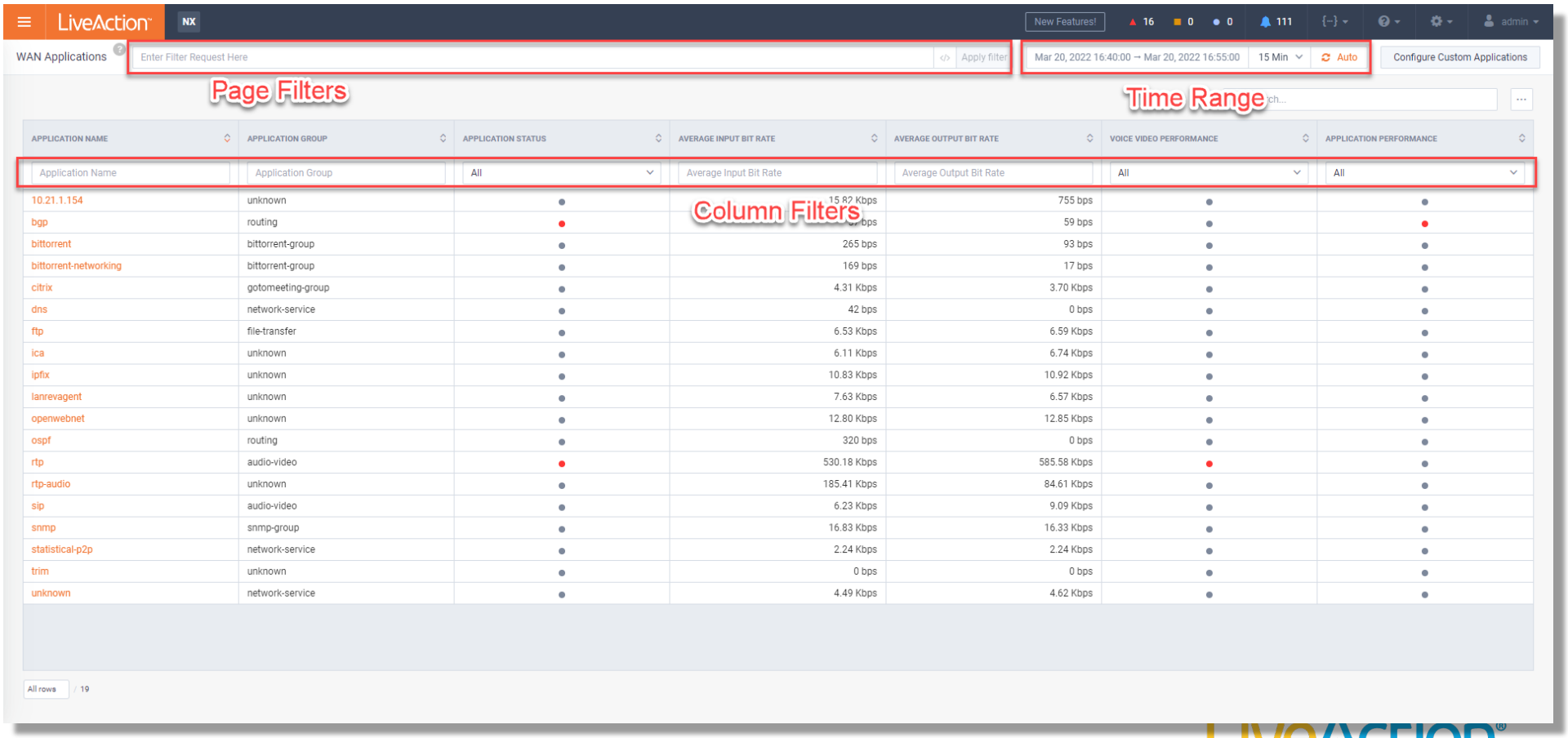


Flow Troubleshooting, Decision Making

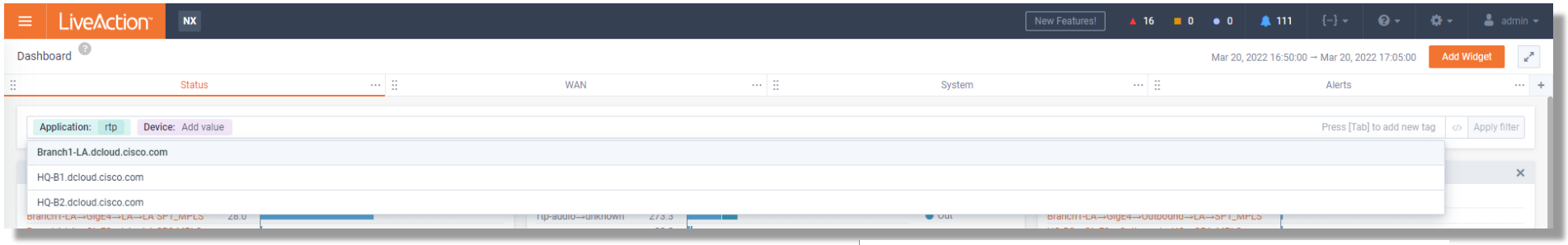
Start with what you know about the issue

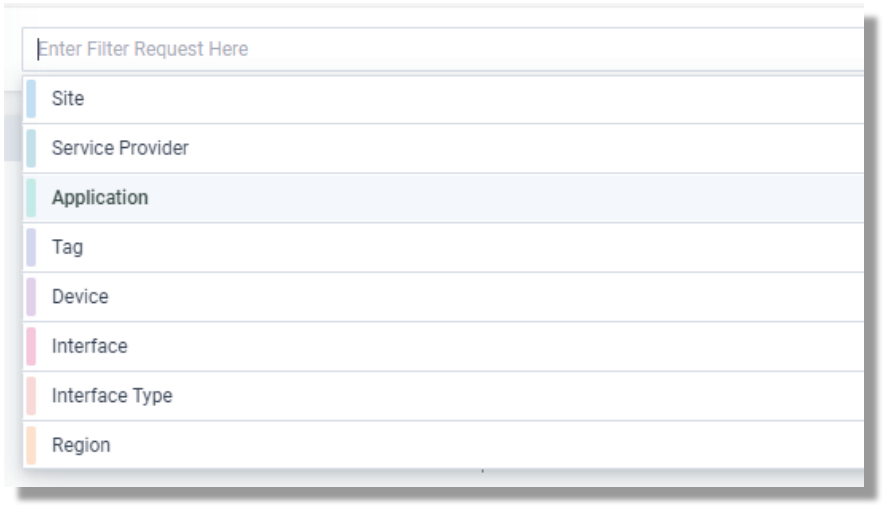


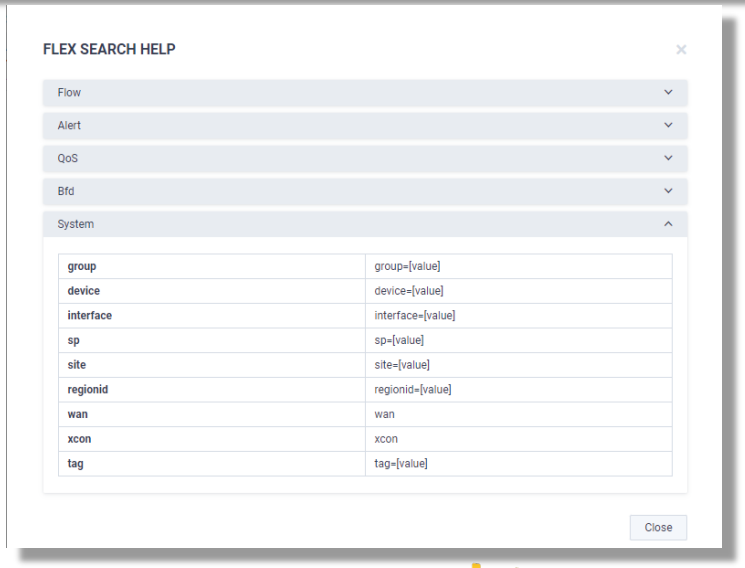
Eliminate the Detractors!



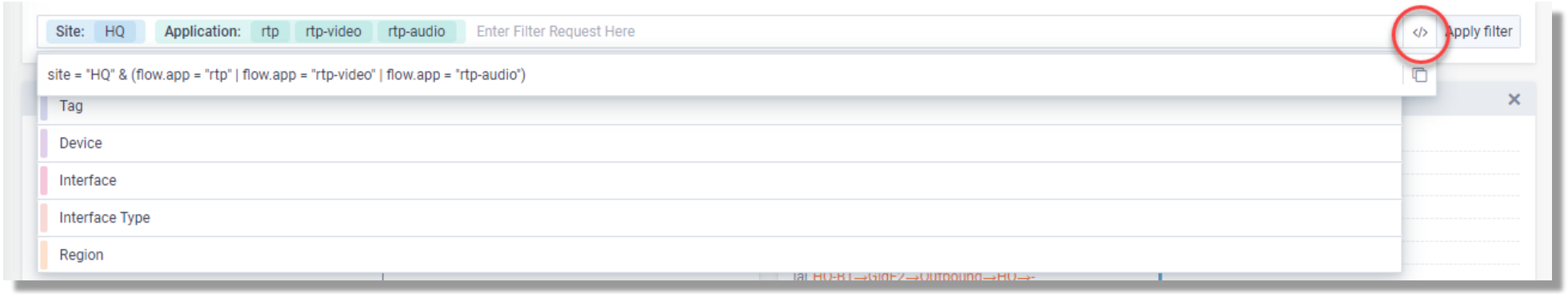
The Search Field







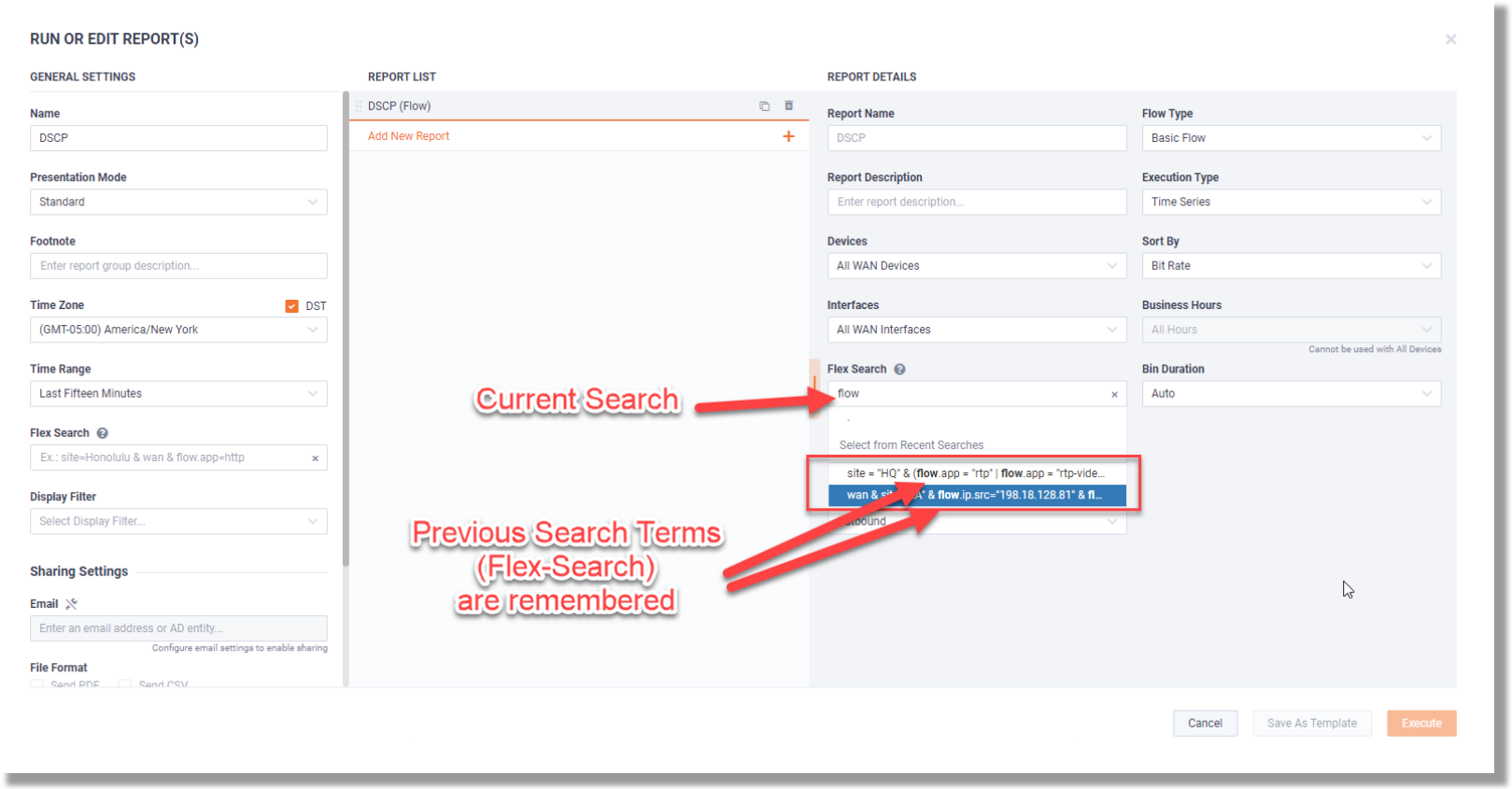
Search Functions and Flex Search



Create a simple page search, and convert to more powerful Flex-Search

1) Enter Page Filter Terms
2) Click </> to view the equivalent Flex-Search String

Filters & Search Retention In Reports

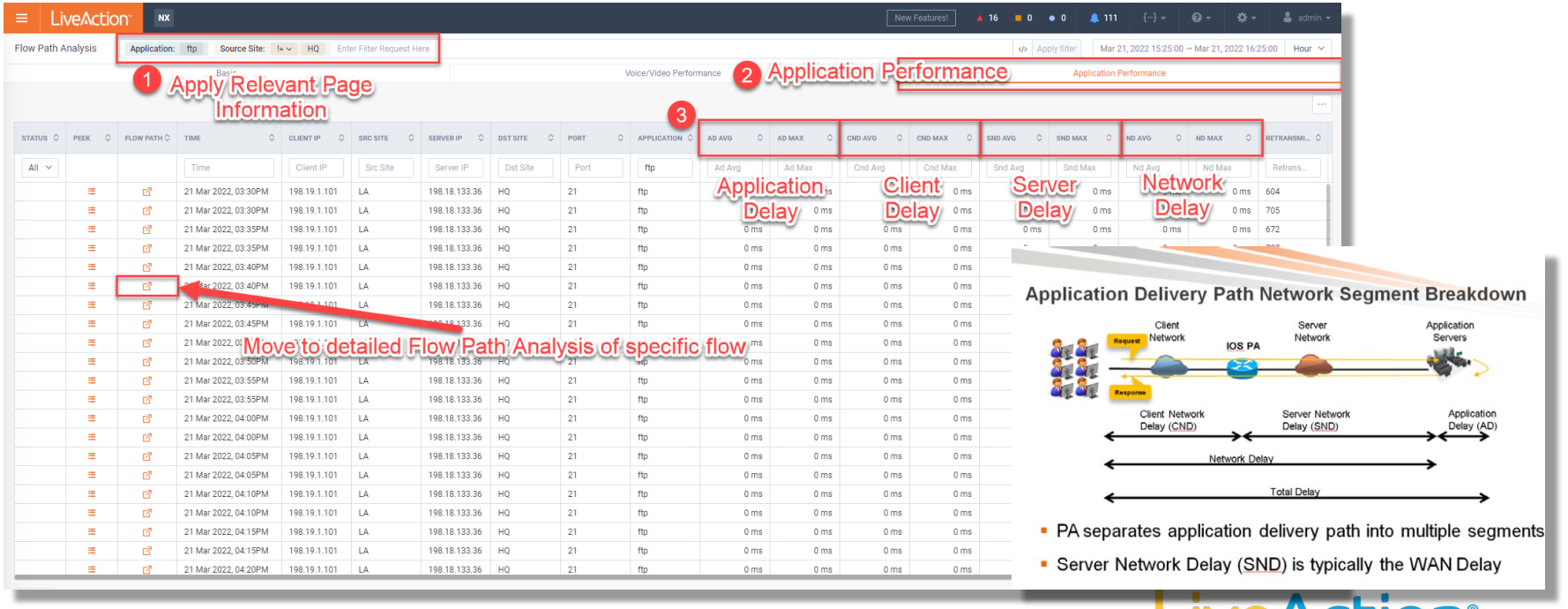


Application Performance (AVC Based) Visualization

Start with Flow Path Analysis

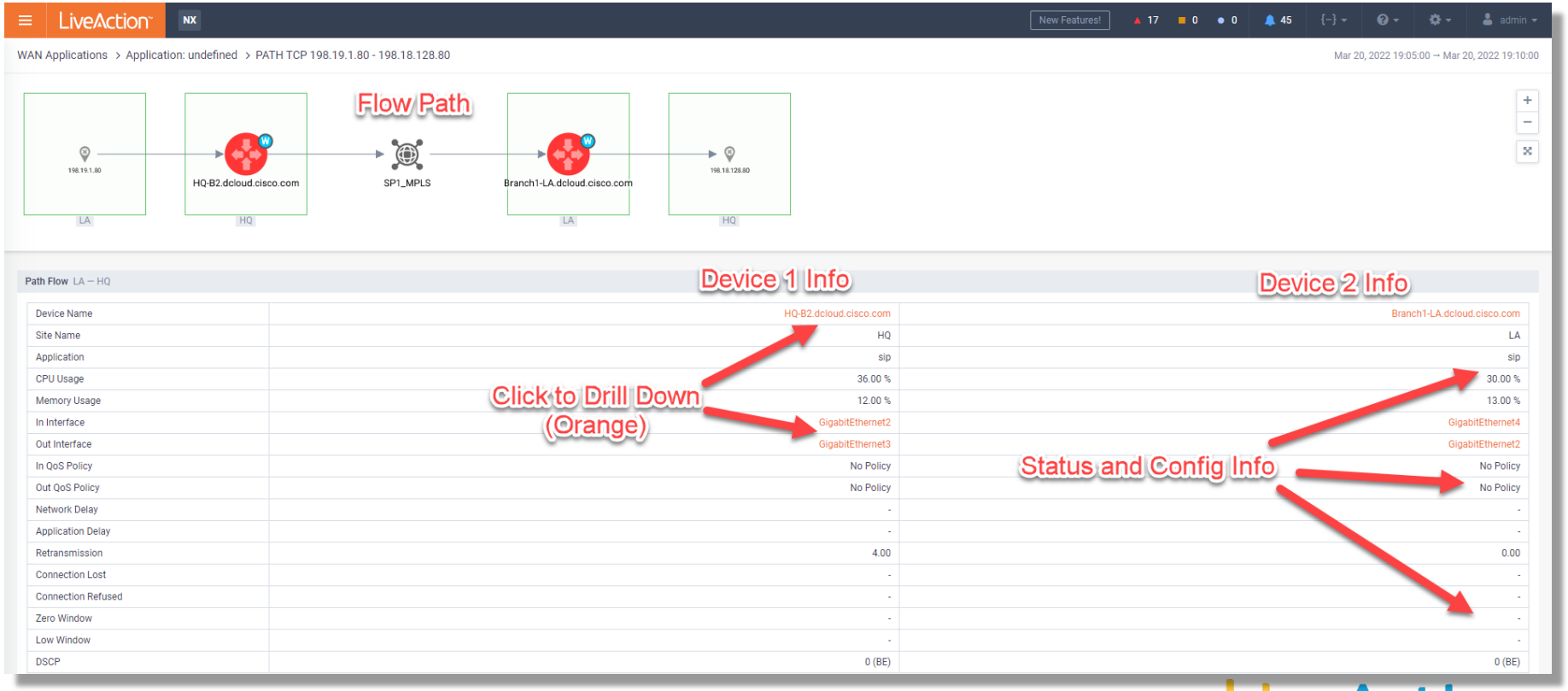
Use the Page Filter to display the interesting traffic flows

Use column filter/sort to reveal the specific flows to look at



Flow Visualization

Specific Flow Details – Devices in Flow – Interfaces, Parameters, Status

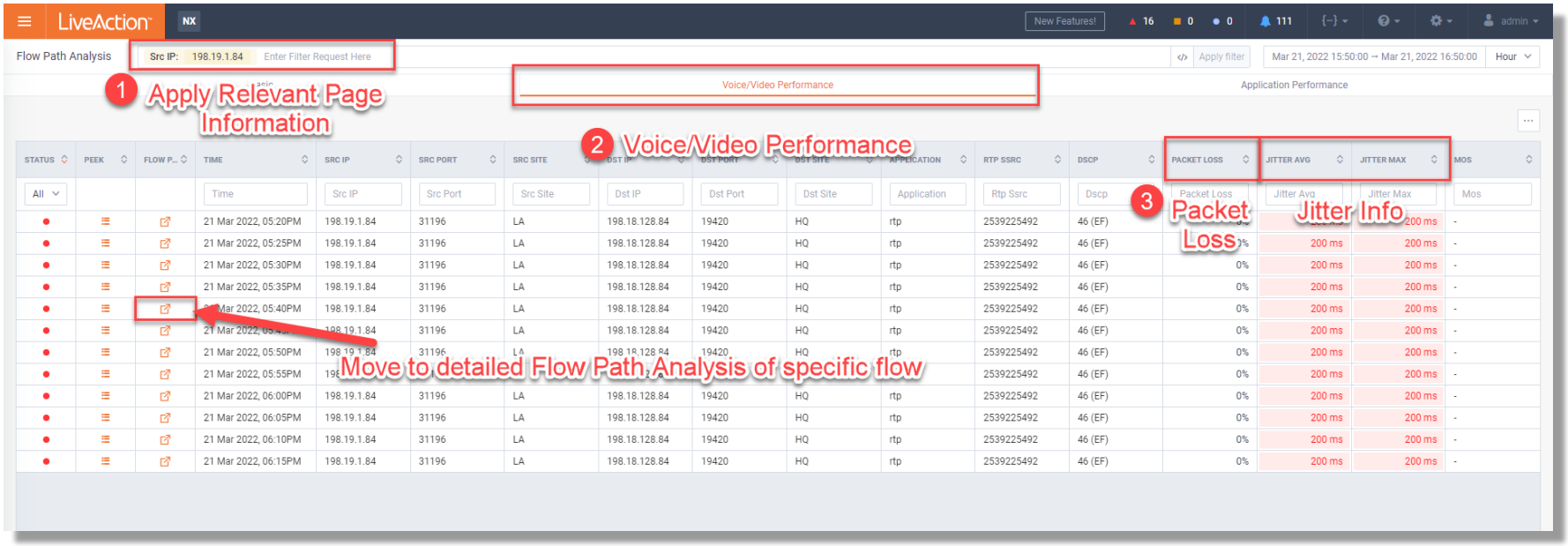


Voice/Video Performance (MediaNet Based) Visualization

Start with Flow Path Analysis (If no data – review the Page Information used)

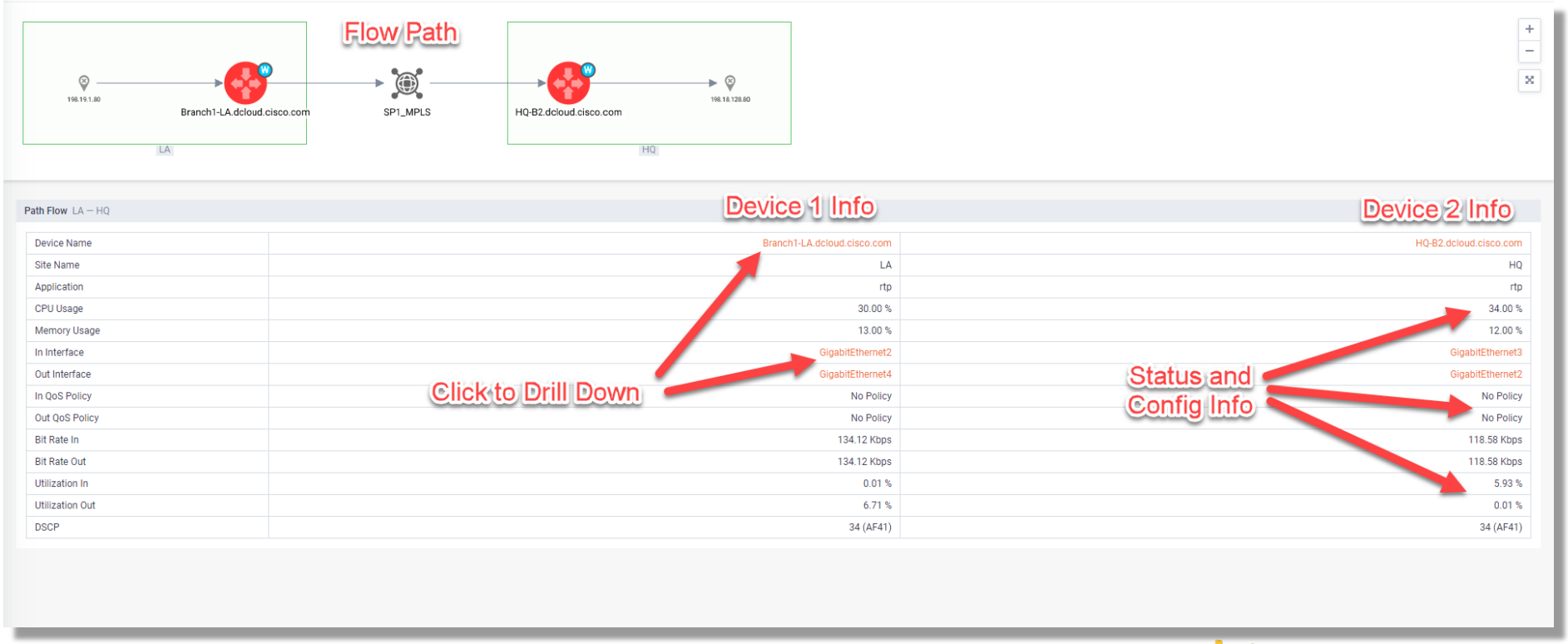
Use the Page Filter to display the interesting traffic flows

Use column filter/sort to reveal the specific flows to look at

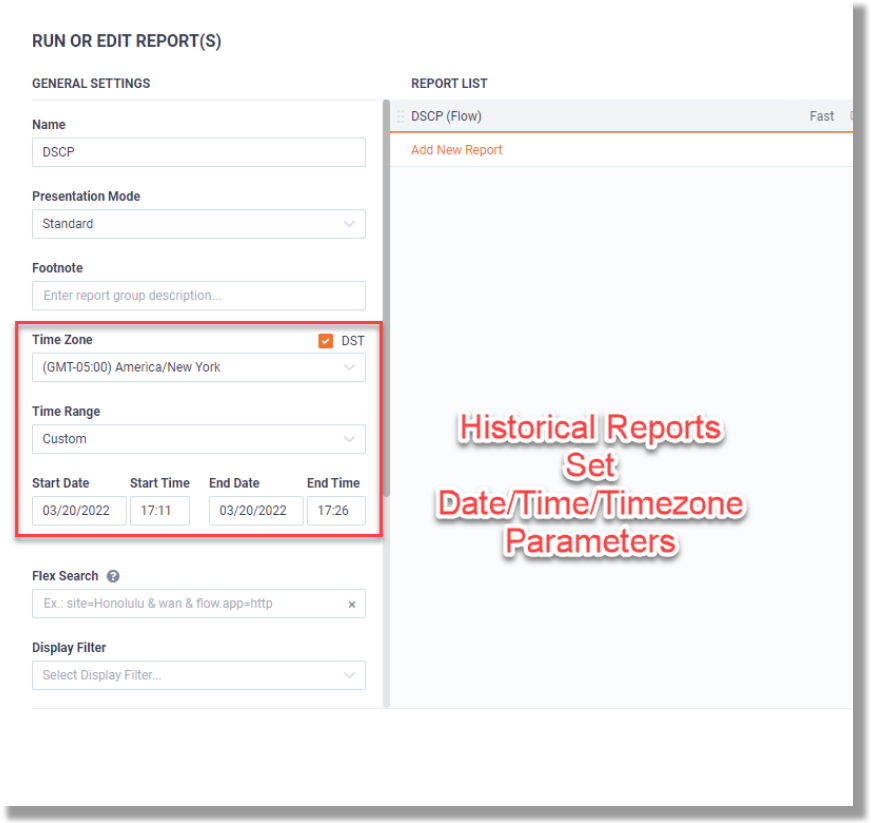


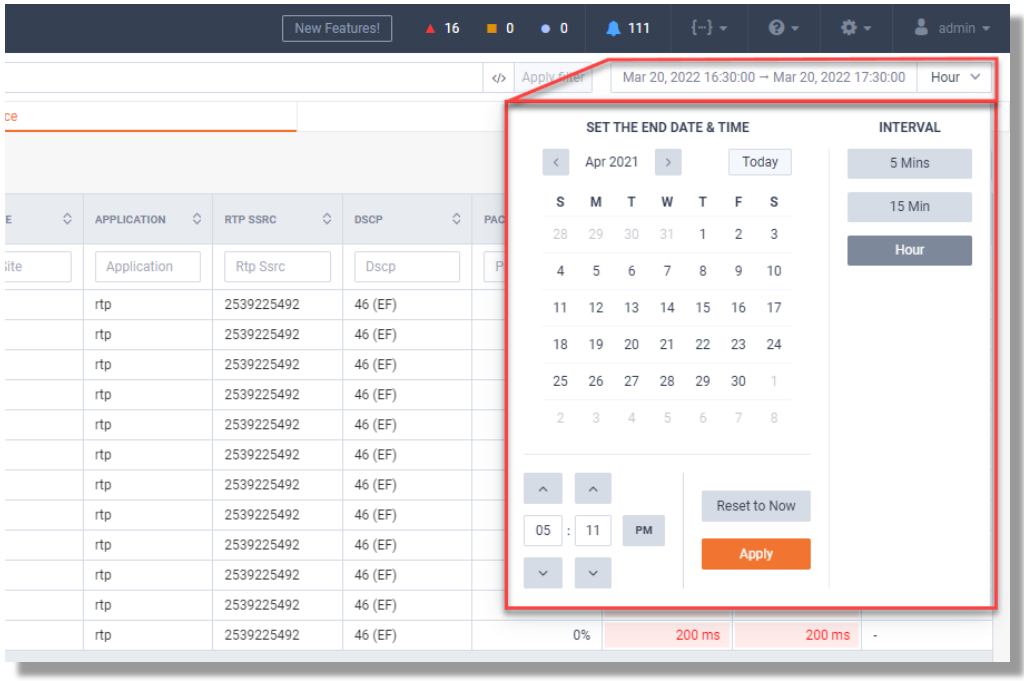
Flow Visualization

Specific Flow Details – Devices in Flow – Interfaces, Parameters, Status



Flow History– Reports and Stories





Device Configuration

LiveAction™

LiveNX WebUI – Perspective

LiveNX through the WebUI acts as a framework to help you visually monitor and troubleshoot your network devices…

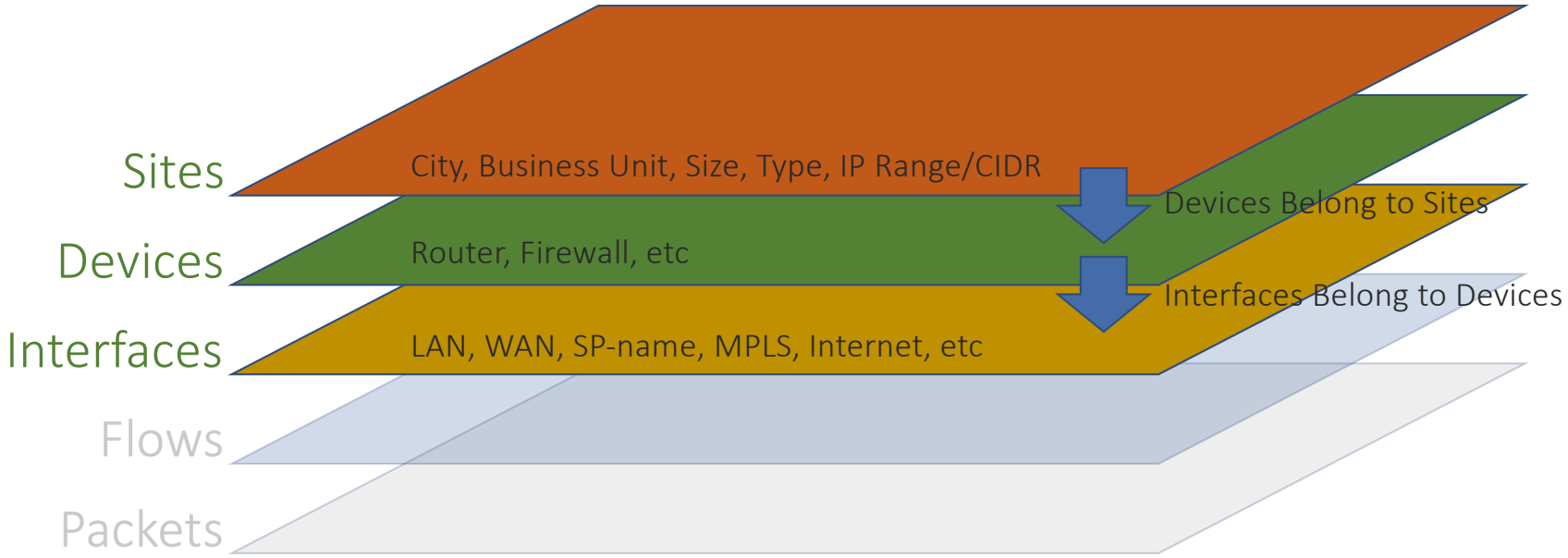
- Structured around three levels:
  - Sites (Level 1)
  - Devices Level 2)
  - Interfaces (Level 3)
- You can view traffic as:
  - Site to Site
  - By Device
  - Flow – by DSCP, Application (or App Group), Source AND/OR Destination (site, IP, Port), **Tag**

Tags are your best friend – Let them support your work in LiveNX

Understanding LiveNX – Semantic Data

The information in LiveNX is structured in dependent layers – in the same way you will rely on these layers as you monitor and troubleshoot.

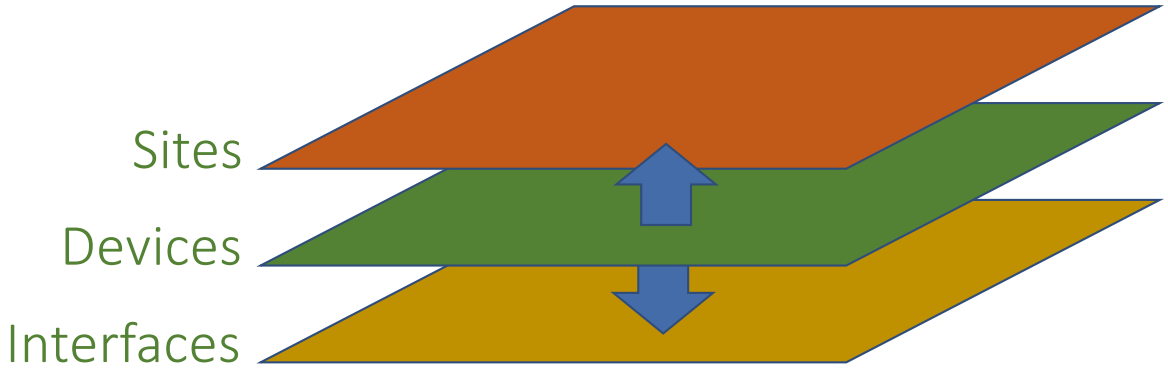
Each layer will use Tags, key words that accumulate similar items on the same layer. Layers below inherit the tags from above.



Best Practice:
Use S prefix for Site level tags, D for Device level tags, I for Interface Level tags.

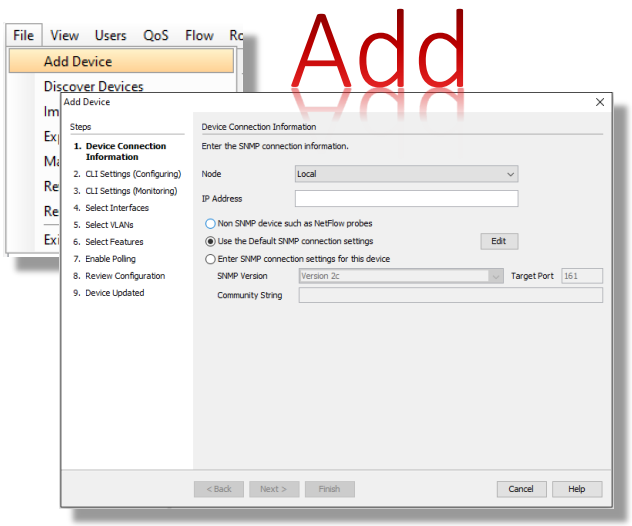
Adding Devices to LiveNX

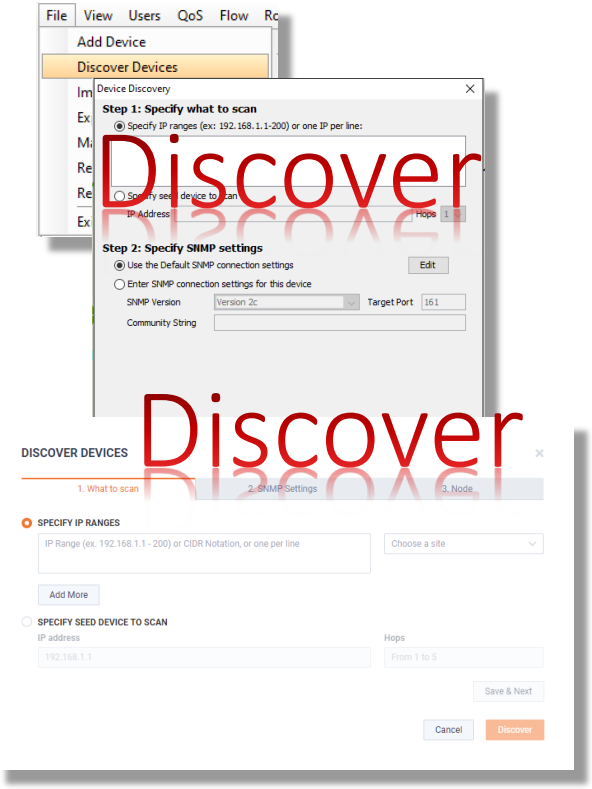
- Adding Devices to LiveNX is more than adding devices. It involves making sure that Sites and Interfaces are configured too.
- By adding devices, we begin the process of adding semantic data, across the three layers within LiveNX.

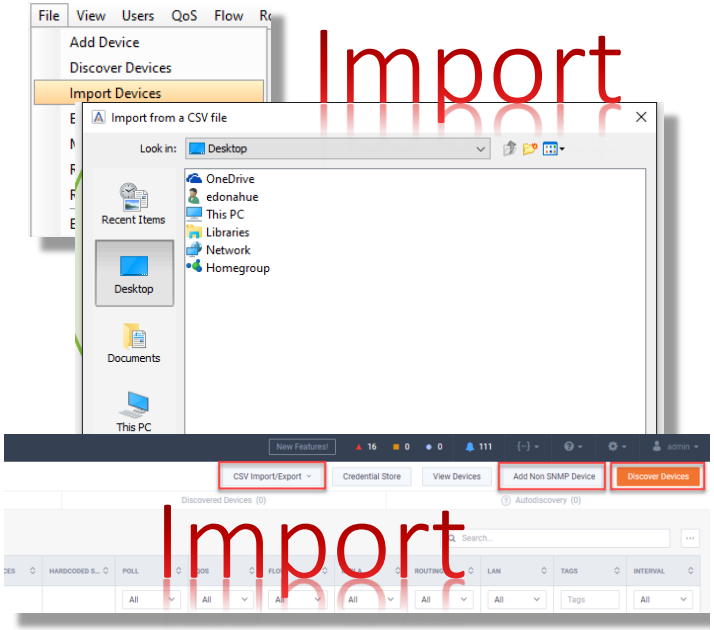


Device Management

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







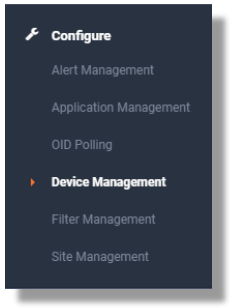
Add – Discover – Import

Both on the Eng Console,

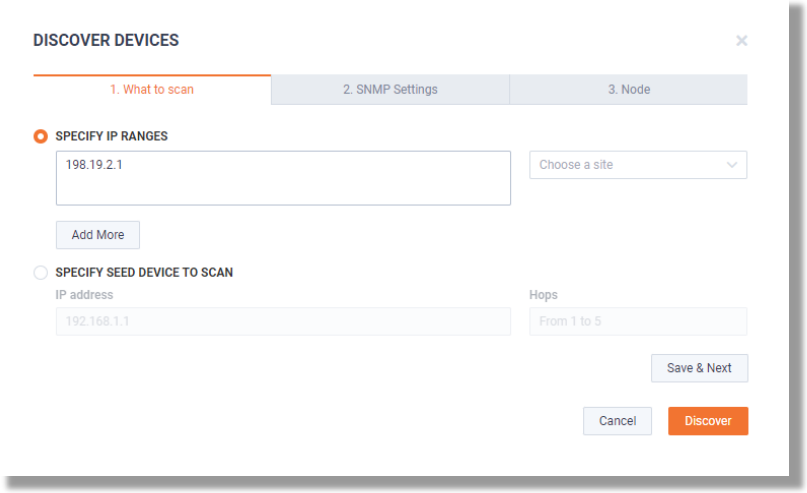
and the WebUI

Device Discovery

Scan and find connected devices

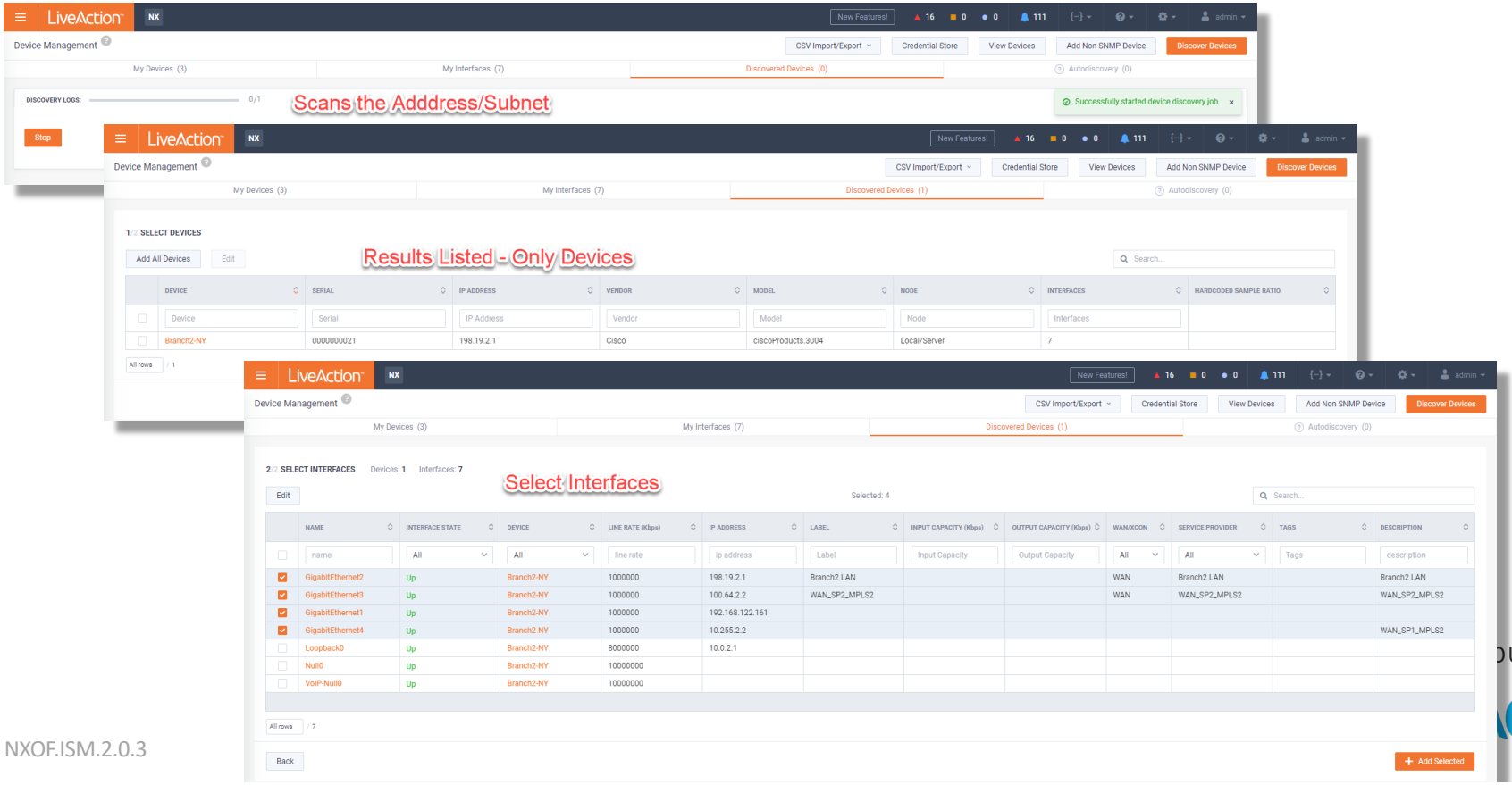


- From within Device Management, under Configure
- Use an IP Address range
- SNMP settings & Credentials
- Is the collection Node Local or…
- Returns a dialog with suggested devices to add.

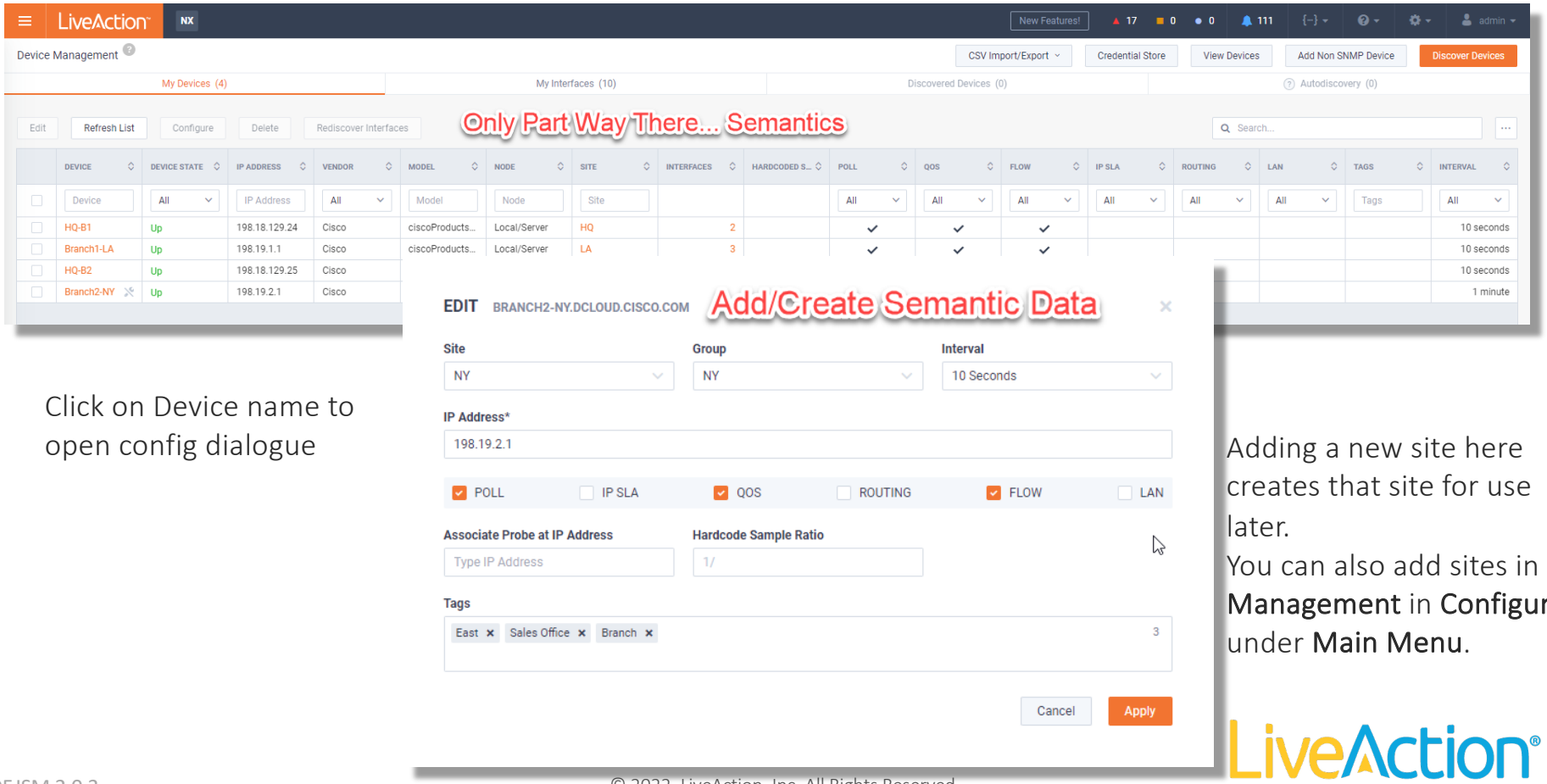


Device Discovery… Simple Steps

Allows you to Devices and Interfaces into LiveNX for gathering Flow data



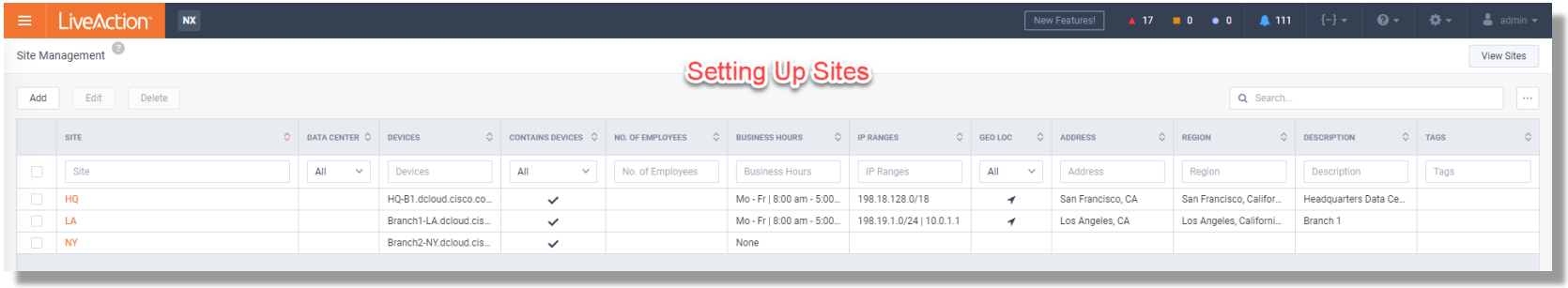
Working Topology – Device Needs Semantic Data

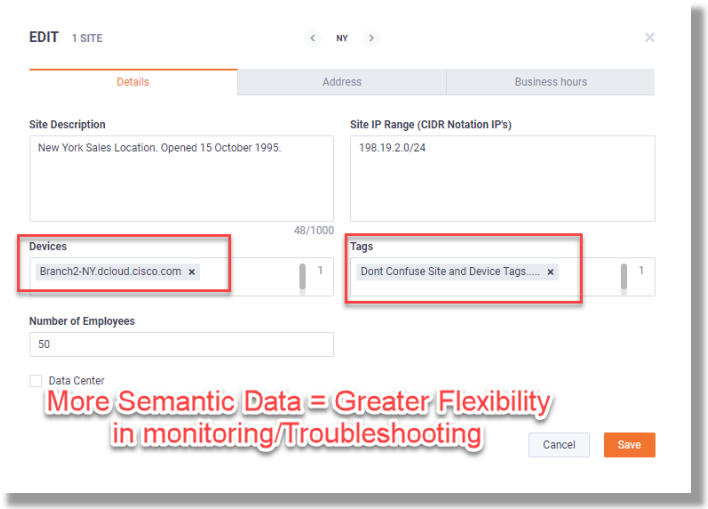


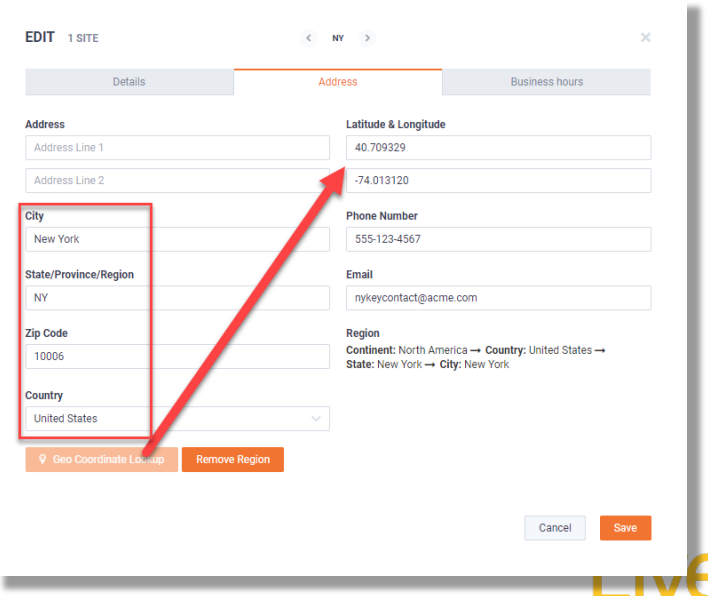
Click on Device name to open config dialogue

Adding a new site here creates that site for use later.
You can also add sites in **Site Management** in **Configure** under **Main Menu**.

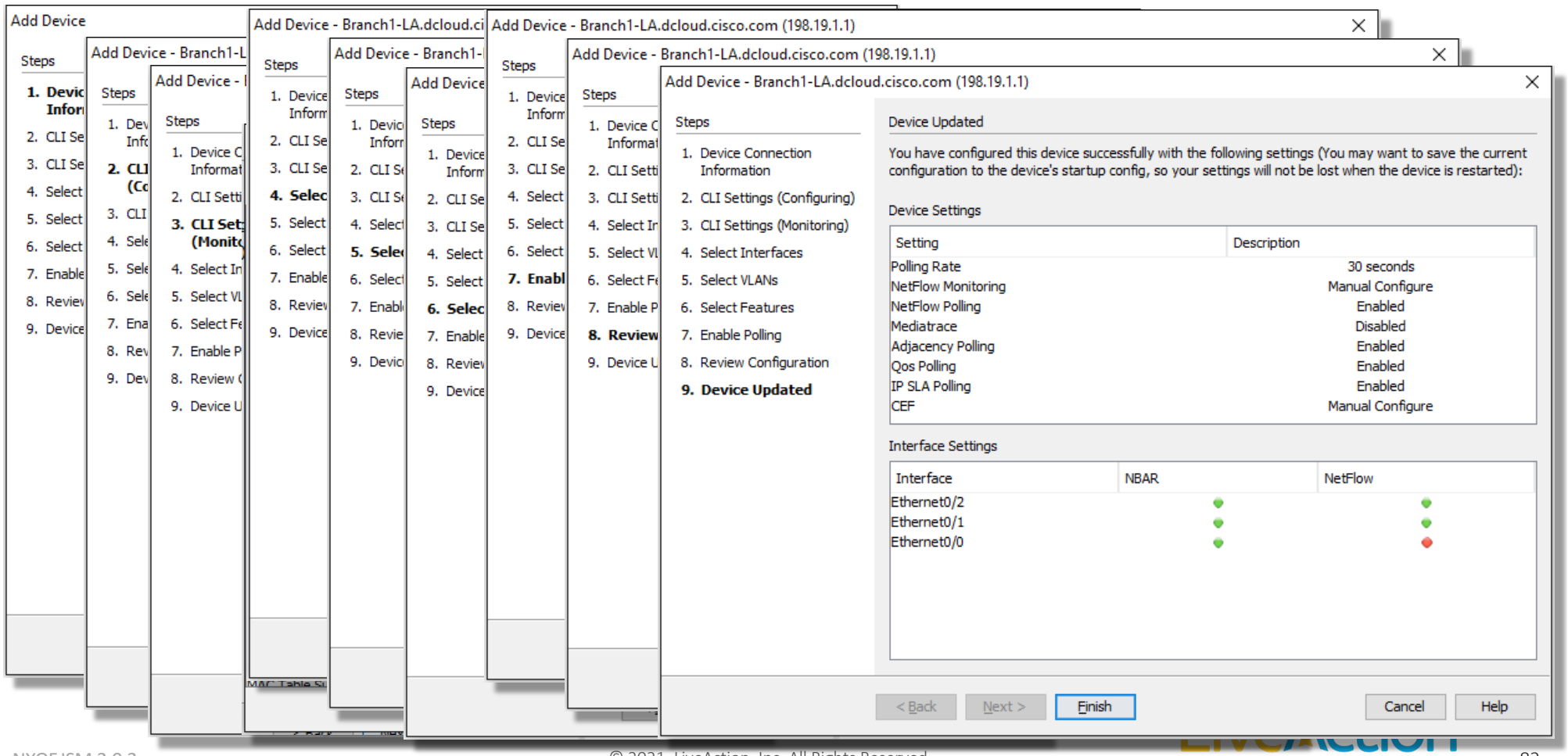
Devices Belong to Sites – Adding Sites And Semantics



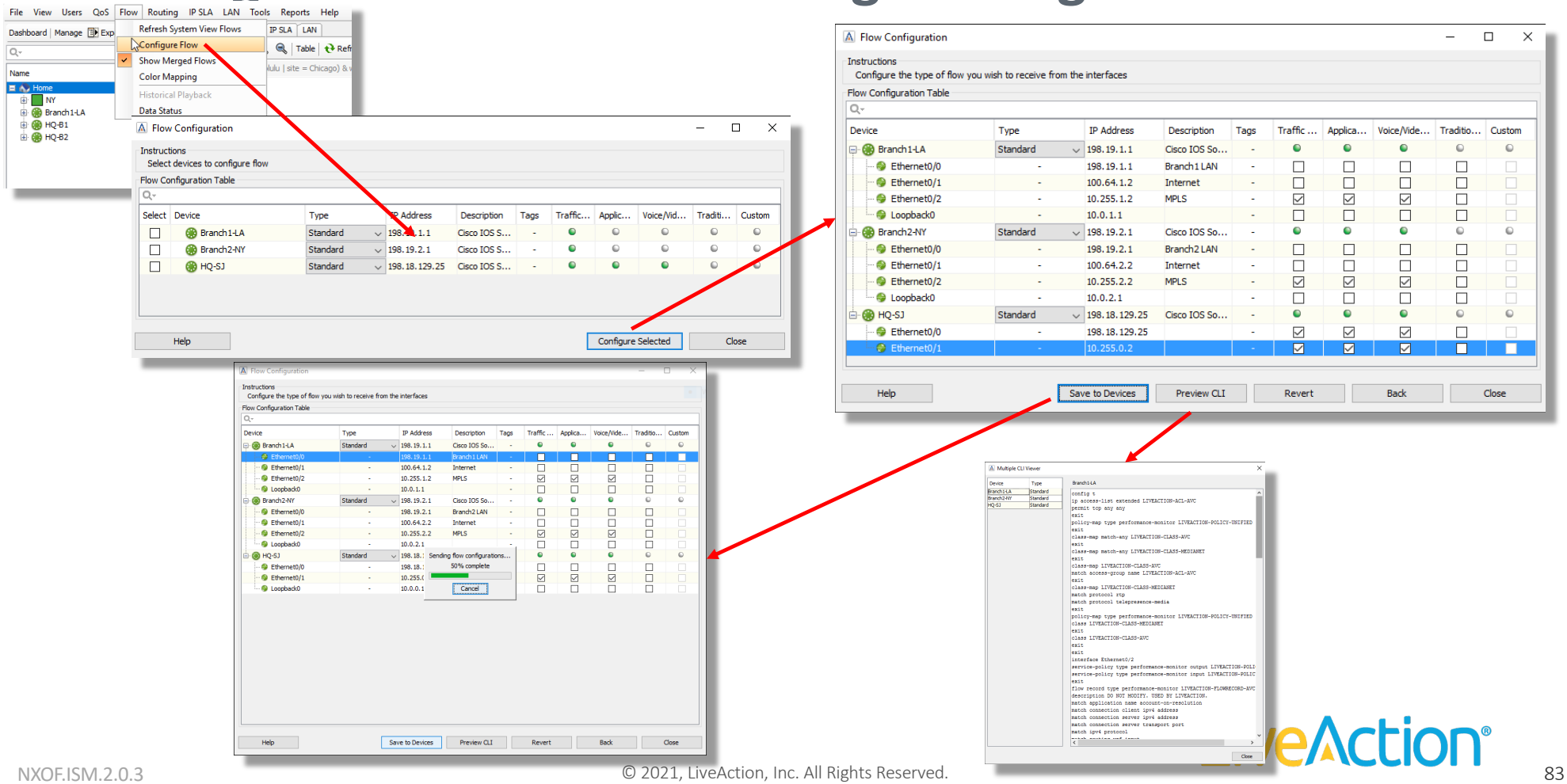




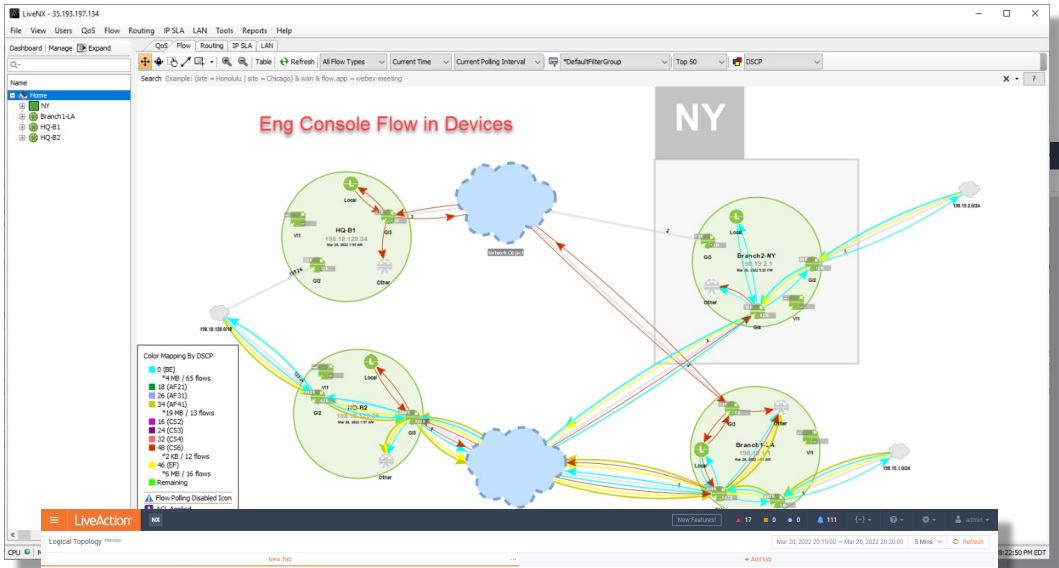
Making the Device Configurable via CLI – Engineering Console

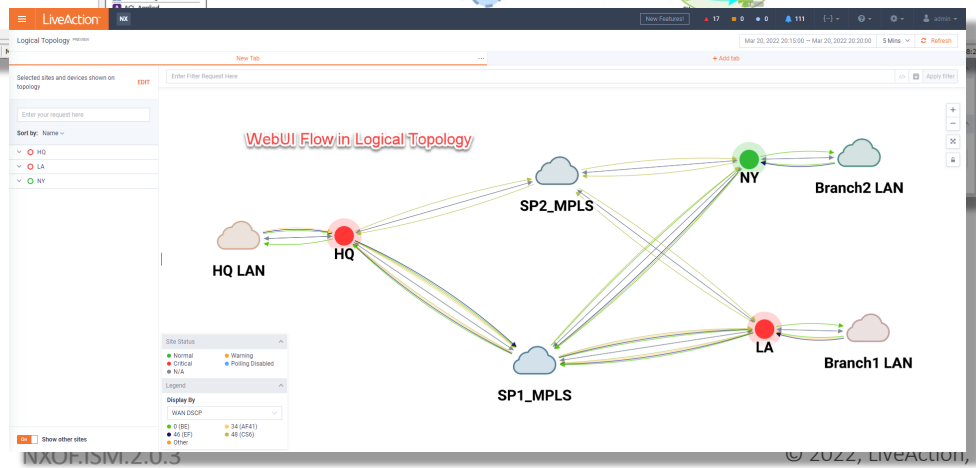


Configure Flow Collection - Engineering Console

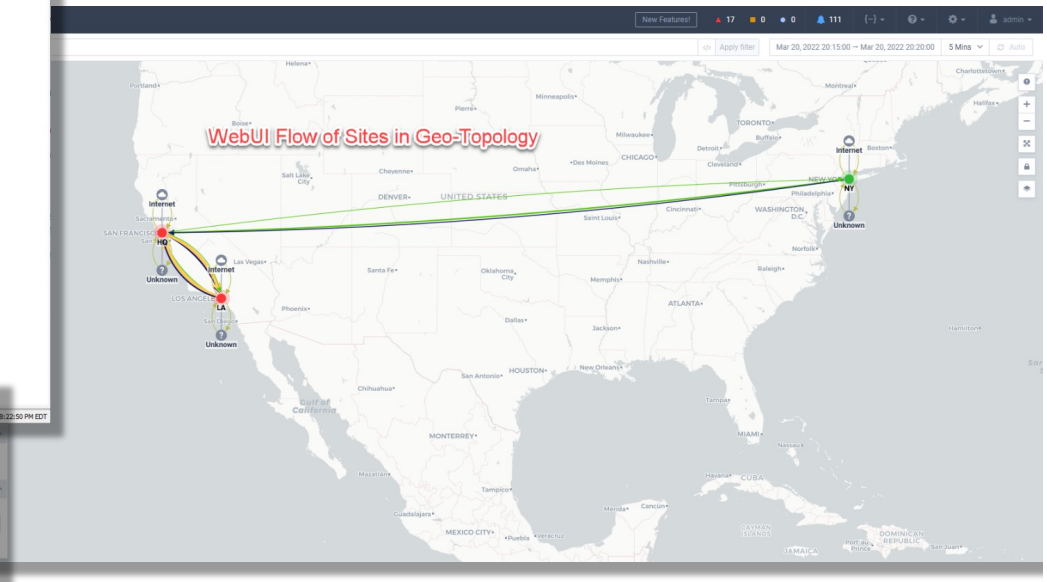


View Traffic Flows!





Notice the locations, Site Names, Network Names etc. That all comes from semantic data

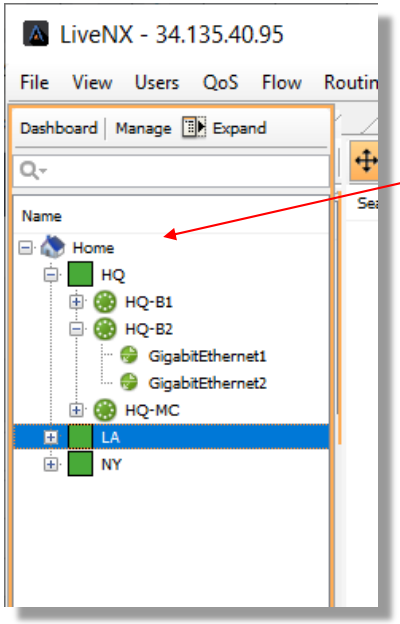


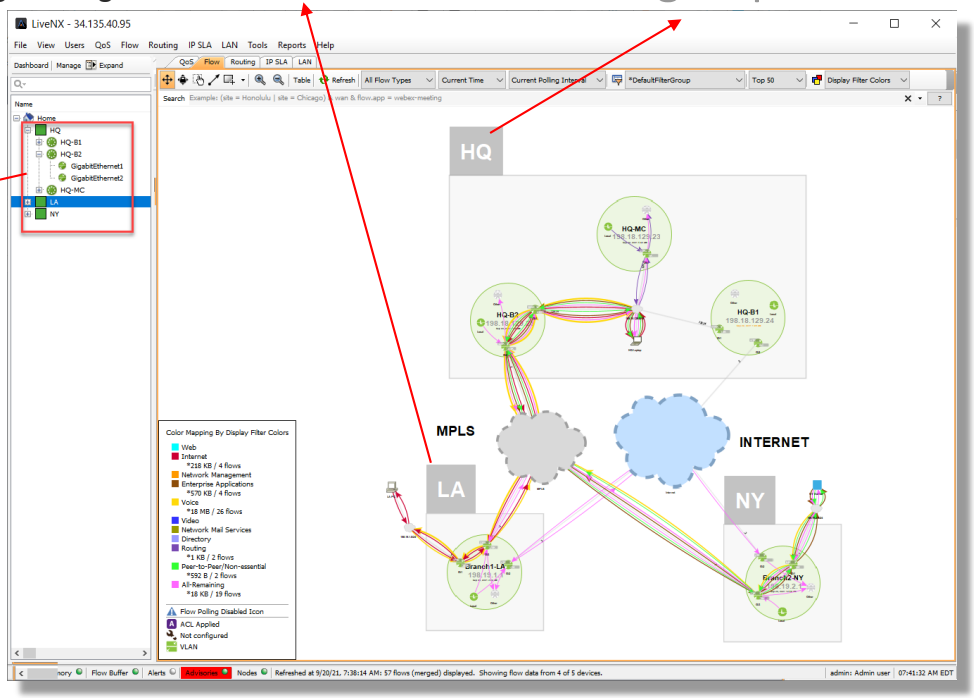
Topology Basics – Grouping in Engineering Console

*Grouping only visually applied in LiveNX Eng Console (WebUI Uses Sites – You need to use BOTH)

*Sites and Groups can be configured in BOTH WebUI and Engineering Console.

Devices appear on the topology within their shaded groups.





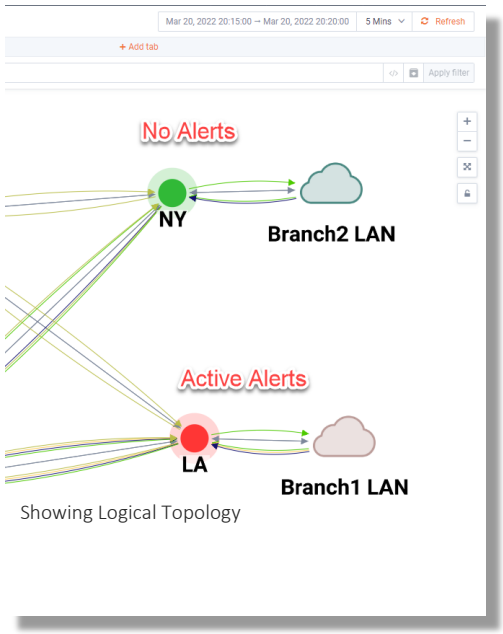
Devices appear collapsed in their groups on the device tree.

Grouping makes device management easier!

LiveAction®

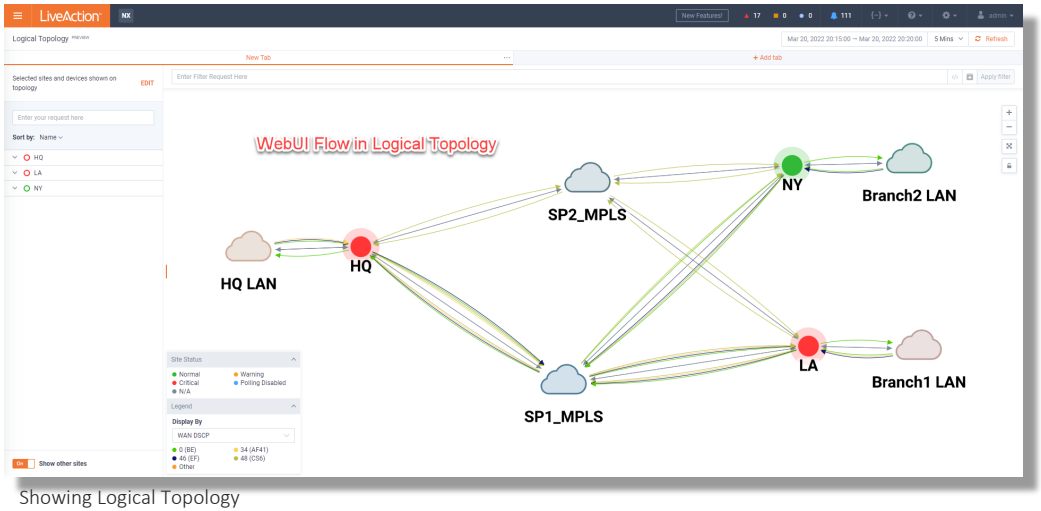
Topology Basics

Devices reporting issues will change colors to prompt for investigation.



Showing Logical Topology

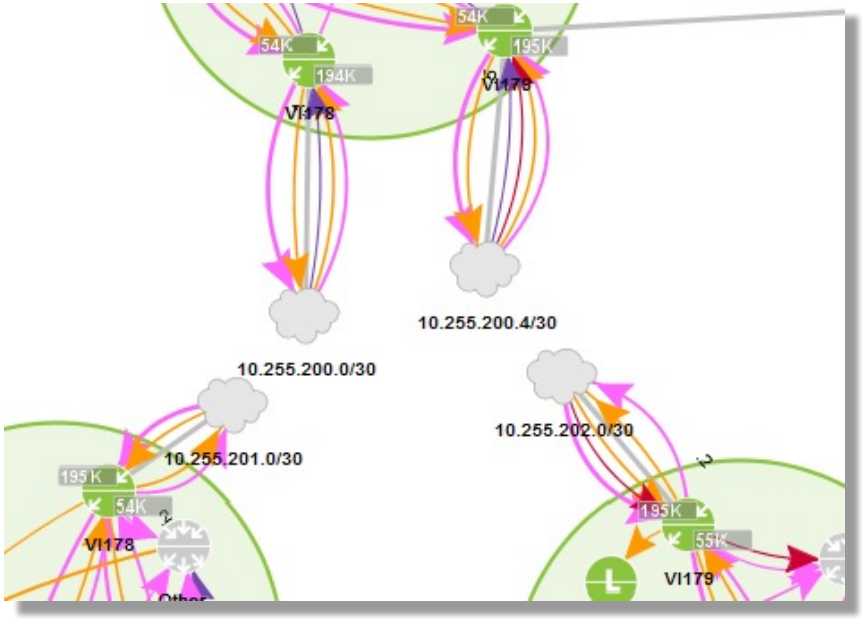
Quickly identify many problem sites visually



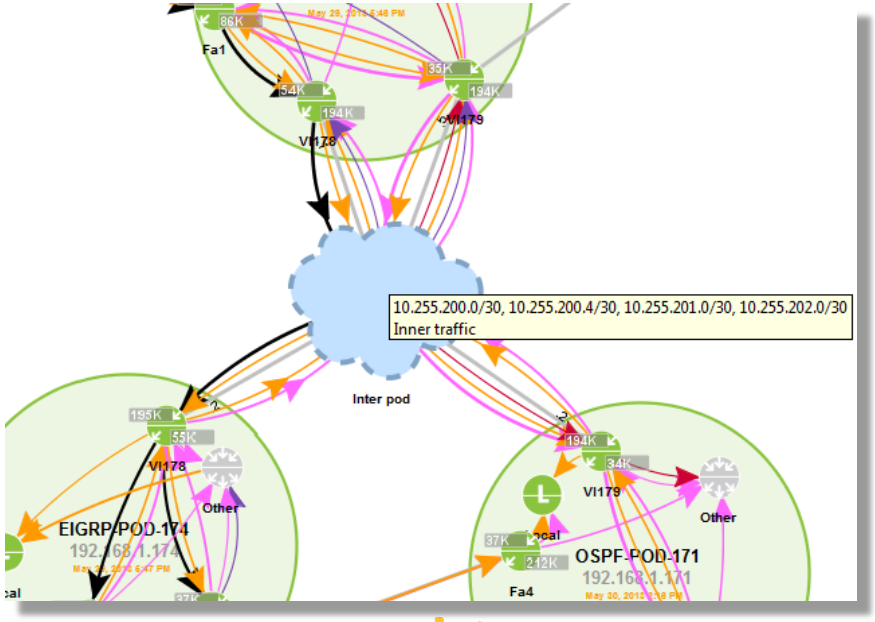
Showing Logical Topology

Merge Clouds*

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



Once merged… flows will properly draw through the topology



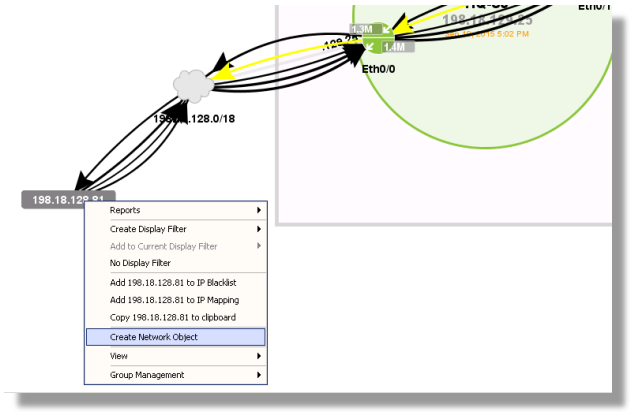
*Merge Clouds only applied in LiveNX Engineering Console

Topology Basics – Add Network Object*

Do it the EASY way!

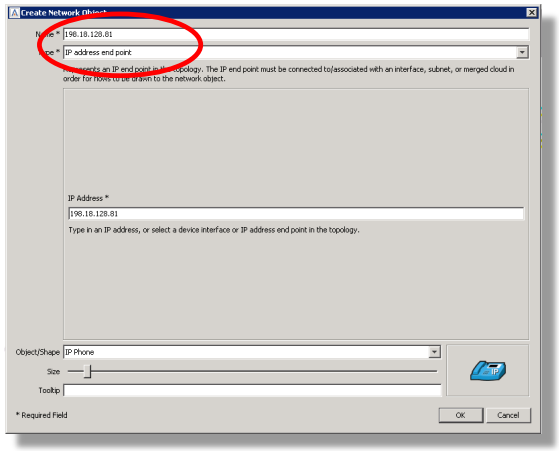
Step 1

Right-Click on Flow Endpoint



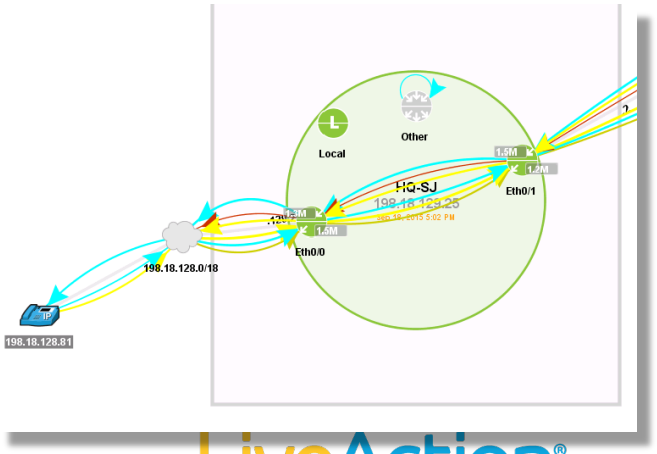
Step 2

Select the Object Shape



Step 3

Flows now connect



*Merge Clouds only applied in LiveNX Engineering Console

LAB 3 & 4: Making the Topology Work

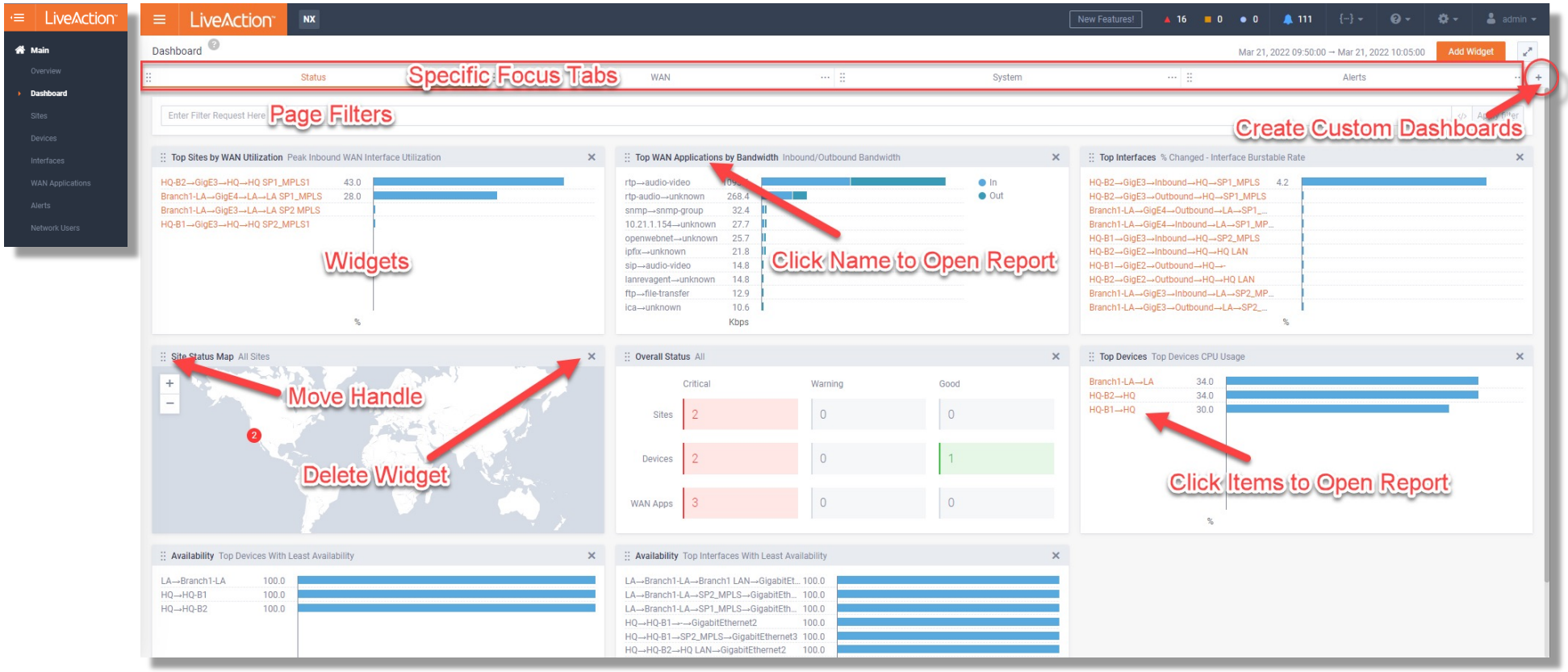
- Add additional device(s)
- Enable / Configure Flow collection
- Remove an Interface
- Device Semantics
- Creating / Modify Groups
- Merge Clouds
- Network Objects

Reports & Alerts

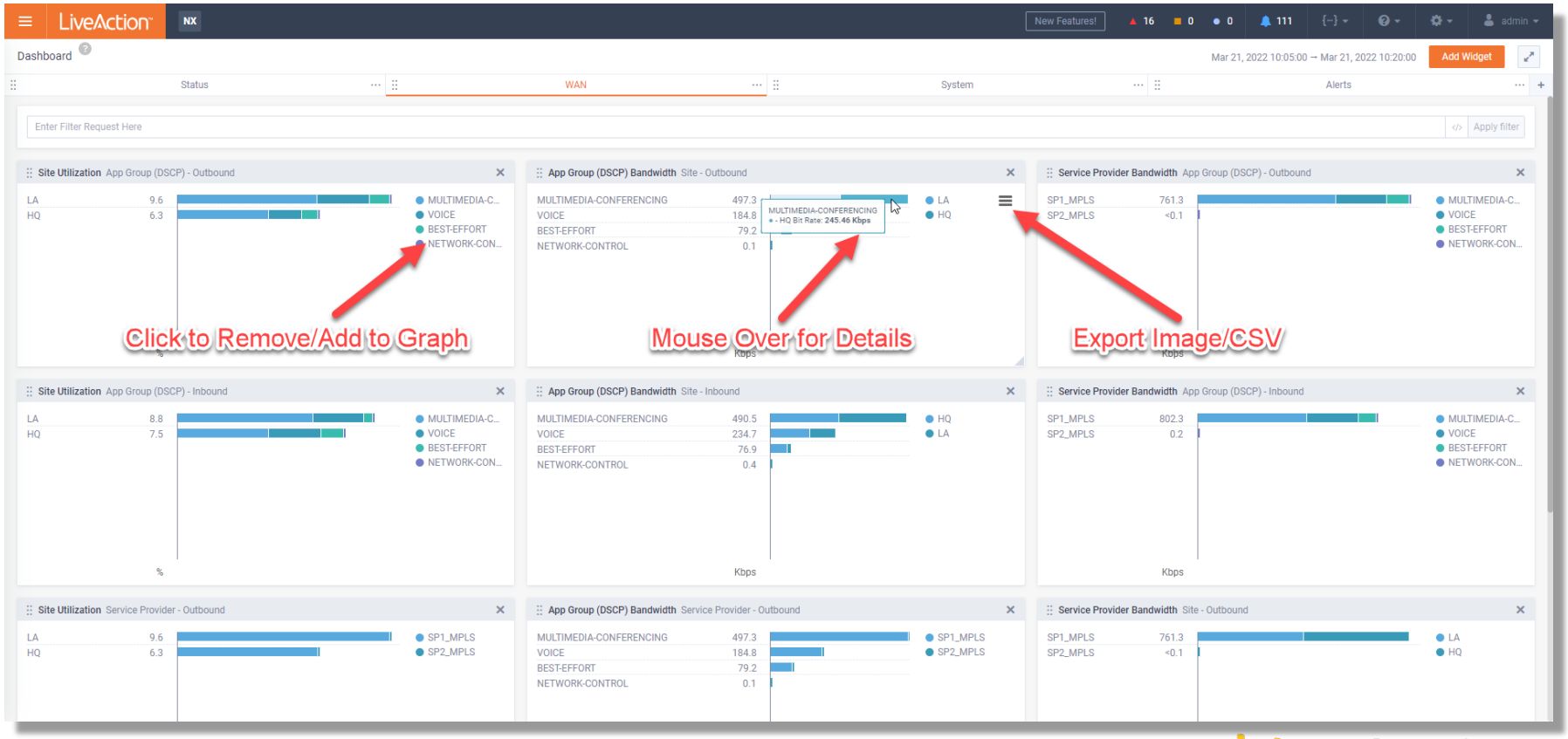
Using LiveNX WebUI

LiveAction™

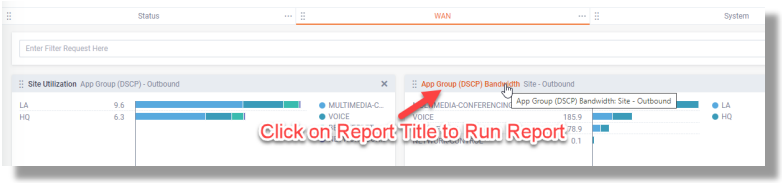
Dashboard

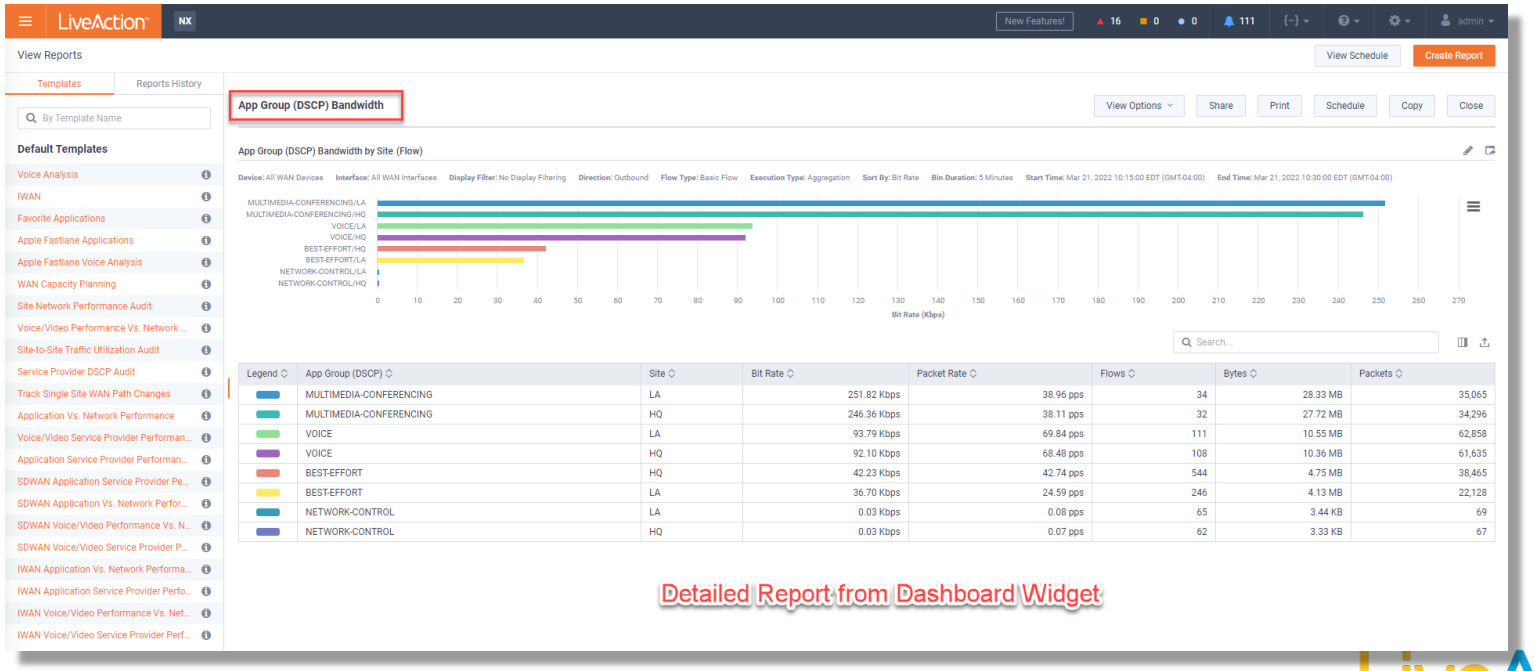


WAN Dashboard – One of the Defaults



Drill-Down to Reports

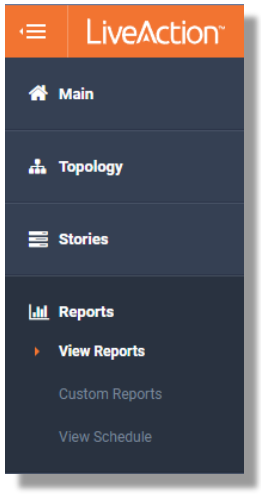




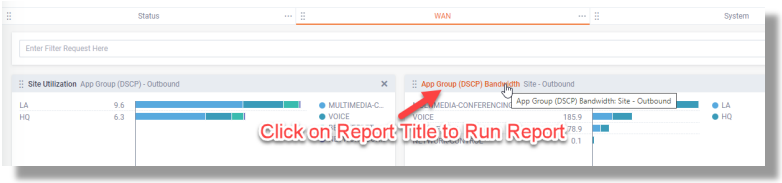
Creating Reports

Multiple Roads Lead to Reports

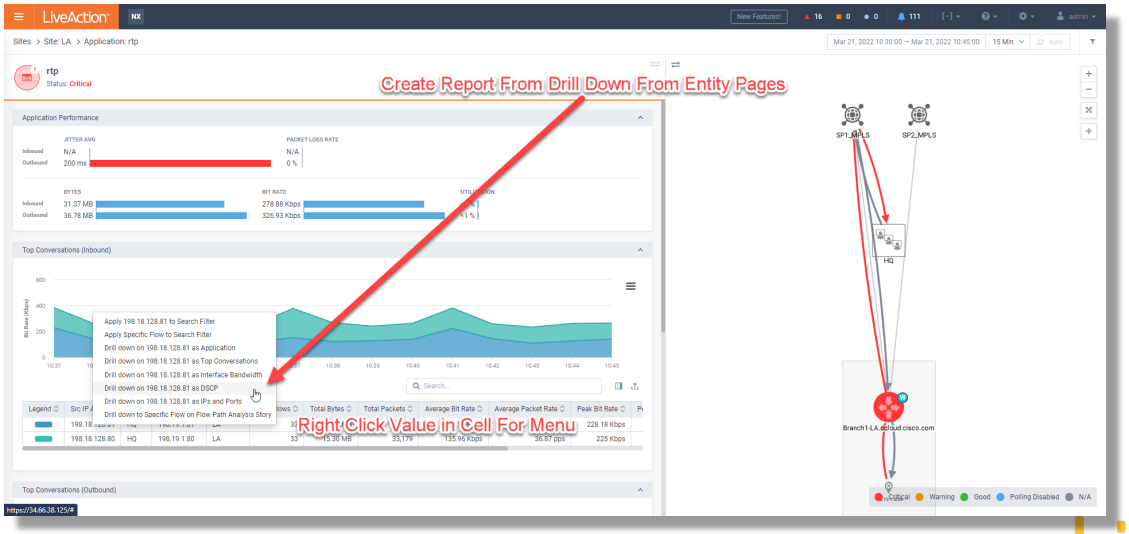
From Navigation Menu



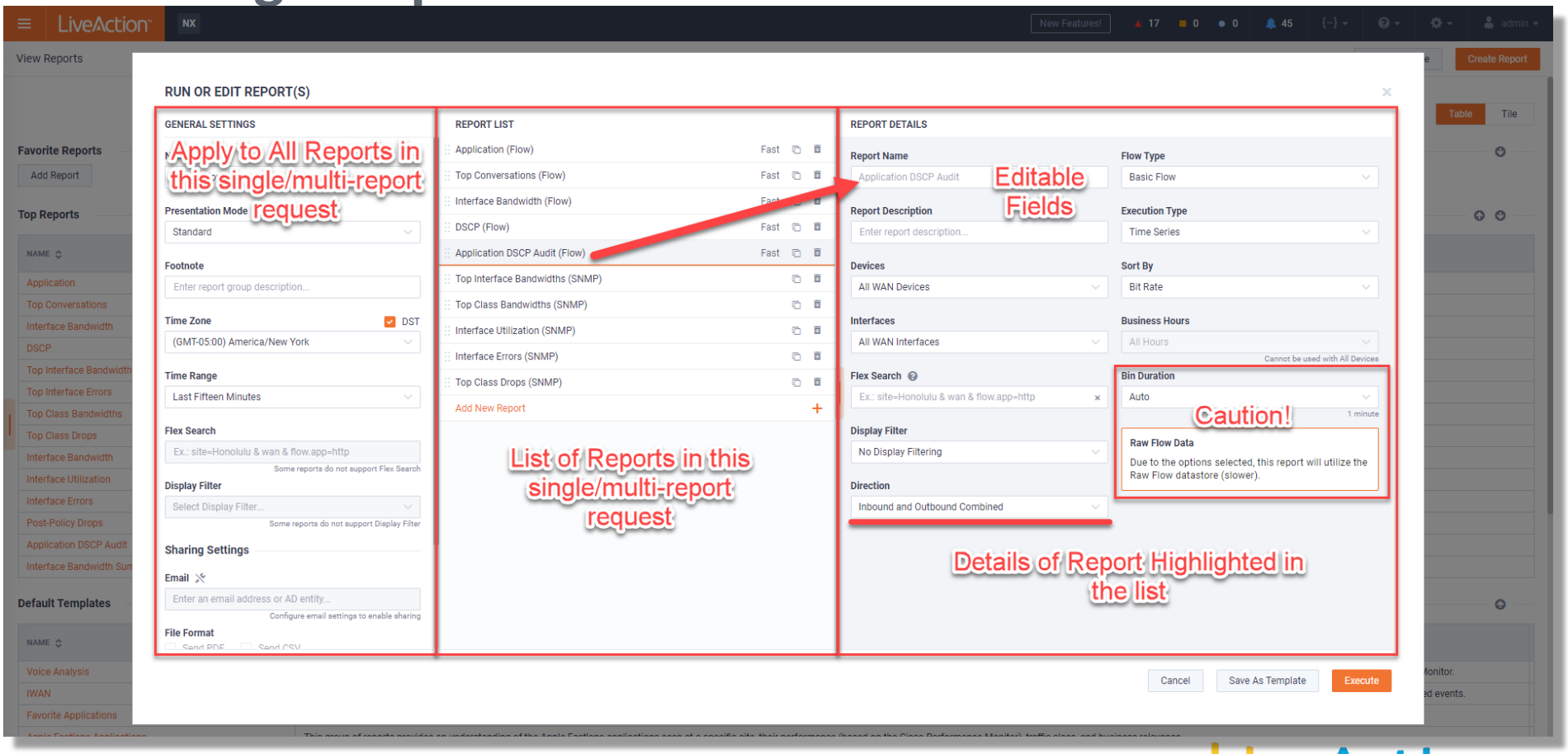
From Any Dashboard Item



Drill Down From Entity Pages



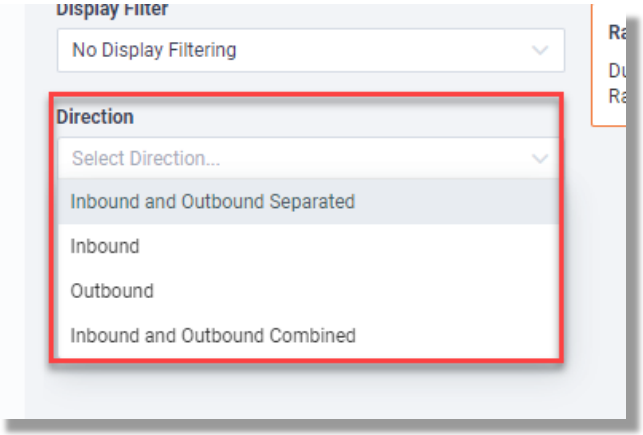
Creating a Report



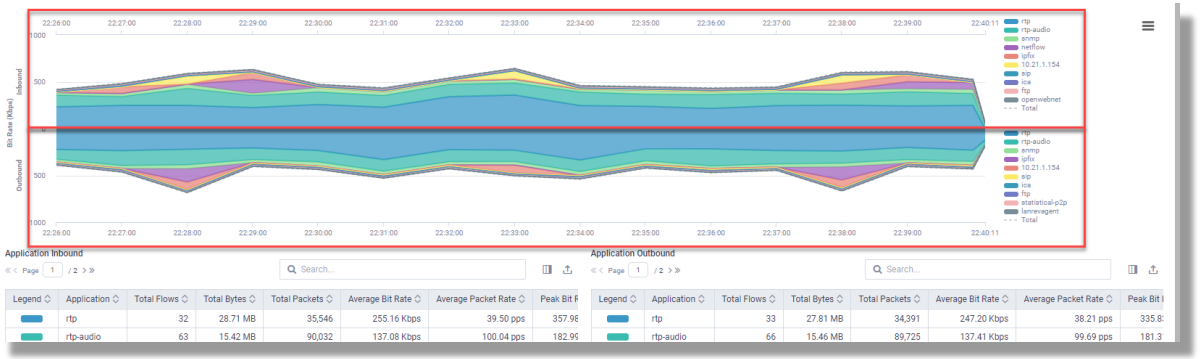
Flow Report - Directionality

Data Volumes can be viewed by ingress, egress, both on one chart, or combined (single number)
You can choose between how the data is presented in reports

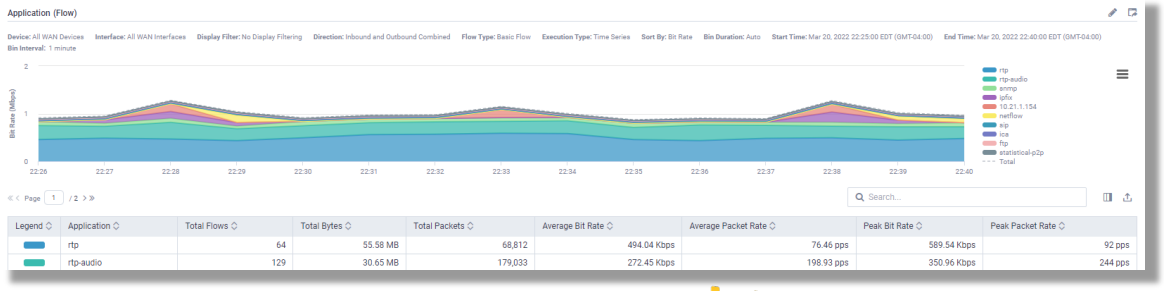
Configured in Report Settings



Inbound and Outbound Separated



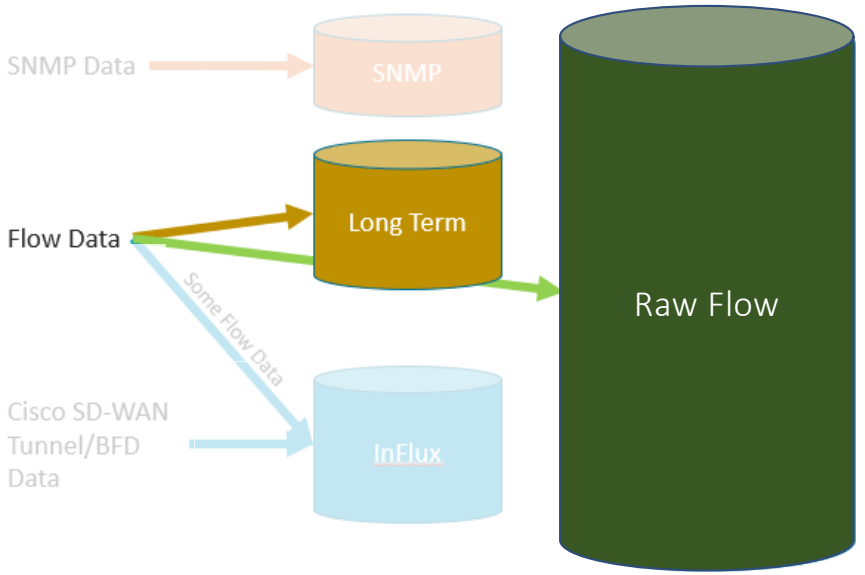
Inbound and Outbound Combined



Automatic Granularity - Report Length / Data Bin

- Granularity is on Flow Data
- Flow Reports are generated from the RAW Store
- Raw Flow Store
  - Short time-range (un-aggregated) or 1 min Bin
- Long-Term Flow Store
  - Longer time-range (aggregated) or 5 min Bin

Bin Size can be selected – Beware!

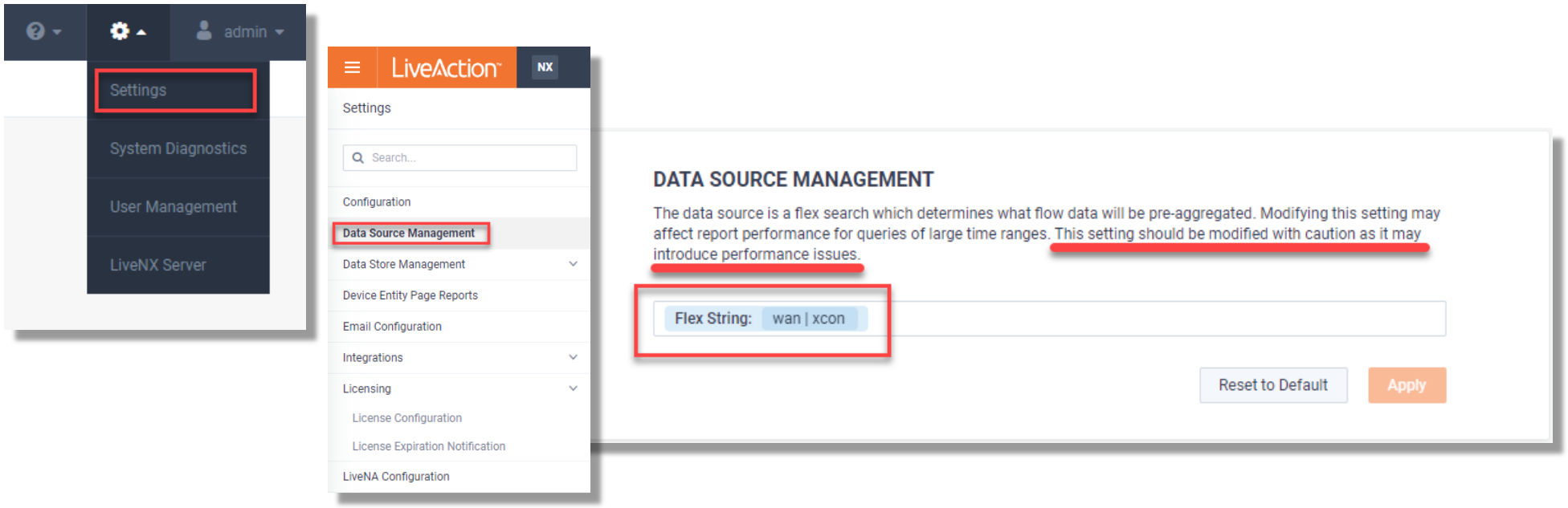


LiveAction®

Long Term Data Storage

How is Long Term Store populated?

The Flow Source configuration alters what devices/interfaces are included for Long Term Report Processing.



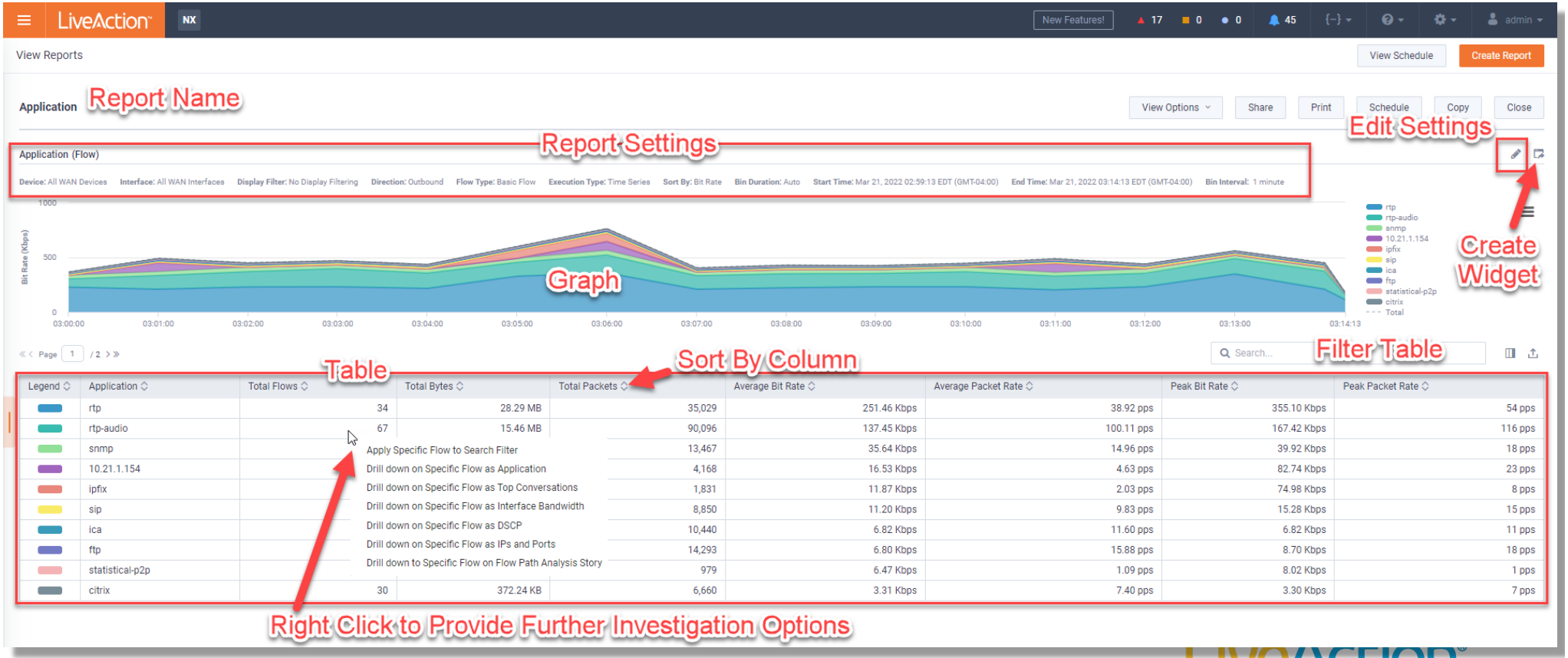
Commonly Used Reports

- Application (Flow)
- Top Conversations (Flow)
- Interface Bandwidth (Flow)
- DSCP (Flow)
- Application DSCP Audit (Flow)
- Top Interface Bandwidths (SNMP)
- Interface Bandwidth (SNMP)
- Interface Utilization (SNMP)
- Interface Errors (SNMP)
- Top Class Drops (SNMP)

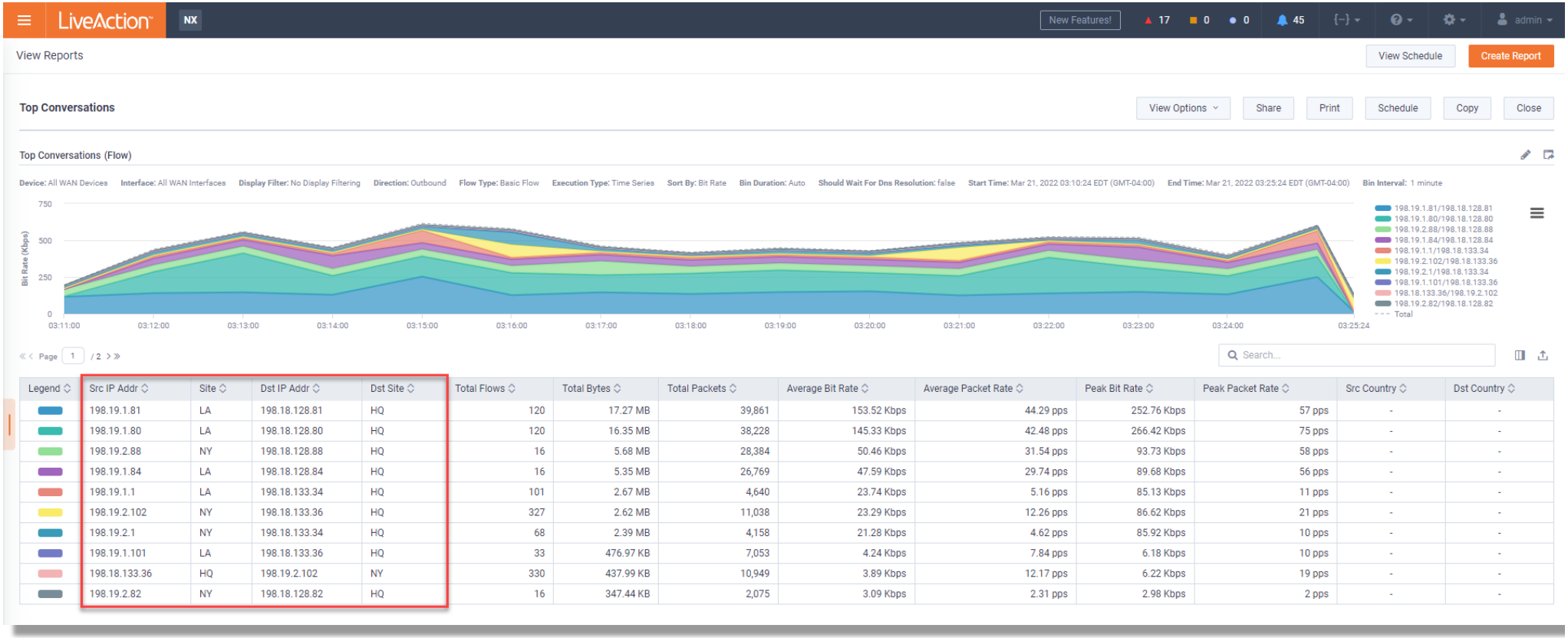
Different data sources will provide different perspectives of your network

They can also give you different counts for what might look like the same number

Application (Flow)

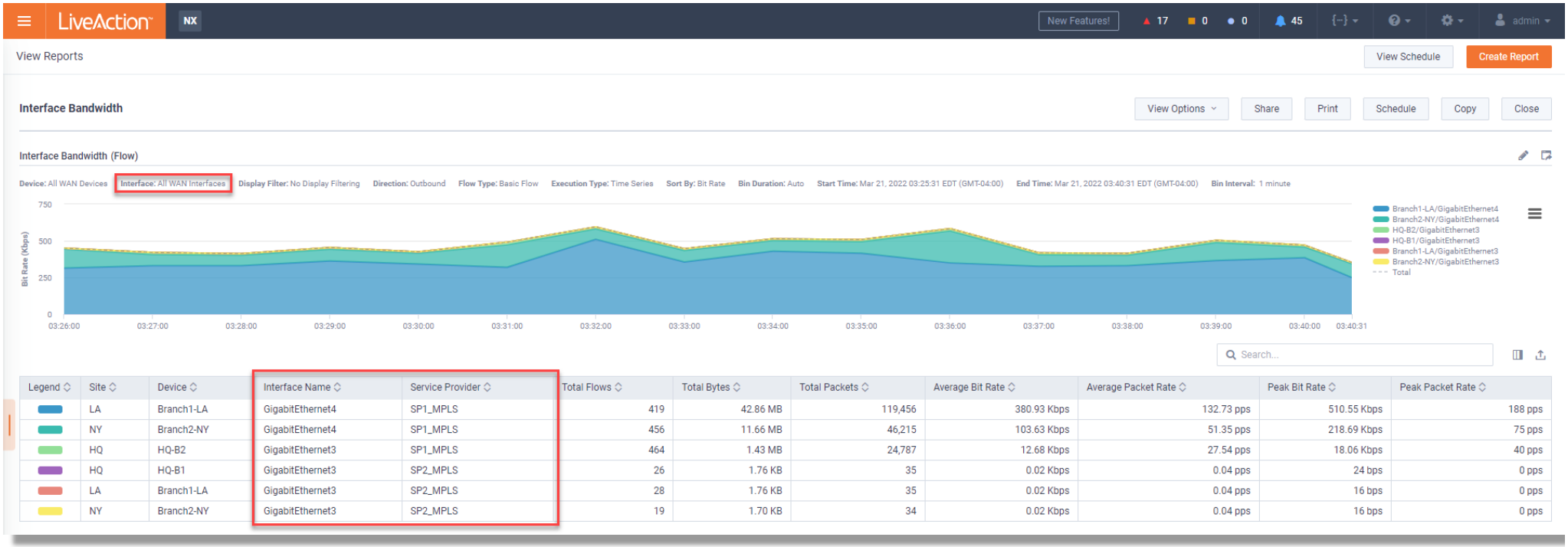


Top Conversations (Flow)



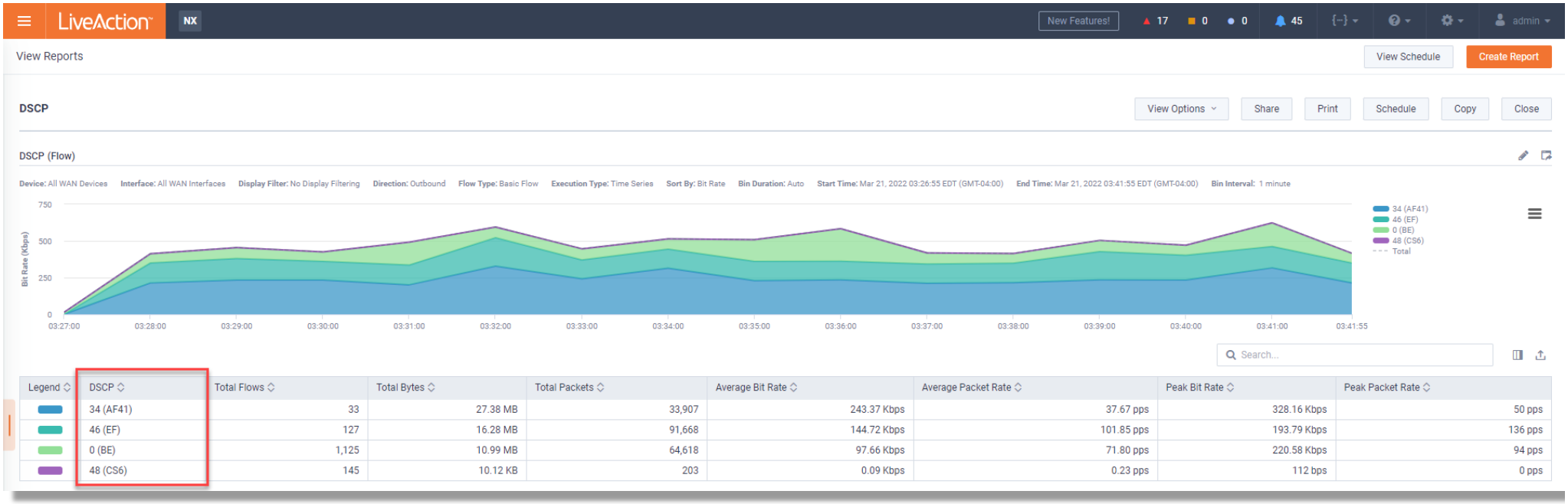
Legend	Src IP Addr	Site	Dst IP Addr	Dst Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate	Src Country	Dst Country
	198.19.1.81	LA	198.18.128.81	HQ	120	17.27 MB	39,861	153.52 Kbps	44.29 pps	252.76 Kbps	57 pps	-	-
	198.19.1.80	LA	198.18.128.80	HQ	120	16.35 MB	38,228	145.33 Kbps	42.48 pps	266.42 Kbps	75 pps	-	-
	198.19.2.88	NY	198.18.128.88	HQ	16	5.68 MB	28,384	50.46 Kbps	31.54 pps	93.73 Kbps	58 pps	-	-
	198.19.1.84	LA	198.18.128.84	HQ	16	5.35 MB	26,769	47.59 Kbps	29.74 pps	89.68 Kbps	56 pps	-	-
	198.19.1.1	LA	198.18.133.34	HQ	101	2.67 MB	4,640	23.74 Kbps	5.16 pps	85.13 Kbps	11 pps	-	-
	198.19.2.102	NY	198.18.133.36	HQ	327	2.62 MB	11,038	23.29 Kbps	12.26 pps	86.62 Kbps	21 pps	-	-
	198.19.2.1	NY	198.18.133.34	HQ	68	2.39 MB	4,158	21.28 Kbps	4.62 pps	85.92 Kbps	10 pps	-	-
	198.19.1.101	LA	198.18.133.36	HQ	33	476.97 KB	7,053	4.24 Kbps	7.84 pps	6.18 Kbps	10 pps	-	-
	198.18.133.36	HQ	198.19.2.102	NY	330	437.99 KB	10,949	3.89 Kbps	12.17 pps	6.22 Kbps	19 pps	-	-
	198.19.2.82	NY	198.18.128.82	HQ	16	347.44 KB	2,075	3.09 Kbps	2.31 pps	2.98 Kbps	2 pps	-	-

Interface Bandwidth (Flow)



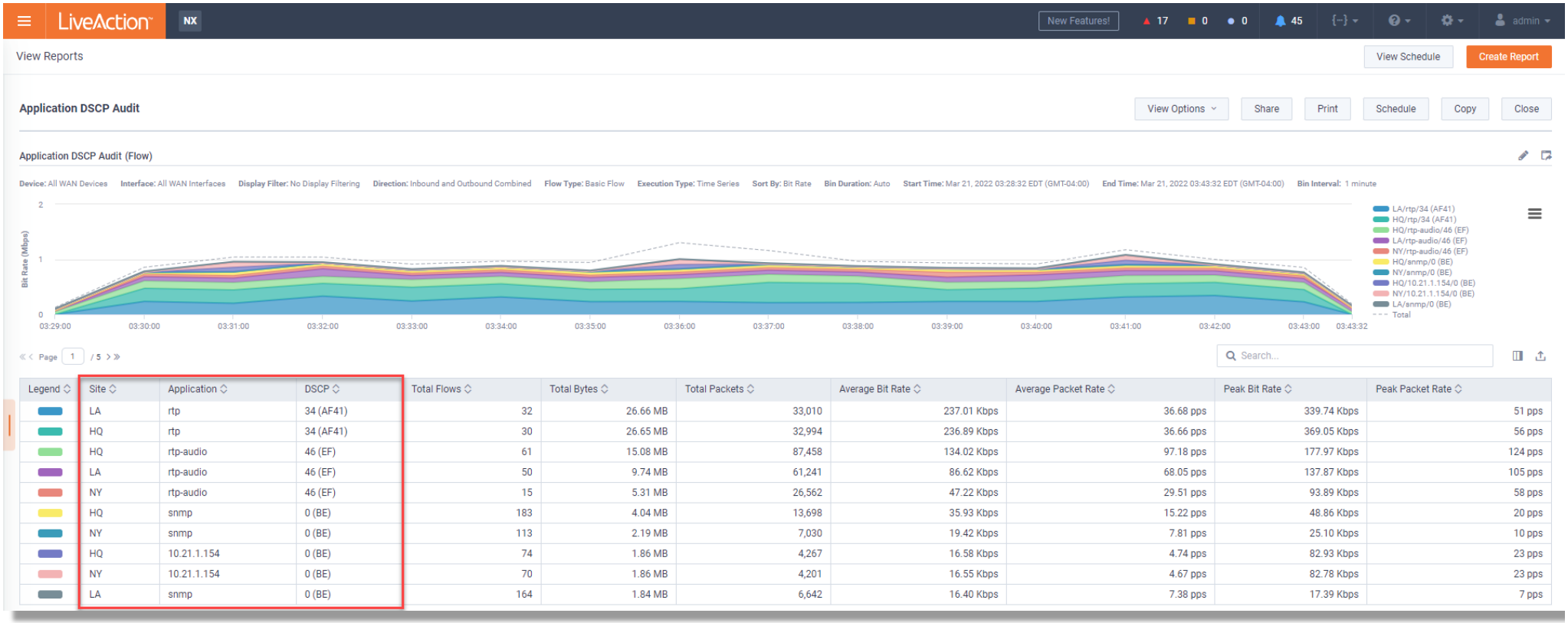
Legend	Site	Device	Interface Name	Service Provider	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	LA	Branch1-LA	GigabitEthernet4	SP1_MPLS	419	42.86 MB	119,456	380.93 Kbps	132.73 pps	510.55 Kbps	188 pps
	NY	Branch2-NY	GigabitEthernet4	SP1_MPLS	456	11.66 MB	46,215	103.63 Kbps	51.35 pps	218.69 Kbps	75 pps
	HQ	HQ-B2	GigabitEthernet3	SP1_MPLS	464	1.43 MB	24,787	12.68 Kbps	27.54 pps	18.06 Kbps	40 pps
	HQ	HQ-B1	GigabitEthernet3	SP2_MPLS	26	1.76 KB	35	0.02 Kbps	0.04 pps	24 bps	0 pps
	LA	Branch1-LA	GigabitEthernet3	SP2_MPLS	28	1.76 KB	35	0.02 Kbps	0.04 pps	16 bps	0 pps
	NY	Branch2-NY	GigabitEthernet3	SP2_MPLS	19	1.70 KB	34	0.02 Kbps	0.04 pps	16 bps	0 pps

DSCP (Flow)



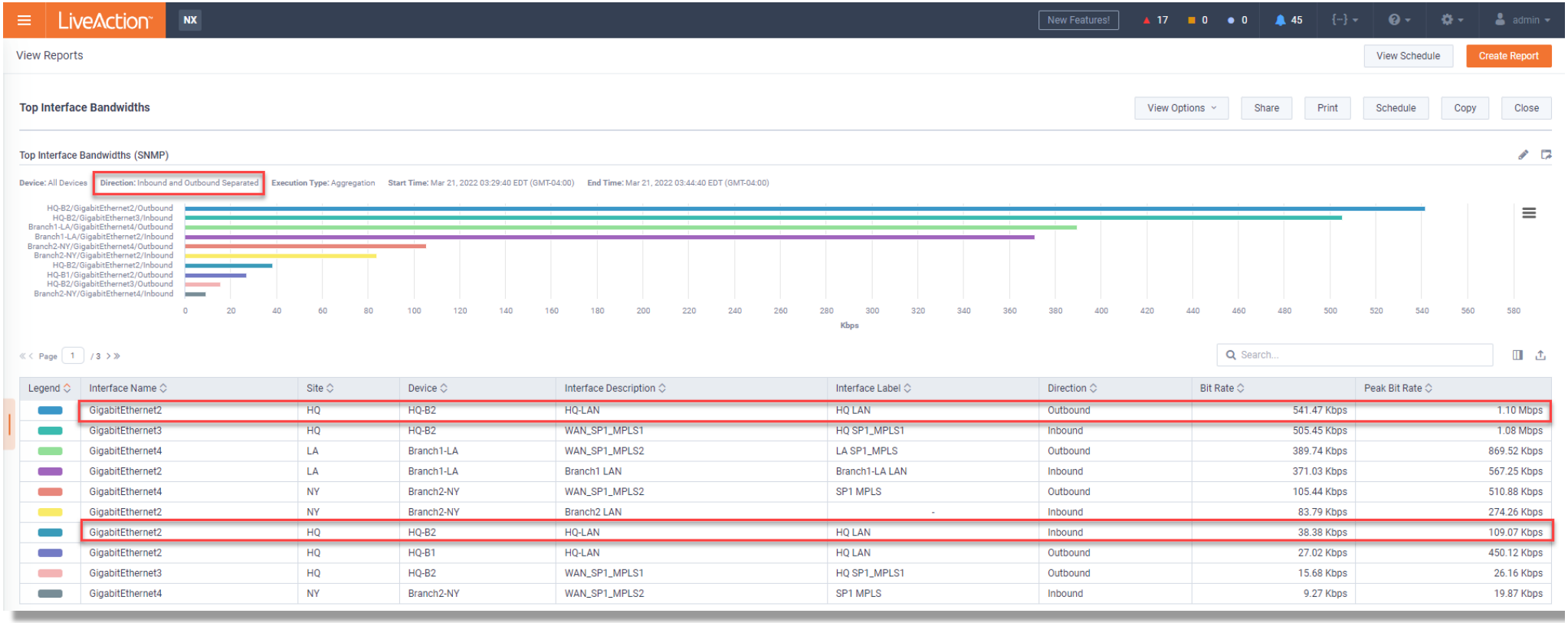
Legend	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	34 (AF41)	33	27.38 MB	33,907	243.37 Kbps	37.67 pps	328.16 Kbps	50 pps
	46 (EF)	127	16.28 MB	91,668	144.72 Kbps	101.85 pps	193.79 Kbps	136 pps
	0 (BE)	1,125	10.99 MB	64,618	97.66 Kbps	71.80 pps	220.58 Kbps	94 pps
	48 (CS6)	145	10.12 KB	203	0.09 Kbps	0.23 pps	112 bps	0 pps

Application DSCP Audit (Flow)



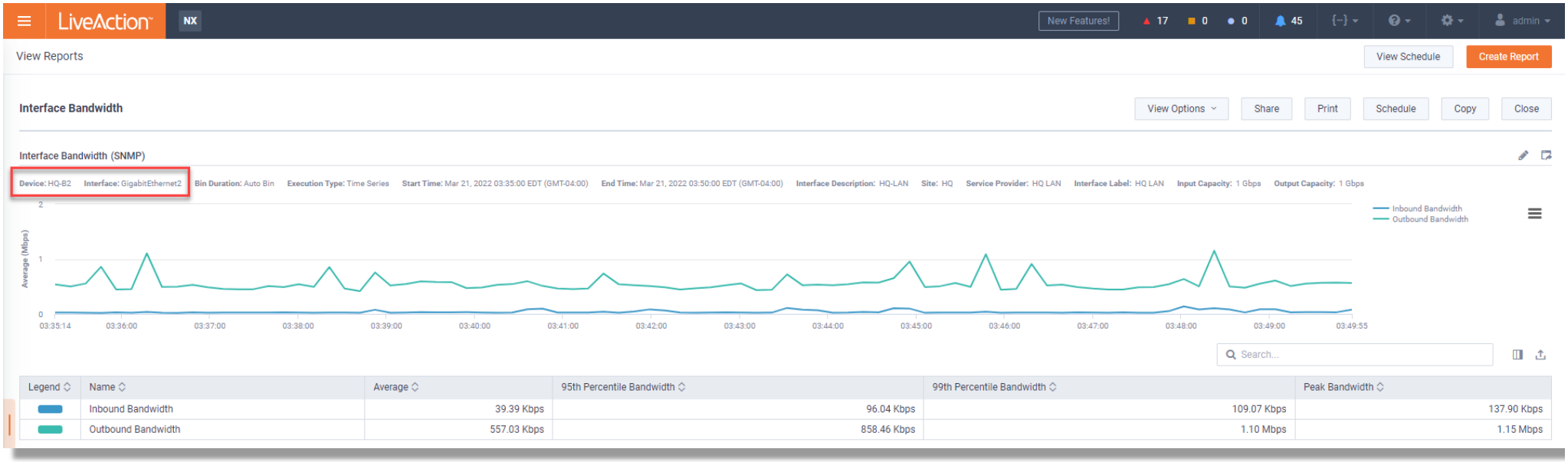
Legend	Site	Application	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	LA	rtp	34 (AF41)	32	26.66 MB	33,010	237.01 Kbps	36.68 pps	339.74 Kbps	51 pps
	HQ	rtp	34 (AF41)	30	26.65 MB	32,994	236.89 Kbps	36.66 pps	369.05 Kbps	56 pps
	HQ	rtp-audio	46 (EF)	61	15.08 MB	87,458	134.02 Kbps	97.18 pps	177.97 Kbps	124 pps
	LA	rtp-audio	46 (EF)	50	9.74 MB	61,241	86.62 Kbps	68.05 pps	137.87 Kbps	105 pps
	NY	rtp-audio	46 (EF)	15	5.31 MB	26,562	47.22 Kbps	29.51 pps	93.89 Kbps	58 pps
	HQ	snmp	0 (BE)	183	4.04 MB	13,698	35.93 Kbps	15.22 pps	48.86 Kbps	20 pps
	NY	snmp	0 (BE)	113	2.19 MB	7,030	19.42 Kbps	7.81 pps	25.10 Kbps	10 pps
	HQ	10.21.1.154	0 (BE)	74	1.86 MB	4,267	16.58 Kbps	4.74 pps	82.93 Kbps	23 pps
	NY	10.21.1.154	0 (BE)	70	1.86 MB	4,201	16.55 Kbps	4.67 pps	82.78 Kbps	23 pps
	LA	snmp	0 (BE)	164	1.84 MB	6,642	16.40 Kbps	7.38 pps	17.39 Kbps	7 pps

Top Interface Bandwidths (SNMP)



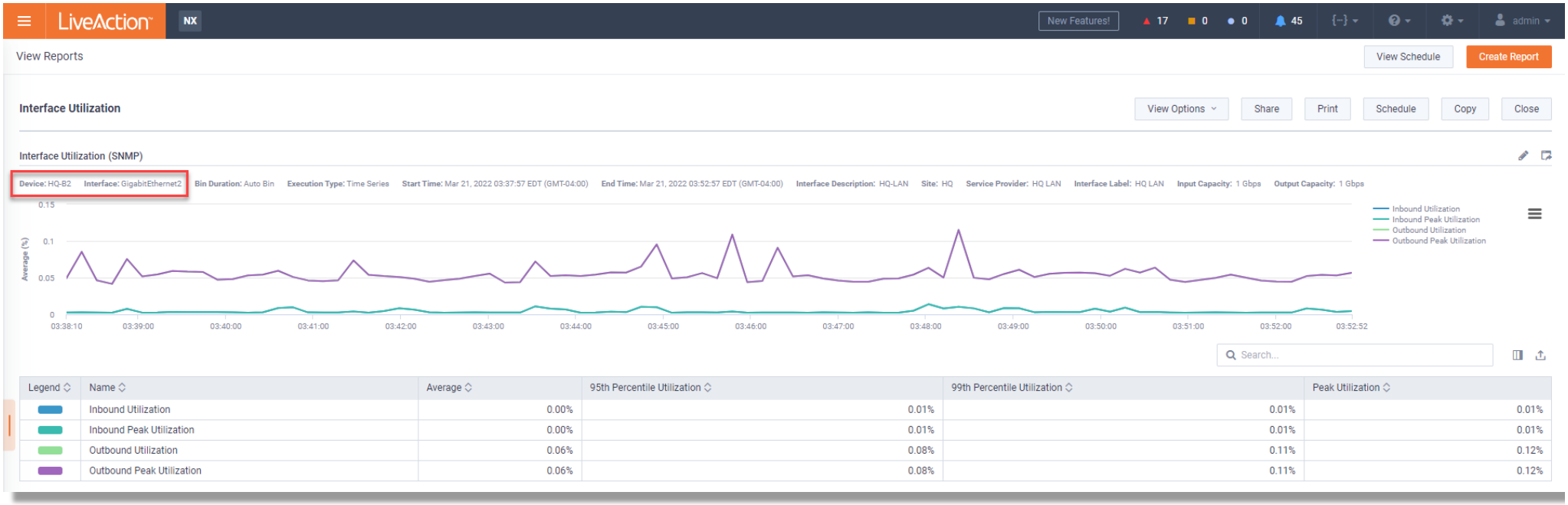
Interface Bandwidth (SNMP)

Single Interface View - Over Time

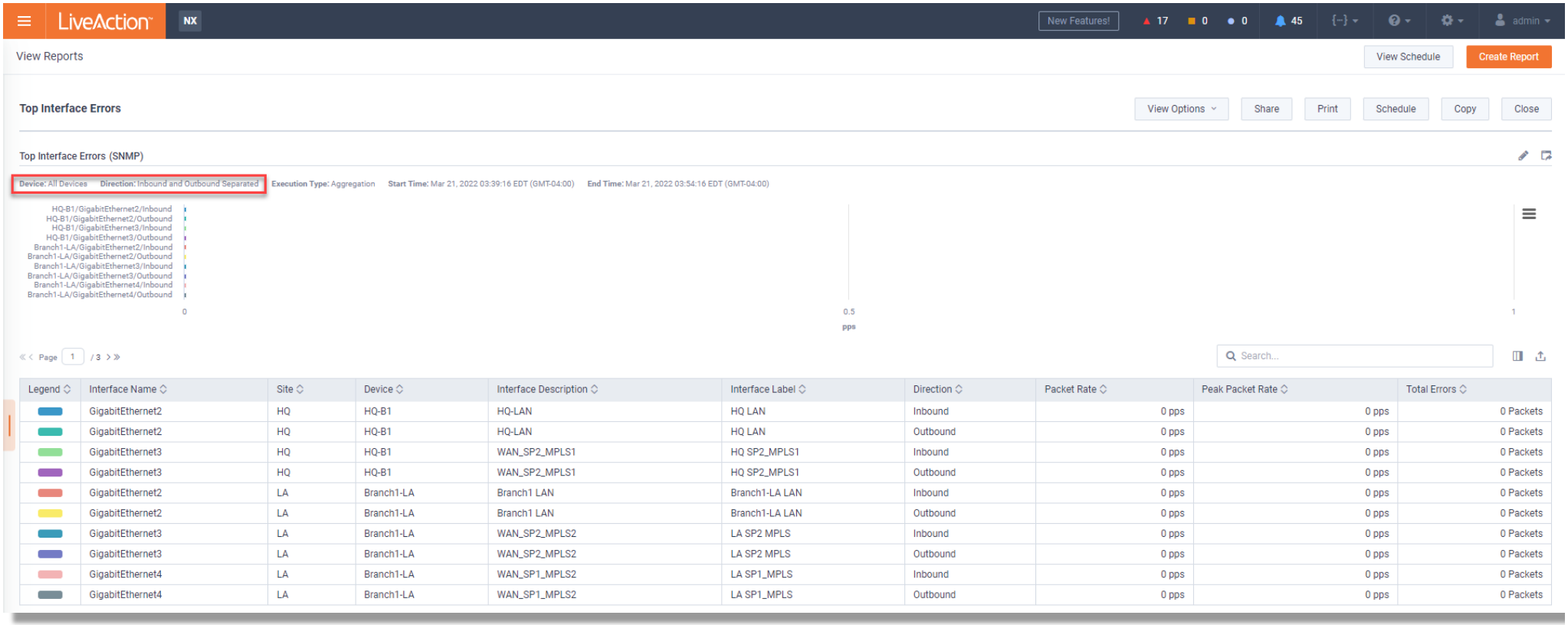


Interface Utilization (SNMP)

Single Interface View - Over Time



Top Interface Errors (SNMP)



Legend	Interface Name	Site	Device	Interface Description	Interface Label	Direction	Packet Rate	Peak Packet Rate	Total Errors
	GigabitEthernet2	HQ	HQ-B1	HQ-LAN	HQ LAN	Inbound	0 pps	0 pps	0 Packets
	GigabitEthernet2	HQ	HQ-B1	HQ-LAN	HQ LAN	Outbound	0 pps	0 pps	0 Packets
	GigabitEthernet3	HQ	HQ-B1	WAN_SP2_MPLS1	HQ SP2_MPLS1	Inbound	0 pps	0 pps	0 Packets
	GigabitEthernet3	HQ	HQ-B1	WAN_SP2_MPLS1	HQ SP2_MPLS1	Outbound	0 pps	0 pps	0 Packets
	GigabitEthernet2	LA	Branch1-LA	Branch1 LAN	Branch1-LA LAN	Inbound	0 pps	0 pps	0 Packets
	GigabitEthernet2	LA	Branch1-LA	Branch1 LAN	Branch1-LA LAN	Outbound	0 pps	0 pps	0 Packets
	GigabitEthernet3	LA	Branch1-LA	WAN_SP2_MPLS2	LA SP2 MPLS	Inbound	0 pps	0 pps	0 Packets
	GigabitEthernet3	LA	Branch1-LA	WAN_SP2_MPLS2	LA SP2 MPLS	Outbound	0 pps	0 pps	0 Packets
	GigabitEthernet4	LA	Branch1-LA	WAN_SP1_MPLS2	LA SP1_MPLS	Inbound	0 pps	0 pps	0 Packets
	GigabitEthernet4	LA	Branch1-LA	WAN_SP1_MPLS2	LA SP1_MPLS	Outbound	0 pps	0 pps	0 Packets

Top Class Drops (SNMP)

LAB 5: Dashboards and Reporting

- Create and View Dashboards
- Create & View Reports

Collecting Flows in LiveNX

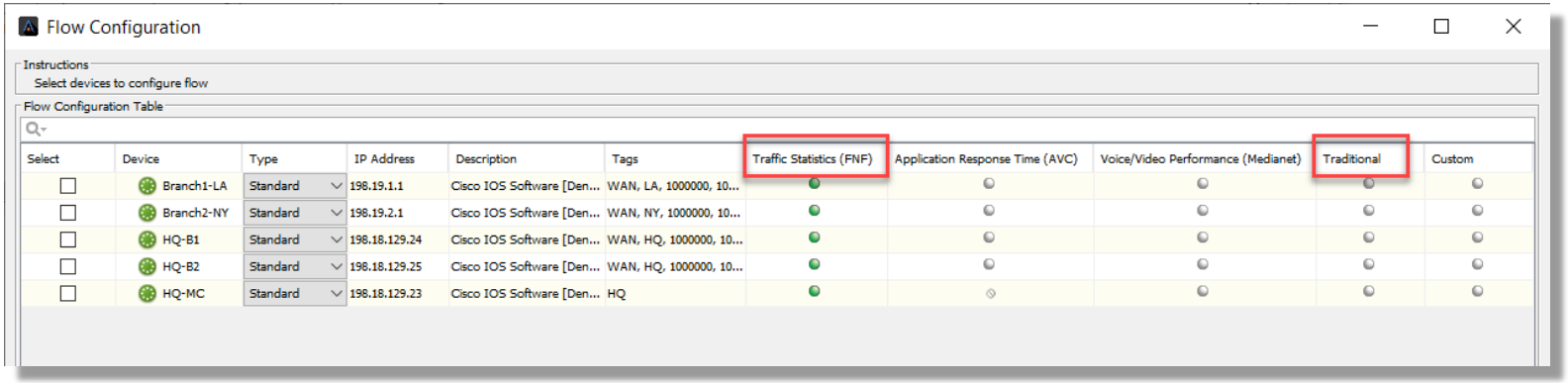
LiveAction™

Flow Collection

- The industry standard for flow type is “IPFIX”
  - Cisco uses sflow for certain devices types, such as Nexus 5k Switch
- Netflow is a brand name for Cisco Flow
  - Like Jaguar is a brand name for an automobile
- 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 Engineering Console)

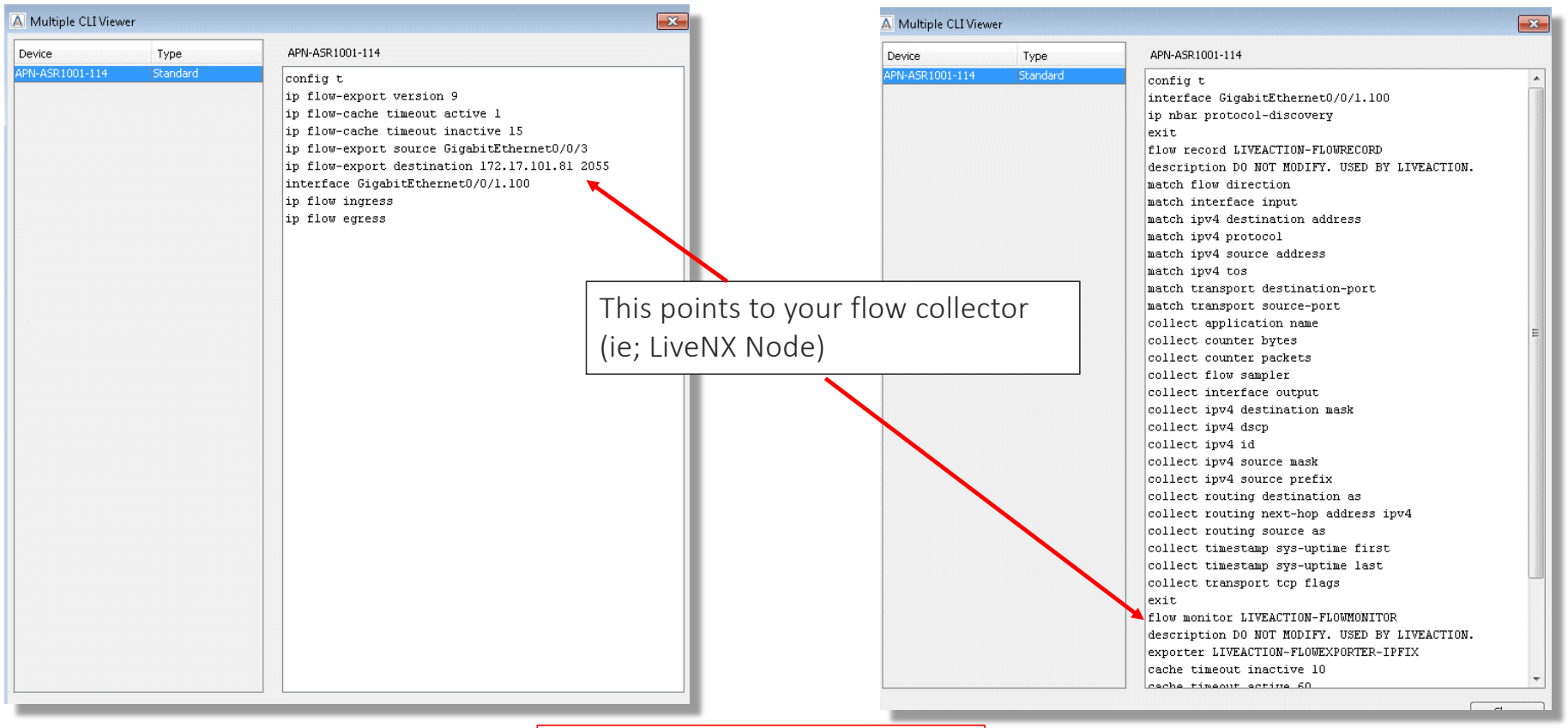
- Two types of Cisco Netflow – Traditional and Flexible
  - Traditional - an older flow type that uses a set record that cannot be configured
  - Flexible - newer flow type that allows for more granular record configuration



- 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

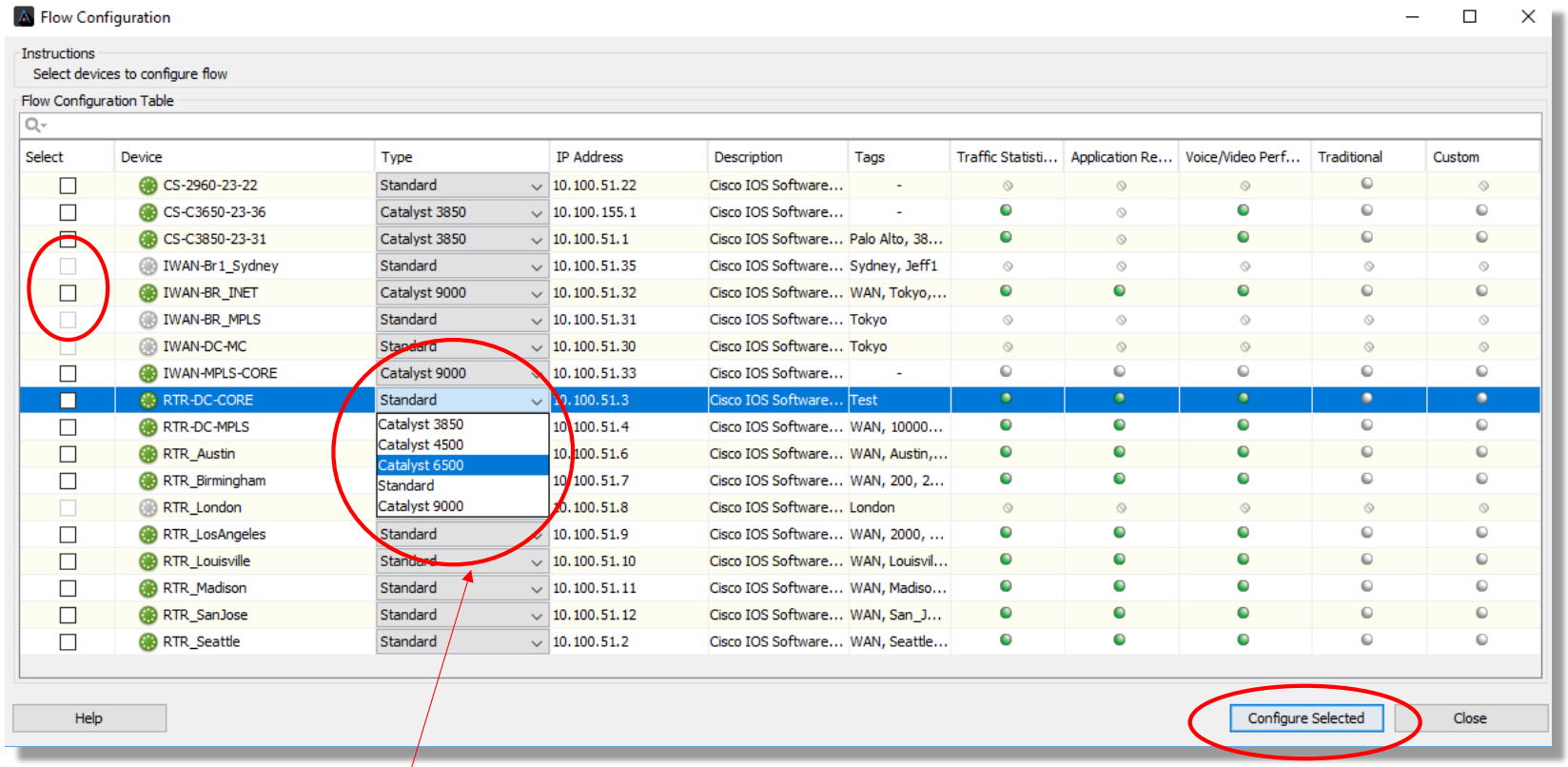
Remember: Configuration of devices is achieved through Engineering Console – or other configuration tools)

Traditional v. Flexible Netflow - Preview CLI



Cisco's Best-Practices Templates

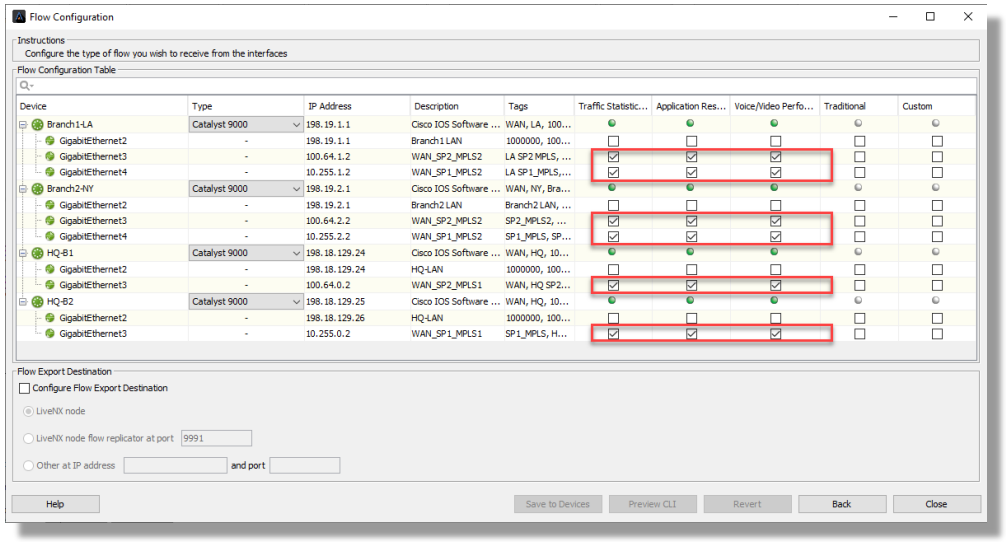
Enable Flow Collection Within LiveNX Engineering Console



Easily Setup Flow Configurations at the *Device* Level

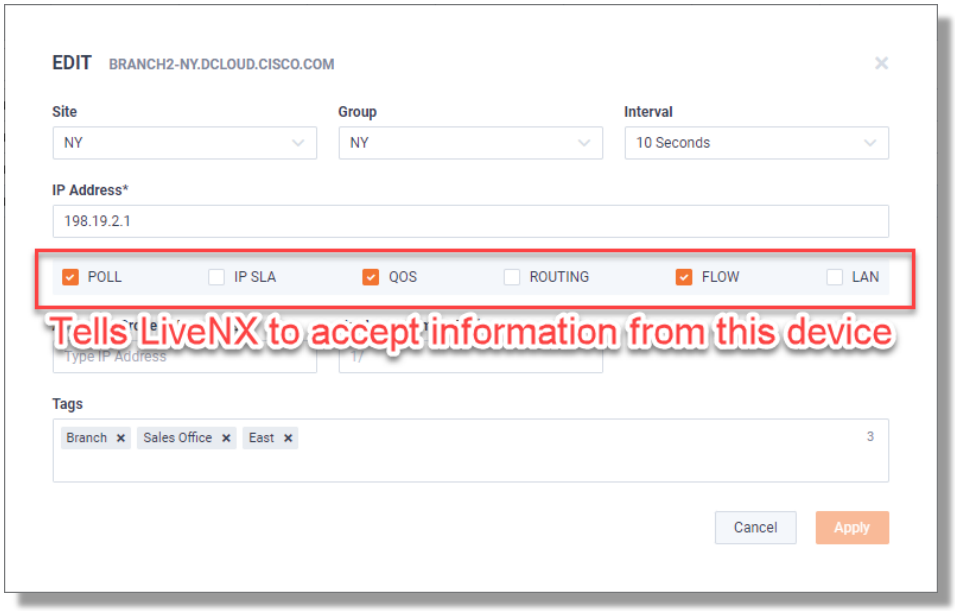
Enable Flow Collection on Interfaces

Engineering Console
Configuring device on what to report
And LiveNX to accept the reports



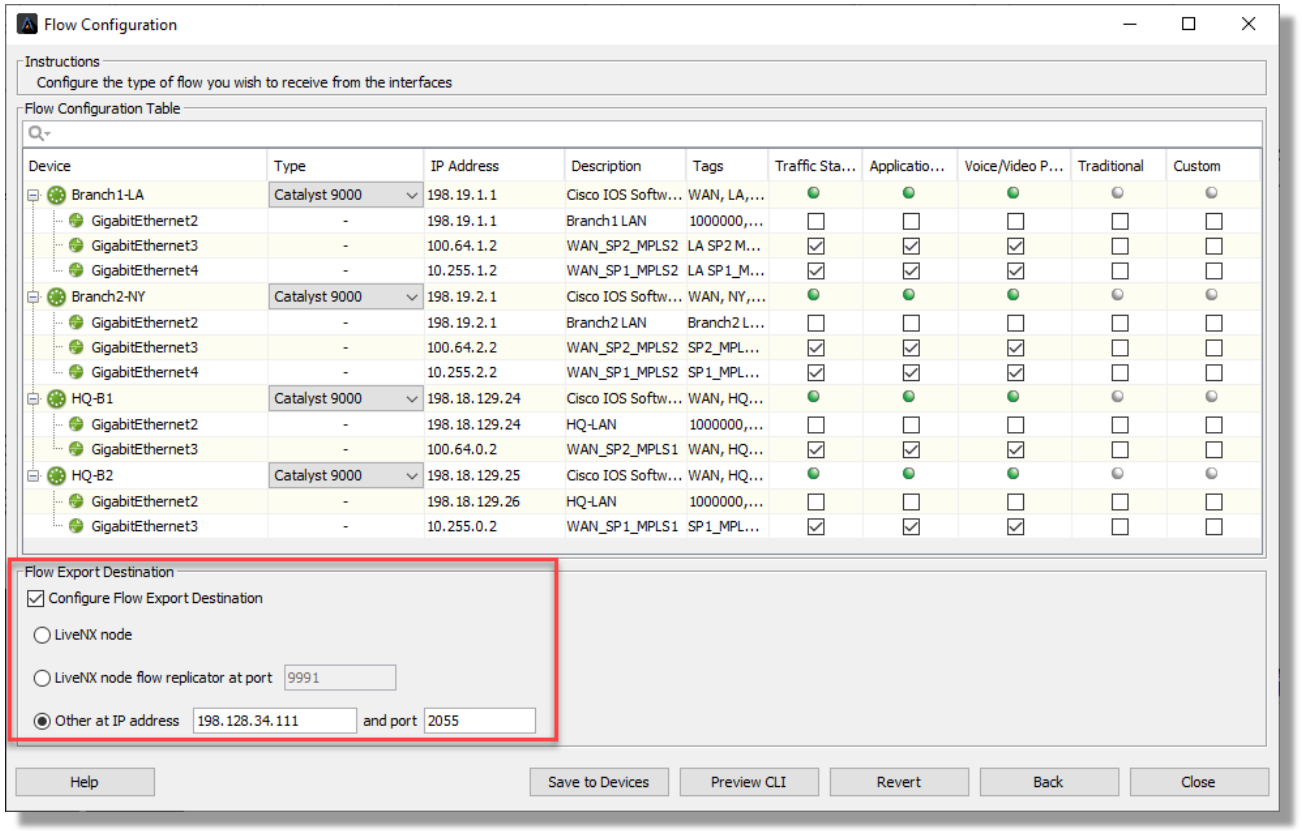
Setup Flow Configurations at the *Interface* Level

WebUI
Configuring LiveNX to accept reports

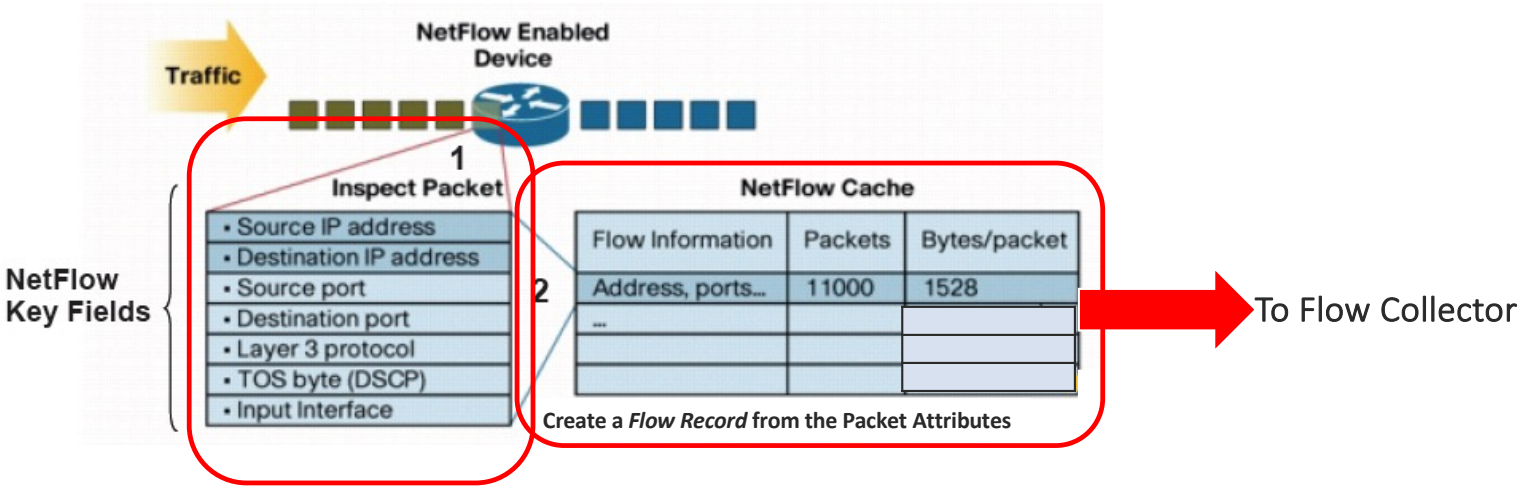


Re-Direct Collected Flows…

- 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…



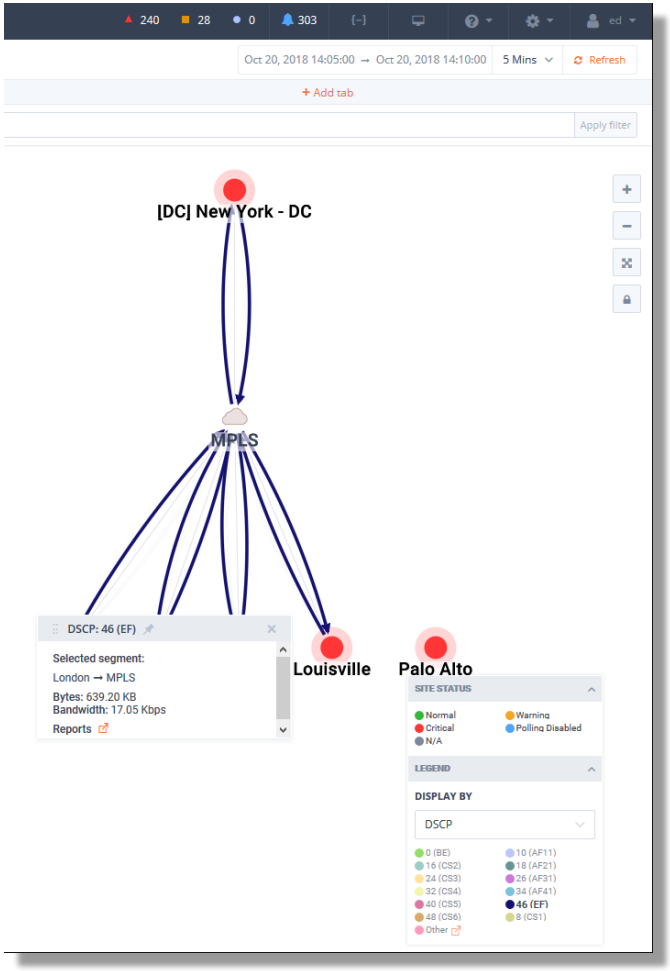
1. **A flow is unidirectional**
2. **Defined by inspecting a packet's key fields (common properties) and identifying the values**
3. **If the set of key field values is unique, create a flow record or cache entry**

Netflow

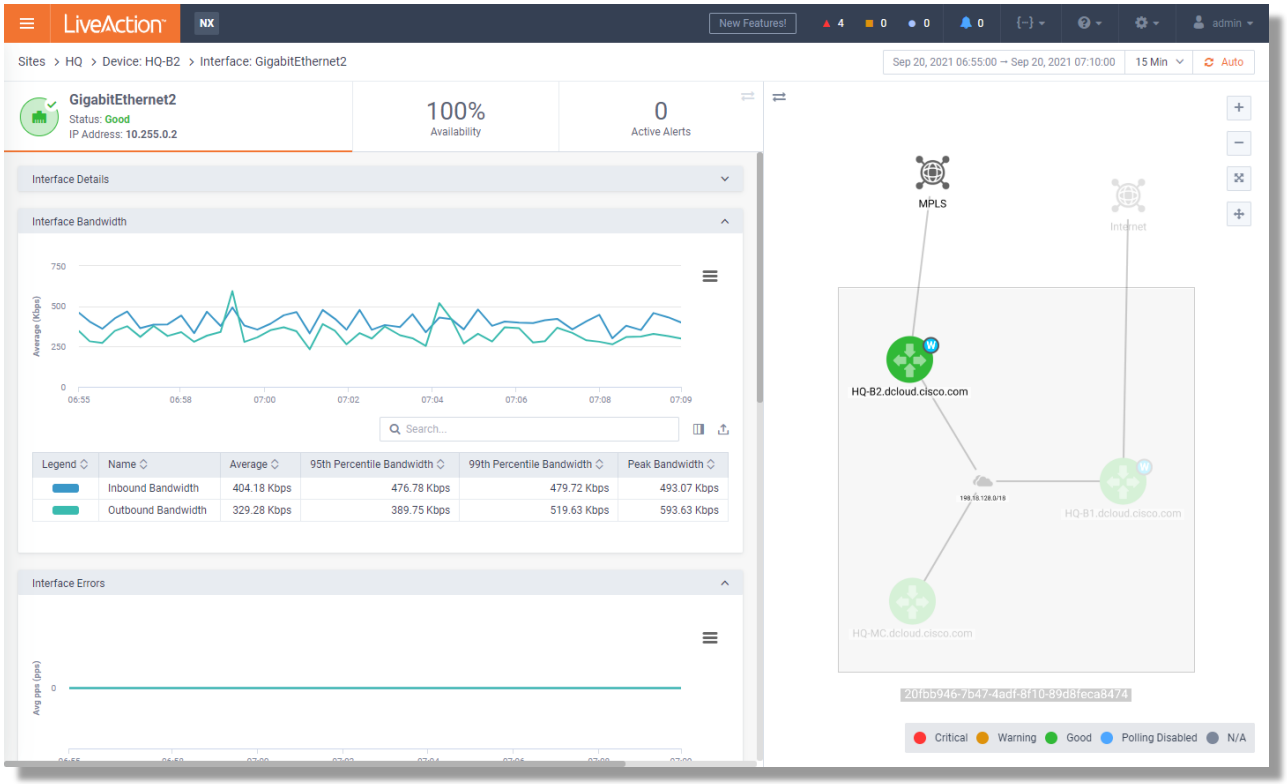
By analyzing the data across interfaces and exporting the Netflow data to LiveAction, a network administrator can determine:

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

per device.



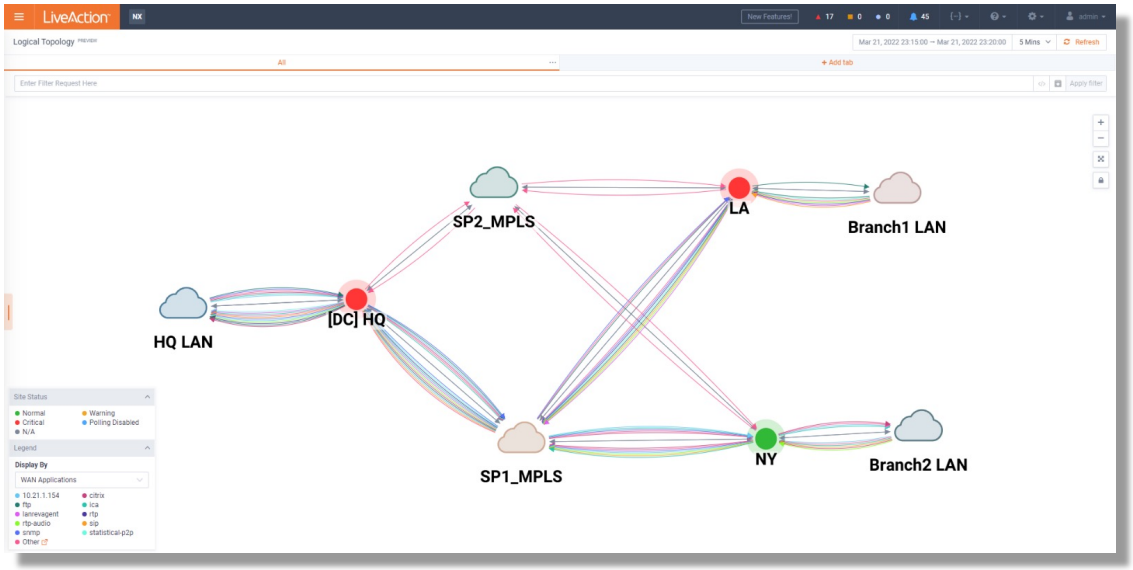
Netflow Interface View



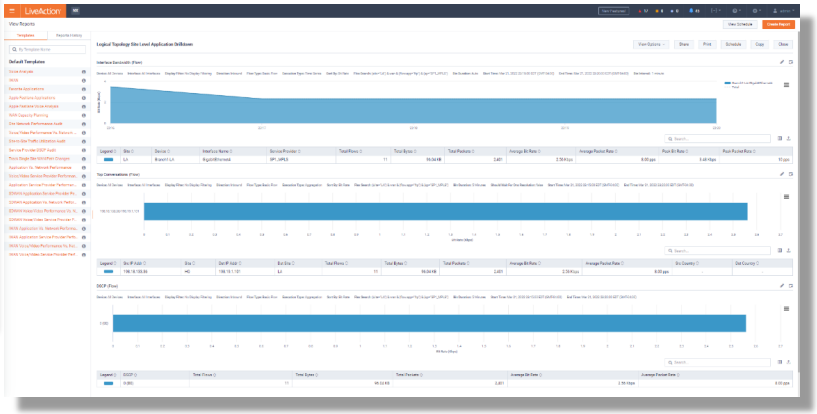
View quantity & type of traffic traversing a specific interface

Application Flow View

Logical Topology View

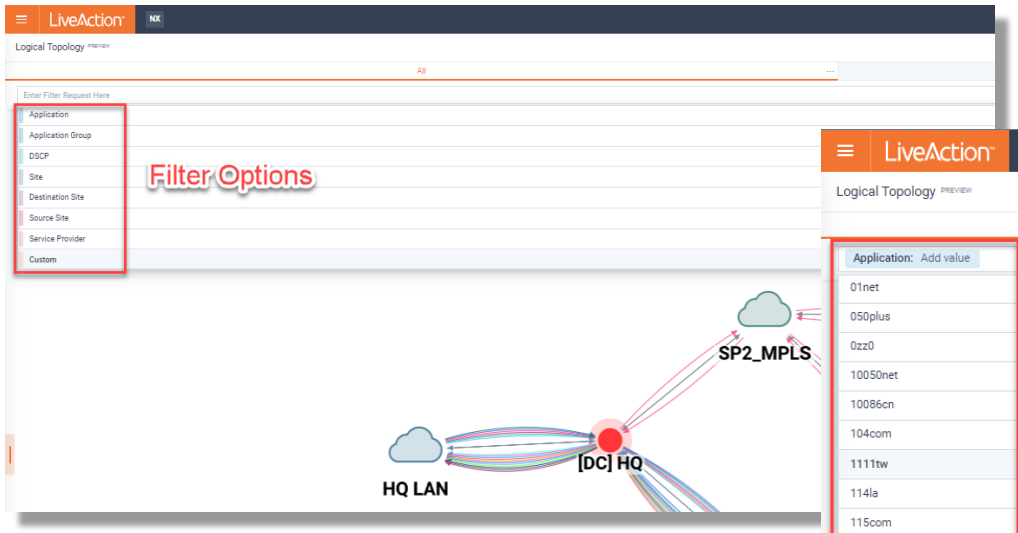


Single Click Drill-Down to Details

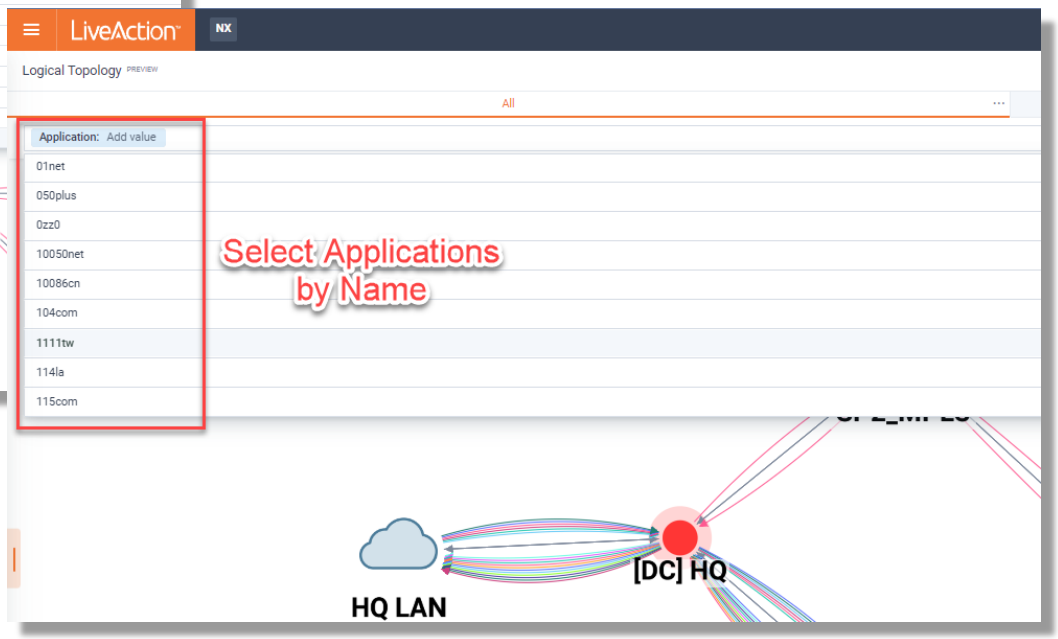


Filtering Topologies

Click in Filter Bar – Select Filtering Option from List



Start Typing and Click Filter by Application Name



Other types of Flow in LiveNX

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

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

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

* Separate License Purchase From Cisco

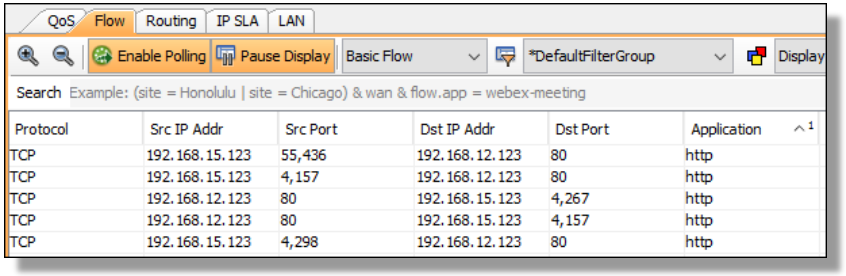
Network Based Application Recognition (NBAR2)

- 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

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

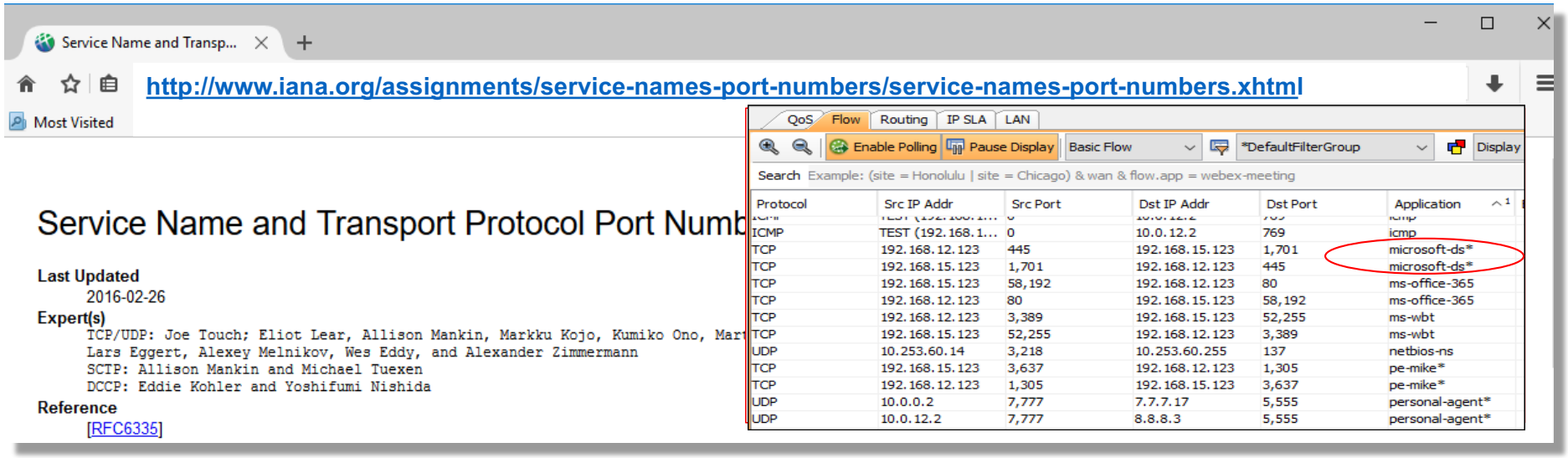


Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application
TCP	192.168.15.123	55,436	192.168.12.123	80	http
TCP	192.168.15.123	4,157	192.168.12.123	80	http
TCP	192.168.12.123	80	192.168.15.123	4,267	http
TCP	192.168.12.123	80	192.168.15.123	4,157	http
TCP	192.168.15.123	4,298	192.168.12.123	80	http

- 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

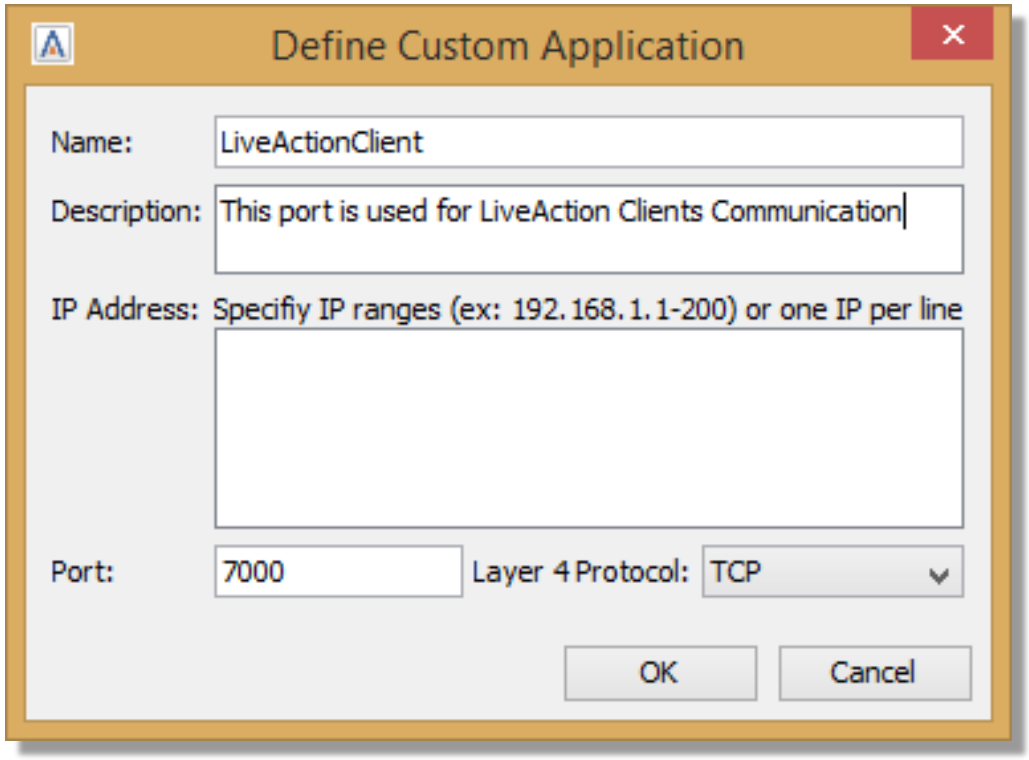
IANA.Org

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



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



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.

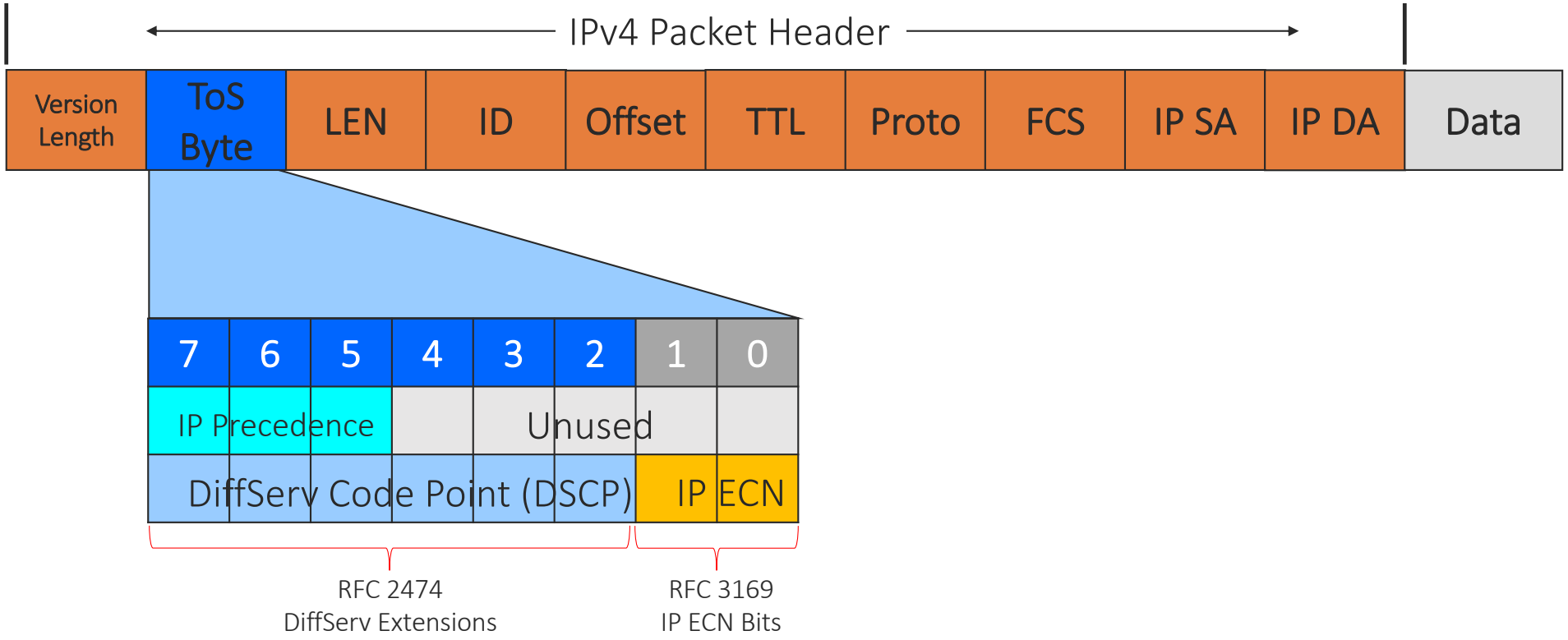
Differentiated Service Control Point (DSCP)

- 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.**

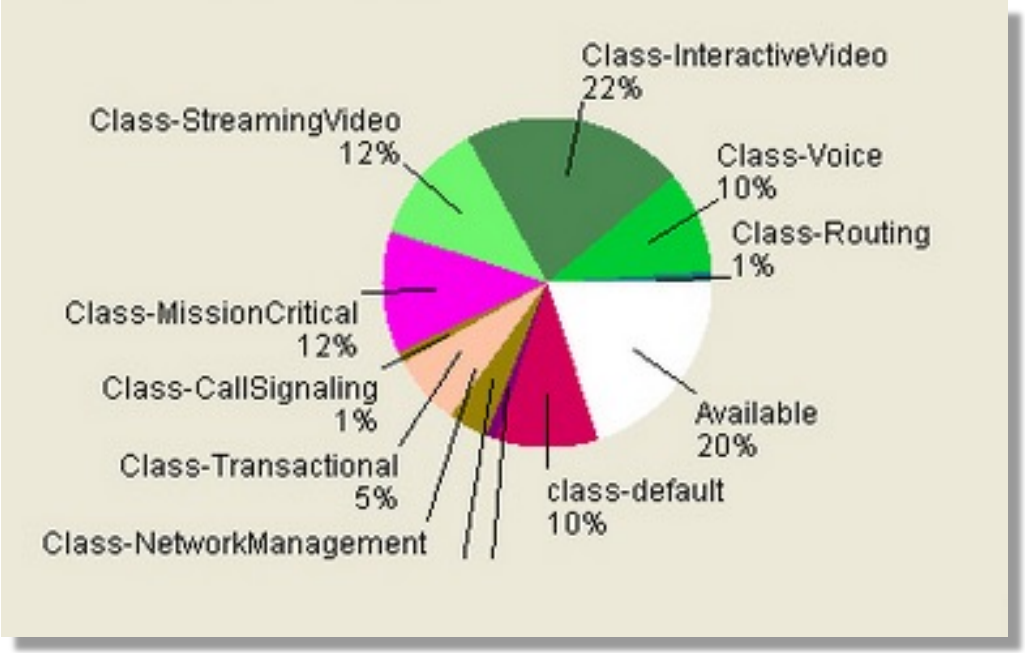
Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency 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

Packets & DSCP Markings



QoS Techniques

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



LAB 6 & 7: Working With Flow and Customizing Filters

- Discover Flows
- Identify Flows
- Create Custom Filters

LiveNX Implementation

Best Practices

LiveAction™

System Requirements

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

- Server Platform Specifications:
  - VMware ESXi v5.0 or higher – VMware Hardware Version 8 (vmx-8)
- Network Hardware – At least two Physical NICS on ESXi
  - Support up to 10 Gbps
  - Virtual NICs on OVA are utilizing E100

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

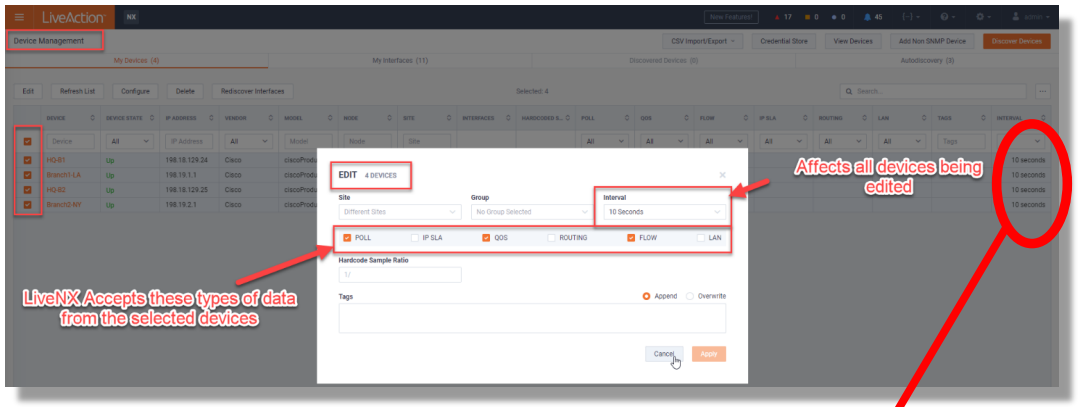
Disk Sizing- SNMP

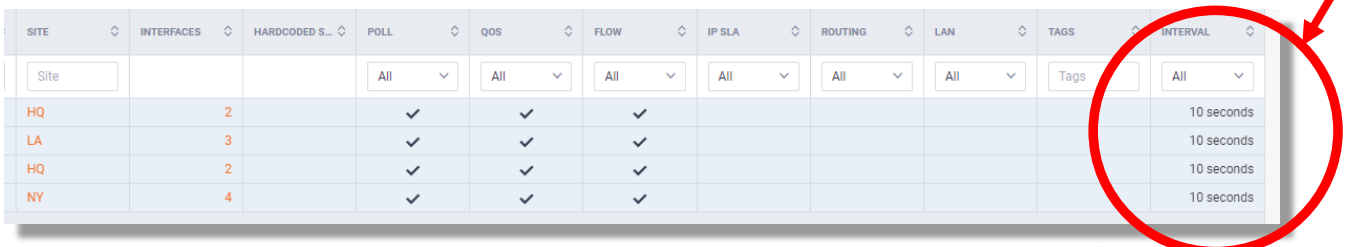
SNMP

- 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





Disk Sizing

SNMP

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

RAW 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 RAW Flow

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

RAW Flow

Avg Flow Rate (K flows sec)	< 25K/sec	< 100K/sec	< 200K/sec	< 300K/sec
RAW 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

NetFlow Bandwidth Overhead – Someone ALWAYS Asks!

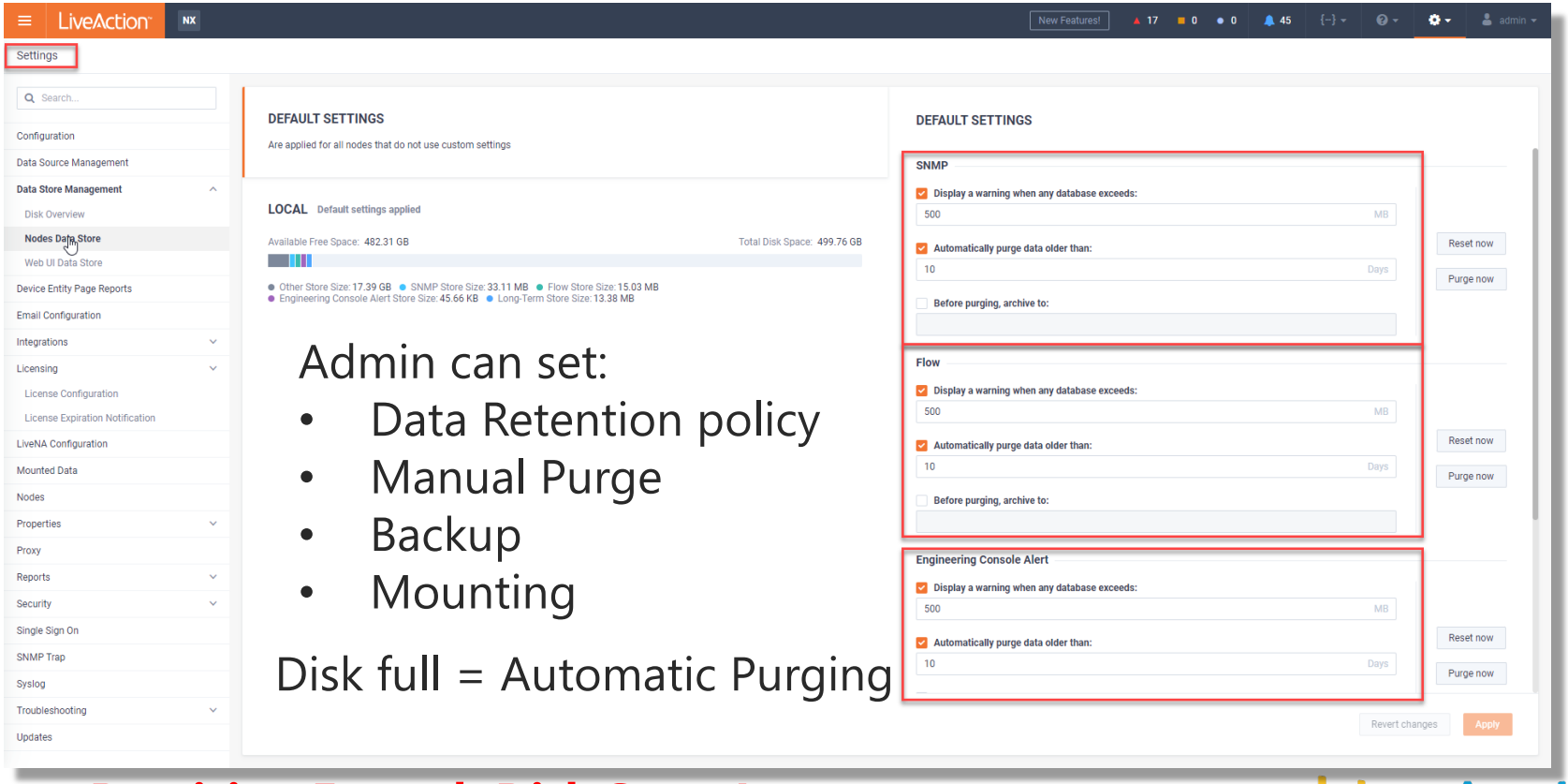
Device Type	Flows/Sec	Full-Duplex User Bandwidth Avg.-Peak	NetFlow Bandwidth Average	NetFlow Bandwidth Peak
WAN Router	.61	158-309Kbps	2Kbps (1%)	14.8Kbps (4%)
WAN Router	34	505K-1.1Mbps	16Kbps (3%)	42.4Kbps (3%)
WAN Router	27	820K-2.6Mbps	22Kbps (2%)	36Kbps (1%)
WAN Router	197	~21-39Mbps	85Kbps (.04%)	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.

Disk Retention

Settings > Data Store Management > Nodes Data Store:



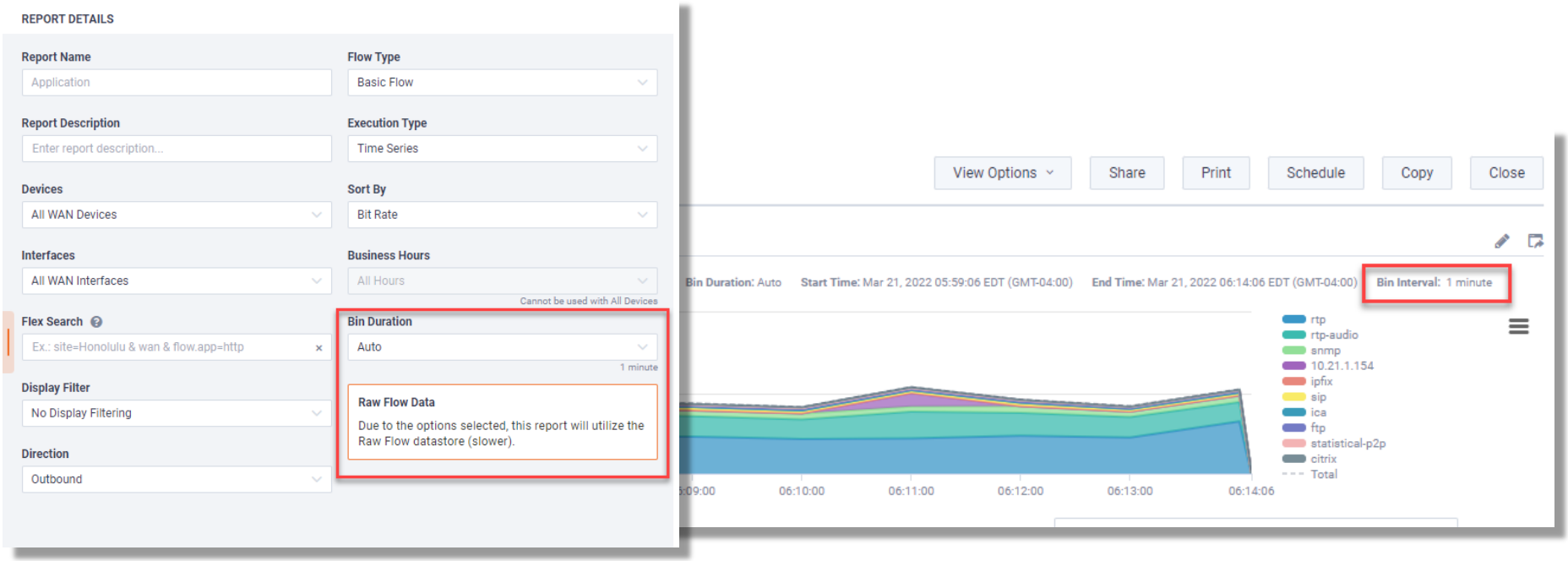
Admin can set:

- Data Retention policy
- Manual Purge
- Backup
- Mounting

Disk full = Automatic Purging

Provision Enough Disk Space!

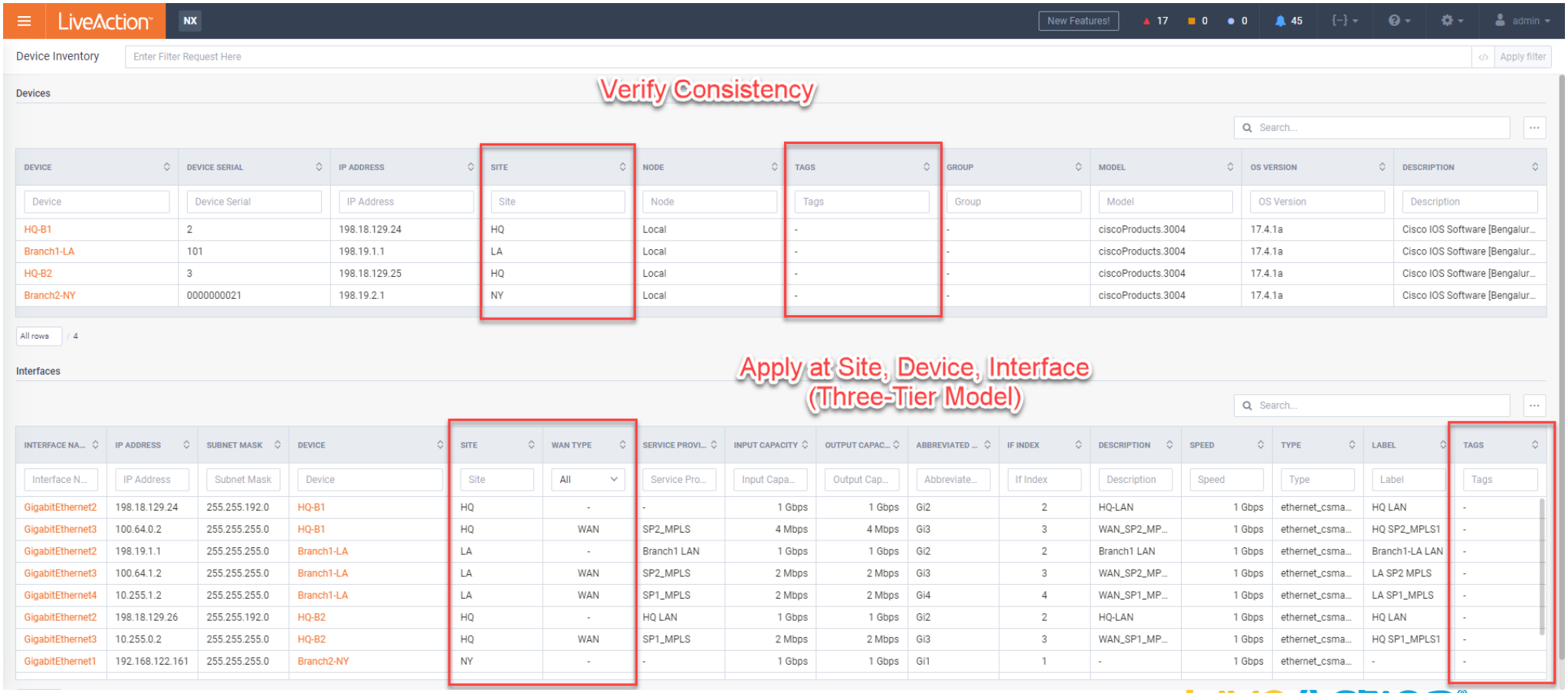
Search – Data Bin



- LiveAction stores all data in the raw in the RAW Flow 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

Device Semantics…

Have a plan for Semantic Data
Create a three-tier model



NetFlow Best Practices

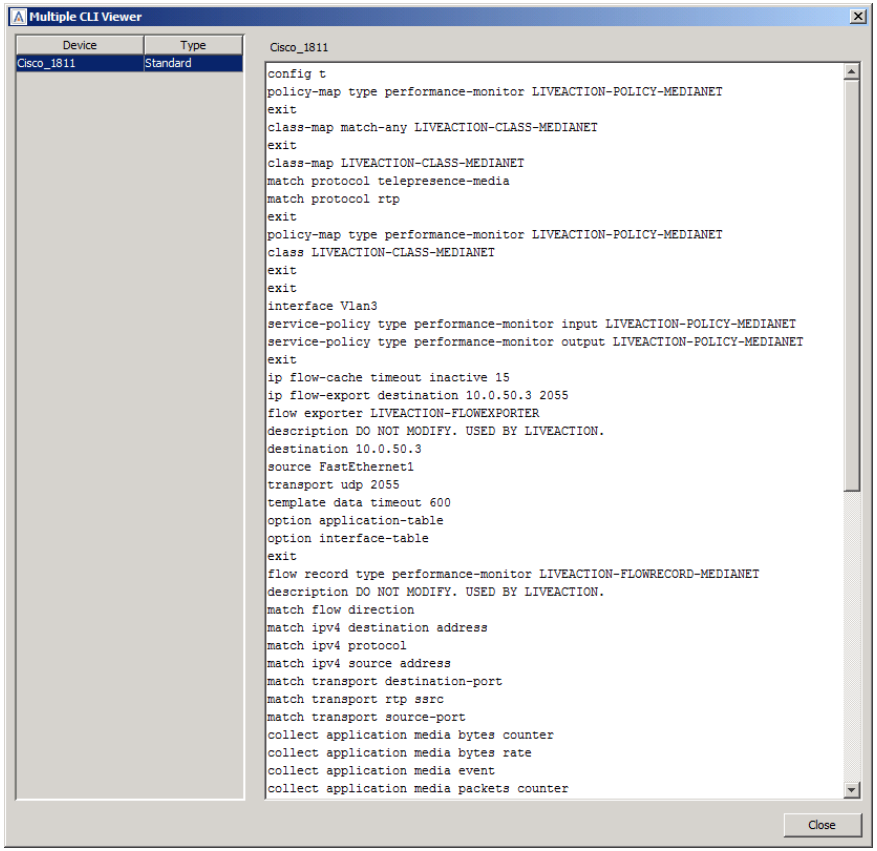
LiveAction™

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

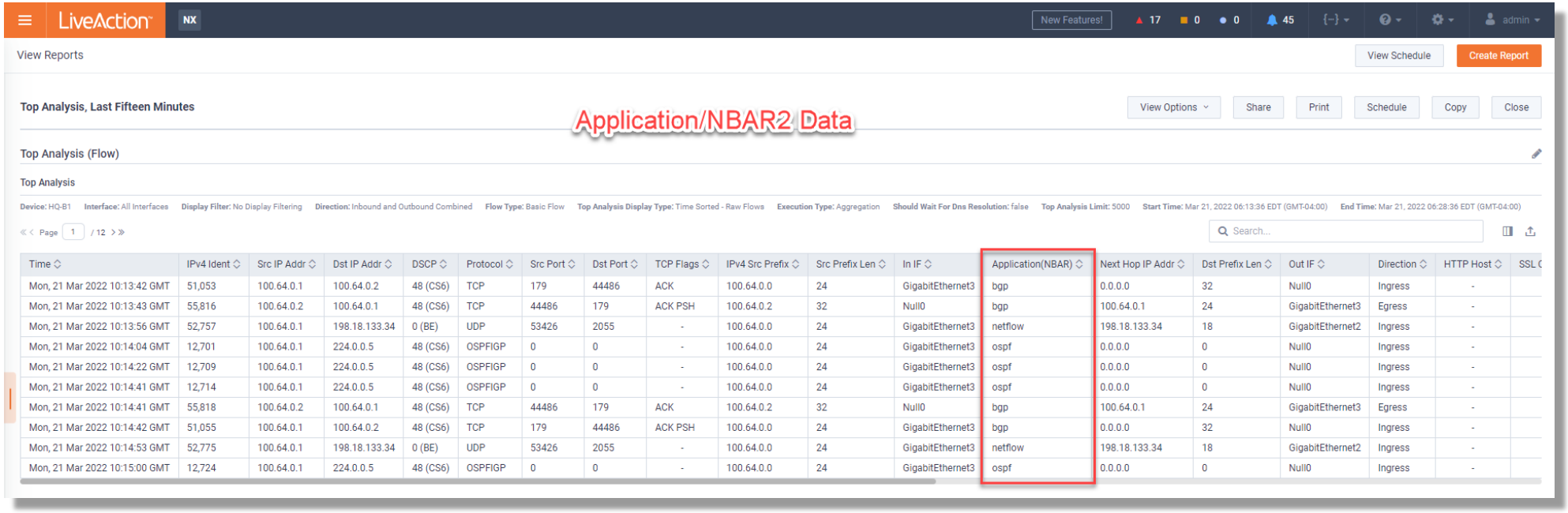
NetFlow – Configuration Management



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



Time	IPv4 Ident	Src IP Addr	Dst IP Addr	DSCP	Protocol	Src Port	Dst Port	TCP Flags	IPv4 Src Prefix	Src Prefix Len	In IF	Application(NBAR)	Next Hop IP Addr	Dst Prefix Len	Out IF	Direction	HTTP Host
Mon, 21 Mar 2022 10:13:42 GMT	51,053	100.64.0.1	100.64.0.2	48 (CS6)	TCP	179	44486	ACK	100.64.0.0	24	GigabitEthernet3	bgp	0.0.0.0	32	Null0	Ingress	-
Mon, 21 Mar 2022 10:13:43 GMT	55,816	100.64.0.2	100.64.0.1	48 (CS6)	TCP	44486	179	ACK PSH	100.64.0.2	32	Null0	bgp	100.64.0.1	24	GigabitEthernet3	Egress	-
Mon, 21 Mar 2022 10:13:56 GMT	52,757	100.64.0.1	198.18.133.34	0 (BE)	UDP	53426	2055	-	100.64.0.0	24	GigabitEthernet3	netflow	198.18.133.34	18	GigabitEthernet2	Ingress	-
Mon, 21 Mar 2022 10:14:04 GMT	12,701	100.64.0.1	224.0.0.5	48 (CS6)	OSPFIGP	0	0	-	100.64.0.0	24	GigabitEthernet3	ospf	0.0.0.0	0	Null0	Ingress	-
Mon, 21 Mar 2022 10:14:22 GMT	12,709	100.64.0.1	224.0.0.5	48 (CS6)	OSPFIGP	0	0	-	100.64.0.0	24	GigabitEthernet3	ospf	0.0.0.0	0	Null0	Ingress	-
Mon, 21 Mar 2022 10:14:41 GMT	12,714	100.64.0.1	224.0.0.5	48 (CS6)	OSPFIGP	0	0	-	100.64.0.0	24	GigabitEthernet3	ospf	0.0.0.0	0	Null0	Ingress	-
Mon, 21 Mar 2022 10:14:41 GMT	55,818	100.64.0.2	100.64.0.1	48 (CS6)	TCP	44486	179	ACK	100.64.0.2	32	Null0	bgp	100.64.0.1	24	GigabitEthernet3	Egress	-
Mon, 21 Mar 2022 10:14:42 GMT	51,055	100.64.0.1	100.64.0.2	48 (CS6)	TCP	179	44486	ACK PSH	100.64.0.0	24	GigabitEthernet3	bgp	0.0.0.0	32	Null0	Ingress	-
Mon, 21 Mar 2022 10:14:53 GMT	52,775	100.64.0.1	198.18.133.34	0 (BE)	UDP	53426	2055	-	100.64.0.0	24	GigabitEthernet3	netflow	198.18.133.34	18	GigabitEthernet2	Ingress	-
Mon, 21 Mar 2022 10:15:00 GMT	12,724	100.64.0.1	224.0.0.5	48 (CS6)	OSPFIGP	0	0	-	100.64.0.0	24	GigabitEthernet3	ospf	0.0.0.0	0	Null0	Ingress	-

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

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

NetFlow – Where to Enable Flow?

The Fewest Interfaces Possible!

Why?

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

Routers

- Usually WAN Interfaces Only

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

NetFlow – AVC/Medianet

- AVC/Medianet enabled on fewest interfaces possible
  - Enable only on WAN interfaces for routers
  - L2/L3 uplinks only on switches

- Modify Interesting traffic class-maps where applicable

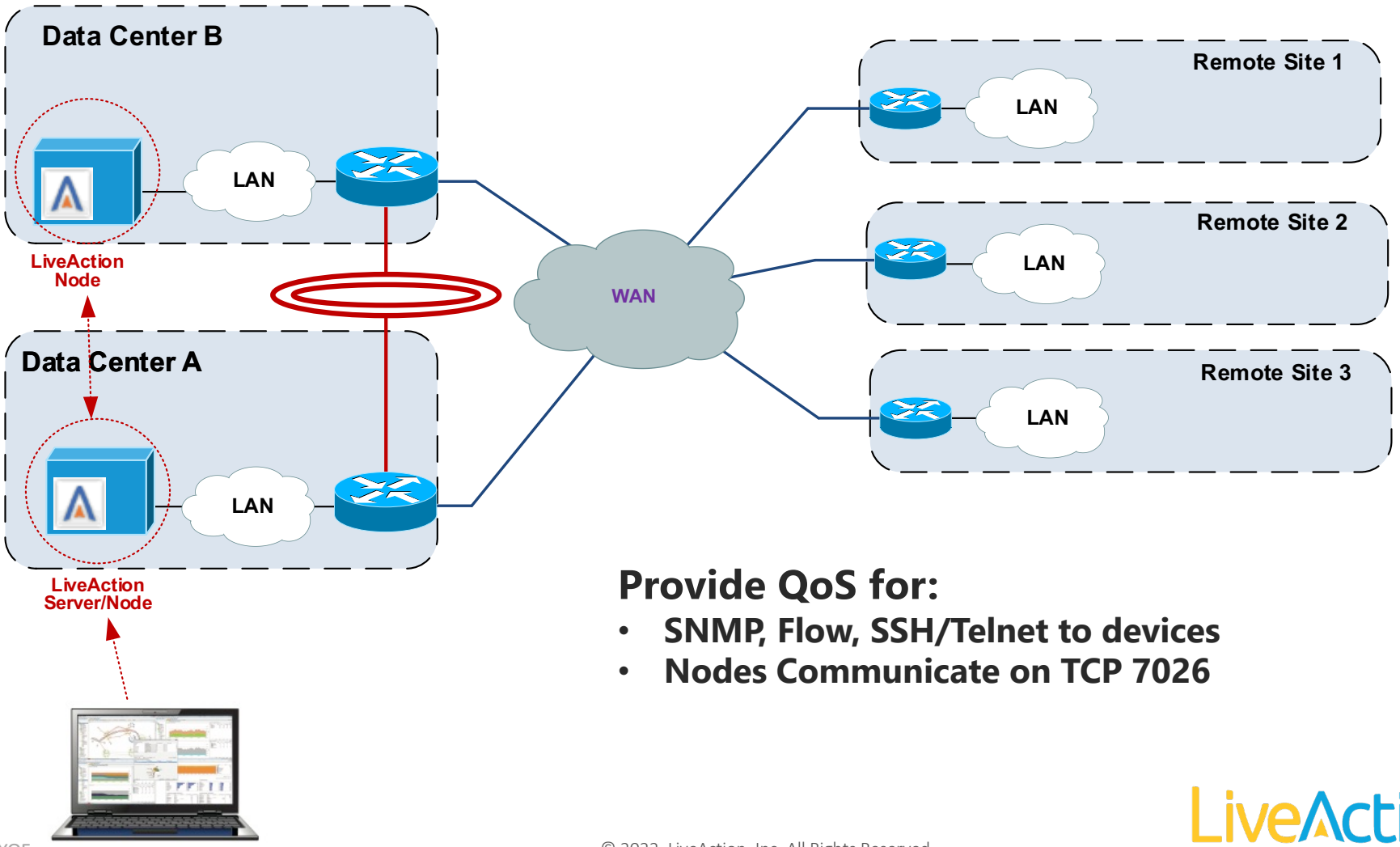
```
class-map match-any LIVEACTION-CLASS-AVC
 match access-group name LIVEACTION-ACL-AVC

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

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

Other Best Practices

LiveAction™

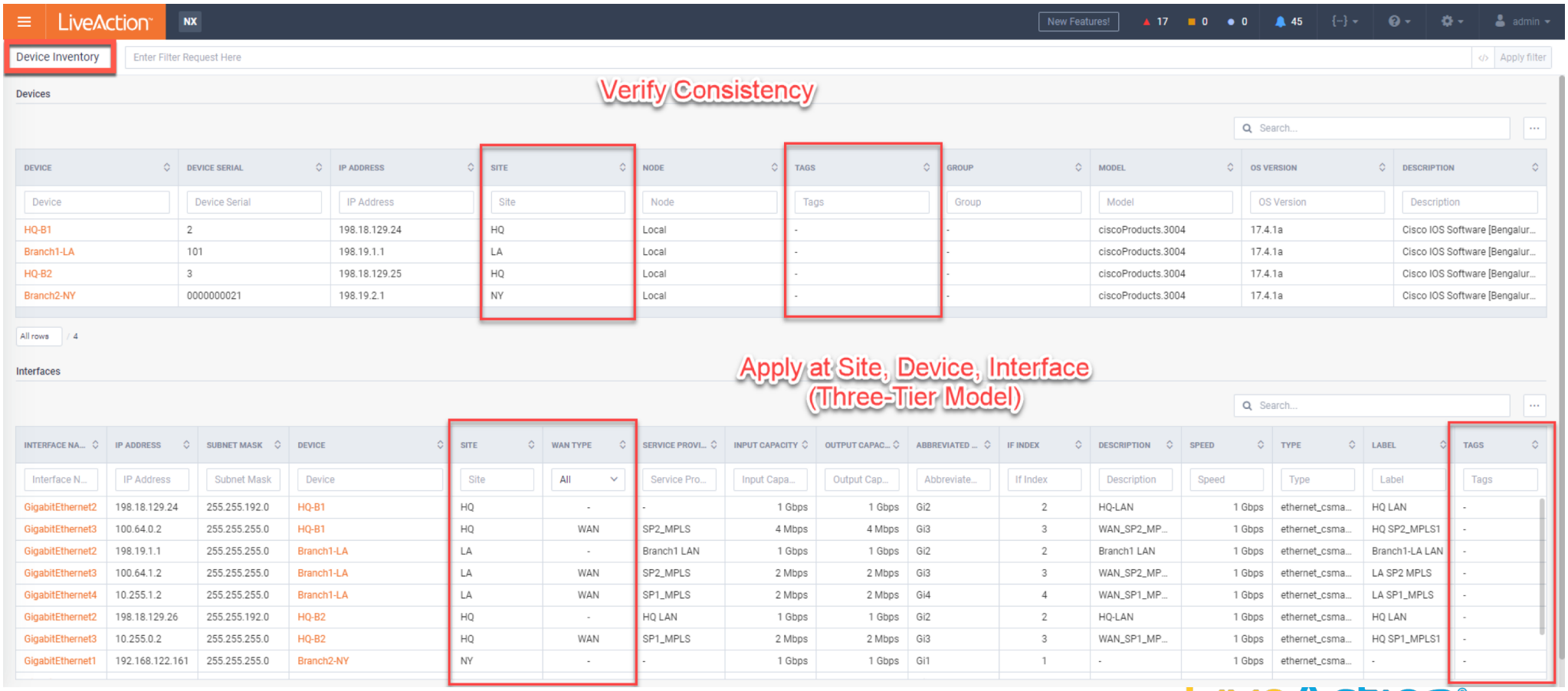


Provide QoS for:

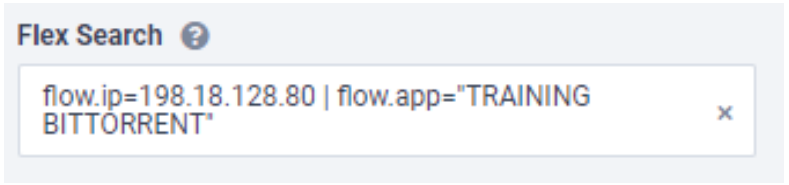
- SNMP, Flow, SSH/Telnet to devices
- Nodes Communicate on TCP 7026

Device Semantics…

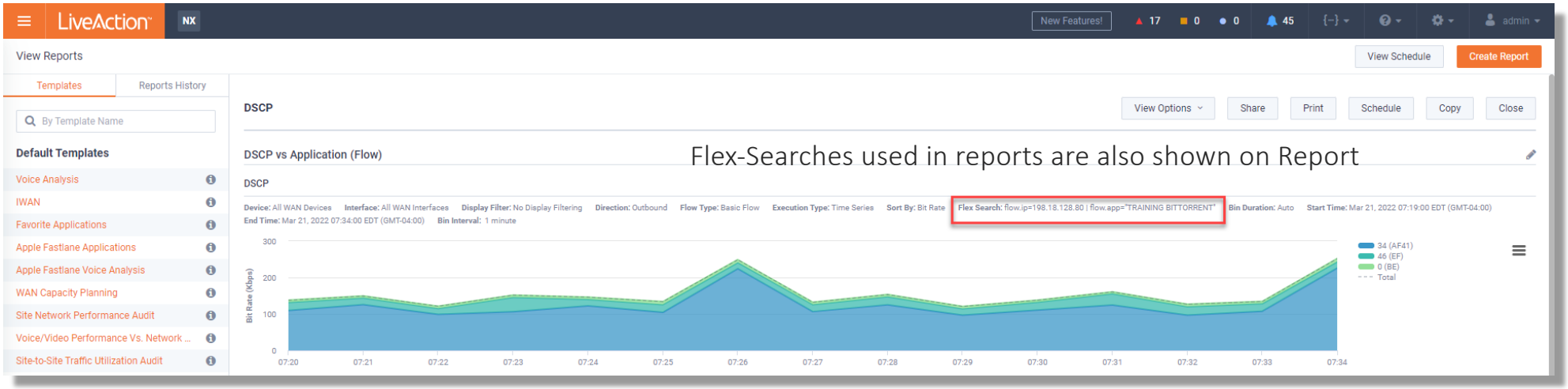
Have a plan for Semantic Data
Create a three-tier model



Semantic Data – In Reporting Example 1

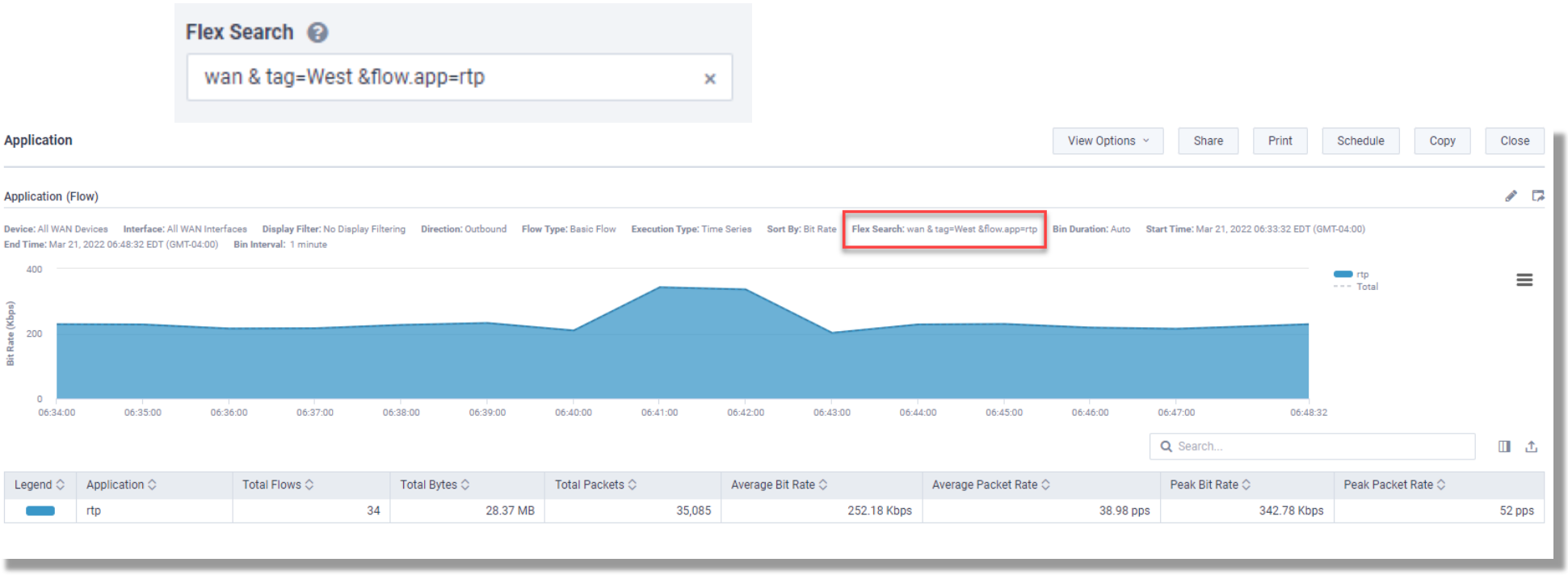


Configure Reports with Flex-Search using Tags (Semantic Data)



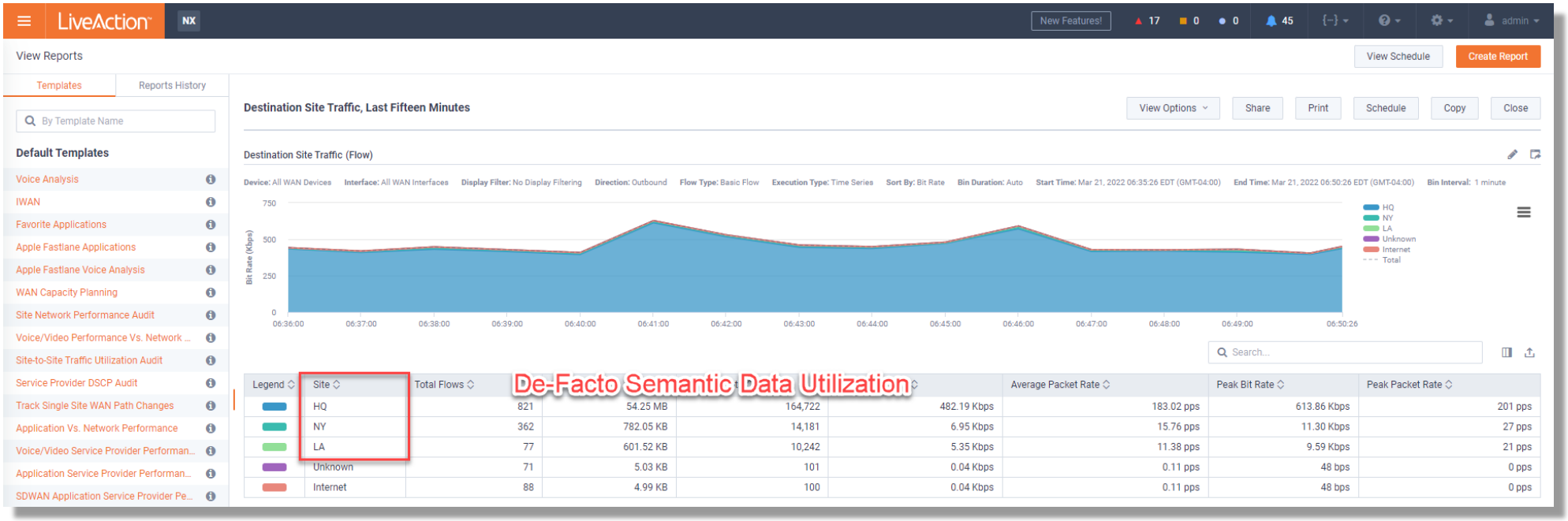
Show me Custom Application Training Bittorrent data to or from 198.18.128.80

Semantic Data – In Reporting Example 2



Show me RTP data from WAN interfaces, that have West as a tag

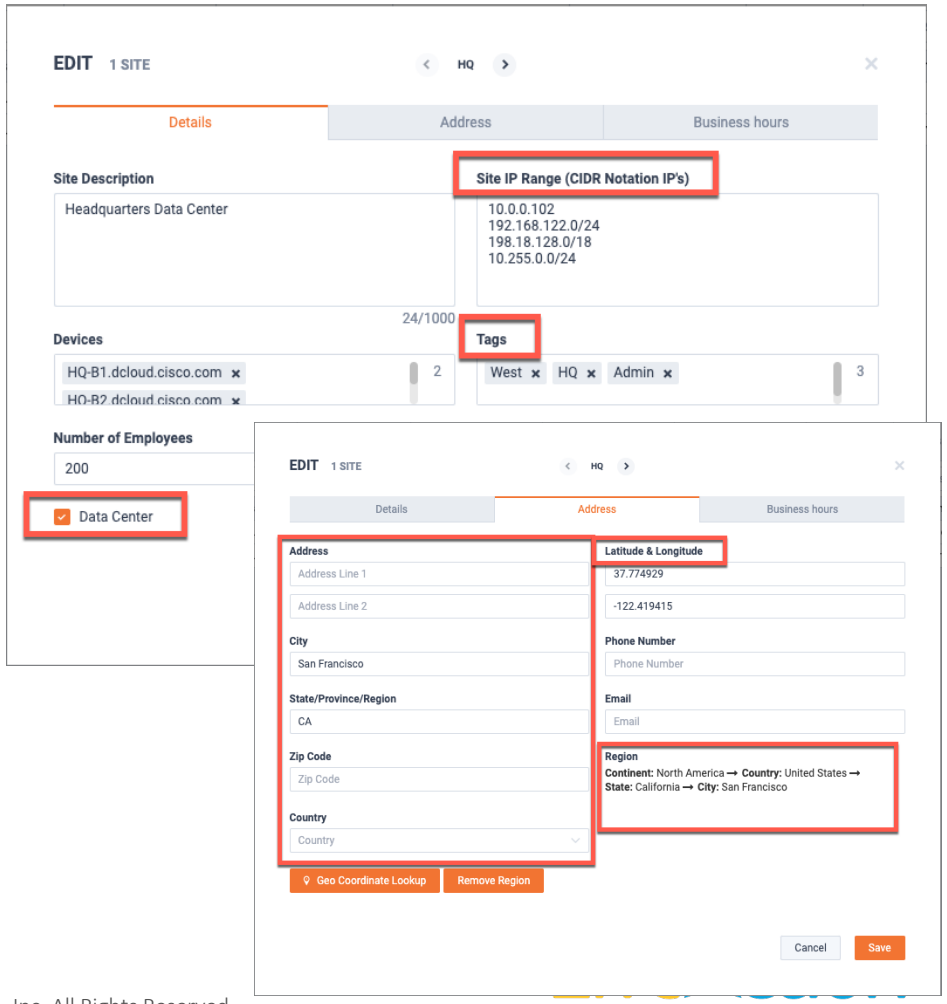
Semantic Data – In Reporting Example 3



Unknown and Internet are created from address ranges without a site:
Public addresses not assigned to a site will show up as **Internet**
Private Addresses not assigned to a site will show up as **unknown**

Semantic Data - Sites

- Descriptors of the Site
- Tags
- Data Center
- IP Address Ranges
- Geographical Location (Region, Country, City, etc)



End of Day 1…
What's Next?

Finish the Labs…

LiveAction™

Agenda - Day 2

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

LiveNX Training

Day 2

03 April 2022

LiveAction™

Agenda - Day 2

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

Quality of Service

Concept Overview

LiveAction™

How to Implement QoS

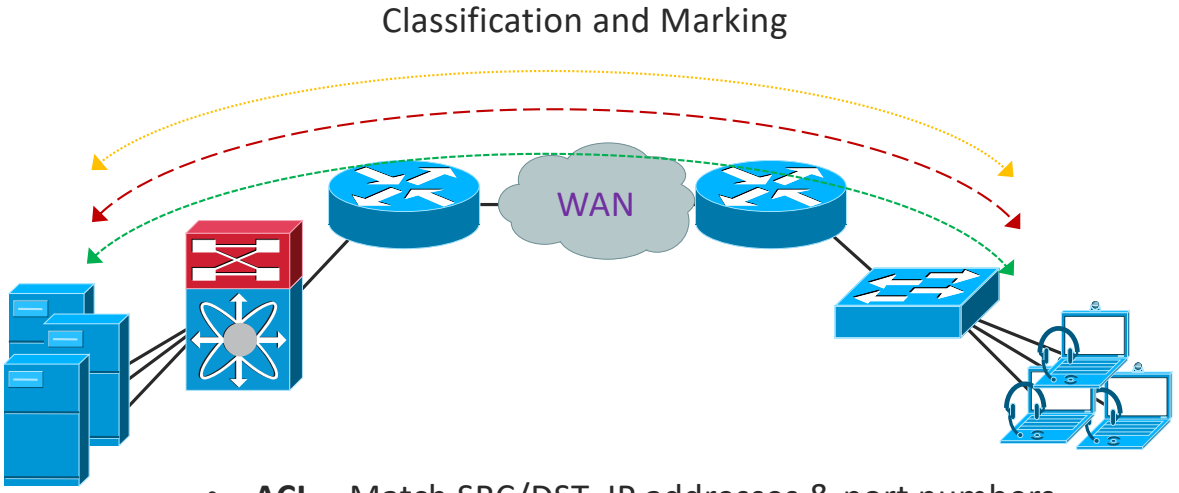
Step 1 - Recognize Application Traffic (Classification and Marking)

Step 2 - Prioritize (Queuing and Shaping)

Step 3 - Throttle Traffic (Policing and WRED)

Step 4 - Buffer Tuning

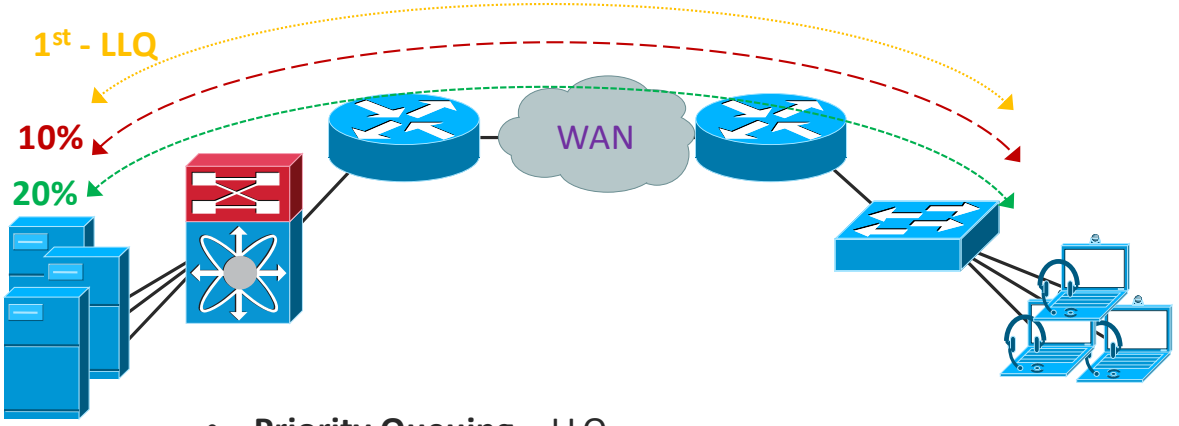
Step 1 - Recognize Application Traffic



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

Step 2 – Prioritize

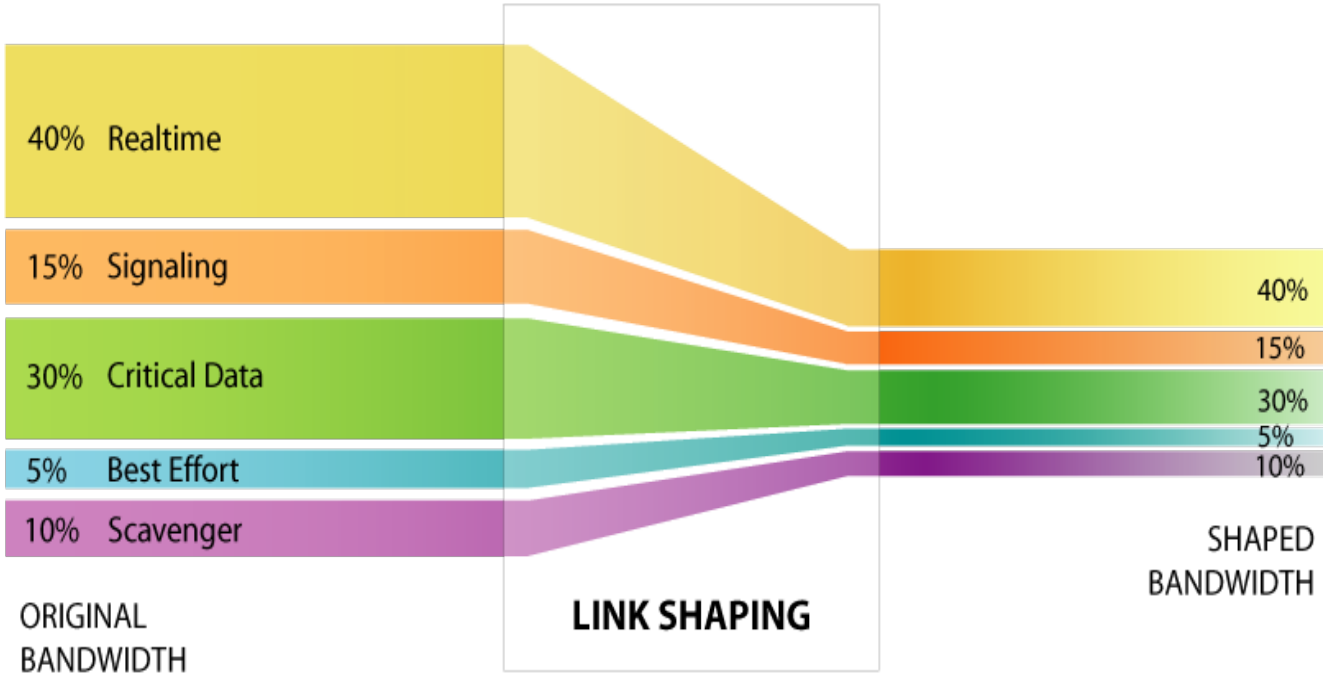
Queuing and Shaping



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

Shaping (or Scaling)

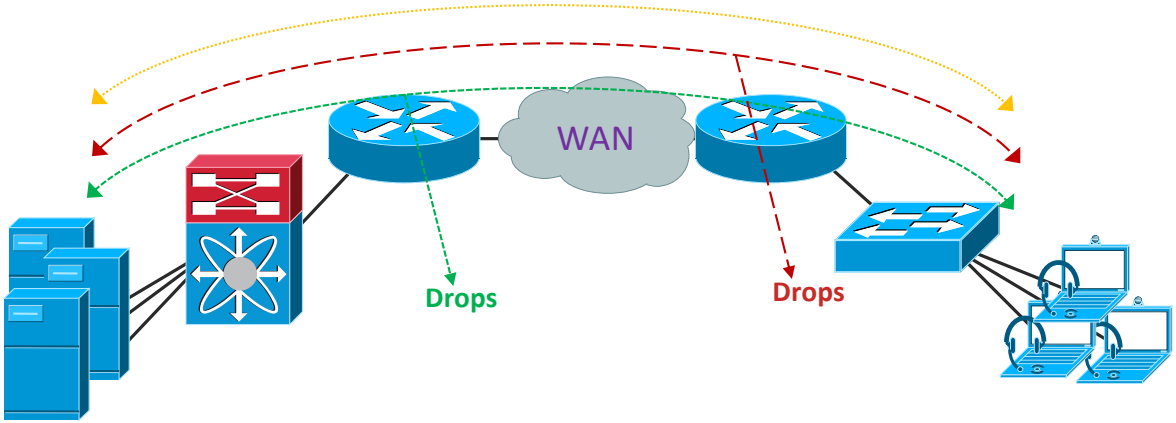
10Gbs



100Mbs

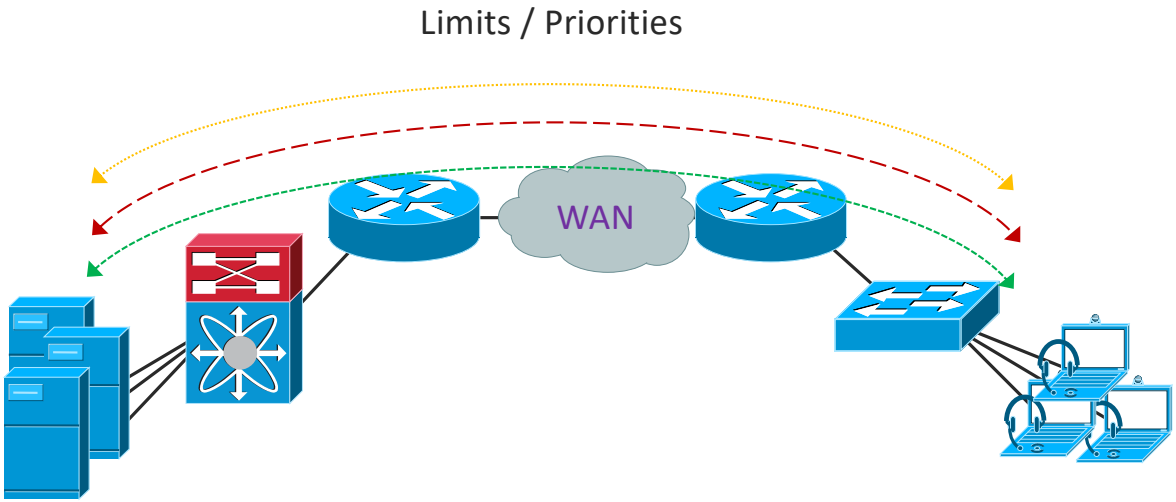
Step 3 –Throttle Traffic

Policing and WRED



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

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

QoS Monitoring & Configuration

LiveAction™

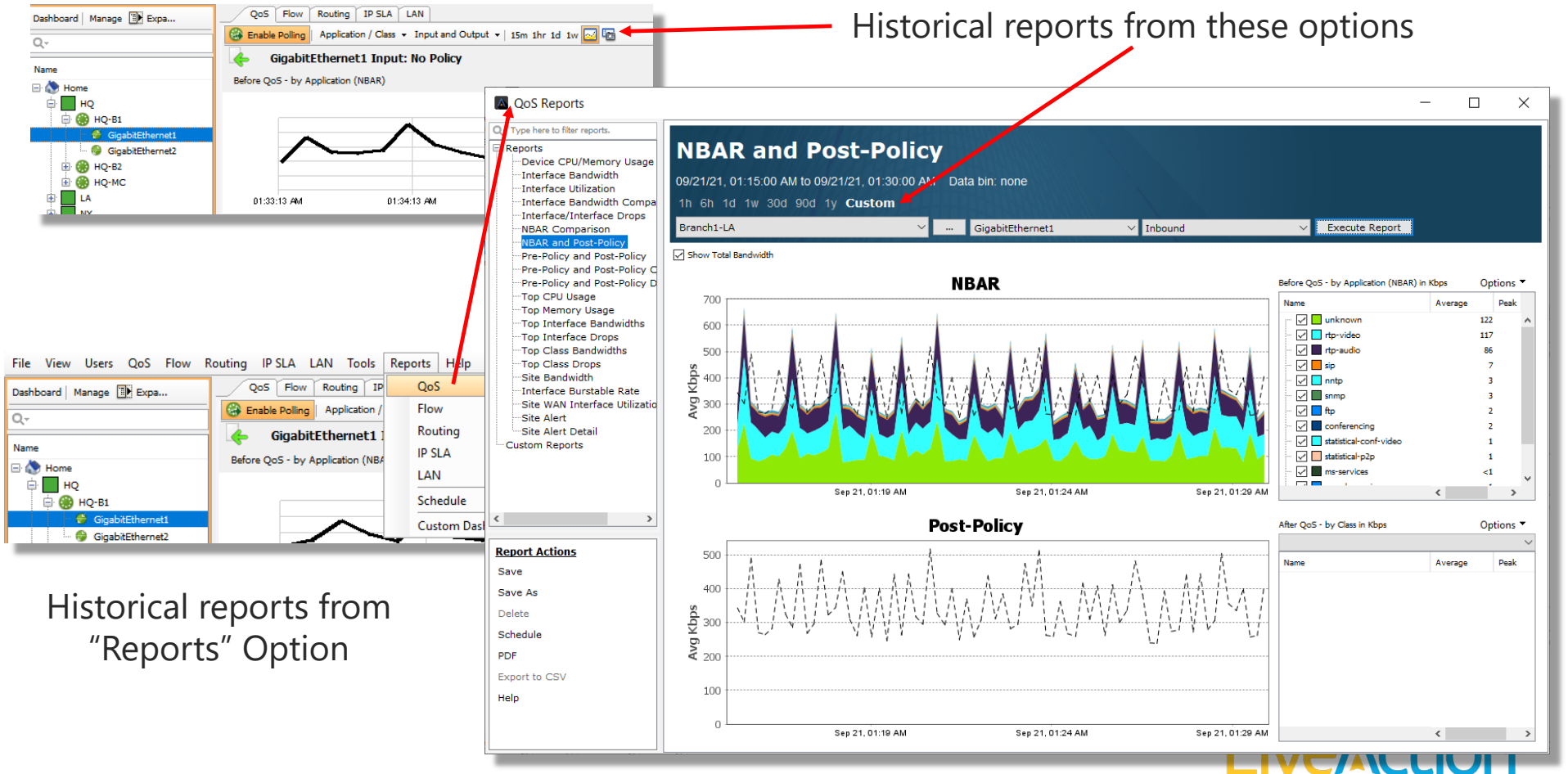
LiveNX QoS Baseline

- 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.

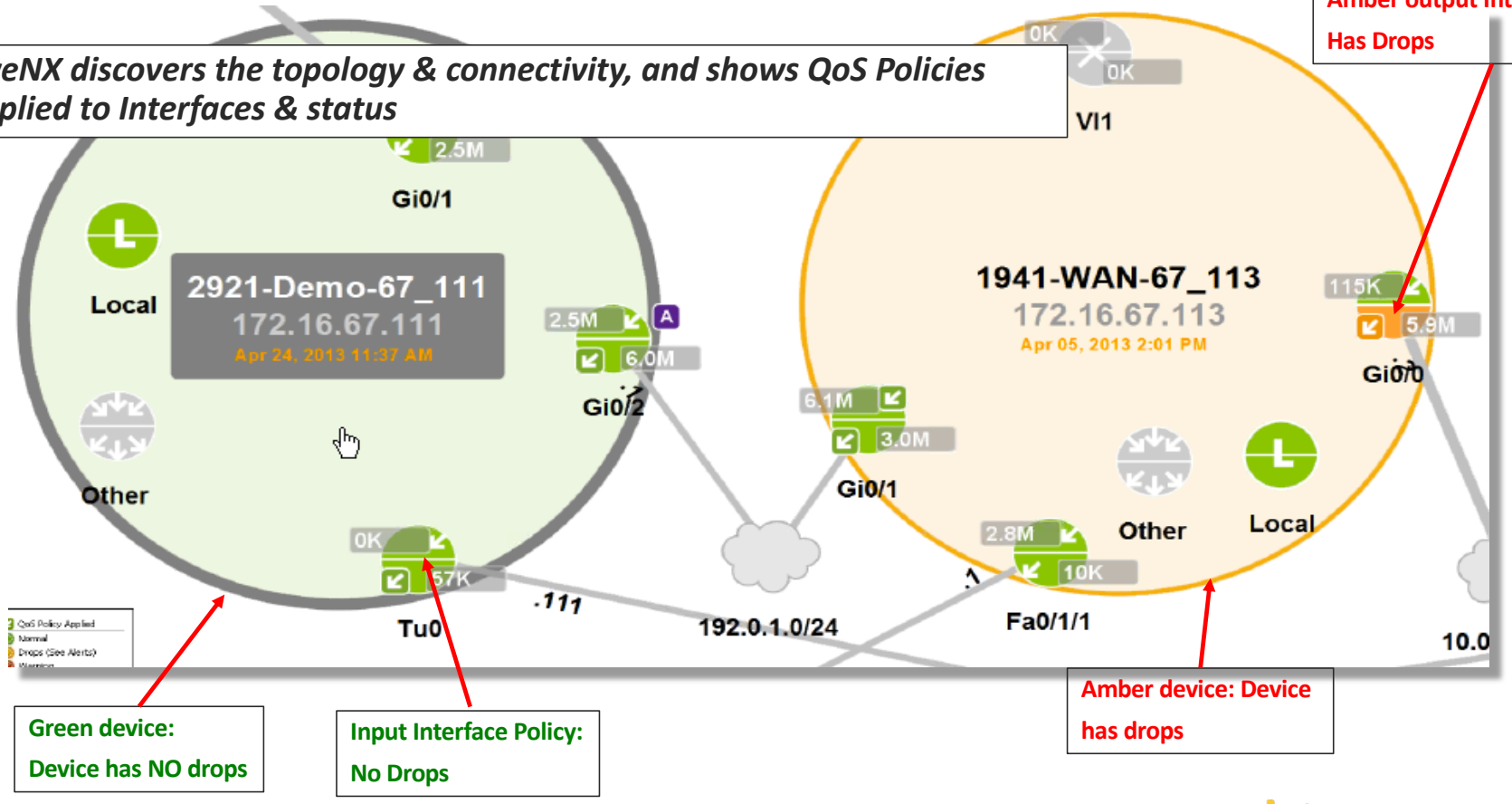
Historical QoS Class View/Reports



Historical reports from "Reports" Option

Discover QoS Policy Enforcement Points

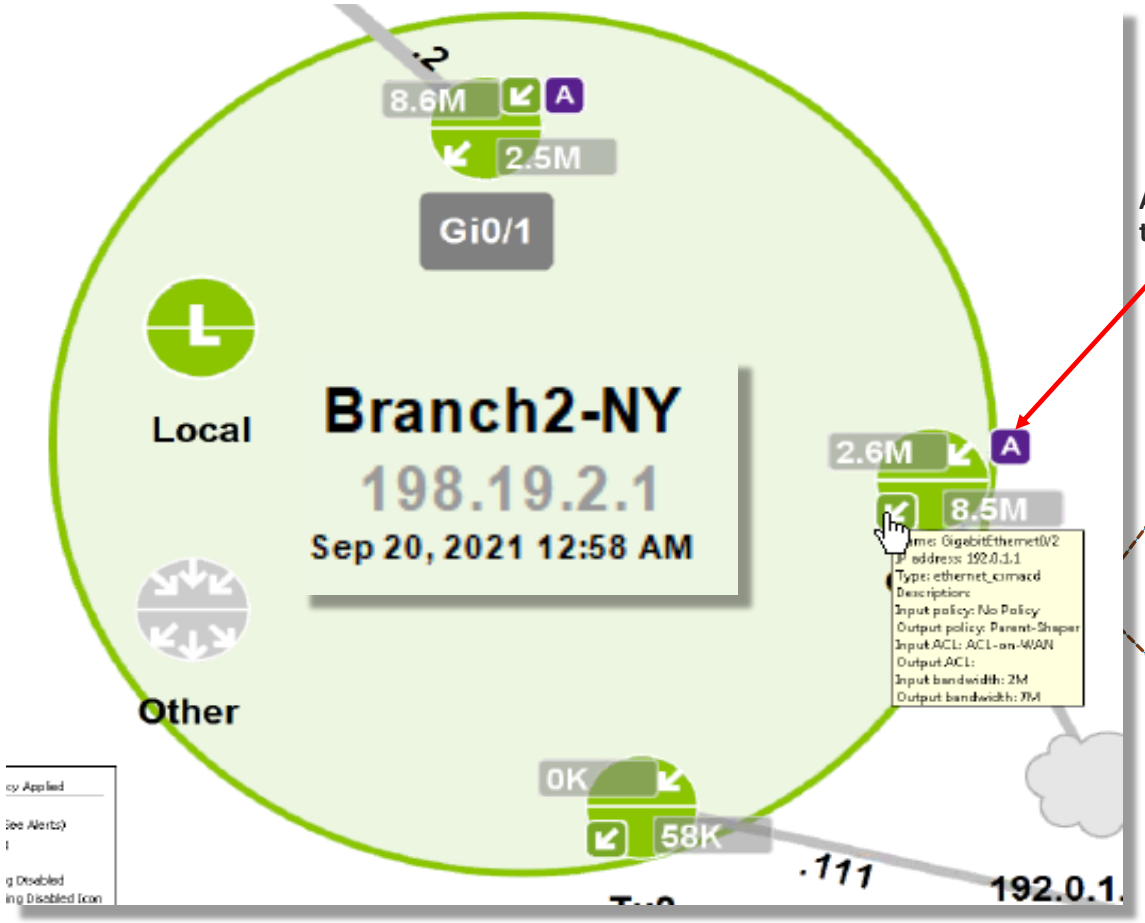
LiveNX discovers the topology & connectivity, and shows QoS Policies applied to Interfaces & status



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

QoS Policy Detail Display



ACL applied in this direction to this interface - could deny some traffic!

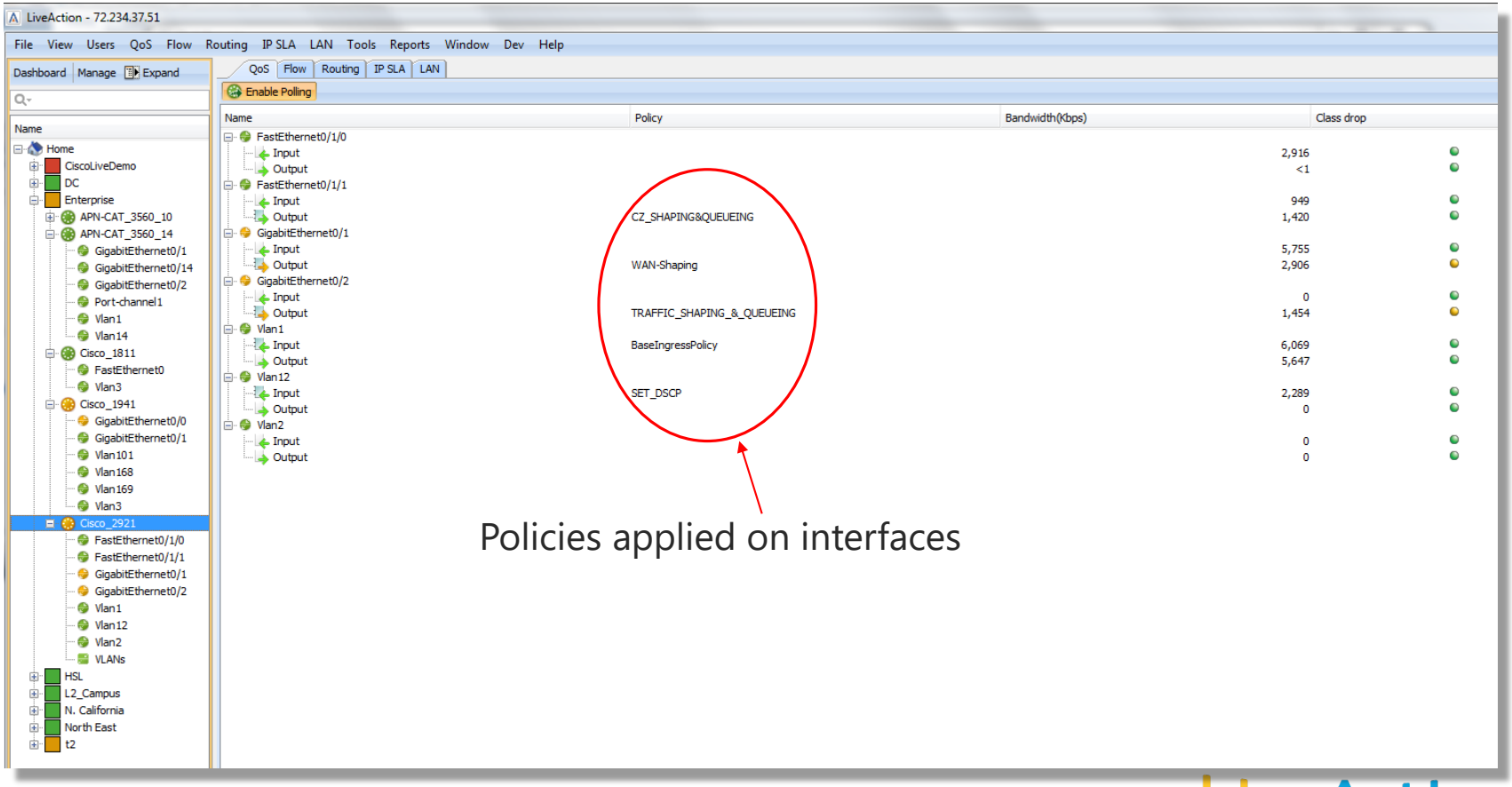
Tool Tip Contains -

- Interface Details
- Policy Name
- ACL Applied?
- Bandwidth

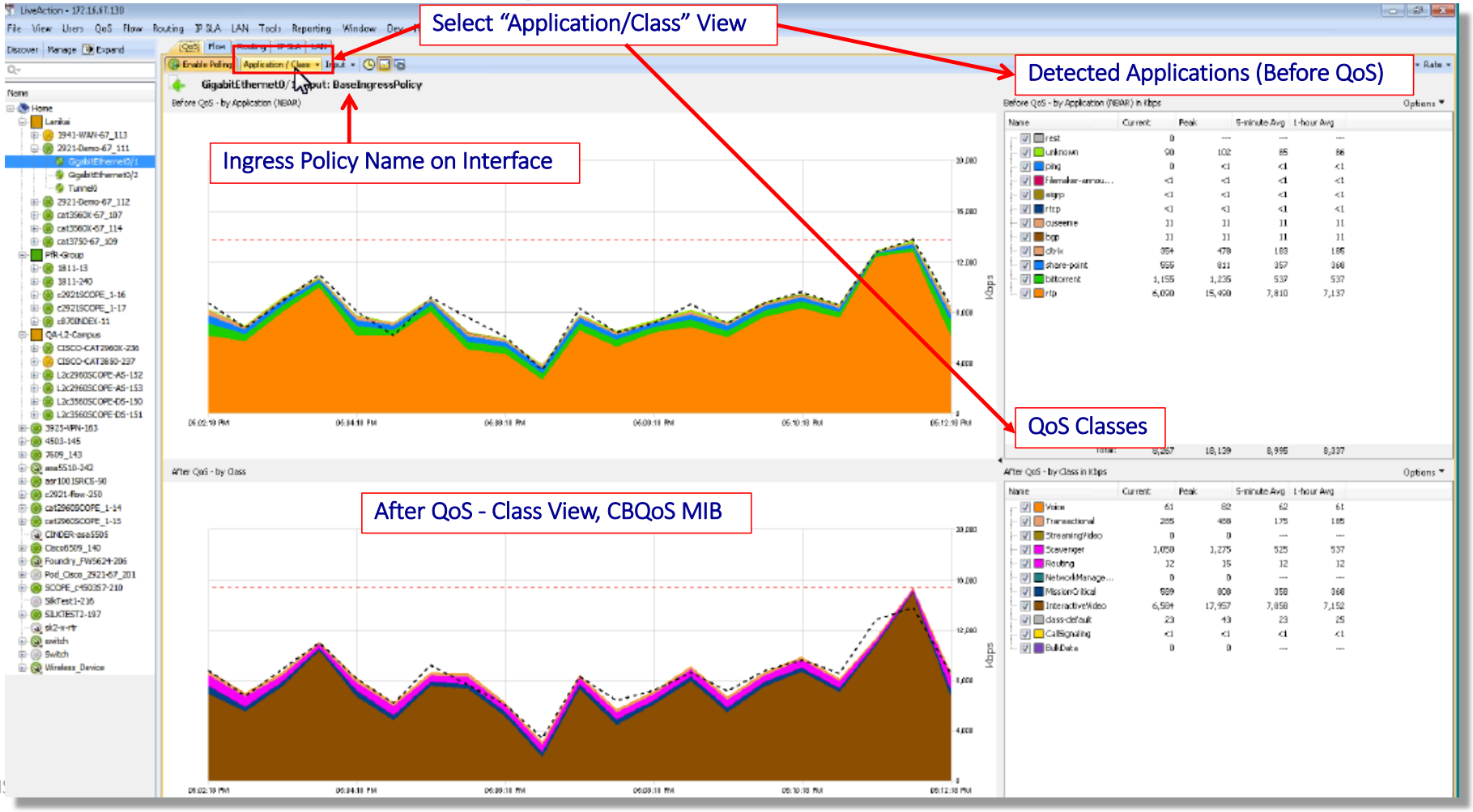
From the CBQoS MIB!

LiveAction®

QoS Device View



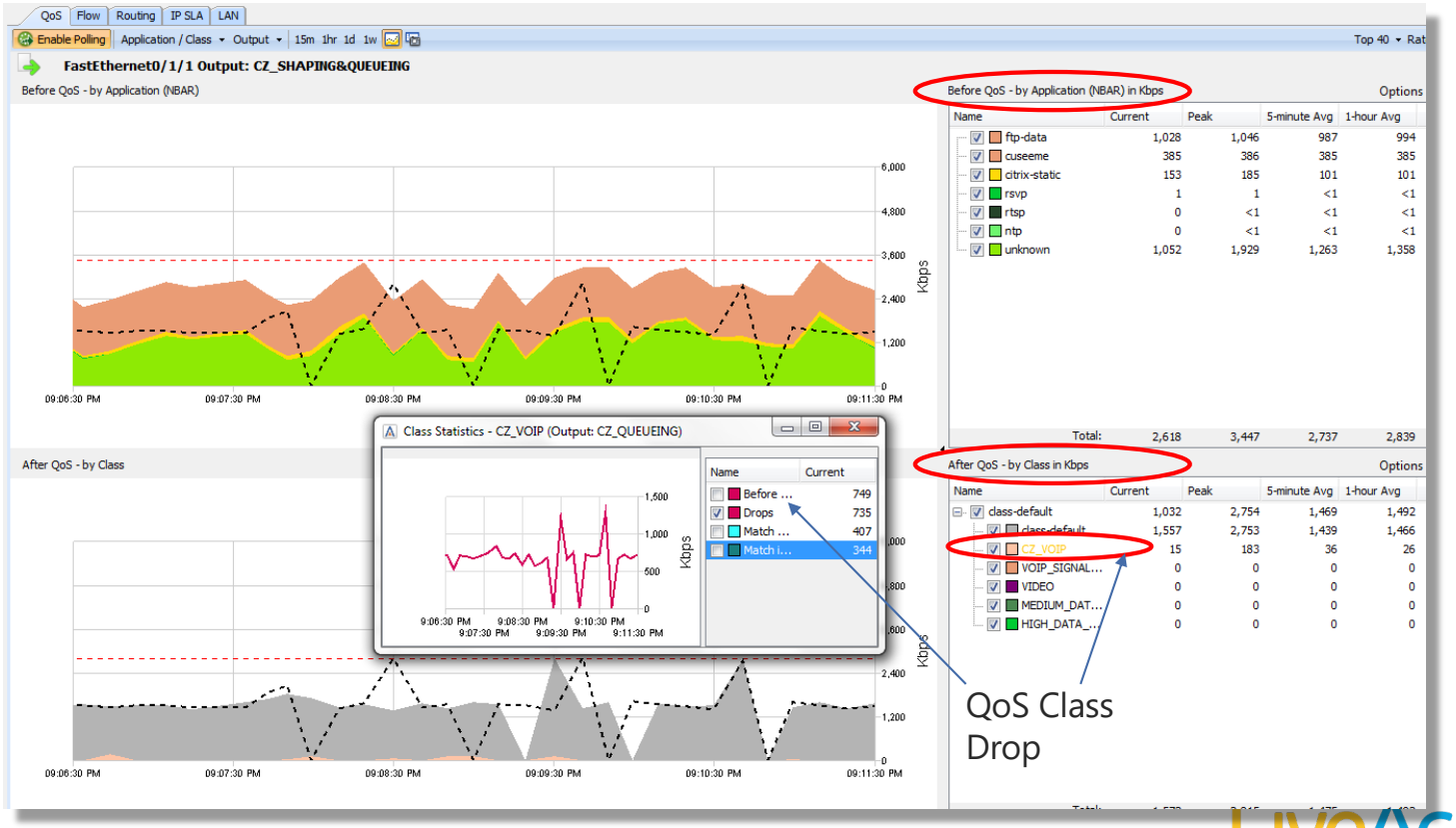
QoS Interface Policy Performance



QoS Troubleshooting

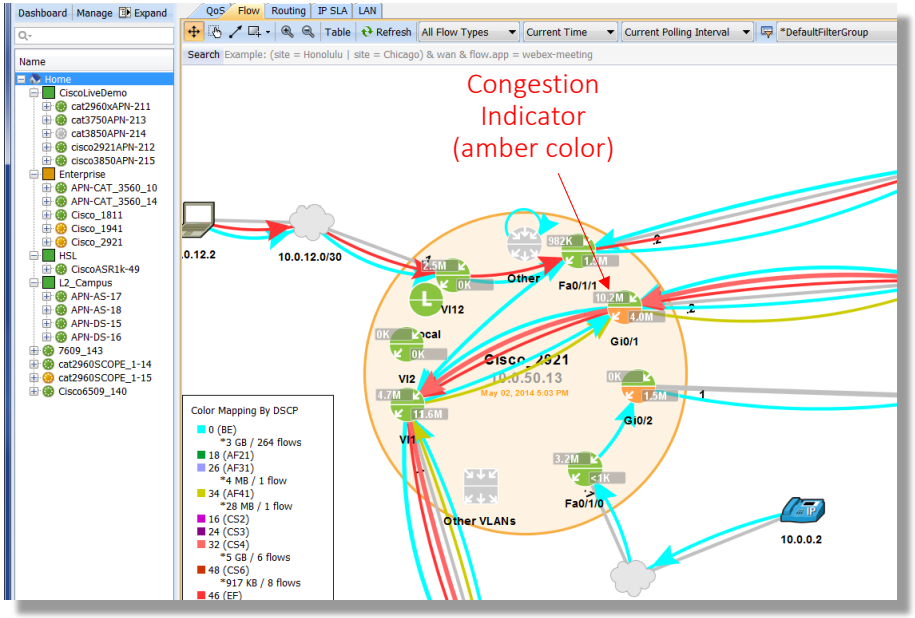
- Real-Time QoS Issues

Amber QoS class color shows class drops

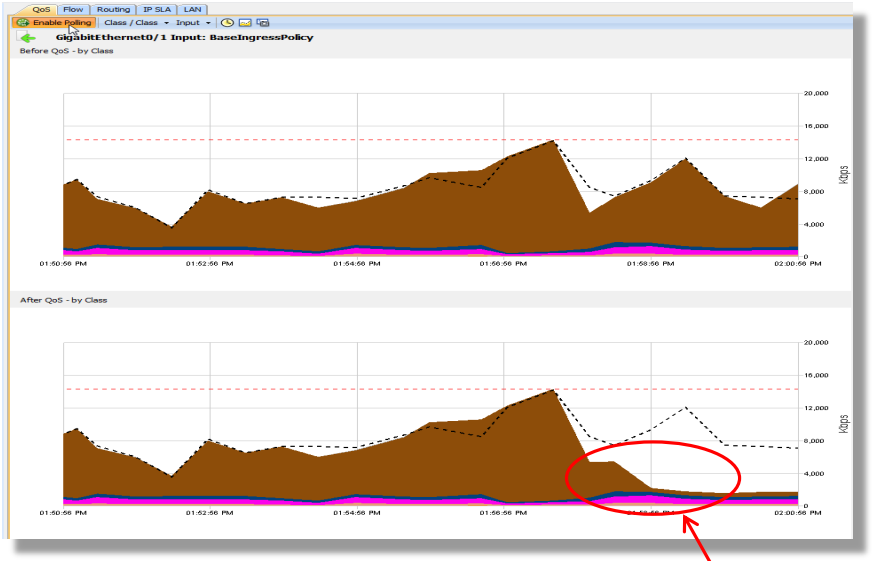


Track QoS Performance & Policy Validation

Visualize QoS Performance

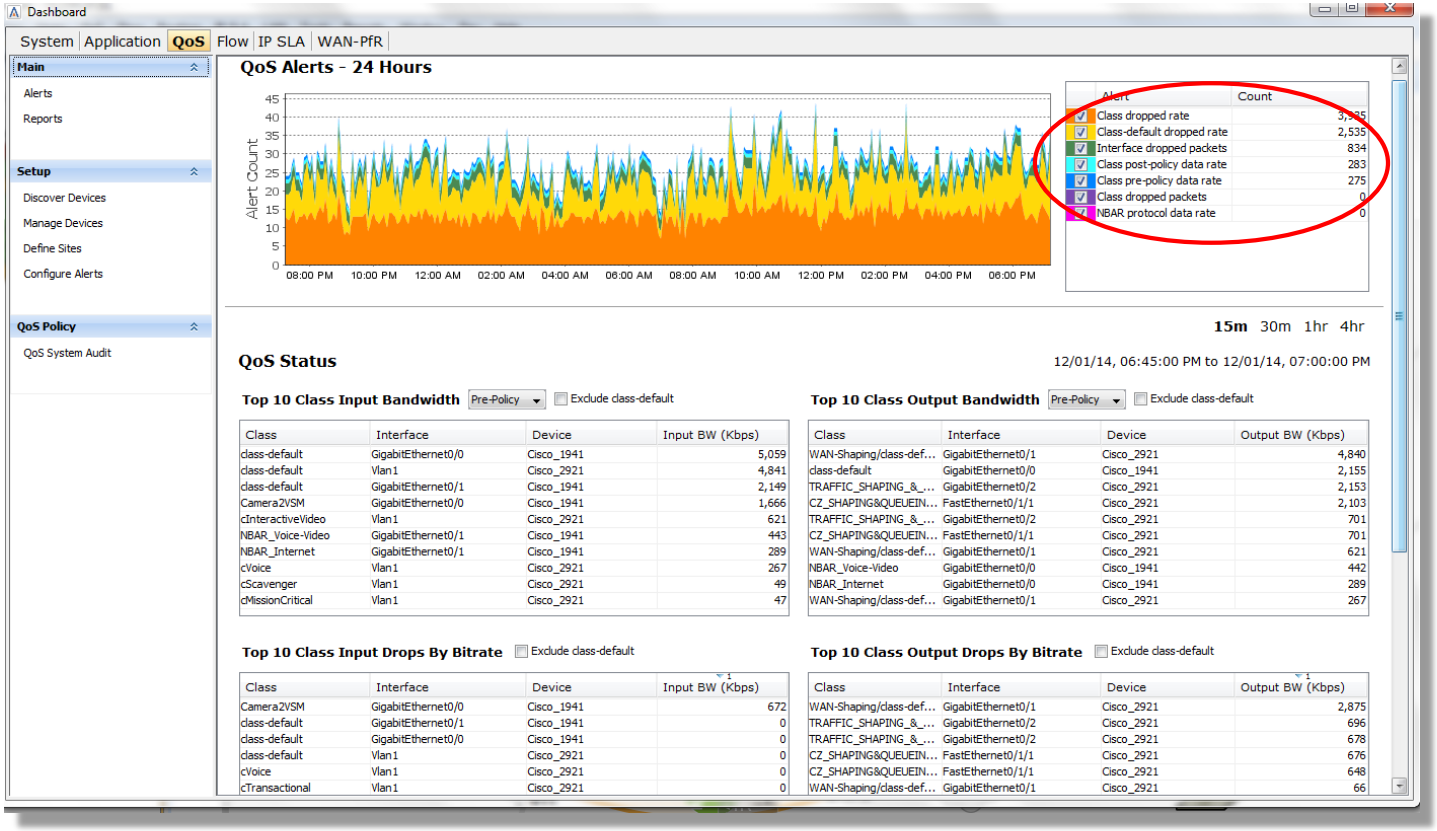


Show Impact of QoS Policy



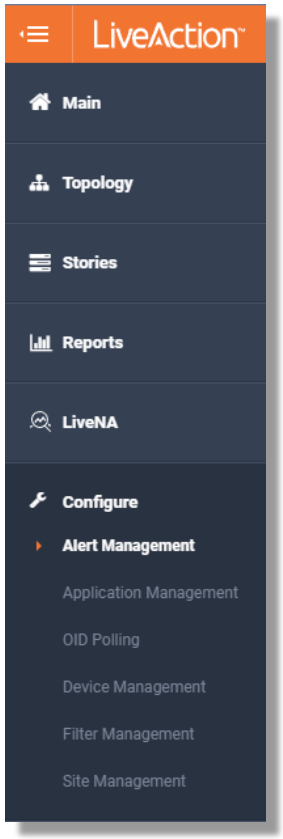
Policy applied to Police Interactive Video to 512 Kbps

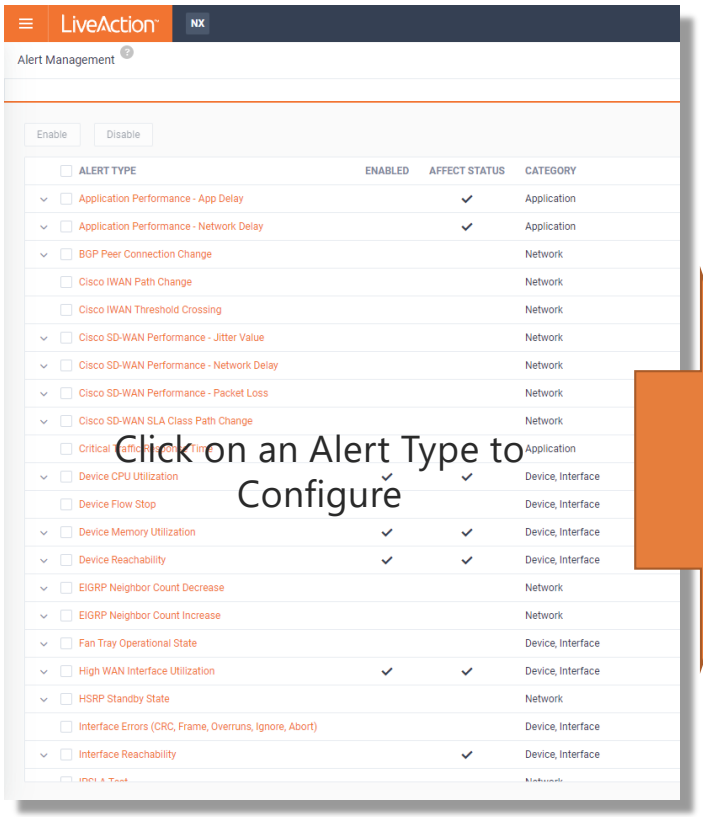
QoS Dashboard



Driven from MIB-II, NBAR, and CBQoS MIBs

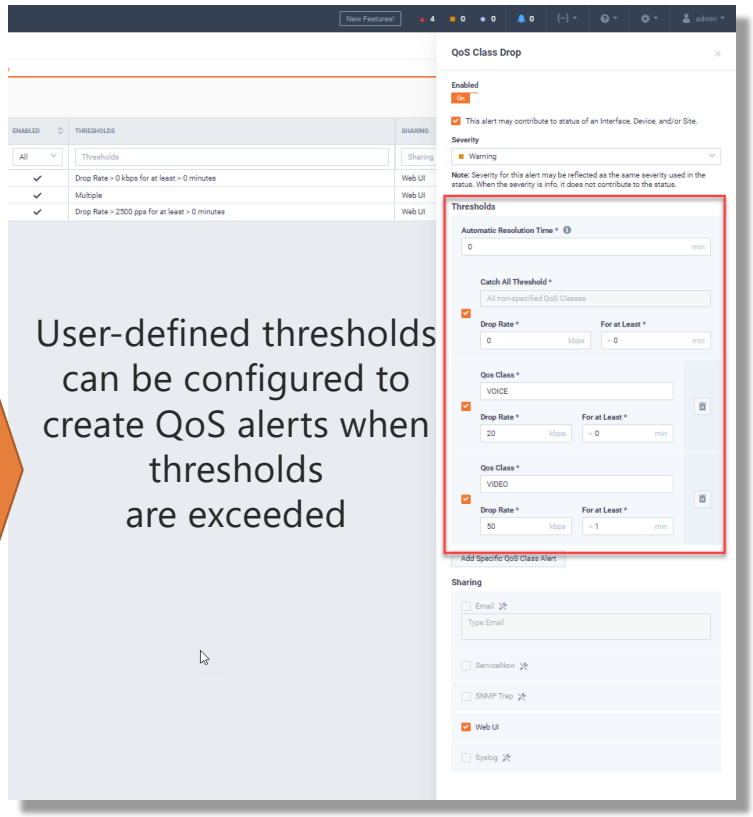
Troubleshooting - Real-Time QoS Alerts





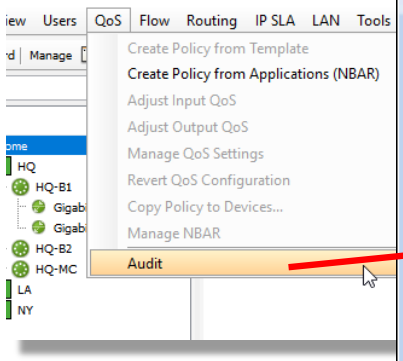
Click on an Alert Type to Configure

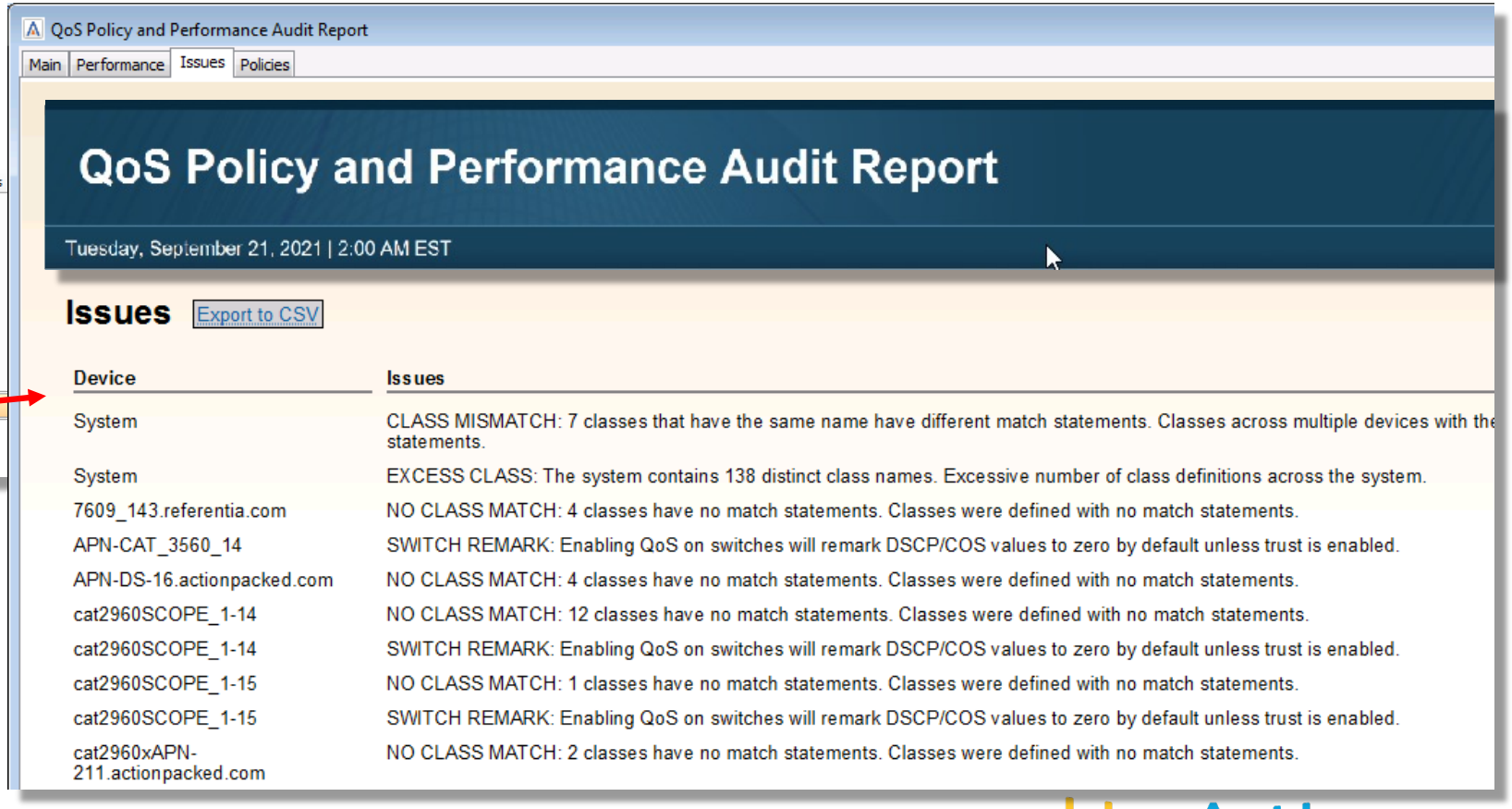
User-defined thresholds can be configured to create QoS alerts when thresholds are exceeded



Troubleshooting – Auditing QoS Policies

Single-click!





LiveNX QoS Configure

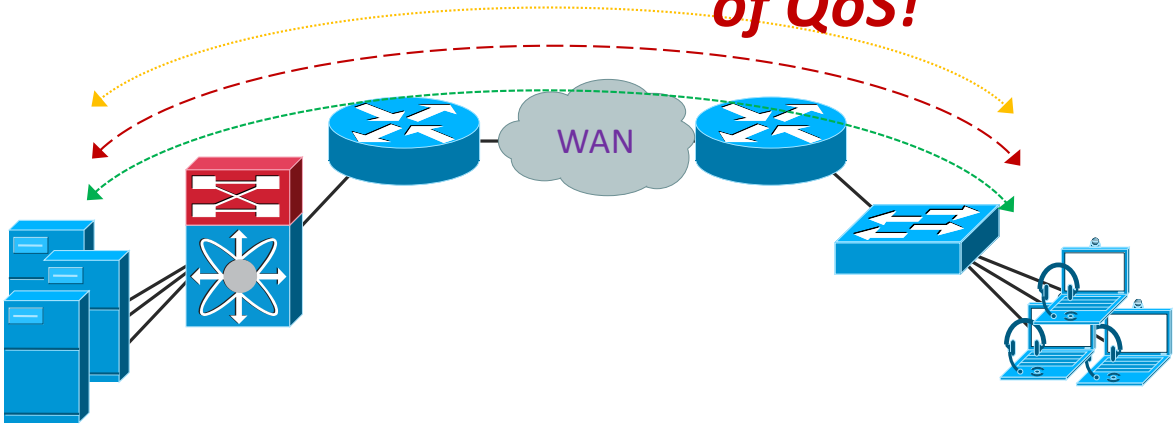
- Full MQC (Modular QoS Configuration) support including WRED, CBWFQ, Priority Queuing, Shaping
- Read pre-existing QoS policies already configured on devices
- Take snapshots of current QoS configuration for future use
- Apply or remove QoS configurations quickly and easily across multiple interfaces
- 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 any time*
- Built-in rules for QoS settings that highlight violations

Step 1: Classification & Marking

LiveAction™

Recognize Application Traffic

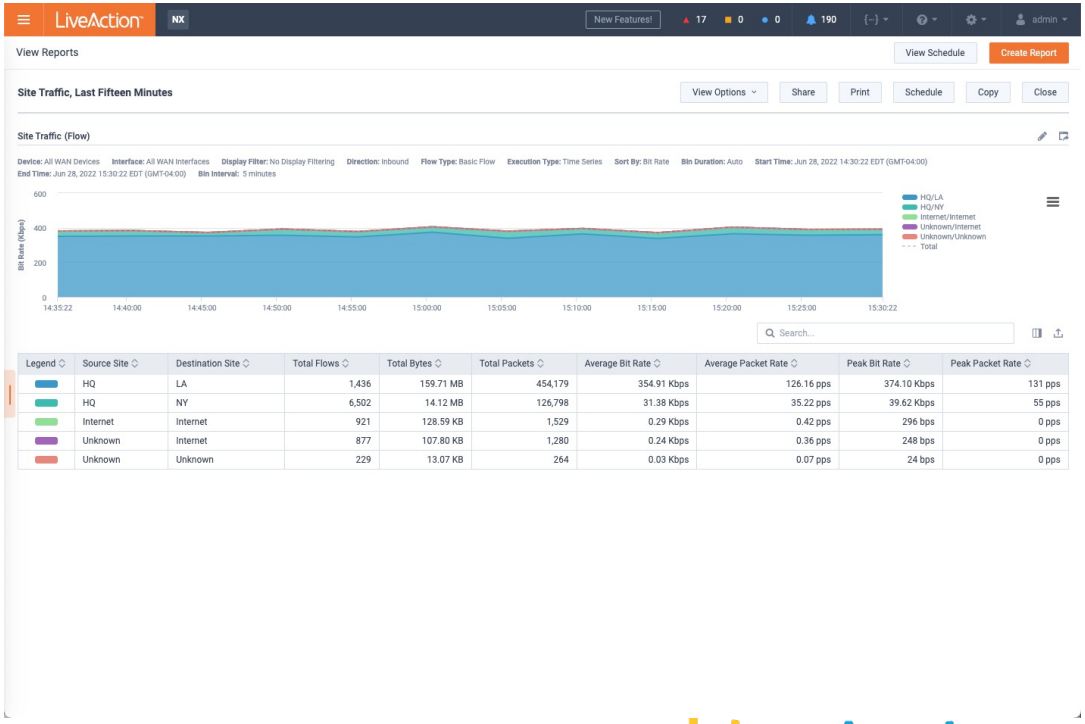
This may be the <u>hardest</u> & <u>most important</u> part of QoS!



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

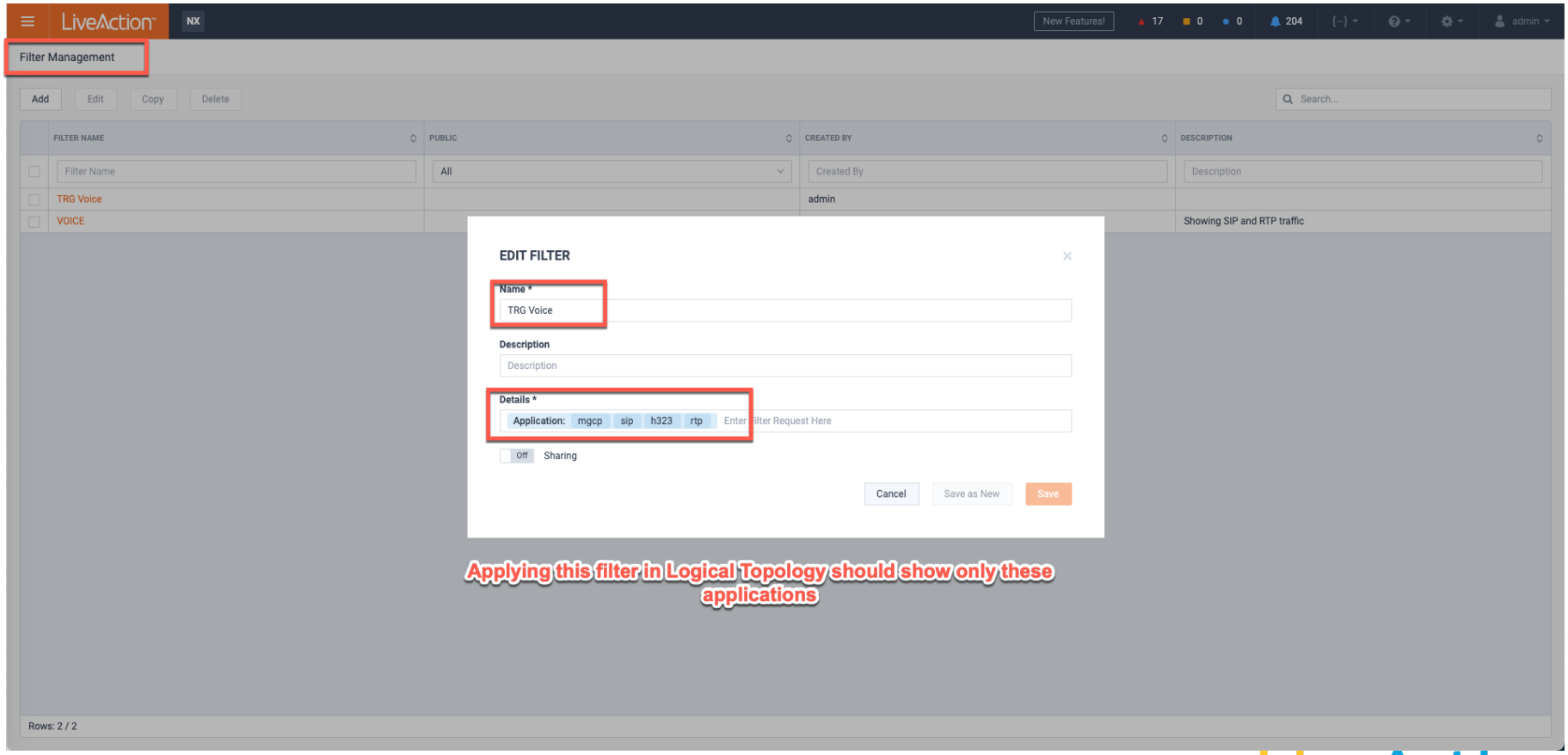
Classification: Day 0: Application Landscape

- 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

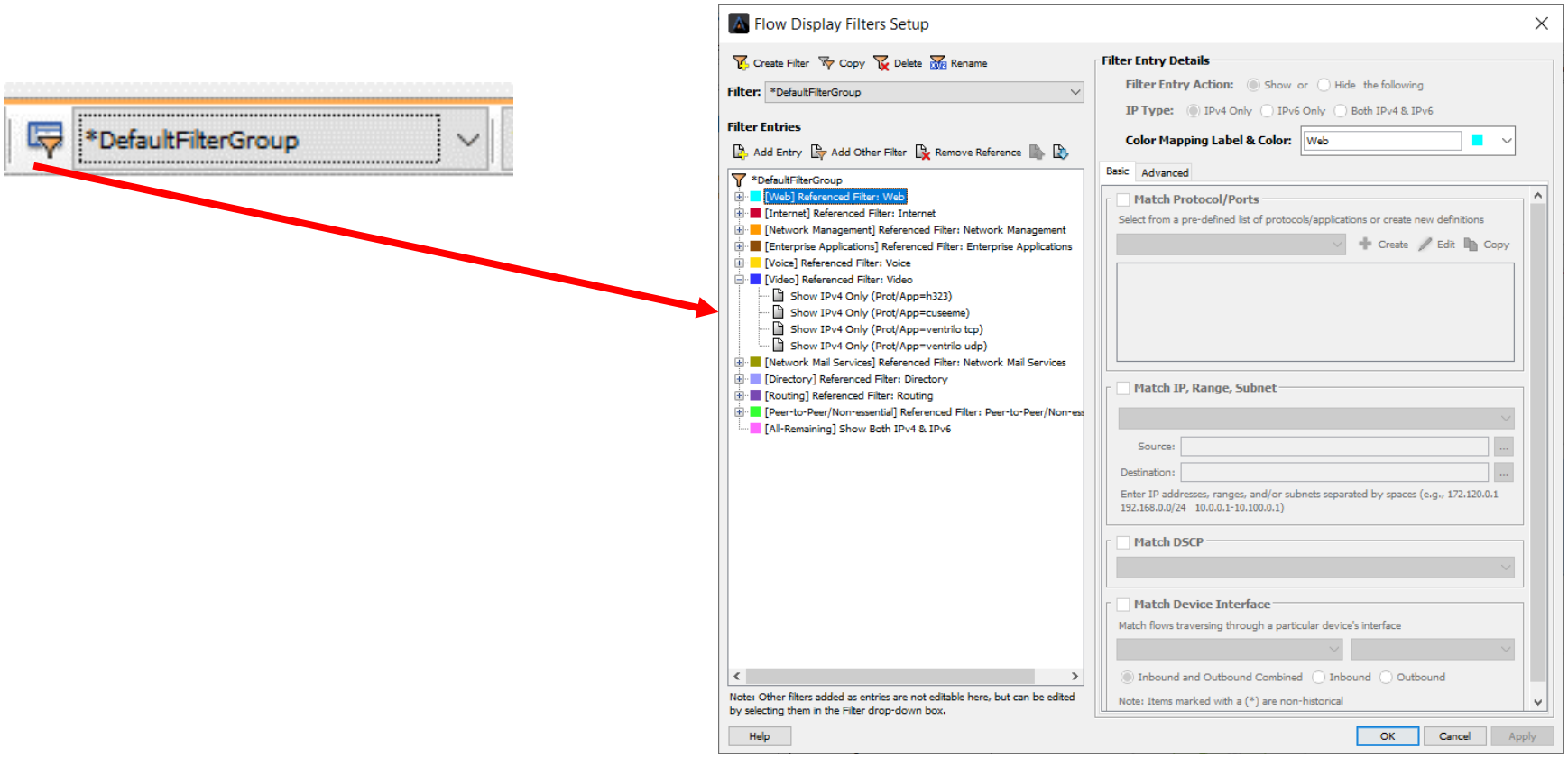


Legend	Source Site	Destination Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	HQ	LA	1,436	159.71 MB	454,179	354.91 Kbps	126.16 pps	374.10 Kbps	131 pps
	HQ	NY	6,502	14.12 MB	126,798	31.38 Kbps	35.22 pps	39.62 Kbps	55 pps
	Internet	Internet	921	128.59 KB	1,529	0.29 Kbps	0.42 pps	296 bps	0 pps
	Unknown	Internet	877	107.80 KB	1,280	0.24 Kbps	0.36 pps	248 bps	0 pps
	Unknown	Unknown	229	13.07 KB	264	0.03 Kbps	0.07 pps	24 bps	0 pps

Classification: Create Custom Filter (WebUI)

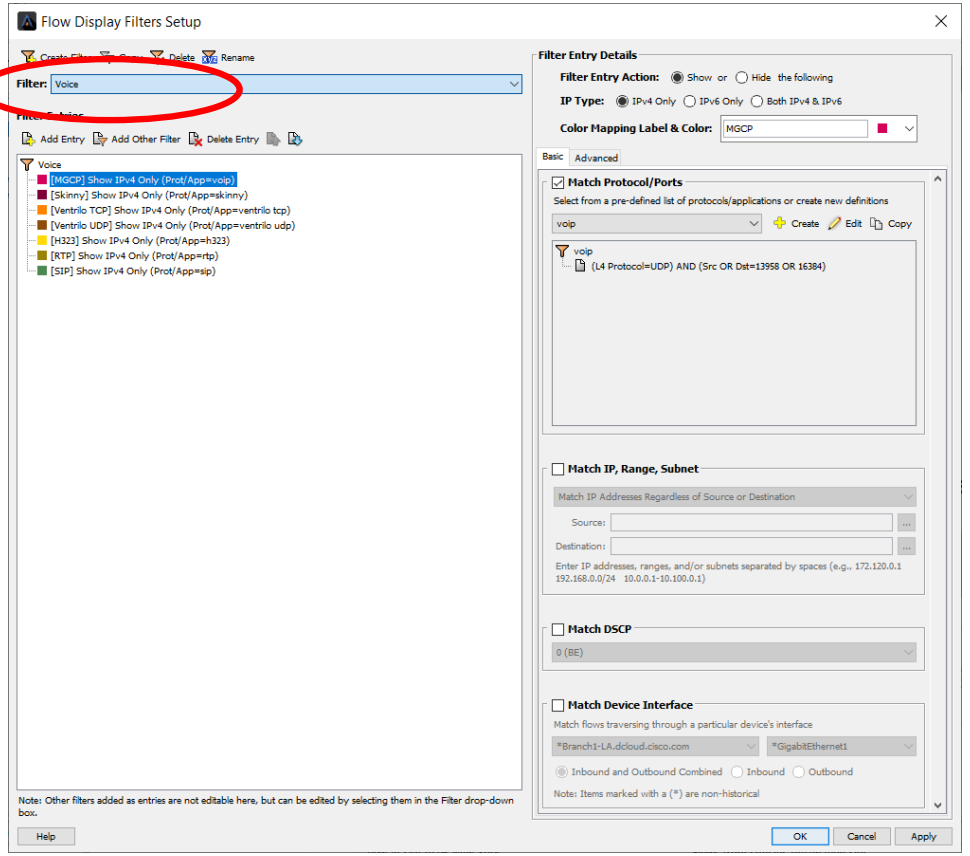


Classification: Create Custom Filter (Eng Console)



Classification: Copy Voice Filter

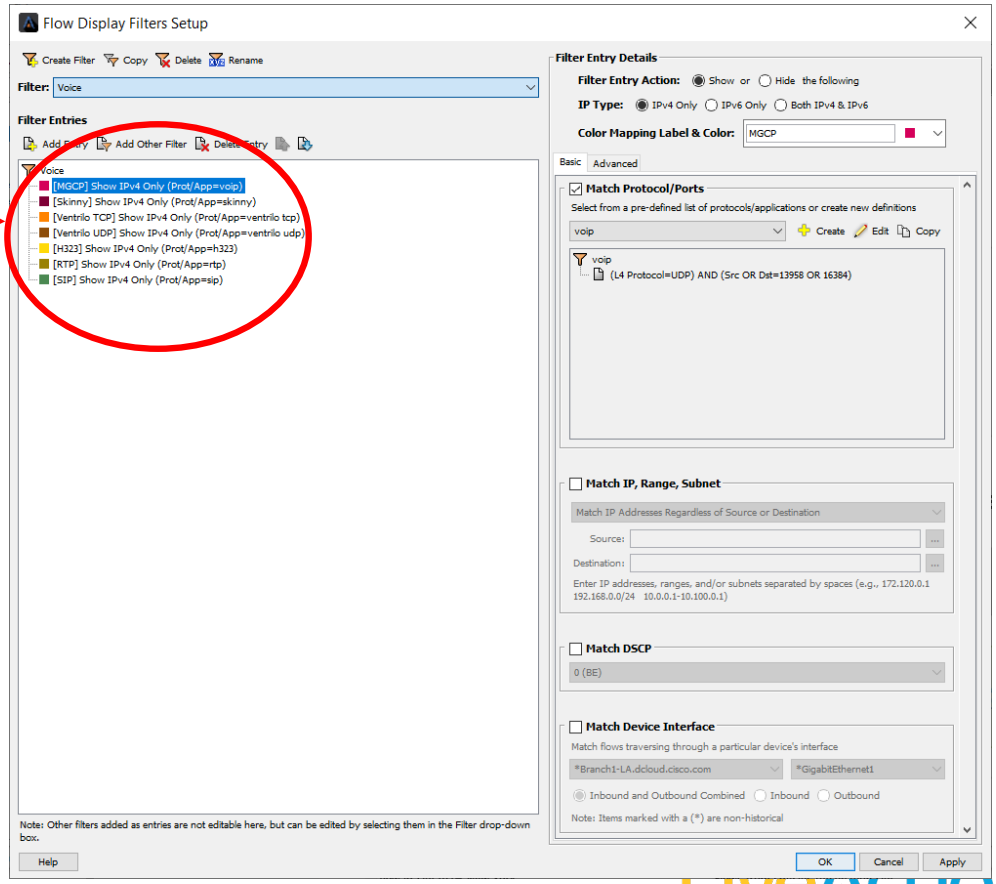
- Find pre-canned Voice filter
- Copy and rename it



Classification: Delete Unused Entries

Delete unused Entries

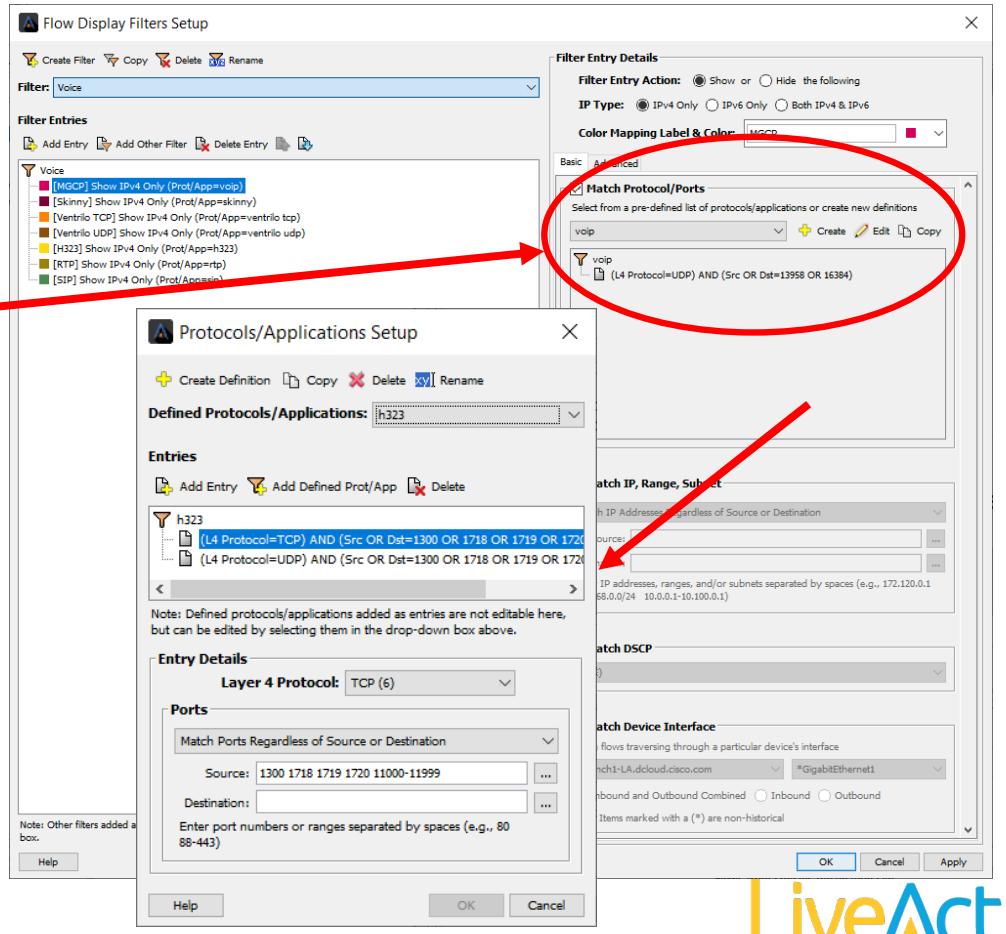
- VoIP
- Ventrilo TCP
- Ventrilo UDP



Classification: Add/Edit Entries

Edit Entries:
- h323
- RTP
- SIP

Add Entry:
- MGCP



Classification: Edit Entries

MGCP

TCP/UDP = Src or Dst = 2427 2727

TCP = Src or Dst = 2428

H323

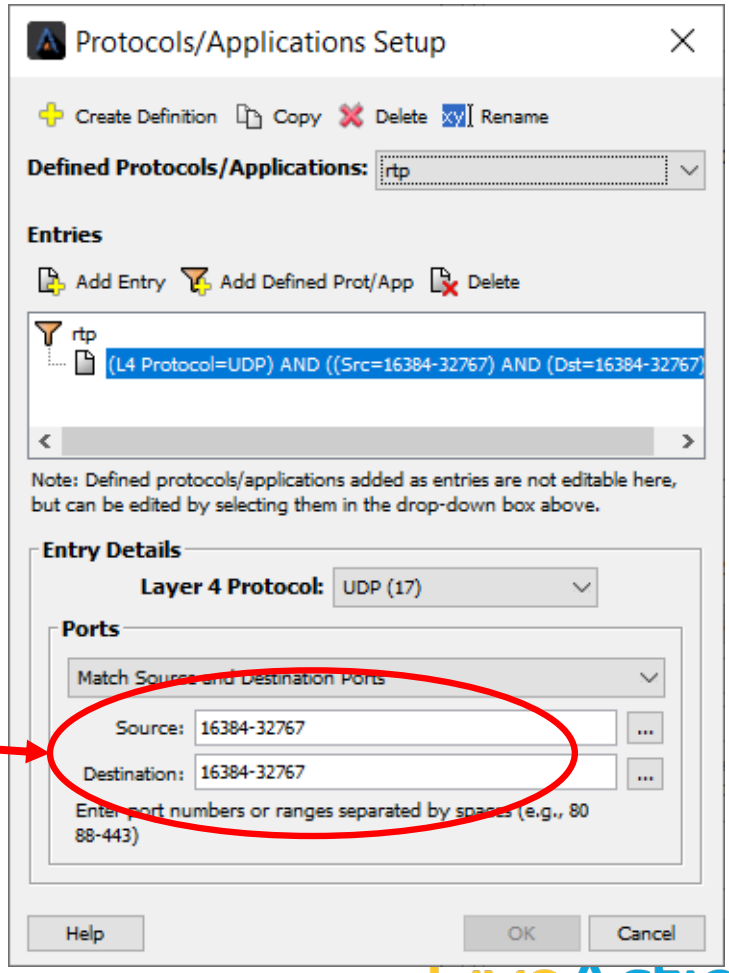
TCP/UDP = Src or Dst = 1718 1719 1720

SIP

TCP/UDP = Src or Dst = 5060 5061 5062

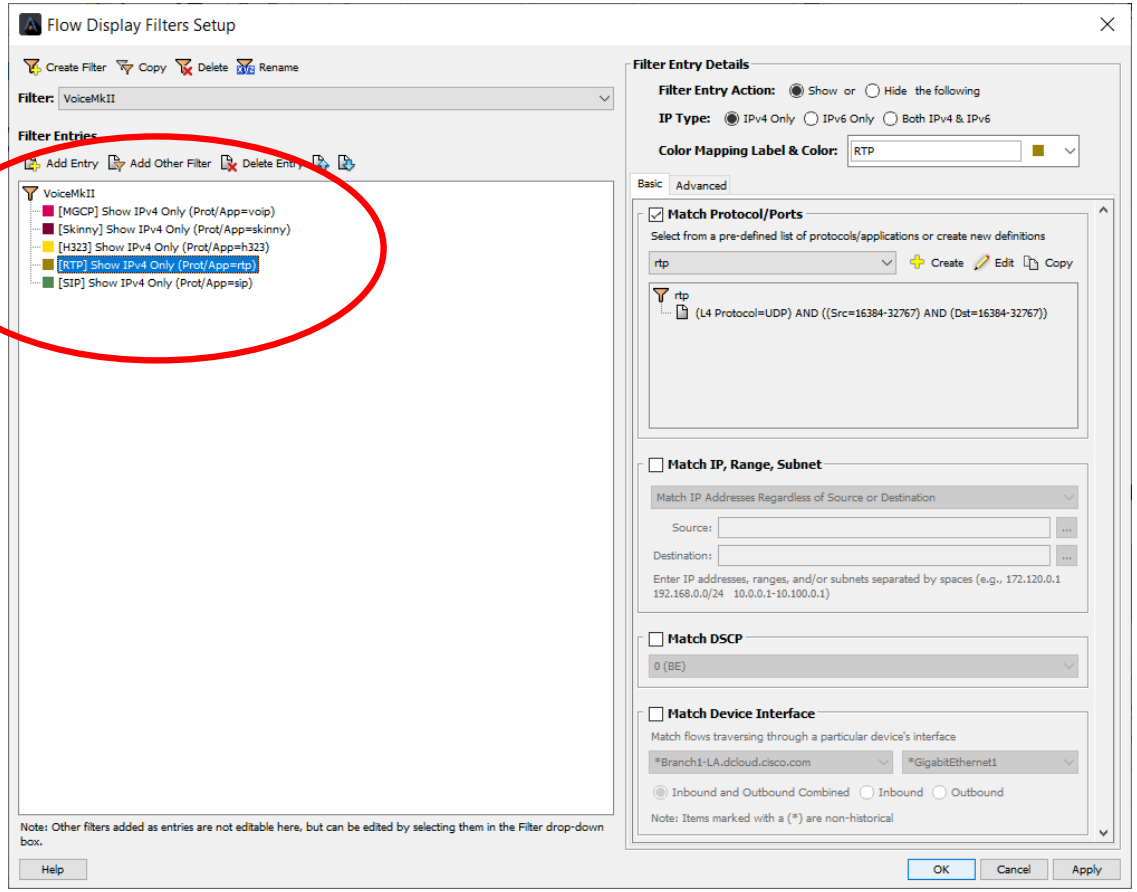
RTP

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



Classification: Voice Filter is ~95 accurate

- MGCP
- Skinny
- h323
- RTP
- SIP



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

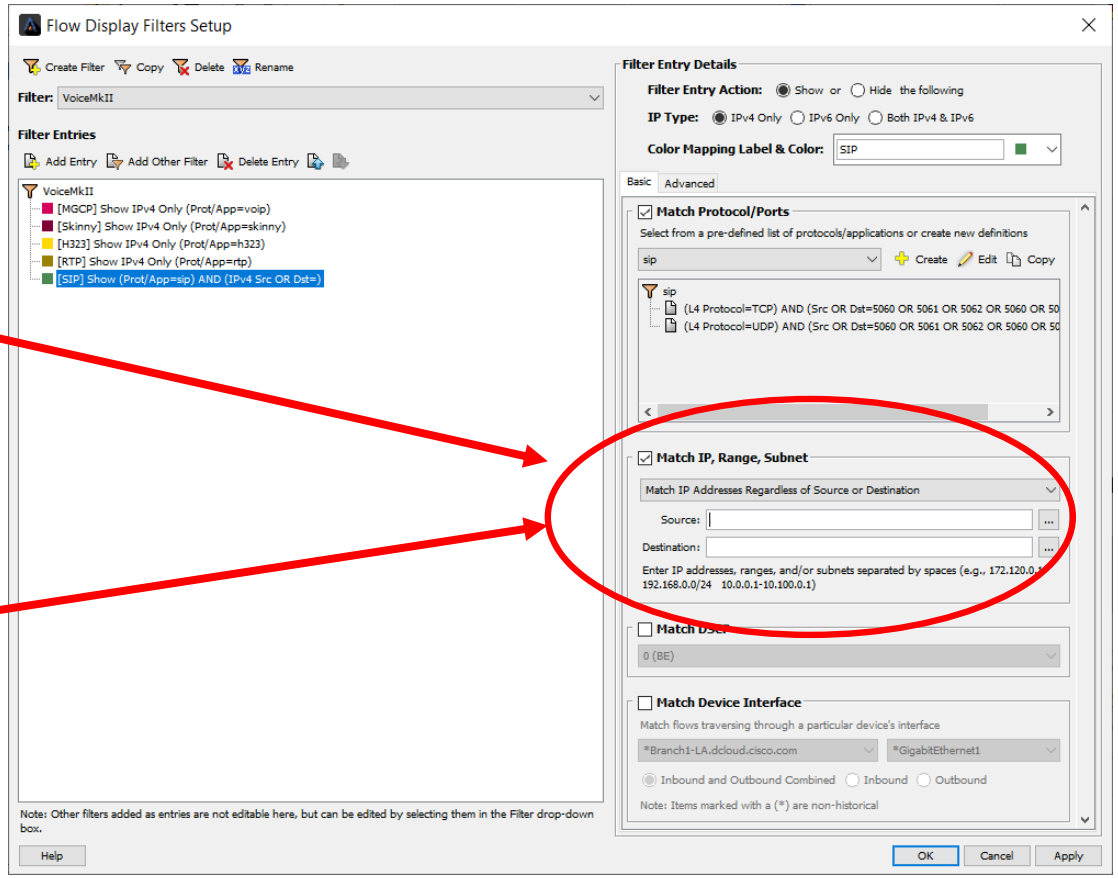
Classification: Voice Filter is ~99 accurate

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

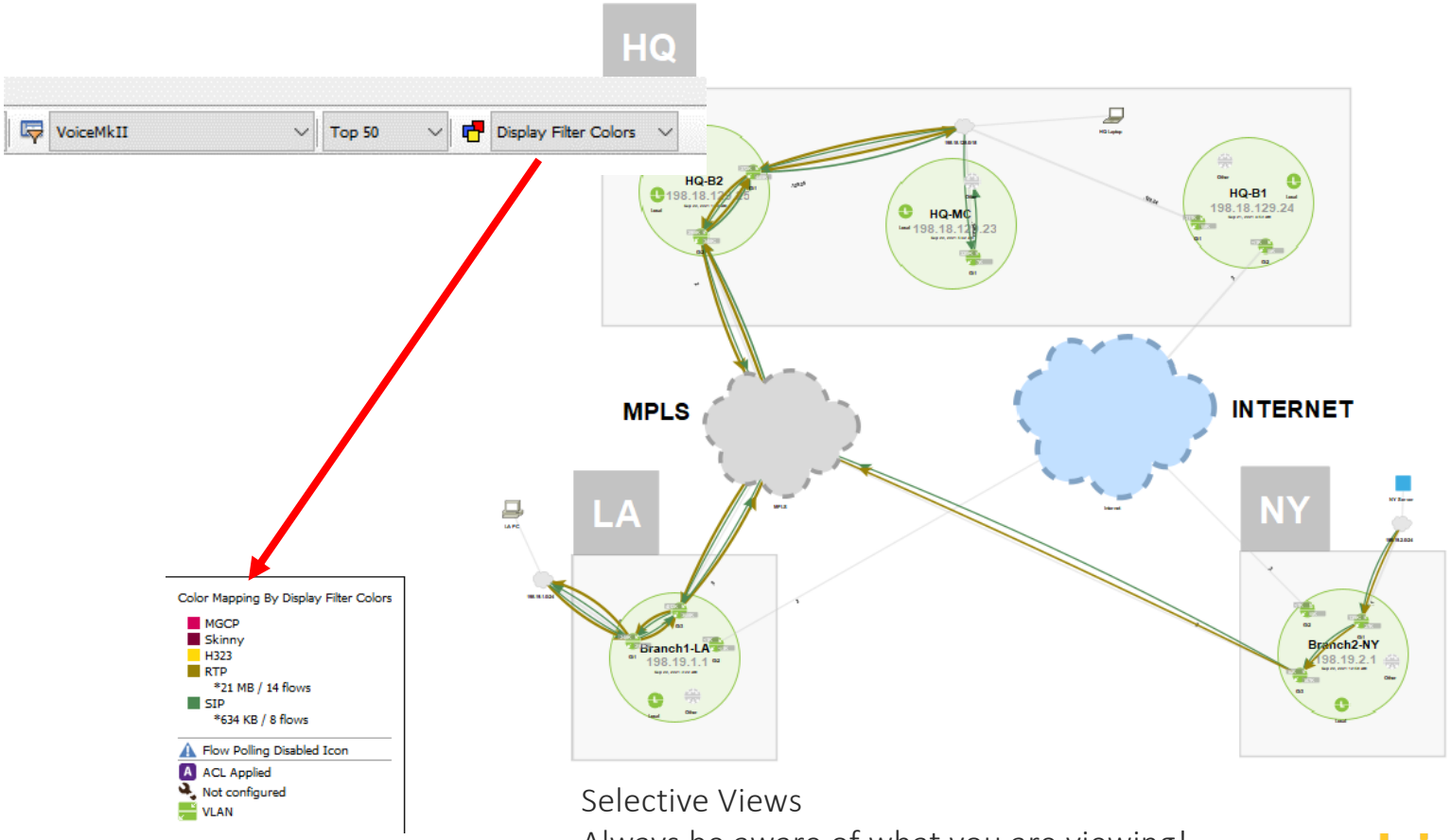
- MGCP
- Skinny
- h323
- SIP

If feasible, add voice subnets to:

- RTP



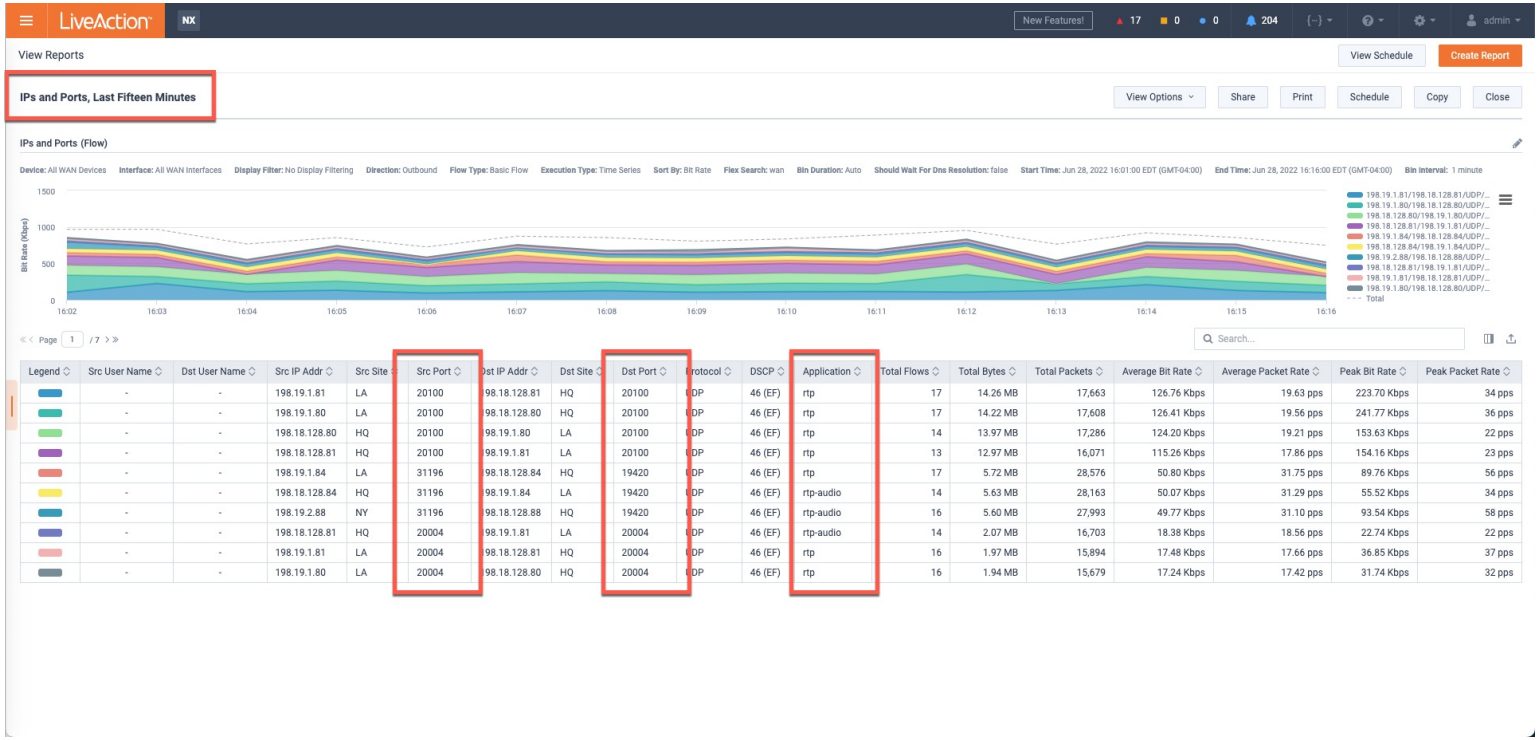
Classification: Display Filter Colors



Selective Views

Always be aware of what you are viewing!

Classification: IPs & Ports Report



Legend	Src User Name	Dst User Name	Src IP Addr	Src Site	Src Port	Dst IP Addr	Dst Site	Dst Port	Protocol	DSCP	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	-	-	198.19.1.81	LA	20100	98.18.128.81	HQ	20100	UDP	46 (EF)	rtp	17	14.26 MB	17,663	126.76 Kbps	19.63 pps	223.70 Kbps	34 pps
	-	-	198.19.1.80	LA	20100	98.18.128.80	HQ	20100	UDP	46 (EF)	rtp	17	14.22 MB	17,608	126.41 Kbps	19.56 pps	241.77 Kbps	36 pps
	-	-	198.18.128.80	HQ	20100	98.19.1.80	LA	20100	UDP	46 (EF)	rtp	14	13.97 MB	17,286	124.20 Kbps	19.21 pps	153.63 Kbps	22 pps
	-	-	198.18.128.81	HQ	20100	98.19.1.81	LA	20100	UDP	46 (EF)	rtp	13	12.97 MB	16,071	115.26 Kbps	17.86 pps	154.16 Kbps	23 pps
	-	-	198.19.1.84	LA	31196	98.18.128.84	HQ	19420	UDP	46 (EF)	rtp	17	5.72 MB	28,576	50.80 Kbps	31.75 pps	89.76 Kbps	56 pps
	-	-	198.18.128.84	HQ	31196	98.19.1.84	LA	19420	UDP	46 (EF)	rtp-audio	14	5.63 MB	28,163	50.07 Kbps	31.29 pps	55.52 Kbps	34 pps
	-	-	198.19.2.88	NY	31196	98.18.128.88	HQ	19420	UDP	46 (EF)	rtp-audio	16	5.60 MB	27,993	49.77 Kbps	31.10 pps	93.54 Kbps	58 pps
	-	-	198.18.128.81	HQ	20004	98.19.1.81	LA	20004	UDP	46 (EF)	rtp-audio	14	2.07 MB	16,703	18.38 Kbps	18.56 pps	22.74 Kbps	22 pps
	-	-	198.19.1.81	LA	20004	98.18.128.81	HQ	20004	UDP	46 (EF)	rtp	16	1.97 MB	15,894	17.48 Kbps	17.66 pps	36.85 Kbps	37 pps
	-	-	198.19.1.80	LA	20004	98.18.128.80	HQ	20004	UDP	46 (EF)	rtp	16	1.94 MB	15,679	17.24 Kbps	17.42 pps	31.74 Kbps	32 pps

Use this report to validate Filter's Accuracy.

NBAR2 is your Friend!

If NBAR doesn't fulfil your needs use **Custom Applications**

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)

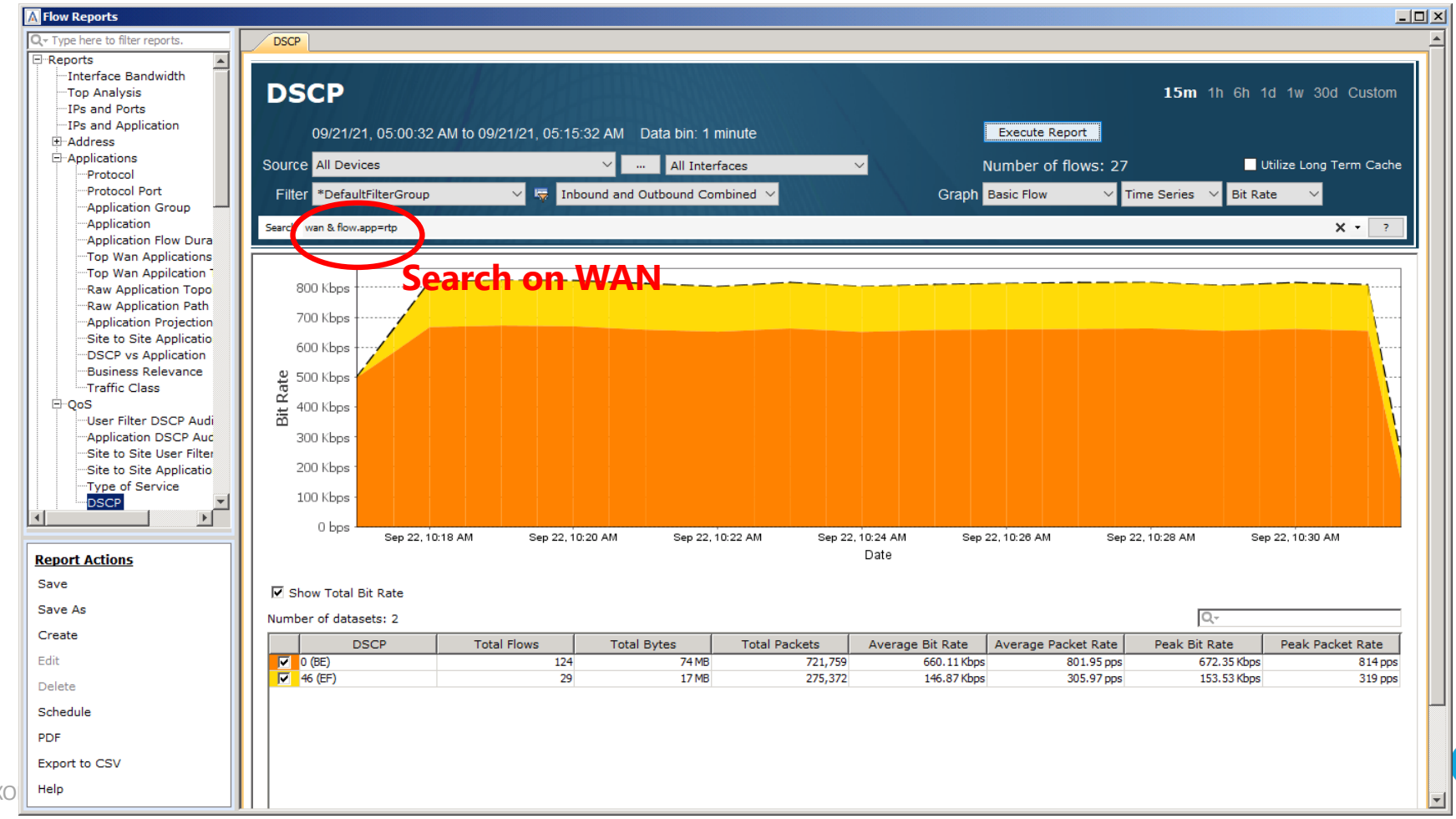
These are just Cisco's recommendations – all values are arbitrary!
You can use any of the 64 values, but you will see these most often.

Marking: DSCP Visualization

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

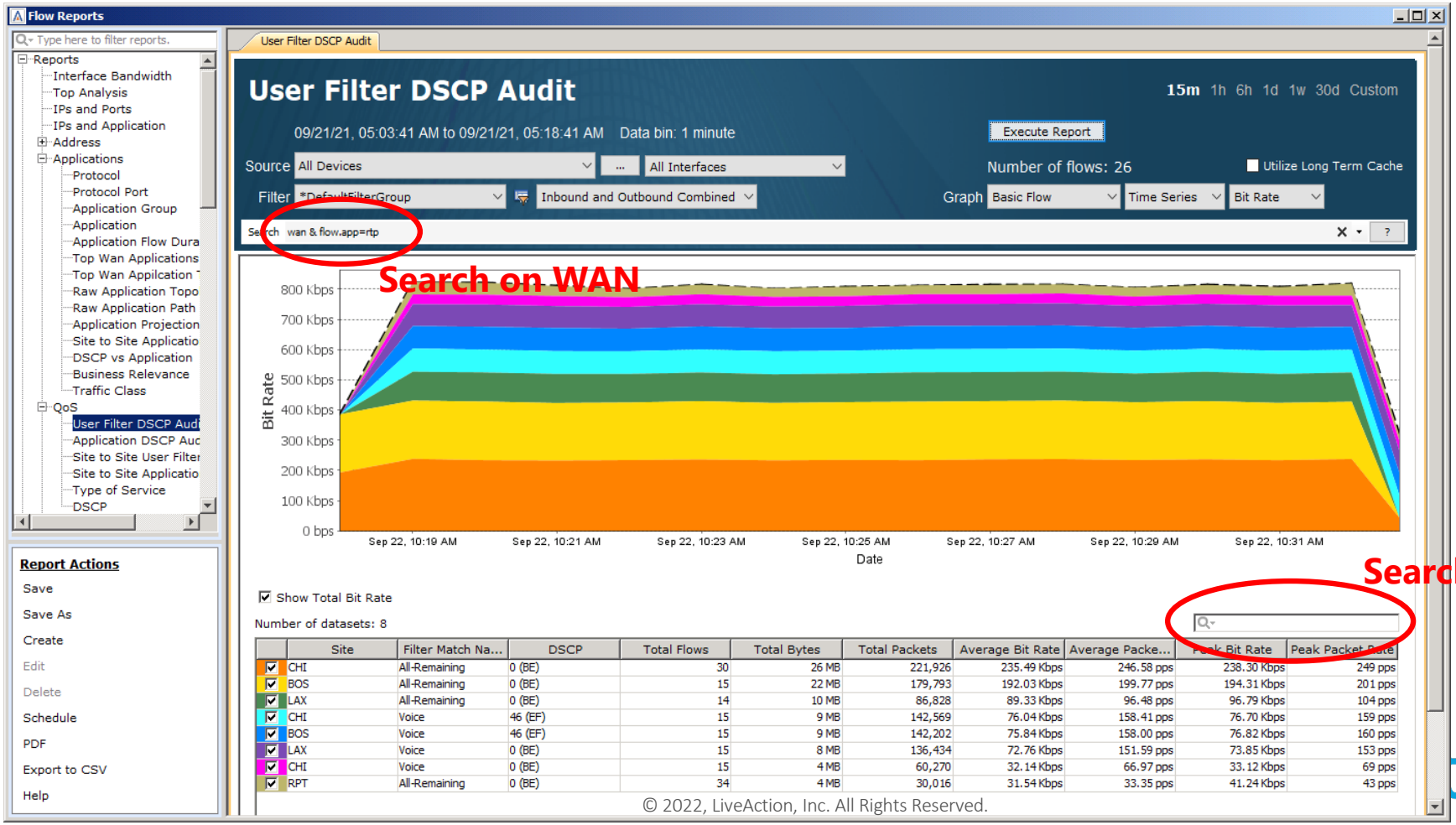
Marking: DSCP Report

Is there any BE VoIP traffic?



Marking: User Filter DSCP Audit

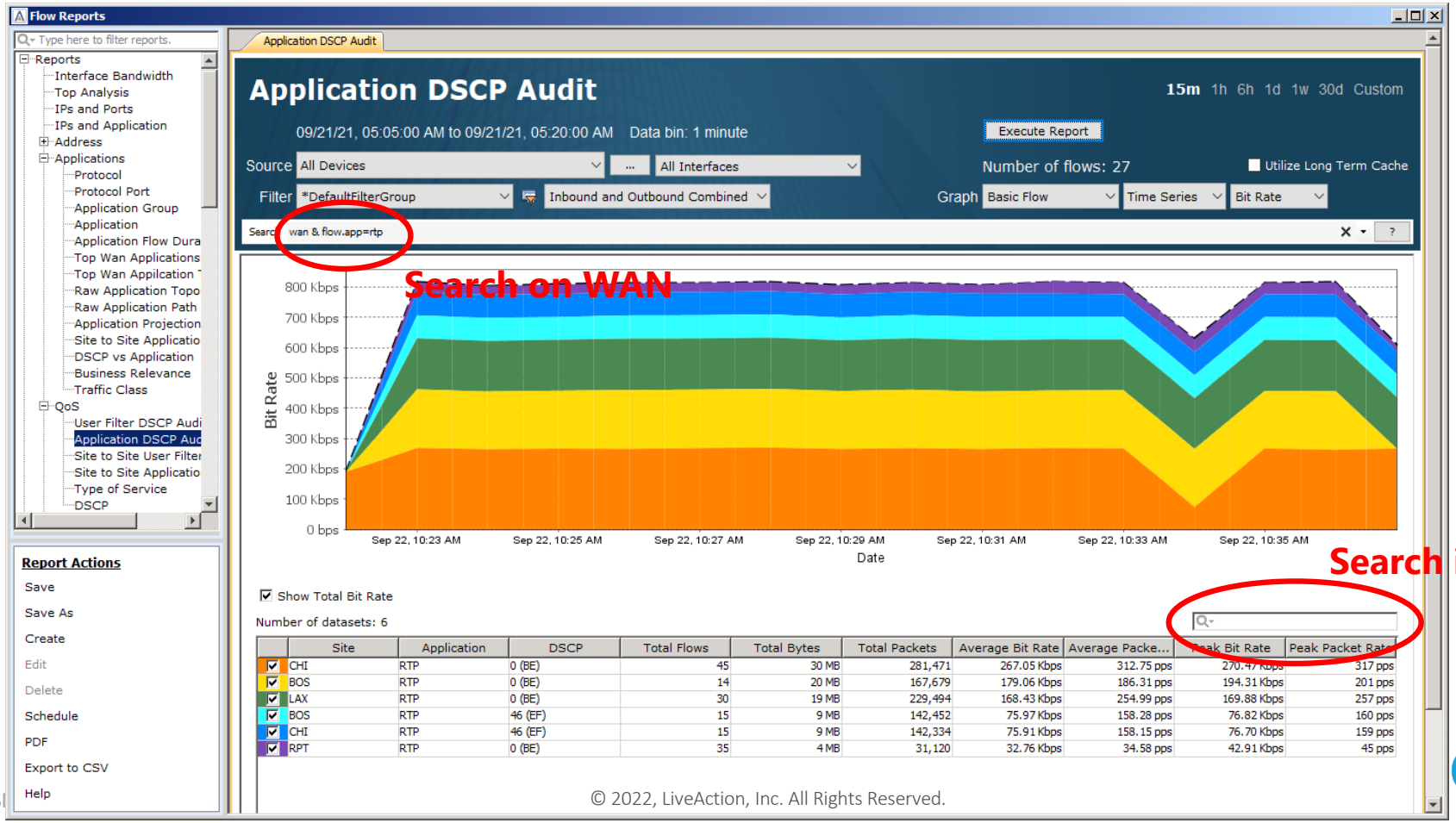
Where is the BE VoIP traffic?



Site	Filter Match Na...	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packe...	Peak Bit Rate	Peak Packet Rate
CHI	All-Remaining	0 (BE)	30	26 MB	221,926	235.49 Kbps	246.58 pps	238.30 Kbps	249 pps
BOS	All-Remaining	0 (BE)	15	22 MB	179,793	192.03 Kbps	199.77 pps	194.31 Kbps	201 pps
LAX	All-Remaining	0 (BE)	14	10 MB	86,828	89.33 Kbps	96.48 pps	96.79 Kbps	104 pps
CHI	Voice	46 (EF)	15	9 MB	142,569	76.04 Kbps	158.41 pps	76.70 Kbps	159 pps
BOS	Voice	46 (EF)	15	9 MB	142,202	75.84 Kbps	158.00 pps	76.82 Kbps	160 pps
LAX	Voice	0 (BE)	15	8 MB	136,434	72.76 Kbps	151.59 pps	73.85 Kbps	153 pps
CHI	Voice	0 (BE)	15	4 MB	60,270	32.14 Kbps	66.97 pps	33.12 Kbps	69 pps
RPT	All-Remaining	0 (BE)	34	4 MB	30,016	31.54 Kbps	33.35 pps	41.24 Kbps	43 pps

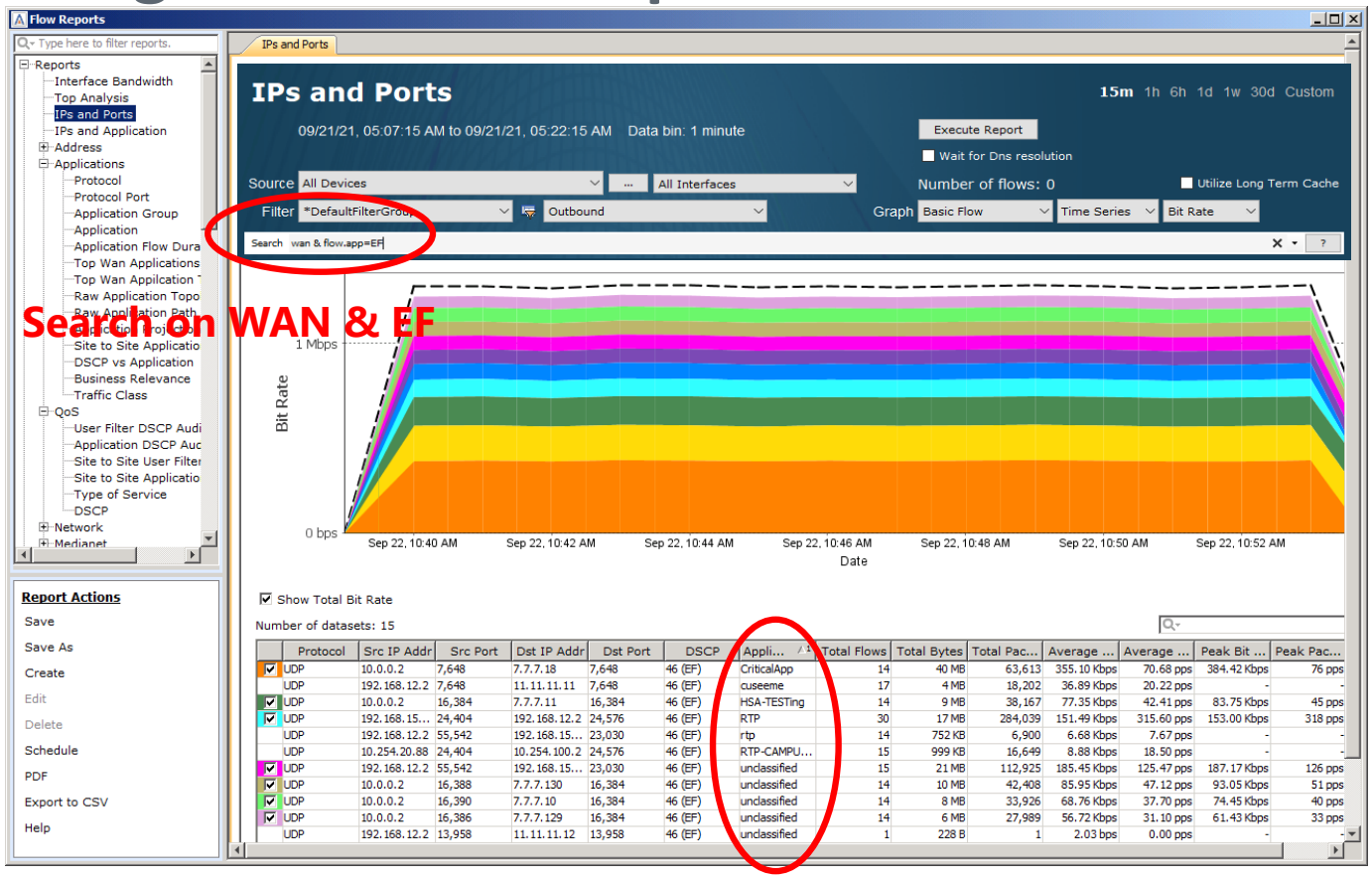
Marking: Application DSCP Audit

Where is the BE VoIP traffic?



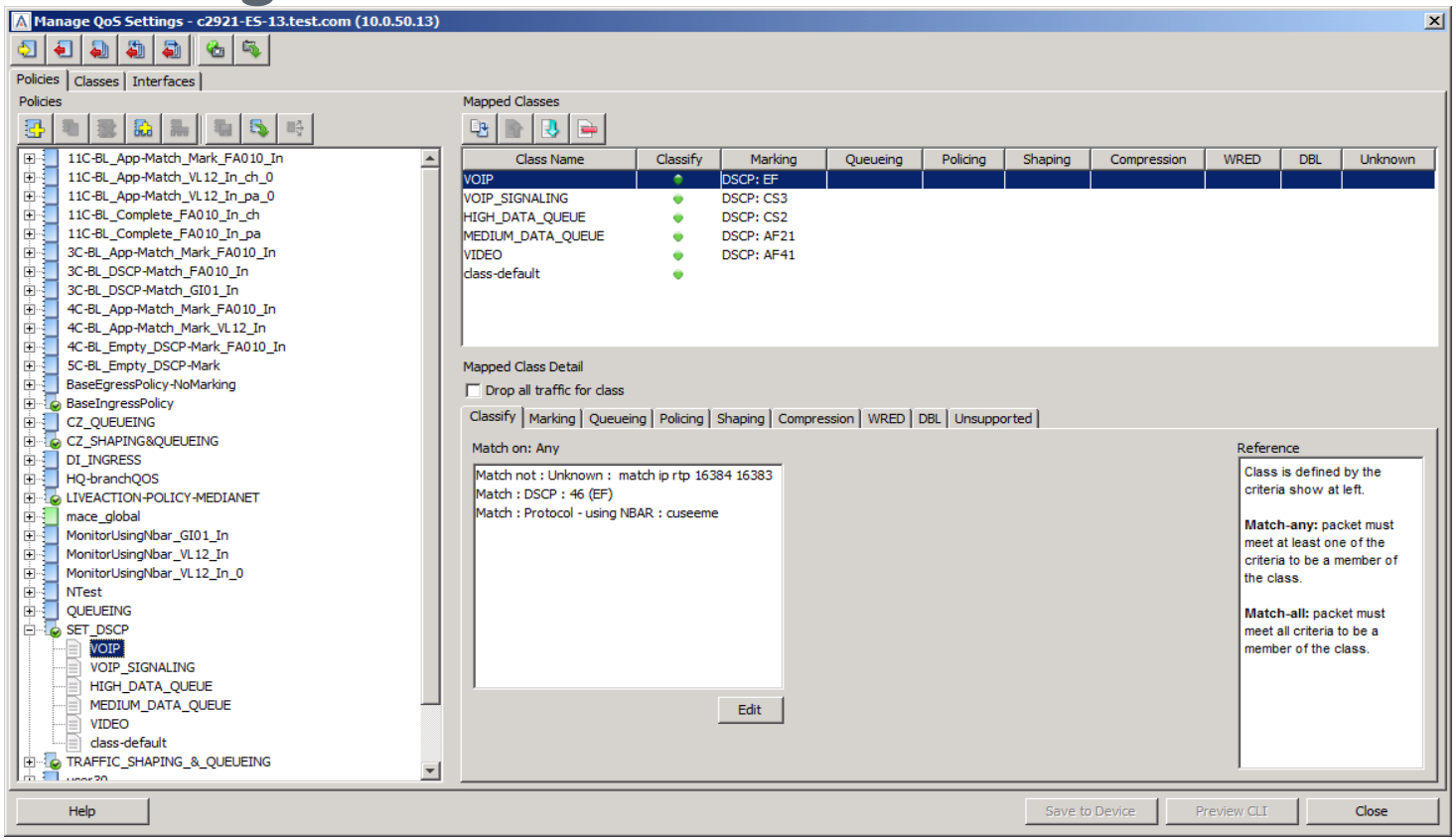
Site	Application	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packe...	Peak Bit Rate	Peak Packet Rate
CHI	RTP	0 (BE)	45	30 MB	281,471	267.05 Kbps	312.75 pps	270.47 Kbps	317 pps
BOS	RTP	0 (BE)	14	20 MB	167,679	179.06 Kbps	186.31 pps	194.31 Kbps	201 pps
LAX	RTP	0 (BE)	30	19 MB	229,494	168.43 Kbps	254.99 pps	169.88 Kbps	257 pps
BOS	RTP	46 (EF)	15	9 MB	142,452	75.97 Kbps	158.28 pps	76.82 Kbps	160 pps
CHI	RTP	46 (EF)	15	9 MB	142,334	75.91 Kbps	158.15 pps	76.70 Kbps	159 pps
RPT	RTP	0 (BE)	35	4 MB	31,120	32.76 Kbps	34.58 pps	42.91 Kbps	45 pps

Marking: IPs & Ports Report



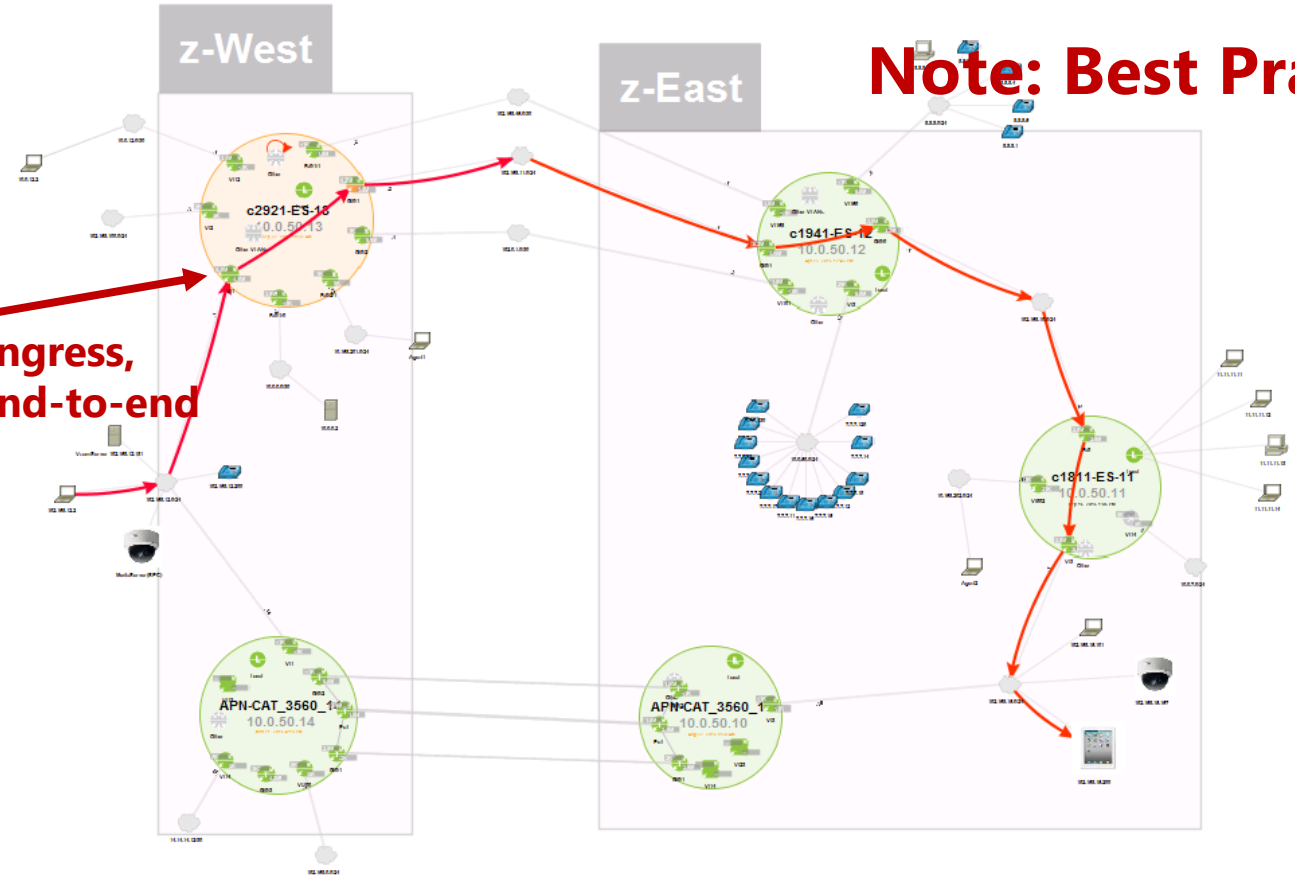
Is there any Rogue EF traffic?

Marking: How to Mark



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

Classifv: Where to Mark

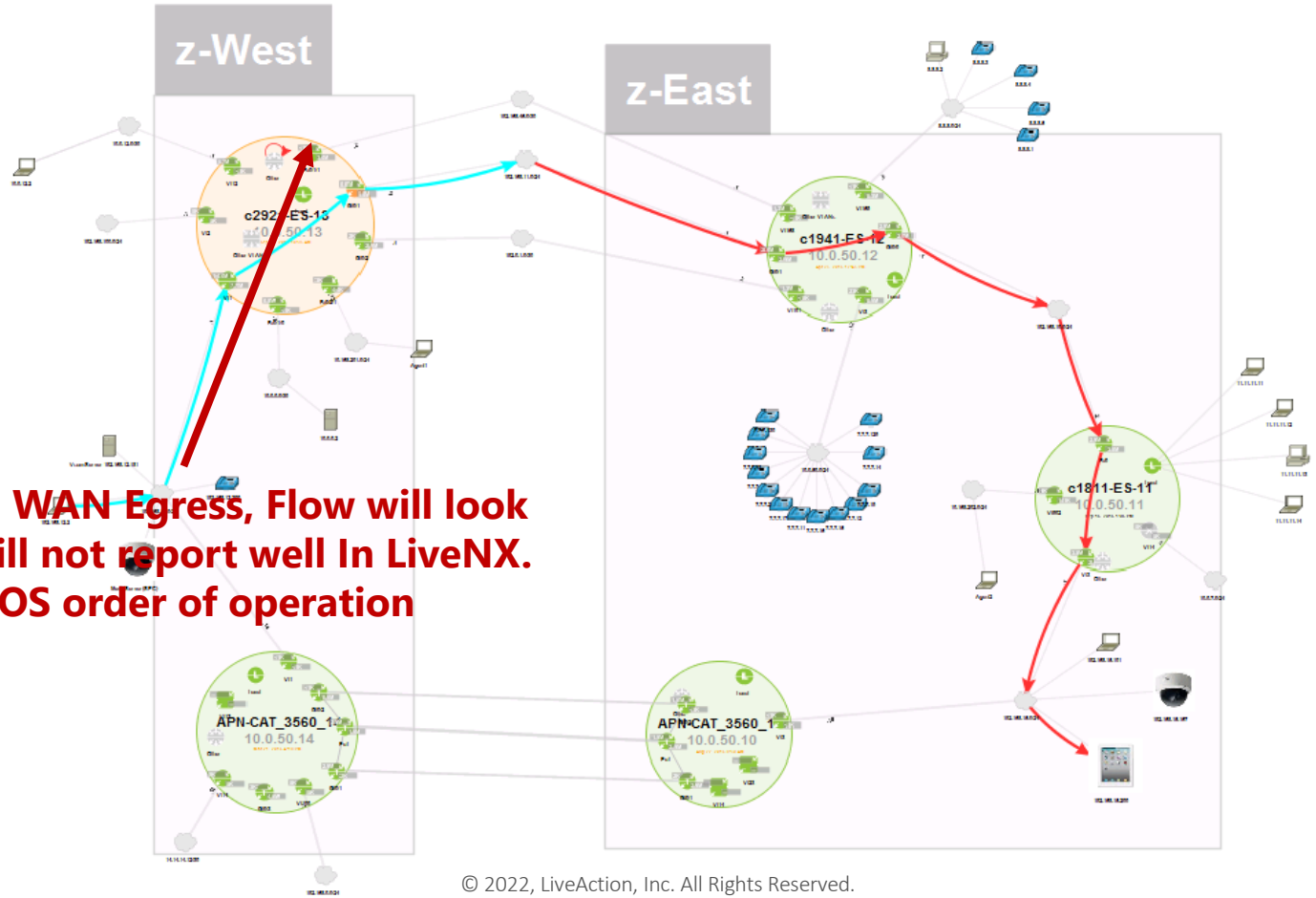


Note: Best Practice

Mark on LAN Ingress,
Flow marked end-to-end

Classify: Where to Mark

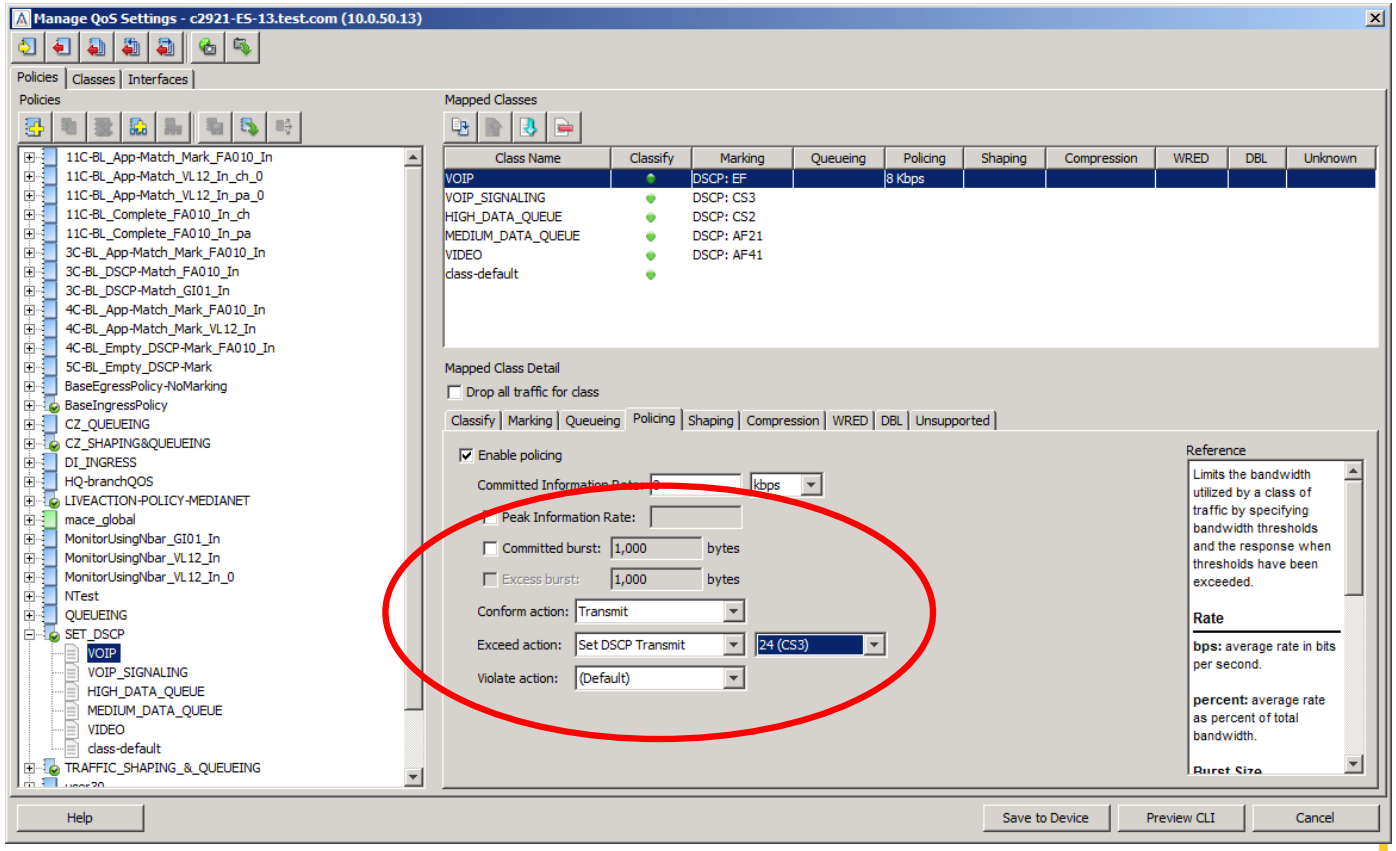
Note: Try not to do this!



If you mark on WAN Egress, Flow will look like this and will not report well In LiveNX. This is due to IOS order of operation

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

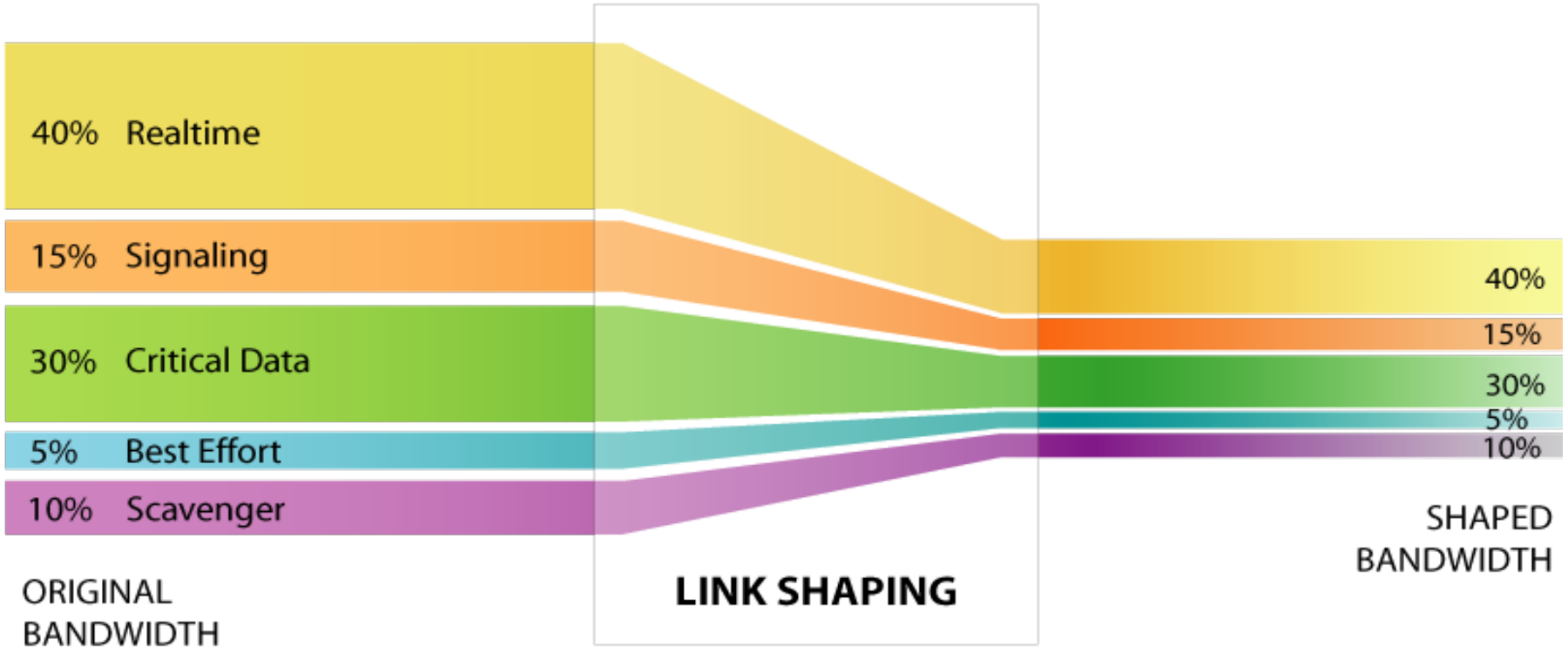
Lab: 1 & 2 Config & Classify / Mark

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

Step 2:
Queueing & Shaping

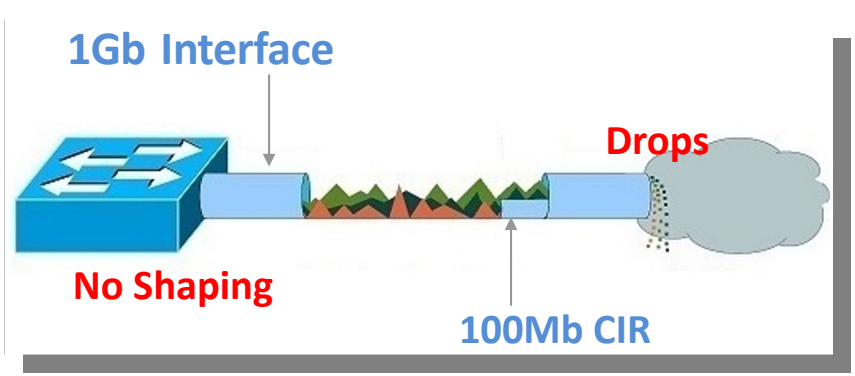
LiveAction™

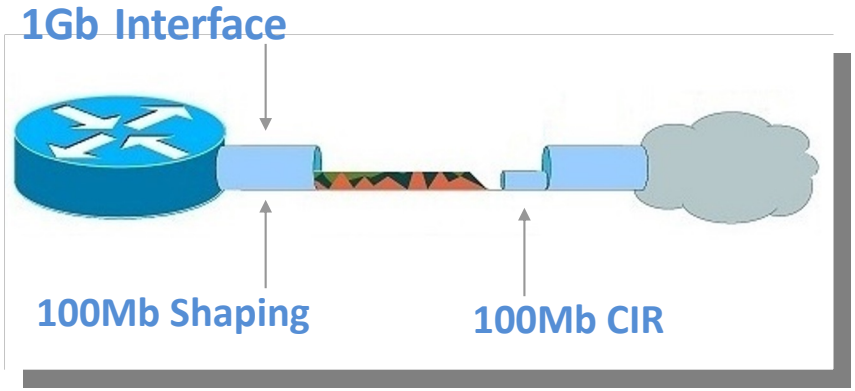
Shaping: Throttle Traffic via software & Queue



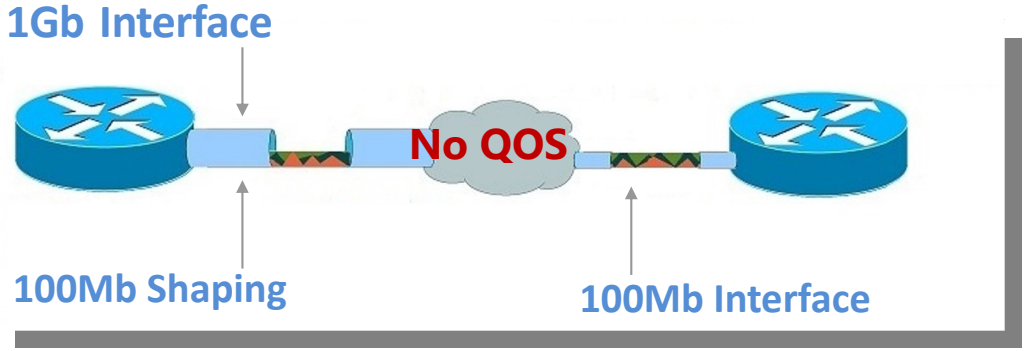
Shaping: Throttle Traffic via software & Queue

Conform to Provider's CIR

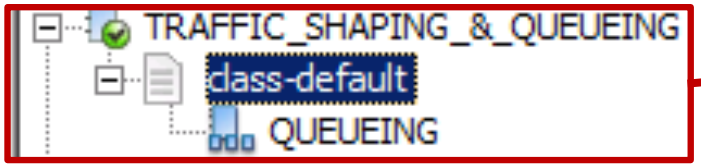


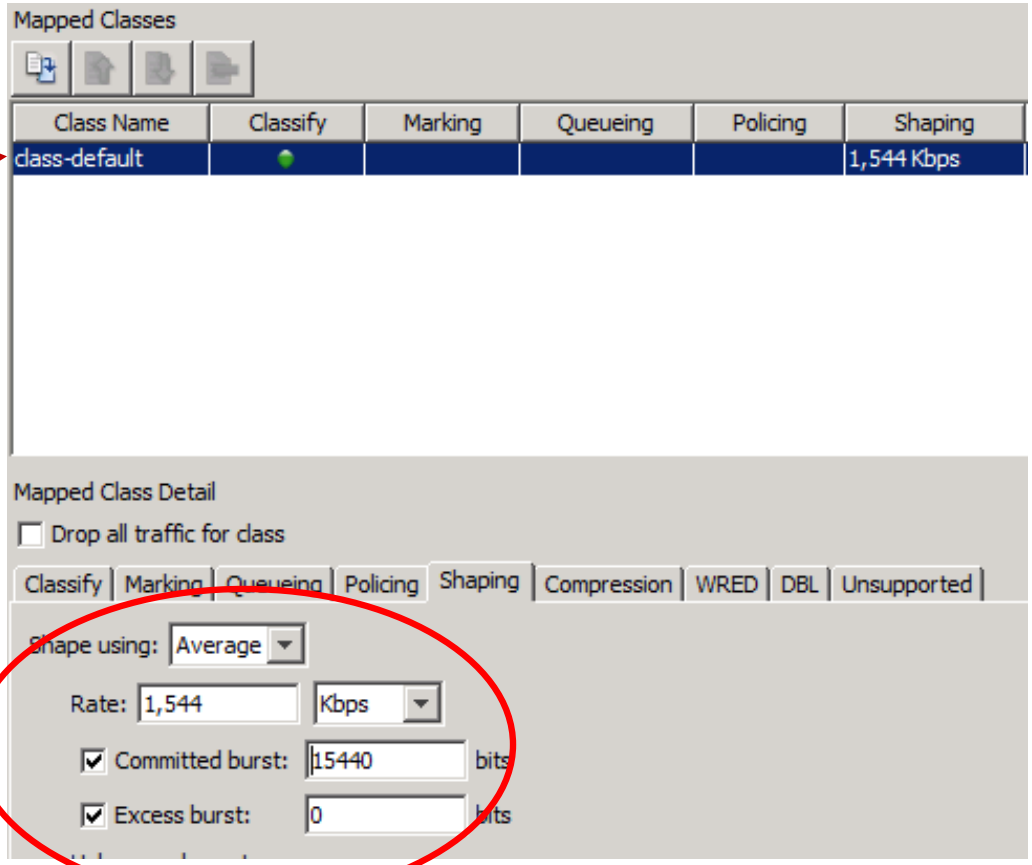


Conform to Network Limitations



Shaping: Configuration





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

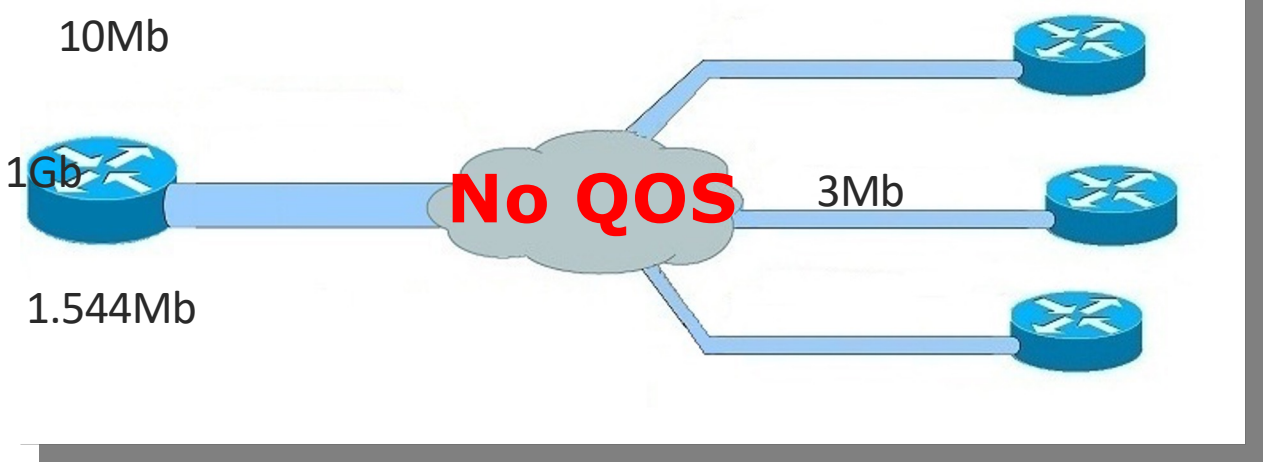
Shape average <CIR> <Bc> <Be>

Bc = 1/100 of CIR

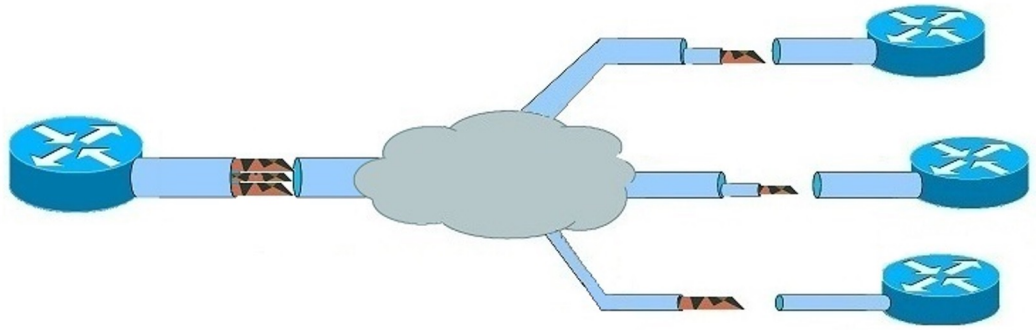
Be = 0

Shape average 1544000 15440 0

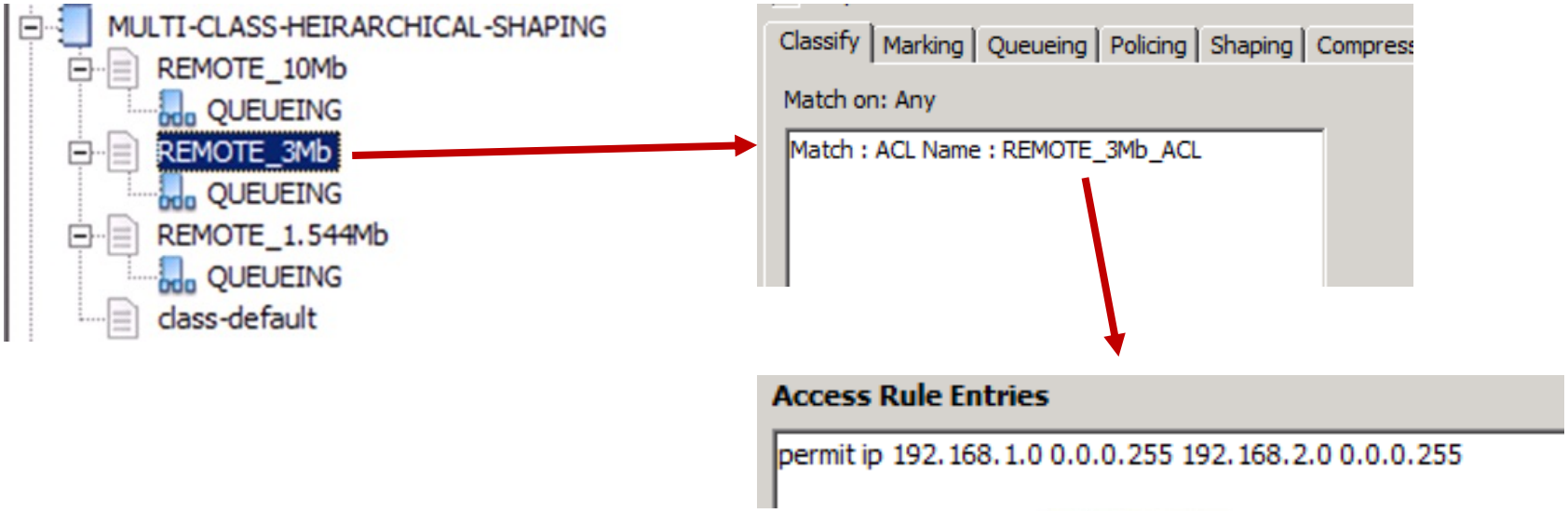
Shaping: Configuration

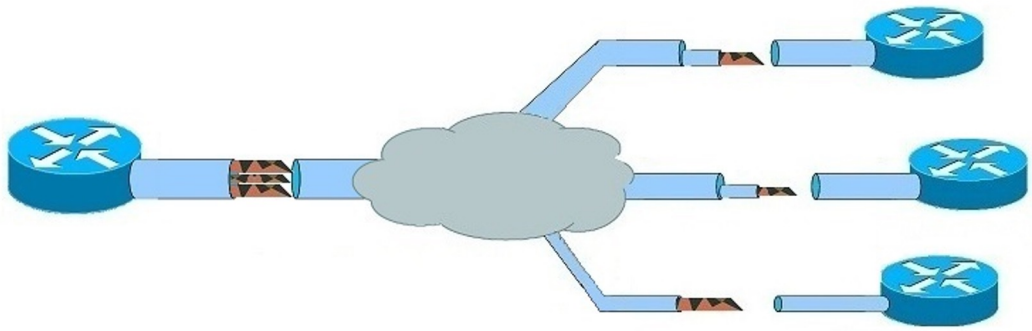


This design requires a Multi-Class Hierarchical Policy
Since the provider doesn't have QOS, you must do it



Shaping: Configuration





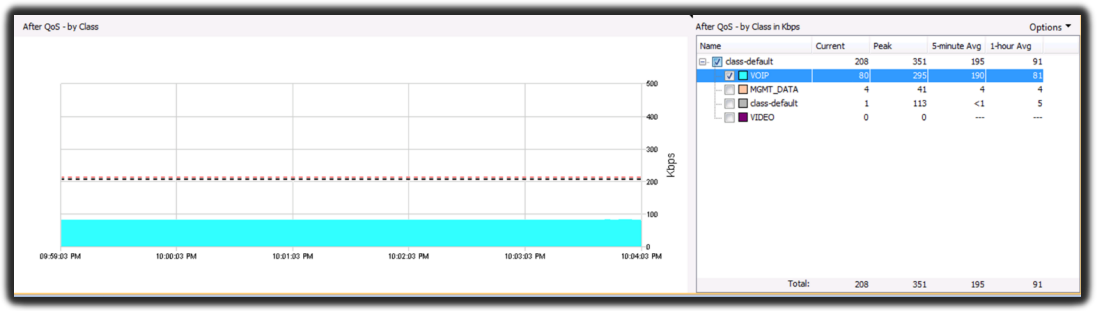
Queueing: Selecting Bandwidth Allocations

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!

Queueing: Understanding Traffic

This is how one voice call looks:

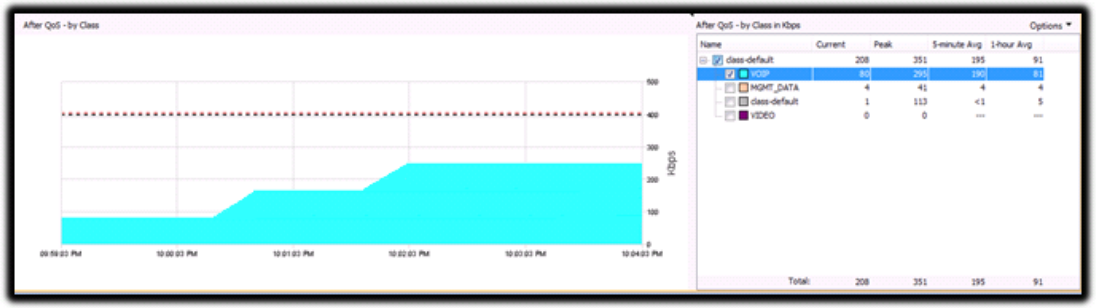


1x G.711 Call is ~82 Kbps
1x G.729 call is ~ 24.6 Kbps

Consistent pps = no burst

Queueing: Understanding Traffic

This is how 3 voice calls look:



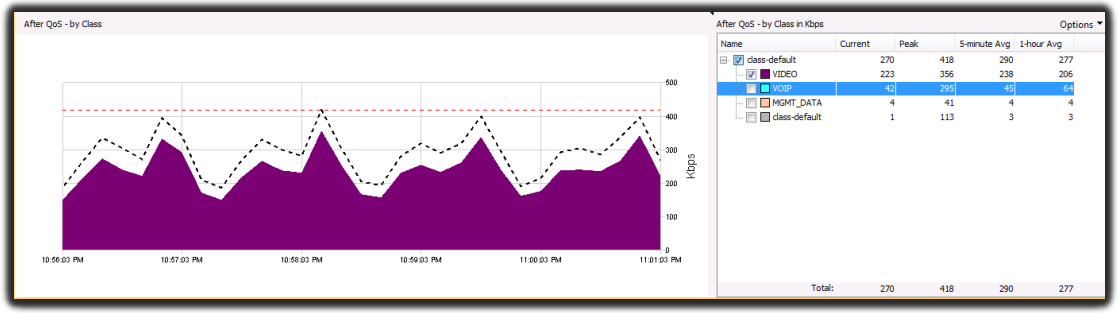
1x G.711 Call is ~82 Kbps
2x G.711 Call is ~164 Kbps
3x G.711 Call is ~246 Kbps

Etc…

No Burst = No Buffer Tuning

Queueing: Understanding Traffic

This is how one video conference call looks:



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

Overprovision Video Queues by 20% & Tune Buffers

Queueing: Understanding Traffic

Know critical apps SLA Targets!

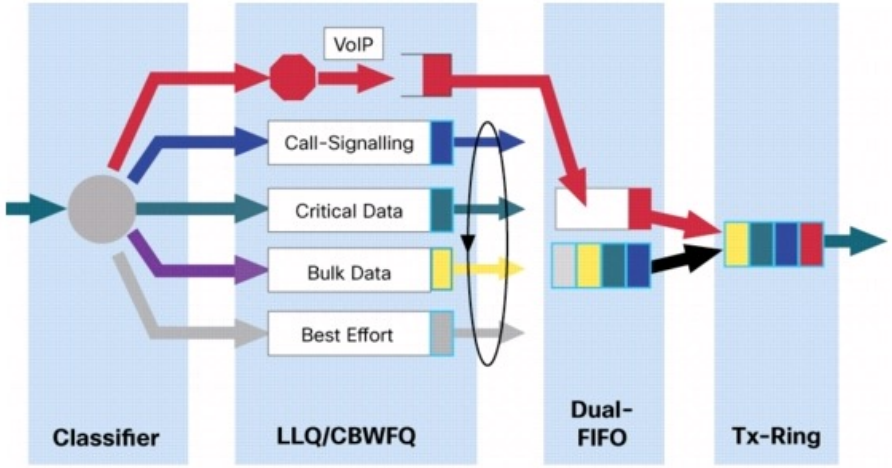
Parameter	VOIP	Traditional Video	HD / Immersive Video
Bandwidth	8-90Kbps	384 -768 kbps + network overhead	1.5 - 12.6 Mbps + network overhead
Latency	150ms	400-450ms	150ms
Jitter	30ms	30-50ms	10ms
Loss	1%	1%	0.05%

Treat with Care!

Queueing: Understanding Traffic

Voice = LLQ /Priority Queue

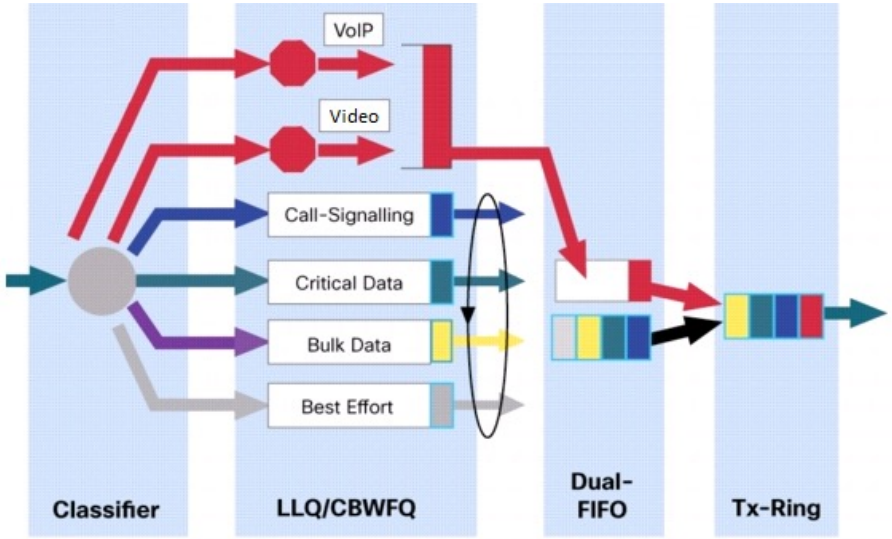
Video = ?



Queueing: Understanding Traffic

Voice = Priority Queue/LLQ

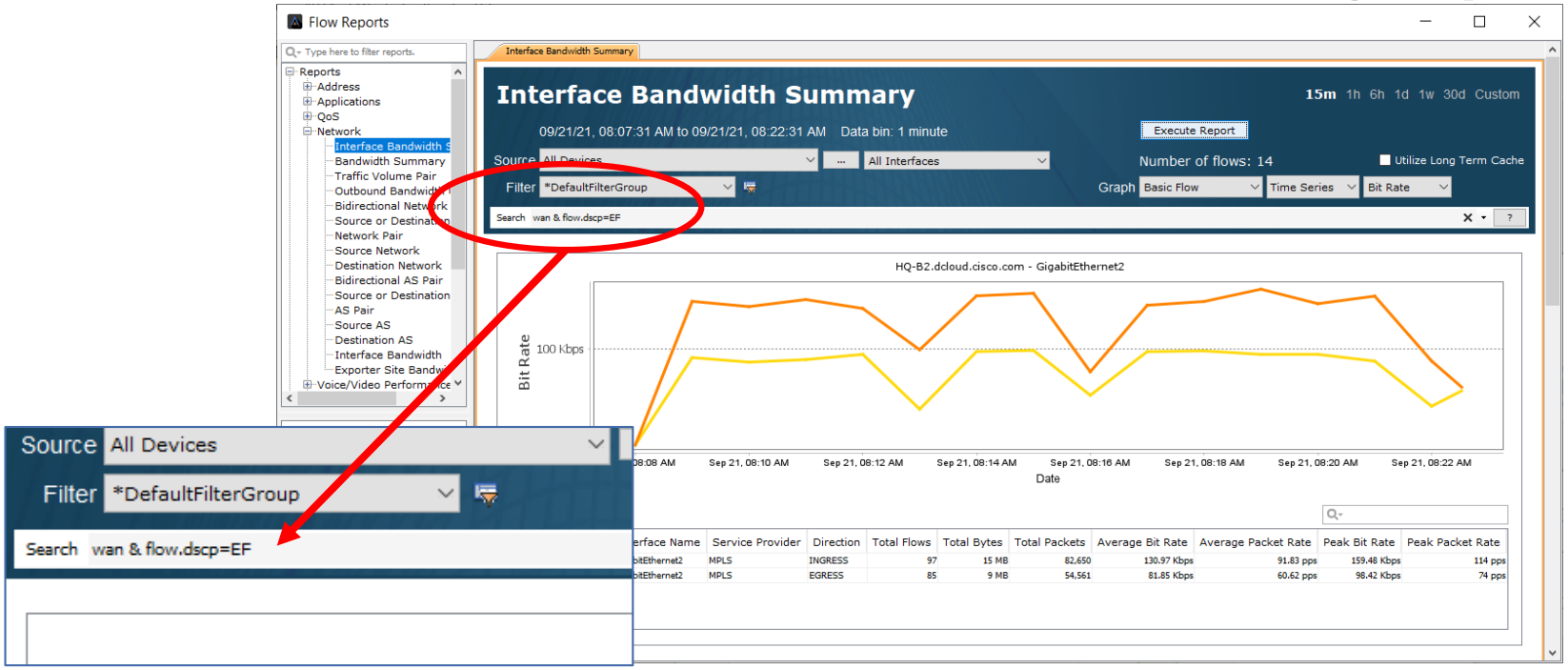
Video = Priority Queue/LLQ



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

Queueing: Sizing/Capacity Planning

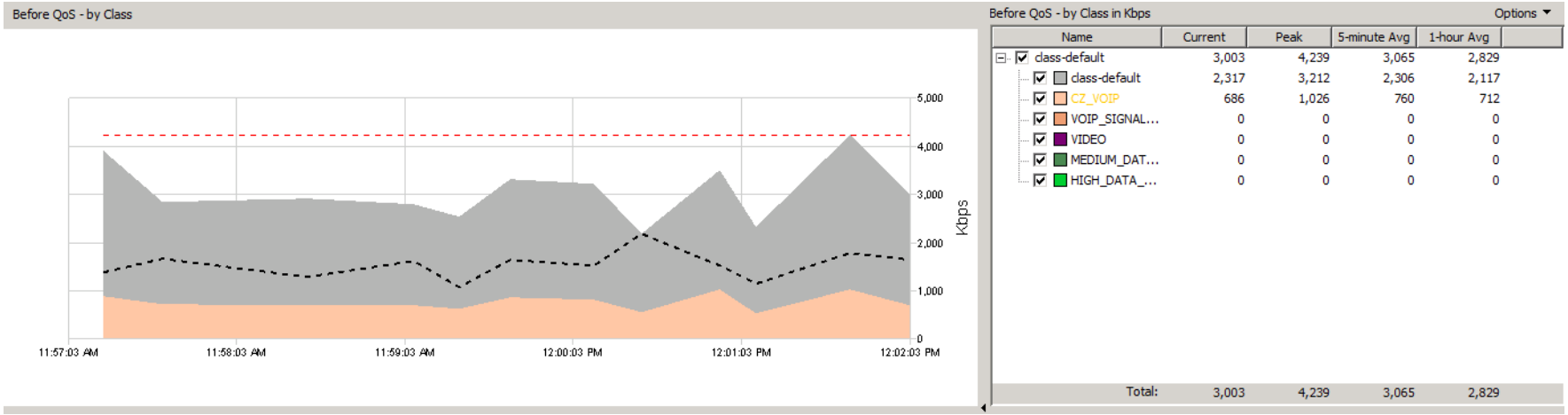
Network > Interface Bandwidth Summary Report



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

Queueing: Sizing/Capacity Planning

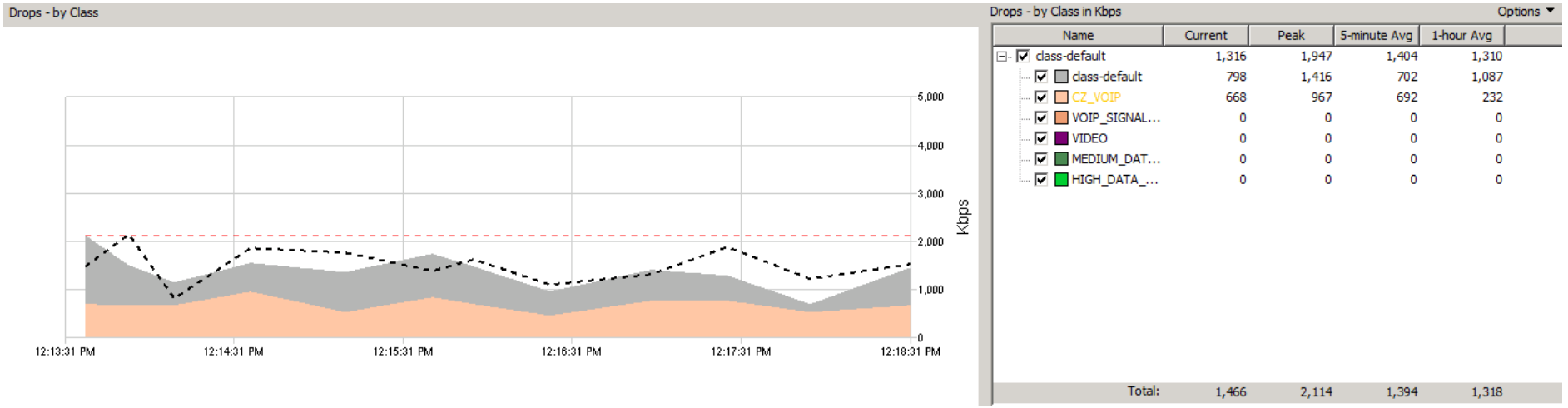
Pre-Policy QoS Report is a Great QoS Sizing Report



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

Queueing: Capacity Planning

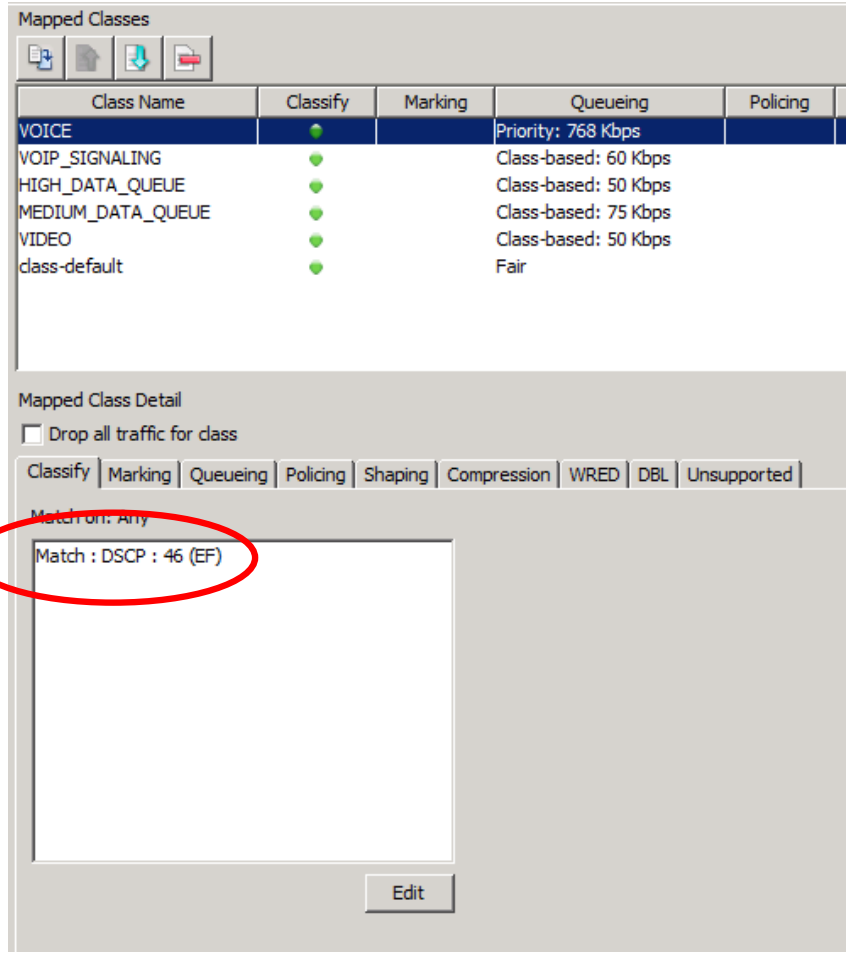
QoS Drop Report can also be a QoS Capacity Report



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!

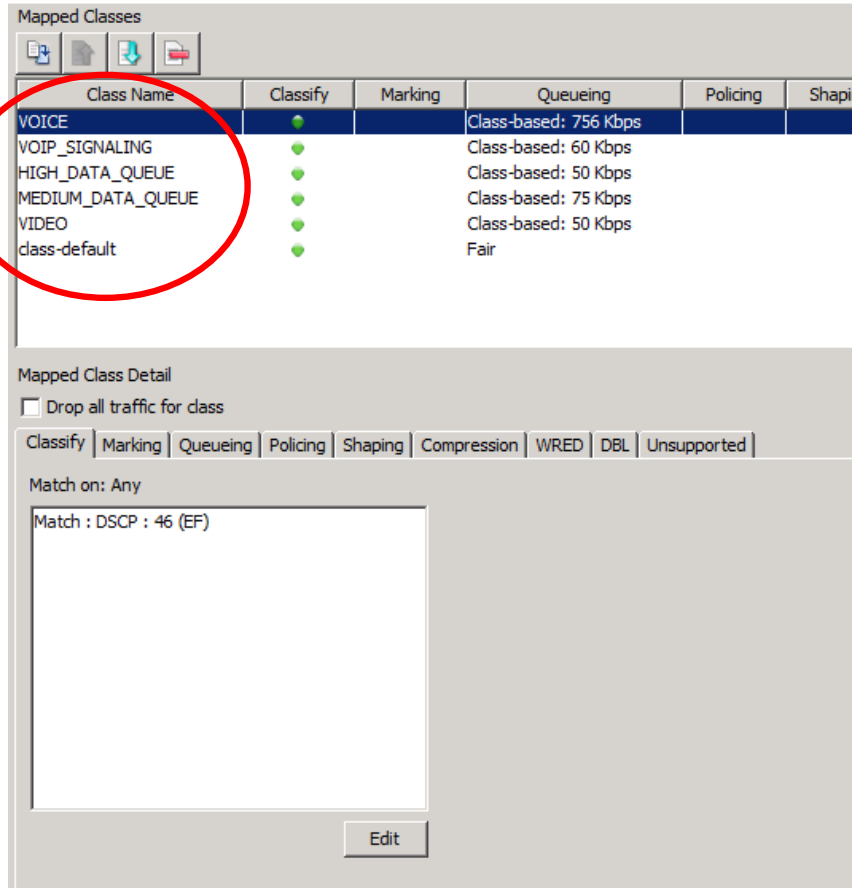
Queueing: Configuration

Match on DSCP

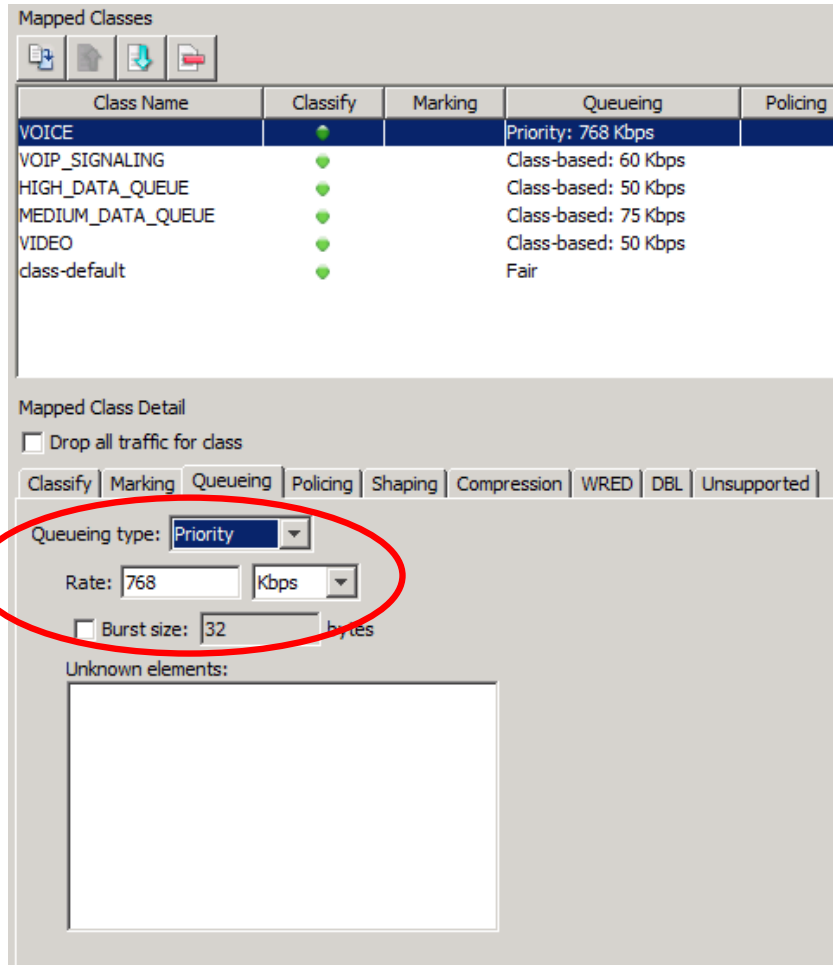


Queueing: Configuration

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.



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

Lab: 3 & 4 Queueing and Shaping

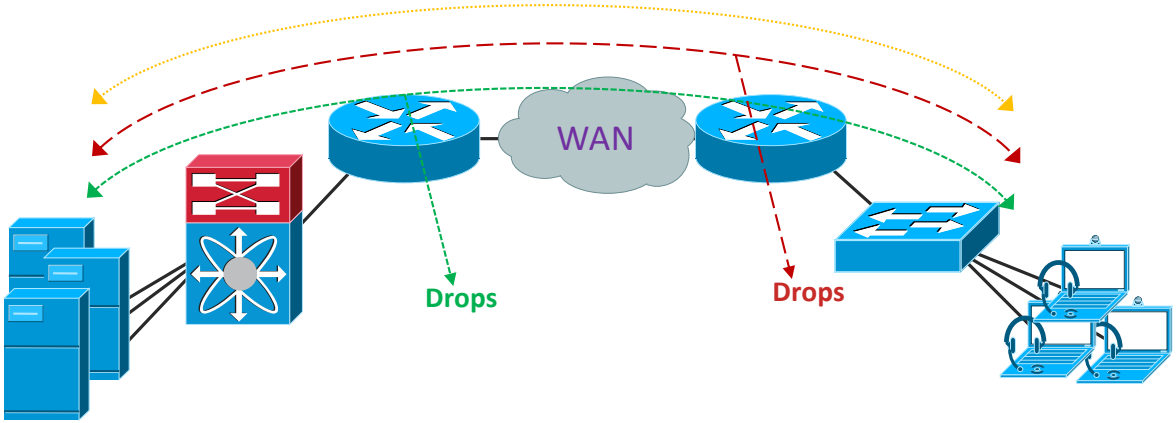
- Prioritization (Queueing & Shaping)
  - Capacity Planning Reports
  - Configure Queueing
  - Configure Shaping
  - Create Validating Policy

Step 3: Throttle Traffic

Policing & WRED

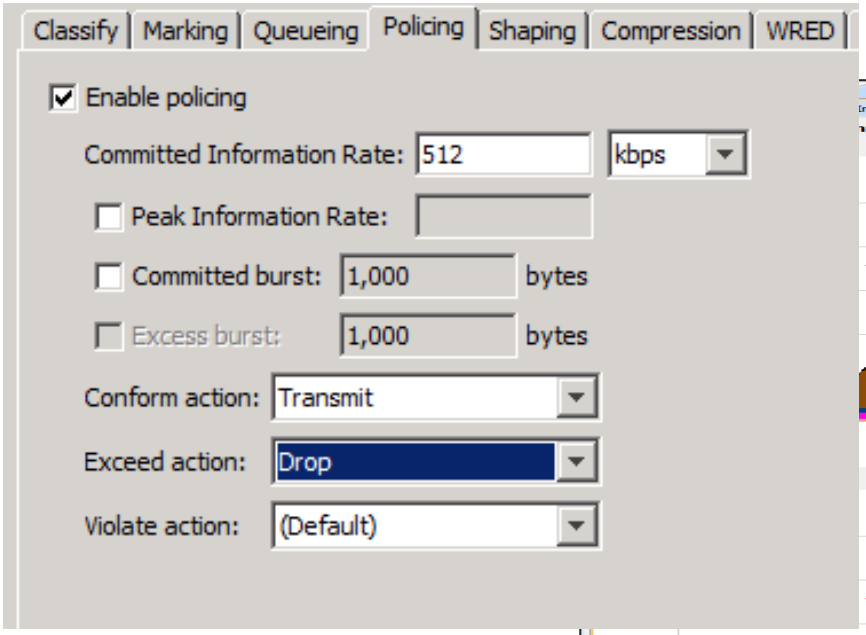
LiveAction™

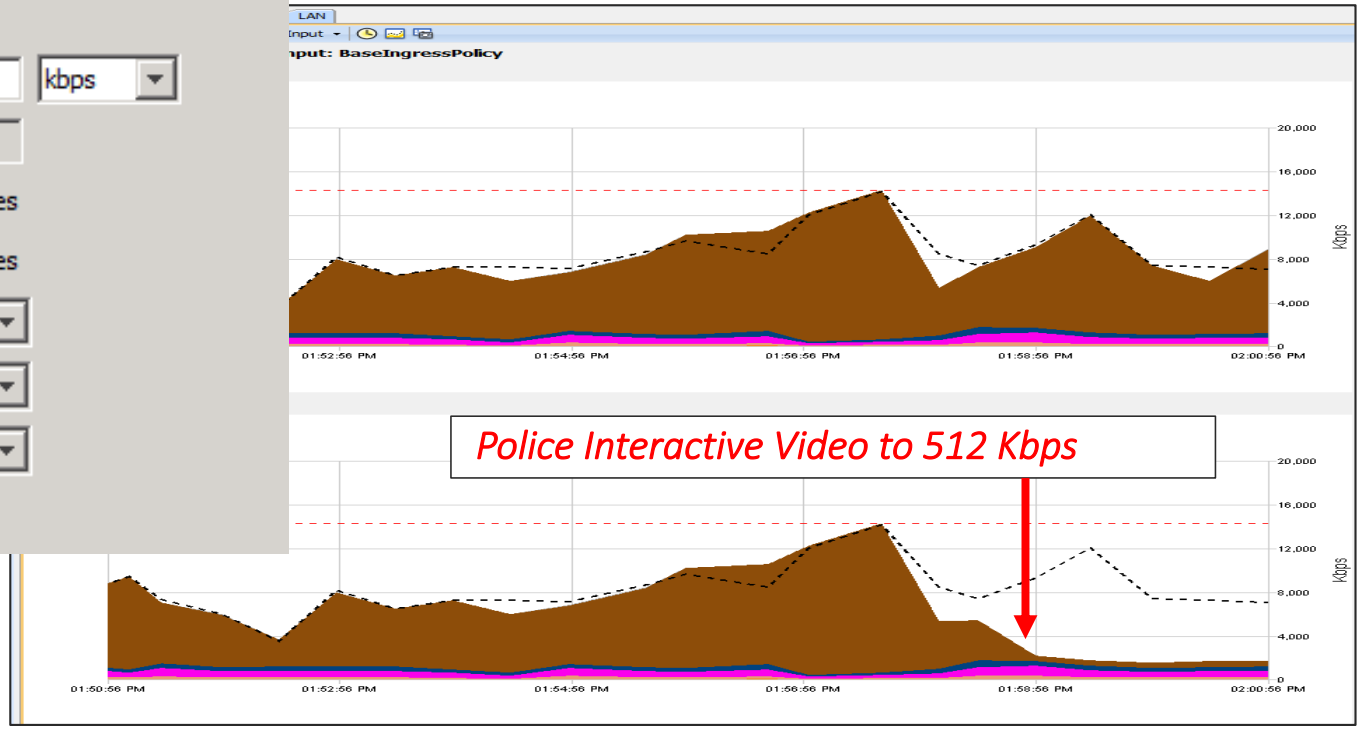
Step 3 –Throttle Traffic (Policing and WRED)



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

Policing

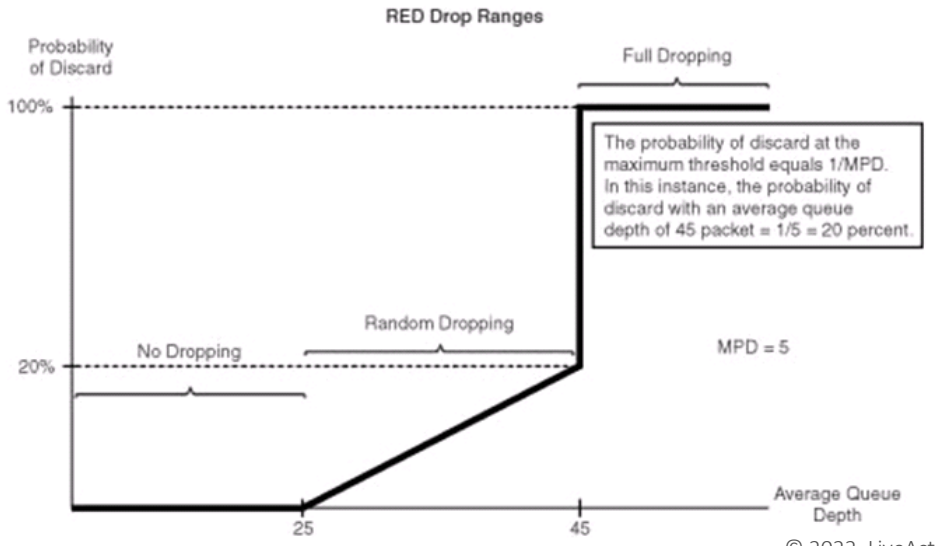


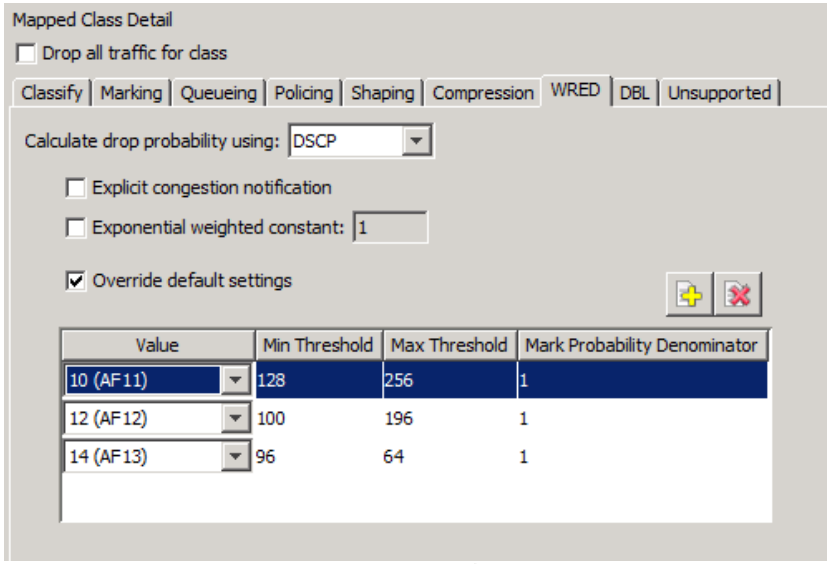


Best done on LAN ingress close to source

WRED – Weighted Random Early Detection

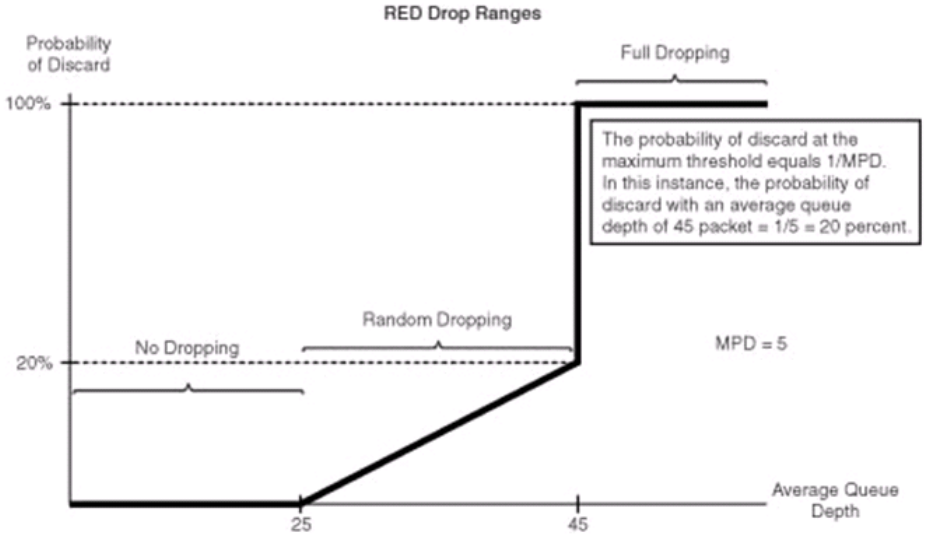
- WRED allows you to randomly start dropping data before the queue is full, to try to avoid congestion (tail drop). Min Thresholds is when random drops begin. Max Threshold = Tail Drop.
- What is a Queue? It's a "holding tank" for when there is too much data to be sent
- Default queue depth is 64 packet. When queue is full, "tail drop" begins
- Can provide "queue-in-queue" like functionality

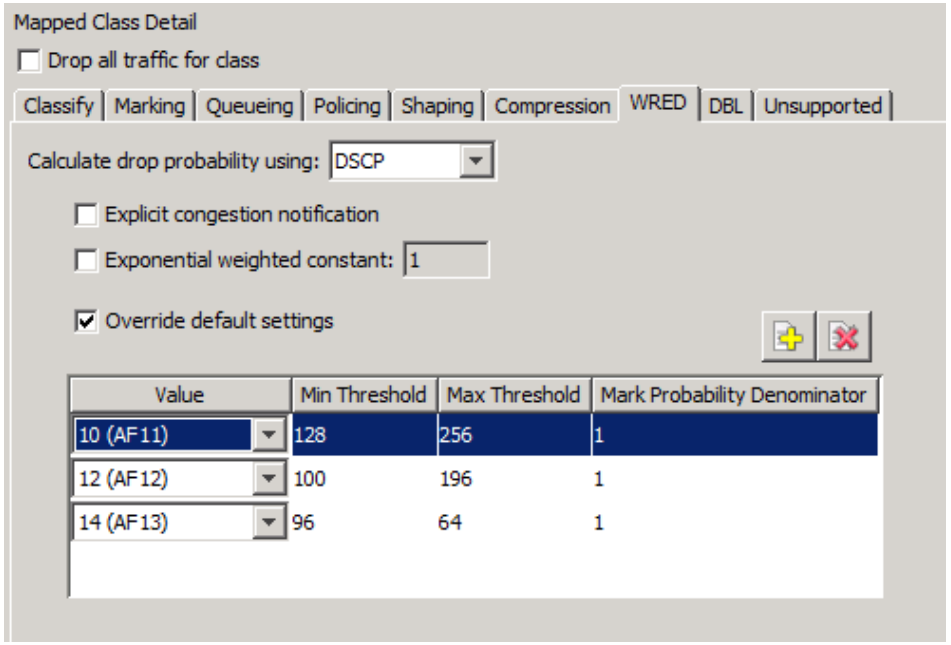




WRED - Warning!

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





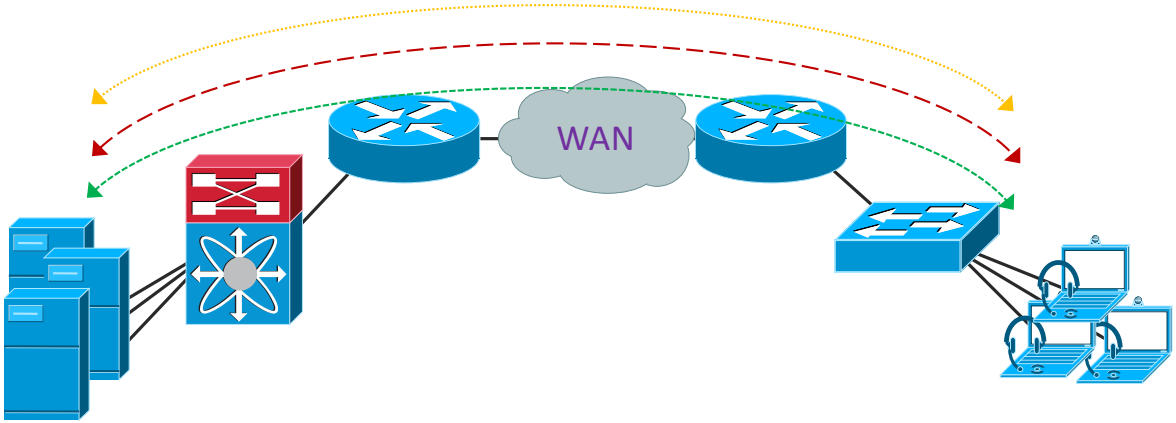
Lab: 5 Throttling & Policing

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

Step 4:
Buffer Tuning

LiveAction™

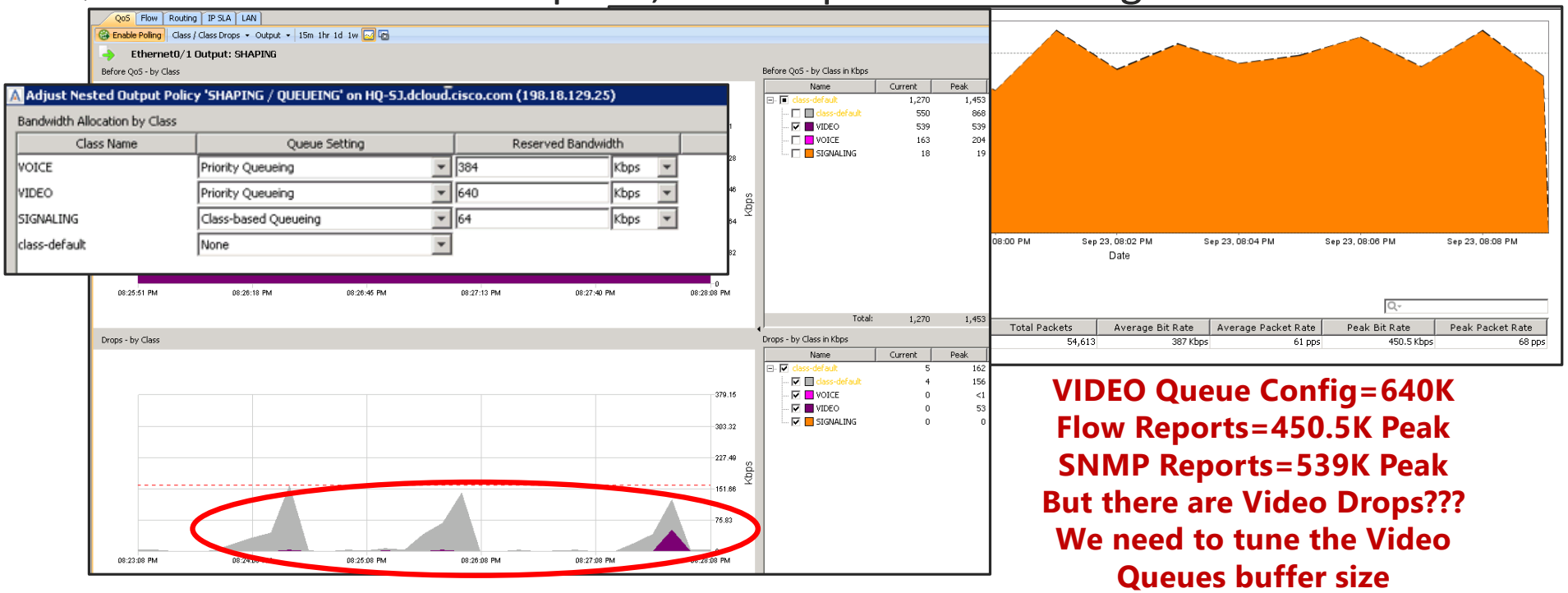
Step 4–Buffer Tuning (Advanced)



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

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

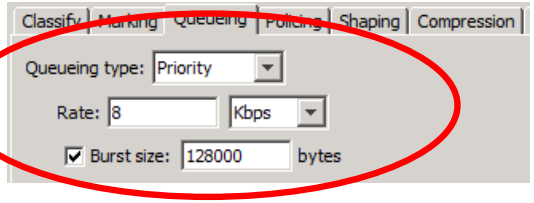
Lab: 6 Buffer Tuning

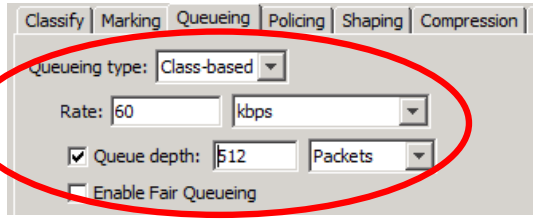
Interface's hold-queue >= total of all queues queue-limit

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: 6 Buffer Tuning

- Buffer Tuning
  - Video Queue Performance Tuning

QoS Deployment Strategies

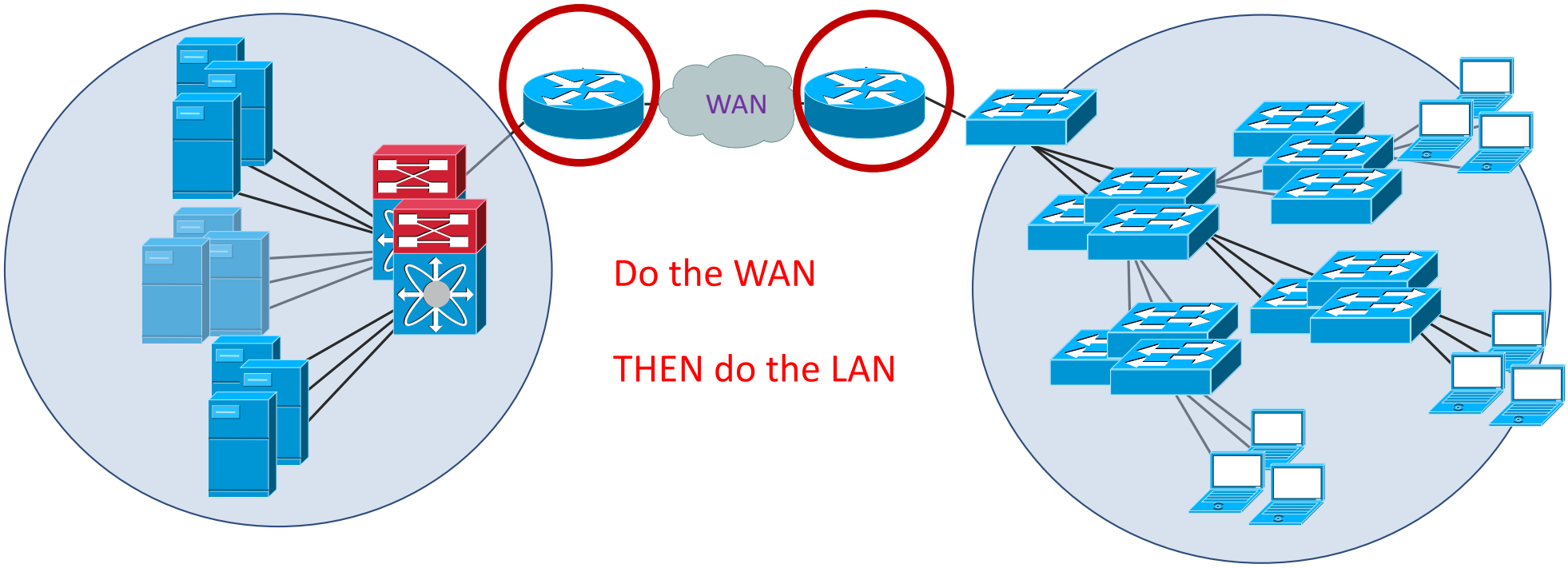
REVIEW

LiveAction™

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.

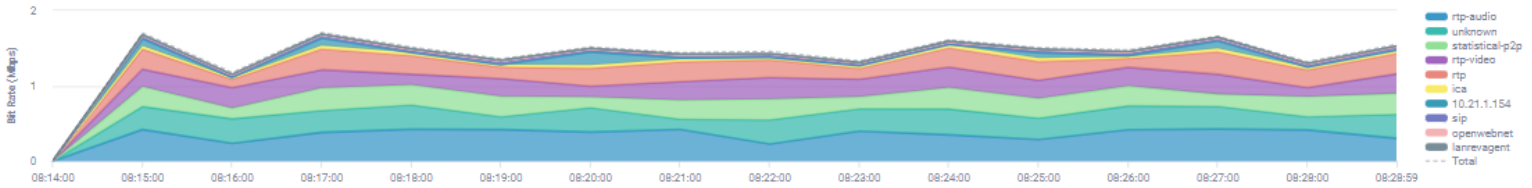
Step 1 : Implement QoS in Phases!



Step 2 - Use NetFlow Tools to Understand Bandwidth Usage

Application (Flow)

Device: All WAN Devices Interface: All WAN Interfaces Display Filter: No Display Filtering Direction: Inbound and Outbound Combined Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Bin Duration: 1 Minute Start Time: Sep 21, 2021 08:13:59 EDT (GMT-04:00)
End Time: Sep 21, 2021 08:28:59 EDT (GMT-04:00) Bin Interval: 1 minute



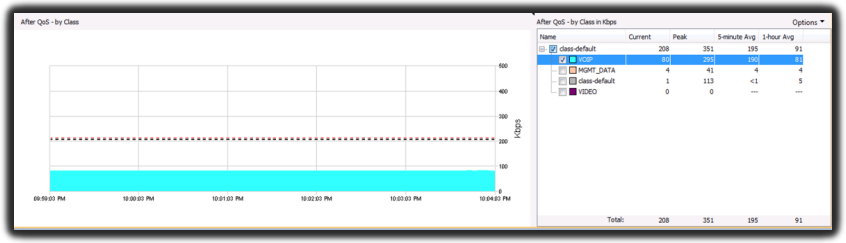
Page 1 / 3

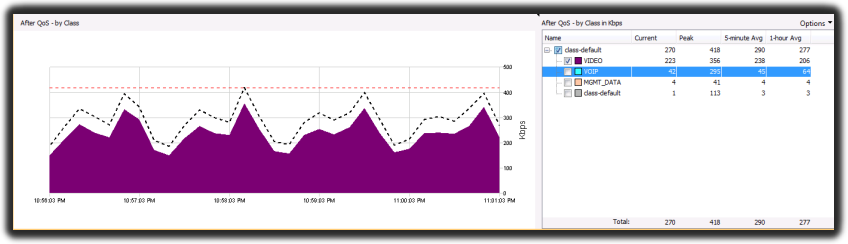
Search...

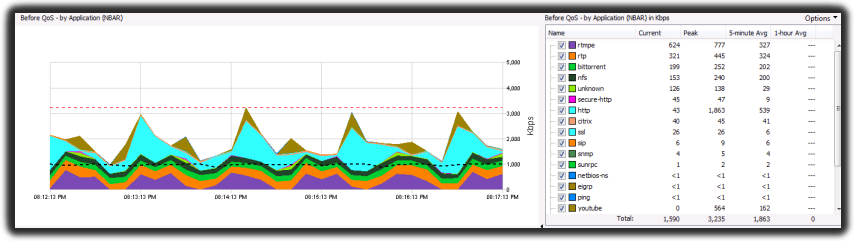
Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
	rtp-audio	171	41.10 MB	251,325	365.33 Kbps	279.25 pps	425.70 Kbps	324 pps
	unknown	145	31.56 MB	60,349	280.56 Kbps	67.05 pps	342.34 Kbps	79 pps
	statistical-p2p	161	27.07 MB	33,981	240.62 Kbps	37.76 pps	298.98 Kbps	46 pps
	rtp-video	27	25.77 MB	31,879	229.08 Kbps	35.42 pps	285.93 Kbps	43 pps
	rtp	26	25.20 MB	31,109	224.00 Kbps	34.57 pps	300.25 Kbps	45 pps
	ica	104	4.38 MB	65,725	38.94 Kbps	73.03 pps	46.22 Kbps	86 pps
	10.21.1.154	160	4.22 MB	11,946	37.54 Kbps	13.27 pps	173.26 Kbps	59 pps
	sip	148	3.40 MB	26,226	30.22 Kbps	29.14 pps	37.11 Kbps	37 pps
	openwebnet	103	1.37 MB	1,836	12.14 Kbps	2.04 pps	16.85 Kbps	2 pps
	lanrevagent	44	921.01 KB	8,712	8.19 Kbps	9.68 pps	11.62 Kbps	14 pps

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

Step 3 - Understand Applications Details







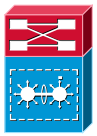
Step 4 - Get Business' Buy-In

Step 5 - Understand the Network

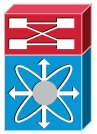
ISR,
ISRG2,
ASR1000

Catalyst
2960,3560,
3750, 3850

Catalyst
4500

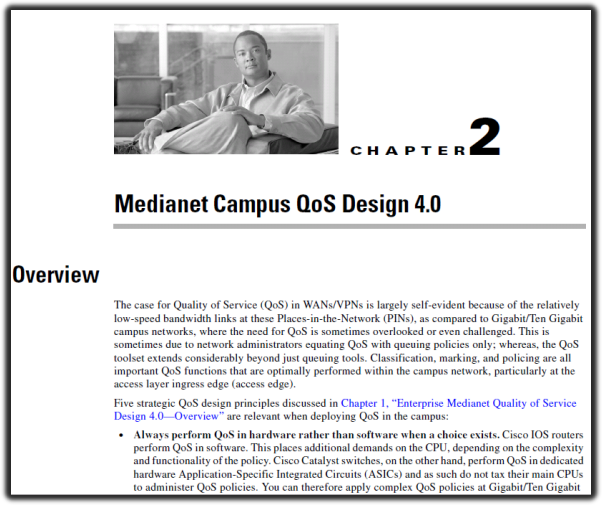


Catalyst
6500



Nexus
7000

www.cisco.com/go/srnd



CHAPTER 2

Medianet Campus QoS Design 4.0

Overview

The case for Quality of Service (QoS) in WANs/VPNs is largely self-evident because of the relatively low-speed bandwidth links at these Places-in-the-Network (PINs), as compared to Gigabit/Ten Gigabit campus networks, where the need for QoS is sometimes overlooked or even challenged. This is sometimes due to network administrators equating QoS with queuing policies only; whereas, the QoS toolset extends considerably beyond just queuing tools. Classification, marking, and policing are all important QoS functions that are optimally performed within the campus network, particularly at the access layer ingress edge (access edge).

Five strategic QoS design principles discussed in Chapter 1, "Enterprise Medianet Quality of Service Design 4.0—Overview" are relevant when deploying QoS in the campus:

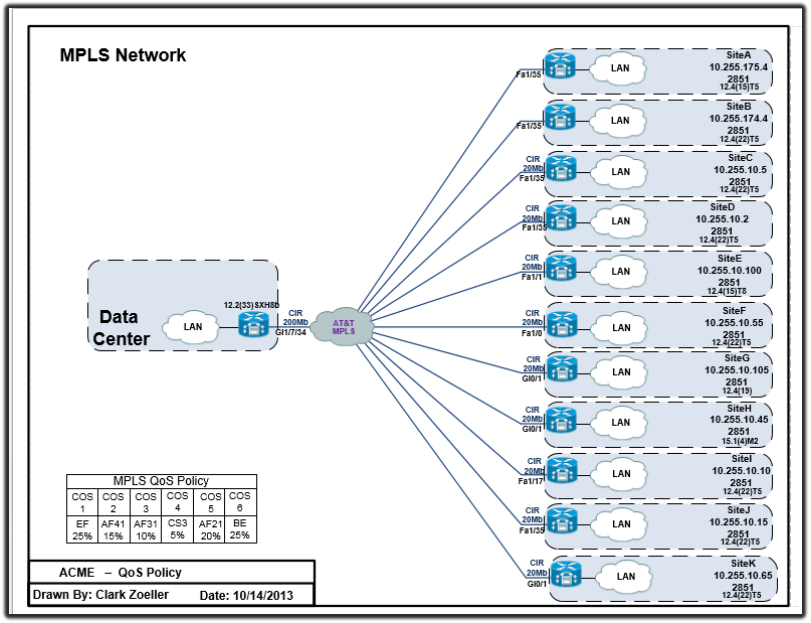
- **Always perform QoS in hardware rather than software when a choice exists.** Cisco IOS routers perform QoS in software. This places additional demands on the CPU, depending on the complexity and functionality of the policy. Cisco Catalyst switches, on the other hand, perform QoS in dedicated hardware Application-Specific Integrated Circuits (ASICs) and as such do not tax their main CPUs to administer QoS policies. You can therefore apply complex QoS policies at Gigabit/Ten Gigabit

With switches, start with SRND4 Auto-QoS where possible

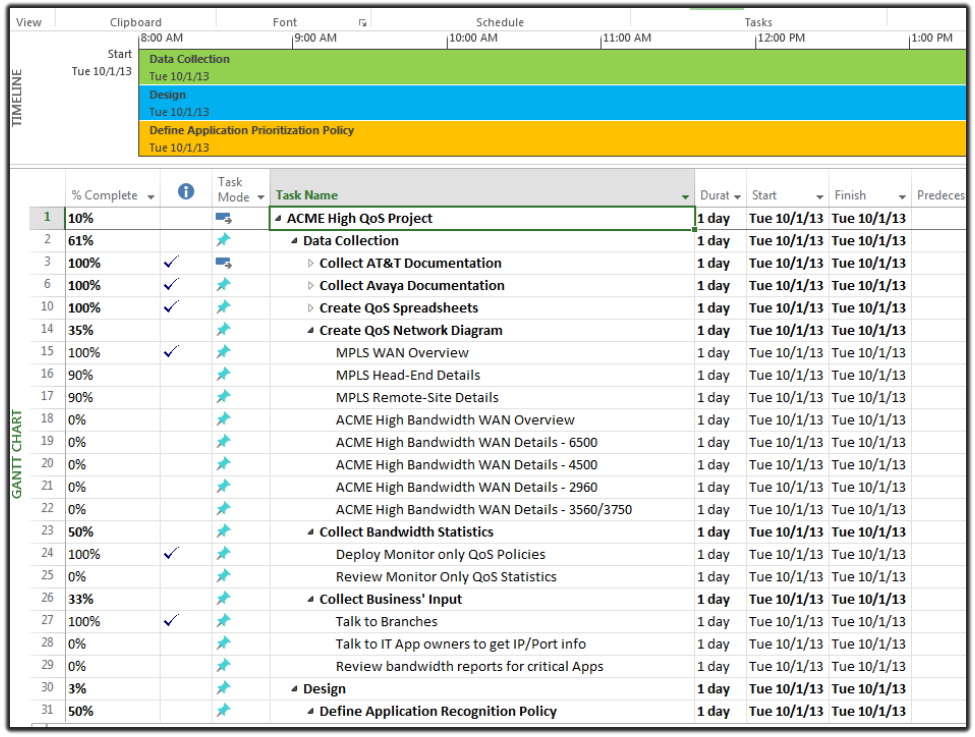
Step 6 - Have a plan

A	B	C	D	E	F	G	H	I	
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		

Step 6 - Have a plan

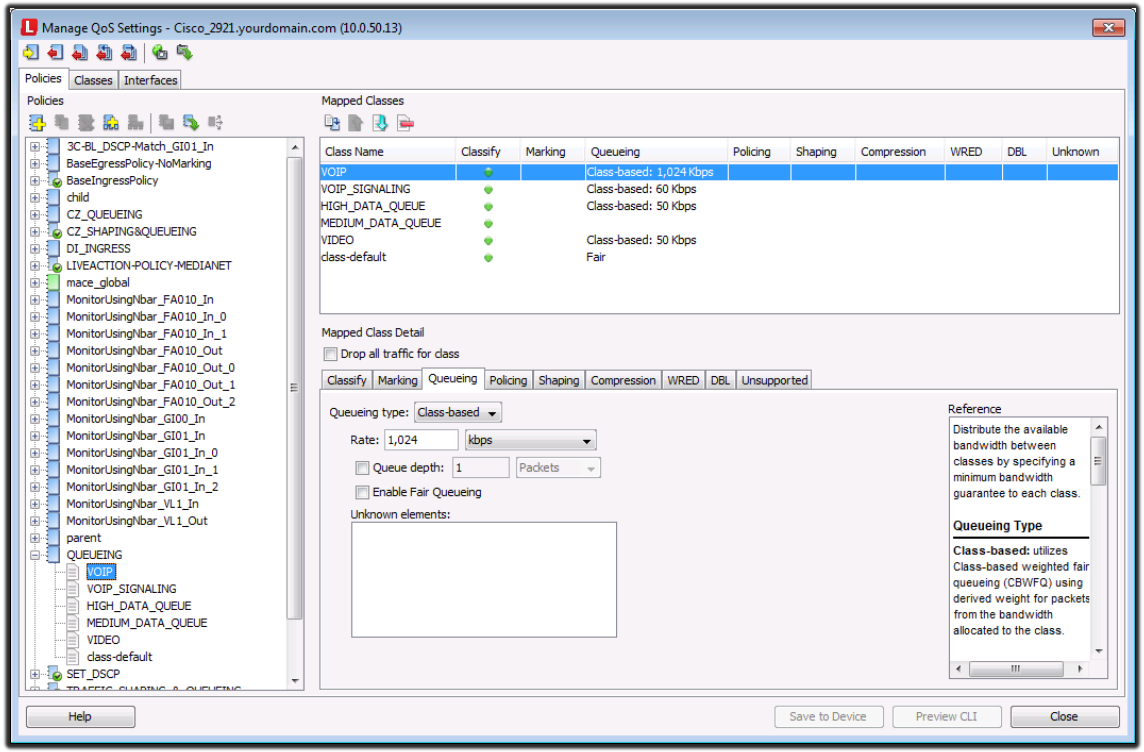


Step 6 - Have a plan



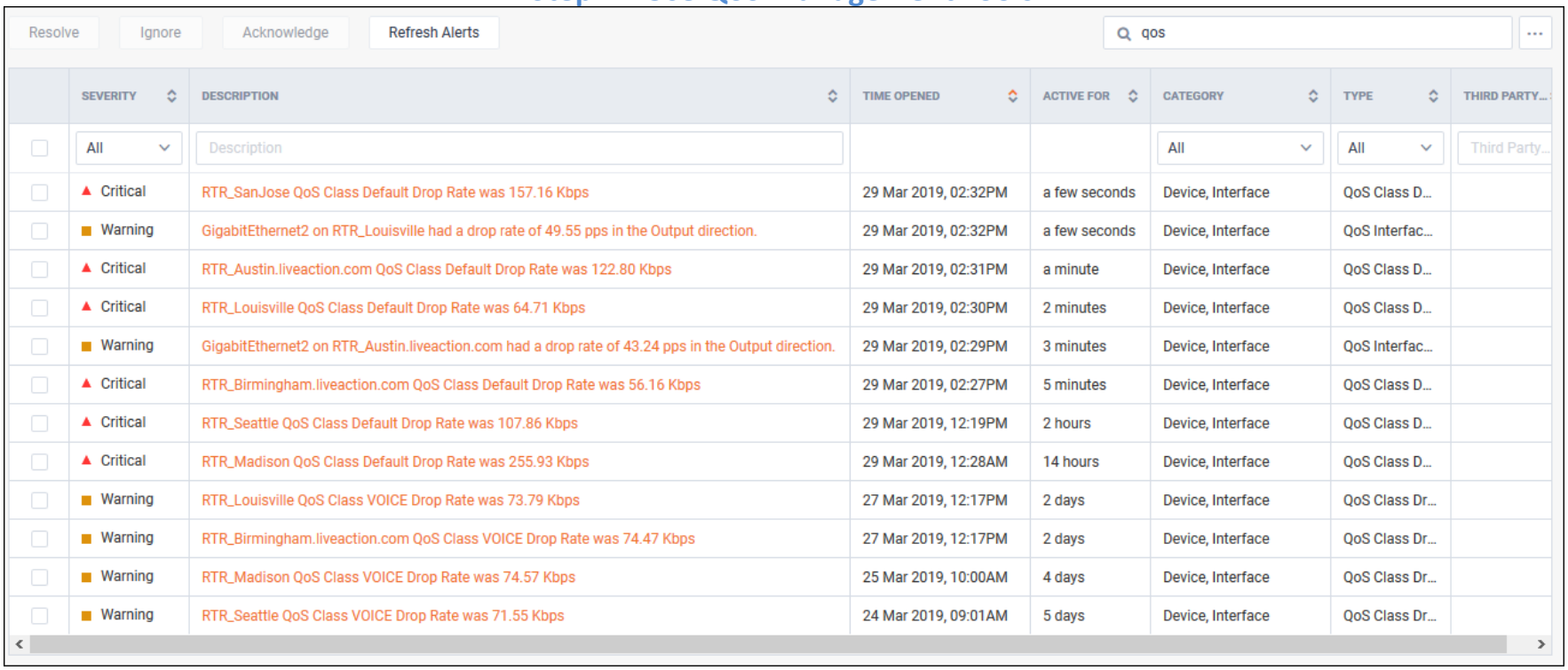
	% Complete		Task Mode	Task Name	Durat	Start	Finish	Predeces
1	**10%**			**ACME High QoS Project**	**1 day**	**Tue 10/1/13**	**Tue 10/1/13**	
2	**61%**			**Data Collection**	**1 day**	**Tue 10/1/13**	**Tue 10/1/13**	
3	**100%**	✓		**Collect AT&T Documentation**	**1 day**	**Tue 10/1/13**	**Tue 10/1/13**	
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**	

Step 7 - Use QoS management Tools



Step 7 - Use QoS management Tools

Step 7 - Use QoS management Tools

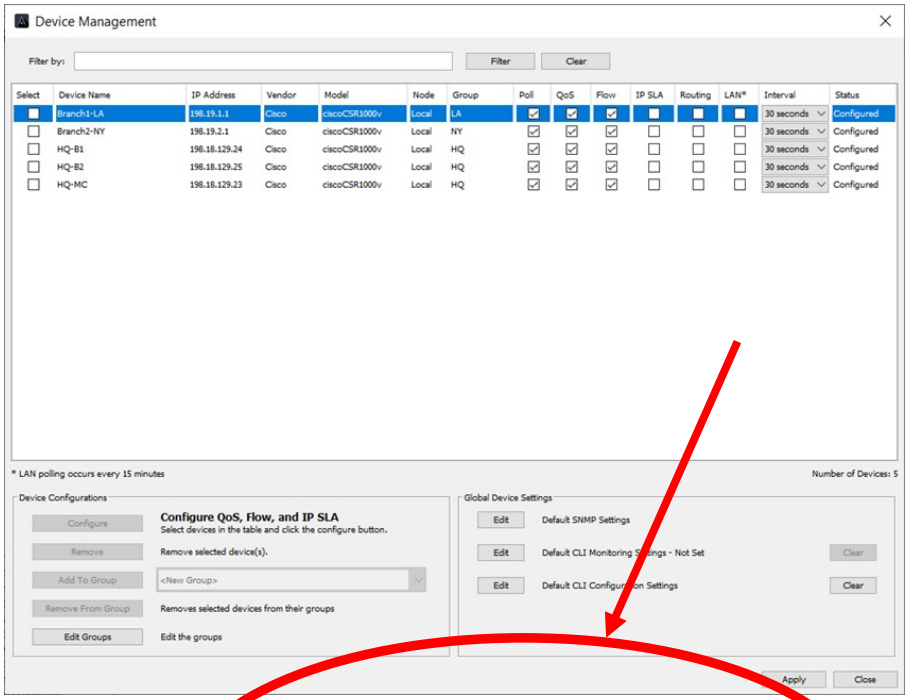


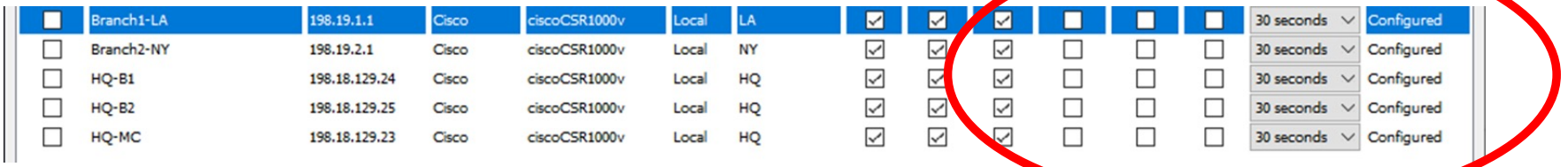
SEVERITY	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	THIRD PARTY...
All	Description			All	All	Third Party...
Critical	RTR_SanJose QoS Class Default Drop Rate was 157.16 Kbps	29 Mar 2019, 02:32PM	a few seconds	Device, Interface	QoS Class D...	
Warning	GigabitEthernet2 on RTR_Louisville had a drop rate of 49.55 pps in the Output direction.	29 Mar 2019, 02:32PM	a few seconds	Device, Interface	QoS Interfac...	
Critical	RTR_Austin.liveaction.com QoS Class Default Drop Rate was 122.80 Kbps	29 Mar 2019, 02:31PM	a minute	Device, Interface	QoS Class D...	
Critical	RTR_Louisville QoS Class Default Drop Rate was 64.71 Kbps	29 Mar 2019, 02:30PM	2 minutes	Device, Interface	QoS Class D...	
Warning	GigabitEthernet2 on RTR_Austin.liveaction.com had a drop rate of 43.24 pps in the Output direction.	29 Mar 2019, 02:29PM	3 minutes	Device, Interface	QoS Interfac...	
Critical	RTR_Birmingham.liveaction.com QoS Class Default Drop Rate was 56.16 Kbps	29 Mar 2019, 02:27PM	5 minutes	Device, Interface	QoS Class D...	
Critical	RTR_Seattle QoS Class Default Drop Rate was 107.86 Kbps	29 Mar 2019, 12:19PM	2 hours	Device, Interface	QoS Class D...	
Critical	RTR_Madison QoS Class Default Drop Rate was 255.93 Kbps	29 Mar 2019, 12:28AM	14 hours	Device, Interface	QoS Class D...	
Warning	RTR_Louisville QoS Class VOICE Drop Rate was 73.79 Kbps	27 Mar 2019, 12:17PM	2 days	Device, Interface	QoS Class Dr...	
Warning	RTR_Birmingham.liveaction.com QoS Class VOICE Drop Rate was 74.47 Kbps	27 Mar 2019, 12:17PM	2 days	Device, Interface	QoS Class Dr...	
Warning	RTR_Madison QoS Class VOICE Drop Rate was 74.57 Kbps	25 Mar 2019, 10:00AM	4 days	Device, Interface	QoS Class Dr...	
Warning	RTR_Seattle QoS Class VOICE Drop Rate was 71.55 Kbps	24 Mar 2019, 09:01AM	5 days	Device, Interface	QoS Class Dr...	

SNMP Polling Interval

LiveAction Recommends

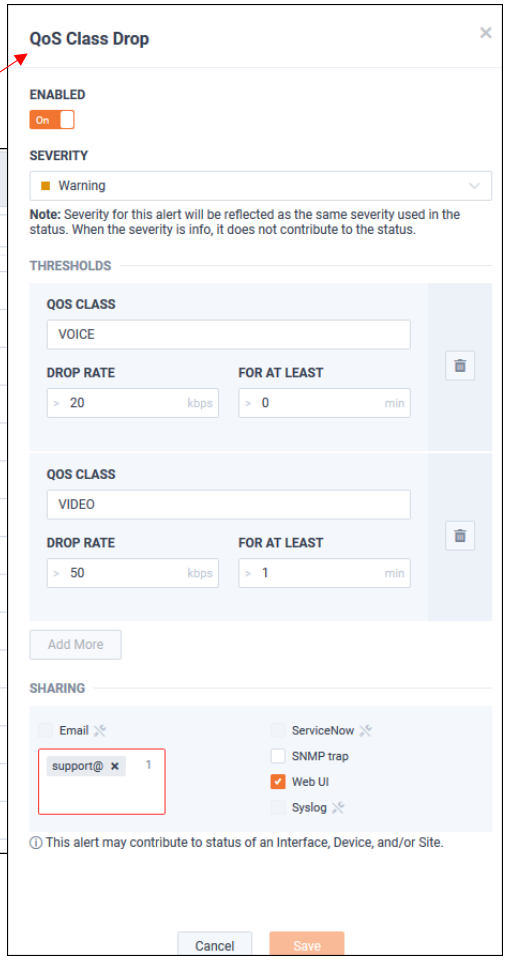
- Router polling = 30 seconds
- Switch polling = 1 minute or 5 minutes
- Poll fewest technologies required





Alerting – Customize Triggers

ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING
Alert Type	All	All	All	Thresholds	Sharing
Interface Reachability	Device, Interface	Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
IPSLA Test	Network	Critical	✓	Total Test Errors > 3 Errors for at least > 0 m...	Web UI
IPSLA Voice/Jitter Test	Network	Critical		Total Test Errors > 3 Errors for at least > 0 m...	Web UI
LiveNX CPU Utilization	System	Critical	✓	Local/Server >= 40 % for at least > 0 minutes	ServiceNow, Web UI
LiveNX Disk Utilization	System	Critical	✓	Local/Server >= 60 % for at least > 0 minutes	ServiceNow, Web UI
LiveNX Memory Utilization	System	Critical	✓	Local/Server >= 40 % for at least > 0 minutes	ServiceNow, Web UI
LiveNX Node Connectivity	System	Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
Media Jitter Max	Application	Critical	✓	Jitter Max >= 10 ms for at least > 0 minutes	ServiceNow, Web UI
Media Jitter Min	Application	Critical	✓	Jitter Min >= 10 ms for at least > 0 minutes	ServiceNow, Web UI
Media Packet Loss	Application	Critical	✓	Packet Loss >= 10 % for at least > 0 minutes	Web UI
Network Delay Per Connection	Network	Critical	✓	Delay Time >= 50 ms for at least > 1 minutes	ServiceNow, Web UI
QoS Class Default Drop	Device, Interface	Critical	✓	Drop Rate > 40 kbps for at least > 0 minutes	ServiceNow, Web UI
QoS Class Drop	Device, Interface	Warning		Qos Class VOICE Drop Rate > 40 kbps for at ...	ServiceNow, Web UI
QoS Interface Drop	Device, Interface	Warning	✓	Drop Rate > 40 pps for at least > 0 minutes	ServiceNow, Web UI
Routing Adjacency State Change	Network	Critical	✓	for at least > 0 minutes	Web UI



Lab 6: Finish The Labs

- Including Lab 7: QoS Alerts

What's Next?
SDWAN

Finish the Labs…

LiveAction™

Agenda

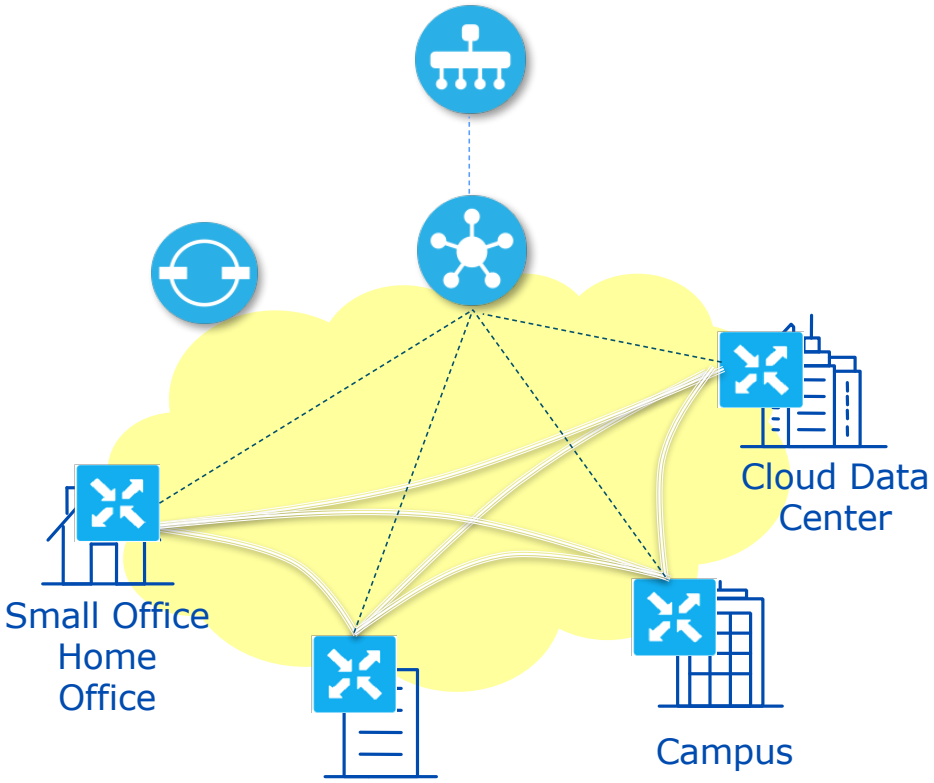
- Cisco/Viptela SDWAN Overview
- LiveNX – SDWAN Integration Overview
- Day 0: Cisco SD WAN Planning for Deployment
- LiveNX - SDWAN Onboarding
- Day 1: Cisco SD WAN Policy Validation and Intent
- Day 2: Cisco SD WAN Operations

LiveNX

Cisco/Viptela SDWAN Overview

LiveAction™

SDWAN Basics



vEdge – SDWAN Edge Router

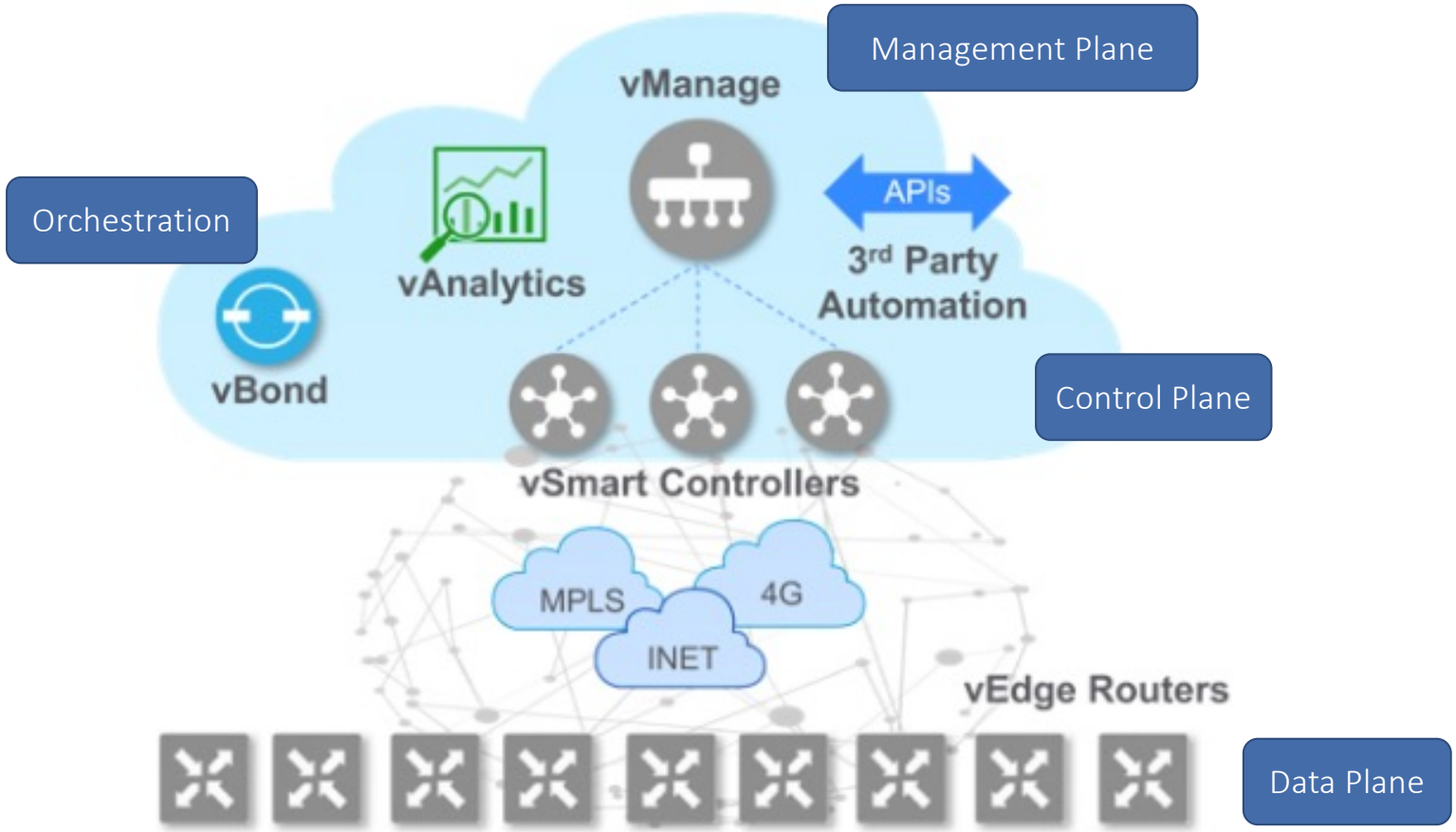
vManage – SDWAN Manager

vBond – SDWAN Orchestrator

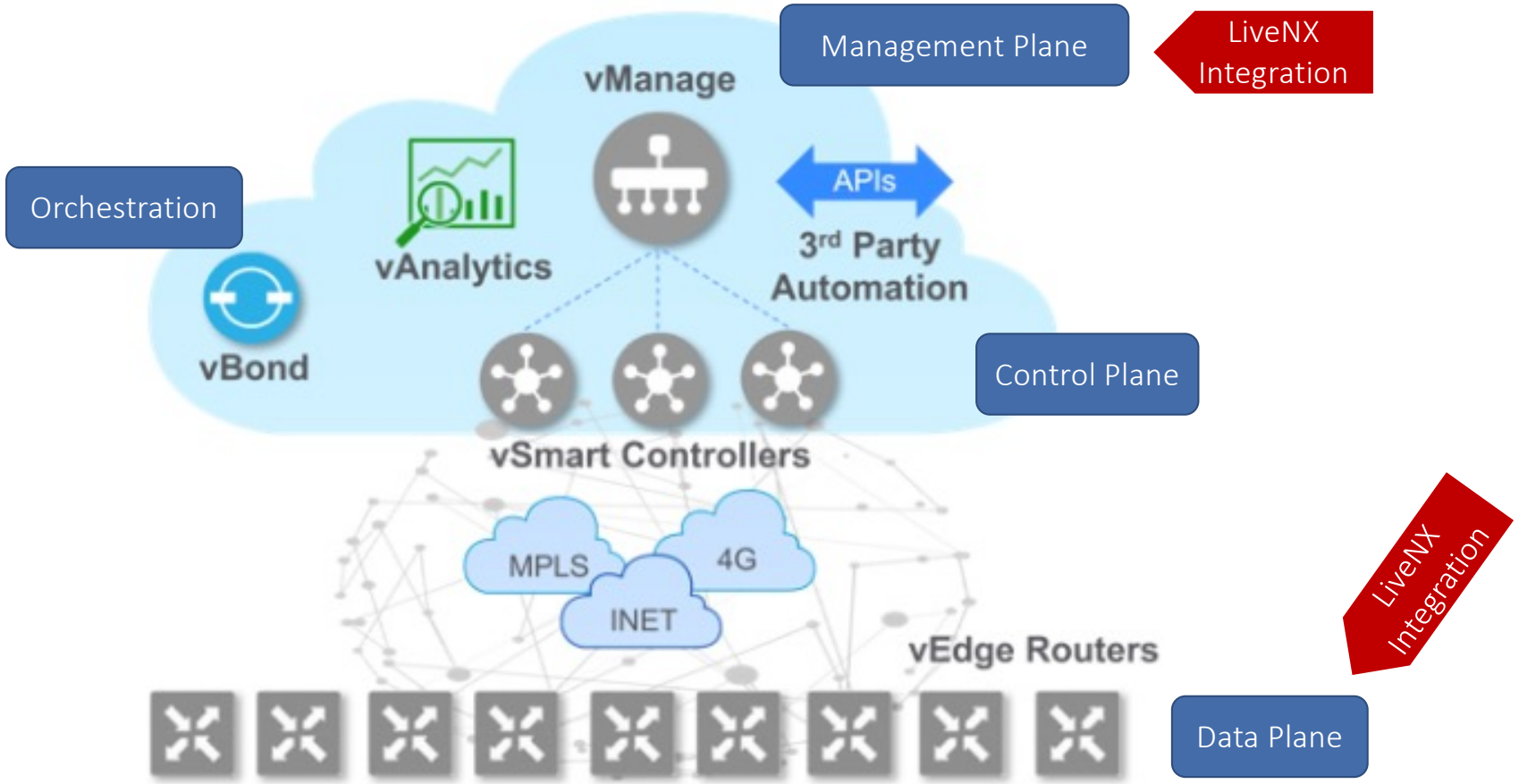
vSmart – SDWAN Controller

LiveAction®

SDWAN Basics



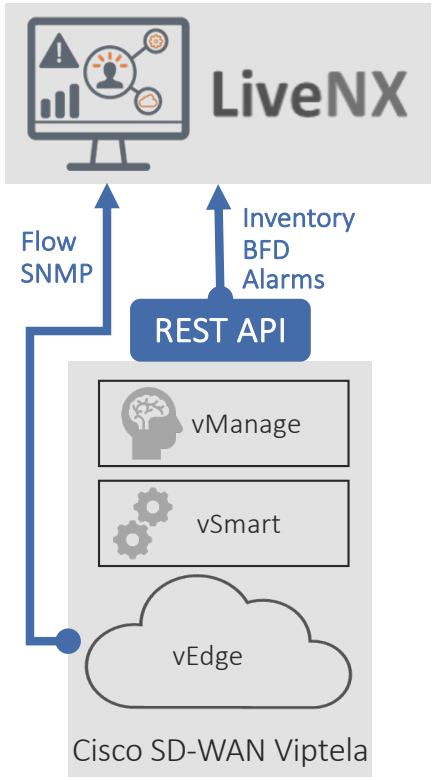
SDWAN Basics



SDWAN Integration Overview

LiveAction™

LiveNX and Cisco SD-WAN Viptela Overview



LiveNX receives data from the vEdges and vManage

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

[1] Bidirectional Forwarding Detection

Network Preparation - Summary

Required Tasks

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

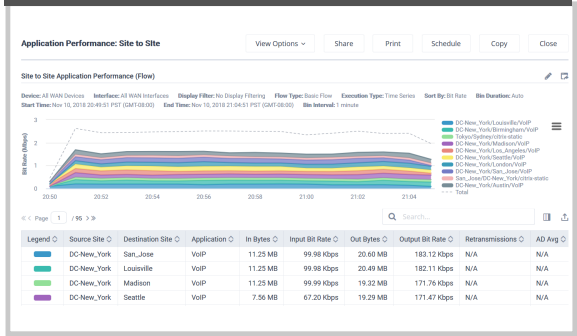
Day 0

Cisco SD WAN Planning for Deployment

LiveAction™

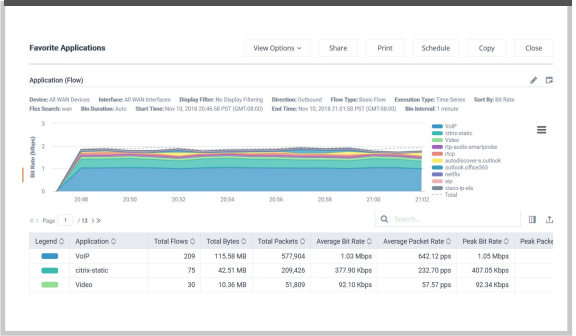
Day 0: Design Baseline performance for policy design

Site to site traffic performance



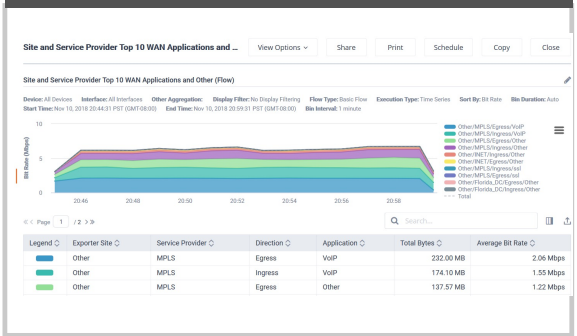
- Site to site traffic type and paths
- Provides data for:
  - Selection of initial pilot sites
  - Usage patterns
  - Site to site traffic behaviors

App group behavior



- App Group behavior
- Policy design inputs:
  - App consumption patterns – bandwidth, class
  - Performance baseline – know targets for SLAs

Service Provider analysis



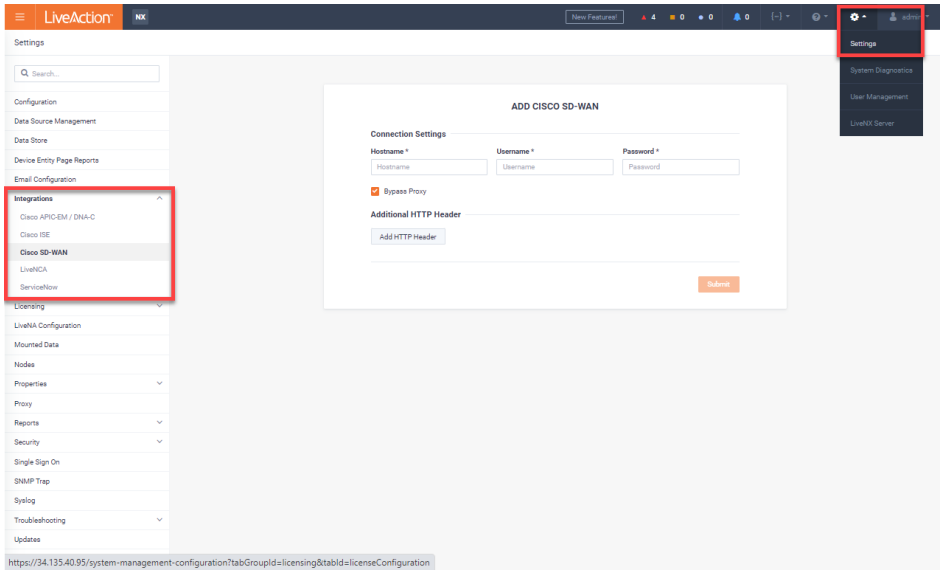
- Service Provider
- Path design inputs:
  - Which telco infrastructure path they should apps take, site by site.
  - Picking application to include in app route policies
  - How SD-WAN enabled vs non SD-WAN traffic maybe handled during deployment

LiveAction®

LiveNX SD-WAN On-Boarding

Required Tasks

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



Day 1

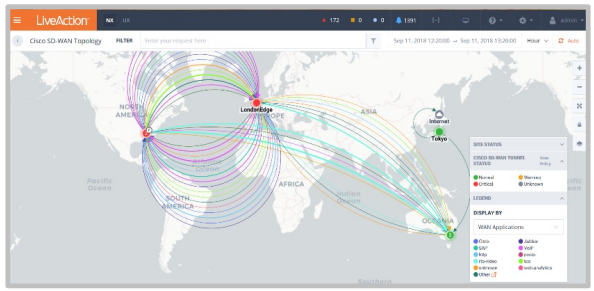
Policy verification at scale

LiveAction™

Day 1: Verify

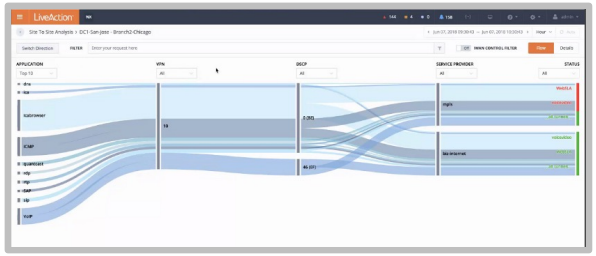
Policy verification at scale

Overlay performance



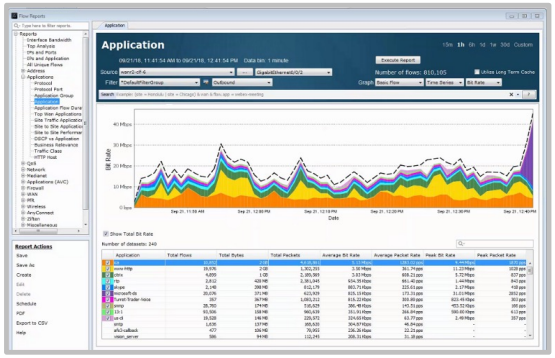
- Transport view
- Geo map
  - Quickly verify site to site behavior during deployment
- Verify the overlay performance:
  - Verify service VPN topology matches the intent set via policy
  - Verify service provider performance
  - Traffic engineering / paths

Policy performance



- Virtual overlay view
- Site to Site diagram - Verify legacy and SD-WAN controlled traffic behavior
- Verify policy enforcement:
  - Verify application and user traffic is associated to correct service VPN
  - Verify split handling of legacy traffic and SD-WAN traffic

Application performance

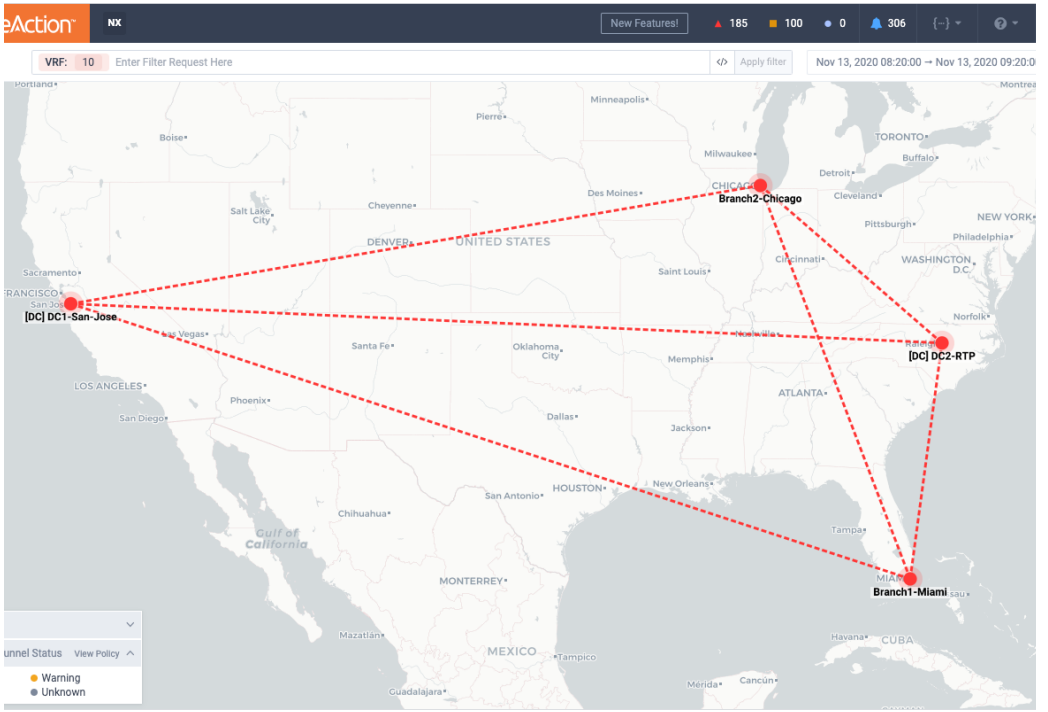


- Custom Reports
- Verify vEdge or cEdge transport VPN connecting to SP network and performance
- In/Out bound resource allocation
  - Bandwidth
  - Latency, jitter, packet drops

LiveAction®

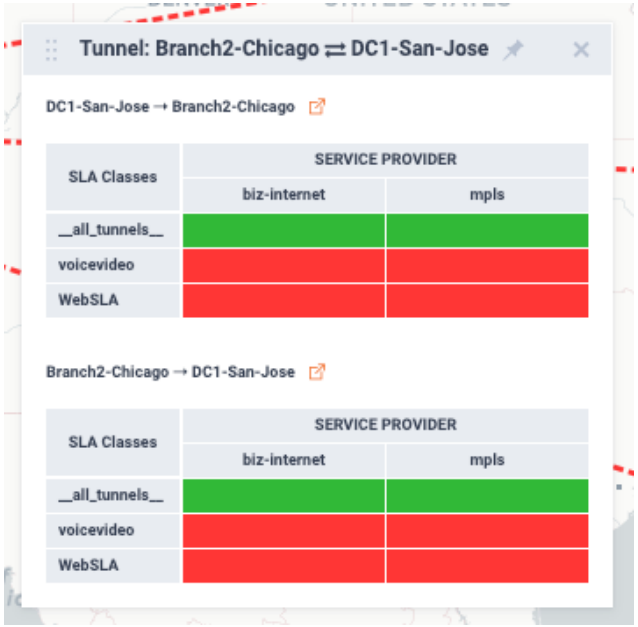
Verify that your control policy is working as intended

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



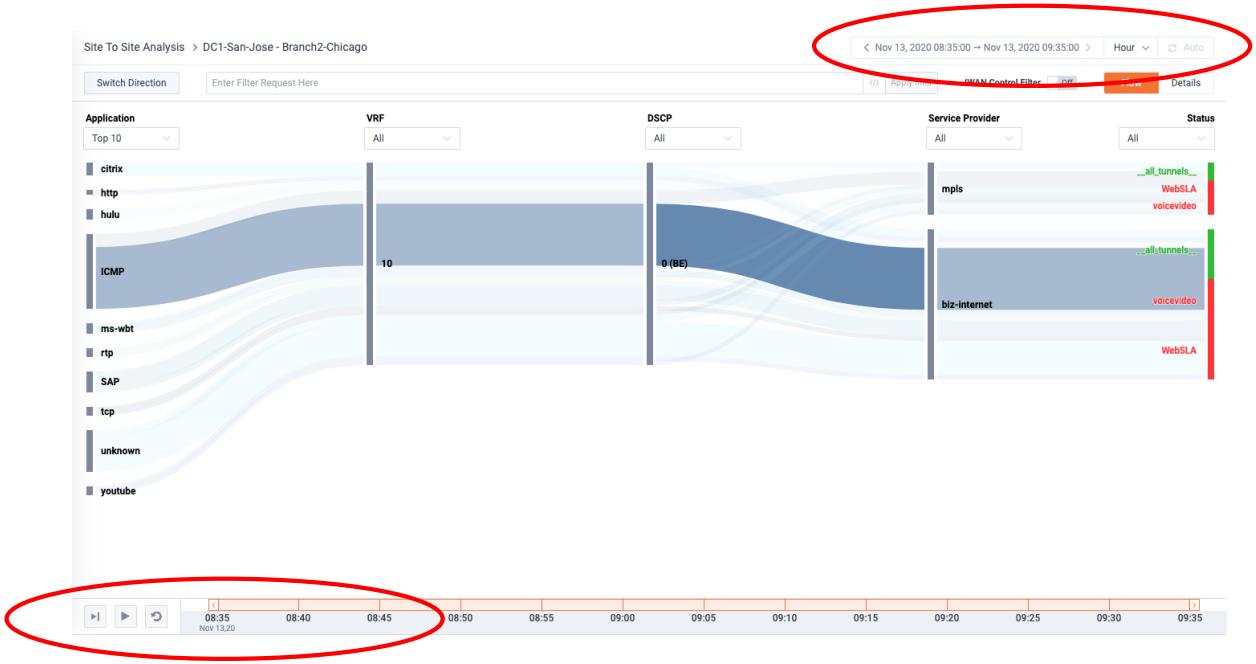
Verify Application Aware Routing Policy

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



Use the Playback feature to verify traffic steering

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



Day 2

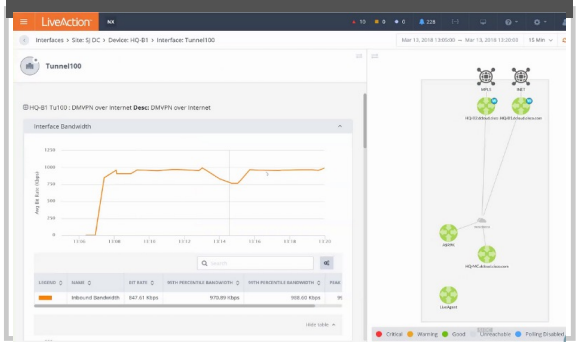
Scale and Operate

LiveAction™

Day 2: Scale and Operate

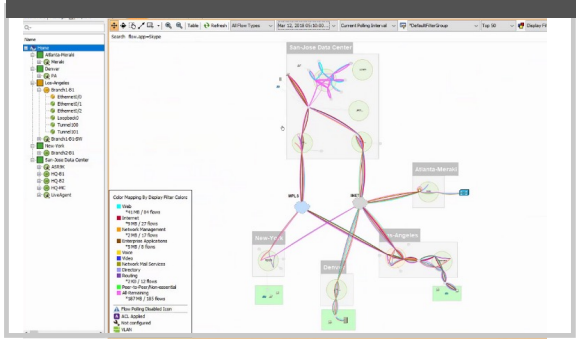
Performance insights for optimization and rapid troubleshooting

Enterprise visibility



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

Flow Path analysis



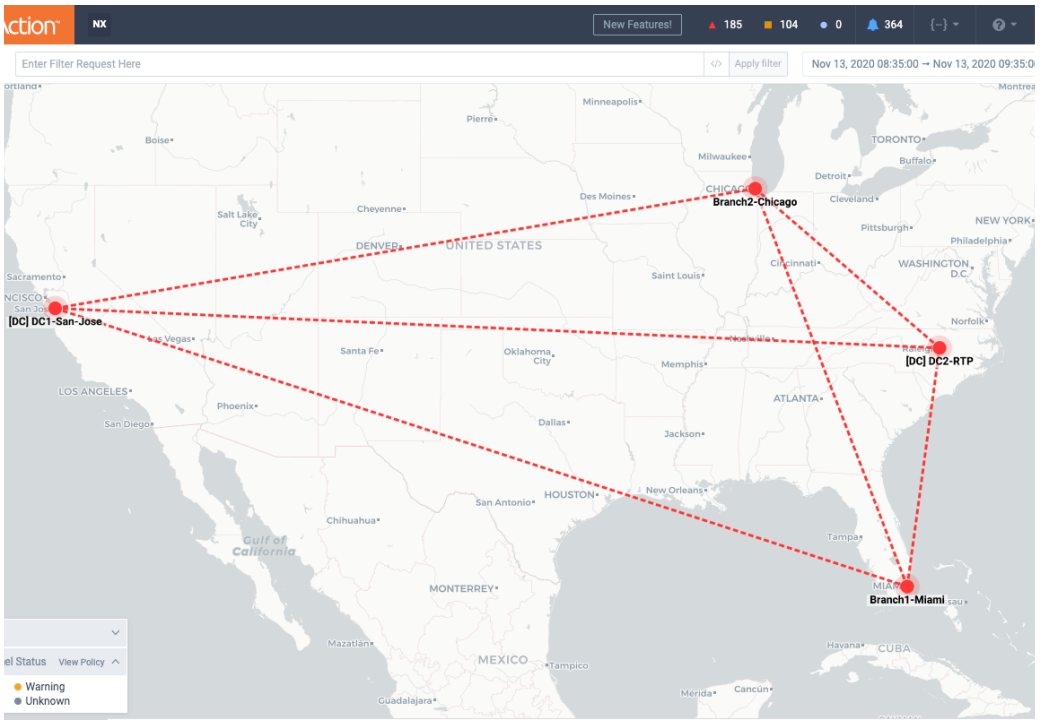
- Visual path analytics
- Verification of policy changes at scale
- Understand app path switching
  - site to site tunnel performance correlated to service provider and policy thresholds

Deep packet analysis

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

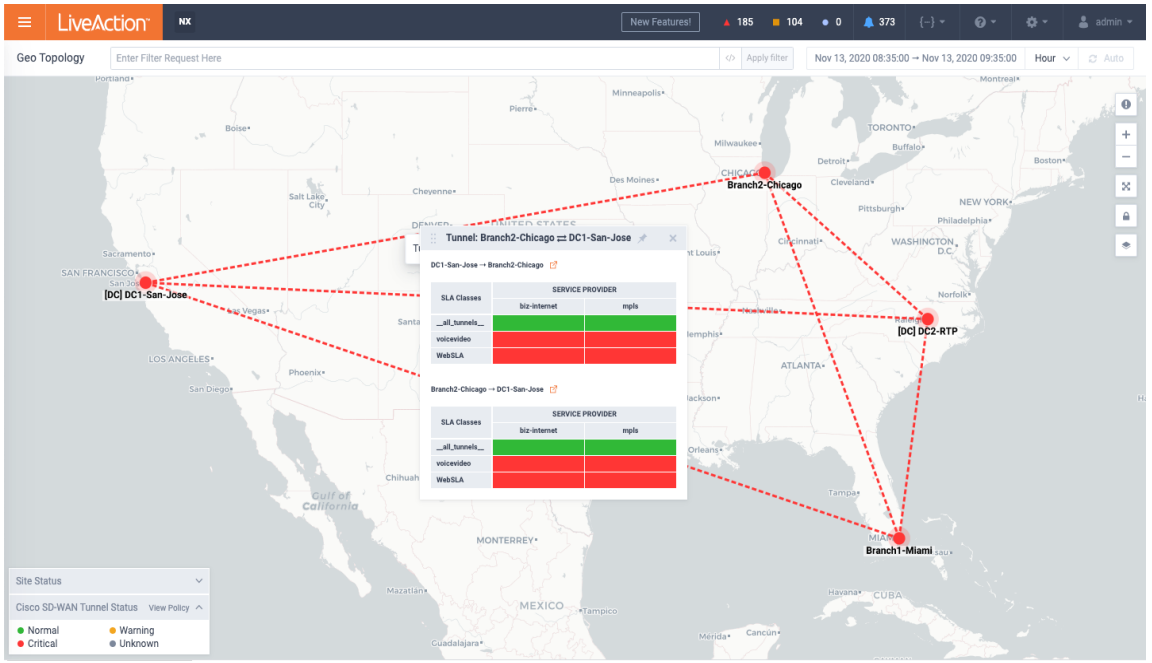
Use the Geo Topology to monitor tunnel status

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



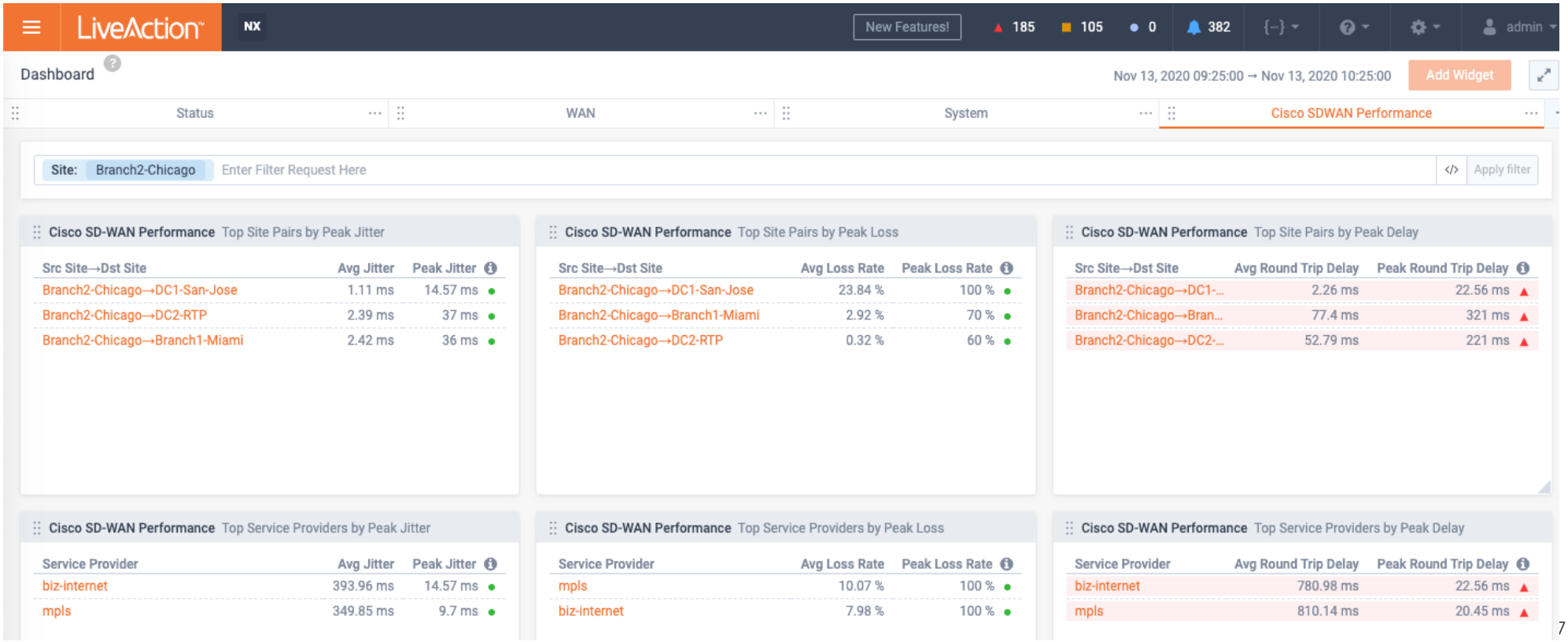
Use the Geo Topology to monitor tunnel status

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

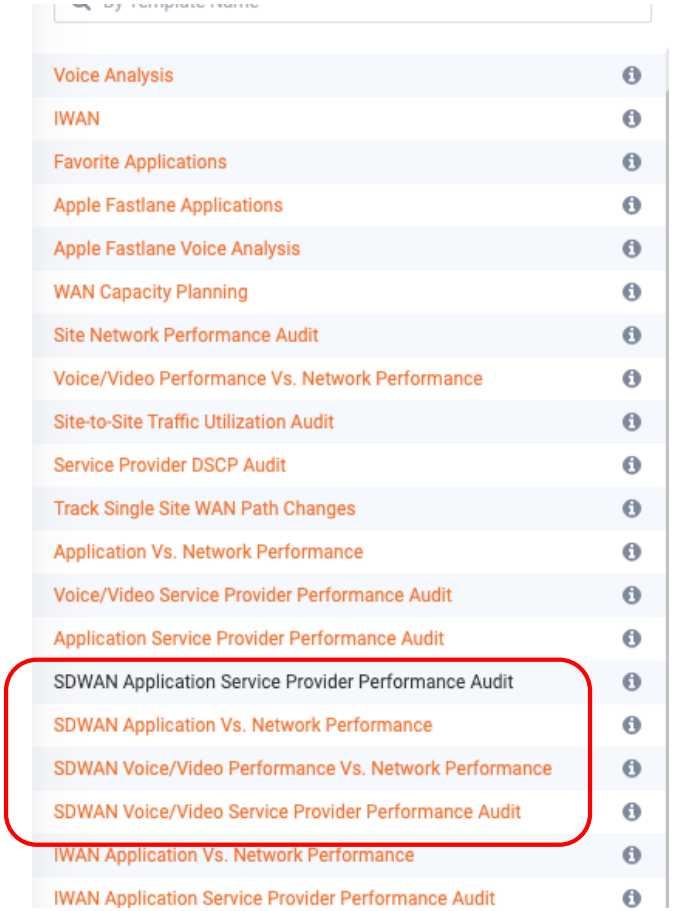


Cisco SDWAN Performance Dashboard

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

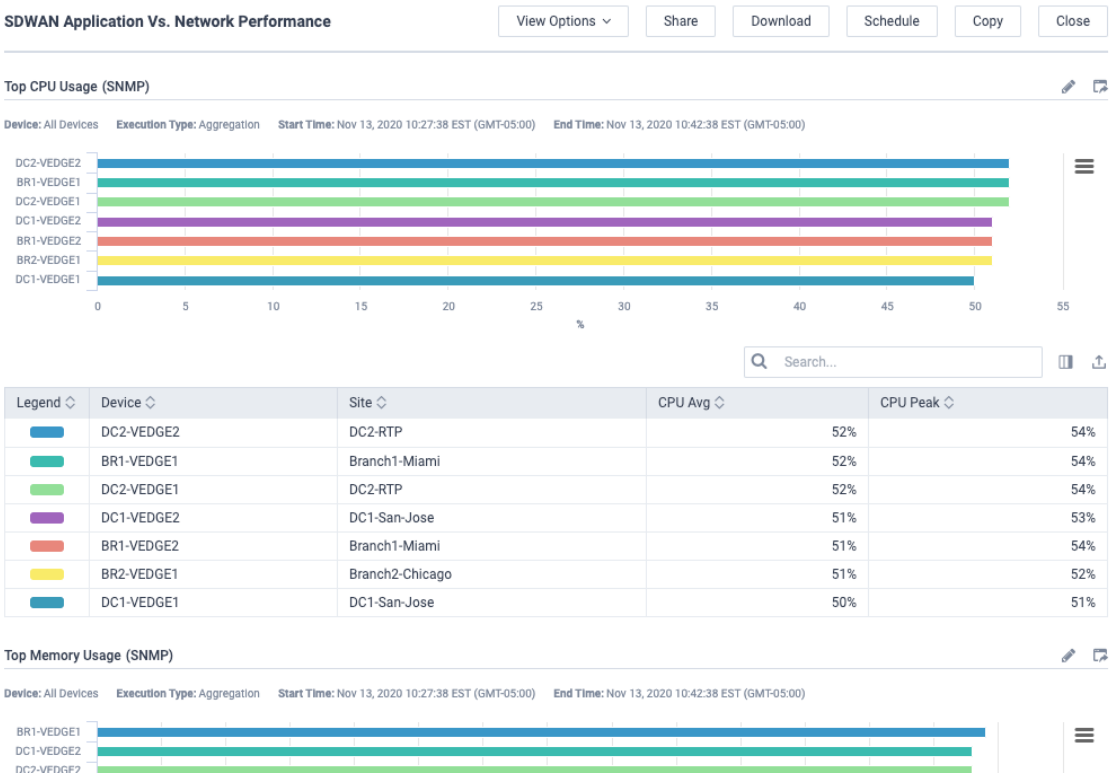


There are also pre-configured SDWAN report templates



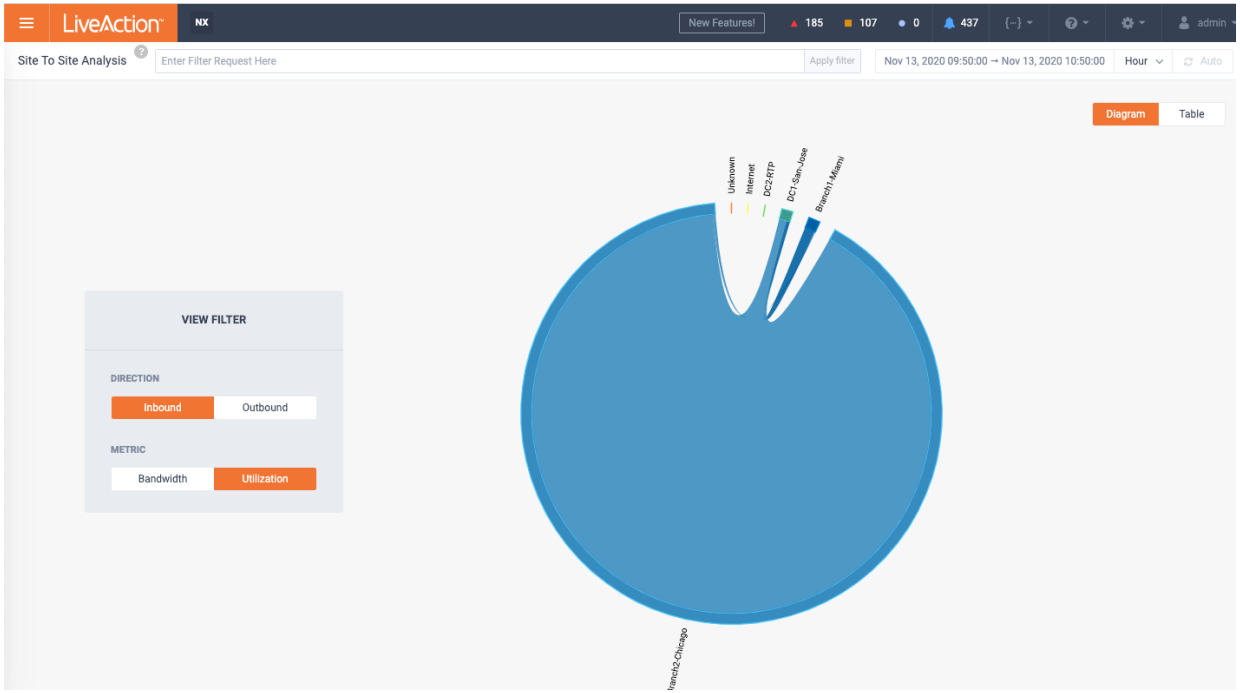
SDWAN Application Vs. Network Performance

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



Site To Site Analysis Story

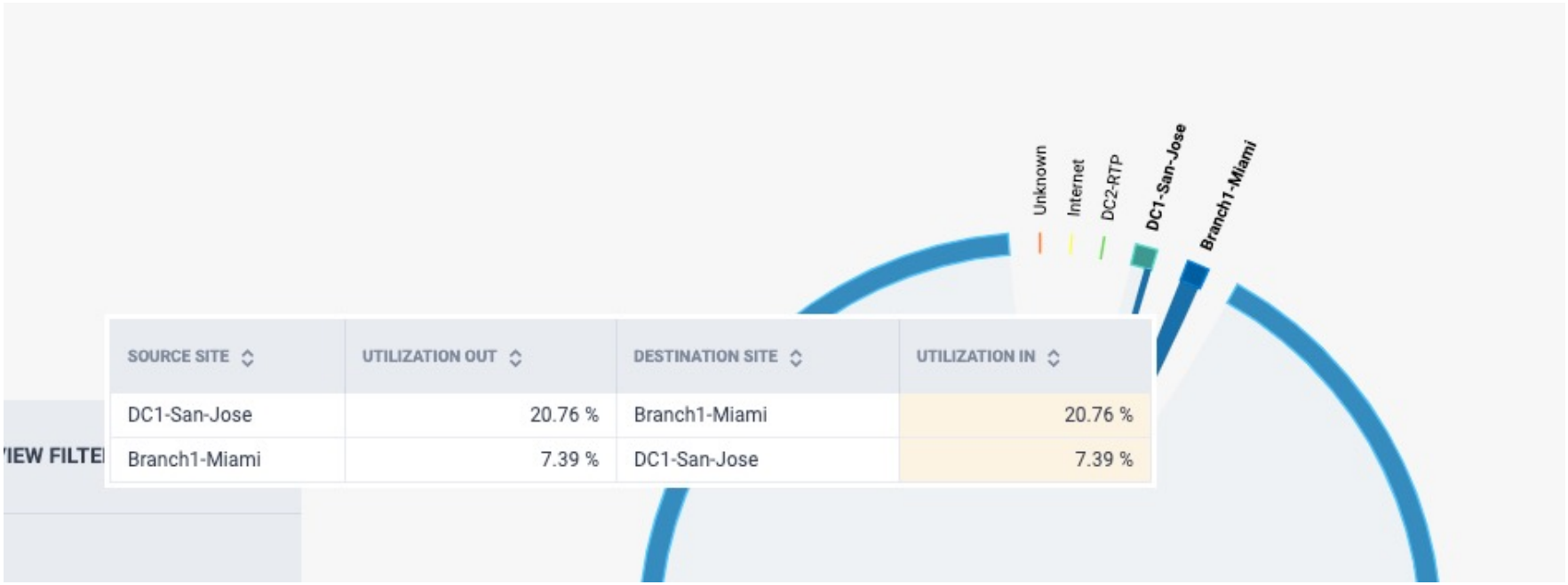
Quick view of traffic between sites



Site To Site Analysis Story

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

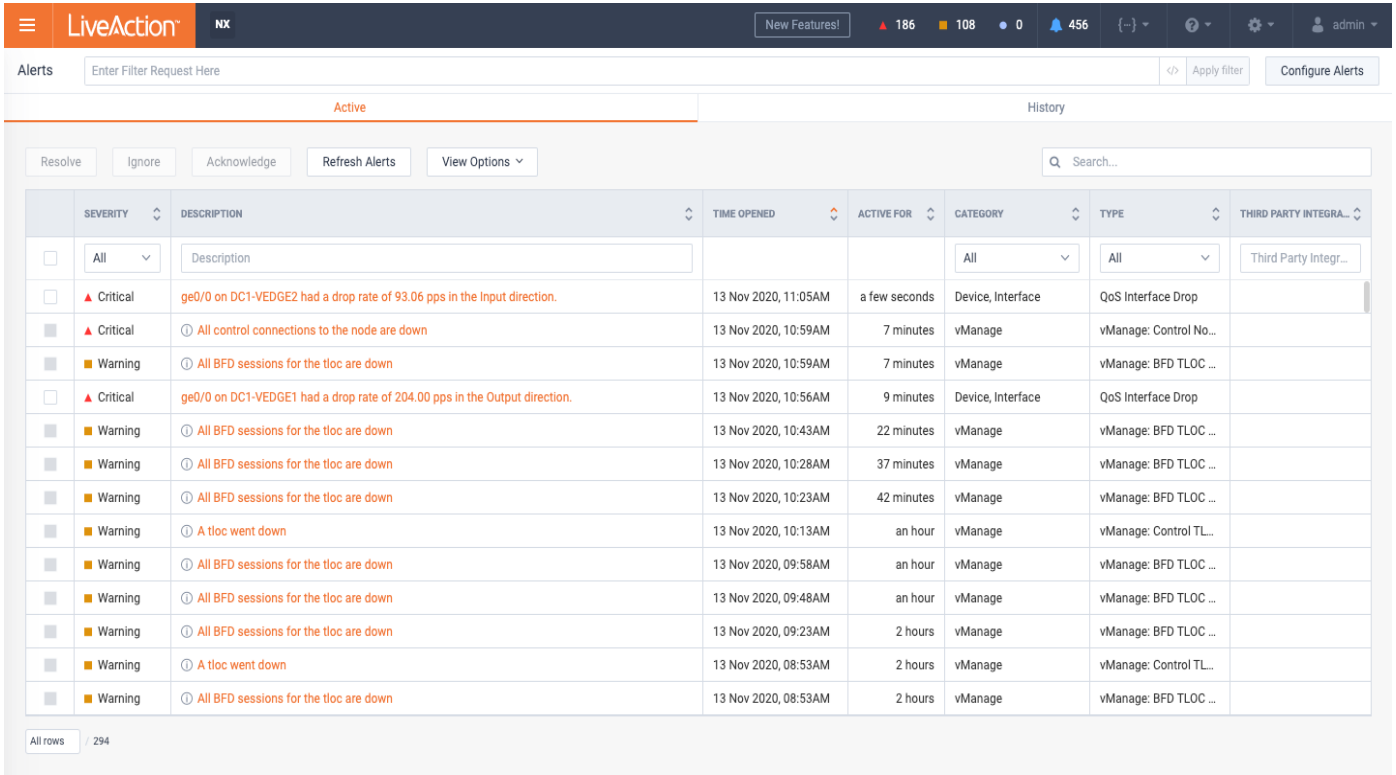
Clicking on a site will launch the Sankey Diagram of all traffic for that site



SOURCE SITE	UTILIZATION OUT	DESTINATION SITE	UTILIZATION IN
DC1-San-Jose	20.76 %	Branch1-Miami	20.76 %
Branch1-Miami	7.39 %	DC1-San-Jose	7.39 %

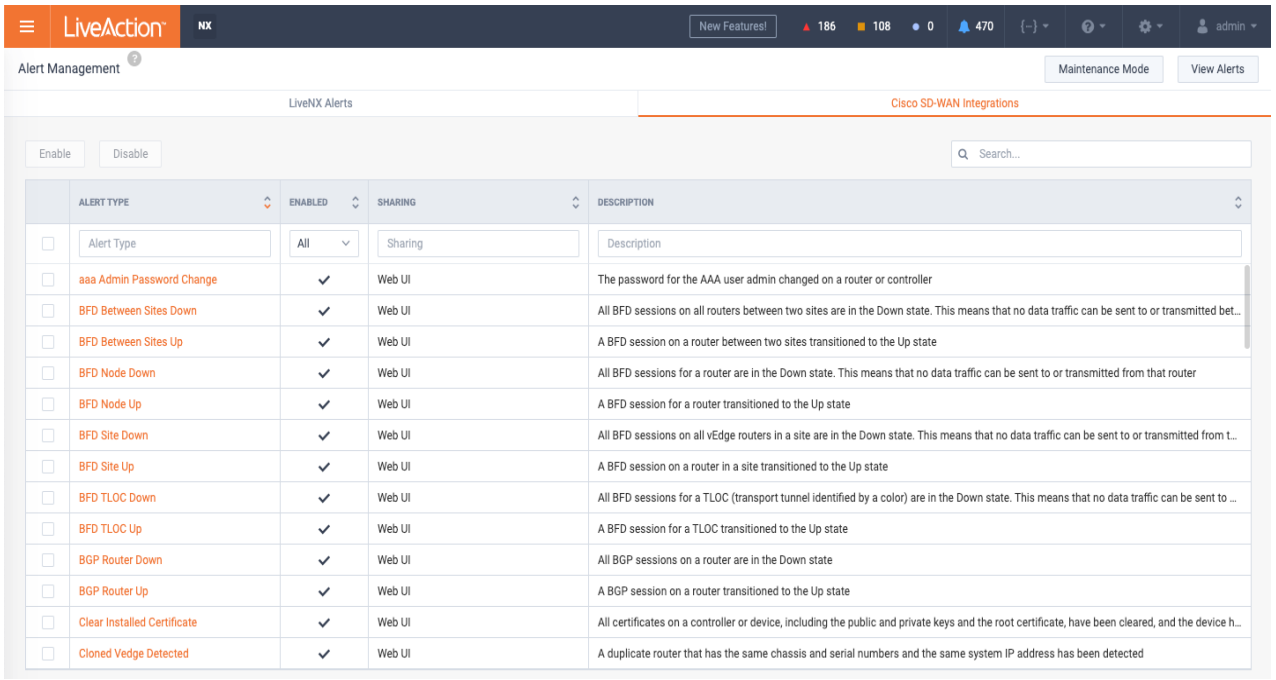
Alerting

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



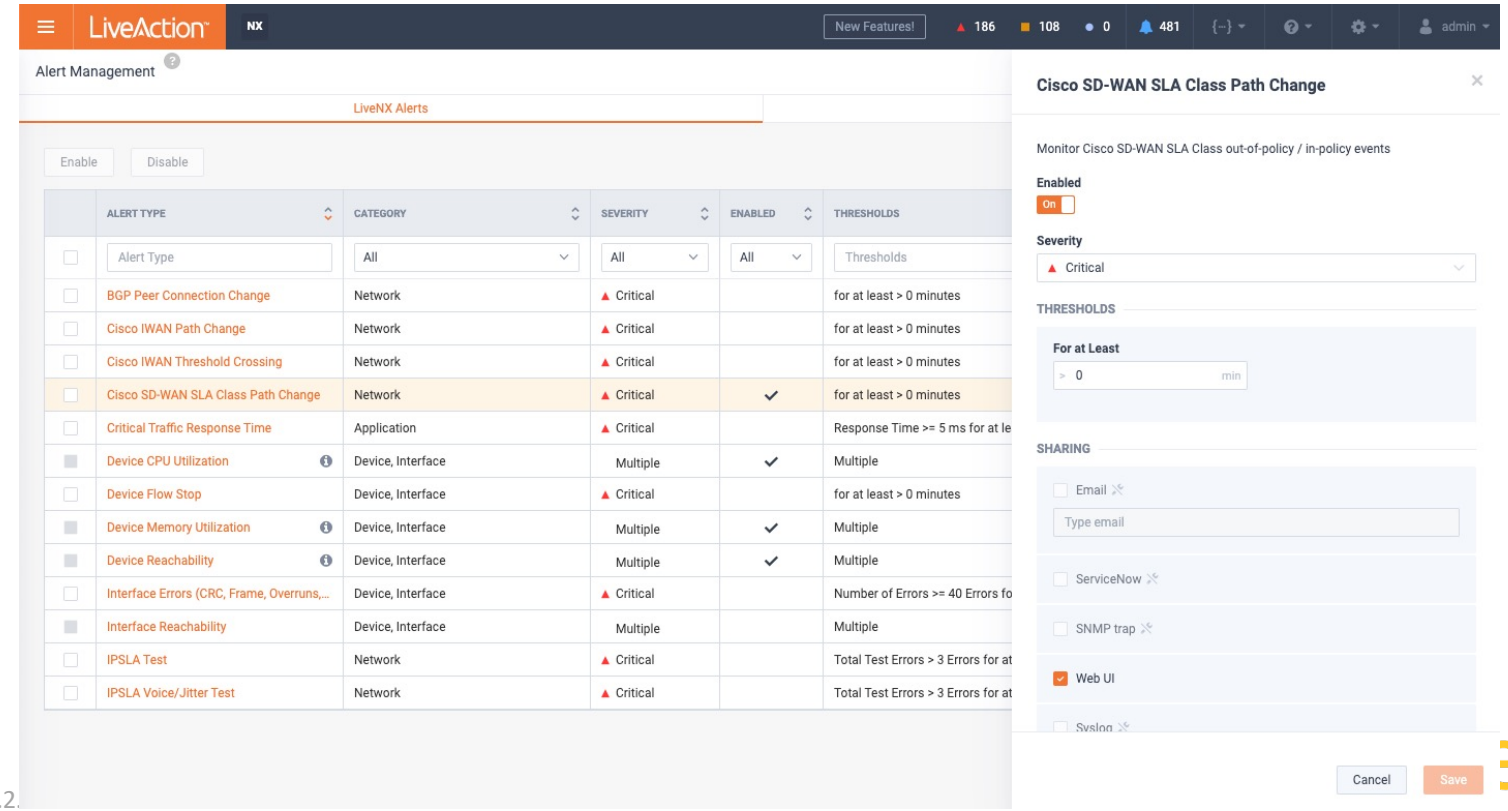
Alert Configuration

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



Cisco SD-WAN SLA Class Path Change Alert

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



Launch the SDWAN Learning Labs…

LiveAction®

Wrap-Up

LiveAction™

LiveAction Support

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

Training Resources

You will get these resources in an email

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

Course Evaluation

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

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

https://survey.alchemer.com/s3/6997006/LiveAction-Training-Survey

Thank You in advance for your participation!

Thank You!

LiveAction™