



# LiveNX Training

Day 1

© 2022, LiveAction, Inc. All Rights Reserved.

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?

A woman with long brown hair, wearing a white button-down shirt, is looking upwards and to the right with a thoughtful expression, her hand resting on her chin. The background is a dark, textured surface, possibly a chalkboard, with a white maze drawn on it. Several arrows are drawn on the maze, pointing in different directions. An orange rectangular overlay is positioned on the left side of the image, containing the text 'LiveNX' and 'Lab Preparation'.

# LiveNX

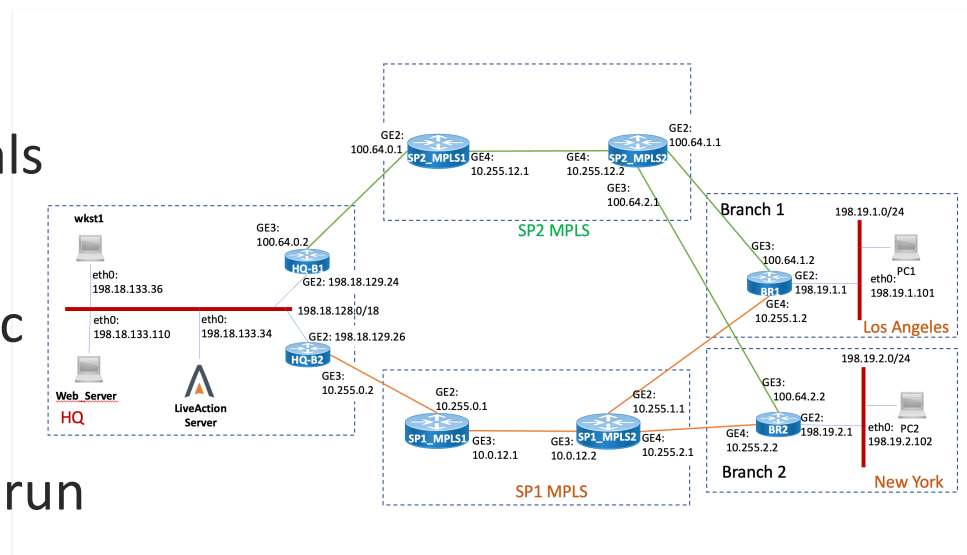
Lab Preparation

© 2022, LiveAction, Inc. All Rights Reserved.

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

CRITERION NETWORKS

← Back

LiveNX Flow Foundation - 2022

0%

Queued Spawning Provisioning Stabilizing Ready

Learning menu

Overview

Lab Introduction

Topology

Access Devices

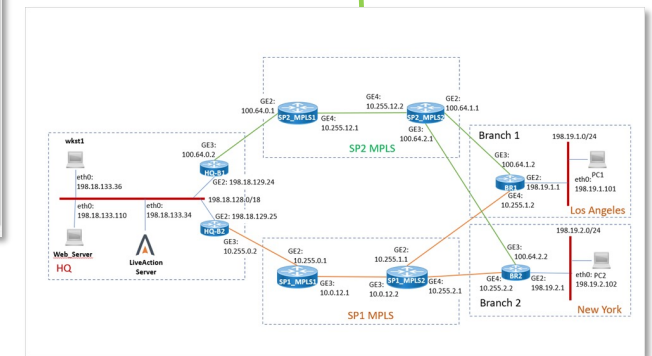
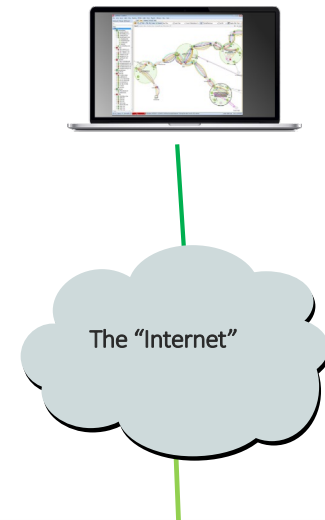
Statistics

Sl No	Role	Hostname	Username	Password	IP Address	Port
1	LiveNX Server	livenx	admin	Student	35.226.145.33	443 or 7000
2	B1-HQ	HQ-B1	admin	Cisco12345	35.226.145.33	20152
3	SP2_MPLS1	SP2_MPLS1	admin	Cisco12345	35.226.145.33	20153
4	SP2_MPLS2	SP2_MPLS2	admin	Cisco12345	35.226.145.33	20155
5	BR1	Branch1-LA	admin	Cisco12345	35.226.145.33	20160
6	B2-HQ	HQ-B2	admin	Cisco12345	35.226.145.33	20157
7	SP1_MPLS1	SP1_MPLS1	admin	Cisco12345	35.226.145.33	20158
8	SP1_MPLS2	SP1_MPLS2	admin	Cisco12345	35.226.145.33	20159
9	BR2	Branch2-NY	admin	Cisco12345	35.226.145.33	20161
10	wkst1	Administrator	Administrator	Cisco12345	35.226.145.33	20201
11	ActiveDirectory	Administrator	Administrator	Cisco12345	35.226.145.33	20202
12	PC1	Administrator	Administrator	Cisco12345	35.226.145.33	20203
13	PC2	Administrator	Administrator	Cisco12345	35.226.145.33	20204

+ Add Hours

Terminate

Prev



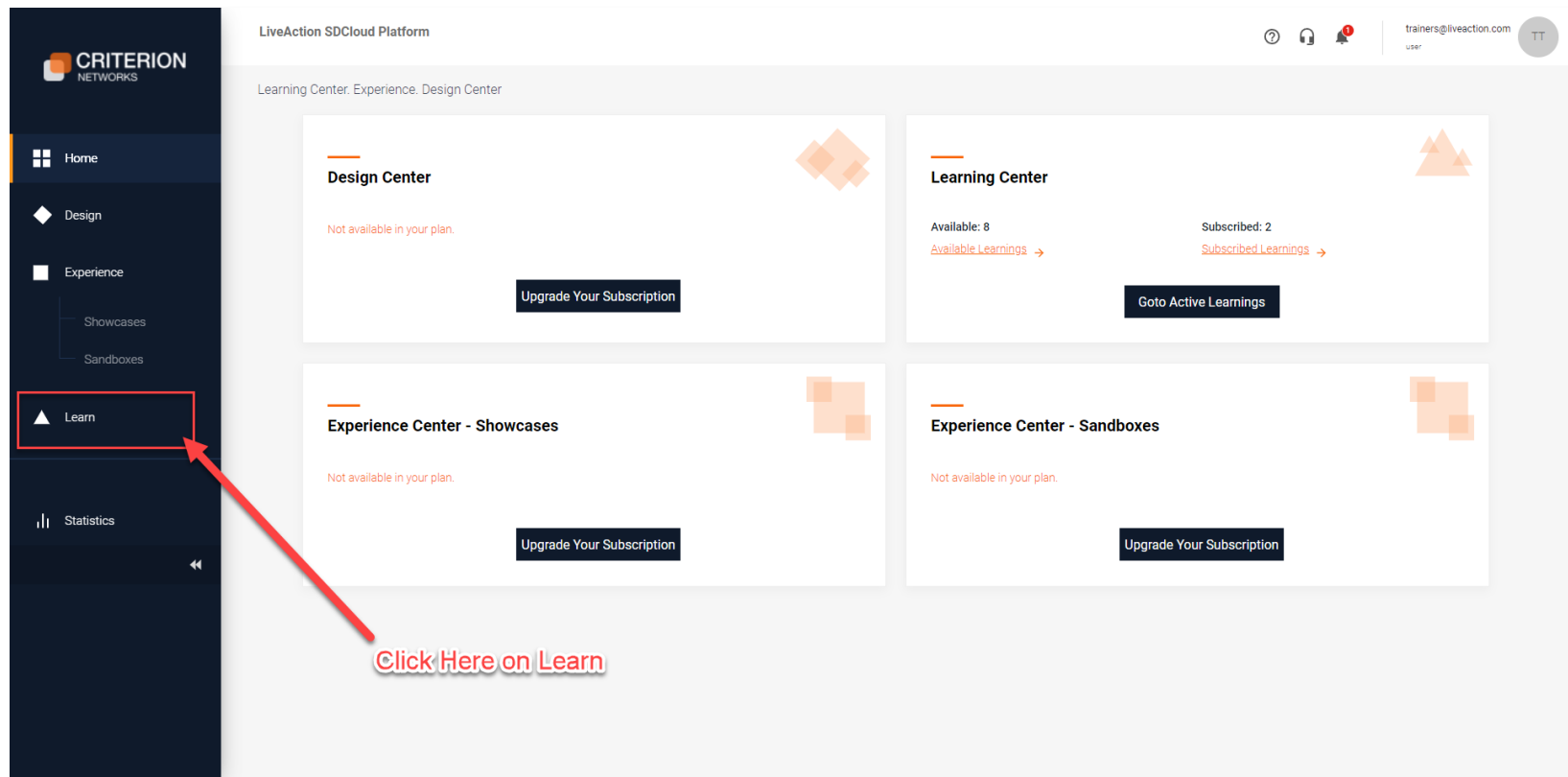
LiveAction®



# Criterion Labs Log On Screen

The image displays the Criterion Networks login interface and its underlying architecture. On the left, the login screen features the Criterion Networks logo, a username field (containing 'user1\_47971562'), a password field, and a checkbox for 'I agree to Terms-of-Service and Privacy Policy of Criterion Networks'. Below these are 'Login' and 'SSO Login' buttons, along with links for 'Sign up here if you have an invite code' and 'Forgot password?'. Red annotations highlight the username/password fields with the text 'Enter your username and password here' and the terms of service checkbox with 'Don't forget to check the Terms of Service box'. On the right, a diagram illustrates the Criterion SDCloud architecture, showing three centers (Design Center, Experience Center, and Learning Center) connected via dashed lines to a central cloud labeled 'Criterion SDCloud®'. The Design Center is connected to a 'Service Provider' cloud, while the Experience Center and Learning Center are connected to an 'Enterprise' cloud.

# Click Learn



Click Here on Learn

# Click Subscribed

The screenshot displays the LiveAction Learning Center interface. On the left is a dark blue sidebar with the 'CRITERION NETWORKS' logo and navigation links: Home, Design, Experience (with sub-links Showcases and Sandboxes), Learn (highlighted with an orange bar), and Statistics. The main content area is titled 'Learning Center' and features a top navigation bar with tabs: Available, Subscribed (highlighted with a red box and a red arrow pointing to it), Active, and Scheduled. Below the tabs is a search bar and two filter buttons: 'All' and 'Others'. The main content area lists three lab entries:

- LIVENX AND CISCO SDWAN INTEGRATION V9.3**: This lab would provide an overview of LiveNX monitoring tool integration with Cisco SDWAN. Though a mix of exercises in this lab, we would run through the setup, integration and necessary steps to integrate Cisco SDWAN setup in the LiveNX monitoring tool. **Note:** For best results, please use **Chrome, Firefox, or Safari** to run this lab. Lab Run Time: 4 Hours | Available Tries: 1. [Schedule](#) [Launch Now](#)
- LIVENX FLOW FOUNDATIONS 2022**: In this lab we will learn how to use **LiveAction** network monitoring and management tools for NetOps professionals in complex network environments. **Note:** For best results, please use **Chrome, Firefox, or Safari** to run this lab. Lab Run Time: 48 Hours | Available Tries: 1. [Schedule](#) [Launch Now](#)
- LIVEACTION BASIC USER LIVENX V9.3**: This lab would provide an overview of **LiveNX** monitoring tool, integrated with a network setup in a LAB environment, from a basic users perspective. Through a mix of exercises in this lab, we would run through the setup and understand how to use the tool for monitoring the enterprise network, readin... [Show more](#) Lab Run Time: 4 Hours | Available Tries: 0. [Schedule](#) [Launch Now](#)
- LIVENX ADMIN USER LAB - LIVENXV9.3**

A red arrow points from the 'Subscribed' tab to the first lab entry, with the text 'Next Click on Subscribed' written in red above it.

# Select the Correct Lab and Click Launch Now

The screenshot shows the LiveAction Learning Center interface. On the left is a dark sidebar with the Criterion Networks logo and navigation links: Home, Design, Experience (with sub-links Showcases and Sandboxes), Learn, and Statistics. The main content area is titled 'Learning Center' and has tabs for Available, Subscribed (active), Active, and Scheduled. At the top right of the main area are icons for help, audio, and notifications, along with a user profile for 'klawton@liveaction.com'. Below the tabs is a search bar and filters for 'All' and 'Others'. Two lab cards are displayed. The first card is 'LIVENX AND CISCO SDWAN INTEGRATION V9.3' with a description, a note about browser requirements, and a 'Launch Now' button. The second card is 'LIVENX FLOW FOUNDATIONS', which is highlighted with a red box. A red arrow points from the text 'Ensure you Launch the LiveNX Flow Foundations Lab' to the 'Launch Now' button of this card. The 'Launch Now' button is also highlighted with a red box.

**CRITERION NETWORKS**

Home  
Design  
Experience  
Showcases  
Sandboxes  
Learn  
Statistics

Learning Center

Available Subscribed Active Scheduled

Search

All Others

**LIVENX AND CISCO SDWAN INTEGRATION V9.3**

This lab would provide an overview of LiveNX monitoring tool integration with Cisco SDWAN. Though a mix of exercises in this lab, we would run through the setup, integration and necessary steps to integrate Cisco SDWAN setup in the LiveNX monitoring tool.

**Note:** For best results, please use **Chrome, Firefox, or Safari** to run this lab.

Lab Run Time : 4 Hours | Available Tries : 1

Schedule Launch Now

**LIVENX FLOW FOUNDATIONS**

In this lab we will learn how to use LiveAction network monitoring and management tools for NetOps professionals in complex network environments

**Note:** For best results, please use **Chrome, Firefox, or Safari** to run this lab.

Lab Run Time : 48 Hours | Available Tries : 1

Schedule Launch Now

**Click Launch Now**

**Ensure you Launch the LiveNX Flow Foundations Lab**



# Click Provision

Launch learning lab

Please fill the details

Name

LiveNX Flow Foundation - 2022

Number of Hours

48

End action

☐ Suspend ☒ Terminate

Provision

No changes needed

Click Provision

# Your Lab Should Begin Start-Up

Learning Center

CRITERION NETWORKS

Home

Design

Experience

Learn

Statistics

Back

LiveNX Flow Foundation

0%

Queued Spawning Provisioning Stabilizing Ready

Overview

Overview

The objective of this lab is to introduce you to LiveAction network monitoring and management tools

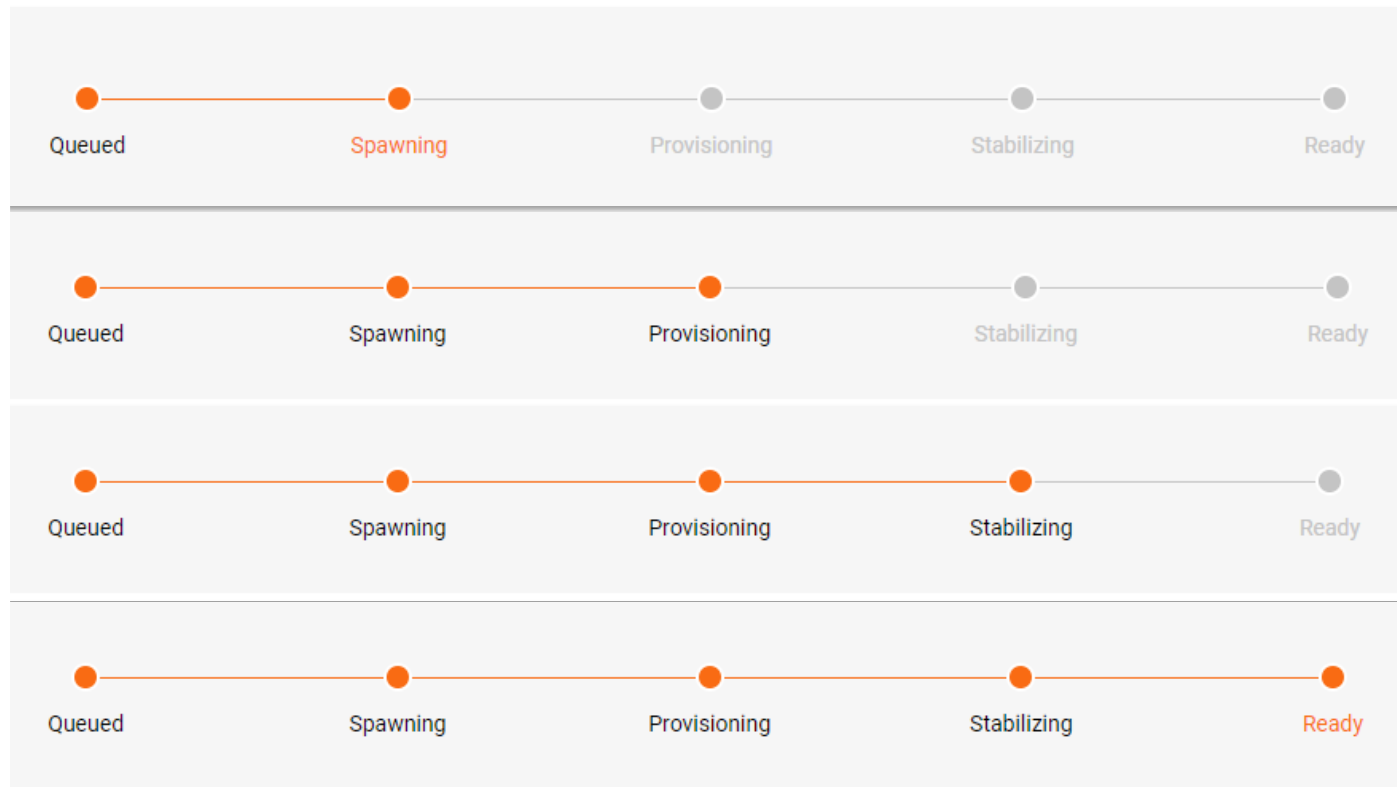
Next

+ Add Hours

Your Lab will begin the start-up process

Let your instructor know your lab is starting-up

# Start-up Takes Around 5 mins



## Sites Used in This Training Course

Course Component	Site	Description
Student Guide	<a href="https://www.liveaction.com/support/training-resources/">https://www.liveaction.com/support/training-resources/</a>	Your copy of the slides to follow the presentation/make notes
Lab Workbook Pt 1	<a href="https://www.liveaction.com/support/training-resources/">https://www.liveaction.com/support/training-resources/</a>	Day 1 Lab Workbook: Lab Exercises
Lab Workbook Pt 2	<a href="https://www.liveaction.com/support/training-resources/">https://www.liveaction.com/support/training-resources/</a>	Day 2 Lab Workbook: Lab Exercises
LiveNX Engineering Console (Mac or Windows)	<a href="https://www.liveaction.com/support/training-resources/">https://www.liveaction.com/support/training-resources/</a>	Client Access to be installed for some exercises
Website for Access to Hands-On Labs	<a href="https://portal.criterionnetworks.com/">https://portal.criterionnetworks.com/</a>	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...



A man in a dark suit and light-colored shirt is standing on a stage, holding a microphone and gesturing with his left hand towards a large screen. The screen displays a complex network diagram with various shapes like circles, hexagons, and rectangles connected by lines. The audience, seen from behind, is seated in rows of chairs, facing the speaker. The overall scene is brightly lit with a blue and white color scheme.

# LiveNX

## System Overview & Architecture

# 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**

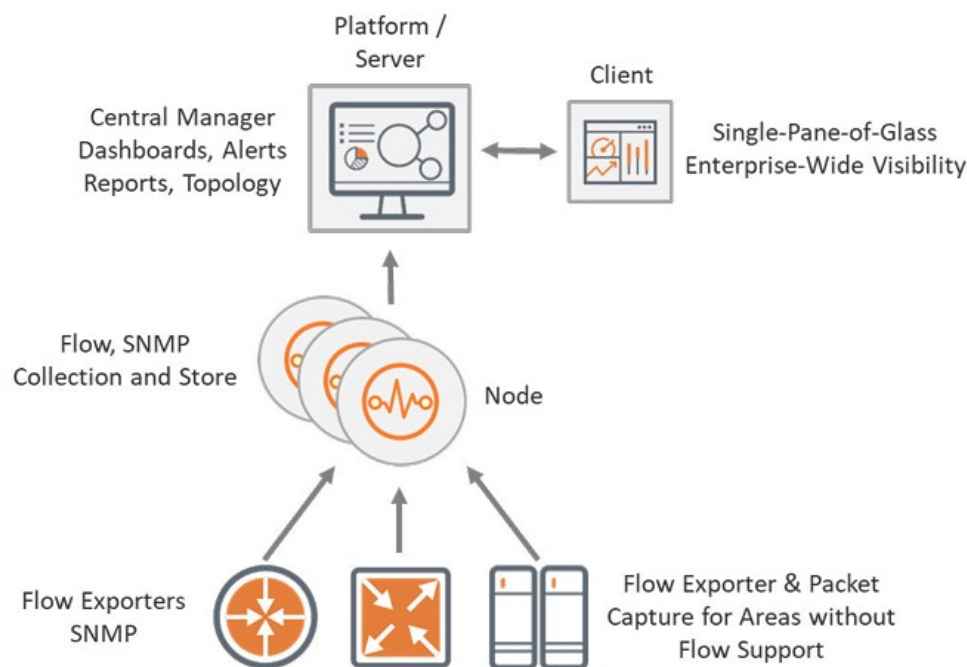
- Single Pane of Glass (SPOG) over entire network
- Limiting user data access by groups per node
- Browser, Windows (32/64-bit), or Mac OSX

- **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: <ul style="list-style-type: none"><li>• 8 vCPU Xeon or i7</li><li>• 16 Gb RAM</li><li>• Max Heap Size 8GB</li><li>• 500GB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 16 vCPU Xeon or i7</li><li>• 32 Gb RAM</li><li>• Max Heap Size 16GB</li><li>• 2TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 16 vCPU Xeon or i7</li><li>• 64 Gb RAM</li><li>• Max Heap Size 31GB</li><li>• 4TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 32 vCPU Xeon or i7</li><li>• 64 Gb RAM</li><li>• Max Heap Size 31GB</li><li>• 8TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 64 vCPU Xeon Gold 5218</li><li>• 768 Gb RAM</li><li>• Max Heap Size 384GB</li><li>• 32TB Data Disk</li><li>(16TB usable with RAID 10)</li></ul>

# 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);

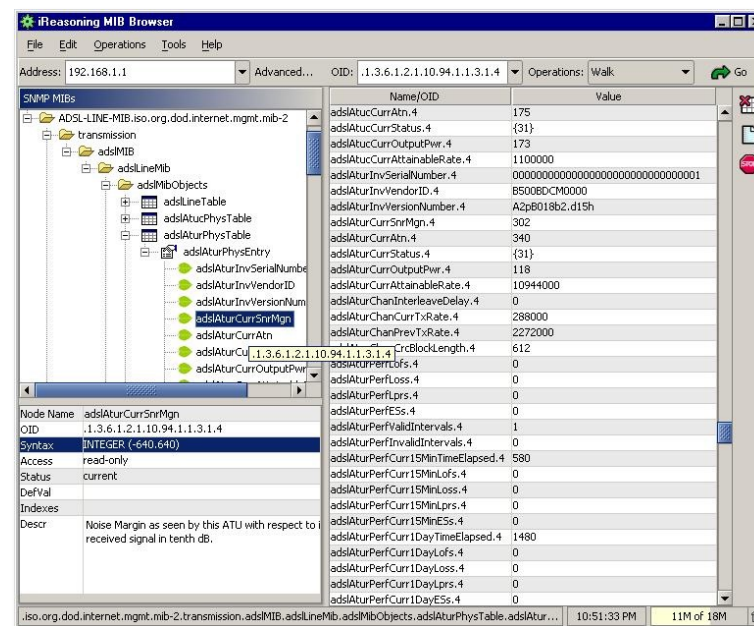
- QoS Configurations
- Netflow Configurations
- IP SLA Configurations
- Policy Based Routing

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

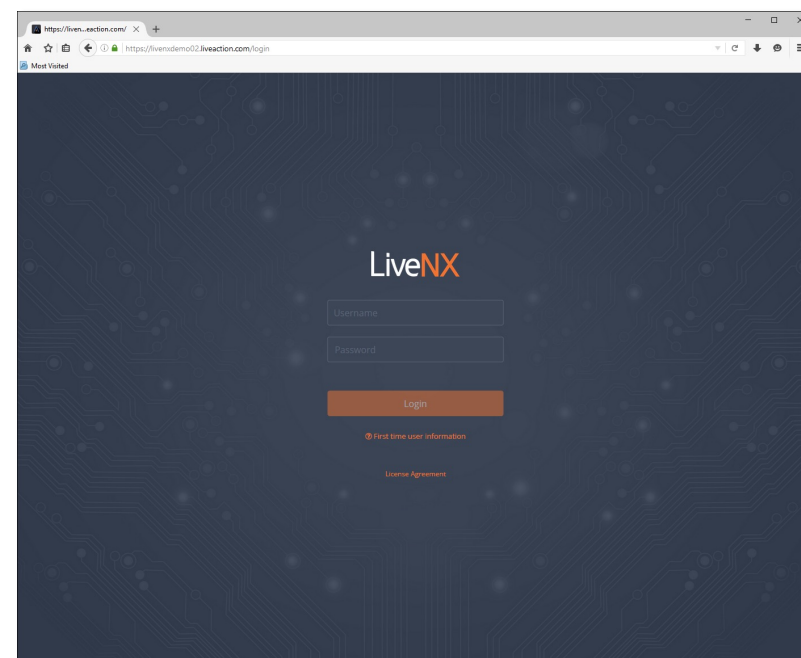
© 2022, LiveAction, Inc. All Rights Reserved.

LiveAction™

# From Any Browser... from Anywhere!

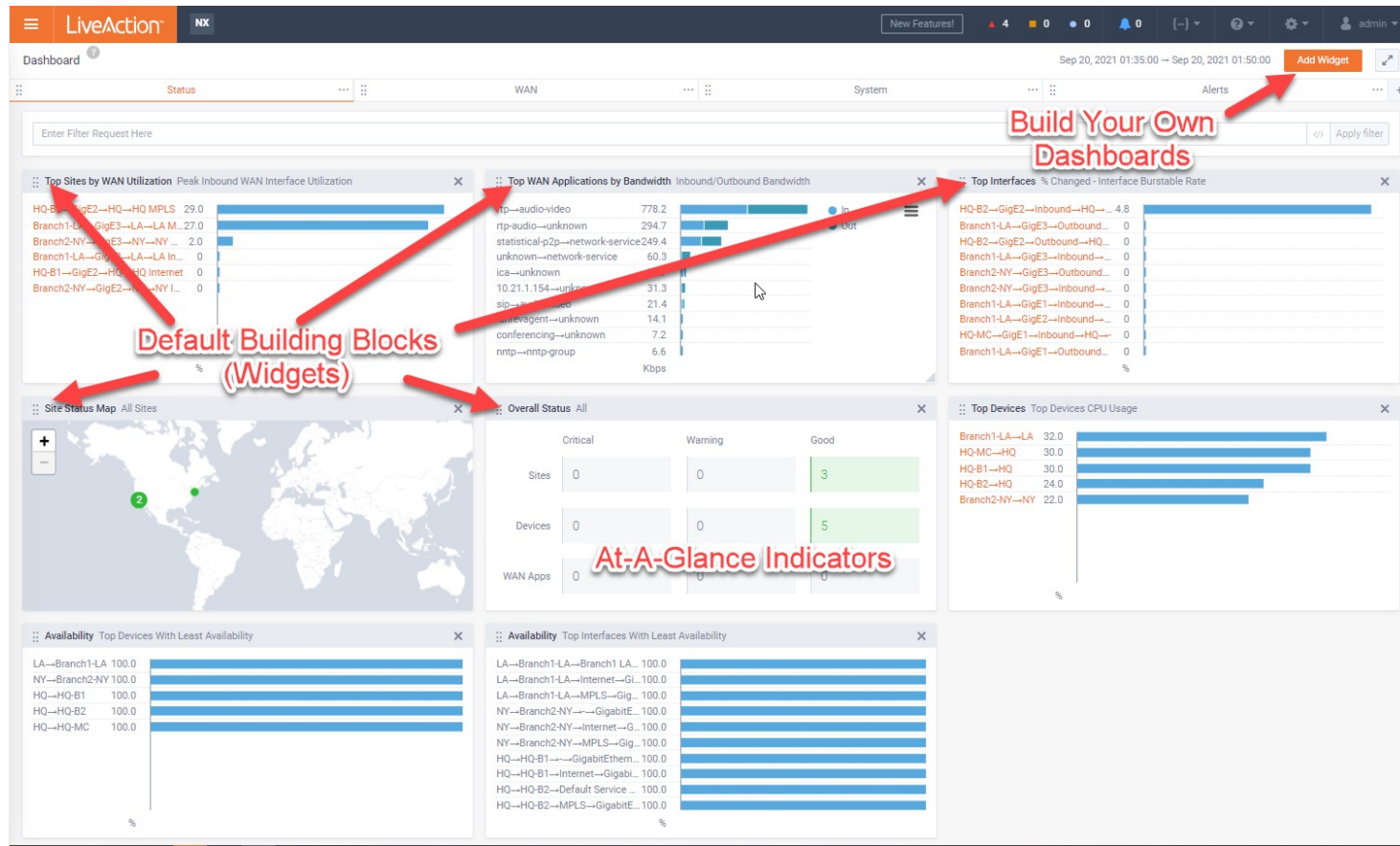
<https://<LiveNXserverIP>>

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



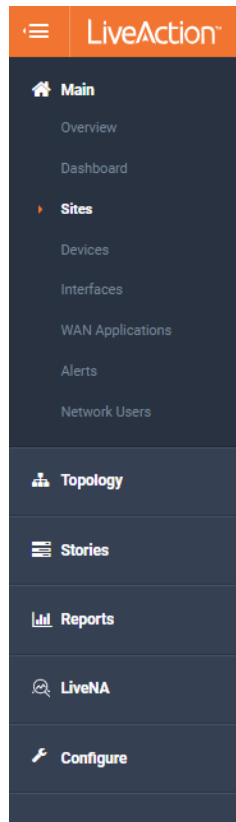
Visualization Philosophy: Shows what you ask it to show

# Customizable Dashboards



# Sites Details

Drill into Sites > Devices > Interfaces...

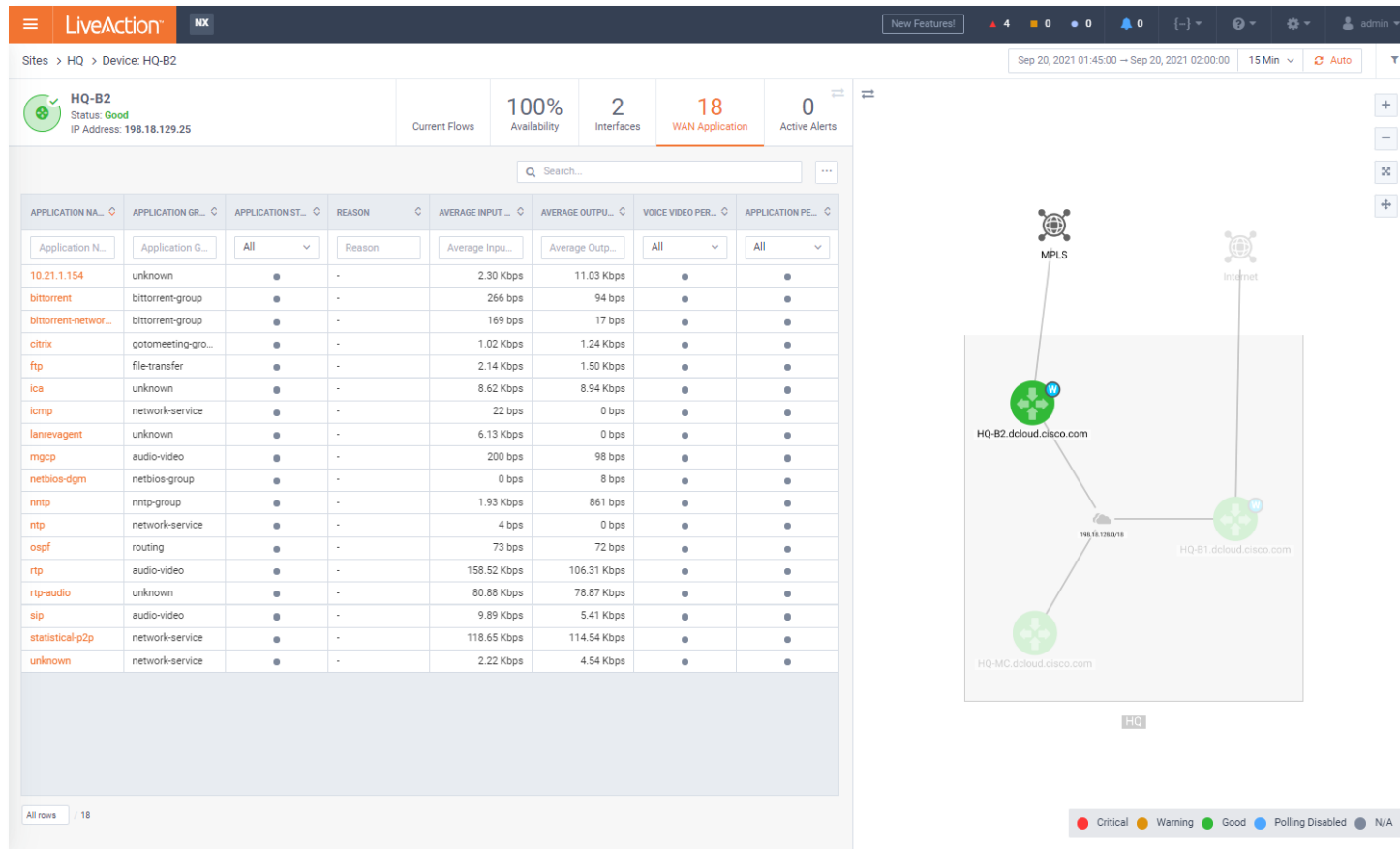


Interfaces											
Enter Filter Request Here											
Search...											
INTERFACE NAME	STATUS	SITE	DEVICE	IP ADDRESS	SUBNET MASK	DESCRIPTION	SERVICE PROVIDER	INPUT CAPACITY	OUTPUT CAPACITY	WAN TYPE	TAGS
Interface Name	All	Site	Device	IP Address	Subnet Mask	Description	Service Provider	Input Capacity	Output Capacity	All	Tags
GigabitEthernet1	●	NY	Branch2-NY	198.19.2.1	255.255.255.0	Branch2 LAN	-	1 Gbps	1 Gbps	-	-
GigabitEthernet2	●	NY	Branch2-NY	100.64.2.2	255.255.255.0	Internet	Internet	2 Mbps	2 Mbps	WAN	-
GigabitEthernet3	●	NY	Branch2-NY	10.255.2.2	255.255.255.0	MPLS	MPLS	2 Mbps	2 Mbps	WAN	-
GigabitEthernet1	●	HQ	HQ-MC	198.18.129.23	255.255.192.0	-	-	1 Gbps	1 Gbps	-	-
GigabitEthernet1	●	LA	Branch1-LA	198.19.1.1	255.255.255.0	Branch1 LAN	Branch1 LAN	1 Gbps	1 Gbps	-	-
GigabitEthernet2	●	LA	Branch1-LA	100.64.1.2	255.255.255.0	Internet	Internet	2 Mbps	2 Mbps	WAN	-
GigabitEthernet3	●	LA	Branch1-LA	10.255.1.2	255.255.255.0	MPLS	MPLS	2 Mbps	2 Mbps	WAN	-
GigabitEthernet1	●	HQ	HQ-B1	198.18.129.24	255.255.192.0	HQ-LAN	-	1 Gbps	1 Gbps	-	-
GigabitEthernet2	●	HQ	HQ-B1	100.64.0.2	255.255.255.0	Internet	Internet	4 Mbps	4 Mbps	WAN	-
GigabitEthernet1	●	HQ	HQ-B2	198.18.129.25	255.255.192.0	-	Default Service Pro...	1 Gbps	1 Gbps	-	-
GigabitEthernet2	●	HQ	HQ-B2	10.255.0.2	255.255.255.0	-	MPLS	2 Mbps	2 Mbps	WAN	-

Response	Percentage
Yes	75%
No	25%

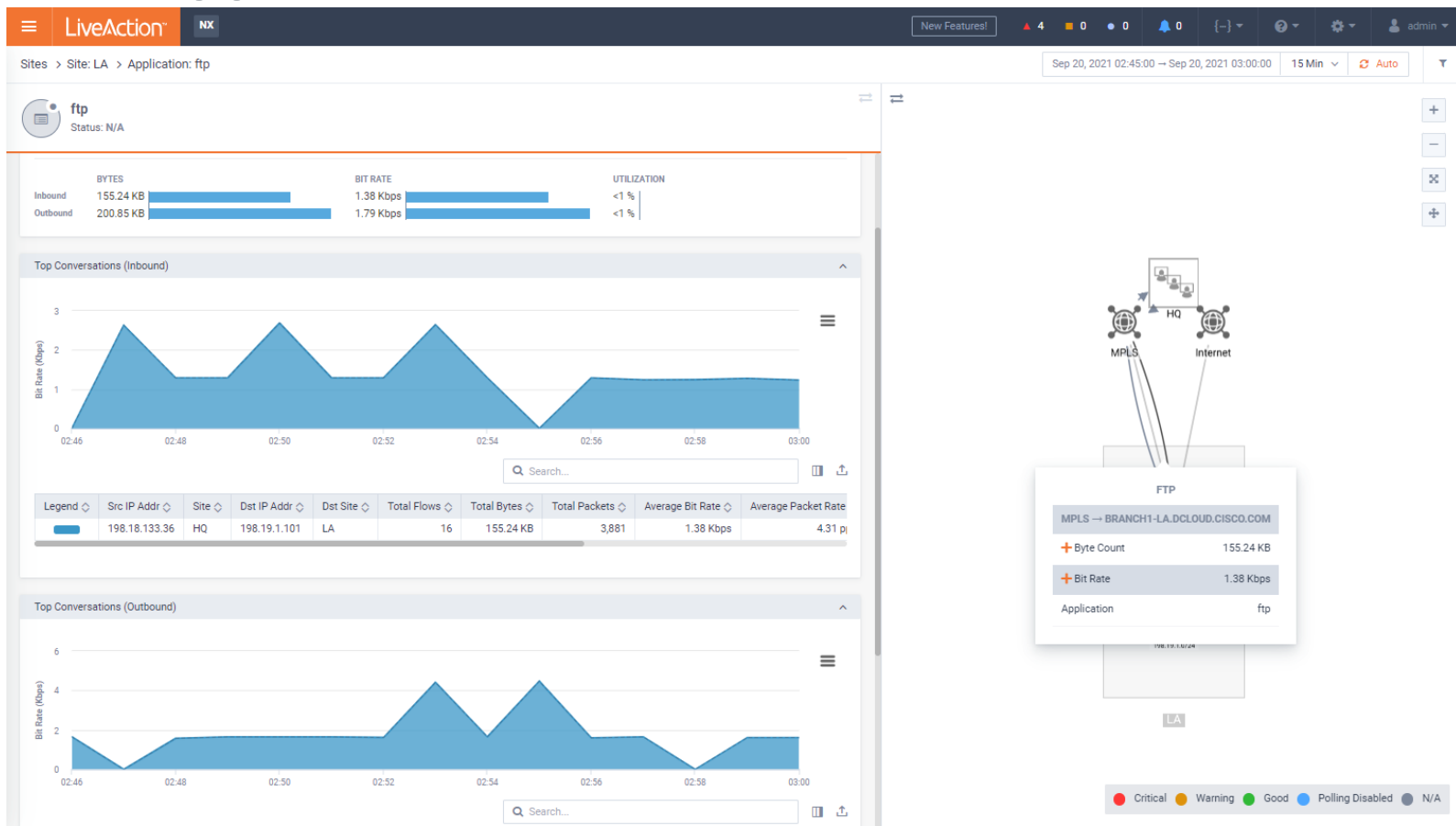


# WAN Applications

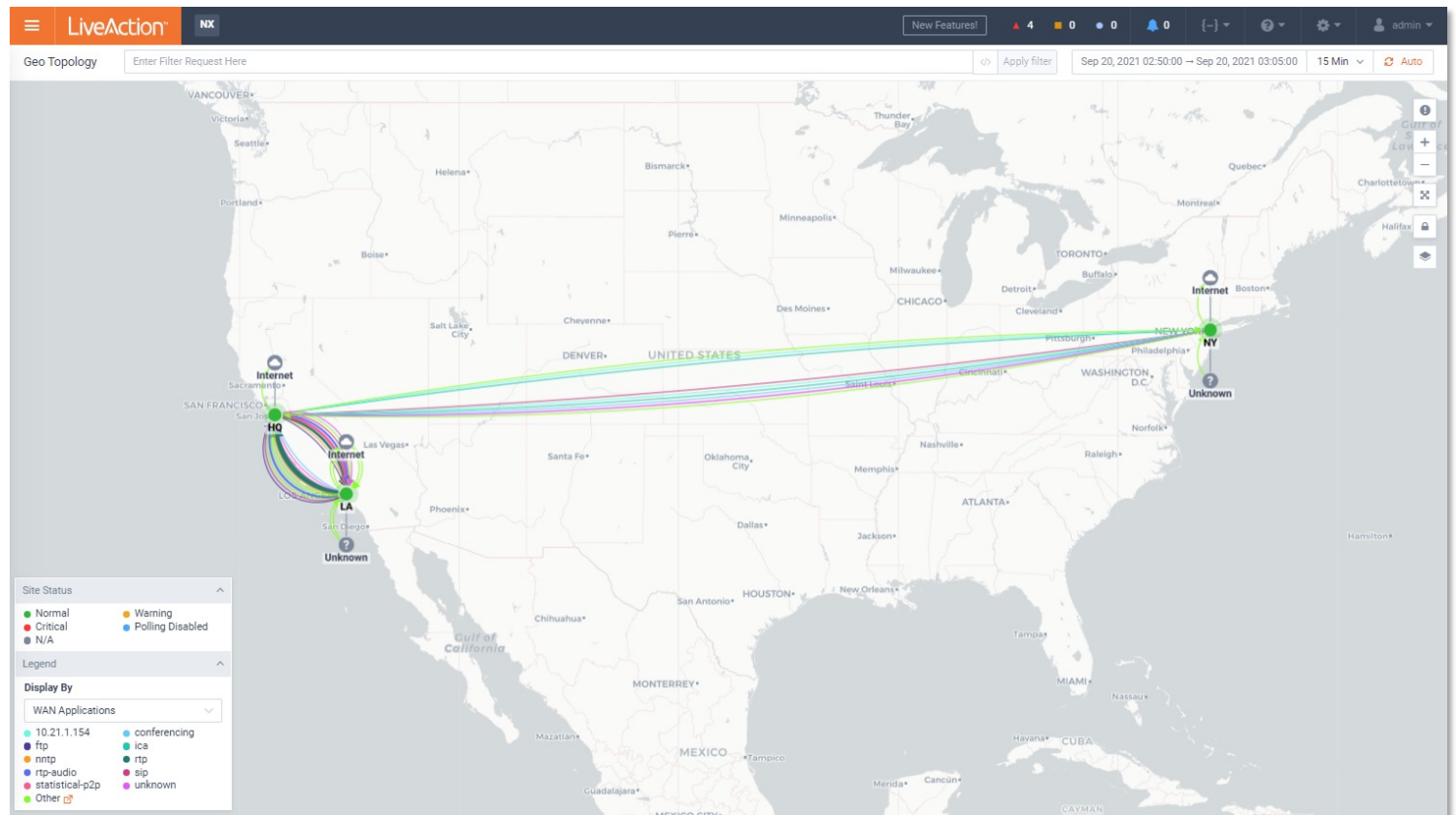




# WAN Applications>Flows



# Geo Topology



# Stories

LiveAction™

Main

Topology

Stories

Device Inventory

Flow Path Analysis

IP SLA

Security Flow Analysis

Site to Site Analysis

Calls by Number

WAN Availability

WAN Capacity Planning

WAN Utilization

Reports

LiveNA

Configure

LiveAction™ NX

New Feature!

4

0

0

0

{-}

admin

Device Inventory

Enter Filter Request Here

Apply filter

Devices

Search...

DEVICE	DEVICE SERIAL	IP ADDRESS	SITE	NODE	TAGS	GROUP	MODEL	OS VERSION	DESCRIPTION
Device	Device Serial	IP Address	Site	Node	Tags	Group	Model	OS Version	Description
HQ-MC	1	198.18.129.23	HQ	Local	-	HQ	ciscoCSR1000v	16.3.2	Cisco IOS Software [Den...
HQ-B1	2	198.18.129.24	HQ	Local	-	HQ	ciscoCSR1000v	16.3.2	Cisco IOS Software [Den...
Branch1-LA	101	198.19.1.1	LA	Local	-	LA	ciscoCSR1000v	16.3.2	Cisco IOS Software [Den...
HQ-B2	3	198.18.129.25	HQ	Local	-	HQ	ciscoCSR1000v	16.3.2	Cisco IOS Software [Den...
Branch2-NY	0000000021	198.19.2.1	NY	Local	-	NY	ciscoCSR1000v	16.3.2	Cisco IOS Software [Den...

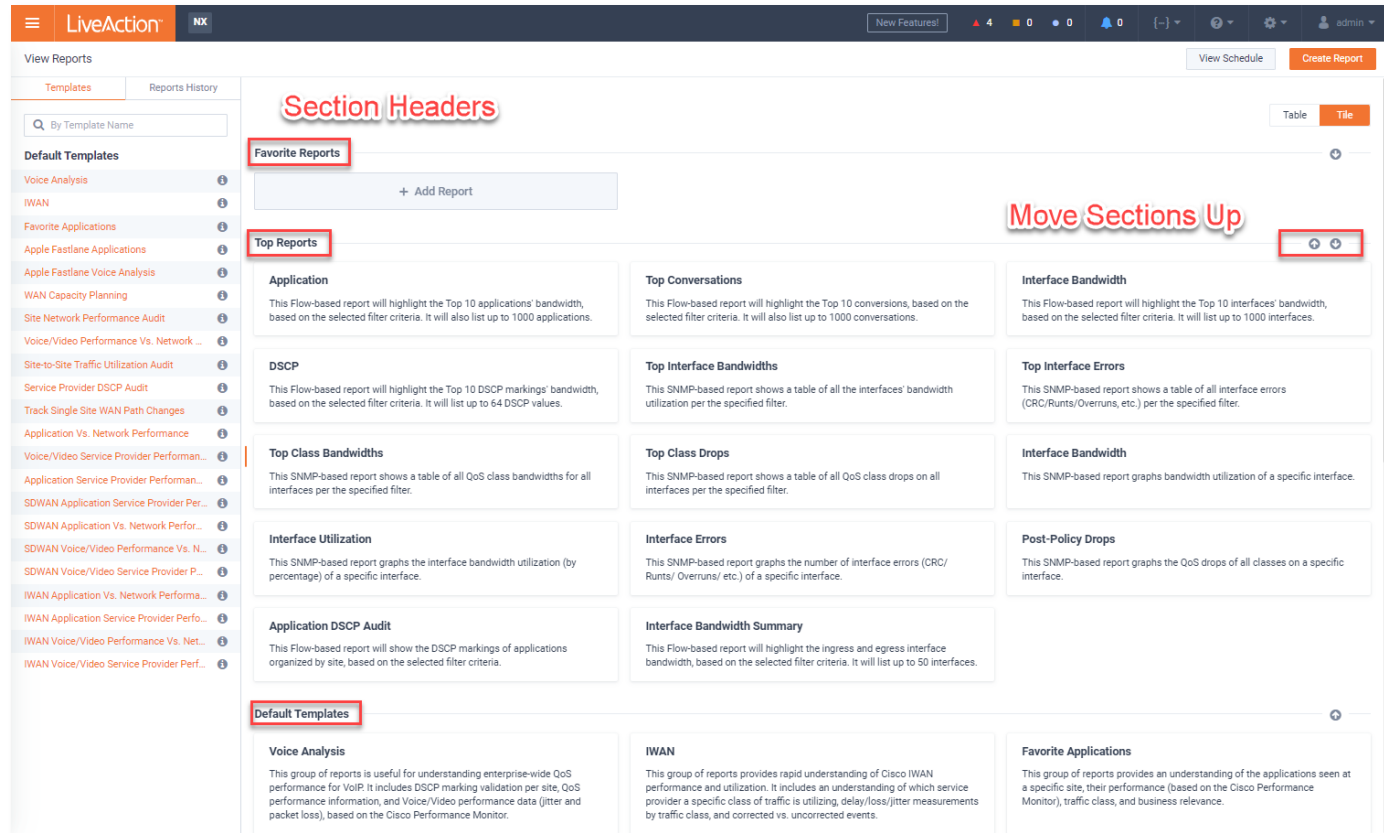
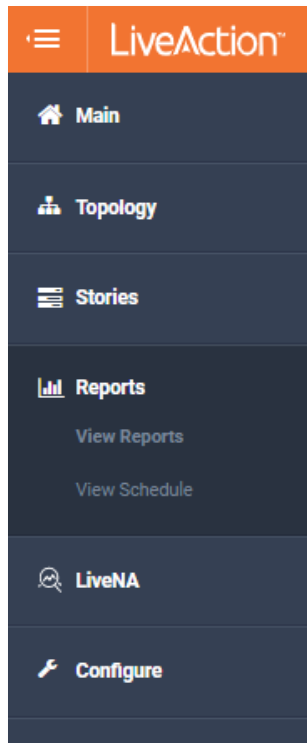
All rows / 5

Interfaces

Search...

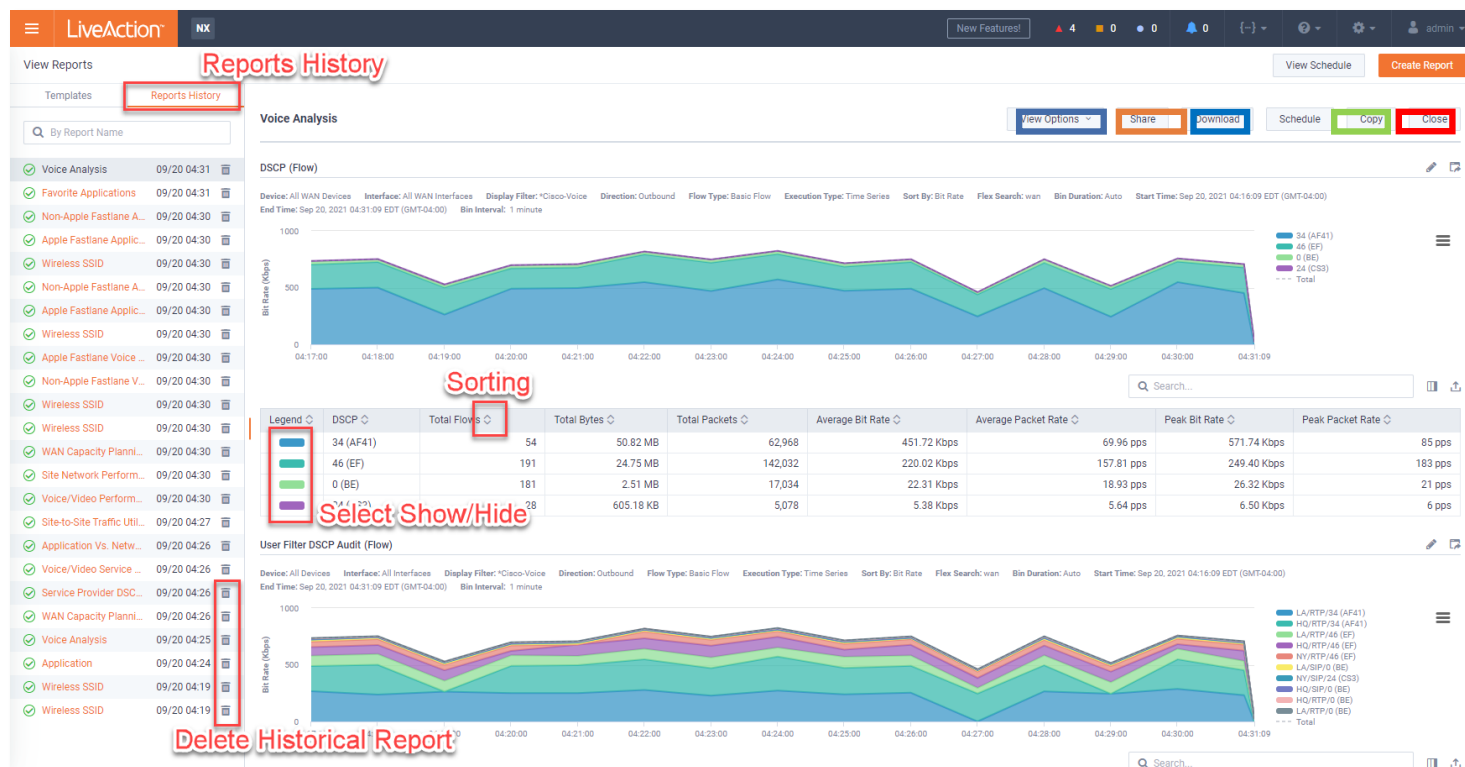
INTERFACE N...	IP ADDRESS	SUBNET MASK	DEVICE	SITE	WAN TYPE	SERVICE PR...	INPUT CAPA...	OUTPUT CAP...	ABBREVIATE...	IF INDEX	DESCRIPTION	SPEED	TYPE	LABEL	TAGS
Interface ...	IP Address	Subnet ...	Device	Site	All	Service P...	Input Ca...	Output C...	Abbreviat...	If Index	Descripti...	Speed	Type	Label	Tag
GigabitEther...	198.18.129.23	255.255.192.0	HQ-MC	HQ	-	-	1 Gbps	1 Gbps	Gi1	1	-	1 Gbps	ethernet_cs...	-	-
GigabitEther...	198.18.129.24	255.255.192.0	HQ-B1	HQ	-	-	1 Gbps	1 Gbps	Gi1	1	HQ-LAN	1 Gbps	ethernet_cs...	HQ LAN	-
GigabitEther...	100.64.0.2	255.255.255.0	HQ-B1	HQ	WAN	Internet	4 Mbps	4 Mbps	Gi2	2	Internet	1 Gbps	ethernet_cs...	HQ Internet	-
GigabitEther...	198.19.1.1	255.255.255.0	Branch1-LA	LA	-	Branch1 LAN	1 Gbps	1 Gbps	Gi1	1	Branch1 LAN	1 Gbps	ethernet_cs...	Branch1-LA ...	-
GigabitEther...	100.64.1.2	255.255.255.0	Branch1-LA	LA	WAN	Internet	2 Mbps	2 Mbps	Gi2	2	Internet	2 Mbps	ethernet_cs...	LA Internet	-
GigabitEther...	10.255.1.2	255.255.255.0	Branch1-LA	LA	WAN	MPLS	2 Mbps	2 Mbps	Gi3	3	MPLS	1 Mbps	ethernet_cs...	LA MPLS	-
GigabitEther...	198.18.129.25	255.255.192.0	HQ-B2	HQ	-	Default Servi...	1 Gbps	1 Gbps	Gi1	1	-	1 Gbps	ethernet_cs...	HQ LAN	-
GigabitEther...	10.255.0.2	255.255.255.0	HQ-B2	HQ	WAN	MPLS	2 Mbps	2 Mbps	Gi2	2	-	1 Gbps	ethernet_cs...	HQ MPLS	-

# View ANY Report Defined in LiveNX





# 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

### VOICE ANALYSIS

REPORTS INCLUDED

- DSCP
- User Filter DSCP Audit
- Application DSCP Audit
- Top Class Drops
- Jitter/Loss Outbound
- Jitter/Loss Inbound

**TIME ZONE** ☒ DST

(GMT-08:00) America/Los Angeles

**TIME RANGE**

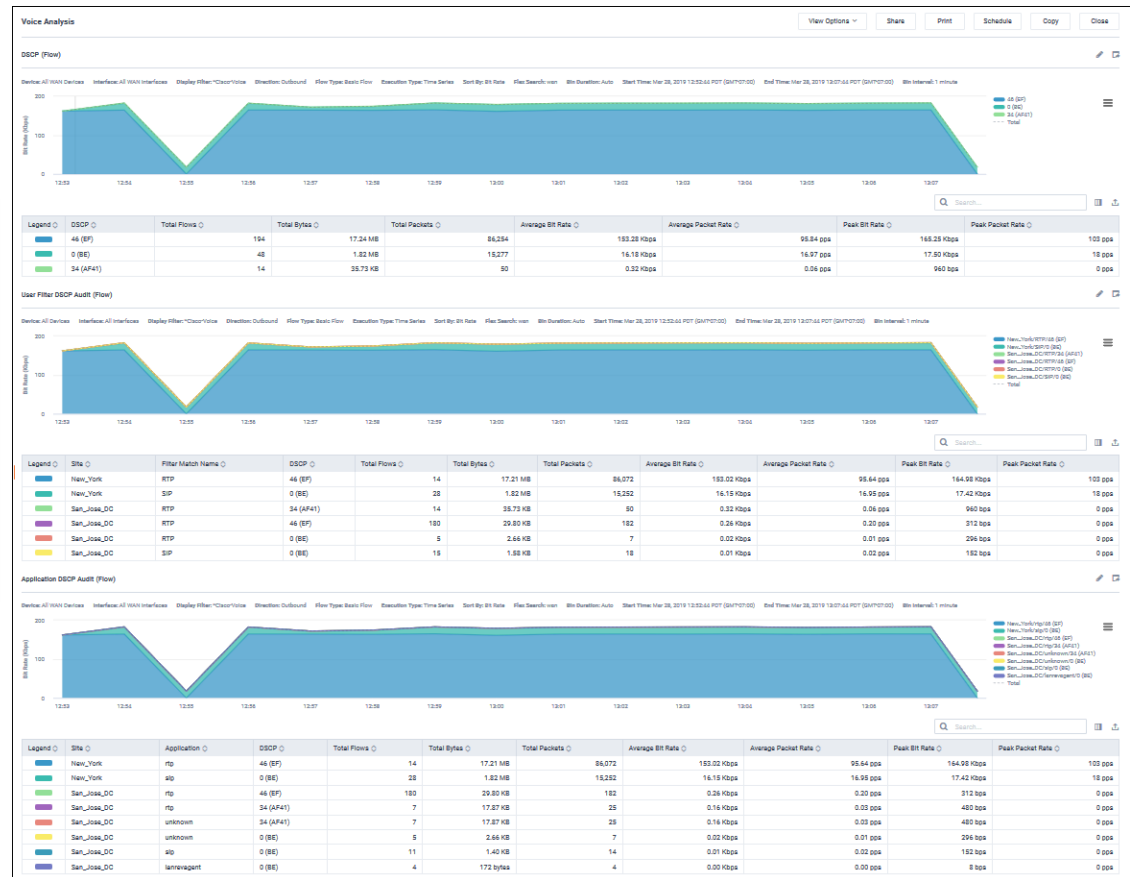
Last Fifteen Minutes

**SHARING** ☐ Send PDF

Enter an email address or AD entity...

**DISPLAY FILTER** **SITE**

\*Cisco-Voice All Sites



# 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

**CREATE REPORT**

**GENERAL SETTINGS**

NAME: My Report Group

PRESENTATION MODE: Standard

FOOTNOTE: Something insightful here

TIME ZONE: (GMT-08:00) America/Los Angeles ☒ DST

TIME RANGE: Last Fifteen Minutes

SHARING: ☐ Send PDF

FLEX SEARCH: Ex: site=Honolulu & wan & flow.app=http

DISPLAY FILTER: Select Display Filter...

**REPORT LIST**

Report Name	Flow Type	Status	Action
Application (Flow)	Fast		
DSCP (Flow)	Fast		
Destination Site Traffic (Flow)	Fast		

**REPORT DETAILS**

REPORT NAME: Destination Site Traffic

REPORT DESCRIPTION: Enter report description...

DEVICES: All WAN Devices

INTERFACES: All WAN Interfaces

FLEX SEARCH: Ex: site=Honolulu & wan & flow.app=http

DISPLAY FILTER: No Display Filtering

DIRECTION: Outbound

FLOW TYPE: Basic Flow

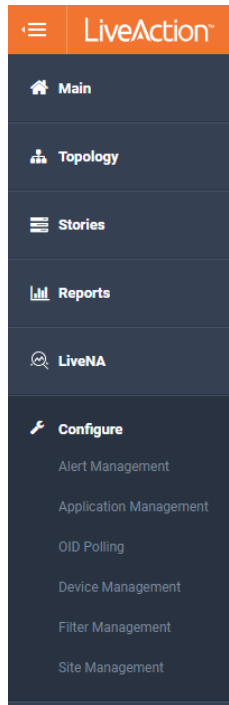
EXECUTION TYPE: Time Series

SORT BY: Bit Rate

Buttons: Cancel, Save As Template, Execute



# LiveNX Alerting



Alert Management						
LiveNX Alerts						
<div>Enable Disable</div> <div>Search...</div>						
ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING	
<input type="checkbox"/> Alert Type	All	All	All	Thresholds	Sharing	
Application Performance - App Delay	Application	Multiple		Multiple	Multiple	
Application Performance - Network Delay	Application	Multiple		Multiple	Multiple	
<input type="checkbox"/> BGP Peer Connection Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI	
<input type="checkbox"/> Cisco IWAN Path Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI	
<input type="checkbox"/> Cisco IWAN Threshold Crossing	Network	▲ Critical	✓	for at least > 0 minutes	Web UI	
Cisco SD-WAN Performance - Jitter Value	Network	Multiple		Multiple	Multiple	
Cisco SD-WAN Performance - Network Delay	Network	Multiple		Multiple	Multiple	
Cisco SD-WAN Performance - Packet Loss	Network	Multiple		Multiple	Multiple	
Cisco SD-WAN SLA Class Path Change	Network	Multiple		Multiple	Multiple	
<input type="checkbox"/> Critical Traffic Response Time	Application	▲ Critical	✓	Response Time >= 5 ms for at least > 0 minutes	Web UI	
<input type="checkbox"/> Device CPU Utilization	Device, Interface	Multiple	✓	Multiple	Multiple	
<input type="checkbox"/> Device Flow Stop	Device, Interface	▲ Critical	✓	for at least > 0 minutes	Web UI	
<input type="checkbox"/> Device Memory Utilization	Device, Interface	Multiple	✓	Multiple	Multiple	
<input type="checkbox"/> Device Reachability	Device, Interface	Multiple	✓	Multiple	Multiple	
EIGRP Neighbor Count Decrease	Network	Multiple		Multiple	Multiple	
EIGRP Neighbor Count Increase	Network	Multiple		Multiple	Multiple	
Fan Tray Operational State	Device, Interface	Multiple		Multiple	Multiple	
High WAN Interface Utilization	Device, Interface	Multiple	✓	Multiple	Multiple	
Low WAN Interface Utilization	Device, Interface	Multiple		Multiple	Multiple	

Rows: 44 / 44

QoS Class Drop

Enabled

On

This alert may contribute to status of an Interface, Device, and/or Site.

Severity

Warning

Note: Severity for this alert may be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status.

Thresholds

Automatic Resolution Time \*

0 min

Catch All Threshold \*

All non-specified QoS Classes

☒ Drop Rate \* For at Least \*

0 kbps > 0 min

QoS Class \*

VOICE

☒ Drop Rate \* For at Least \*

20 kbps > 0 min

QoS Class \*

VIDEO

☒ Drop Rate \* For at Least \*

50 kbps > 1 min

Add Specific QoS Class Alert

Sharing

☐ Email

Type Email

☐ ServiceNow

☐ SNMP Trap

☒ Web UI

☐ Syslog

Cancel Save

---

# 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 NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS	SESSION TIMEOUT
admin	admin	Local	Admin	Enabled	4 Hours

Authentication Type

LOCAL

LDAP

RADIUS

TACACS+

SSO

Username \*

Display Name \*

Group \*

Session Timeout \*

Repeat Password \*

# 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 Management

User Management

Group Management

Sessions

LDAP Management

WMIC Management

TACACS+ Authentication

RADIUS Authentication

Add Edit Delete

Search...

	USER NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS	SESSION
<input type="checkbox"/>	User Name	Display Name	Directory	Group	Status	Sessio
<input type="checkbox"/>	admin	admin		Admin	Enabled	4 Hours

Settings

System Diagnostics

User Management

LiveNX Server

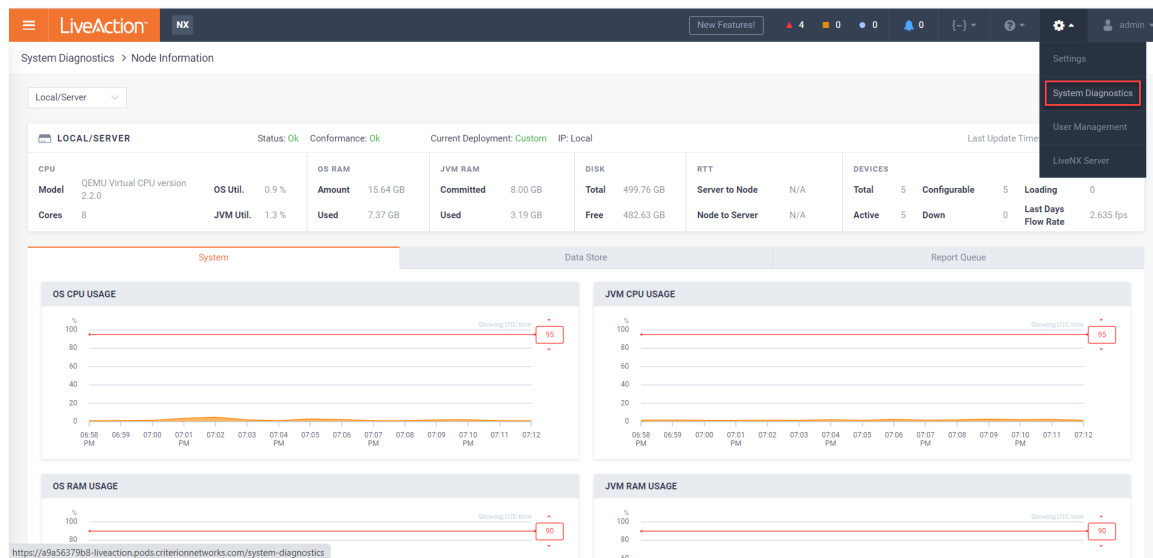
---

## 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

The screenshot shows the LiveAction NX console interface. On the left is a sidebar menu with categories like Settings, Device Entity Page Reports, Email Configuration, Integrations, Licensing, LiveNA Configuration, Mounted Data, Nodes, Properties, Proxy, Reports, Security, Single Sign On, SNMP Trap, Syslog, Troubleshooting, and Logs. The 'Logs' item is highlighted with a red circle labeled '3'. In the top right corner, a user profile dropdown menu is open, showing options like Settings, System Diagnostics, User Management, and LiveNX Server, with the 'Settings' option highlighted by a red circle labeled '1'. The main content area is titled 'LOGS' and shows the 'LiveNX Log Level' set to 'DEBUG'. Below this is a 'Manage Logs' section with a table of logs. The table has columns for Node Name, Source, File Path, Collection Start Time, State, Size, Download, and Upload to Cloud. There are 5 rows of log data shown.

	NODE NAME	SOURCE	FILE PATH	COLLECTION START TIME	STATE	SIZE	DOWNLOAD	UPLOAD TO CLOUD
<input type="checkbox"/>	Node name	Source	File Path	Collection start time	State	Size		
<input type="checkbox"/>	Local	LiveNX	/data/livenx-server/data/log-zip/20...	Tue Sep 21 2...	OK	37.15 MB		
<input type="checkbox"/>	Local	LiveNX	/data/livenx-server/data/log-zip/20...	Tue Sep 21 2...	OK	37.07 MB		
<input type="checkbox"/>	Local	LiveNX	/data/livenx-server/data/log-zip/20...	Mon Sep 20 ...	OK	32.82 MB		
<input type="checkbox"/>	Local	LiveNX	/data/livenx-server/data/log-zip/20...	Mon Sep 20 ...	OK	30.56 MB		
<input type="checkbox"/>	Local	LiveNX	/data/livenx-server/data/log-zip/20...	Mon Sep 20 ...	OK	29.75 MB		

# LAB 1: Using the Web UI

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





A hand is shown interacting with a tablet. The tablet screen displays a complex technical interface with various graphs, including a line graph with a red trend line and a bar chart. The background is blurred, showing other screens and blue light. An orange rectangular box is overlaid on the left side of the image, containing the title text.

# The LiveNX Engineering Console

© 2022, LiveAction, Inc. All Rights Reserved.

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 screenshot displays the LiveNX Eng Console interface, which is a network management tool. The interface is divided into several sections:

- Home Tree View:** A sidebar on the left showing a hierarchical tree of network elements, including 'CocoLiveDemo', 'DC', 'HSL', 'L2\_Campus', 'N\_California', 'North East', 'South West', 'I2', 'z-East', and 'z-West'. The 'z-East' group is currently selected.
- Module Tabs:** A row of tabs at the top, including 'QoS', 'Flow', 'Routing', 'IP SLA', 'LAN', 'Tools', 'Reports', 'Window', 'Dev', and 'Help'. The 'Flow' tab is active.
- Search:** A search bar located below the module tabs, with a placeholder text 'Search Example: (site = Honolulu) & wan & flow.app = webex-meet'.
- Filter:** A dropdown menu next to the search bar, currently set to 'All Flow Types'.
- Group Container:** A central area displaying a network topology diagram. It shows two main groups, 'z-West' and 'z-East', each containing a central switch (APN-CAT\_3560\_14) and several connected devices. The diagram uses color-coded lines to represent different flow types.
- Topology Pane:** A pane at the bottom of the group container, showing a detailed view of the selected device, 'APN-CAT\_3560\_14'.
- Devices:** A list of devices connected to the selected switch, including 'APN-CAT\_3560\_14' and 'APN-CAT\_3560\_15'.
- Alerts & Notifications:** A status bar at the bottom of the interface, showing various alerts and notifications, including 'CPU 1', 'Memory', 'Flow Buffer', 'Advisories', and 'Nodes'.

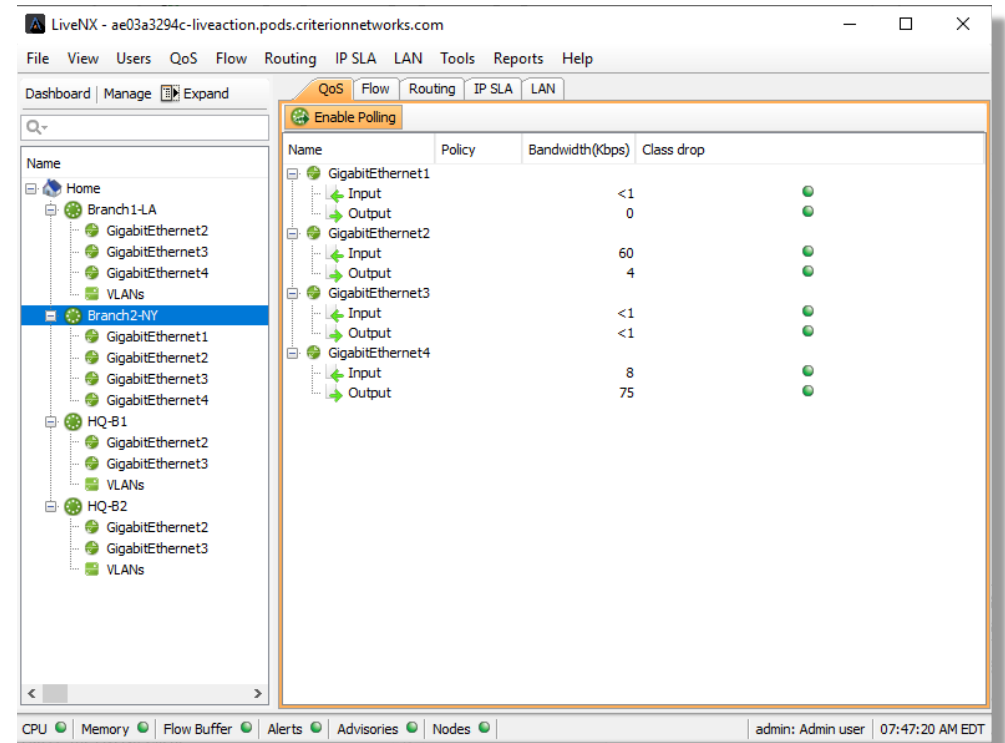
Color Mapping By DSCP:

- 0 (BE)
- 2 GB / 221 flows
- 10 (AF21)
- 20 (AF31)
- 3 MB / 1 flow
- 34 (AF41)
- \*4 MB / 2 flows
- 16 (CS2)
- 24 (CS3)
- 32 (CS4)
- 40 (CS6)
- 48 (EF)
- \*54 MB / 17 flows
- Remaining
- \*0 B / 14 flows
- Flow Polling Disabled Icon
- ACL Applied
- Not configured
- VLAN

LiveAction®

# The Home Tree-view

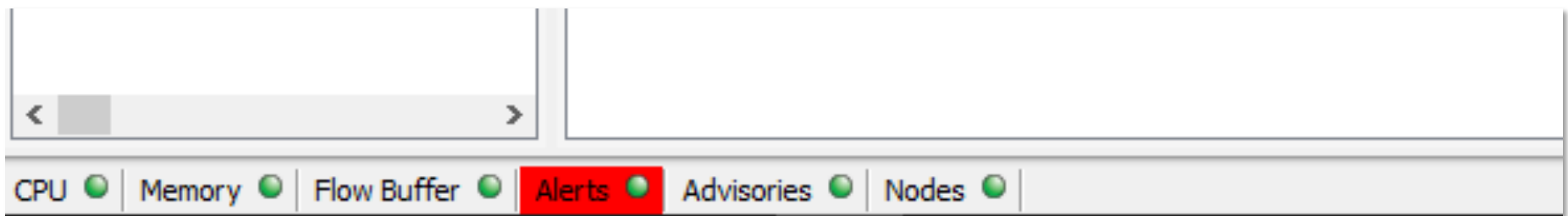
- Groups
  - Devices
    - Interfaces
- Select Home to view all Groups/Devices in the Topology Pane
- Select & Modify Devices & Interfaces
- Right-click Zoom-to...



## Immediate Feedback...

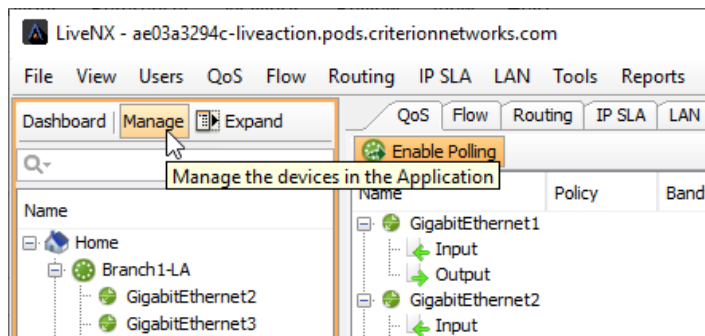
Look at the bottom of the screen for information about:

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

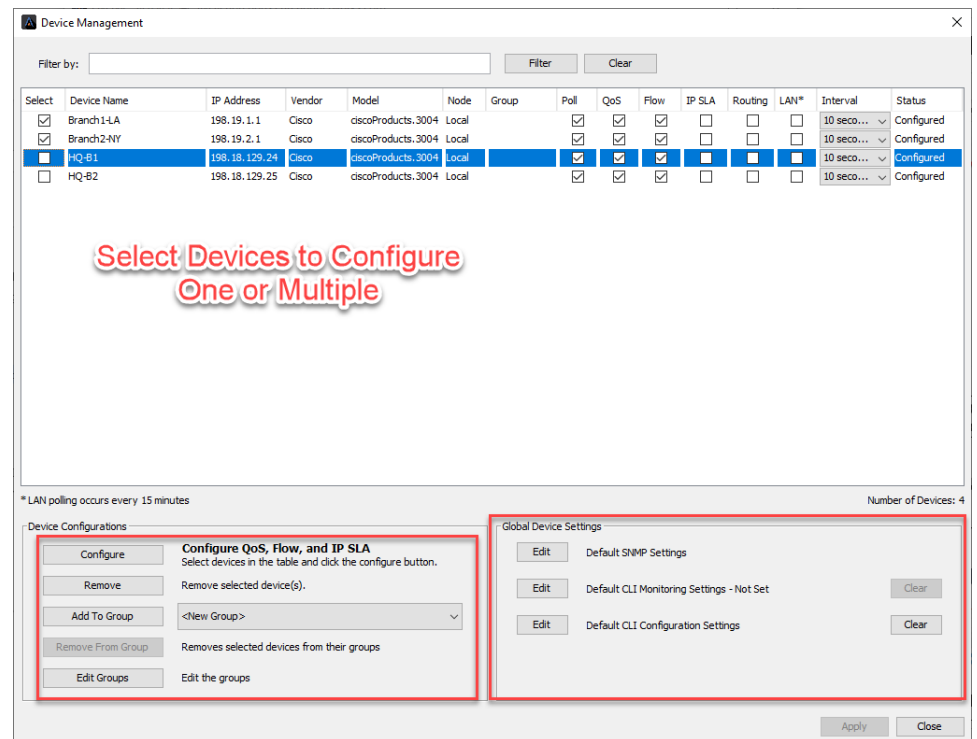


# Main Configuration Tool

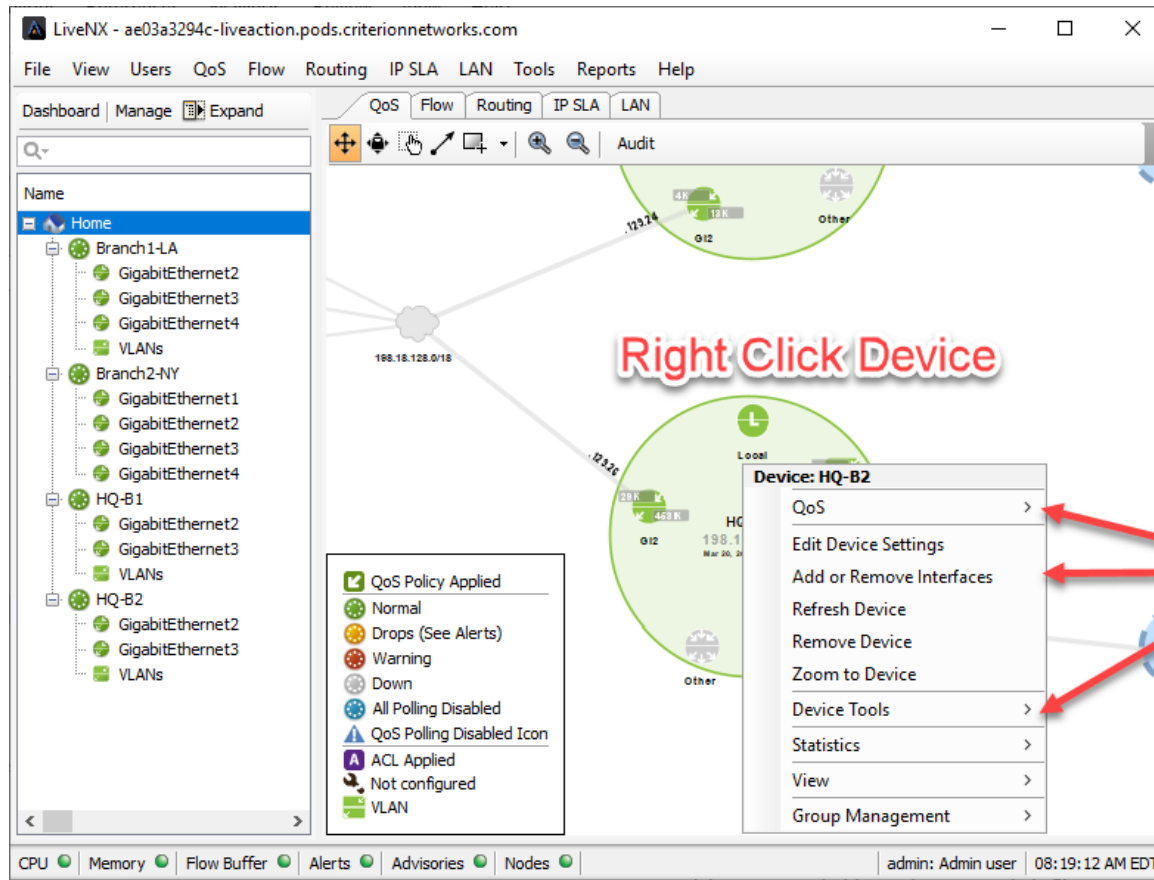
Click **Manage** to open **Device Management** window



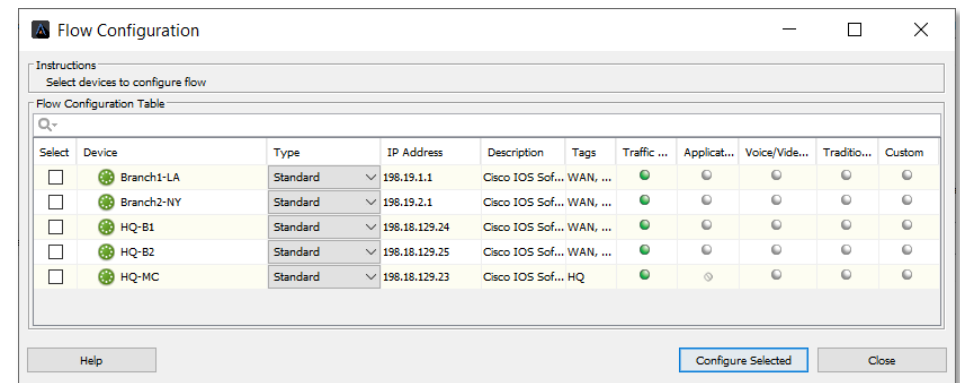
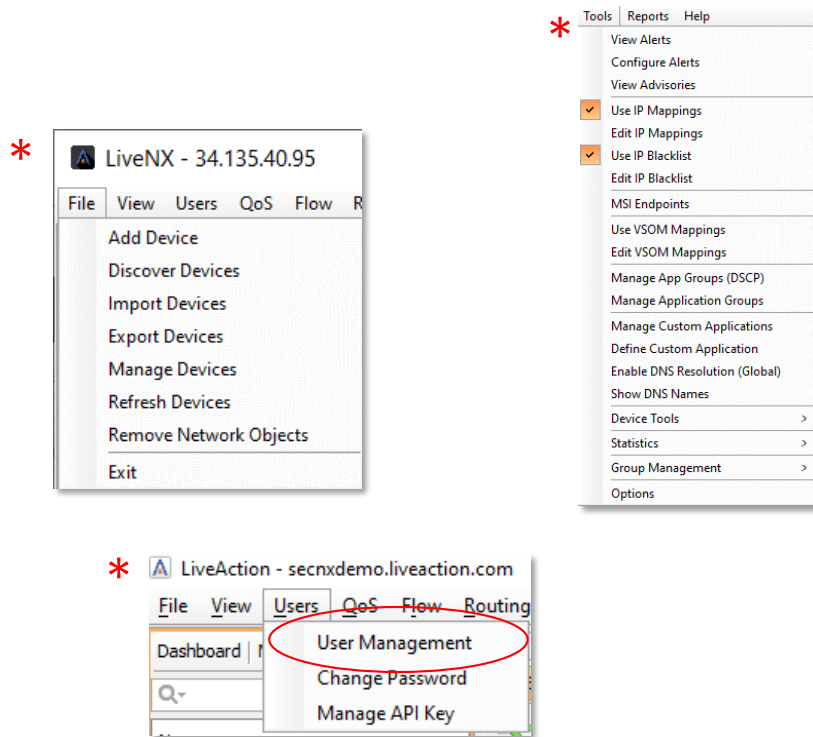
We will use the **Configuration** capabilities extensively in the class



# 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

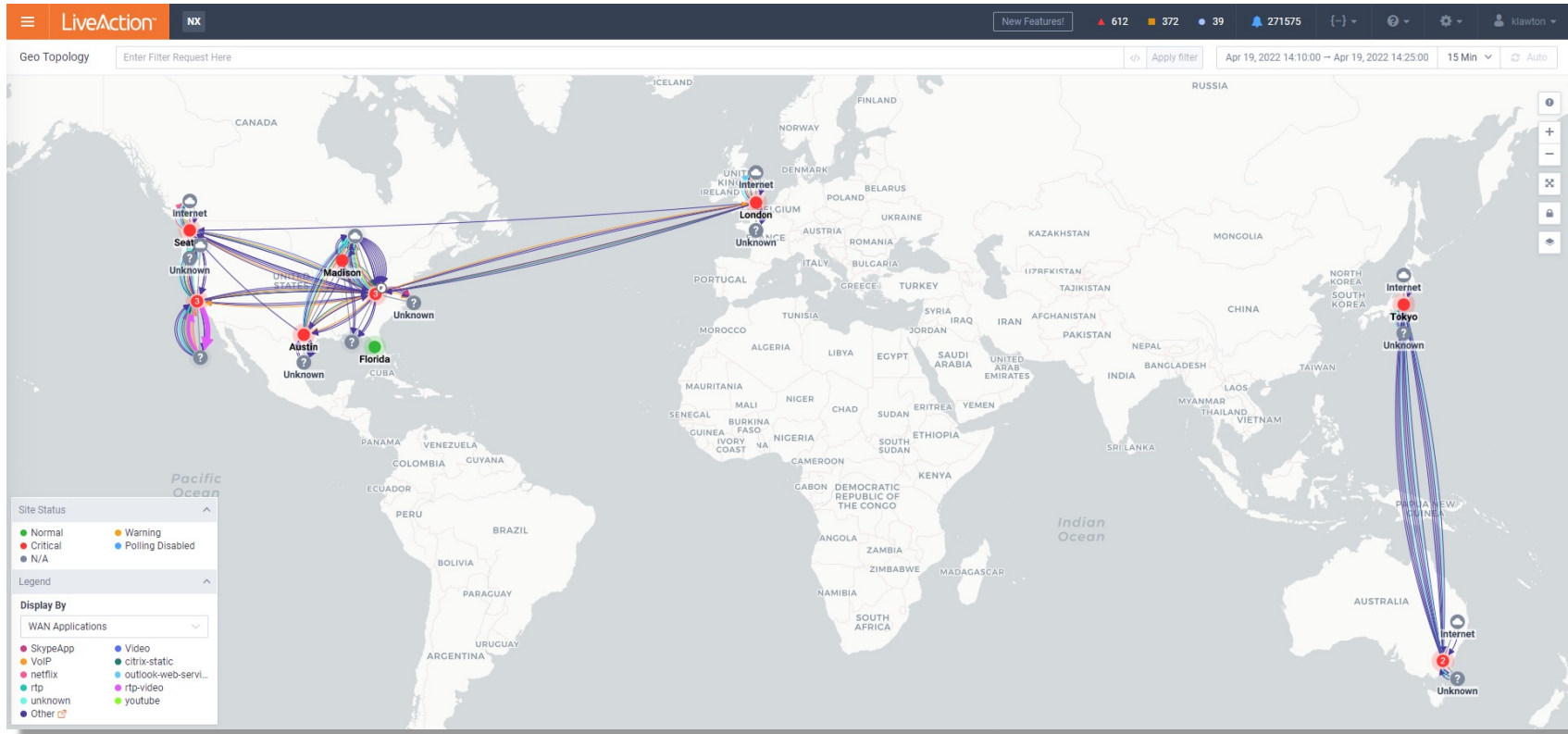


A woman with long brown hair, wearing a white button-down shirt, is looking upwards and to the right with a thoughtful expression, her hand resting on her chin. The background is a dark, textured surface with a white maze pattern. Several arrows are drawn on the maze lines, pointing in various directions: up, down, left, and right. An orange rectangular box is overlaid on the left side of the image, containing the word 'Visualizations' in white text.

# Visualizations

# 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

The screenshot displays the LiveAction NX interface for the 'Device: HQ-B1' page. The interface is divided into several sections:

- Header:** Includes the LiveAction logo, a 'New Features!' button, and a status bar showing 16 alerts, 0 warnings, 0 errors, and 111 notifications. The user 'admin' is logged in.
- Navigation:** A sidebar on the left contains a menu with items like 'Device Details', 'Device CPU/Memory Usage', 'Top Applications (Inbound)', 'Top Applications (Outbound)', 'Top DSCP (Inbound)', 'Top DSCP (Outbound)', 'Top Conversations (Inbound)', and 'Top Conversations (Outbound)'. The 'Device Details' item is highlighted with a red circle 8.
- Summary:** A central section displays key metrics for HQ-B1: Status: Good, IP Address: 198.18.129.24, Current Flows: 2, Availability: 100%, Interfaces: 2, WAN Application: 18, and Active Alerts: 0. These metrics are numbered 1 through 6.
- Network Diagram:** A large diagram on the right (numbered 7) shows the network topology. It includes a 'Service Provider' box labeled 'SP1\_MPLS' and 'SP2\_MPLS', and two cloud icons labeled 'HQ-B1.dcloud.cisco.com' and 'HQ-B2.dcloud.cisco.com'. The diagram is numbered 9.
- Legend:** A legend at the bottom right of the diagram area shows status indicators: Critical (red), Warning (yellow), Good (green), Polling Disabled (blue), and N/A (grey).

# Flow Troubleshooting, Decision Making

Start with what you know about the issue

LiveAction NX

Flow Path Analysis

Application: rtp rtp-audio rtp-video Enter Filter Request Here

Basic

Start with Flow Path Analysis

Explicit info to include in view

Start with Basic Info

Drill to Specific Flow Analysis

PEEK	FLOW P...	TIME	PROTOCOL	SRC IP ADDR	SRC SITE	SRC PORT	DST IP ADDR	DST SITE	DST PORT	DSCP	APPLICATION	TOTAL FLOWS	TOTAL BYTES	TOTAL PACKETS	AVERAGE BIT R...	AVERAGE PACK...
		Time	Protocol	Src IP Addr	Src Site	Src Port	Dst IP Addr	Dst Site	Dst Port	DSCP	Application	Total Flows	Total Bytes	Total Packets	Average Bit ...	Average Pa...
		21 Mar 2022, 01:45PM	UDP	198.18.128.80	HQ	20100	198.19.1.80	LA	20100	34 (AF41)	rtp	6	5.20 MB	6,444	11.56 Kbps	1.79 pps
		21 Mar 2022, 01:45PM	UDP	198.18.128.80	HQ	20100	198.19.1.80	LA	20100	34 (AF41)	rtp	6	5.19 MB	6,404	11.52 Kbps	1.78 pps
		21 Mar 2022, 01:25PM	UDP	198.18.128.80	HQ	20100	198.19.1.80	LA	20100	34 (AF41)	rtp	6	5.18 MB	6,399	11.51 Kbps	1.78 pps

LiveAction NX

WAN Applications > Application: rtp > PATH UDP 198.18.128.80 : 20100 - 198.19.1.80 : 20100

Mar 21, 2022 13:45:00 ~ Mar 21, 2022 13:50:00

Flow Path

Path Flow HQ - LA

Device 1 Info

Device 2 Info

Click to Drill Down (Orange)

Status and Config Info

Device Name	Branch1-LA.dcloud.cisco.com	HQ-B2.dcloud.cisco.com
Site Name	LA	HQ
Application	rtp	rtp
CPU Usage	35.00 %	35.00 %
Memory Usage	13.00 %	12.00 %
In Interface	GigabitEthernet4	GigabitEthernet2
Out Interface	Null0	GigabitEthernet3
In QoS Policy	No Policy	No Policy
Out QoS Policy	No Policy	No Policy
Bit Rate In	111.56 Kbps	138.29 Kbps
Bit Rate Out	111.56 Kbps	138.29 Kbps
Utilization In	5.58 %	0.01 %
Utilization Out	-	6.91 %
DSCP	34 (AF41)	34 (AF41)

LiveAction®

# Eliminate the Detractors!

LiveAction NX

New Features! 16 0 0 111 {--} ? ? ? admin

WAN Applications Enter Filter Request Here </> Apply filter Mar 20, 2022 16:40:00 → Mar 20, 2022 16:55:00 15 Min Auto Configure Custom Applications

Page Filters Time Range

APPLICATION NAME	APPLICATION GROUP	APPLICATION STATUS	AVERAGE INPUT BIT RATE	AVERAGE OUTPUT BIT RATE	VOICE VIDEO PERFORMANCE	APPLICATION PERFORMANCE
Application Name	Application Group	All	Average Input Bit Rate	Average Output Bit Rate	All	All
10.21.1.154	unknown	●	15.87 Kbps	755 bps	●	●
bgp	routing	●	59 bps	59 bps	●	●
bittorrent	bittorrent-group	●	265 bps	93 bps	●	●
bittorrent-networking	bittorrent-group	●	169 bps	17 bps	●	●
citrix	gotomeeting-group	●	4.31 Kbps	3.70 Kbps	●	●
dns	network-service	●	42 bps	0 bps	●	●
ftp	file-transfer	●	6.53 Kbps	6.59 Kbps	●	●
ica	unknown	●	6.11 Kbps	6.74 Kbps	●	●
ipfix	unknown	●	10.83 Kbps	10.92 Kbps	●	●
lanrevagent	unknown	●	7.63 Kbps	6.57 Kbps	●	●
openwebnet	unknown	●	12.80 Kbps	12.85 Kbps	●	●
ospf	routing	●	320 bps	0 bps	●	●
rtp	audio-video	●	530.18 Kbps	585.58 Kbps	●	●
rtp-audio	unknown	●	185.41 Kbps	84.61 Kbps	●	●
sip	audio-video	●	6.23 Kbps	9.09 Kbps	●	●
snmp	snmp-group	●	16.83 Kbps	16.33 Kbps	●	●
statistical-p2p	network-service	●	2.24 Kbps	2.24 Kbps	●	●
trim	unknown	●	0 bps	0 bps	●	●
unknown	network-service	●	4.49 Kbps	4.62 Kbps	●	●

All rows / 19



# The Search Field

The screenshot shows the LiveAction dashboard interface. At the top, there's a navigation bar with the LiveAction logo, a menu icon, and a user profile. Below the navigation bar, the dashboard is divided into sections: Status, WAN, System, and Alerts. A search bar is located in the top right of the dashboard area, with a dropdown menu showing suggestions for search filters. The dropdown menu includes options like 'Application: rtp', 'Device: Add value', and a list of devices: 'Branch1-LA.dcloud.cisco.com', 'HQ-B1.dcloud.cisco.com', and 'HQ-B2.dcloud.cisco.com'. The dashboard also displays various charts and graphs, including a line chart for 'Branch1-LA' and a bar chart for 'HQ-B1'.

This screenshot shows a close-up of the search field dropdown menu. It features a text input field labeled 'Enter Filter Request Here'. Below the input field, there is a list of filter categories: Site, Service Provider, Application, Tag, Device, Interface, Interface Type, and Region. The 'Application' category is currently selected and highlighted in blue.

This screenshot shows the 'FLEX SEARCH HELP' dialog box. It contains a list of search filters categorized by type: Flow, Alert, QoS, Bfd, and System. The 'System' category is expanded, showing a table of search filters and their corresponding values. The table has two columns: the filter name and the value. The filters listed are group, device, interface, sp, site, regionid, wan, xcon, and tag. The values are represented as {value}.

Filter	Value
group	group={value}
device	device={value}
interface	interface={value}
sp	sp={value}
site	site={value}
regionid	regionid={value}
wan	wan
xcon	xcon
tag	tag={value}

# Search Functions and Flex Search

The screenshot shows a search interface with a filter bar at the top. The filter bar includes tabs for 'Site: HQ', 'Application: rtp', 'rtp-video', and 'rtp-audio', followed by a text input field 'Enter Filter Request Here'. Below the filter bar, a dropdown menu is open, displaying a list of filter categories: Tag, Device, Interface, Interface Type, and Region. To the right of the dropdown, a red circle highlights a '</>' icon, and next to it is a button labeled 'Apply filter'. Below the dropdown, a text area contains the generated Flex-Search string: 'site = "HQ" & (flow.app = "rtp" | flow.app = "rtp-video" | flow.app = "rtp-audio")'. At the bottom of the interface, a breadcrumb trail is visible: 'Site: HQ > Side > Outgoing > HQ > ...'.

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

The screenshot displays the 'RUN OR EDIT REPORT(S)' interface with three main panels: GENERAL SETTINGS, REPORT LIST, and REPORT DETAILS.

**GENERAL SETTINGS:**

- Name: DSCP
- Presentation Mode: Standard
- Footnote: Enter report group description...
- Time Zone: ☒ DST (GMT-05:00) America/New York
- Time Range: Last Fifteen Minutes
- Flex Search: Ex.: site=Honolulu & wan & flow.app=http
- Display Filter: Select Display Filter...
- Sharing Settings: Email (Enter an email address or AD entity...)
- File Format: ☐ Save PDF ☐ Save CSV

**REPORT LIST:**

- Report Name: DSCP (Flow)
- Buttons: Add New Report, Edit, Delete

**REPORT DETAILS:**

- Report Name: DSCP
- Flow Type: Basic Flow
- Report Description: Enter report description...
- Execution Type: Time Series
- Devices: All WAN Devices
- Sort By: Bit Rate
- Interfaces: All WAN Interfaces
- Business Hours: All Hours (Cannot be used with All Devices)
- Bin Duration: Auto

**Flex Search:**

- Current Search: flow
- Previous Search Terms (Flex-Search) are remembered: wan & site=Honolulu & flow.ip.src=198.18.128.81 & flow.app=http

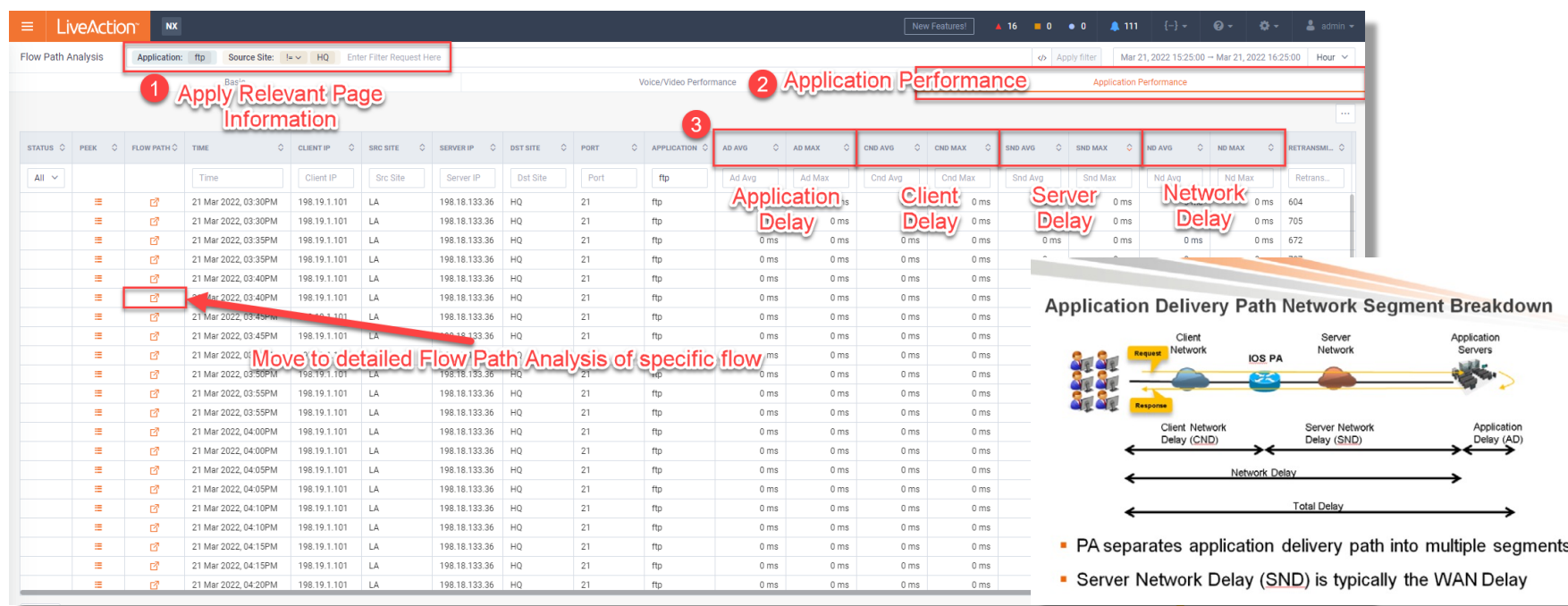
Buttons at the bottom: Cancel, Save As Template, Execute

# Application Performance (AVC Based) Visualization

Start with Flow Path Analysis

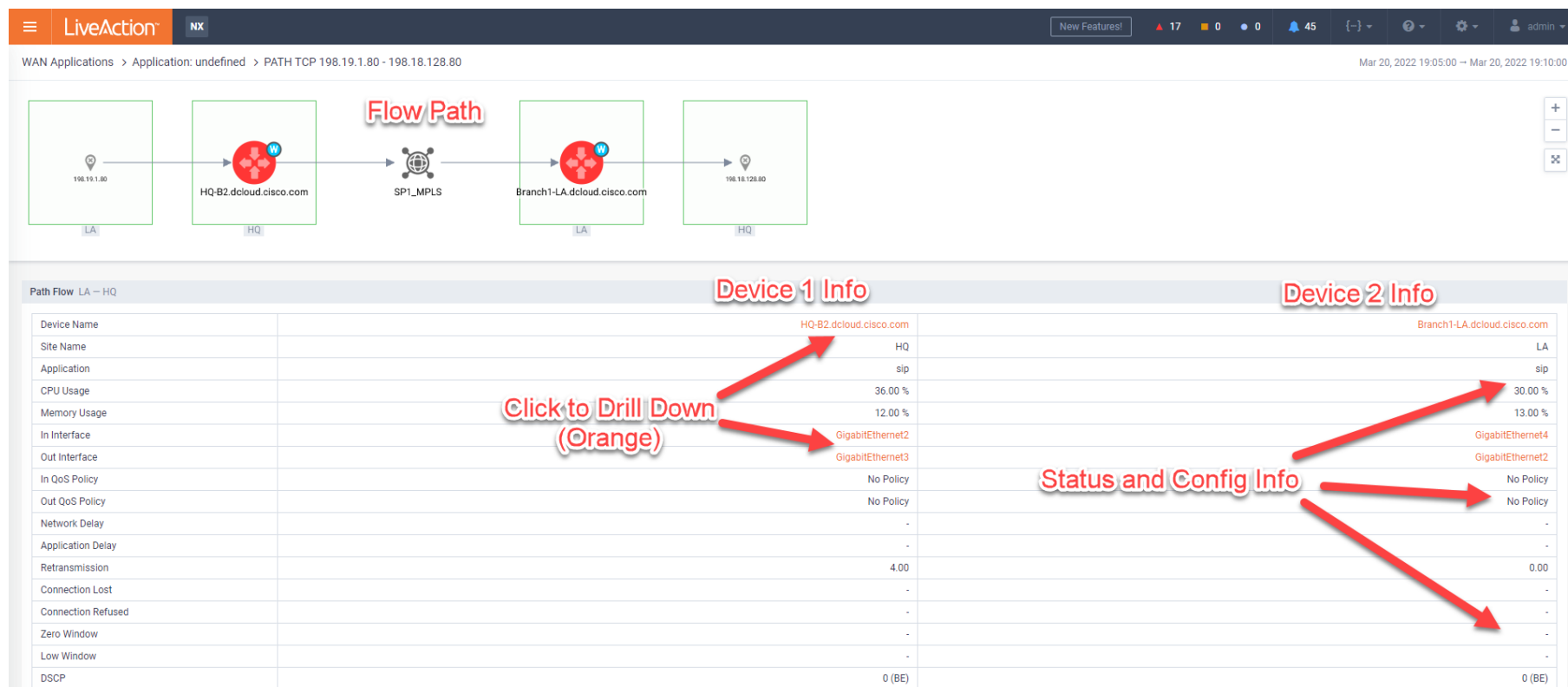
Use the Page Filter to display the interesting traffic flows

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

**1 Apply Relevant Page Information**

**2 Voice/Video Performance**

**3 Packet Loss**

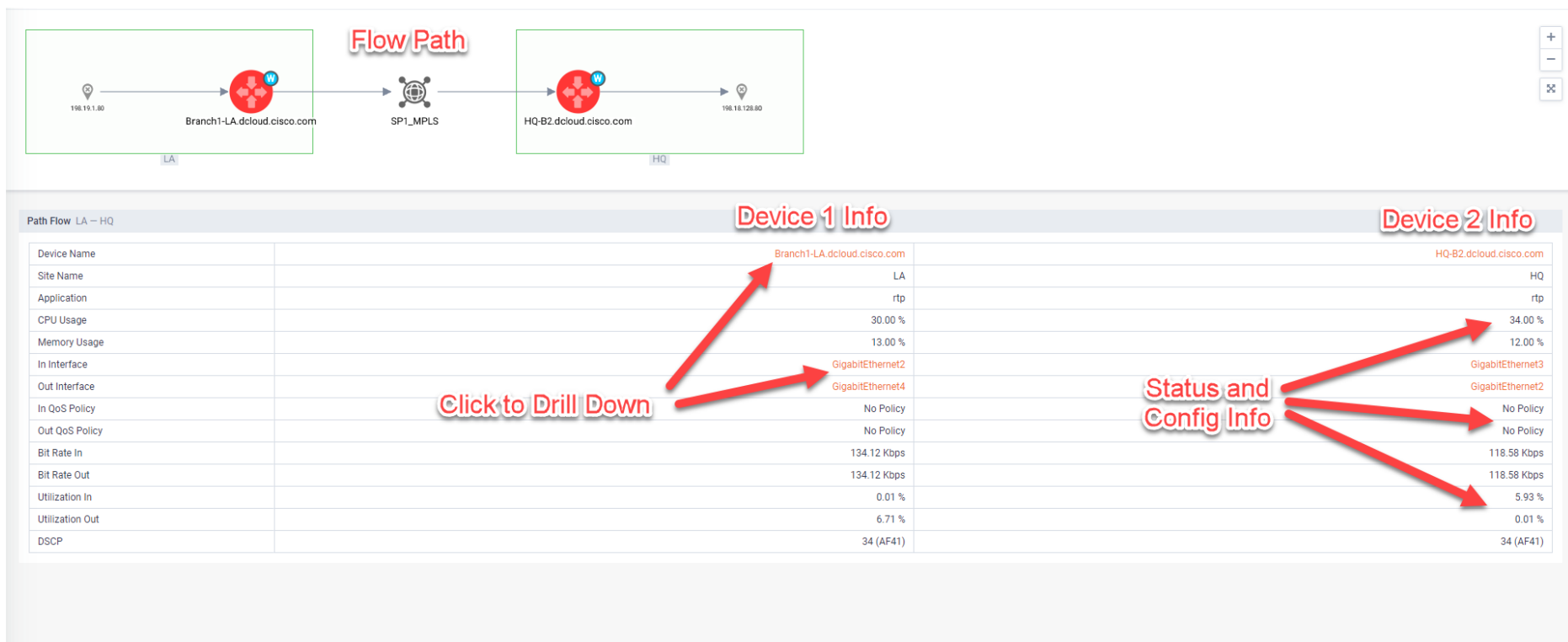
**Jitter Info**

**Move to detailed Flow Path Analysis of specific flow**

STATUS	PEEK	FLOW P.	TIME	SRC IP	SRC PORT	SRC SITE	DST IP	DST PORT	DST SITE	APPLICATION	RTP Ssrc	DSCP	PACKET LOSS	JITTER AVG	JITTER MAX	MOS
●	≡	🔍	21 Mar 2022, 05:20PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:25PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:30PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:35PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:40PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:45PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:50PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 05:55PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 06:00PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 06:05PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 06:10PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-
●	≡	🔍	21 Mar 2022, 06:15PM	198.19.1.84	31196	LA	198.18.128.84	19420	HQ	rtp	2539225492	46 (EF)	0%	200 ms	200 ms	-

# Flow Visualization

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



Responsibility	Percentage
Current government	45%
Other	55%

## RUN OR EDIT REPORT(S)

### GENERAL SETTINGS

**Name**

DSCP

**Presentation Mode**

Standard

**Footnote**

Enter report group description...

**Time Zone**

☒ DST  
(GMT-05:00) America/New York

**Time Range**

Custom

**Start Date**

03/20/2022

**Start Time**

17:11

**End Date**

03/20/2022

**End Time**

17:26

**Flex Search** ⓘ

Ex.: site=Honolulu & wan & flow.app=http

**Display Filter**

Select Display Filter...

### REPORT LIST

DSCP (Flow)Fast

Add New Report

## Historical Reports Set Date/Time/Timezone Parameters

New Features!

▲ 16

■ 0

● 0

111

admin

</>

Apply Filter

Mar 20, 2022 16:30:00 → Mar 20, 2022 17:30:00

Hour ▼

ce

E	APPLICATION	RTP SSRC	DSCP	PAC
Site	Application	Rtp Ssrc	Dscp	P
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	
	rtsp	2539225492	46 (EF)	

SET THE END DATE & TIME

<

Apr 2021

>

Today

S

M

T

W

T

F

S

28

29

30

31

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

1

2

3

4

5

6

7

8

^

^

05

:

11

PM

Reset to Now

▼

▼

Apply

INTERVAL

5 Mins

15 Min

Hour

0%

200 ms

200 ms

-



# Device Configuration

---

## 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**

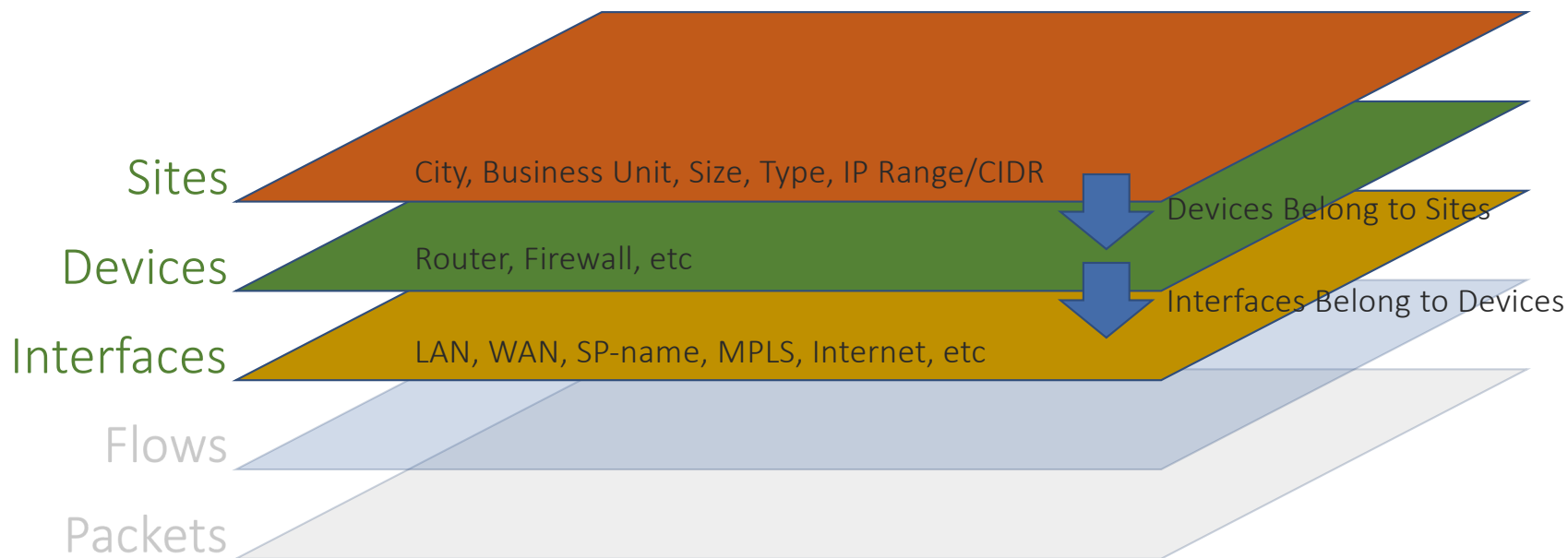
Tags are your best friend – Let them support your work in LiveNX



# 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.

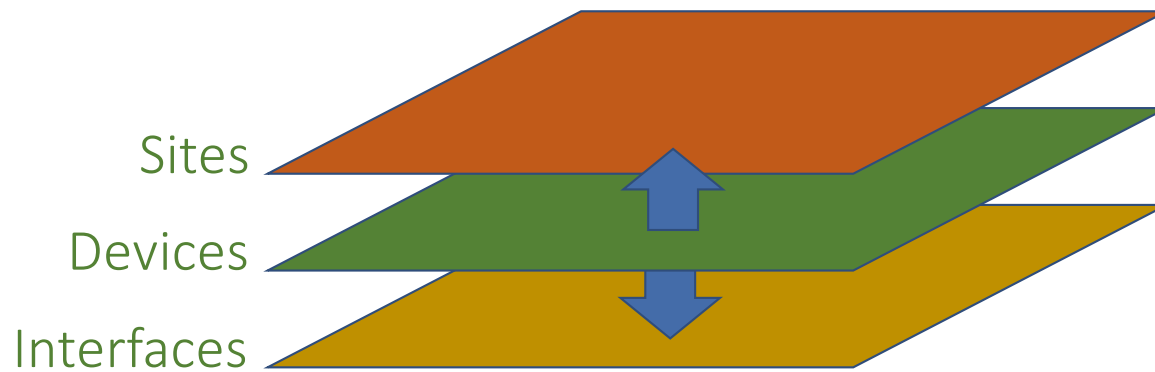


Best Practice:

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

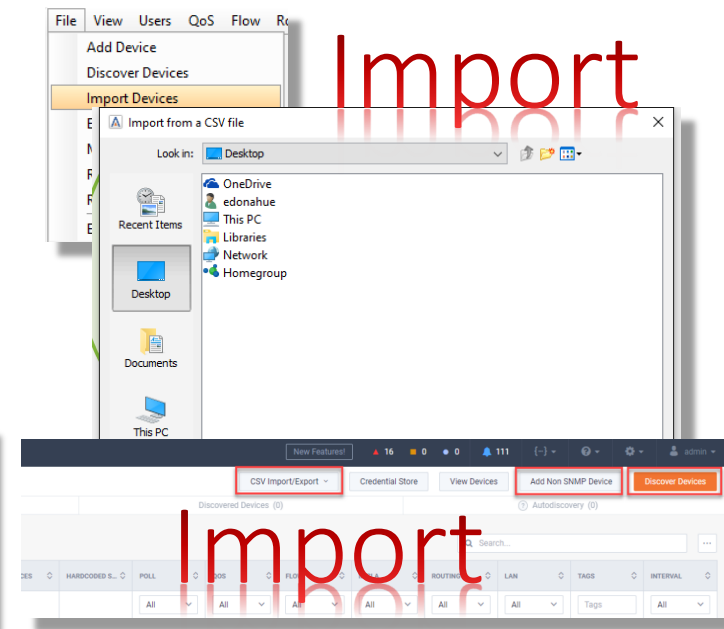
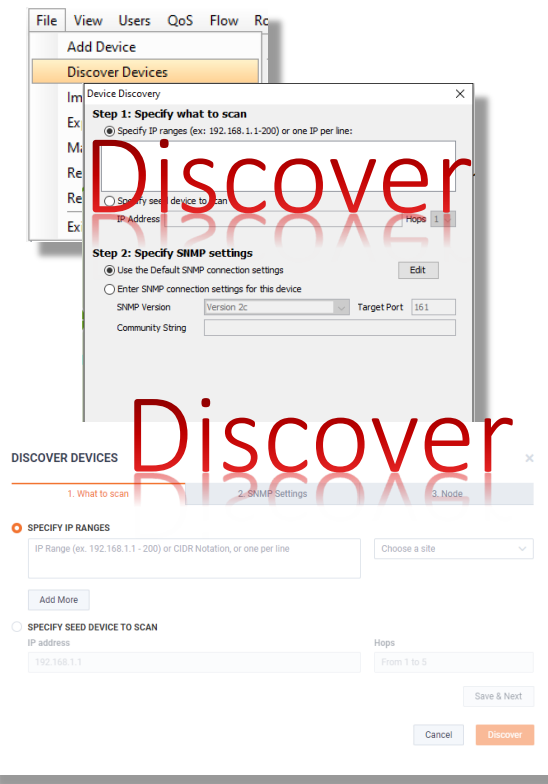
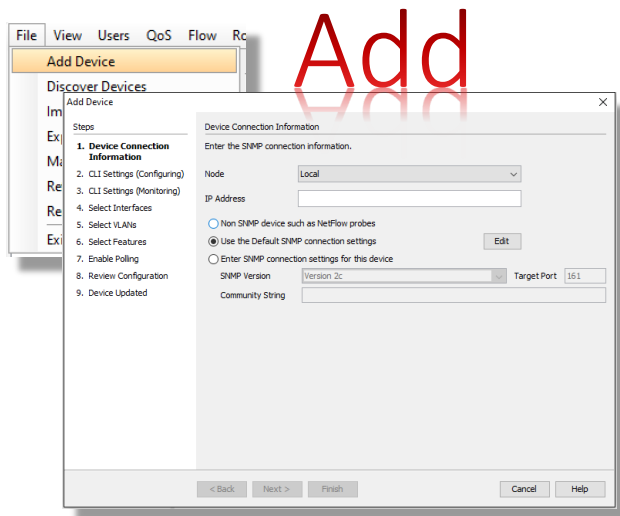
## Adding Devices to LiveNX

- 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...

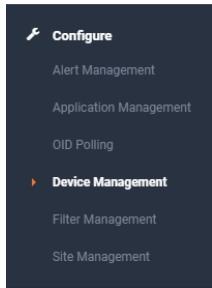


Add – Discover – Import  
Both on the Eng Console,  
and the WebUI

# 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.

A screenshot of the 'DISCOVER DEVICES' dialog box. The dialog has a title bar with a close button (X). Below the title bar is a progress indicator with three steps: '1. What to scan' (active), '2. SNMP Settings', and '3. Node'. The main content area has two radio button options: 'SPECIFY IP RANGES' (selected) and 'SPECIFY SEED DEVICE TO SCAN'. Under 'SPECIFY IP RANGES', there is a text input field containing '198.19.2.1' and a dropdown menu labeled 'Choose a site'. Below this is an 'Add More' button. Under 'SPECIFY SEED DEVICE TO SCAN', there is a text input field for 'IP address' containing '192.168.1.1' and a text input field for 'Hops' containing 'From 1 to 5'. At the bottom right, there are three buttons: 'Save & Next', 'Cancel', and 'Discover'.

# Device Discovery... Simple Steps

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

The screenshots illustrate the process of adding devices and interfaces to LiveNX:

- Step 1:** The 'Discover Devices' button is highlighted. A red box labeled 'Scans the Address/Subnet' points to the 'Discover Devices' button.
- Step 2:** The 'SELECT DEVICES' screen is shown. A red box labeled 'Results Listed - Only Devices' points to the table of discovered devices.
- Step 3:** The 'SELECT INTERFACES' screen is shown. A red box labeled 'Select Interfaces' points to the table of available interfaces.

**Table 1: Discovered Devices**

DEVICE	SERIAL	IP ADDRESS	VENDOR	MODEL	NODE	INTERFACES	HARDCODED SAMPLE RATE
Device	Serial	IP Address	Vendor	Model	Node	Interfaces	
Branch2-NY	0000000021	198.19.2.1	Cisco	ciscoProducts 3004	Local/Server	7	

**Table 2: Selected Interfaces**

NAME	INTERFACE STATE	DEVICE	LINE RATE (Kbps)	IP ADDRESS	LABEL	INPUT CAPACITY (Kbps)	OUTPUT CAPACITY (Kbps)	WAN/CON	SERVICE PROVIDER	TAGS	DESCRIPTION
GigabitEthernet2	Up	Branch2-NY	1000000	198.19.2.1	Branch2 LAN			WAN	Branch2 LAN		Branch2 LAN
GigabitEthernet3	Up	Branch2-NY	1000000	100.64.2.2	WAN_SP2_MPLS2			WAN	WAN_SP2_MPLS2		WAN_SP2_MPLS2
GigabitEthernet1	Up	Branch2-NY	1000000	192.168.122.161							
GigabitEthernet4	Up	Branch2-NY	1000000	10.255.2.2							WAN_SP1_MPLS2
Loopback0	Up	Branch2-NY	8000000	10.0.2.1							
Null0	Up	Branch2-NY	10000000								
Vlan-Null0	Up	Branch2-NY	10000000								

# Working Topology – Device Needs Semantic Data

Device Management

My Devices (4) My Interfaces (10) Discovered Devices (0) Autodiscovery (0)

Only Part Way There... Semantics

DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED S...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS	INTERVAL
HQ-B1	Up	198.18.129.24	Cisco	ciscoProducts...	Local/Server	HQ	2		✓	✓	✓					10 seconds
Branch1-LA	Up	198.19.1.1	Cisco	ciscoProducts...	Local/Server	LA	3		✓	✓	✓					10 seconds
HQ-B2	Up	198.18.129.25	Cisco													10 seconds
Branch2-NY	Up	198.19.2.1	Cisco													1 minute

Click on Device name to open config dialogue

Add/Create Semantic Data

EDIT BRANCH2-NY.DCLOUD.CISCO.COM

Site: NY Group: NY Interval: 10 Seconds

IP Address\*: 198.19.2.1

☒ POLL ☐ IP SLA ☒ QOS ☐ ROUTING ☒ FLOW ☐ LAN

Associate Probe at IP Address: Type IP Address Hardcode Sample Ratio: 1/

Tags: East Sales Office Branch 3

Cancel Apply

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

LiveAction®

# Devices Belong to Sites – Adding Sites And Semantics

LiveAction NX

New Features! 17 0 0 111

Site Management

Setting Up Sites

Add Edit Delete

Search...

	SITE	DATA CENTER	DEVICES	CONTAINS DEVICES	NO. OF EMPLOYEES	BUSINESS HOURS	IP RANGES	GEO LOC	ADDRESS	REGION	DESCRIPTION	TAGS
<input type="checkbox"/>	Site	All	Devices	All	No. of Employees	Business Hours	IP Ranges	All	Address	Region	Description	Tags
<input type="checkbox"/>	HQ		HQ-B1.dcloud.cisco.co...	✓		Mo - Fr   8:00 am - 5:00...	198.18.128.0/18	↗	San Francisco, CA	San Francisco, Califor...	Headquarters Data Ce...	
<input type="checkbox"/>	LA		Branch1-LA.dcloud.cis...	✓		Mo - Fr   8:00 am - 5:00...	198.19.1.0/24   10.0.1.1	↗	Los Angeles, CA	Los Angeles, Californi...	Branch 1	
<input type="checkbox"/>	NY		Branch2-NY.dcloud.cis...	✓		None						

EDIT 1 SITE

Details Address Business hours

Site Description  
New York Sales Location. Opened 15 October 1995.

Site IP Range (CIDR Notation IP's)  
198.19.2.0/24

Devices  
Branch2-NY.dcloud.cisco.com x 1

Tags  
Dont Confuse Site and Device Tags..... x 1

Number of Employees  
50

☐ Data Center

More Semantic Data = Greater Flexibility in monitoring/Troubleshooting

Cancel Save

EDIT 1 SITE

Details Address Business hours

Address  
Address Line 1  
Address Line 2

Latitude & Longitude  
40.709329  
-74.013120

City  
New York

State/Province/Region  
NY

Zip Code  
10006

Country  
United States

Phone Number  
555-123-4567

Email  
nykeycontact@acme.com

Region  
Continent: North America → Country: United States → State: New York → City: New York

Geo Coordinate Lookup Remove Region

Cancel Save

Response	Percentage
Yes	75%
No	25%





# Configure Flow Collection - Engineering Console

**Flow Configuration Table (Screenshot 2):**

Select	Device	Type	IP Address	Description	Tags	Traffic...	Applica...	Voice/Vide...	Traditio...	Custom
<input type="checkbox"/>	Branch1-LA	Standard	198.19.1.1	Cisco IOS S...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Branch2-NY	Standard	198.19.2.1	Cisco IOS S...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	HQ-SJ	Standard	198.18.129.25	Cisco IOS S...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Flow Configuration Table (Screenshot 3):**

Device	Type	IP Address	Description	Tags	Traffic ...	Applica...	Voice/Vide...	Traditio...	Custom
Branch1-LA	Standard	198.19.1.1	Cisco IOS So...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/0	-	198.19.1.1	Branch1 LAN	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/1	-	100.64.1.2	Internet	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/2	-	10.255.1.2	MPLS	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loopback0	-	10.0.1.1	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Branch2-NY	Standard	198.19.2.1	Cisco IOS So...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/0	-	198.19.2.1	Branch2 LAN	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/1	-	100.64.2.2	Internet	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/2	-	10.255.2.2	MPLS	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loopback0	-	10.0.2.1	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HQ-SJ	Standard	198.18.129.25	Cisco IOS So...	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/0	-	198.18.129.25	-	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethernet0/1	-	10.255.0.2	-	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

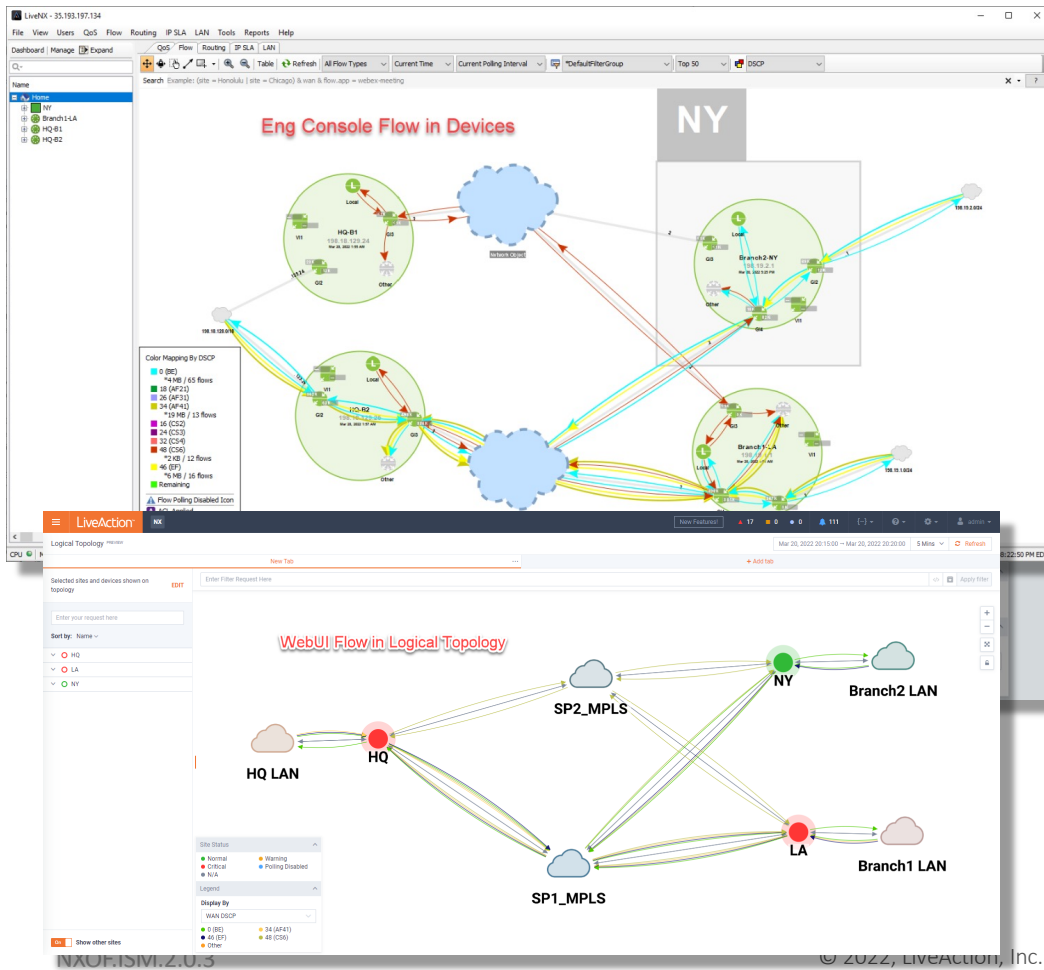
**Multiple CLI Viewer (Screenshot 4):**

```

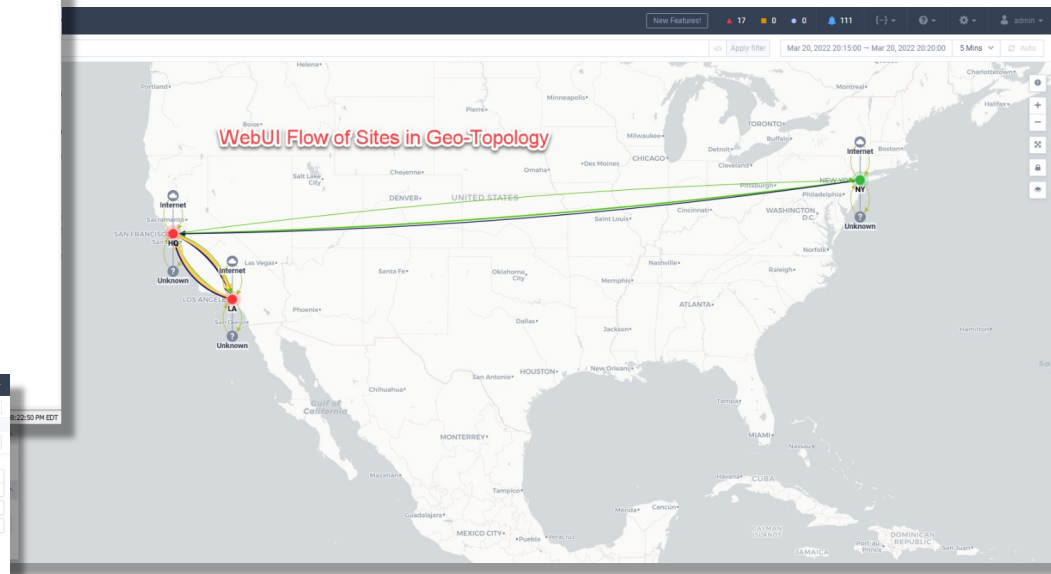
Branch1-LA
config t
ip access-list extended LIVEACTION-ACL-AVC
permit top any any
exit
policy-map type performance-monitor LIVEACTION-POLICY-THRESH
class-map match-any LIVEACTION-CLASS-AVC
exit
class-map match-any LIVEACTION-CLASS-MEDIANET
exit
class-map LIVEACTION-CLASS-AVC
match access-group name LIVEACTION-ACL-AVC
exit
class-map LIVEACTION-CLASS-MEDIANET
match protocol rtp
match protocol telepresence-media
exit
policy-map type performance-monitor LIVEACTION-POLICY-THRESH
class LIVEACTION-CLASS-AVC
class LIVEACTION-CLASS-MEDIANET
exit
interface Ethernet0/2
service-policy type performance-monitor output LIVEACTION-POLICY
service-policy type performance-monitor input LIVEACTION-POLICY
flow record type performance-monitor LIVEACTION-FLOWRECORD-AVC
description DO NOT MODIFY. USED BY LIVEACTION.
match application name account-on-revolution
match connection client ip address
match connection server ip address
match connection server transport port
match ipv4 protocol
match protocol

```

# View Traffic Flows!



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



LiveAction®

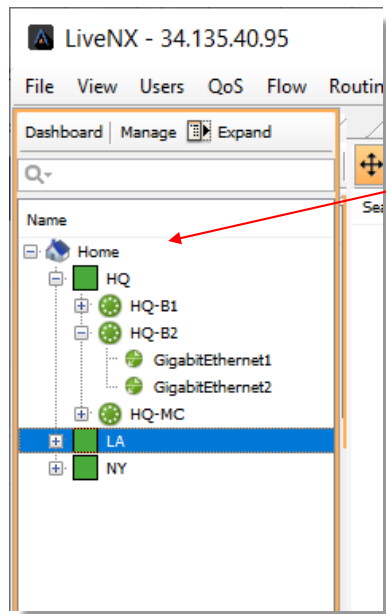
© 2022, LiveAction, Inc. All Rights Reserved.

# Topology Basics – Grouping in Engineering Console

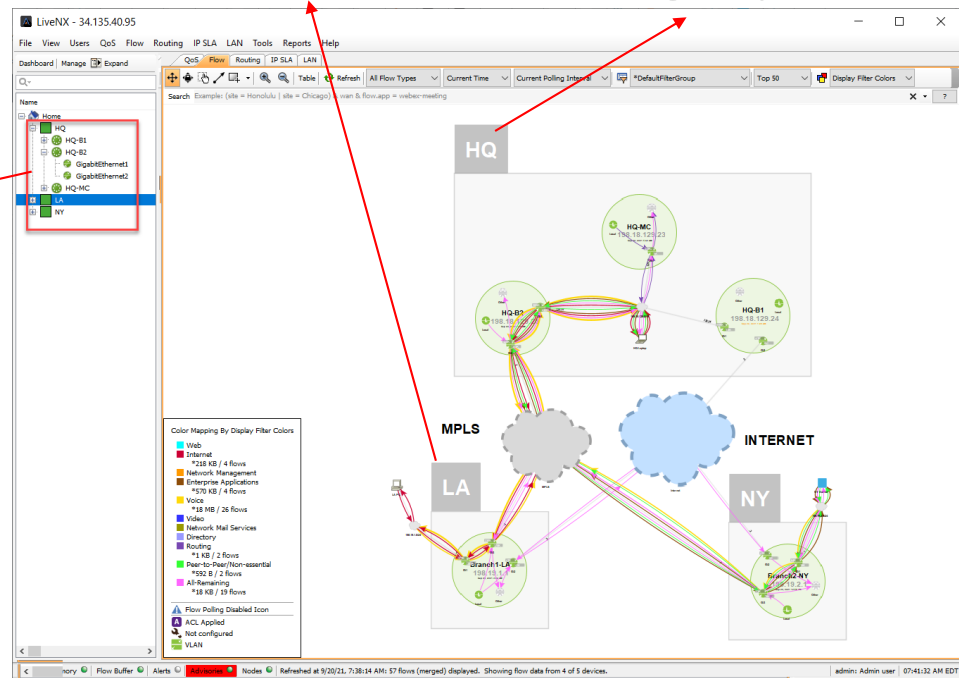
\*Grouping only visually applied in LiveNX Eng Console (WebUI Uses Sites – You need to use BOTH)

\*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.

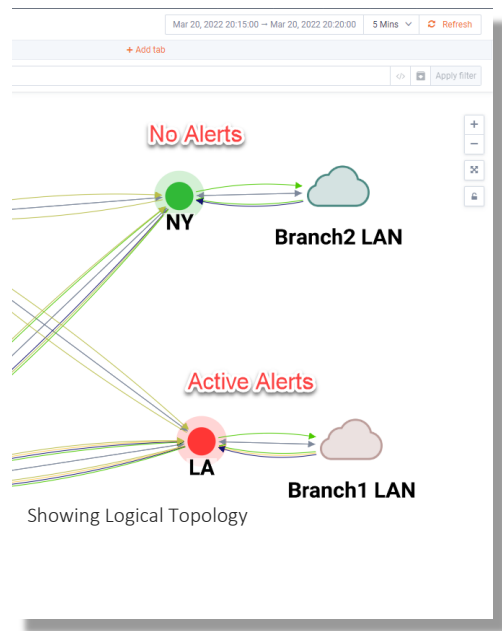


Grouping makes device management easier!

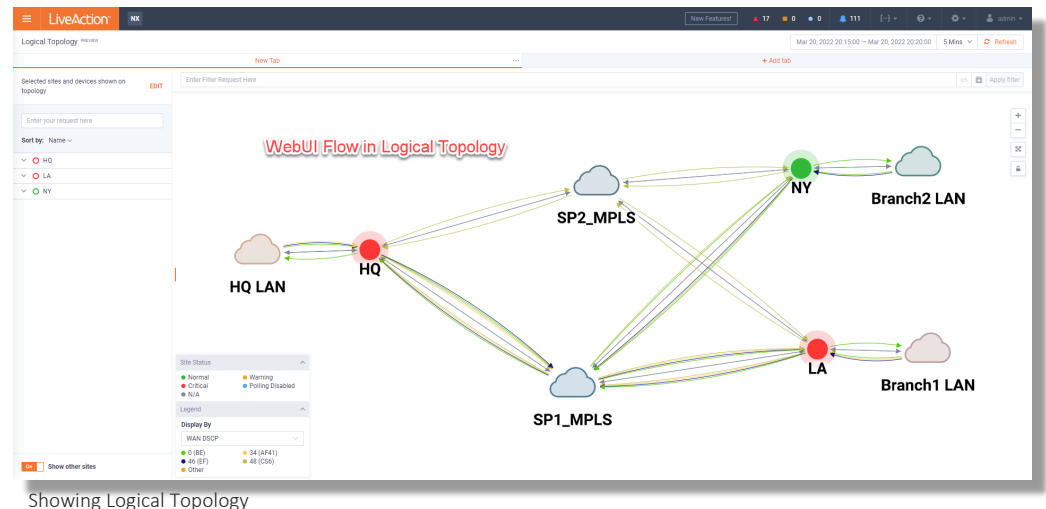
LiveAction®

# Topology Basics

Devices reporting issues will change colors to prompt for investigation.



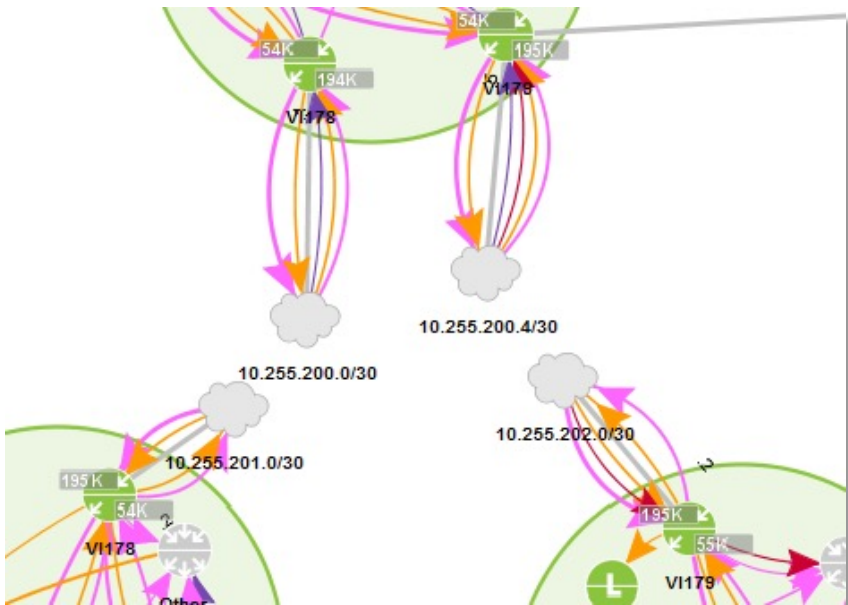
Quickly identify many problem sites visually



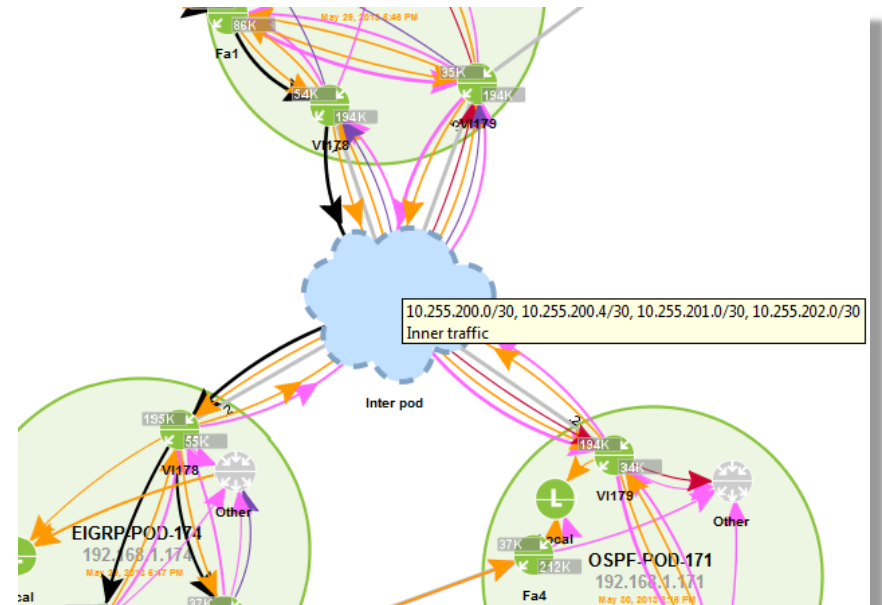
# Merge Clouds\*

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



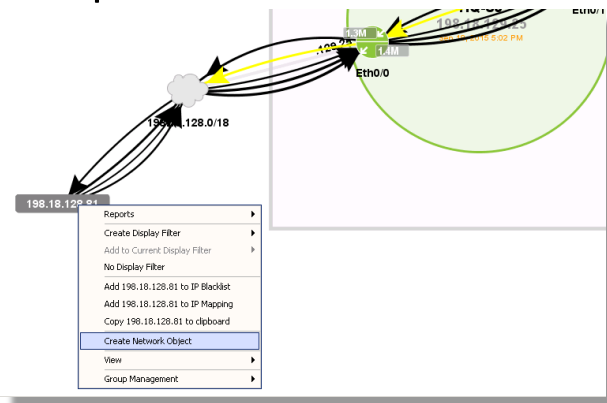
LiveAction®

# Topology Basics – Add Network Object\*

Do it the EASY way!

## Step 1

Right-Click on Flow Endpoint

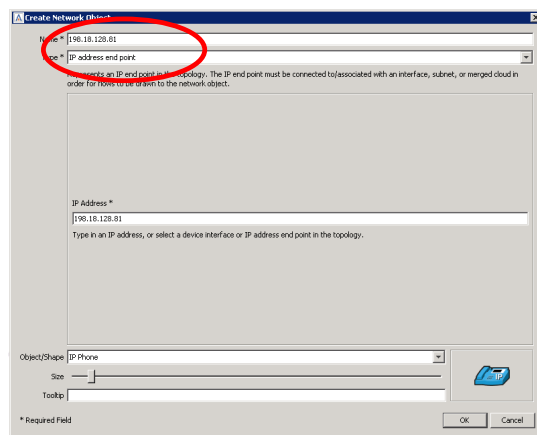


\*Merge Clouds only applied in LiveNX Engineering Console

NXOF.ISM.2.0.3

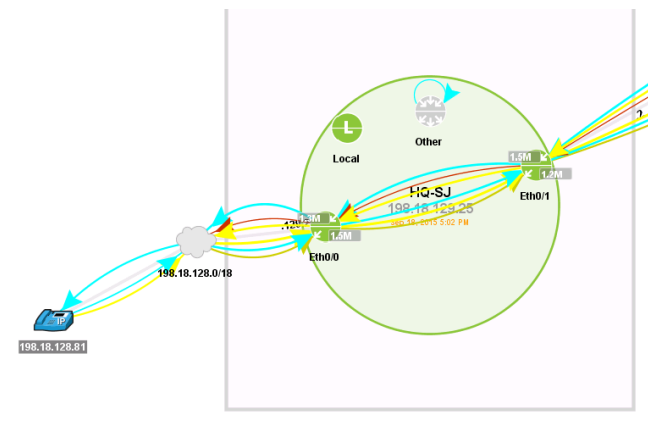
## Step 2

Select the Object Shape



## Step 3

Flows now connect



LiveAction®

© 2022, LiveAction, Inc. All Rights Reserved.

# 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





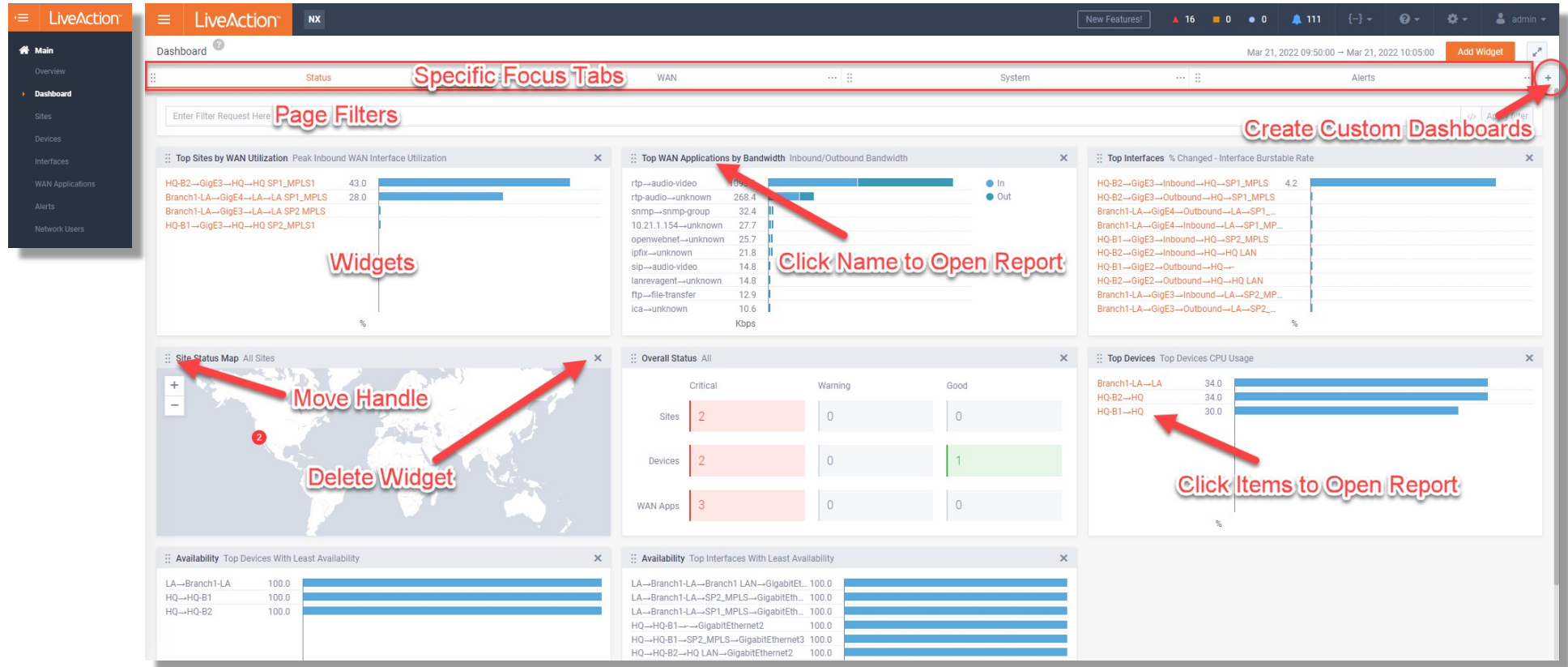


# Reports & Alerts

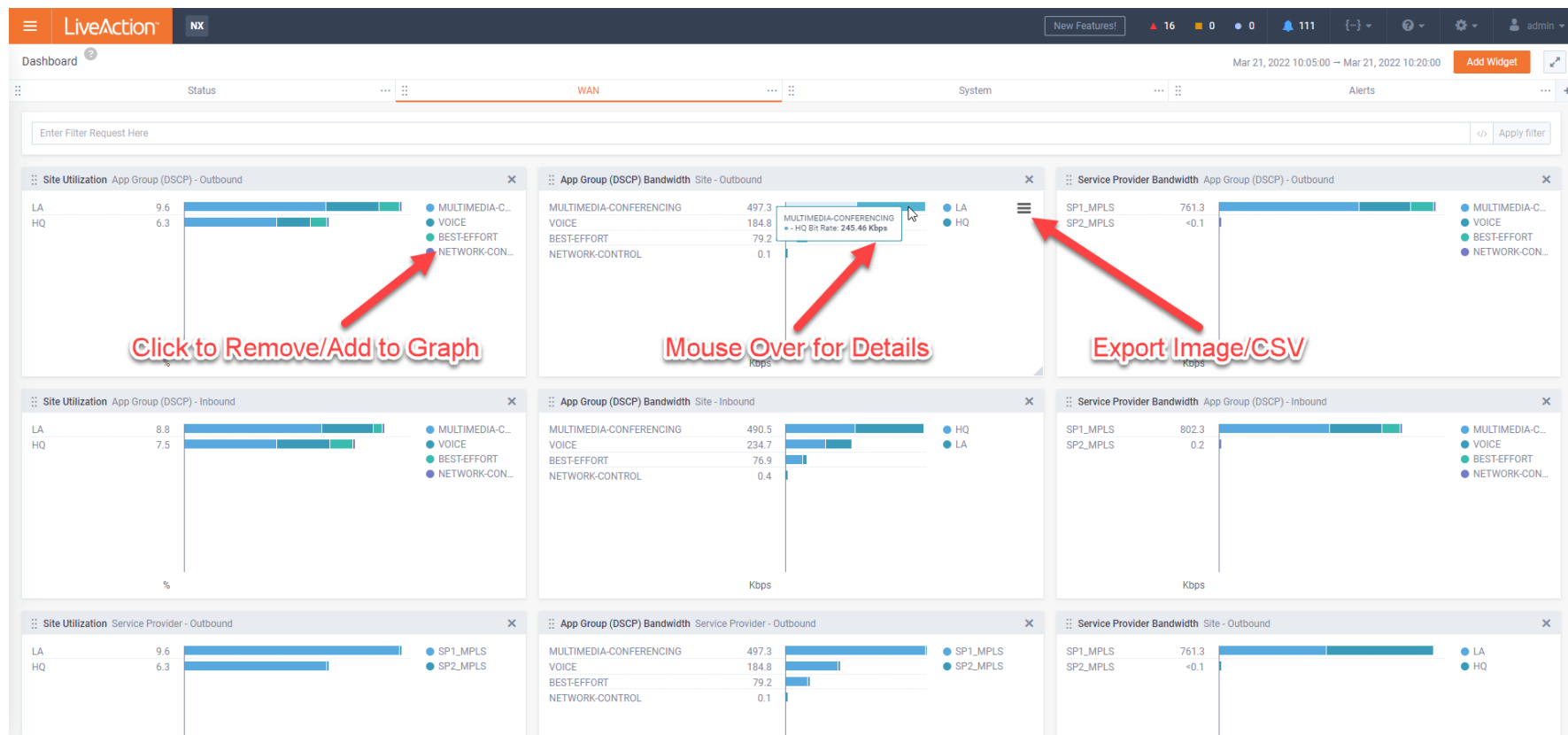
Using LiveNX WebUI



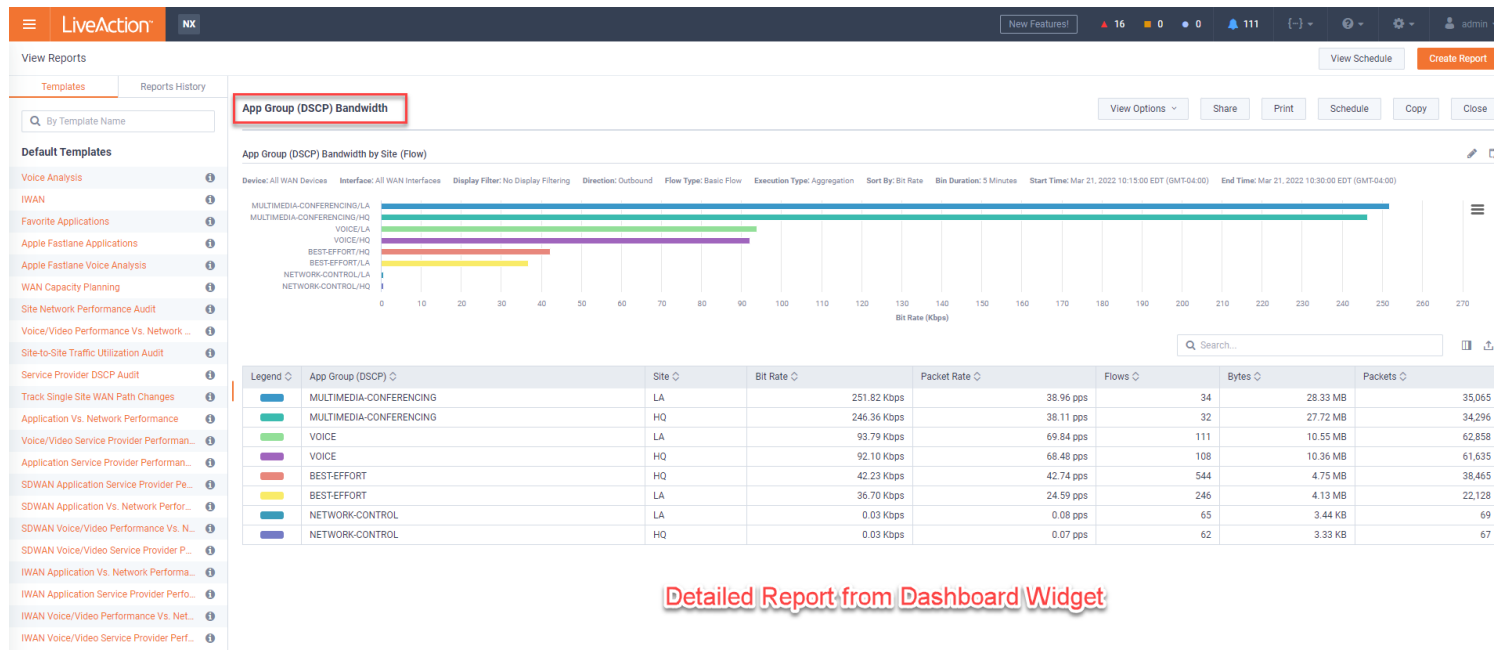
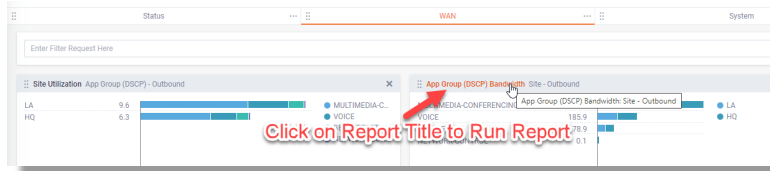
# Dashboard



# WAN Dashboard – One of the Defaults



# Drill-Down to Reports

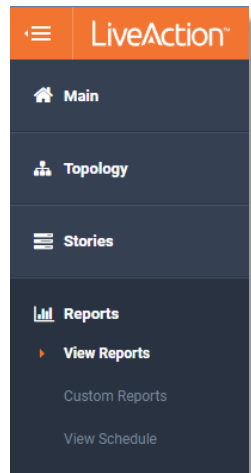


Detailed Report from Dashboard Widget

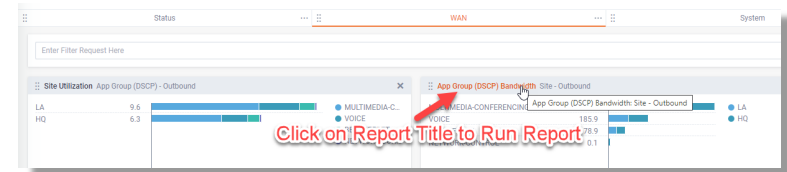
# Creating Reports

## Multiple Roads Lead to Reports

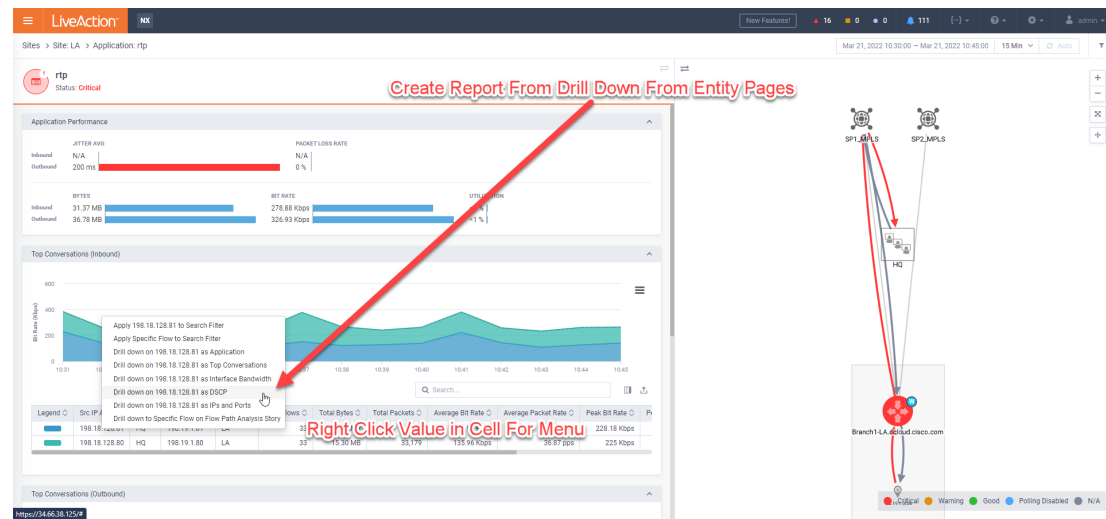
From Navigation Menu



From Any Dashboard Item



Drill Down From Entity Pages



# Creating a Report

The screenshot shows the 'RUN OR EDIT REPORT(S)' dialog box in the LiveAction interface. The dialog is divided into three main sections: GENERAL SETTINGS, REPORT LIST, and REPORT DETAILS.

- GENERAL SETTINGS:** Includes fields for Presentation Mode (Standard), Footnote, Time Zone (GMT-05:00 America/New York), Time Range (Last Fifteen Minutes), Flex Search (Ex: site=Honolulu & wan & flow.app=http), Display Filter (Select Display Filter...), Sharing Settings, Email, and File Format (Send PDF, Send CSV).
- REPORT LIST:** A table listing various reports. The 'Application DSCP Audit (Flow)' report is highlighted with a red box and a red arrow pointing to it. A red annotation 'Apply to All Reports in this single/multi-report request' points to the top of the list. Another red annotation 'List of Reports in this single/multi-report request' points to the list itself.
- REPORT DETAILS:** Includes fields for Report Name (Application DSCP Audit), Report Description (Enter report description...), Devices (All WAN Devices), Interfaces (All WAN Interfaces), Flex Search (Ex: site=Honolulu & wan & flow.app=http), Display Filter (No Display Filtering), Direction (Inbound and Outbound Combined), Flow Type (Basic Flow), Execution Type (Time Series), Sort By (Bit Rate), Business Hours (All Hours), and Bin Duration (Auto). A red annotation 'Editable Fields' points to the Report Name field. A red annotation 'Details of Report Highlighted in the list' points to the Report Name field. A red box highlights the Bin Duration section, containing a 'Caution!' note: 'Raw Flow Data: Due to the options selected, this report will utilize the Raw Flow datastore (slower).'

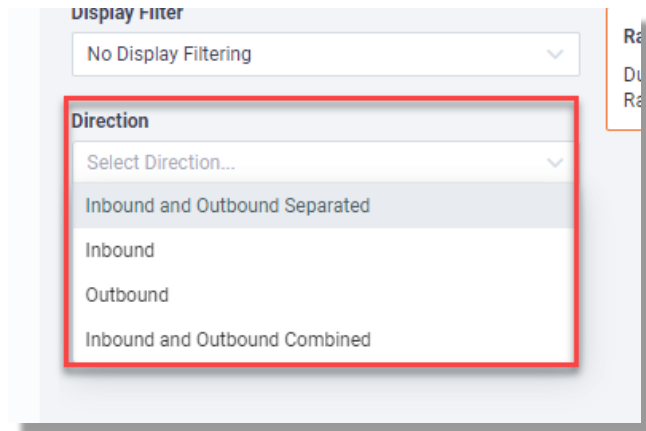
Buttons at the bottom include Cancel, Save As Template, and Execute.

# Flow Report - Directionality

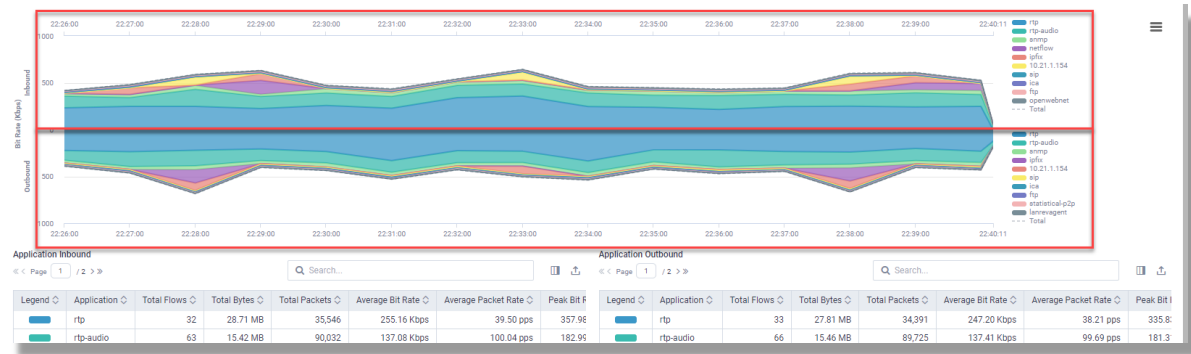
Data Volumes can be viewed by ingress, egress, both on one chart, or combined (single number)

You can choose between how the data is presented in reports

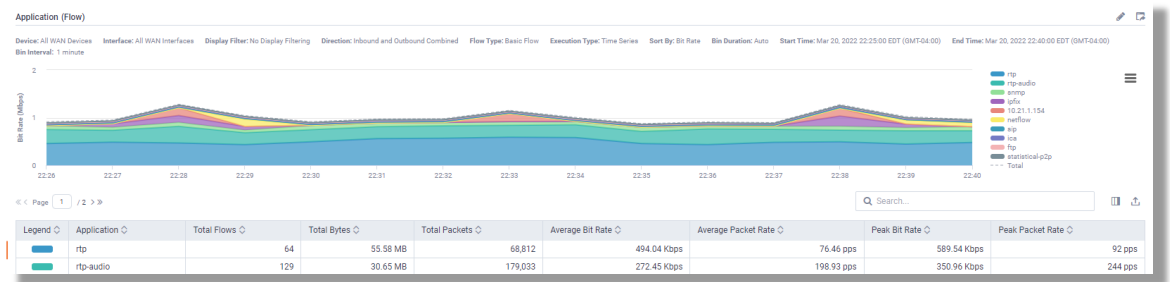
Configured in Report Settings



Inbound and Outbound Separated



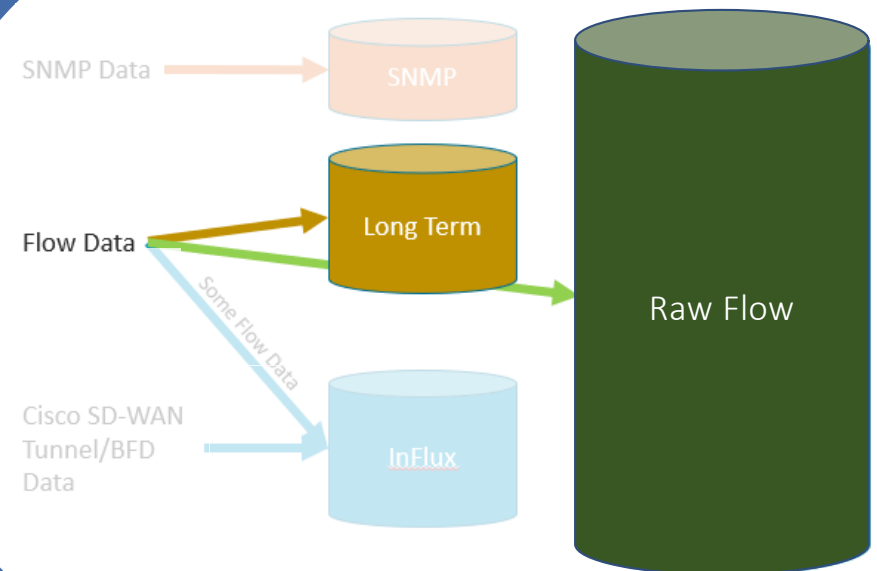
Inbound and Outbound Combined



## 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!



# 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.

The screenshot displays the LiveAction NX web interface. On the left, a dark sidebar menu contains the following items: Settings (highlighted with a red box), System Diagnostics, User Management, and LiveNX Server. The main content area is titled 'Settings' and includes a search bar. A list of configuration categories is shown, with 'Data Source Management' highlighted by a red box. Below this, the 'Flex String' configuration is visible, showing the value 'wan | xcon' (also highlighted with a red box). A warning message states: 'The data source is a flex search which determines what flow data will be pre-aggregated. Modifying this setting may affect report performance for queries of large time ranges. This setting should be modified with caution as it may introduce performance issues.' At the bottom right of the configuration area are 'Reset to Default' and 'Apply' buttons.



---

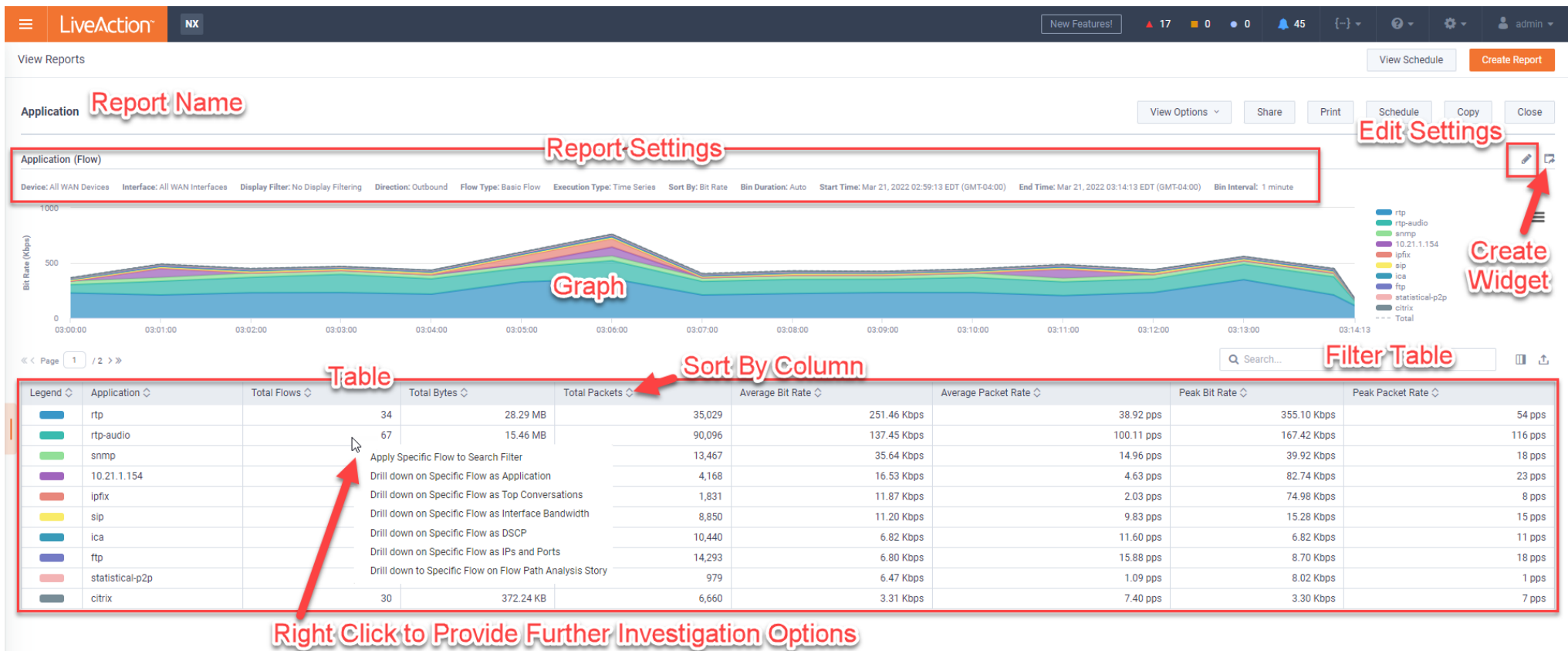
## Commonly Used Reports

- 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)

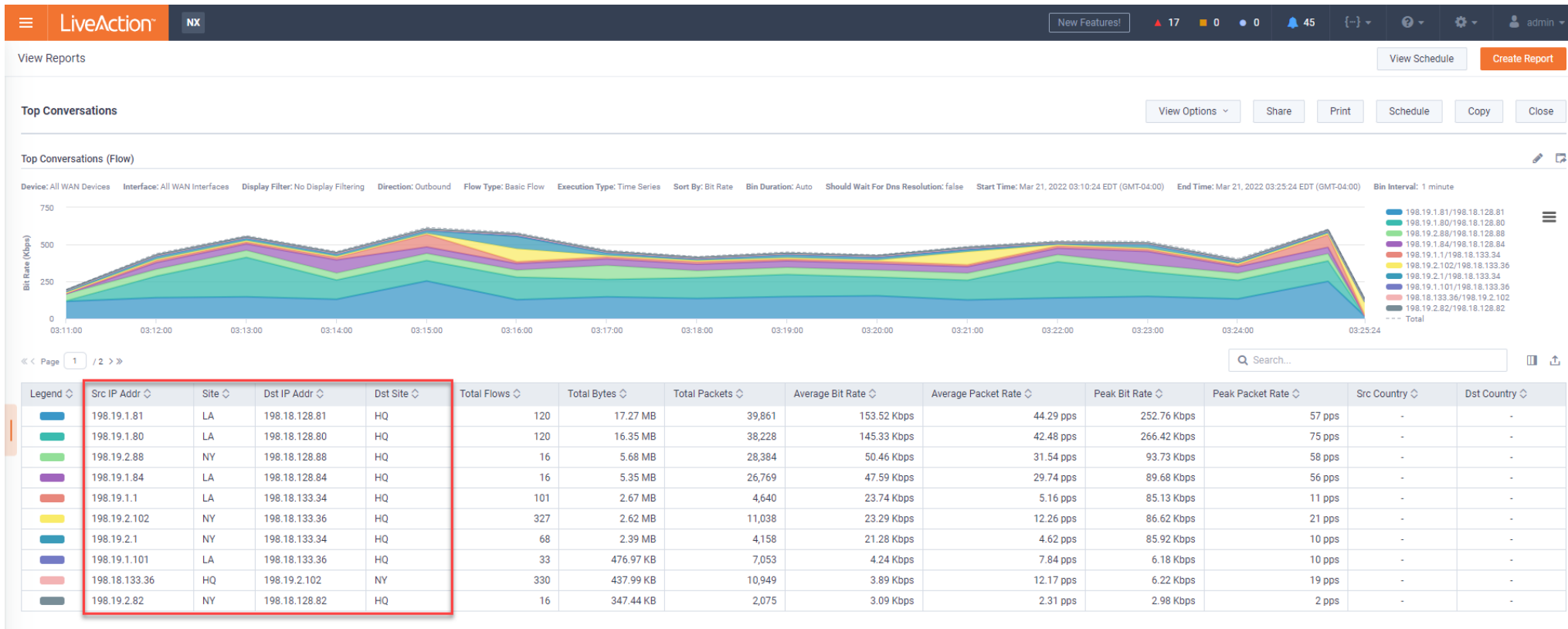
Different data sources will provide different perspectives of your network

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

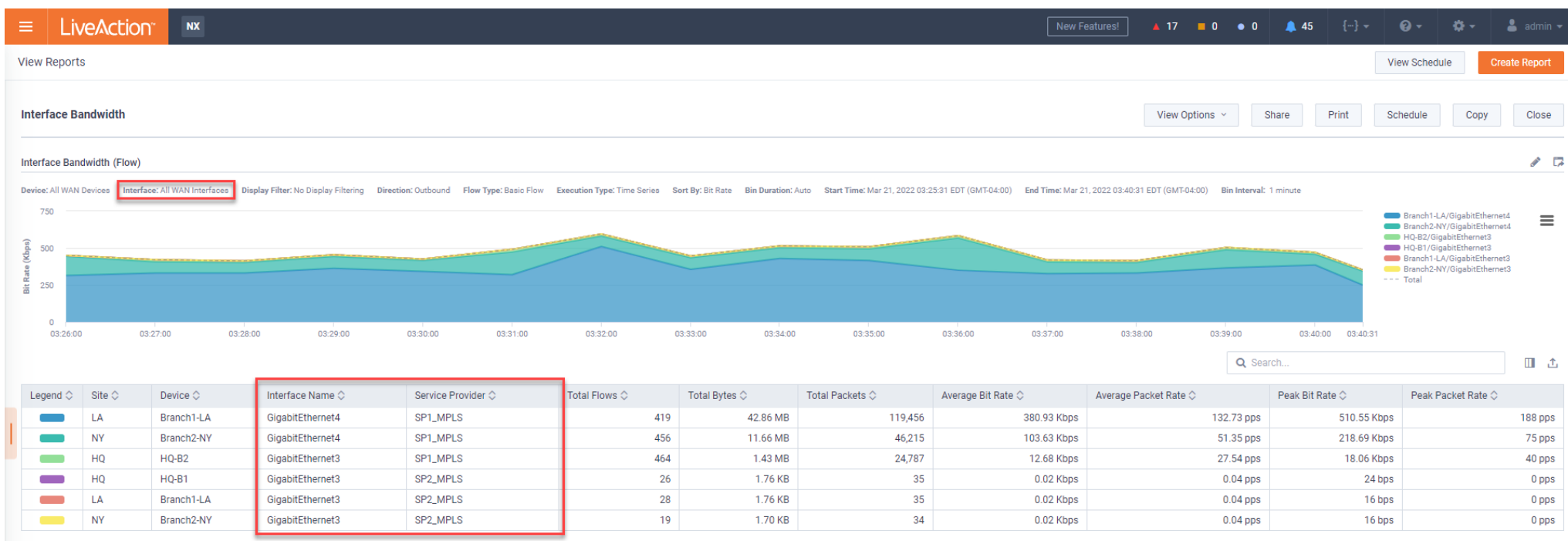
# Application (Flow)



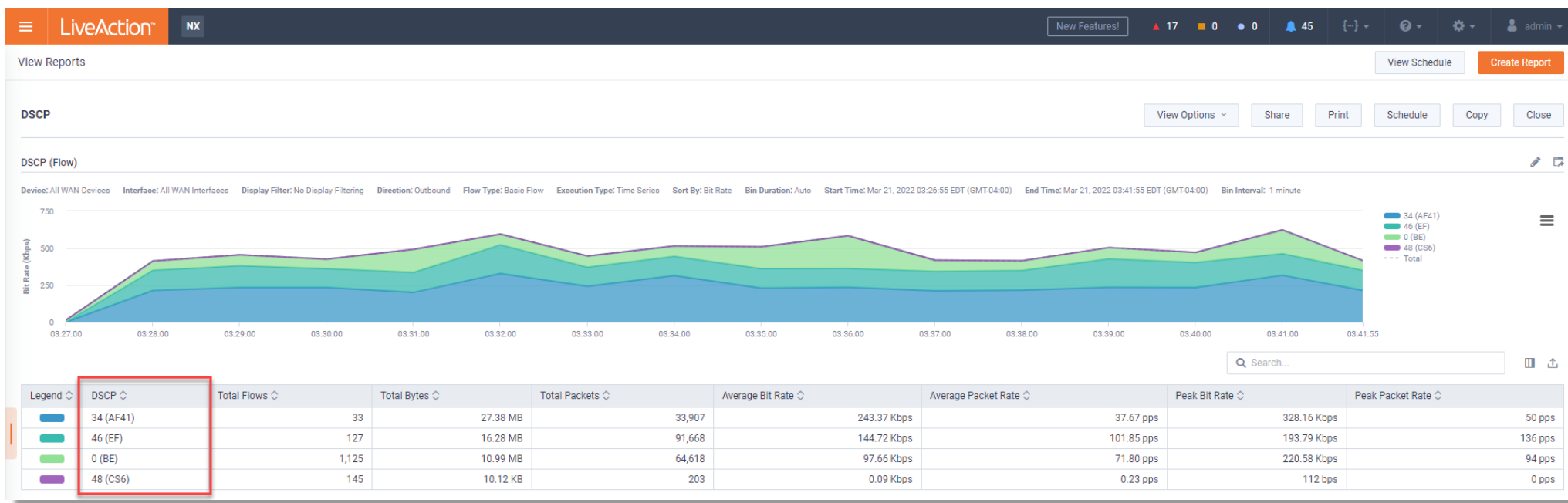
# Top Conversations (Flow)



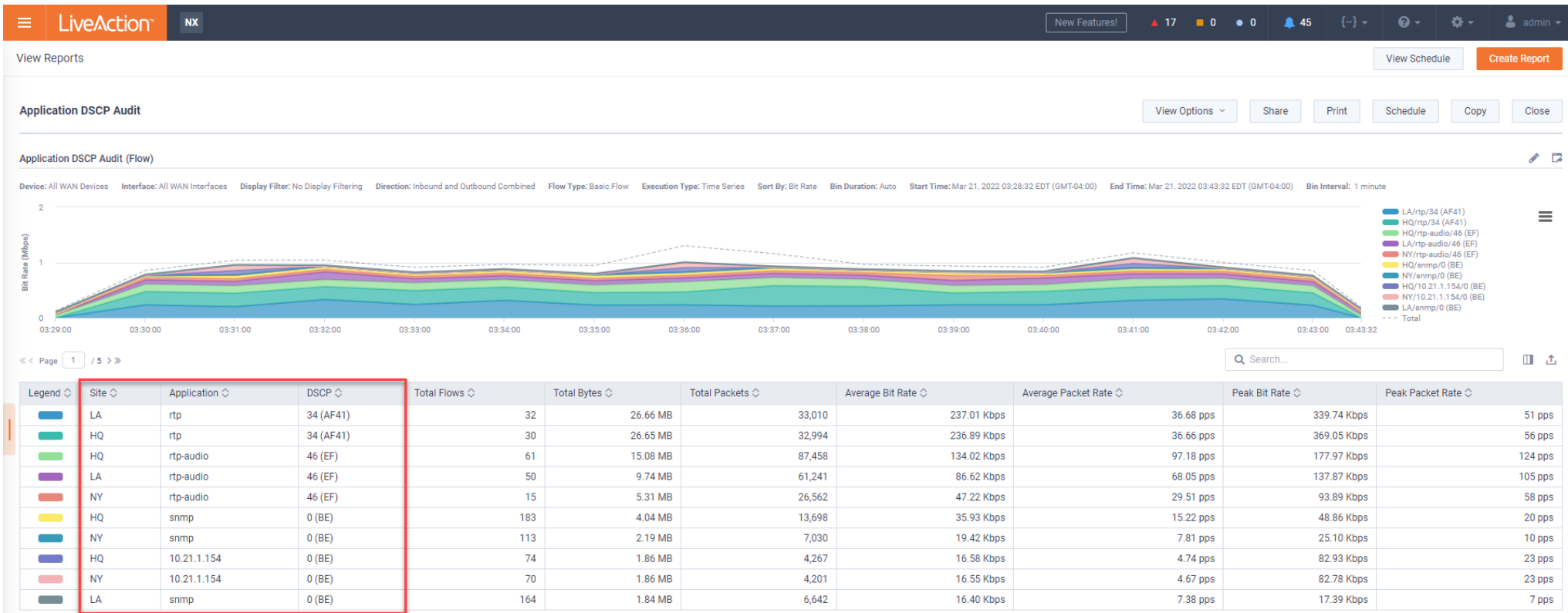
# Interface Bandwidth (Flow)



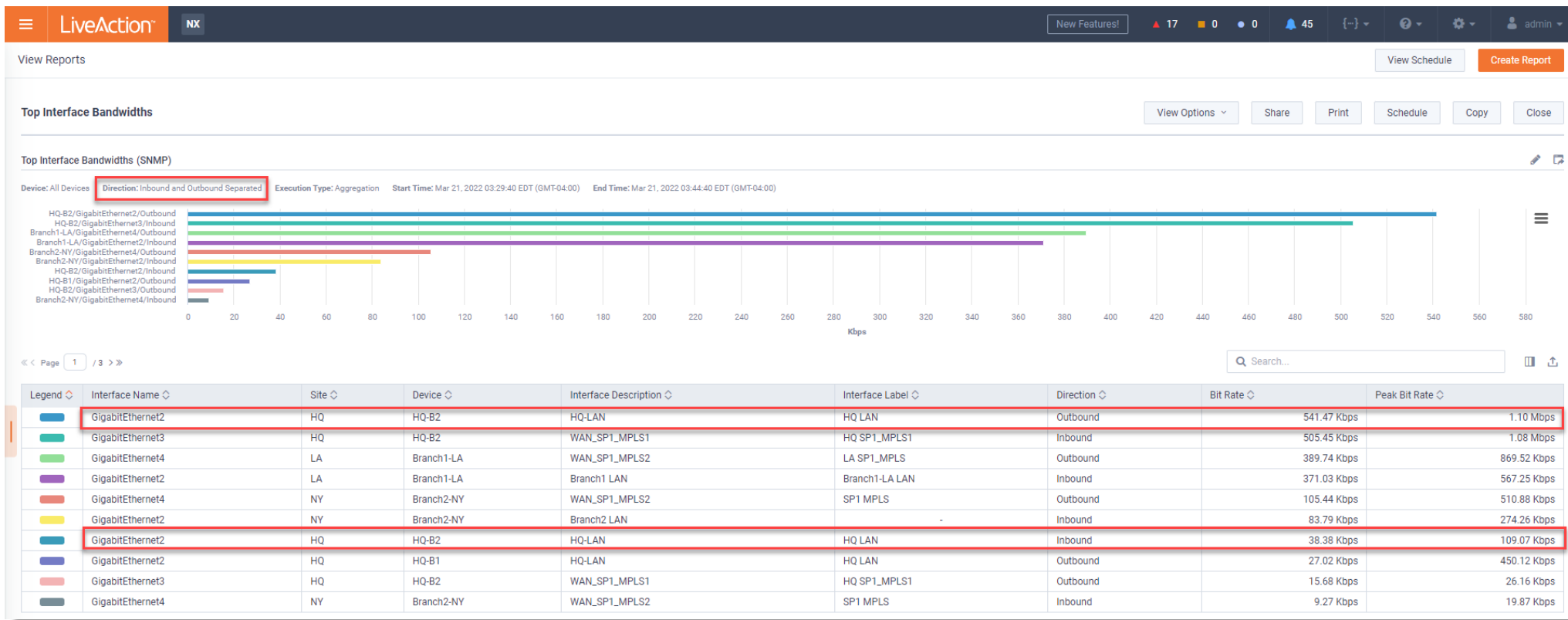
# DSCP (Flow)



# Application DSCP Audit (Flow)

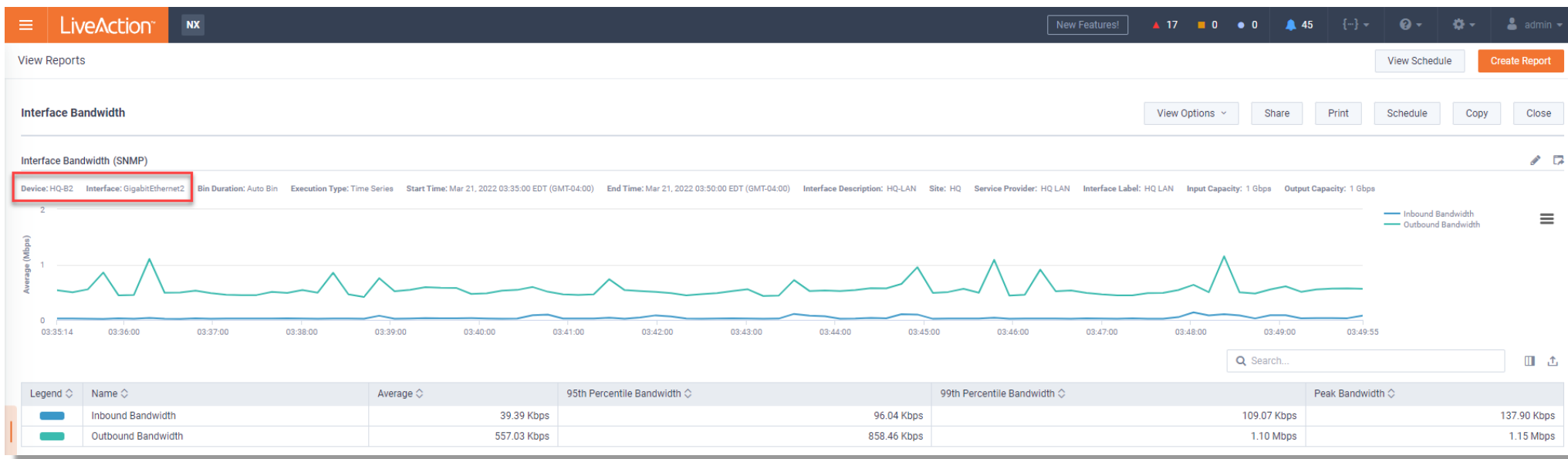


# Top Interface Bandwidths (SNMP)



# Interface Bandwidth (SNMP)

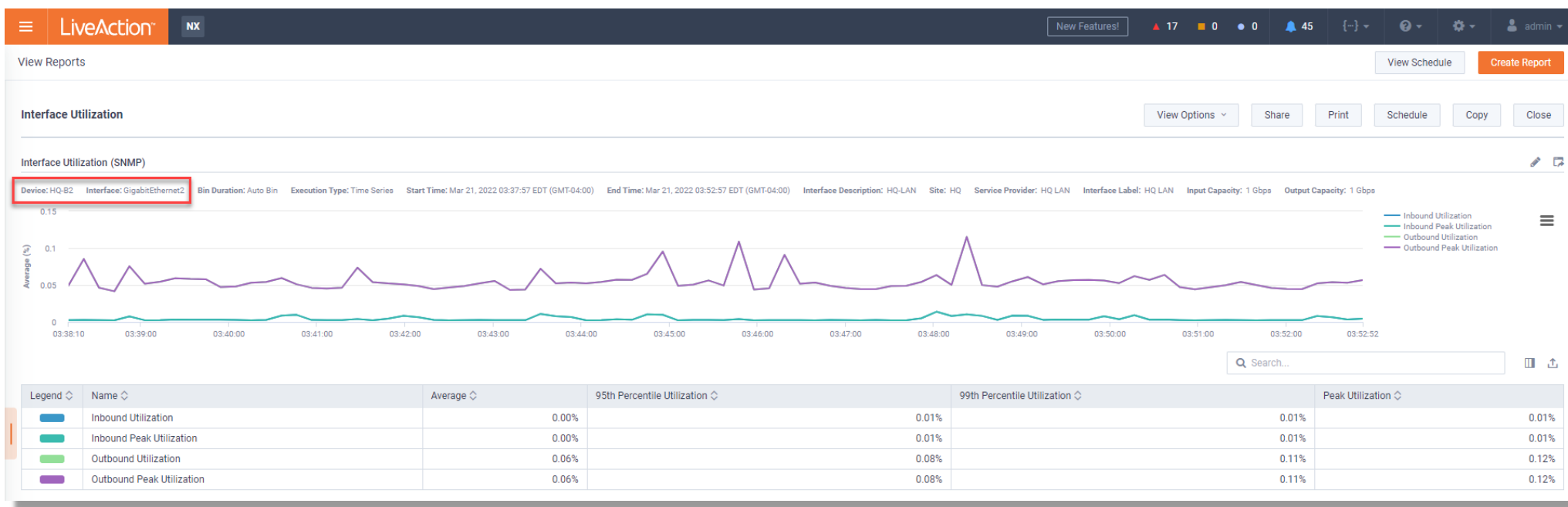
## Single Interface View - Over Time



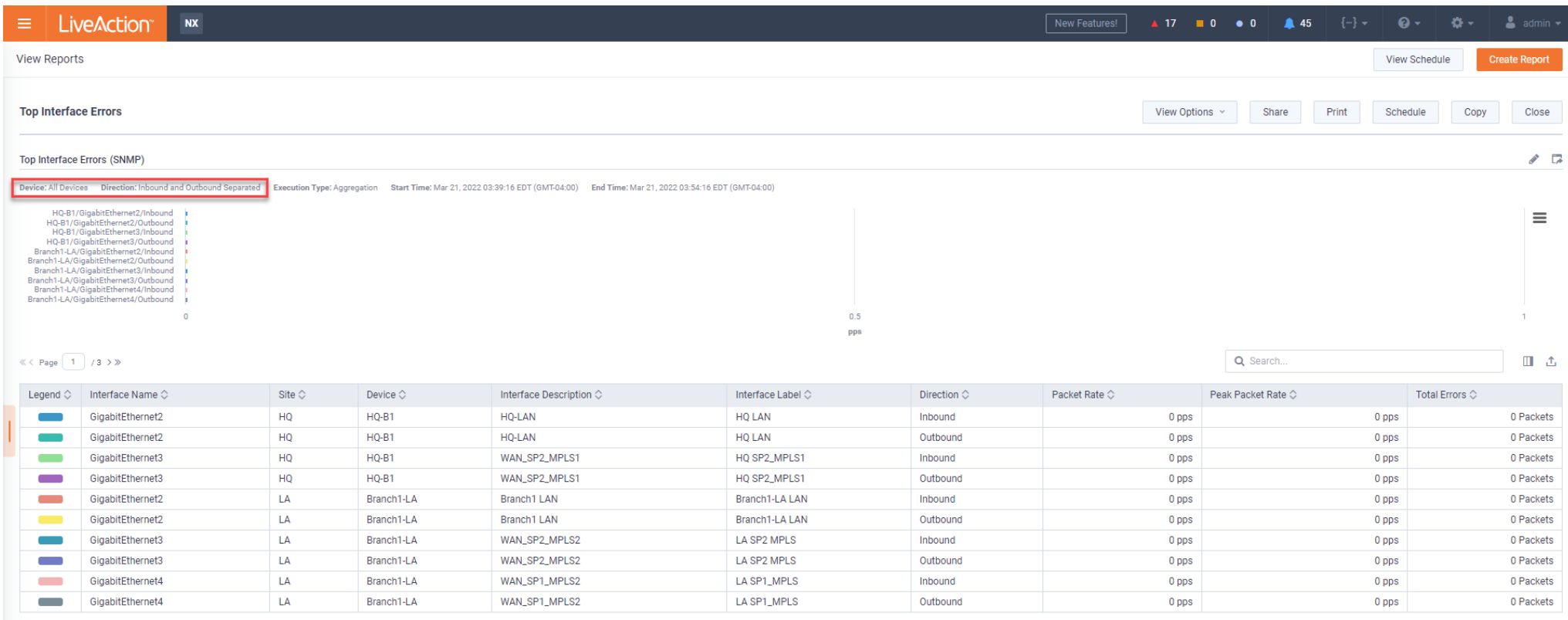


# Interface Utilization (SNMP)

## Single Interface View - Over Time



# Top Interface Errors (SNMP)



# Top Class Drops (SNMP)

LiveAction<sup>®</sup>

NX

New Features!

▲ 17

■ 0

● 0

🔔 45

{-}

?

⚙️

admin

View Reports

View Schedule

Create Report

Top Class Drops

View Options

Share

Print

Schedule

Copy

Close

Top Class Drops (SNMP)

Device: All Devices Exclude Class Defaults: false Unit: Bit Rate Direction: Inbound and Outbound Separated Execution Type: Aggregation Start Time: Mar 21, 2022 03:41:01 EDT (GMT-04:00) End Time: Mar 21, 2022 03:56:01 EDT (GMT-04:00)

No data

Sometimes It's Nice to Get an Empty Report

Successfully run

# LAB 5: Dashboards and Reporting

- Create and View Dashboards
- Create & View Reports



A man in a dark suit and light shirt is standing on a stage, holding a microphone and gesturing with his left hand towards a large screen. The screen displays a complex flow diagram with various shapes like circles, rectangles, and arrows connected by lines. The audience, seen from behind, is seated in rows of chairs, facing the speaker. The overall scene is brightly lit with a blue and white color scheme.

## Collecting Flows in LiveNX

---

## 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

Select	Device	Type	IP Address	Description	Tags	Traffic Statistics (FNF)	Application Response Time (AVC)	Voice/Video Performance (Medianet)	Traditional	Custom
<input type="checkbox"/>	Branch1-LA	Standard	198.19.1.1	Cisco IOS Software [Den...	WAN, LA, 1000000, 10...	●	●	●	●	●
<input type="checkbox"/>	Branch2-NY	Standard	198.19.2.1	Cisco IOS Software [Den...	WAN, NY, 1000000, 10...	●	●	●	●	●
<input type="checkbox"/>	HQ-B1	Standard	198.18.129.24	Cisco IOS Software [Den...	WAN, HQ, 1000000, 10...	●	●	●	●	●
<input type="checkbox"/>	HQ-B2	Standard	198.18.129.25	Cisco IOS Software [Den...	WAN, HQ, 1000000, 10...	●	●	●	●	●
<input type="checkbox"/>	HQ-MC	Standard	198.18.129.23	Cisco IOS Software [Den...	HQ	●	●	●	●	●

- 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

Multiple CLI Viewer

Device	Type
APN-ASR1001-114	Standard

```
config t
ip flow-export version 9
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export source GigabitEthernet0/0/3
ip flow-export destination 172.17.101.81 2055
interface GigabitEthernet0/0/1.100
ip flow ingress
ip flow egress
```

Multiple CLI Viewer

Device	Type
APN-ASR1001-114	Standard

```
config t
interface GigabitEthernet0/0/1.100
ip nbar protocol-discovery
exit
flow record LIVEACTION-FLOWRECORD
description DO NOT MODIFY. USED BY LIVEACTION.
match flow direction
match interface input
match ipv4 destination address
match ipv4 protocol
match ipv4 source address
match ipv4 tos
match transport destination-port
match transport source-port
collect application name
collect counter bytes
collect counter packets
collect flow sampler
collect interface output
collect ipv4 destination mask
collect ipv4 dscp
collect ipv4 id
collect ipv4 source mask
collect ipv4 source prefix
collect routing destination as
collect routing next-hop address ipv4
collect routing source as
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect transport tcp flags
exit
flow monitor LIVEACTION-FLOWMONITOR
description DO NOT MODIFY. USED BY LIVEACTION.
exporter LIVEACTION-FLOWEXPORTER-IPFIX
cache timeout inactive 10
cache timeout active 60
```

This points to your flow collector (ie; LiveNX Node)

Cisco's Best-Practices Templates

LiveAction®



# Enable Flow Collection Within LiveNX Engineering Console

Flow Configuration

Instructions  
Select devices to configure flow

Flow Configuration Table

Select	Device	Type	IP Address	Description	Tags	Traffic Statist...	Application Re...	Voice/Video Perf...	Traditional	Custom
<input type="checkbox"/>	CS-2960-23-22	Standard	10.100.51.22	Cisco IOS Software...	-	⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	CS-C3650-23-36	Catalyst 3850	10.100.155.1	Cisco IOS Software...	-	⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	CS-C3850-23-31	Catalyst 3850	10.100.51.1	Cisco IOS Software... Palo Alto, 38...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	IWAN-Br 1_Sydney	Standard	10.100.51.35	Cisco IOS Software... Sydney, Jeff1		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	IWAN-BR_INET	Catalyst 9000	10.100.51.32	Cisco IOS Software... WAN, Tokyo,...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	IWAN-BR_MPLS	Standard	10.100.51.31	Cisco IOS Software... Tokyo		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	IWAN-DC-MC	Standard	10.100.51.30	Cisco IOS Software... Tokyo		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	IWAN-MPLS-CORE	Catalyst 9000	10.100.51.33	Cisco IOS Software...	-	⦿	⦿	⦿	⦿	⦿
<input checked="" type="checkbox"/>	RTR-DC-CORE	Standard	10.100.51.3	Cisco IOS Software... Test		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR-DC-MPLS	Catalyst 3850	10.100.51.4	Cisco IOS Software... WAN, 10000...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_Austin	Catalyst 4500	10.100.51.6	Cisco IOS Software... WAN, Austin,...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_Birmingham	Catalyst 6500	10.100.51.7	Cisco IOS Software... WAN, 200, 2...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_London	Standard	10.100.51.8	Cisco IOS Software... London		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_LosAngeles	Standard	10.100.51.9	Cisco IOS Software... WAN, 2000, ...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_Louisville	Standard	10.100.51.10	Cisco IOS Software... WAN, Louisvil...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_Madison	Standard	10.100.51.11	Cisco IOS Software... WAN, Madiso...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_SanJose	Standard	10.100.51.12	Cisco IOS Software... WAN, San_J...		⦿	⦿	⦿	⦿	⦿
<input type="checkbox"/>	RTR_Seattle	Standard	10.100.51.2	Cisco IOS Software... WAN, Seattle...		⦿	⦿	⦿	⦿	⦿

Help

Configure Selected

Close

Easily Setup Flow Configurations at the *Device* Level

LiveAction®

# Enable Flow Collection on Interfaces

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

Flow Configuration

Instructions  
Configure the type of flow you wish to receive from the interfaces

Flow Configuration Table

Device	Type	IP Address	Description	Tags	Traffic Statistics	Application Res.	Voice/Video Perfo...	Traditional	Custom
Branch1-LA	Catalyst 9000	198.19.1.1	Cisco IOS Software ...	WAN, LA, 100...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet2	-	198.19.1.1	Branch1 LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet3	-	100.64.1.2	WAN_SP2_MPLS2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet4	-	10.255.1.2	WAN_SP1_MPLS2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Branch2-NY	Catalyst 9000	198.19.2.1	Cisco IOS Software ...	WAN, NY, Bra...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet2	-	198.19.2.1	Branch2 LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet3	-	100.64.2.2	WAN_SP2_MPLS2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet4	-	10.255.2.2	WAN_SP1_MPLS2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HQ-81	Catalyst 9000	198.18.129.24	Cisco IOS Software ...	WAN, HQ, 10...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet2	-	198.18.129.24	HQ-LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet3	-	100.64.0.2	WAN_SP2_MPLS1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet4	-	198.18.129.25	WAN, HQ, 10...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HQ-82	Catalyst 9000	198.18.129.26	Cisco IOS Software ...	WAN, HQ, 10...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	GigabitEthernet2	-	198.18.129.26	HQ-LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Flow Export Destination

☐ Configure Flow Export Destination

☒ LiveNX node

☐ LiveNX node flow replicator at port 9991

☐ Other at IP address and port

Help Save to Devices Preview CLI Revert Back Close

Setup Flow Configurations at the *Interface* Level

WebUI  
Configuring LiveNX to accept reports

EDIT BRANCH2-NY.DCLOUD.CISCO.COM

Site: NY Group: NY Interval: 10 Seconds

IP Address\*: 198.19.2.1

☒ POLL ☐ IP SLA ☒ QOS ☐ ROUTING ☒ FLOW ☐ LAN

Tells LiveNX to accept information from this device

Type IP Address

Tags: Branch x Sales Office x East x 3

Cancel Apply

# 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...)

**Flow Configuration**

Instructions  
Configure the type of flow you wish to receive from the interfaces

Flow Configuration Table

Device	Type	IP Address	Description	Tags	Traffic Sta...	Applicatio...	Voice/Video P...	Traditional	Custom
Branch1-LA	Catalyst 9000	198.19.1.1	Cisco IOS Softw...	WAN, LA,...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	-	198.19.1.1	Branch1 LAN	1000000,...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet3	-	100.64.1.2	WAN_SP2_MPLS2	LA SP2 M...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet4	-	10.255.1.2	WAN_SP1_MPLS2	LA SP1_M...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Branch2-NY	Catalyst 9000	198.19.2.1	Cisco IOS Softw...	WAN, NY,...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	-	198.19.2.1	Branch2 LAN	Branch2 L...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet3	-	100.64.2.2	WAN_SP2_MPLS2	SP2_MPL...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet4	-	10.255.2.2	WAN_SP1_MPLS2	SP1_MPL...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HQ-B1	Catalyst 9000	198.18.129.24	Cisco IOS Softw...	WAN, HQ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	-	198.18.129.24	HQ-LAN	1000000,...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet3	-	100.64.0.2	WAN_SP2_MPLS1	WAN, HQ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HQ-B2	Catalyst 9000	198.18.129.25	Cisco IOS Softw...	WAN, HQ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	-	198.18.129.26	HQ-LAN	1000000,...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet3	-	10.255.0.2	WAN_SP1_MPLS1	SP1_MPL...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Flow Export Destination

☒ Configure Flow Export Destination

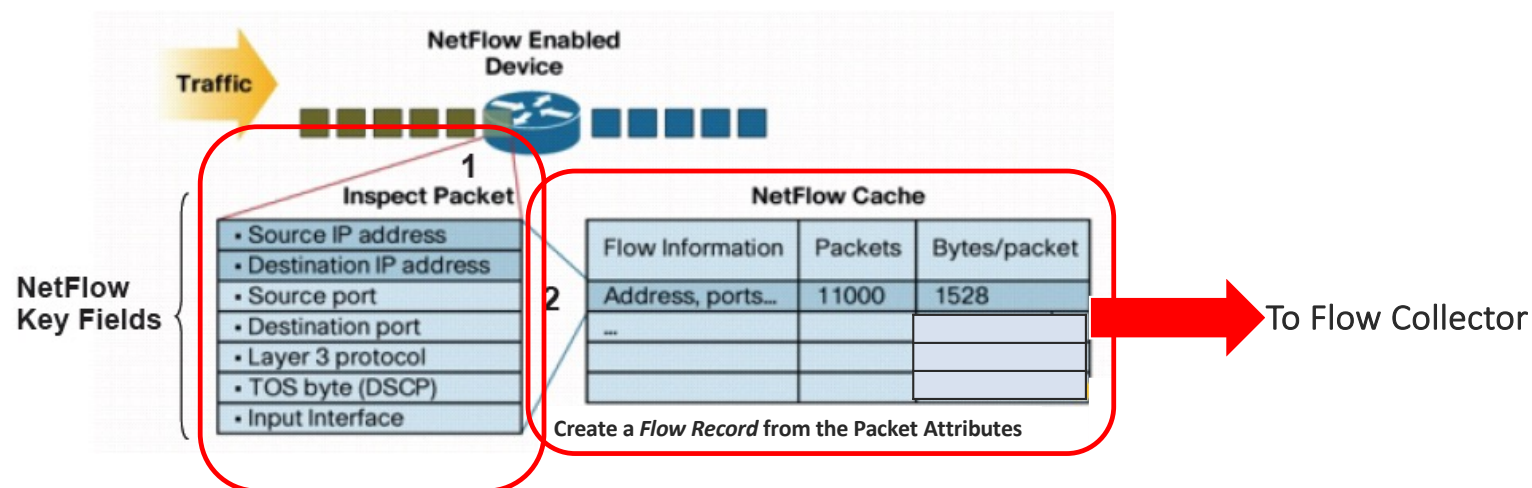
☐ LiveNX node

☐ LiveNX node flow replicator at port 9991

☒ Other at IP address 198.128.34.111 and port 2055

Help Save to Devices Preview CLI Revert Back Close

# NetFlow Collects *Statistics* on Packets as they pass...



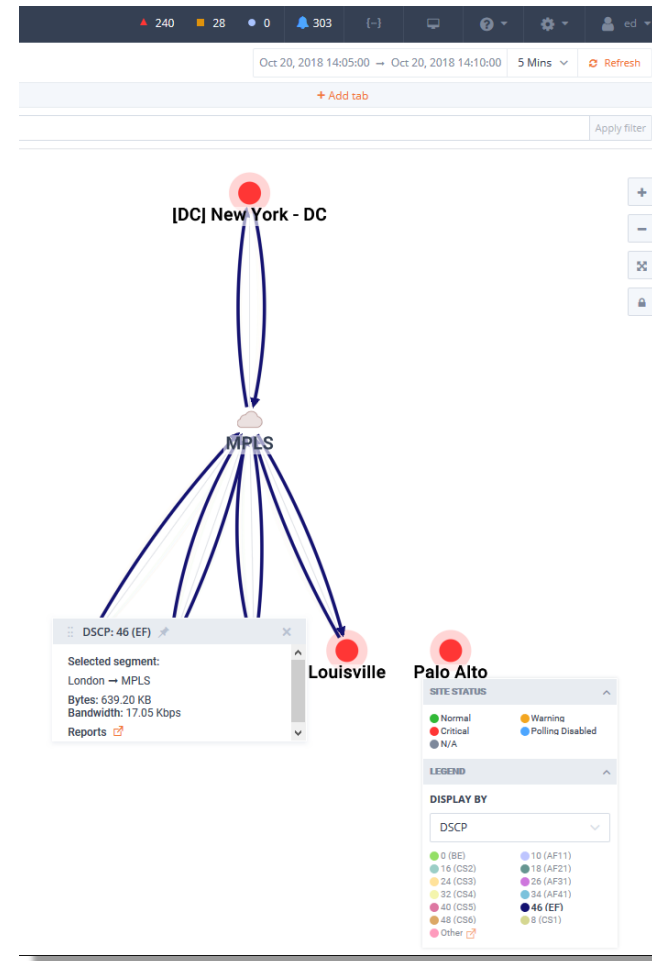
1. A flow is unidirectional
2. Defined by inspecting a packet's **key fields** (common properties) and identifying the values
3. If the set of key field values is unique, create a flow record or cache entry

# Netflow

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

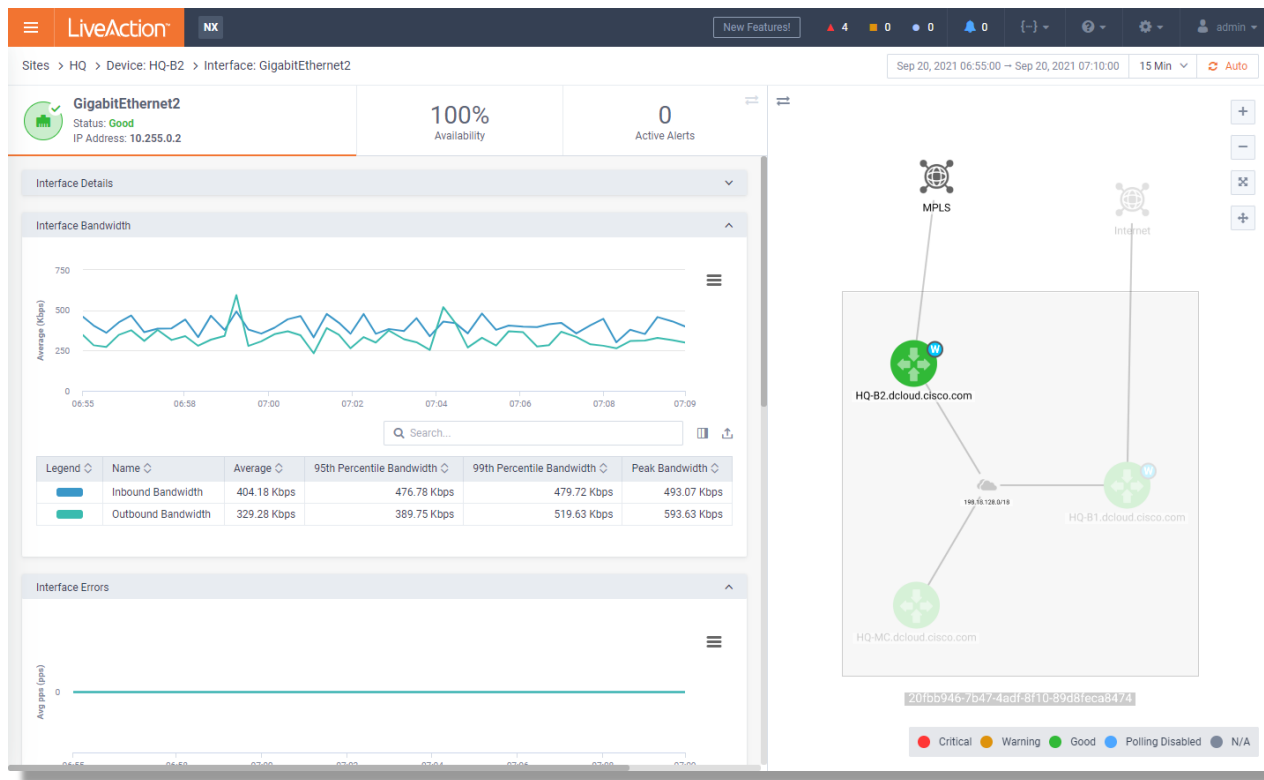
- Traffic source and destination
- Class of service
- Protocol
- Ports
- etc...

per device.



LiveAction®

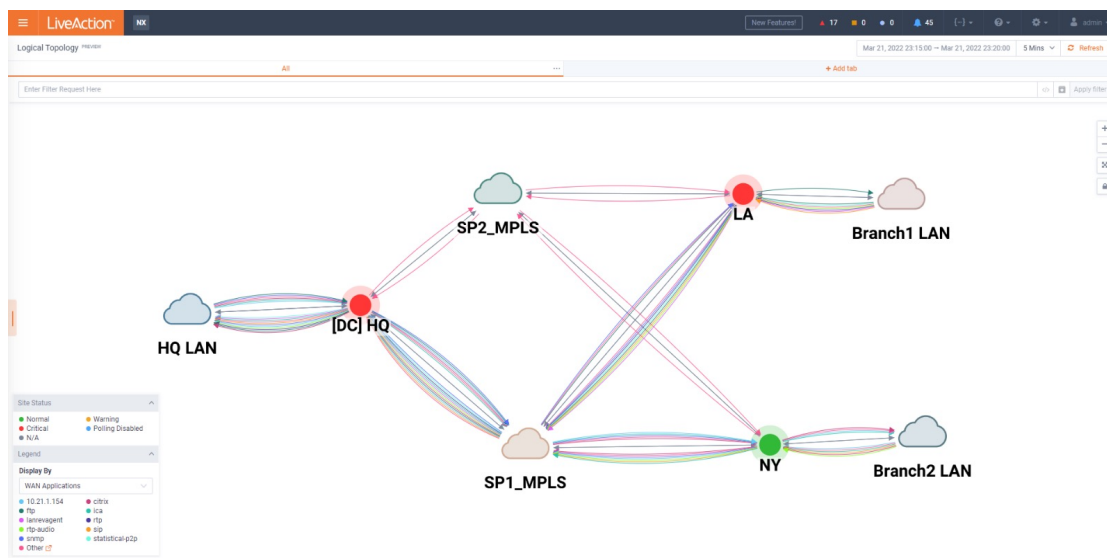
# Netflow Interface View



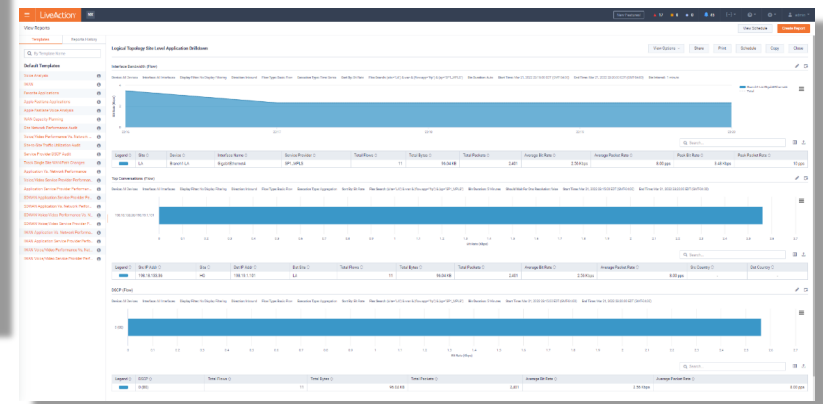
View quantity & type of traffic traversing a specific interface

## Application Flow View

## Logical Topology View

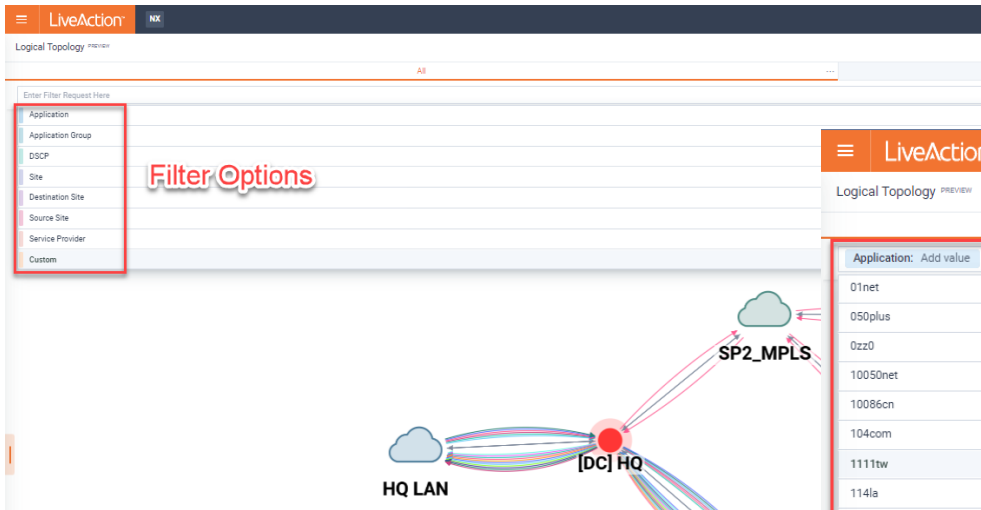


## Single Click Drill-Down to Details

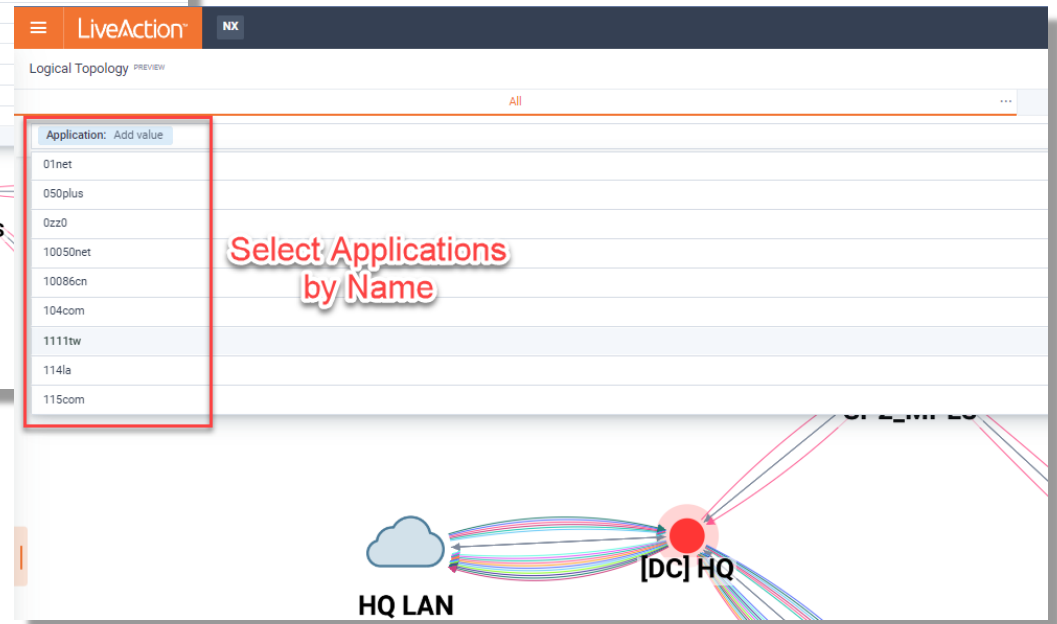


# Filtering Topologies

Click in Filter Bar – Select Filtering Option from List



Start Typing and Click Filter by Application Name





---

## Other types of Flow in LiveNX

- LiveNX can 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

---

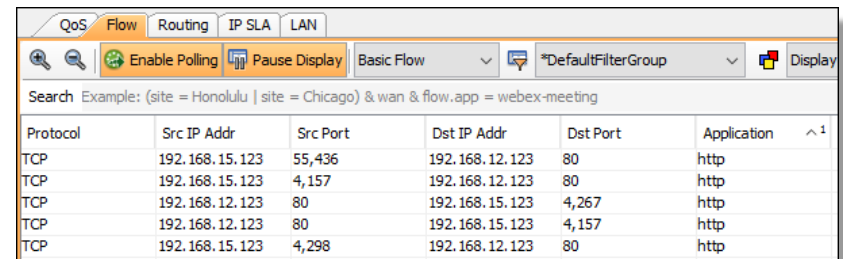
# Network Based Application Recognition (NBAR2)

- NBAR2 uses the Service Control Engine (SCE) with advanced classification techniques called PDLs (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](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



The screenshot shows the 'Flow' tab in the LiveAction interface. It displays a table of network flows with the following columns: Protocol, Src IP Addr, Src Port, Dst IP Addr, Dst Port, and Application. The table contains five rows of data, all for TCP protocol. The search criteria at the top are: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting.

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.

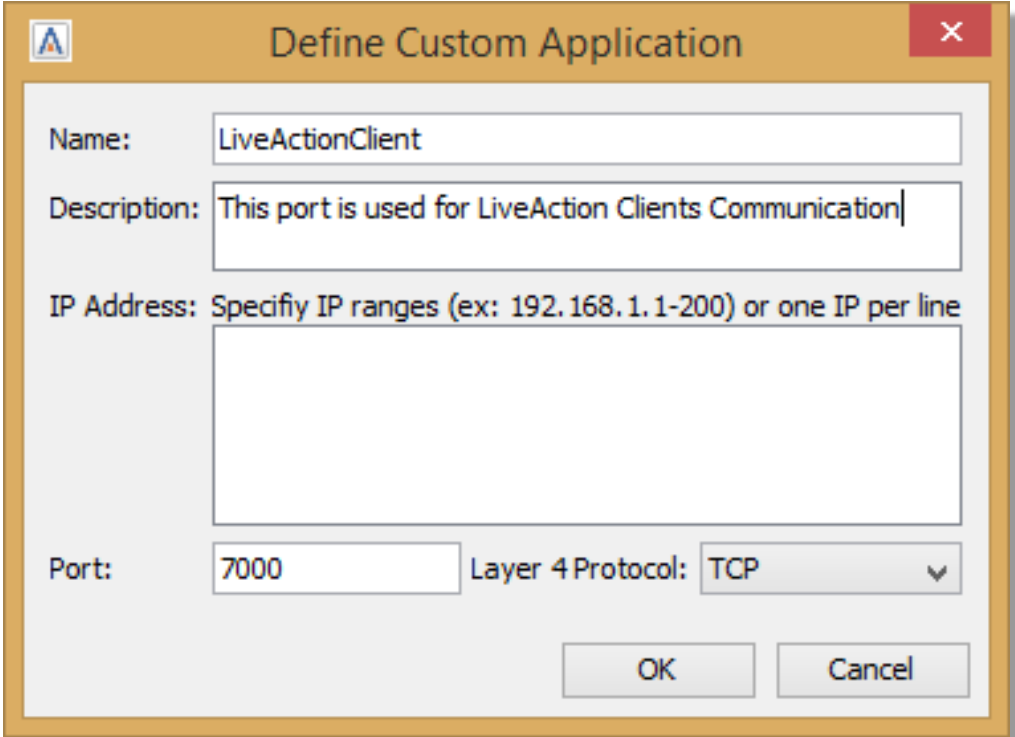
The screenshot shows a web browser window with the address bar displaying <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>. The page title is "Service Name and Transport Protocol Port Number Registry". Below the title, it says "Last Updated 2016-02-26" and "Expert(s) TCP/UDP: Joe Touch; Eliot Lear, Allison Mankin, Markku Kojo, Kumiko Ono, Martin Lars Eggert, Alexey Melnikov, Wes Eddy, and Alexander Zimmermann; SCTP: Allison Mankin and Michael Tuexen; DCCP: Eddie Kohler and Yoshifumi Nishida". A "Reference" link points to [\[RFC6335\]](#).

Overlaid on the bottom right of the browser window is a screenshot of a network device's configuration interface. It shows a table with columns: Protocol, Src IP Addr, Src Port, Dst IP Addr, Dst Port, and Application. The table lists various protocols and their associated ports. Two entries for "microsoft-ds\*" are circled in red, corresponding to ports 445 and 1,701.

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application
ICMP	TEST (192.168.1.1)	0	10.0.12.2	769	icmp
TCP	192.168.12.123	445	192.168.15.123	1,701	microsoft-ds*
TCP	192.168.15.123	1,701	192.168.12.123	445	microsoft-ds*
TCP	192.168.15.123	58,192	192.168.12.123	80	ms-office-365
TCP	192.168.12.123	80	192.168.15.123	58,192	ms-office-365
TCP	192.168.12.123	3,389	192.168.15.123	52,255	ms-wbt
TCP	192.168.15.123	52,255	192.168.12.123	3,389	ms-wbt
UDP	10.253.60.14	3,218	10.253.60.255	137	netbios-ns
TCP	192.168.15.123	3,637	192.168.12.123	1,305	pe-mike*
TCP	192.168.12.123	1,305	192.168.15.123	3,637	pe-mike*
UDP	10.0.0.2	7,777	7.7.7.17	5,555	personal-agent*
UDP	10.0.12.2	7,777	8.8.8.3	5,555	personal-agent*

## 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



**Define Custom Application**

Name:

Description:

IP Address: Specify IP ranges (ex: 192.168.1.1-200) or one IP per line

Port:  Layer 4 Protocol:

---

## 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.

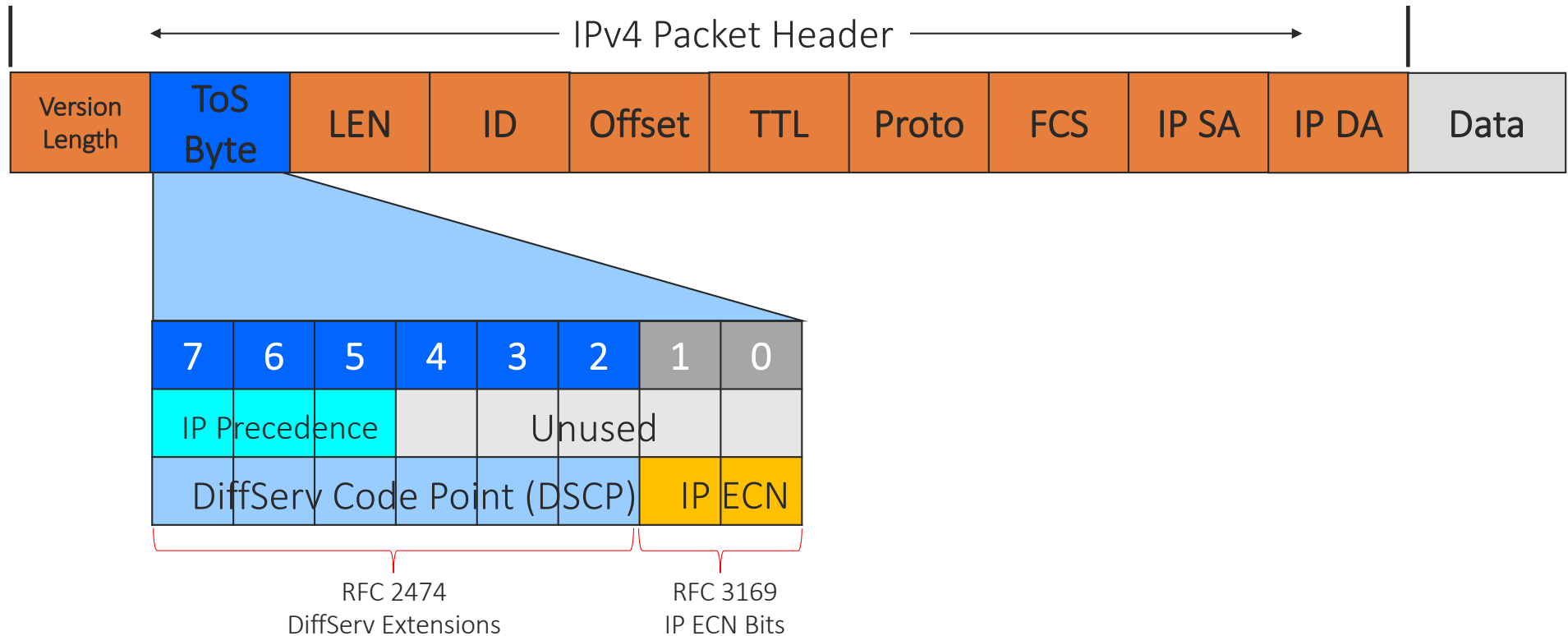


## Differentiated Service Control Point (DSCP)

- 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**.

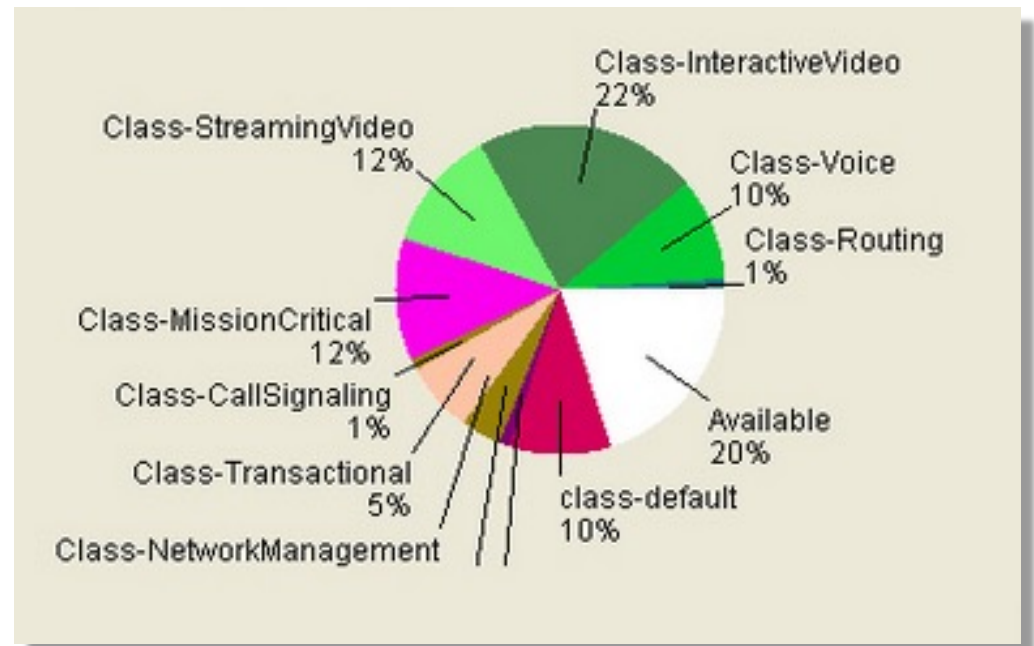
Application	L3 Classification		IETF RFC
	PHB	DSCP	
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency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

# 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: <ul style="list-style-type: none"><li>• 8 vCPU Xeon or i7</li><li>• 16 Gb RAM</li><li>• Max Heap Size 8GB</li><li>• 500GB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 16 vCPU Xeon or i7</li><li>• 32 Gb RAM</li><li>• Max Heap Size 16GB</li><li>• 2TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 16 vCPU Xeon or i7</li><li>• 64 Gb RAM</li><li>• Max Heap Size 31GB</li><li>• 4TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 32 vCPU Xeon or i7</li><li>• 64 Gb RAM</li><li>• Max Heap Size 31GB</li><li>• 8TB Data Disk</li></ul>	Min Requirements: <ul style="list-style-type: none"><li>• 64 vCPU Xeon Gold 5218</li><li>• 768 Gb RAM</li><li>• Max Heap Size 384GB</li><li>• 32TB Data Disk</li><li>(16TB usable with RAID 10)</li></ul>

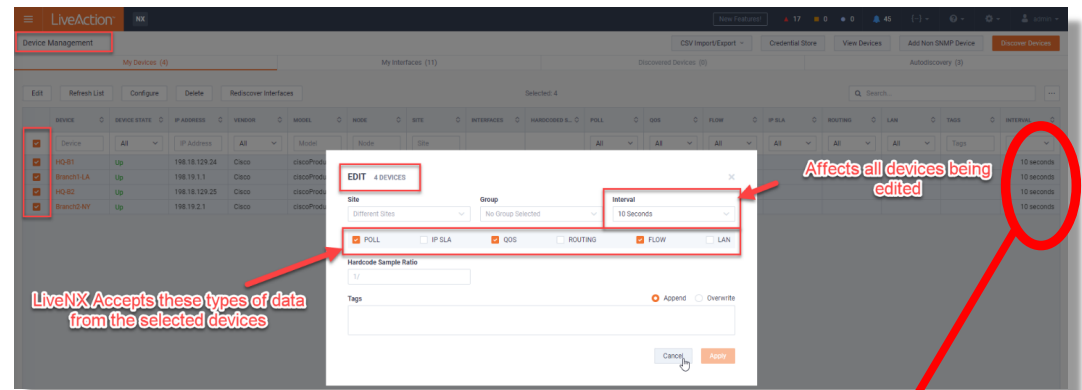
# Disk Sizing- SNMP

## 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



SITE	INTERFACES	HARDCODED S...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS	INTERVAL
Site			All	All	All	All	All	All	Tags	All
HQ	2		✓	✓	✓					10 seconds
LA	3		✓	✓	✓					10 seconds
HQ	2		✓	✓	✓					10 seconds
NY	4		✓	✓	✓					10 seconds



# 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:

**Settings**

Configuration

Data Source Management

Data Store Management

Disk Overview

**Nodes Data Store**

Web UI Data Store

Device Entity Page Reports

Email Configuration

Integrations

Licensing

License Configuration

License Expiration Notification

LiveNA Configuration

Mounted Data

Nodes

Properties

Proxy

Reports

Security

Single Sign On

SNMP Trap

Syslog

Troubleshooting

Updates

**DEFAULT SETTINGS**  
Are applied for all nodes that do not use custom settings

**LOCAL** Default settings applied

Available Free Space: 482.31 GB Total Disk Space: 499.76 GB

Other Store Size: 17.39 GB SNMP Store Size: 33.11 MB Flow Store Size: 15.03 MB  
Engineering Console Alert Store Size: 45.66 KB Long-Term Store Size: 13.38 MB

**SNMP**

☒ Display a warning when any database exceeds: 500 MB

☒ Automatically purge data older than: 10 Days

☐ Before purging, archive to:

Reset now

Purge now

**Flow**

☒ Display a warning when any database exceeds: 500 MB

☒ Automatically purge data older than: 10 Days

☐ Before purging, archive to:

Reset now

Purge now

**Engineering Console Alert**

☒ Display a warning when any database exceeds: 500 MB

☒ Automatically purge data older than: 10 Days

Reset now

Purge now

Revert changes Apply

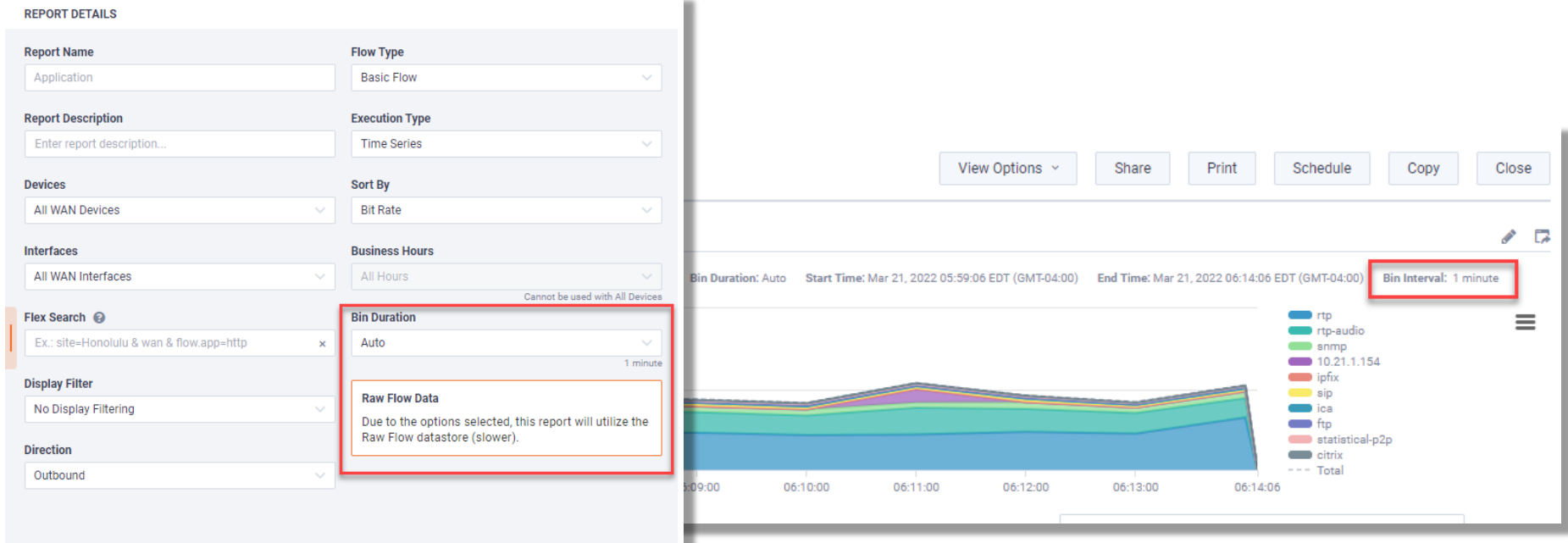
Admin can set:

- 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  $\geq$  1 hours search

# Device Semantics...

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

LiveActionNX

New Features!170045

admin

Device InventoryEnter Filter Request HereApply filter

Devices

Verify Consistency

DEVICE	DEVICE SERIAL	IP ADDRESS	SITE	NODE	TAGS	GROUP	MODEL	OS VERSION	DESCRIPTION
HQ-B1	2	198.18.129.24	HQ	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
Branch1-LA	101	198.19.1.1	LA	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
HQ-B2	3	198.18.129.25	HQ	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
Branch2-NY	0000000021	198.19.2.1	NY	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...

Interfaces

Apply at Site, Device, Interface  
(Three-Tier Model)

INTERFACE NA...	IP ADDRESS	SUBNET MASK	DEVICE	SITE	WAN TYPE	SERVICE PROVL...	INPUT CAPACITY	OUTPUT CAPAC...	ABBREVIATED ...	IF INDEX	DESCRIPTION	SPEED	TYPE	LABEL	TAGS
GigabitEthernet2	198.18.129.24	255.255.192.0	HQ-B1	HQ	-	-	1 Gbps	1 Gbps	Gi2	2	HQ-LAN	1 Gbps	ethernet_csma...	HQ LAN	-
GigabitEthernet3	100.64.0.2	255.255.255.0	HQ-B1	HQ	WAN	SP2_MPLS	4 Mbps	4 Mbps	Gi3	3	WAN_SP2_MP...	1 Gbps	ethernet_csma...	HQ SP2_MPLS1	-
GigabitEthernet2	198.19.1.1	255.255.255.0	Branch1-LA	LA	-	Branch1 LAN	1 Gbps	1 Gbps	Gi2	2	Branch1 LAN	1 Gbps	ethernet_csma...	Branch1-LA LAN	-
GigabitEthernet3	100.64.1.2	255.255.255.0	Branch1-LA	LA	WAN	SP2_MPLS	2 Mbps	2 Mbps	Gi3	3	WAN_SP2_MP...	1 Gbps	ethernet_csma...	LA SP2_MPLS	-
GigabitEthernet4	10.255.1.2	255.255.255.0	Branch1-LA	LA	WAN	SP1_MPLS	2 Mbps	2 Mbps	Gi4	4	WAN_SP1_MP...	1 Gbps	ethernet_csma...	LA SP1_MPLS	-
GigabitEthernet2	198.18.129.26	255.255.192.0	HQ-B2	HQ	-	HQ LAN	1 Gbps	1 Gbps	Gi2	2	HQ-LAN	1 Gbps	ethernet_csma...	HQ LAN	-
GigabitEthernet3	10.255.0.2	255.255.255.0	HQ-B2	HQ	WAN	SP1_MPLS	2 Mbps	2 Mbps	Gi3	3	WAN_SP1_MP...	1 Gbps	ethernet_csma...	HQ SP1_MPLS1	-
GigabitEthernet1	192.168.122.161	255.255.255.0	Branch2-NY	NY	-	-	1 Gbps	1 Gbps	Gi1	1	-	1 Gbps	ethernet_csma...	-	-

# NetFlow Best Practices



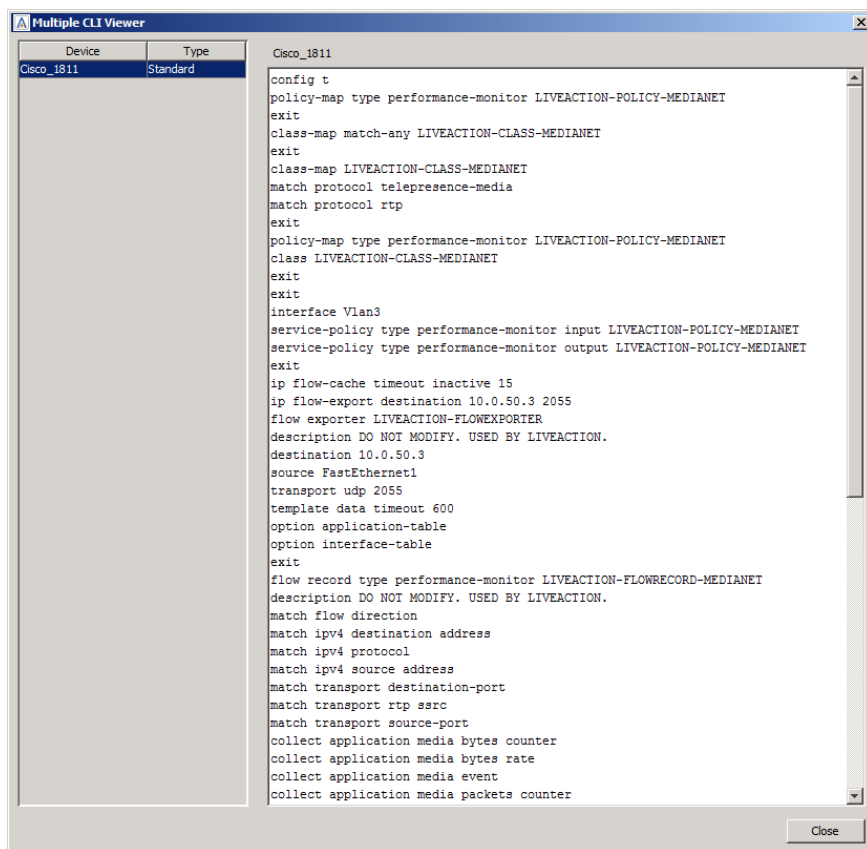
---

## 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

LiveAction NX

New Features!

17 0 0 45

admin

View Reports

View Schedule Create Report

Top Analysis, Last Fifteen Minutes

Application/NBAR2 Data

View Options Share Print Schedule Copy Close

Top Analysis (Flow)

Top Analysis

Device: HQ-B1 Interface: All Interfaces Display Filter: No Display Filtering Direction: Inbound and Outbound Combined Flow Type: Basic Flow Top Analysis Display Type: Time Sorted - Raw Flows Execution Type: Aggregation Should Wait For Dns Resolution: false Top Analysis Limit: 5000 Start Time: Mar 21, 2022 06:13:36 EDT (GMT-04:00) End Time: Mar 21, 2022 06:28:36 EDT (GMT-04:00)

<< Page 1 / 12 >>

Search...

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	SSL C
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)	OSPF	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)	OSPF	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)	OSPF	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)	OSPF	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**

**LiveAction®**

## 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 adedge: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

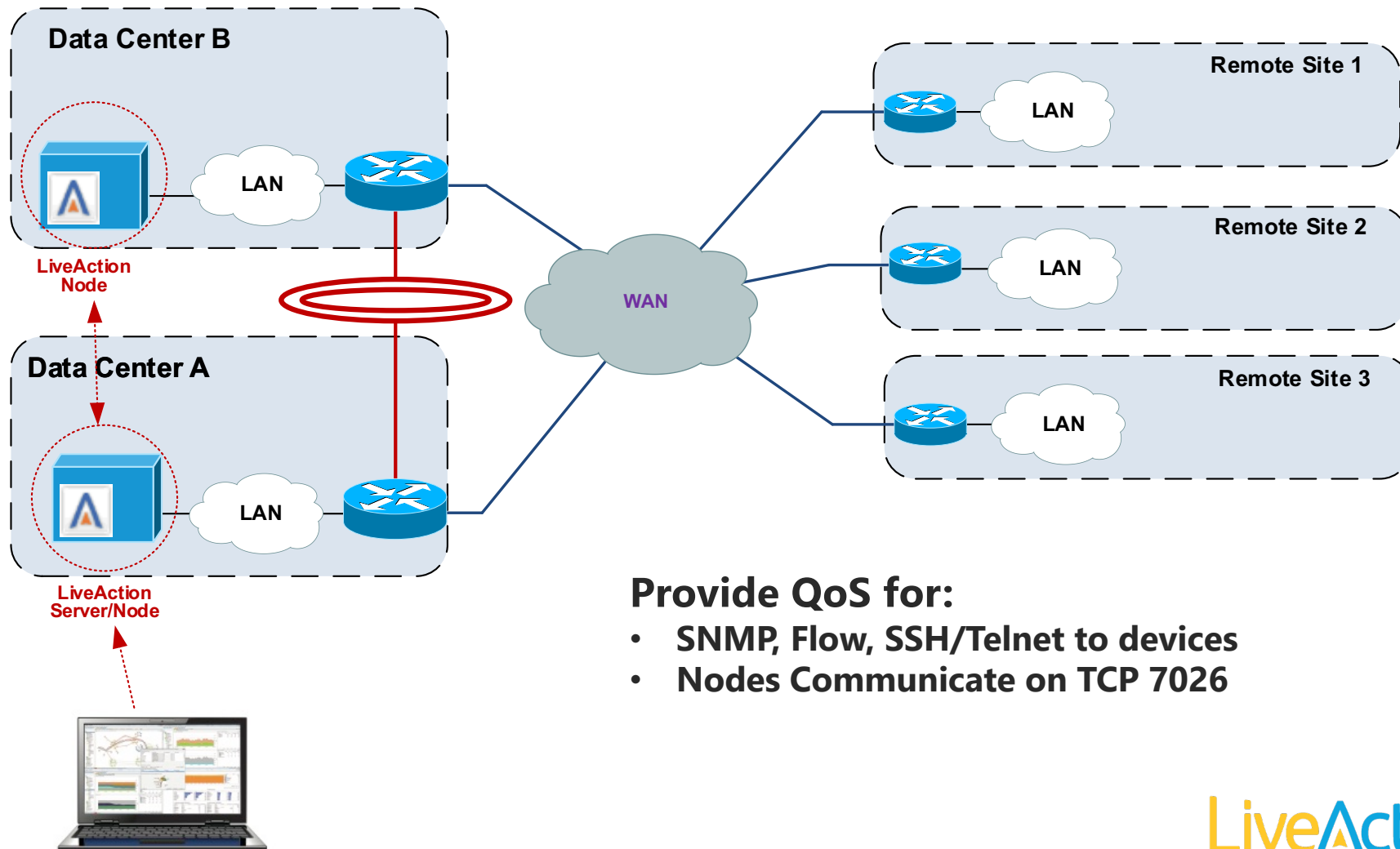
```
class-map match-any LIVEACTION-CLASS-AVC  
  match access-group name LIVEACTION-ACL-AVC
```

```
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





## 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

LiveAction

NX

New Features!

17

0

0

45

{-}

?

⚙

admin

Device Inventory

Enter Filter Request Here

Apply filter

Devices

Verify Consistency

Search...

...

DEVICE	DEVICE SERIAL	IP ADDRESS	SITE	NODE	TAGS	GROUP	MODEL	OS VERSION	DESCRIPTION
Device	Device Serial	IP Address	Site	Node	Tags	Group	Model	OS Version	Description
HQ-B1	2	198.18.129.24	HQ	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
Branch1-LA	101	198.19.1.1	LA	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
HQ-B2	3	198.18.129.25	HQ	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...
Branch2-NY	0000000021	198.19.2.1	NY	Local	-	-	ciscoProducts.3004	17.4.1a	Cisco IOS Software [Bengalur...

All rows / 4

Interfaces

Apply at Site, Device, Interface  
(Three-Tier Model)

Search...

...

INTERFACE NA...	IP ADDRESS	SUBNET MASK	DEVICE	SITE	WAN TYPE	SERVICE PROVL...	INPUT CAPACITY	OUTPUT CAPAC...	ABBREVIATED ...	IF INDEX	DESCRIPTION	SPEED	TYPE	LABEL	TAGS
Interface N...	IP Address	Subnet Mask	Device	Site	All	Service Pro...	Input Capa...	Output Cap...	Abbreviate...	If Index	Description	Speed	Type	Label	Tags
GigabitEthernet2	198.18.129.24	255.255.192.0	HQ-B1	HQ	-	-	1 Gbps	1 Gbps	Gi2	2	HQ-LAN	1 Gbps	ethernet_csma...	HQ LAN	-
GigabitEthernet3	100.64.0.2	255.255.255.0	HQ-B1	HQ	WAN	SP2_MPLS	4 Mbps	4 Mbps	Gi3	3	WAN_SP2_MP...	1 Gbps	ethernet_csma...	HQ SP2_MPLS1	-
GigabitEthernet2	198.19.1.1	255.255.255.0	Branch1-LA	LA	-	Branch1 LAN	1 Gbps	1 Gbps	Gi2	2	Branch1 LAN	1 Gbps	ethernet_csma...	Branch1-LA LAN	-
GigabitEthernet3	100.64.1.2	255.255.255.0	Branch1-LA	LA	WAN	SP2_MPLS	2 Mbps	2 Mbps	Gi3	3	WAN_SP2_MP...	1 Gbps	ethernet_csma...	LA SP2_MPLS	-
GigabitEthernet4	10.255.1.2	255.255.255.0	Branch1-LA	LA	WAN	SP1_MPLS	2 Mbps	2 Mbps	Gi4	4	WAN_SP1_MP...	1 Gbps	ethernet_csma...	LA SP1_MPLS	-
GigabitEthernet2	198.18.129.26	255.255.192.0	HQ-B2	HQ	-	HQ LAN	1 Gbps	1 Gbps	Gi2	2	HQ-LAN	1 Gbps	ethernet_csma...	HQ LAN	-
GigabitEthernet3	10.255.0.2	255.255.255.0	HQ-B2	HQ	WAN	SP1_MPLS	2 Mbps	2 Mbps	Gi3	3	WAN_SP1_MP...	1 Gbps	ethernet_csma...	HQ SP1_MPLS1	-
GigabitEthernet1	192.168.122.161	255.255.255.0	Branch2-NY	NY	-	-	1 Gbps	1 Gbps	Gi1	1	-	1 Gbps	ethernet_csma...	-	-

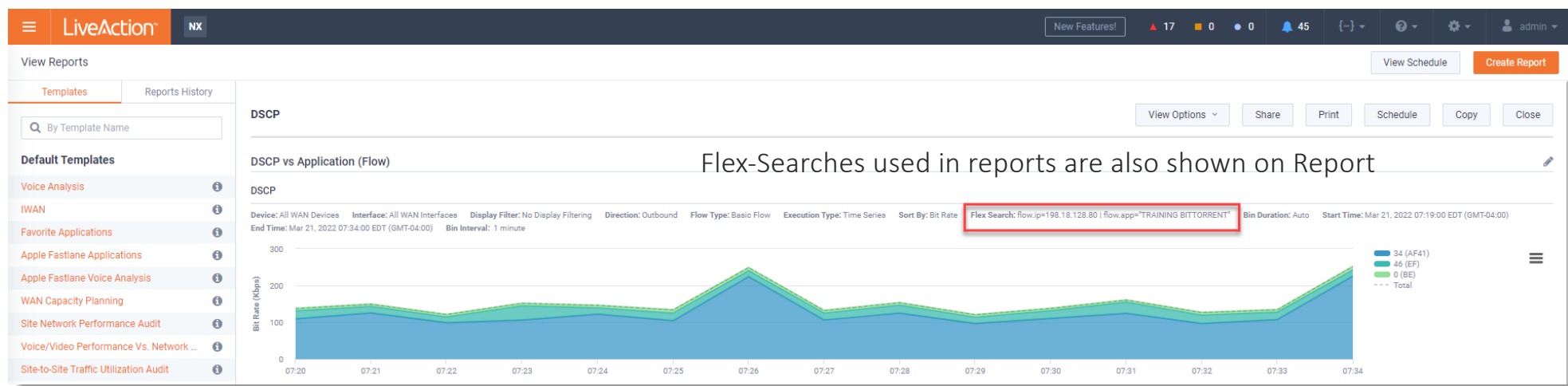


# Semantic Data – In Reporting Example 1

## Flex Search ?

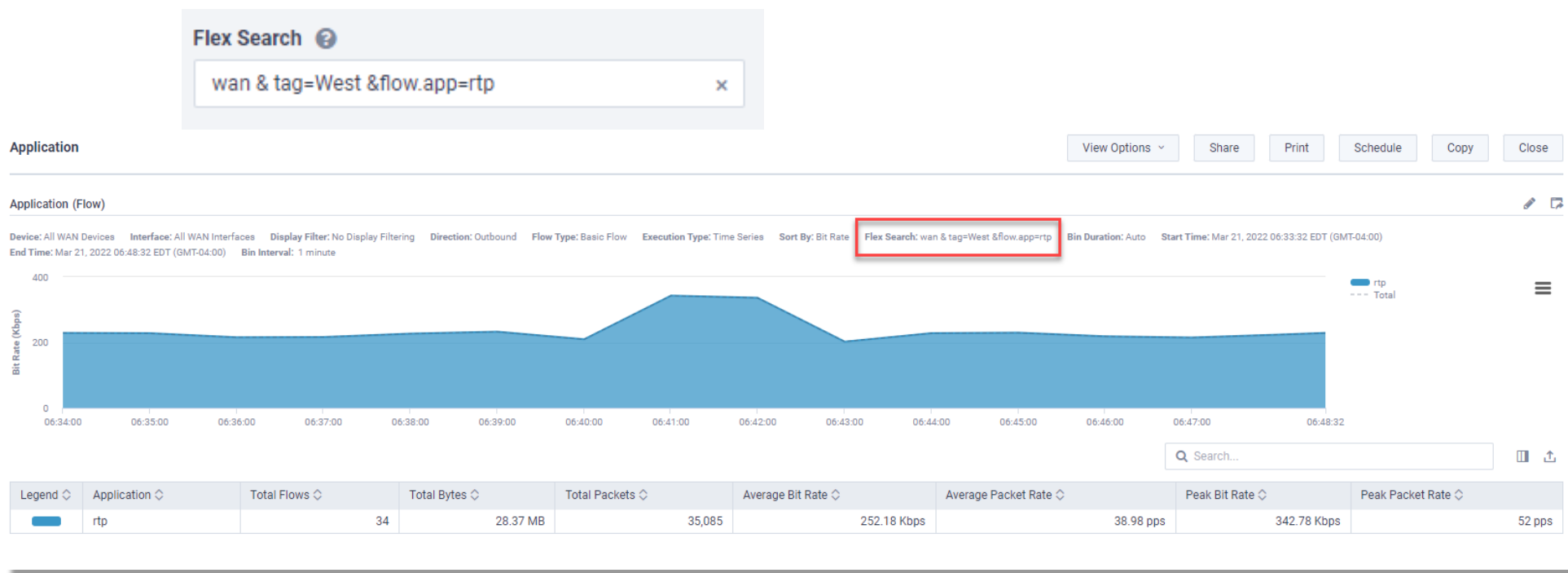
flow.ip=198.18.128.80 | flow.app="TRAINING BITTORRENT"

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



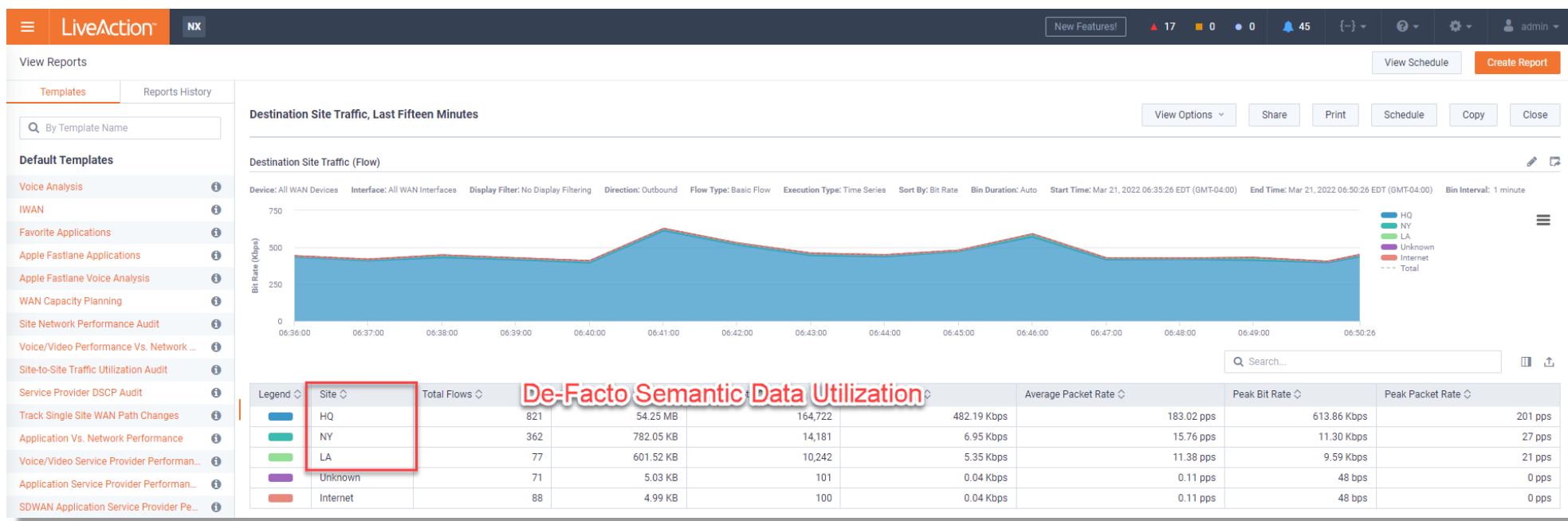
Show me Custom Application **Training Bittorrent** data to or from 198.18.128.80

## 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)

The image displays two screenshots of the 'EDIT 1 SITE' interface, showing various semantic data fields for a site. The top screenshot shows the 'Details' tab with fields for 'Site Description' (Headquarters Data Center), 'Site IP Range (CIDR Notation IP's)' (10.0.0.102, 192.168.122.0/24, 198.18.128.0/18, 10.255.0.0/24), 'Devices' (HQ-B1.dcloud.cisco.com, HQ-B2.dcloud.cisco.com), 'Number of Employees' (200), and 'Tags' (West, HQ, Admin). The bottom screenshot shows the 'Address' tab with fields for 'Address' (Address Line 1, Address Line 2), 'City' (San Francisco), 'State/Province/Region' (CA), 'Zip Code' (Zip Code), 'Country' (Country), 'Latitude & Longitude' (37.774929, -122.419415), 'Phone Number' (Phone Number), 'Email' (Email), and 'Region' (Continent: North America → Country: United States → State: California → City: San Francisco). Red boxes highlight the 'Site IP Range (CIDR Notation IP's)', 'Tags', 'Data Center' checkbox, 'Address' field, 'Latitude & Longitude' field, and 'Region' field in both screenshots.



# End of Day 1... What's Next?

Finish the Labs...

---

## 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

© 2022, LiveAction, Inc. All Rights Reserved.

LiveAction™

161

---

## 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



A man in a grey suit and blue tie stands with his arms outstretched and head tilted back, looking up. The background is a soft-focus bokeh of blue and white light circles. An orange rectangular box is overlaid on the left side of the image, containing the text 'Quality of Service' and 'Concept Overview'.

# Quality of Service

## Concept Overview

---

# How to Implement QoS

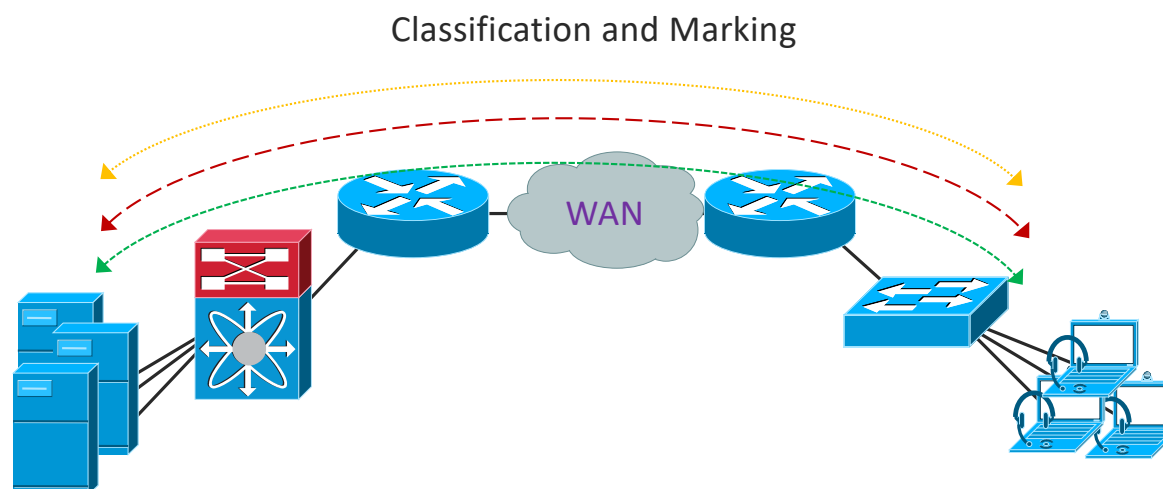
**Step 1 - Recognize Application Traffic** (Classification and Marking)

**Step 2 - Prioritize** (Queuing and Shaping)

**Step 3 - Throttle Traffic** (Policing and WRED)

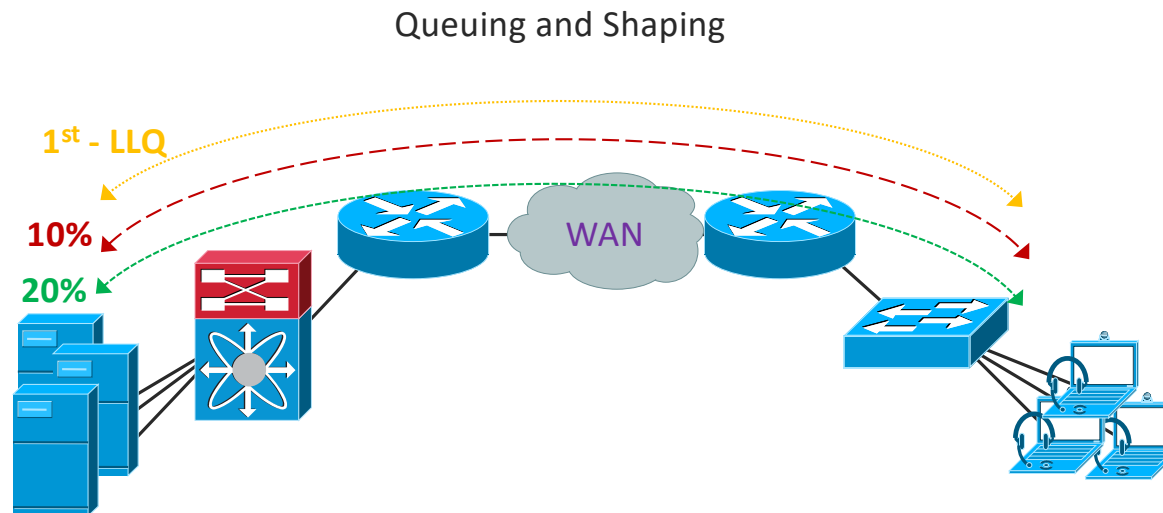
**Step 4 - Buffer Tuning**

# Step 1 - Recognize Application Traffic



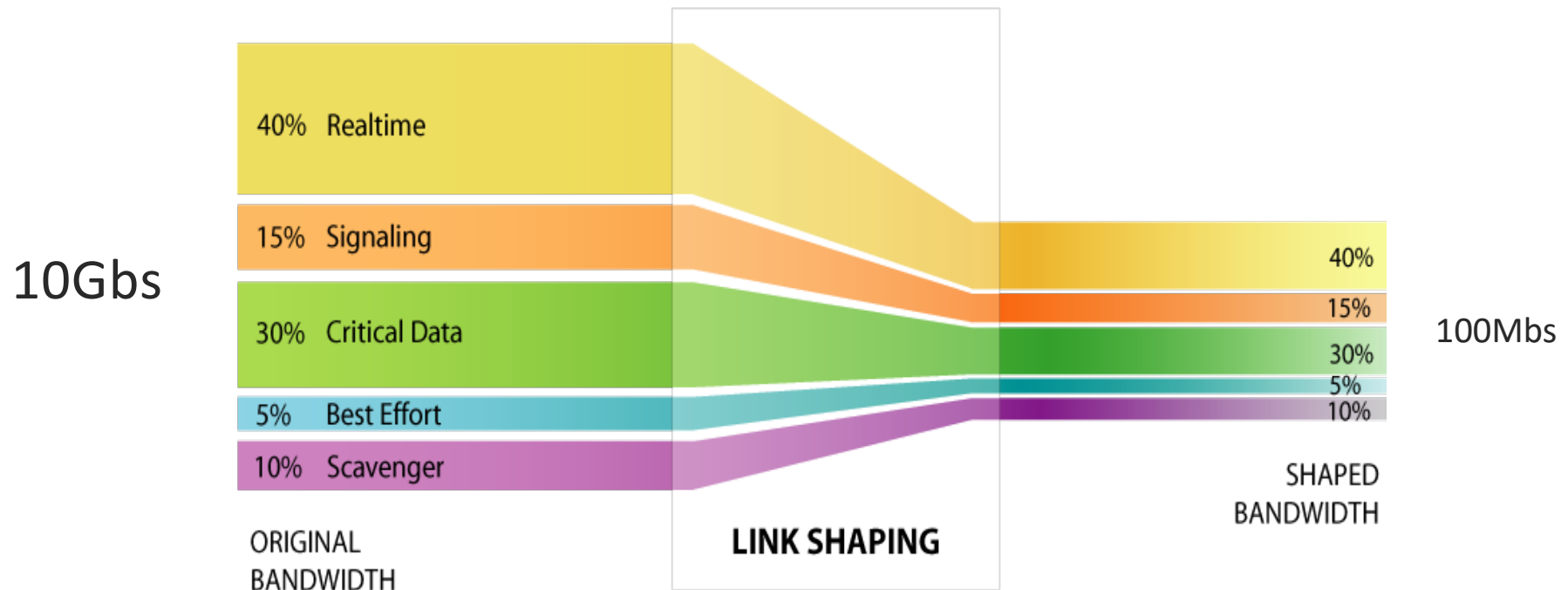
- **ACL** – Match SRC/DST IP addresses & port numbers
- **DSCP** - TOS byte QoS markings
- **NBAR** – Protocol discovery by Cisco devices

## Step 2 – Prioritize

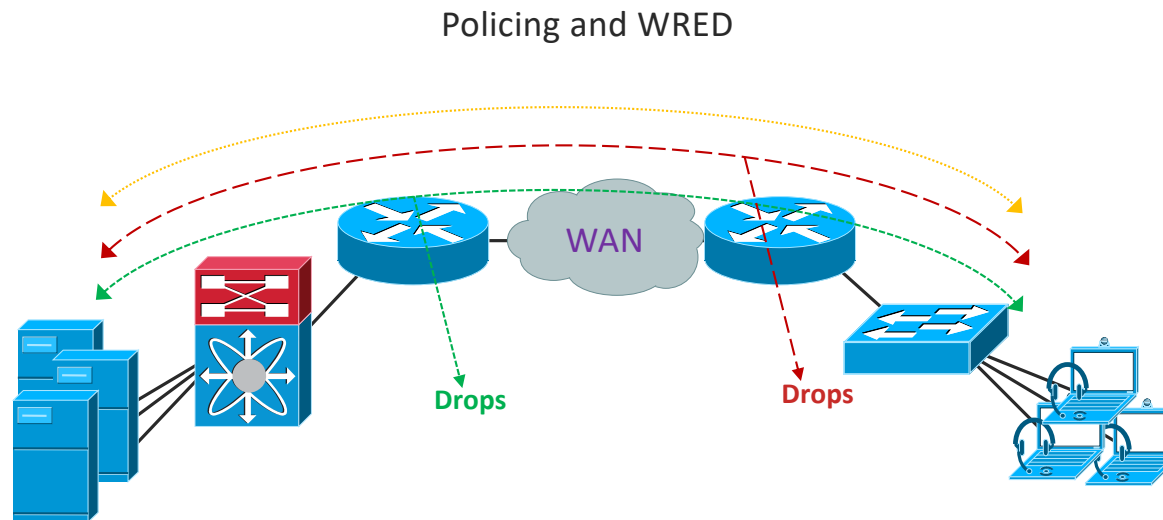


- **Priority Queuing – LLQ**
- **CBWFQ** - Guaranteed bandwidth
- **Shaping** - Transmit data to software set limit, buffer and queue overage

# Shaping (or Scaling)

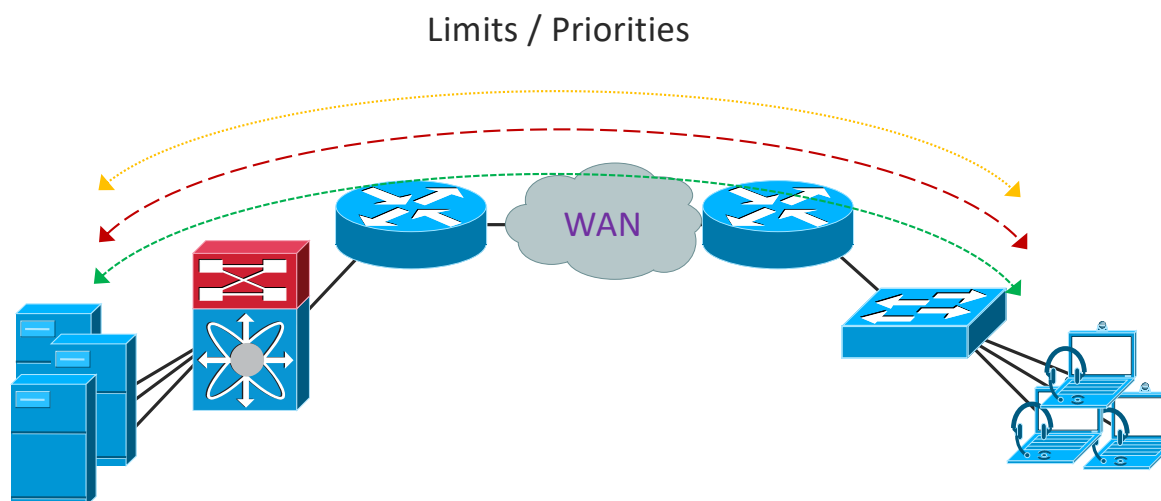


## Step 3 –Throttle Traffic



- **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

A man in a dark suit and light-colored shirt is standing at the front of a room, holding a microphone and gesturing with his right hand towards a large screen. The screen displays a complex network diagram with various nodes and connecting lines. The audience, consisting of several men in business attire, is seated in the foreground, facing the speaker. The overall scene is brightly lit with a blue and white color scheme.

# QoS Monitoring & Configuration



---

## 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 these options

Historical reports from "Reports" Option

**NBAR and Post-Policy**  
09/21/21, 01:15:00 AM to 09/21/21, 01:30:00 AM Data bin: none  
1h 6h 1d 1w 30d 90d 1y Custom

Branch1-LA GigabitEthernet1 Inbound Execute Report

☒ Show Total Bandwidth

**NBAR**

**Post-Policy**

Before QoS - by Application (NBAR) in Kbps

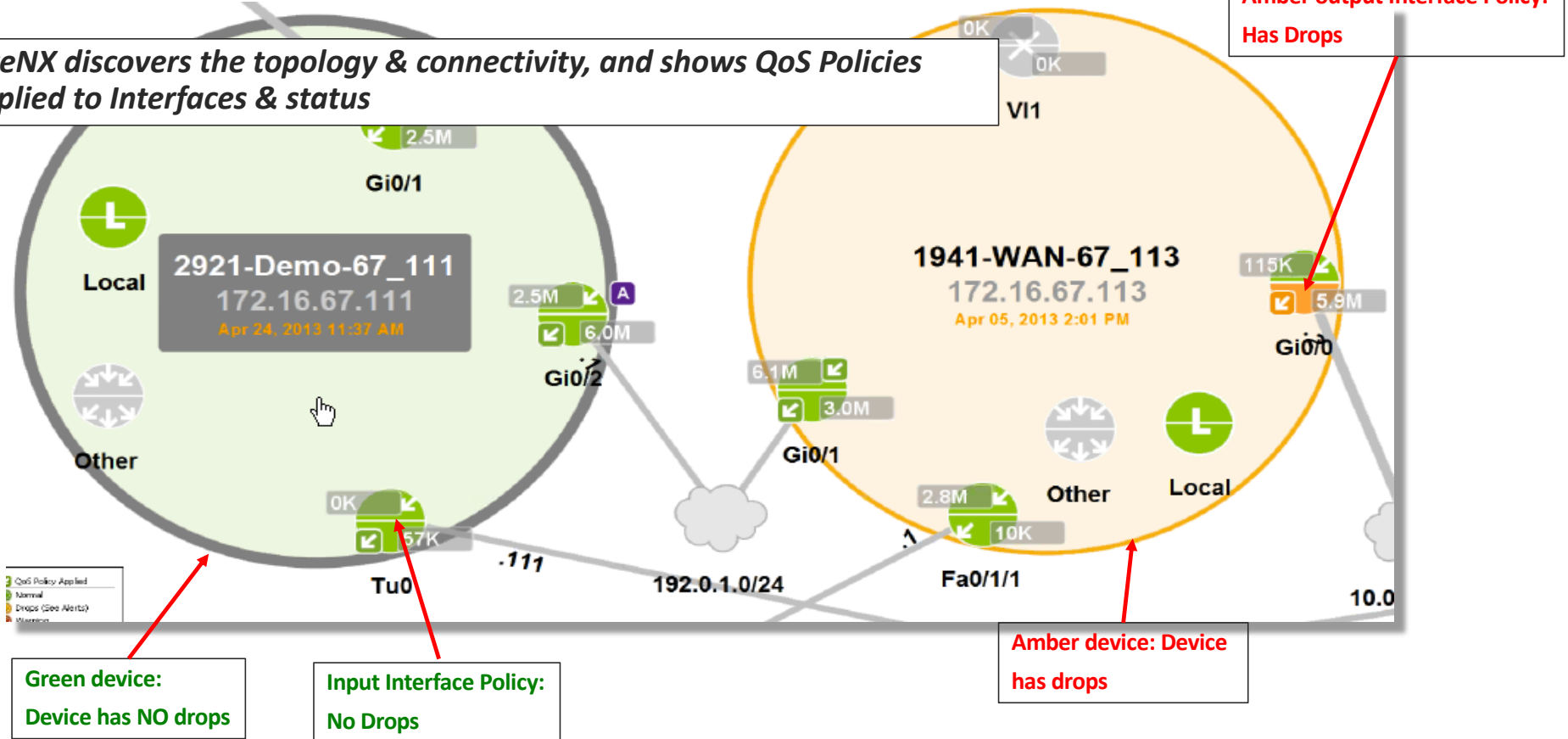
Name	Average	Peak
unknown	122	
rtp-video	117	
rtp-audio	86	
sip	7	
nntp	3	
snmp	3	
ftp	2	
conferencing	2	
statistical-conf-video	1	
statistical-p2p	1	
ms-services	<1	

After QoS - by Class in Kbps

Name	Average	Peak
------	---------	------

# Discover QoS Policy Enforcement Points

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

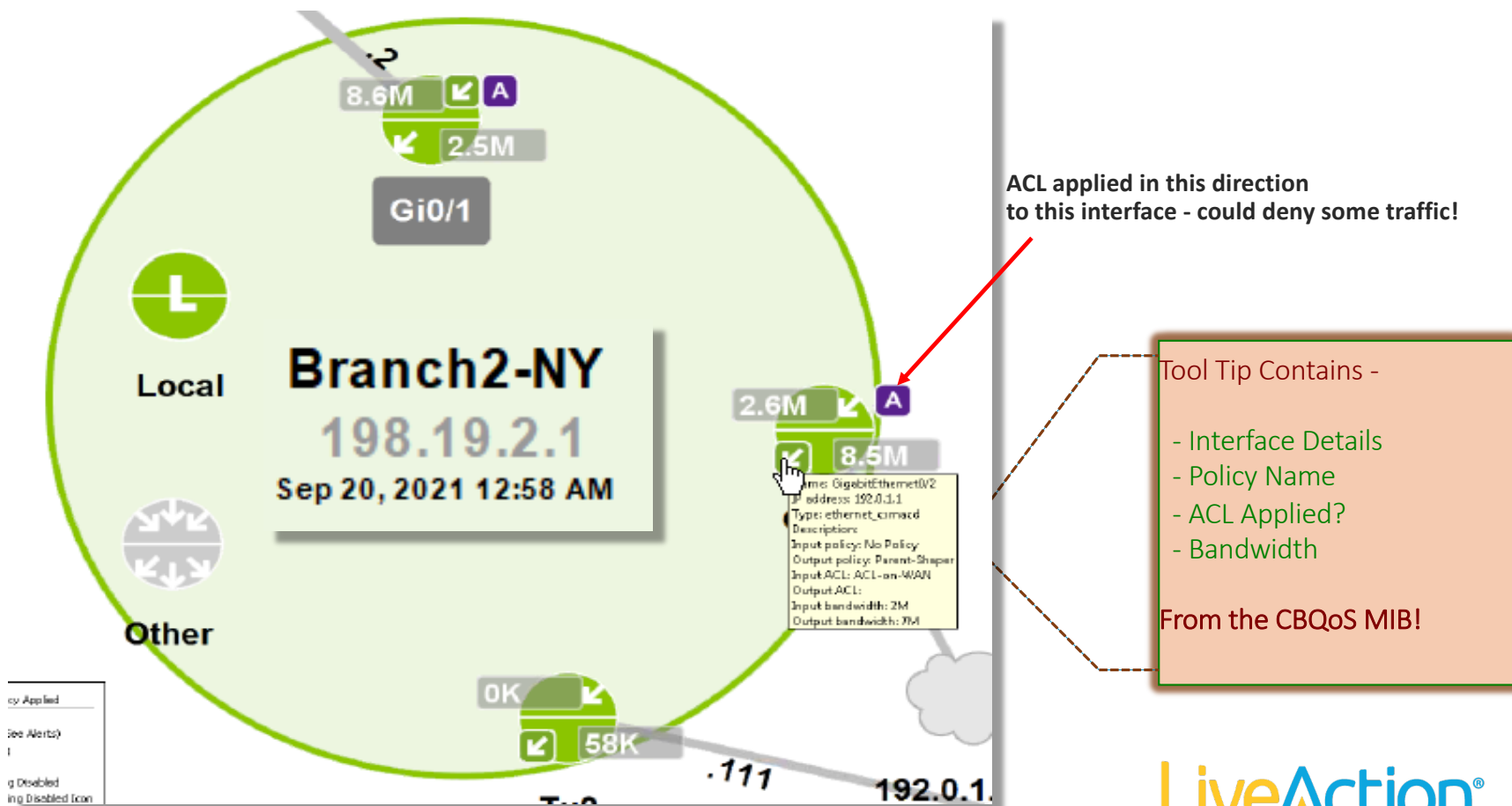


---

## 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



# QoS Device View

LiveAction - 72.234.37.51

File View Users QoS Flow Routing IP SLA LAN Tools Reports Window Dev Help

Dashboard Manage Expand

QoS Flow Routing IP SLA LAN

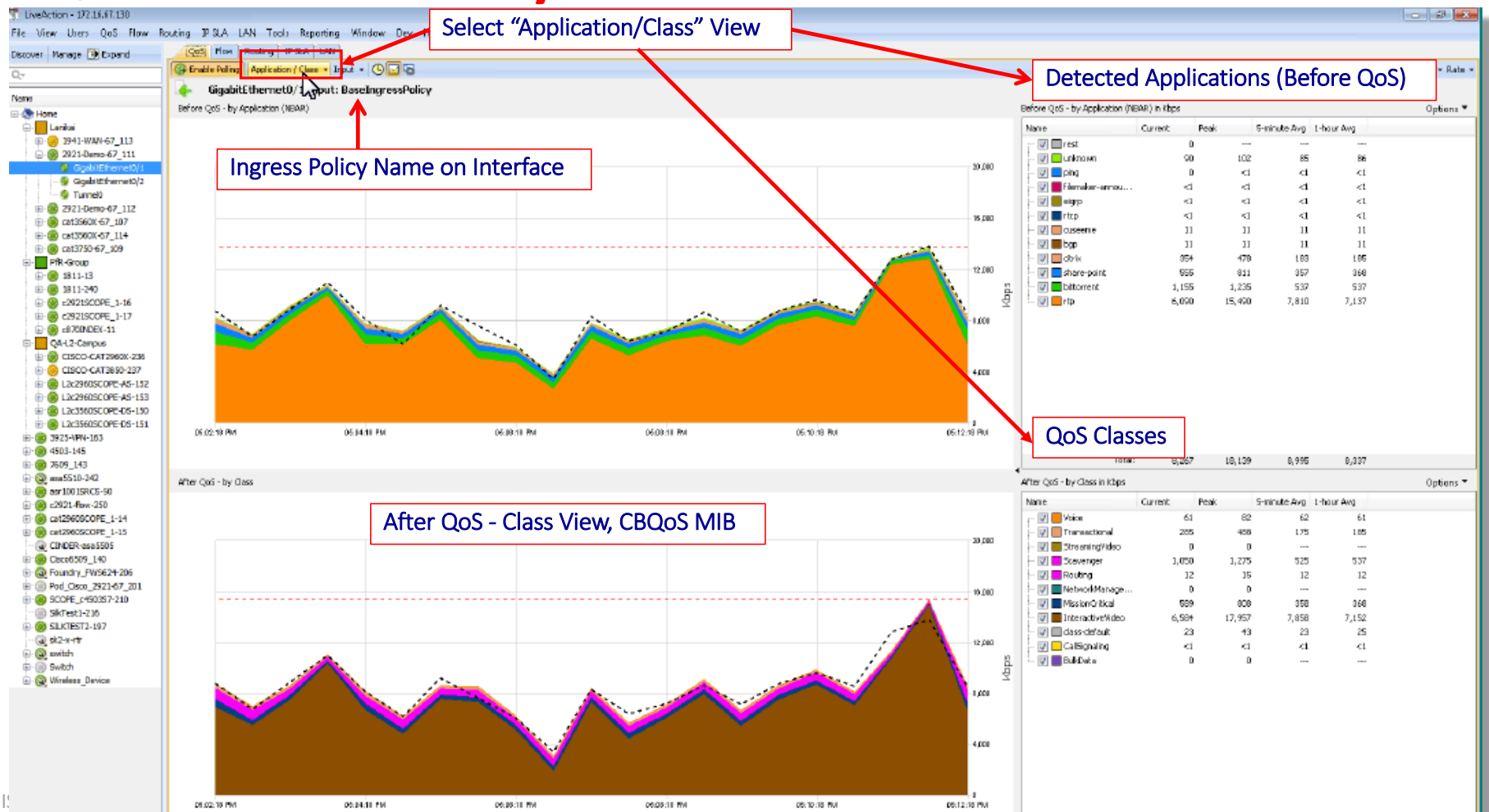
Enable Polling

Name	Policy	Bandwidth(Kbps)	Class drop
FastEthernet0/1/0	Input	2,916	<1
FastEthernet0/1/1	Input	949	
GigabitEthernet0/1	Output	1,420	
GigabitEthernet0/2	Input	5,755	
Vlan1	Output	2,906	
Vlan12	Input	0	
Vlan168	Output	1,454	
Vlan169	Input	6,069	
Vlan3	Output	5,647	
Vlan101	Input	2,289	
Vlan102	Output	0	
Vlan103	Input	0	
Vlan104	Output	0	

Policies applied on interfaces

Policies applied on interfaces

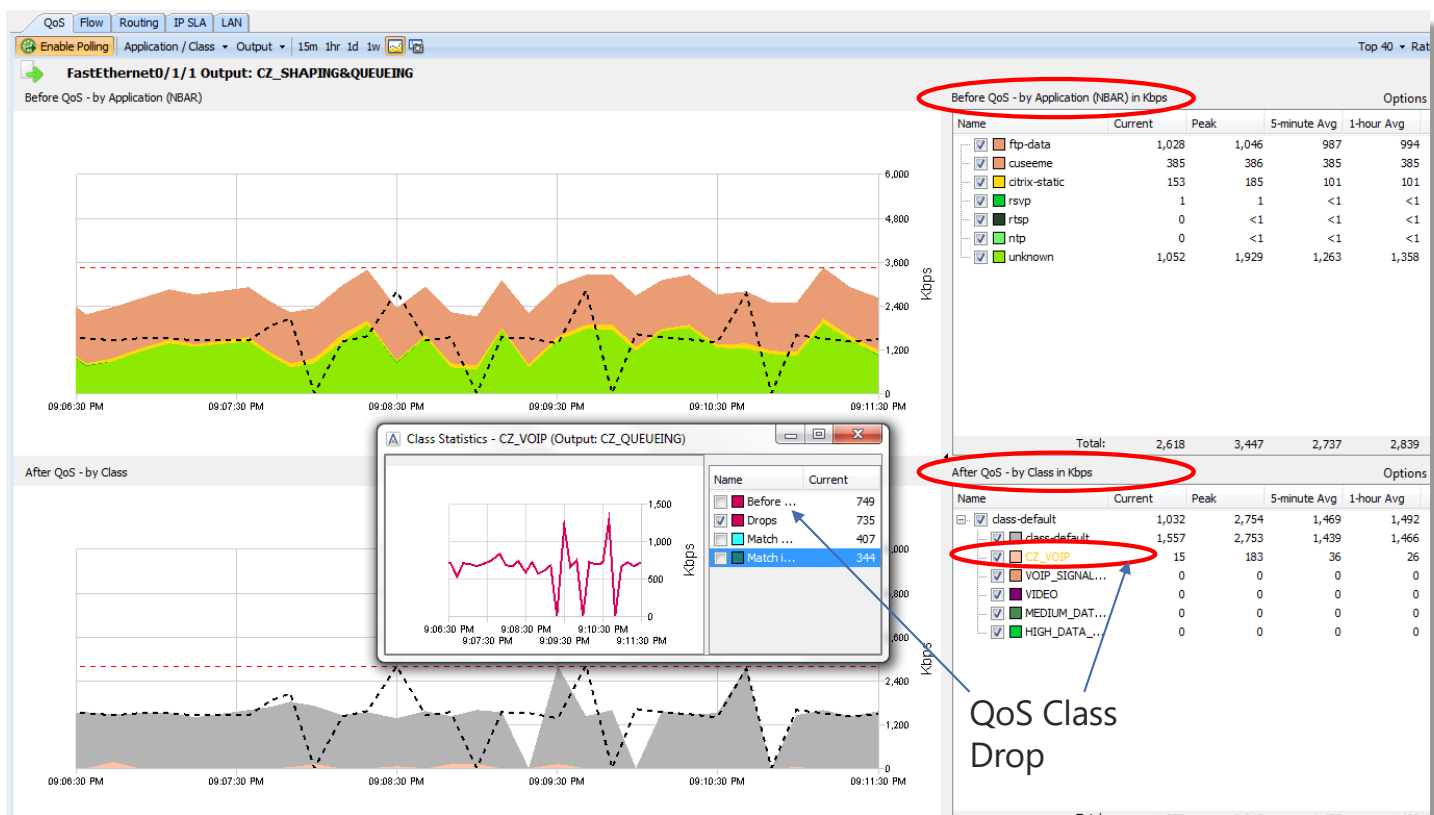
# QoS Interface Policy Performance



# QoS Troubleshooting

- Real-Time QoS Issues

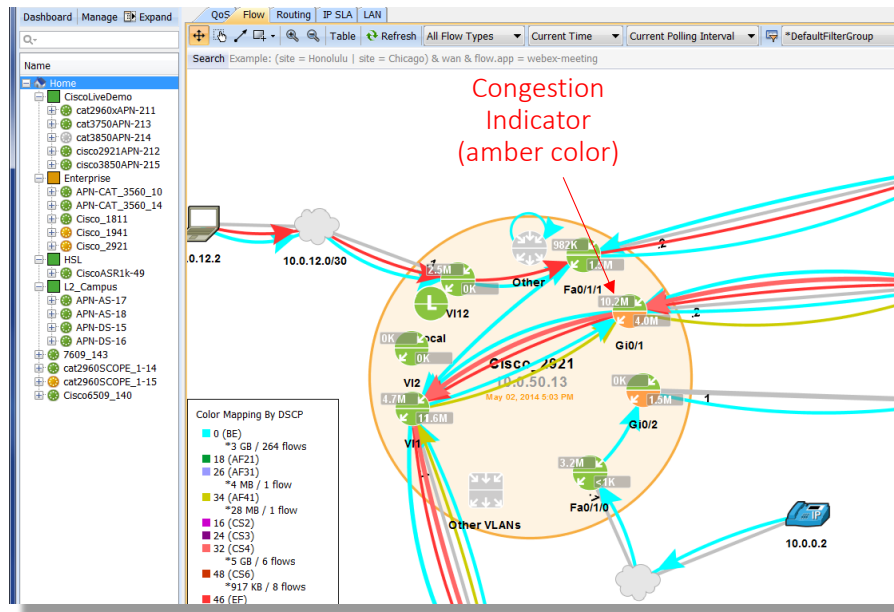
Amber QoS class color shows class drops



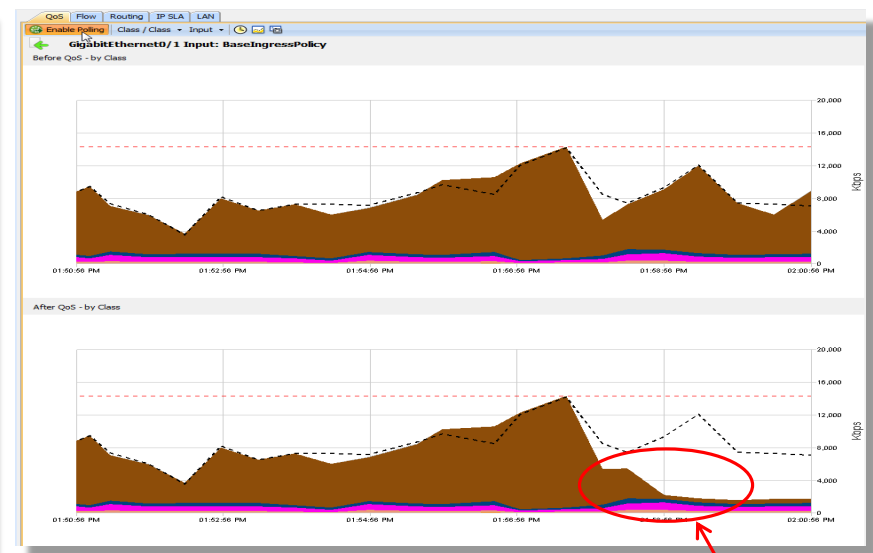


# Track QoS Performance & Policy Validation

## Visualize QoS Performance



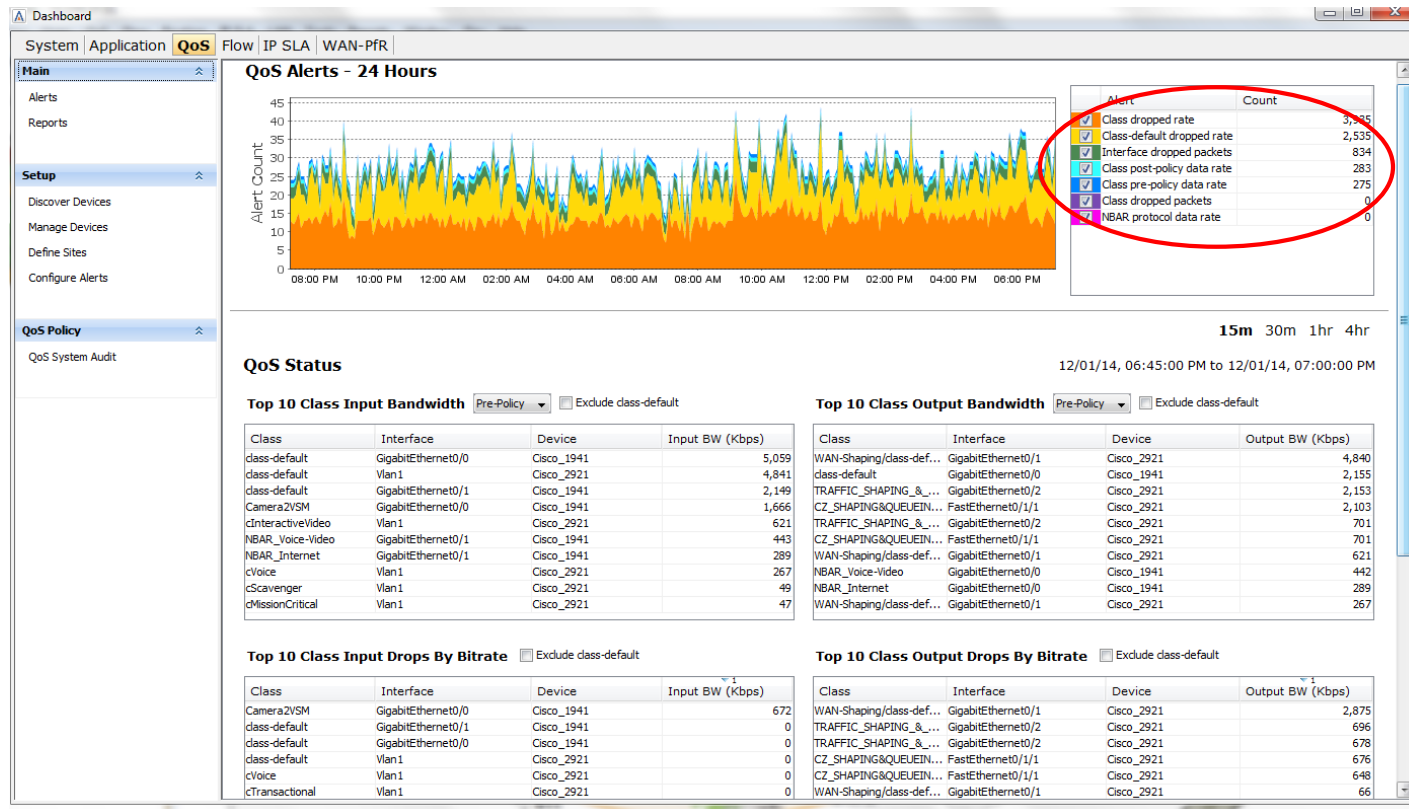
## Show Impact of QoS Policy



Policy applied to Police Interactive Video to 512 Kbps

LiveAction®

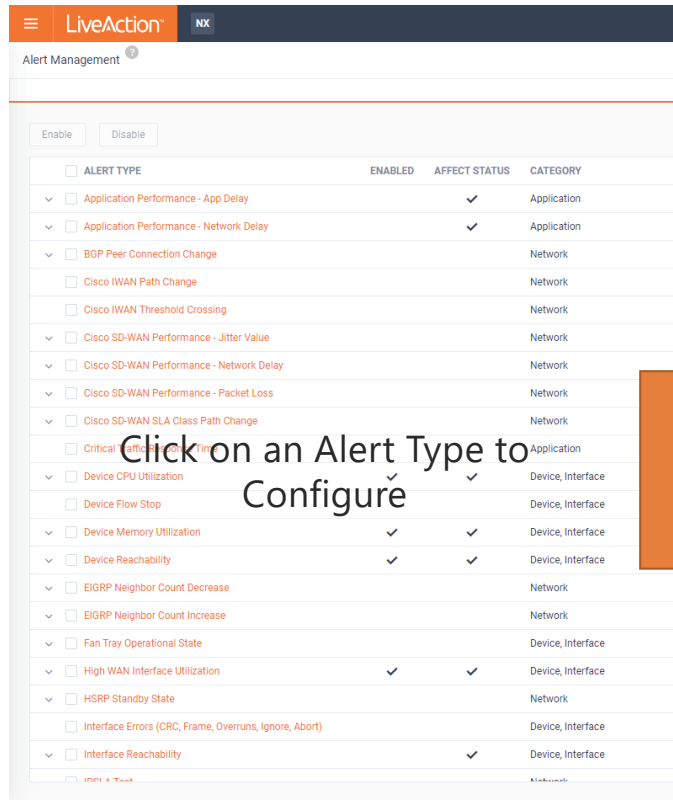
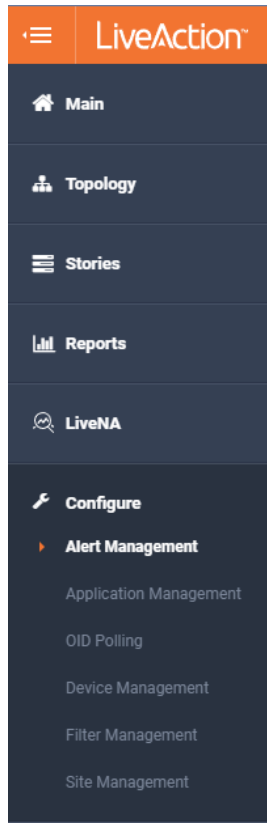
# QoS Dashboard



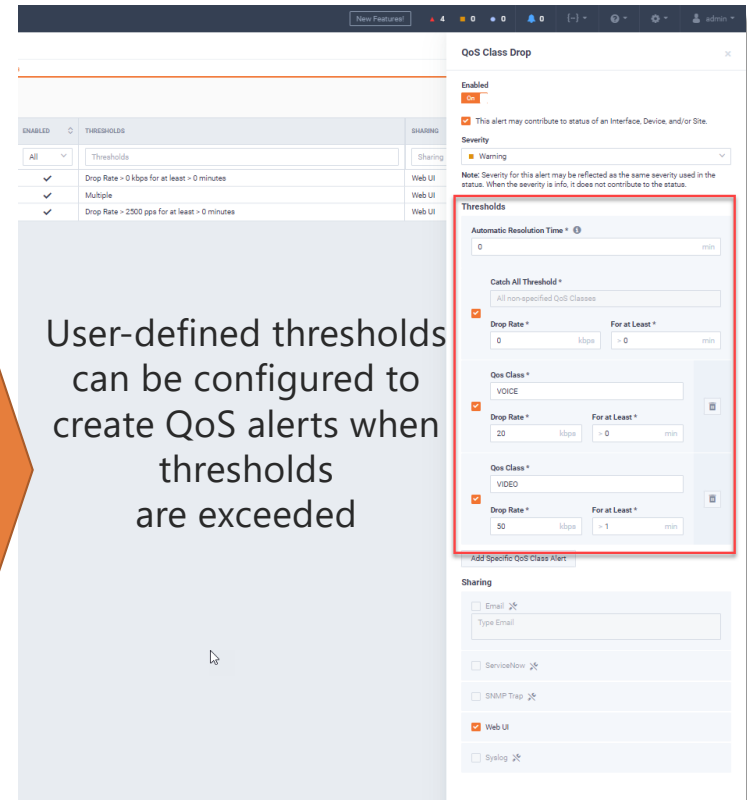
Driven from MIB-II, NBAR, and CBQoS MIBs

LiveAction®

# Troubleshooting - Real-Time QoS Alerts

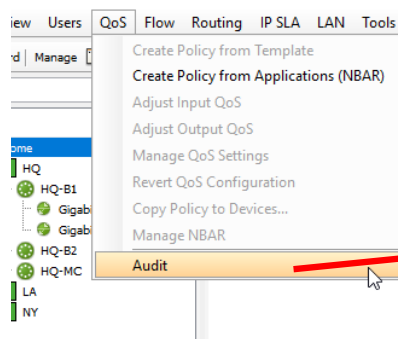


Click on an Alert Type to Configure



# Troubleshooting – Auditing QoS Policies

Single-click!



**QoS Policy and Performance Audit Report**

Tuesday, September 21, 2021 | 2:00 AM EST

**Issues** [Export to CSV](#)

Device	Issues
System	CLASS MISMATCH: 7 classes that have the same name have different match statements. Classes across multiple devices with the same name have different match statements.
System	EXCESS CLASS: The system contains 138 distinct class names. Excessive number of class definitions across the system.
7609_143.referentia.com	NO CLASS MATCH: 4 classes have no match statements. Classes were defined with no match statements.
APN-CAT_3560_14	SWITCH REMARK: Enabling QoS on switches will remark DSCP/COS values to zero by default unless trust is enabled.
APN-DS-16.actionpacked.com	NO CLASS MATCH: 4 classes have no match statements. Classes were defined with no match statements.
cat2960SCOPE_1-14	NO CLASS MATCH: 12 classes have no match statements. Classes were defined with no match statements.
cat2960SCOPE_1-14	SWITCH REMARK: Enabling QoS on switches will remark DSCP/COS values to zero by default unless trust is enabled.
cat2960SCOPE_1-15	NO CLASS MATCH: 1 classes have no match statements. Classes were defined with no match statements.
cat2960SCOPE_1-15	SWITCH REMARK: Enabling QoS on switches will remark DSCP/COS values to zero by default unless trust is enabled.
cat2960xAPN-211.actionpacked.com	NO CLASS MATCH: 2 classes have no match statements. Classes were defined with no match statements.

---

## LiveNX QoS Configure

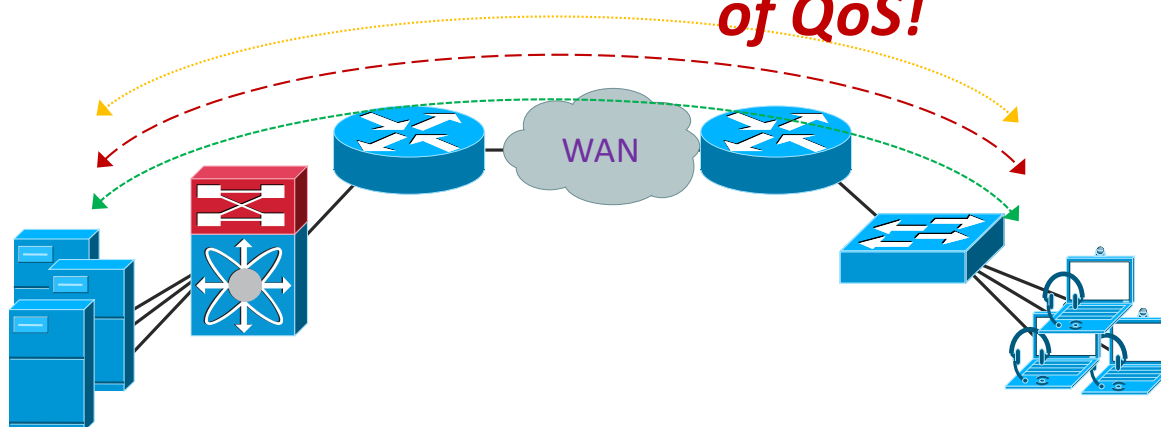
- Full MQC (Modular QoS Configuration) support including WRED, CBWFQ, Priority Queuing, Shaping
- Read pre-existing QoS policies already configured on devices
- Take snapshots of current QoS configuration for future use
- Apply or remove QoS configurations quickly and easily across multiple interfaces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



# Recognize Application Traffic

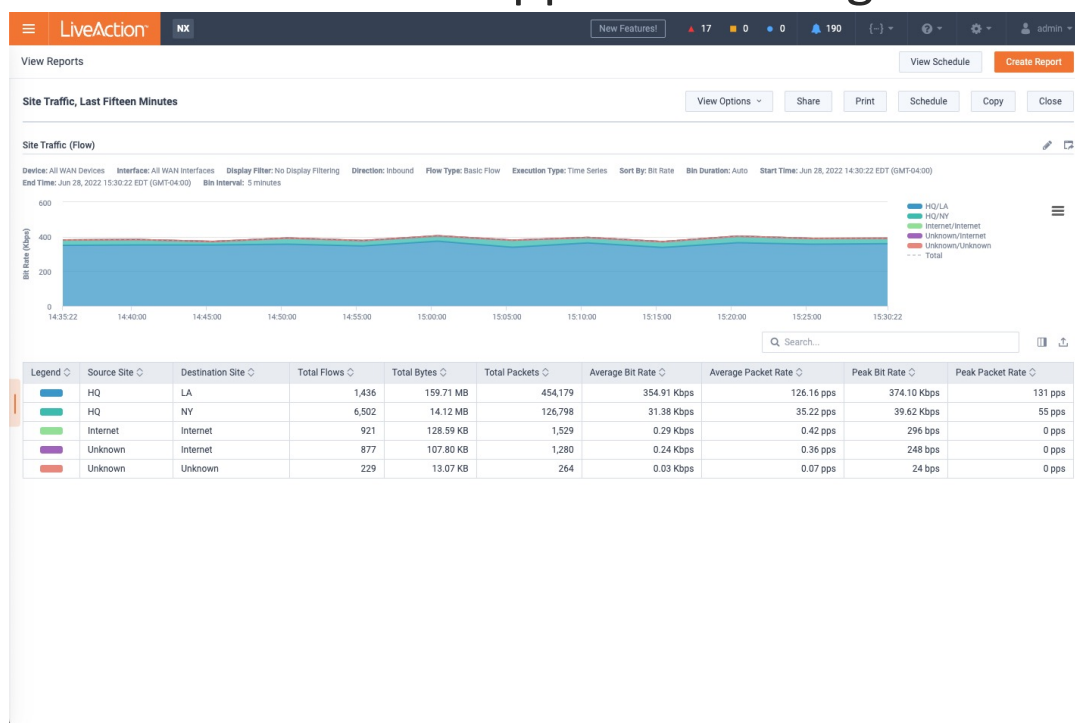
*This may be the hardest & most important part of QoS!*



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

# 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





# Classification: Create Custom Filter (WebUI)

The screenshot displays the LiveAction WebUI interface. At the top, the 'LiveAction' logo and 'NX' tab are visible. The 'Filter Management' section is highlighted with a red box. Below it, there are buttons for 'Add', 'Edit', 'Copy', and 'Delete'. A table lists filters with columns for 'FILTER NAME', 'PUBLIC', 'CREATED BY', and 'DESCRIPTION'. The table contains two entries: 'TRG Voice' and 'VOICE'. An 'EDIT FILTER' modal is open in the center, showing fields for 'Name \*', 'Description', and 'Details \*'. The 'Name \*' field contains 'TRG Voice'. The 'Details \*' field contains 'Application: mgcp sip h323 rtp'. Below the 'Details \*' field, there is a checkbox for 'Off' and a 'Sharing' button. At the bottom of the modal are 'Cancel', 'Save as New', and 'Save' buttons. A red text overlay at the bottom of the modal reads: 'Applying this filter in Logical Topology should show only these applications'. The bottom of the page shows 'Rows: 2 / 2'.

FILTER NAME	PUBLIC	CREATED BY	DESCRIPTION
Filter Name	All	Created By	Description
TRG Voice		admin	Showing SIP and RTP traffic
VOICE			

**EDIT FILTER**

Name \*  
TRG Voice

Description  
Description

Details \*  
Application: mgcp sip h323 rtp Enter Filter Request Here

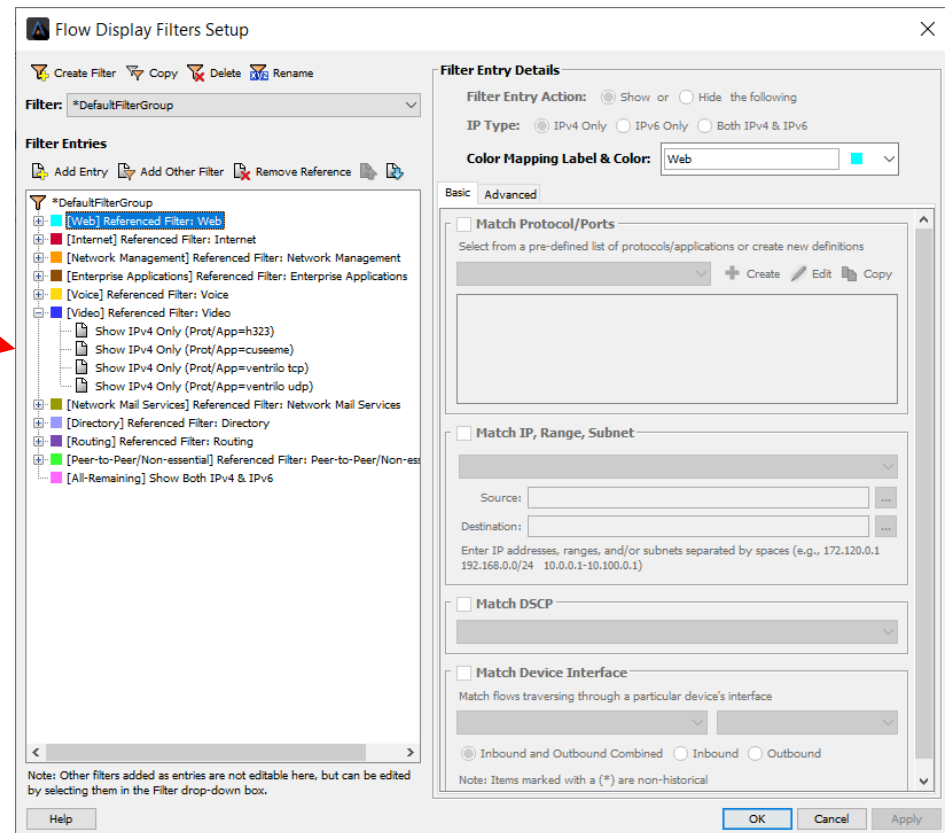
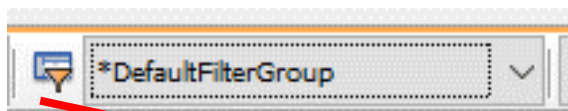
☐ Off Sharing

Cancel Save as New Save

Applying this filter in Logical Topology should show only these applications

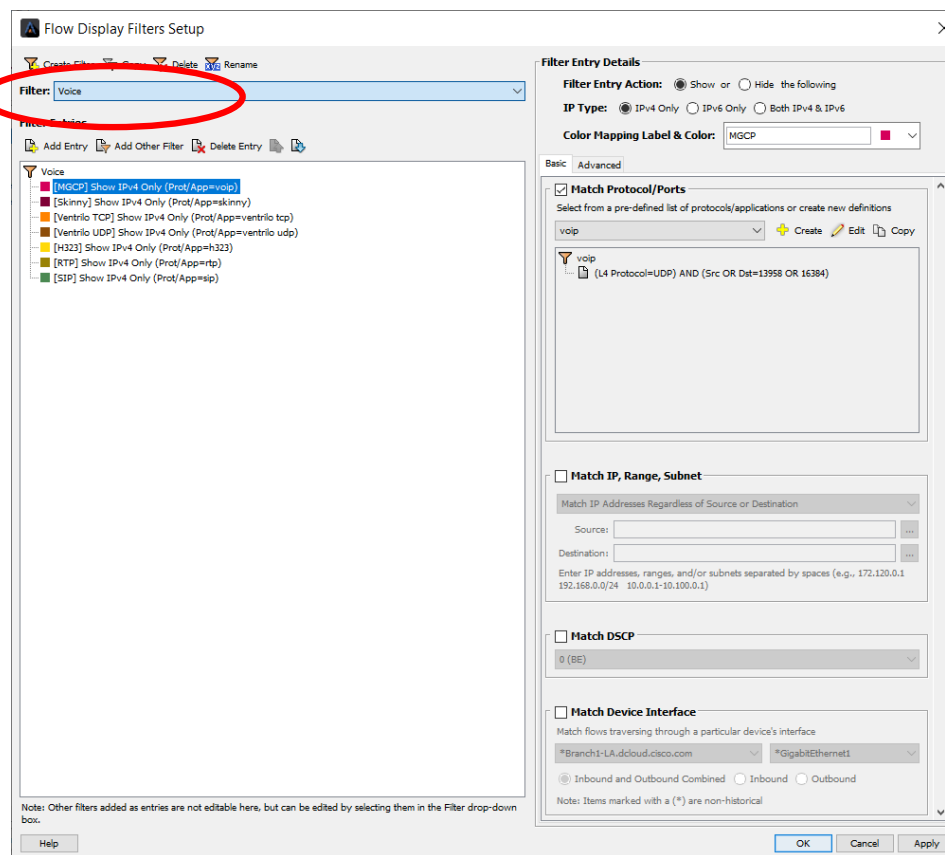
Rows: 2 / 2

# Classification: Create Custom Filter (Eng Console)



# Classification: Copy Voice Filter

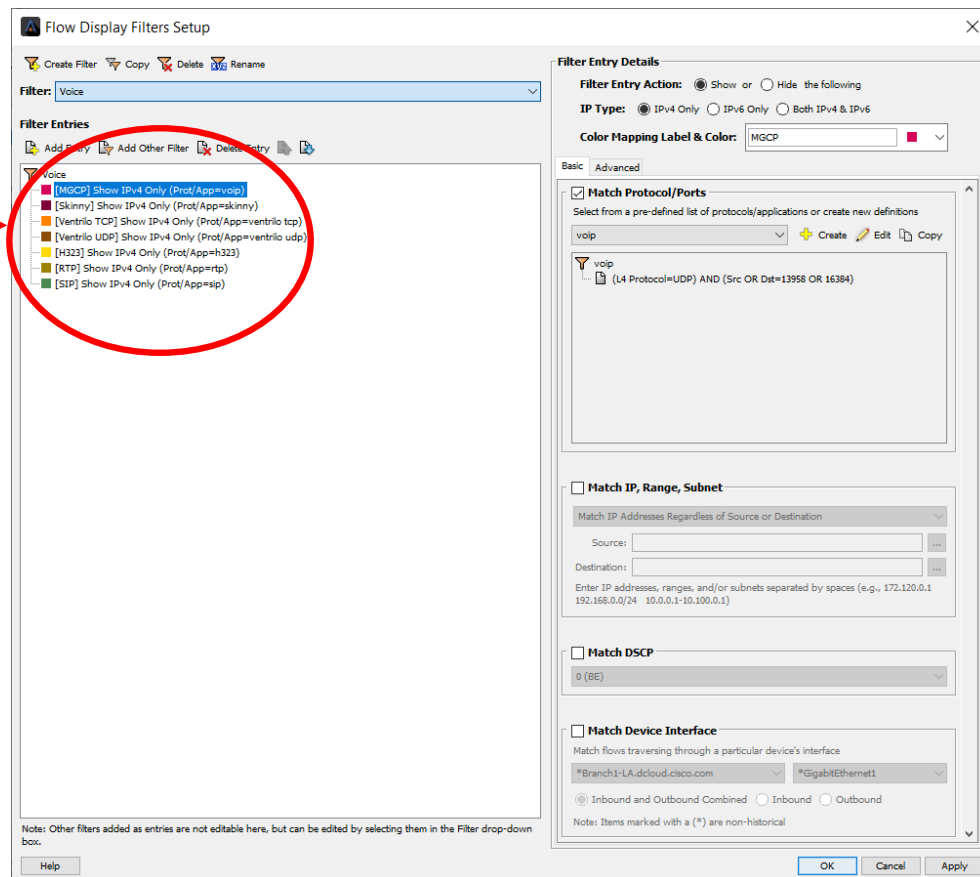
- Find pre-canned Voice filter
- Copy and rename it



# Classification: Delete Unused Entries

## Delete unused Entries

- VoIP
- Ventrilo TCP
- Ventrilo UDP



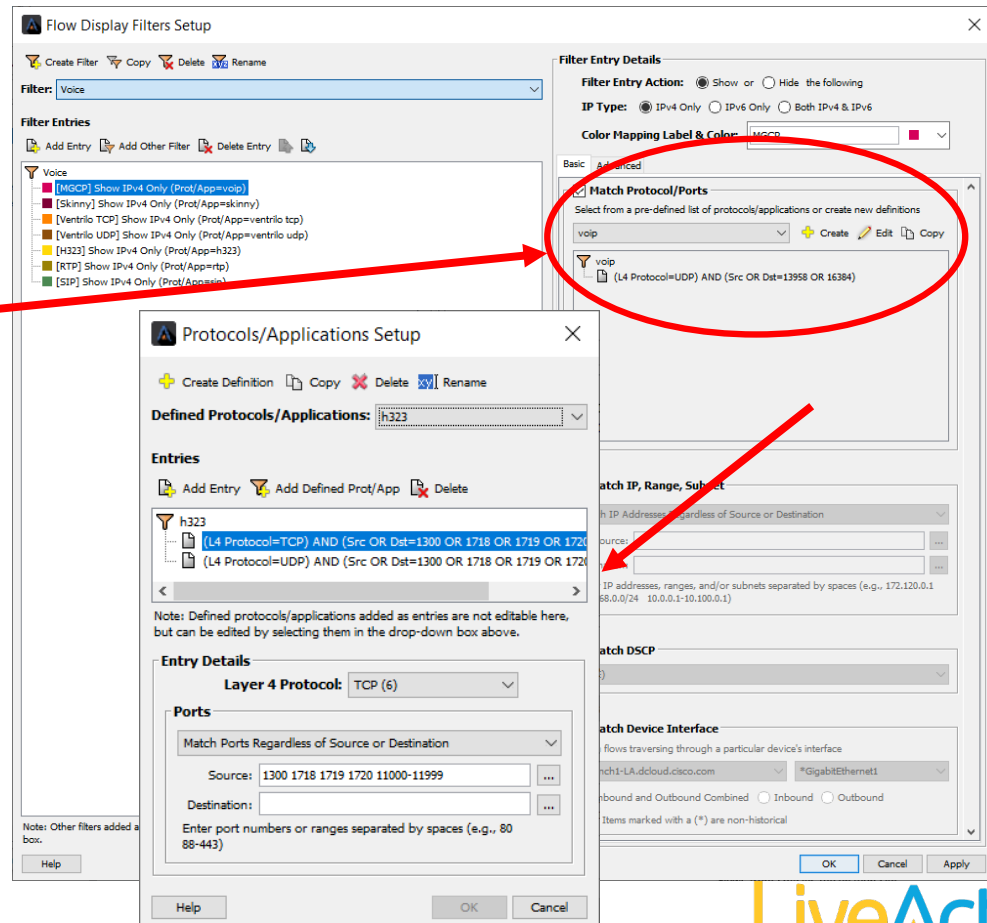
# Classification: Add/Edit Entries

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

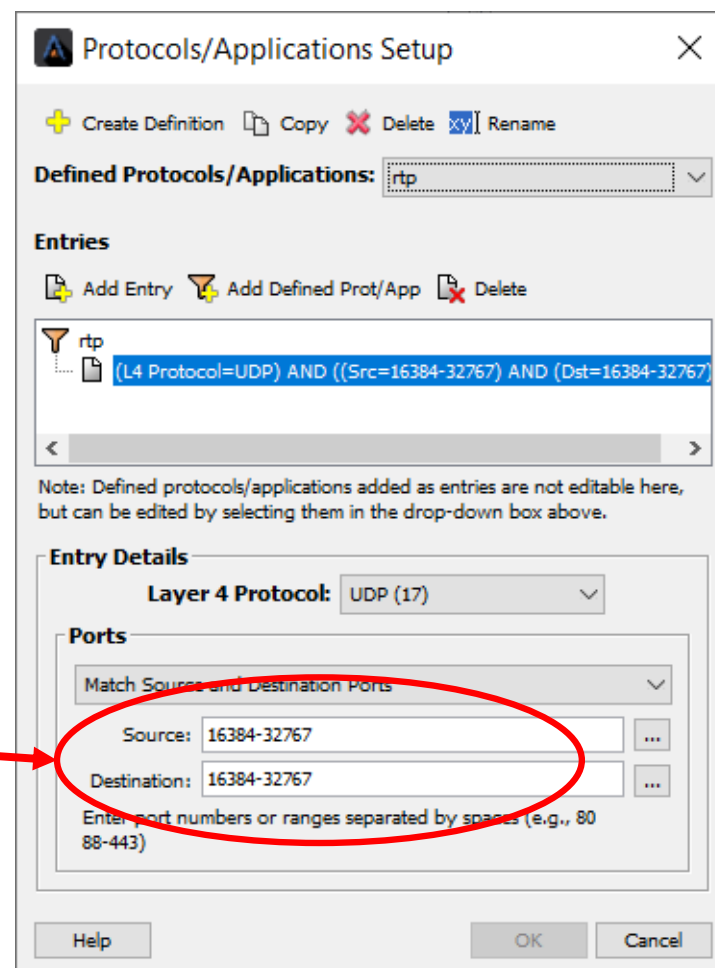
TCP/UDP = Src or Dst = 1718 1719 1720

## SIP

TCP/UDP = Src or Dst = 5060 5061 5062

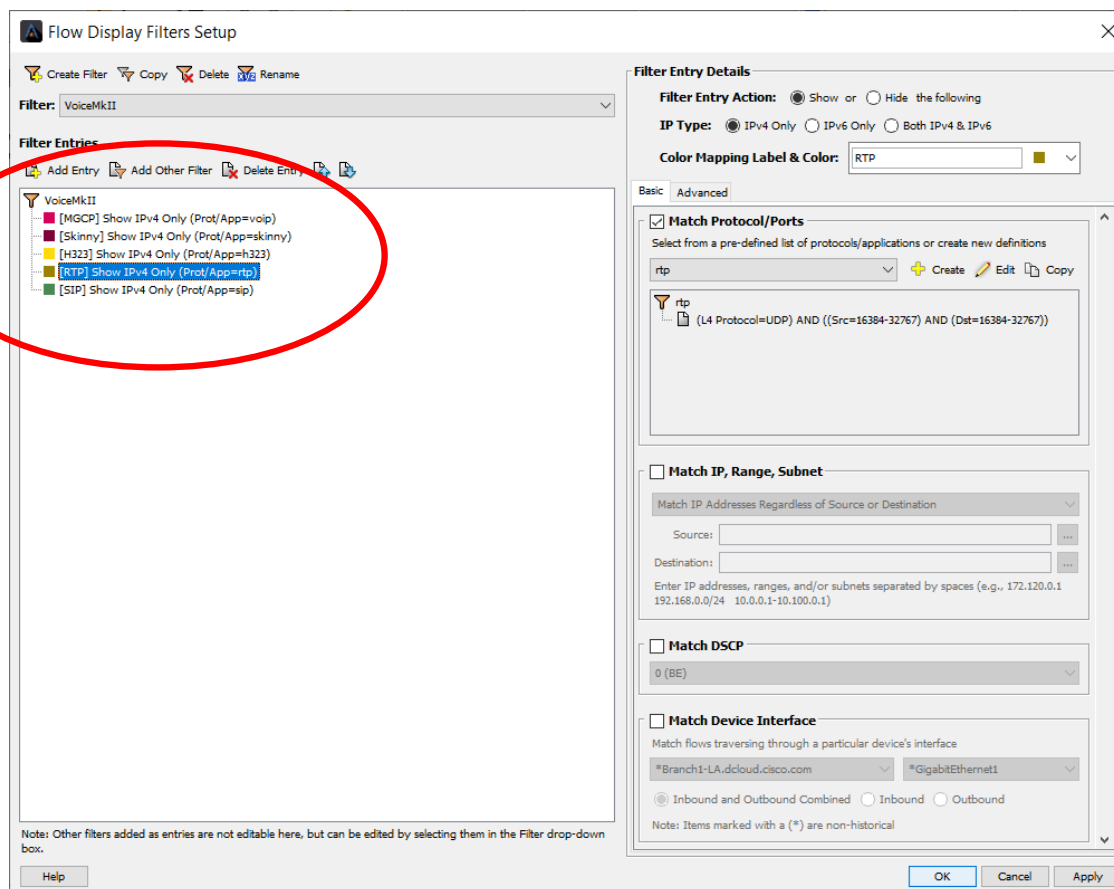
## RTP

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**

LiveAction®

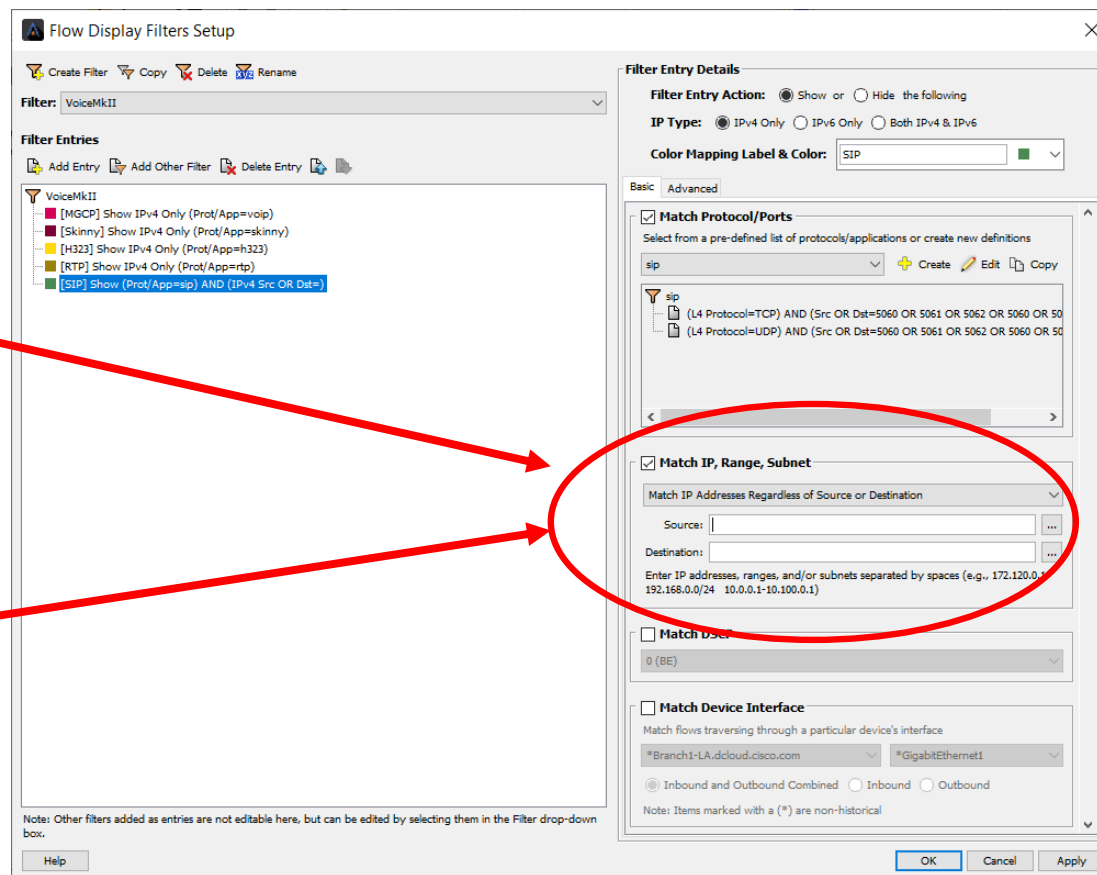
## Classification: Voice Filter is ~99 accurate

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

- MGCP
- Skinny
- h323
- SIP

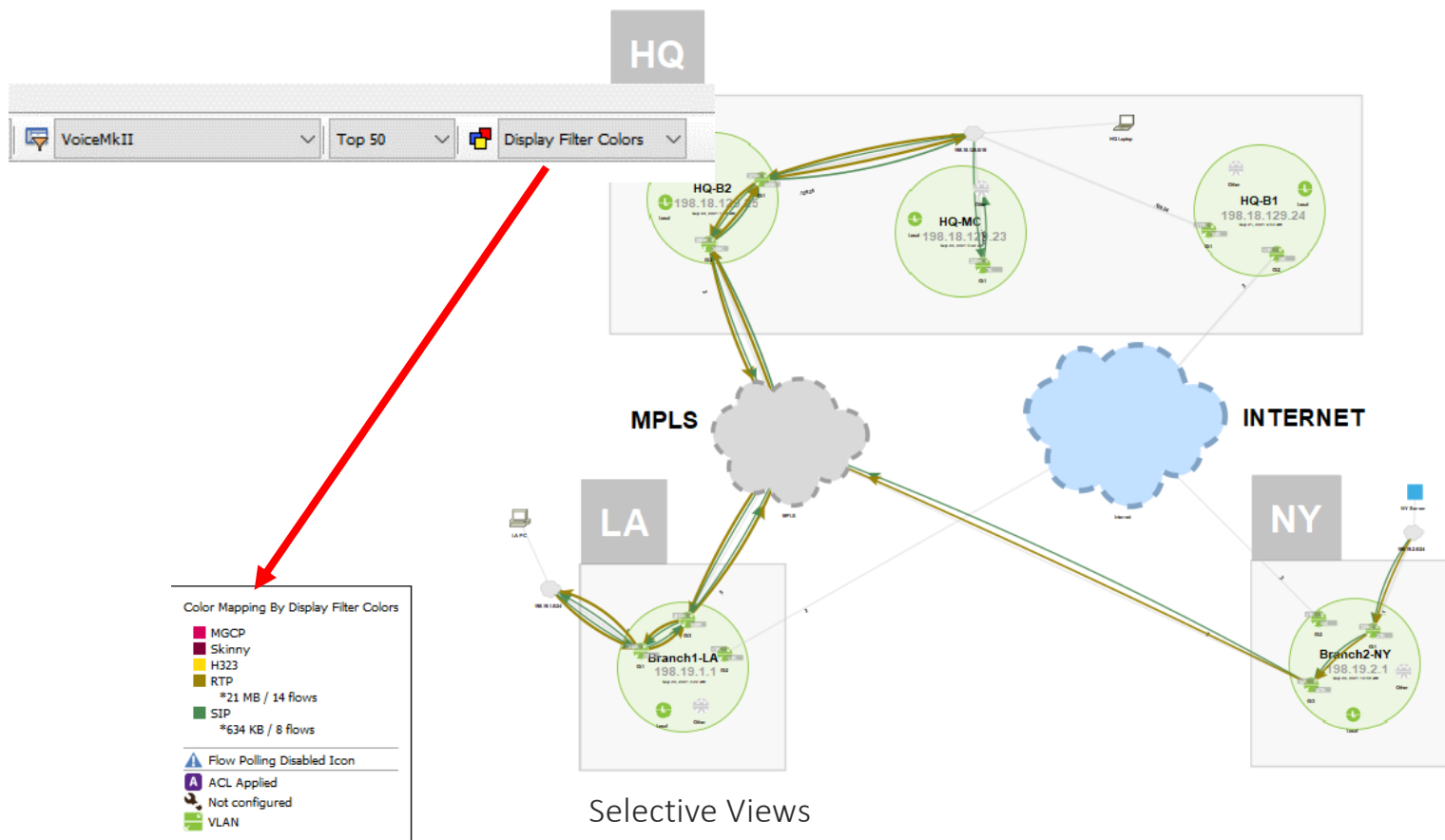
If feasible, add voice subnets to:

- RTP



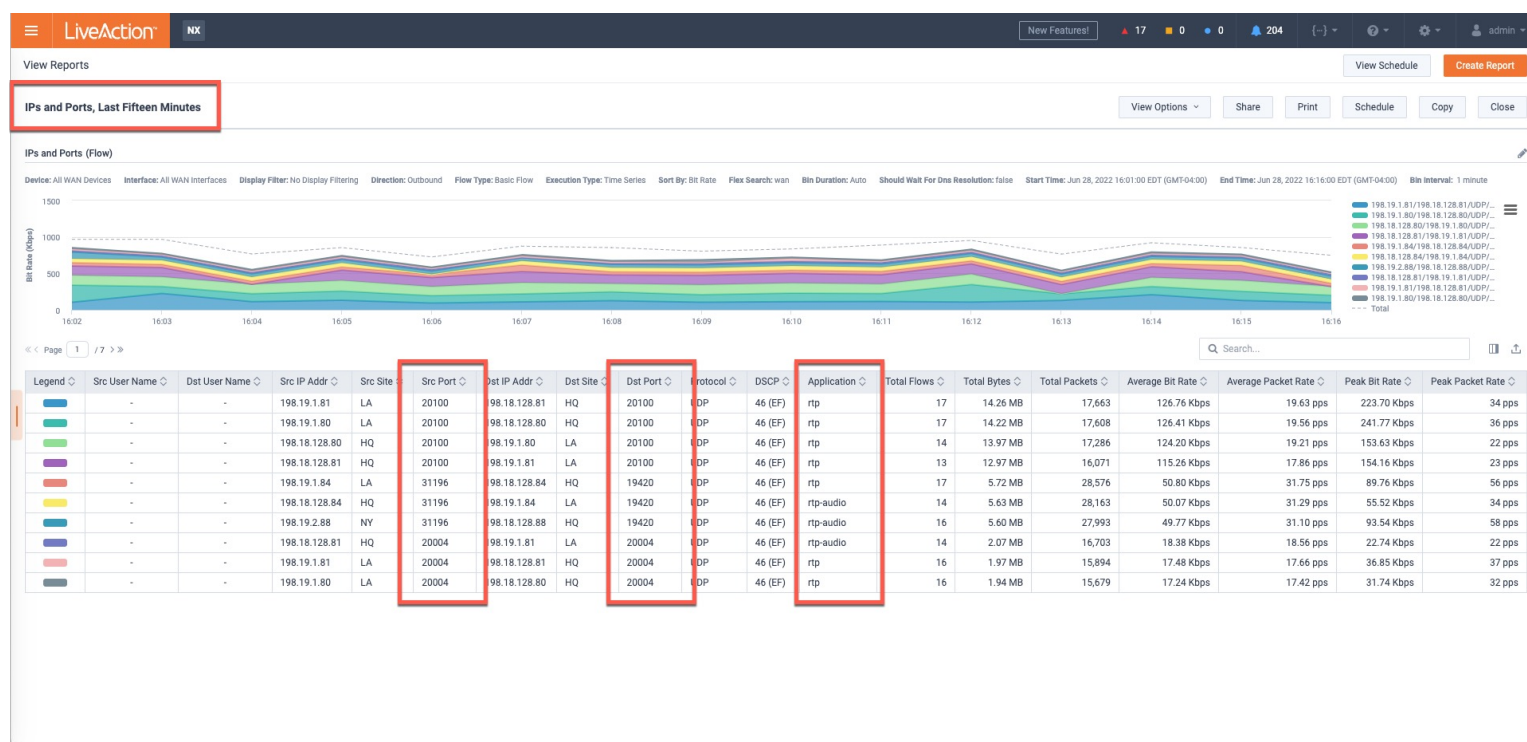


# Classification: Display Filter Colors



Selective Views  
Always be aware of what you are viewing!

# Classification: IPs & Ports Report



Use this report to validate Filter's Accuracy.

NBAR2 is your Friend!

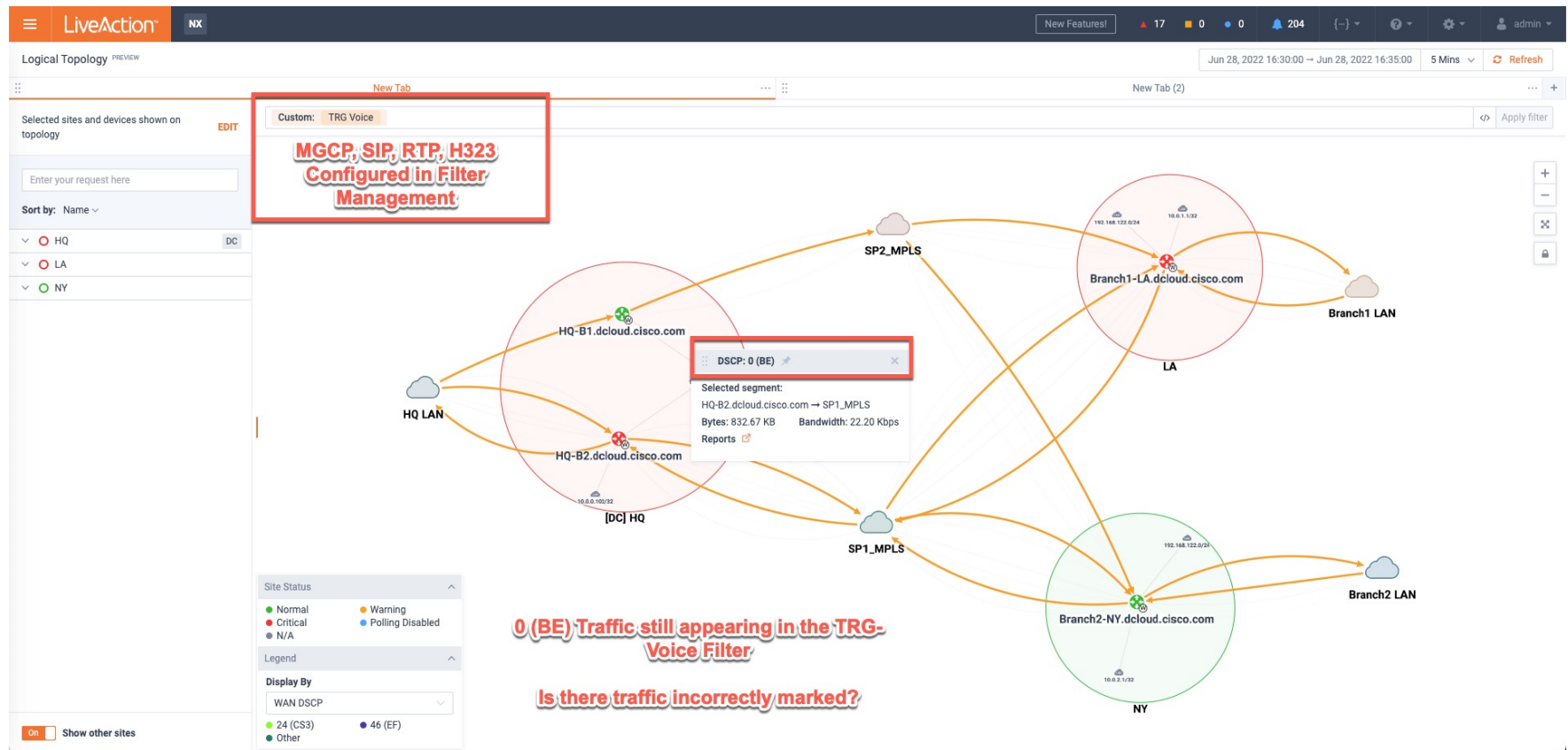
If NBAR doesn't fulfil your needs use **Custom Applications**

## 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)
Network Management		CS6 (48)	CS2 (16)
Transactional Data / Low-Latency Data	AF41 (34) AF42 (36) AF43 (38) AF31 (26) AF32 (28) AF33 (30) AF21 (18) AF22 (20) AF23 (22) AF11 (10) AF12 (12) AF13 (14)	AF41 (34) AF42 (36) AF43 (38) AF21 (18) AF22 (20) AF23 (22) AF11 (10) AF12 (12) AF13 (14)	AF21 (18) AF22 (20) AF23 (22)
Bulk Data / High Throughput Data			AF11 (10) AF12 (12) AF13 (14)
Scavenger / Low-Priority Data		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.**

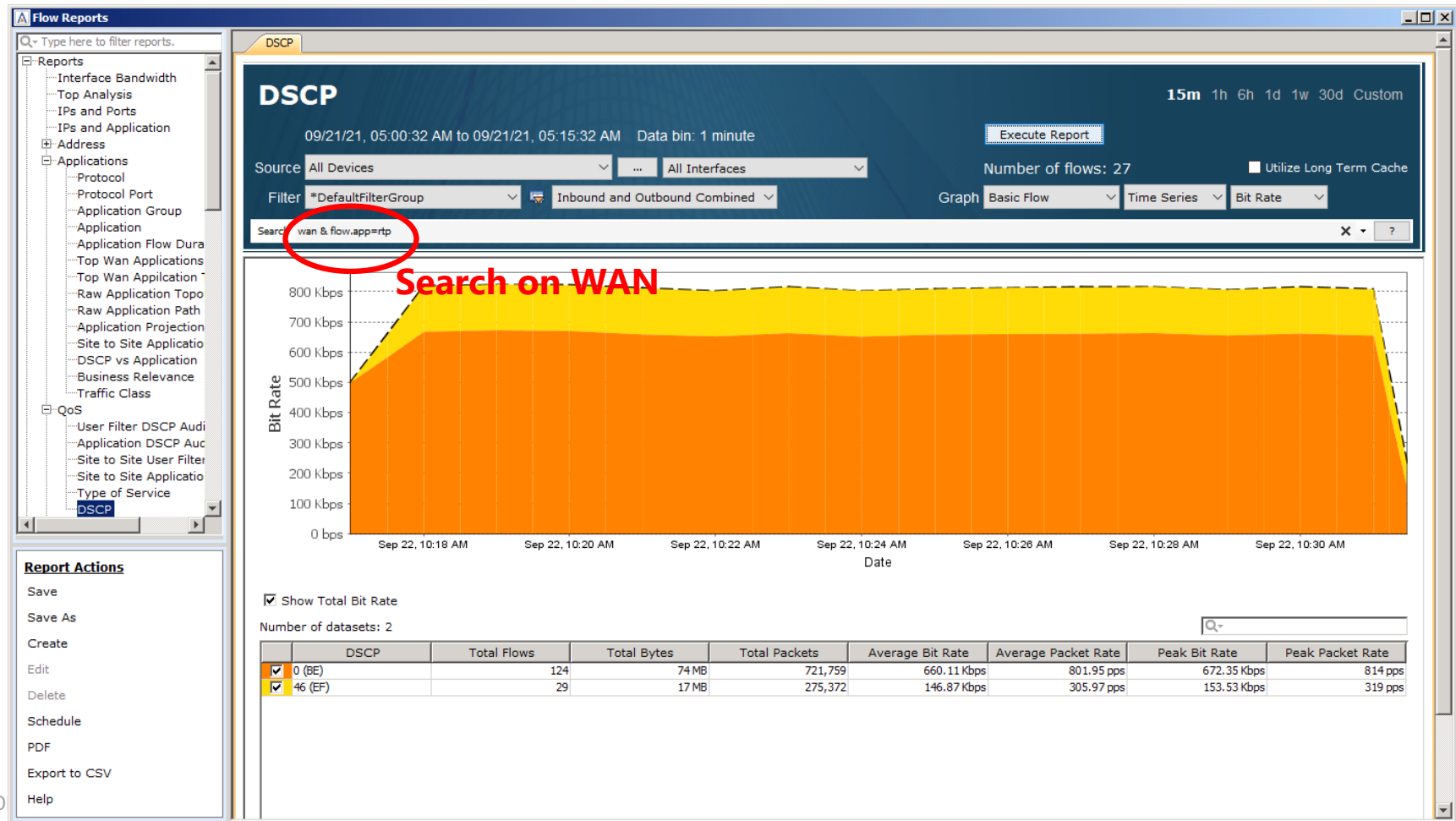
# Marking: DSCP Visualization



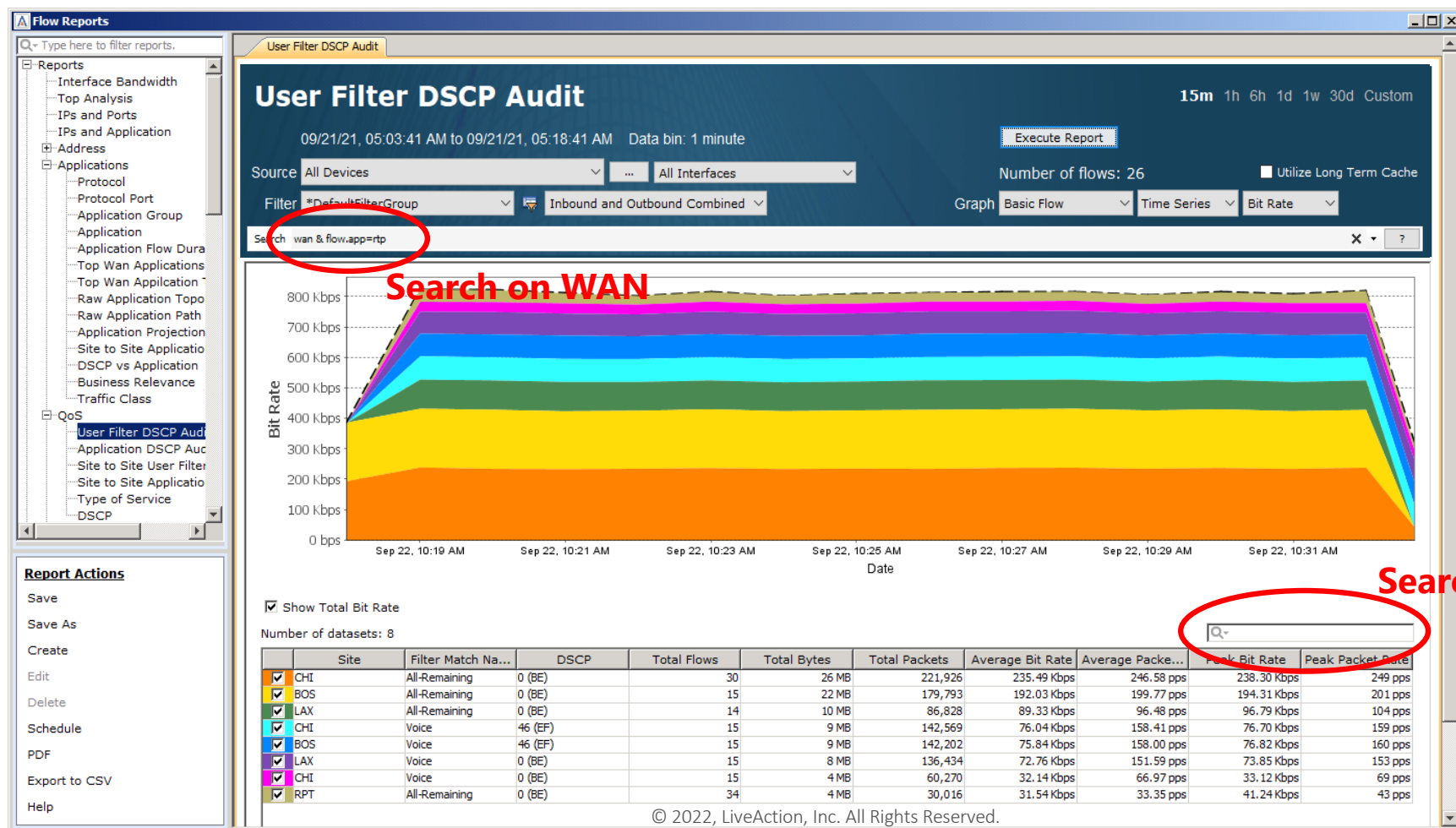
Look for BE traffic, Why is there any BE VoIP traffic? **LiveAction®**

# Marking: DSCP Report

Is there any BE VoIP traffic?

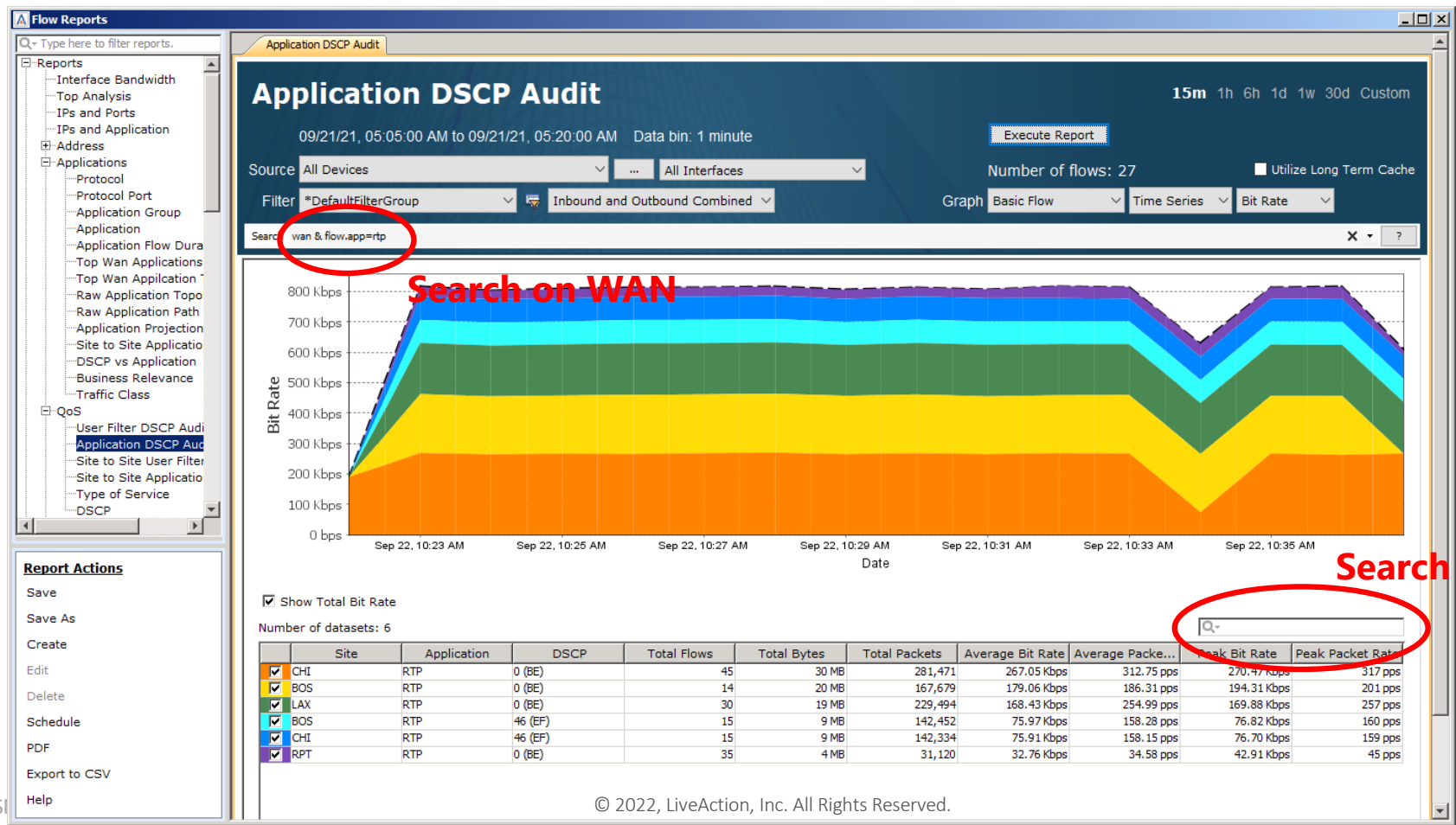


# Marking: User Filter DSCP Audit Where is the BE VoIP traffic?



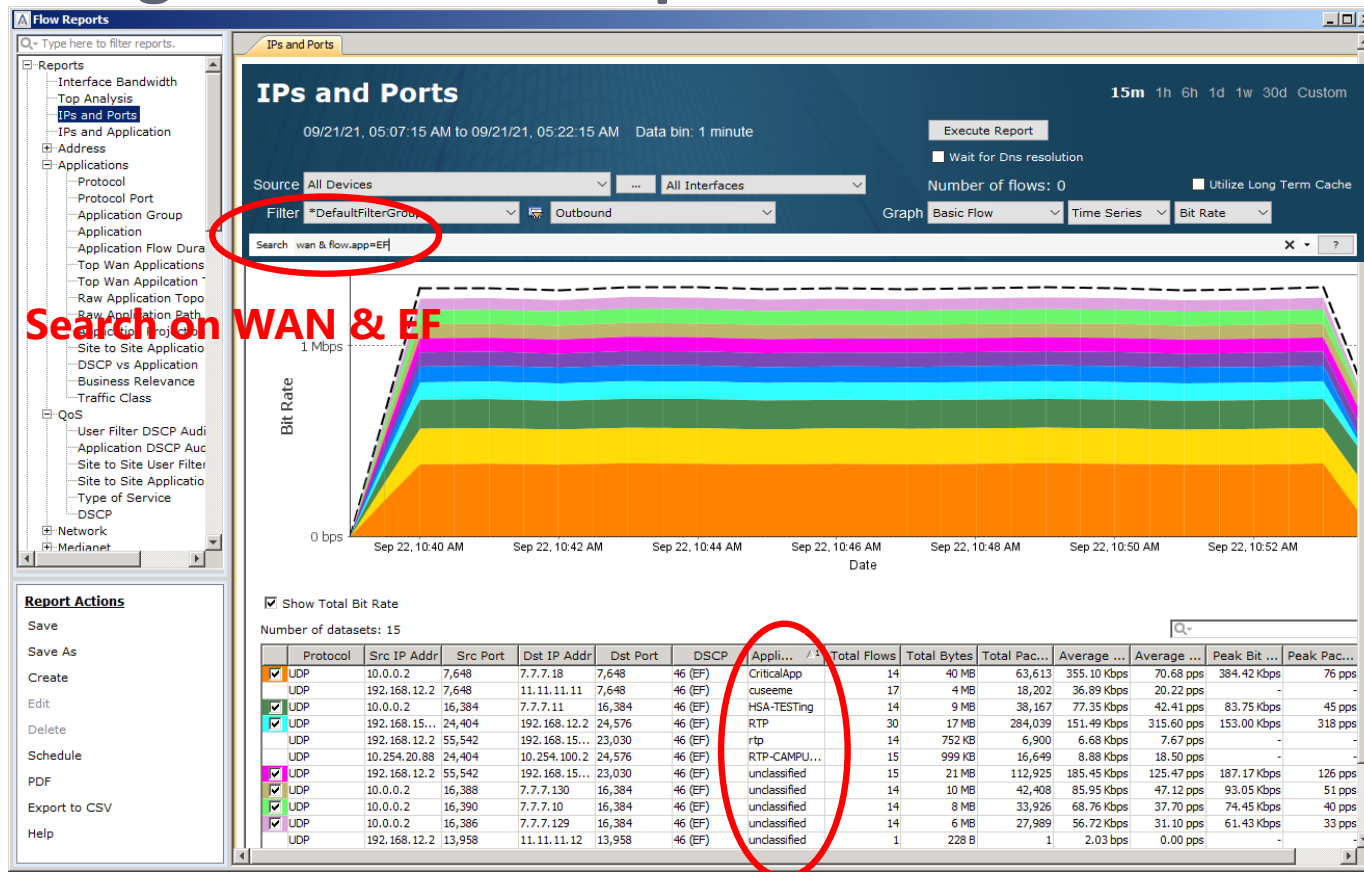
# Marking: Application DSCP Audit

Where is the BE VoIP traffic?





# Marking: IPs & Ports Report



Is there any Rogue EF traffic?

LiveAction®



# Marking: How to Mark

**Manage QoS Settings - c2921-ES-13.test.com (10.0.50.13)**

Policies | Classes | Interfaces

**Mapping Classes**

Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●	DSCP: EF							
VOIP_SIGNALING	●	DSCP: CS3							
HIGH_DATA_QUEUE	●	DSCP: CS2							
MEDIUM_DATA_QUEUE	●	DSCP: AF21							
VIDEO	●	DSCP: AF41							
class-default	●								

**Mapping Class Detail**

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Match on: Any

Match not : Unknown : match ip rtp 16384 16383  
 Match : DSCP : 46 (EF)  
 Match : Protocol - using NBAR : cuseeme

**Reference**

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

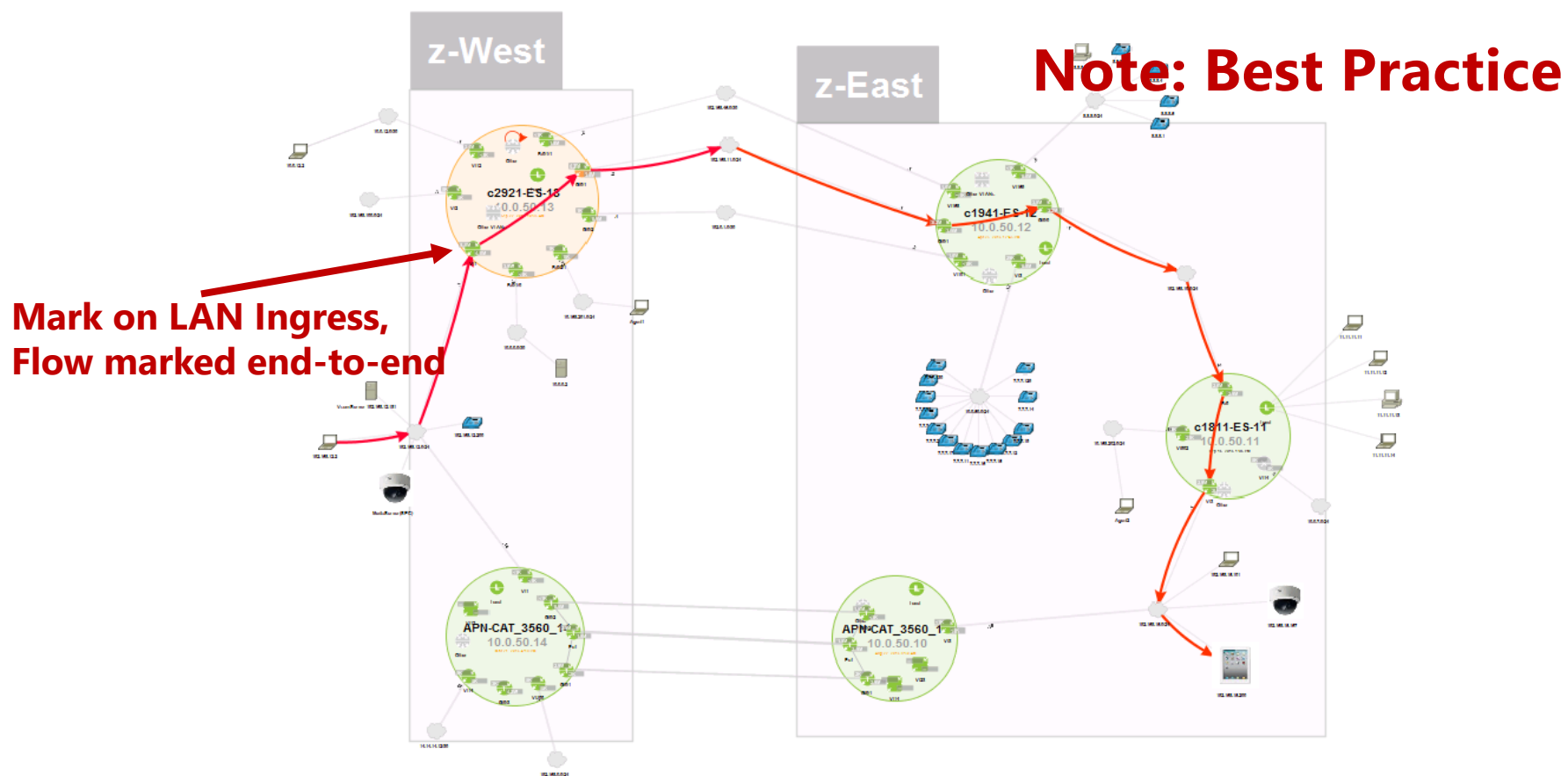
**Match-all:** packet must meet all criteria to be a member of the class.

Help | Save to Device | Preview CLI | Close

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

LiveAction®

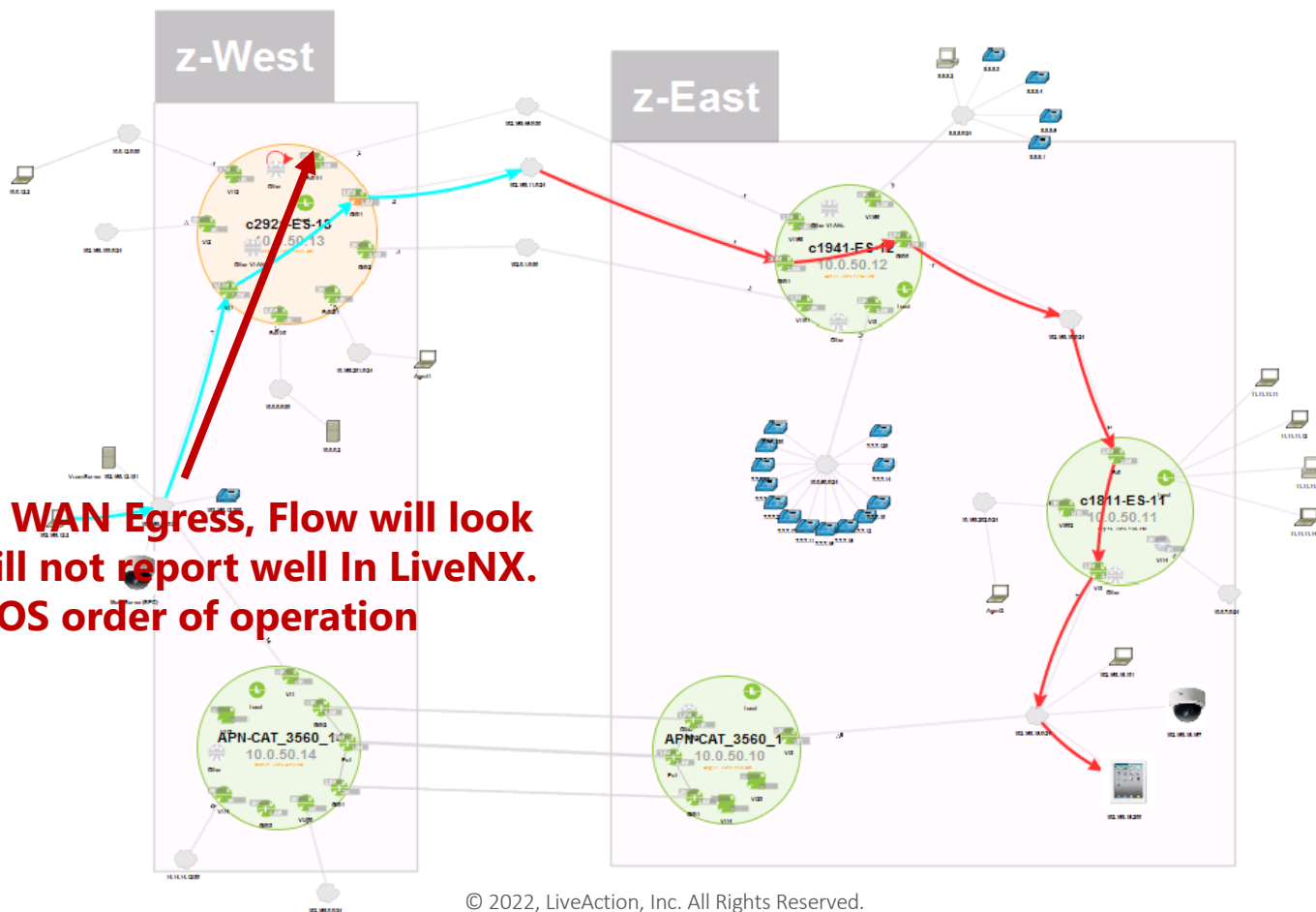
# Classify: Where to Mark



## Classify: Where to Mark

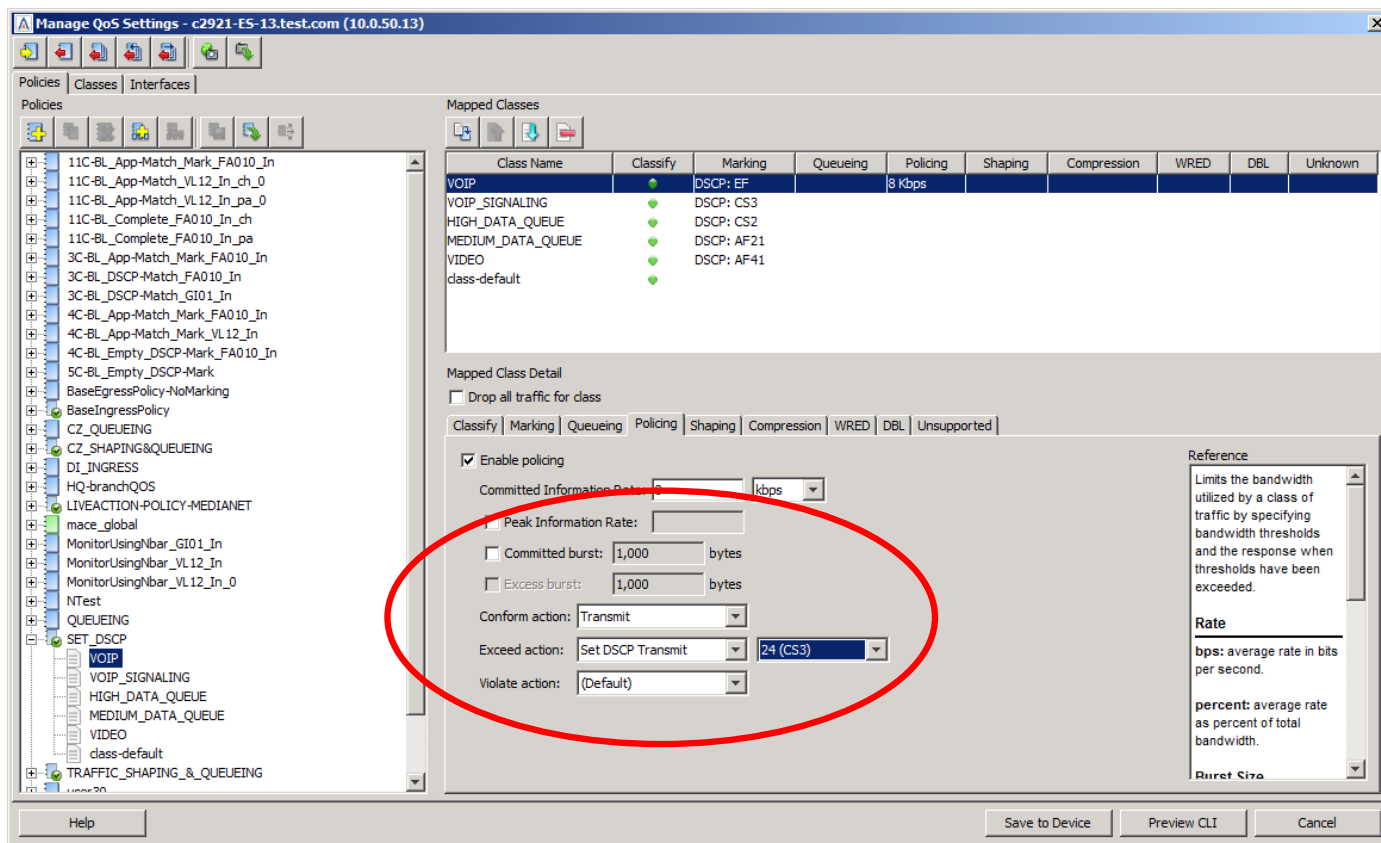
**Note: Try not to do this!**

**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

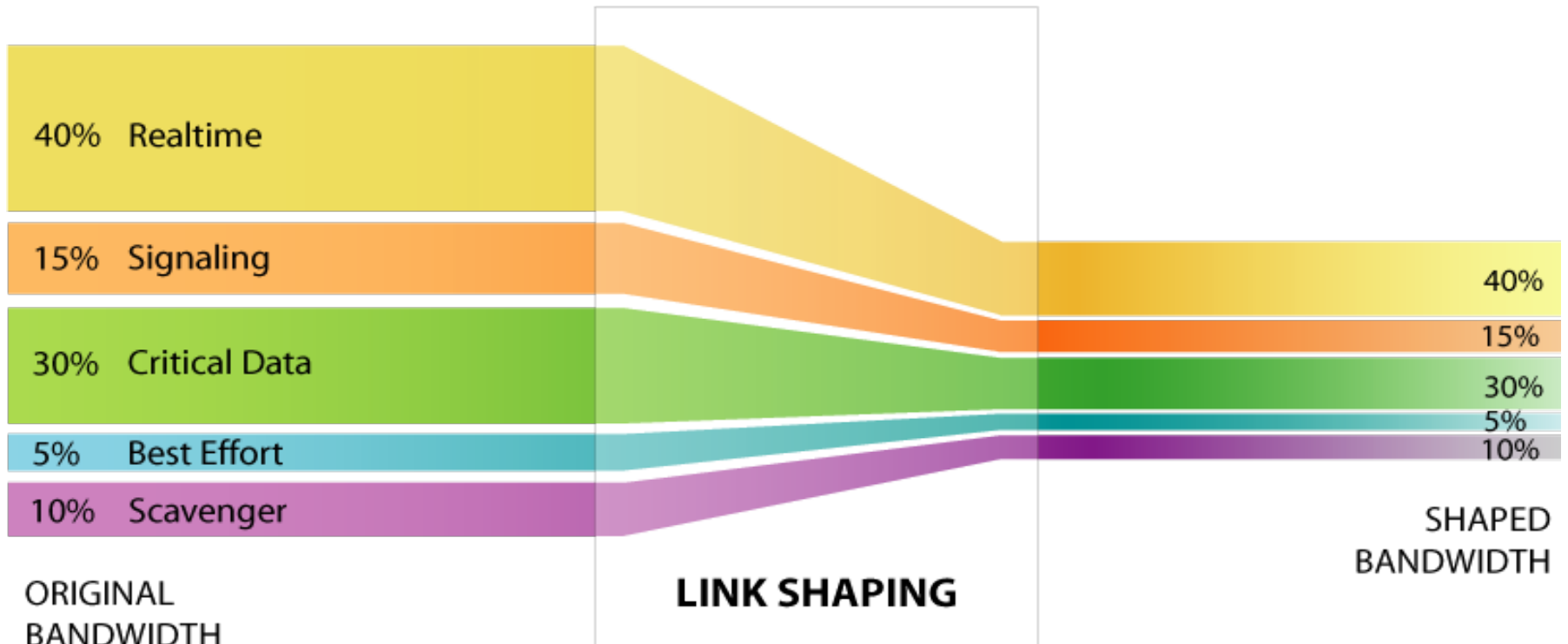
- Run Reports
- Recognize application traffic
- Mark
- Validate DSCP values



## Step 2: Queueing & Shaping



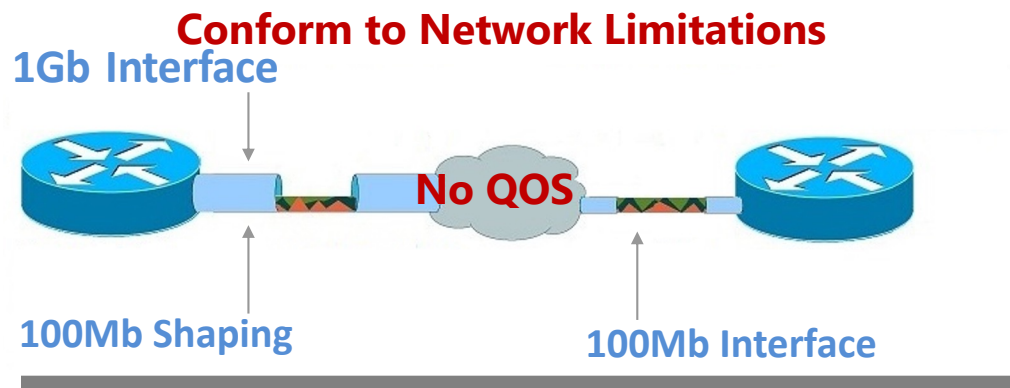
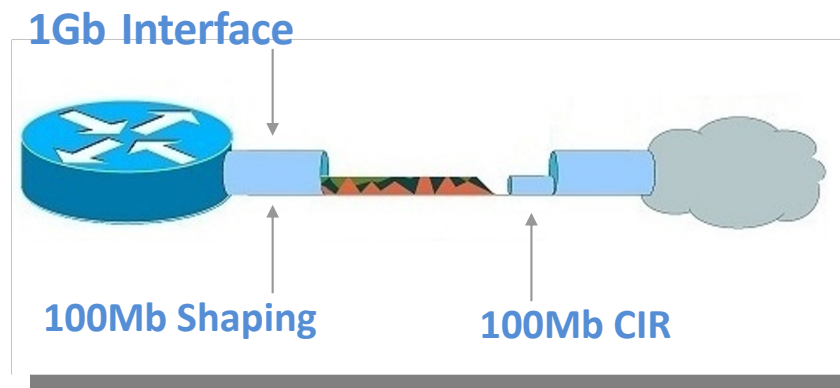
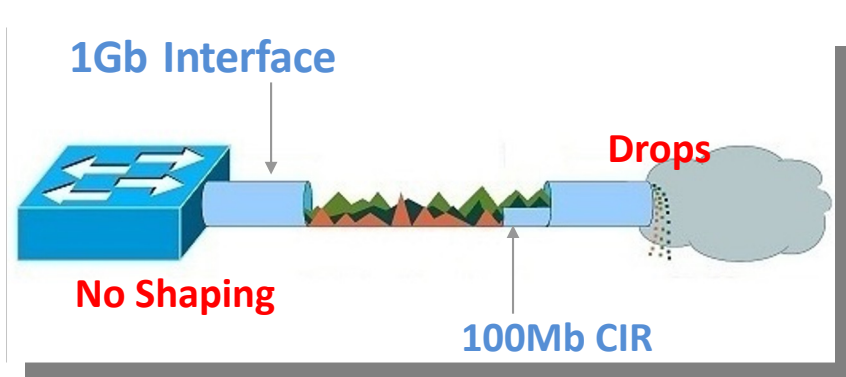
## Shaping: Throttle Traffic via software & Queue



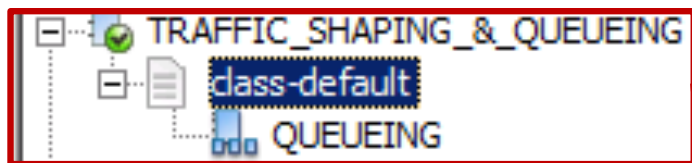


# Shaping: Throttle Traffic via software & Queue

**Conform to Provider's CIR**



# 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

The screenshot shows two configuration windows. The top window, 'Mapped Classes', contains a table with the following data:

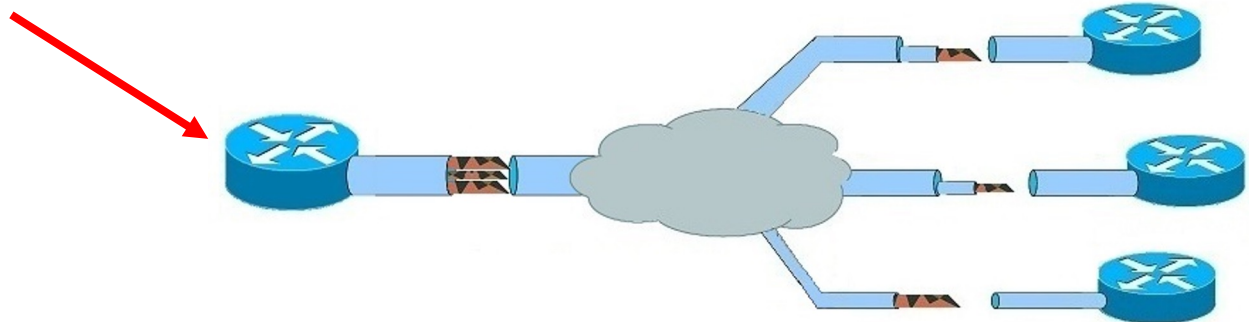
Class Name	Classify	Marking	Queueing	Policing	Shaping
class-default					1,544 Kbps

The bottom window, 'Mapped Class Detail', shows the configuration for the 'class-default' class. The 'Shaping' tab is selected. The 'Shape using' dropdown is set to 'Average'. The 'Rate' is set to '1,544' Kbps. The 'Committed burst' is checked and set to '15440' bits. The 'Excess burst' is checked and set to '0' bits. A red circle highlights the 'Shaping' configuration section, and a red arrow points from the text 'Best Practice is to set CIR, BC, & BE:' to it.

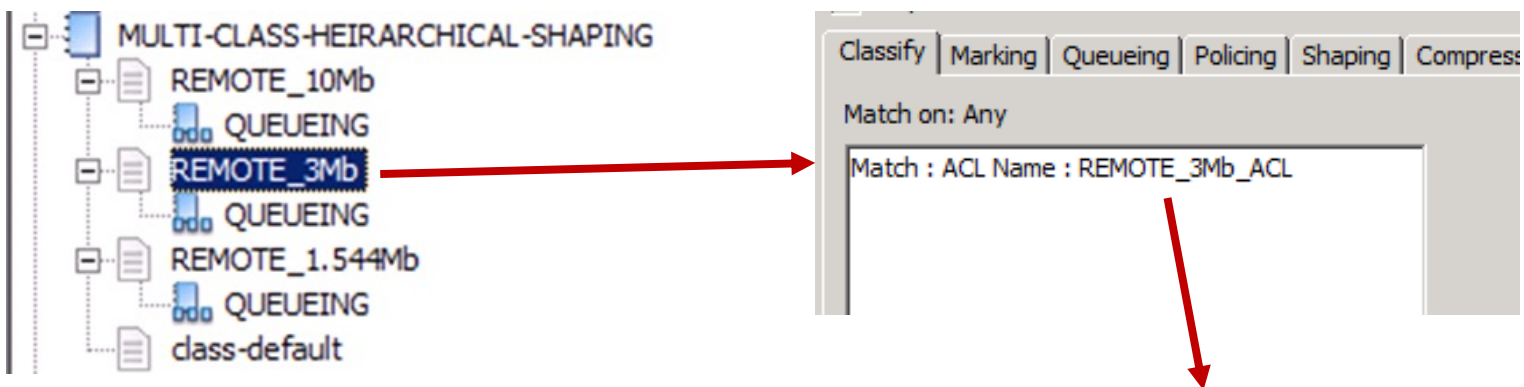
## Shaping: Configuration



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

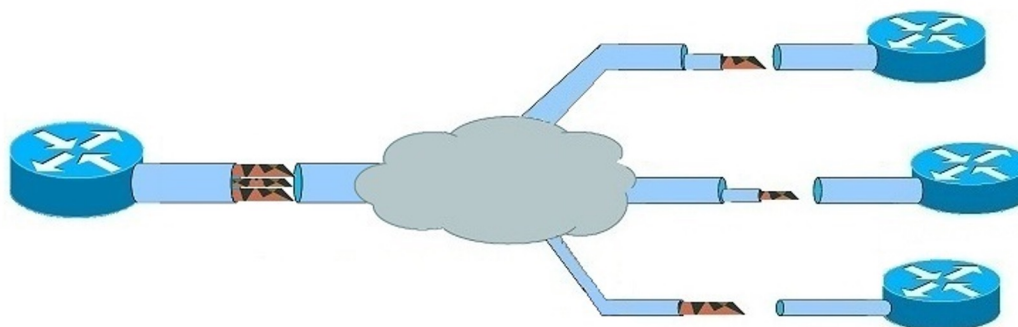


# Shaping: Configuration



## Access Rule Entries

permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255



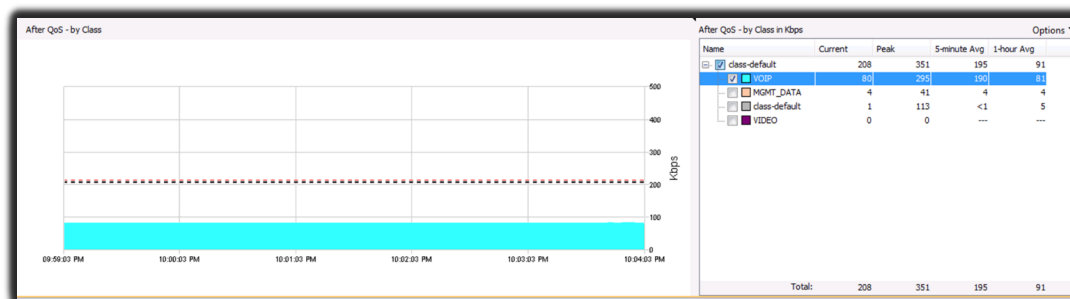
# Queueing: Selecting Bandwidth Allocations

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	≤5%	1%	1%
Best Effort		<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:



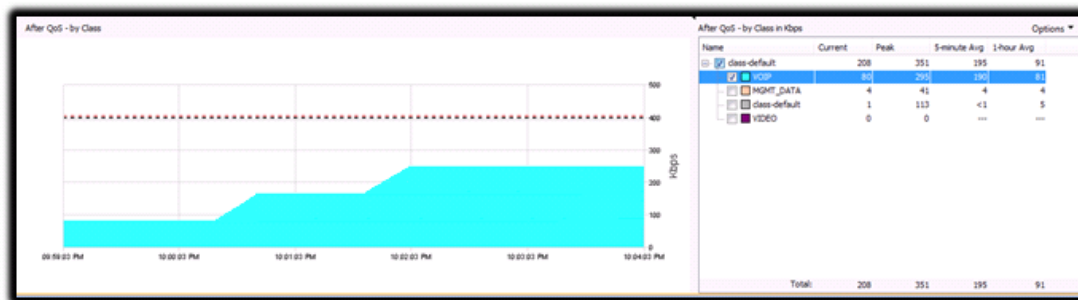
1x G.711 Call is ~82 Kbps

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

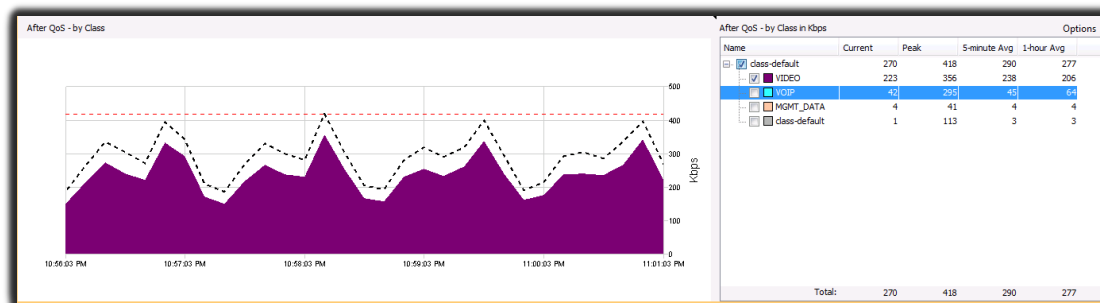
3x G.711 Call is ~246 Kbps

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!**

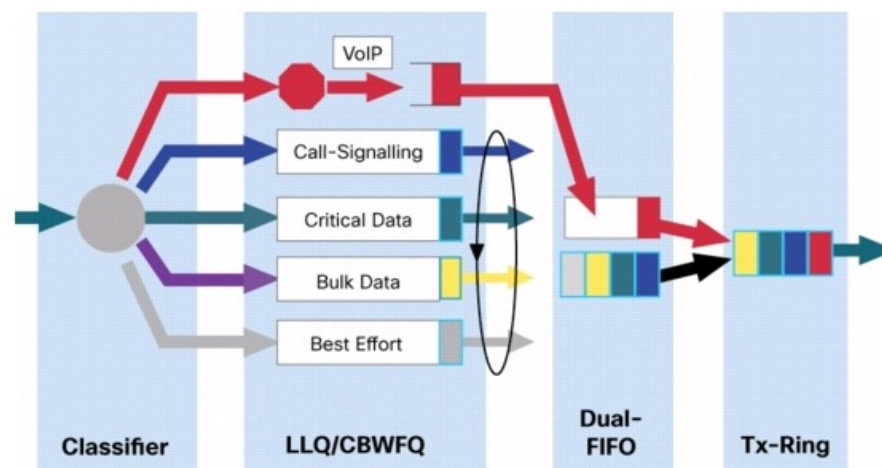
Parameter	VOIP	Traditional Video	HD / Immersive Video
Bandwidth	8-90Kbps	384 -768 kbps + network overhead	1.5 - 12.6 Mbps + network overhead
Latency	150ms	400-450ms	150ms
Jitter	30ms	30-50ms	10ms
Loss	1%	1%	0.05%

**Treat with Care!**

# Queueing: Understanding Traffic

Voice = LLQ /Priority Queue

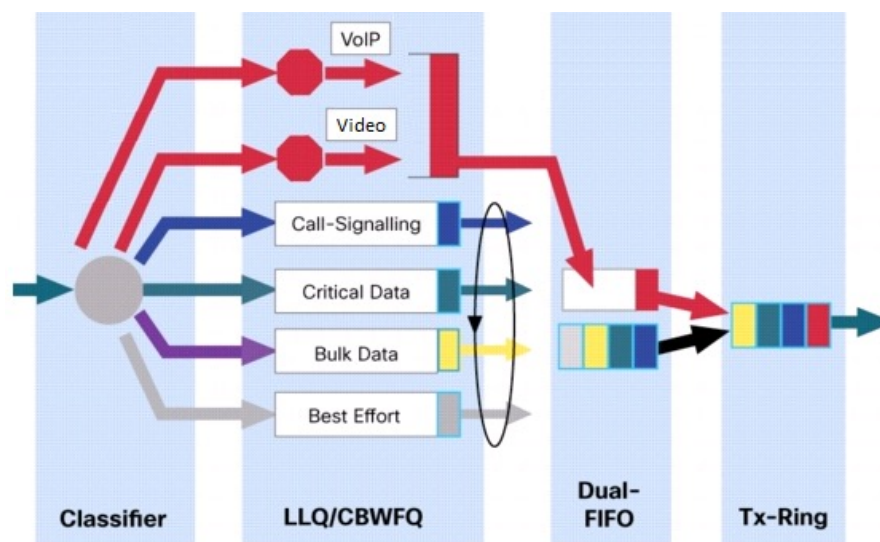
Video = ?



# Queueing: Understanding Traffic

Voice = Priority Queue/LLQ

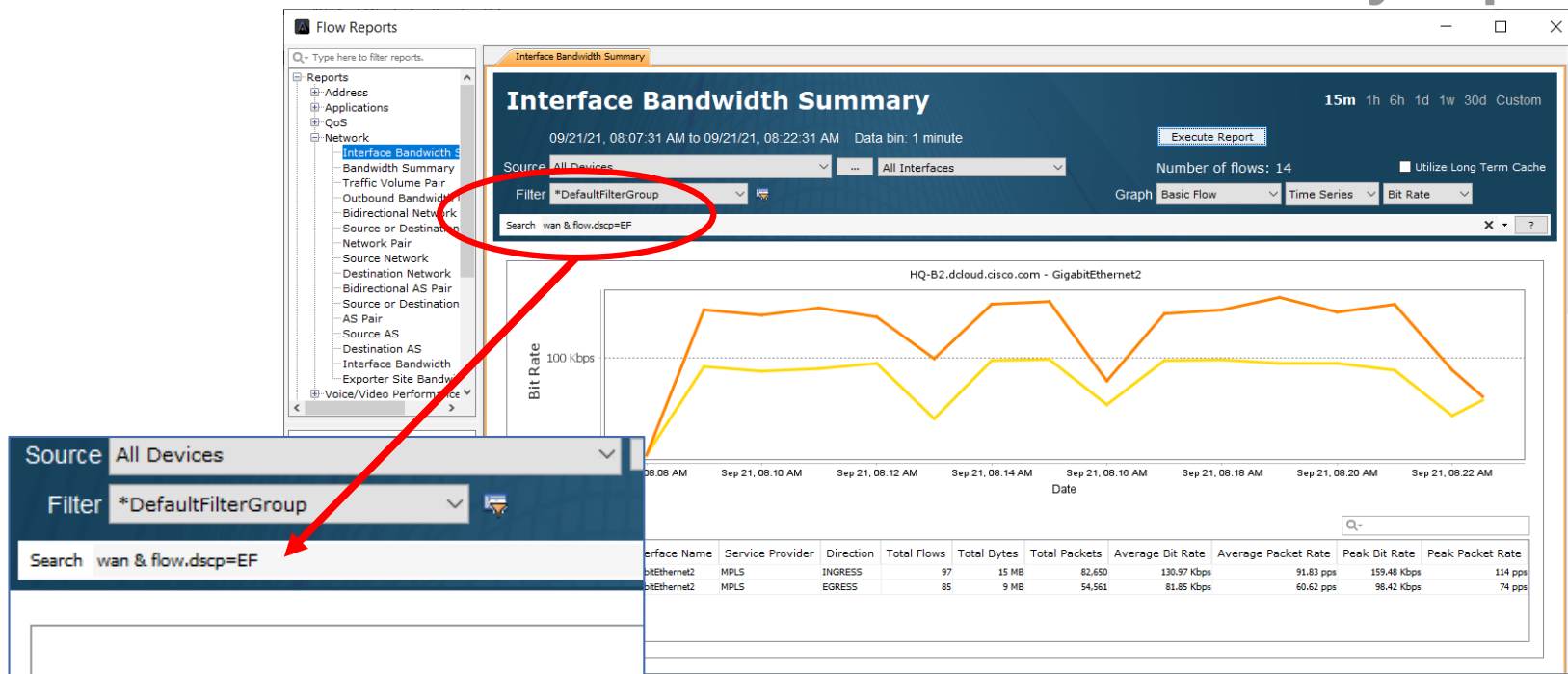
Video = Priority Queue/LLQ



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

# Queueing: Sizing/Capacity Planning

## Network > Interface Bandwidth Summary Report

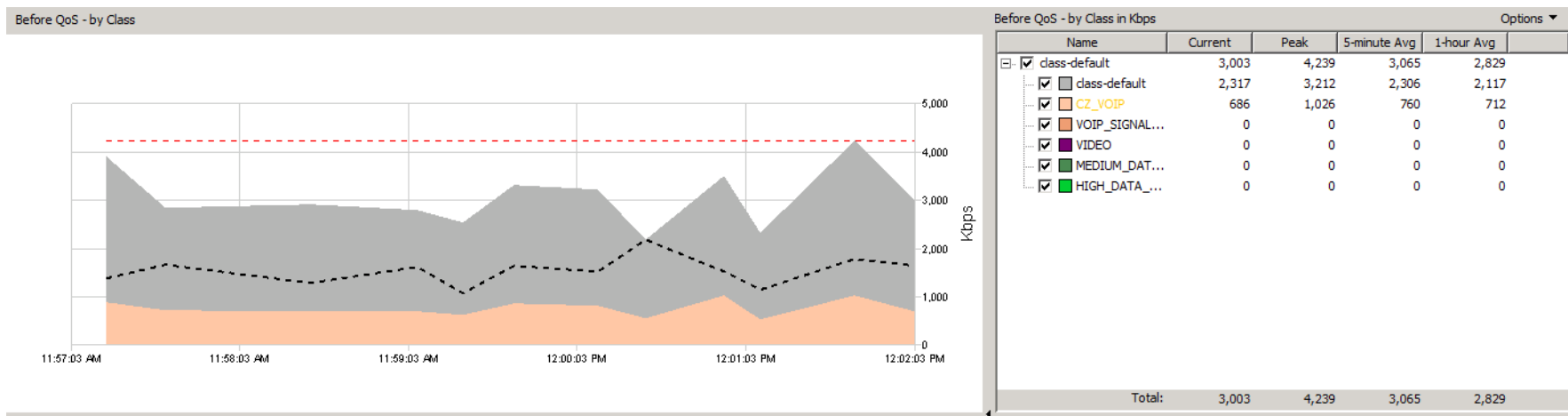


**If Classification & Marking are in place, Flow is a great way to do queue sizing**

LiveAction®

# Queueing: Sizing/Capacity Planning

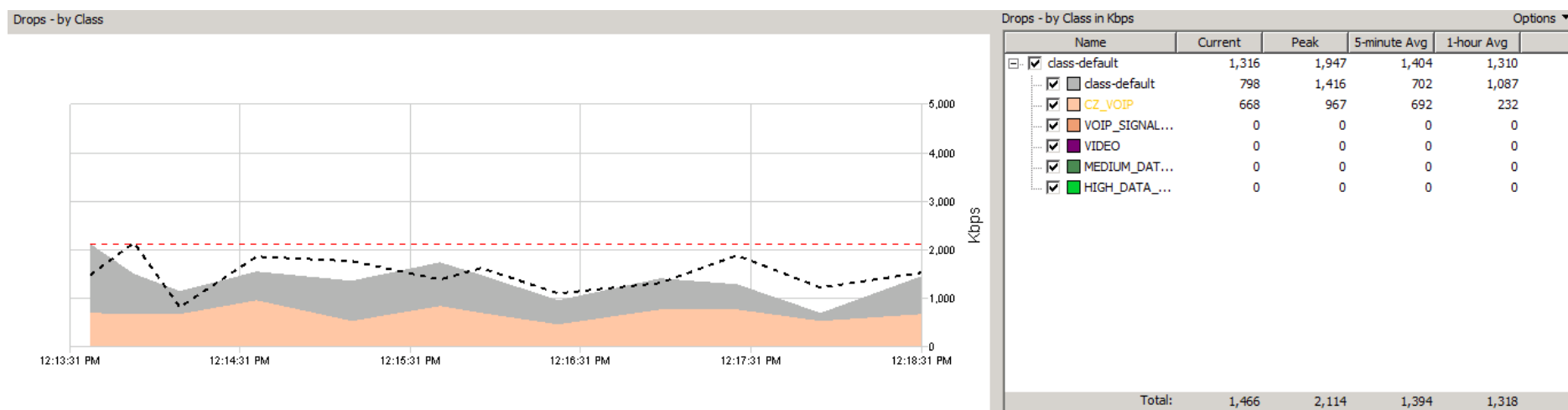
## Pre-Policy QoS Report is a Great QoS Sizing Report



**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

**Mapped Classes**

Class Name	Classify	Marking	Queueing	Policing
VOICE	●		Priority: 768 Kbps	
VOIP_SIGNALING	●		Class-based: 60 Kbps	
HIGH_DATA_QUEUE	●		Class-based: 50 Kbps	
MEDIUM_DATA_QUEUE	●		Class-based: 75 Kbps	
VIDEO	●		Class-based: 50 Kbps	
class-default	●		Fair	

**Mapped Class Detail**

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Match on: Any

- Match : DSCP : 46 (EF)

Edit

# 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.

Class Name	Classify	Marking	Queueing	Policing	Shaping
VOICE	●		Class-based: 756 Kbps		
VOIP_SIGNALING	●		Class-based: 60 Kbps		
HIGH_DATA_QUEUE	●		Class-based: 50 Kbps		
MEDIUM_DATA_QUEUE	●		Class-based: 75 Kbps		
VIDEO	●		Class-based: 50 Kbps		
class-default	●		Fair		

**Mapped Class Detail**

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

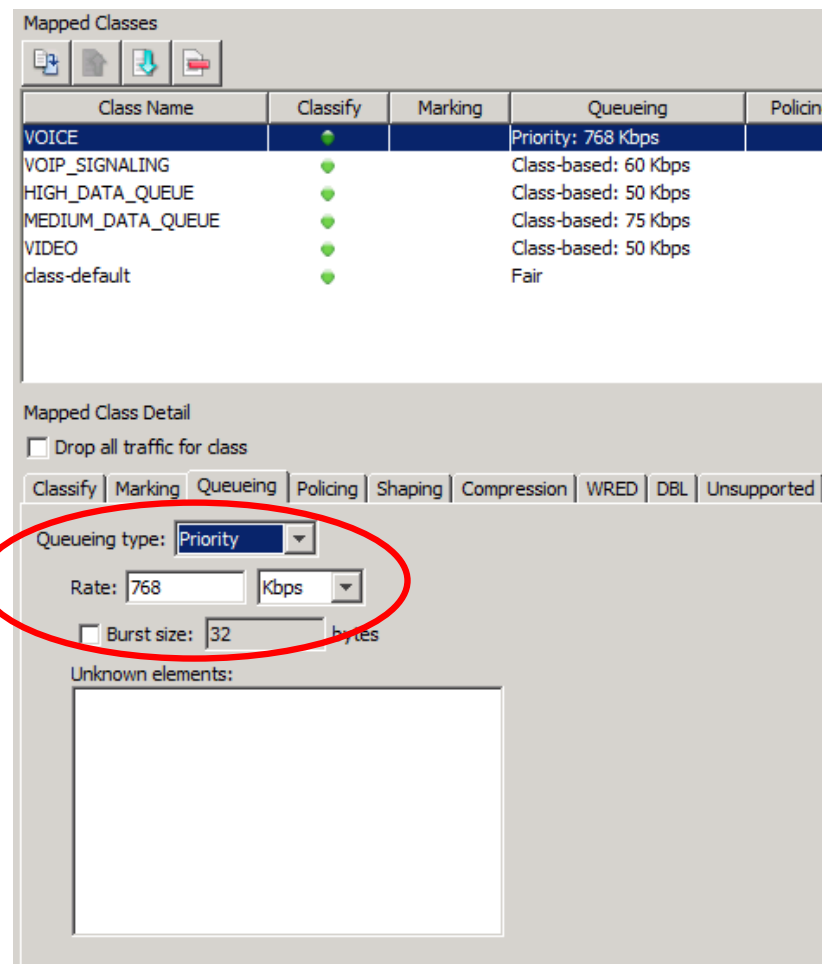
Match on: Any

Match : DSCP : 46 (EF)

Edit



# Queueing: Configuration



Class Name	Classify	Marking	Queueing	Policing
VOICE	●		Priority: 768 Kbps	
VOIP_SIGNALING	●		Class-based: 60 Kbps	
HIGH_DATA_QUEUE	●		Class-based: 50 Kbps	
MEDIUM_DATA_QUEUE	●		Class-based: 75 Kbps	
VIDEO	●		Class-based: 50 Kbps	
class-default	●		Fair	

**Mapped Class Detail**

☐ Drop all traffic for class

Classify | Marking | **Queueing** | Policing | Shaping | Compression | WRED | DBL | Unsupported

Queueing type: **Priority** ▼

Rate: 768 Kbps ▼

☐ Burst size: 32 bytes

Unknown elements:

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

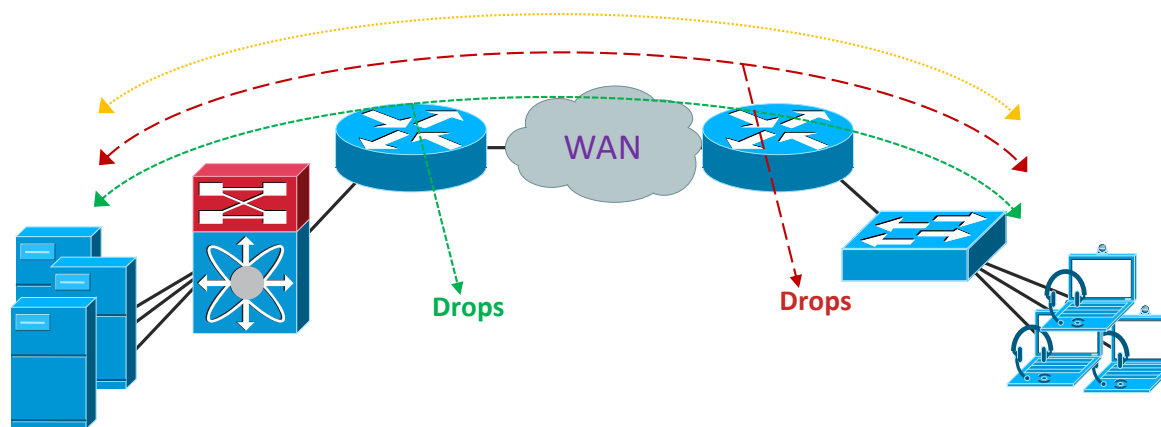




## Step 3: Throttle Traffic

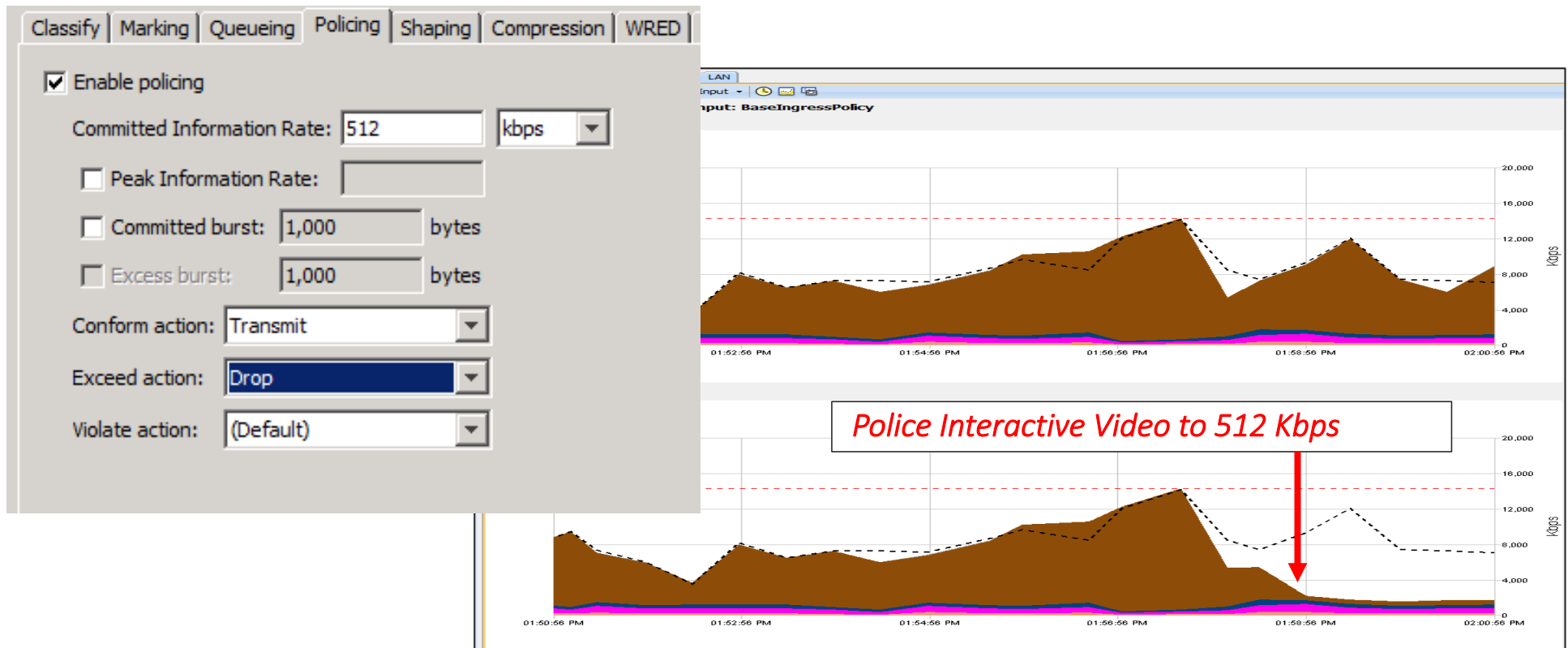
Policing & WRED

### Step 3 –Throttle Traffic (Policing and WRED)



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

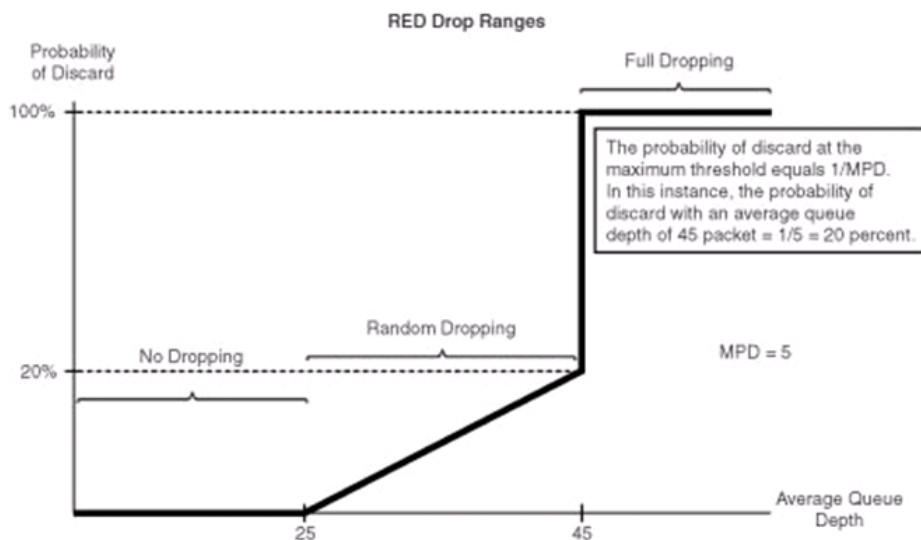
# Policing



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



INXOF.ISIVI.Z.U.3

Mapped Class Detail

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Calculate drop probability using: DSCP

☐ Explicit congestion notification

☐ Exponential weighted constant: 1

☒ Override default settings

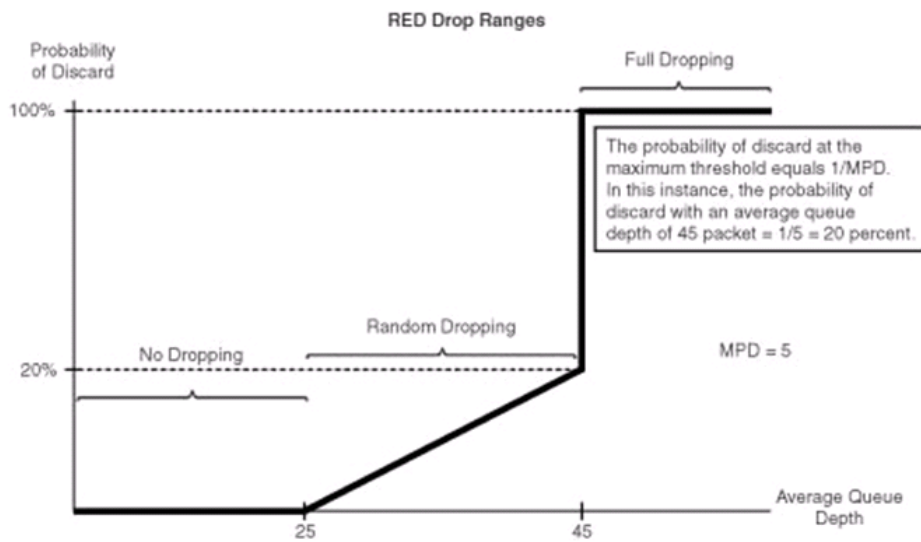
Value	Min Threshold	Max Threshold	Mark Probability Denominator
10 (AF11)	128	256	1
12 (AF12)	100	196	1
14 (AF13)	96	64	1

LiveAction®

© 2022, LiveAction, Inc. All Rights Reserved.

## WRED - Warning!

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



Mapped Class Detail

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Calculate drop probability using: DSCP

☐ Explicit congestion notification

☐ Exponential weighted constant: 1

☒ Override default settings

Value	Min Threshold	Max Threshold	Mark Probability Denominator
10 (AF11)	128	256	1
12 (AF12)	100	196	1
14 (AF13)	96	64	1




## Lab: 5 Throttling & Policing

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

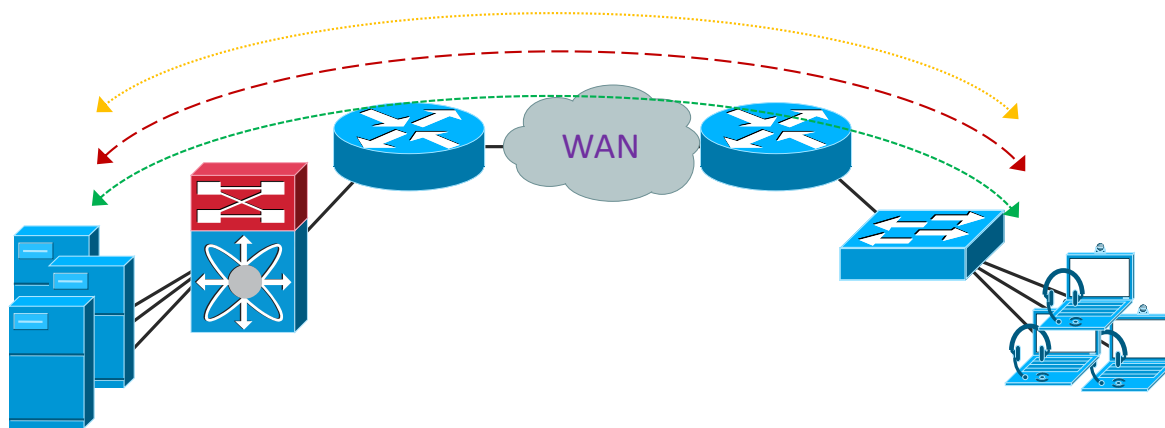




A man in a dark suit and light-colored shirt is standing on a stage, holding a microphone and gesturing with his right hand towards a large screen. The screen displays a complex network diagram with various shapes like circles, hexagons, and rectangles connected by lines. The audience, seen from behind, is seated in rows, facing the speaker. The overall scene is brightly lit with a blue and white color scheme.

## Step 4: Buffer Tuning

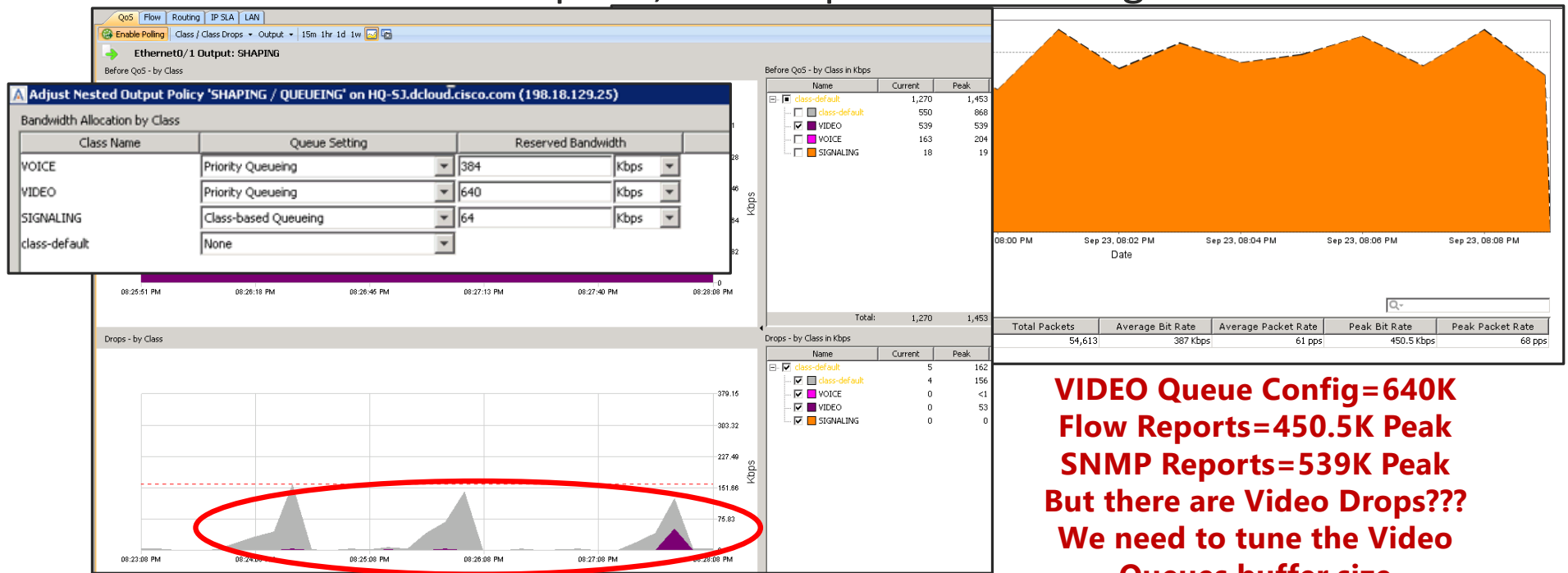
#### Step 4–Buffer Tuning (Advanced)



- **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...



## 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
```

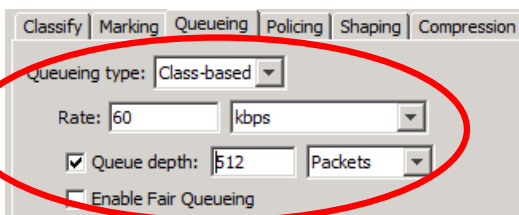
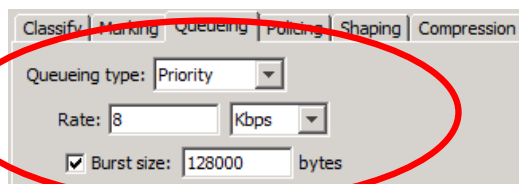
```
priority 8 128000
```

```
exit
```

```
class VOIP_SIGNALING
```

```
bandwidth 60
```

```
queue-limit 512
```



# Lab: 6 Buffer Tuning

- Buffer Tuning
  - Video Queue Performance Tuning







# QoS Deployment Strategies

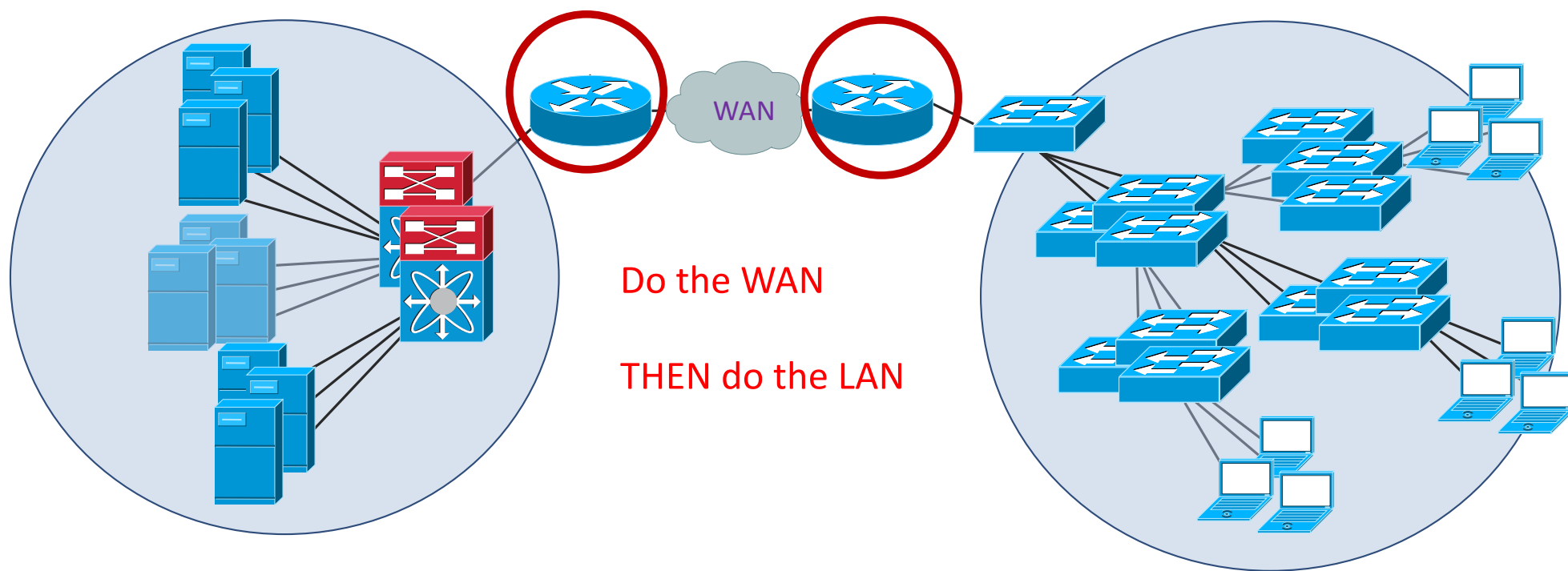
REVIEW

---

## QoS Deployment Strategies

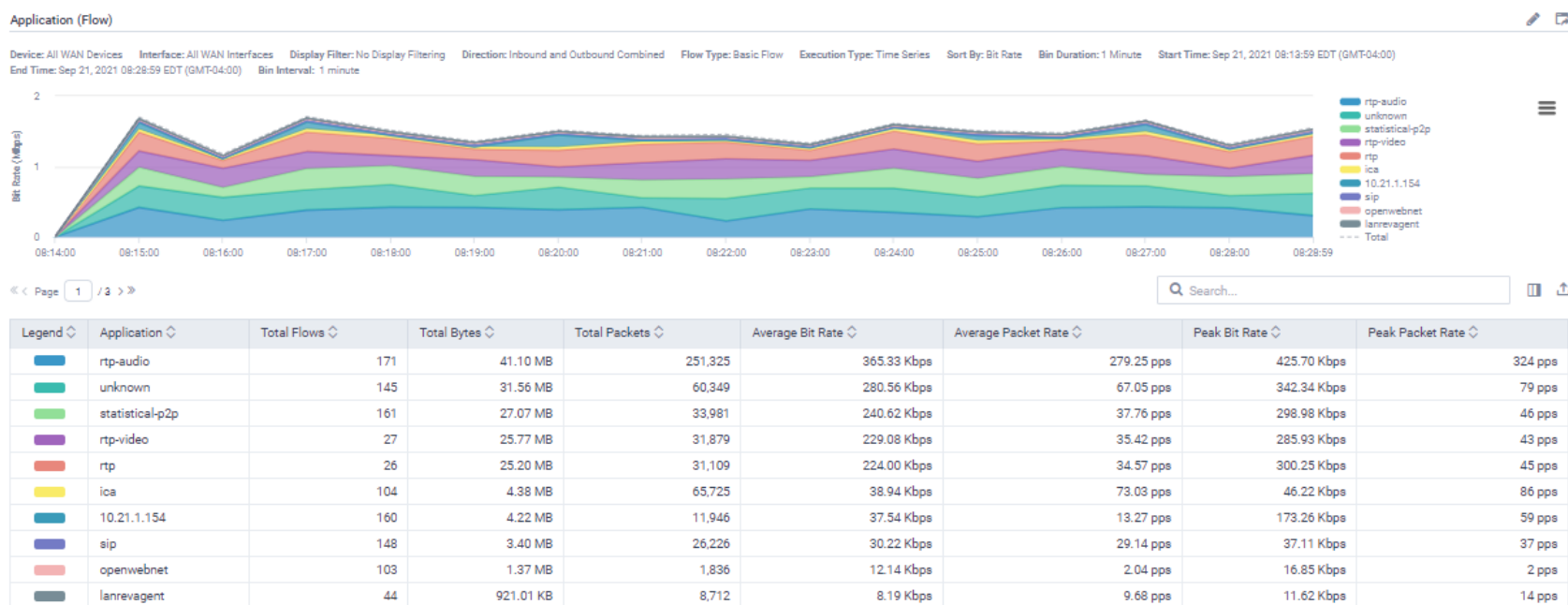
- Step 1 - Deploy QoS in Phases**
- Step 2 - Use NetFlow Tools to Understand Bandwidth Usage**
- Step 3 - Understand Application Details**
- Step 4 - Get Business' Buy-In**
- Step 5 - Understand the Network**
- Step 6 - Have a Plan**
- Step 7 - Use QoS Management Tools**
- Step 8 - K.I.S.S.**

## Step 1 : Implement QoS in Phases!





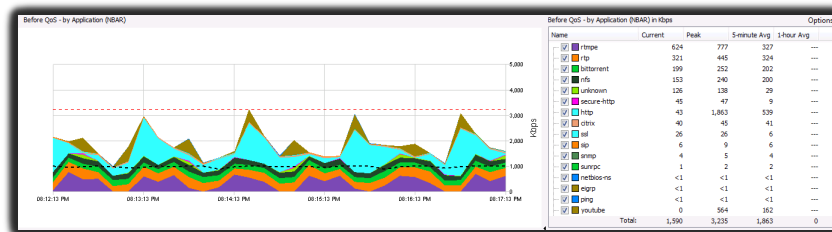
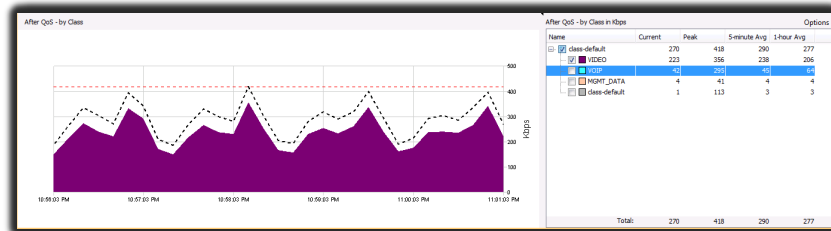
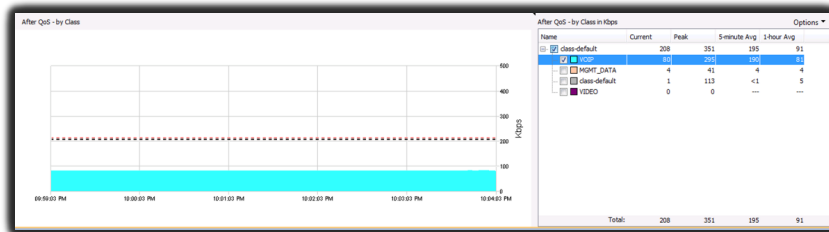
## Step 2 - Use NetFlow Tools to Understand Bandwidth Usage



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

**LiveAction®**

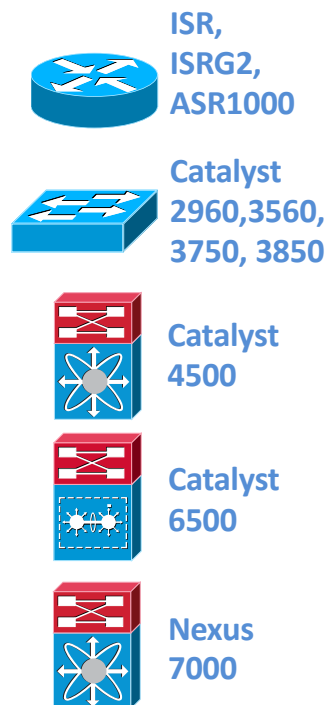
### Step 3 - Understand Applications Details



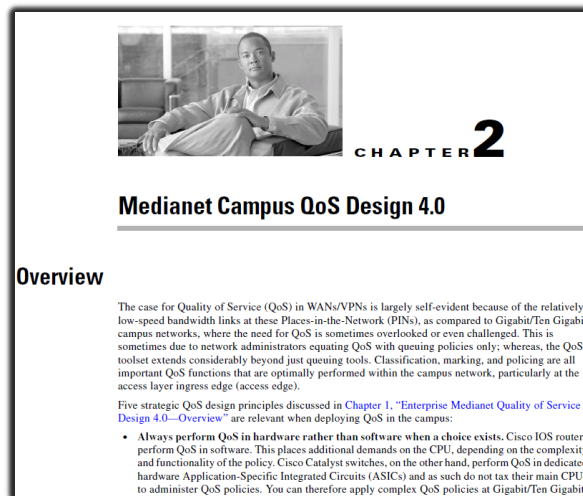
#### Step 4 - Get Business' Buy-In



## Step 5 - Understand the Network



[www.cisco.com/go/srnd](http://www.cisco.com/go/srnd)

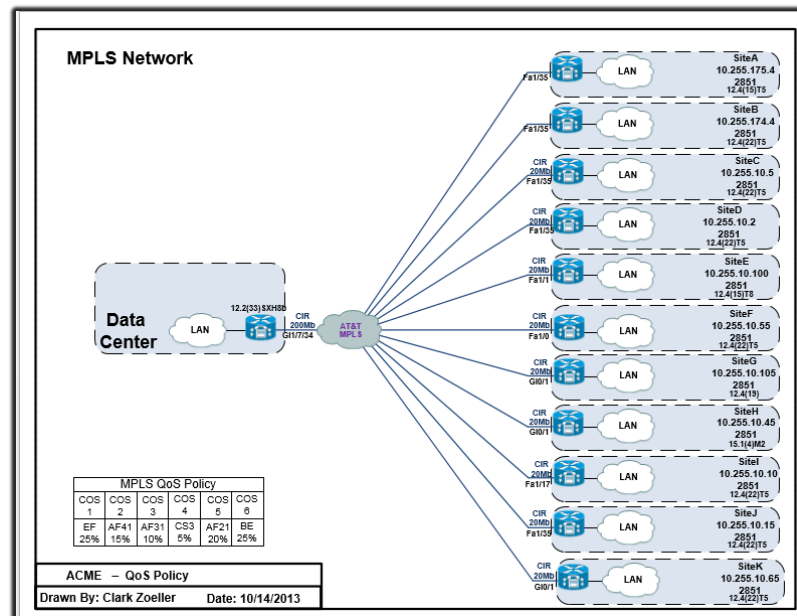


**With switches, start with SRND4 Auto-QoS where possible**

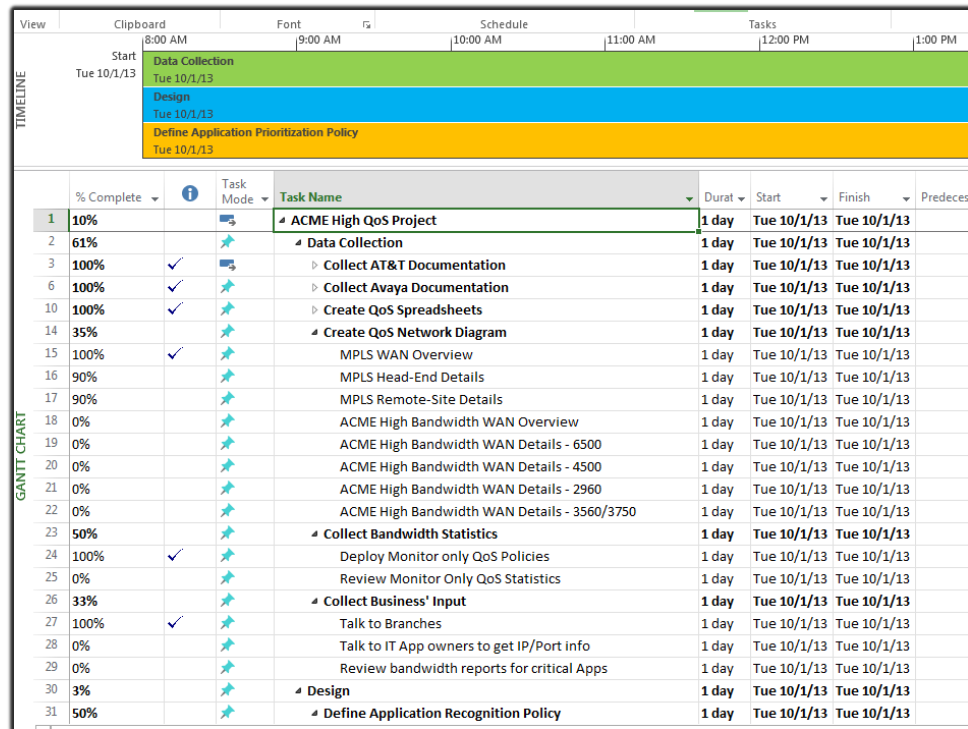
## Step 6 - Have a plan

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		

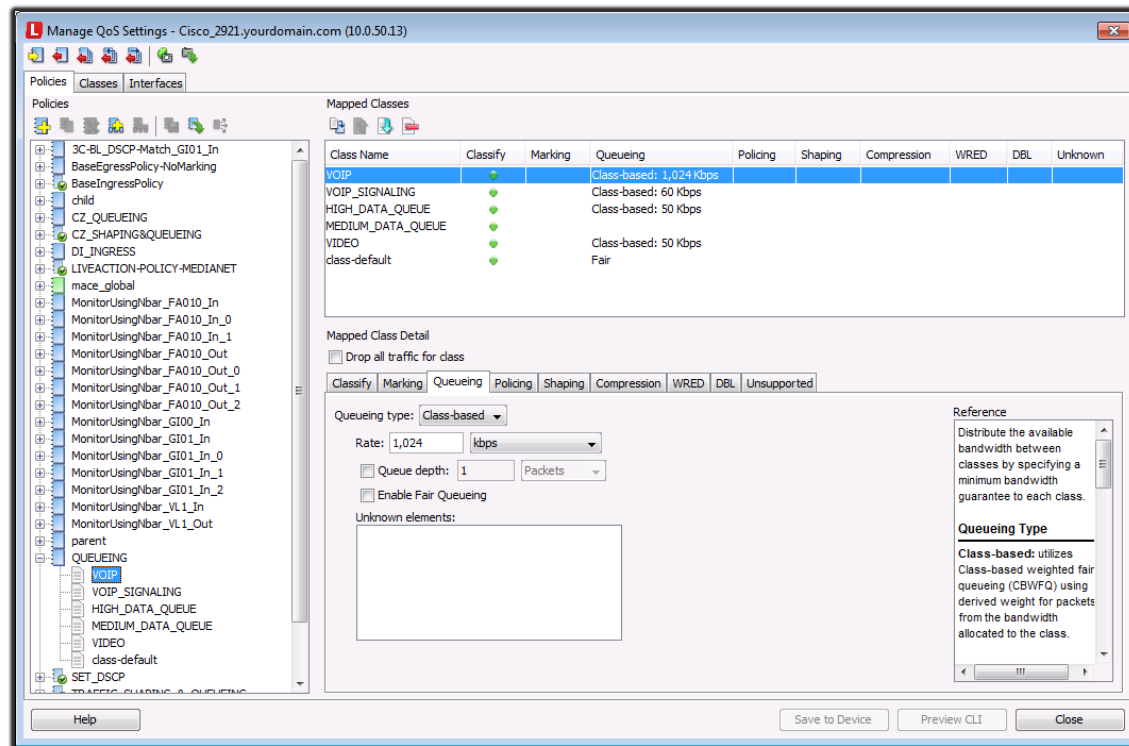
## Step 6 - Have a plan



## Step 6 - Have a plan

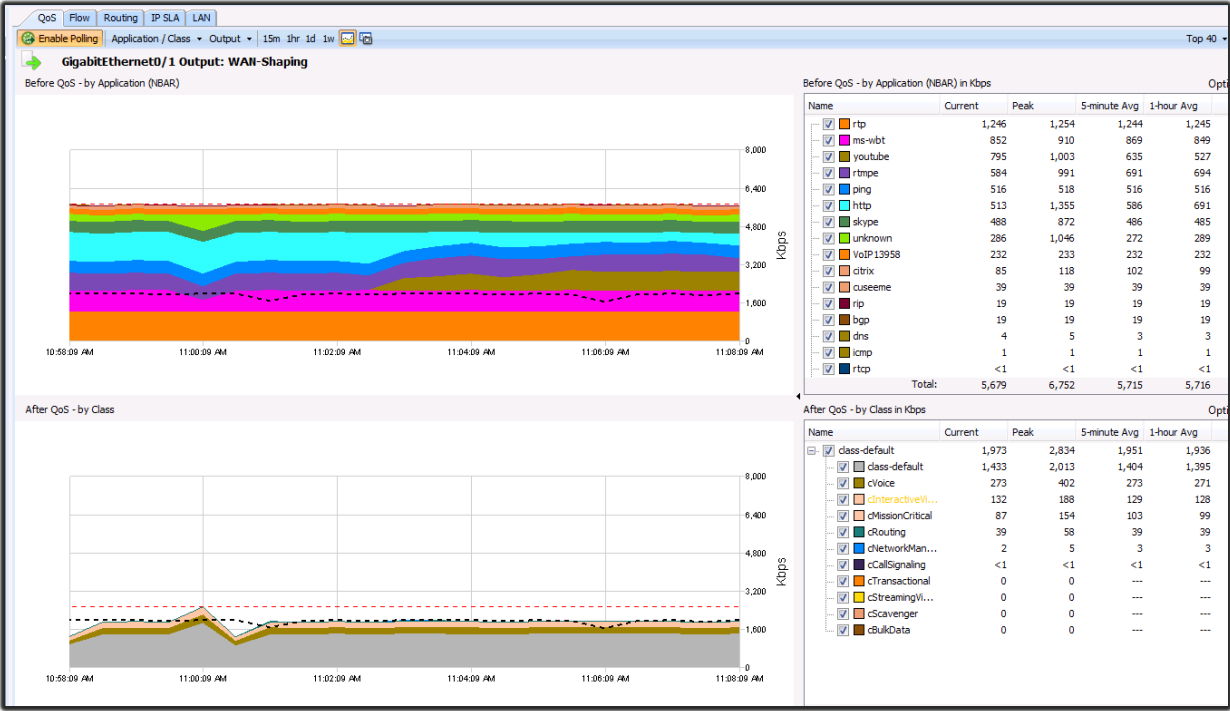


## Step 7 - Use QoS management Tools





# Step 7 - Use QoS management Tools



## Step 7 - Use QoS management Tools

<div> Resolve Ignore Acknowledge Refresh Alerts </div> <div> Q qos </div>							
	SEVERITY	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	THIRD PARTY...
<input type="checkbox"/>	All	Description			All	All	Third Party...
<input type="checkbox"/>	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...	
<input type="checkbox"/>	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...	
<input type="checkbox"/>	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...	
<input type="checkbox"/>	Critical	RTR_Louisville QoS Class Default Drop Rate was 64.71 Kbps	29 Mar 2019, 02:30PM	2 minutes	Device, Interface	QoS Class D...	
<input type="checkbox"/>	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...	
<input type="checkbox"/>	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...	
<input type="checkbox"/>	Critical	RTR_Seattle QoS Class Default Drop Rate was 107.86 Kbps	29 Mar 2019, 12:19PM	2 hours	Device, Interface	QoS Class D...	
<input type="checkbox"/>	Critical	RTR_Madison QoS Class Default Drop Rate was 255.93 Kbps	29 Mar 2019, 12:28AM	14 hours	Device, Interface	QoS Class D...	
<input type="checkbox"/>	Warning	RTR_Louisville QoS Class VOICE Drop Rate was 73.79 Kbps	27 Mar 2019, 12:17PM	2 days	Device, Interface	QoS Class Dr...	
<input type="checkbox"/>	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...	
<input type="checkbox"/>	Warning	RTR_Madison QoS Class VOICE Drop Rate was 74.57 Kbps	25 Mar 2019, 10:00AM	4 days	Device, Interface	QoS Class Dr...	
<input type="checkbox"/>	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

The screenshot shows the 'Device Management' window. At the top, there's a 'Filter by:' field and 'Filter' and 'Clear' buttons. Below is a table with columns: Select, Device Name, IP Address, Vendor, Model, Node, Group, Poll, QoS, Flow, IP SLA, Routing, LAN\*, Interval, and Status. The table lists five devices: Branch1-LA, Branch2-NY, HQ-B1, HQ-B2, and HQ-MC. All devices are configured with a 30-second polling interval. Below the table, there are sections for 'Device Configurations' and 'Global Device Settings'. A red arrow points from the 'Global Device Settings' section to the 'Default SNMP Settings' row, which is circled in red. The 'Default SNMP Settings' row has an 'Edit' button and a 'Clear' button. The 'Default CLI Monitoring Settings' row has a 'Clear' button. The 'Default CLI Configuration Settings' row has a 'Clear' button. The 'Apply' and 'Close' buttons are at the bottom right.

Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval	Status
<input checked="" type="checkbox"/>	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local	LA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local	NY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured

\* LAN polling occurs every 15 minutes

Number of Devices: 5

Device Configurations

Configure QoS, Flow, and IP SLA  
Select devices in the table and click the configure button.

Remove selected device(s).

<New Group>

Removes selected devices from their groups

Edit the groups

Global Device Settings

Edit Default SNMP Settings

Edit Default CLI Monitoring Settings - Not Set

Edit Default CLI Configuration Settings

Apply Close

<input checked="" type="checkbox"/>	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local	LA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local	NY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured
<input type="checkbox"/>	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30 seconds	Configured

# Alerting – Customize Triggers

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

QoS Class Drop

ENABLED

On

SEVERITY

Warning

Note: Severity for this alert will be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status.

THRESHOLDS

QOS CLASS

VOICE

DROP RATE

> 20 kbps

FOR AT LEAST

> 0 min

QOS CLASS

VIDEO

DROP RATE

> 50 kbps

FOR AT LEAST

> 1 min

Add More

SHARING

Email

support@ 1

ServiceNow

SNMP trap

Web UI

Syslog

This alert may contribute to status of an Interface, Device, and/or Site.

Cancel

Save

## Lab 6: Finish The Labs

- Including Lab 7: QoS Alerts





# What's Next? SDWAN

Finish the Labs...

---

# 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



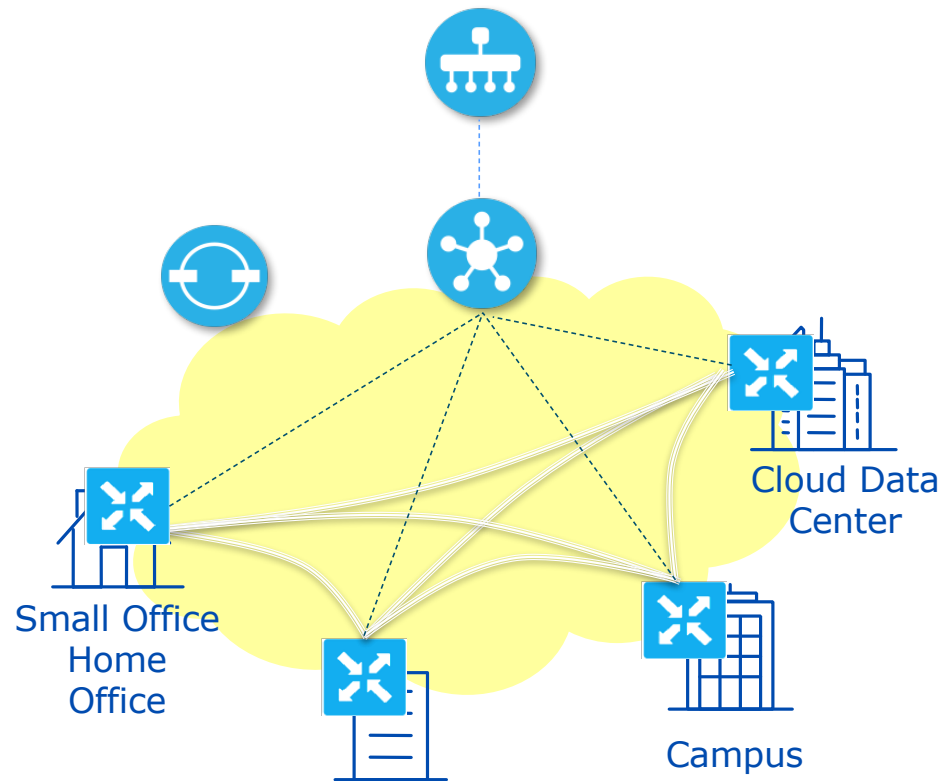


# LiveNX

Cisco/Viptela SDWAN Overview



# SDWAN Basics



vEdge – SDWAN Edge Router



vManage – SDWAN Manager



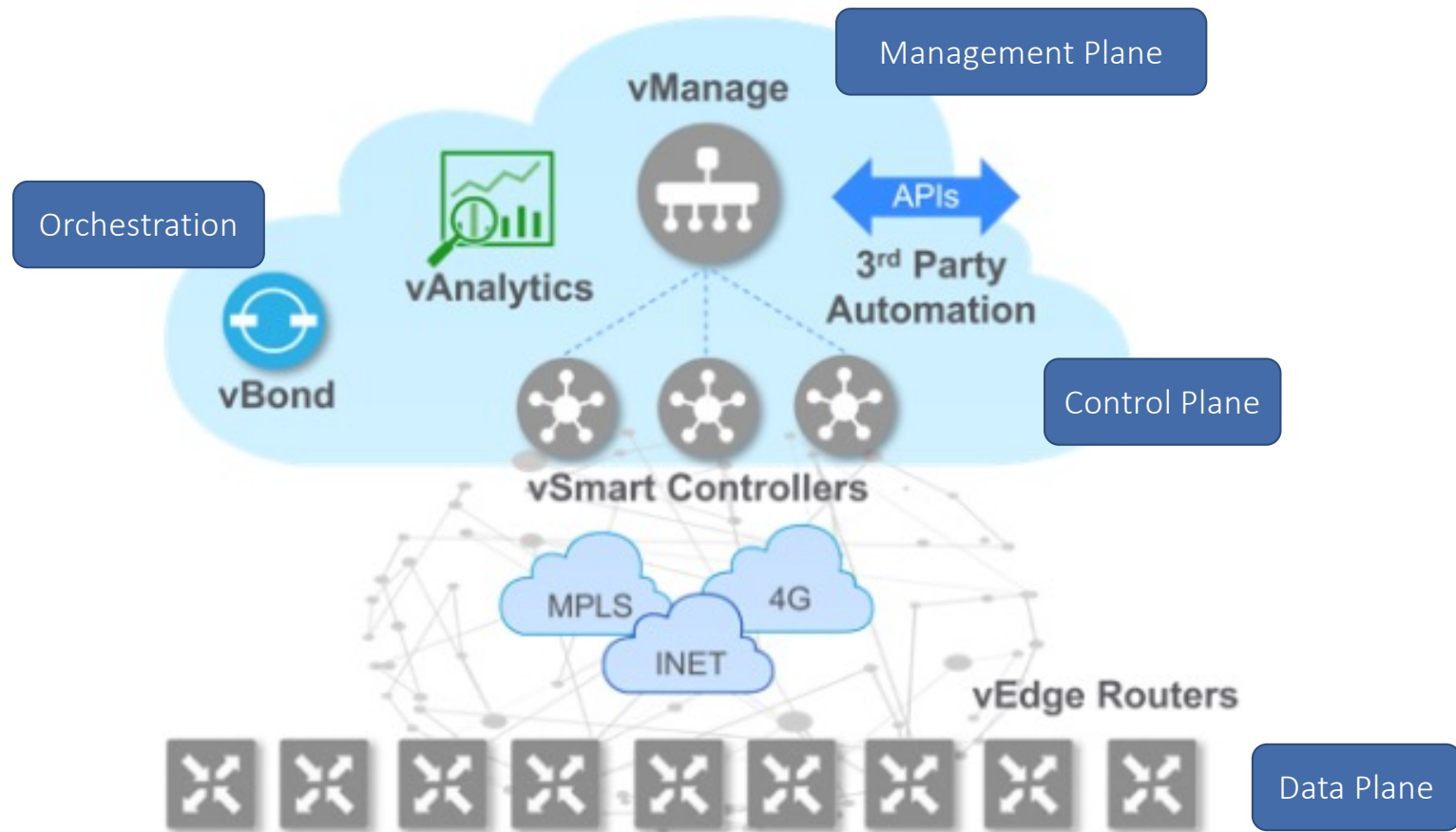
vBond – SDWAN Orchestrator



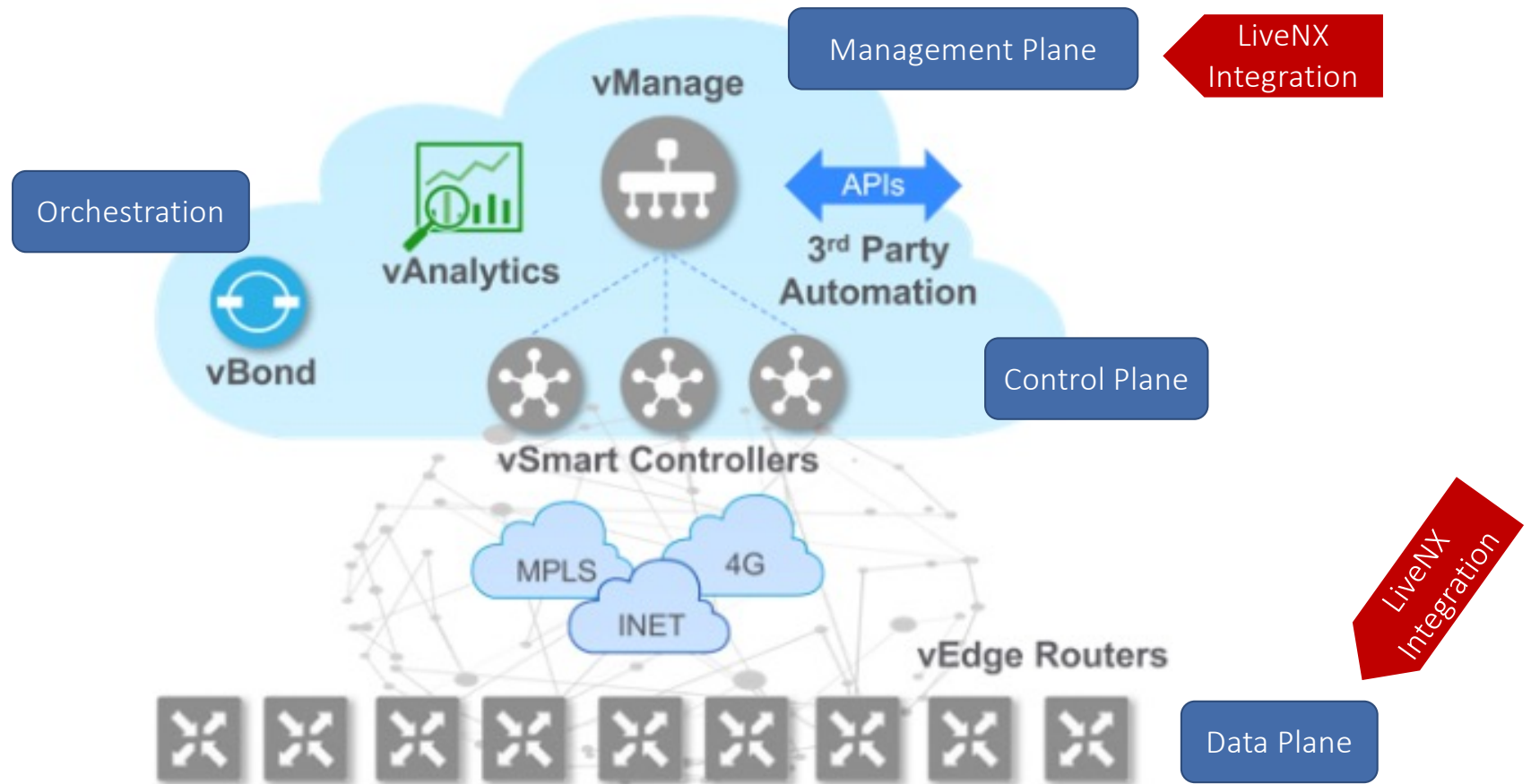
vSmart – SDWAN Controller

LiveAction®

# SDWAN Basics



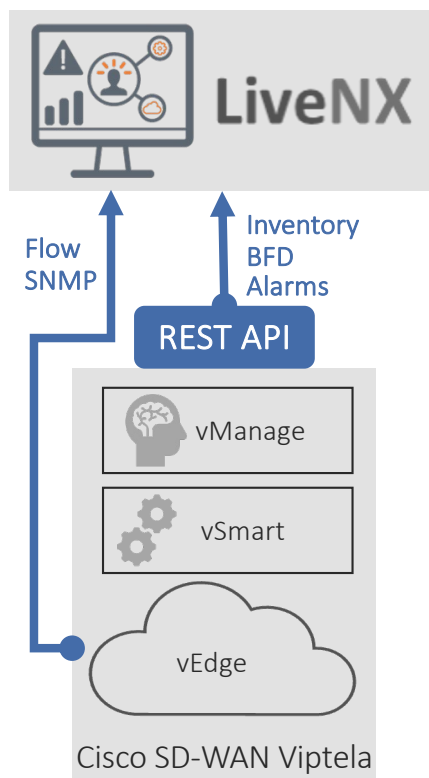
# SDWAN Basics





# SDWAN Integration Overview

# 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

---

# 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)



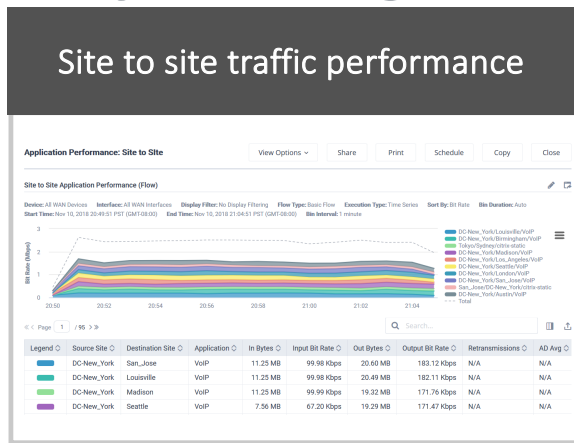


# Day 0

Cisco SD WAN Planning for Deployment

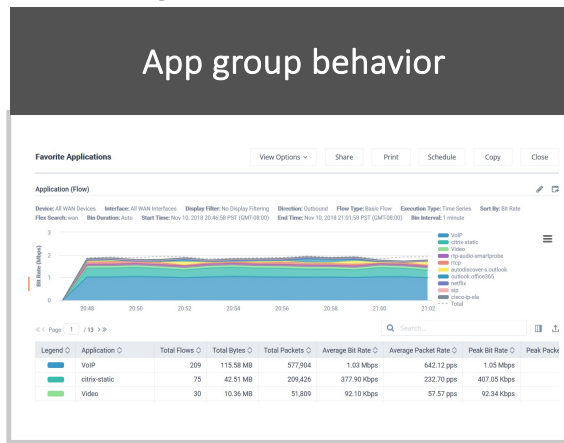
# Day 0: Design Baseline performance for policy design

## Site to site traffic performance



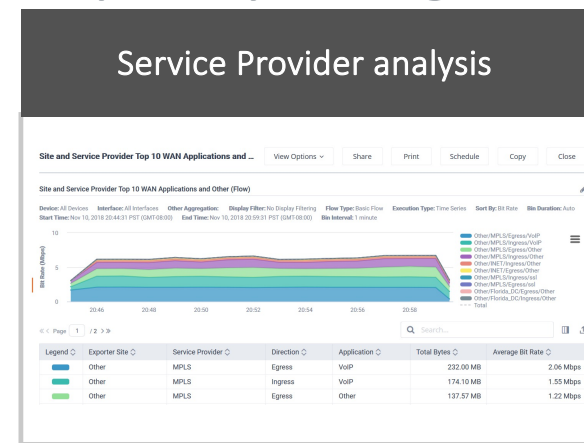
- Site to site traffic type and paths
- Provides data for:
  - Selection of initial pilot sites
  - Usage patterns
  - Site to site traffic behaviors

## App group behavior



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

## Service Provider analysis



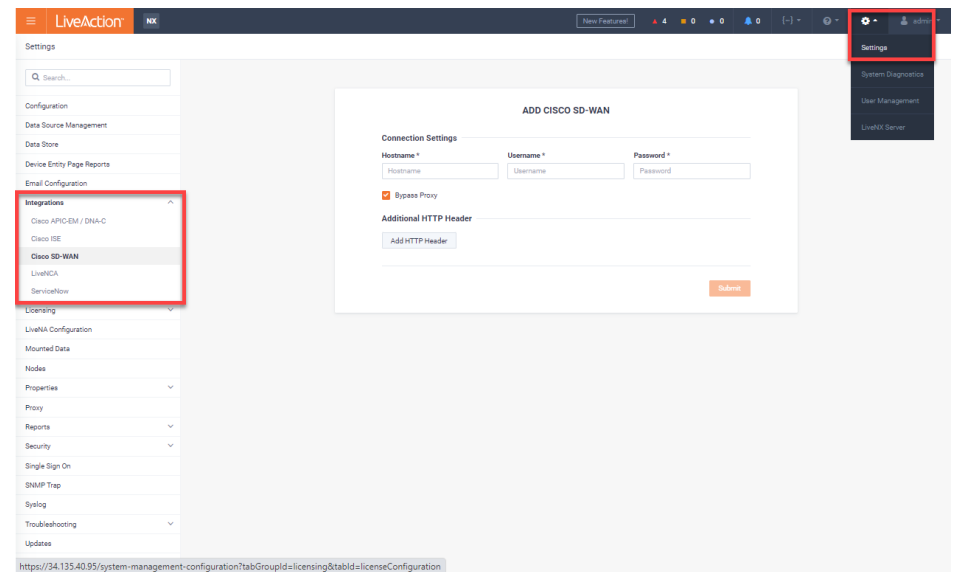
- Service Provider
- Path design inputs:
  - Which telco infrastructure path they should apps take, site by site.
  - Picking application to include in app route policies
  - How SD-WAN enabled vs non SD-WAN traffic maybe handled during deployment



# 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



A woman with long brown hair, wearing a white button-down shirt, is looking upwards and to the right with a thoughtful expression, her hand resting on her chin. The background is a dark, textured surface with white lines forming a complex maze. Several arrows are drawn on the maze, pointing in different directions: one points left, one points right, one points down, and another points right. The overall image has a professional, contemplative feel.

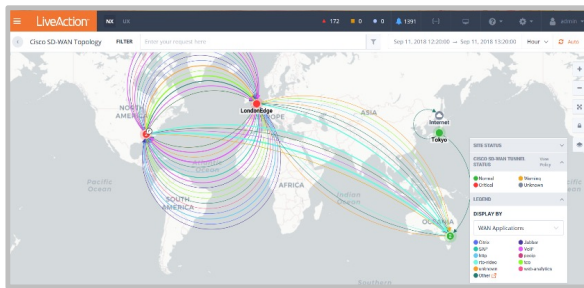
# Day 1

Policy verification at scale

# Day 1: Verify

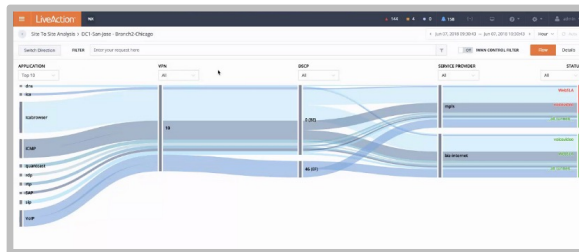
## Policy verification at scale

### Overlay performance



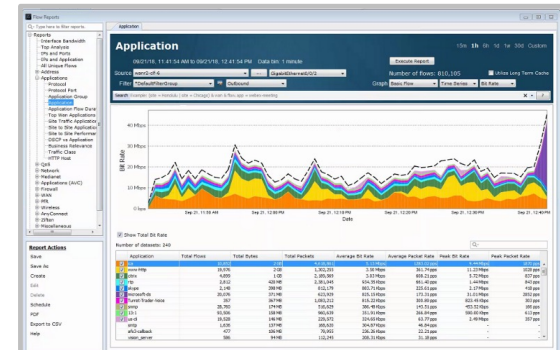
- Transport view
- Geo map
  - Quickly verify site to site behavior during deployment
- Verify the overlay performance:
  - Verify service VPN topology matches the intent set via policy
  - Verify service provider performance
  - Traffic engineering / paths

### 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

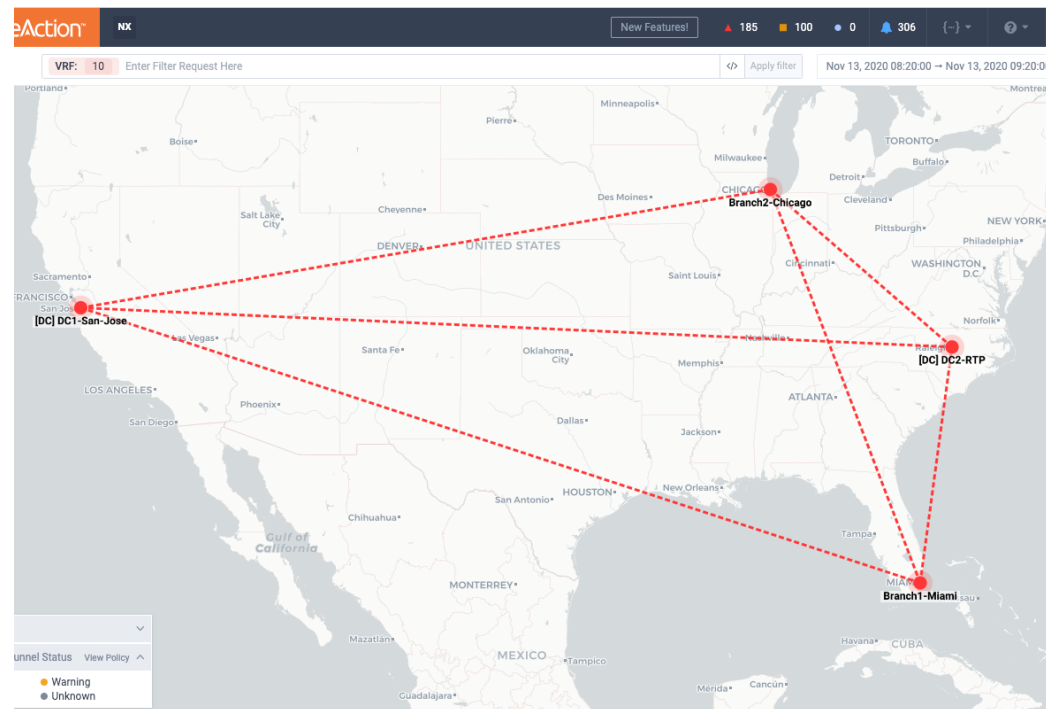
### Application performance



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

# 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-to-Site story or from the Geo Topology Map

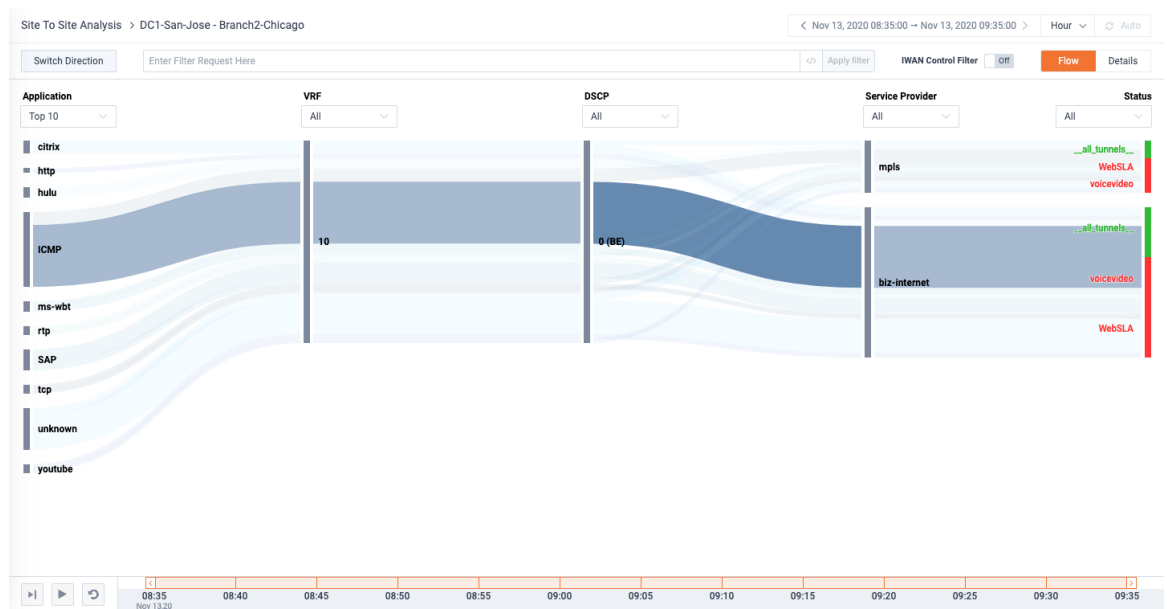
**Tunnel: Branch2-Chicago ⇌ DC1-San-Jose**

DC1-San-Jose → Branch2-Chicago

SLA Classes	SERVICE PROVIDER	
	biz-internet	mpls
__all_tunnels__	Green	Green
voicevideo	Red	Red
WebSLA	Red	Red

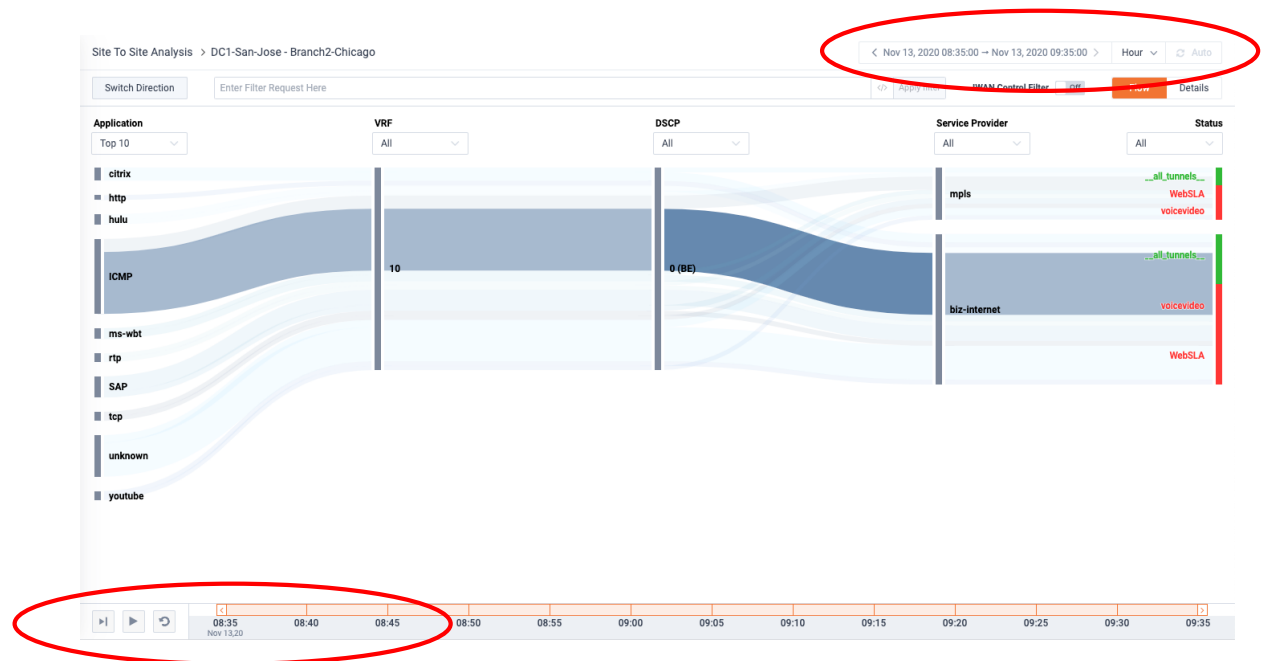
Branch2-Chicago → DC1-San-Jose

SLA Classes	SERVICE PROVIDER	
	biz-internet	mpls
__all_tunnels__	Green	Green
voicevideo	Red	Red
WebSLA	Red	Red



# 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





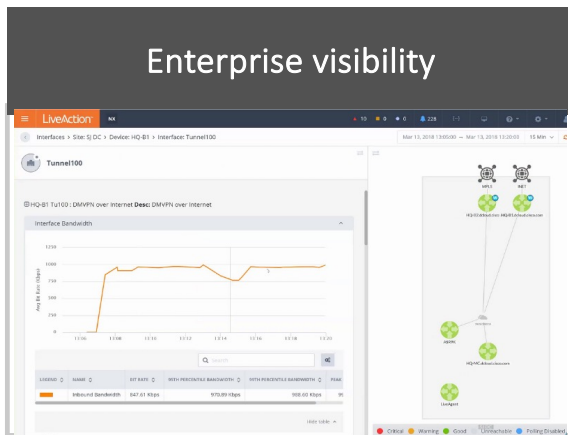


# Day 2

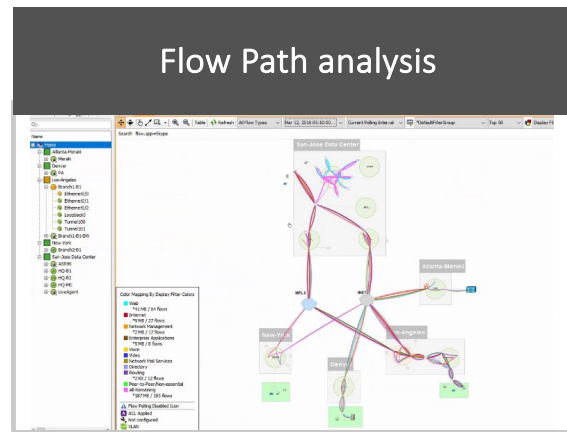
Scale and Operate

# Day 2: Scale and Operate

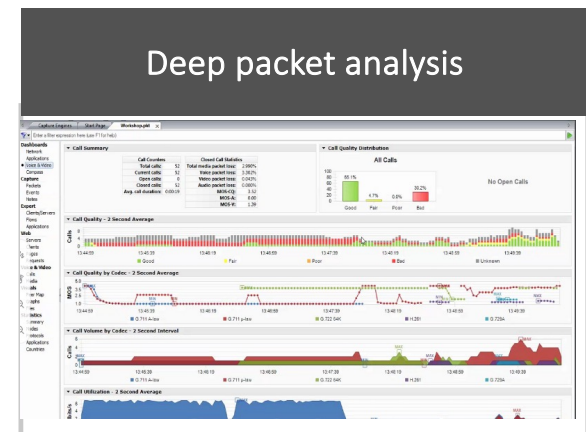
## Performance insights for optimization and rapid troubleshooting



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



- 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



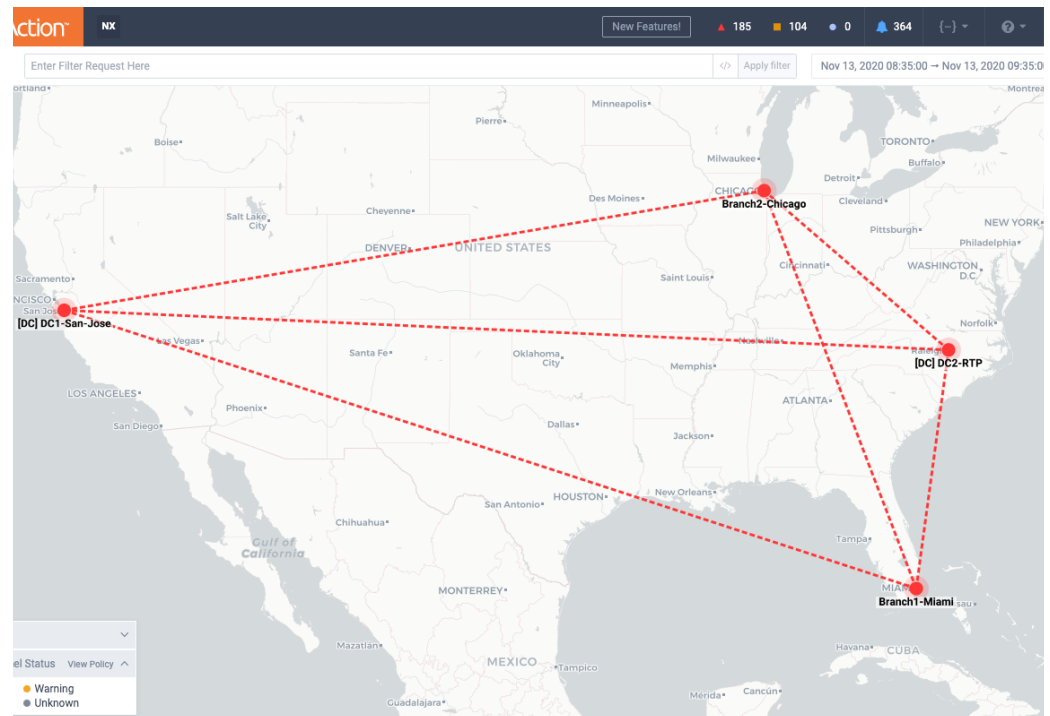
- LiveWire and Omniplance packet capture and analysis appliance
- Packet drill down
- Delivers intuitive visualization and robust forensics for faster incident resolution of network issues
- application performance issues and security investigations.

LiveAction®



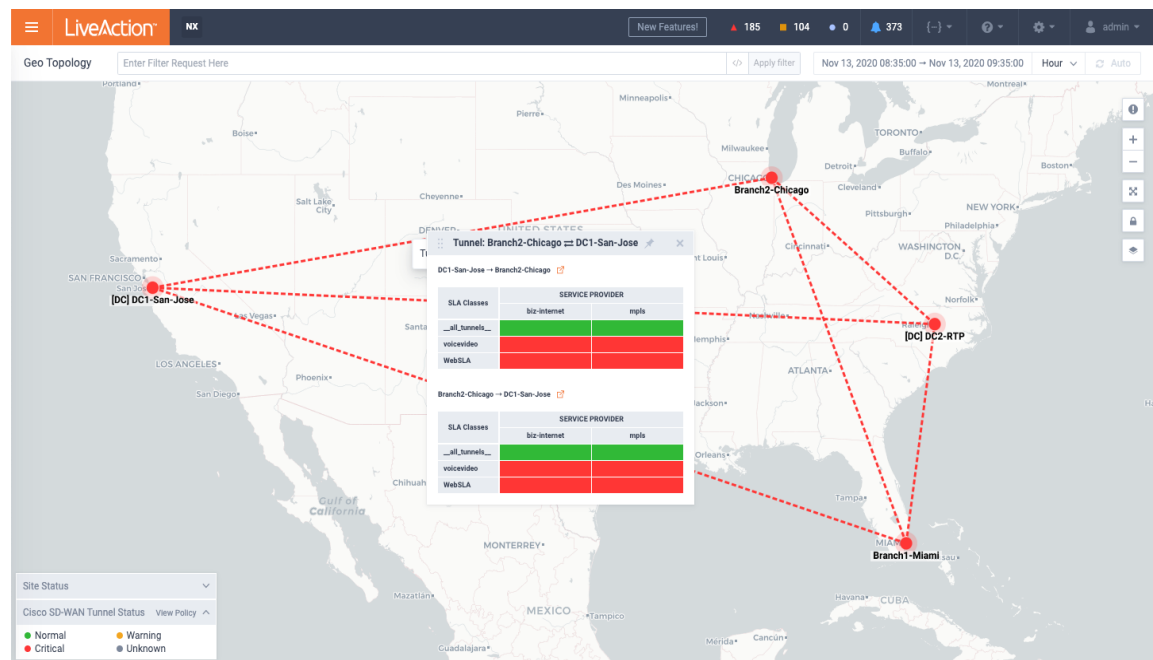
# Use the Geo Topology to monitor tunnel status

- 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

LiveActionNX

New Features!

▲ 185

■ 105

● 0

🔔 382

{-}

?

⚙️

admin

Dashboard

Nov 13, 2020 09:25:00 → Nov 13, 2020 10:25:00Add Widget

StatusWANSystemCisco SDWAN Performance

Site: Branch2-ChicagoEnter Filter Request Here</>Apply filter

Cisco SD-WAN Performance Top Site Pairs by Peak Jitter

Src Site→Dst Site	Avg Jitter	Peak Jitter
Branch2-Chicago→DC1-San-Jose	1.11 ms	14.57 ms
Branch2-Chicago→DC2-RTP	2.39 ms	37 ms
Branch2-Chicago→Branch1-Miami	2.42 ms	36 ms

Cisco SD-WAN Performance Top Site Pairs by Peak Loss

Src Site→Dst Site	Avg Loss Rate	Peak Loss Rate
Branch2-Chicago→DC1-San-Jose	23.84 %	100 %
Branch2-Chicago→Branch1-Miami	2.92 %	70 %
Branch2-Chicago→DC2-RTP	0.32 %	60 %

Cisco SD-WAN Performance Top Site Pairs by Peak Delay

Src Site→Dst Site	Avg Round Trip Delay	Peak Round Trip Delay
Branch2-Chicago→DC1-...	2.26 ms	22.56 ms
Branch2-Chicago→Bran...	77.4 ms	321 ms
Branch2-Chicago→DC2-...	52.79 ms	221 ms

Cisco SD-WAN Performance Top Service Providers by Peak Jitter

Service Provider	Avg Jitter	Peak Jitter
biz-internet	393.96 ms	14.57 ms
mpls	349.85 ms	9.7 ms

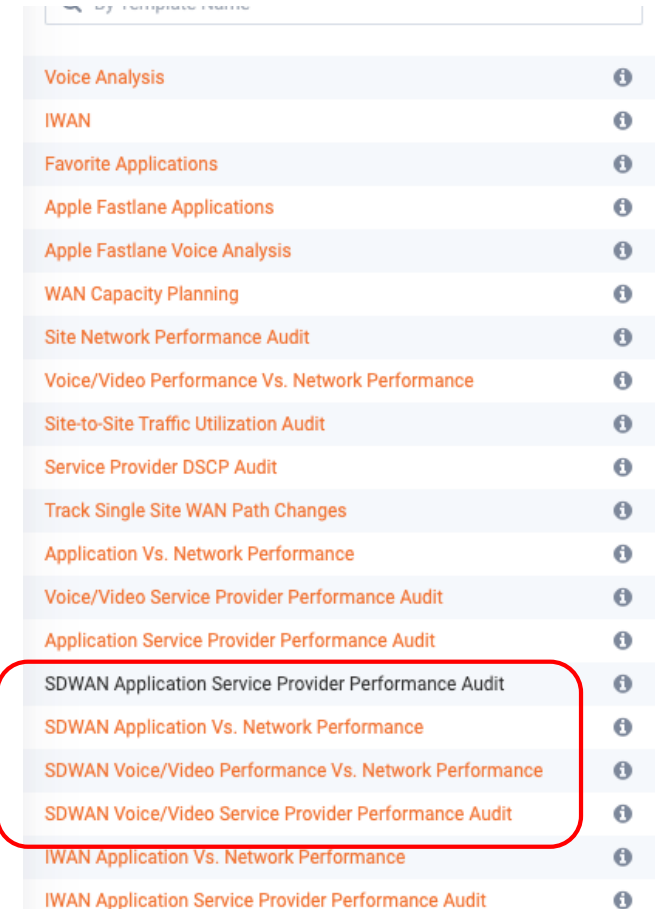
Cisco SD-WAN Performance Top Service Providers by Peak Loss

Service Provider	Avg Loss Rate	Peak Loss Rate
mpls	10.07 %	100 %
biz-internet	7.98 %	100 %

Cisco SD-WAN Performance Top Service Providers by Peak Delay

Service Provider	Avg Round Trip Delay	Peak Round Trip Delay
biz-internet	780.98 ms	22.56 ms
mpls	810.14 ms	20.45 ms

# There are also pre-configured SDWAN report templates

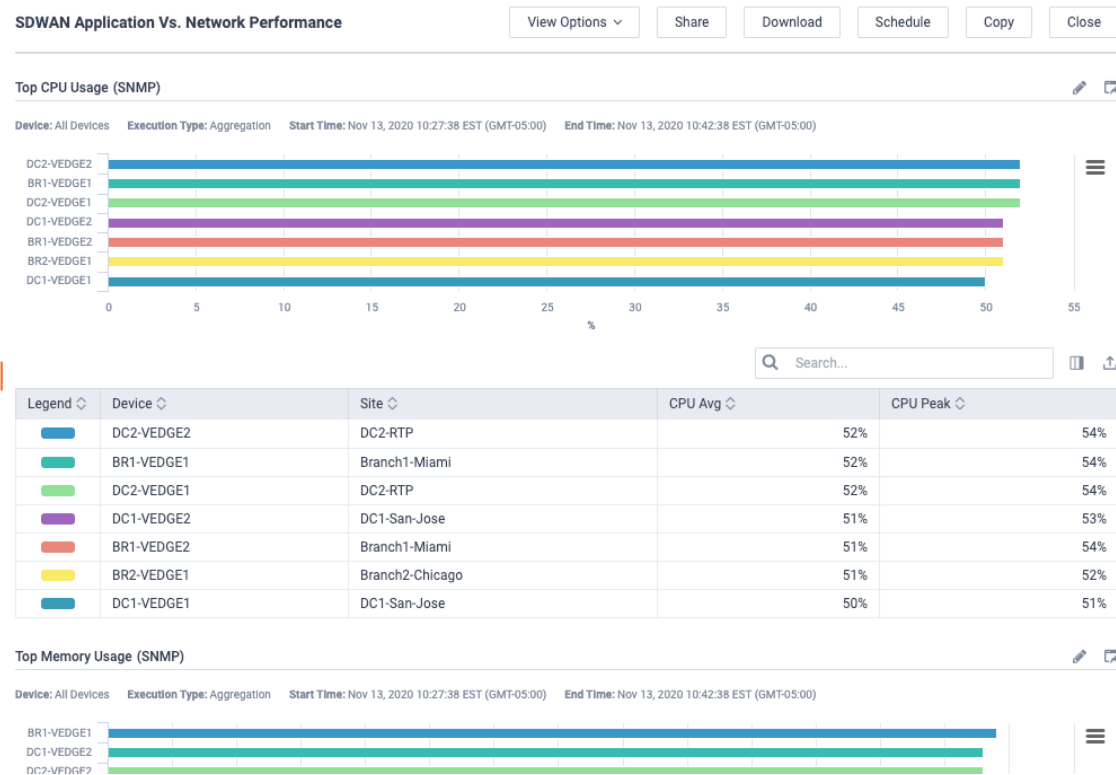


A screenshot of a web application menu for report templates. The menu is a vertical list of items, each with an information icon (i) to its right. A red rounded rectangle highlights a group of four items: 'SDWAN Application Service Provider Performance Audit', 'SDWAN Application Vs. Network Performance', 'SDWAN Voice/Video Performance Vs. Network Performance', and 'SDWAN Voice/Video Service Provider Performance Audit'. The other items in the menu are 'Voice Analysis', 'IWAN', 'Favorite Applications', 'Apple Fastlane Applications', 'Apple Fastlane Voice Analysis', 'WAN Capacity Planning', 'Site Network Performance Audit', 'Voice/Video Performance Vs. Network Performance', 'Site-to-Site Traffic Utilization Audit', 'Service Provider DSCP Audit', 'Track Single Site WAN Path Changes', 'Application Vs. Network Performance', 'Voice/Video Service Provider Performance Audit', 'Application Service Provider Performance Audit', 'IWAN Application Vs. Network Performance', and 'IWAN Application Service Provider Performance Audit'.

Voice Analysis	i
IWAN	i
Favorite Applications	i
Apple Fastlane Applications	i
Apple Fastlane Voice Analysis	i
WAN Capacity Planning	i
Site Network Performance Audit	i
Voice/Video Performance Vs. Network Performance	i
Site-to-Site Traffic Utilization Audit	i
Service Provider DSCP Audit	i
Track Single Site WAN Path Changes	i
Application Vs. Network Performance	i
Voice/Video Service Provider Performance Audit	i
Application Service Provider Performance Audit	i
SDWAN Application Service Provider Performance Audit	i
SDWAN Application Vs. Network Performance	i
SDWAN Voice/Video Performance Vs. Network Performance	i
SDWAN Voice/Video Service Provider Performance Audit	i
IWAN Application Vs. Network Performance	i
IWAN Application Service Provider Performance Audit	i

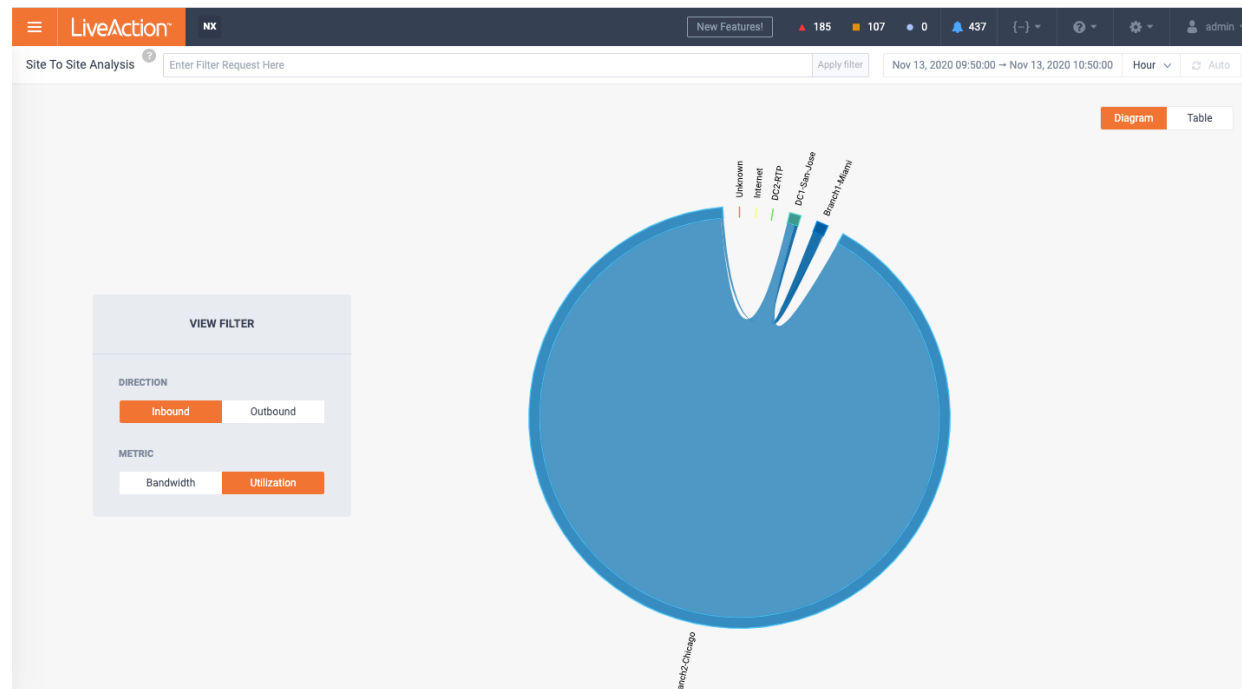
# SDWAN Application Vs. Network Performance

- 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

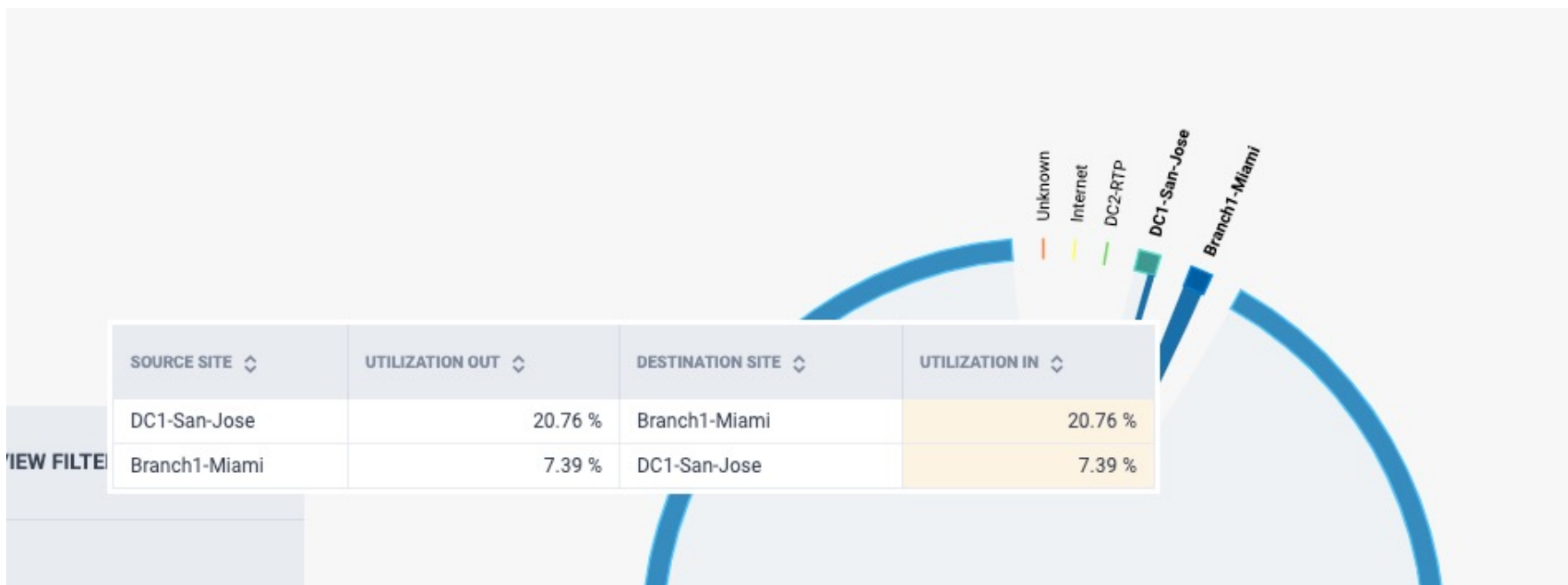
Quick view of traffic between sites



# 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



# Alerting

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

The screenshot displays the LiveAction NX Alerts interface. The top navigation bar includes the LiveAction logo, a user menu, and various status indicators (186, 108, 0, 456). The main section is titled 'Alerts' and features a search bar and a filter button. Below this, there are tabs for 'Active' and 'History'. The 'Active' tab is selected, showing a list of alerts. The table has columns for SEVERITY, DESCRIPTION, TIME OPENED, ACTIVE FOR, CATEGORY, TYPE, and THIRD PARTY INTEGRATION. The alerts are sorted by time opened, with the most recent at the top. The table shows a mix of Critical and Warning severity alerts, primarily related to BFD sessions and QoS interface drops.

	SEVERITY	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	THIRD PARTY INTEGRATION
<input type="checkbox"/>	All	Description			All	All	Third Party Integr...
<input type="checkbox"/>	Critical	ge0/0 on DC1-VEDGE2 had a drop rate of 93.06 pps in the Input direction.	13 Nov 2020, 11:05AM	a few seconds	Device, Interface	QoS Interface Drop	
<input type="checkbox"/>	Critical	All control connections to the node are down	13 Nov 2020, 10:59AM	7 minutes	vManage	vManage: Control No...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 10:59AM	7 minutes	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Critical	ge0/0 on DC1-VEDGE1 had a drop rate of 204.00 pps in the Output direction.	13 Nov 2020, 10:56AM	9 minutes	Device, Interface	QoS Interface Drop	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 10:43AM	22 minutes	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 10:28AM	37 minutes	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 10:23AM	42 minutes	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	A tloc went down	13 Nov 2020, 10:13AM	an hour	vManage	vManage: Control TL...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 09:58AM	an hour	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 09:48AM	an hour	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 09:23AM	2 hours	vManage	vManage: BFD TLOC ...	
<input type="checkbox"/>	Warning	A tloc went down	13 Nov 2020, 08:53AM	2 hours	vManage	vManage: Control TL...	
<input type="checkbox"/>	Warning	All BFD sessions for the tloc are down	13 Nov 2020, 08:53AM	2 hours	vManage	vManage: BFD TLOC ...	

At the bottom of the table, it indicates 'All rows / 294'.



# Alert Configuration

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

The screenshot shows the LiveAction NX Alert Management interface. The top navigation bar includes the LiveAction logo, 'NX', a 'New Features!' button, and status indicators for 186 alerts, 108 integrations, 0 notifications, and 470 users. The main section is titled 'Alert Management' and contains a 'LiveNX Alerts' tab and a 'Cisco SD-WAN Integrations' tab. Below the tabs is a search bar and a table of alert configurations.

ALERT TYPE	ENABLED	SHARING	DESCRIPTION
<input type="checkbox"/> Alert Type	All	Sharing	Description
<input type="checkbox"/> aaa Admin Password Change	✓	Web UI	The password for the AAA user admin changed on a router or controller
<input type="checkbox"/> BFD Between Sites Down	✓	Web UI	All BFD sessions on all routers between two sites are in the Down state. This means that no data traffic can be sent to or transmitted bet...
<input type="checkbox"/> BFD Between Sites Up	✓	Web UI	A BFD session on a router between two sites transitioned to the Up state
<input type="checkbox"/> BFD Node Down	✓	Web UI	All BFD sessions for a router are in the Down state. This means that no data traffic can be sent to or transmitted from that router
<input type="checkbox"/> BFD Node Up	✓	Web UI	A BFD session for a router transitioned to the Up state
<input type="checkbox"/> BFD Site Down	✓	Web UI	All BFD sessions on all vEdge routers in a site are in the Down state. This means that no data traffic can be sent to or transmitted from t...
<input type="checkbox"/> BFD Site Up	✓	Web UI	A BFD session on a router in a site transitioned to the Up state
<input type="checkbox"/> BFD TLOC Down	✓	Web UI	All BFD sessions for a TLOC (transport tunnel identified by a color) are in the Down state. This means that no data traffic can be sent to ...
<input type="checkbox"/> BFD TLOC Up	✓	Web UI	A BFD session for a TLOC transitioned to the Up state
<input type="checkbox"/> BGP Router Down	✓	Web UI	All BGP sessions on a router are in the Down state
<input type="checkbox"/> BGP Router Up	✓	Web UI	A BGP session on a router transitioned to the Up state
<input type="checkbox"/> Clear Installed Certificate	✓	Web UI	All certificates on a controller or device, including the public and private keys and the root certificate, have been cleared, and the device h...
<input type="checkbox"/> Cloned Vedge Detected	✓	Web UI	A duplicate router that has the same chassis and serial numbers and the same system IP address has been detected

# 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

The screenshot displays the LiveAction NX Alert Management interface. The main table lists various alert types, with 'Cisco SD-WAN SLA Class Path Change' highlighted. To the right, a configuration panel for this specific alert is shown, including options to enable the alert, set its severity to 'Critical', and configure thresholds (set to 'For at Least' > 0 min). The sharing section is also visible, with 'Web UI' selected.

**Alert Management**

LiveNX Alerts

Enable Disable

	ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS
<input type="checkbox"/>	Alert Type	All	All	All	Thresholds
<input type="checkbox"/>	BGP Peer Connection Change	Network	▲ Critical		for at least > 0 minutes
<input type="checkbox"/>	Cisco IWAN Path Change	Network	▲ Critical		for at least > 0 minutes
<input type="checkbox"/>	Cisco IWAN Threshold Crossing	Network	▲ Critical		for at least > 0 minutes
<input type="checkbox"/>	Cisco SD-WAN SLA Class Path Change	Network	▲ Critical	✓	for at least > 0 minutes
<input type="checkbox"/>	Critical Traffic Response Time	Application	▲ Critical		Response Time >= 5 ms for at le
<input checked="" type="checkbox"/>	Device CPU Utilization	Device, Interface	Multiple	✓	Multiple
<input type="checkbox"/>	Device Flow Stop	Device, Interface	▲ Critical		for at least > 0 minutes
<input checked="" type="checkbox"/>	Device Memory Utilization	Device, Interface	Multiple	✓	Multiple
<input checked="" type="checkbox"/>	Device Reachability	Device, Interface	Multiple	✓	Multiple
<input type="checkbox"/>	Interface Errors (CRC, Frame, Overruns,...)	Device, Interface	▲ Critical		Number of Errors >= 40 Errors fo
<input checked="" type="checkbox"/>	Interface Reachability	Device, Interface	Multiple		Multiple
<input type="checkbox"/>	IPSLA Test	Network	▲ Critical		Total Test Errors > 3 Errors for at
<input type="checkbox"/>	IPSLA Voice/Jitter Test	Network	▲ Critical		Total Test Errors > 3 Errors for at

**Cisco SD-WAN SLA Class Path Change**

Monitor Cisco SD-WAN SLA Class out-of-policy / in-policy events

**Enabled**  
☒ On

**Severity**  
▲ Critical

**THRESHOLDS**

**For at Least**  
> 0 min

**SHARING**

☐ Email  
Type email

☐ ServiceNow

☐ SNMP trap

☒ Web UI

☐ Syslog

Cancel Save

# Launch the SDWAN Learning Labs...

© 2022, LiveAction, Inc. All Rights Reserved.

LiveAction®

A man in a grey suit and blue tie stands with his arms outstretched and head tilted back, looking upwards. The background is a soft-focus bokeh of blue and white light circles. An orange rectangular box is overlaid on the left side of the image.

# Wrap-Up

---

# LiveAction Support

- Global support
  - Contact [support@liveaction.com](mailto:support@liveaction.com)
  - Call: 408-217-6501
    - Monday-Friday 6am -7pm Pacific Time
  - 24x7 *Priority One* support
- “Resources” website
  - [www.liveaction.com/support/resources/](http://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](mailto: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!**