LiveAction®

LiveAction Training

Lab Workbook Pt. 1

While every precaution has been taken in the preparation of this document, LiveAction assumes no responsibility for errors or omissions. This document and features described herein are subject to change without notice.
This LiveAction Training Material may not be sold by any company other than LiveAction without prior written permission. Neither LiveAction nor any authorized distributor or reseller shall be liable to the purchaser or any other person or entity with respect to any liability, loss, or damage caused or alleged to have been caused directly or indirectly by this material.

2021-Aug.

Table of Contents

IMPORTANT INFORMATION – Please Read!

The step-by-step Labs in this Workbook have been written specifically for the LiveAction Training Student Pod, documented herein. All "Pods" have been pre-configured with the appropriate software and generated traffic to successfully perform these labs. Pay attention to any Notes presented as:

Note: This is a note example which gives additional information to the specific context.

The Diagrams, or screen shots, throughout this Workbook are *examples* for demonstration purposes and may not reflect the appropriate parameters for the classroom and/or your specific subnet. Unless specifically directed to do so, do not attempt to match the settings displayed in the screen shots to your configuration.

Traffic collected by your assigned Pod may not be synchronized with other Student Pods, and in some cases… due to specific application traffic timing, may not display the exact result specified in the Labs. The main intent is to know HOW to access the information… not to attain specific lab results.

Throughout this document *italics,* **bold** fonts, and words in CAPS, are used to place emphasis on specific procedures or results.

Lab .0

Lab 0: Setup and Get Connected

Lab 0.1: Connect to the Lab Network

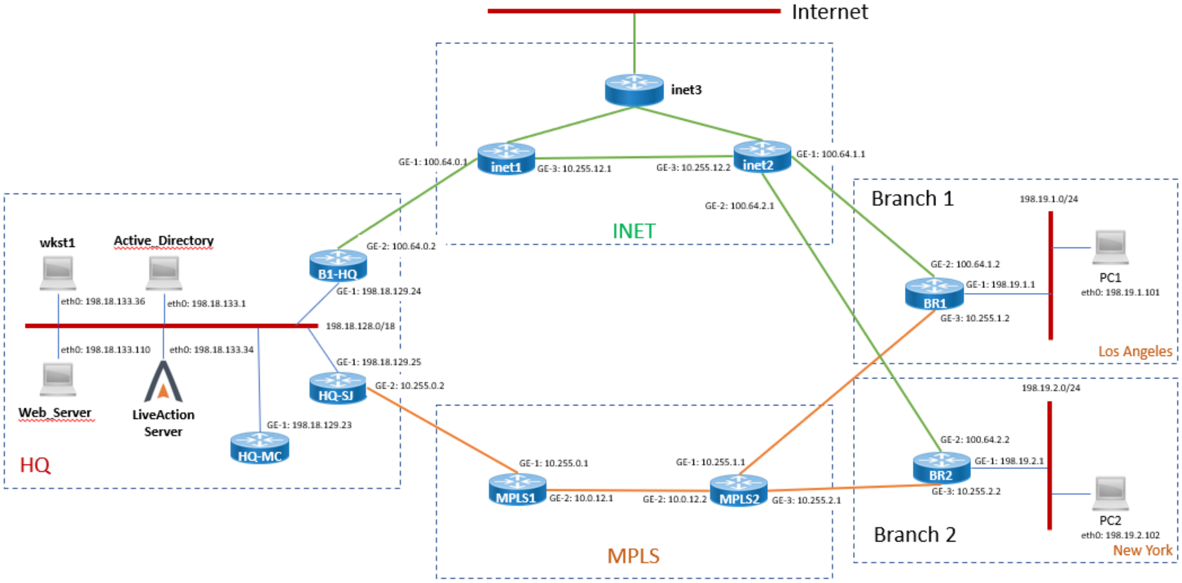
For this class, each attendee or Student will connect to and manage their own LiveNX installation. In this lab you will connect to the classroom lab environment. In some locations you may first be asked to connect your laptop to the Internet.

Your instructor will assign a dedicated environment or “Pod” to each Student and may provide you with a handout containing connectivity information specific to your Pod. Each Pod has the LiveNX Server and Client pre-installed, with some initial configuration already performed. Each Student will manage:

Local:
1 x PC Workstation to be used as a Management PC (Your Laptop)
1 x Installed LiveNX Client
1 x Browser

Remote Student Pod
1 x Windows Workstation accessed via RDC (optional) with an installed LiveNX Client and Browser
1 x LiveNX OVA Linux install
    1 LiveNX Server
    1 LiveNX Node (installed on LiveNX Server)

DIAGRAM



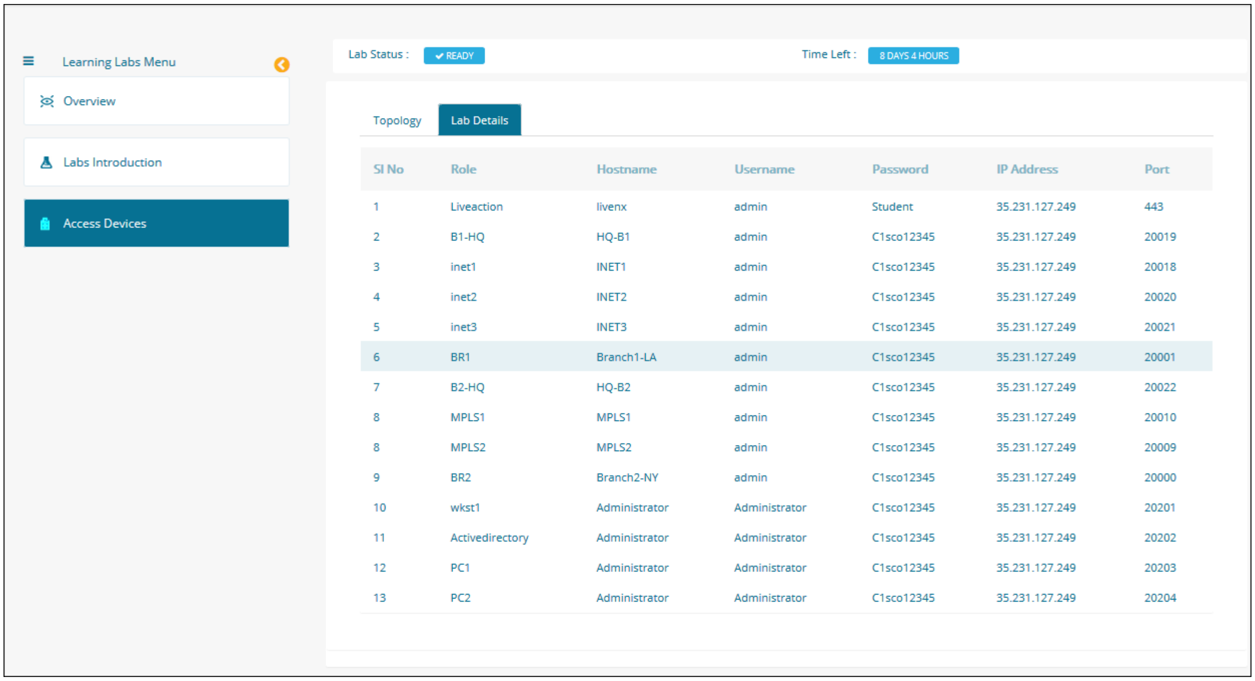
In the diagram above your workstation is connected over the LAN or WAN to your assigned Training Pod resources.

Note: Make sure to consult the Infrastructure Diagram, as well as specific classroom instructions for names, IP addresses, and other parameters. **The screen shots in this Lab**

Workbook are *examples* which may **NOT** reflect the appropriate parameters for the classroom and/or your specific subnet.

Each student is provided with login credentials to our Training Lab Website, which includes connection information as illustrated below. Your instructor may provide additional class-specific addressing and credentials. You may wish to Bookmark this Web Page or Make *a written note* of this information for later reference.

DIAGRAM



Lab Status : ✓ READY

Time Left : 8 DAYS 4 HOURS

SI No	Role	Hostname	Username	Password	IP Address	Port
1	Liveaction	livenx	admin	Student	35.231.127.249	443
2	B1-HQ	HQ-B1	admin	C1sco12345	35.231.127.249	20019
3	inet1	INET1	admin	C1sco12345	35.231.127.249	20018
4	inet2	INET2	admin	C1sco12345	35.231.127.249	20020
5	inet3	INET3	admin	C1sco12345	35.231.127.249	20021
6	BR1	Branch1-LA	admin	C1sco12345	35.231.127.249	20001
7	B2-HQ	HQ-B2	admin	C1sco12345	35.231.127.249	20022
8	MPLS1	MPLS1	admin	C1sco12345	35.231.127.249	20010
8	MPLS2	MPLS2	admin	C1sco12345	35.231.127.249	20009
9	BR2	Branch2-NY	admin	C1sco12345	35.231.127.249	20000
10	wkst1	Administrator	Administrator	C1sco12345	35.231.127.249	20201
11	Activedirectory	Administrator	Administrator	C1sco12345	35.231.127.249	20202
12	PC1	Administrator	Administrator	C1sco12345	35.231.127.249	20203
13	PC2	Administrator	Administrator	C1sco12345	35.231.127.249	20204

Lab Steps:

1. Connect your workstation to the Management Network with an Ethernet cable (or, if available, connect to the Wireless network per the instructions provided by your instructor).
2. Verify connectivity to the Internet by opening a browser to www.liveaction.com.

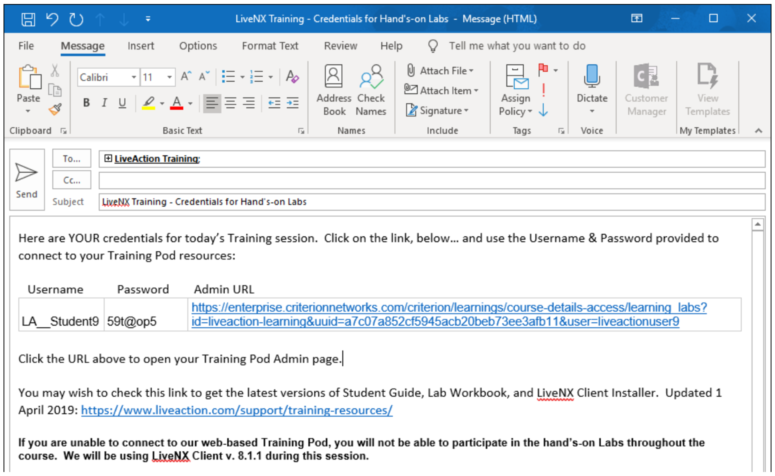
Note: Make sure to consult the Infrastructure Diagram and worksheets, as well as specific classroom instructions for names, IP addresses, and other parameters. **The screen shots in this Lab Workbook are *examples*** which may not reflect the appropriate parameters for the classroom and/or your specific subnet.

Lab 0.2: Connecting to Your Training Pod

Throughout this Lab Workbook, you will be directed to connect to your Pod resources… use the IP Address & Port information provided in your assigned Web connection document.

The instructor will have emailed credentials/login information to you prior to the start of the Training Session… like that below…

DIAGRAM



To... LiveAction Training;

Subject: LiveNX Training - Credentials for Hand's-on Labs

Here are YOUR credentials for today's Training session. Click on the link, below… and use the Username & Password provided to connect to your Training Pod resources:

Username	Password	Admin URL
LA__Student9	59t@op5	https://enterprise.criterionnetworks.com/criterion/learnings/course-details-access/learning_labs?id=liveaction-learning&uuid=a7c07a852cf5945acb20beb73ee3afb11&user=liveactionuser9

Click the URL above to open your Training Pod Admin page.

You may wish to check this link to get the latest versions of Student Guide, Lab Workbook, and LiveNX Client Installer. Updated 1 April 2019: https://www.liveaction.com/support/training-resources/

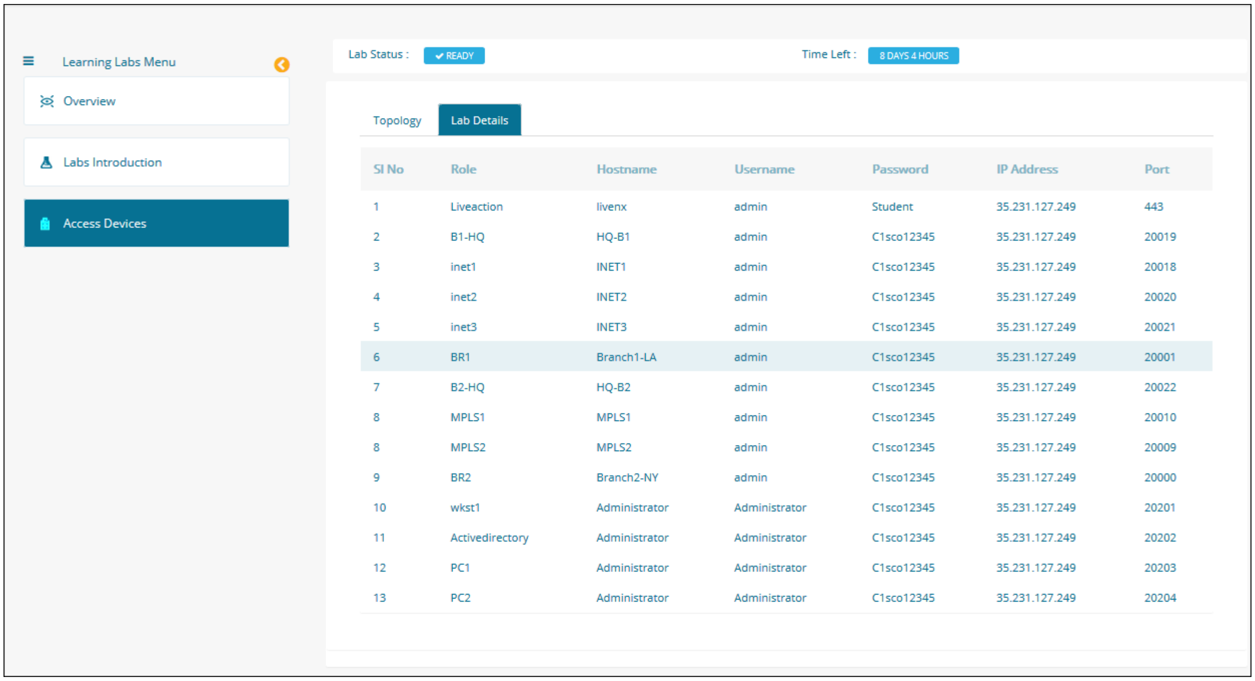
If you are unable to connect to our web-based Training Pod, you will not be able to participate in the hand's-on Labs throughout the course. We will be using LiveNX Client v. 8.1.1 during this session.

Lab Steps:

1. Click the URL provided in the email.

Note: If clicking-on the URL does not automatically launch your default browser you may need to copy the URL to your browser address bar.

2. Enter the **Username & Password** as provided in the email.
3. **Tick** the "Terms of Service" box.
4. Click **Enter**.
5. In the **Learning Labs** menu click **Access Devices** to display your **Lab Details**.



Lab Status : ✓ READY

Time Left : 8 DAYS 4 HOURS

SI No	Role	Hostname	Username	Password	IP Address	Port
1	Liveaction	livenx	admin	Student	35.231.127.249	443
2	B1-HQ	HQ-B1	admin	C1sco12345	35.231.127.249	20019
3	inet1	INET1	admin	C1sco12345	35.231.127.249	20018
4	inet2	INET2	admin	C1sco12345	35.231.127.249	20020
5	inet3	INET3	admin	C1sco12345	35.231.127.249	20021
6	BR1	Branch1-LA	admin	C1sco12345	35.231.127.249	20001
7	B2-HQ	HQ-B2	admin	C1sco12345	35.231.127.249	20022
8	MPLS1	MPLS1	admin	C1sco12345	35.231.127.249	20010
8	MPLS2	MPLS2	admin	C1sco12345	35.231.127.249	20009
9	BR2	Branch2-NY	admin	C1sco12345	35.231.127.249	20000
10	wkst1	Administrator	Administrator	C1sco12345	35.231.127.249	20201
11	Activedirectory	Administrator	Administrator	C1sco12345	35.231.127.249	20202
12	PC1	Administrator	Administrator	C1sco12345	35.231.127.249	20203
13	PC2	Administrator	Administrator	C1sco12345	35.231.127.249	20204

Lab 0.3: Install the LiveNX Client

A direct connection from the LiveNX Client installed on your workstation is the most efficient method to connect with the Engineering Console. You'll install the LiveNX Client now, so it is ready for use in future labs.

Note: The Instructor will provide version information prior to the training session (via facilitation email). Make sure to download & install the appropriate version of the LiveNX Client as directed.

To install the LiveNX Client:

1. Download the appropriate Client version from the LiveAction Web Pages, or from the Training Resources page.
   a. https://cloudkeys.liveaction.com/downloads
   b. http://www.liveaction.com/support/training-resources/
2. Launch the installer.
3. Accept all the defaults, as appropriate.

Note: At this point we will NOT login to the LiveNX Server… instructions for connecting & login are provided in a subsequent Lab.

Lab 1

Lab 1: The LiveNX Web UI

Lab 1.1: Explore the Web UI

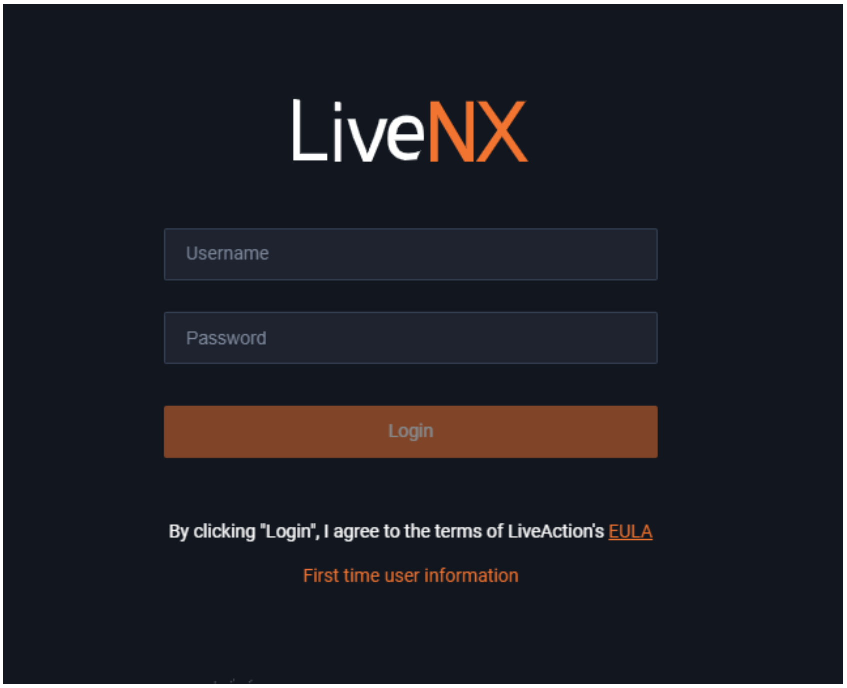
The LiveNX WebUI provides an easy, convenient way to view the data collected by LiveNX. You may create custom Dashboards to give visibility across your entire Enterprise, perform LiveNX configuration, view & troubleshoot topology & devices, as well as view/run/schedule reports. Dashboard settings are saved per-user login but may be initially based-upon the admin users' setup.

Note: The displays in these UI labs will vary, depending upon how long your Pod has been running, as well as the variety of traffic. These labs are meant to illustrate *how* to get at the information… results are not important. Diagrams are for illustration purposes and may not reflect the data you may view on your Training Pod.

In this, and all subsequent Labs, utilize the addressing <ipaddress> and TCP ports <port> provided on the Access Devices web page. In this Lab you will view the different features of the LiveNX WebUI.

Lab Steps:

1. Open your Browser and navigate to the LiveNX Server at https://<ipaddress>
2. Login to the WebUI using: **Username**: admin **Password**: Student



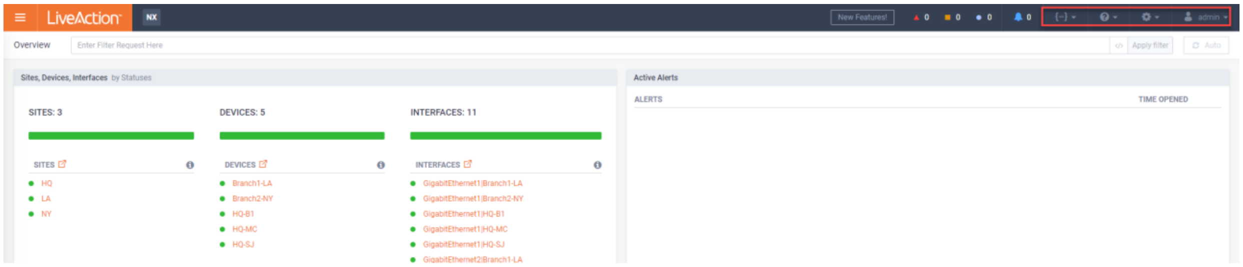
By clicking "Login", I agree to the terms of LiveAction's EULA

First time user information

The Overview screen will appear.

Note: The contents of this screen may change dependent upon the *version* of LiveNX being run.

3. Hover over and/or click the various icons at the Top-Right of the screen to see what they do!



Sites, Devices, Interfaces by Statuses

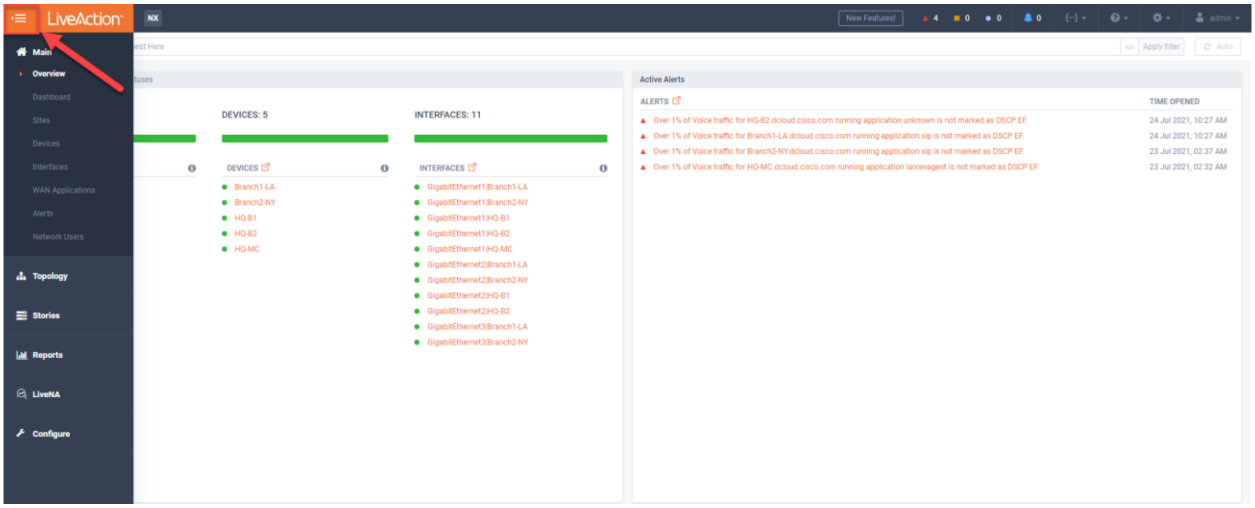
SITES: 3

DEVICES: 5

INTERFACES: 11

SITES	DEVICES	INTERFACES
HQ	Branch1-LA	GigabitEthernet1|Branch1-LA
LA	Branch2-NY	GigabitEthernet1|Branch2-NY
NY	HQ-B1	GigabitEthernet1|HQ-B1
	HQ-MC	GigabitEthernet1|HQ-MC
	HQ-SJ	GigabitEthernet1|HQ-SJ
		GigabitEthernet2|Branch1-LA

4. Click the **Menu** icon at the Top-Left and explore the menus.



DEVICES: 5

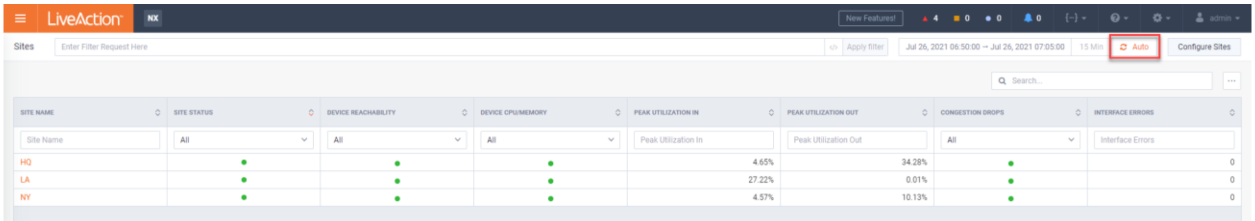
INTERFACES: 11

DEVICES	INTERFACES
Branch1-LA	GigabitEthernet1|Branch1-LA
Branch2-NY	GigabitEthernet1|Branch2-NY
HQ-B1	GigabitEthernet1|HQ-B1
HQ-B2	GigabitEthernet1|HQ-B2
HQ-MC	GigabitEthernet1|HQ-MC
	GigabitEthernet2|Branch1-LA
	GigabitEthernet2|Branch2-NY
	GigabitEthernet2|HQ-B1
	GigabitEthernet2|HQ-B2
	GigabitEthernet3|Branch1-LA
	GigabitEthernet3|Branch2-NY

Active Alerts

ALERTS	TIME OPENED
Over 1% of Voice traffic for HQ-B2.dcloud.cisco.com running application unknown is not marked as DSCP EF.	24 Jul 2021, 10:27 AM
Over 1% of Voice traffic for Branch1-LA.dcloud.cisco.com running application sip is not marked as DSCP EF.	24 Jul 2021, 10:27 AM
Over 1% of Voice traffic for Branch2-NY.dcloud.cisco.com running application sip is not marked as DSCP EF.	23 Jul 2021, 02:37 AM
Over 1% of Voice traffic for HQ-MC.dcloud.cisco.com running application lanrevagent is not marked as DSCP EF.	23 Jul 2021, 02:32 AM

5. Select **Sites.**



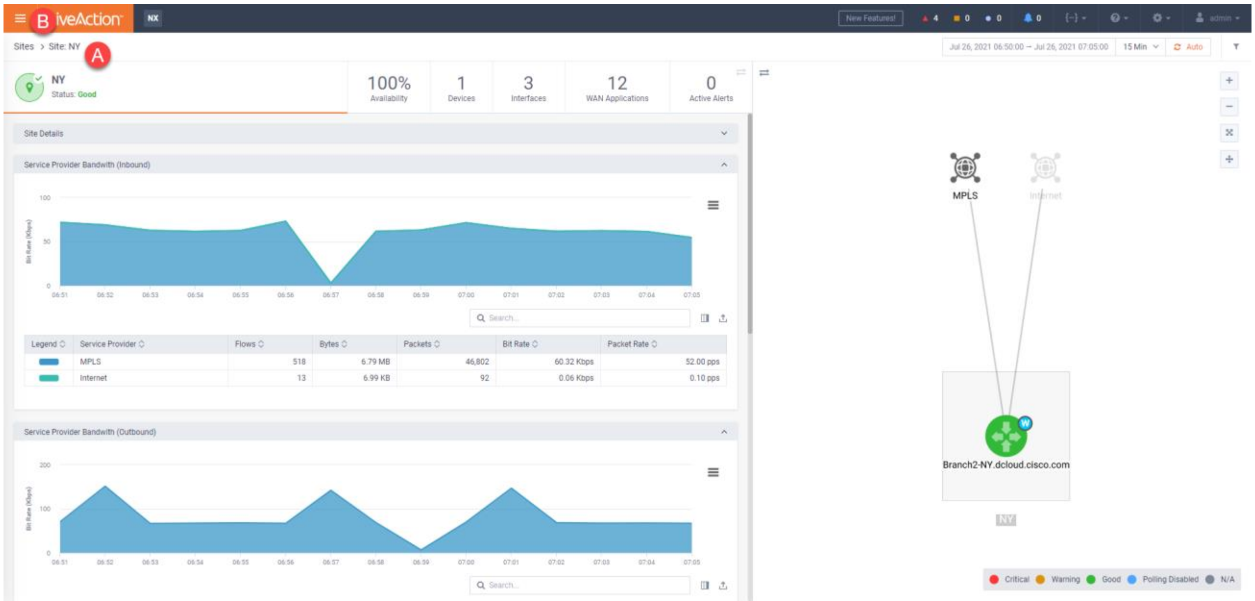
SITE NAME	SITE STATUS	DEVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION DROPS	INTERFACE ERRORS
Site Name	All	All	All	Peak Utilization In	Peak Utilization Out	All	Interface Errors
HQ	●	●	●	4.65%	34.28%	●	0
LA	●	●	●	27.22%	0.01%	●	0
NY	●	●	●	4.57%	10.13%	●	0

Note that the sites, and their associated statistics, are listed in columnar format.

Note: Detailed site information is specified in the *Device Semantics* Lab.

6. Note: Status, Utilization, Drops, Errors, etc.…
7. Toggle the **Auto Update** to ON.
8. Click on the link to **Los_Angeles** to see additional site info.

Anytime you wish to return to a prior level, or the WebUI home, you can click the Breadcrumbs (A) or Menu icon (B).

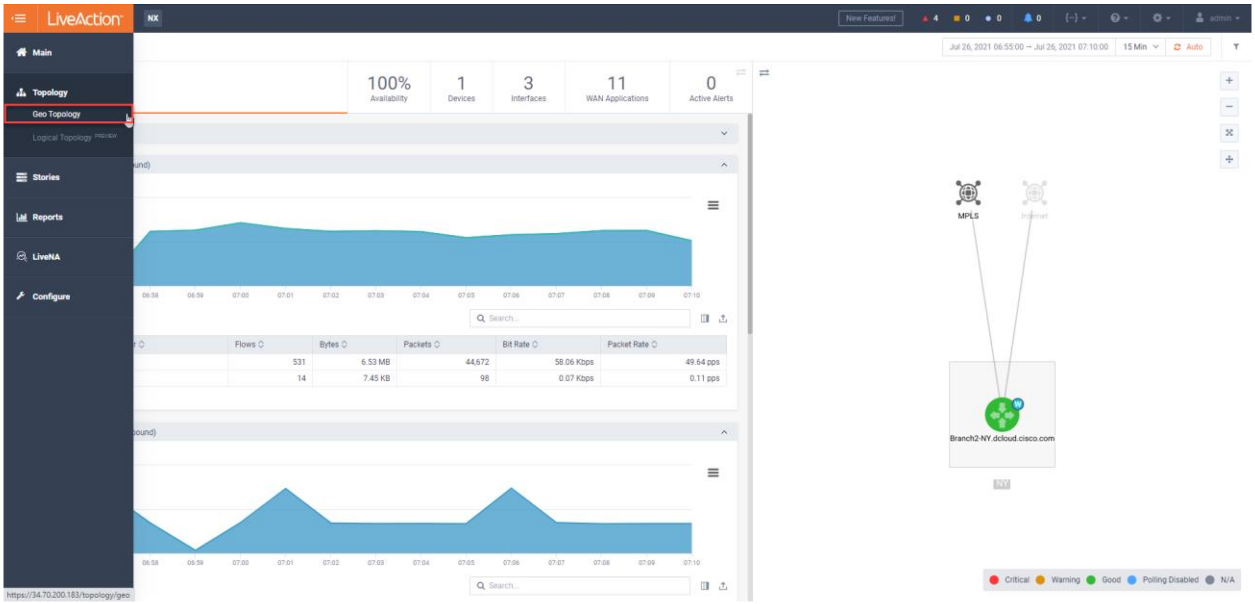


NY
Status: Good

100%	1	3	12	0
Availability	Devices	Interfaces	WAN Applications	Active Alerts

Legend	Service Provider	Flows	Bytes	Packets	Bit Rate	Packet Rate
🟦	MPLS	518	6.79 MB	46,802	60.32 Kbps	52.00 pps
🟩	Internet	13	6.99 KB	92	0.06 Kbps	0.10 pps

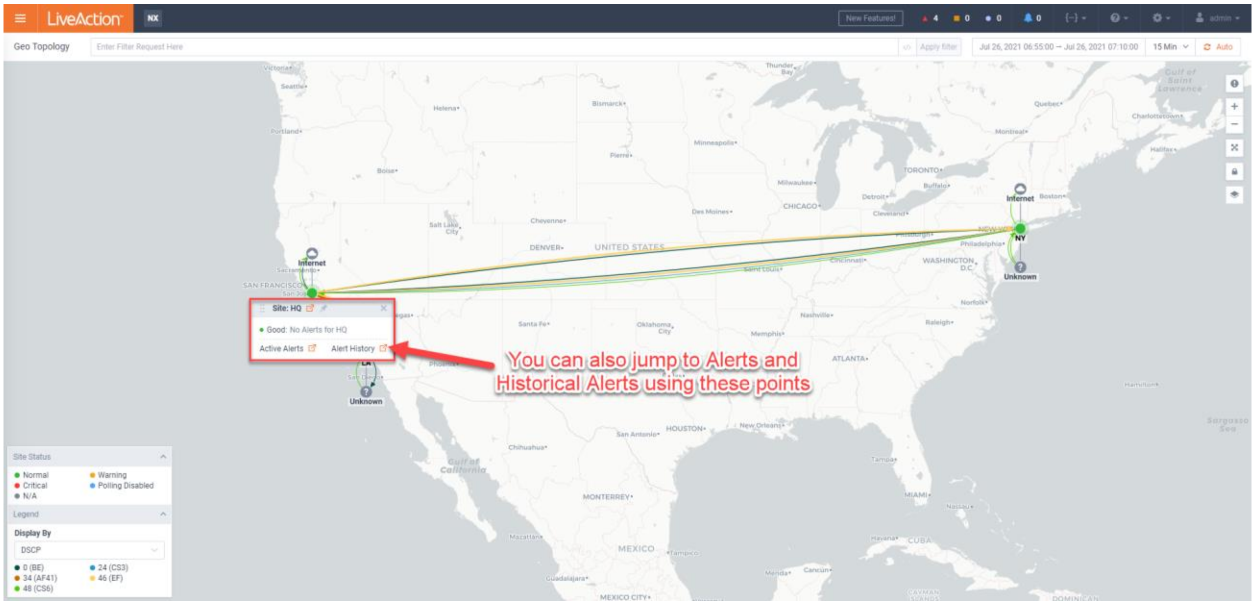
9. Select **Topology** > **Geo Topology**



100%	1	3	11	0
Availability	Devices	Interfaces	WAN Applications	Active Alerts

Flows	Bytes	Packets	Bit Rate	Packet Rate
531	6.53 MB	44,672	58.06 Kbps	49.64 pps
14	7.45 KB	98	0.07 Kbps	0.11 pps

10. Click on a Site to see additional information & links.



Jul 26, 2021 06:55:00 – Jul 26, 2021 07:10:00 15 Min

Site: HQ

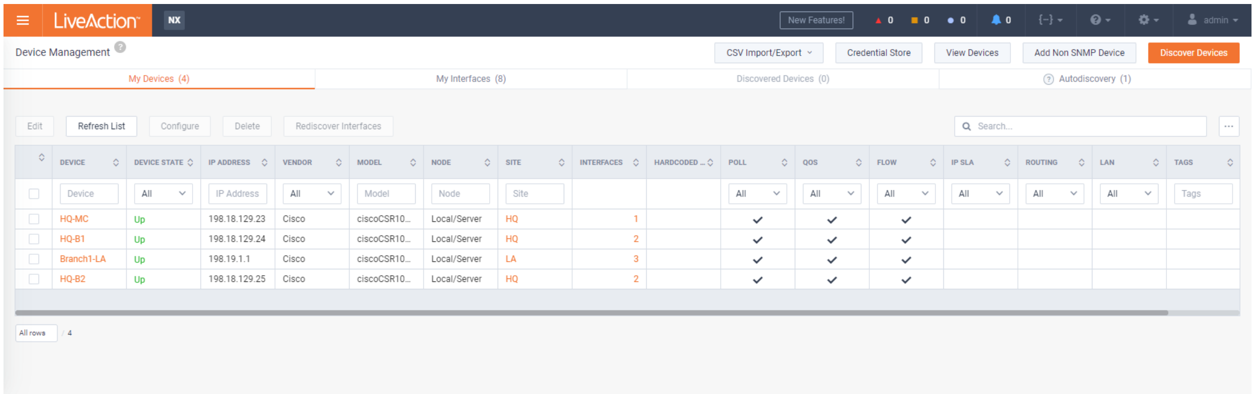
● Good: No Alerts for HQ

Active Alerts Alert History

You can also jump to Alerts and Historical Alerts using these points

11. Click on the **Menu** button in the upper left, then select **Configure** at the bottom.

12. Select **Device Management**.



	DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED ...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS
□	Device	All	IP Address	All	Model	Node	Site			All	All	All	All	All	All	Tags
□	HQ-MC	Up	198.18.129.23	Cisco	ciscoCSR10...	Local/Server	HQ	1		✓	✓	✓				
□	HQ-B1	Up	198.18.129.24	Cisco	ciscoCSR10...	Local/Server	HQ	2		✓	✓	✓				
□	Branch1-LA	Up	198.19.1.1	Cisco	ciscoCSR10...	Local/Server	LA	3		✓	✓	✓				
□	HQ-B2	Up	198.18.129.25	Cisco	ciscoCSR10...	Local/Server	HQ	2		✓	✓	✓				

See that you can add devices, and run Device Discovery, from the WebUI.   We'll run Discover Devices in a subsequent Lab.

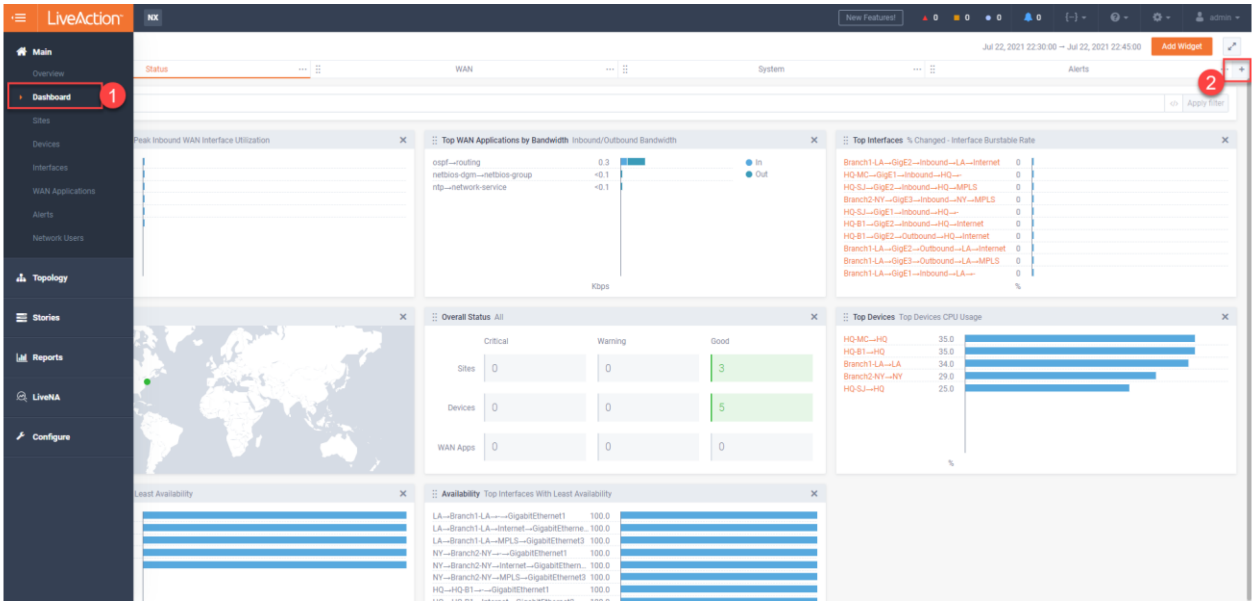
Lab 1.2: Create a Custom Dashboard

Note: The displays in these UI labs will vary, depending upon how long your Pod has been running, as well as the variety of traffic. These labs are meant to illustrate *how* to get at the information… results are not important. Diagrams are for illustration purposes and may not reflect the data you may view on the Training Pod.

In this Lab you will Create and Modify your own Custom Dashboard.

Lab Steps:

1. From the **Main** menu, click on **Dashboard** (1), then click on the **+** icon (2) to create a new tab in the dashboard space Dashboard. This will appear as “New Tab”.



Top WAN Applications by Bandwidth Inbound/Outbound Bandwidth

ospf→routing	0.3
netbios-dgm→netbios-group	<0.1
ntp→network-service	<0.1

Top Interfaces % Changed - Interface Burstable Rate

Branch1-LA→GigE2→Inbound→LA→Internet	0
HQ-MC→GigE1→Inbound→HQ→-	0
HQ-SJ→GigE2→Inbound→HQ→MPLS	0
Branch2-NY→GigE3→Inbound→NY→MPLS	0
HQ-SJ→GigE1→Inbound→HQ→-	0
HQ-B1→GigE2→Inbound→HQ→Internet	0
HQ-B1→GigE2→Outbound→HQ→Internet	0
Branch1-LA→GigE2→Outbound→LA→Internet	0
Branch1-LA→GigE3→Outbound→LA→MPLS	0
Branch1-LA→GigE1→Inbound→LA→-	0

Overall Status All

	Critical	Warning	Good
Sites	0	0	3
Devices	0	0	5
WAN Apps	0	0	0

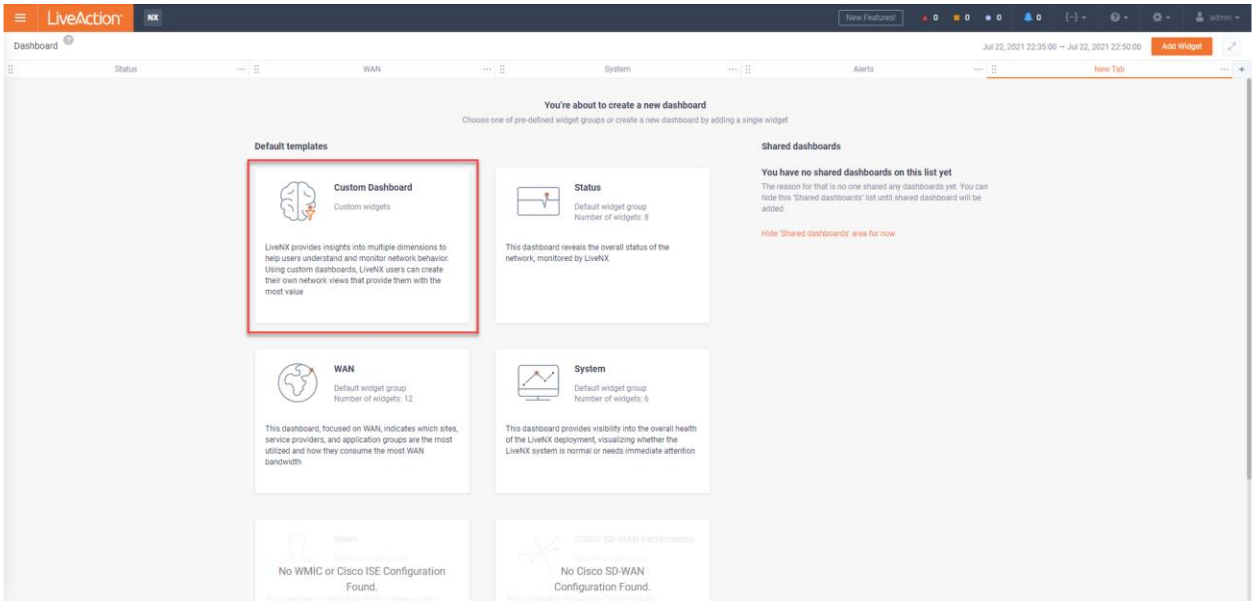
Top Devices Top Devices CPU Usage

HQ-MC→HQ	35.0
HQ-B1→HQ	35.0
Branch1-LA→LA	34.0
Branch2-NY→NY	29.0
HQ-SJ→HQ	25.0

Availability Top Interfaces With Least Availability

LA→Branch1-LA→-→GigabitEthernet1	100.0
LA→Branch1-LA→Internet→GigabitEtherne...	100.0
LA→Branch1-LA→MPLS→GigabitEthernet3	100.0
NY→Branch2-NY→-→GigabitEthernet1	100.0
NY→Branch2-NY→Internet→GigabitEthern...	100.0
NY→Branch2-NY→MPLS→GigabitEthernet3	100.0
HQ→HQ-B1→-→GigabitEthernet1	100.0

2. Click **Custom Dashboard** (marked in Red in the screenshot).



You're about to create a new dashboard

Choose one of pre-defined widget groups or create a new dashboard by adding a single widget

Default templates

Custom Dashboard
Custom widgets

LiveNX provides insights into multiple dimensions to help users understand and monitor network behavior. Using custom dashboards, LiveNX users can create their own network views that provide them with the most value

Status
Default widget group
Number of widgets: 8

This dashboard reveals the overall status of the network, monitored by LiveNX

WAN
Default widget group
Number of widgets: 12

This dashboard, focused on WAN, indicates which sites, service providers, and application groups are the most utilized and how they consume the most WAN bandwidth

System
Default widget group
Number of widgets: 6

This dashboard provides visibility into the overall health of the LiveNX deployment, visualizing whether the LiveNX system is normal or needs immediate attention

No WMIC or Cisco ISE Configuration Found.

No Cisco SD-WAN Configuration Found.

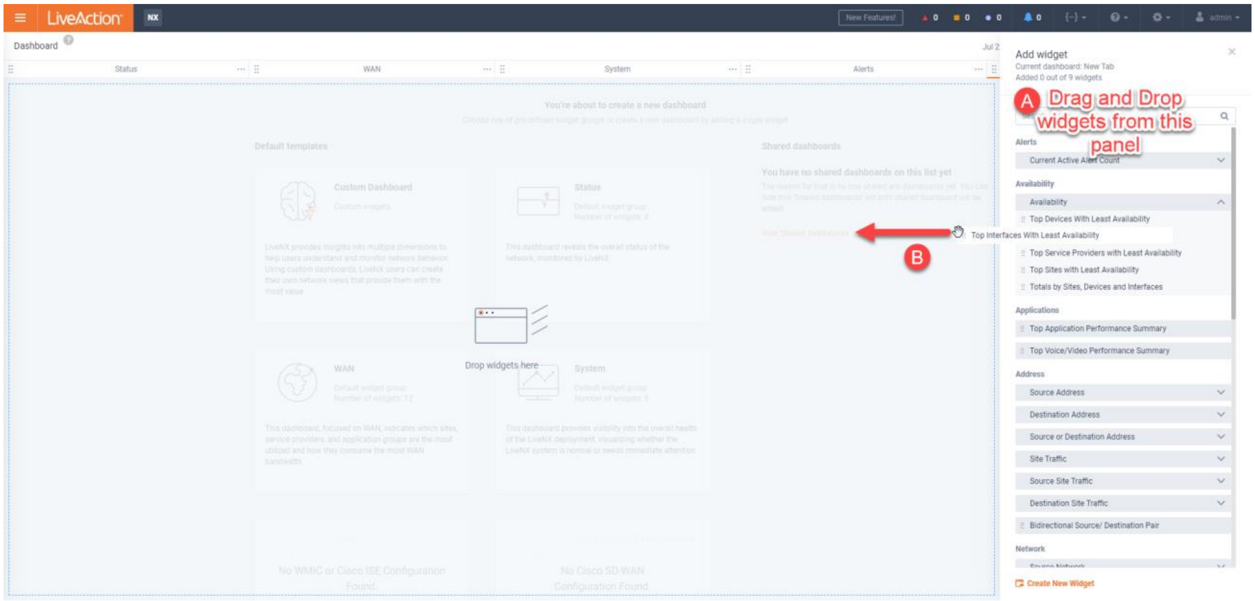
Shared dashboards

You have no shared dashboards on this list yet

The reason for that is no one shared any dashboards yet. You can hide this 'Shared dashboards' list until shared dashboard will be added.

Hide 'Shared dashboards' area for now

3. Some options can be expanded to show more details, while others can be directly dragged to the dashboard. Drag-and-drop (A) or click **+** to add Widgets to your custom dashboard.

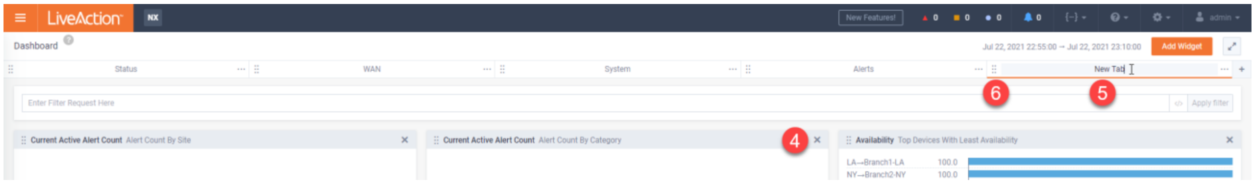

LiveAction
NX
New Features!
Dashboard
Status
WAN
System
Alerts
You're about to create a new dashboard
Default templates
Custom Dashboard
Status
WAN
System
Shared dashboards
You have no shared dashboards on this list yet
Drop widgets here
No WMIC or Cisco ISE Configuration Found
No Cisco SD-WAN Configuration Found
Add widget
Current dashboard: New Tab
Added 0 out of 9 widgets
A
Drag and Drop widgets from this panel
B
Alerts
Current Active Alert Count
Availability
Availability
Top Devices With Least Availability
Top Interfaces With Least Availability
Top Service Providers with Least Availability
Top Sites with Least Availability
Totals by Sites, Devices and Interfaces
Applications
Top Application Performance Summary
Top Voice/Video Performance Summary
Address
Source Address
Destination Address
Source or Destination Address
Site Traffic
Source Site Traffic
Destination Site Traffic
Bidirectional Source/ Destination Pair
Network
Create New Widget

Note: For the purposes of this Lab, you may choose any combination of widgets to add to your custom dashboard. You can add up to 9 widgets on a single Dashboard.

4. **Delete** un-wanted Widgets by clicking the **X** at top right of the widget.

5. To give the dashboard tab a more appropriate name, simply select the **New Tab** text and rename your dashboard.

6. You can also change the order


LiveAction
NX
New Features!
admin
Dashboard
Jul 22, 2021 22:55:00 → Jul 22, 2021 23:10:00
Add Widget
Status
WAN
System
Alerts
New Tab
6
5
Enter Filter Request Here
Apply filter
Current Active Alert Count Alert Count By Site
Current Active Alert Count Alert Count By Category
4
Availability Top Devices With Least Availability
LA→Branch1-LA 100.0
NY→Branch2-NY 100.0

You may edit or add to your Dashboard by using the Add Widget icon at the Top-Right.

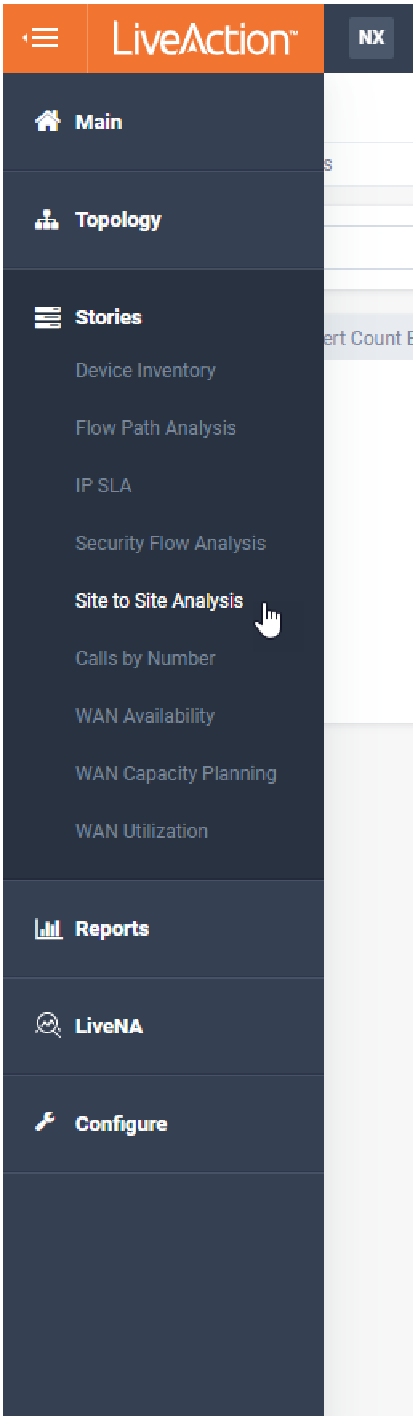
Note: Since LiveNX stores *breadcrumbs* it will retain a trail of the last page you've visited in the WebUI, based-upon your individual login credentials. Unless shared… Your custom Dashboard will not be visible to others.

Lab 1.3: Pre-Configured Stories

The LiveNX WebUI has several pre-configured *walk-thrus*, or Stories, built-in. These Stories may help you easily find specific workflows and statistical information regarding your monitored devices.

Lab Steps:

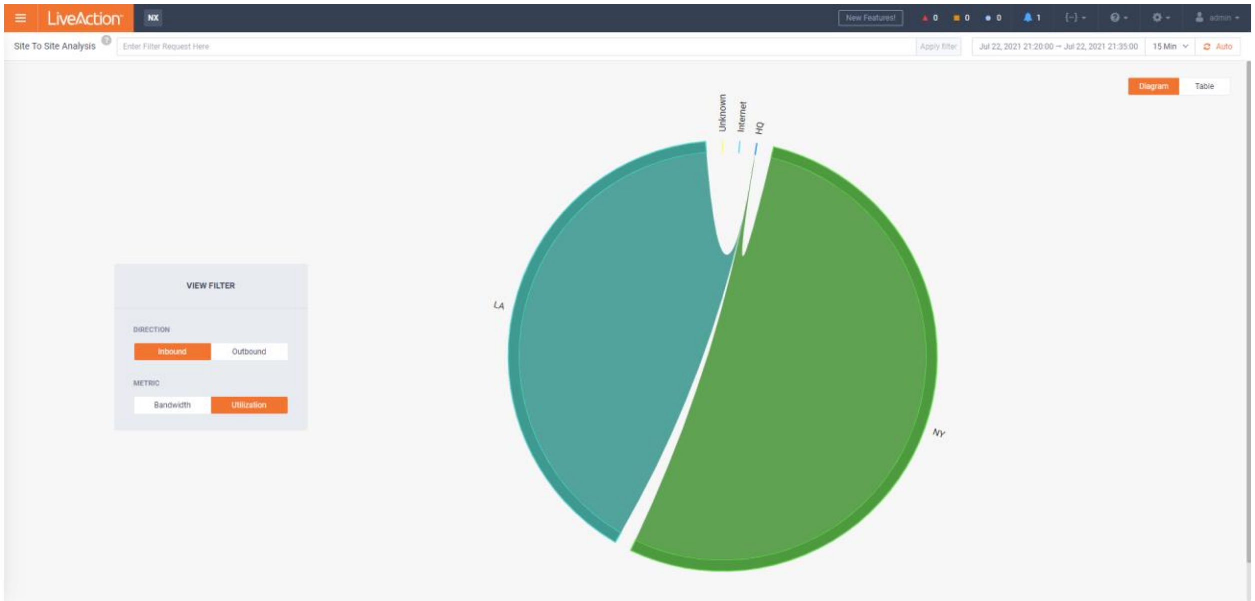
1. Click the **Menu** icon.
2. Select **Stories**, and **Site-to-Site Analysis**.



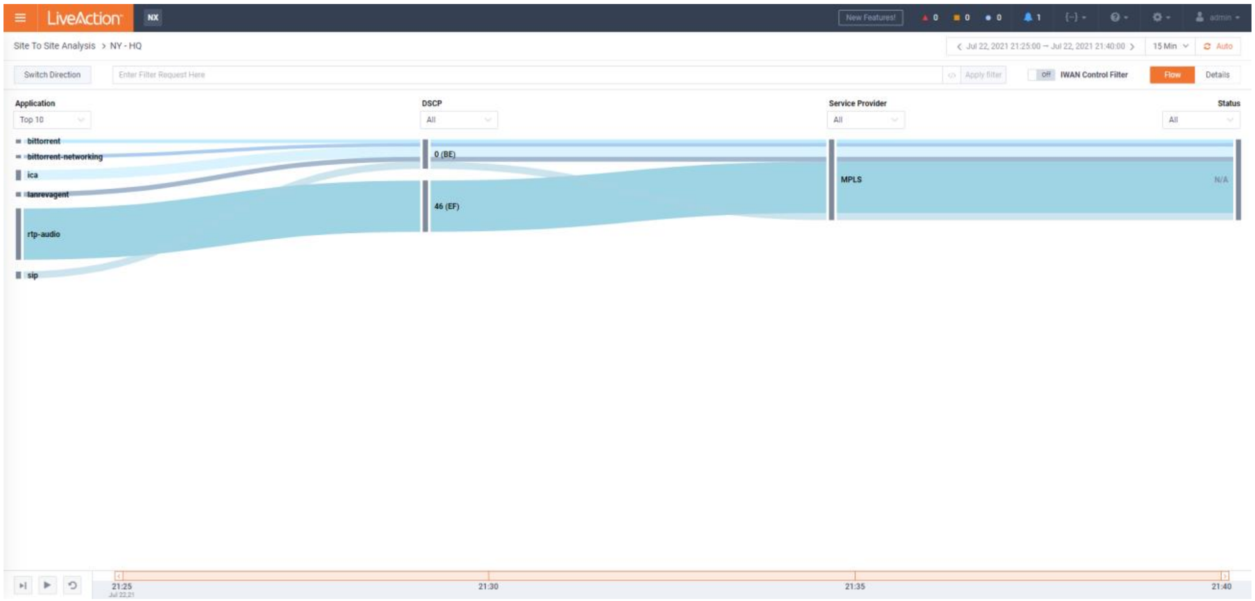
Note: Diagrams are for illustration purposes and may not reflect the data in your Training Pod. These labs are meant to illustrate *how* to get at the information.

3. Select **Direction > Inbound.**

DIAGRAM



4. **Hover-over** for Utilization info or **select** an area of the chart to display a **Sankey Flow Diagram**.



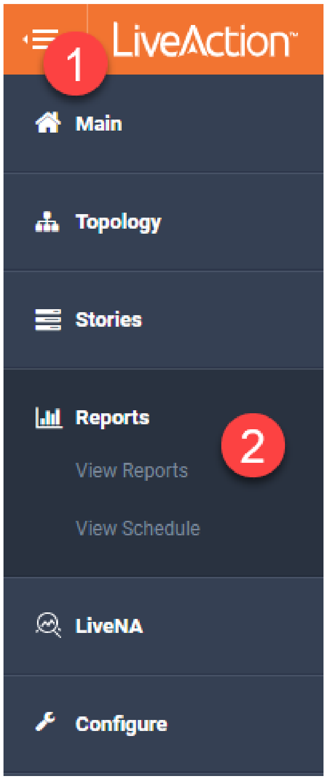
View the other pre-configured Stories to discover how they may help you with Capacity Planning, Inventory, and Network Management.

Lab 1.4: WebUI Reports

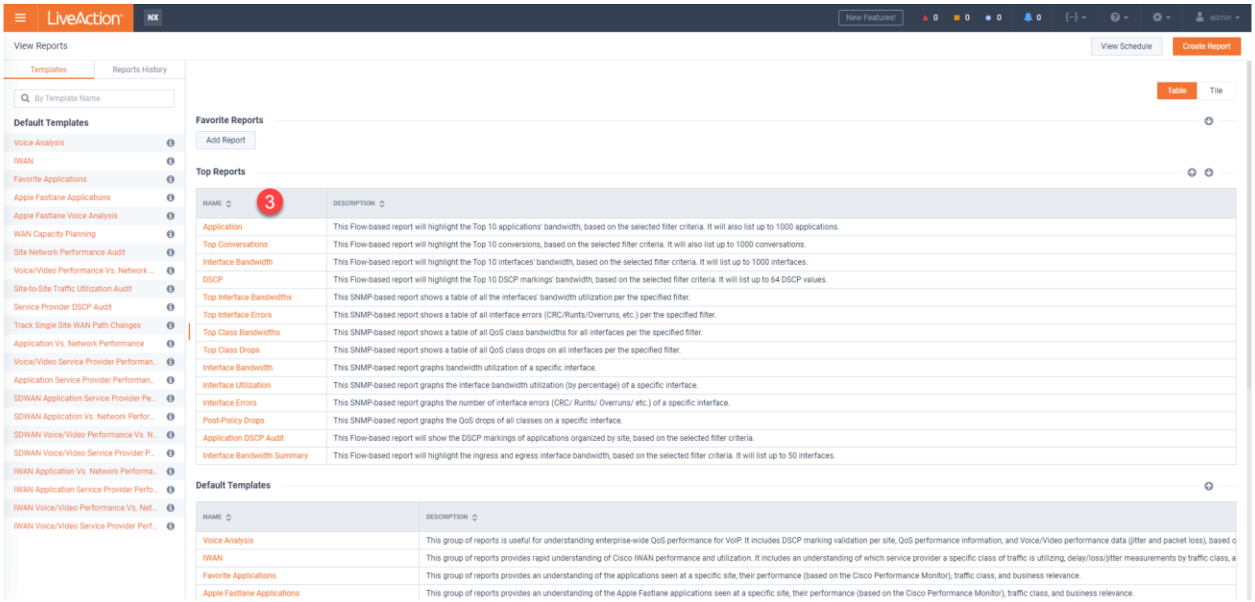
You may access any of the default reports in the WebUI, as well as utilize as a *template* any Dynamic Reports created in the LiveNX Client.

Lab Steps:

1. Click the **Menu** icon.



2. Select **Reports**, and **View Reports**.
3. From the Top Reports section, select **Application**



Default Templates

- Voice Analysis
- IWAN
- Favorite Applications
- Apple Fastlane Applications
- Apple Fastlane Voice Analysis
- WAN Capacity Planning
- Site Network Performance Audit
- Voice/Video Performance Vs. Network ...
- Site-to-Site Traffic Utilization Audit
- Service Provider DSCP Audit
- Track Single Site WAN Path Changes
- Application Vs. Network Performance
- Voice/Video Service Provider Performan...
- Application Service Provider Performan...
- SDWAN Application Service Provider Pe...
- SDWAN Application Vs. Network Perfor...
- SDWAN Voice/Video Performance Vs. N...
- SDWAN Voice/Video Service Provider P...
- IWAN Application Vs. Network Performa...
- IWAN Application Service Provider Perfo...
- IWAN Voice/Video Performance Vs. Net...
- IWAN Voice/Video Service Provider Perf...

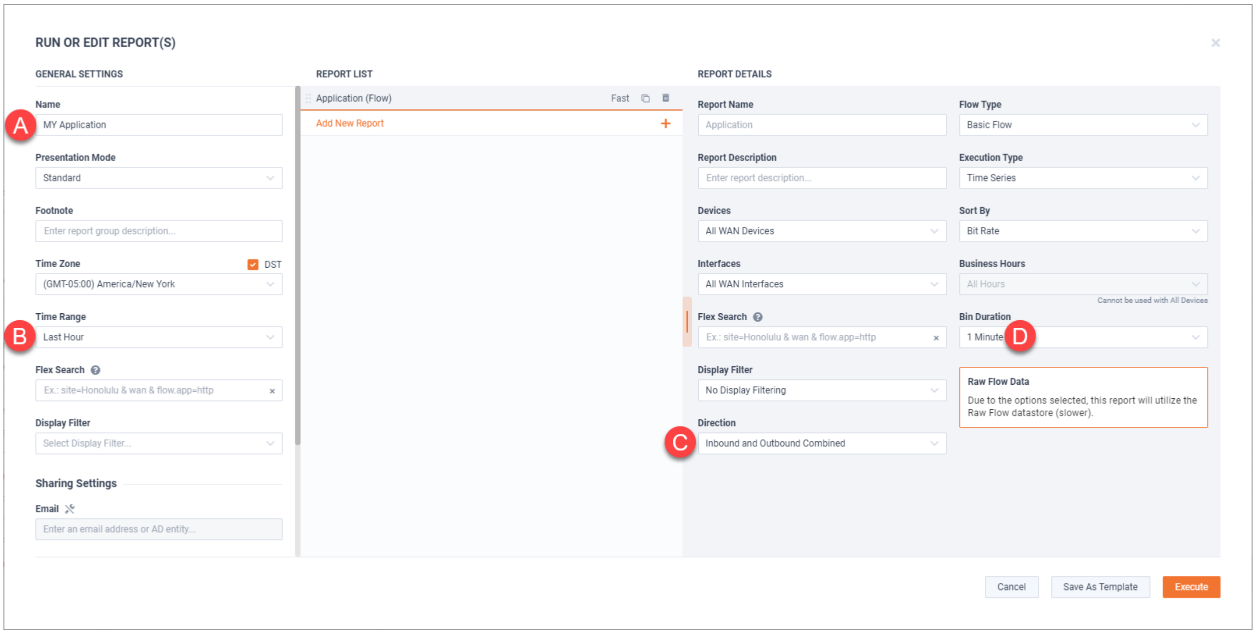
Favorite Reports

Top Reports

NAME	DESCRIPTION
Application	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.
Top Conversations	This Flow-based report will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.
Interface Bandwidth	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.
DSCP	This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
Top Interface Bandwidths	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.
Top Interface Errors	This SNMP-based report shows a table of all interface errors (CRC/Runts/Overruns, etc.) per the specified filter.
Top Class Bandwidths	This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.
Top Class Drops	This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.
Interface Bandwidth	This SNMP-based report graphs bandwidth utilization of a specific interface.
Interface Utilization	This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.
Interface Errors	This SNMP-based report graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.
Post-Policy Drops	This SNMP-based report graphs the QoS drops of all classes on a specific interface.
Application DSCP Audit	This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.
Interface Bandwidth Summary	This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.

Default Templates

NAME	DESCRIPTION
Voice Analysis	This group of reports is useful for understanding enterprise-wide QoS performance for VoIP. It includes DSCP marking validation per site, QoS performance information, and Voice/Video performance data (jitter and packet loss), based o
IWAN	This group of reports provides rapid understanding of Cisco IWAN performance and utilization. It includes an understanding of which service provider a specific class of traffic is utilizing, delay/loss/jitter measurements by traffic class, a
Favorite Applications	This group of reports provides an understanding of the applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic class, and business relevance.
Apple Fastlane Applications	This group of reports provides an understanding of the Apple Fastlane applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic class, and business relevance.



RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Name: MY Application

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone: (GMT-05:00) America/New York ☑ DST

Time Range: Last Hour

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

Display Filter: Select Display Filter...

Sharing Settings

Email: Enter an email address or AD entity...

REPORT LIST

Application (Flow) — Fast

Add New Report +

REPORT DETAILS

Report Name: Application

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

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

Bin Duration: 1 Minute

Display Filter: No Display Filtering

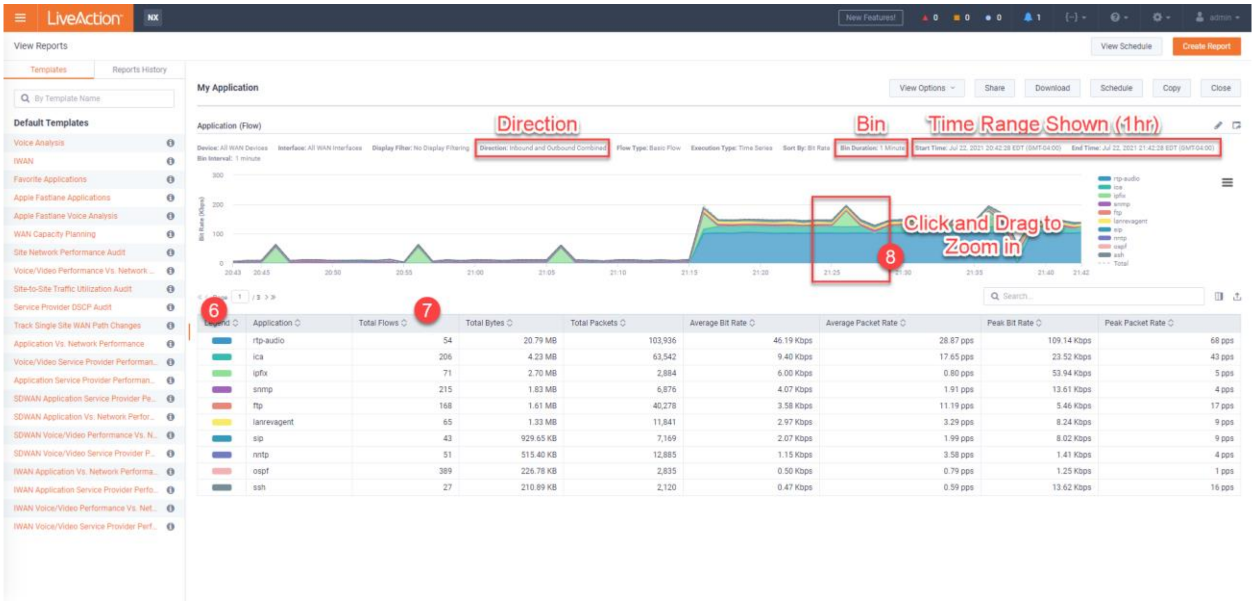
Direction: Inbound and Outbound Combined

Raw Flow Data

Due to the options selected, this report will utilize the Raw Flow datastore (slower).

4. Select Options.
   a. **Name**: My Application
   b. **Time Range**: Last Hour
   c. **Direction**: Inbound and Outbound Combined
   d. **Bin Duration**: 1 Minute

5. Click Execute.



Default Templates

- Voice Analysis
- IWAN
- Favorite Applications
- Apple Fastlane Applications
- Apple Fastlane Voice Analysis
- WAN Capacity Planning
- Site Network Performance Audit
- Voice/Video Performance Vs. Network ...
- Site-to-Site Traffic Utilization Audit
- Service Provider DSCP Audit
- Track Single Site WAN Path Changes
- Application Vs. Network Performance
- Voice/Video Service Provider Performan...
- Application Service Provider Performan...
- SDWAN Application Service Provider Pe...
- SDWAN Application Vs. Network Perfor...
- SDWAN Voice/Video Performance Vs. N...
- SDWAN Voice/Video Service Provider P...
- IWAN Application Vs. Network Performa...
- IWAN Application Service Provider Perfo...
- IWAN Voice/Video Performance Vs. Net...
- IWAN Voice/Video Service Provider Perf...

My Application

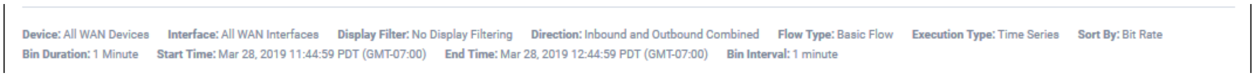
Application (Flow)

Device: All WAN Devices **Interface:** All WAN Interfaces **Display Filter:** No Display Filtering **Direction:** Inbound and Outbound Combined **Flow Type:** Basic Flow **Execution Type:** Time Series **Sort By:** Bit Rate **Bin Duration:** 1 Minute **Start Time:** Jul 22, 2021 20:42:28 EDT (GMT-04:00) **End Time:** Jul 22, 2021 21:42:28 EDT (GMT-04:00)
Bin Interval: 1 minute

Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
▬	rtp-audio	54	20.79 MB	103,936	46.19 Kbps	28.87 pps	109.14 Kbps	68 pps
▬	ica	206	4.23 MB	63,542	9.40 Kbps	17.65 pps	23.52 Kbps	43 pps
▬	ipfix	71	2.70 MB	2,884	6.00 Kbps	0.80 pps	53.94 Kbps	5 pps
▬	snmp	215	1.83 MB	6,876	4.07 Kbps	1.91 pps	13.61 Kbps	4 pps
▬	ftp	168	1.61 MB	40,278	3.58 Kbps	11.19 pps	5.46 Kbps	17 pps
▬	lanrevagent	65	1.33 MB	11,841	2.97 Kbps	3.29 pps	8.24 Kbps	9 pps
▬	sip	43	929.65 KB	7,169	2.07 Kbps	1.99 pps	8.02 Kbps	9 pps
▬	nntp	51	515.40 KB	12,885	1.15 Kbps	3.58 pps	1.41 Kbps	4 pps
▬	ospf	389	226.78 KB	2,835	0.50 Kbps	0.79 pps	1.25 Kbps	1 pps
▬	ssh	27	210.89 KB	2,120	0.47 Kbps	0.59 pps	13.62 Kbps	16 pps

This report displays all the applications transiting the network in the **past hour**, in table format, with color references for the top 10 items by Total Bytes. All reports display 10 metrics per display page.

Note the **Report Options** on the image.

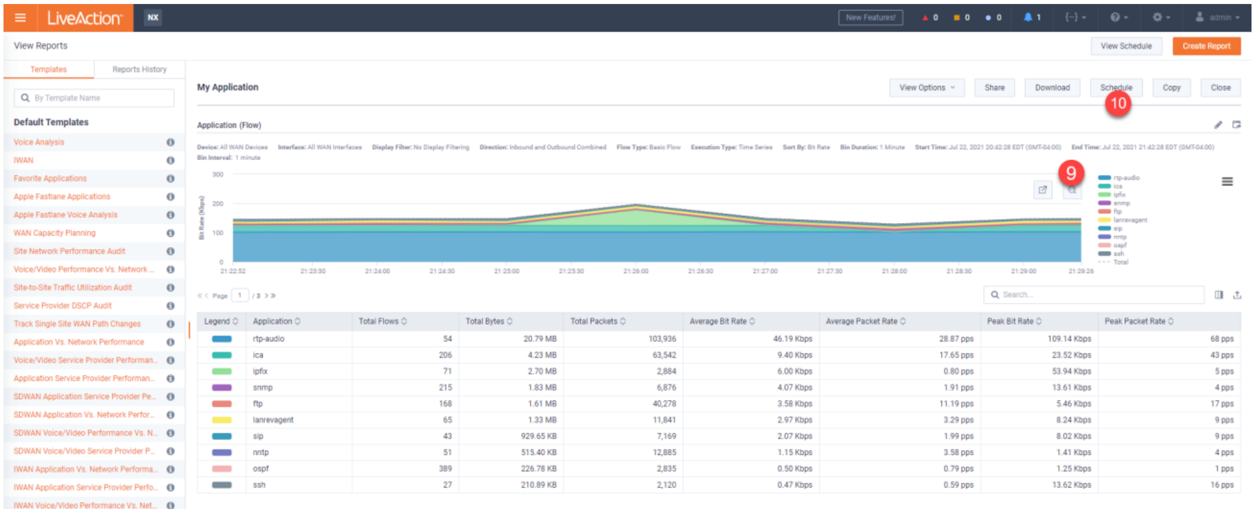


Device: All WAN Devices **Interface:** All WAN Interfaces **Display Filter:** No Display Filtering **Direction:** Inbound and Outbound Combined **Flow Type:** Basic Flow **Execution Type:** Time Series **Sort By:** Bit Rate
Bin Duration: 1 Minute **Start Time:** Mar 28, 2019 11:44:59 PDT (GMT-07:00) **End Time:** Mar 28, 2019 12:44:59 PDT (GMT-07:00) **Bin Interval:** 1 minute

6. **Hide** a metric by clicking on the Legend.

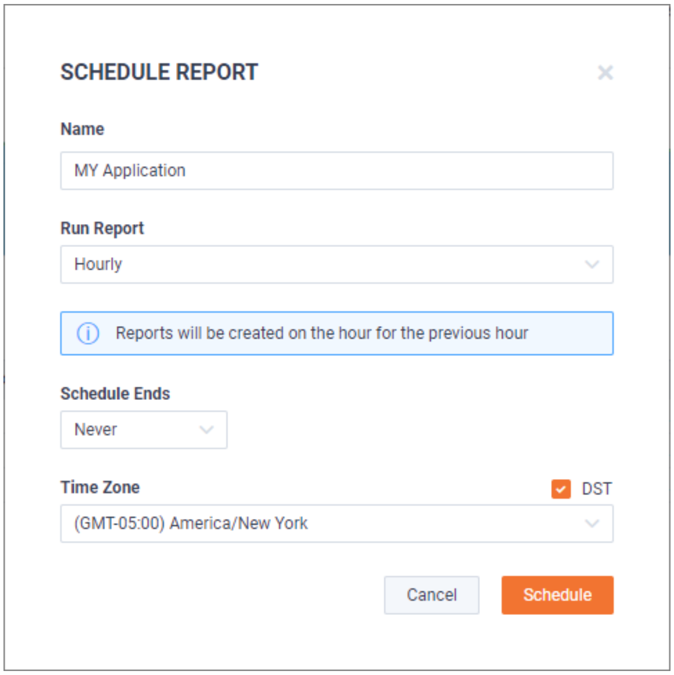
7. Re-sort by clicking on the **Sort Arrows**.

8. **Zoom-in** by Left-click-drag a portion of the chart.
9. **Reset** Zoom to normal.
10. **Schedule** the Report to run Hourly.


LiveAction
NX
New Features!
View Reports
View Schedule
Create Report
Templates
Reports History
By Template Name
Default Templates
Voice Analysis
IWAN
Favorite Applications
Apple Fastlane Applications
Apple Fastlane Voice Analysis
WAN Capacity Planning
Site Network Performance Audit
Voice/Video Performance Vs. Network ...
Site-to-Site Traffic Utilization Audit
Service Provider DSCP Audit
Track Single Site WAN Path Changes
Application Vs. Network Performance
Voice/Video Service Provider Performan...
Application Service Provider Performan...
SDWAN Application Service Provider Pe...
SDWAN Application Vs. Network Perfor...
SDWAN Voice/Video Performance Vs. N...
SDWAN Voice/Video Service Provider P...
IWAN Application Vs. Network Performa...
IWAN Application Service Provider Perfo...
IWAN Voice/Video Performance Vs. Net...
My Application
View Options
Share
Download
Schedule
Copy
Close
10
Application (Flow)
9
300
200
100
0
Bit Rate (Kbps)
21:22:52
21:23:30
21:24:00
21:24:30
21:25:00
21:25:30
21:26:00
21:26:30
21:27:00
21:27:30
21:28:00
21:28:30
21:29:00
21:29:26
rtp-audio
ica
ipfix
snmp
ftp
lanrevagent
sip
nntp
ospf
ssh
Total
Page 1 / 3
Search...

Device: All WAN Devices **Interface:** All WAN Interfaces **Display Filter:** No Display Filtering **Direction:** Inbound and Outbound Combined **Flow Type:** Basic Flow **Execution Type:** Time Series **Sort By:** Bit Rate **Bin Duration:** 1 Minute **Start Time:** Jul 22, 2021 20:42:28 EDT (GMT-04:00) **End Time:** Jul 22, 2021 21:42:28 EDT (GMT-04:00)
Bin Interval: 1 minute

Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
🟦	rtp-audio	54	20.79 MB	103,936	46.19 Kbps	28.87 pps	109.14 Kbps	68 pps
🟩	ica	206	4.23 MB	63,542	9.40 Kbps	17.65 pps	23.52 Kbps	43 pps
🟩	ipfix	71	2.70 MB	2,884	6.00 Kbps	0.80 pps	53.94 Kbps	5 pps
🟪	snmp	215	1.83 MB	6,876	4.07 Kbps	1.91 pps	13.61 Kbps	4 pps
🟥	ftp	168	1.61 MB	40,278	3.58 Kbps	11.19 pps	5.46 Kbps	17 pps
🟨	lanrevagent	65	1.33 MB	11,841	2.97 Kbps	3.29 pps	8.24 Kbps	9 pps
🟦	sip	43	929.65 KB	7,169	2.07 Kbps	1.99 pps	8.02 Kbps	9 pps
🟪	nntp	51	515.40 KB	12,885	1.15 Kbps	3.58 pps	1.41 Kbps	4 pps
🟥	ospf	389	226.78 KB	2,835	0.50 Kbps	0.79 pps	1.25 Kbps	1 pps
⬛	ssh	27	210.89 KB	2,120	0.47 Kbps	0.59 pps	13.62 Kbps	16 pps



SCHEDULE REPORT

Name

MY Application

Run Report

Hourly

ⓘ Reports will be created on the hour for the previous hour

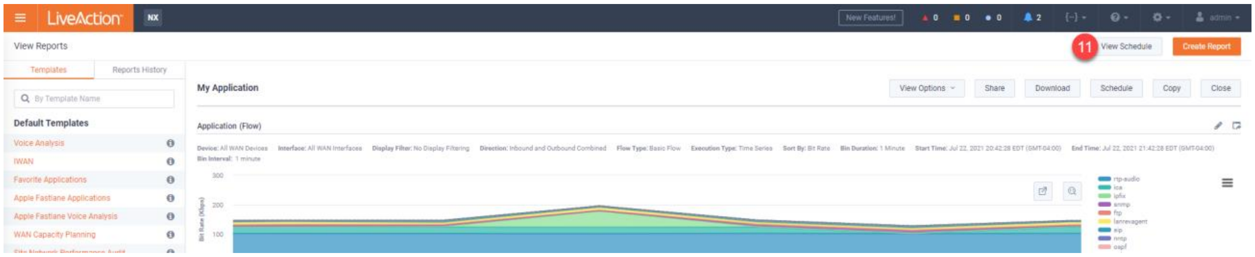
Schedule Ends

Never

Time Zone ☑ DST

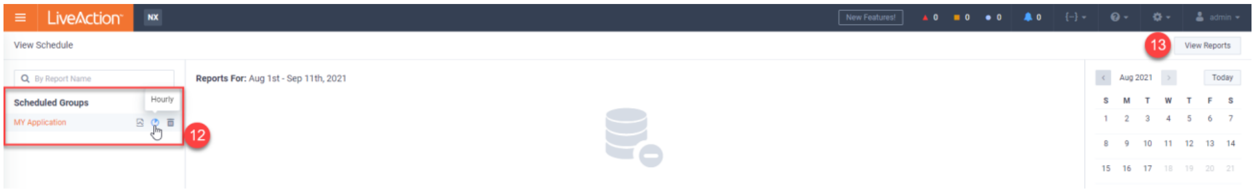
(GMT-05:00) America/New York

11. Verify that the report is now scheduled by navigating to **View Schedule.**



Device: All WAN Devices **Interface:** All WAN Interfaces **Display Filter:** No Display Filtering **Direction:** Inbound and Outbound Combined **Flow Type:** Basic Flow **Execution Type:** Time Series **Sort By:** Bit Rate **Bin Duration:** 1 Minute **Start Time:** Jul 22, 2021 20:42:28 EDT (GMT-04:00) **End Time:** Jul 22, 2021 21:42:28 EDT (GMT-04:00)
Bin Interval: 1 minute

12. Within this list you can see any report previously scheduled.

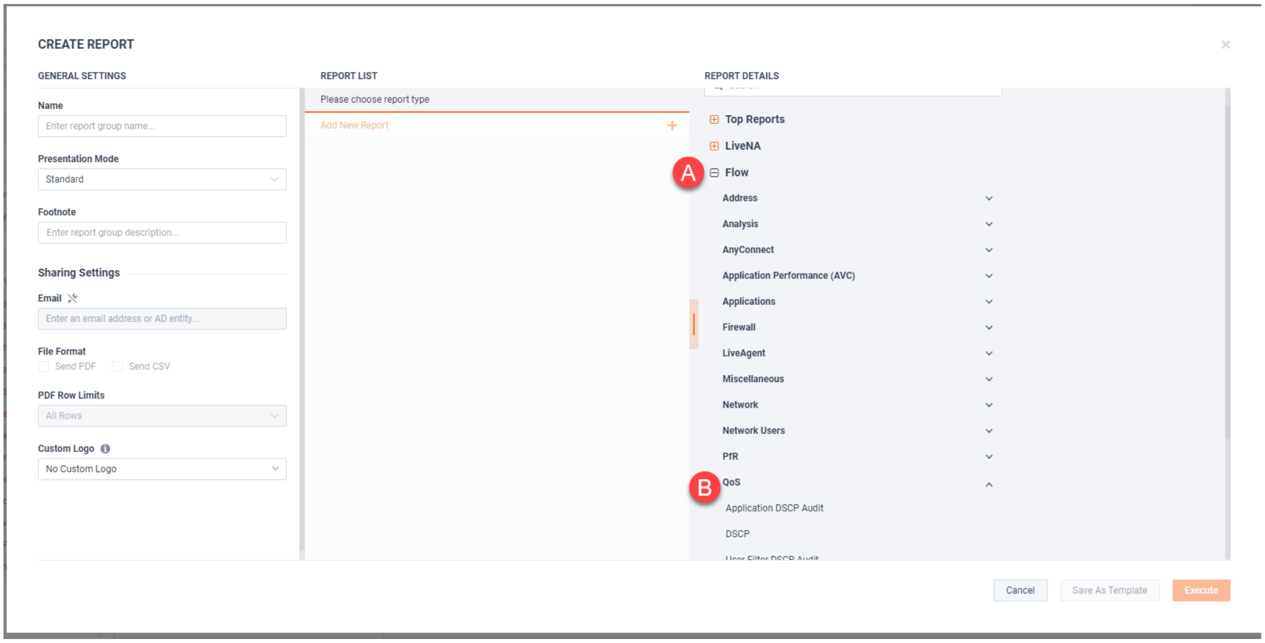


Reports For: Aug 1st - Sep 11th, 2021

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

Lets have a look at creating a **Custom Report**

13. Navigate back to reports by clicking **Reports > View Reports**.
14. Click **Create Report** (top right of screen)
15. Expand (A) **Flow** and then expand (B) **QoS.**



Name: Enter report group name...

Presentation Mode: Standard

Footnote: Enter report group description...

Sharing Settings

Email: Enter an email address or AD entity...

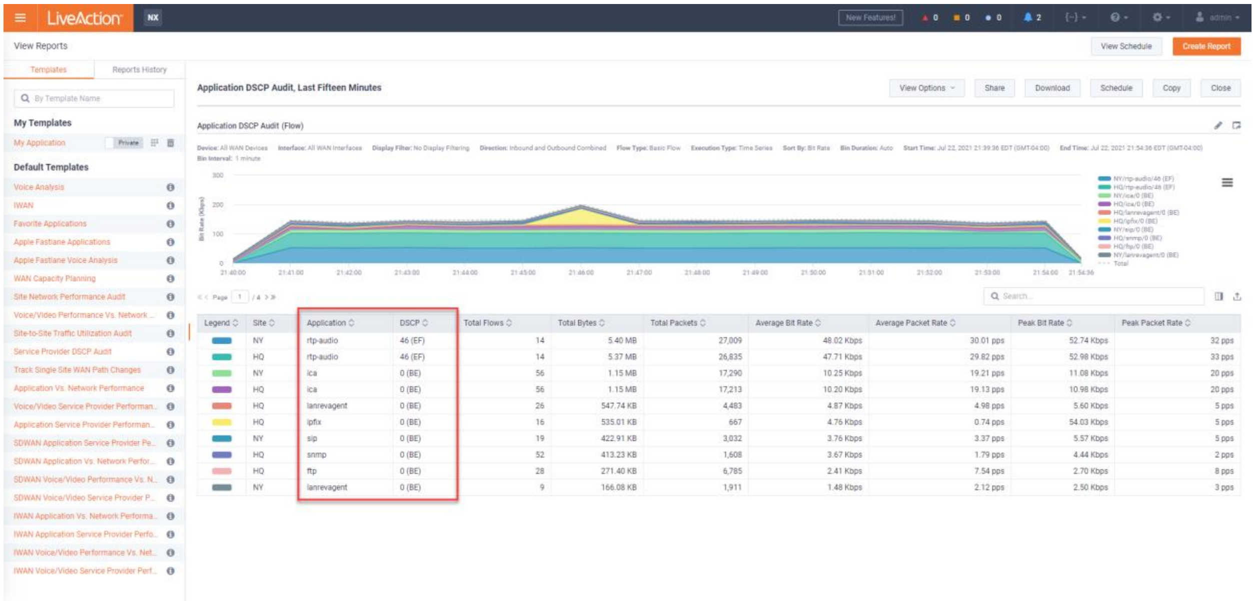
File Format: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

Custom Logo: No Custom Logo

Please choose report type

16. Select **Application DSCP Audit.**
17. Click **Execute**.
18. Verify the Application to DSCP values


LiveAction
NX
New Features!
admin
View Reports
View Schedule
Create Report
Templates
Reports History
By Template Name
My Templates
My Application
Private
Default Templates
Voice Analysis
IWAN
Favorite Applications
Apple Fastlane Applications
Apple Fastlane Voice Analysis
WAN Capacity Planning
Site Network Performance Audit
Voice/Video Performance Vs. Network ...
Site-to-Site Traffic Utilization Audit
Service Provider DSCP Audit
Track Single Site WAN Path Changes
Application Vs. Network Performance
Voice/Video Service Provider Performan...
Application Service Provider Performan...
SDWAN Application Service Provider Pe...
SDWAN Application Vs. Network Perfor...
SDWAN Voice/Video Performance Vs. N...
SDWAN Voice/Video Service Provider P...
IWAN Application Vs. Network Performa...
IWAN Application Service Provider Perfo...
IWAN Voice/Video Performance Vs. Net...
IWAN Voice/Video Service Provider Perf...
View Options
Share
Download
Schedule
Copy
Close
Bit Rate (Kbps)
300
200
100
0
21:40:00
21:41:00
21:42:00
21:43:00
21:44:00
21:45:00
21:46:00
21:47:00
21:48:00
21:49:00
21:50:00
21:51:00
21:52:00
21:53:00
21:54:00
21:54:36
NY/rtp-audio/46 (EF)
HQ/rtp-audio/46 (EF)
NY/ica/0 (BE)
HQ/ica/0 (BE)
HQ/lanrevagent/0 (BE)
HQ/ipfix/0 (BE)
NY/sip/0 (BE)
HQ/snmp/0 (BE)
HQ/ftp/0 (BE)
NY/lanrevagent/0 (BE)
Total
Page 1 / 4
Search...

Application DSCP Audit, Last Fifteen Minutes

Application DSCP Audit (Flow)

Device: All WAN Devices Interface: All WAN Interfaces Display Filter: No Display Filtering Direction: Inbound and Outbound Combined Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Bin Duration: Auto Start Time: Jul 22, 2021 21:39:36 EDT (GMT-04:00) End Time: Jul 22, 2021 21:54:36 EDT (GMT-04:00) Bin Interval: 1 minute

Legend	Site	Application	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
▬	NY	rtp-audio	46 (EF)	14	5.40 MB	27,009	48.02 Kbps	30.01 pps	52.74 Kbps	32 pps
▬	HQ	rtp-audio	46 (EF)	14	5.37 MB	26,835	47.71 Kbps	29.82 pps	52.98 Kbps	33 pps
▬	NY	ica	0 (BE)	56	1.15 MB	17,290	10.25 Kbps	19.21 pps	11.08 Kbps	20 pps
▬	HQ	ica	0 (BE)	56	1.15 MB	17,213	10.20 Kbps	19.13 pps	10.98 Kbps	20 pps
▬	HQ	lanrevagent	0 (BE)	26	547.74 KB	4,483	4.87 Kbps	4.98 pps	5.60 Kbps	5 pps
▬	HQ	ipfix	0 (BE)	16	535.01 KB	667	4.76 Kbps	0.74 pps	54.03 Kbps	5 pps
▬	NY	sip	0 (BE)	19	422.91 KB	3,032	3.76 Kbps	3.37 pps	5.57 Kbps	5 pps
▬	HQ	snmp	0 (BE)	52	413.23 KB	1,608	3.67 Kbps	1.79 pps	4.44 Kbps	2 pps
▬	HQ	ftp	0 (BE)	28	271.40 KB	6,785	2.41 Kbps	7.54 pps	2.70 Kbps	8 pps
▬	NY	lanrevagent	0 (BE)	9	166.08 KB	1,911	1.48 Kbps	2.12 pps	2.50 Kbps	3 pps

Lab 1.5: Enable / Customize Alerts

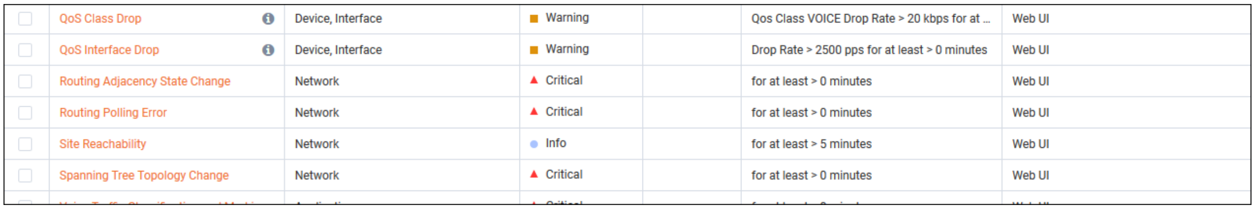
The LiveNX Alert System is able to visually, or via email, inform you if there is any anomolous behavior or issues with your monitored devices. A wide variety of issues may be brought to the attention of users with LiveNX Alerts.

Note: By default, no alerts are enabled during initial LiveNX installation. It is up to the administrator to turn on alerts & notifications.

In this Lab you'll enable and customize alerting for Voice or Video packet drops.

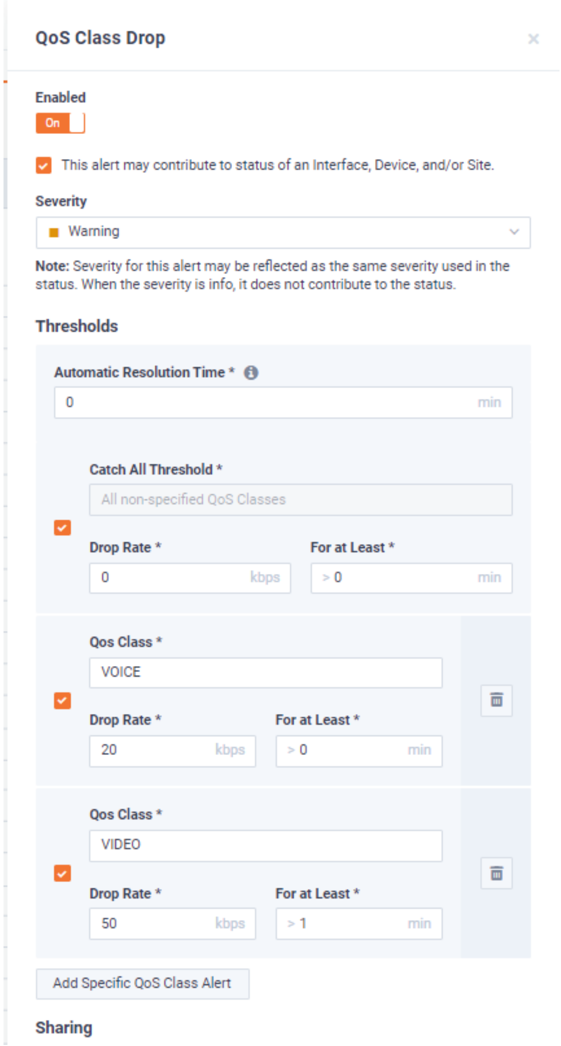
Lab Steps:

1. Click the **Menu** icon.
2. Select **Configure**, and **Alert Management**.



□	QoS Class Drop ⓘ	Device, Interface	■ Warning		Qos Class VOICE Drop Rate > 20 kbps for at ...	Web UI
□	QoS Interface Drop ⓘ	Device, Interface	■ Warning		Drop Rate > 2500 pps for at least > 0 minutes	Web UI
□	Routing Adjacency State Change	Network	▲ Critical		for at least > 0 minutes	Web UI
□	Routing Polling Error	Network	▲ Critical		for at least > 0 minutes	Web UI
□	Site Reachability	Network	● Info		for at least > 5 minutes	Web UI
□	Spanning Tree Topology Change	Network	▲ Critical		for at least > 0 minutes	Web UI

3. Click on **QoS Class Drop**.



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 *: 0 kbps — For at Least *: > 0 min

☑ 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 Specific QoS Class Alert

Sharing

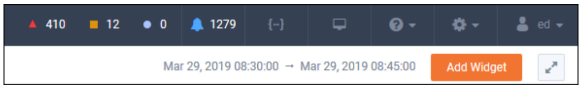
4. Select to **Enable** this alert.

5. Change the Severity if desired.
6. **Enter** QoS Class “VOICE”.
7. **Define** a DROP RATE of 20.
8. Leave FOR AT LEAST of “0”.

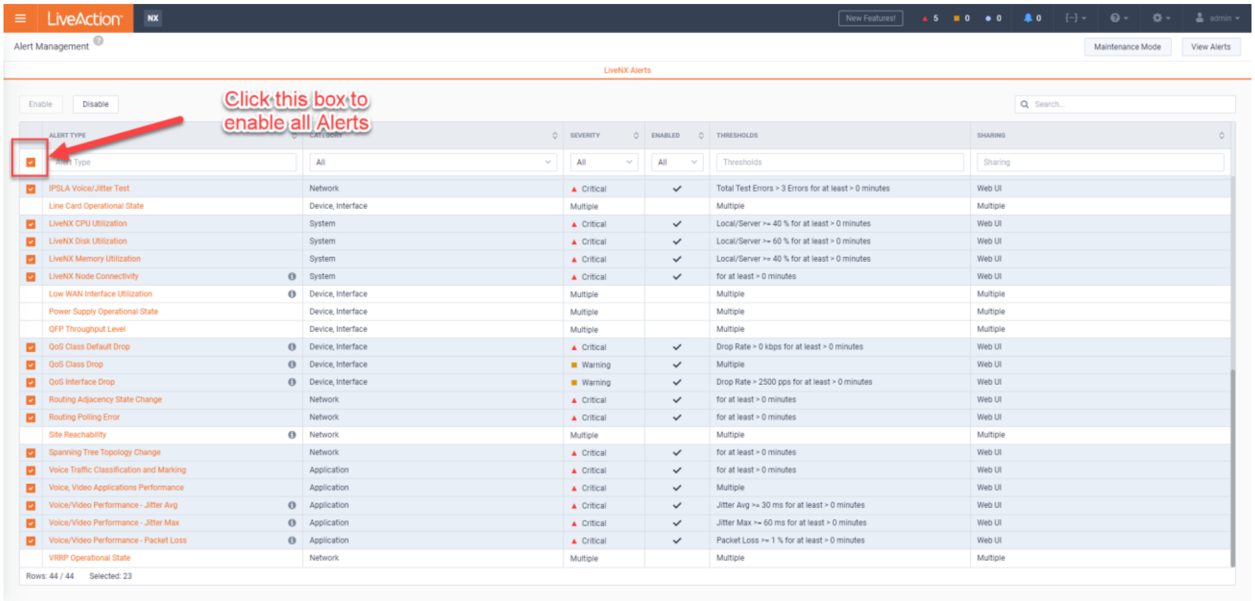
Note: The effect of 0 mins means ANY occurrence will trigger the alert.

9. Click **Add More**
10. Enter **QoS Class** “VIDEO”.
11. Define a **DROP RATE** of “50”.
12. **Define** the interval of “1” min.
13. Click **Save**.

Although you may not see immediate alerts based-upon this customization… future QoS Labs will activate this alert… depending upon traffic reply on the Training Pod. Alerts notification is at the top of the WebUI.



14. Enable ALL alerts (This is for use in a later Lab).



Click this box to enable all Alerts

	ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING
☑	Alert Type	All	All	All	Thresholds	Sharing
☑	IPSLA Voice/Jitter Test	Network	▲ Critical	✓	Total Test Errors > 3 Errors for at least > 0 minutes	Web UI
	Line Card Operational State	Device, Interface	Multiple		Multiple	Multiple
☑	LiveNX CPU Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least > 0 minutes	Web UI
☑	LiveNX Disk Utilization	System	▲ Critical	✓	Local/Server >= 60 % for at least > 0 minutes	Web UI
☑	LiveNX Memory Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least > 0 minutes	Web UI
☑	LiveNX Node Connectivity ℹ	System	▲ Critical	✓	for at least > 0 minutes	Web UI
	Low WAN Interface Utilization ℹ	Device, Interface	Multiple		Multiple	Multiple
	Power Supply Operational State	Device, Interface	Multiple		Multiple	Multiple
	QFP Throughput Level	Device, Interface	Multiple		Multiple	Multiple
☑	QoS Class Default Drop ℹ	Device, Interface	▲ Critical	✓	Drop Rate > 0 kbps for at least > 0 minutes	Web UI
☑	QoS Class Drop ℹ	Device, Interface	■ Warning	✓	Multiple	Web UI
☑	QoS Interface Drop ℹ	Device, Interface	■ Warning	✓	Drop Rate > 2500 pps for at least > 0 minutes	Web UI
☑	Routing Adjacency State Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI
☑	Routing Polling Error	Network	▲ Critical	✓	for at least > 0 minutes	Web UI
	Site Reachability ℹ	Network	Multiple		Multiple	Multiple
☑	Spanning Tree Topology Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI
☑	Voice Traffic Classification and Marking	Application	▲ Critical	✓	for at least > 0 minutes	Web UI
☑	Voice, Video Applications Performance	Application	▲ Critical	✓	Multiple	Web UI
☑	Voice/Video Performance - Jitter Avg ℹ	Application	▲ Critical	✓	Jitter Avg >= 30 ms for at least > 0 minutes	Web UI
☑	Voice/Video Performance - Jitter Max ℹ	Application	▲ Critical	✓	Jitter Max >= 60 ms for at least > 0 minutes	Web UI
☑	Voice/Video Performance - Packet Loss ℹ	Application	▲ Critical	✓	Packet Loss >= 1 % for at least > 0 minutes	Web UI
	VRRP Operational State	Network	Multiple		Multiple	Multiple

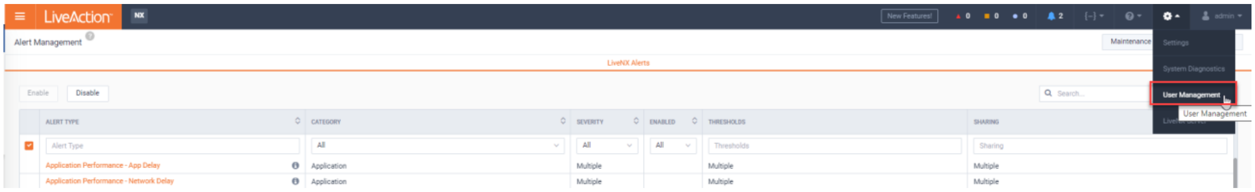
Rows: 44 / 44 Selected: 23

Lab 1.6: Add a User Account

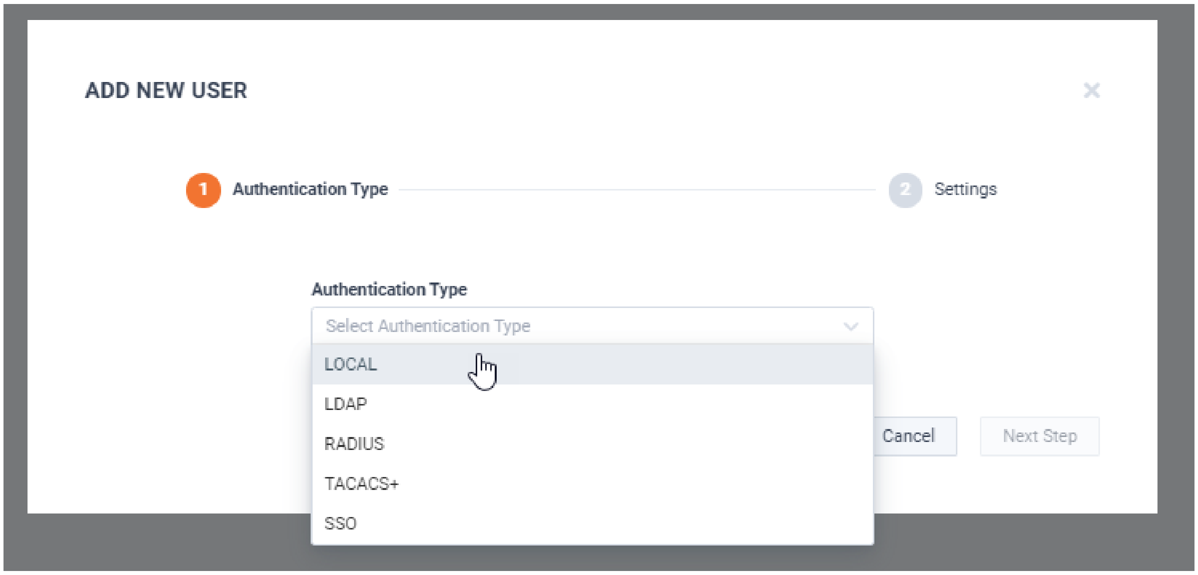
One of the first things to do after installing LiveNX is to grant additional user access, as well as to ensure that if you lose the credentials for the initial admin account, you will be able to login with appropriate privileges with a backup account.

Lab Steps:

1. In the Browser interface, click on the gear icon to configure, select Users Management



2. Click **Add User.**
3. For this exercise we will add a **Local** user.



4. Enter a **username** and a **Display Name** (something you'll remember).
5. Select the **Admin** role from the **Group** drop-down, and a **Session Timeout** value.
6. Enter a **password** (again, something you'll remember or write down). Re-enter the password for **confirmation**.

Note: On first login the user will be prompted to change the initial password.

7. Click **Add User**.

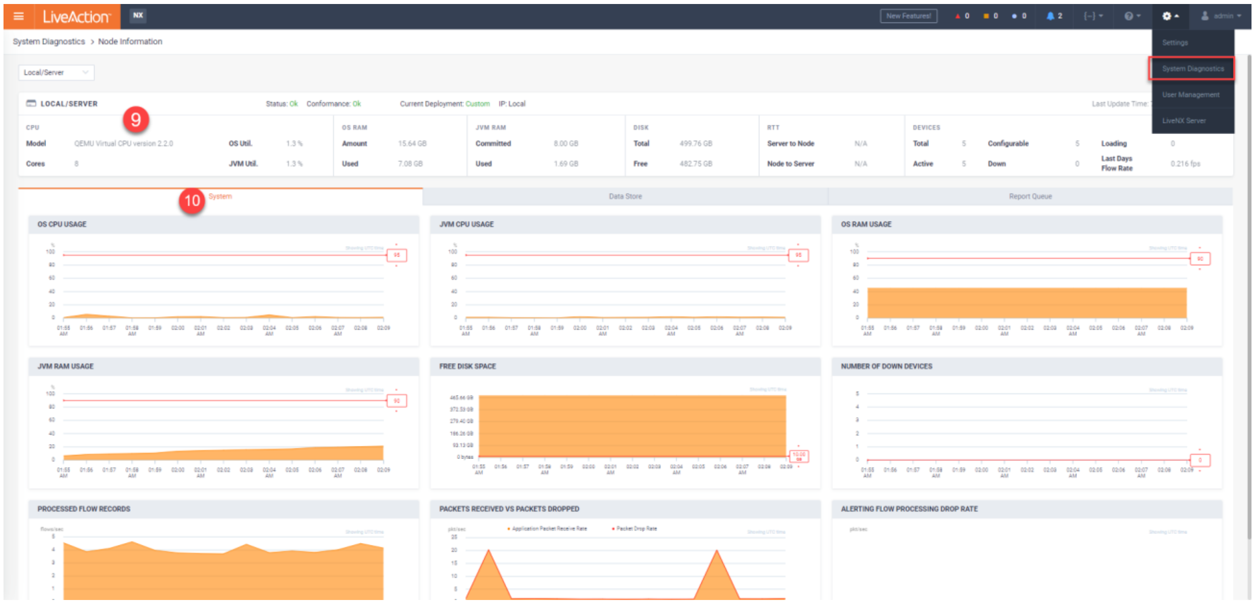
Note: You now have a backup login in case you forget the administrator credentials. **Throughout the remainder of this class**, we will use the credentials associated with the *admin* login.

Lab 1.7: View and Navigate System Diagnostics

Within System Diagnostics, System health, Data store and report queue are viewable.

Lab Steps:

8. In the Browser interface, click on the gear icon to configure, select System Diagnostics.
9. Click anywhere in the Local/Server to expand the details of the server.

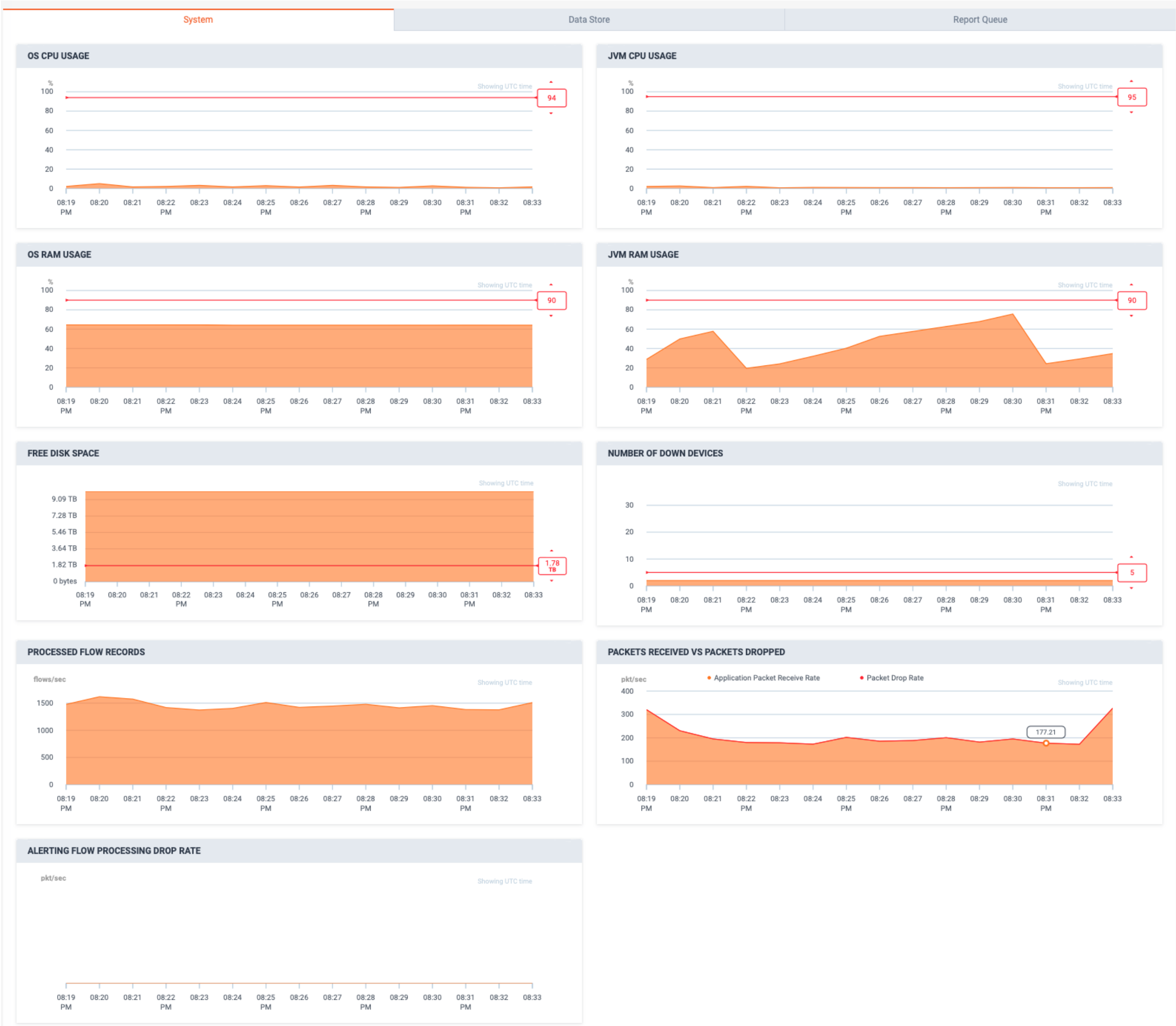


LOCAL/SERVER Status: Ok Conformance: Ok Current Deployment: Custom IP: Local Last Update Time:

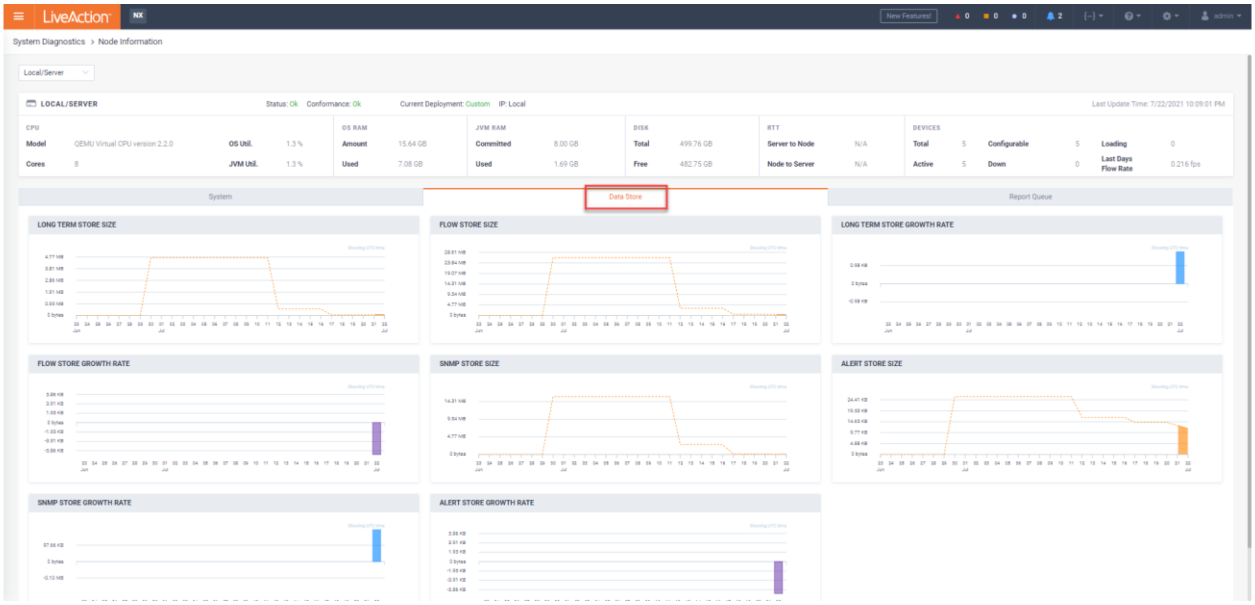
CPU				OS RAM		JVM RAM		DISK		RTT		DEVICES					
Model	QEMU Virtual CPU version 2.2.0	OS Util.	1.3 %	Amount	15.64 GB	Committed	8.00 GB	Total	499.76 GB	Server to Node	N/A	Total	5	Configurable	5	Loading	0
Cores	8	JVM Util.	1.3 %	Used	7.08 GB	Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5	Down	0	Last Days Flow Rate	0.216 fps

Note: If you have additional nodes, there will be multiple entries for each additional node and the details for those nodes can be seen as well.

10. Within the expanded server information are three tabs.
11. **System** tab will show you CPU usage, RAM usage, Disk Space, Down Devices and Flow details.



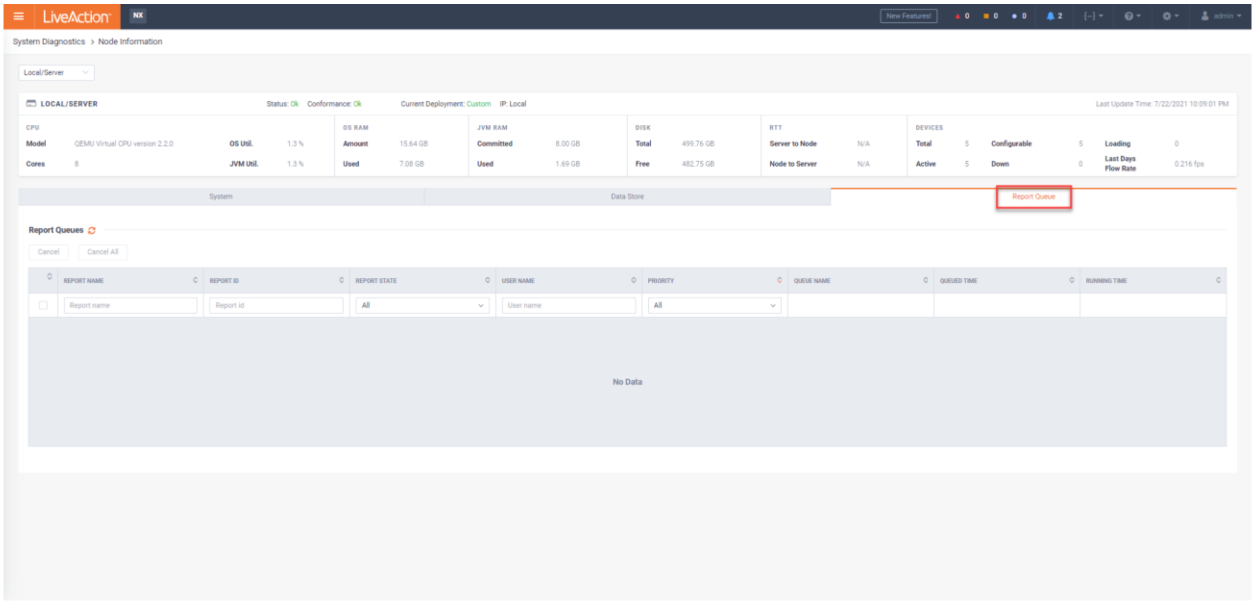
12. **Data Store** tab will allow viewing the storage details applicable to the server.



LOCAL/SERVER Status: Ok Conformance: Ok Current Deployment: Custom IP: Local Last Update Time: 7/22/2021 10:09:01 PM

CPU				OS RAM		JVM RAM		DISK		RTT		DEVICES					
Model	QEMU Virtual CPU version 2.2.0	OS Util.	1.3 %	Amount	15.64 GB	Committed	8.00 GB	Total	499.76 GB	Server to Node	N/A	Total	5	Configurable	5	Loading	0
Cores	8	JVM Util.	1.3 %	Used	7.08 GB	Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5	Down	0	Last Days Flow Rate	0.216 fps

13. Report Queue tab will allow viewing any reports currently running on the server.



System Diagnostics > Node Information

Local/Server

LOCAL/SERVER Status: Ok Conformance: Ok Current Deployment: Custom IP: Local Last Update Time: 7/22/2021 10:09:01 PM

CPU				OS RAM		JVM RAM		DISK		RTT		DEVICES					
Model	QEMU Virtual CPU version 2.2.0	OS Util.	1.3 %	Amount	15.64 GB	Committed	8.00 GB	Total	499.76 GB	Server to Node	N/A	Total	5	Configurable	5	Loading	0
Cores	8	JVM Util.	1.3 %	Used	7.08 GB	Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5	Down	0	Last Days Flow Rate	0.216 fps

Report Queues

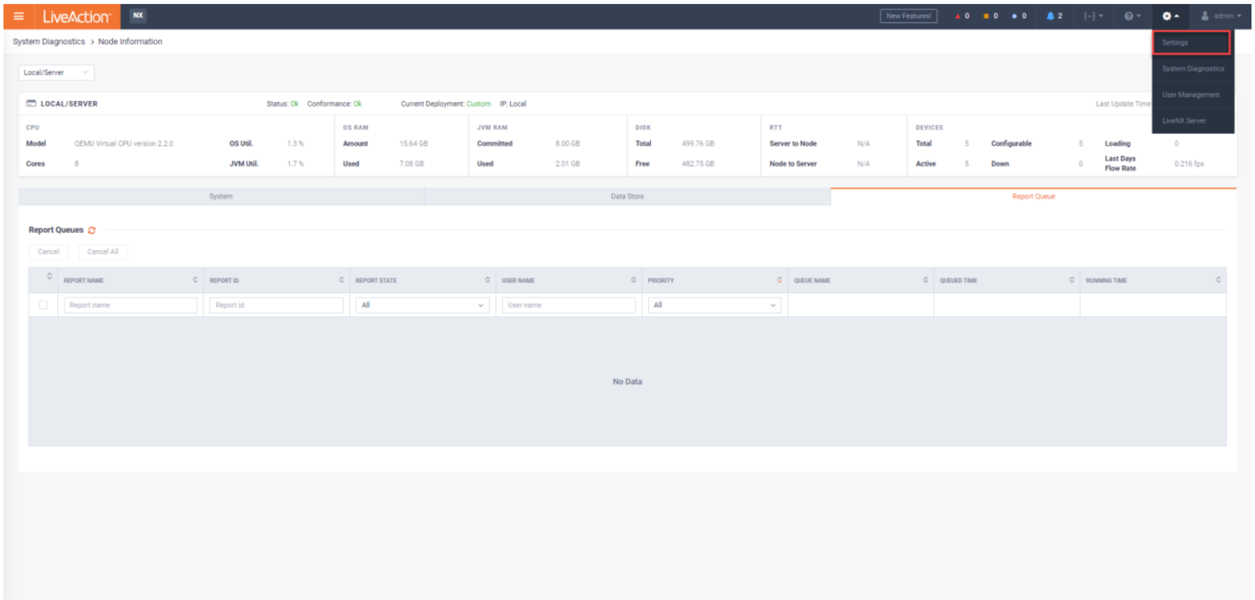
	REPORT NAME	REPORT ID	REPORT STATE	USER NAME	PRIORITY	QUEUE NAME	QUEUED TIME	RUNNING TIME
□	Report name	Report id	All	User name	All			

No Data

Lab 1.8: Support and Troubleshooting

If support is needed, logs will need to be generated and collected.

1. Navigate to the **Settings** menu.

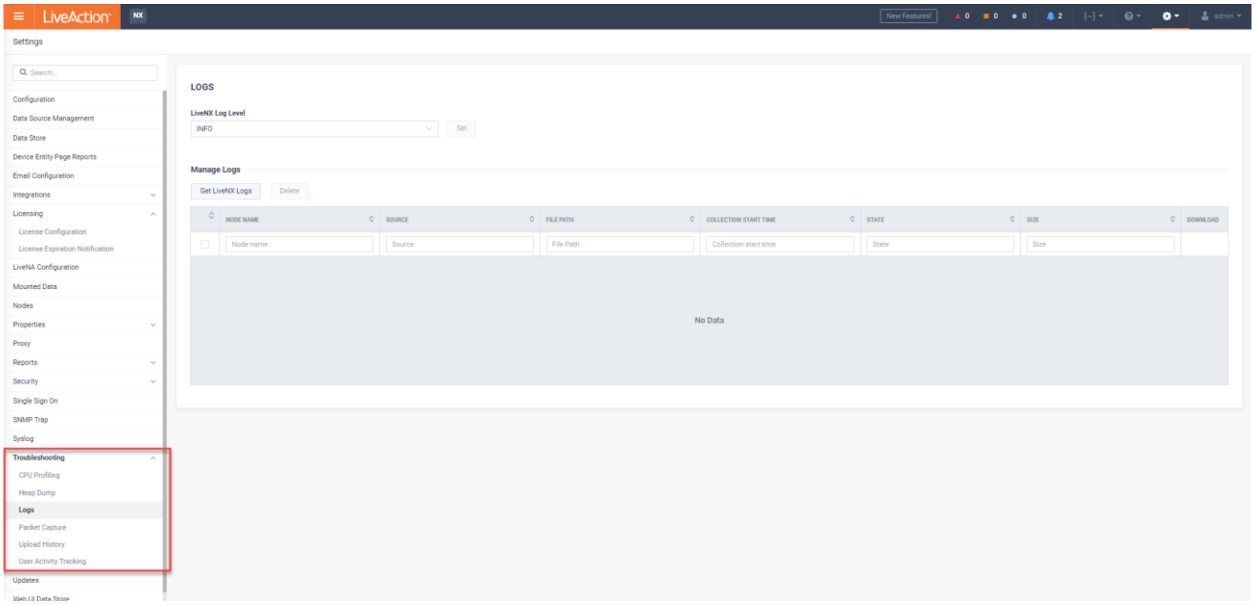


Status: Ok Conformance: Ok Current Deployment: Custom IP: Local

CPU				OS RAM		JVM RAM		DISK		RTT		DEVICES					
Model	QEMU Virtual CPU version 2.2.0	OS Util.	1.3 %	Amount	15.64 GB	Committed	8.00 GB	Total	499.76 GB	Server to Node	N/A	Total	5	Configurable	5	Loading	0
Cores	8	JVM Util.	1.7 %	Used	7.08 GB	Used	2.01 GB	Free	482.75 GB	Node to Server	N/A	Active	5	Down	0	Last Days Flow Rate	0.216 fps

	REPORT NAME	REPORT ID	REPORT STATE	USER NAME	PRIORITY	QUEUE NAME	QUEUED TIME	RUNNING TIME
□	Report name	Report id	All	User name	All			

2. Navigate and expand **Troubleshooting** and then click **Logs.**

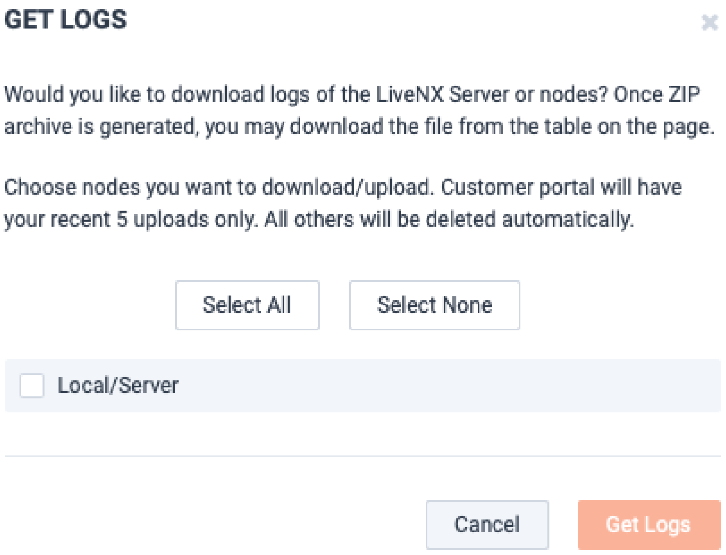


LiveNX Log Level: INFO

	NODE NAME	SOURCE	FILE PATH	COLLECTION START TIME	STATE	SIZE	DOWNLOAD
□	Node name	Source	File Path	Collection start time	State	Size	

Note: Most cases, will just require the default setting **INFO** Log Level. The support team will indicate if a different level is needed.

3. Click **Get LiveNX Logs**.



GET LOGS

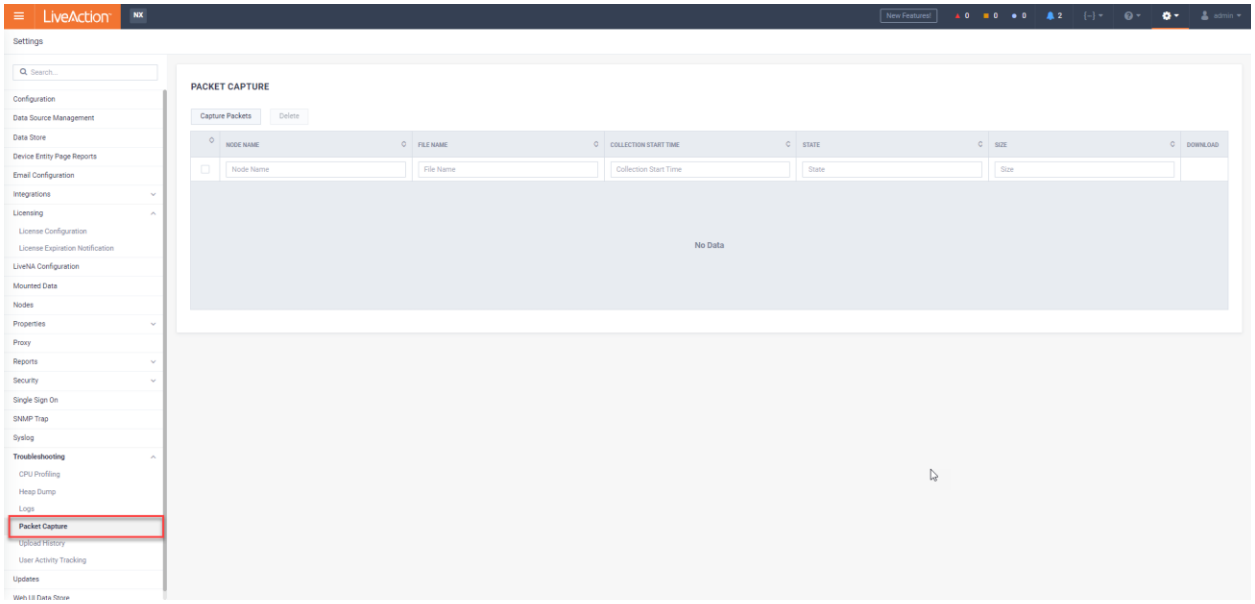
Would you like to download logs of the LiveNX Server or nodes? Once ZIP archive is generated, you may download the file from the table on the page.

Choose nodes you want to download/upload. Customer portal will have your recent 5 uploads only. All others will be deleted automatically.

□ Local/Server

Note: If there are multiple nodes installed within the environment, there will be additional items selectable.

4. Once logs are generated, you can Download the zip file. Once downloaded locally, the logs can be shared with the LiveAction support team.
5. Navigate to **Packet Capture** under **Troubleshooting.**

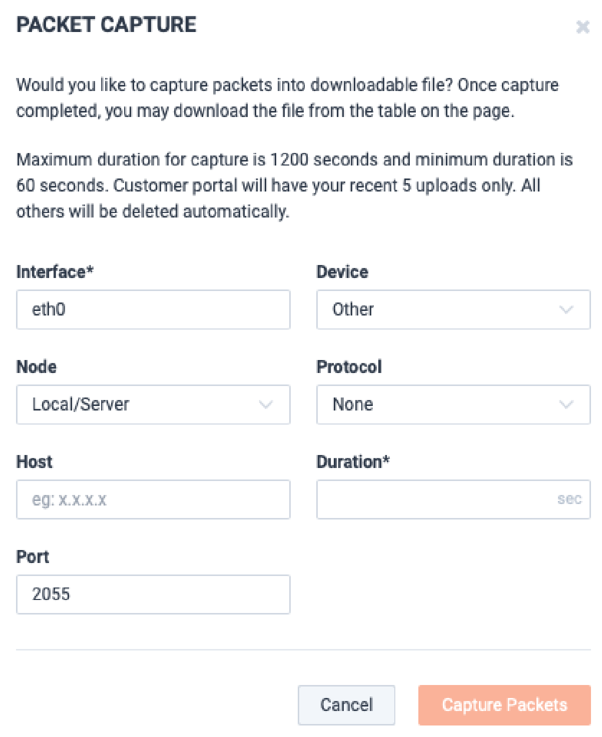


PACKET CAPTURE

	NODE NAME	FILE NAME	COLLECTION START TIME	STATE	SIZE	DOWNLOAD
□	Node Name	File Name	Collection Start Time	State	Size	

No Data

6. Click **Capture Packets.**



PACKET CAPTURE

Would you like to capture packets into downloadable file? Once capture completed, you may download the file from the table on the page.

Maximum duration for capture is 1200 seconds and minimum duration is 60 seconds. Customer portal will have your recent 5 uploads only. All others will be deleted automatically.

Interface*: eth0

Device: Other

Node: Local/Server

Protocol: None

Host: eg: x.x.x.x

Duration*: sec

Port: 2055

7. This allows you to capture packets on a specific device, protocol, port, and a specific duration.

Note: If directed by support to capture packets, they will indicate the duration and other applicable details needed.

8. As in Logs, you can download the zip file. Once downloaded locally, the logs can be shared with the LiveAction support team.

Lab 2

Lab 2: The LiveNX Client

Lab 2.1: Launch the LiveNX Client

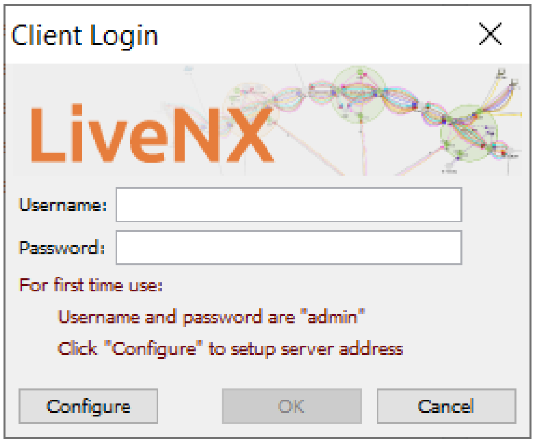
The LiveNX Client is a Java application which may be loaded and launched on your local workstation. In this class you may alternatively run the Client on the virtual workstation connected via Remote Desktop Connection. The Client may be downloaded at https://cloudkeys.liveaction.com/downloads, and installation is straight-forward

A Mac version is also available for install if needed.

Lab Steps:

1. **Launch** the LiveNX Client.

DIAGRAM



Client Login

Username:

Password:

For first time use:

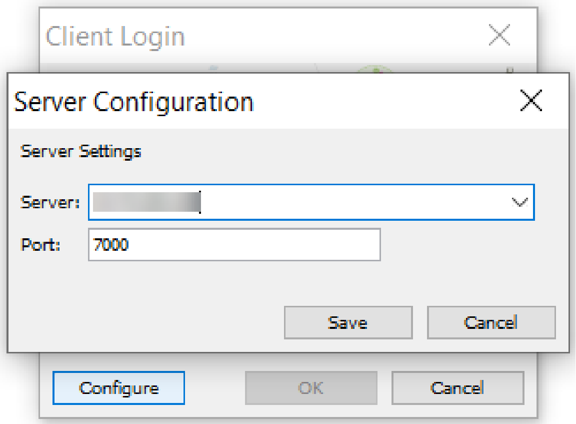
Username and password are "admin"

Click "Configure" to setup server address

2. Click **Configure** to verify server settings.

Note: A single client installation may connect to multiple LiveNX Servers simply by modifying the Server IP and Port. In this class we will always connect to the LiveNX Server in our Training Pod. Use the <ipaddress> from your Lab Access Worksheet. The "For first time use" instructions only apply to an un-configured Server.

3. Enter the LiveNX information (IP address and Port) from your Lab Access worksheet



Server Configuration

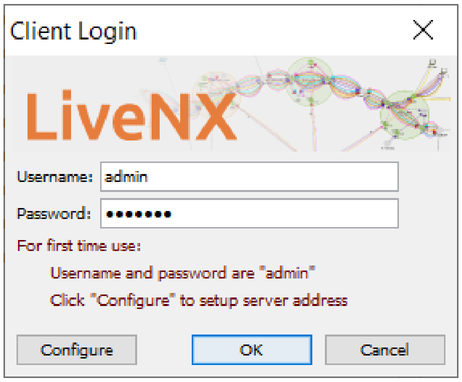
Server Settings

Server: [redacted]

Port: 7000

4. **Click** Save
5. Enter the **Username** & **Password**.
   Username: admin

Password: Student (note the capital S)



Client Login

Username: admin

Password: •••••••

For first time use:

Username and password are "admin"

Click "Configure" to setup server address

6. Click **OK**

The Client will launch…

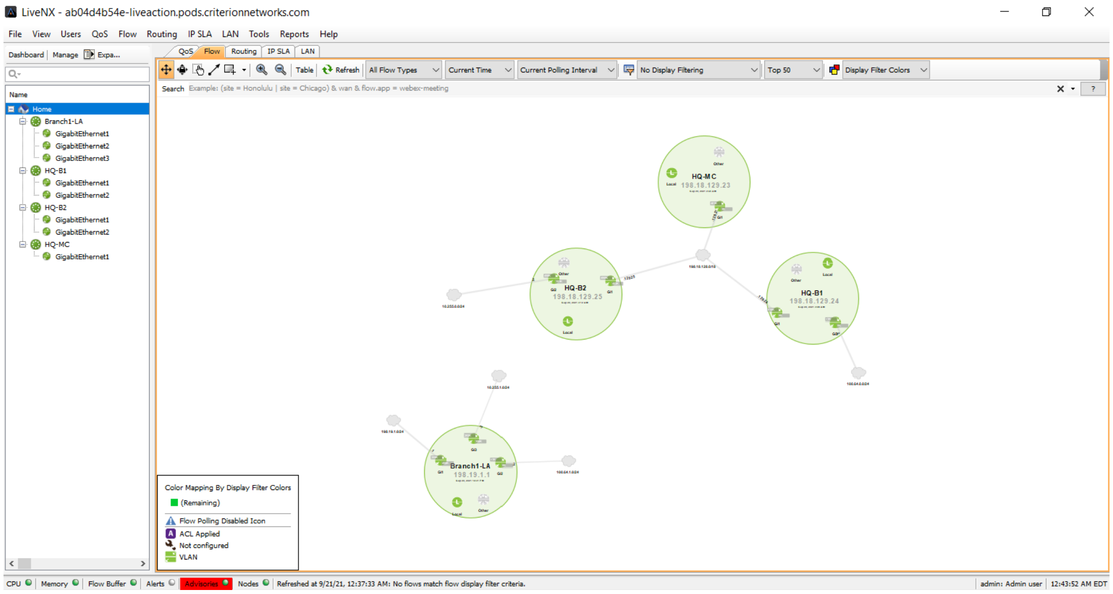
Loading...

Loaded Current User

© 2008-2021 LiveAction, Inc. All Right Reserved.

www.liveaction.com

… and will open showing the current configured Topology.



LiveNX - ab04d4b54e-liveaction.pods.criterionnetworks.com

Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

All Flow Types | Current Time | Current Polling Interval | No Display Filtering | Top 50 | Display Filter Colors

Color Mapping By Display Filter Colors

🟩 (Remaining)

Flow Polling Disabled Icon

ACL Applied

Not configured

VLAN

CPU | Memory | Flow Buffer | Alerts | Advisories | Nodes | Refreshed at 9/21/21, 12:37:33 AM: No flows match flow display filter criteria. | admin: Admin user | 12:43:52 AM EDT

Note: Your topology may be different from the screenshot above. Some of the items may be stacked directly on top of each other, requiring you to click and drag to make them more visible

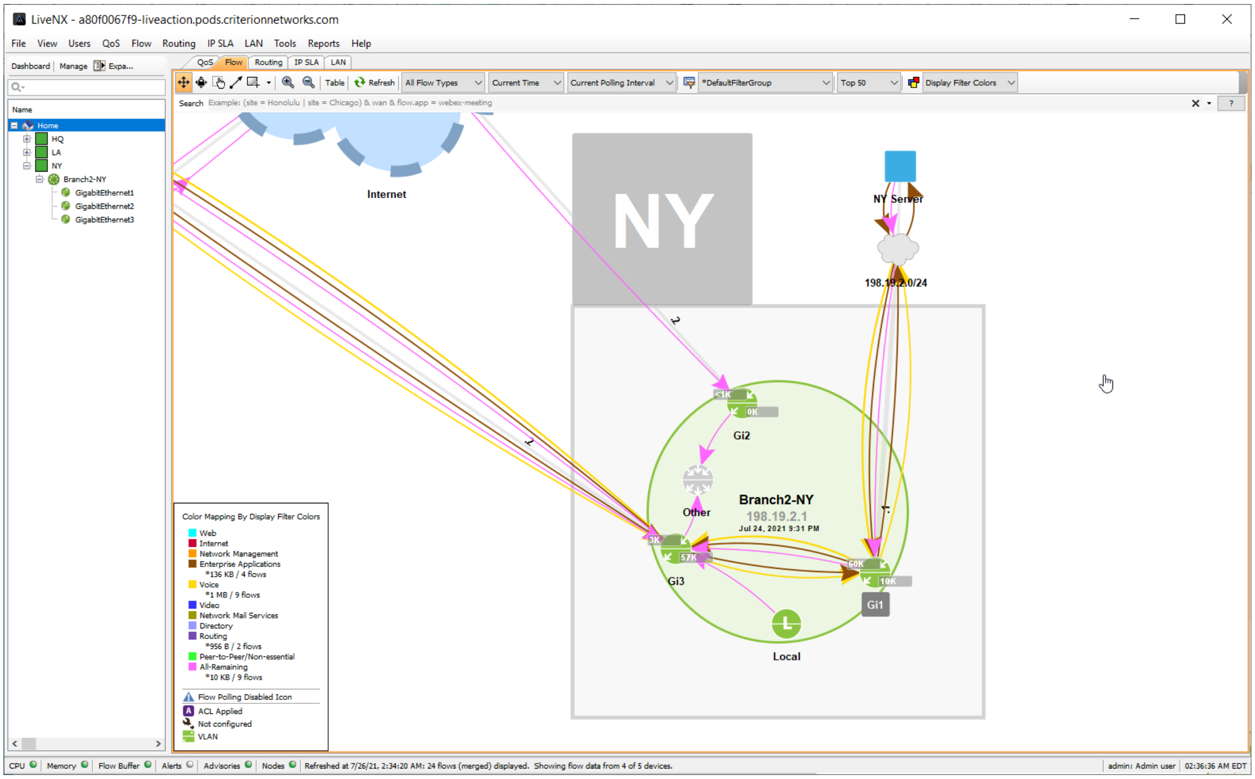
Lab 2.2: Explore the LiveNX Client

Although we've already pre-configured one or more devices… LiveNX *may not* be collecting any flow data. In a subsequent Lab we will verify & complete the configuration of our class network by adding more devices and enabling flow collection, as needed. For now, let's look at some of the menus and feature availability of the LiveNX Client.

Lab Steps:

1. Right-click on device **HQ-B2** and select **Zoom to Device** to zoom into the **HQ-B2** Device, and center it on the screen.

DIAGRAM


LiveNX - a80f0067f9-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard | Manage | Expa...
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval *DefaultFilterGroup Top 50 Display Filter Colors
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
HQ
LA
NY
Branch2-NY
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
Internet
NY
NY Server
198.19.2.0/24
2
1
<1K
0K
Gi2
Other
Branch2-NY
198.19.2.1
Jul 24, 2021 9:31 PM
3K
57K
Gi3
60K
10K
Gi1
Local
Color Mapping By Display Filter Colors
Web
Internet
Network Management
Enterprise Applications
*136 KB / 4 flows
Voice
*1 MB / 9 flows
Video
Network Mail Services
Directory
Routing
*956 B / 2 flows
Peer-to-Peer/Non-essential
All-Remaining
*10 KB / 9 flows
Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN
CPU Memory Flow Buffer Alerts Advisories Nodes
admin: Admin user
02:36:36 AM EDT

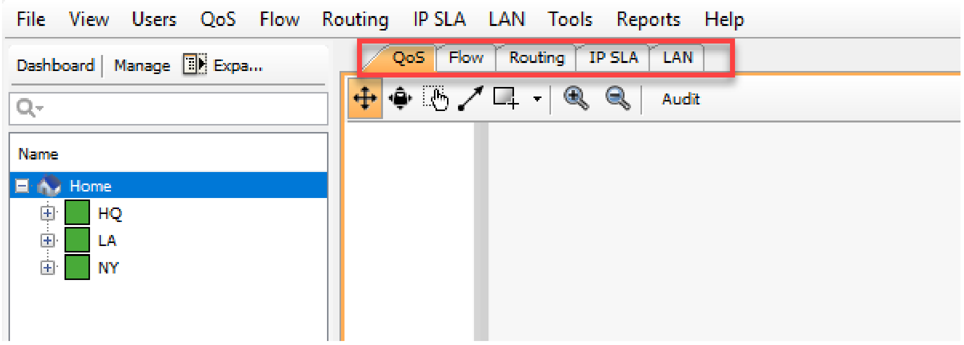
Refreshed at 7/26/21, 2:34:20 AM: 24 flows (merged) displayed. Showing flow data from 4 of 5 devices.

Note: Your topology may be different from the screenshot above.

2. Left click anywhere in the white area and move the mouse to re-position the device(s) in the window.
3. Use the mouse scroll-wheel to zoom in & out.

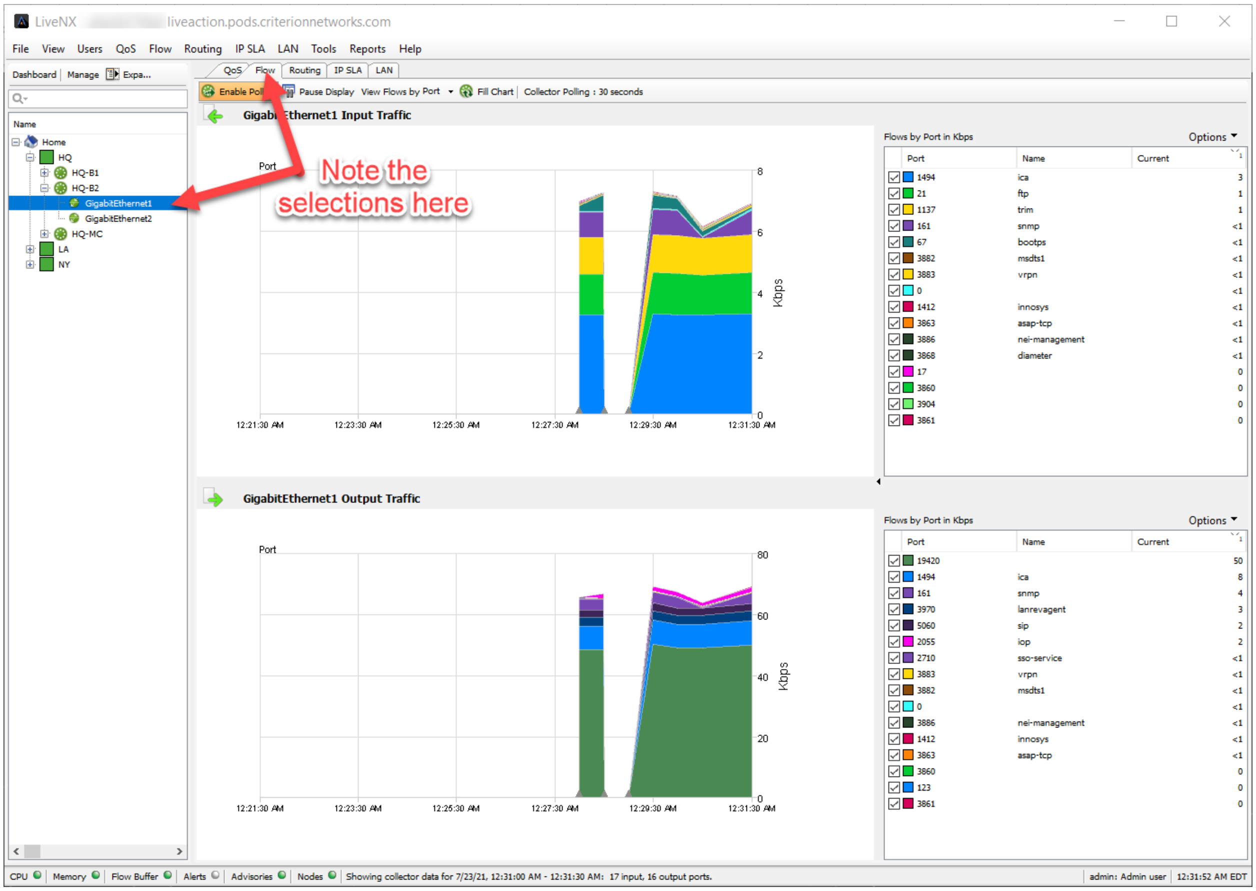
4. Note the 5 Module Tabs to the top-left of the Topology Pane.

DIAGRAM



Note: Once we confirm the collection Flow and SNMP data these tabs will be a lot more useful!

5. Click on **Flow** tab, and on the **Home** icon in the tree-view pane to the left of the screen.
6. **Expand** the **HQ-B2** device in the **Home** Tree View.
7. Click on one of the interfaces… note how the information displayed in the Topology Pane changes.



Flows by Port in Kbps

	Port	Name	Current
☑ 🟦	1494	ica	3
☑ 🟩	21	ftp	1
☑ 🟨	1137	trim	1
☑ 🟪	161	snmp	<1
☑ 🟦	67	bootps	<1
☑ 🟫	3882	msdts1	<1
☑ 🟨	3883	vrpn	<1
☑ 🟦	0		<1
☑ 🟥	1412	innosys	<1
☑ 🟧	3863	asap-tcp	<1
☑ 🟩	3886	nei-management	<1
☑ 🟩	3868	diameter	<1
☑ 🟪	17		0
☑ 🟩	3860		0
☑ 🟩	3904		0
☑ 🟥	3861		0

Flows by Port in Kbps

	Port	Name	Current
☑ 🟩	19420		50
☑ 🟦	1494	ica	8
☑ 🟪	161	snmp	4
☑ 🟦	3970	lanrevagent	3
☑ 🟪	5060	sip	2
☑ 🟪	2055	iop	2
☑ 🟪	2710	sso-service	<1
☑ 🟨	3883	vrpn	<1
☑ 🟫	3882	msdts1	<1
☑ 🟦	0		<1
☑ 🟩	3886	nei-management	<1
☑ 🟥	1412	innosys	<1
☑ 🟧	3863	asap-tcp	<1
☑ 🟩	3860		0
☑ 🟦	123		0
☑ 🟥	3861		0

Showing collector data for 7/23/21, 12:31:00 AM - 12:31:30 AM: 17 input, 16 output ports.

Note: You are welcome to poke around the LiveNX Client… don’t worry, you won’t break anything… but we will get some real usage, and see real data, in the coming labs!

Lab 3

Lab 3: Configuring Devices

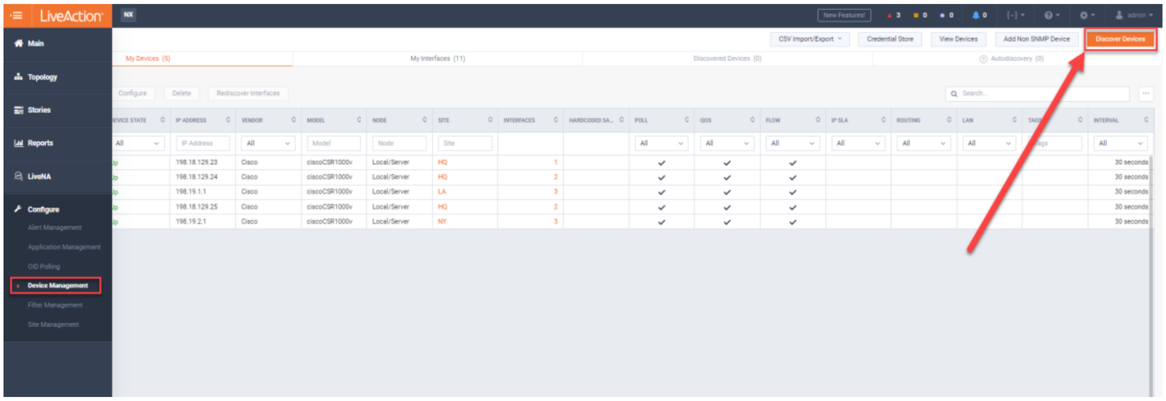
Lab 3.1: Add Device

Adding devices into LiveAction and managing them properly is very important to the overall usability of LiveAction itself.

In this Lab we'll go to the WebUI to Discover & Add a device to our LiveNX Server.

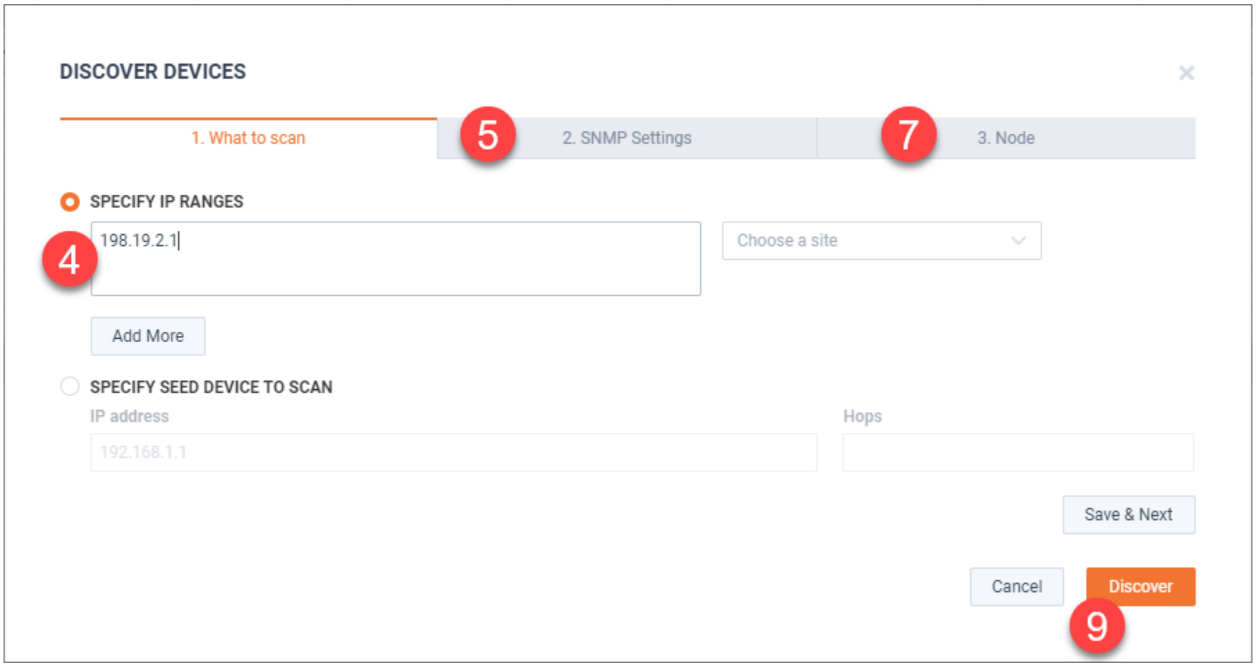
Lab Steps:

1. Login to the LiveNX WebUI
2. Select **Configure** > **Device Management**



DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED SA...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS	INTERVAL
All	IP Address	All	Model	Node	Site			All	All	All	All	All	All	Tags	All
Up	198.18.129.23	Cisco	ciscoCSR1000v	Local/Server	HQ	1		✓	✓	✓					30 seconds
Up	198.18.129.24	Cisco	ciscoCSR1000v	Local/Server	HQ	2		✓	✓	✓					30 seconds
Up	198.19.1.1	Cisco	ciscoCSR1000v	Local/Server	LA	3		✓	✓	✓					30 seconds
Up	198.18.129.25	Cisco	ciscoCSR1000v	Local/Server	HQ	2		✓	✓	✓					30 seconds
Up	198.19.2.1	Cisco	ciscoCSR1000v	Local/Server	NY	3		✓	✓	✓					30 seconds

3. Click **Discover Devices**.



● SPECIFY IP RANGES

198.19.2.1

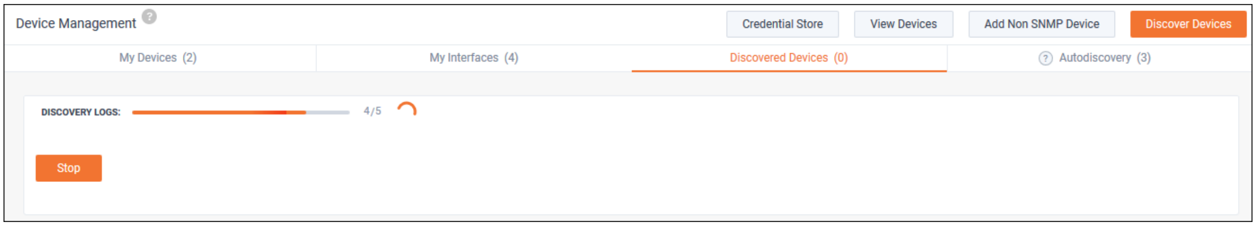
Choose a site

○ SPECIFY SEED DEVICE TO SCAN

IP address: 192.168.1.1

Hops

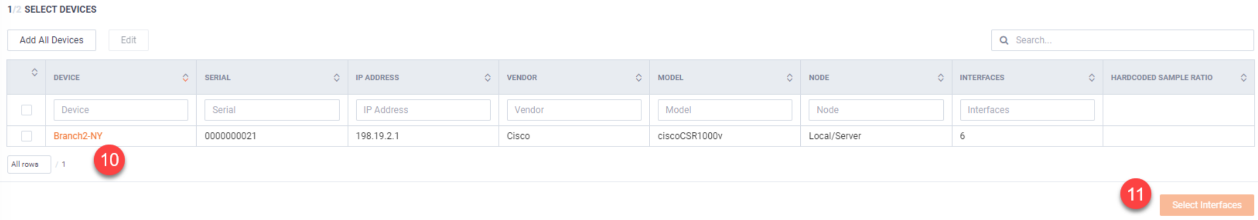
4. Enter **198.19.2.1**, in the IP Address field.
5. Select the **SNMP Settings** tab.
6. Click "**Default SNMP connection settings**".
7. Select the **Node** tab.
8. Select **Local/Server**.
9. Click **Discover**.



Device Management

DISCOVERY LOGS: 4/5

Note: Discovery may take a minute or two. If you've specified a large subnet to scan, and Discovery seems to take too long… click Stop.



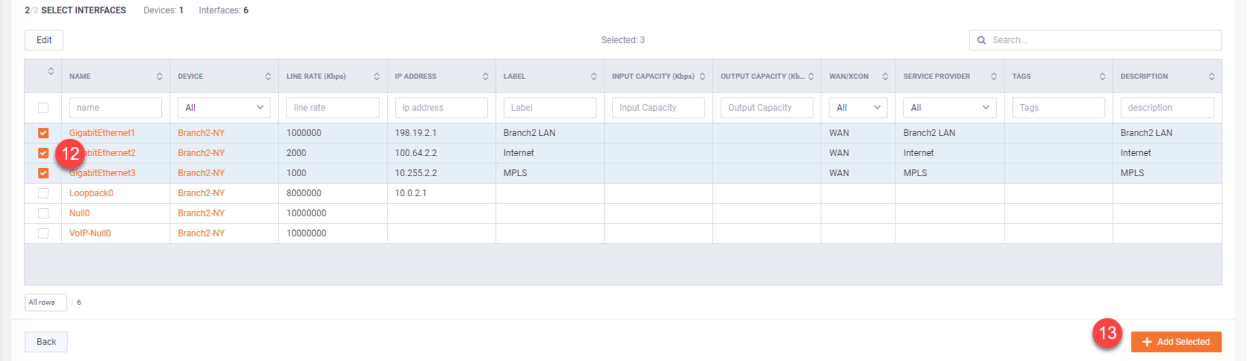
1/2 SELECT DEVICES

	DEVICE	SERIAL	IP ADDRESS	VENDOR	MODEL	NODE	INTERFACES	HARDCODED SAMPLE RATIO
□	Device	Serial	IP Address	Vendor	Model	Node	Interfaces	
□	Branch2-NY	0000000021	198.19.2.1	Cisco	ciscoCSR1000v	Local/Server	6	

All rows / 1

10. Tick the box next to **Branch2-NY**.

11. Click **Select Interfaces**.



2/2 SELECT INTERFACES Devices: 1 Interfaces: 6

Selected: 3

	NAME	DEVICE	LINE RATE (Kbps)	IP ADDRESS	LABEL	INPUT CAPACITY (Kbps)	OUTPUT CAPACITY (Kb...	WAN/XCON	SERVICE PROVIDER	TAGS	DESCRIPTION
□	name	All	line rate	ip address	Label	Input Capacity	Output Capacity	All	All	Tags	description
☑	GigabitEthernet1	Branch2-NY	1000000	198.19.2.1	Branch2 LAN			WAN	Branch2 LAN		Branch2 LAN
☑	GigabitEthernet2	Branch2-NY	2000	100.64.2.2	Internet			WAN	Internet		Internet
☑	GigabitEthernet3	Branch2-NY	1000	10.255.2.2	MPLS			WAN	MPLS		MPLS
□	Loopback0	Branch2-NY	8000000	10.0.2.1							
□	Null0	Branch2-NY	10000000								
□	VoIP-Null0	Branch2-NY	10000000								

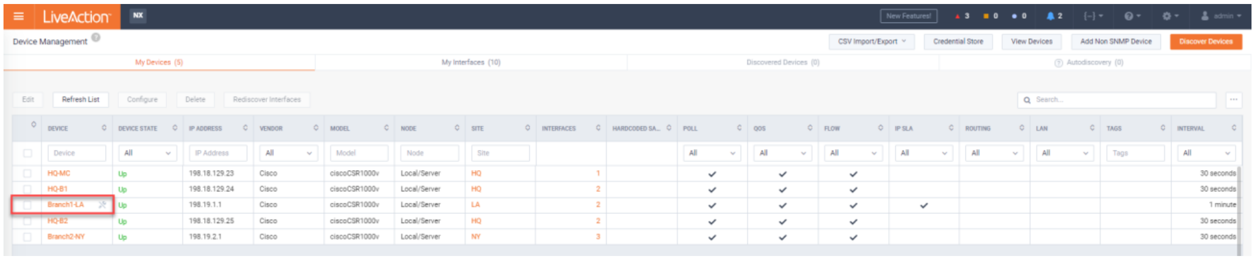
All rows / 6

12. Select **GigabitEthernet1**, **GigabitEthernet2** & **GigabitEthernet3**.

13. Click **Add Selected**.

LiveNX displays the available configured interface on the device(s) that were discovered. Notice that LiveNX also discovers additional device *semantic* information such as Line Rate, Capacities, Labels, etc.…

Note: LiveNX's Rapid Device Discovery feature will automatically select the Top 4 interfaces based-upon interface utilization. It is important that you confirm, or select, the interfaces you wish to monitor. LiveNX may monitor up to 1000 interfaces on a single device.



Device Management

	DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED SA...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS	INTERVAL
□	Device	All	IP Address	All	Model	Node	Site			All	All	All	All	All	All	Tags	All
□	HQ-MC	Up	198.18.129.23	Cisco	ciscoCSR1000v	Local/Server	HQ	1		✓	✓	✓					30 seconds
□	HQ-B1	Up	198.18.129.24	Cisco	ciscoCSR1000v	Local/Server	HQ	2		✓	✓	✓					30 seconds
□	Branch1-LA	Up	198.19.1.1	Cisco	ciscoCSR1000v	Local/Server	LA	2		✓	✓	✓	✓				1 minute
□	HQ-B2	Up	198.18.129.25	Cisco	ciscoCSR1000v	Local/Server	HQ	2		✓	✓	✓					30 seconds
□	Branch2-NY	Up	198.19.2.1	Cisco	ciscoCSR1000v	Local/Server	NY	3		✓	✓	✓					30 seconds

You now see we've added **Branch2-NY** for monitoring by LiveNX. Notice that there is a "not-configured" symbol next to the link. This means we still have some configuration to complete.

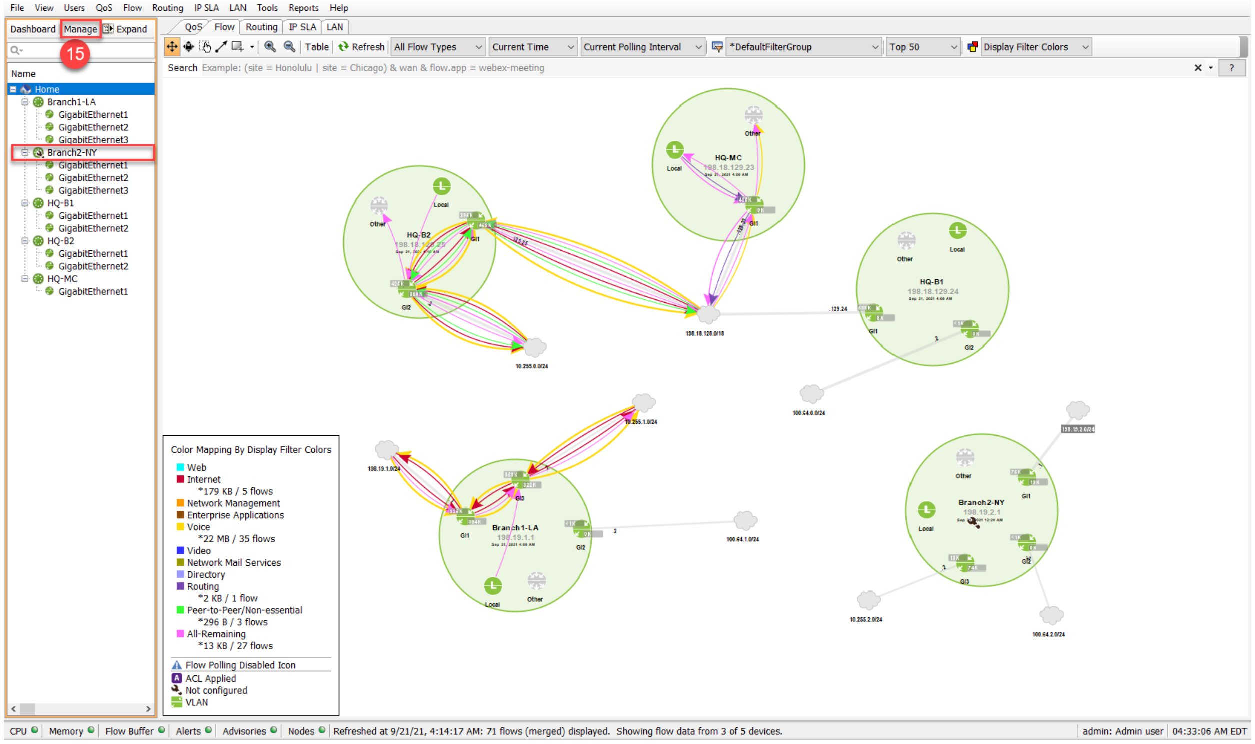
Lab 3.2: Manage & Configure Devices

You may perform many management tasks via the WebUI… but since we'll need to go to the LiveNX Client to configure Flow Collection in the next lab… let's complete our Device Configuration in the Console.

Note: You can find instructions for Adding Devices via the Client in the Appendix of this Lab Workbook.

Lab Steps:

14. Login to the LiveNX Client.
15. Right-click on **Home** and **Expand All.**



Name
- Home
  - Branch1-LA
    - GigabitEthernet1
    - GigabitEthernet2
    - GigabitEthernet3
  - Branch2-NY
    - GigabitEthernet1
    - GigabitEthernet2
    - GigabitEthernet3
  - HQ-B1
    - GigabitEthernet1
    - GigabitEthernet2
  - HQ-B2
    - GigabitEthernet1
    - GigabitEthernet2
  - HQ-MC
    - GigabitEthernet1

Color Mapping By Display Filter Colors

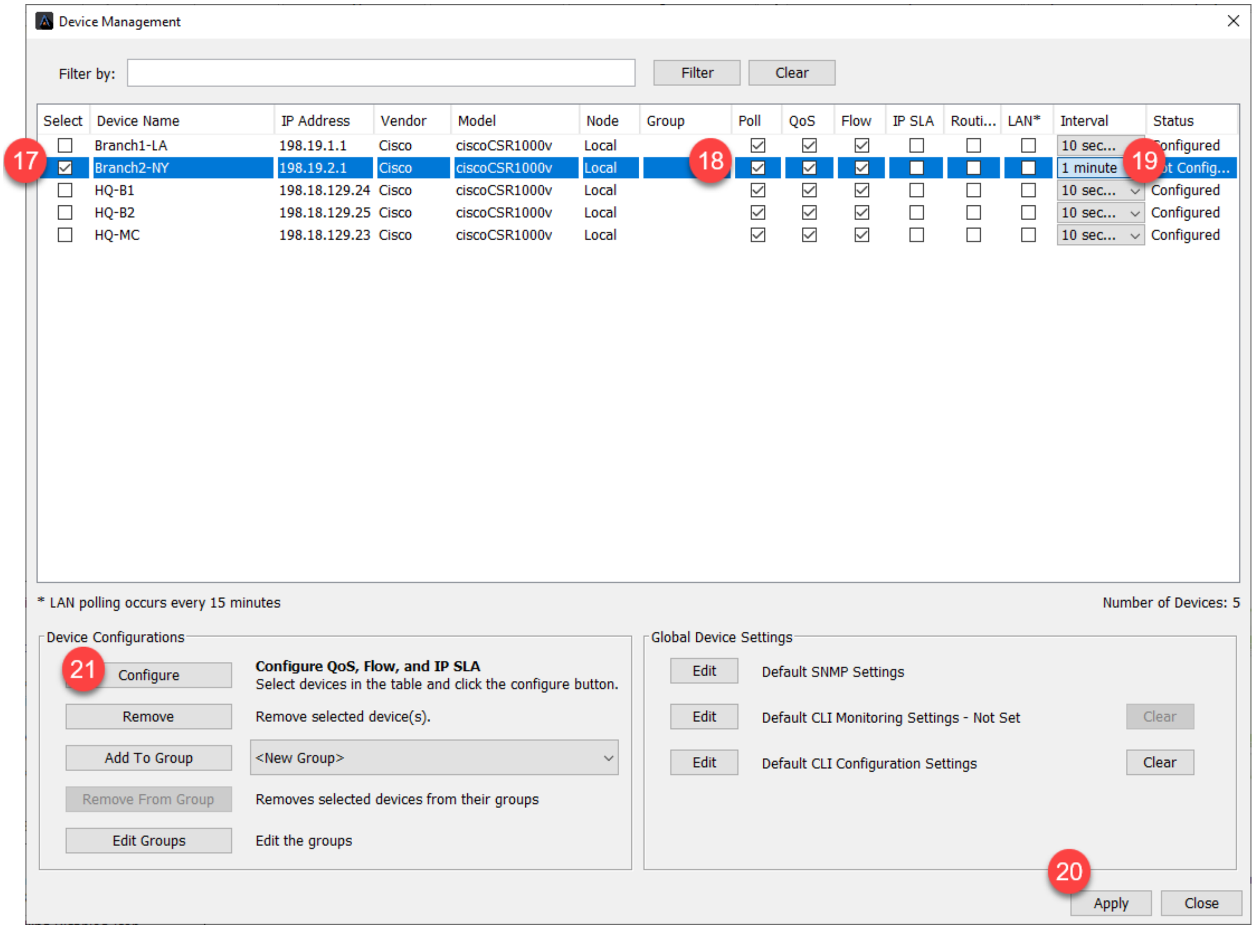
- Web
- Internet
  - *179 KB / 5 flows
- Network Management
- Enterprise Applications
- Voice
  - *22 MB / 35 flows
- Video
- Network Mail Services
- Directory
- Routing
  - *2 KB / 1 flow
- Peer-to-Peer/Non-essential
  - *296 B / 3 flows
- All-Remaining
  - *13 KB / 27 flows

Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN

CPU | Memory | Flow Buffer | Alerts | Advisories | Nodes | Refreshed at 9/21/21, 4:14:17 AM: 71 flows (merged) displayed. Showing flow data from 3 of 5 devices. | admin: Admin user | 04:33:06 AM EDT

Notice that the Topology Pane contains all the devices listed in the Home Tree view. Also note that the **Branch2-NY** device needs to be configured.

16. Click **Manage** (Above the Home Tree).
17. Select only **Branch2-NY**



Device Management

Filter by: [ ] Filter Clear

Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routi...	LAN*	Interval	Status
□	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	10 sec...	onfigured
☑	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	1 minute	t Config...
□	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	10 sec...	Configured
□	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	10 sec...	Configured
□	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	10 sec...	Configured

* LAN polling occurs every 15 minutes

Number of Devices: 5

Device Configurations

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

Remove — Remove selected device(s).

Add To Group — <New Group>

Remove From Group — Removes selected devices from their groups

Edit Groups — Edit the groups

Global Device Settings

Edit — Default SNMP Settings

Edit — Default CLI Monitoring Settings - Not Set — Clear

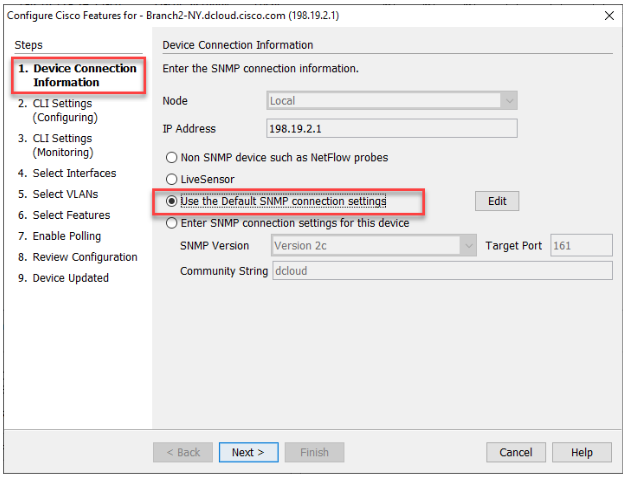
Edit — Default CLI Configuration Settings — Clear

Apply Close

18. Check ONLY **Poll, QoS** and **Flow** for each device
19. Change the Interval on all devices to **10 seconds**.
20. Click **Apply**.
21. Click **Configure**.

LiveNX starts the Add Device wizard… we will basically select to use whatever defaults are already configured…

22. Step1: Use the **Default SNMP**… Click Next
23. Step2: Use **My Default Configuration CLI**… Click Next



Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

Device Connection Information

Enter the SNMP connection information.

Node: Local

IP Address: 198.19.2.1

○ Non SNMP device such as NetFlow probes

○ LiveSensor

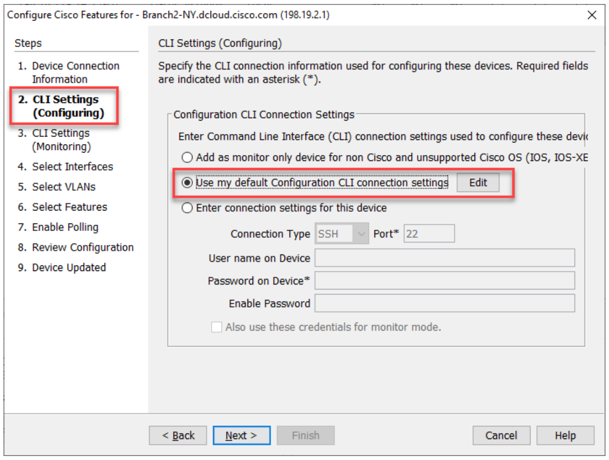
● Use the Default SNMP connection settings — Edit

○ Enter SNMP connection settings for this device

SNMP Version: Version 2c — Target Port: 161

Community String: dcloud

< Back — Next > — Finish — Cancel — Help



Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devi

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE

● Use my default Configuration CLI connection settings — Edit

○ Enter connection settings for this device

Connection Type: SSH — Port*: 22

User name on Device:

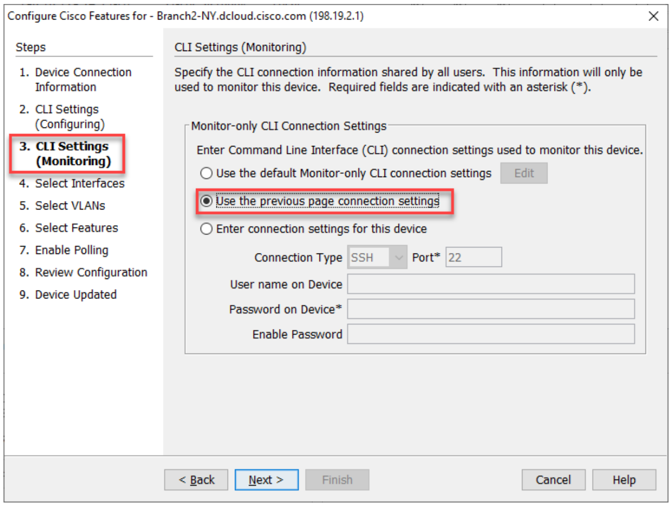
Password on Device*:

Enable Password:

□ Also use these credentials for monitor mode.

< Back — Next > — Finish — Cancel — Help

24. Step 3: Check Use the **Previous Page Connection Settings** … Click **Next**. You will be shown a list of configuration elements to verify. Click Continue.


Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)
< Back
Next >
Finish
Cancel
Help
Edit

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings

● Use the previous page connection settings

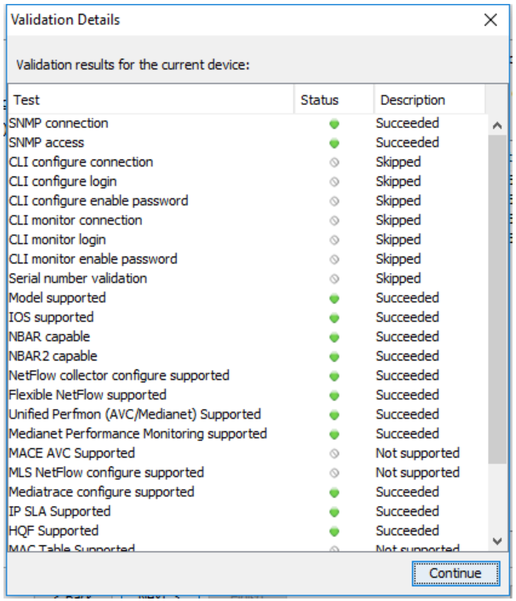
○ Enter connection settings for this device

Connection Type SSH Port* 22

User name on Device

Password on Device*

Enable Password

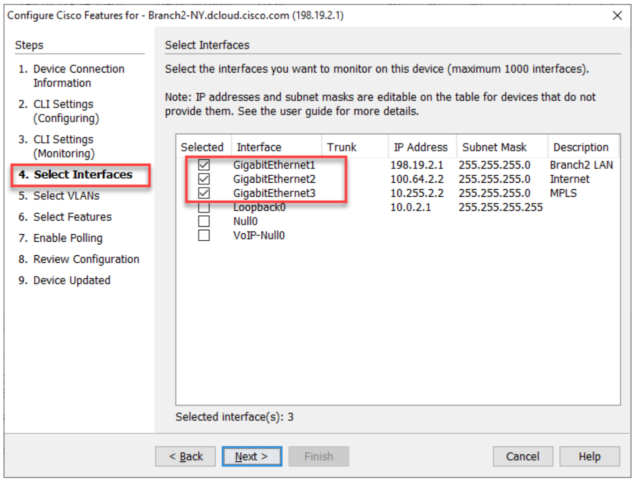


Validation results for the current device:

Test	Status	Description
SNMP connection	●	Succeeded
SNMP access	●	Succeeded
CLI configure connection	⊘	Skipped
CLI configure login	⊘	Skipped
CLI configure enable password	⊘	Skipped
CLI monitor connection	⊘	Skipped
CLI monitor login	⊘	Skipped
CLI monitor enable password	⊘	Skipped
Serial number validation	⊘	Skipped
Model supported	●	Succeeded
IOS supported	●	Succeeded
NBAR capable	●	Succeeded
NBAR2 capable	●	Succeeded
NetFlow collector configure supported	●	Succeeded
Flexible NetFlow supported	●	Succeeded
Unified Perfmon (AVC/Medianet) Supported	●	Succeeded
Medianet Performance Monitoring supported	●	Succeeded
MACE AVC Supported	⊘	Not supported
MLS NetFlow configure supported	⊘	Not supported
Mediatrace configure supported	●	Succeeded
IP SLA Supported	●	Succeeded
HQF Supported	●	Succeeded
MAC Table Supported	⊘	Not supported

Note: Any changes to the **Select Features** dialog will generate a CLI push to update the current configuration. Before sending a new configuration to the device, you can verify the configurations that LiveNX created.

25. Step 5: Ensure the correct interfaces are selected… Click **Next**
    a. You will want to include all GE interfaces
    b. You can include Loopback, but not necessary. The point is to understand you can choose both logical and physical interfaces.


Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)
< Back
Next >
Finish
Cancel
Help

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. **Select Interfaces**
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

Select Interfaces

Select the interfaces you want to monitor on this device (maximum 1000 interfaces).

Note: IP addresses and subnet masks are editable on the table for devices that do not provide them. See the user guide for more details.

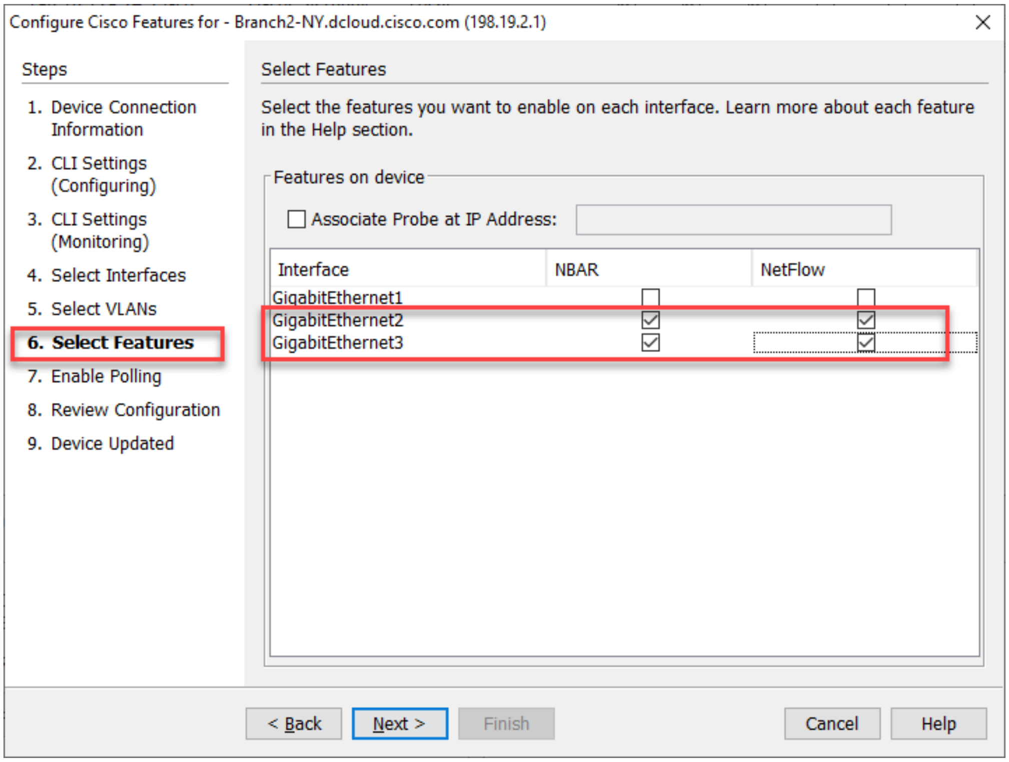
Selected	Interface	Trunk	IP Address	Subnet Mask	Description
☑	GigabitEthernet1		198.19.2.1	255.255.255.0	Branch2 LAN
☑	GigabitEthernet2		100.64.2.2	255.255.255.0	Internet
☑	GigabitEthernet3		10.255.2.2	255.255.255.0	MPLS
□	Loopback0		10.0.2.1	255.255.255.255	
□	Null0				
□	VoIP-Null0				

Selected interface(s): 3

26. Step 5: Since there are no VLANs configured on this device, none will be displayed. You may monitor up to 25 configured VLANs on each device. Click **Next.**

27. Step 6: The **Select Features** dialog allows you to turn-on specific Cisco technologies per device interface using the templates included in LiveNX. This dialog displays the

current IOS configuration of the device you are currently viewing. Match the settings for **GigabitEthernet2** and **GigabitEthernet3 (WAN interfaces only)**. Click **Next**.



Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. **Select Features**
7. Enable Polling
8. Review Configuration
9. Device Updated

Select Features

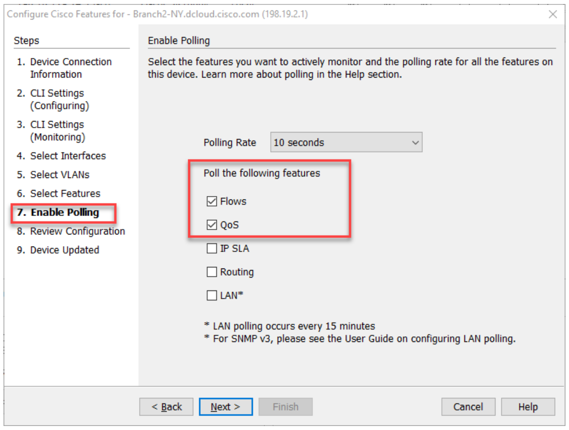
Select the features you want to enable on each interface. Learn more about each feature in the Help section.

Features on device

□ Associate Probe at IP Address:

Interface	NBAR	NetFlow
GigabitEthernet1	□	□
GigabitEthernet2	☑	☑
GigabitEthernet3	☑	☑

28. Step 7: Enable **Polling** is set for **10 Seconds** and ensure **Flows** and **QoS** are selected Next. Click Continue



Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. **Enable Polling**
8. Review Configuration
9. Device Updated

Enable Polling

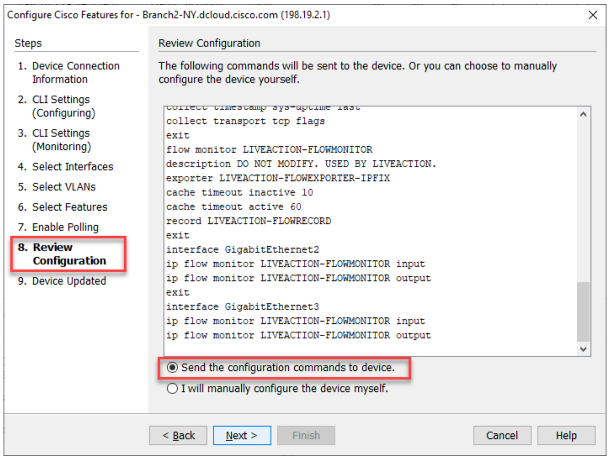
Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section.

Polling Rate: 10 seconds

Poll the following features

☑ Flows
☑ QoS
□ IP SLA
□ Routing
□ LAN*

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.



Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. **Review Configuration**
9. Device Updated

Review Configuration

The following commands will be sent to the device. Or you can choose to manually configure the device yourself.

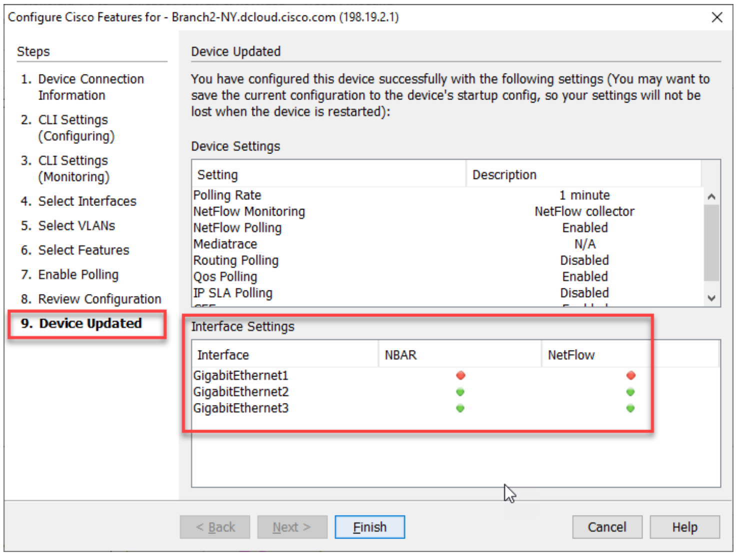
```
collect timestamp sys-uptime last
collect transport tcp flags
exit
flow monitor LIVEACTION-FLOWMONITOR
description DO NOT MODIFY. USED BY LIVEACTION.
exporter LIVEACTION-FLOWEXPORTER-IPFIX
cache timeout inactive 10
cache timeout active 60
record LIVEACTION-FLOWRECORD
exit
interface GigabitEthernet2
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
exit
interface GigabitEthernet3
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
```

● Send the configuration commands to device.
○ I will manually configure the device myself.

29. Step 8: Review the code of the changes that have been made. For this lab select “**Send the configuration commands to device”** radio button. You may not want to do this in your actual deployment – it can depend on your configuration management processes. Just know, LiveNX is able to send the config instructions if you wish.

30. Click **Next**.

31. Click **Finish**.


Configure Cisco Features for - Branch2-NY.dcloud.cisco.com (198.19.2.1)
Steps
1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated
< Back
Next >
Finish
Cancel
Help

Device Updated

You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):

Device Settings

Setting	Description
Polling Rate	1 minute
NetFlow Monitoring	NetFlow collector
NetFlow Polling	Enabled
Mediatrace	N/A
Routing Polling	Disabled
Qos Polling	Enabled
IP SLA Polling	Disabled

Interface Settings

Interface	NBAR	NetFlow
GigabitEthernet1	🔴	🔴
GigabitEthernet2	🟢	🟢
GigabitEthernet3	🟢	🟢

32. Step 9: You will see the summary of the changes made. Click **Finish**.

The device will be added to the Topology Pane in LiveNX. You will notice it no longer shows the Wrench icon, meaning it has been configured in the LiveNX system.

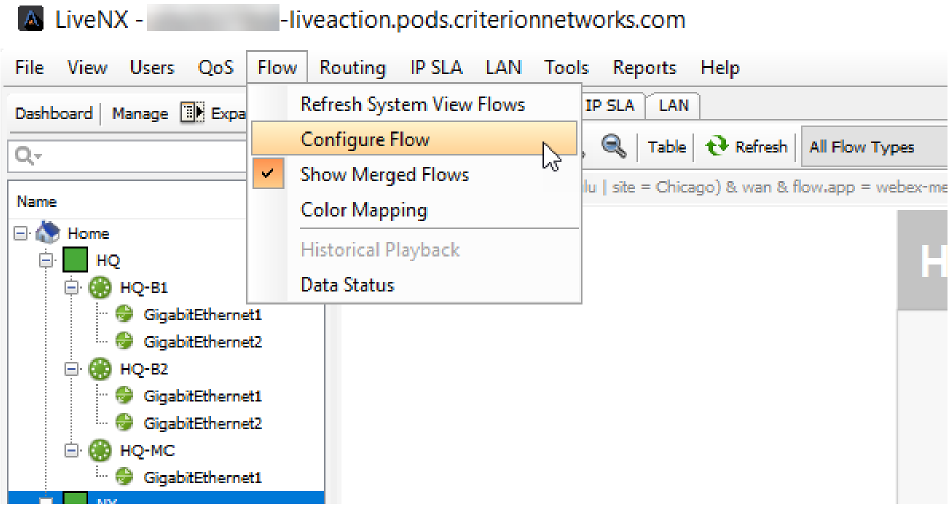
Note: Your new device may not be immediately visible. Use the **View** > **Fit to View** command to include all devices in the main view. Arrange as required.

Lab 3.3: Configure Flow on Devices

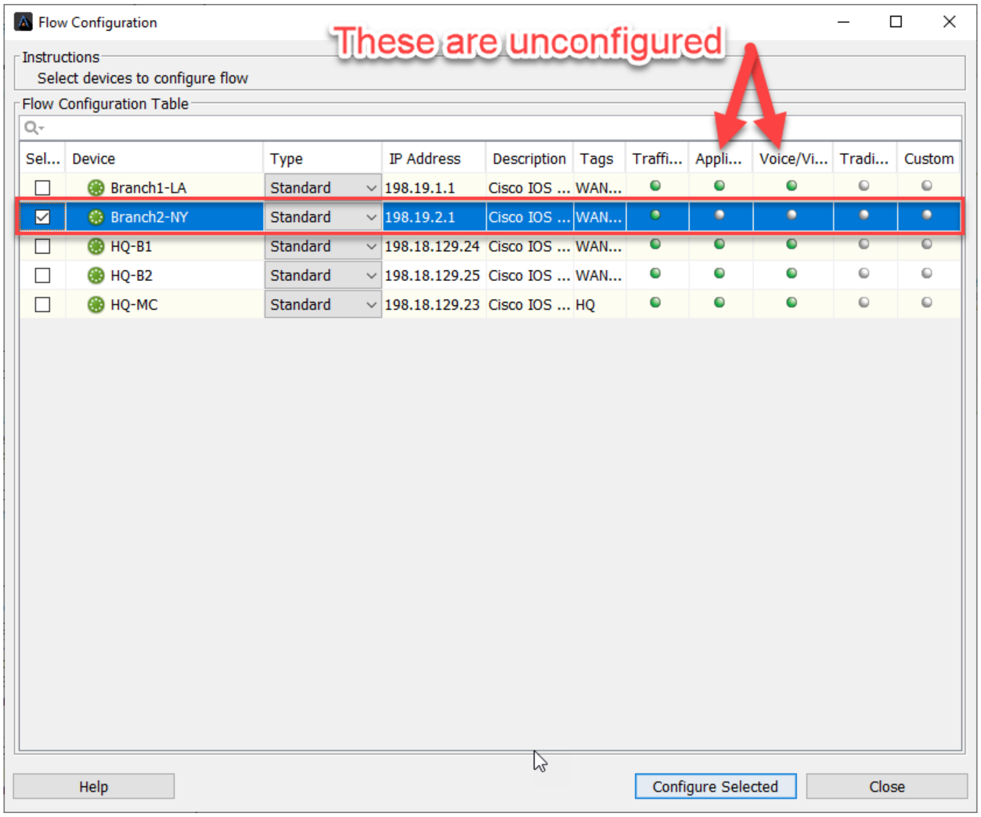
Before removing unwanted interfaces, you should remove any existing flow configurations those interfaces have been configured with… this will avoid any issues when writing new configuration data to the device. In this lab, we will turn on flow for **Branch2-NY** and **HQ-MC.**

Lab Steps:

33. Select **Flow** from the Menu Bar, choose **Configure Flow**.



34. Select **Branch2-NY** and **HQ-MC**, click **Configure Selected**.



Instructions

Select devices to configure flow

Flow Configuration Table

Sel...	Device	Type	IP Address	Description	Tags	Traffi...	Appli...	Voice/Vi...	Tradi...	Custom
☐	Branch1-LA	Standard	198.19.1.1	Cisco IOS ...	WAN...	●	●	●	○	○
☑	Branch2-NY	Standard	198.19.2.1	Cisco IOS ...	WAN...	●	○	○	○	○
☐	HQ-B1	Standard	198.18.129.24	Cisco IOS ...	WAN...	●	●	●	○	○
☐	HQ-B2	Standard	198.18.129.25	Cisco IOS ...	WAN...	●	●	●	○	○
☐	HQ-MC	Standard	198.18.129.23	Cisco IOS ...	HQ	●	●	●	○	○

Note: If the device is grayed-out you must return to the Home tree, right-click on the appropriate device, and select Refresh, before continuing.

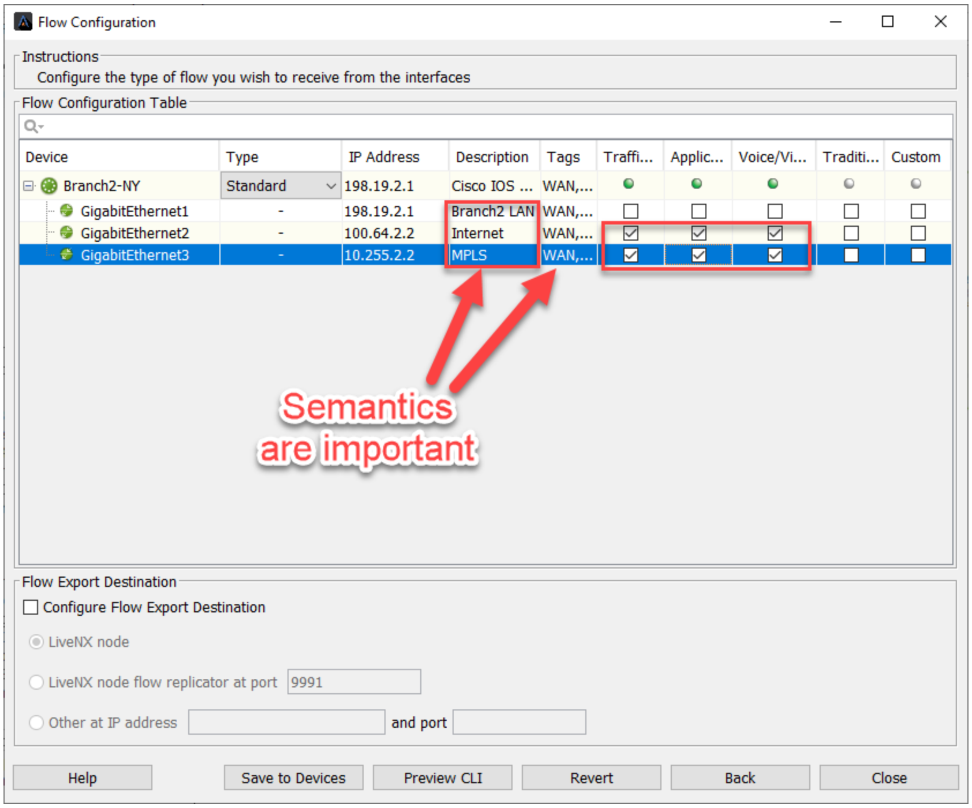
Guidance: Best Practices dictate the following for deciding which interfaces to monitor for flow.

- **WAN interfaces** (rule of thumb, all WAN interfaces on a device, unless there is a reason to not monitor).
- Only Interface for **Router-On-A-Stick**.
- Data Center Devices that are running **East-West traffic**.

Note: Your settings may be different from the screenshot above. Diagrams are for illustration purposes and may not reflect the data you may view on your Training Pod.

35. **Select** Traffic Statistics (FNF), Application Performance (AVC), and Voice/Video (Medianet) on **Branch2-NY** interfaces **GigabitEthernet2** and **GigabitEthernet3**

Note: Your screen should look like that below before moving forward.



Instructions

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

Flow Configuration Table

Device	Type	IP Address	Description	Tags	Traffi...	Applic...	Voice/Vi...	Traditi...	Custom
Branch2-NY	Standard	198.19.2.1	Cisco IOS ...	WAN,...	●	●	●	○	○
GigabitEthernet1	-	198.19.2.1	Branch2 LAN	WAN,...	□	□	□	□	□
GigabitEthernet2	-	100.64.2.2	Internet	WAN,...	☑	☑	☑	□	□
GigabitEthernet3	-	10.255.2.2	MPLS	WAN,...	☑	☑	☑	□	□

Semantics are important

Flow Export Destination

□ Configure Flow Export Destination

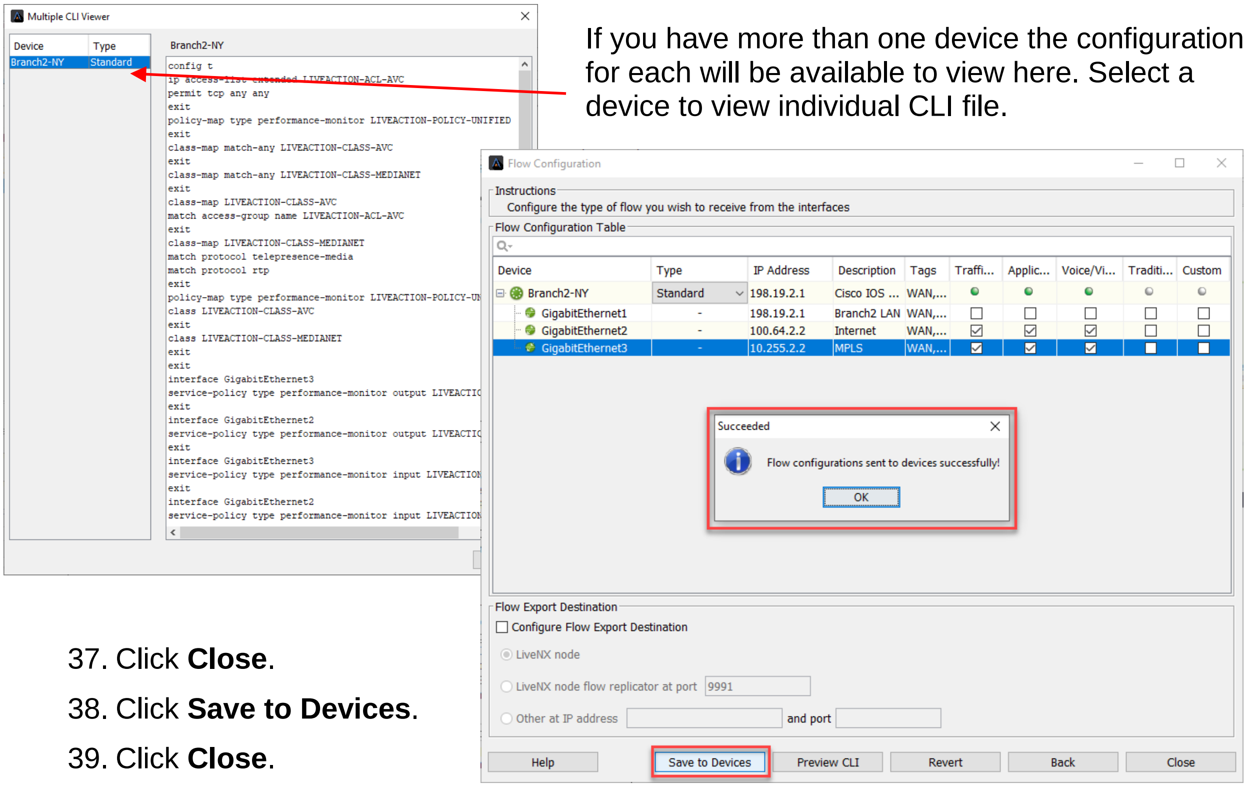
● LiveNX node

○ LiveNX node flow replicator at port 9991

○ Other at IP address and port

36. **Click** Preview CLI.

If you have more than one device the configuration for each will be available to view here. Select a device to view individual CLI file.



Multiple CLI Viewer

Device	Type
Branch2-NY	Standard

Branch2-NY

```
config t
ip access-list extended LIVEACTION-ACL-AVC
permit tcp any any
exit
policy-map type performance-monitor LIVEACTION-POLICY-UNIFIED
exit
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 telepresence-media
match protocol rtp
exit
policy-map type performance-monitor LIVEACTION-POLICY-UN
class LIVEACTION-CLASS-AVC
exit
class LIVEACTION-CLASS-MEDIANET
exit
exit
interface GigabitEthernet3
service-policy type performance-monitor output LIVEACTIC
exit
interface GigabitEthernet2
service-policy type performance-monitor output LIVEACTIC
exit
interface GigabitEthernet3
service-policy type performance-monitor input LIVEACTION
exit
interface GigabitEthernet2
service-policy type performance-monitor input LIVEACTION
```

Flow Configuration

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

Flow Configuration Table

Device	Type	IP Address	Description	Tags	Traffi...	Applic...	Voice/Vi...	Traditi...	Custom
Branch2-NY	Standard	198.19.2.1	Cisco IOS ...	WAN,...	●	●	●	○	○
GigabitEthernet1	-	198.19.2.1	Branch2 LAN	WAN,...	□	□	□	□	□
GigabitEthernet2	-	100.64.2.2	Internet	WAN,...	☑	☑	☑	□	□
GigabitEthernet3	-	10.255.2.2	MPLS	WAN,...	☑	☑	☑	□	□

Succeeded

Flow configurations sent to devices successfully!

OK

Flow Export Destination

□ Configure Flow Export Destination

○ LiveNX node

○ LiveNX node flow replicator at port 9991

○ Other at IP address and port

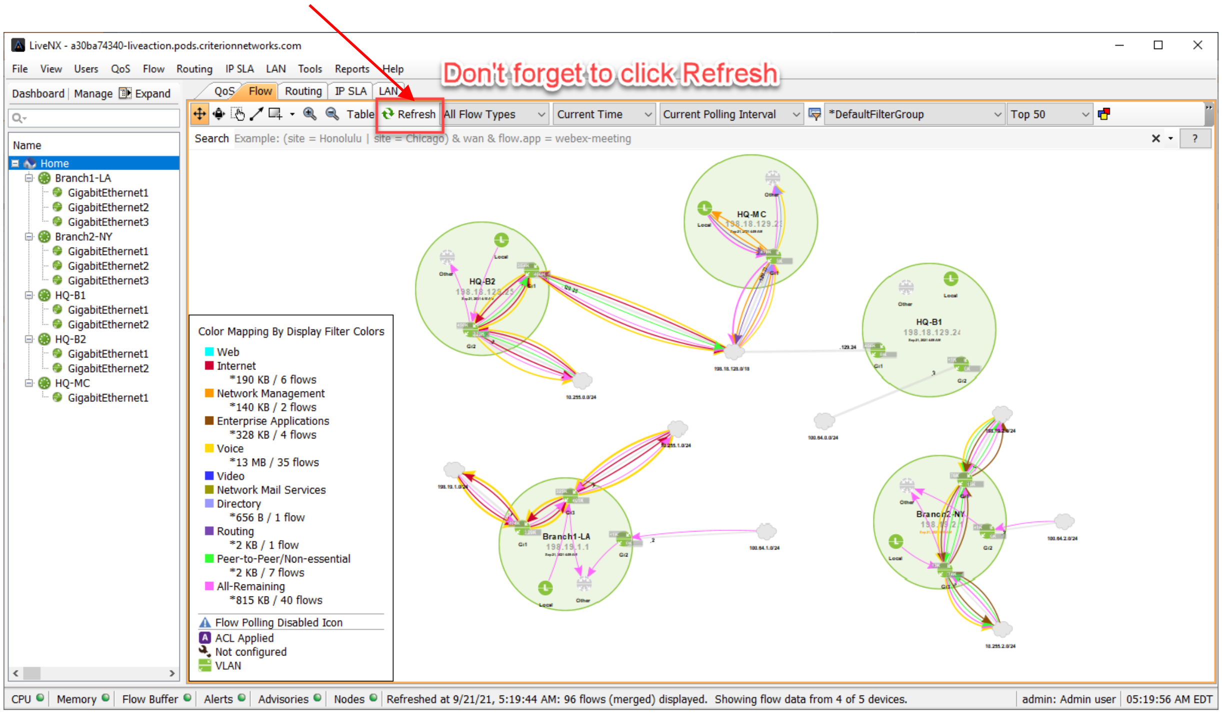
37. Click **Close**.

38. Click **Save to Devices**.

39. Click **Close**.

Note: Now that we've configured Flow Collection on **Branch2-NY**… we'll be able to view flows on all devices in the Topology Pane!

40. Don't forget to click **Refresh** in the Filter Bar.



Don't forget to click Refresh

LiveNX - a30ba74340-liveaction.pods.criterionnetworks.com

File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expand
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval *DefaultFilterGroup Top 50

Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

Name
- Home
  - Branch1-LA
    - GigabitEthernet1
    - GigabitEthernet2
    - GigabitEthernet3
  - Branch2-NY
    - GigabitEthernet1
    - GigabitEthernet2
    - GigabitEthernet3
  - HQ-B1
    - GigabitEthernet1
    - GigabitEthernet2
  - HQ-B2
    - GigabitEthernet1
    - GigabitEthernet2
  - HQ-MC
    - GigabitEthernet1

Color Mapping By Display Filter Colors

- 🟦 Web
- 🟥 Internet
  *190 KB / 6 flows
- 🟧 Network Management
  *140 KB / 2 flows
- 🟫 Enterprise Applications
  *328 KB / 4 flows
- 🟨 Voice
  *13 MB / 35 flows
- 🟦 Video
- 🟩 Network Mail Services
- 🟪 Directory
  *656 B / 1 flow
- 🟪 Routing
  *2 KB / 1 flow
- 🟩 Peer-to-Peer/Non-essential
  *2 KB / 7 flows
- 🟪 All-Remaining
  *815 KB / 40 flows

⚠ Flow Polling Disabled Icon
A ACL Applied
Not configured
VLAN

CPU ● Memory ● Flow Buffer ● Alerts ● Advisories ● Nodes ● Refreshed at 9/21/21, 5:19:44 AM: 96 flows (merged) displayed. Showing flow data from 4 of 5 devices. admin: Admin user 05:19:56 AM EDT

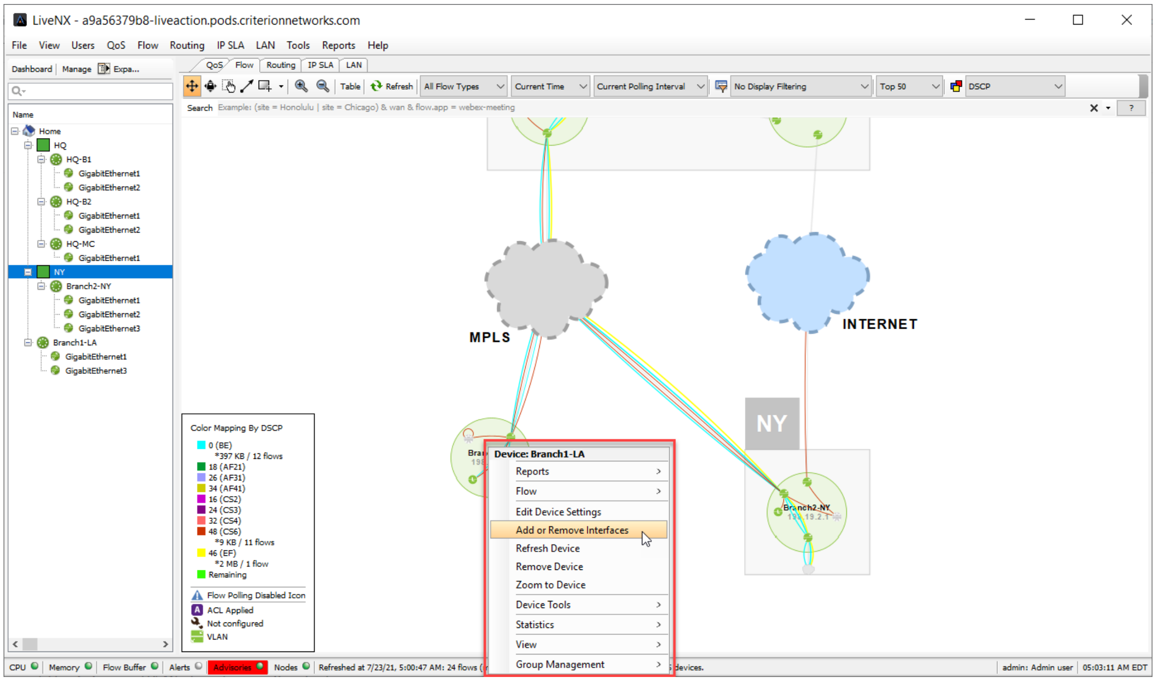
Lab 3.4: Add/Remove Interfaces

You can add or remove any interfaces as your network evolves. This action removes the interface from LiveNX, not from the router configuration.

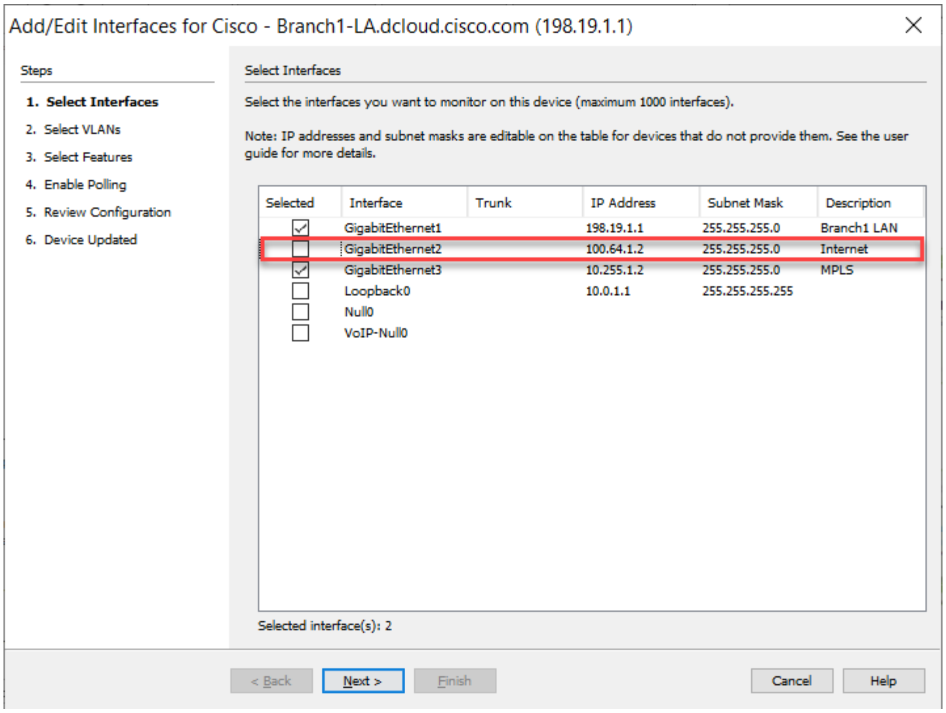
Note: Your Instructor may have already performed this process when they configured your Training Pod.

Lab Steps:

41. Right-click on the **Branch1-LA** device and **select** Add or Remove Interfaces.



42. Deselect **GigabitEthernet2**.


Add/Edit Interfaces for Cisco - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Steps

1. **Select Interfaces**
2. Select VLANs
3. Select Features
4. Enable Polling
5. Review Configuration
6. Device Updated

Select Interfaces

Select the interfaces you want to monitor on this device (maximum 1000 interfaces).

Note: IP addresses and subnet masks are editable on the table for devices that do not provide them. See the user guide for more details.

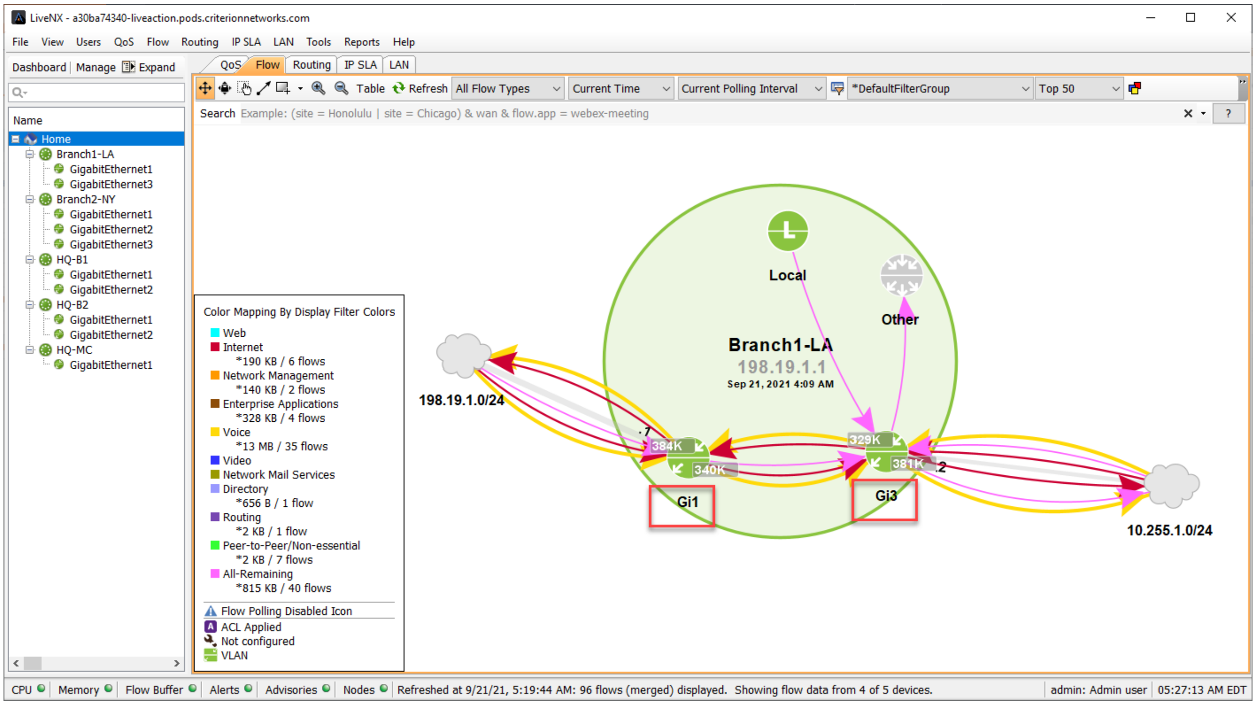
Selected	Interface	Trunk	IP Address	Subnet Mask	Description
☑	GigabitEthernet1		198.19.1.1	255.255.255.0	Branch1 LAN
☐	GigabitEthernet2		100.64.1.2	255.255.255.0	Internet
☑	GigabitEthernet3		10.255.1.2	255.255.255.0	MPLS
☐	Loopback0		10.0.1.1	255.255.255.255	
☐	Null0				
☐	VoIP-Null0				

Selected interface(s): 2

43. Select **Next** until the **Device Updated** window is displayed.

44. Select **Finish** to update the device.

Notice that the device now has 2 active interfaces, represented by **GigabitEthernet1** and **GigabtEthernet3**



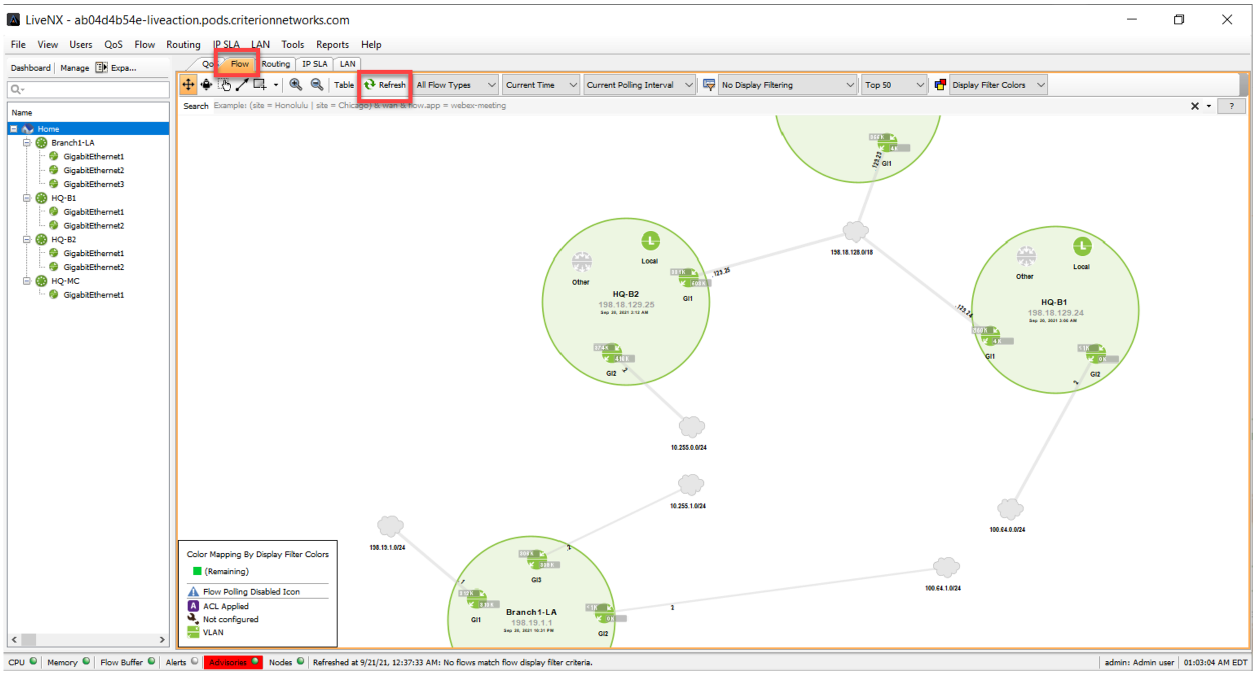
Refreshed at 9/21/21, 5:19:44 AM: 96 flows (merged) displayed. Showing flow data from 4 of 5 devices.

45. Repeat from Lab Step 1 above to perform interface addition/removal on **Branch2-NY** (as needed).

Note: You may also remove multiple interfaces at a time from multiple devices. See the Appendix for instructions to Export/Import Devices.

Lab 3.5: Merge Clouds in Topology

Now that the LiveNX topology has discovered devices, and you've defined the correct interfaces and NetFlow configurations, you may Refresh your Flow Tab to view any network flows collected in the Current Polling Interval.


LiveNX - ab04d4b54e-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expa...
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval No Display Filtering Top 50 Display Filter Colors
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
Branch1-LA
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
HQ-B1
GigabitEthernet1
GigabitEthernet2
HQ-B2
GigabitEthernet1
GigabitEthernet2
HQ-MC
GigabitEthernet1
HQ-B2
198.18.129.25
HQ-B1
198.18.129.24
Branch1-LA
198.19.1.1
198.18.128.0/18
10.255.0.0/24
10.255.1.0/24
198.19.1.0/24
100.64.0.0/24
100.64.1.0/24
Color Mapping By Display Filter Colors
(Remaining)
Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN
CPU Memory Flow Buffer Alerts Advisories Nodes
admin: Admin user 01:03:04 AM EDT

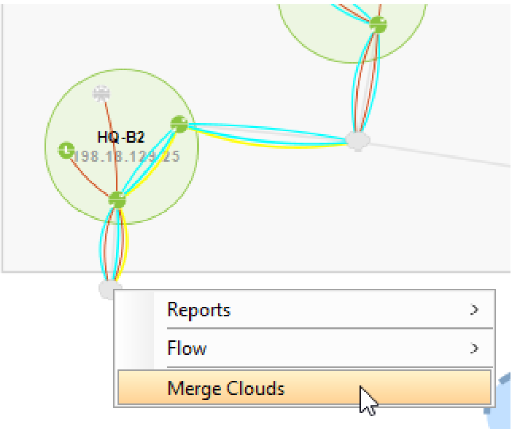
Refreshed at 9/21/21, 12:37:33 AM: No flows match flow display filter criteria.

Notice on your topology that the *network clouds* are not connecting between devices. Since these clouds are across a service provider it is necessary to merge the clouds so that NetFlow can be properly visualized across the topology.

Note: You must be in the Topology Pane to perform these steps. Click Home to ensure.

Lab Steps:

46. Right-click on the HQ-B2 Device's **GigabitEthernet2** 10.255.0.0/24 network cloud and select Merge Clouds.

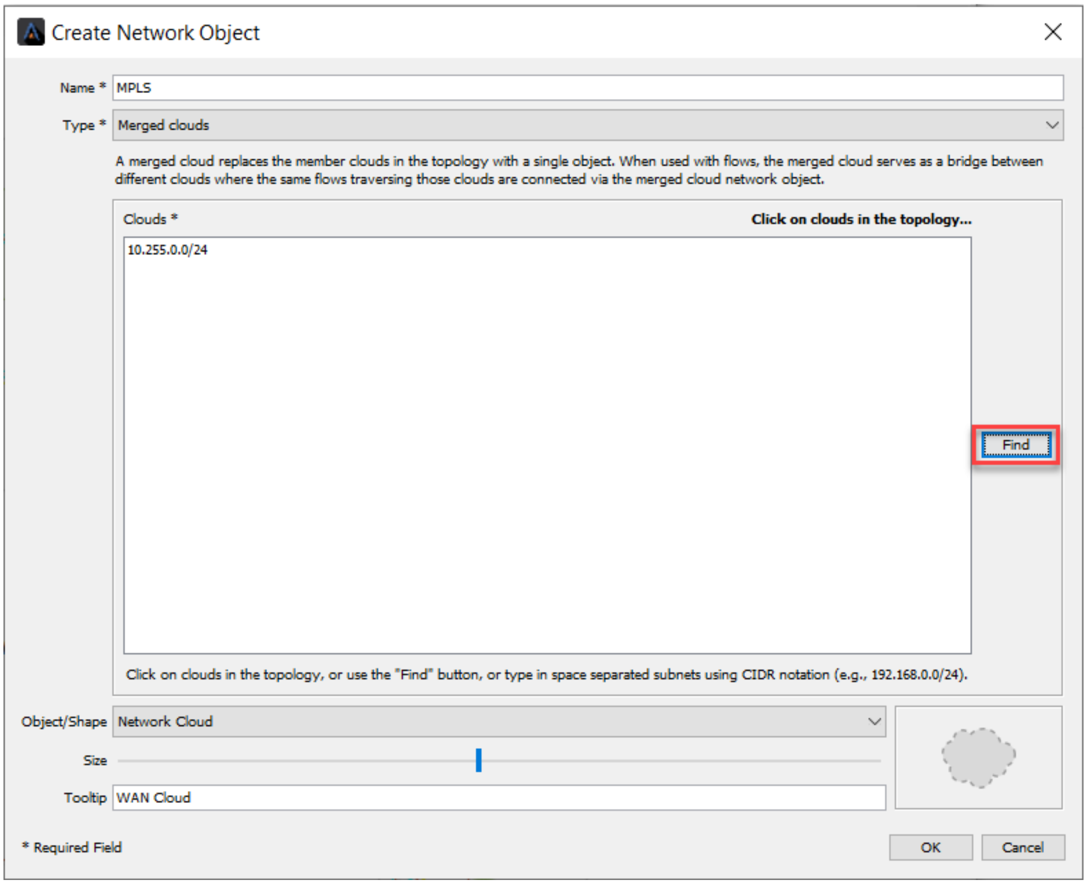


47. On the Create Network Object dialog and configure the **Network Name** (This could be your Service Provider, or Transport ID) We have used **MPLS**.

48. Select the **Object/Shape** as appropriate and useful for simple visual recognition.

Note: You may also give the tooltip a name of WAN Cloud.

49. Select “**Find**” to add more networks.



Create Network Object

Name * MPLS

Type * Merged clouds

A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud network object.

Clouds * **Click on clouds in the topology...**

10.255.0.0/24

Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).

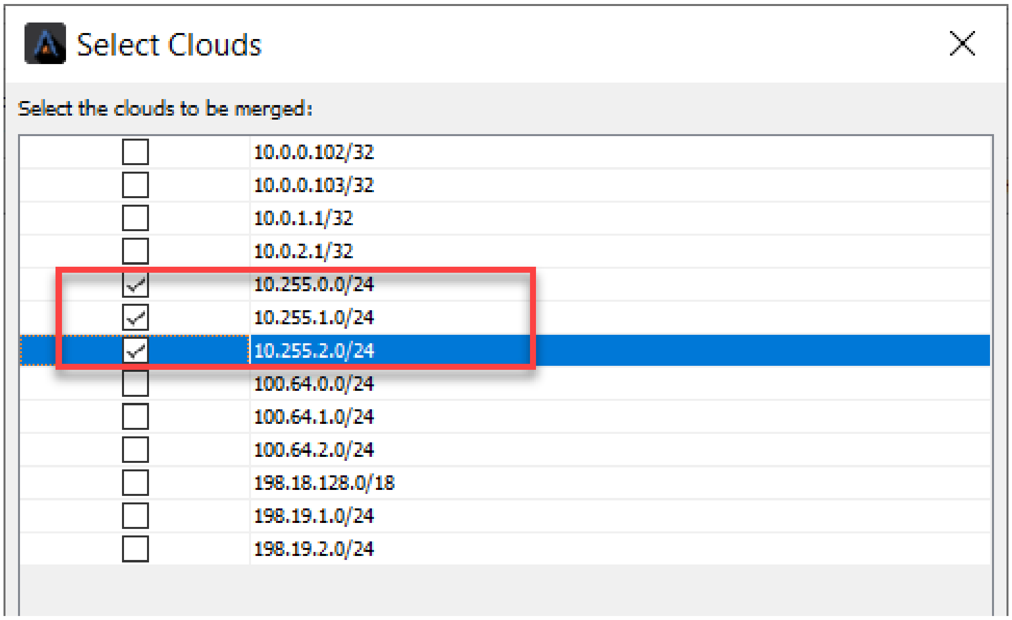
Object/Shape Network Cloud

Size

Tooltip WAN Cloud

* Required Field

50. Select the following networks and then select ok:
10.255.0.0/24
10.255.1.0/24
10.255.2.0/24



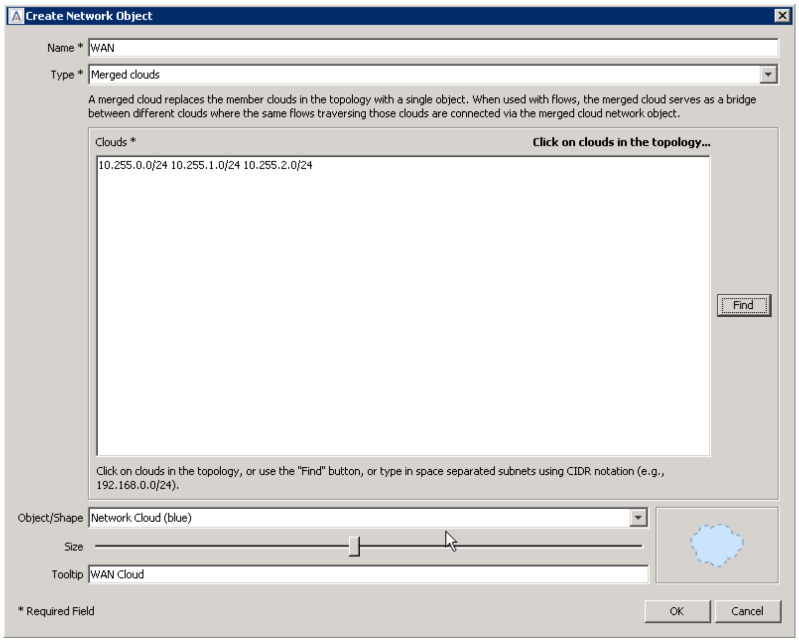
Select Clouds

Select the clouds to be merged:

☐ 10.0.0.102/32
☐ 10.0.0.103/32
☐ 10.0.1.1/32
☐ 10.0.2.1/32
☑ 10.255.0.0/24
☑ 10.255.1.0/24
☑ 10.255.2.0/24
☐ 100.64.0.0/24
☐ 100.64.1.0/24
☐ 100.64.2.0/24
☐ 198.18.128.0/18
☐ 198.19.1.0/24
☐ 198.19.2.0/24

51. Click **OK**.

52. Click **OK** to finish.



Name * WAN

Type * Merged clouds

A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud network object.

Clouds * **Click on clouds in the topology...**

10.255.0.0/24 10.255.1.0/24 10.255.2.0/24

Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).

Object/Shape Network Cloud (blue)

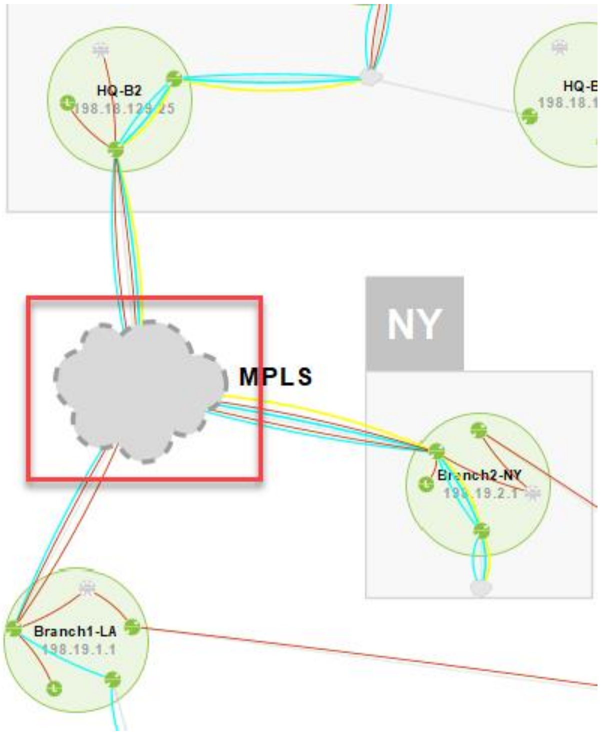
Size

Tooltip WAN Cloud

* Required Field

Now all three devices should have a link to the WAN Merged cloud. Try moving the devices around to create a topology view which makes sense for you.

53. Click the Refresh button in the Flow tab to query flows from the devices and draw them on the topology.



Lab 4

Lab 4: Traffic Flows

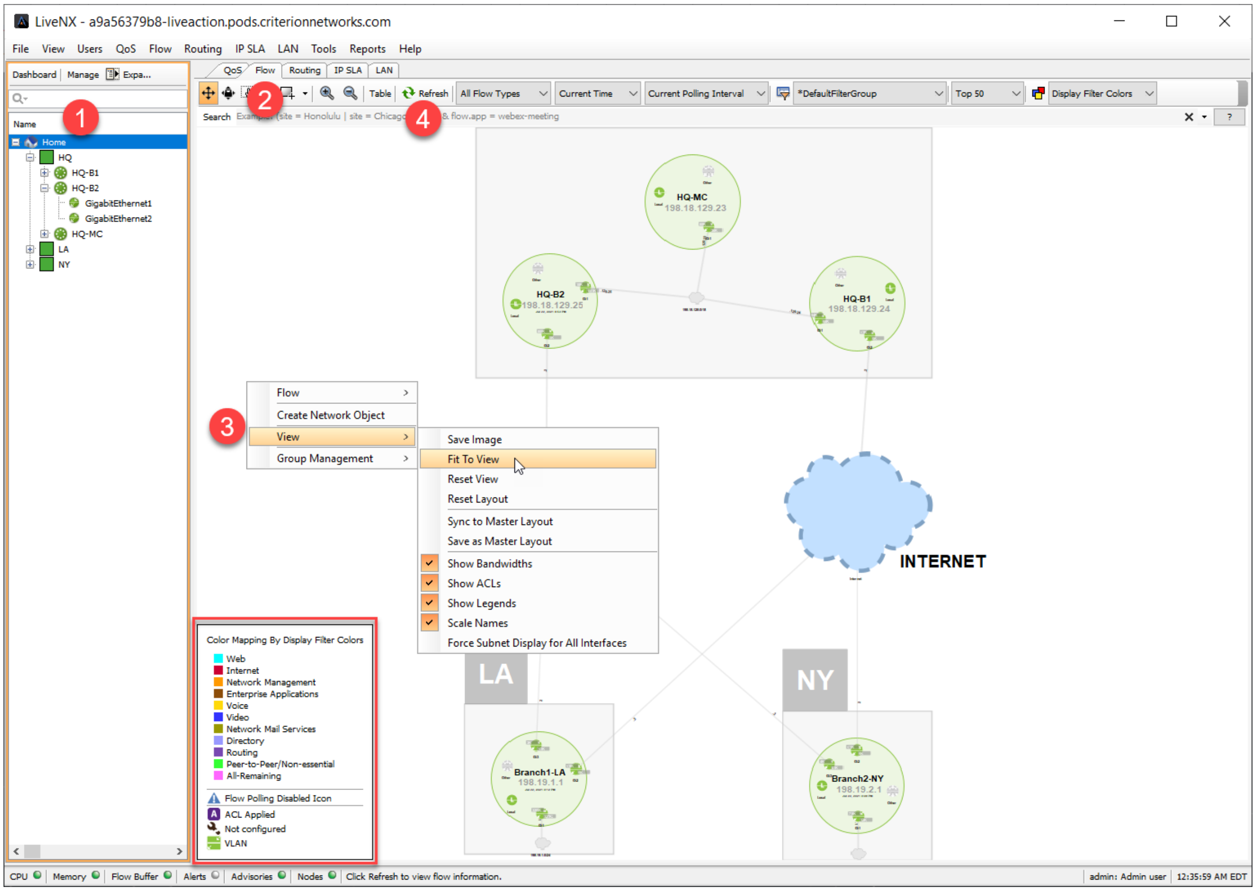
Lab 4.1: Discover Flows

One of the strongest features of LiveNX is its ability to differentiate traffic flows by collecting NetFlow & SNMP from devices and mapping the flows visually in the LiveNX Client Topology Pane.

In this Lab we need to find the address pair which has been generating so much FTP traffic over the past few hours. We can make it easy to find with the application of just a few Filter Bar selections!

Lap Steps:

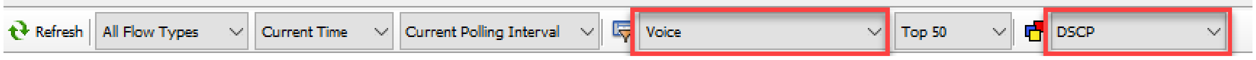
1. Select **Home** level of the topology.
2. Select the **Flow** Tab.
3. Reset the view to **Fit To View**.
4. Refresh the **Topology** Pane.


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expa...
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval *DefaultFilterGroup Top 50 Display Filter Colors
Search Examples: (site = Honolulu | site = Chicago) & flow.app = webex-meeting
Name
Home
HQ
HQ-B1
HQ-B2
GigabitEthernet1
GigabitEthernet2
HQ-MC
LA
NY
1
2
3
4
HQ-MC 198.18.129.23
HQ-B2 198.18.129.25
HQ-B1 198.18.129.24
Flow
Create Network Object
View
Group Management
Save Image
Fit To View
Reset View
Reset Layout
Sync to Master Layout
Save as Master Layout
Show Bandwidths
Show ACLs
Show Legends
Scale Names
Force Subnet Display for All Interfaces
INTERNET
LA
NY
Branch1-LA 198.19.1.1
Branch2-NY 198.19.2.1
Color Mapping By Display Filter Colors
Web
Internet
Network Management
Enterprise Applications
Voice
Video
Network Mail Services
Directory
Routing
Peer-to-Peer/Non-essential
All-Remaining
Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN
CPU Memory Flow Buffer Alerts Advisories Nodes Click Refresh to view flow information.
admin: Admin user 12:35:59 AM EDT

You'll note some traffic, but even referring to the legend at the bottom-left corner may not help identify the specific flows!

5. Set the filters to match:

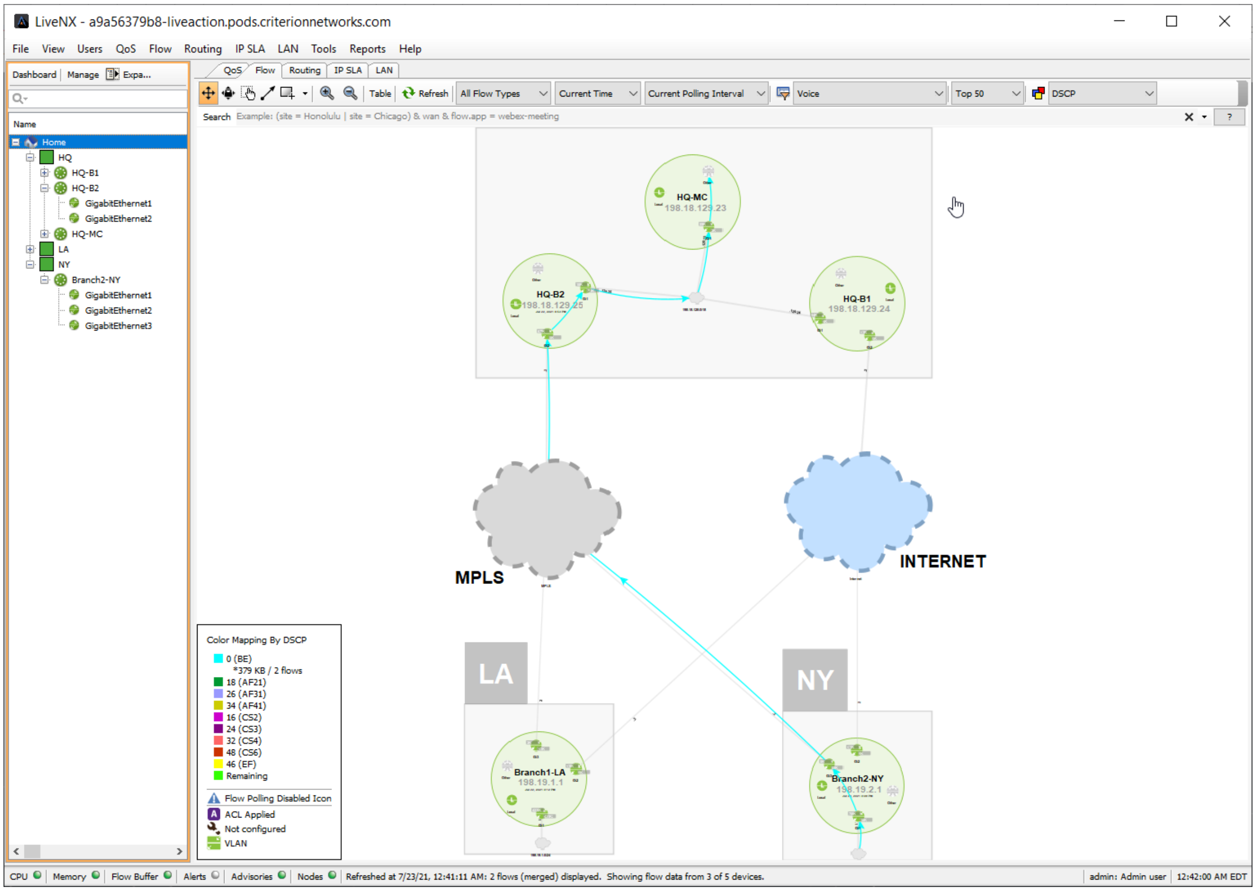
Note: Make sure to specify **Voice** for Display Filtering, and **DSCP** for color marking.



Refresh | All Flow Types | Current Time | Current Polling Interval | Voice | Top 50 | DSCP

6. Refresh the **Topology** Pane, if needed.

See how easy that was? The following screen shot clearly shows the Voice traffic.



All Flow Types | Current Time | Current Polling Interval | Voice | Top 50 | DSCP

Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

Color Mapping By DSCP

- 🟦 0 (BE)
  *379 KB / 2 flows
- 🟩 18 (AF21)
- 🟪 26 (AF31)
- 🟨 34 (AF41)
- 🟪 16 (CS2)
- 🟪 24 (CS3)
- 🟥 32 (CS4)
- 🟥 48 (CS6)
- 🟨 46 (EF)
- 🟩 Remaining

Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN

Refreshed at 7/23/21, 12:41:11 AM: 2 flows (merged) displayed. Showing flow data from 3 of 5 devices.

admin: Admin user | 12:42:00 AM EDT

7. **Hover** over the colored lines to see the volume of Voice transmissions.
8. **Click** on the colored flow line to see the IP endpoints.

What other applications can you identify across our network?

Application Port# IP Pairs

______________________ _____ ______________________

______________________ _____ ______________________

______________________ _____ ______________________

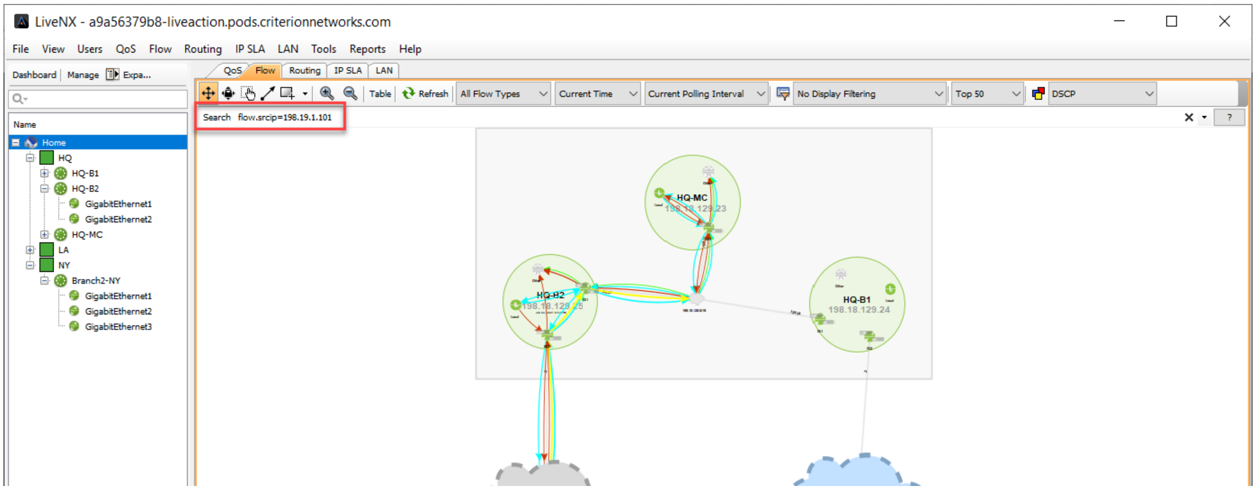
______________________ _____ ______________________

______________________ _____ ______________________

Lab 4.2: Discover Specific Flows

Note: You must be in the Topology Pane to perform these steps. Click Home to ensure.

1. In the **Search** bar, at the top left of the Topology pane enter a search string of "flow.srcip=198.19.1.101".
2. Select **No Display Filtering**.
3. Click **Refresh**
4. Click on the displayed flow indicator.



All Flow Types | Current Time | Current Polling Interval | No Display Filtering | Top 50 | DSCP

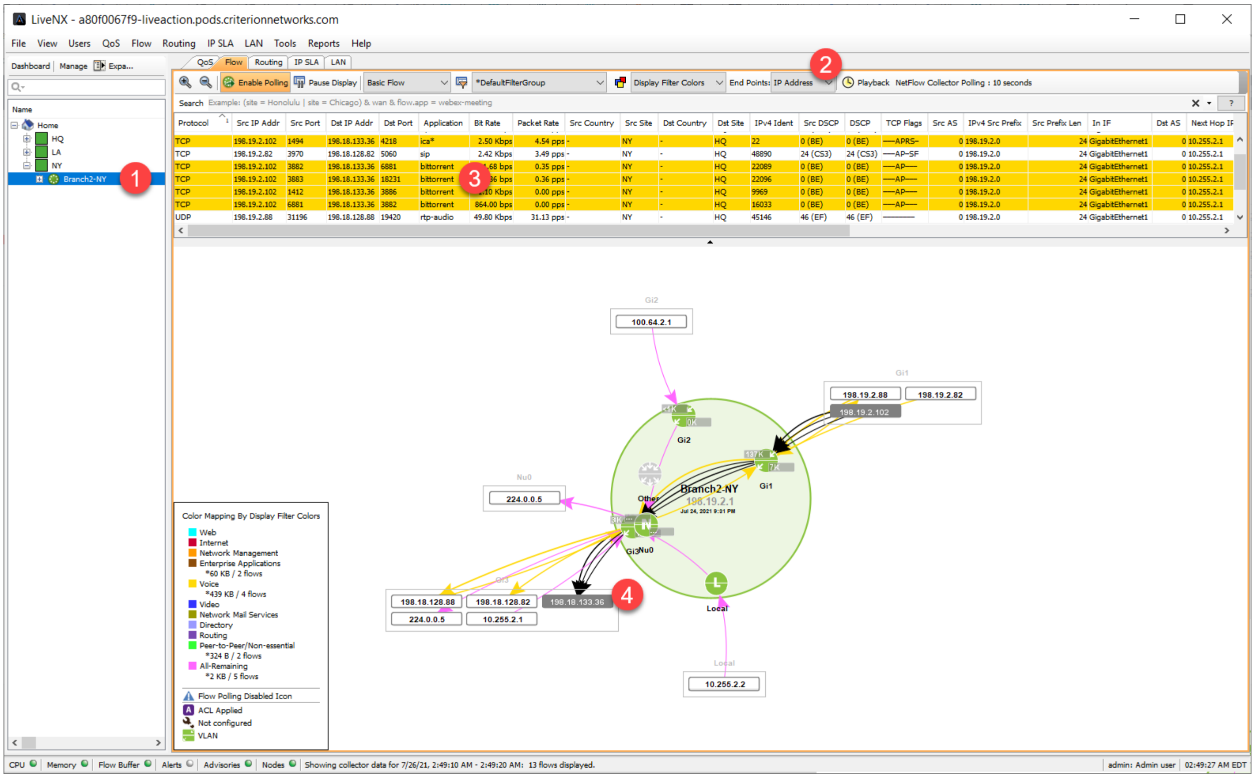
Search flow.srcip=198.19.1.101

Notice that LiveNX has identified one or more *end-to-end* flows across the network.

Lab 4.3: Examine Specific Traffic

Another way to quickly discover flows among IP Addresses is to use the Device View * Table. Let's discover where most of our BitTorrent traffic is sourced in our NY Branch.

1. Double-click on the Branch2-NY Device or select it on the Home Tree.
2. Select **IP Addresses** as the endpoint display type



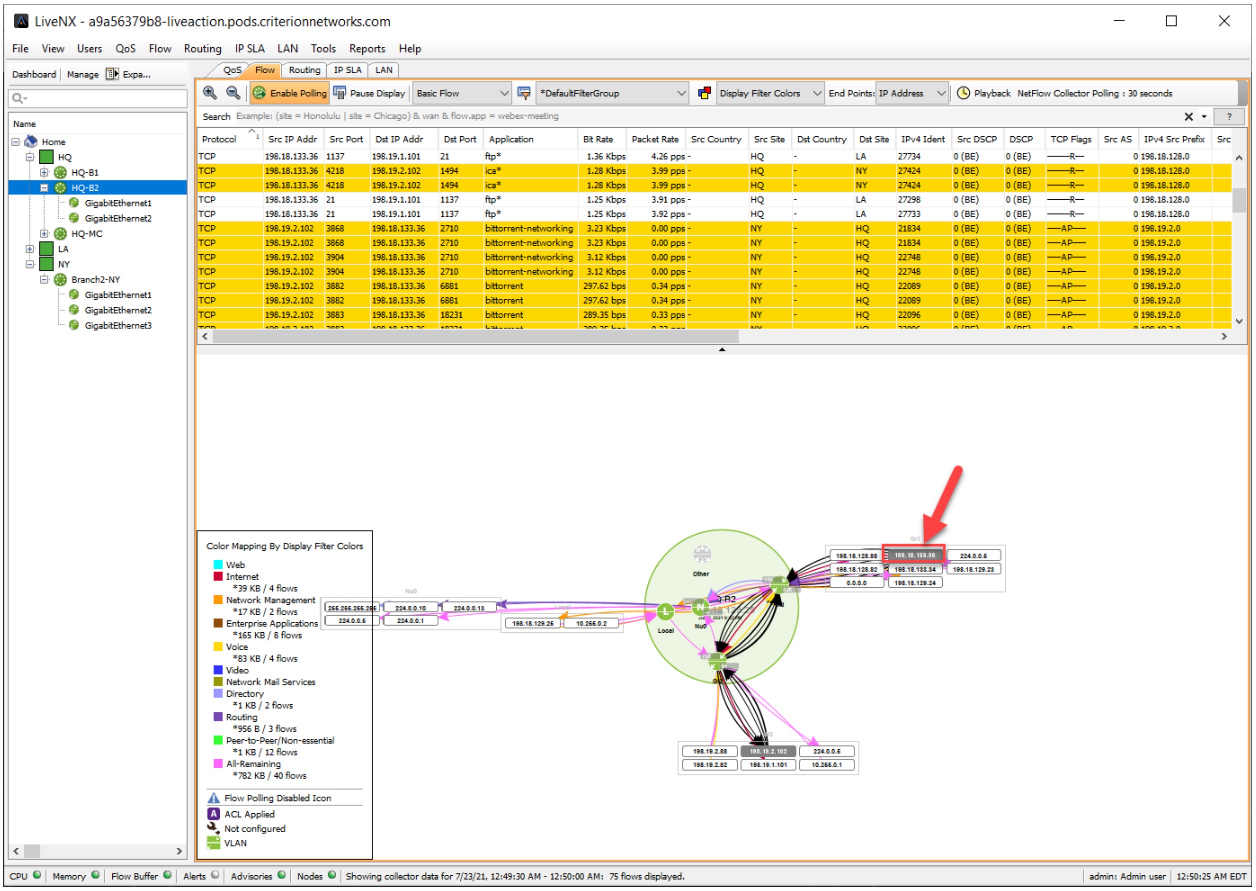
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Bit Rate	Packet Rate	Src Country	Src Site	Dst Country	Dst Site	IPv4 Ident	Src DSCP	DSCP	TCP Flags	Src AS	IPv4 Src Prefix	Src Prefix Len	In IF	Dst AS	Next Hop IP
TCP	198.19.2.102	1494	198.18.133.36	4218	ica*	2.50 Kbps	4.54 pps	-	NY	-	HQ	22	0 (BE)	0 (BE)	——APRS–	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
TCP	198.19.2.82	3970	198.18.128.82	5060	sip	2.42 Kbps	3.49 pps	-	NY	-	HQ	48890	24 (CS3)	24 (CS3)	——AP–SF	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
TCP	198.19.2.102	3882	198.18.133.36	6881	bittorrent	.68 bps	0.35 pps	-	NY	-	HQ	22089	0 (BE)	0 (BE)	——AP——	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
TCP	198.19.2.102	3883	198.18.133.36	18231	bittorrent	36 bps	0.36 pps	-	NY	-	HQ	22096	0 (BE)	0 (BE)	——AP——	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
TCP	198.19.2.102	1412	198.18.133.36	3886	bittorrent	.10 Kbps	0.00 pps	-	NY	-	HQ	9969	0 (BE)	0 (BE)	——AP——	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
TCP	198.19.2.102	6881	198.18.133.36	3882	bittorrent	864.00 bps	0.00 pps	-	NY	-	HQ	16033	0 (BE)	0 (BE)	——AP——	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1
UDP	198.19.2.88	31196	198.18.128.88	19420	rtp-audio	49.80 Kbps	31.13 pps	-	NY	-	HQ	45146	46 (EF)	46 (EF)	———	0	198.19.2.0	24	GigabitEthernet1	0	10.255.2.1

Showing collector data for 7/26/21, 2:49:10 AM - 2:49:20 AM: 13 flows displayed.

Almost too easy, wasn't it? What are the IP endpoints of all that BitTorrent traffic?

________________ to/from _______________

3. Click on one of the endpoints.


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expa...
Name
Home
HQ
HQ-B1
HQ-B2
GigabitEthernet1
GigabitEthernet2
HQ-MC
LA
NY
Branch2-NY
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
QoS Flow Routing IP SLA LAN
Enable Polling
Pause Display
Basic Flow
*DefaultFilterGroup
Display Filter Colors
End Points: IP Address
Playback NetFlow Collector Polling : 30 seconds
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Other
Local
Nu0

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Bit Rate	Packet Rate	Src Country	Src Site	Dst Country	Dst Site	IPv4 Ident	Src DSCP	DSCP	TCP Flags	Src AS	IPv4 Src Prefix	Src
TCP	198.18.133.36	1137	198.19.1.101	21	ftp*	1.36 Kbps	4.26 pps	-	HQ	-	LA	27734	0 (BE)	0 (BE)	——R—	0	198.18.128.0	
TCP	198.18.133.36	4218	198.19.2.102	1494	ica*	1.28 Kbps	3.99 pps	-	HQ	-	NY	27424	0 (BE)	0 (BE)	——R—	0	198.18.128.0	
TCP	198.18.133.36	4218	198.19.2.102	1494	ica*	1.28 Kbps	3.99 pps	-	HQ	-	NY	27424	0 (BE)	0 (BE)	——R—	0	198.18.128.0	
TCP	198.18.133.36	21	198.19.1.101	1137	ftp*	1.25 Kbps	3.91 pps	-	HQ	-	LA	27298	0 (BE)	0 (BE)	——R—	0	198.18.128.0	
TCP	198.18.133.36	21	198.19.1.101	1137	ftp*	1.25 Kbps	3.92 pps	-	HQ	-	LA	27733	0 (BE)	0 (BE)	——R—	0	198.18.128.0	
TCP	198.19.2.102	3868	198.18.133.36	2710	bittorrent-networking	3.23 Kbps	0.00 pps	-	NY	-	HQ	21834	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3868	198.18.133.36	2710	bittorrent-networking	3.23 Kbps	0.00 pps	-	NY	-	HQ	21834	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3904	198.18.133.36	2710	bittorrent-networking	3.12 Kbps	0.00 pps	-	NY	-	HQ	22748	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3904	198.18.133.36	2710	bittorrent-networking	3.12 Kbps	0.00 pps	-	NY	-	HQ	22748	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3882	198.18.133.36	6881	bittorrent	297.62 bps	0.34 pps	-	NY	-	HQ	22089	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3882	198.18.133.36	6881	bittorrent	297.62 bps	0.34 pps	-	NY	-	HQ	22089	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	
TCP	198.19.2.102	3883	198.18.133.36	18231	bittorrent	289.35 bps	0.33 pps	-	NY	-	HQ	22096	0 (BE)	0 (BE)	—AP—	0	198.19.2.0	

Color Mapping By Display Filter Colors

- 🟦 Web
- 🟥 Internet
  - *39 KB / 4 flows
- 🟧 Network Management
  - *17 KB / 2 flows
- 🟫 Enterprise Applications
  - *165 KB / 8 flows
- 🟨 Voice
  - *83 KB / 4 flows
- 🟦 Video
- 🟩 Network Mail Services
- 🟪 Directory
  - *1 KB / 2 flows
- 🟪 Routing
  - *956 B / 3 flows
- 🟩 Peer-to-Peer/Non-essential
  - *1 KB / 12 flows
- 🟪 All-Remaining
  - *782 KB / 40 flows

- Flow Polling Disabled Icon
- ACL Applied
- Not configured
- VLAN

CPU | Memory | Flow Buffer | Alerts | Advisories | Nodes | Showing collector data for 7/23/21, 12:49:30 AM - 12:50:00 AM: 75 flows displayed. | admin: Admin user | 12:50:25 AM EDT

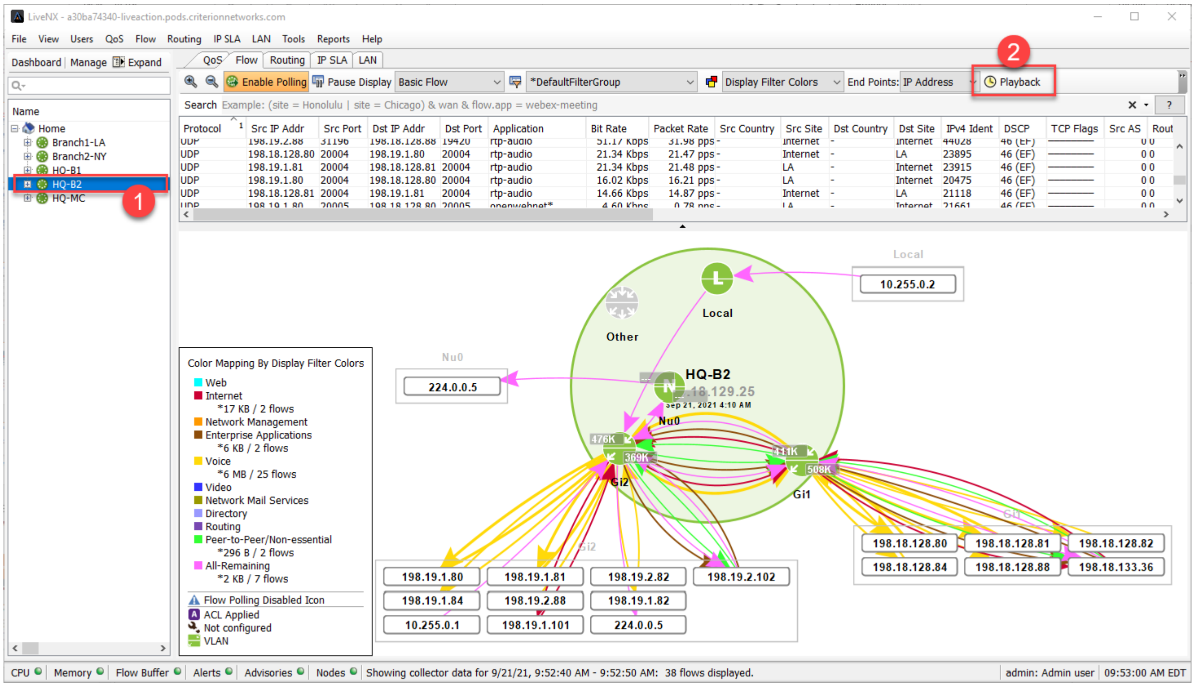
There is some other traffic, such as rtp, sip, and Citrix… but these 2 IPs are mostly generating BitTorrent. Make sure there isn’t a ghost server in your network serving movies and such!

Lab 4.4: Troubleshoot Issues

Users in the Marketing Department at our San Jose Headquarters have been complaining that their workstations seem to be "slowing down" numerous times a day. A pattern is developing that this happens about 4x per hour!

It looks as though we may have an infected PC on the HQ sub-net… we need to identify the source PC by IP Address so that we can re-load anti-virus software on the identified user's workstation.

1. Open the **HQ-B2** device. Double-click on it OR select from the **Home Tree** view.
2. Click the **Playback** button in the **Filter Bar**.



Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Bit Rate	Packet Rate	Src Country	Src Site	Dst Country	Dst Site	IPv4 Ident	DSCP	TCP Flags	Src AS	Rout
UDP	198.19.2.88	31196	198.18.128.88	19420	rtp-audio	51.17 Kbps	31.98 pps	-	Internet	-	Internet	44028	46 (EF)	———	0	0
UDP	198.18.128.80	20004	198.19.1.80	20004	rtp-audio	21.34 Kbps	21.47 pps	-	Internet	-	LA	23895	46 (EF)	———	0	0
UDP	198.19.1.81	20004	198.18.128.81	20004	rtp-audio	21.34 Kbps	21.48 pps	-	LA	-	Internet	23915	46 (EF)	———	0	0
UDP	198.19.1.80	20004	198.18.128.80	20004	rtp-audio	16.02 Kbps	16.21 pps	-	LA	-	Internet	20475	46 (EF)	———	0	0
UDP	198.18.128.81	20004	198.19.1.81	20004	rtp-audio	14.66 Kbps	14.87 pps	-	Internet	-	LA	21118	46 (EF)	———	0	0
UDP	198.19.1.80	20005	198.18.128.80	20005	openwebnet*	4.60 Kbps	0.78 pps	-	LA	-	Internet	21661	46 (EF)	———	0	0

Color Mapping By Display Filter Colors

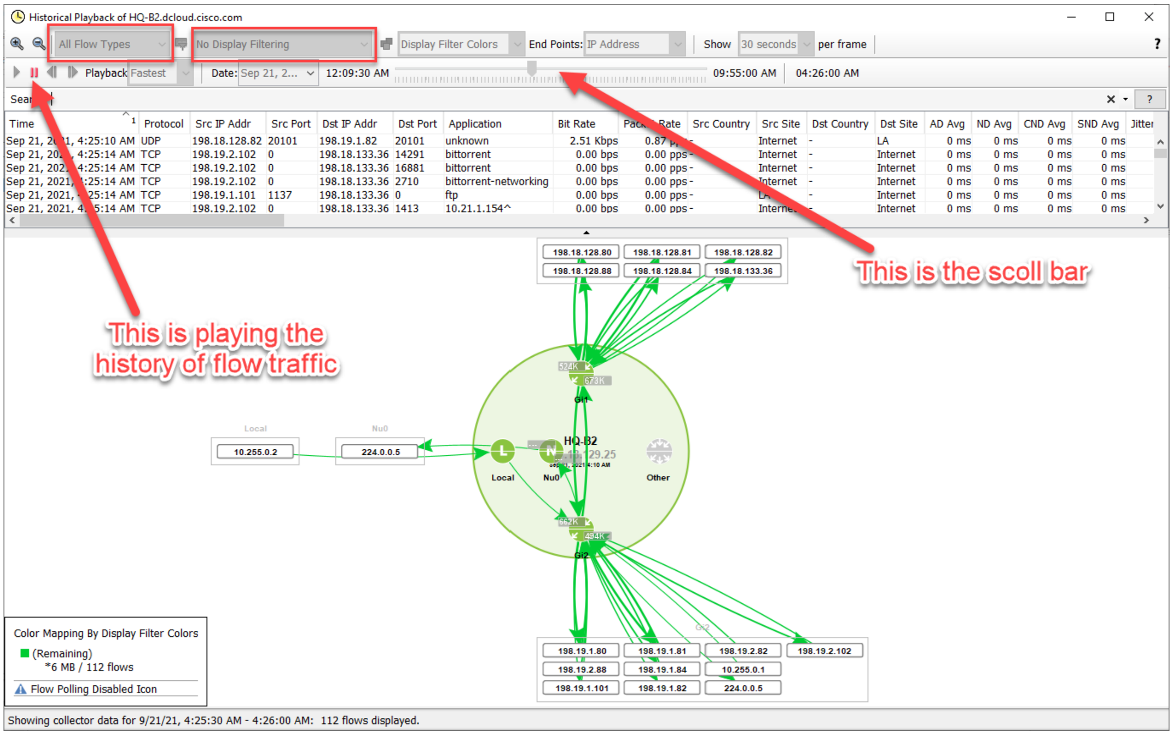
- 🟦 Web
- 🟥 Internet
  - *17 KB / 2 flows
- 🟧 Network Management
- 🟫 Enterprise Applications
  - *6 KB / 2 flows
- 🟨 Voice
  - *6 MB / 25 flows
- 🟦 Video
- 🟩 Network Mail Services
- 🟪 Directory
- 🟪 Routing
- 🟩 Peer-to-Peer/Non-essential
  - *296 B / 2 flows
- 🟪 All-Remaining
  - *2 KB / 7 flows

⚠ Flow Polling Disabled Icon

- A ACL Applied
- Not configured
- VLAN

CPU ● | Memory ● | Flow Buffer ● | Alerts ● | Advisories ● | Nodes ● | Showing collector data for 9/21/21, 9:52:40 AM - 9:52:50 AM: 38 flows displayed. | admin: Admin user | 09:53:00 AM EDT

3. Scroll through the time display until you discover anomalous behavior.



Historical Playback of HQ-B2.dcloud.cisco.com

All Flow Types | No Display Filtering | Display Filter Colors | End Points: IP Address | Show 30 seconds per frame

Playback Fastest | Date: Sep 21, 2... | 12:09:30 AM | 09:55:00 AM | 04:26:00 AM

Search

Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Bit Rate	Packet Rate	Src Country	Src Site	Dst Country	Dst Site	AD Avg	ND Avg	CND Avg	SND Avg	Jitter
Sep 21, 2021, 4:25:10 AM	UDP	198.18.128.82	20101	198.19.1.82	20101	unknown	2.51 Kbps	0.87 pps	-	Internet	-	LA	0 ms	0 ms	0 ms	0 ms	
Sep 21, 2021, 4:25:14 AM	TCP	198.19.2.102	0	198.18.133.36	14291	bittorrent	0.00 bps	0.00 pps	-	Internet	-	Internet	0 ms	0 ms	0 ms	0 ms	
Sep 21, 2021, 4:25:14 AM	TCP	198.19.2.102	0	198.18.133.36	16881	bittorrent	0.00 bps	0.00 pps	-	Internet	-	Internet	0 ms	0 ms	0 ms	0 ms	
Sep 21, 2021, 4:25:14 AM	TCP	198.19.2.102	0	198.18.133.36	2710	bittorrent-networking	0.00 bps	0.00 pps	-	Internet	-	Internet	0 ms	0 ms	0 ms	0 ms	
Sep 21, 2021, 4:25:14 AM	TCP	198.19.1.101	1137	198.18.133.36	0	ftp	0.00 bps	0.00 pps	-	LA	-	Internet	0 ms	0 ms	0 ms	0 ms	
Sep 21, 2021, 4:25:14 AM	TCP	198.19.2.102	0	198.18.133.36	1413	10.21.1.154^	0.00 bps	0.00 pps	-	Internet	-	Internet	0 ms	0 ms	0 ms	0 ms	

This is the scoll bar

This is playing the history of flow traffic

Color Mapping By Display Filter Colors

🟩 (Remaining)
*6 MB / 112 flows

⚠ Flow Polling Disabled Icon

Showing collector data for 9/21/21, 4:25:30 AM - 4:26:00 AM: 112 flows displayed.

Note: The traffic we are looking for happens every 15 minutes (approx.). It helps if you have the Flow Filter set to **All Flow Type**, and **No Display Filtering**.

The instructor will review this Lab so everyone will see the results!

Lab 5

Lab 5: Custom Filters

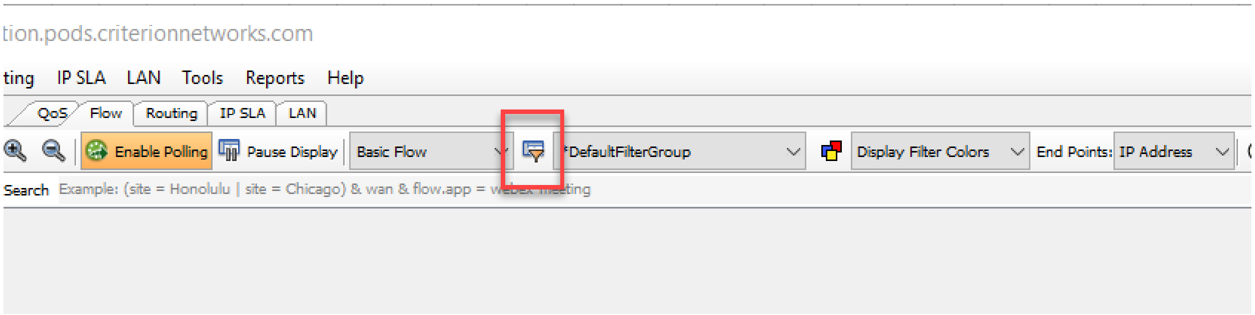
Lab 5.1: Creating Custom Filters

Creating and using Custom filters will help you in your day to day use of LiveNX. It is recommended that you create custom filters for common traffic types that you are interested in viewing regularly.

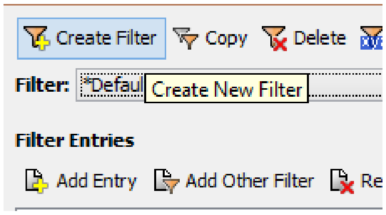
- In this lab you'll create a custom filter based-upon given ports to identify SIP and RTP traffic and verify their markings. Ports being used for the filters in this lab are:
  - SIP Ports: 5060 5061 5062
  - RTP Ports: 16384–32767

Lab Steps:

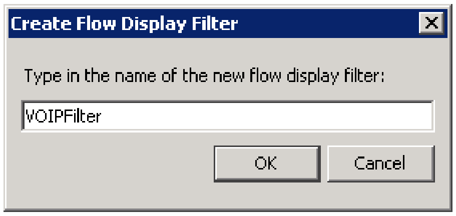
1. Select **HQ-B2**, and then click the **Filter** icon (looks like a funnel) to Open the Flow Display Filters Set-Up.


tion.pods.criterionnetworks.com
ting IP SLA LAN Tools Reports Help
QoS Flow Routing IP SLA LAN
Enable Polling
Pause Display
Basic Flow
*DefaultFilterGroup
Display Filter Colors
End Points: IP Address
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

2. Click **Create Filter** on the top right of the Flow Display Filters Set-Up.



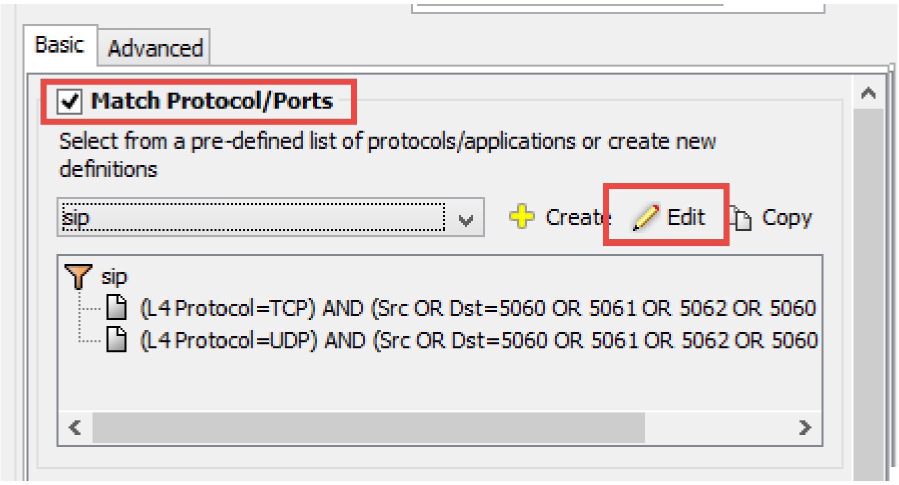
3. Enter a Name label:



Type in the name of the new flow display filter:

VOIPFilter

4. On the **Basic** Tab, check **Match Protocol/Ports** and select the **SIP** Protocol.
5. Click Edit.



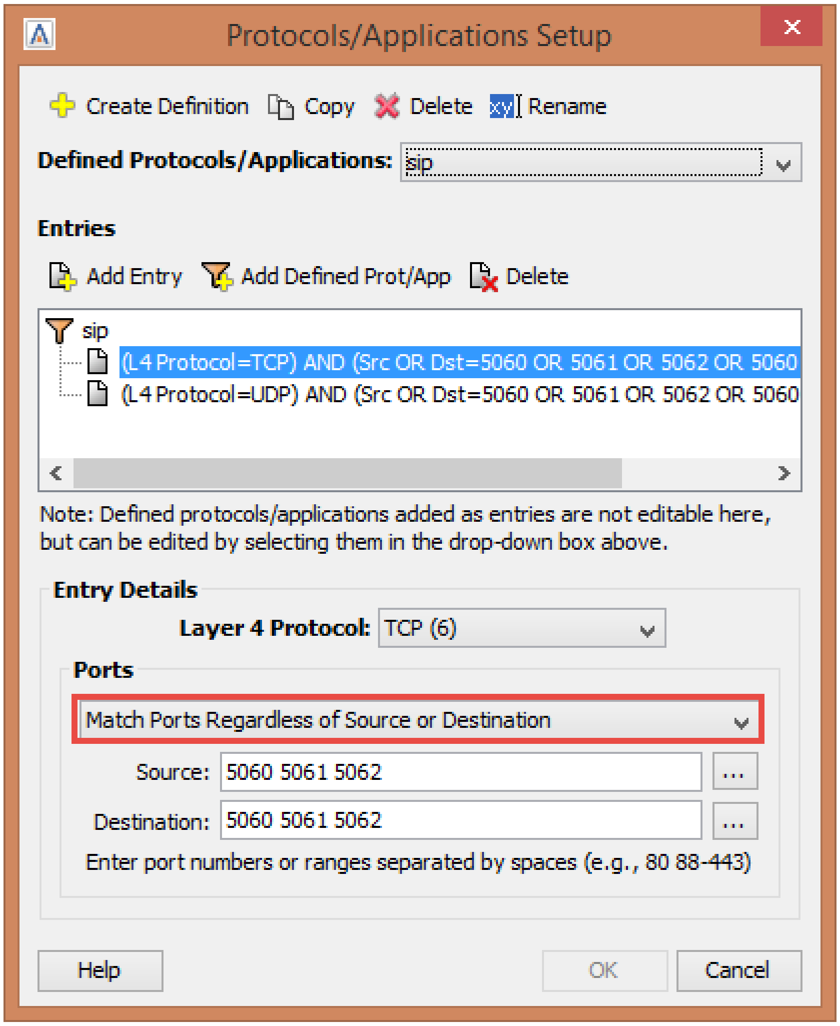
☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

sip

- sip
  - (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
  - (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060

6. Edit both entries, for TCP and UDP, to match the ports provided.
7. Select to "**Match Ports Regardless of Source and Destination**" for both TCP and UDP.



Defined Protocols/Applications: sip

Entries

- sip
  - (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
  - (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060

Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.

Entry Details

Layer 4 Protocol: TCP (6)

Ports

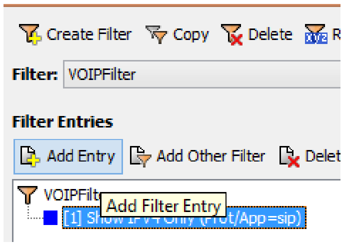
Match Ports Regardless of Source or Destination

Source: 5060 5061 5062

Destination: 5060 5061 5062

Enter port numbers or ranges separated by spaces (e.g., 80 88-443)

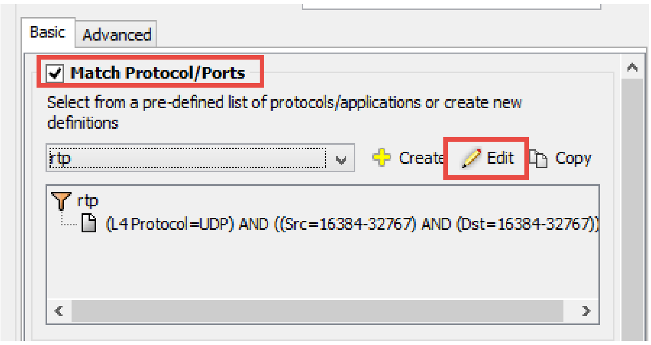
8. Click **OK**
9. Click **Add Entry**.



Filter: VOIPFilter

VOIPFilt
[1] Show IPv4 Only (Prot/App=sip)

10. Select the "**rtp**" Protocol and **Edit** the ports.



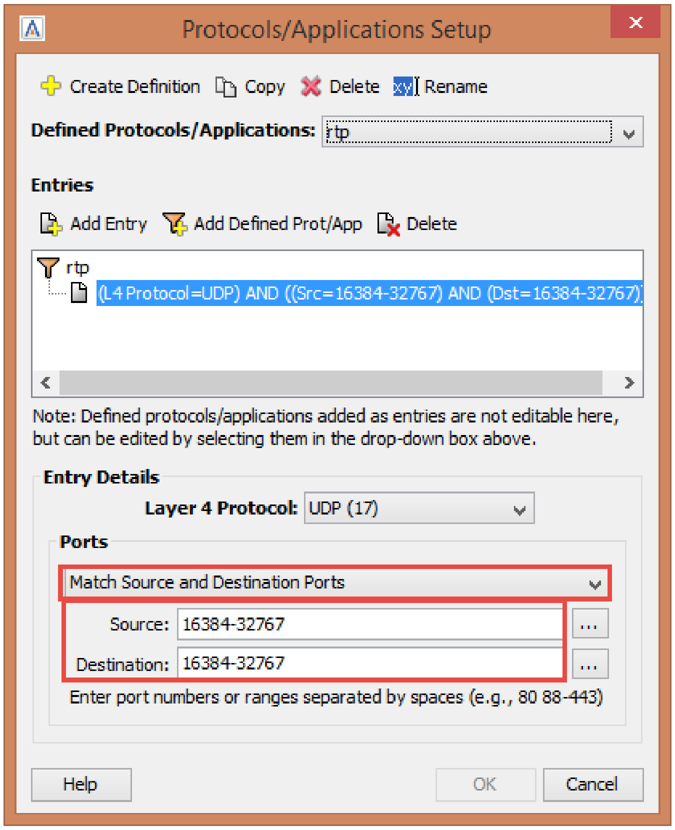
☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

rtp

rtp
(L4 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767))

11. Edit the UDP Entry to "**Match Source and Destination Ports**" to **16384-32767** for both **source and destination**.



Defined Protocols/Applications: rtp

rtp
(L4 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767))

Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.

Layer 4 Protocol: UDP (17)

Match Source and Destination Ports

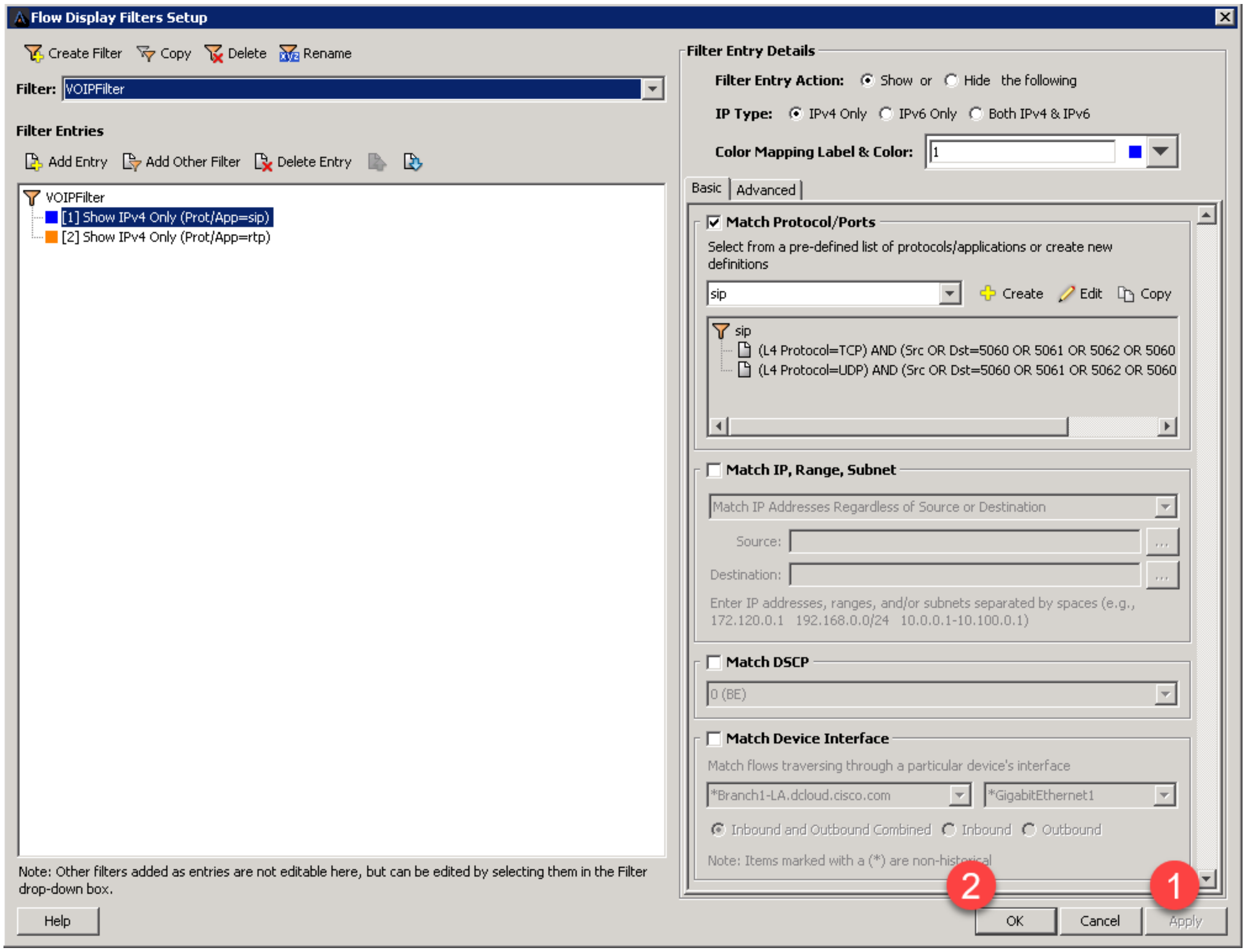
Source: 16384-32767

Destination: 16384-32767

Enter port numbers or ranges separated by spaces (e.g., 80 88-443)

12. Click **OK**

13. Click **Apply** to save the custom filter, then Click **OK**.



Filter: VOIPFilter

Filter Entries

- VOIPFilter
  - 🟦 [1] Show IPv4 Only (Prot/App=sip)
  - 🟧 [2] Show IPv4 Only (Prot/App=rtp)

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: 1 🟦

☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

sip

- sip
  - (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
  - (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060

☐ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

☐ Match DSCP

0 (BE)

☐ Match Device Interface

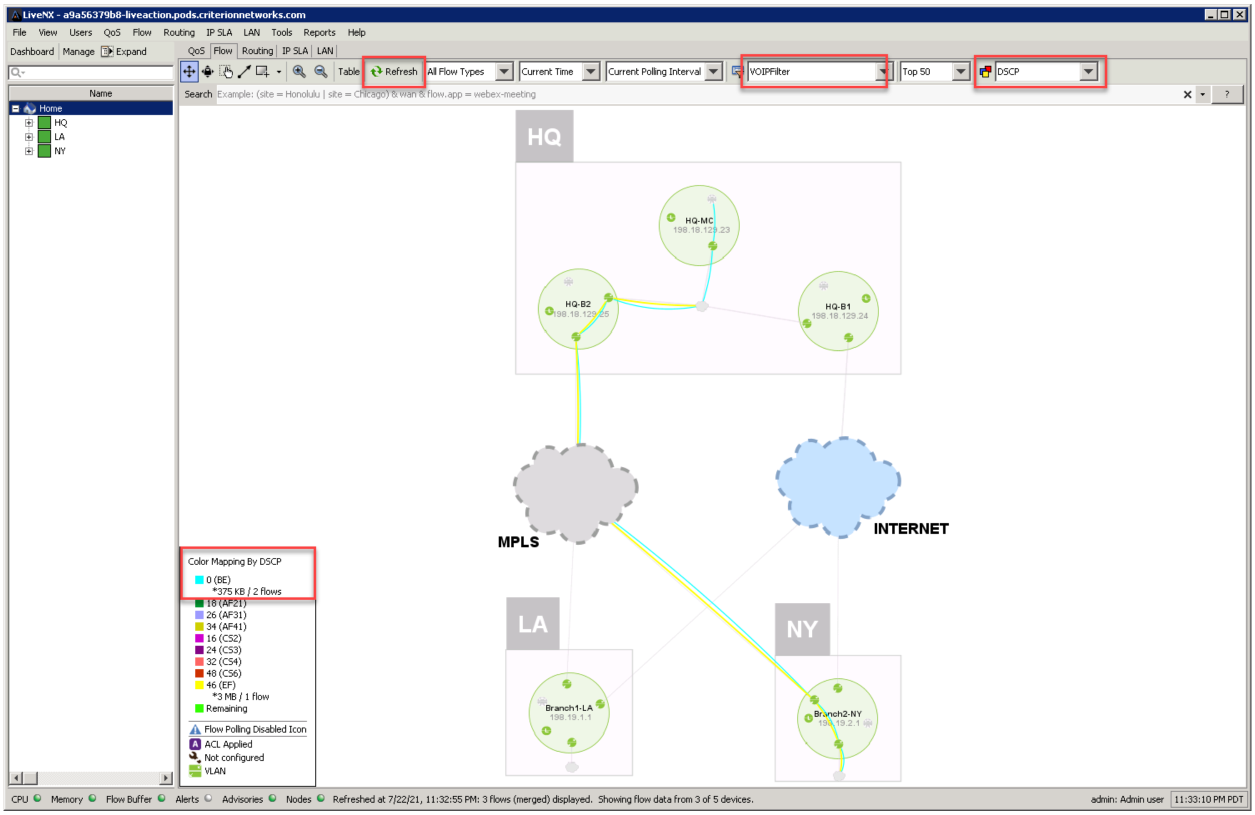
Match flows traversing through a particular device's interface

*Branch1-LA.dcloud.cisco.com *GigabitEthernet1

● Inbound and Outbound Combined ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

14. Select your new filter, select "**DSCP**" and select "**Refresh**" to verify the DSCP markings for your SIP and RTP traffic.


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expand
QoS Flow Routing IP SLA LAN
Table Refresh
Name
Home
HQ
LA
NY
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
HQ
HQ-MC 198.18.129.23
HQ-B2 198.18.129.25
HQ-B1 198.18.129.24
MPLS
INTERNET
LA
Branch1-LA 198.19.1.1
NY
Branch2-NY 198.19.2.1
Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN
CPU Memory Flow Buffer Alerts Advisories Nodes

All Flow Types | Current Time | Current Polling Interval | VOIPFilter | Top 50 | DSCP

Color Mapping By DSCP

- 🟦 0 (BE)
  *375 KB / 2 flows
- 🟩 18 (AF21)
- 🟪 26 (AF31)
- 🟨 34 (AF41)
- 🟪 16 (CS2)
- 🟪 24 (CS3)
- 🟥 32 (CS4)
- 🟥 48 (CS6)
- 🟨 46 (EF)
  *3 MB / 1 flow
- 🟩 Remaining

Refreshed at 7/22/21, 11:32:55 PM: 3 flows (merged) displayed. Showing flow data from 3 of 5 devices.

admin: Admin user 11:33:10 PM PDT

Do you see any BE or Best Effort Marked Traffic in your Lab? Best Effort is the *default* traffic type for any un-marked flows.

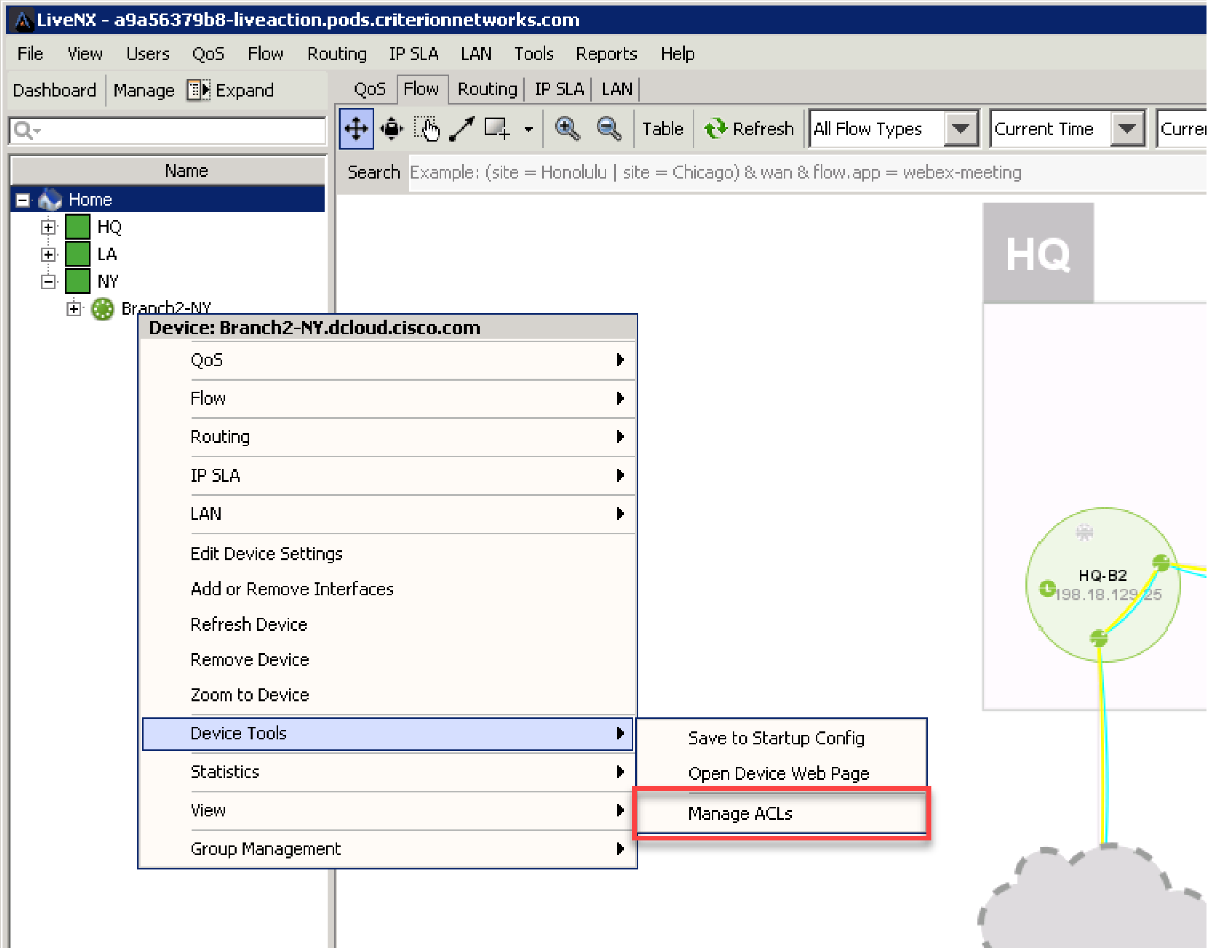
Lab 5.2: ACL Creation

LiveNX gives you the ability to easily create and monitor ACLs with its intuitive User Interface. You can manually create ACLs, or you can create them based upon flow information with only a few clicks. You can also monitor the statistics of how an ACL is performing without having to access the router/switch CLI.

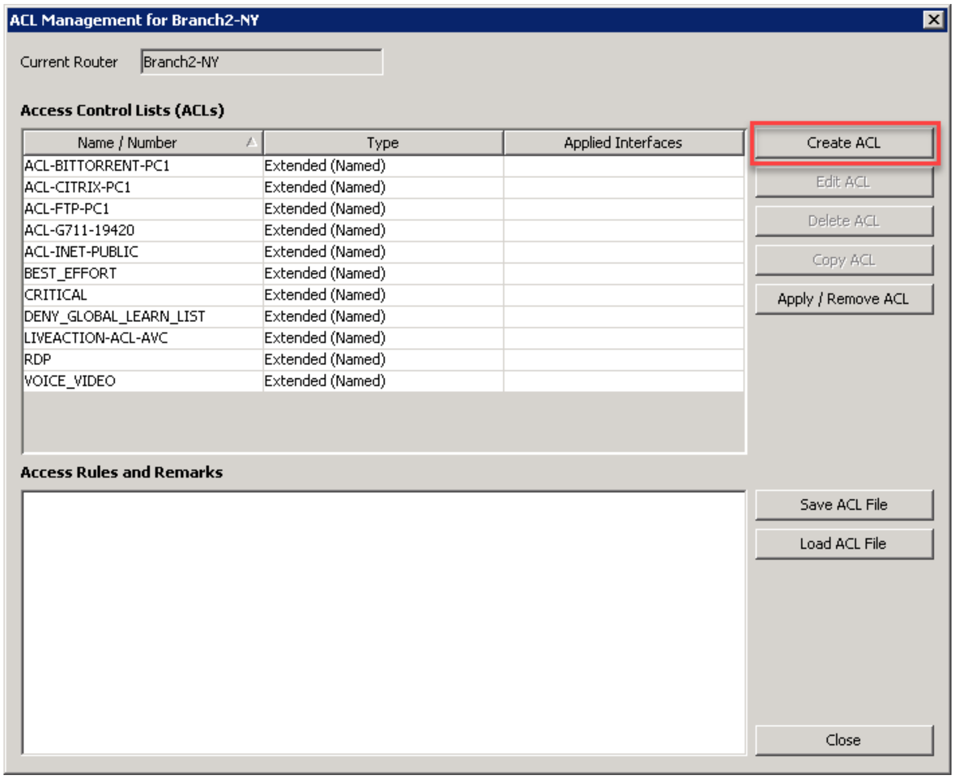
In this lab you'll create an ACL to identify the SIP and RTP traffic to be used in a QoS Marking Policy.

Lab Steps:

1. Right-click on the **Branch2-NY** device (you may also right-click on the device in the Topology Pane) and **Manage ACLs**.


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expand
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Curre
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
HQ
LA
NY
Branch2-NY
Device: Branch2-NY.dcloud.cisco.com
QoS
Flow
Routing
IP SLA
LAN
Edit Device Settings
Add or Remove Interfaces
Refresh Device
Remove Device
Zoom to Device
Device Tools
Statistics
View
Group Management
Save to Startup Config
Open Device Web Page
Manage ACLs
HQ
HQ-B2
198.18.129.25

2. Select "**Create ACL**"



ACL Management for Branch2-NY

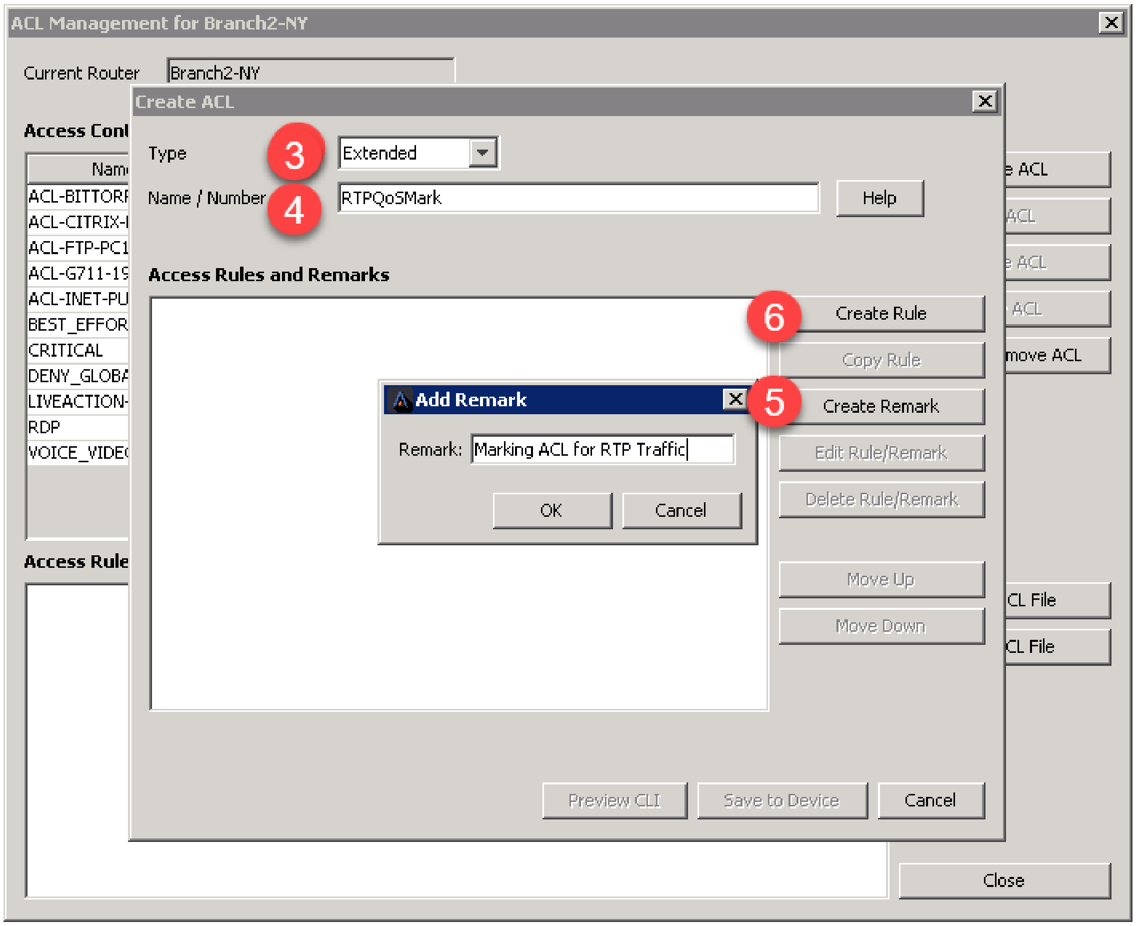
Current Router: Branch2-NY

Access Control Lists (ACLs)

Name / Number	Type	Applied Interfaces
ACL-BITTORRENT-PC1	Extended (Named)	
ACL-CITRIX-PC1	Extended (Named)	
ACL-FTP-PC1	Extended (Named)	
ACL-G711-19420	Extended (Named)	
ACL-INET-PUBLIC	Extended (Named)	
BEST_EFFORT	Extended (Named)	
CRITICAL	Extended (Named)	
DENY_GLOBAL_LEARN_LIST	Extended (Named)	
LIVEACTION-ACL-AVC	Extended (Named)	
RDP	Extended (Named)	
VOICE_VIDEO	Extended (Named)	

Access Rules and Remarks

3. Select “**Extended**” for the **ACL Type**.
4. Give a name to the ACL, such as “**RTPQoSMark**”.
5. Click **Create Remark** to document your work!
6. Select **Create Rule**.



ACL Management for Branch2-NY

Current Router: Branch2-NY

Create ACL

3 Type: Extended

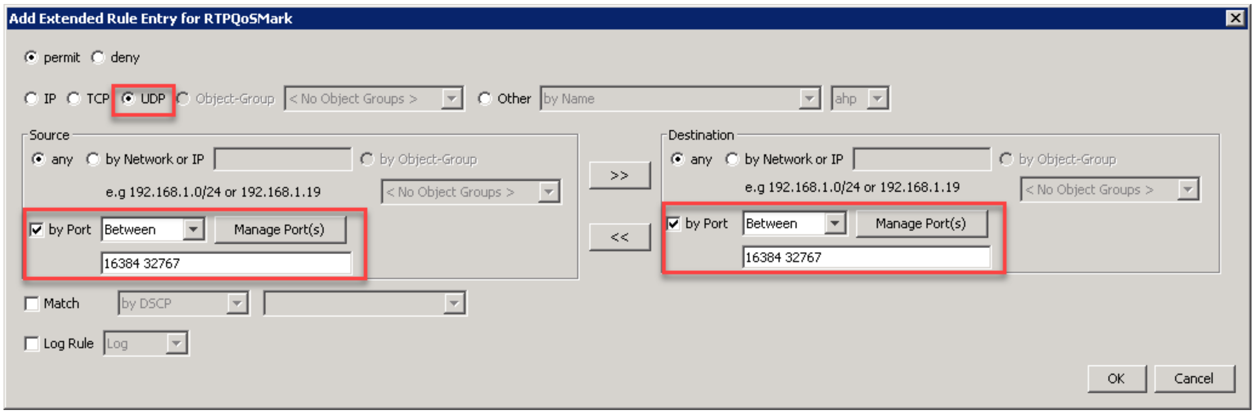
4 Name / Number: RTPQoSMark

Add Remark

Remark: Marking ACL for RTP Traffic

ACL Rule Editor

7. Select “**UDP**” as the protocol type.
8. For **Source** and **Destination** check the “**by Port**” box.
9. Select “**Between**” as the operator value.
10. In the entry box use “**16384 32767**” as the field entry.
11. Click **OK** when your fields match the diagram below.



Add Extended Rule Entry for RTPQoSMark

● permit ○ deny

○ IP ○ TCP ● UDP ○ Object-Group < No Object Groups > ○ Other by Name ahp

Source: ● any ○ by Network or IP ○ by Object-Group < No Object Groups >

e.g 192.168.1.0/24 or 192.168.1.19

☑ by Port Between 16384 32767

Destination: ● any ○ by Network or IP ○ by Object-Group < No Object Groups >

e.g 192.168.1.0/24 or 192.168.1.19

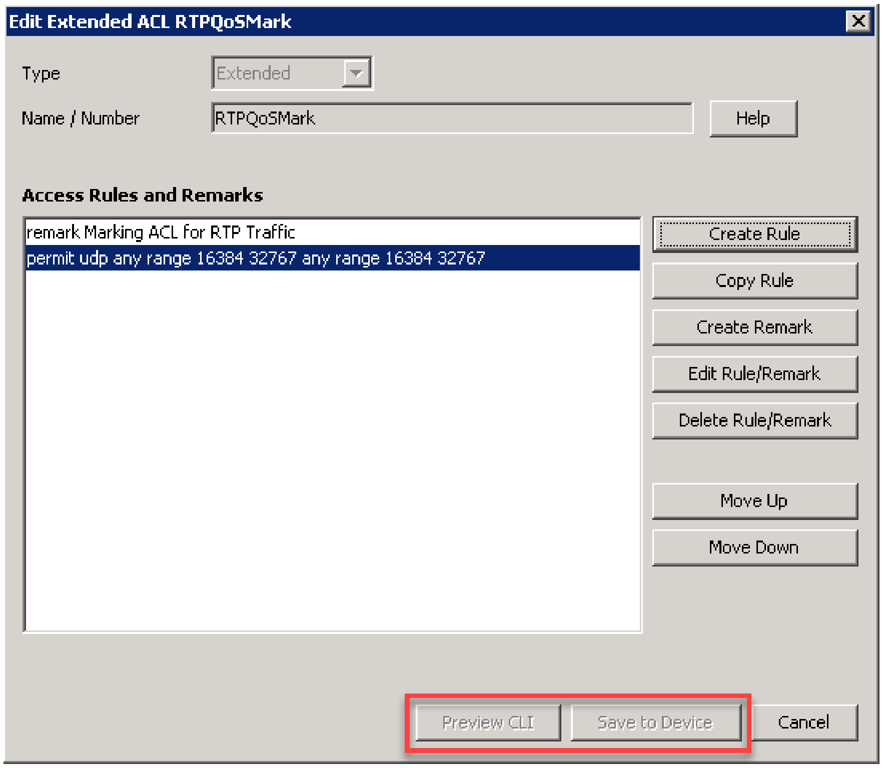
☑ by Port Between 16384 32767

☐ Match by DSCP

☐ Log Rule Log

Once completed you can use “**Preview CLI**” to see the configuration that will be pushed to the device.

12. Click **Save to Device**.



Edit Extended ACL RTPQoSMark

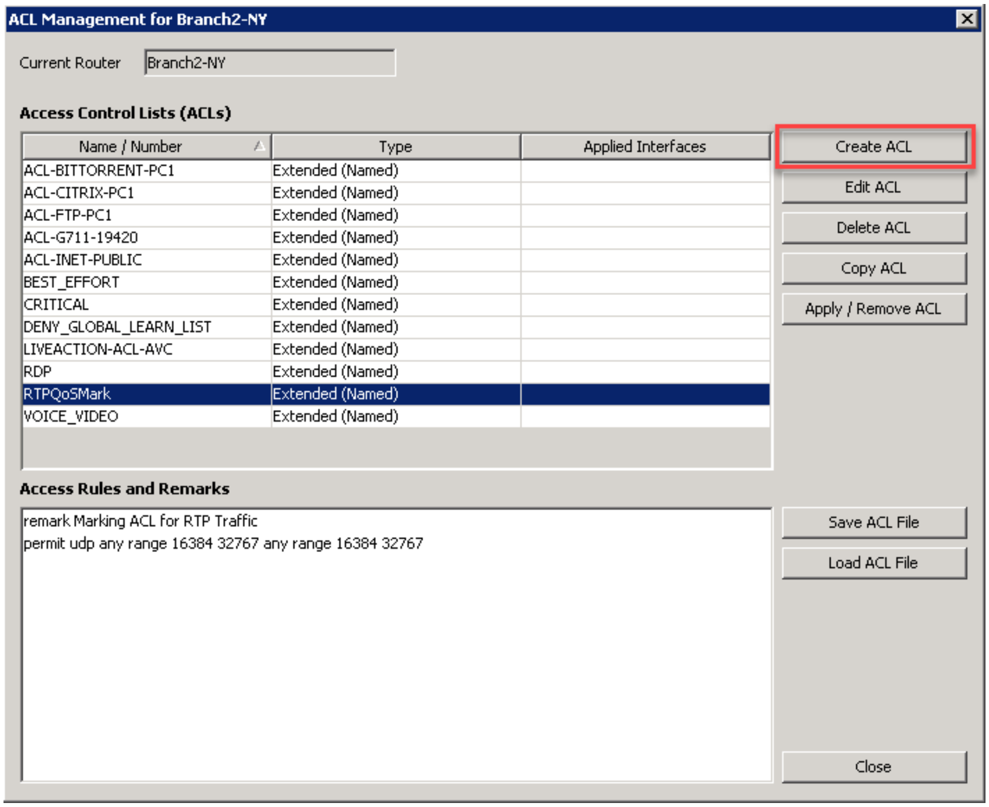
Type: Extended

Name / Number: RTPQoSMark

Access Rules and Remarks

```
remark Marking ACL for RTP Traffic
permit udp any range 16384 32767 any range 16384 32767
```

13. **Create ACLs** for the SIP ports.



Current Router: Branch2-NY

Access Control Lists (ACLs)

Name / Number	Type	Applied Interfaces
ACL-BITTORRENT-PC1	Extended (Named)	
ACL-CITRIX-PC1	Extended (Named)	
ACL-FTP-PC1	Extended (Named)	
ACL-G711-19420	Extended (Named)	
ACL-INET-PUBLIC	Extended (Named)	
BEST_EFFORT	Extended (Named)	
CRITICAL	Extended (Named)	
DENY_GLOBAL_LEARN_LIST	Extended (Named)	
LIVEACTION-ACL-AVC	Extended (Named)	
RDP	Extended (Named)	
RTPQoSMark	Extended (Named)	
VOICE_VIDEO	Extended (Named)	

Access Rules and Remarks

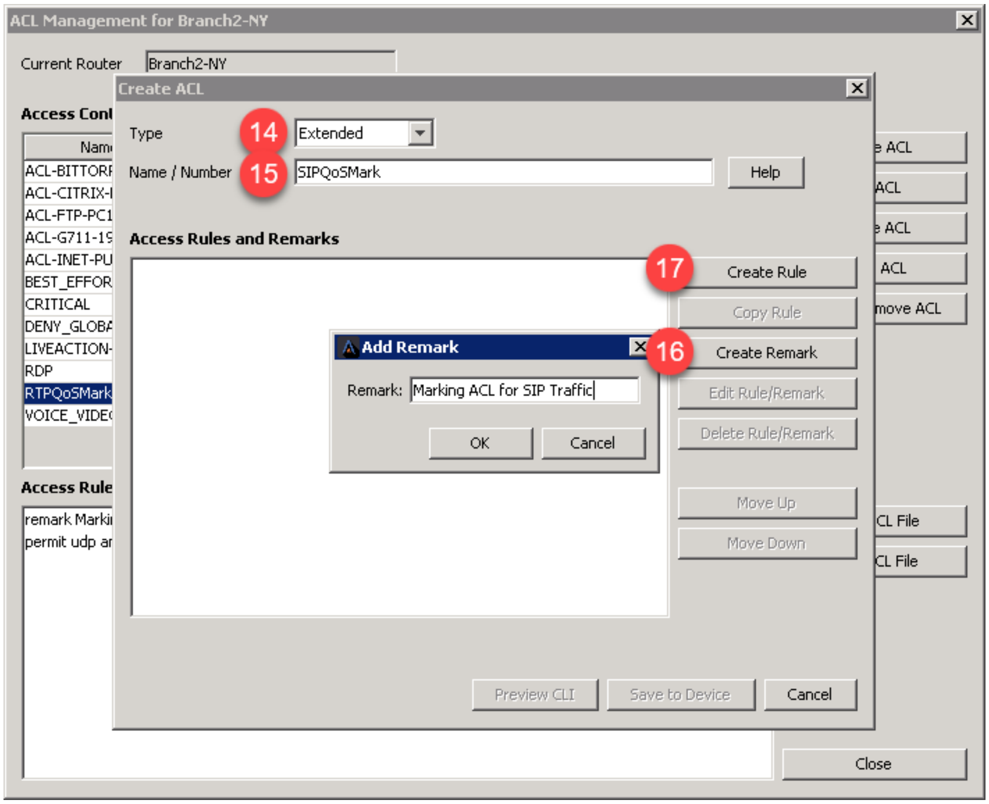
```
remark Marking ACL for RTP Traffic
permit udp any range 16384 32767 any range 16384 32767
```

14. Select “**Extended**” for the ACL Type.

15. Give a name to the ACL, such as “**SIPQoSMark**”.

16. Click **Create Remark** to document your work!

17. Select **Create Rule**.



Current Router: Branch2-NY

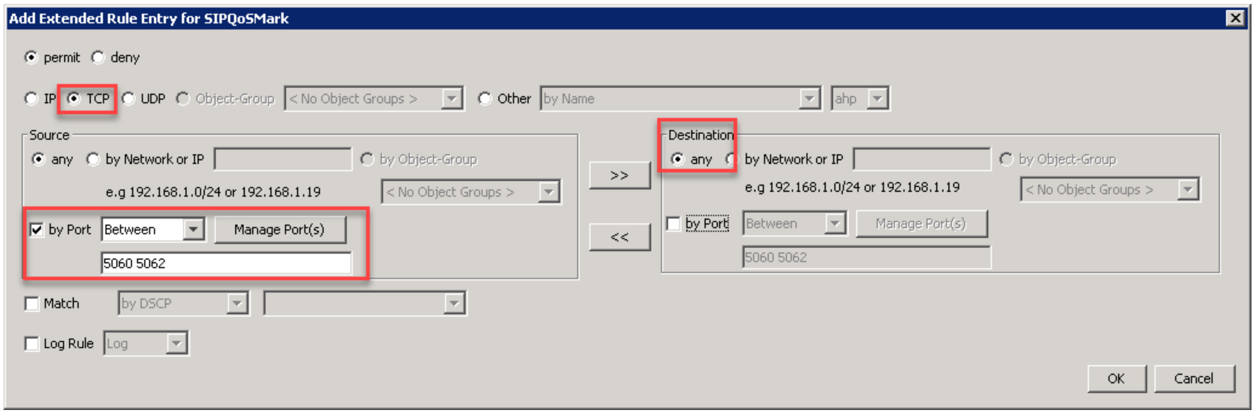
Type: Extended

Name / Number: SIPQoSMark

Access Rules and Remarks

Remark: Marking ACL for SIP Traffic

18. Select "**TCP**" as the protocol type.
19. For **Source** check the "**by Port**" box.
20. Select "**Between**" as the operator value.
21. In the entry box use "**5060 5062**" as the field entry.
22. For **Destination** check **Any**
23. Click **OK** when your fields match the diagram below.



Add Extended Rule Entry for SIPQoSMark

● permit ○ deny

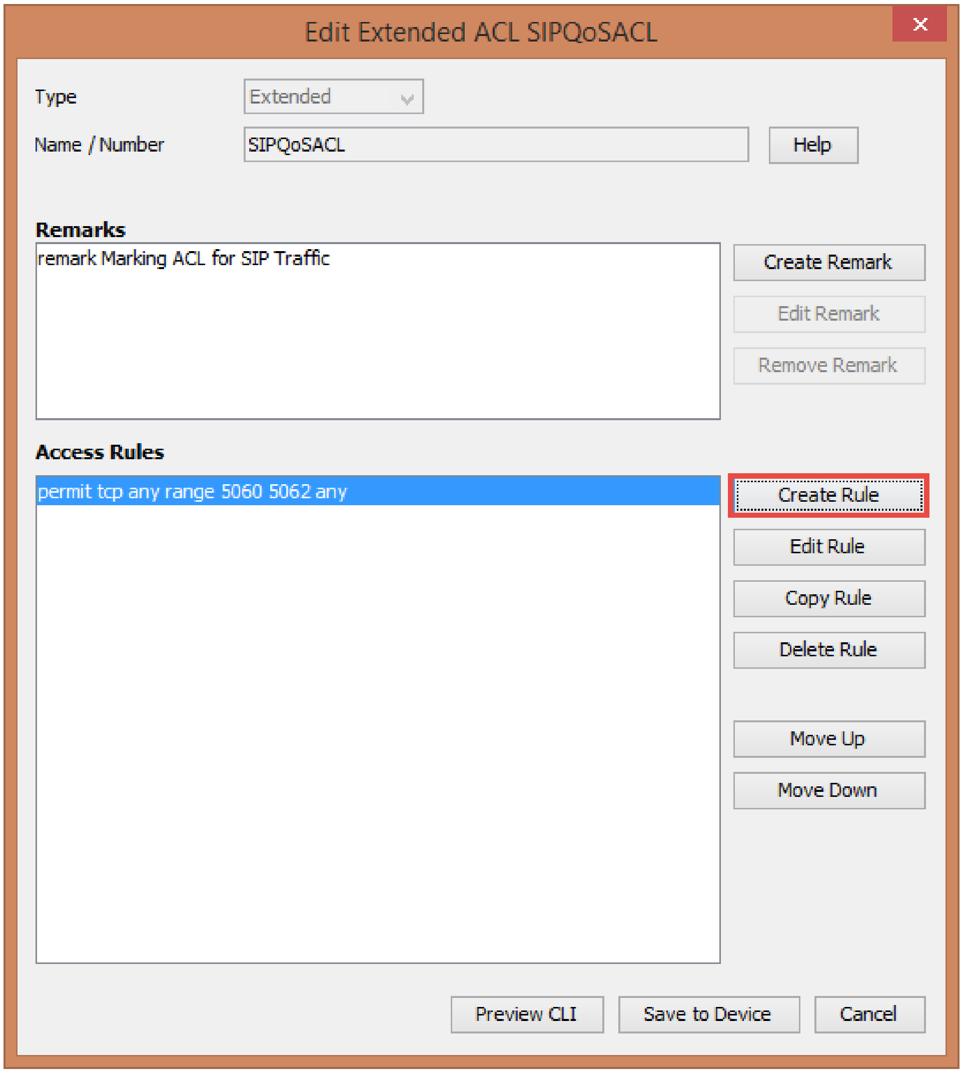
○ IP ● TCP ○ UDP ○ Object-Group < No Object Groups > ○ Other by Name ahp

Source
● any ○ by Network or IP ○ by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >
☑ by Port Between Manage Port(s)
5060 5062

Destination
● any ○ by Network or IP ○ by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >
□ by Port Between Manage Port(s)
5060 5062

□ Match by DSCP
□ Log Rule Log

Next create another rule for destination SIP Ports.



Edit Extended ACL SIPQoSACL

Type: Extended

Name / Number: SIPQoSACL

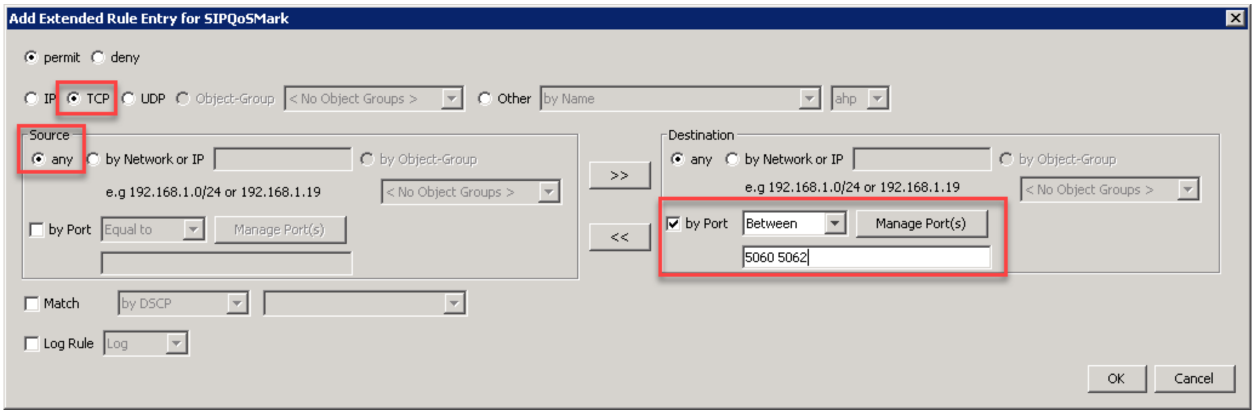
Remarks

remark Marking ACL for SIP Traffic

Access Rules

permit tcp any range 5060 5062 any

24. Select “**TCP**” as the protocol type.
25. For **Source** check **Any**.
26. In **Destination** select **By Port**.
27. Select “**Between**” as the operator value.
28. In the entry box use “**5060 5062**” as the field entry.
29. Click **OK** when your fields match the diagram below



Add Extended Rule Entry for SIPQoSMark

● permit ○ deny

○ IP ● TCP ○ UDP ○ Object-Group < No Object Groups > ○ Other by Name ahp

Source: ● any ○ by Network or IP ○ by Object-Group < No Object Groups >

e.g 192.168.1.0/24 or 192.168.1.19

□ by Port Equal to

Destination: ● any ○ by Network or IP ○ by Object-Group < No Object Groups >

e.g 192.168.1.0/24 or 192.168.1.19

☑ by Port Between

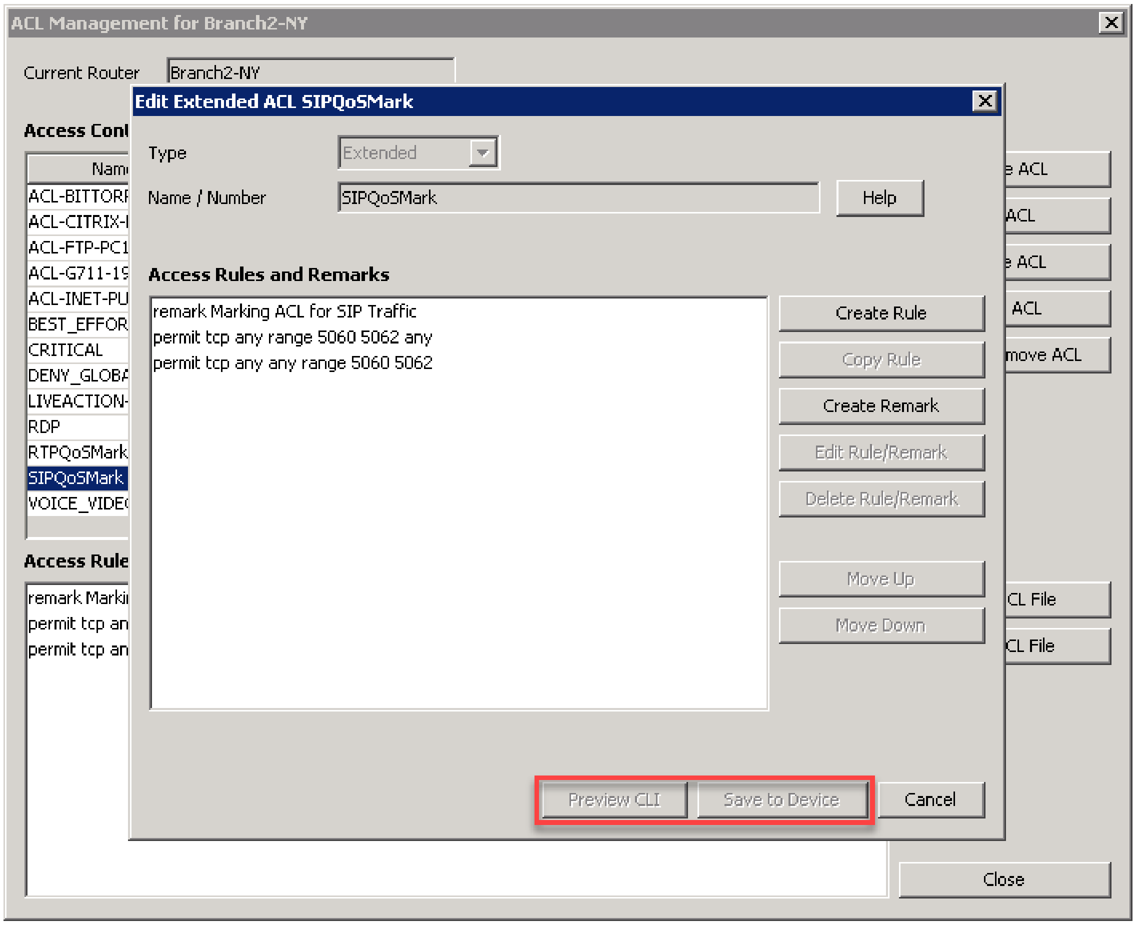
5060 5062

□ Match by DSCP

□ Log Rule Log

30. Click **Preview CLI** to review the configuration to push.

31. Click **Save to Device**.



ACL Management for Branch2-NY

Current Router: Branch2-NY

Edit Extended ACL SIPQoSMark

Type: Extended

Name / Number: SIPQoSMark

Access Rules and Remarks

```
remark Marking ACL for SIP Traffic
permit tcp any range 5060 5062 any
permit tcp any any range 5060 5062
```

You've now created an Access Control List (ACL) via the LiveNX Console. The ACL just created may not produce any results, based-upon traffic availability & timing… but the main point to this lab was to demonstrate the process required to create the ACL.

Lab 6

Lab 6: Making the Topology Work

Lab 6.1: Setting Device Semantics

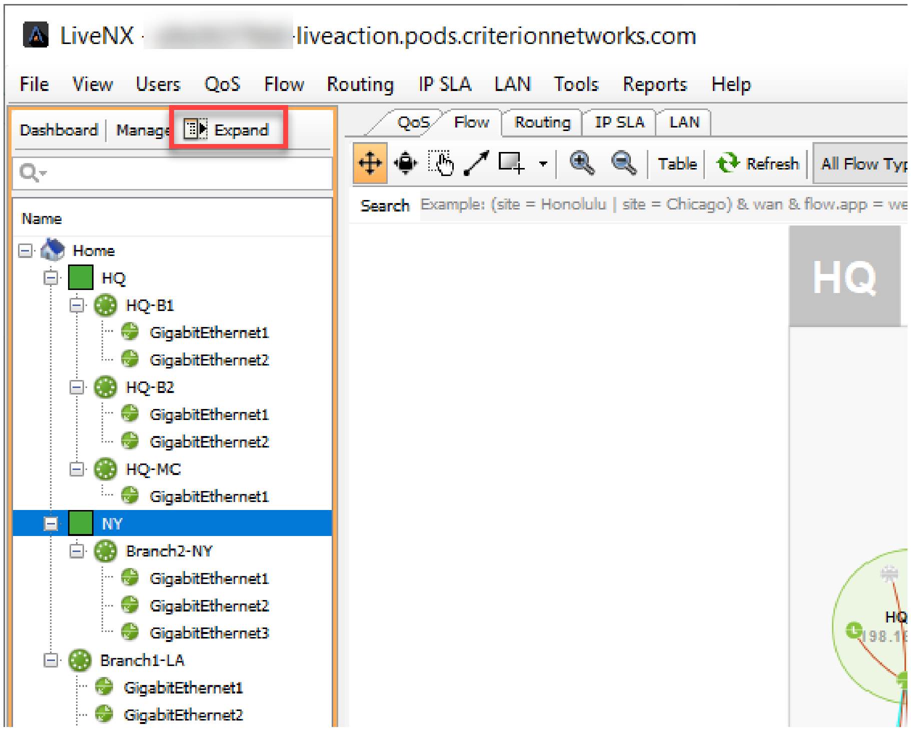
Note: Semantics may have already been configured on most of the devices in this Lab. You need to ensure that all the devices have their semantics entered.

Device semantics are very useful for getting the most out of your LiveNX deployment. Whether it's grouping devices according to region, or identifying high priority links, setting semantics will help you in your day-to-day operations.

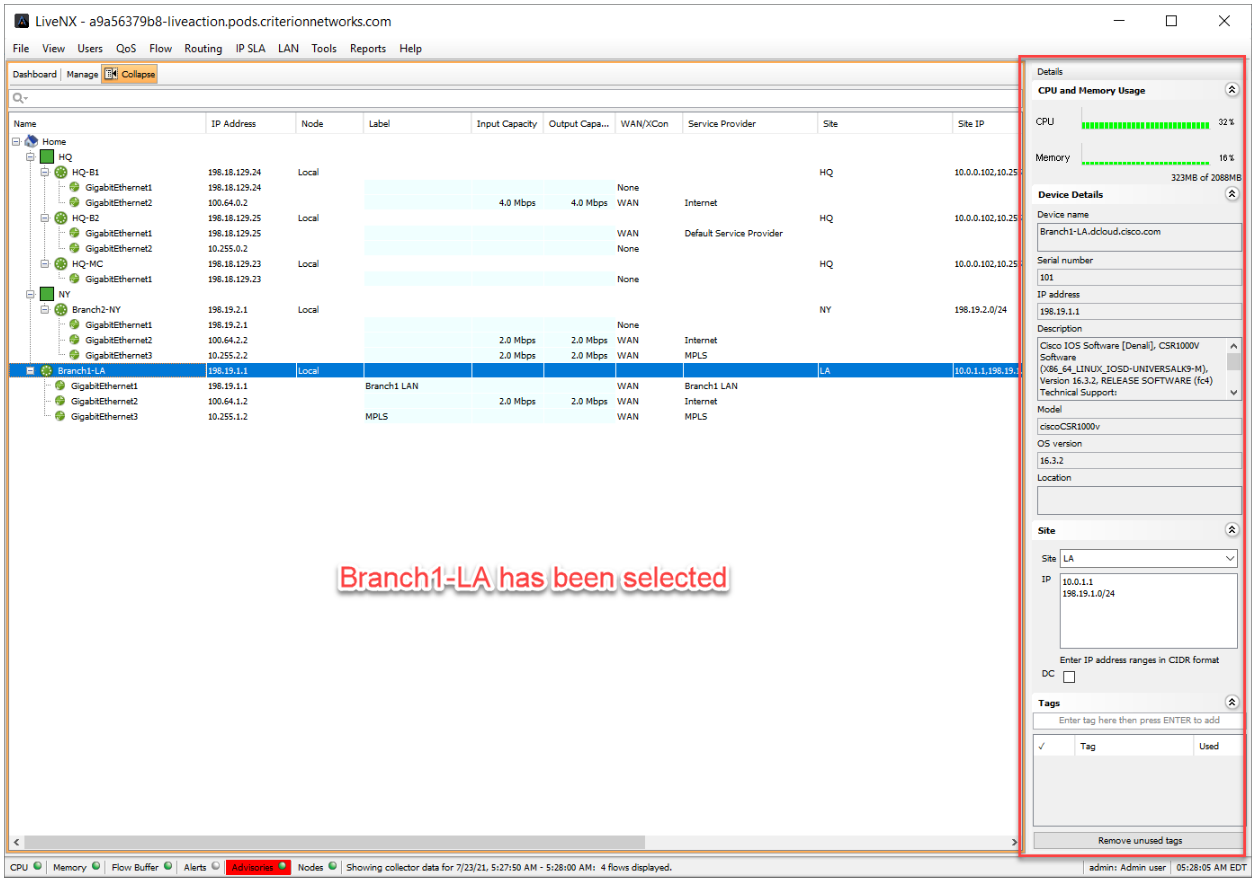
Your task in this Lab will be to identify WAN links and tag them to populate dashboard data, set bandwidth rates for these links, group devices, and merge clouds.

Lab Steps:

1. Select Expand to set semantics for devices.



Expanding the window Home Pane shows an overview of configured device options… as well as a Detail view of a selected device including CPU and memory utilization, Serial Number, Device Name, Mode, etc.



Name	IP Address	Node	Label	Input Capacity	Output Capa...	WAN/XCon	Service Provider	Site	Site IP
Home									
HQ									
HQ-B1	198.18.129.24	Local						HQ	10.0.0.102,10.25
GigabitEthernet1	198.18.129.24					None			
GigabitEthernet2	100.64.0.2			4.0 Mbps	4.0 Mbps	WAN	Internet		
HQ-B2	198.18.129.25	Local						HQ	10.0.0.102,10.25
GigabitEthernet1	198.18.129.25					WAN	Default Service Provider		
GigabitEthernet2	10.255.0.2					None			
HQ-MC	198.18.129.23	Local						HQ	10.0.0.102,10.25
GigabitEthernet1	198.18.129.23					None			
NY									
Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24
GigabitEthernet1	198.19.2.1					None			
GigabitEthernet2	100.64.2.2			2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.2.2			2.0 Mbps	2.0 Mbps	WAN	MPLS		
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1,198.19.1
GigabitEthernet1	198.19.1.1		Branch1 LAN			WAN	Branch1 LAN		
GigabitEthernet2	100.64.1.2			2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.1.2		MPLS			WAN	MPLS		

Branch1-LA has been selected

Details

CPU and Memory Usage

CPU 32 %

Memory 16 %

323MB of 2088MB

Device Details

Device name: Branch1-LA.dcloud.cisco.com

Serial number: 101

IP address: 198.19.1.1

Description: Cisco IOS Software [Denali], CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.3.2, RELEASE SOFTWARE (fc4) Technical Support:

Model: ciscoCSR1000v

OS version: 16.3.2

Location:

Site

Site: LA

IP: 10.0.1.1
198.19.1.0/24

Enter IP address ranges in CIDR format

DC □

Tags

Enter tag here then press ENTER to add

✓	Tag	Used

Remove unused tags

CPU ● | Memory ● | Flow Buffer ● | Alerts ○ | Advisories ● | Nodes ● | Showing collector data for 7/23/21, 5:27:50 AM - 5:28:00 AM: 4 flows displayed. | admin: Admin user | 05:28:05 AM EDT

Note: LiveAction recommends tagging your WAN interfaces so that the corresponding NetFlow data goes to the Dashboard to give you high-level information about data crossing through those interfaces. Besides setting the WAN tags, you can set other information such as a Label, Capacity and Site to give you usage rates for the tagged interface.

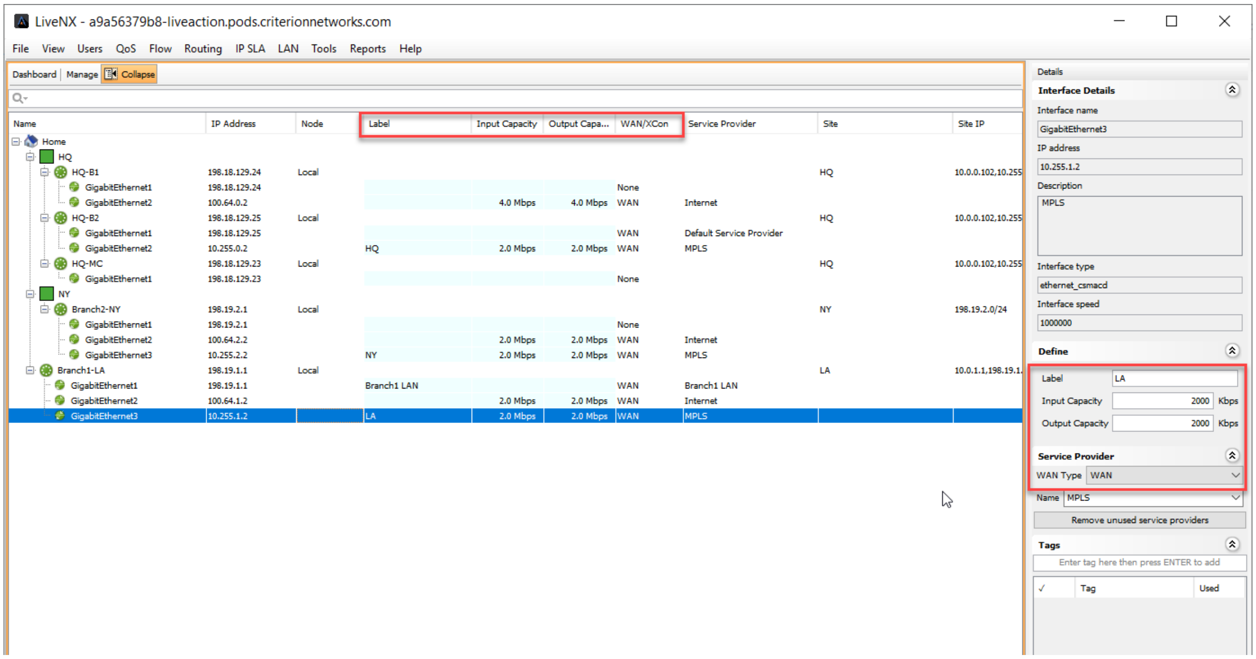
Adding semantic information to an interface allows you to more easily filter information to see exactly what you are looking for.

To allow this, check the semantic settings of the following devices.

Device	Interface	Label	Input Capacity	Output Capacity	WAN
Branch1-LA	GigabitEthernet3	LA	2000kbps	2000kbps	WAN
Branch2-NY	GigabitEthernet3	NY	2000kbps	2000kbps	WAN
HQ-B2	GigabitEthernet2	HQ	2000kbps	2000kbps	WAN

Note: Tags such as WAN and Labels can be used in conjunction with the search string for the topology and in reports.

You can also tag individual or multiple devices that may belong to a site. This information can be used with the Dashboard, topology search, and reports.


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard
Manage
Collapse

Name	IP Address	Node	Label	Input Capacity	Output Capa...	WAN/XCon	Service Provider	Site	Site IP
Home									
HQ									
HQ-B1	198.18.129.24	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.24					None			
GigabitEthernet2	100.64.0.2			4.0 Mbps	4.0 Mbps	WAN	Internet		
HQ-B2	198.18.129.25	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.25					WAN	Default Service Provider		
GigabitEthernet2	10.255.0.2		HQ	2.0 Mbps	2.0 Mbps	WAN	MPLS		
HQ-MC	198.18.129.23	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.23					None			
NY									
Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24
GigabitEthernet1	198.19.2.1					None			
GigabitEthernet2	100.64.2.2			2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.2.2		NY	2.0 Mbps	2.0 Mbps	WAN	MPLS		
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1,198.19.1.
GigabitEthernet1	198.19.1.1		Branch1 LAN			WAN	Branch1 LAN		
GigabitEthernet2	100.64.1.2			2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.1.2		LA	2.0 Mbps	2.0 Mbps	WAN	MPLS		

Details

Interface Details

Interface name: GigabitEthernet3

IP address: 10.255.1.2

Description: MPLS

Interface type: ethernet_csmacd

Interface speed: 1000000

Define

Label: LA

Input Capacity: 2000 Kbps

Output Capacity: 2000 Kbps

Service Provider

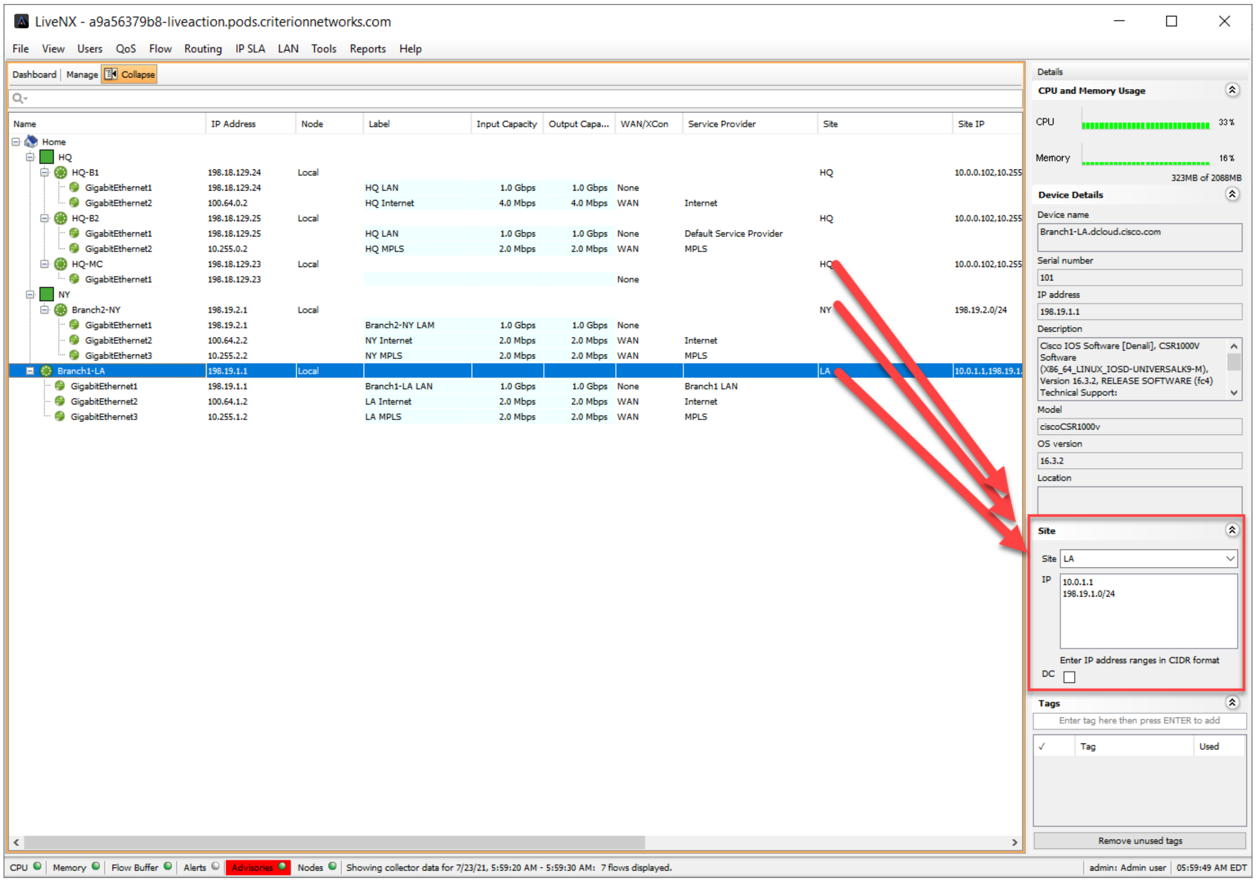
WAN Type: WAN

Name: MPLS

Remove unused service providers
Tags
Enter tag here then press ENTER to add
✓
Tag
Used

2. Select the device and then on the bottom right portion you will see a **Site** field.

3. Configure each device to a site as shown below:
    a. **Branch1-LA** Device as **LA**
    b. **Branch2-NY** Device as **NY**
    c. **HQ-B2** Device as **HQ**



Name	IP Address	Node	Label	Input Capacity	Output Capa...	WAN/XCon	Service Provider	Site	Site IP
Home									
HQ									
HQ-B1	198.18.129.24	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.24		HQ LAN	1.0 Gbps	1.0 Gbps	None			
GigabitEthernet2	100.64.0.2		HQ Internet	4.0 Mbps	4.0 Mbps	WAN	Internet		
HQ-B2	198.18.129.25	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.25		HQ LAN	1.0 Gbps	1.0 Gbps	None	Default Service Provider		
GigabitEthernet2	10.255.0.2		HQ MPLS	2.0 Mbps	2.0 Mbps	WAN	MPLS		
HQ-MC	198.18.129.23	Local						HQ	10.0.0.102,10.255
GigabitEthernet1	198.18.129.23					None			
NY									
Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24
GigabitEthernet1	198.19.2.1		Branch2-NY LAM	1.0 Gbps	1.0 Gbps	None			
GigabitEthernet2	100.64.2.2		NY Internet	2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.2.2		NY MPLS	2.0 Mbps	2.0 Mbps	WAN	MPLS		
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1,198.19.1.
GigabitEthernet1	198.19.1.1		Branch1-LA LAN	1.0 Gbps	1.0 Gbps	None	Branch1 LAN		
GigabitEthernet2	100.64.1.2		LA Internet	2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet3	10.255.1.2		LA MPLS	2.0 Mbps	2.0 Mbps	WAN	MPLS		

CPU 33 %

Memory 16 %

323MB of 2088MB

Device name: Branch1-LA.dcloud.cisco.com

Serial number: 101

IP address: 198.19.1.1

Description: Cisco IOS Software [Denali], CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.3.2, RELEASE SOFTWARE (fc4) Technical Support:

Model: ciscoCSR1000v

OS version: 16.3.2

Location:

Site

Site: LA

IP: 10.0.1.1
198.19.1.0/24

Enter IP address ranges in CIDR format

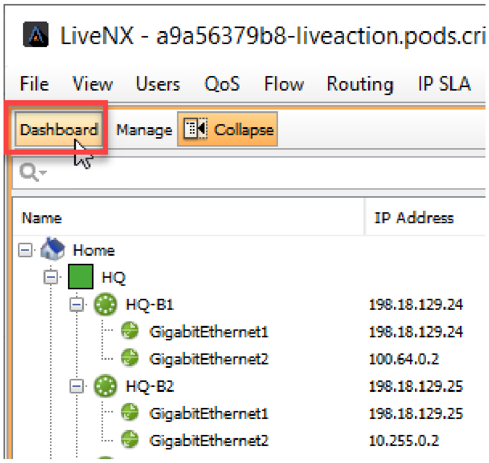
DC □

✓	Tag	Used

CPU ● | Memory ● | Flow Buffer ● | Alerts ● | Advisories ● | Nodes ● | Showing collector data for 7/23/21, 5:59:20 AM - 5:59:30 AM: 7 flows displayed. | admin: Admin user | 05:59:49 AM EDT

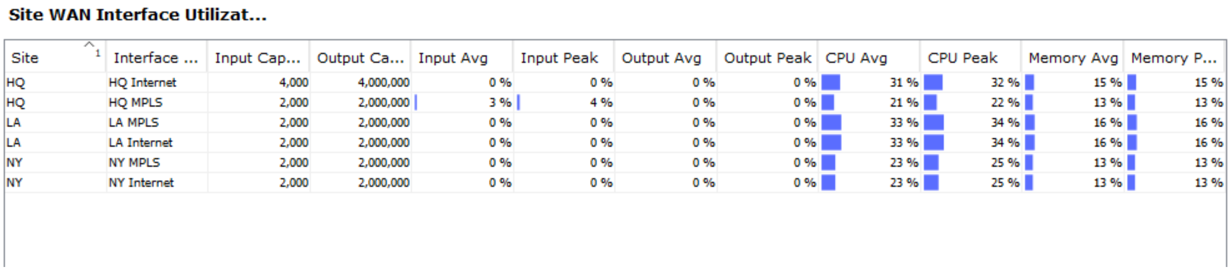
4. Open the dashboard to ensure that data is populating correctly.

Note: It may take up to 15 minutes for the Dashboard to populate with data.



Name	IP Address
Home	
HQ	
HQ-B1	198.18.129.24
GigabitEthernet1	198.18.129.24
GigabitEthernet2	100.64.0.2
HQ-B2	198.18.129.25
GigabitEthernet1	198.18.129.25
GigabitEthernet2	10.255.0.2

On the System Dashboard, if you scroll all the way to the bottom on the window you should see data populating the Site WAN Interface Utilization if you configured the semantics correctly.

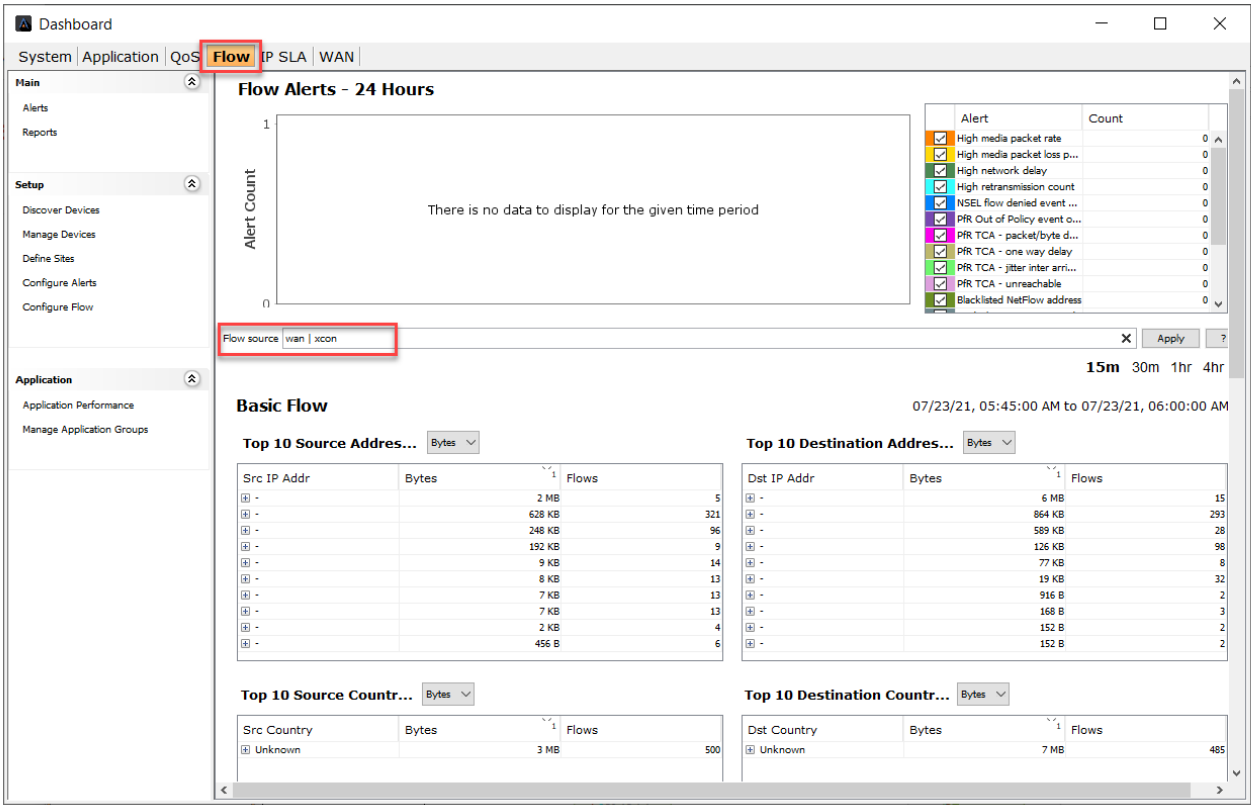


Site WAN Interface Utilizat...

Site	Interface ...	Input Cap...	Output Ca...	Input Avg	Input Peak	Output Avg	Output Peak	CPU Avg	CPU Peak	Memory Avg	Memory P...
HQ	HQ Internet	4,000	4,000,000	0 %	0 %	0 %	0 %	31 %	32 %	15 %	15 %
HQ	HQ MPLS	2,000	2,000,000	3 %	4 %	0 %	0 %	21 %	22 %	13 %	13 %
LA	LA MPLS	2,000	2,000,000	0 %	0 %	0 %	0 %	33 %	34 %	16 %	16 %
LA	LA Internet	2,000	2,000,000	0 %	0 %	0 %	0 %	33 %	34 %	16 %	16 %
NY	NY MPLS	2,000	2,000,000	0 %	0 %	0 %	0 %	23 %	25 %	13 %	13 %
NY	NY Internet	2,000	2,000,000	0 %	0 %	0 %	0 %	23 %	25 %	13 %	13 %

5. Scroll back up on the Dashboard window and select the **Flow** tab.

Notice the Flow Source is set as “**WAN | XCON**”. You can modify the flow source to use other tags, such as Site and Device, if you wish to monitor that specific data on the dashboard.



Flow Alerts - 24 Hours

There is no data to display for the given time period

	Alert	Count
☑	High media packet rate	0
☑	High media packet loss p...	0
☑	High network delay	0
☑	High retransmission count	0
☑	NSEL flow denied event ...	0
☑	PfR Out of Policy event o...	0
☑	PfR TCA - packet/byte d...	0
☑	PfR TCA - one way delay	0
☑	PfR TCA - jitter inter arri...	0
☑	PfR TCA - unreachable	0
☑	Blacklisted NetFlow address	0

Flow source wan | xcon

Basic Flow

07/23/21, 05:45:00 AM to 07/23/21, 06:00:00 AM

Top 10 Source Addres... Bytes

Src IP Addr	Bytes	Flows
⊞ -	2 MB	5
⊞ -	628 KB	321
⊞ -	248 KB	96
⊞ -	192 KB	9
⊞ -	9 KB	14
⊞ -	8 KB	13
⊞ -	7 KB	13
⊞ -	7 KB	13
⊞ -	2 KB	4
⊞ -	456 B	6

Top 10 Destination Addres... Bytes

Dst IP Addr	Bytes	Flows
⊞ -	6 MB	15
⊞ -	864 KB	293
⊞ -	589 KB	28
⊞ -	126 KB	98
⊞ -	77 KB	8
⊞ -	19 KB	32
⊞ -	916 B	2
⊞ -	168 B	3
⊞ -	152 B	2
⊞ -	152 B	2

Top 10 Source Countr... Bytes

Src Country	Bytes	Flows
⊞ Unknown	3 MB	500

Top 10 Destination Countr... Bytes

Dst Country	Bytes	Flows
⊞ Unknown	7 MB	485

Note: Data in the Flow and Application Dashboard widgets are automatically sent to the long-term flow store.

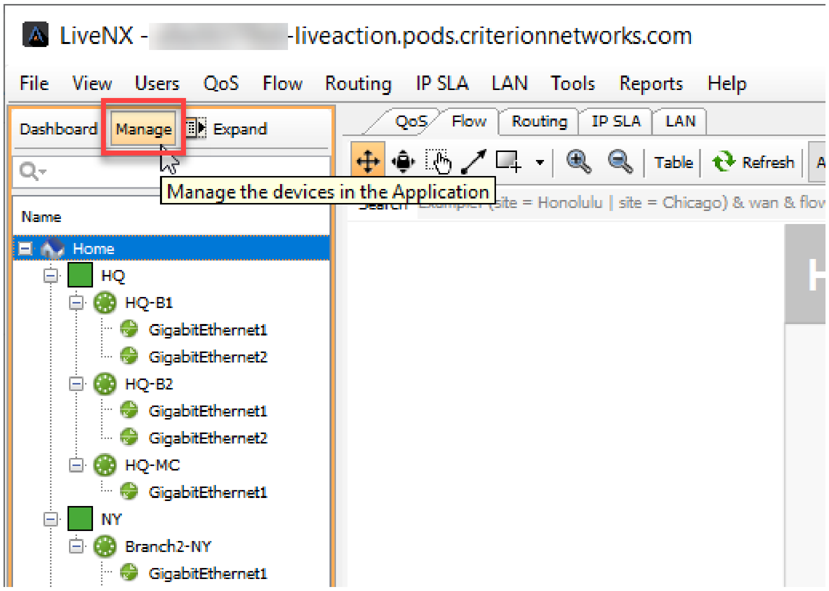
Lab 6.2: Adding Devices to Groups

Having devices in groups makes it easier to manage the topology. You can also use group tags in reports and topology searches.

In this Lab you will create three groups, one called **LA**, one called **NY**, one called **HQ**.

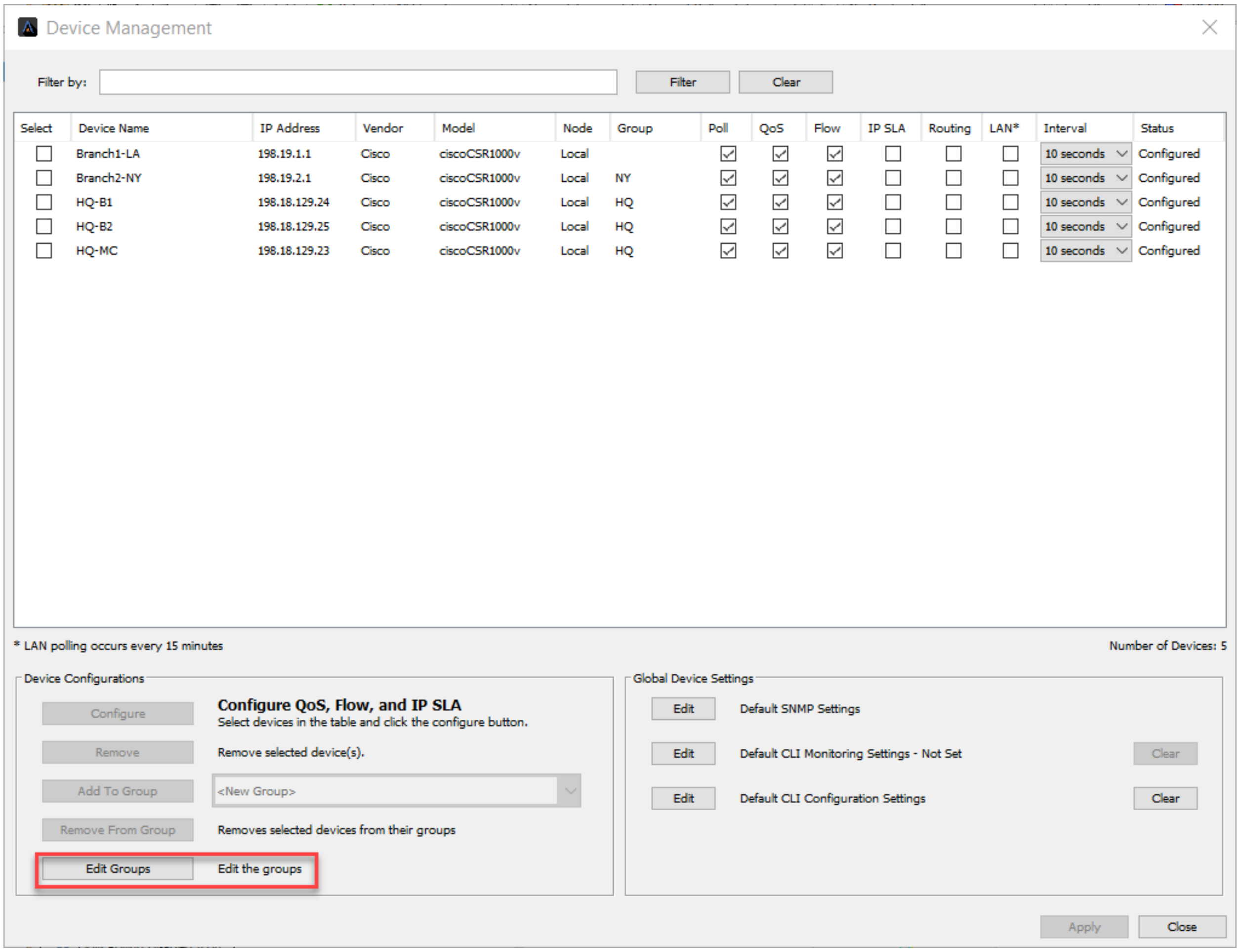
Lab Steps:

1. Open the Device Management window by selecting Manage.


LiveNX - [redacted]-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard
Manage
Expand
QoS Flow Routing IP SLA LAN
Table
Refresh
Manage the devices in the Application
Search
Example: (site = Honolulu | site = Chicago) & wan & flow
Name
Home
HQ
HQ-B1
GigabitEthernet1
GigabitEthernet2
HQ-B2
GigabitEthernet1
GigabitEthernet2
HQ-MC
GigabitEthernet1
NY
Branch2-NY
GigabitEthernet1

On the **Device Management** window note that you can modify many settings for the device, such as polling technologies, polling intervals, manage CLI configuration settings, etc.

2. Select "**Edit Groups**"



Filter by:

Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval	Status
□	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local		☑	☑	☑	□	□	□	10 seconds	Configured
□	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local	NY	☑	☑	☑	□	□	□	10 seconds	Configured
□	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local	HQ	☑	☑	☑	□	□	□	10 seconds	Configured
□	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local	HQ	☑	☑	☑	□	□	□	10 seconds	Configured
□	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local	HQ	☑	☑	☑	□	□	□	10 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

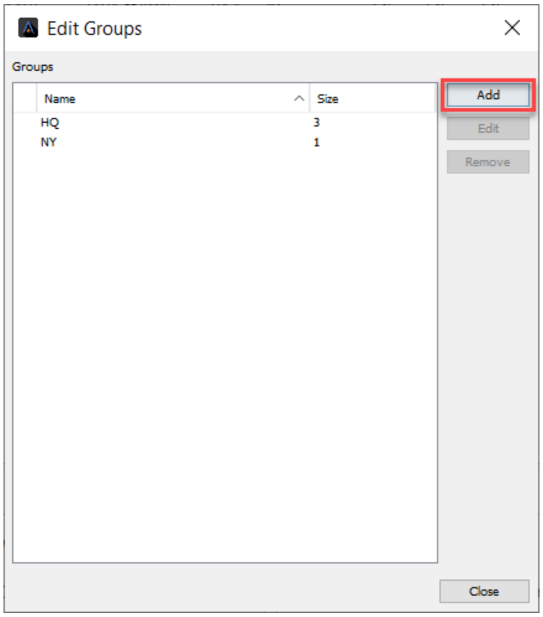
Global Device Settings

Default SNMP Settings

Default CLI Monitoring Settings - Not Set

Default CLI Configuration Settings

3. Click **Add**

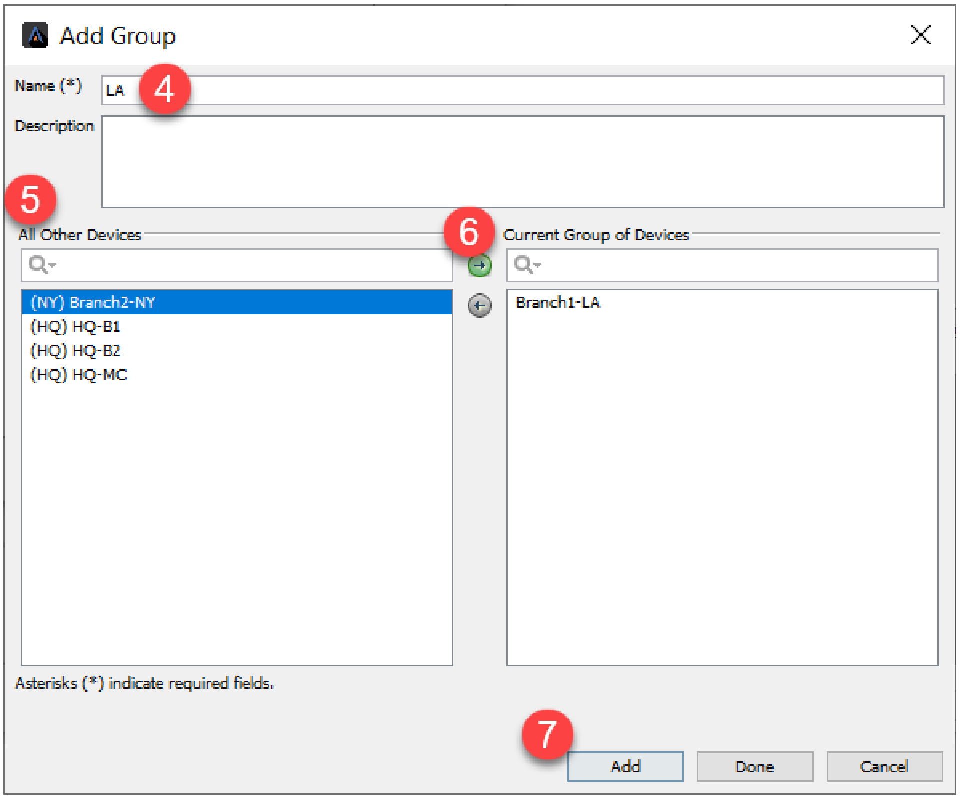


Groups

Name	Size
HQ	3
NY	1

4. Enter **LA** in the Name field.
5. Select **Branch1-LA** from the **All Other Devices** list

6. click the green **Right** arrow.
7. Click **Add**.
8. Repeat the steps above to create any other groups as necessary.



Name (*) LA

Description

(NY) Branch2-NY
(HQ) HQ-B1
(HQ) HQ-B2
(HQ) HQ-MC

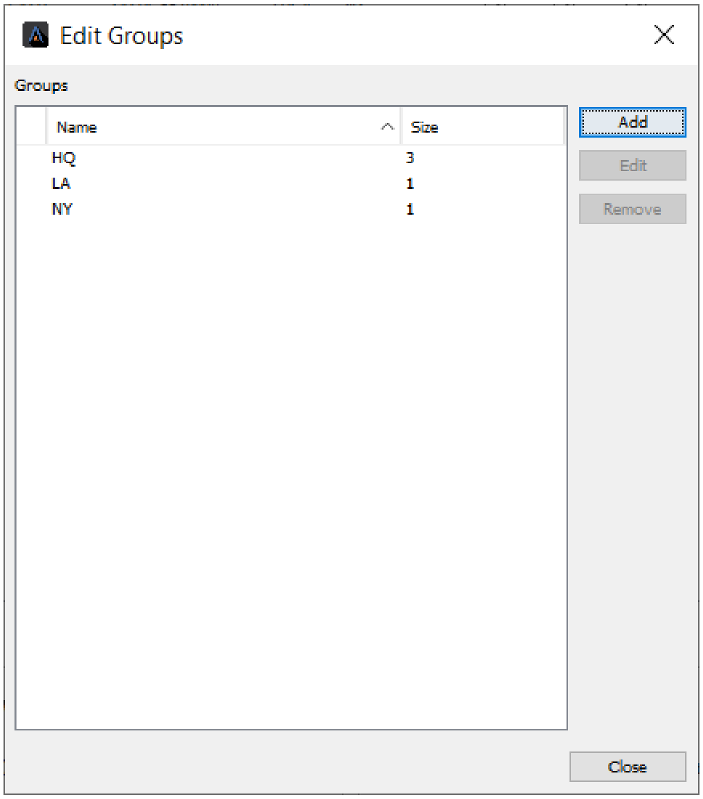
Branch1-LA

Asterisks (*) indicate required fields.

9. Once all groups have been created and devices correctly added, select **Done**.

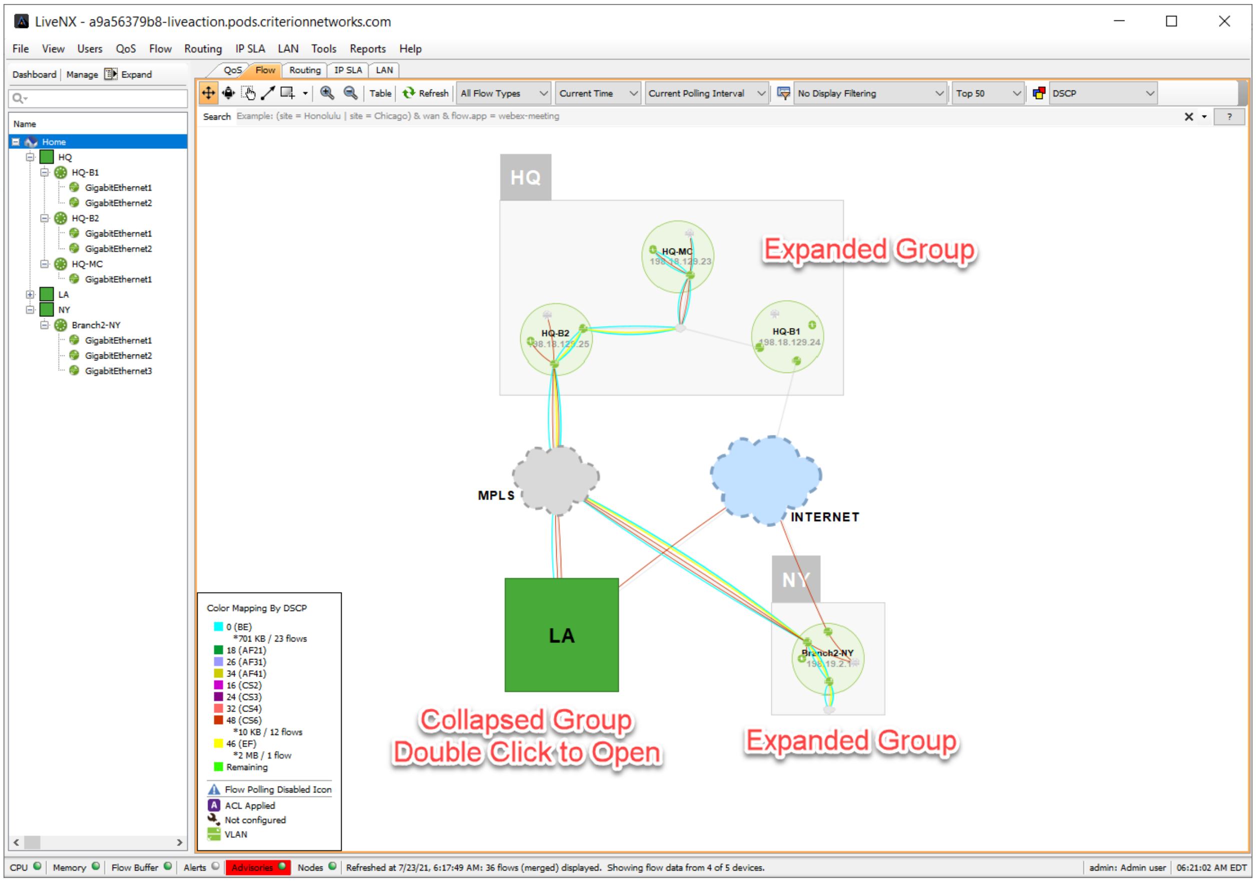
Once completed your groups should look like the one below.

10. Click OK and return to the topology pane to see the changes.



Name	Size
HQ	3
LA	1
NY	1

11. You may need to exit out of the previous windows to return to the **Device Management** window.
12. Double-click on the group to expand.



Expanded Group

Collapsed Group
Double Click to Open

Expanded Group

Color Mapping By DSCP

- 🟦 0 (BE)
  *701 KB / 23 flows
- 🟩 18 (AF21)
- 🟪 26 (AF31)
- 🟨 34 (AF41)
- 🟪 16 (CS2)
- 🟪 24 (CS3)
- 🟥 32 (CS4)
- 🟥 48 (CS6)
  *10 KB / 12 flows
- 🟨 46 (EF)
  *2 MB / 1 flow
- 🟩 Remaining

- ⚠ Flow Polling Disabled Icon
- A ACL Applied
- 🔧 Not configured
- VLAN

Refreshed at 7/23/21, 6:17:49 AM: 36 flows (merged) displayed. Showing flow data from 4 of 5 devices.

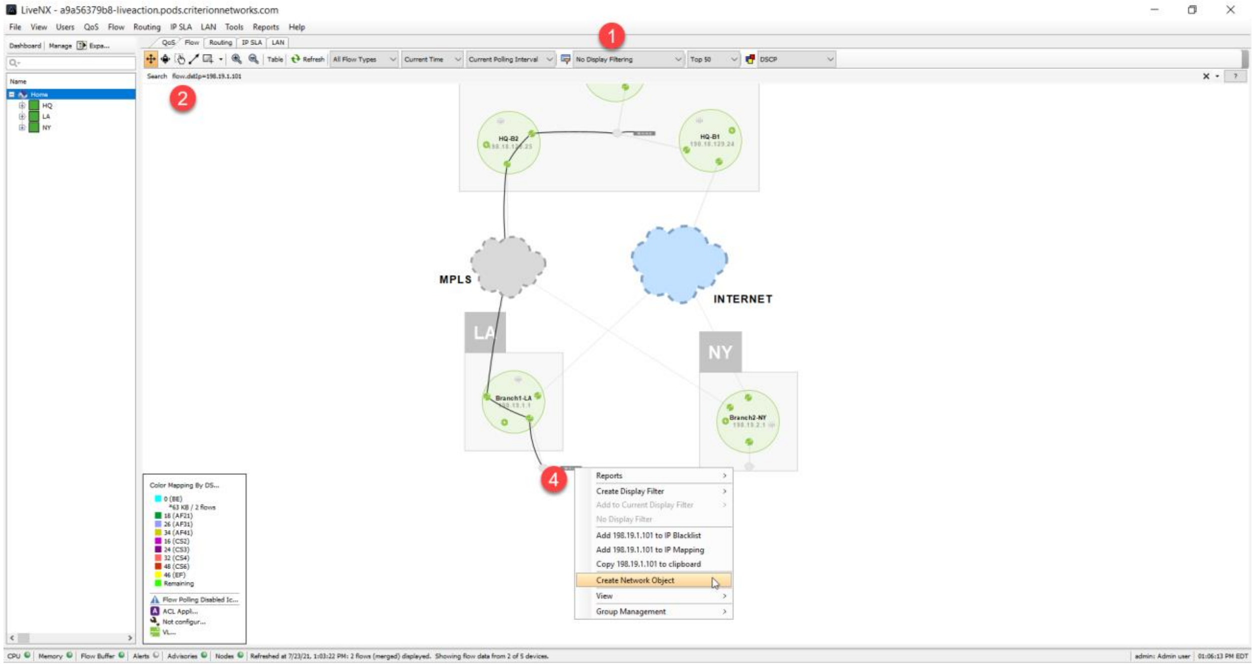
Lab 6.3: Creating Network Objects

Network objects can be used to better visualize and understand how traffic traverses the topology. LiveNX allows you to assign various icons to flow endpoints, such as laptop or server icons for those host-types, as well as phone set or camera icons, to denote appropriate infrastructure.

In this Lab we'll identify several specific flows and assign appropriate end-point objects.

Lab Steps:

1. Make sure that there is no filter being applied (**No Display Filtering**)
2. In the **Flow** tab, Enter the search string: flow.dstip=198.19.1.101
3. Click on the Flow line to select it…. And note the IP endpoints.
4. Right click on the IP Address endpoint **198.19.1.101** and select **Create Network Object**

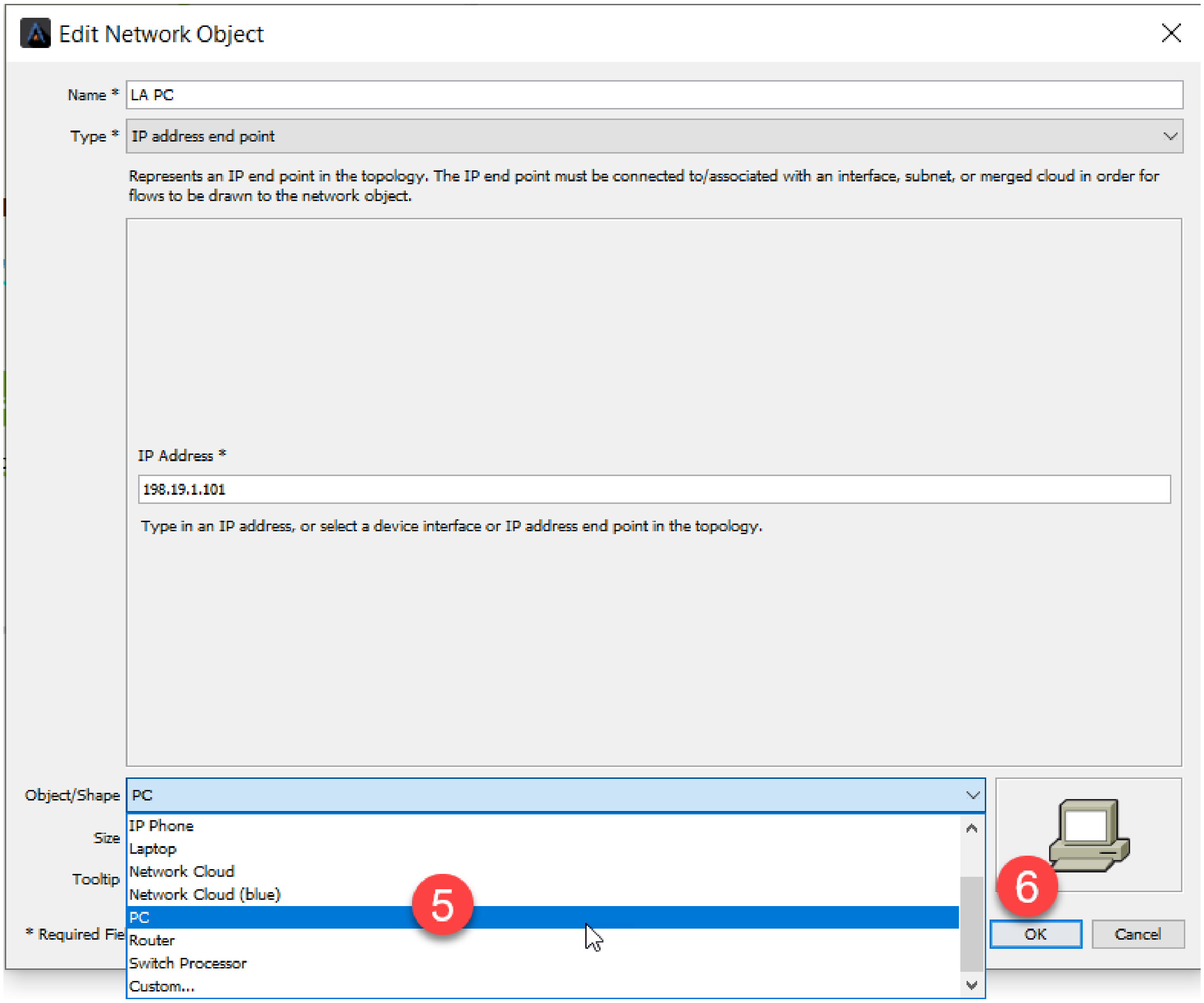


LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com

Search flow.dstip=198.19.1.101

Refreshed at 7/23/21, 1:03:22 PM: 2 flows (merged) displayed. Showing flow data from 2 of 5 devices.

5. Select an **Object/Shape** as "PC".
6. Click **OK**.



Edit Network Object

Name * LA PC

Type * IP address end point

Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merged cloud in order for flows to be drawn to the network object.

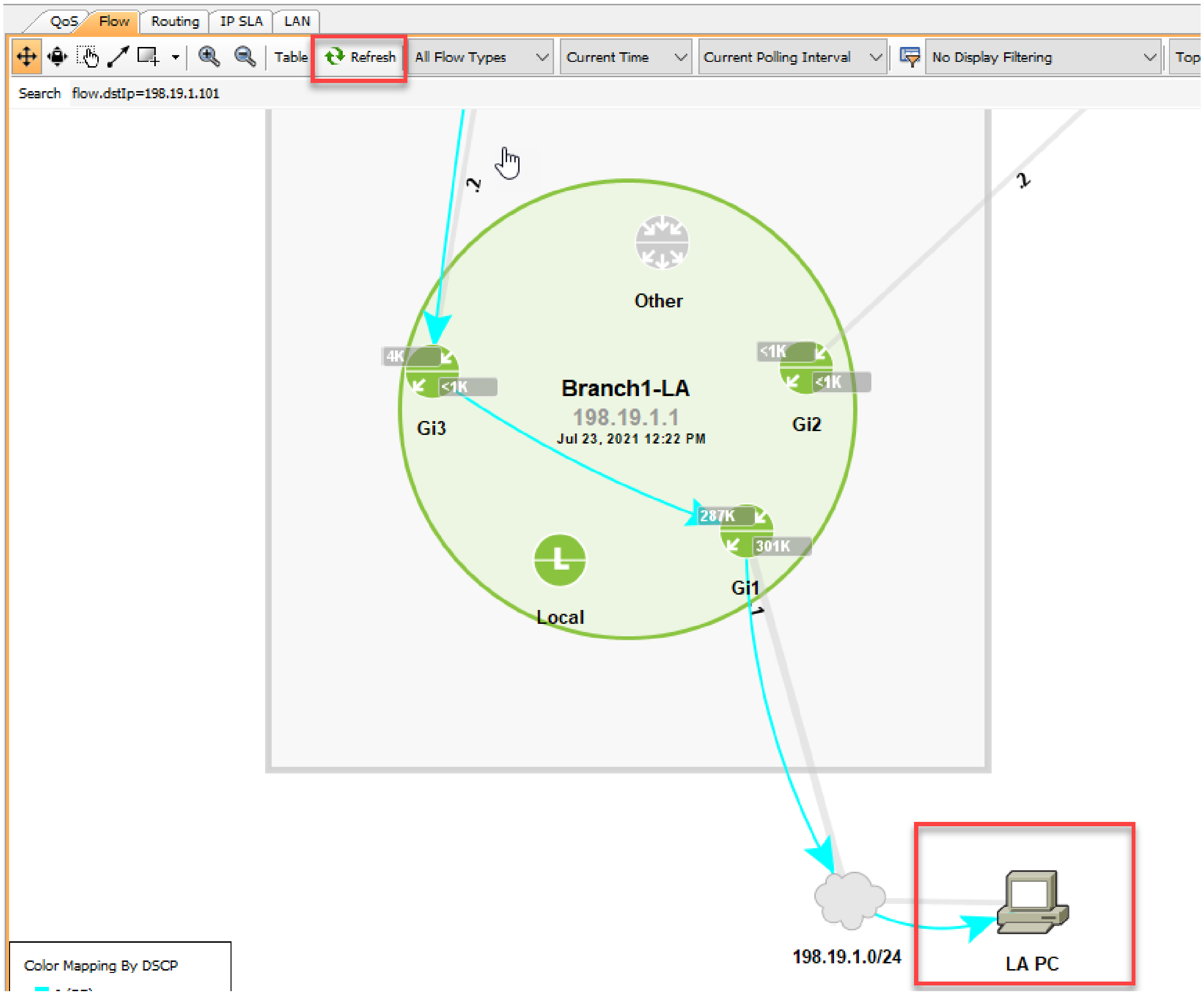
IP Address * 198.19.1.101

Type in an IP address, or select a device interface or IP address end point in the topology.

Object/Shape PC

7. Click Refresh.

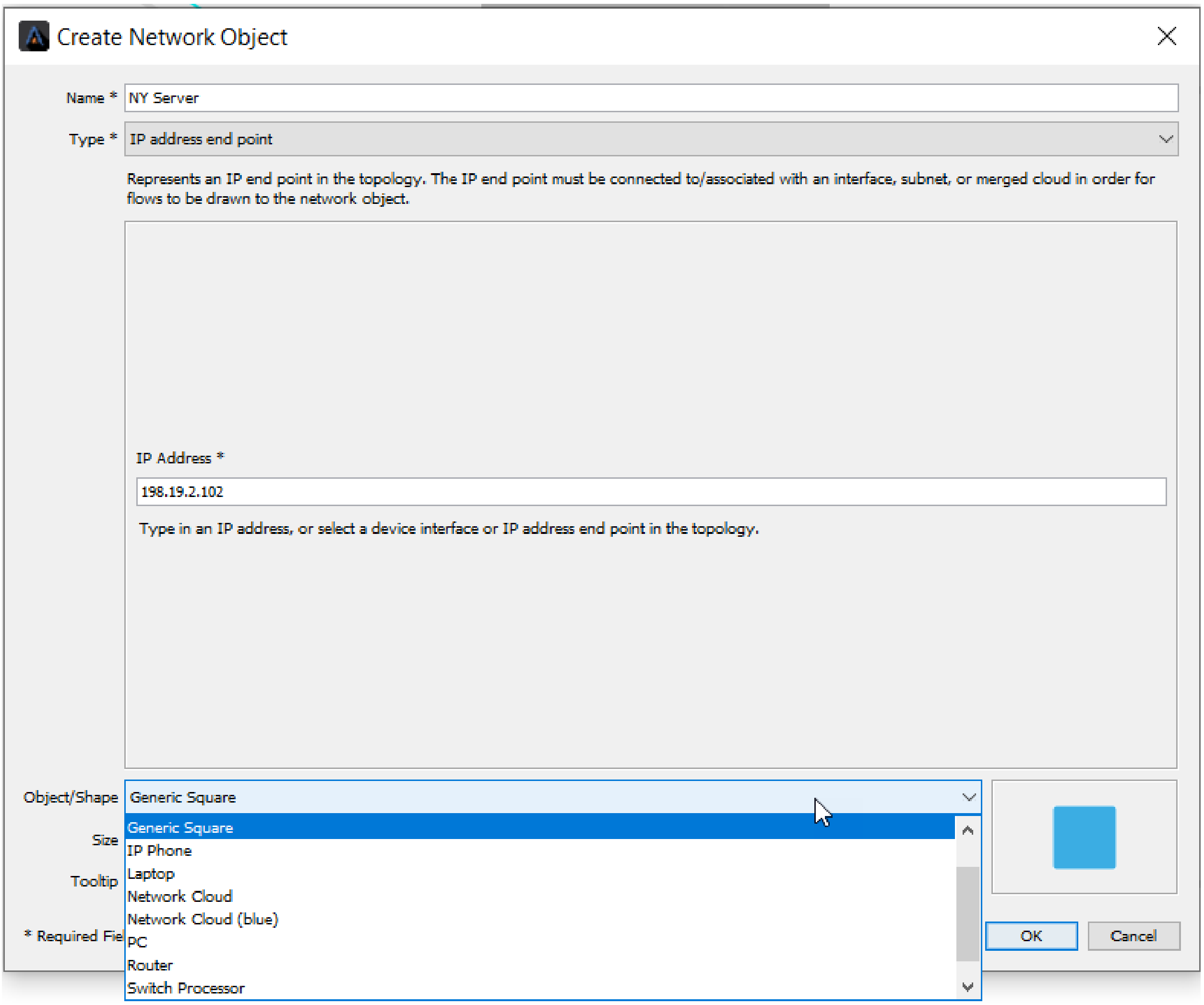
You will now see the flows to your new network object.



Search flow.dstIp=198.19.1.101

Note: Assigning representative icons to the flow endpoints makes it easier to locate potential trouble spots!

8. Enter the search string: flow.srcip=198.19.2.102
9. Select the flow (it will be near the NY router), right click on the IP Address endpoint.
10. Select **Create Network Object**



Create Network Object

Name * NY Server

Type * IP address end point

Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merged cloud in order for flows to be drawn to the network object.

IP Address *

198.19.2.102

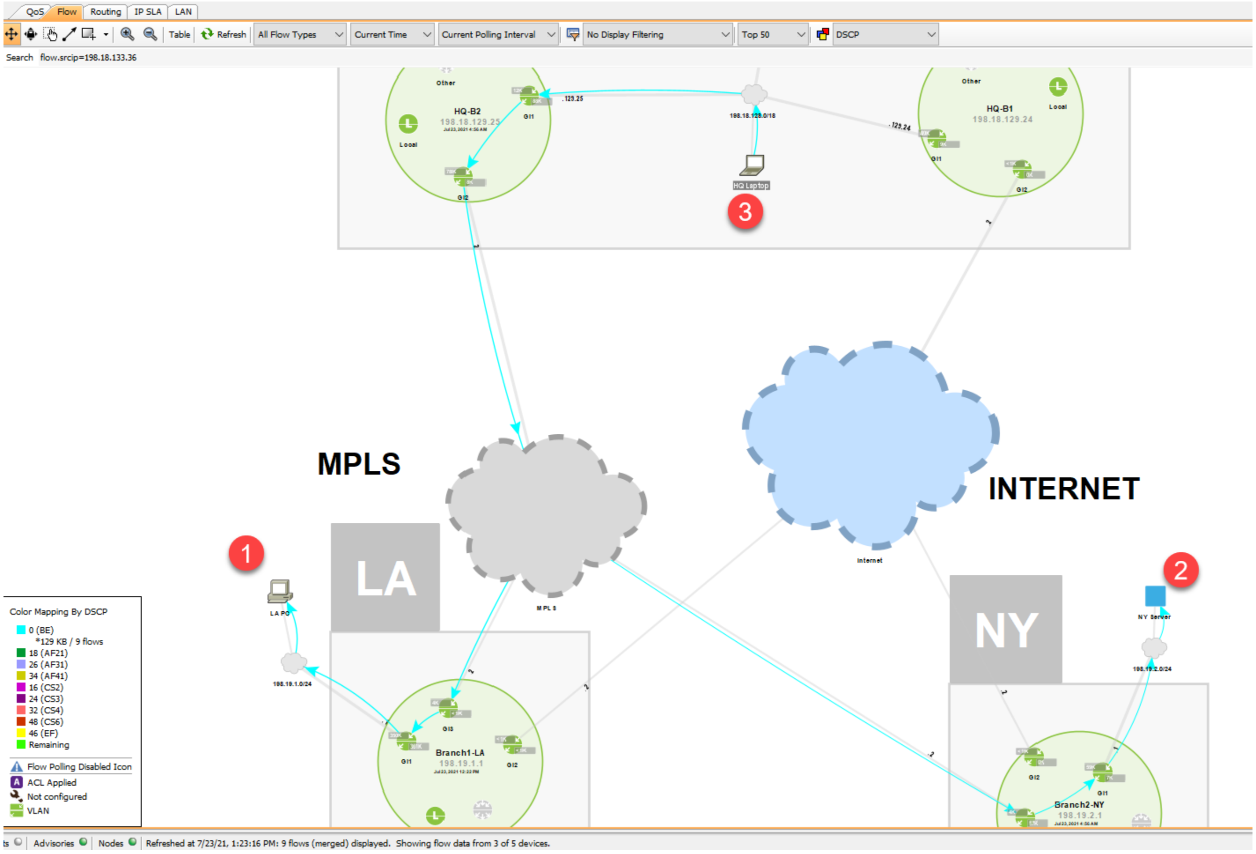
Type in an IP address, or select a device interface or IP address end point in the topology.

Object/Shape Generic Square

11. Select an Object/Shape as “**File Server**”.
12. Click **OK**. This will add the device to the diagram

13. Next, add a Laptop in HQ.
14. Enter the search string: flow.srcip=198.18.133.36
15. Select the flow (it will be near the HQ-B1 and HQ-B2 routers), right click on the IP Address endpoint.
16. Select **Create Network Object**.
17. Select an Object/Shape as “**Laptop**”.
18. Click **OK**.
19. Click **Refresh**.

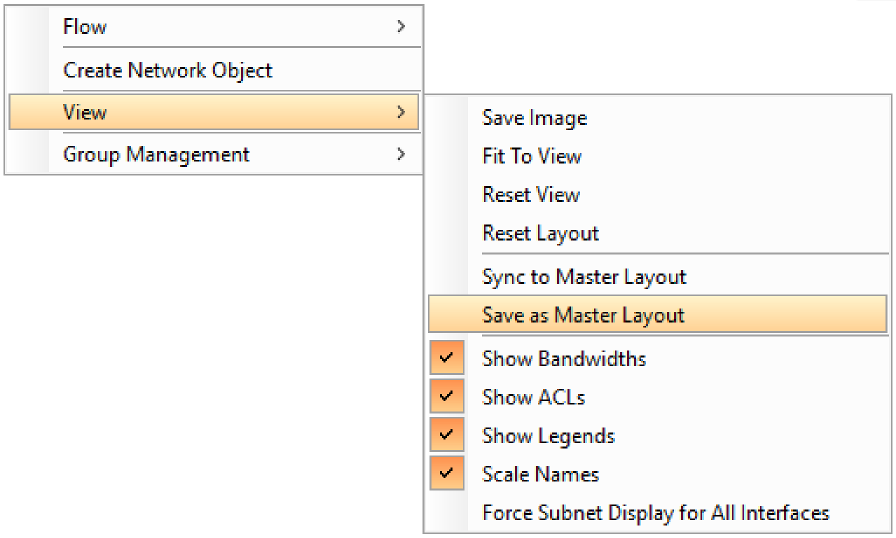
You will now see the flows to your new network objects.



Refreshed at 7/23/21, 1:23:16 PM: 9 flows (merged) displayed. Showing flow data from 3 of 5 devices.

Note: It is always good practice to save your best laid out topology as **Master Layout** (if you are an administrator) so that if you accidentally move devices on your topology, or would like to share your layout with others, you may then **Sync to Master Layout.**

20. To save the current layout as the master layout, right click anywhere on the white background, click **View**, and **Save as Master Layout**.



Lab 7

Lab 7: Dashboards & Reports

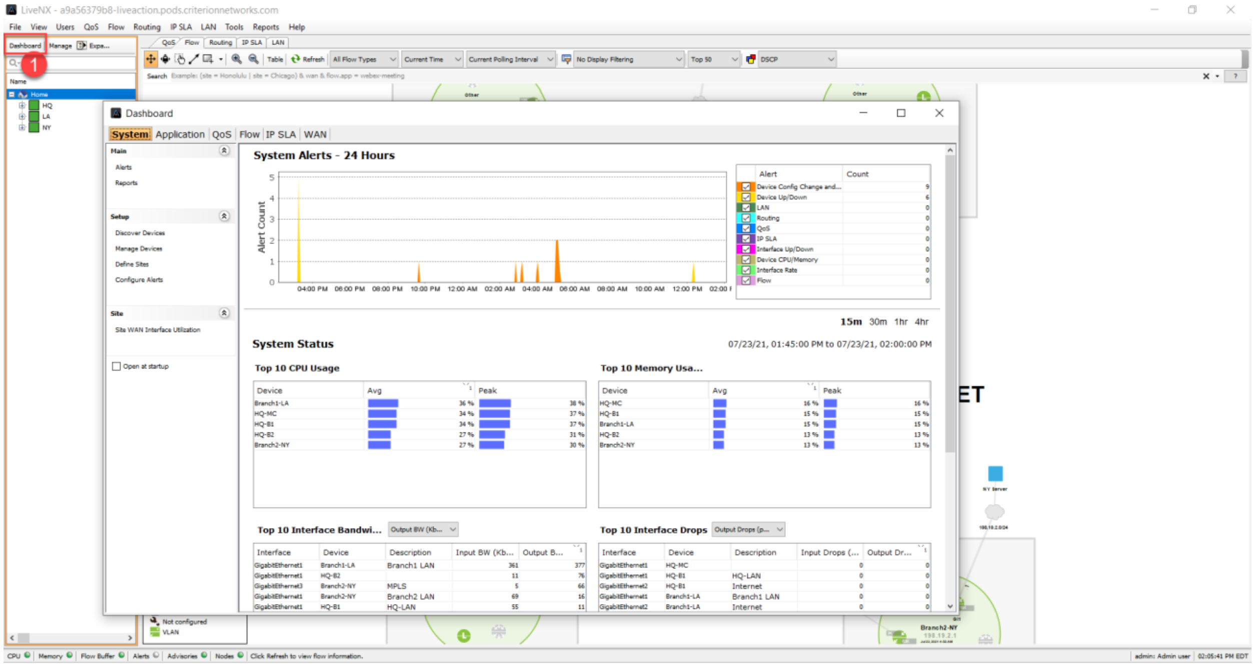
Lab 7.1: The Dashboard

The LiveNX Dashboard is your first stop to view overall network health. Alerts, Top CPU & Memory Usage, Bandwidth, Packet Drops, and more, are displayed in a System view. You may also view information, statistics, and alerts from Application, Flow, QoS, IP SLA, and WAN provided in separate tabs.

In this Lab you'll examine the data provided within the Dashboard views, and later use this as a launching-point to configure Alerts based-upon Dashboard results. We will investigate the Dashboards from both the Client and WebUI view.

Lab Steps:

1. Click the **Dashboard** tab (above the Home Tree-view). You will first see the **System** Dashboard.



LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expo...
1
Home
HQ
LA
NY
Dashboard
System Application QoS Flow IP SLA WAN
Main
Alerts
Reports
Setup
Discover Devices
Manage Devices
Define Sites
Configure Alerts
Site
Site WAN Interface Utilization
Open at startup
System Alerts - 24 Hours
Alert Count
04:00 PM 06:00 PM 08:00 PM 10:00 PM 12:00 AM 02:00 AM 04:00 AM 06:00 AM 08:00 AM 10:00 AM 12:00 PM 02:00 PM
15m 30m 1hr 4hr

Alert	Count
☑ Device Config Change and...	9
☑ Device Up/Down	6
☑ LAN	0
☑ Routing	0
☑ QoS	0
☑ IP SLA	0
☑ Interface Up/Down	0
☑ Device CPU/Memory	0
☑ Interface Rate	0
☑ Flow	0

System Status

07/23/21, 01:45:00 PM to 07/23/21, 02:00:00 PM

Top 10 CPU Usage

Device	Avg	Peak
Branch1-LA	36 %	38 %
HQ-MC	34 %	37 %
HQ-B1	34 %	37 %
HQ-B2	27 %	31 %
Branch2-NY	27 %	30 %

Top 10 Memory Usa...

Device	Avg	Peak
HQ-MC	16 %	16 %
HQ-B1	15 %	15 %
Branch1-LA	15 %	15 %
HQ-B2	13 %	13 %
Branch2-NY	13 %	13 %

Top 10 Interface Bandwi... Output BW (Kb...

Interface	Device	Description	Input BW (Kb...	Output B...
GigabitEthernet1	Branch1-LA	Branch1 LAN	361	377
GigabitEthernet1	HQ-B2		11	76
GigabitEthernet3	Branch2-NY	MPLS	5	66
GigabitEthernet1	Branch2-NY	Branch2 LAN	69	16
GigabitEthernet1	HQ-B1	HQ-LAN	55	11

Top 10 Interface Drops Output Drops (p...

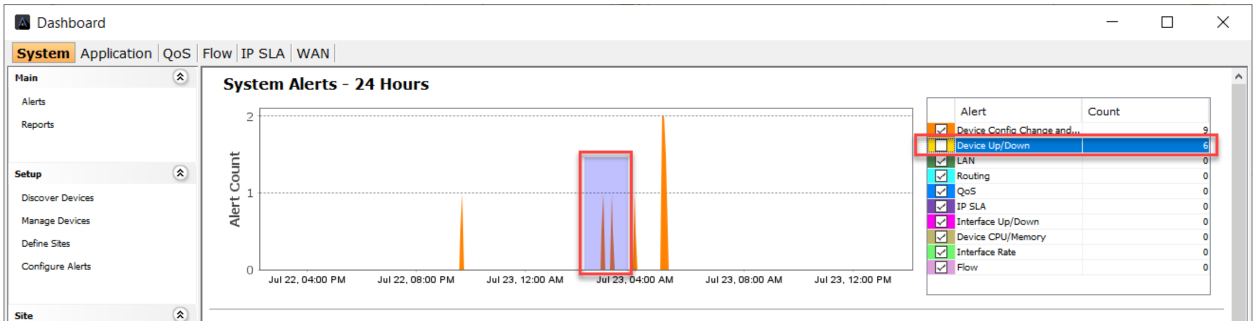
Interface	Device	Description	Input Drops (...	Output Dr...
GigabitEthernet1	HQ-MC		0	0
GigabitEthernet1	HQ-B1	HQ-LAN	0	0
GigabitEthernet2	HQ-B1	Internet	0	0
GigabitEthernet1	Branch1-LA	Branch1 LAN	0	0
GigabitEthernet2	Branch1-LA	Internet	0	0

Click Refresh to view flow information.

The Dashboard displays, showing a time-series of Alert Counts for the past 24-hours. To the right of the time-series note the Alert Type and Count.

2. Un-check any alerts that are not relevant to your view (in this case, device up down as we have been working in a lab environment to build this course – we know what those incidents are)

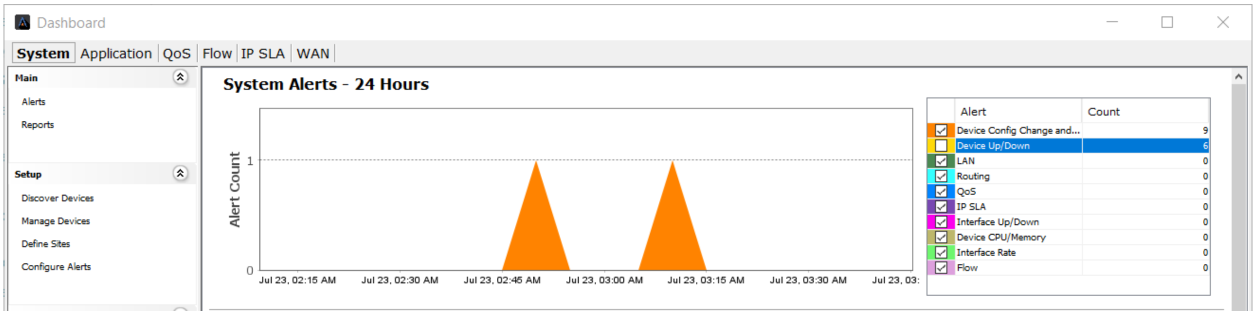
3. Left-click-Drag to Zoom into a flow of interest.



Alert	Count
☑ Device Config Change and...	9
□ Device Up/Down	6
☑ LAN	0
☑ Routing	0
☑ QoS	0
☑ IP SLA	0
☑ Interface Up/Down	0
☑ Device CPU/Memory	0
☑ Interface Rate	0
☑ Flow	0

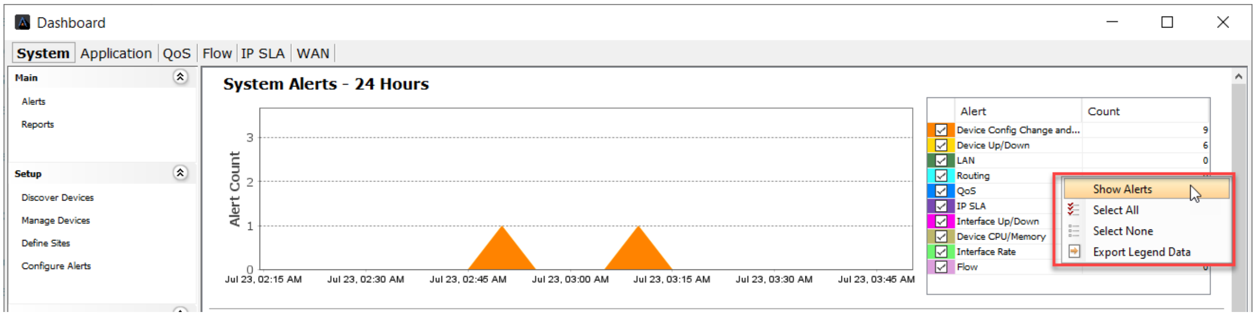
Note: Your results may not look the same as the images in this Lab. These images are for example purposes only.

Note: The following lab depends upon specific traffic being present at the specific time you are viewing. The *process* is important here… not the results!



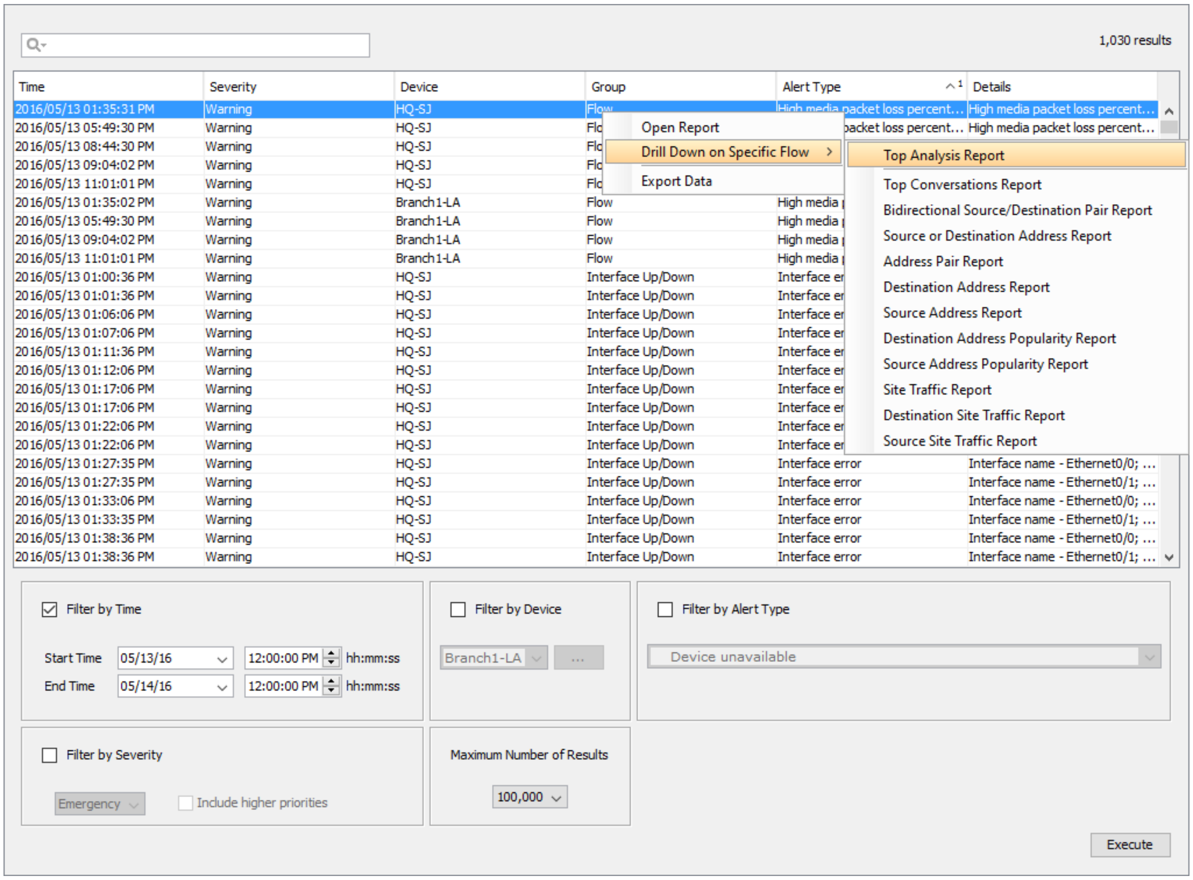
	Alert	Count
☑	Device Config Change and...	9
□	Device Up/Down	6
☑	LAN	0
☑	Routing	0
☑	QoS	0
☑	IP SLA	0
☑	Interface Up/Down	0
☑	Device CPU/Memory	0
☑	Interface Rate	0
☑	Flow	0

4. Right-click on the **Flow** Alert to the right side and select Show Alerts.



	Alert	Count
☑	Device Config Change and...	9
☑	Device Up/Down	6
☑	LAN	0
☑	Routing	[illegible]
☑	QoS	
☑	IP SLA	
☑	Interface Up/Down	
☑	Device CPU/Memory	
☑	Interface Rate	
☑	Flow	0

5. Click the **Alert Type** column header to re-sort.
6. Right-click a Flow alert and select Drill Down… and Top Analysis Report.



1,030 results

Time	Severity	Device	Group	Alert Type	Details
2016/05/13 01:35:31 PM	Warning	HQ-SJ	Flow	High media packet loss percent…	High media packet loss percent…
2016/05/13 05:49:30 PM	Warning	HQ-SJ	Flo	packet loss percent…	High media packet loss percent…
2016/05/13 08:44:30 PM	Warning	HQ-SJ	Flo		
2016/05/13 09:04:02 PM	Warning	HQ-SJ	Flo		
2016/05/13 11:01:01 PM	Warning	HQ-SJ	Flo		
2016/05/13 01:35:02 PM	Warning	Branch1-LA	Flow	High media	
2016/05/13 05:49:30 PM	Warning	Branch1-LA	Flow	High media	
2016/05/13 09:04:02 PM	Warning	Branch1-LA	Flow	High media	
2016/05/13 11:01:01 PM	Warning	Branch1-LA	Flow	High media	
2016/05/13 01:00:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:01:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:06:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:07:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:11:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:12:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:17:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:17:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	
2016/05/13 01:27:35 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; …
2016/05/13 01:27:35 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; …
2016/05/13 01:33:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; …
2016/05/13 01:33:35 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; …
2016/05/13 01:38:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; …
2016/05/13 01:38:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; …

Open Report
Drill Down on Specific Flow
Export Data
Top Analysis Report
Top Conversations Report
Bidirectional Source/Destination Pair Report
Source or Destination Address Report
Address Pair Report
Destination Address Report
Source Address Report
Destination Address Popularity Report
Source Address Popularity Report
Site Traffic Report
Destination Site Traffic Report
Source Site Traffic Report

☑ Filter by Time

Start Time 05/13/16 12:00:00 PM hh:mm:ss

End Time 05/14/16 12:00:00 PM hh:mm:ss

☐ Filter by Device

Branch1-LA

☐ Filter by Alert Type

Device unavailable

☐ Filter by Severity

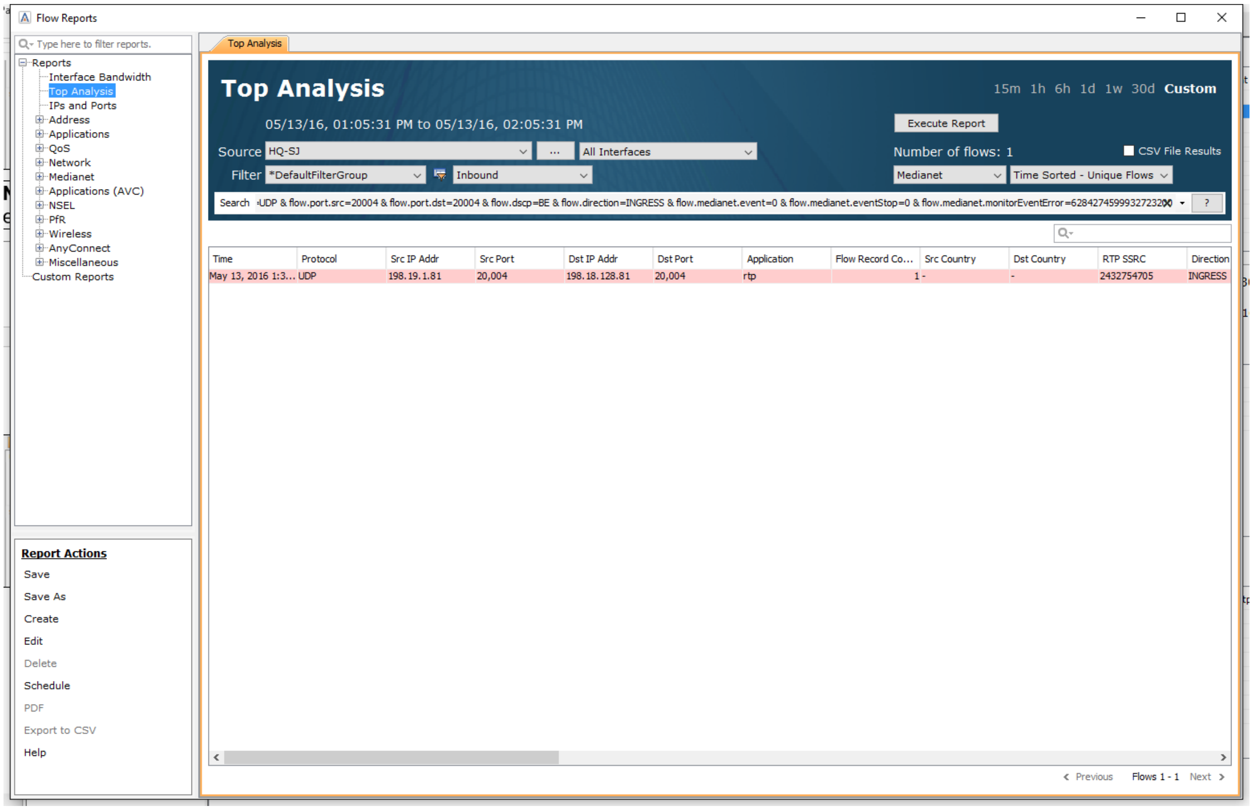
Emergency ☐ Include higher priorities

Maximum Number of Results

100,000

Note: The alert window contains a variety of Search and Filtering options. Although there is very little traffic in our lab Pods, remember… with a lot of time/data comes a lot of detractors. Filter/Search/Sort as needed in a production environment.

7. Review the Top Analysis Report.



Top Analysis

05/13/16, 01:05:31 PM to 05/13/16, 02:05:31 PM

Source: HQ-SJ, All Interfaces

Filter: *DefaultFilterGroup, Inbound

Number of flows: 1

Medianet, Time Sorted - Unique Flows

Search: UDP & flow.port.src=20004 & flow.port.dst=20004 & flow.dscp=BE & flow.direction=INGRESS & flow.medianet.event=0 & flow.medianet.eventStop=0 & flow.medianet.monitorEventError=62842745999327232

Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co...	Src Country	Dst Country	RTP SSRC	Direction
May 13, 2016 1:3...	UDP	198.19.1.81	20,004	198.18.128.81	20,004	rtp	1	-	-	2432754705	INGRESS

With about 5 clicks we’ve discovered WHICH flow was having troubles, what the problem may be, and the device, address pair, protocol, ports, etc. This Report may be printed/saved for documentation purposes.

Take some time to review the information in the other Dashboards; Application, QoS, etc.…, to familiarize yourself with the available statistics displayed.

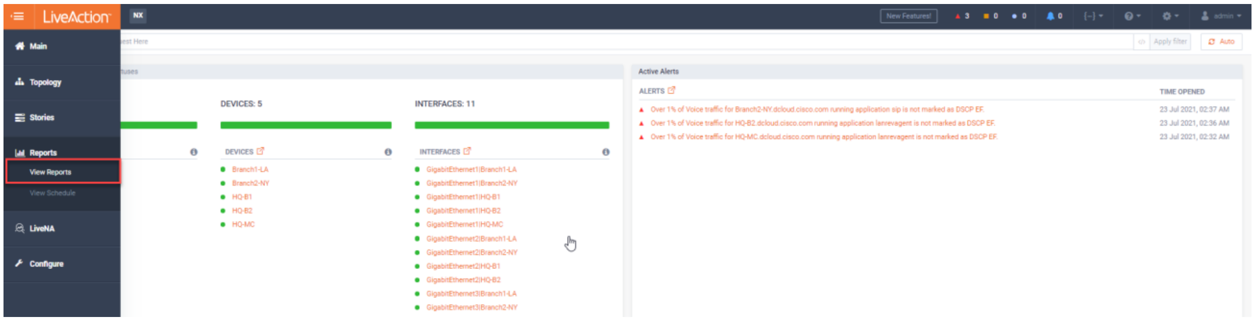
Lab 7.2: Viewing Reports

We'll run 3 of the most used reports, based-upon available data in our Training Pods. Reports work the same with any installation… only the data is changed (… to protect the innocent? ;-).

Lab Steps:

Run an Applications Report

1. You will be using the **WebUI** for this part of the lab.
2. Select **View Reports** from the menu on the left.



DEVICES: 5

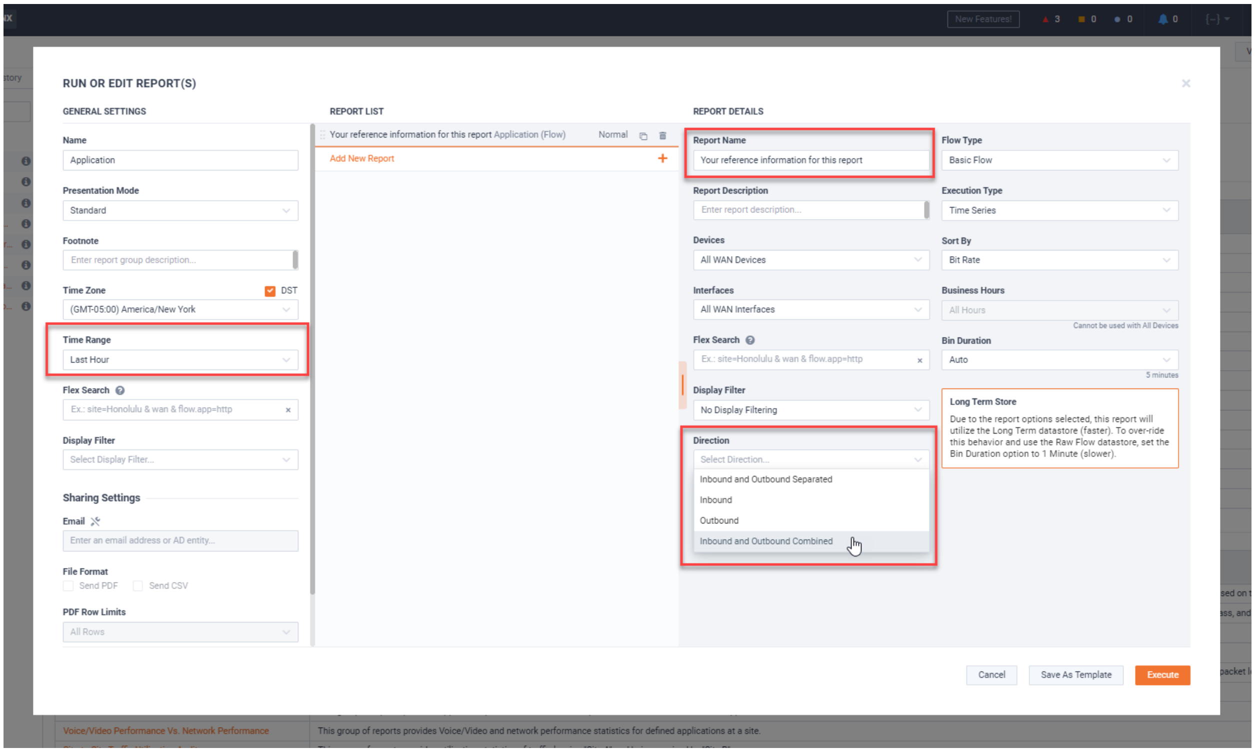
INTERFACES: 11

DEVICES
- Branch1-LA
- Branch2-NY
- HQ-B1
- HQ-B2
- HQ-MC

INTERFACES
- GigabitEthernet1|Branch1-LA
- GigabitEthernet1|Branch2-NY
- GigabitEthernet1|HQ-B1
- GigabitEthernet1|HQ-B2
- GigabitEthernet1|HQ-MC
- GigabitEthernet2|Branch1-LA
- GigabitEthernet2|Branch2-NY
- GigabitEthernet2|HQ-B1
- GigabitEthernet2|HQ-B2
- GigabitEthernet3|Branch1-LA
- GigabitEthernet3|Branch2-NY

ALERTS	TIME OPENED
Over 1% of Voice traffic for Branch2-NY.dcloud.cisco.com running application sip is not marked as DSCP EF.	23 Jul 2021, 02:37 AM
Over 1% of Voice traffic for HQ-B2.dcloud.cisco.com running application lanrevagent is not marked as DSCP EF.	23 Jul 2021, 02:36 AM
Over 1% of Voice traffic for HQ-MC.dcloud.cisco.com running application lanrevagent is not marked as DSCP EF.	23 Jul 2021, 02:32 AM

3. Select the **Application** report from **Top Reports**.
4. Enter a meaningful name for your report and select other options that are relevant to your task. Here I have chosen 1hour for the **Time Range.** You may want to view just a site, or a device. Be aware of what is needed.
5. Select the **Inbound and Outbound Combined** filter.



RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Name: Application

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone: (GMT-05:00) America/New York ☑ DST

Time Range: Last Hour

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: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

REPORT LIST

Your reference information for this report Application (Flow) Normal

REPORT DETAILS

Report Name: Your reference information for this report

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

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

Bin Duration: Auto

5 minutes

Display Filter: No Display Filtering

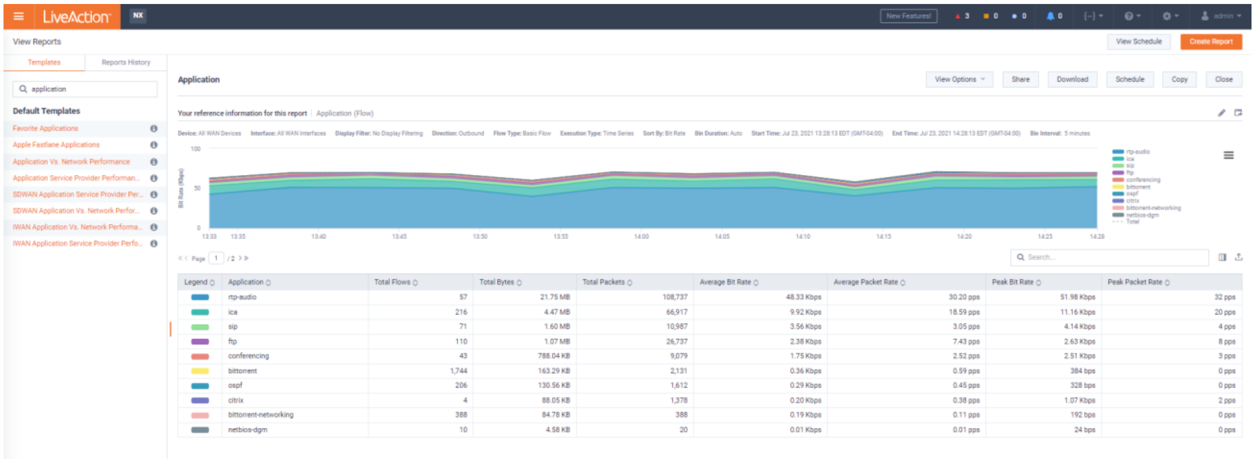
Long Term Store

Due to the report options selected, this report will utilize the Long Term datastore (faster). To over-ride this behavior and use the Raw Flow datastore, set the Bin Duration option to 1 Minute (slower).

Direction: Select Direction...
- Inbound and Outbound Separated
- Inbound
- Outbound
- Inbound and Outbound Combined

Voice/Video Performance Vs. Network Performance — This group of reports provides Voice/Video and network performance statistics for defined applications at a site.

6. Click **Execute**.



Your reference information for this report | Application (Flow)

Device: All WAN Devices Interface: All WAN Interfaces Display Filter: No Display Filtering Direction: Outbound Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Bin Duration: Auto Start Time: Jul 23, 2021 13:28:13 EDT (GMT-04:00) End Time: Jul 23, 2021 14:28:13 EDT (GMT-04:00) Bin Interval: 5 minutes

Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
▬	rtp-audio	57	21.75 MB	108,737	48.33 Kbps	30.20 pps	51.98 Kbps	32 pps
▬	ica	216	4.47 MB	66,917	9.92 Kbps	18.59 pps	11.16 Kbps	20 pps
▬	sip	71	1.60 MB	10,987	3.56 Kbps	3.05 pps	4.14 Kbps	4 pps
▬	ftp	110	1.07 MB	26,737	2.38 Kbps	7.43 pps	2.63 Kbps	8 pps
▬	conferencing	43	788.04 KB	9,079	1.75 Kbps	2.52 pps	2.51 Kbps	3 pps
▬	bittorrent	1,744	163.29 KB	2,131	0.36 Kbps	0.59 pps	384 bps	0 pps
▬	ospf	206	130.56 KB	1,612	0.29 Kbps	0.45 pps	328 bps	0 pps
▬	citrix	4	88.05 KB	1,378	0.20 Kbps	0.38 pps	1.07 Kbps	2 pps
▬	bittorrent-networking	388	84.78 KB	388	0.19 Kbps	0.11 pps	192 bps	0 pps
▬	netbios-dgm	10	4.58 KB	20	0.01 Kbps	0.01 pps	24 bps	0 pps

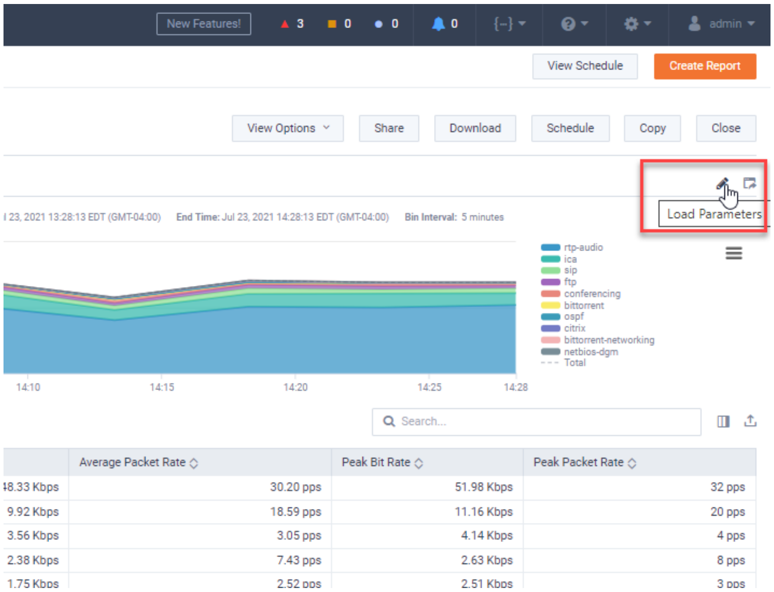
Note: Your results may not look the same as the images in this Lab. These images are for example purposes only.

The default **Application** report is displayed when you select Reports, and after you clicked Execute Report the system filled-in the report template with current 15-minute data. Notice the report parameters **(A)**, the various applications **(B)**, view options **(C)**, export options **(D)** and the actual data in the report **(E)**.

When you run a report… try to do filtering and searching so the system only needs to pull appropriate data to answer your question. LEAVE THE REPORT OPEN!

Run a Top Talkers Report

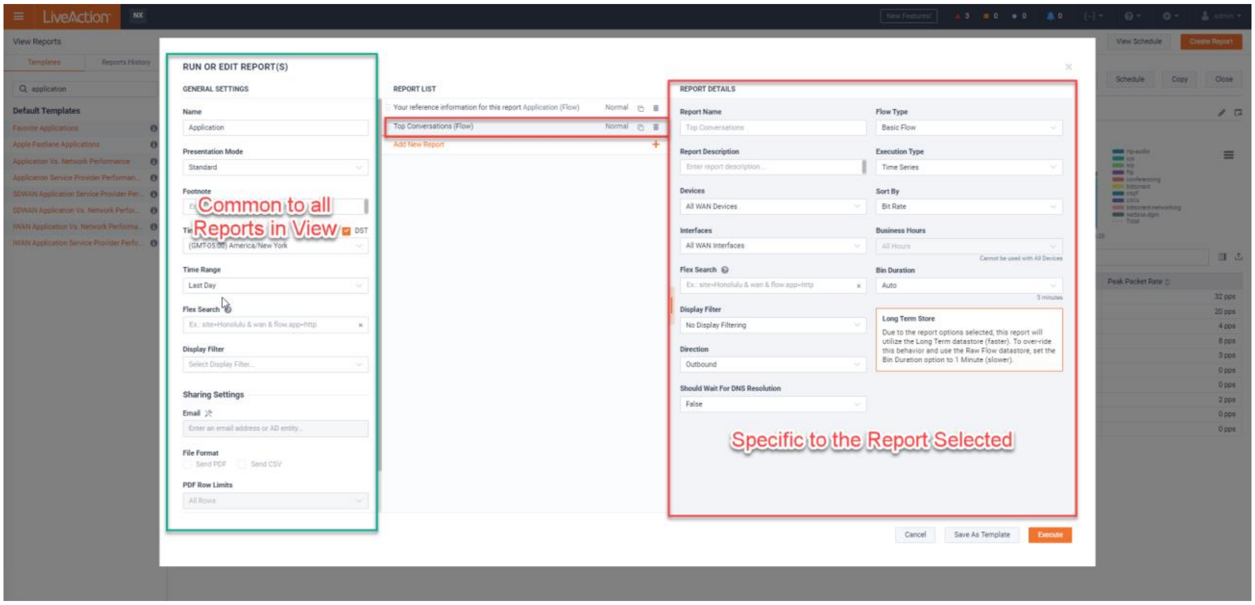
1. Click on the Pen icon near the top-right side of the report to load the current report parameters.



l 23, 2021 13:28:13 EDT (GMT-04:00) End Time: Jul 23, 2021 14:28:13 EDT (GMT-04:00) Bin Interval: 5 minutes

	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
48.33 Kbps	30.20 pps	51.98 Kbps	32 pps
9.92 Kbps	18.59 pps	11.16 Kbps	20 pps
3.56 Kbps	3.05 pps	4.14 Kbps	4 pps
2.38 Kbps	7.43 pps	2.63 Kbps	8 pps
1.75 Kbps	2.52 pps	2.51 Kbps	3 pps

2. Click **Add New** Report, and then select **Top Conversations**.
3. You will be able to configure parameters that will affect both reports, and certain parameters specifically for the **Top Conversations** report. These parameters are independent of the original **Applications** report.


Common to all Reports in View
Specific to the Report Selected
Cancel
Save As Template
Execute

RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Name: Application

Presentation Mode: Standard

Time Zone: (GMT-05:00) America/New York ☑ DST

Time Range: Last Day

Display Filter: Select Display Filter...

Sharing Settings

File Format: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

REPORT LIST

Your reference information for this report Application (Flow) Normal

Top Conversations (Flow) Normal

Add New Report

REPORT DETAILS

Report Name: Top Conversations

Flow Type: Basic Flow

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 (5 minutes)

Display Filter: No Display Filtering

Direction: Outbound

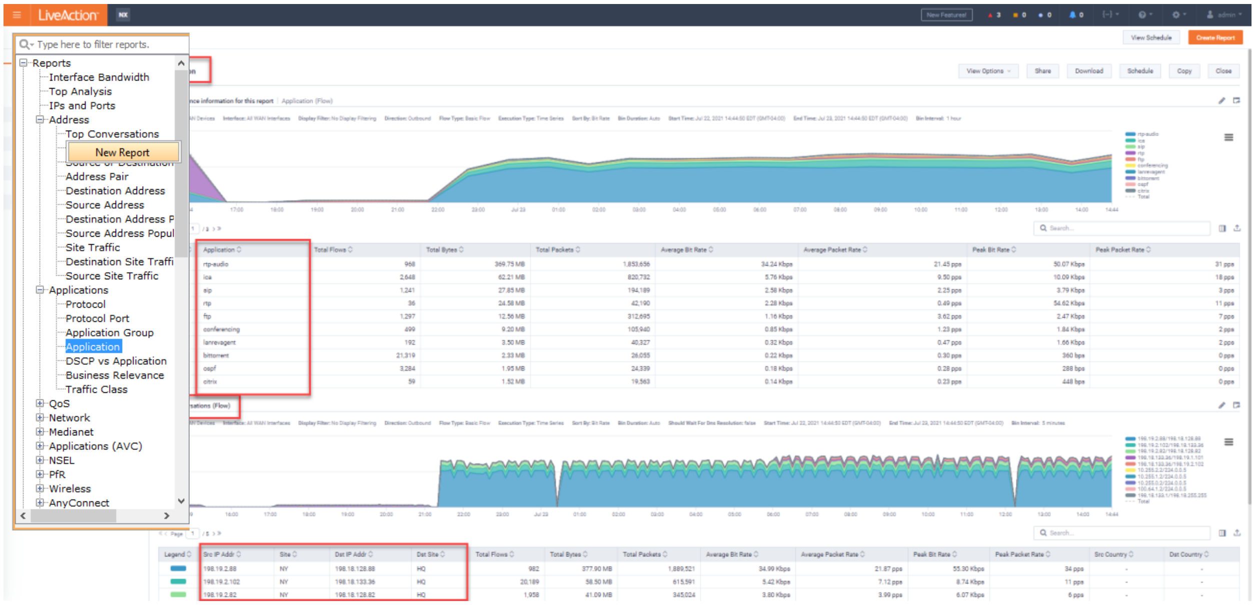
Should Wait For DNS Resolution: False

Long Term Store

Due to the report options selected, this report will utilize the Long Term datastore (faster). To over-ride this behavior and use the Raw Flow datastore, set the Bin Duration option to 1 Minute (slower).

4. Click **Execute**.

Note: Your results may not look the same as the images in this Lab. These images are for example purposes only.



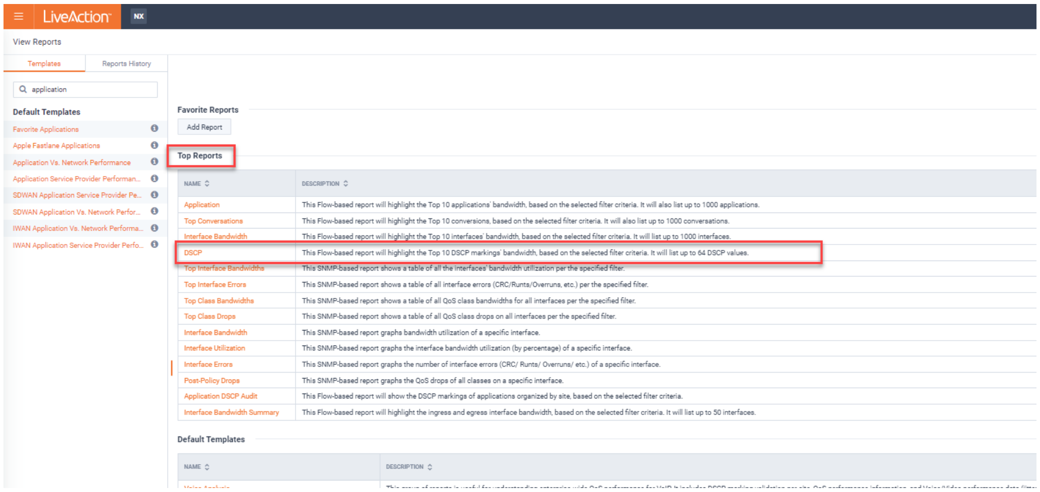
Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
rtp-audio	968	369.75 MB	1,853,656	34.24 Kbps	21.45 pps	50.07 Kbps	31 pps
ica	2,648	62.21 MB	820,732	5.76 Kbps	9.50 pps	10.09 Kbps	18 pps
sip	1,241	27.85 MB	194,189	2.58 Kbps	2.25 pps	3.79 Kbps	3 pps
rtp	36	24.58 MB	42,190	2.28 Kbps	0.49 pps	54.62 Kbps	11 pps
ftp	1,297	12.56 MB	312,695	1.16 Kbps	3.62 pps	2.47 Kbps	7 pps
conferencing	499	9.20 MB	105,940	0.85 Kbps	1.23 pps	1.84 Kbps	2 pps
lanrevagent	192	3.50 MB	40,327	0.32 Kbps	0.47 pps	1.66 Kbps	2 pps
bittorrent	21,319	2.33 MB	26,055	0.22 Kbps	0.30 pps	360 bps	0 pps
ospf	3,284	1.95 MB	24,339	0.18 Kbps	0.28 pps	288 bps	0 pps
citrix	59	1.52 MB	19,563	0.14 Kbps	0.23 pps	448 bps	0 pps

Legend	Src IP Addr	Site	Dst IP Addr	Dst Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate	Src Country	Dst Country
🟦	198.19.2.88	NY	198.18.128.88	HQ	982	377.90 MB	1,889,521	34.99 Kbps	21.87 pps	55.30 Kbps	34 pps	-	-
🟩	198.19.2.102	NY	198.18.133.36	HQ	20,189	58.50 MB	615,591	5.42 Kbps	7.12 pps	8.74 Kbps	11 pps	-	-
🟩	198.19.2.82	NY	198.18.128.82	HQ	1,958	41.09 MB	345,024	3.80 Kbps	3.99 pps	6.07 Kbps	6 pps	-	-

This **Top Conversations** report has been appended to the **Applications** report. in the selected time period including Source address, Destination address, total flows, etc.… a good way to see who is using the bandwidth, and what for… All that BitTorrent may not be good for business! Right-clicking to open a New Report leaves the prior reports open, in a tabbed manner, for comparison purposes. Bin Duration has been singled out as different.

Flow Identification

1. Close the report view. Next, we will look at QoS information by **DSCP** value.
2. On the report menu, click **DSCP**.



Default Templates

- Favorite Applications
- Apple Fastlane Applications
- Application Vs. Network Performance
- Application Service Provider Performan...
- SDWAN Application Service Provider Pe...
- SDWAN Application Vs. Network Perfor...
- IWAN Application Vs. Network Performa...
- IWAN Application Service Provider Perfo...

Favorite Reports

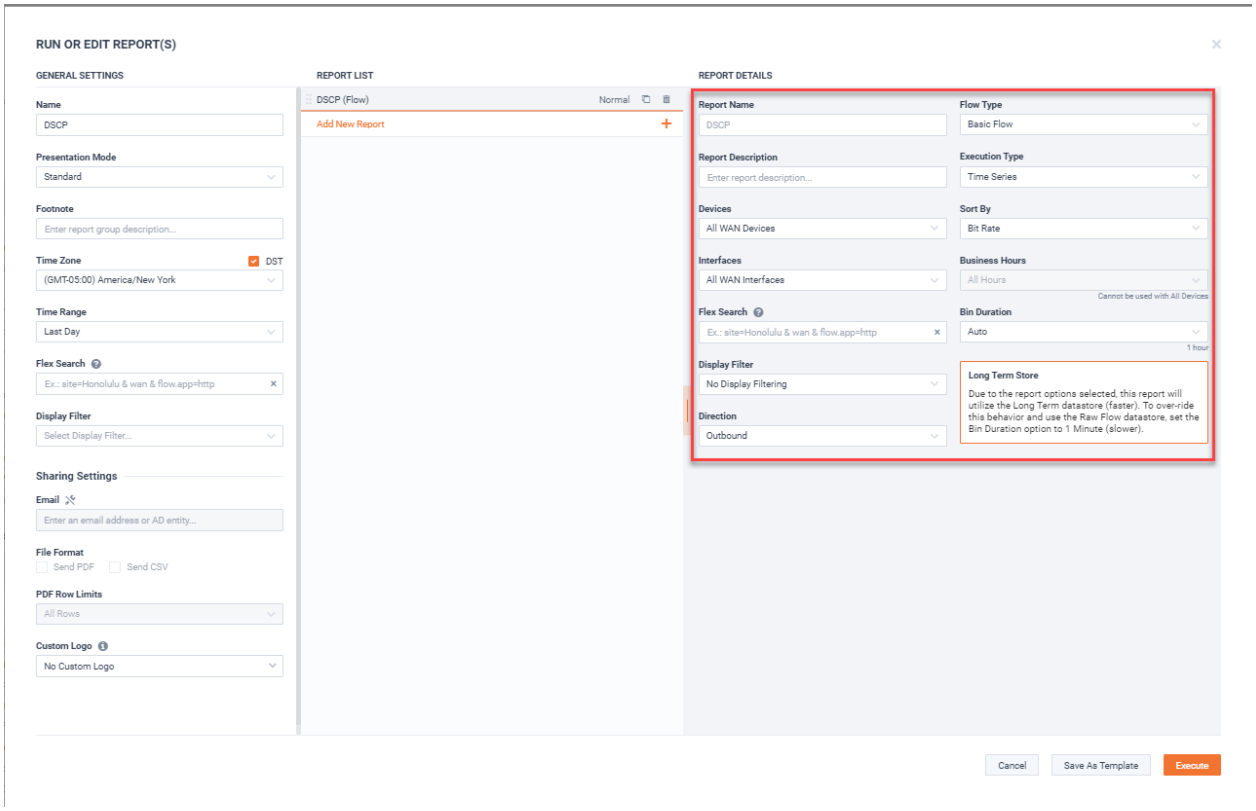
Top Reports

NAME	DESCRIPTION
Application	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.
Top Conversations	This Flow-based report will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.
Interface Bandwidth	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.
DSCP	This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
Top Interface Bandwidths	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.
Top Interface Errors	This SNMP-based report shows a table of all interface errors (CRC/Runts/Overruns, etc.) per the specified filter.
Top Class Bandwidths	This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.
Top Class Drops	This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.
Interface Bandwidth	This SNMP-based report graphs bandwidth utilization of a specific interface.
Interface Utilization	This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.
Interface Errors	This SNMP-based report graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.
Post-Policy Drops	This SNMP-based report graphs the QoS drops of all classes on a specific interface.
Application DSCP Audit	This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.
Interface Bandwidth Summary	This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.

Default Templates

NAME	DESCRIPTION

3. For this exercise, do not alter any default parameters, but review the options available.



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: Last Day

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: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

Custom Logo: No Custom Logo

REPORT LIST

DSCP (Flow) Normal

Add New Report +

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

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

Bin Duration: Auto

1 hour

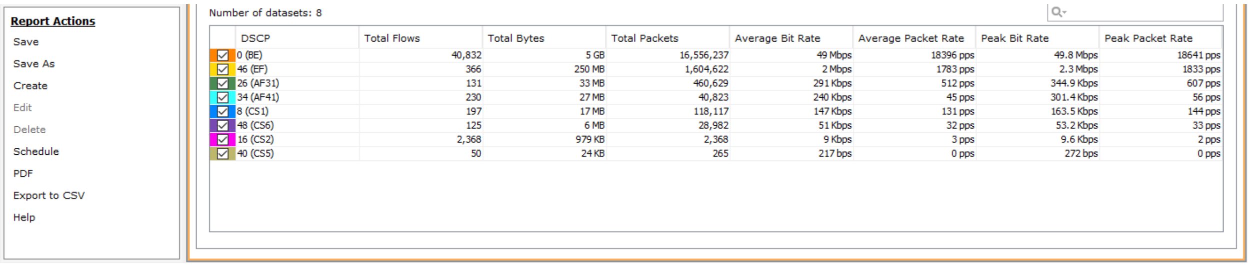
Display Filter: No Display Filtering

Direction: Outbound

Long Term Store

Due to the report options selected, this report will utilize the Long Term datastore (faster). To over-ride this behavior and use the Raw Flow datastore, set the Bin Duration option to 1 Minute (slower).

4. Click **Execute**.



Report Actions

- Save
- Save As
- Create
- Edit
- Delete
- Schedule
- PDF
- Export to CSV
- Help

Number of datasets: 8

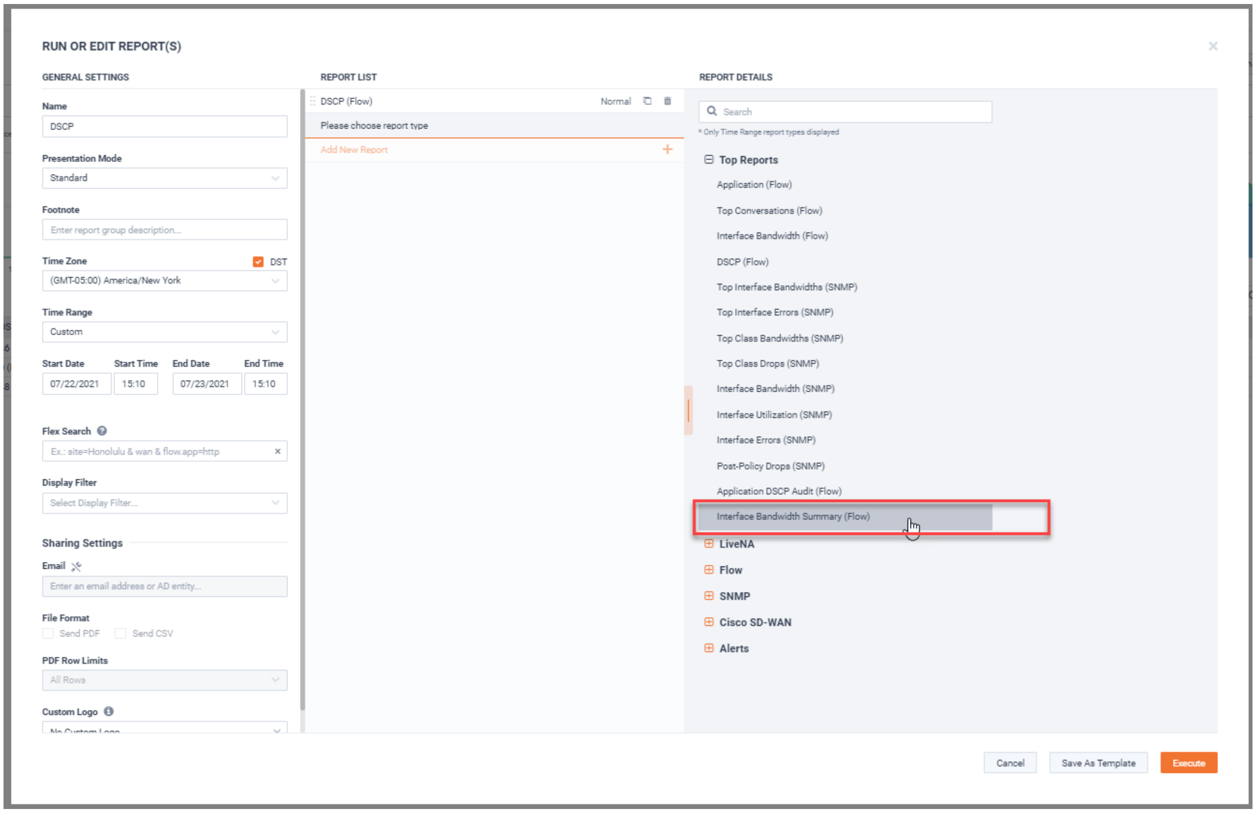
	DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
🟧 ☑	0 (BE)	40,832	5 GB	16,556,237	49 Mbps	18396 pps	49.8 Mbps	18641 pps
🟨 ☑	46 (EF)	366	250 MB	1,604,622	2 Mbps	1783 pps	2.3 Mbps	1833 pps
🟩 ☑	26 (AF31)	131	33 MB	460,629	291 Kbps	512 pps	344.9 Kbps	607 pps
☑	34 (AF41)	230	27 MB	40,823	240 Kbps	45 pps	301.4 Kbps	56 pps
🟦 ☑	8 (CS1)	197	17 MB	118,117	147 Kbps	131 pps	163.5 Kbps	144 pps
🟪 ☑	48 (CS6)	125	6 MB	28,982	51 Kbps	32 pps	53.2 Kbps	33 pps
☑	16 (CS2)	2,368	979 KB	2,368	9 Kbps	3 pps	9.6 Kbps	2 pps
☑	40 (CS5)	50	24 KB	265	217 bps	0 pps	272 bps	0 pps

Look at the distribution of discovered traffic across the DSCP values. What does the amount of traffic marked 0(BE) tell you?

0(BE) traffic has not been recognized as a certain type by the router and it will use its BEST EFFORT to route it. This **may** be a candidate for marking so that QoS may use priority routing.

Bandwidth by Flow Type

5. Let's add some more information to our page. Click the **Load** Parameters pen icon and add **Interface Bandwidth Summary** from the Top Reports section.



RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Name: DSCP

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone: (GMT-05:00) America/New York ☑ DST

Time Range: Custom

Start Date	Start Time	End Date	End Time
07/22/2021	15:10	07/23/2021	15:10

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: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

Custom Logo: No Custom Logo

REPORT LIST

DSCP (Flow) Normal

Please choose report type

Add New Report +

REPORT DETAILS

Search

* Only Time Range report types displayed

⊟ Top Reports
- Application (Flow)
- Top Conversations (Flow)
- Interface Bandwidth (Flow)
- DSCP (Flow)
- Top Interface Bandwidths (SNMP)
- Top Interface Errors (SNMP)
- Top Class Bandwidths (SNMP)
- Top Class Drops (SNMP)
- Interface Bandwidth (SNMP)
- Interface Utilization (SNMP)
- Interface Errors (SNMP)
- Post-Policy Drops (SNMP)
- Application DSCP Audit (Flow)
- Interface Bandwidth Summary (Flow)

⊞ LiveNA

⊞ Flow

⊞ SNMP

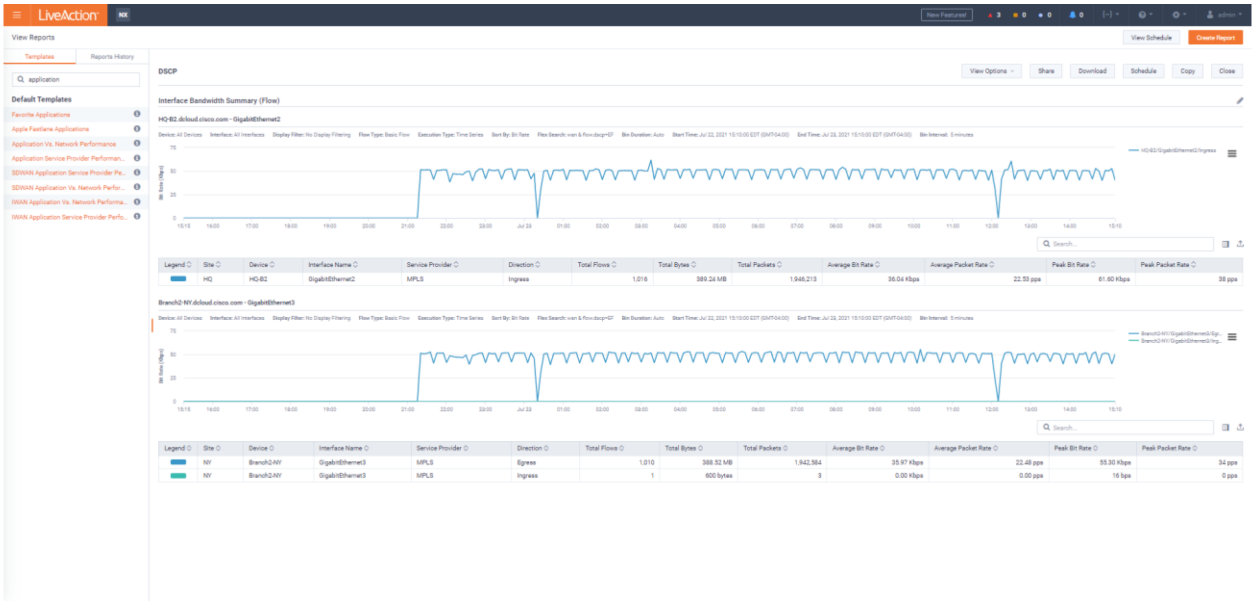
⊞ Cisco SD-WAN

⊞ Alerts

6. Enter a Search String: **wan & flow.dscp=EF** (note upper-case).

7. Select **All** devices.

8. Click **Execute**.



Default Templates
- Favorite Applications
- Apple Fastlane Applications
- Application Vs. Network Performance
- Application Service Provider Performan...
- SDWAN Application Service Provider Pe...
- SDWAN Application Vs. Network Perfor...
- IWAN Application Vs. Network Performa...
- IWAN Application Service Provider Perfo...

DSCP

Interface Bandwidth Summary (Flow)

HQ-B2.dcloud.cisco.com - GigabitEthernet2

Device: All Devices Interface: All Interfaces Display Filter: No Display Filtering Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Flex Search: wan & flow.dscp=EF Bin Duration: Auto Start Time: Jul 22, 2021 15:10:00 EDT (GMT-04:00) End Time: Jul 23, 2021 15:10:00 EDT (GMT-04:00) Bin Interval: 5 minutes

Legend	Site	Device	Interface Name	Service Provider	Direction	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
🟦	HQ	HQ-B2	GigabitEthernet2	MPLS	Ingress	1,016	389.24 MB	1,946,213	36.04 Kbps	22.53 pps	61.60 Kbps	38 pps

Branch2-NY.dcloud.cisco.com - GigabitEthernet3

Device: All Devices Interface: All Interfaces Display Filter: No Display Filtering Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Flex Search: wan & flow.dscp=EF Bin Duration: Auto Start Time: Jul 22, 2021 15:10:00 EDT (GMT-04:00) End Time: Jul 23, 2021 15:10:00 EDT (GMT-04:00) Bin Interval: 5 minutes

Legend	Site	Device	Interface Name	Service Provider	Direction	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
🟦	NY	Branch2-NY	GigabitEthernet3	MPLS	Egress	1,010	388.52 MB	1,942,584	35.97 Kbps	22.48 pps	55.30 Kbps	34 pps
🟩	NY	Branch2-NY	GigabitEthernet3	MPLS	Ingress	1	600 bytes	3	0.00 Kbps	0.00 pps	16 bps	0 pps

This report shows the INGRESS & EGRESS flows for each relevant interface, for all marked EF traffic flows. This is a Quick way to see how much traffic "stays inside" and how much transits the device.

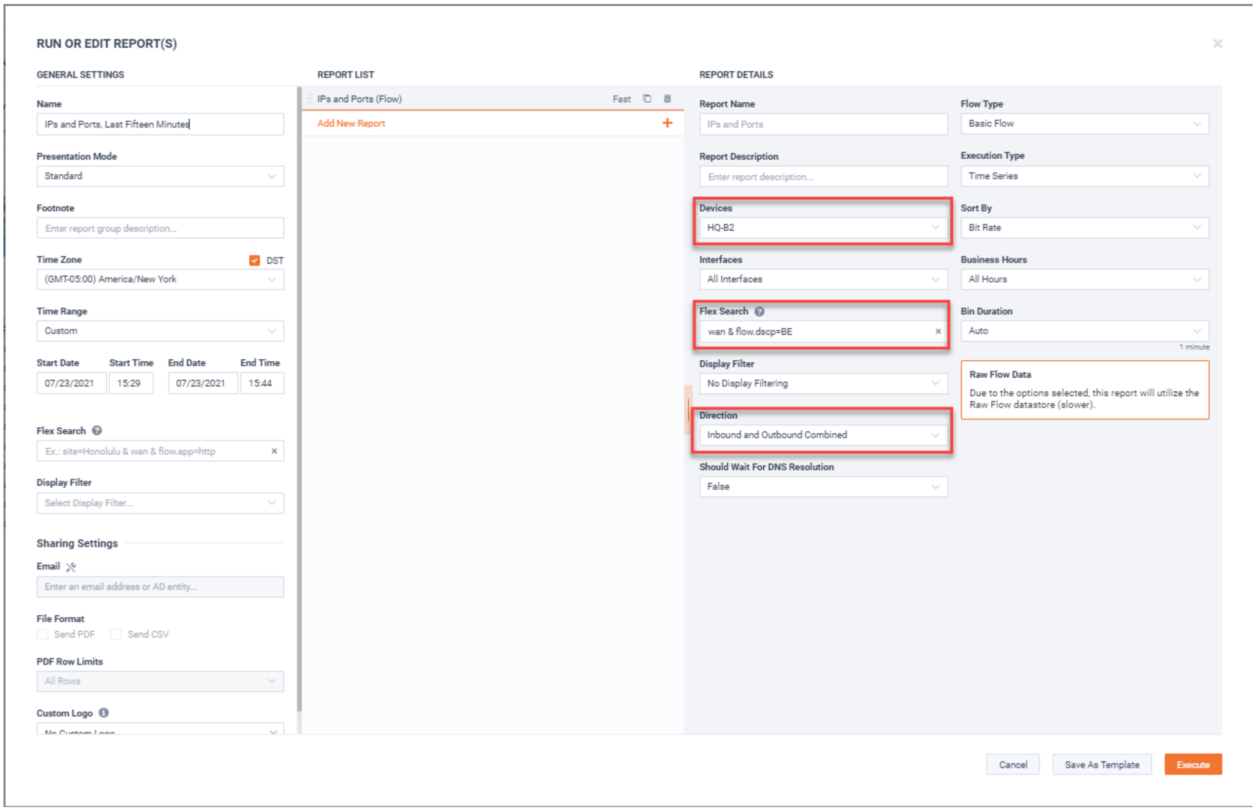
Note: Your results may not look the same as the images in this Lab. These images are for example purposes only.

Lab 7.3: Create a Custom Report

In this Lab you'll create a Custom Report to display the last of the most popular reports. Although the IPs and Ports are now an included report, due to its popularity, we'll create a similar Custom report to visualize the process.

Lab Steps:

1. In the **View Reports** page, click on **Create Report** at the top-right of the screen.
2. Click on **Flow**, then **Analysis**, and select **IPs and Ports**.
    a. Name your report. (**Do not use "&"**)
3. Select **HQ-B2** device.
4. Enter **wan & flow.dscp=EF** in the Flex Search field.
5. Set the **Direction** as **Inbound and Outbound Combined**. the Fields as indicated in the diagram, below.
6. Click Execute Report.



RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Name: IPs and Ports, Last Fifteen Minutes

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone: (GMT-05:00) America/New York ☑ DST

Time Range: Custom

Start Date	Start Time	End Date	End Time
07/23/2021	15:29	07/23/2021	15:44

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: □ Send PDF □ Send CSV

PDF Row Limits: All Rows

Custom Logo: No Custom Logo

REPORT LIST

IPs and Ports (Flow) Fast

Add New Report +

REPORT DETAILS

Report Name: IPs and Ports

Report Description: Enter report description...

Devices: HQ-B2

Interfaces: All Interfaces

Flex Search: wan & flow.dscp=BE

Display Filter: No Display Filtering

Direction: Inbound and Outbound Combined

Should Wait For DNS Resolution: False

Flow Type: Basic Flow

Execution Type: Time Series

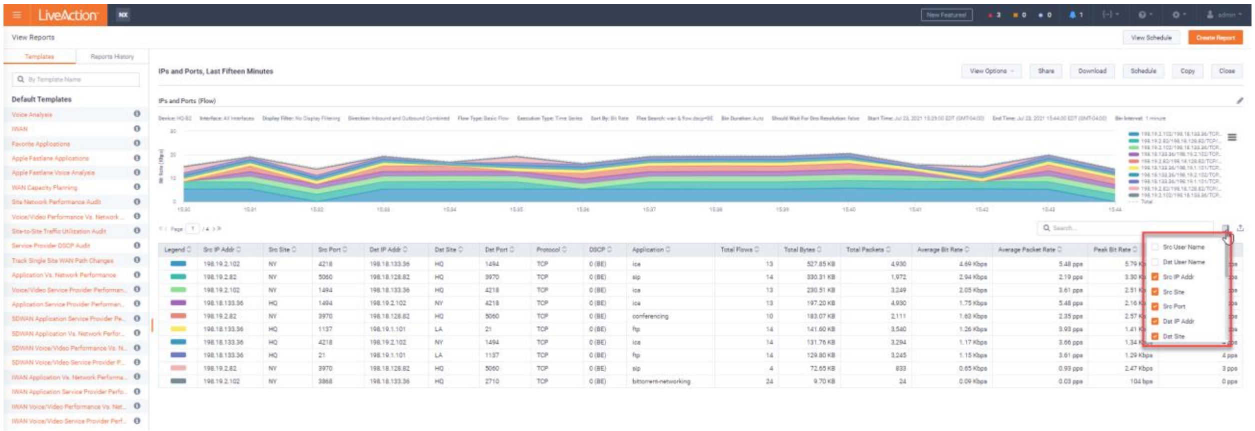
Sort By: Bit Rate

Business Hours: All Hours

Bin Duration: Auto (1 minute)

Raw Flow Data

Due to the options selected, this report will utilize the Raw Flow datastore (slower).


LiveAction
NX
New Features!
3
0
0
1
admin
View Reports
View Schedule
Create Report
Templates
Reports History
By Template Name
Default Templates
Voice Analysis
IWAN
Favorite Applications
Apple Fastlane Applications
Apple Fastlane Voice Analysis
WAN Capacity Planning
Site Network Performance Audit
Voice/Video Performance Vs. Network ...
Site-to-Site Traffic Utilization Audit
Service Provider DSCP Audit
Track Single Site WAN Path Changes
Application Vs. Network Performance
Voice/Video Service Provider Performan...
Application Service Provider Performan...
SDWAN Application Service Provider Pe...
SDWAN Application Vs. Network Perfor...
SDWAN Voice/Video Performance Vs. N...
SDWAN Voice/Video Service Provider P...
IWAN Application Vs. Network Performa...
IWAN Application Service Provider Perfo...
IWAN Voice/Video Performance Vs. Net...
IWAN Voice/Video Service Provider Perf...
View Options
Share
Download
Schedule
Copy
Close
Bit Rate (Mbps)
30
20
10
0
15:30
15:31
15:32
15:33
15:34
15:35
15:36
15:37
15:38
15:39
15:40
15:41
15:42
15:43
15:44
198.19.2.102/198.18.133.36/TCP...
198.19.2.82/198.18.128.82/TCP/...
198.19.2.102/198.18.133.36/TCP...
198.18.133.36/198.19.2.102/TCP...
198.19.2.82/198.18.128.82/TCP/...
198.18.133.36/198.19.1.101/TCP...
198.18.133.36/198.19.2.102/TCP...
198.18.133.36/198.19.1.101/TCP...
198.19.2.82/198.18.128.82/TCP/...
198.19.2.102/198.18.133.36/TCP...
Total
Page 1 / 4
Search...
☐ Src User Name
☐ Dst User Name
☑ Src IP Addr
☑ Src Site
☑ Src Port
☑ Dst IP Addr
☑ Dst Site

IPs and Ports, Last Fifteen Minutes

IPs and Ports (Flow)

Device: HQ-B2 Interface: All Interfaces Display Filter: No Display Filtering Direction: Inbound and Outbound Combined Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Flex Search: wan & flow.dscp=BE Bin Duration: Auto Should Wait For Dns Resolution: false Start Time: Jul 23, 2021 15:29:00 EDT (GMT-04:00) End Time: Jul 23, 2021 15:44:00 EDT (GMT-04:00) Bin Interval: 1 minute

Legend	Src IP Addr	Src Site	Src Port	Dst IP Addr	Dst Site	Dst Port	Protocol	DSCP	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	
🟦	198.19.2.102	NY	4218	198.18.133.36	HQ	1494	TCP	0 (BE)	ica	13	527.85 KB	4,930	4.69 Kbps	5.48 pps	5.79 K	
🟩	198.19.2.82	NY	5060	198.18.128.82	HQ	3970	TCP	0 (BE)	sip	14	330.31 KB	1,972	2.94 Kbps	2.19 pps	3.30 K	
🟩	198.19.2.102	NY	1494	198.18.133.36	HQ	4218	TCP	0 (BE)	ica	13	230.51 KB	3,249	2.05 Kbps	3.61 pps	2.51 K	
🟪	198.18.133.36	HQ	1494	198.19.2.102	NY	4218	TCP	0 (BE)	ica	13	197.20 KB	4,930	1.75 Kbps	5.48 pps	2.16 K	
🟥	198.19.2.82	NY	3970	198.18.128.82	HQ	5060	TCP	0 (BE)	conferencing	10	183.07 KB	2,111	1.63 Kbps	2.35 pps	2.57 K	
🟨	198.18.133.36	HQ	1137	198.19.1.101	LA	21	TCP	0 (BE)	ftp	14	141.60 KB	3,540	1.26 Kbps	3.93 pps	1.41 K	
🟦	198.18.133.36	HQ	4218	198.19.2.102	NY	1494	TCP	0 (BE)	ica	14	131.76 KB	3,294	1.17 Kbps	3.66 pps	1.34 K	
🟦	198.18.133.36	HQ	21	198.19.1.101	LA	1137	TCP	0 (BE)	ftp	14	129.80 KB	3,245	1.15 Kbps	3.61 pps	1.29 Kbps	4 pps
🟥	198.19.2.82	NY	3970	198.18.128.82	HQ	5060	TCP	0 (BE)	sip	4	72.65 KB	833	0.65 Kbps	0.93 pps	2.47 Kbps	3 pps
⬛	198.19.2.102	NY	3868	198.18.133.36	HQ	2710	TCP	0 (BE)	bittorrent-networking	24	9.70 KB	24	0.09 Kbps	0.03 pps	104 bps	0 pps

You now have a report which, at-a-glance, shows all the flows that are using **Best Effort**. You can select which columns to show or hide simply by selecting and deselecting them in the **Filter Columns dropdown**.

Lab 8

Lab 8: QoS

Lab 8.1: QoS Marking Policy

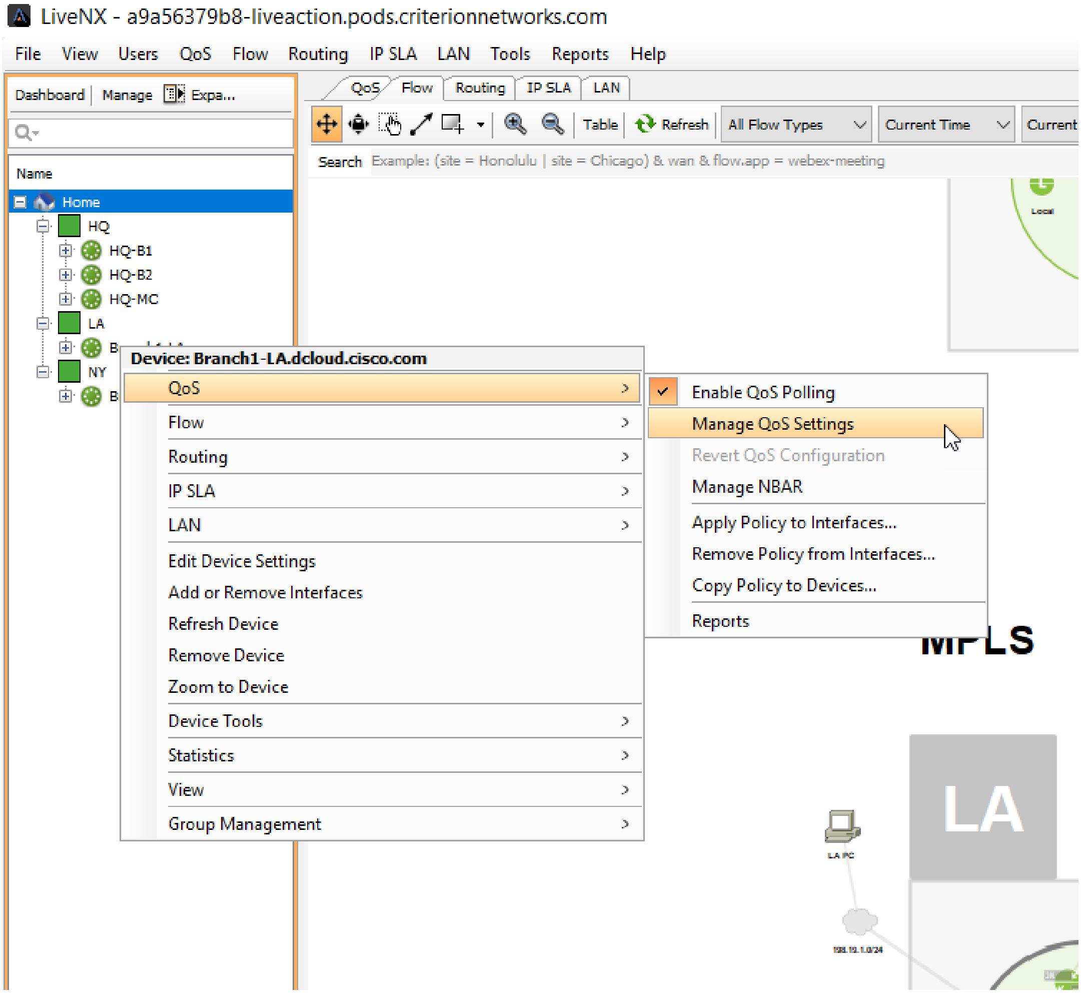
LiveNX can help with creating your Marking policies by using pre-defined templates, or you may easily create new policies within the QoS Module. You can validate how well your marking policies are performing by using NetFlow data to observe what the markings are, for each conversation, on a hop-by-hop basis.

Since you've installed ACLs to use in your INGRESS marking policy, let's create the QoS marking policy using the **LiveNX client**.

Lab Steps:

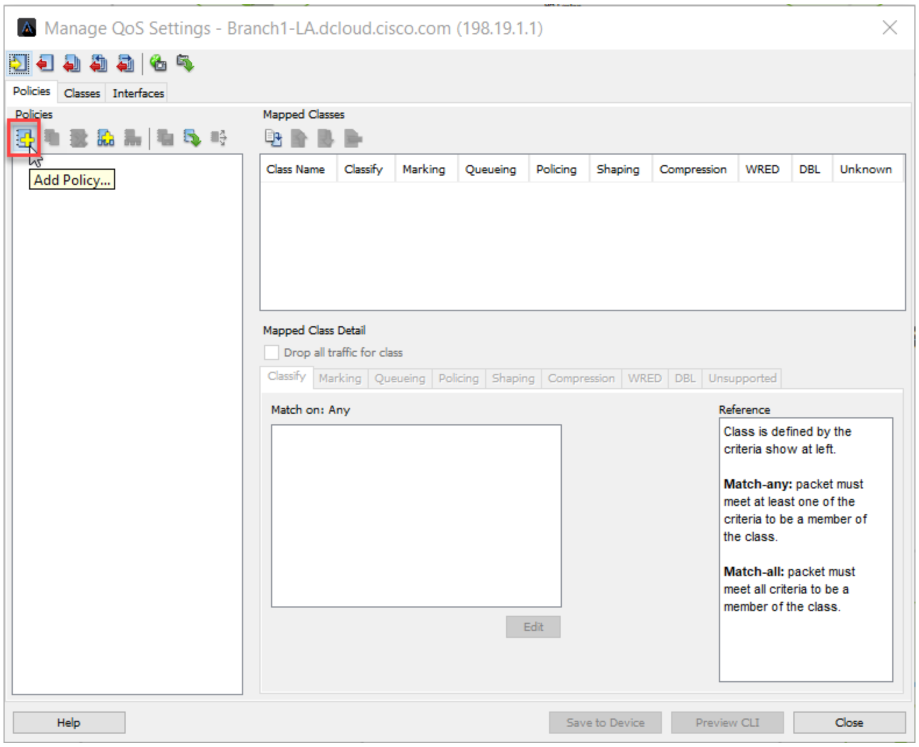
7. From the Home menu location (top-left of screen) right click on the "**Branch1-LA**" device.

8. Highlight QoS and select Manage QoS Settings.



LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard | Manage | Expa...
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
HQ
HQ-B1
HQ-B2
HQ-MC
LA
NY
Device: Branch1-LA.dcloud.cisco.com
QoS
Flow
Routing
IP SLA
LAN
Edit Device Settings
Add or Remove Interfaces
Refresh Device
Remove Device
Zoom to Device
Device Tools
Statistics
View
Group Management
Enable QoS Polling
Manage QoS Settings
Revert QoS Configuration
Manage NBAR
Apply Policy to Interfaces...
Remove Policy from Interfaces...
Copy Policy to Devices...
Reports
MPLS
LA
LA PC
Local

9. Click the **Add Policy** Icon.



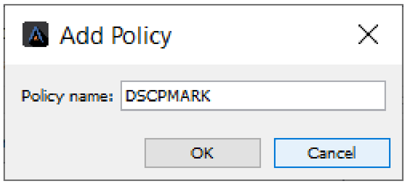
Match on: Any

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.

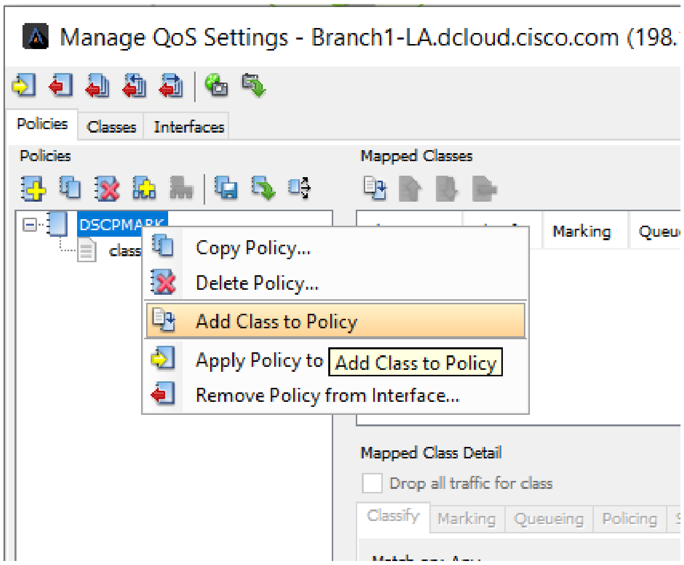
10. Give the new Policy a name, such as “DSCPMARK”



Policy name: DSCPMARK

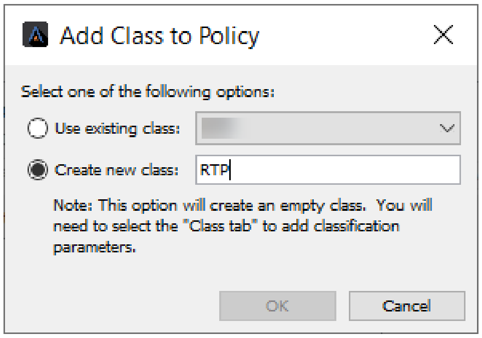
11. We are going to add two classes to this policy: **RTP** and **SIP**

12. Right Click on your new “**DSCPMARK**” policy and select “**Add Class to Policy**”



13. Select “Create a new class” and give the class a name RTP.

14. Click **OK**



Add Class to Policy

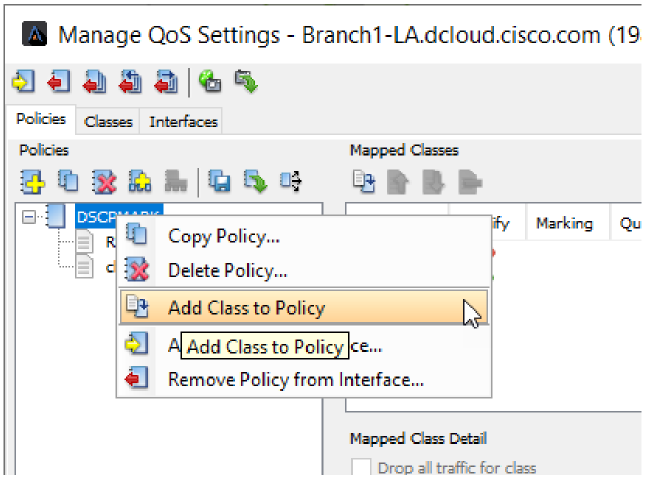
Select one of the following options:

○ Use existing class:

● Create new class: RTP

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

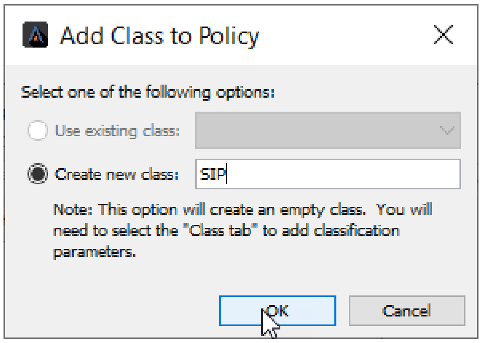
15. Select “Add Class to Policy”



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (19

16. Click Create new class, Label it SIP.

17. Click OK.



Add Class to Policy

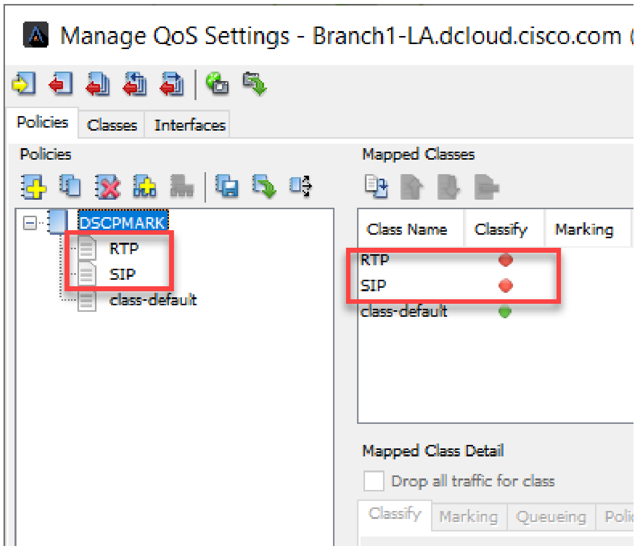
Select one of the following options:

○ Use existing class:

● Create new class: SIP

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

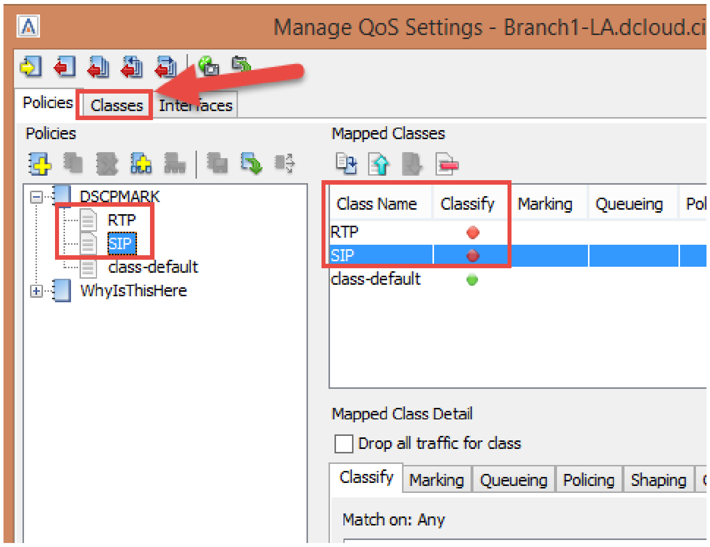
You should now see your two new classes added to the “**DSCPMARK**” policy.



Class Name	Classify	Marking
RTP	●	
SIP	●	
class-default	●	

□ Drop all traffic for class

18. Select the “**Classes**” tab to match them to the created ACL’s.



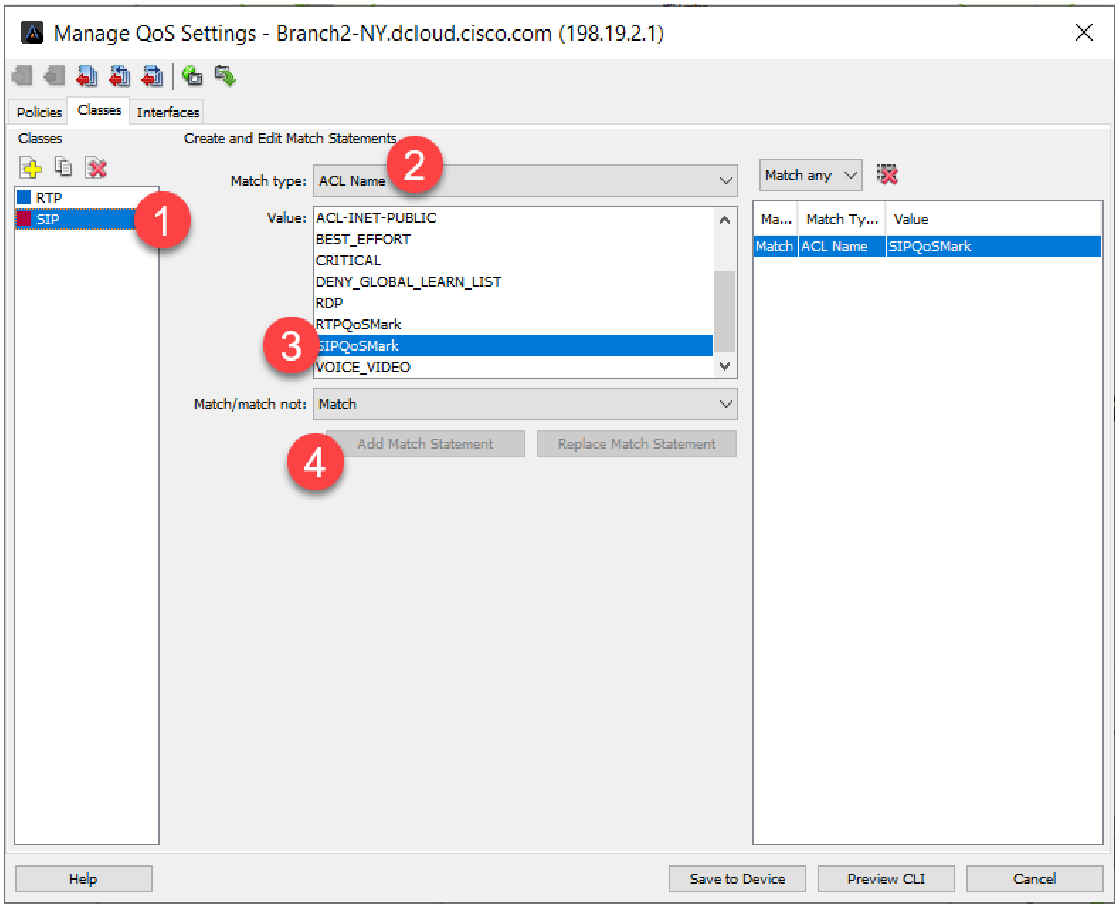
Class Name	Classify	Marking	Queueing	Pol
RTP	●			
SIP	●			
class-default	●			

□ Drop all traffic for class

Match on: Any

Select and match the SIP class…

19. Select the **SIP** Class.
20. For **Match Type** select **ACL Name**.
21. Select the **SIPQoSMark** ACL you created.
22. Select **Add Match Statement**.



Manage QoS Settings - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Match type: ACL Name

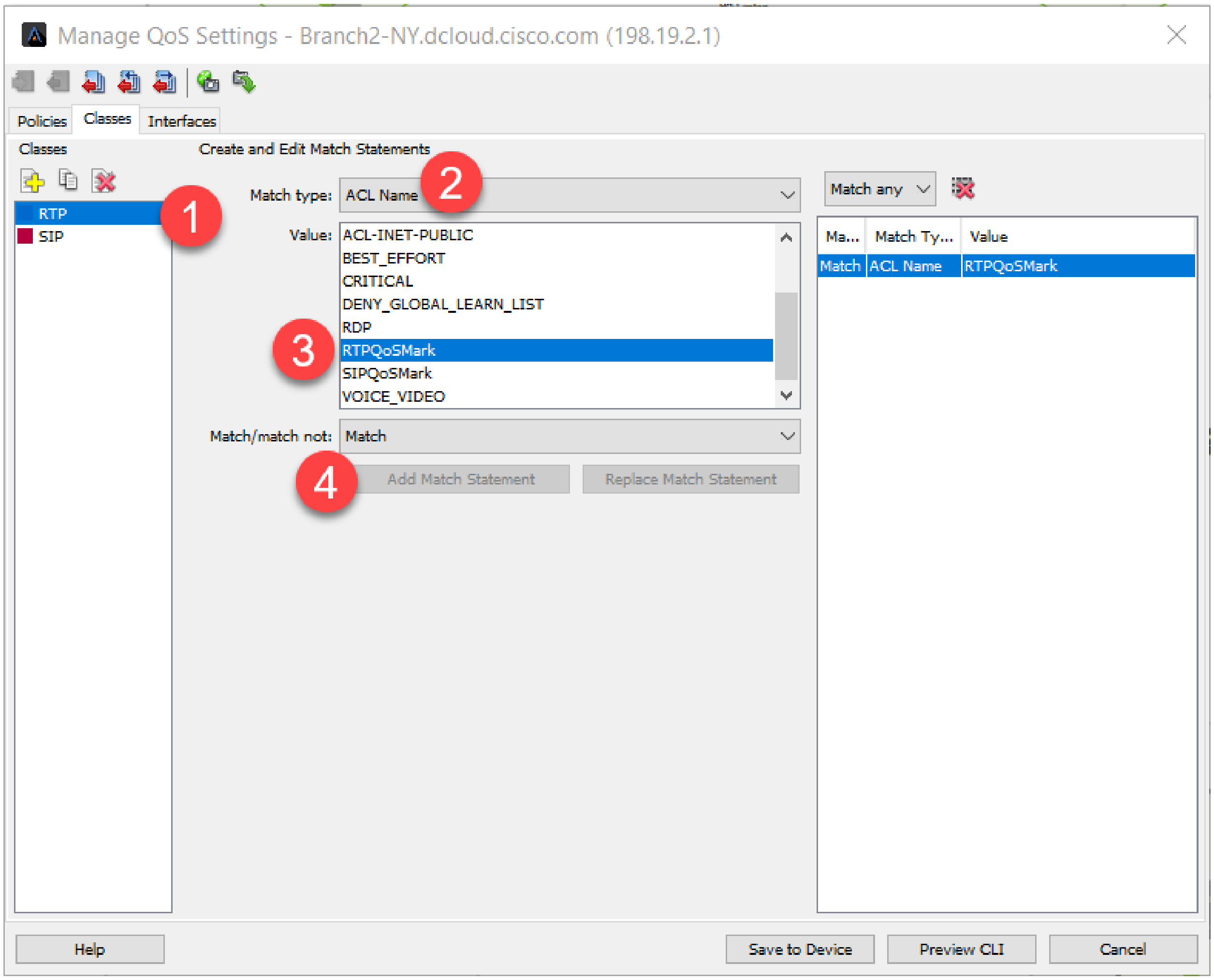
Value: ACL-INET-PUBLIC, BEST_EFFORT, CRITICAL, DENY_GLOBAL_LEARN_LIST, RDP, RTPQoSMark, SIPQoSMark, VOICE_VIDEO

Match/match not: Match

Ma...	Match Ty...	Value
Match	ACL Name	SIPQoSMark

Next select the RTP Class and do the same…

23. Select the **RTP** Class.
24. For **Match Type** select **ACL Name**.
25. Select the **RTPQoSMark** ACL you created.
26. Select **Add Match Statement**.



Classes

- RTP
- SIP

Match type: ACL Name

Value:

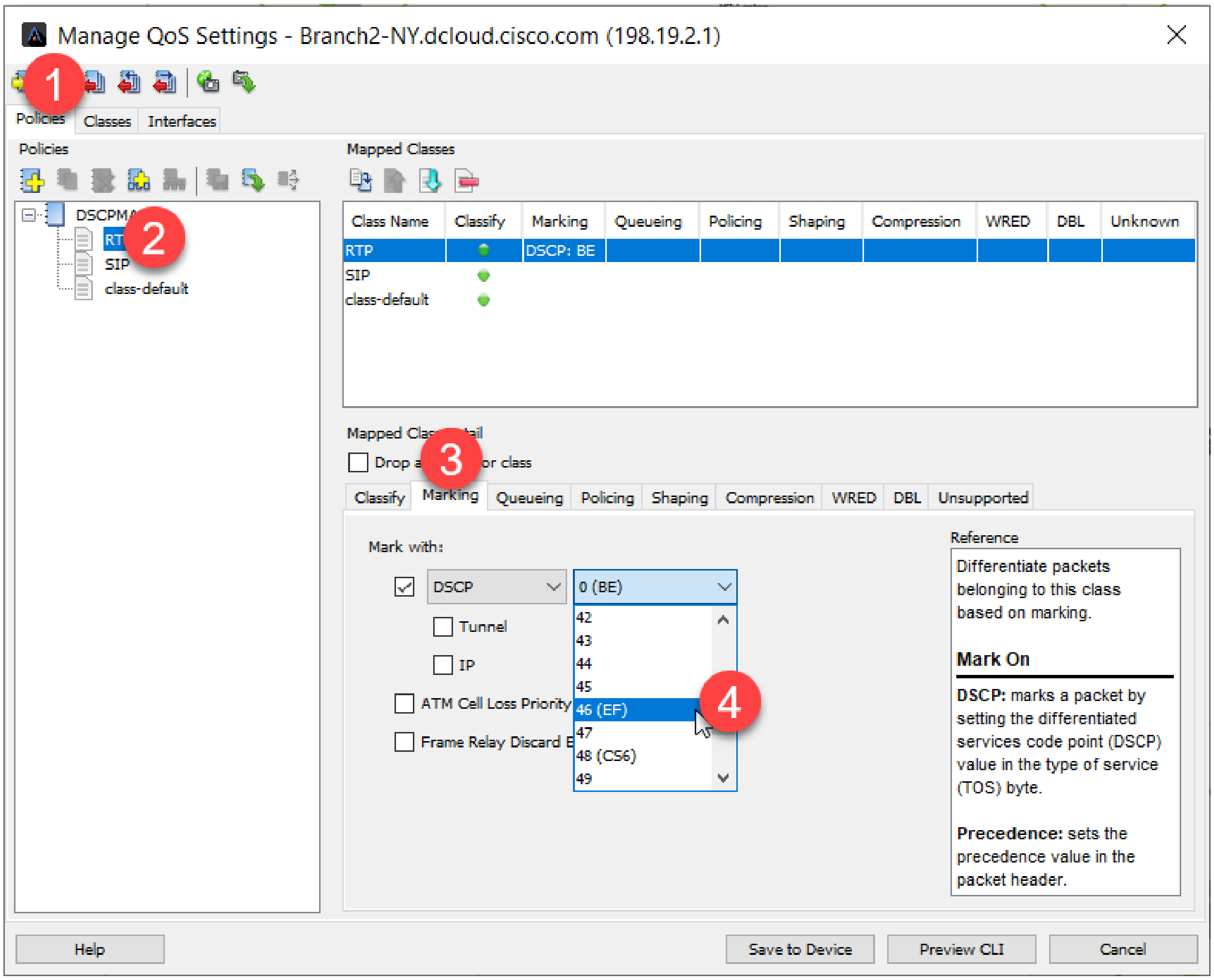
- ACL-INET-PUBLIC
- BEST_EFFORT
- CRITICAL
- DENY_GLOBAL_LEARN_LIST
- RDP
- RTPQoSMark
- SIPQoSMark
- VOICE_VIDEO

Match/match not: Match

Match any

Ma...	Match Ty...	Value
Match	ACL Name	RTPQoSMark

27. Select the **Policies** Tab.
28. Select the **RTP** Class.
29. Select the **Marking** Tab
30. Choose to mark the RTP Traffic with DSCP **46 (EF)**.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
RTP	●	DSCP: BE							
SIP	●								
class-default	●								

☑ DSCP — 0 (BE)

Differentiate packets belonging to this class based on marking.

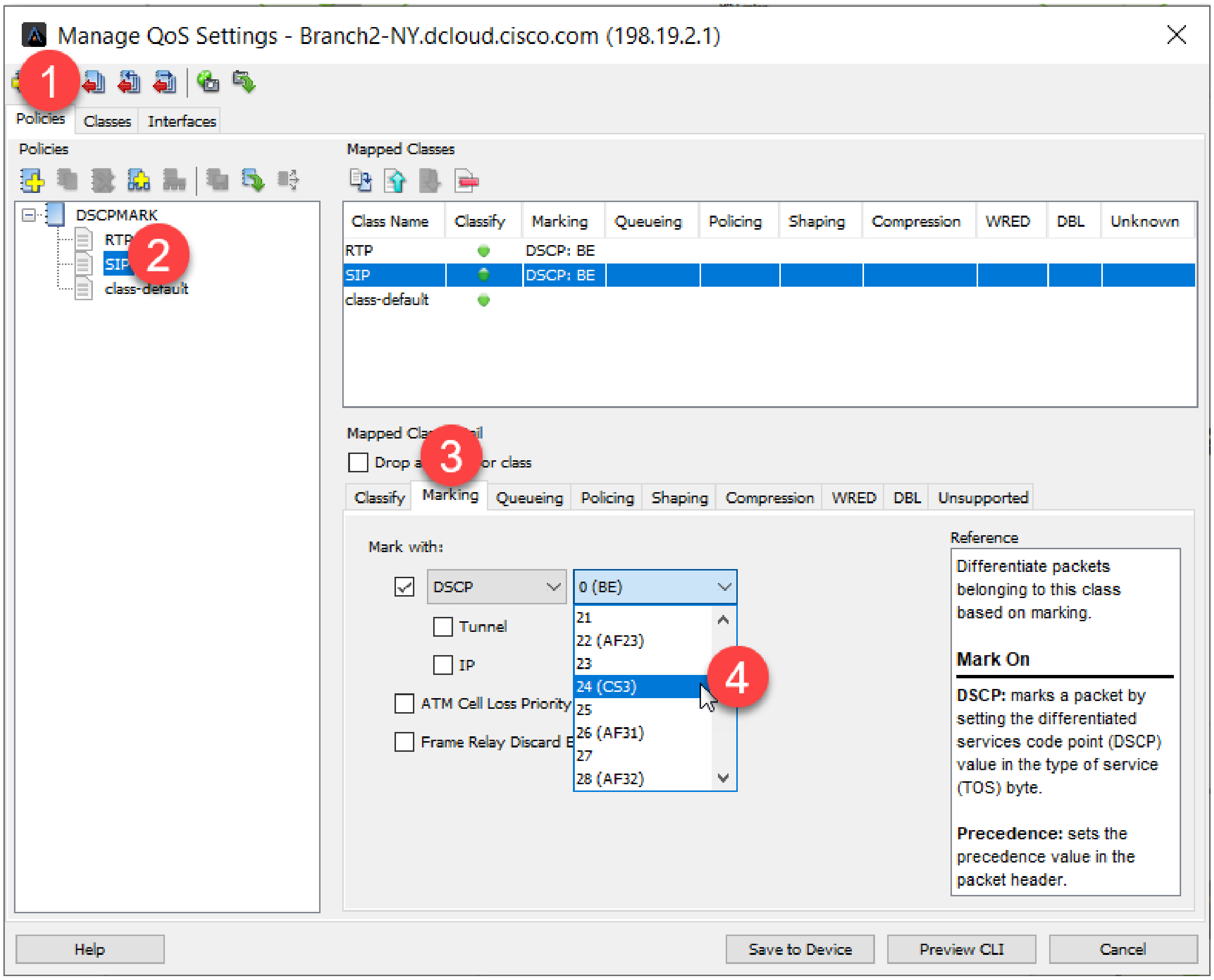
Mark On

DSCP: marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte.

Precedence: sets the precedence value in the packet header.

Next it is necessary to set the DSCP Markings for the SIP Class.

31. Select **SIP**
32. Select the **Marking** tab.
33. Mark with **DSCP** as below.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
RTP	●	DSCP: BE							
SIP	●	DSCP: BE							
class-default	●								

Mapped Class Detail

□ Drop all traffic for class

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

Mark with:

☑ DSCP 0 (BE)

□ Tunnel

□ IP

□ ATM Cell Loss Priority

□ Frame Relay Discard Eligibility

21
22 (AF23)
23
24 (CS3)
25
26 (AF31)
27
28 (AF32)

Reference

Differentiate packets belonging to this class based on marking.

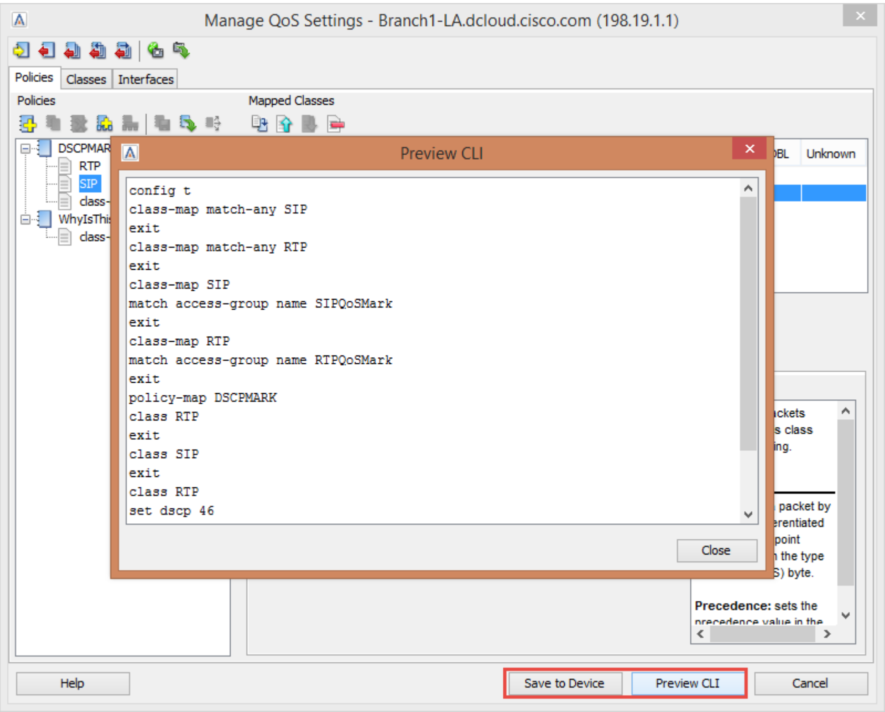
Mark On

DSCP: marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte.

Precedence: sets the precedence value in the packet header.

34. Click **Preview CLI** to see the policy you have created.

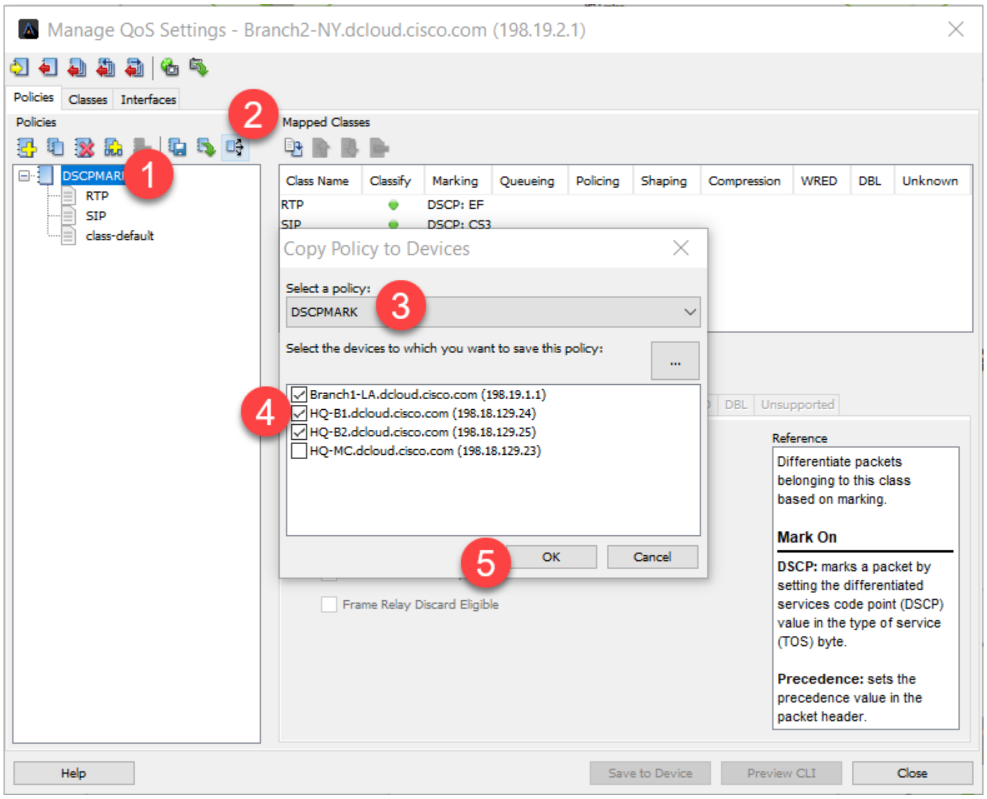
35. Click **Save to Device** if satisfied.



```
config t
class-map match-any SIP
exit
class-map match-any RTP
exit
class-map SIP
match access-group name SIPQoSMark
exit
class-map RTP
match access-group name RTPQoSMark
exit
policy-map DSCPMARK
class RTP
exit
class SIP
exit
class RTP
set dscp 46
```

We can now push our newly created polies to *multiple* devices.

36. Select the "**DSCPMARK**" policy.
37. Click the "**three arrow**" icon to copy policy to devices.
38. Select the **DSCPMARK** Policy.
39. Select the other relevant devices in the topology.
40. Click **OK**



Manage QoS Settings - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Mapped Classes

Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
RTP	●	DSCP: EF							
SIP	●	DSCP: CS3							

Copy Policy to Devices

Select a policy: DSCPMARK

Select the devices to which you want to save this policy:

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ HQ-B1.dcloud.cisco.com (198.18.129.24)
☑ HQ-B2.dcloud.cisco.com (198.18.129.25)
☐ HQ-MC.dcloud.cisco.com (198.18.129.23)

Reference

Differentiate packets belonging to this class based on marking.

Mark On

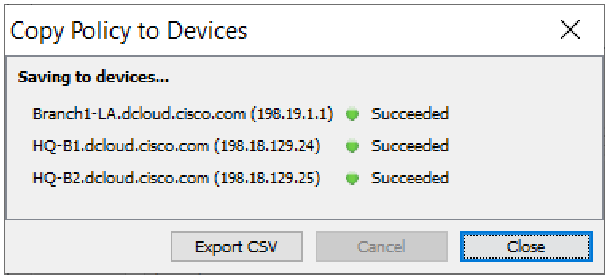
DSCP: marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte.

Precedence: sets the precedence value in the packet header.

☐ Frame Relay Discard Eligible

You should see that both policies copied to the device successfully.

41. Close the **Copy Policy** window, and the **Manage QoS** Window to return to the Topology pane.



Copy Policy to Devices

Saving to devices...

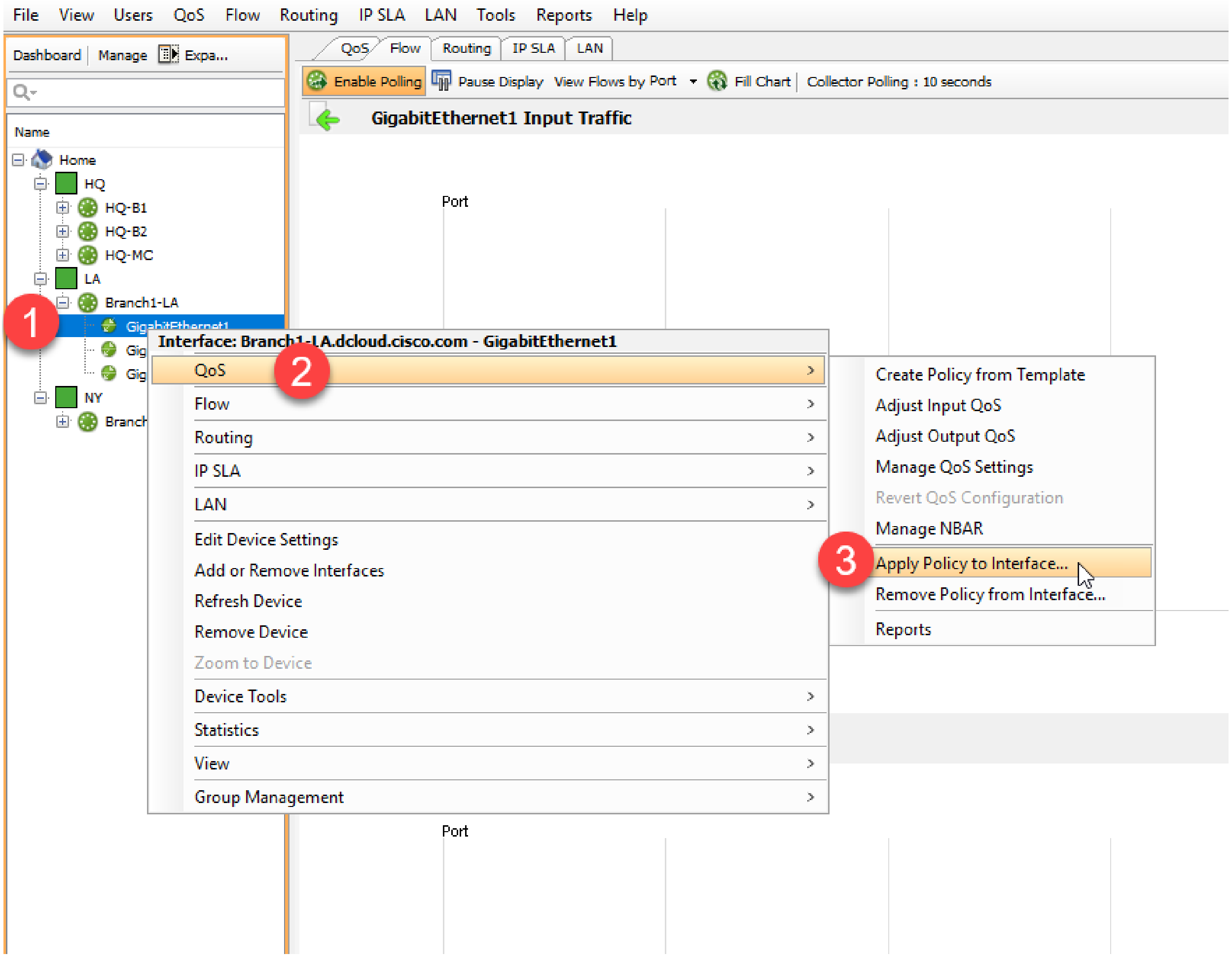
Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded
HQ-B1.dcloud.cisco.com (198.18.129.24) ● Succeeded
HQ-B2.dcloud.cisco.com (198.18.129.25) ● Succeeded

Note: You want to apply marking policies as close as possible to where traffic enters the network.

In this scenario we will be applying the marking policies on the *ingress* of the **LAN interfaces** for each device. Perform the following steps on EACH DEVICE.

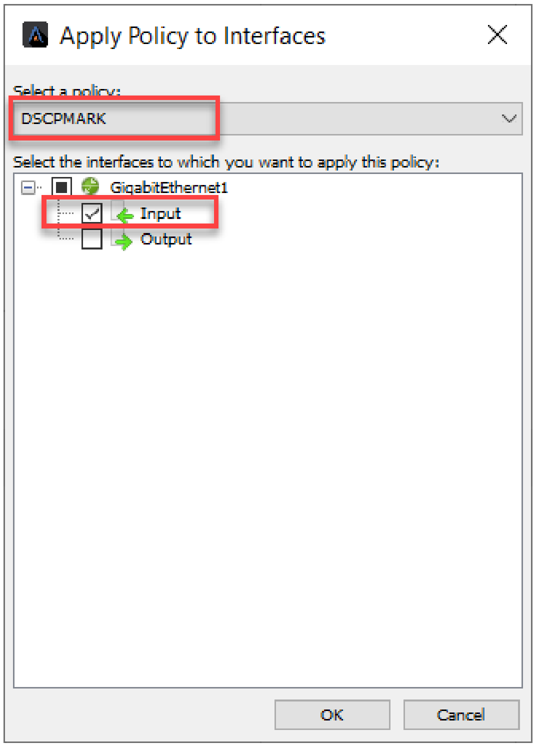
42. In the main device menu on the top-left, right-Click on the appropriate interface.

43. Select **QoS**, and then **Apply Policy to Interface**.



44. Select the “**DSCPMARK**” policy.

45. Click the **Input** of the **LAN Interface**



Apply Policy to Interfaces

Select a policy:

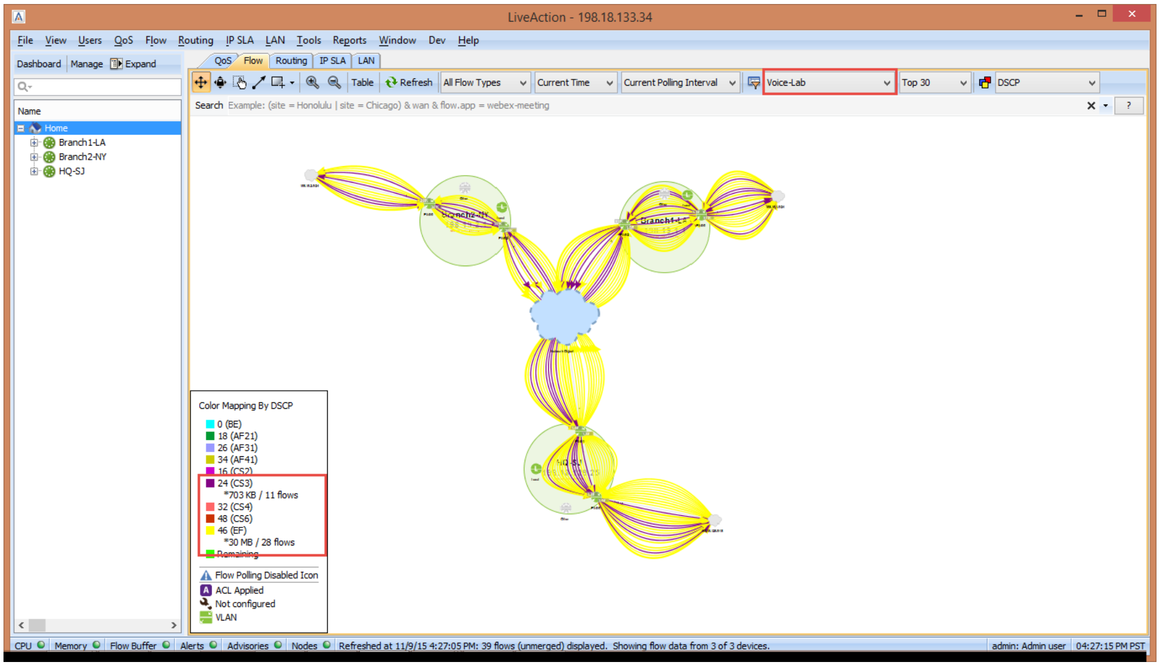
DSCPMARK

Select the interfaces to which you want to apply this policy:

- ■ GigabitEthernet1
  - ☑ Input
  - □ Output

Do this for each **LAN interface**! (Loop to #1 above for each device)

Using your Voice Filter, and then refreshing the Topology, you should no longer see any BE Traffic – Remember, it may take a bit of time for Netflow to catch up.


LiveAction - 198.18.133.34
File View Users QoS Flow Routing IP SLA LAN Tools Reports Window Dev Help
Dashboard Manage Expand
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
Branch1-LA
Branch2-NY
HQ-SJ
CPU Memory Flow Buffer Alerts Advisories Nodes
admin: Admin user 04:27:15 PM PST

Voice-Lab | Top 30 | DSCP

Color Mapping By DSCP

- 🟦 0 (BE)
- 🟩 18 (AF21)
- 🟦 26 (AF31)
- 🟨 34 (AF41)
- 🟪 16 (CS2)
- 🟪 24 (CS3)
  - *703 KB / 11 flows
- 🟥 32 (CS4)
- 🟥 48 (CS6)
- 🟨 46 (EF)
  - *30 MB / 28 flows
- 🟩 Remaining

Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN

Refreshed at 11/9/15 4:27:05 PM: 39 flows (unmerged) displayed. Showing flow data from 3 of 3 devices.

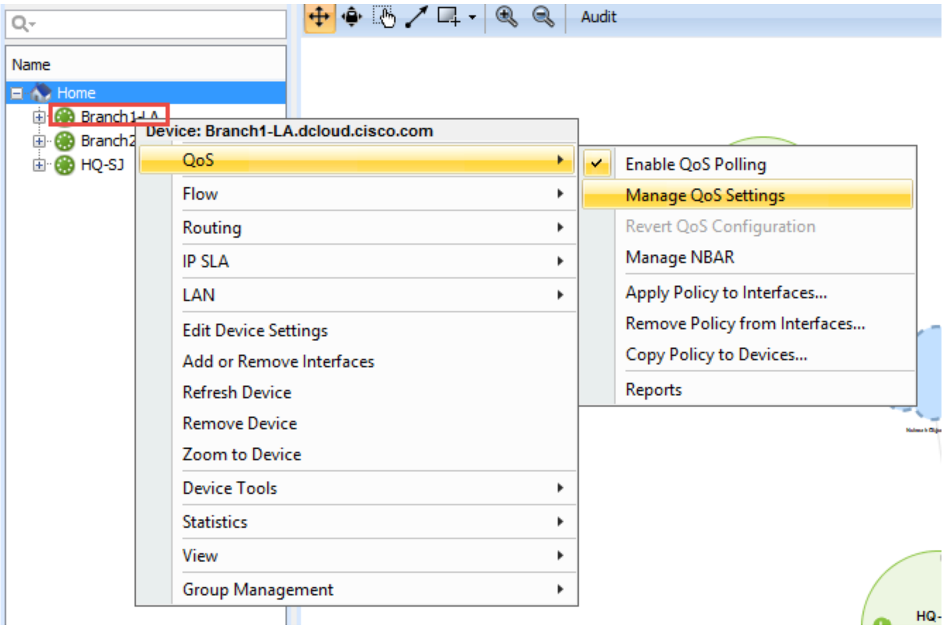
Lab 8.2: QoS Queueing Policy

As in the prior Lab, LiveNX also makes it easy to manage your Queueing policies by either using our pre-defined templates or create them in the LiveNX interface. You can validate how your queueing policies are performing by utilizing our QoS Tab and the CBQoS MIB.

Now that you've verified your traffic is marked correctly through the network, using Netflow, you can create a queuing policy to protect the critical traffic.

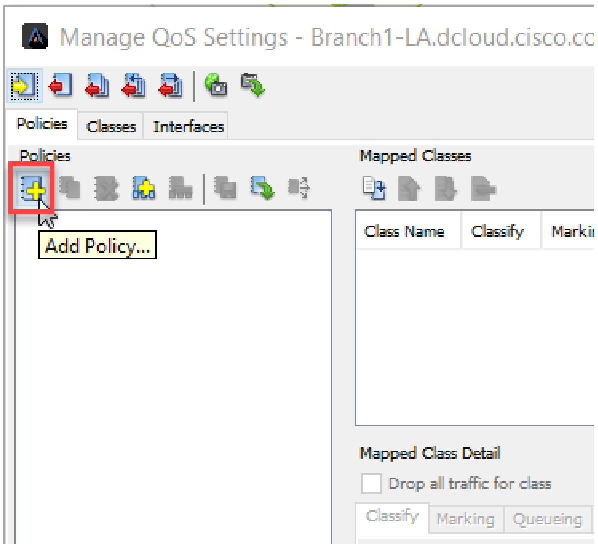
Lab Steps:

46. Right-click on the Branch1-LA Device, select QoS, and Manage QoS Settings.

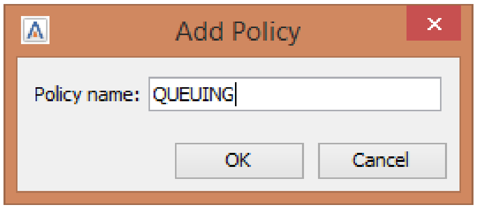


47. Select the **Policies** Tab.

48. Click **Add Policy** to create a queuing policy.

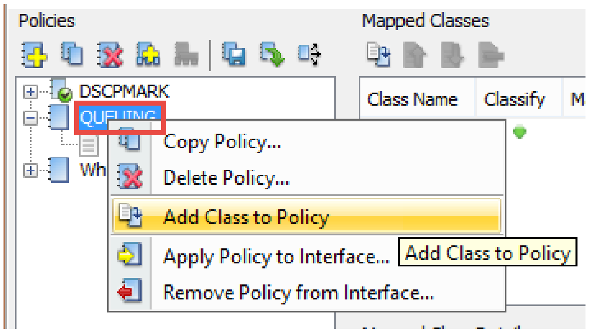


49. Name the new policy QUEUEING.



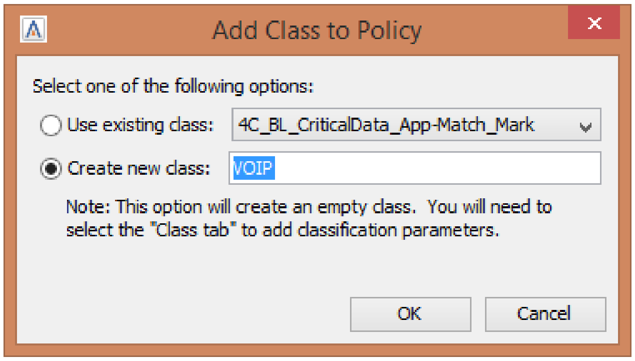
Policy name: QUEUING

50. Right-click on the new QUEUEING Policy, select Add Class to Policy.



51. Create a new class labeled VOIP.

52. Click OK.



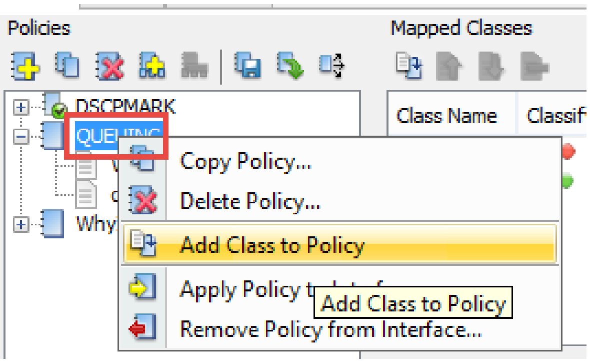
Select one of the following options:

○ Use existing class: 4C_BL_CriticalData_App-Match_Mark

● Create new class: VOIP

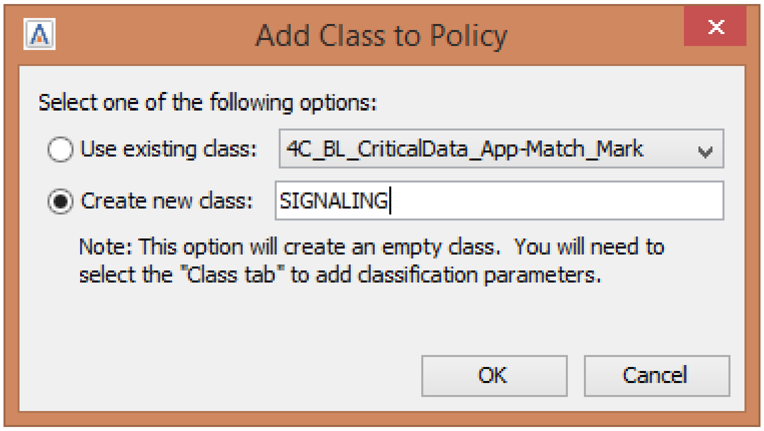
Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

53. Right-click, again, on the QUEUEING Policy, select Add Class to Policy.



54. Create a new class and label it SIGNALING.

55. Click OK



Add Class to Policy

Select one of the following options:

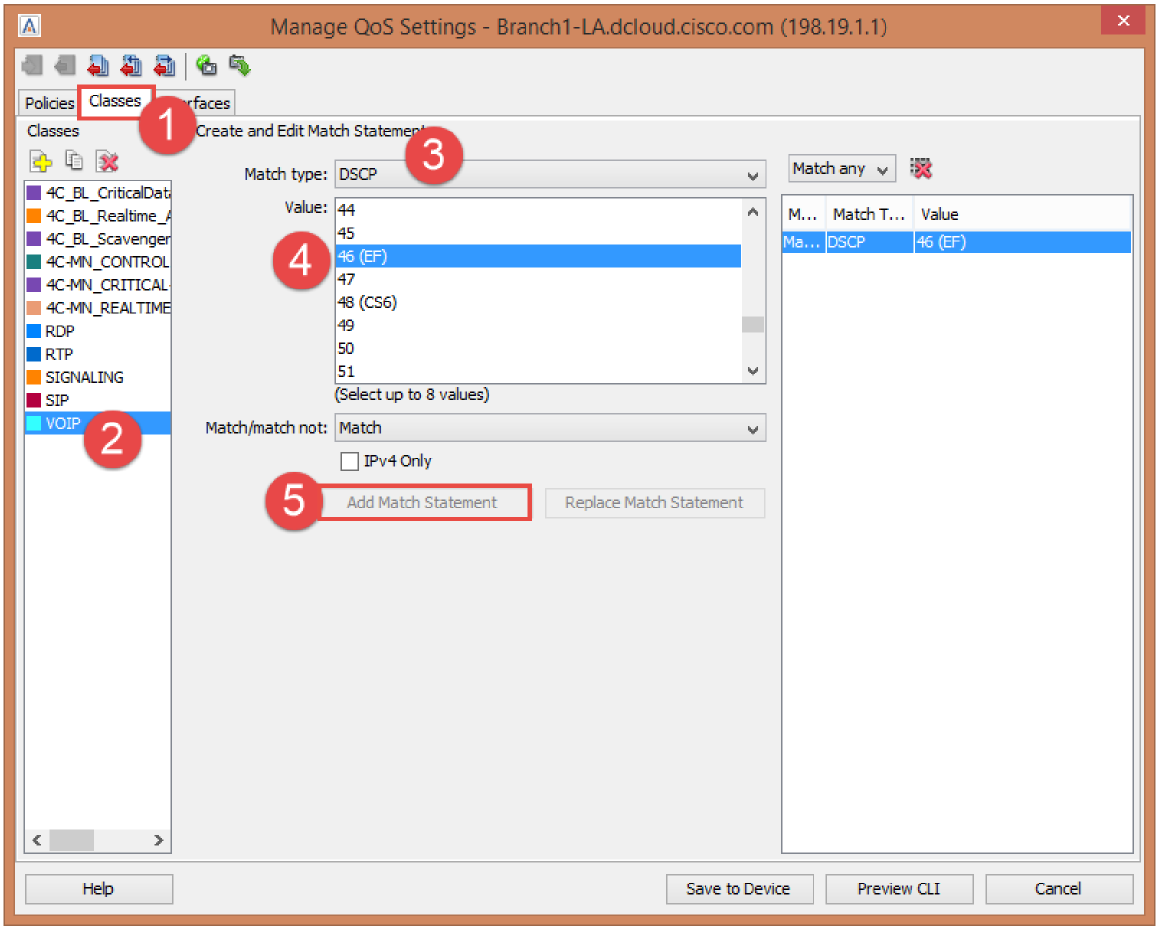
○ Use existing class: 4C_BL_CriticalData_App-Match_Mark

● Create new class: SIGNALING

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

Configure VOIP Class:

1. Click the Classes Tab.
2. Select the VOIP Class.
3. Select the Match Type as DSCP.
4. Select 46 (EF).
5. Click Add Match Statement



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Classes

- 4C_BL_CriticalDat
- 4C_BL_Realtime_A
- 4C_BL_Scavenger
- 4C-MN_CONTROL
- 4C-MN_CRITICAL
- 4C-MN_REALTIME
- RDP
- RTP
- SIGNALING
- SIP
- VOIP

Create and Edit Match Statement

Match type: DSCP

Value: 44, 45, 46 (EF), 47, 48 (CS6), 49, 50, 51

(Select up to 8 values)

Match/match not: Match

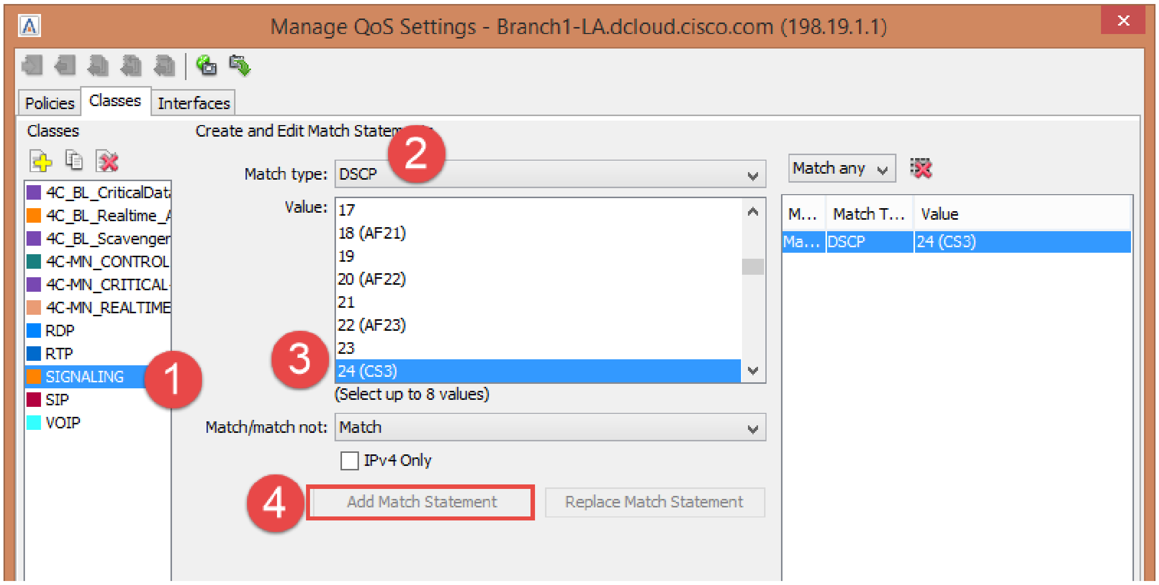
□ IPv4 Only

Match any

M...	Match T...	Value
Ma...	DSCP	46 (EF)

Configure SIGNALING Class:

56. Select SIGNALING.
57. Use DSCP as Match Type.
58. Select 24 (CS3).
59. Click Add Match Statement.



Match type: DSCP

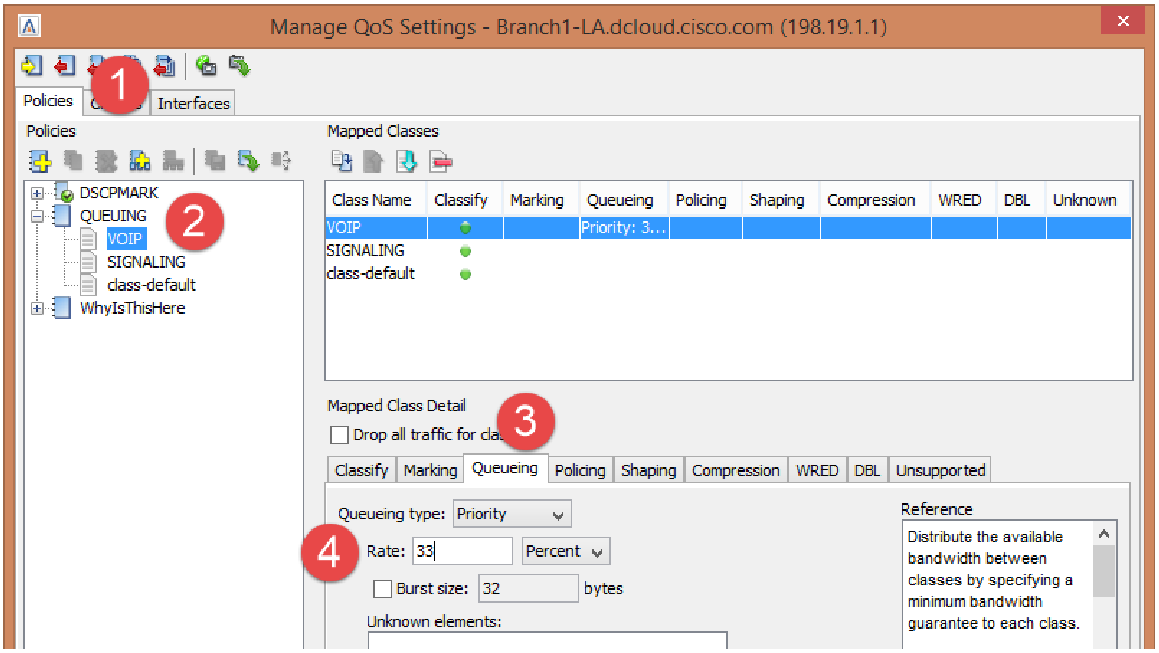
Value: 24 (CS3)

Match/match not: Match

M...	Match T...	Value
Ma...	DSCP	24 (CS3)

Setup VoIP Priorities:

60. Select the Policies Tab.
61. Select the VOIP Class.
62. Select the Queuing Tab.
63. Select Priority Queuing, enter a rate of 33%.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●								
class-default	●								

Queueing type: Priority

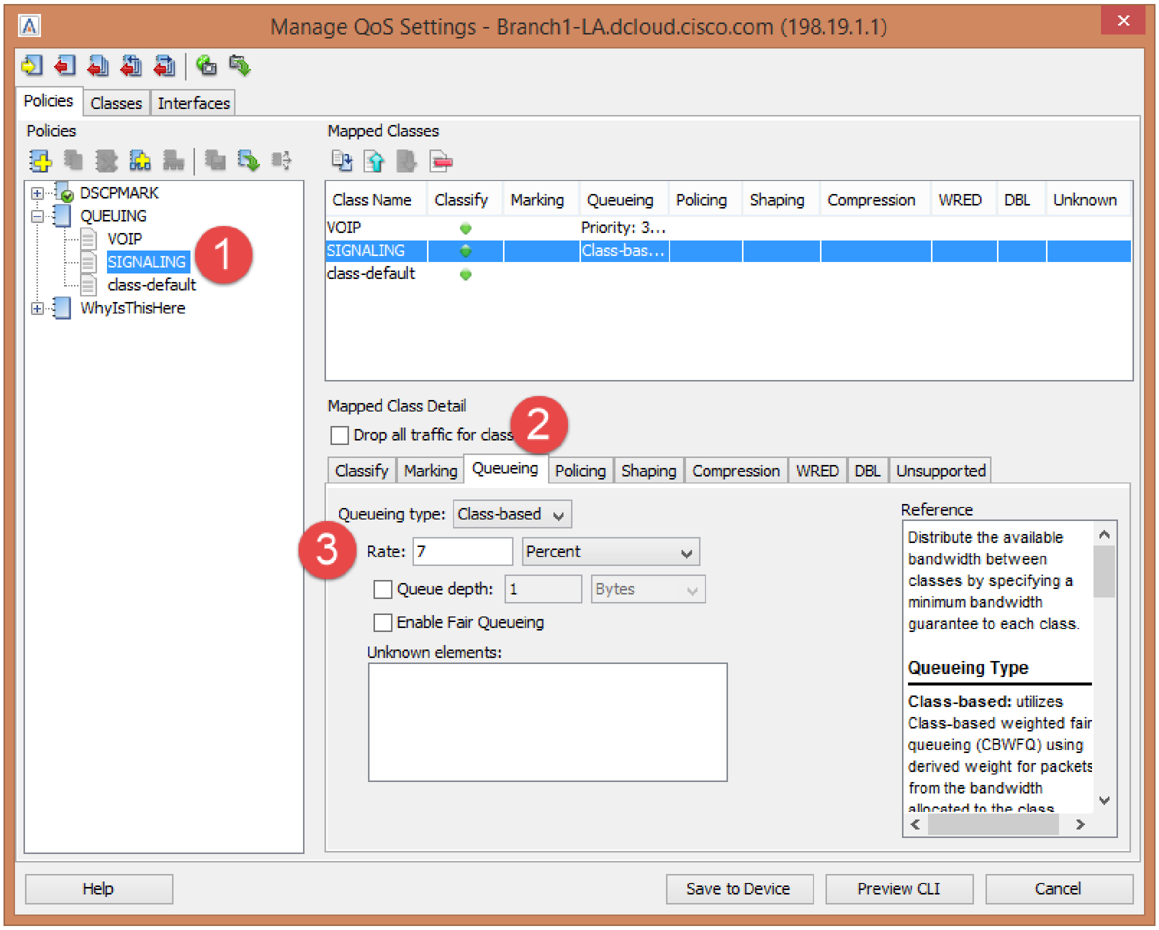
Rate: 33 Percent

□ Burst size: 32 bytes

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

Setup Signaling Priorities:

64. Select the Signaling Class.
65. Select The Queueing Tab.
66. Select Class-Based with a rate of 7%.



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Mapped Classes

Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●		Class-bas...						
class-default	●								

Mapped Class Detail

□ Drop all traffic for class

Queueing type: Class-based

Rate: 7 Percent

□ Queue depth: 1 Bytes

□ Enable Fair Queueing

Unknown elements:

Reference

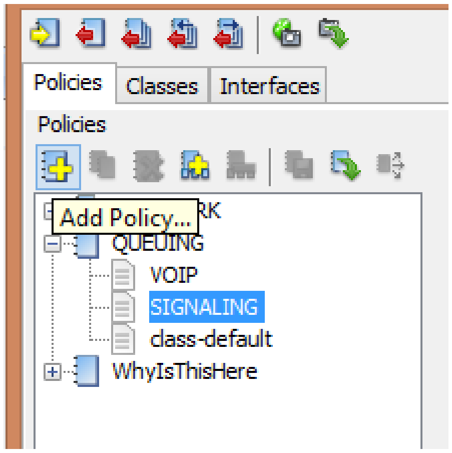
Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

Queueing Type

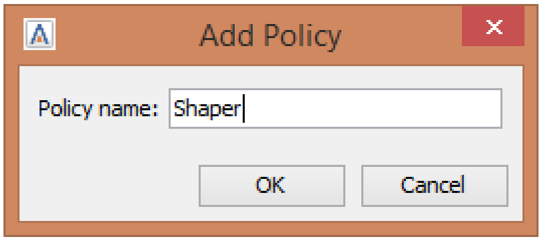
Class-based: utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class

Create a Shaping Policy:

67. Click Add Policy.



68. Give the Policy a name of Shaper.

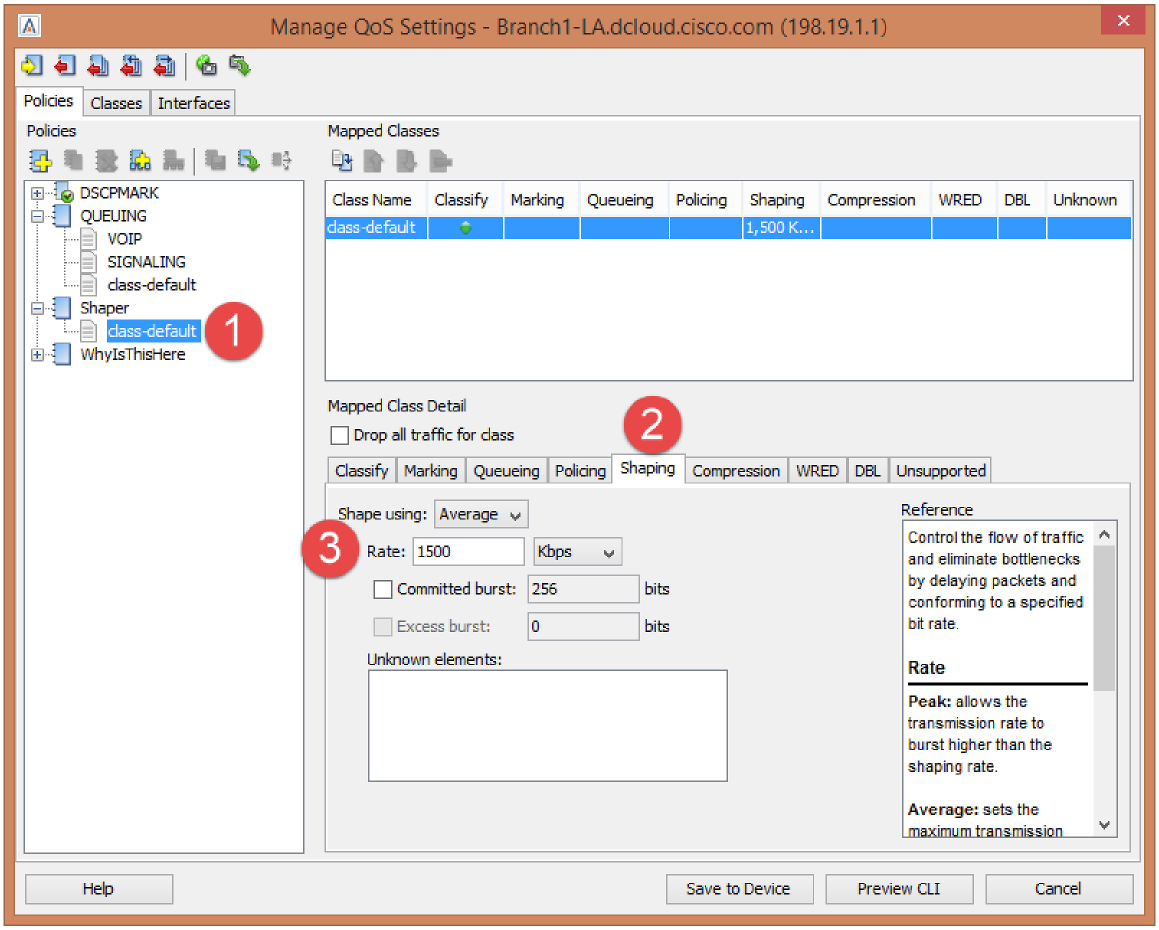


Policy name: Shaper

69. Select the **class-default** class under Shaper.

70. Select the Shaping tab.

71. Select Average, enter 1500 Kbps.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
class-default	●				1,500 K...				

□ Drop all traffic for class

Shape using: Average

Rate: 1500 Kbps

□ Committed burst: 256 bits

□ Excess burst: 0 bits

Unknown elements:

Reference

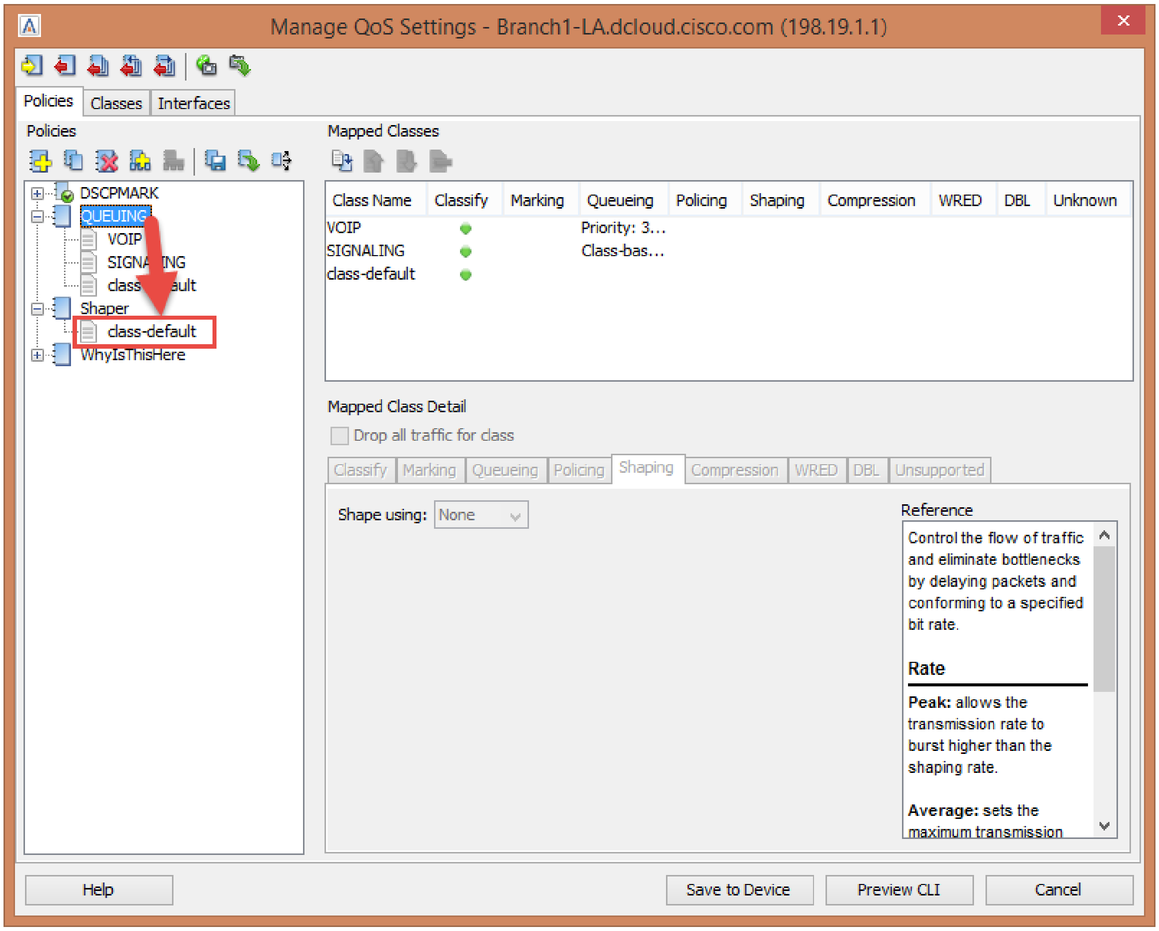
Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

Rate

Peak: allows the transmission rate to burst higher than the shaping rate.

Average: sets the maximum transmission

72. Click and Drag the QUEUEING Policy on top of **class-default** class for the **Shaper.**



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●		Class-bas...						
class-default	●								

□ Drop all traffic for class

Shape using: None

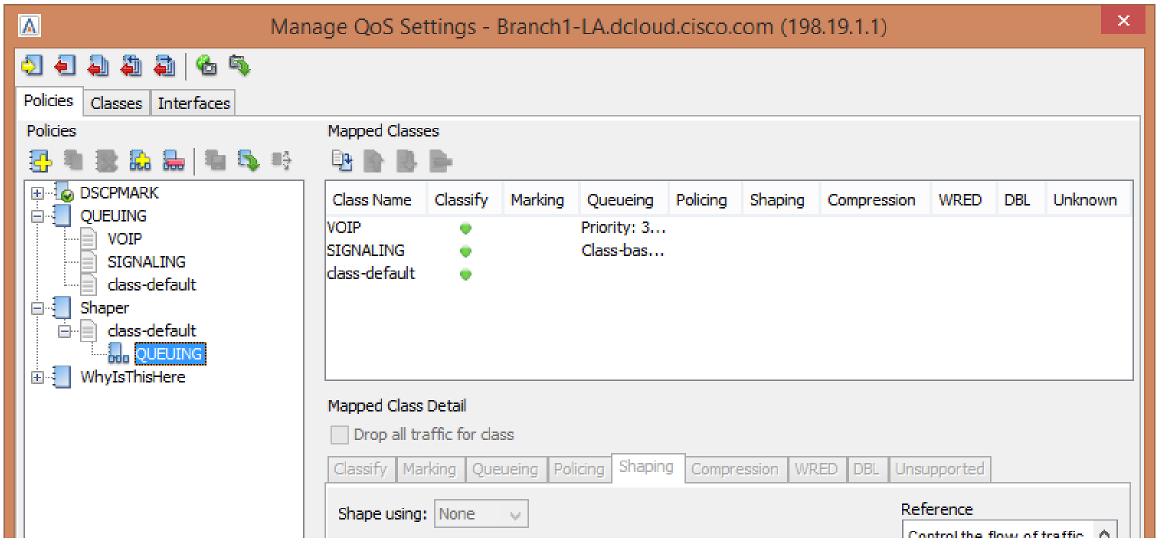
Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

Rate

Peak: allows the transmission rate to burst higher than the shaping rate.

Average: sets the maximum transmission

Now you should see the QUEUEING Policy as part of the shaper. This allows you to reserve the percentage of BW in the shaping policy!



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●		Class-bas...						
class-default	●								

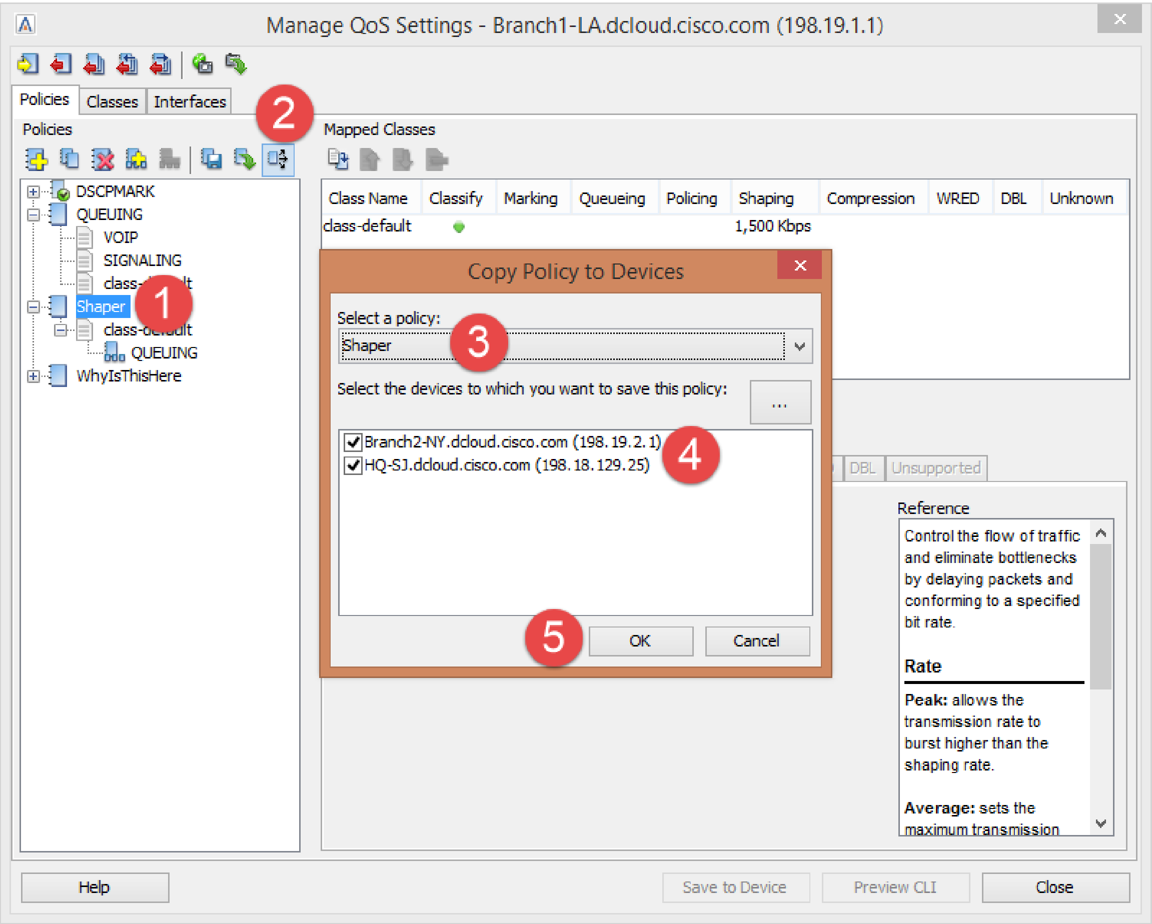
□ Drop all traffic for class

Shape using: None

Control the flow of traffic

Copy the shaping policy to the other devices:

73. Select the Shaper Policy.
74. Click the three-arrow icon to copy the policy.
75. Ensure the Shaper Policy is selected.
76. Select the other two devices.
77. Click OK to push the policy.



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Mapped Classes

Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
class-default	●				1,500 Kbps				

Copy Policy to Devices

Select a policy: Shaper

Select the devices to which you want to save this policy:

☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)
☑ HQ-SJ.dcloud.cisco.com (198.18.129.25)

Reference

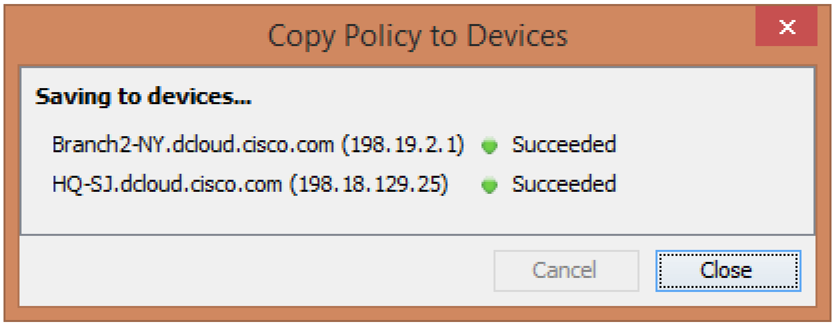
Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

Rate

Peak: allows the transmission rate to burst higher than the shaping rate.

Average: sets the maximum transmission

78. Click Close.
79. Click OK.



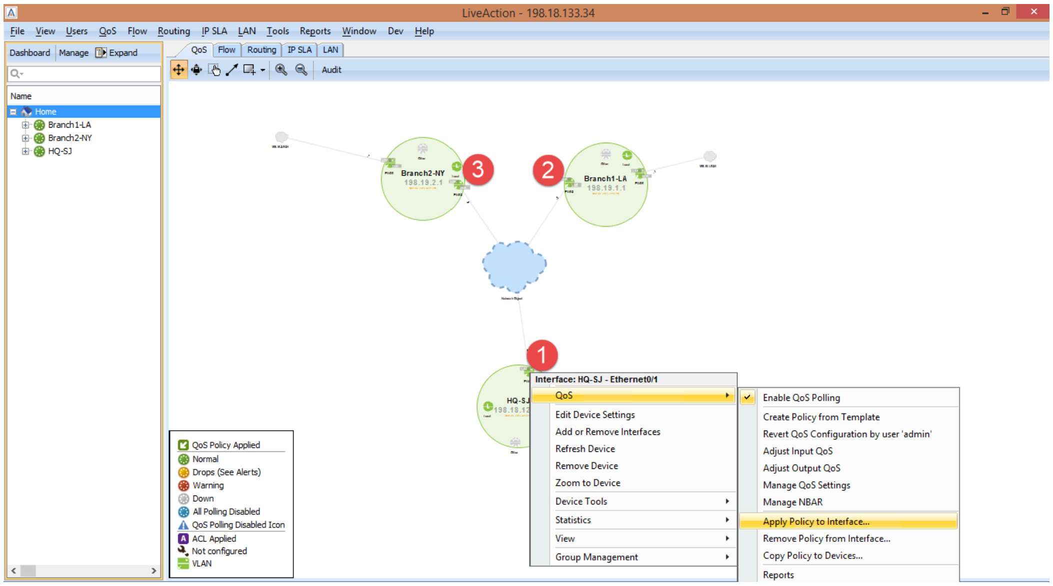
Copy Policy to Devices

Saving to devices...

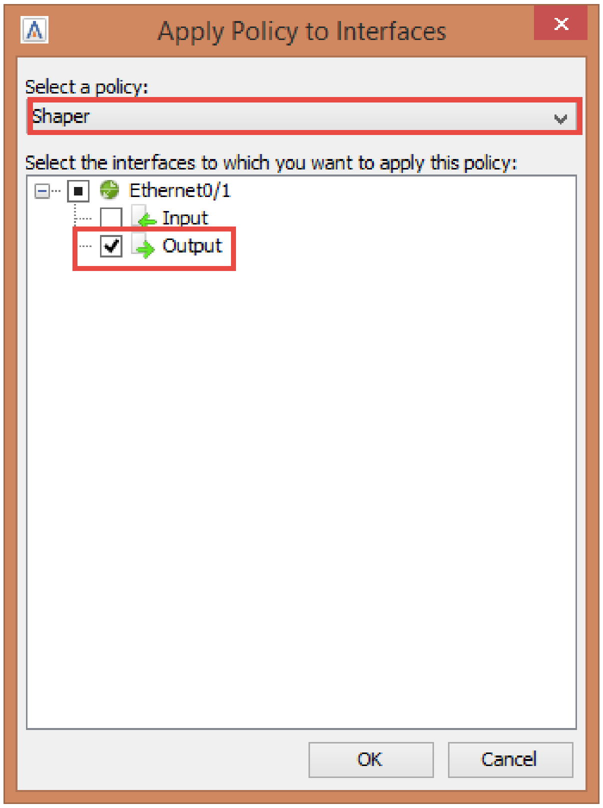
Branch2-NY.dcloud.cisco.com (198.19.2.1) ● Succeeded
HQ-SJ.dcloud.cisco.com (198.18.129.25) ● Succeeded

We still need to apply the policy to the WAN interfaces. Do the following steps on EACH of the 3 devices.

80. Right-click on the WAN interface and select QoS and Apply Policy to Interface.



81. Select the Shaper Policy and the Output for the WAN interface.


Apply Policy to Interfaces

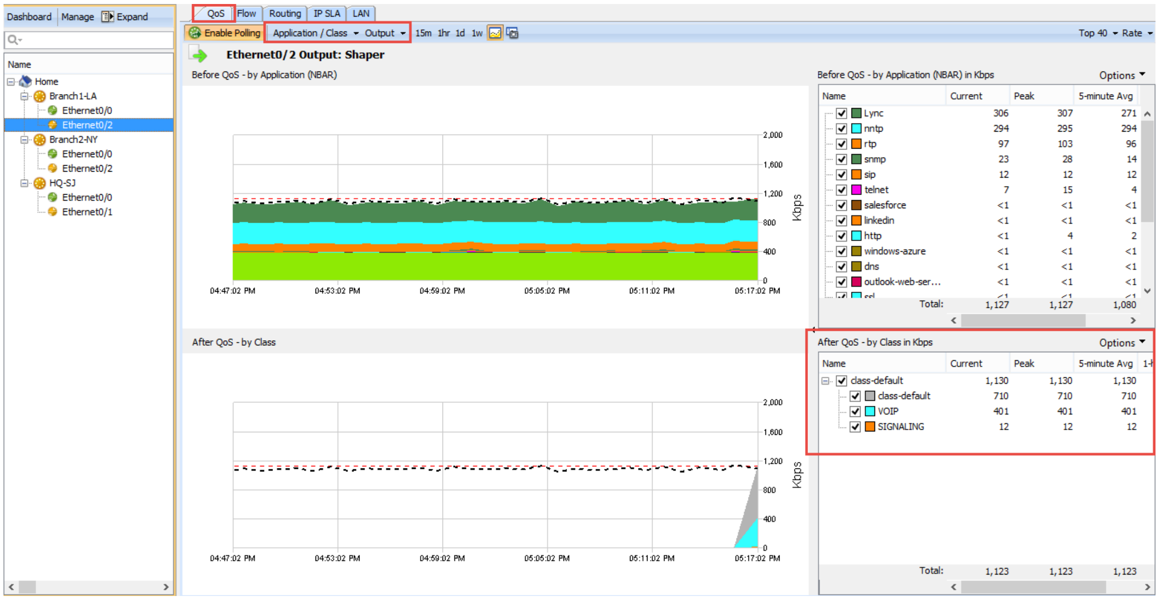
Select a policy:
Shaper

Select the interfaces to which you want to apply this policy:

- ■ Ethernet0/1
  - □ Input
  - ☑ Output

82. Click **OK**.

Once Completed you can go to the QoS Tab, select a devices WAN Interface, Select Application/Class and view the Output of the policy.



Before QoS - by Application (NBAR) in Kbps

Name	Current	Peak	5-minute Avg
☑ 🟩 Lync	306	307	271
☑ 🟦 nntp	294	295	294
☑ 🟧 rtp	97	103	96
☑ 🟩 snmp	23	28	14
☑ 🟧 sip	12	12	12
☑ 🟪 telnet	7	15	4
☑ 🟫 salesforce	<1	<1	<1
☑ 🟧 linkedin	<1	<1	<1
☑ 🟦 http	<1	4	2
☑ 🟫 windows-azure	<1	<1	<1
☑ 🟫 dns	<1	<1	<1
☑ 🟥 outlook-web-ser…	<1	<1	<1
☑ 🟦 ssl	<1	<1	<1
Total:	1,127	1,127	1,080

After QoS - by Class in Kbps

Name	Current	Peak	5-minute Avg	1-I
☑ class-default	1,130	1,130	1,130	
☑ ⬜ class-default	710	710	710	
☑ 🟦 VOIP	401	401	401	
☑ 🟧 SIGNALING	12	12	12	
Total:	1,123	1,123	1,123	

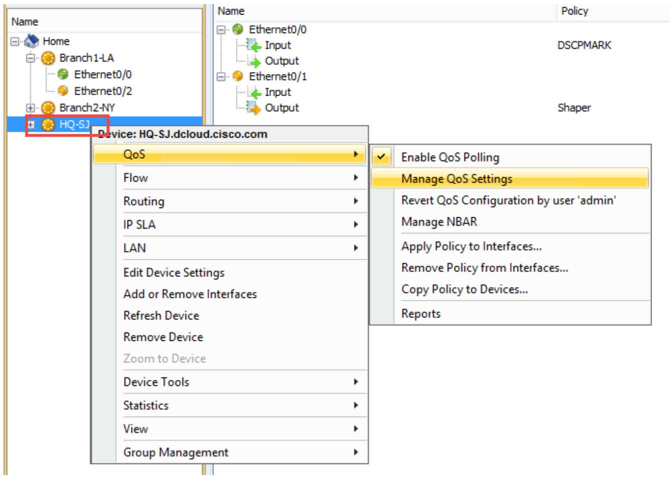
Do you notice any drops on your VOIP class or your Class-Default? Let’s add some more protection to those classes with increasing the burst size for VOIP and adding a scavenger class for bit torrent traffic.

Lab 8.3: QoS Verification

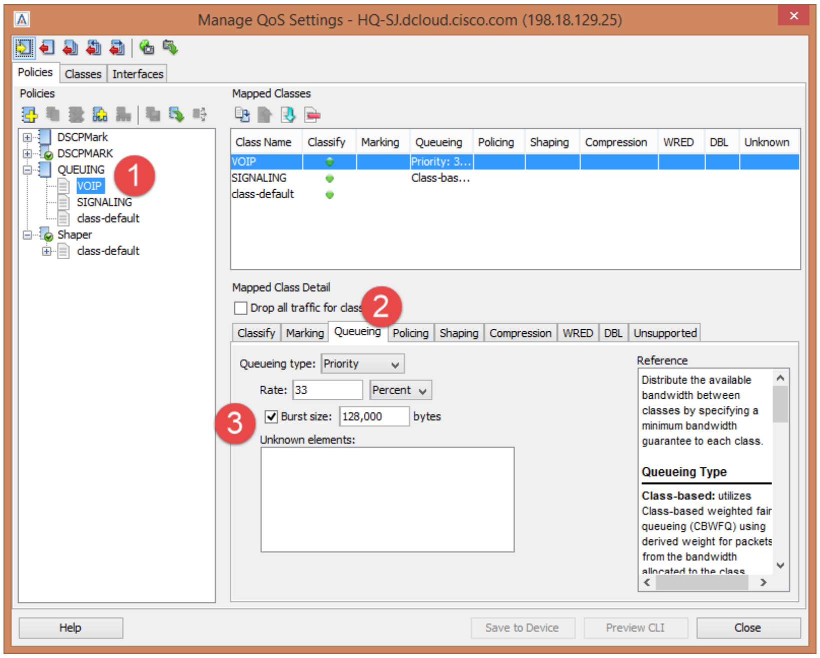
Managing QoS is an ongoing process where you may need to adjust your policies according to your network needs. You can use LiveAction elements such as NetFlow analysis or CBQoS Statistics to determine if policy changes are necessary.

Since there seem to be drops on our device, let's investigate the drops and add a more granular QoS configuration.

Lab Steps:
Select a device and select **QoS** and **Manage QoS Settings**.



83. Select the **VOIP** Class.
84. Click the **Queueing** Tab.
85. Select **Burst Size** of **128000**.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●		Class-bas...						
class-default	●								

□ Drop all traffic for class

Queueing type: Priority
Rate: 33 Percent
☑ Burst size: 128,000 bytes
Unknown elements:

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

Queueing Type

Class-based: utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class

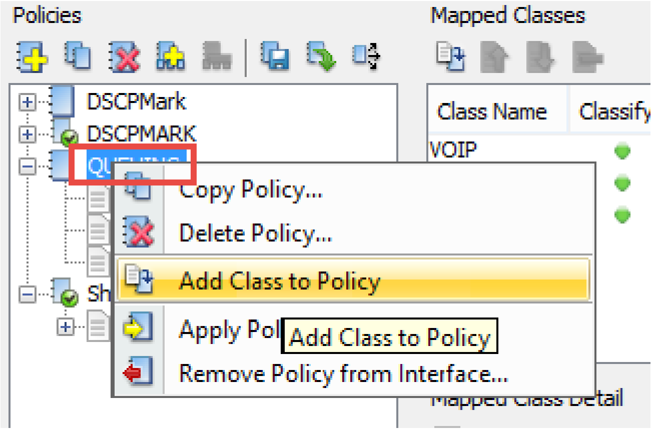
Note: Configuring a burst rate is something that is not always common and should be fully understood before looking to implement in your own network.

Read more about configuring a burst rate here:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.html

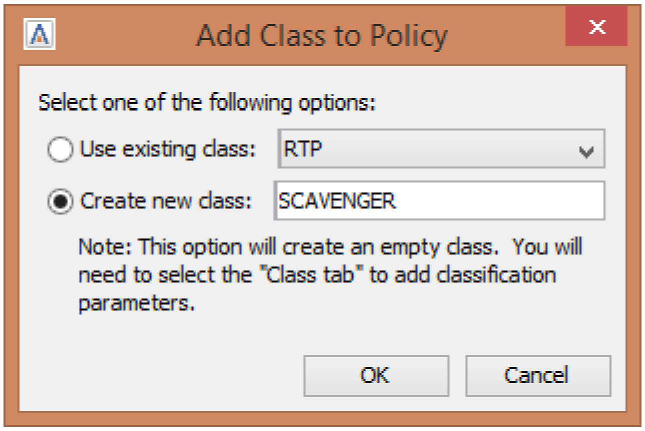
An excerpt about the math behind deciding the burst rate would be:
Cisco recommends the following values for the normal and extended burst parameters:
normal burst = configured rate * (1 byte)/ (8 bits) * 1.5 seconds
extended burst = 2 * normal burst

86. Right-click on the **QUEUEING** Policy.

87. Select **Add Class to Policy**.



88. Give the new class a label of **SCAVENGER**.


Add Class to Policy

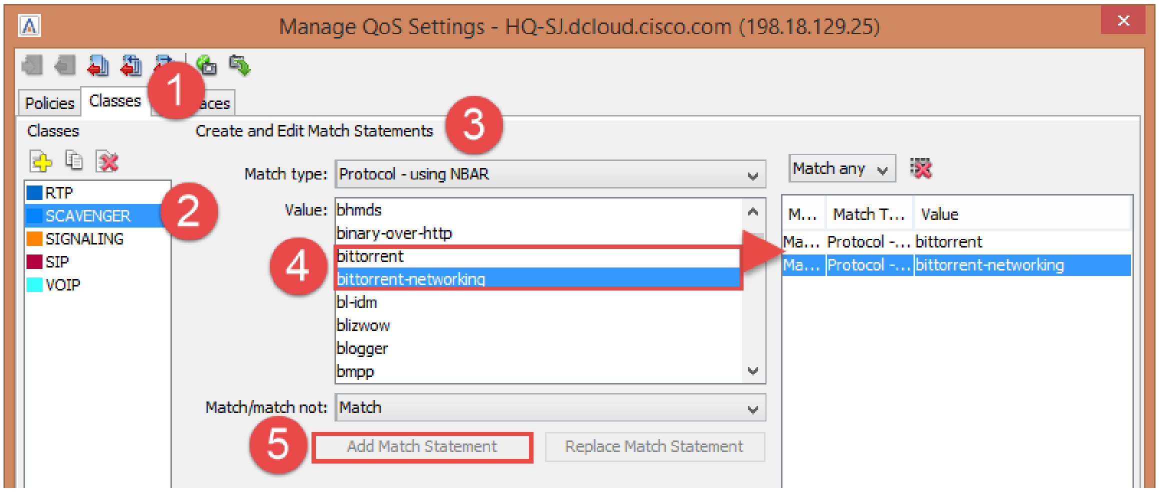
Select one of the following options:

○ Use existing class: RTP

● Create new class: SCAVENGER

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

89. Select the **Classes** Tab.
90. Select the **Scavenger** Class.
91. For Match Type select **Protocol – Using NBAR**.
92. Select **both** “bittorrent” and “bittorrent-networking”.
93. Click **Add Match Statement** for both Applications.



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Classes

- RTP
- SCAVENGER
- SIGNALING
- SIP
- VOIP

Create and Edit Match Statements

Match type: Protocol - using NBAR

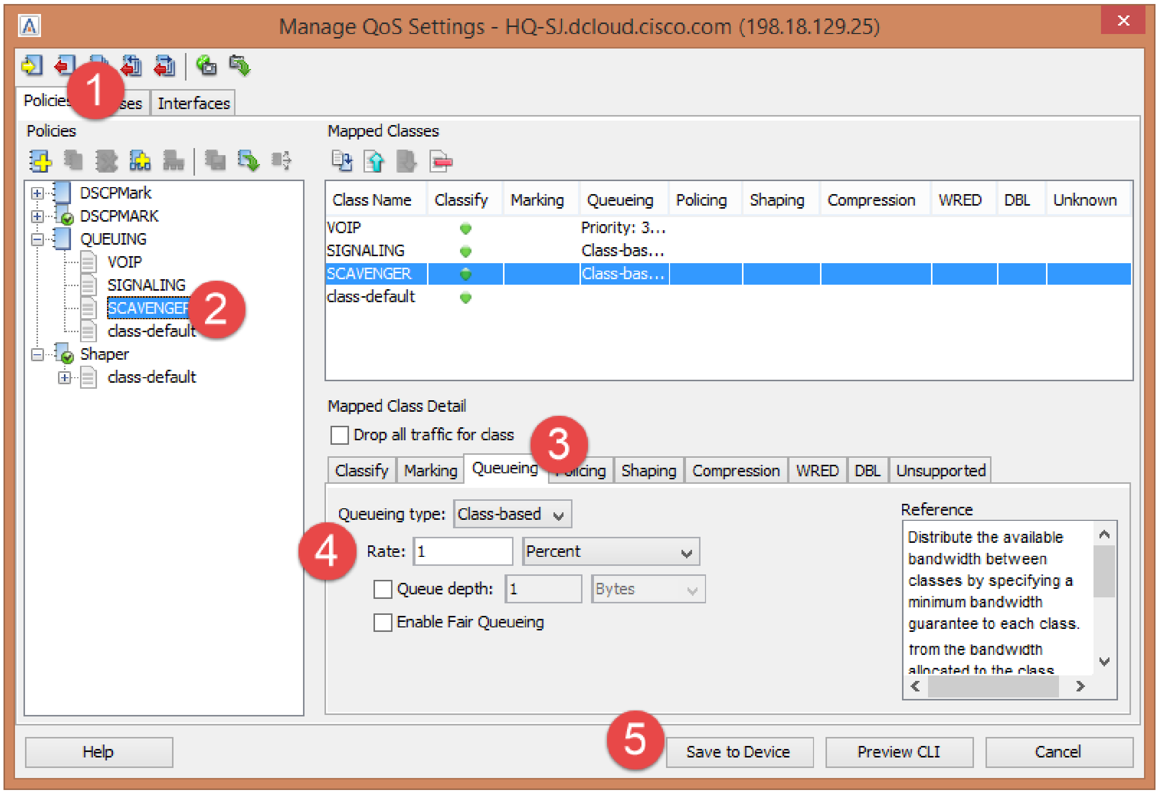
Value: bhmds, binary-over-http, bittorrent, bittorrent-networking, bl-idm, blizwow, blogger, bmpp

Match any

M...	Match T...	Value
Ma...	Protocol -...	bittorrent
Ma...	Protocol -...	bittorrent-networking

Match/match not: Match

94. Now let’s go back to the **Policies** Tab
95. Select the **Scavenger** Class
96. Then select the **Queueing** Tab
97. Next select **Class-based** and give the class a rate of **1 percent**
98. Finally select **Save** to Device



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Policies

- DSCPMark
- DSCPMARK
- QUEUING
  - VOIP
  - SIGNALING
  - SCAVENGER
  - class-default
- Shaper
  - class-default

Mapped Classes

Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
VOIP	●		Priority: 3...						
SIGNALING	●		Class-bas...						
SCAVENGER	●		Class-bas...						
class-default	●								

Mapped Class Detail

□ Drop all traffic for class

Queueing type: Class-based

Rate: 1 Percent

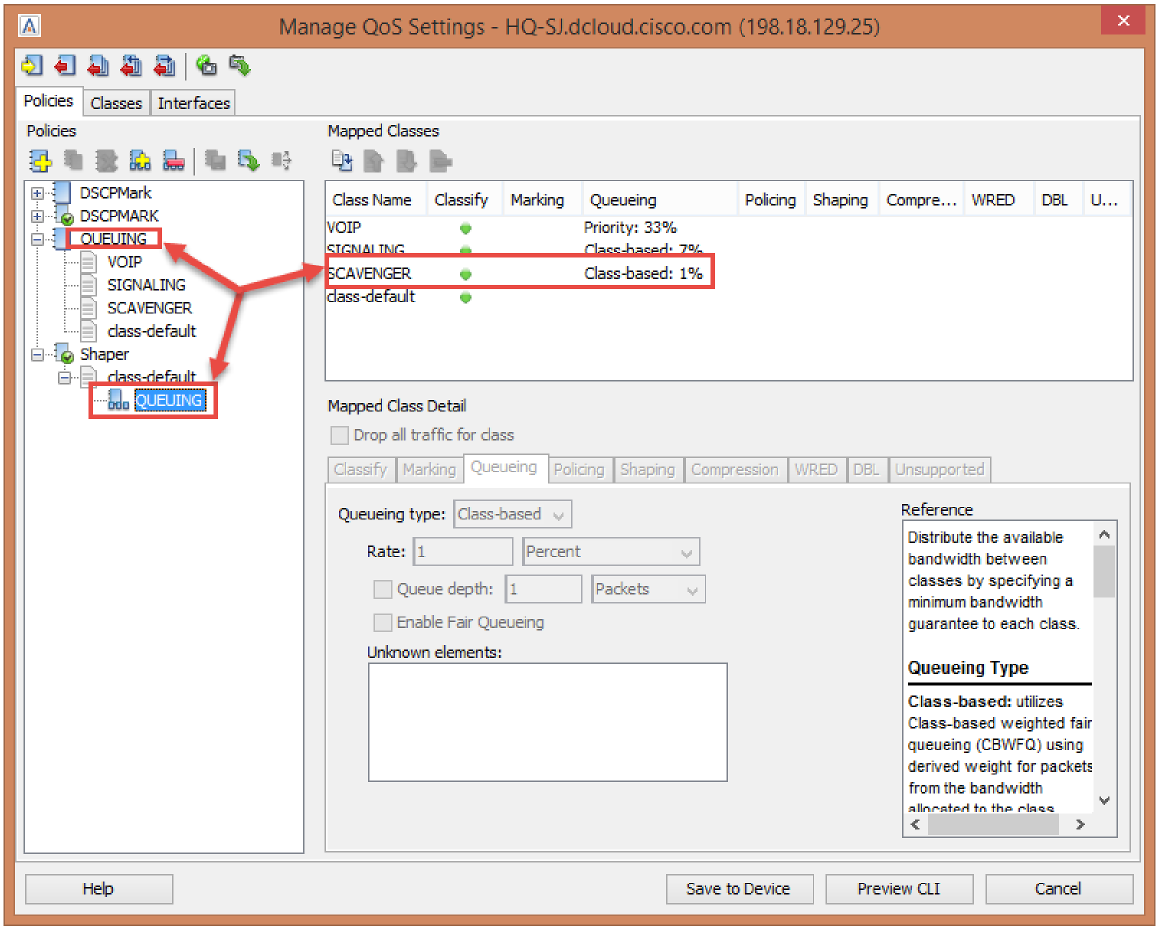
□ Queue depth: 1 Bytes

□ Enable Fair Queueing

Reference

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. from the bandwidth allocated to the class

When making changes to the **QUEUEING** Policy it will also affect the Shaping Policy.



Class Name	Classify	Marking	Queueing	Policing	Shaping	Compre...	WRED	DBL	U...
VOIP	●		Priority: 33%						
SIGNALING	●		Class-based: 7%						
SCAVENGER	●		Class-based: 1%						
class-default	●								

□ Drop all traffic for class

Queueing type: Class-based

Rate: 1 Percent

□ Queue depth: 1 Packets

□ Enable Fair Queueing

Unknown elements:

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

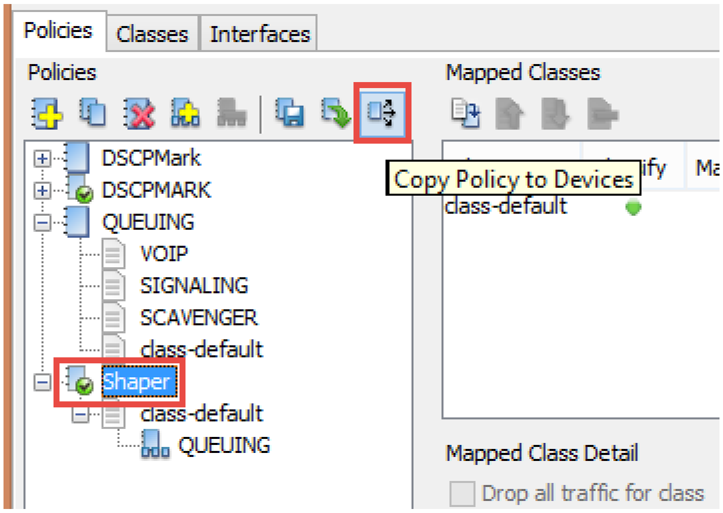
Queueing Type

Class-based: utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class

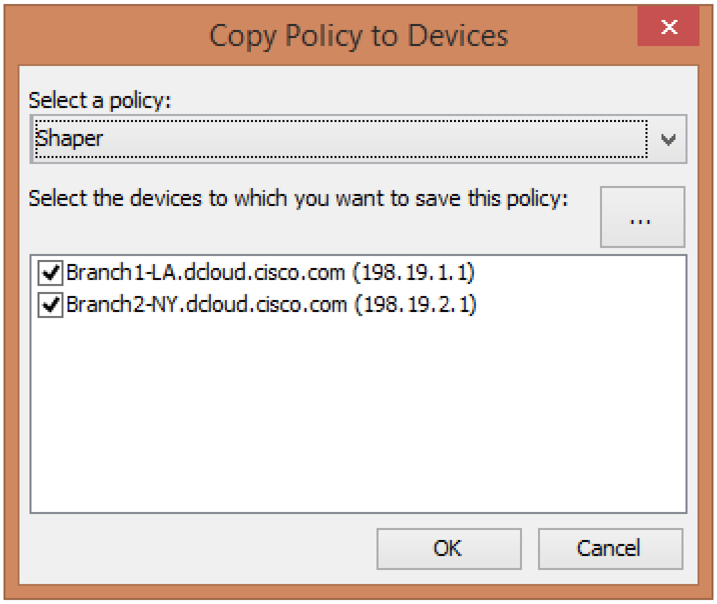
Copy the updated policy to other devices in the topology.

99. Select the **Shaper** Policy

100. Click the **Policy to Devices** button.



101. Select **Shaper** and select the other devices.



Copy Policy to Devices

Select a policy:

Shaper

Select the devices to which you want to save this policy: ...

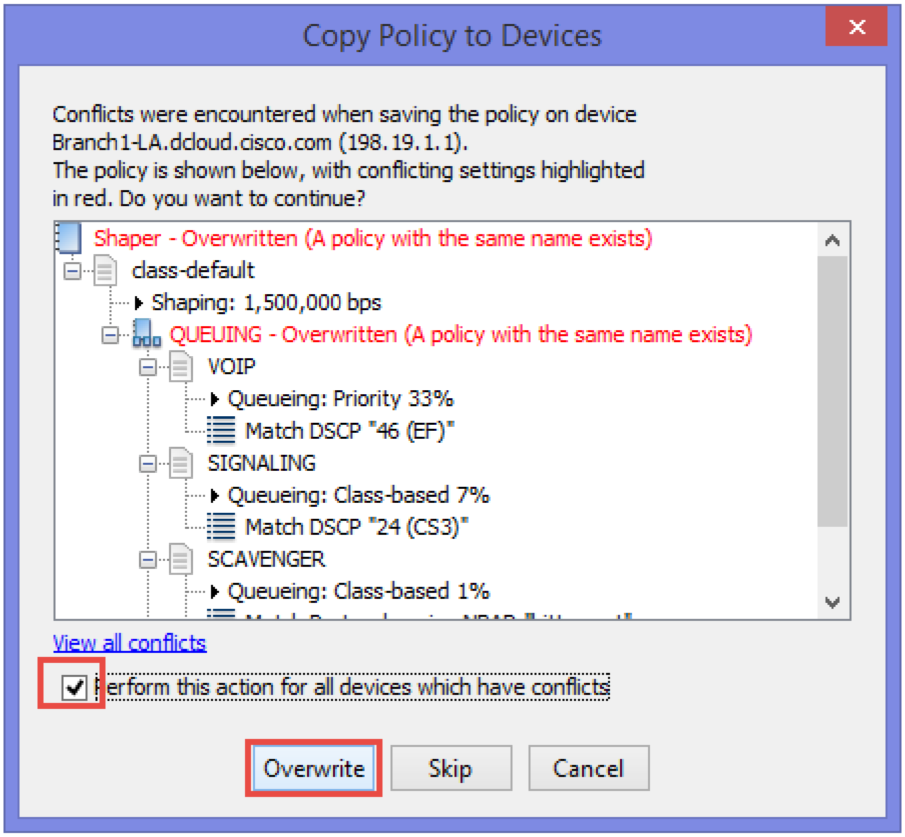
☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)

OK Cancel

You are given a warning that you are overwriting a policy on both devices. This is what we want to do!

102. Select **perform this action for all devices which have conflicts**.

103. Click **Overwrite**.



Copy Policy to Devices

Conflicts were encountered when saving the policy on device Branch1-LA.dcloud.cisco.com (198.19.1.1).
The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?

```
Shaper - Overwritten (A policy with the same name exists)
  class-default
    Shaping: 1,500,000 bps
    QUEUING - Overwritten (A policy with the same name exists)
      VOIP
        Queueing: Priority 33%
        Match DSCP "46 (EF)"
      SIGNALING
        Queueing: Class-based 7%
        Match DSCP "24 (CS3)"
      SCAVENGER
        Queueing: Class-based 1%
```

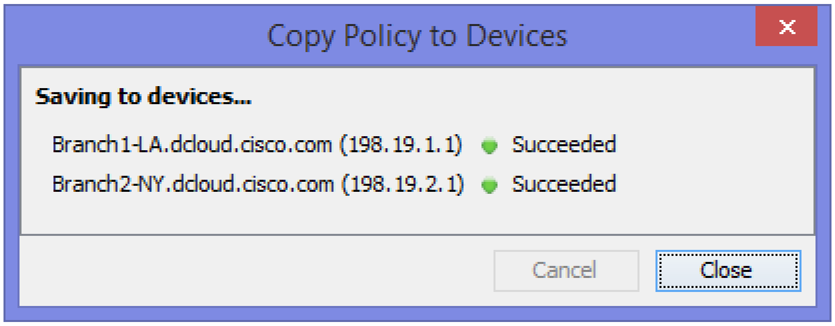
View all conflicts

☑ Perform this action for all devices which have conflicts

Overwrite Skip Cancel

Ensure the copy is successful.

104. Click **Close**.

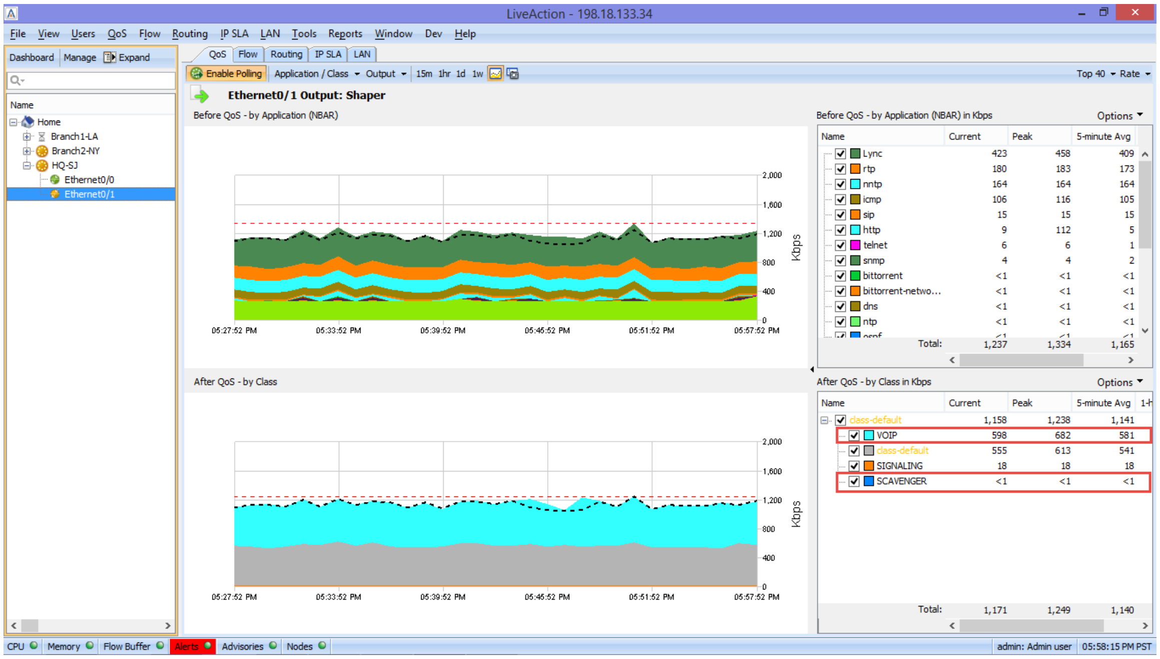


Saving to devices...

Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded

Branch2-NY.dcloud.cisco.com (198.19.2.1) ● Succeeded

When completed you should no longer see VOIP Class drops, and you should see traffic in the scavenger class in the QoS Interface View.



LiveAction - 198.18.133.34
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 Application / Class Output 15m 1hr 1d 1w
Top 40 Rate
Name
Home
Branch1-LA
Branch2-NY
HQ-SJ
Ethernet0/0
Ethernet0/1
Before QoS - by Application (NBAR)
After QoS - by Class
2,000
1,600
1,200
800
400
0
Kbps
05:27:52 PM
05:33:52 PM
05:39:52 PM
05:45:52 PM
05:51:52 PM
05:57:52 PM
Options
CPU Memory Flow Buffer Alerts Advisories Nodes
admin: Admin user 05:58:15 PM PST

Ethernet0/1 Output: Shaper

Before QoS - by Application (NBAR) in Kbps

Name	Current	Peak	5-minute Avg
☑ Lync	423	458	409
☑ rtp	180	183	173
☑ nntp	164	164	164
☑ icmp	106	116	105
☑ sip	15	15	15
☑ http	9	112	5
☑ telnet	6	6	1
☑ snmp	4	4	2
☑ bittorrent	<1	<1	<1
☑ bittorrent-netwo...	<1	<1	<1
☑ dns	<1	<1	<1
☑ ntp	<1	<1	<1
Total:	1,237	1,334	1,165

After QoS - by Class in Kbps

Name	Current	Peak	5-minute Avg	1-h
☑ class-default	1,158	1,238	1,141	
☑ VOIP	598	682	581	
☑ class-default	555	613	541	
☑ SIGNALING	18	18	18	
☑ SCAVENGER	<1	<1	<1	
Total:	1,171	1,249	1,140	

Good job! You have successfully created Marking and Queueing policies for your network devices! There still may be drops in the class-default, but that is the purpose of this Lab… to help you identify and eliminate issues.

Lab A

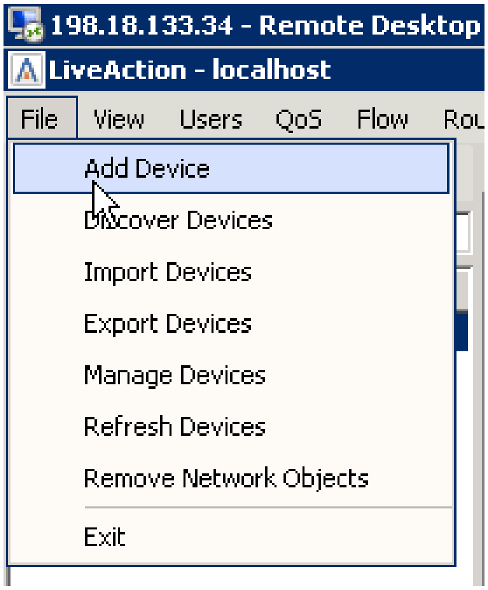
Lab A: Appendix

Lab A.1: Add Device

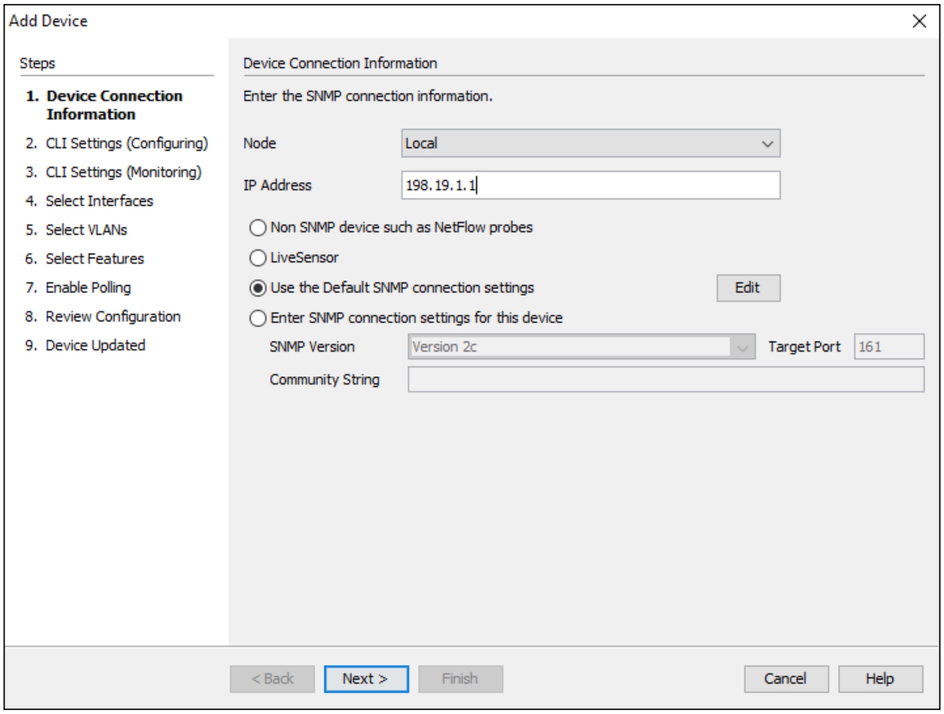
Adding devices into LiveAction and managing them properly is very important to the overall usability of LiveAction itself.

Lab Steps:

1. Select File, **Add Device**



2. Enter 198.19.1.1 in the IP Address field.
3. Select “Use the Default SNMP connection settings”.



Device Connection Information

Enter the SNMP connection information.

Node: Local

IP Address: 198.19.1.1

○ Non SNMP device such as NetFlow probes

○ LiveSensor

● Use the Default SNMP connection settings

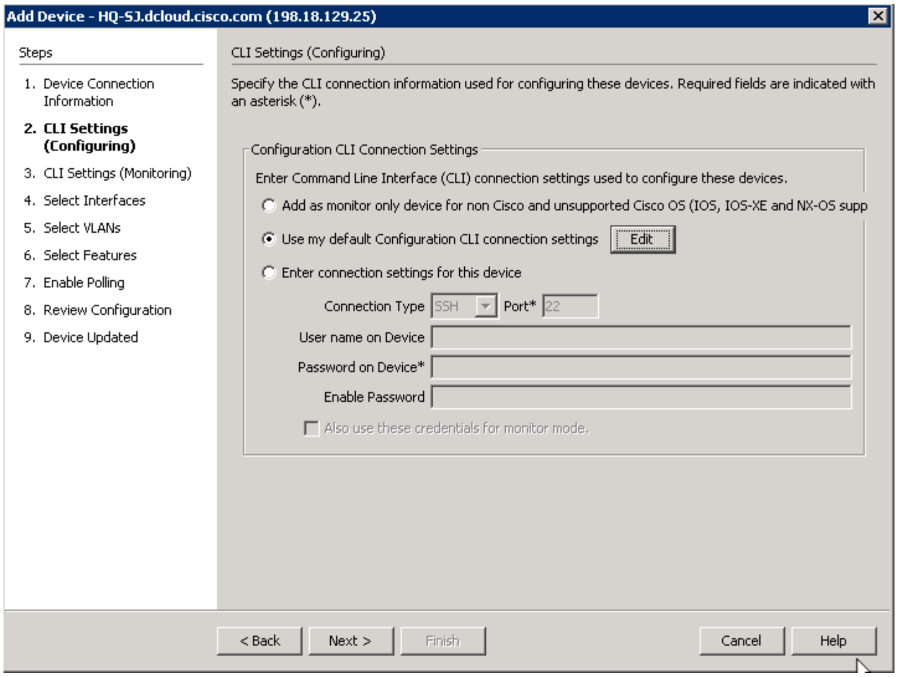
○ Enter SNMP connection settings for this device

SNMP Version: Version 2c   Target Port: 161

Community String:

4. Click Next.

5. Select “Use my default Configuration CLI connection settings”.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. **CLI Settings (Configuring)**
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

● Use my default Configuration CLI connection settings [Edit]

○ Enter connection settings for this device

Connection Type SSH Port* 22

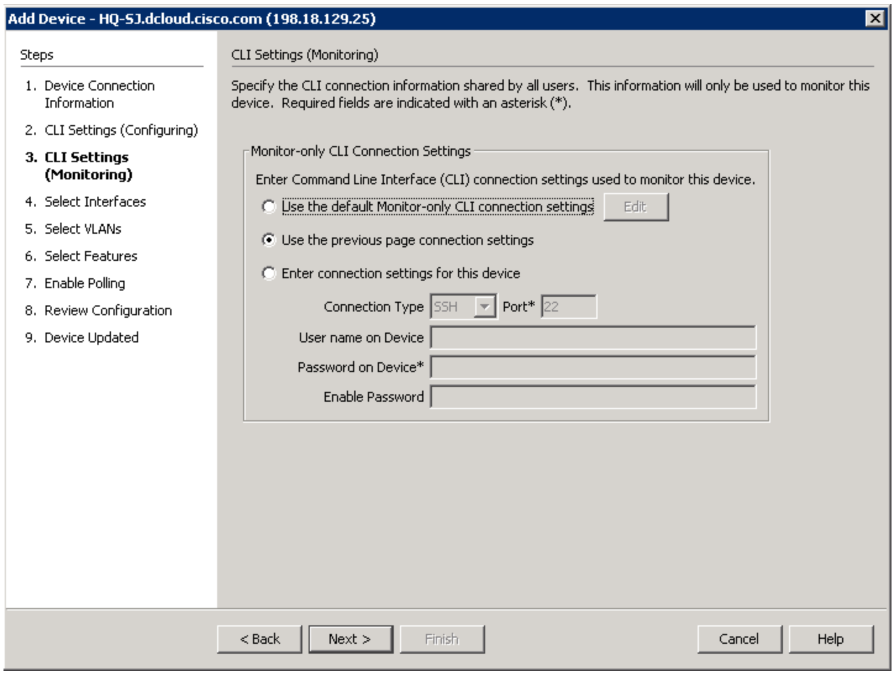
User name on Device

Password on Device*

Enable Password

□ Also use these credentials for monitor mode.

6. Click Next.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings [Edit]

● Use the previous page connection settings

○ Enter connection settings for this device

Connection Type SSH Port* 22

User name on Device

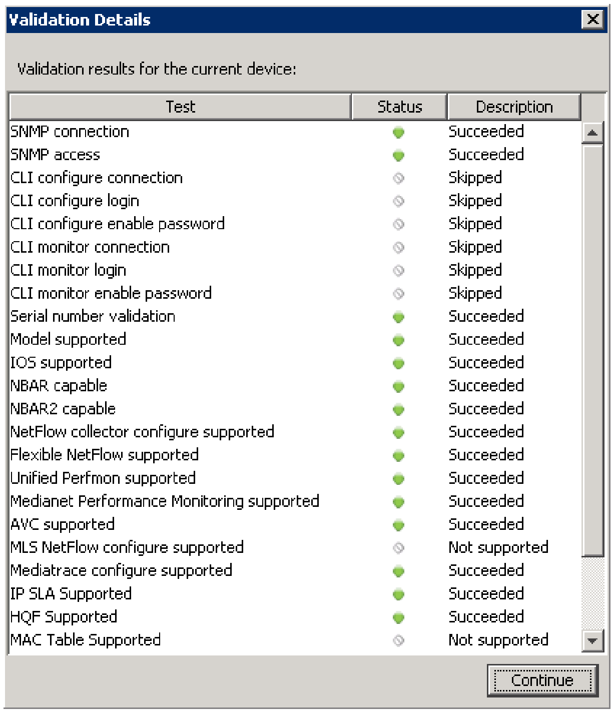
Password on Device*

Enable Password

7. Select “Use the previous page connection settings”.
8. Click Next.

You can verify what capabilities LiveAction is able to interact with the device.

9. Click Continue.

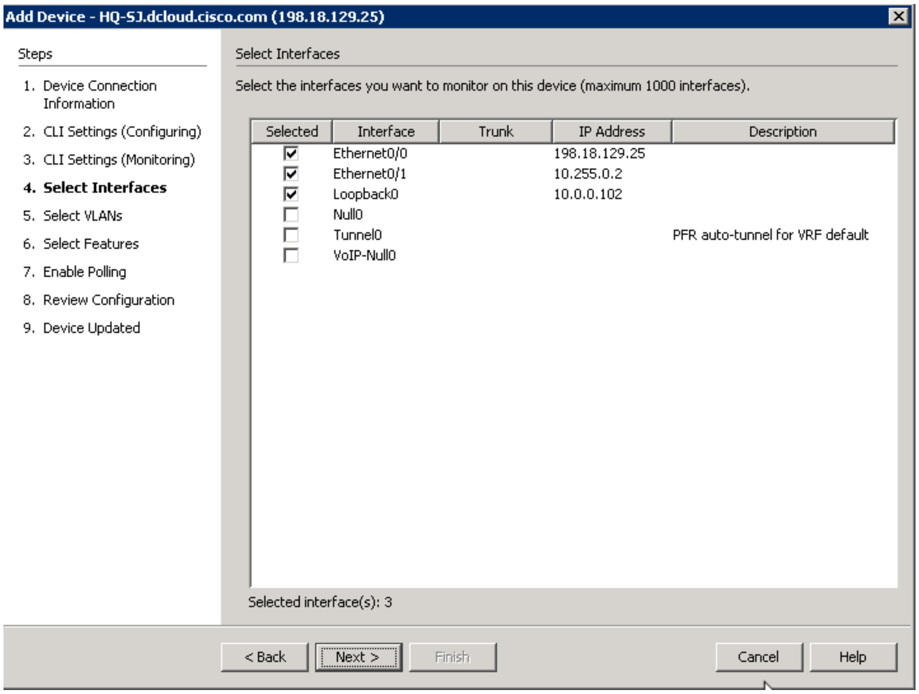


Validation Details

Validation results for the current device:

Test	Status	Description
SNMP connection	●	Succeeded
SNMP access	●	Succeeded
CLI configure connection	⊘	Skipped
CLI configure login	⊘	Skipped
CLI configure enable password	⊘	Skipped
CLI monitor connection	⊘	Skipped
CLI monitor login	⊘	Skipped
CLI monitor enable password	⊘	Skipped
Serial number validation	●	Succeeded
Model supported	●	Succeeded
IOS supported	●	Succeeded
NBAR capable	●	Succeeded
NBAR2 capable	●	Succeeded
NetFlow collector configure supported	●	Succeeded
Flexible NetFlow supported	●	Succeeded
Unified Perfmon supported	●	Succeeded
Medianet Performance Monitoring supported	●	Succeeded
AVC supported	●	Succeeded
MLS NetFlow configure supported	⊘	Not supported
Mediatrace configure supported	●	Succeeded
IP SLA Supported	●	Succeeded
HQF Supported	●	Succeeded
MAC Table Supported	⊘	Not supported

On the select interfaces window you may notice 3 interfaces are already selected. LiveAction automatically selects the interfaces based on the highest bit rate.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. **Select Interfaces**
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

Select Interfaces

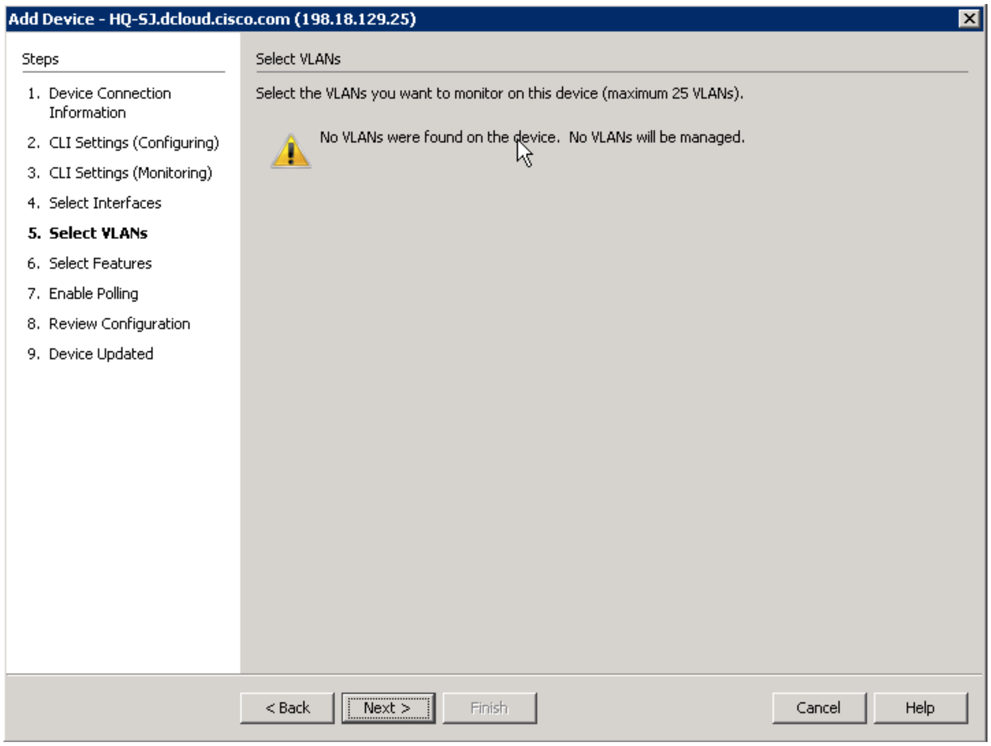
Select the interfaces you want to monitor on this device (maximum 1000 interfaces).

Selected	Interface	Trunk	IP Address	Description
☑	Ethernet0/0		198.18.129.25	
☑	Ethernet0/1		10.255.0.2	
☑	Loopback0		10.0.0.102	
☐	Null0			
☐	Tunnel0			PFR auto-tunnel for VRF default
☐	VoIP-Null0			

Selected interface(s): 3

10. Click Next.

Note: Since there are no VLANs configured on this device, none will be displayed. You may monitor up to 25 configured VLANs on each device.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

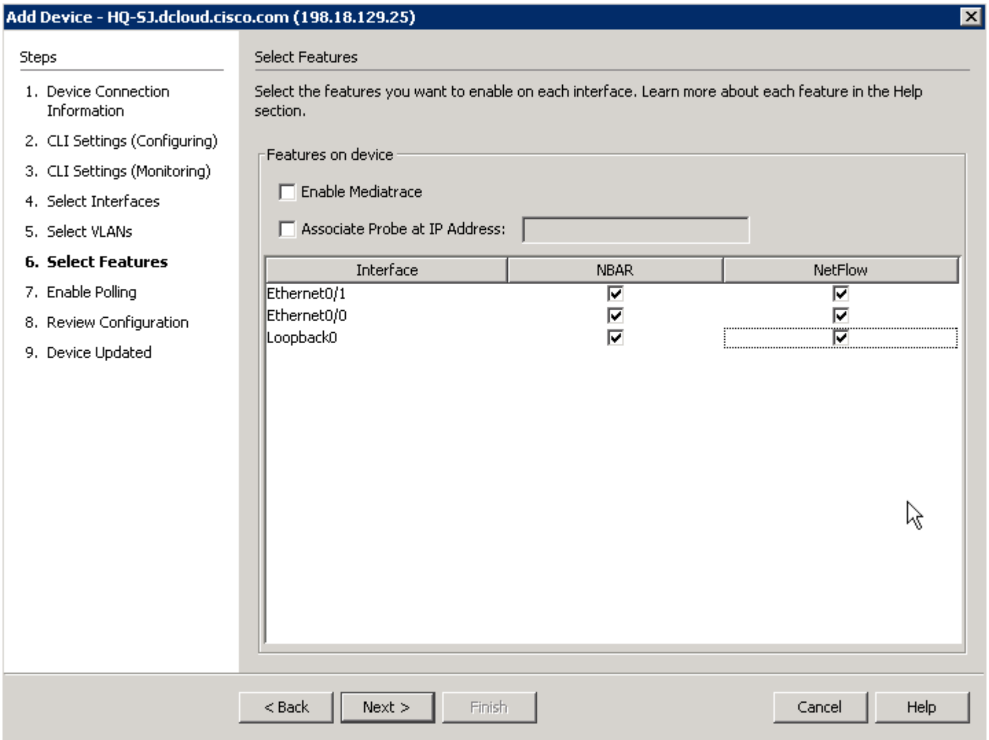
Select VLANs

Select the VLANs you want to monitor on this device (maximum 25 VLANs).

No VLANs were found on the device. No VLANs will be managed.

11. Click Next.

The **Select Features** dialog allows you to turn-on specific Cisco technologies using the templates included in LiveNX. This dialog displays the current IOS configuration of the device you are currently viewing. Leave this screen **AS-IS**.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Select Features

Select the features you want to enable on each interface. Learn more about each feature in the Help section.

Features on device

□ Enable Mediatrace

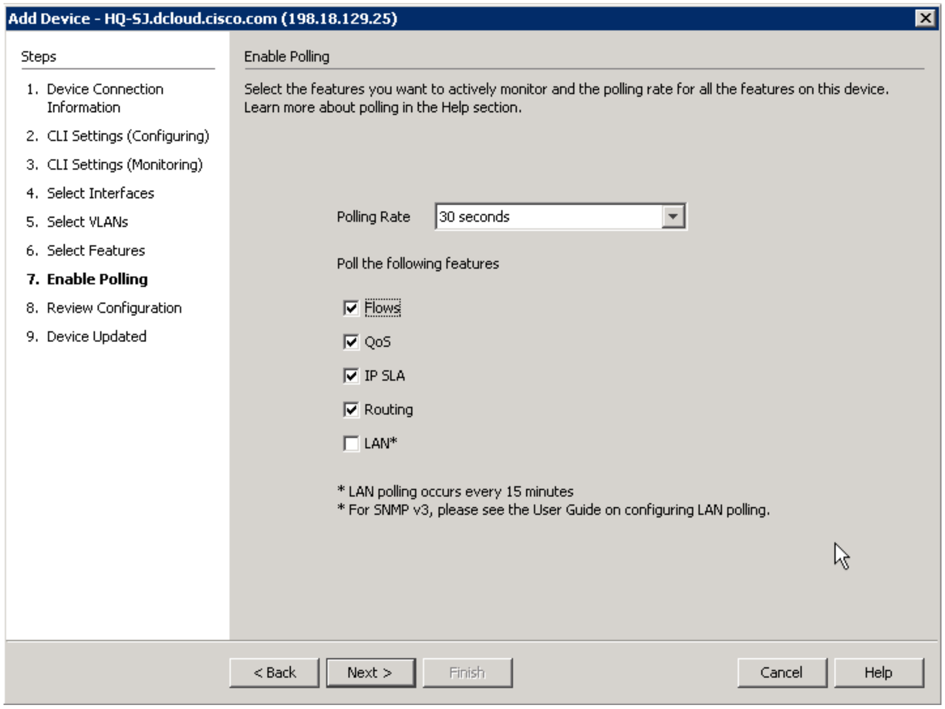
□ Associate Probe at IP Address:

Interface	NBAR	NetFlow
Ethernet0/1	☑	☑
Ethernet0/0	☑	☑
Loopback0	☑	☑

12. Click Next.

13. Change the polling rate to 30 seconds.

14. Verify that ONLY the **Flow** & **QoS** boxes remain checked.



Enable Polling

Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section.

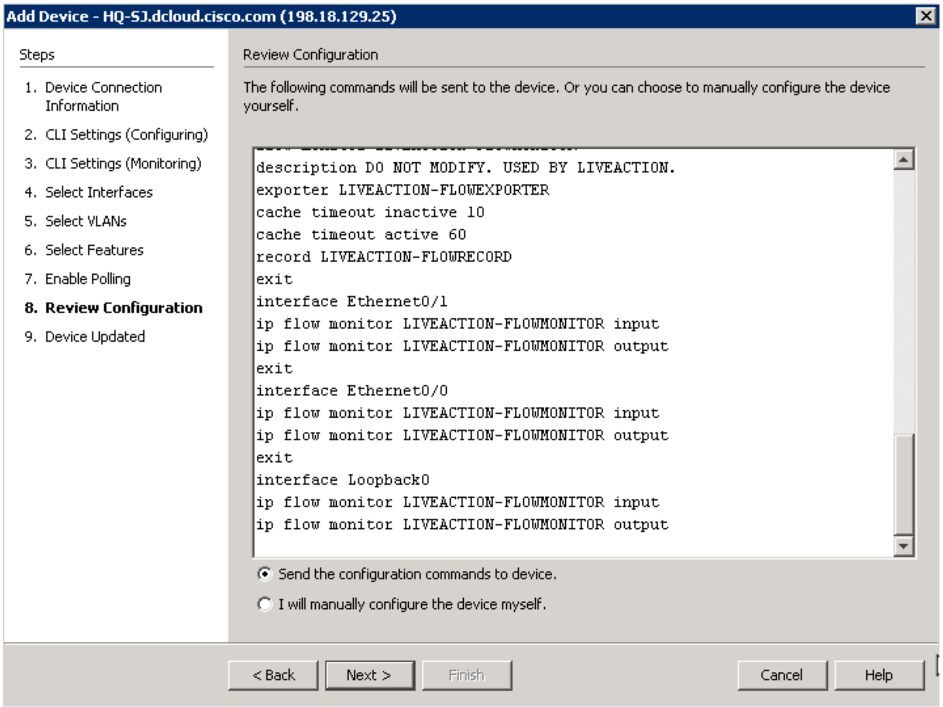
Polling Rate: 30 seconds

Poll the following features

☑ Flows
☑ QoS
☑ IP SLA
☑ Routing
☐ LAN*

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.

Note: Any changes to the Select Features dialog will generate a CLI push to update the current configuration. Before sending the NetFlow configurations to the device, you can verify the configurations that LiveAction created.



Review Configuration

The following commands will be sent to the device. Or you can choose to manually configure the device yourself.

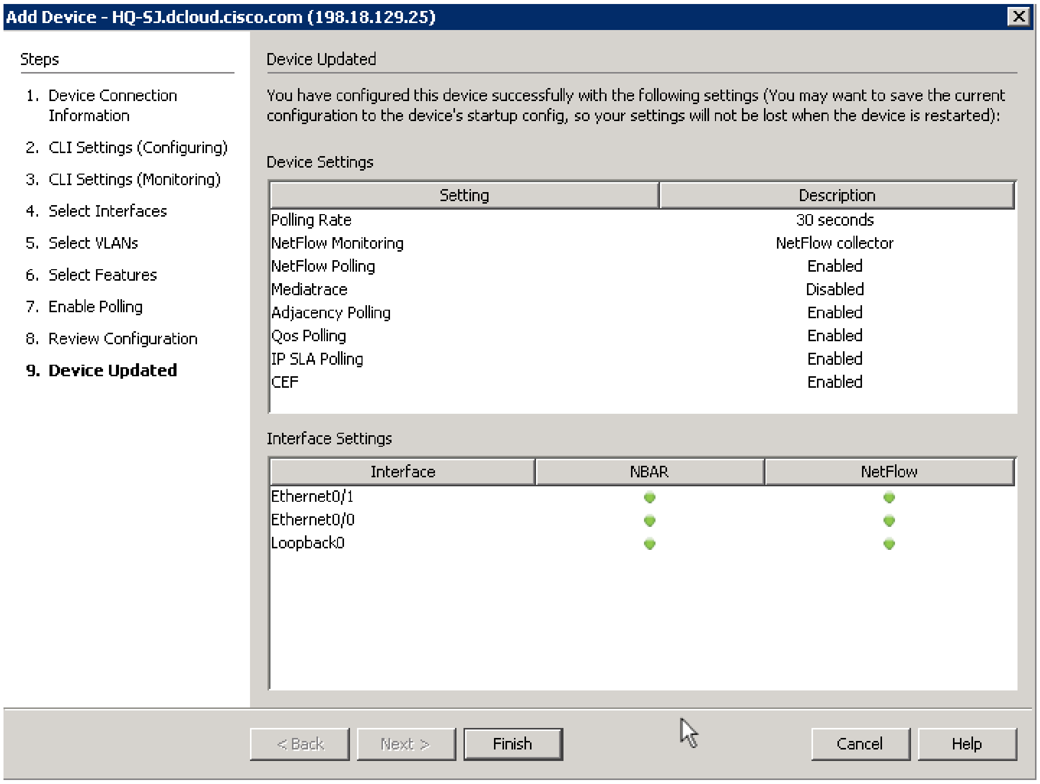
```
description DO NOT MODIFY. USED BY LIVEACTION.
exporter LIVEACTION-FLOWEXPORTER
cache timeout inactive 10
cache timeout active 60
record LIVEACTION-FLOWRECORD
exit
interface Ethernet0/1
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
exit
interface Ethernet0/0
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
exit
interface Loopback0
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
```

● Send the configuration commands to device.
○ I will manually configure the device myself.

15. Select "Send the configuration…" radio button, if available.

16. Click Next.

17. Click Finish.



Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. **Device Updated**

Device Updated

You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):

Device Settings

Setting	Description
Polling Rate	30 seconds
NetFlow Monitoring	NetFlow collector
NetFlow Polling	Enabled
Mediatrace	Disabled
Adjacency Polling	Enabled
Qos Polling	Enabled
IP SLA Polling	Enabled
CEF	Enabled

Interface Settings

Interface	NBAR	NetFlow
Ethernet0/1	●	●
Ethernet0/0	●	●
Loopback0	●	●

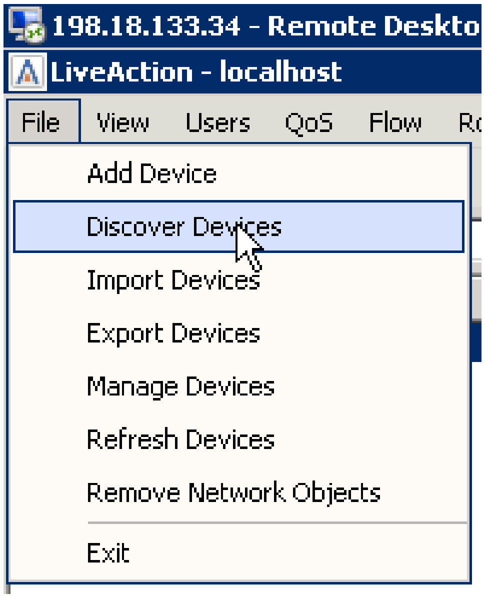
The device will be added to the Topology Pane in LiveNX. Note that LiveNX will not automatically position a new device with reference to any existing devices… you may need to scroll-about in the Topology Pane to locate your new device(s).

Lab A.2: Client Device Discovery

As we discovered in a prior Lab, the LiveNX Server in your topology has had device(s) pre-installed. In the following Lab you may add additional devices to your Topology, configure those devices to send flow and SNMP data to the LiveNX Server, and discover what data your LiveNX solution is gathering.

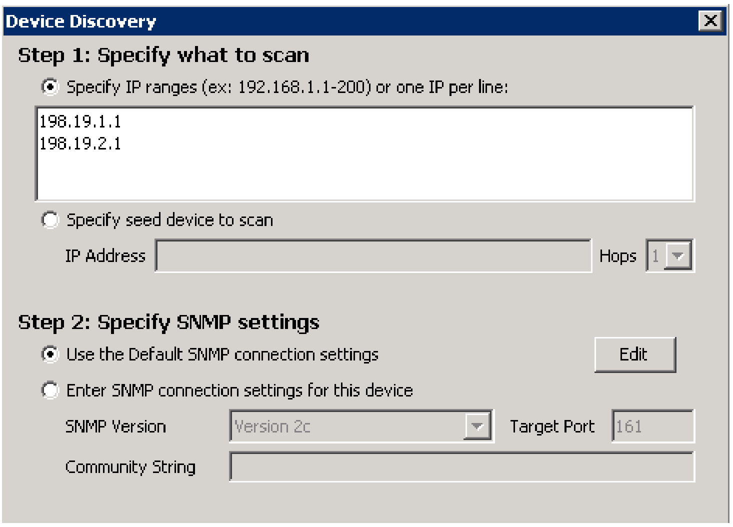
Lab Steps:
Adding several devices at once is as easy as adding a single device at a time. To do this:

1. Select File and Discover Devices.



2. Specify the following IP addresses:
   198.19.1.1
   198.19.2.1

3. **Select** Use the default SNMP connection settings.



Step 1: Specify what to scan

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

```
198.19.1.1
198.19.2.1
```

○ Specify seed device to scan

IP Address: Hops: 1

Step 2: Specify SNMP settings

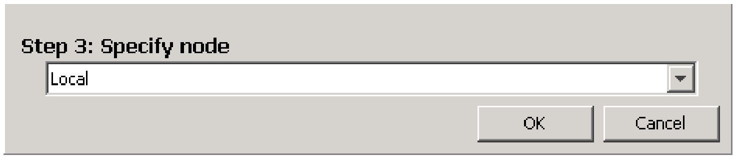
● Use the Default SNMP connection settings

○ Enter SNMP connection settings for this device

SNMP Version: Version 2c Target Port: 161

Community String:

Note: In the Lab infrastructure we are utilizing the Local LiveNX Node included with the Server installation. If you require access to a Remote Node to access the subnets or addressing in "Step 1: Specify what to scan" you would use the Specify node drop-down at the bottom of this dialog box.

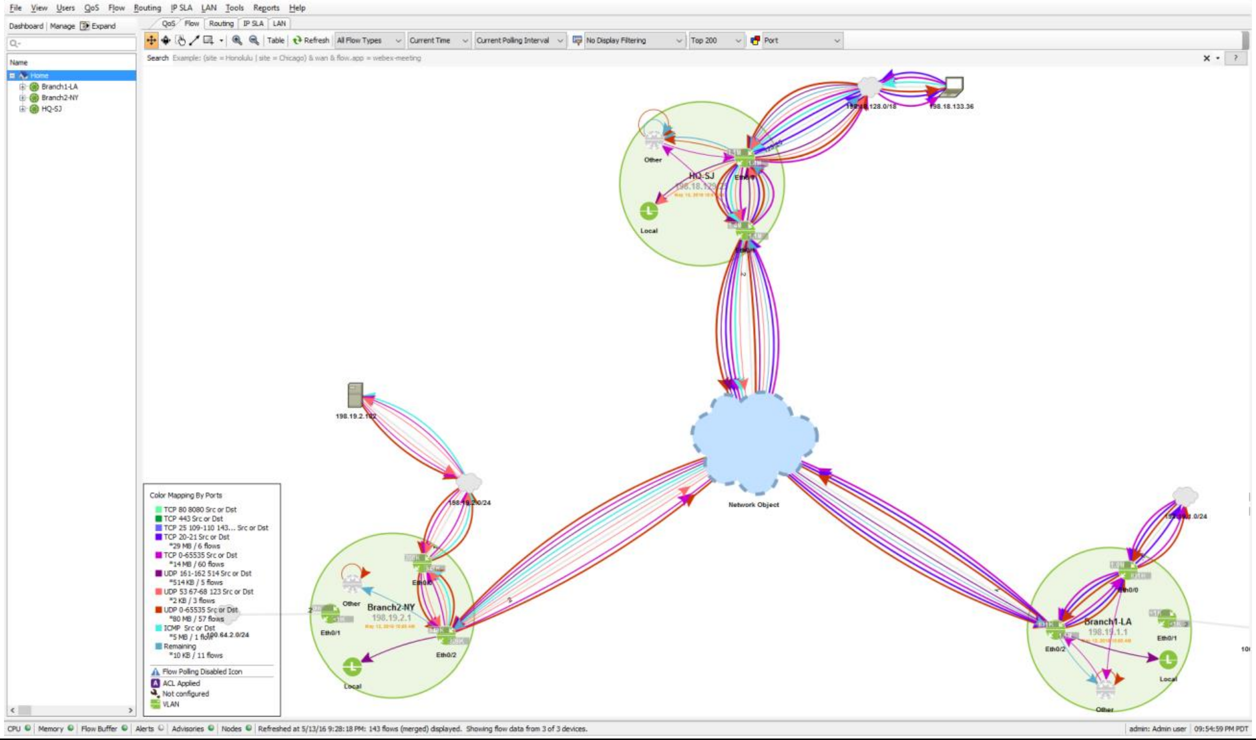


Step 3: Specify node

Local

4. Click OK.
5. Verify that both devices were found, and then select Add Devices.

Note: LiveNX may only discover a single router in the above steps. Your Student Pod may already be pre-configured with multiple devices. Your instructor may direct you to add one or more devices in this
lab.



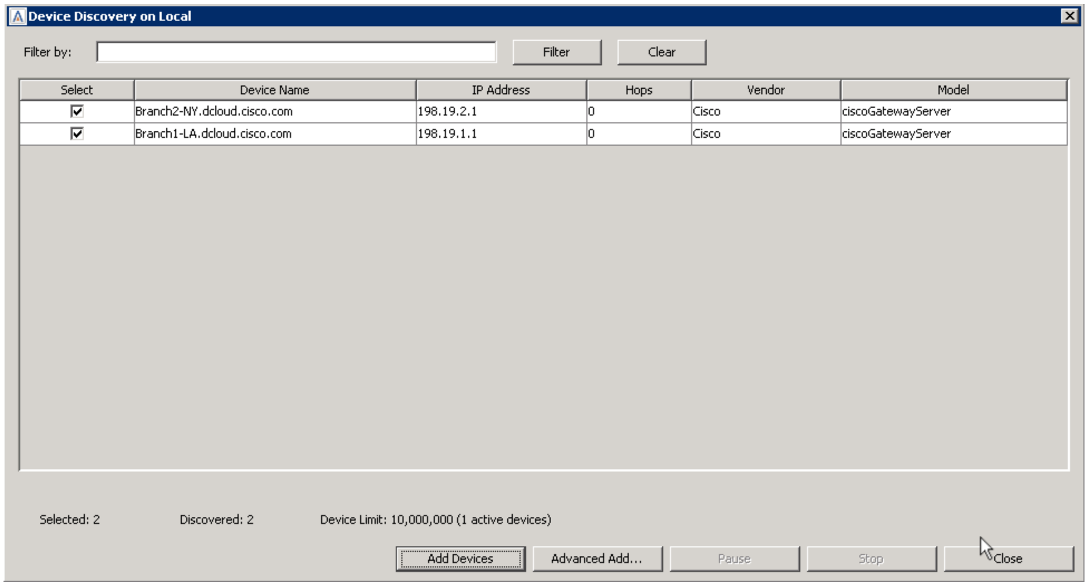
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard | Manage | Expand
QoS Flow Routing IP SLA LAN
Table | Refresh | All Flow Types | Current Time | Current Polling Interval | No Display Filtering | Top 200 | Port
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
Branch1-LA
Branch2-NY
HQ-SJ
Other
HQ-SJ
198.18.128.0/18
198.18.133.36
Local
198.19.2.102
Network Object
Other
Branch2-NY
198.19.2.1
Eth0/1
Eth0/2
Local
100.64.2.0/24
Branch1-LA
198.19.1.1
Eth0/1
Eth0/2
Local
Other

Color Mapping By Ports

- 🟩 TCP 80 8080 Src or Dst
- 🟩 TCP 443 Src or Dst
- 🟦 TCP 25 109-110 143... Src or Dst
- 🟦 TCP 20-21 Src or Dst
  *29 MB / 6 flows
- 🟪 TCP 0-65535 Src or Dst
  *14 MB / 60 flows
- 🟪 UDP 161-162 514 Src or Dst
  *514 KB / 5 flows
- 🟥 UDP 53 67-68 123 Src or Dst
  *2 KB / 3 flows
- 🟥 UDP 0-65535 Src or Dst
  *80 MB / 57 flows
- 🟦 ICMP Src or Dst
  *5 MB / 1 flow
- 🟦 Remaining
  *10 KB / 11 flows

Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN

CPU | Memory | Flow Buffer | Alerts | Advisories | Nodes | Refreshed at 5/13/16 9:28:18 PM: 143 flows (merged) displayed. Showing flow data from 3 of 3 devices. | admin: Admin user | 09:54:59 PM PDT

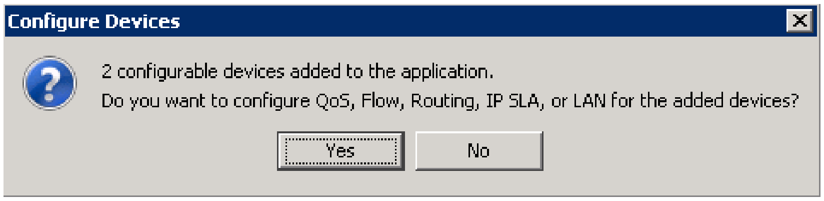

Device Discovery on Local

Filter by:

Select	Device Name	IP Address	Hops	Vendor	Model
☑	Branch2-NY.dcloud.cisco.com	198.19.2.1	0	Cisco	ciscoGatewayServer
☑	Branch1-LA.dcloud.cisco.com	198.19.1.1	0	Cisco	ciscoGatewayServer

Selected: 2 Discovered: 2 Device Limit: 10,000,000 (1 active devices)

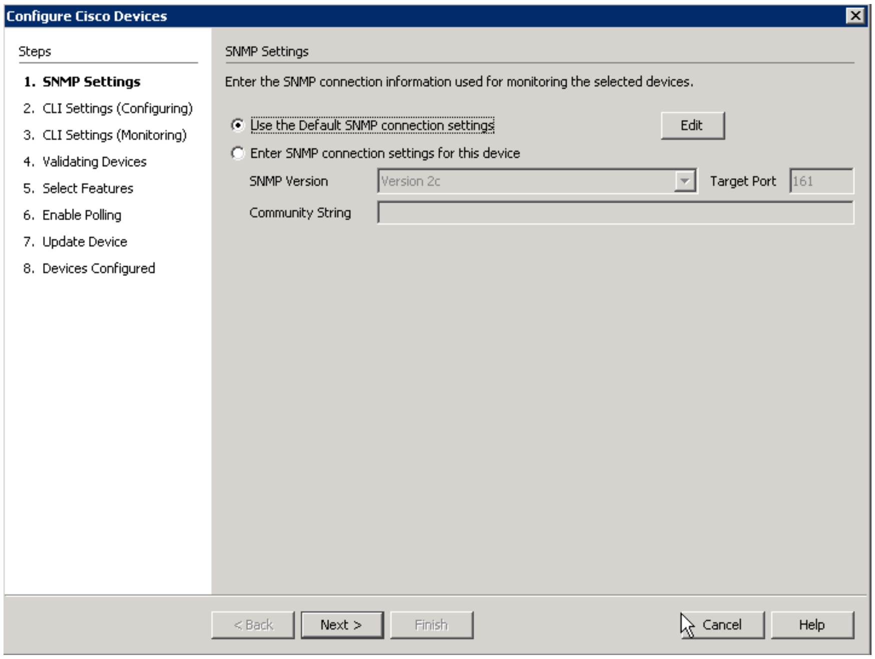
6. Select Yes on the configure devices dialog.


Configure Devices

2 configurable devices added to the application.
Do you want to configure QoS, Flow, Routing, IP SLA, or LAN for the added devices?

7. Use the default SNMP connection settings and then select Next

Note: You must be logged-in as the original admin user so that the LiveNX Wizard will inherit the appropriate credentials. Ask your instructor for clarification on this, if desired.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

SNMP Settings

Enter the SNMP connection information used for monitoring the selected devices.

● Use the Default SNMP connection settings

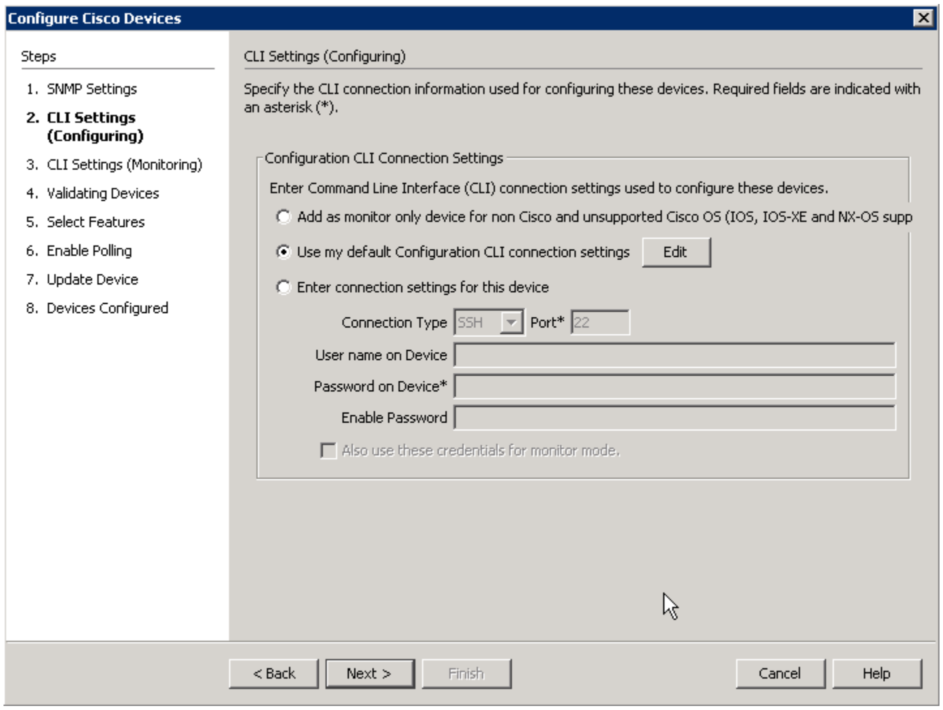
○ Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port: 161

Community String:

8. Select Use my default Configuration CLI connection settings.
9. Click next.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

● Use my default Configuration CLI connection settings

○ Enter connection settings for this device

Connection Type: SSH

Port*: 22

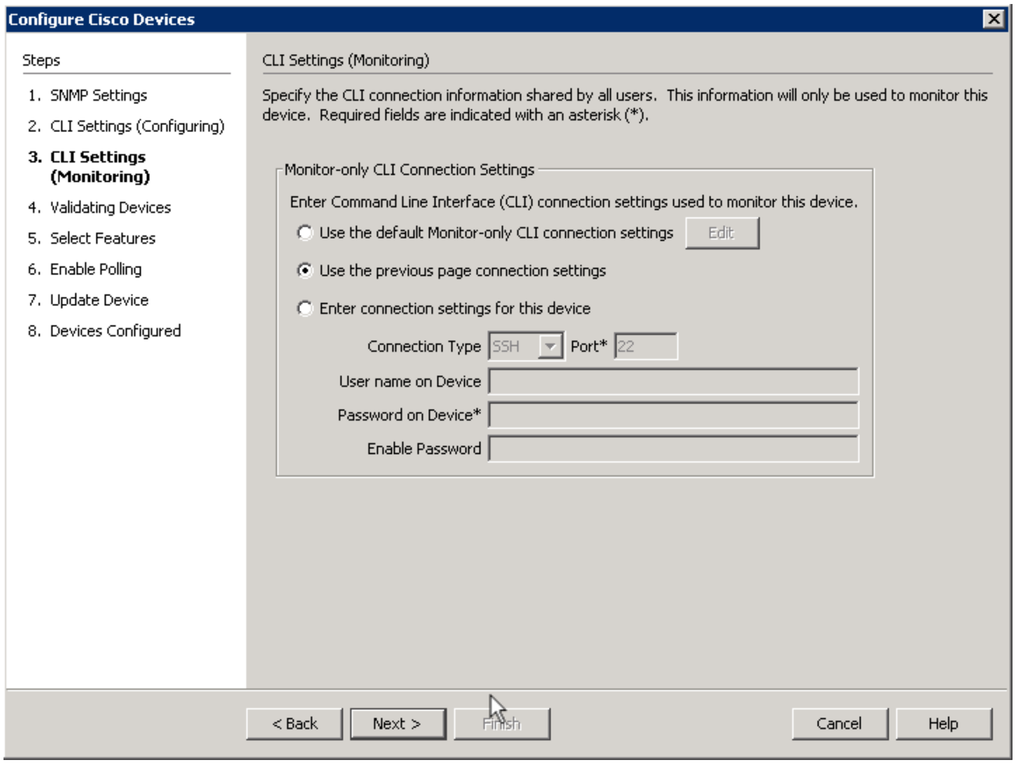
User name on Device:

Password on Device*:

Enable Password:

☐ Also use these credentials for monitor mode.

10. Select Use the previous page connection settings.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings

● Use the previous page connection settings

○ Enter connection settings for this device

Connection Type SSH Port* 22

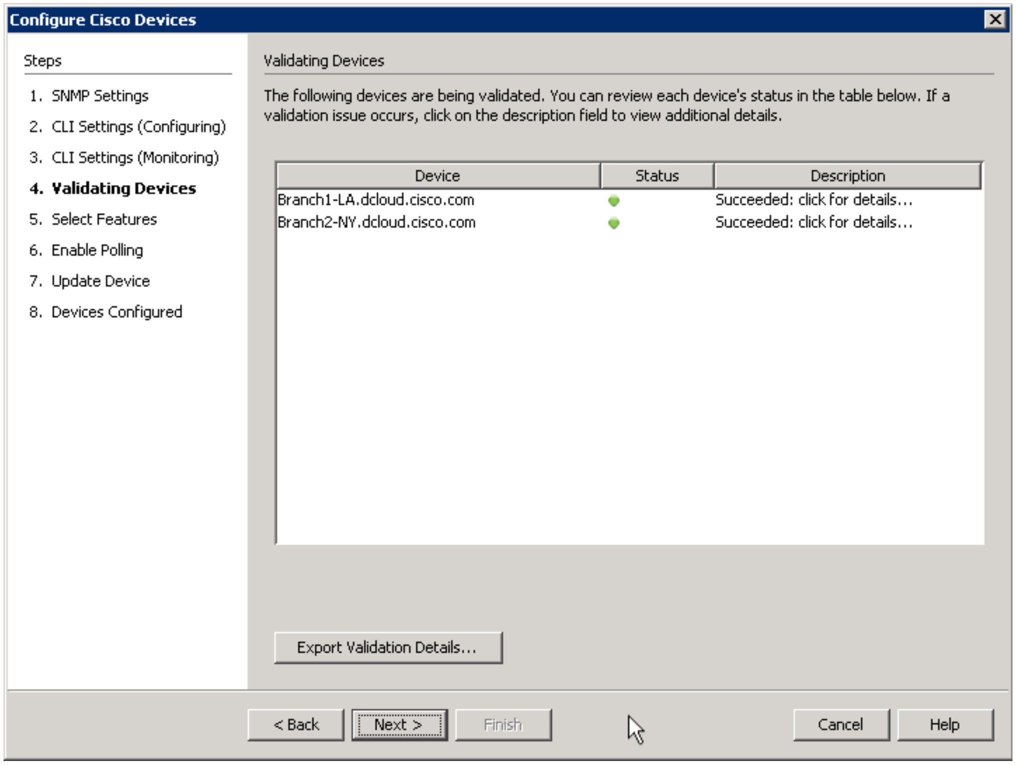
User name on Device

Password on Device*

Enable Password

11. Click Next

12. After verifying that the device validation is successful, Click Next.



Configure Cisco Devices

Steps

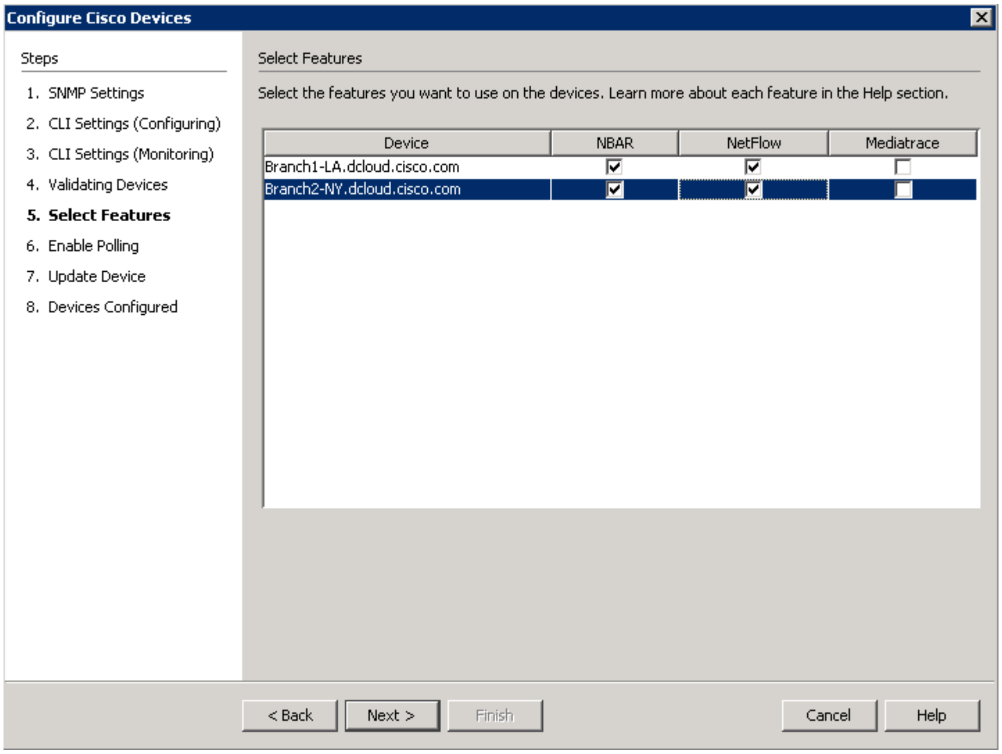
1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. **Validating Devices**
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

Validating Devices

The following devices are being validated. You can review each device's status in the table below. If a validation issue occurs, click on the description field to view additional details.

Device	Status	Description
Branch1-LA.dcloud.cisco.com	●	Succeeded: click for details...
Branch2-NY.dcloud.cisco.com	●	Succeeded: click for details...

13. Select NBAR and NetFlow for both devices, Click Next.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. **Select Features**
6. Enable Polling
7. Update Device
8. Devices Configured

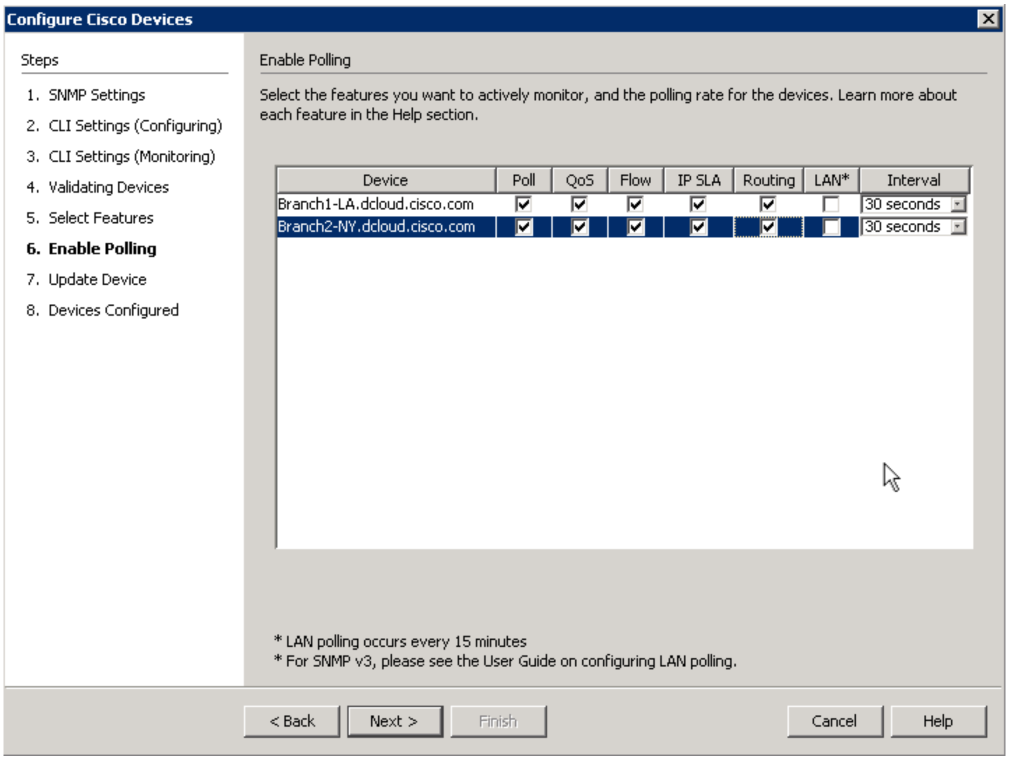
Select Features

Select the features you want to use on the devices. Learn more about each feature in the Help section.

Device	NBAR	NetFlow	Mediatrace
Branch1-LA.dcloud.cisco.com	☑	☑	□
Branch2-NY.dcloud.cisco.com	☑	☑	□

14. Select all technologies excepting LAN.

15. Set the interval to 30 seconds for each device, Click Next.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. **Enable Polling**
7. Update Device
8. Devices Configured

Enable Polling

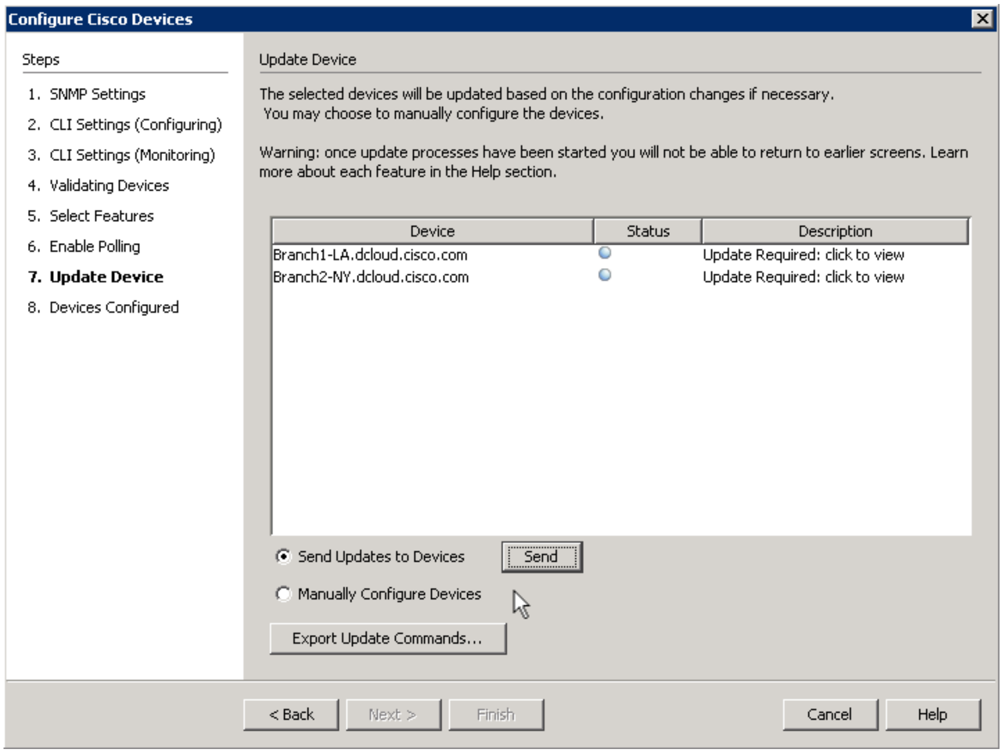
Select the features you want to actively monitor, and the polling rate for the devices. Learn more about each feature in the Help section.

Device	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval
Branch1-LA.dcloud.cisco.com	☑	☑	☑	☑	☑	□	30 seconds
Branch2-NY.dcloud.cisco.com	☑	☑	☑	☑	☑	□	30 seconds

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.

Note: For our class Labs we are gathering data every 30 seconds to reduce wait time when we make changes. In a production environment this may generate more network traffic than desired.

16. Select Send Updates to Devices and click Send.



The selected devices will be updated based on the configuration changes if necessary.
You may choose to manually configure the devices.

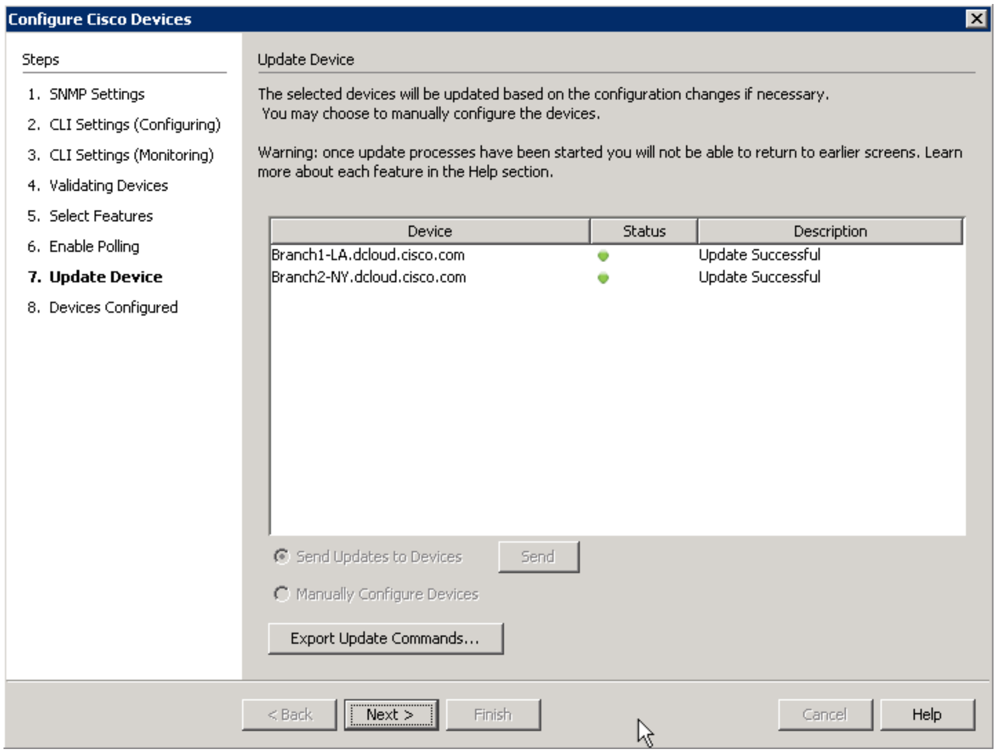
Warning: once update processes have been started you will not be able to return to earlier screens. Learn more about each feature in the Help section.

Device	Status	Description
Branch1-LA.dcloud.cisco.com	●	Update Required: click to view
Branch2-NY.dcloud.cisco.com	●	Update Required: click to view

● Send Updates to Devices

○ Manually Configure Devices

17. Once the updates are pushed successfully, click next.



The selected devices will be updated based on the configuration changes if necessary.
You may choose to manually configure the devices.

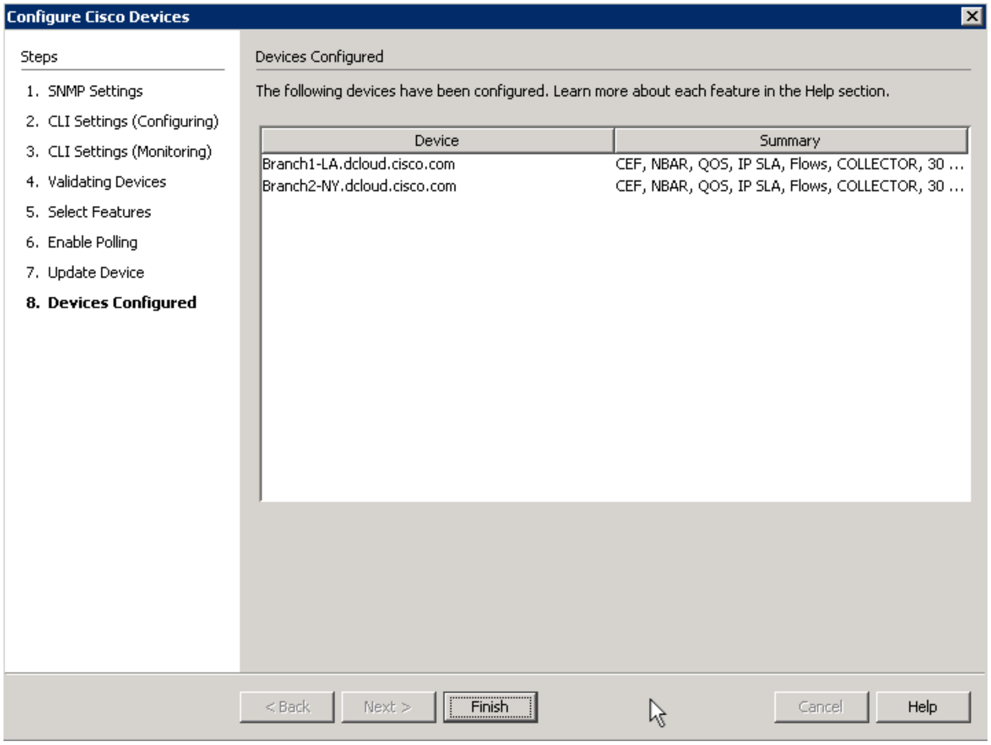
Warning: once update processes have been started you will not be able to return to earlier screens. Learn more about each feature in the Help section.

Device	Status	Description
Branch1-LA.dcloud.cisco.com	🟢	Update Successful
Branch2-NY.dcloud.cisco.com	🟢	Update Successful

● Send Updates to Devices

○ Manually Configure Devices

18. Click finish to add the devices into the topology.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. **Devices Configured**

Devices Configured

The following devices have been configured. Learn more about each feature in the Help section.

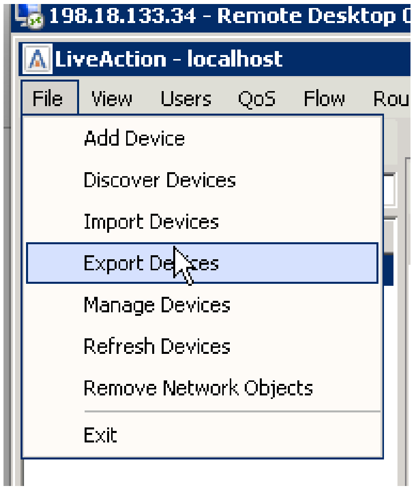
Device	Summary
Branch1-LA.dcloud.cisco.com	CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 ...
Branch2-NY.dcloud.cisco.com	CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 ...

Now that you have added three devices to the topology, they should look familiar to the image below. What is important to remember is that you should only bring in interfaces that will have interesting traffic, to you, traversing them. We will not need all the interfaces that have been included, so in one of the next Labs we'll remove the unneeded interfaces.

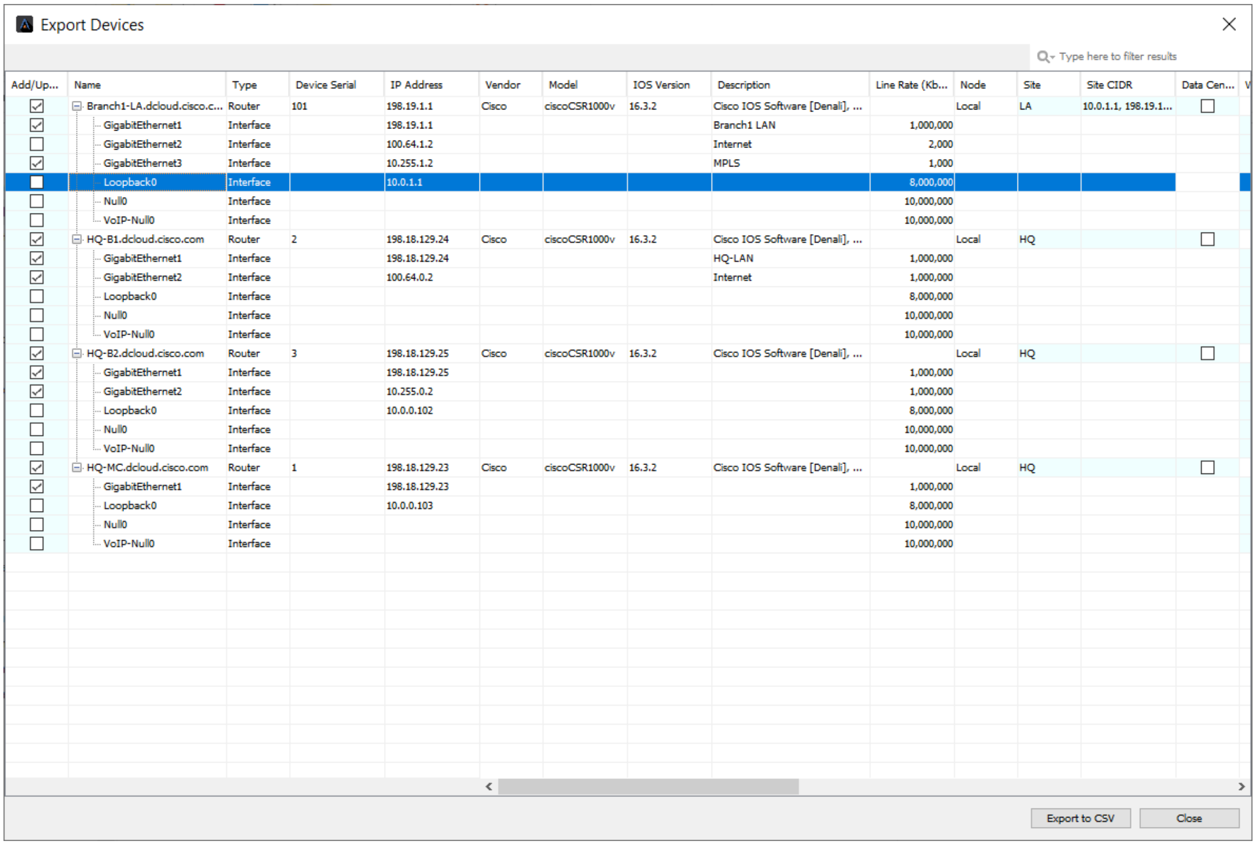
Lab A.3: Export/Import Device Configuration

Lab Steps:

1. From the File Menu select Export Devices.



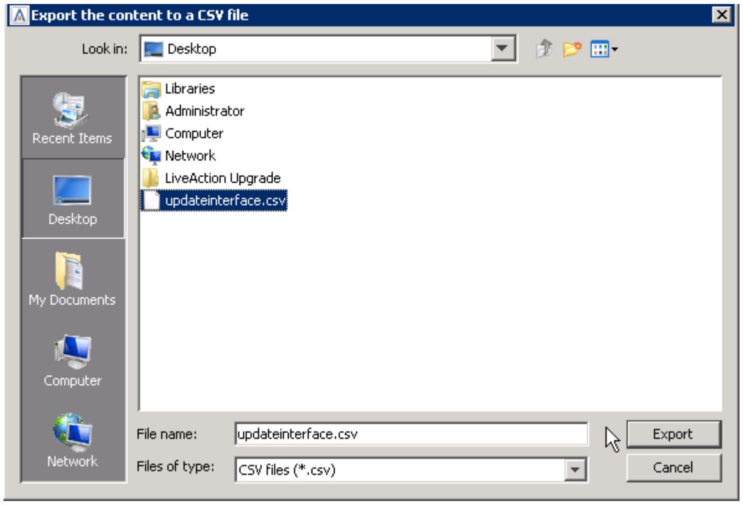
2. Deselect **GigabitEthernet2** and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.



Add/Up...	Name	Type	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (Kb...	Node	Site	Site CIDR	Data Cen...	V
☑	⊟ Branch1-LA.dcloud.cisco.c...	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	LA	10.0.1.1, 198.19.1...	☐	
☑	GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000					
☐	GigabitEthernet2	Interface		100.64.1.2				Internet	2,000					
☑	GigabitEthernet3	Interface		10.255.1.2				MPLS	1,000					
☐	Loopback0	Interface		10.0.1.1					8,000,000					
☐	Null0	Interface							10,000,000					
☐	VoIP-Null0	Interface							10,000,000					
☑	⊟ HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		☐	
☑	GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000					
☑	GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000					
☐	Loopback0	Interface							8,000,000					
☐	Null0	Interface							10,000,000					
☐	VoIP-Null0	Interface							10,000,000					
☑	⊟ HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		☐	
☑	GigabitEthernet1	Interface		198.18.129.25					1,000,000					
☑	GigabitEthernet2	Interface		10.255.0.2					1,000,000					
☐	Loopback0	Interface		10.0.0.102					8,000,000					
☐	Null0	Interface							10,000,000					
☐	VoIP-Null0	Interface							10,000,000					
☑	⊟ HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		☐	
☑	GigabitEthernet1	Interface		198.18.129.23					1,000,000					
☐	Loopback0	Interface		10.0.0.103					8,000,000					
☐	Null0	Interface							10,000,000					
☐	VoIP-Null0	Interface							10,000,000					

3. Select Export to csv.

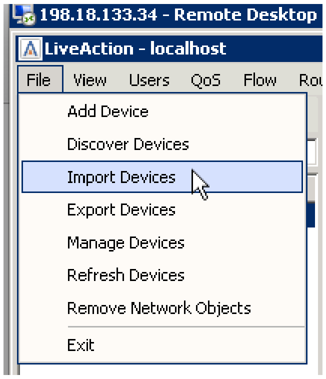
4. On the Export window give the file a name.
5. Export the csv to the desktop, or appropriate directory.



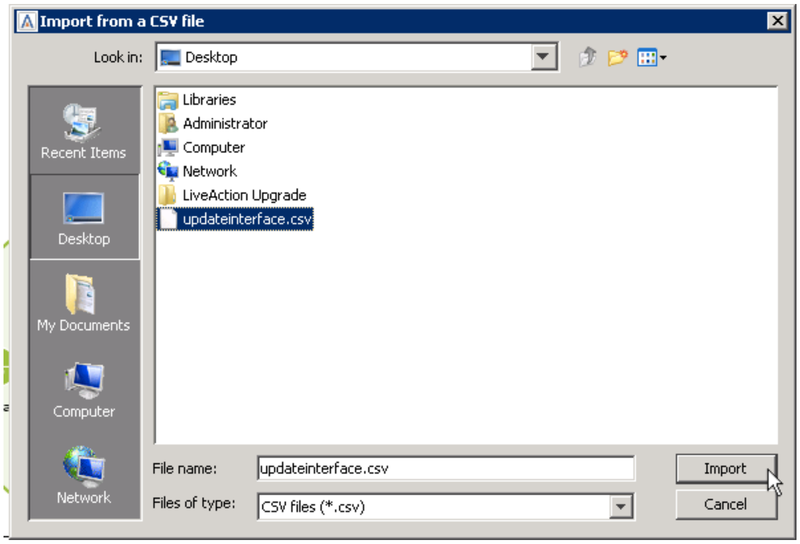
File name: updateinterface.csv

Files of type: CSV files (*.csv)

6. Close the export devices window.
7. Select File and Import Devices.



8. Select the file you previously exported.



Import from a CSV file

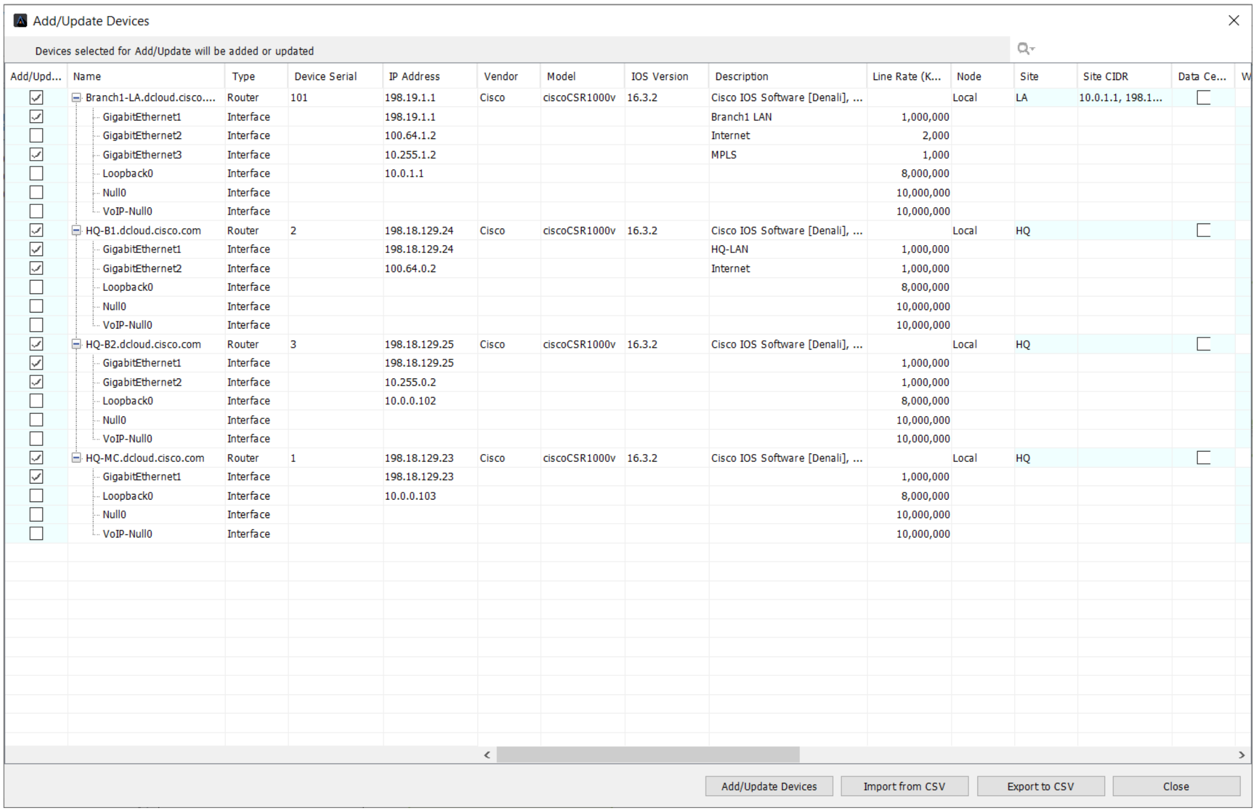
Look in: Desktop

- Libraries
- Administrator
- Computer
- Network
- LiveAction Upgrade
- updateinterface.csv

File name: updateinterface.csv

Files of type: CSV files (*.csv)

9. Click Add/Update Devices.

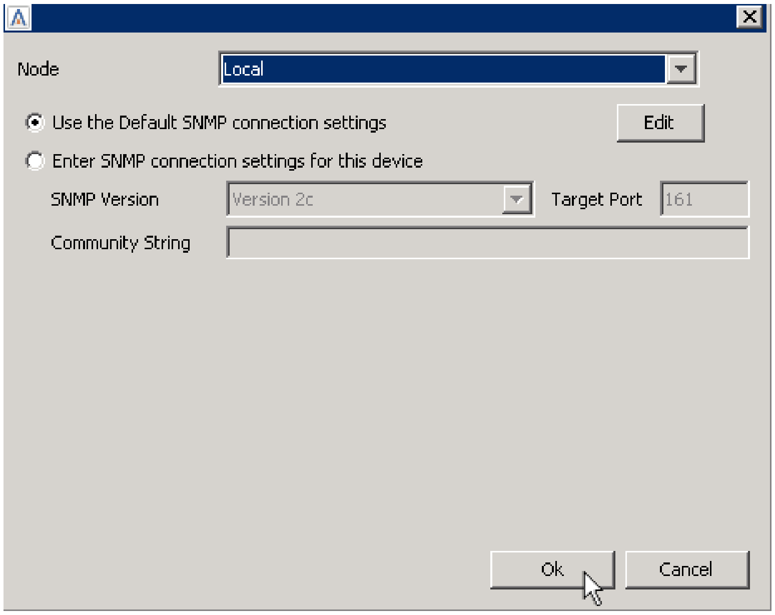


Add/Update Devices

Devices selected for Add/Update will be added or updated

Add/Upd...	Name	Type	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K...	Node	Site	Site CIDR	Data Ce...	W
☑	Branch1-LA.dcloud.cisco....	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	LA	10.0.1.1, 198.1...	□	
☑	GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000					
□	GigabitEthernet2	Interface		100.64.1.2				Internet	2,000					
☑	GigabitEthernet3	Interface		10.255.1.2				MPLS	1,000					
□	Loopback0	Interface		10.0.1.1					8,000,000					
□	Null0	Interface							10,000,000					
□	VoIP-Null0	Interface							10,000,000					
☑	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		□	
☑	GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000					
☑	GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000					
□	Loopback0	Interface							8,000,000					
□	Null0	Interface							10,000,000					
□	VoIP-Null0	Interface							10,000,000					
☑	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		□	
☑	GigabitEthernet1	Interface		198.18.129.25					1,000,000					
☑	GigabitEthernet2	Interface		10.255.0.2					1,000,000					
□	Loopback0	Interface		10.0.0.102					8,000,000					
□	Null0	Interface							10,000,000					
□	VoIP-Null0	Interface							10,000,000					
☑	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		□	
☑	GigabitEthernet1	Interface		198.18.129.23					1,000,000					
□	Loopback0	Interface		10.0.0.103					8,000,000					
□	Null0	Interface							10,000,000					
□	VoIP-Null0	Interface							10,000,000					

10. Click OK to use the Default SNMP settings.



Node: Local

● Use the Default SNMP connection settings

○ Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port: 161

Community String:

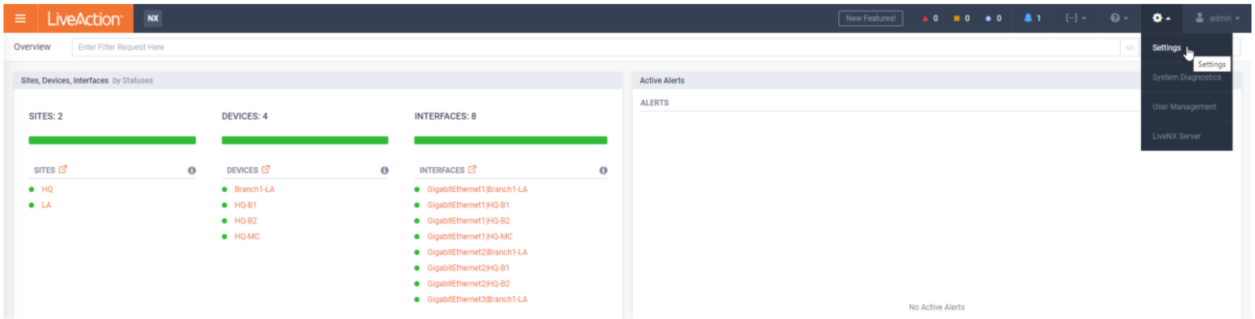
Your Topology Pane will now show the appropriate devices/configurations.

Lab A.4: Saving Server Configurations

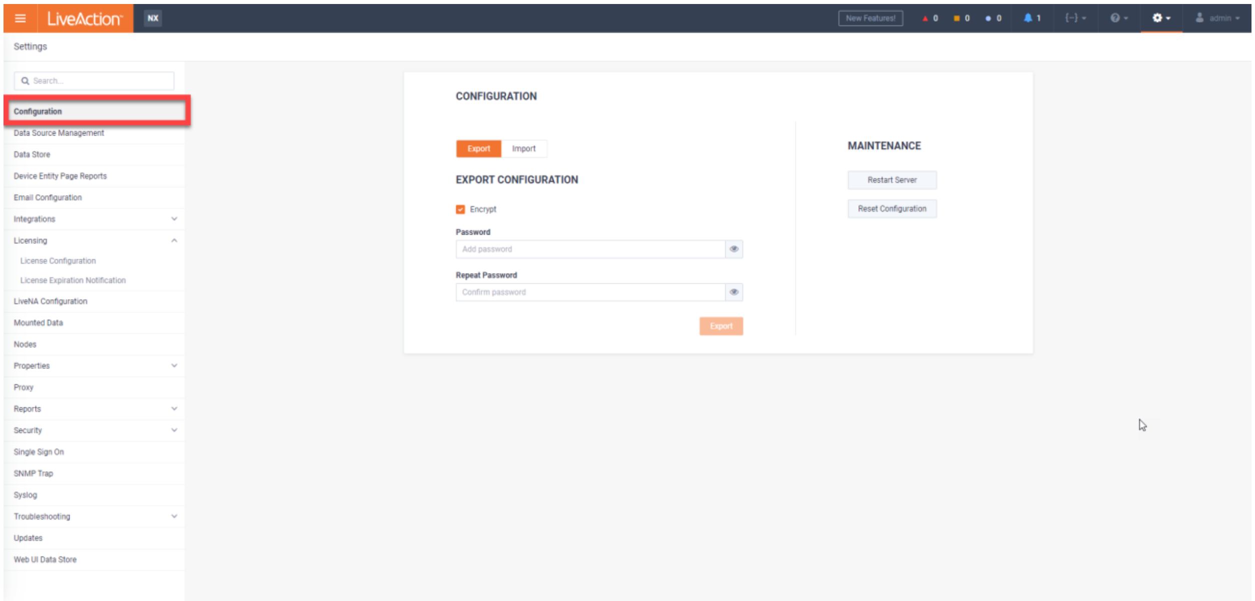
Prior to upgrading the LiveAction Software, or to retain existing Server configuration for use in the case of a hardware failure or misconfiguration, the current configuration file may be Exported to a local or network drive.

Lab Steps:

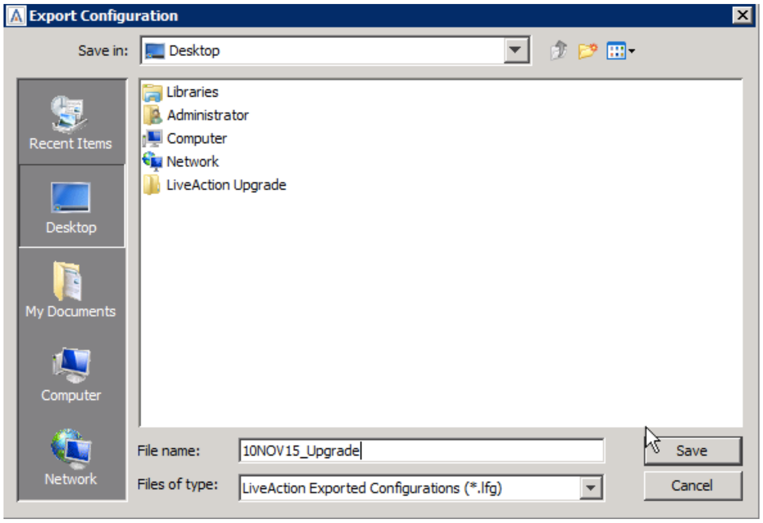
1. Open the LiveNX WebUI, select **Settings**.



2. Select **Configuration**.



3. Click **Export**.
4. Enter encryption password if preferred.



Export Configuration

Save in: Desktop

File name: 10NOV15_Upgrade

Files of type: LiveAction Exported Configurations (*.lfg)

5. Select an appropriate place to save the file, give the file a name, then click Save.

Lab A.5: Connect via Remote Desktop Connection

A direct connection from the LiveNX Client installed on your workstation is the most efficient method to connect, but you may use RDC as an *alternate* way to connect to your Student Pod. SKIP this Lab if directly connecting with the LiveNX Client on your local workstation.

To connect using Microsoft Remote Desktop on Windows, or a compatible Remote Desktop client on Linux and Macintosh, follow the steps below. On Windows you can typically find Remote Desktop in START > ALL PROGRAMS > ACCESSORIES.

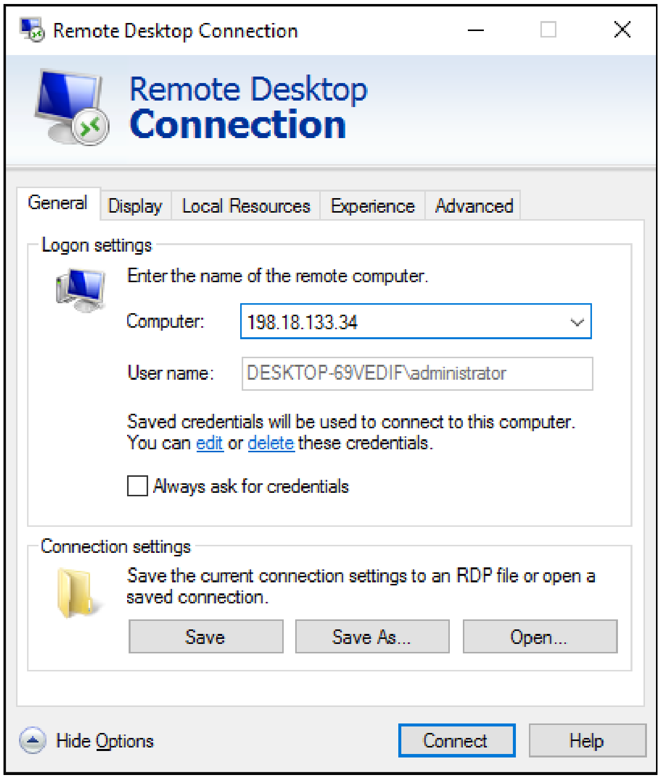
Note: Use the information from the Lab Details table to connect to the desired device.

Lab Steps:

Connect to the virtual Windows Workstation Desktop using the IP Address, username, and password pre-printed on the Class Worksheet, unless otherwise instructed.

6. Launch a Remote Desktop Connection.
7. BEFORE selecting Connect, click the General tab. (On Macintosh this will be the Preferences menu and Login tab.)

DIAGRAM



Enter the name of the remote computer.

Computer: 198.18.133.34

User name: DESKTOP-69VEDIF\administrator

Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

□ Always ask for credentials

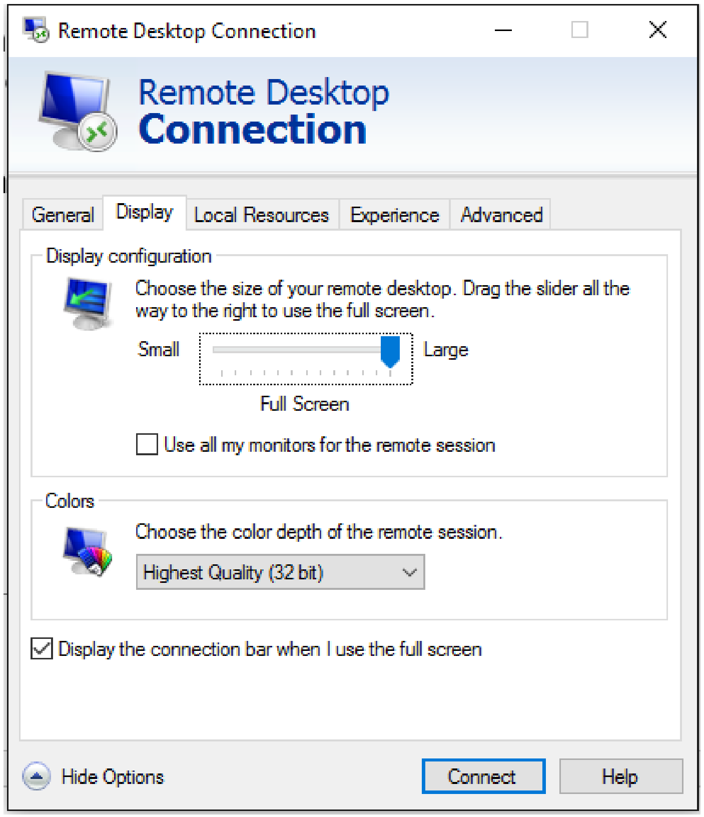
Save the current connection settings to an RDP file or open a saved connection.

   a. Enter the following fields:
      •Computer: **<ipaddress> :20201**
      (From your Lab Access worksheet)
      •Username: **administrator** (or otherwise defined by instructor)

8. Set the RDC session properties on the Display tab so that your video is a minimum of 1200x800 resolution… this may NOT be changed once the connection is active. See next page for example.

✓

DIAGRAM



Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Small — Large

Full Screen

□ Use all my monitors for the remote session

Colors

Choose the color depth of the remote session.

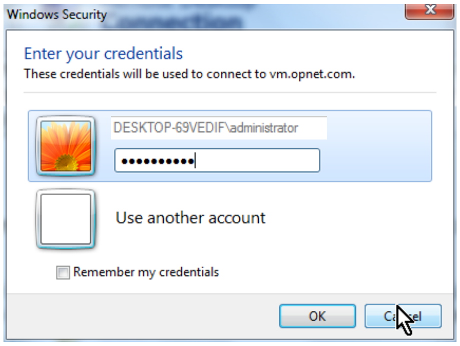
Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

9. Select Connect.

10. Enter the workstation password: **C1sco12345** (or otherwise defined by instructor).

DIAGRAM



Enter your credentials

These credentials will be used to connect to vm.opnet.com.

DESKTOP-69VEDIF\administrator

••••••••••

Use another account

□ Remember my credentials

11. Click OK.

Once successfully connected to your Pod you will see the Windows Desktop, and be able to access the LiveNX Server, Client, and other pod resources.

Note: Occasionally Remote Desktop may freeze its connection to the Pod workstation. If this happens, close the Remote Desktop window, and start again at Step 1 above. This will continue your lab session and will generally not lose any work.