



# LiveAction Training

*Lab Workbook Pt. 1*



© Copyright 2021, LiveAction, Inc.

All rights reserved. This product and related documentation are protected by copyright and distribution under licensing restricting their use, copy and distribution. No part of this document may be used or reproduced in any form or by any means, or stored in a database or retrieval system, without prior written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Making copies of any part of this Training Material for any other purpose is in violation of United States copyright laws.

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.

**Trademarks:**

LiveAction, its marks and logos, are registered trademarks of LiveAction, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

All other products or services mentioned herein are trademarks or registered trademarks of their respective owners.

Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

2021-Aug.

# Table of Contents

Table of Contents .....	4
<b>Lab 0: Setup and Get Connected</b> .....	6
Lab 0.1: Connect to the Lab Network .....	7
Lab 0.2: Connecting to Your Training Pod .....	9
Lab 0.3: Install the LiveNX Client .....	11
<b>Lab 1: The LiveNX Web UI</b> .....	12
Lab 1.1: Explore the Web UI .....	13
Lab 1.2: Create a Custom Dashboard .....	18
Lab 1.3: Pre-Configured Stories .....	20
Lab 1.4: WebUI Reports .....	22
Lab 1.5: Enable / Customize Alerts .....	26
Lab 1.6: Add a User Account .....	29
Lab 1.7: View and Navigate System Diagnostics .....	30
Lab 1.8: Support and Troubleshooting .....	33
<b>Lab 2: The LiveNX Client</b> .....	36
Lab 2.1: Launch the LiveNX Client .....	37
Lab 2.2: Explore the LiveNX Client .....	39
<b>Lab 3: Configuring Devices</b> .....	41
Lab 3.1: Add Device .....	42
Lab 3.2: Manage & Configure Devices .....	44
Lab 3.3: Configure Flow on Devices .....	49
Lab 3.4: Add/Remove Interfaces .....	52
Lab 3.5: Merge Clouds in Topology .....	54
<b>Lab 4: Traffic Flows</b> .....	57
Lab 4.1: Discover Flows .....	58
Lab 4.2: Discover Specific Flows .....	60
Lab 4.3: Examine Specific Traffic .....	61
Lab 4.4: Troubleshoot Issues .....	63
<b>Lab 5: Filtering, Identifying, Marking</b> .....	65
Lab 5.1: Creating Custom Filters .....	66
Lab 5.2: ACL Creation .....	71
<b>Lab 6: Making the Topology Work</b> .....	79
Lab 6.1: Setting Device Semantics .....	80
Lab 6.2: Adding Devices to Groups .....	85
Lab 6.3: Creating Network Objects .....	90
<b>Lab 7: Dashboards &amp; Reports</b> .....	95
Lab 7.1: The Dashboard .....	96
Lab 7.2: Viewing Reports .....	100
Lab 7.3: Create a Custom Report .....	106
<b>Lab 8: QoS</b> .....	108
Lab 8.1: QoS Marking Policy .....	109
Lab 8.2: QoS Queueing Policy .....	121
Lab 8.3: QoS Verification .....	131
<b>Lab A: Appendix</b> .....	137
Lab A.1: Add Device .....	138
Lab A.2: Client Device Discovery .....	144
Lab A.3: Export/Import Device Configuration .....	152
Lab A.4: Saving Server Configurations .....	156
Lab A.5: Connect via Remote Desktop Connection .....	158



## 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:

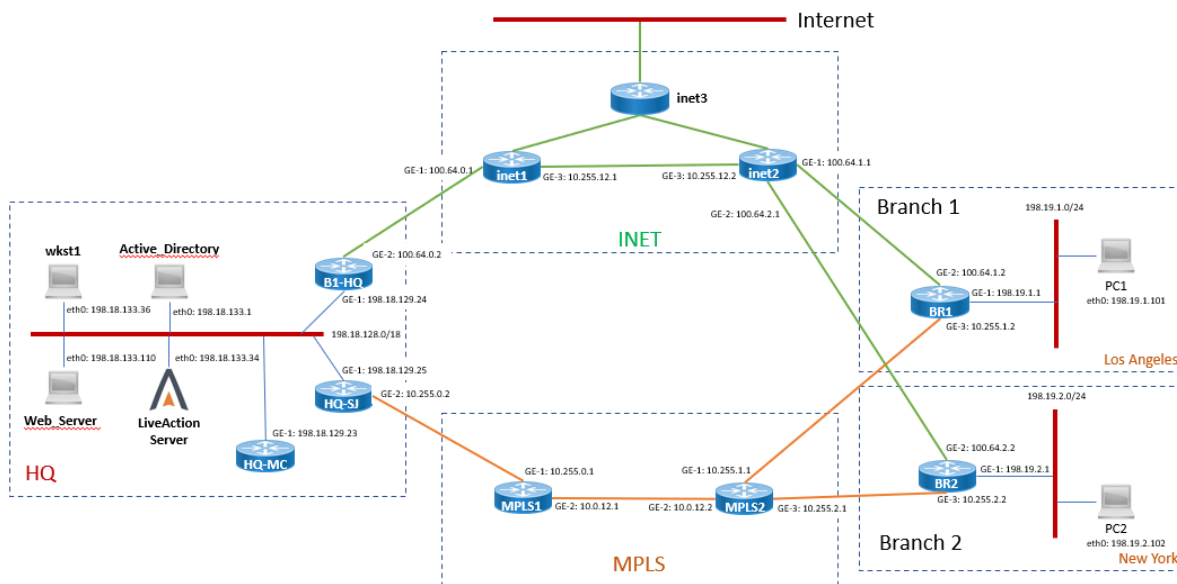
Local:

- 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

The screenshot shows the 'Lab Details' tab of a web application. On the left is a sidebar with a 'Learning Labs Menu' containing 'Overview', 'Labs Introduction', and 'Access Devices'. The main area displays a table of lab devices. At the top, it shows 'Lab Status: READY' and 'Time Left: 8 DAYS 4 HOURS'. The table has columns for 'Sl No', 'Role', 'Hostname', 'Username', 'Password', 'IP Address', and 'Port'.

Sl No	Role	Hostname	Username	Password	IP Address	Port
1	Liveaction	livenx	admin	Student	35.231.127.249	443
2	B1-HQ	HQ-B1	admin	Cisco12345	35.231.127.249	20019
3	inet1	INET1	admin	Cisco12345	35.231.127.249	20018
4	inet2	INET2	admin	Cisco12345	35.231.127.249	20020
5	inet3	INET3	admin	Cisco12345	35.231.127.249	20021
6	BR1	Branch1-LA	admin	Cisco12345	35.231.127.249	20001
7	B2-HQ	HQ-B2	admin	Cisco12345	35.231.127.249	20022
8	MPLS1	MPLS1	admin	Cisco12345	35.231.127.249	20010
8	MPLS2	MPLS2	admin	Cisco12345	35.231.127.249	20009
9	BR2	Branch2-NY	admin	Cisco12345	35.231.127.249	20000
10	wkst1	Administrator	Administrator	Cisco12345	35.231.127.249	20201
11	Activedirectory	Administrator	Administrator	Cisco12345	35.231.127.249	20202
12	PC1	Administrator	Administrator	Cisco12345	35.231.127.249	20203
13	PC2	Administrator	Administrator	Cisco12345	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](http://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.

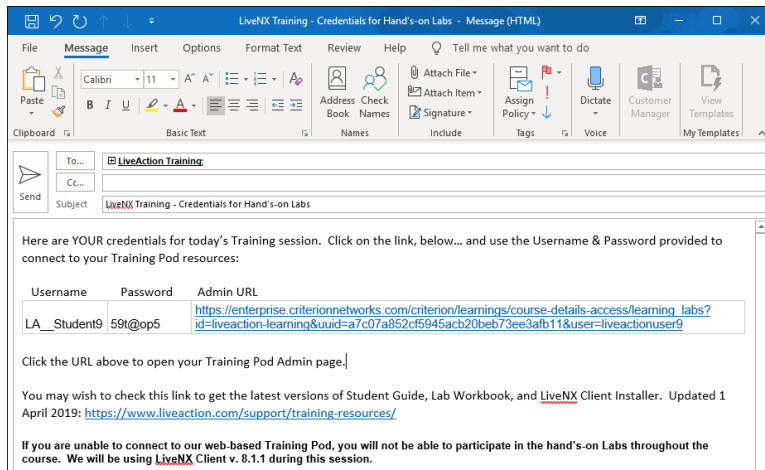
---

# 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



## 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**.

Learning Labs Menu

Overview

Labs Introduction

Access Devices

Lab Status : ✓ READY

Time Left : 8 DAYS 4 HOURS

Topology

Lab Details

Sl No	Role	Hostname	Username	Password	IP Address	Port
1	Liveaction	livenx	admin	Student	35.231.127.249	443
2	B1-HQ	HQ-B1	admin	Cisco12345	35.231.127.249	20019
3	inet1	INET1	admin	Cisco12345	35.231.127.249	20018
4	inet2	INET2	admin	Cisco12345	35.231.127.249	20020
5	inet3	INET3	admin	Cisco12345	35.231.127.249	20021
6	BR1	Branch1-LA	admin	Cisco12345	35.231.127.249	20001
7	B2-HQ	HQ-B2	admin	Cisco12345	35.231.127.249	20022
8	MPLS1	MPLS1	admin	Cisco12345	35.231.127.249	20010
8	MPLS2	MPLS2	admin	Cisco12345	35.231.127.249	20009
9	BR2	Branch2-NY	admin	Cisco12345	35.231.127.249	20000
10	wkst1	Administrator	Administrator	Cisco12345	35.231.127.249	20201
11	Activedirectory	Administrator	Administrator	Cisco12345	35.231.127.249	20202
12	PC1	Administrator	Administrator	Cisco12345	35.231.127.249	20203
13	PC2	Administrator	Administrator	Cisco12345	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.

---

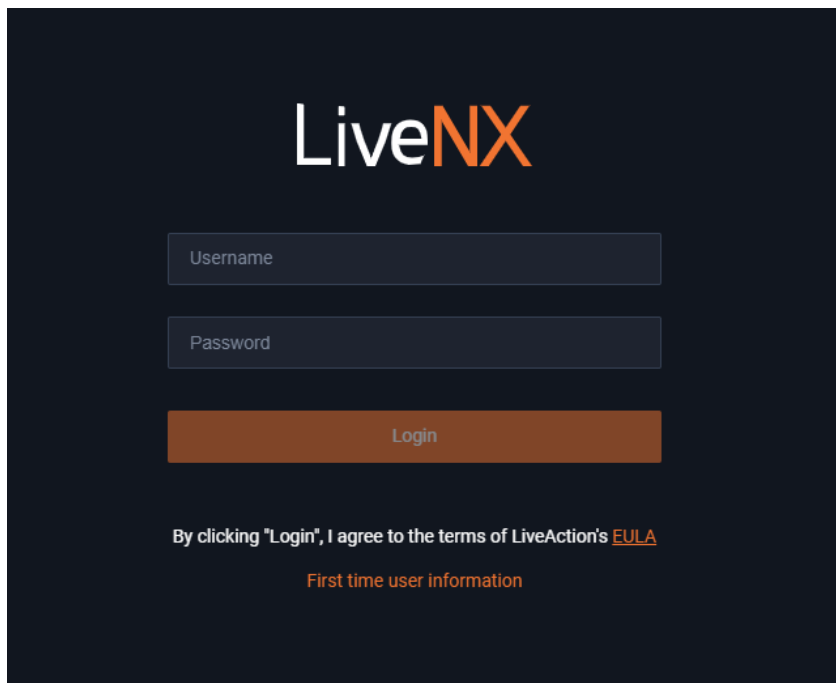
**Note:** The displays in these UI labs will vary, depending upon how long your Pod has been running, as well as the variety of traffic. These labs are meant to illustrate *how* to get at the information... results are not important. Diagrams are for illustration purposes and may not reflect the data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



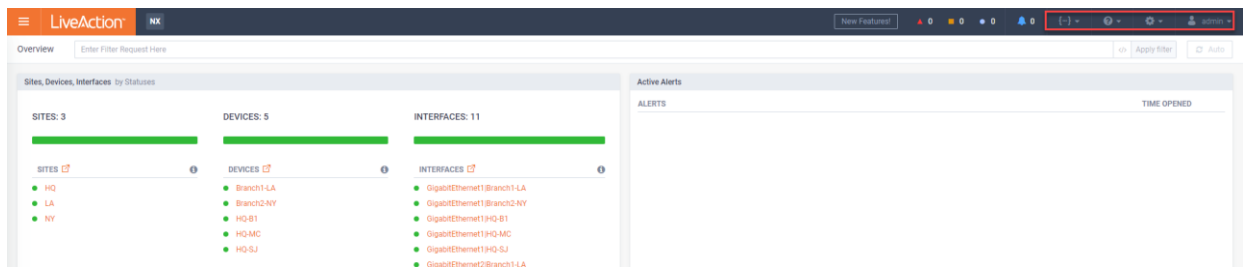
The Overview screen will appear.

---

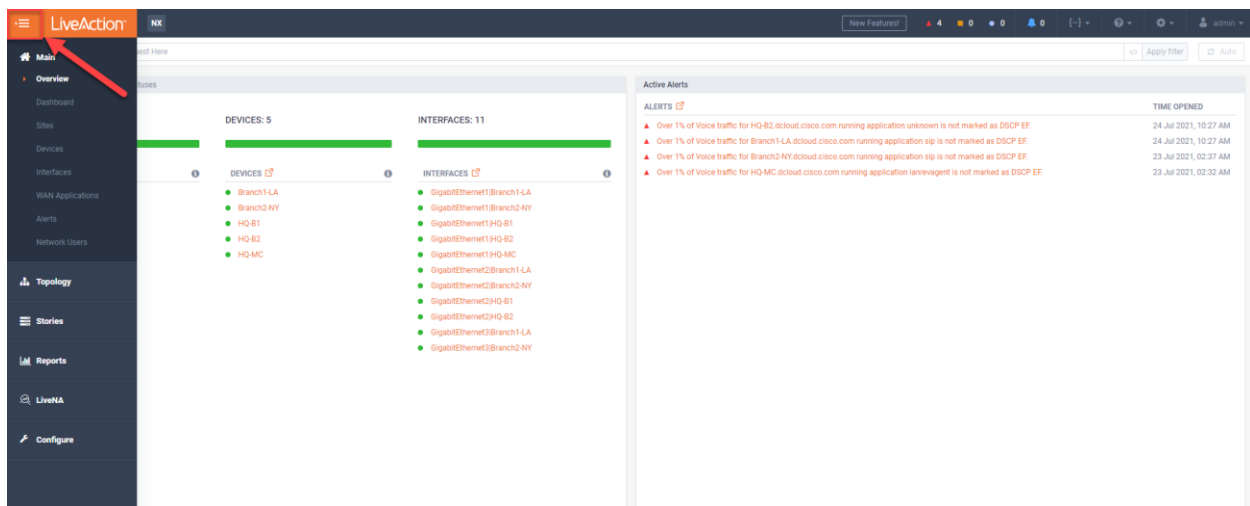
**Note:** The contents of this screen may change dependent upon the *version* of LiveNX being run.

---

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



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



5. Select **Sites**.

The screenshot shows the LiveAction Sites page. It features a table with columns for Site Name, Site Status, Service Reachability, Device CPU/Memory, Peak Utilization In, Peak Utilization Out, Congestion Drops, and Interface Errors. The table lists three sites: HQ, LA, and NY. The 'Auto' toggle is set to ON.

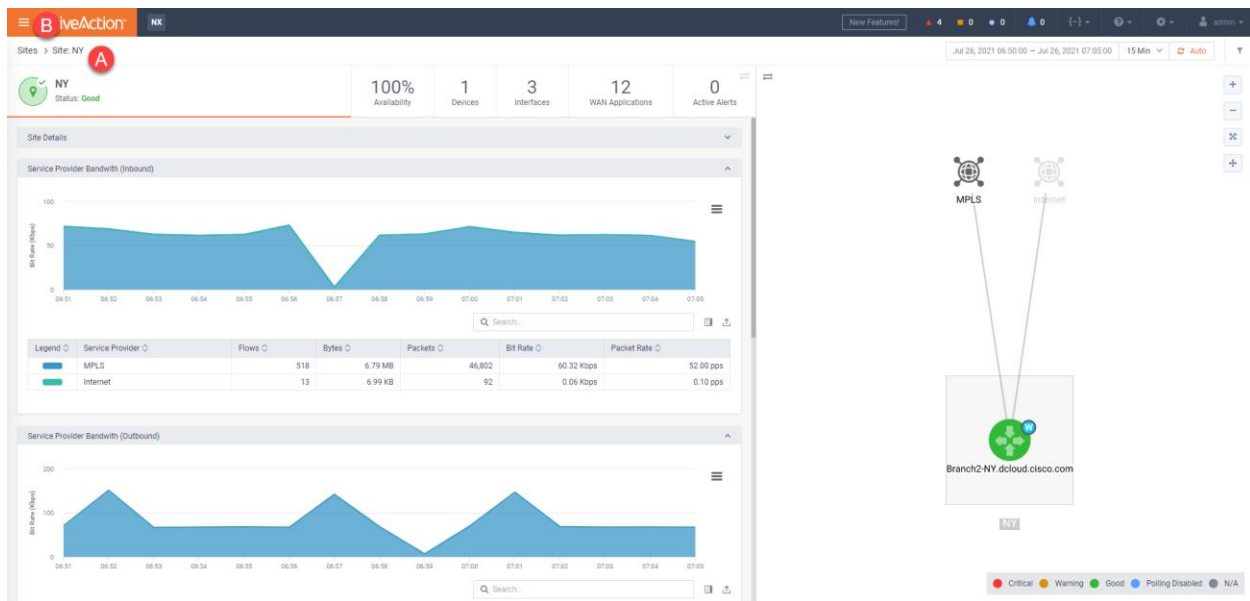
SITE NAME	SITE STATUS	SERVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION DROPS	INTERFACE ERRORS
HQ	●	●	●	4.65%	34.28%	●	0
LA	●	●	●	27.22%	0.01%	●	0
NY	●	●	●	4.57%	10.13%	●	0

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

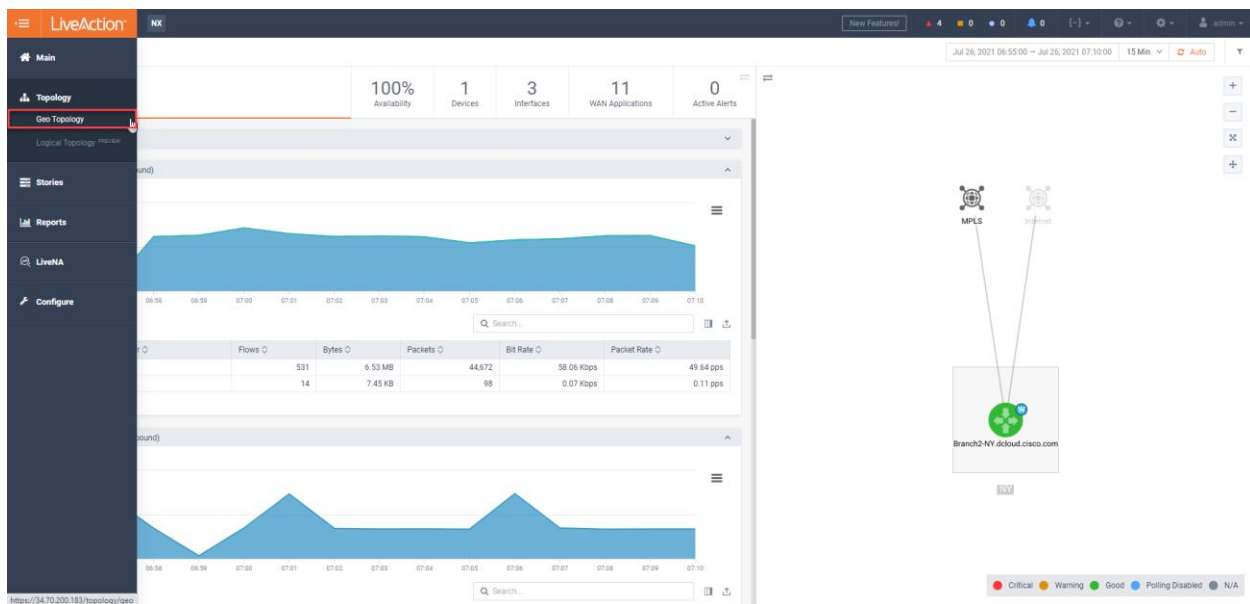
**Note:** Detailed site information is specified in the *Device Semantics* Lab.

- Note: Status, Utilization, Drops, Errors, etc....
- Toggle the **Auto Update** to ON.
- Click on the link to **Los\_Angeles** to see additional site info.

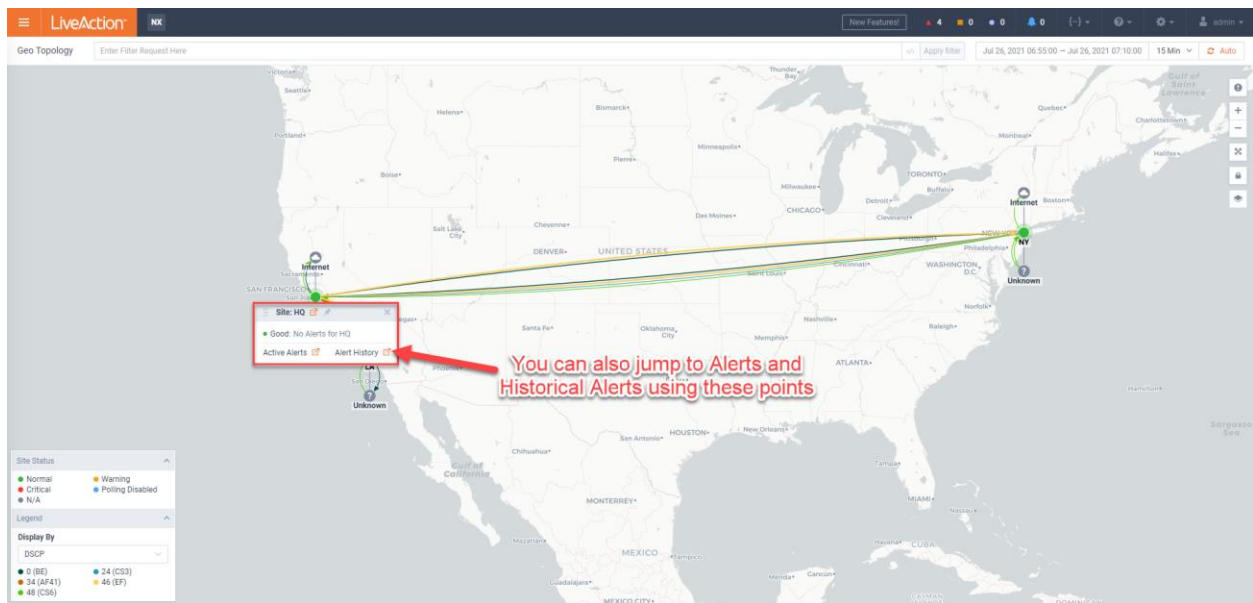
Anytime you wish to return to a prior level, or the WebUI home, you can click the Breadcrumbs (A) or Menu icon (B).



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



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



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

12. Select **Device Management**.

The screenshot displays the LiveAction NX Device Management web interface. At the top, there's a navigation bar with the LiveAction logo and a 'Menu' button. Below the navigation bar, the 'Device Management' section is active, showing a table of devices. The table has columns for Device, Device State, IP Address, Vendor, Model, Node, Site, Interfaces, Hardcoded, Poll, QOS, Flow, IP SLA, Routing, LAN, and Tags. Four devices are listed: HQ-MC, HQ-B1, Branch1-LA, and HQ-B2, all with a state of 'Up'. The interface also includes buttons for 'Discover Devices', 'Add Non SNMP Device', 'View Devices', 'Credential Store', and 'CSV Import/Export'.

DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	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.

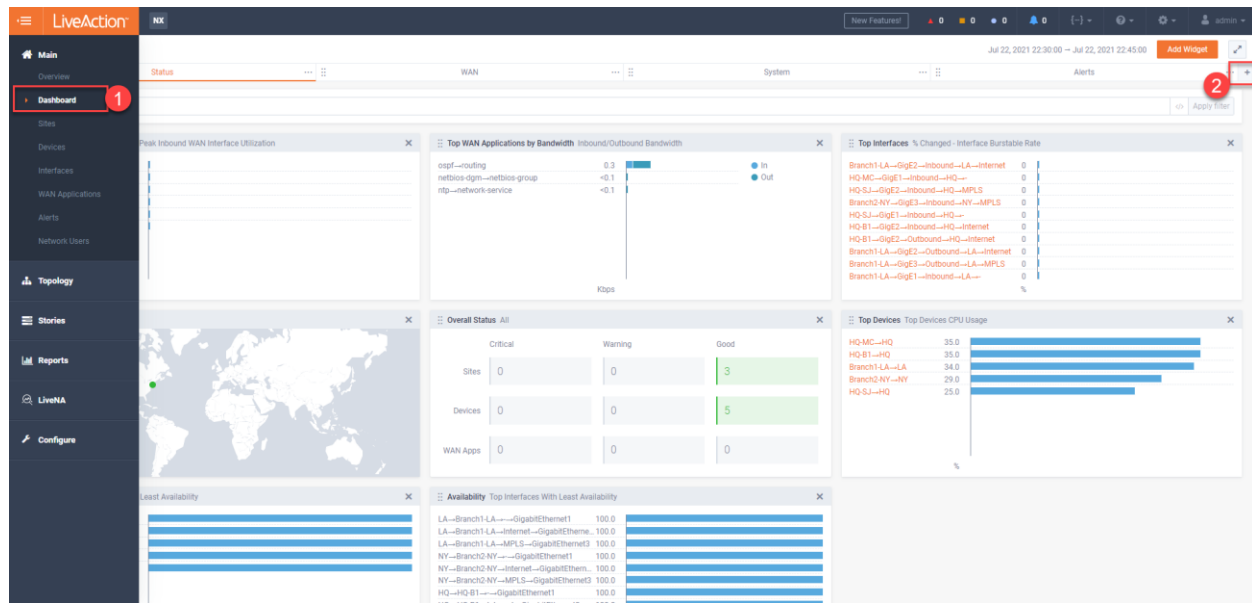
# Lab 1.2: Create a Custom Dashboard

**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.

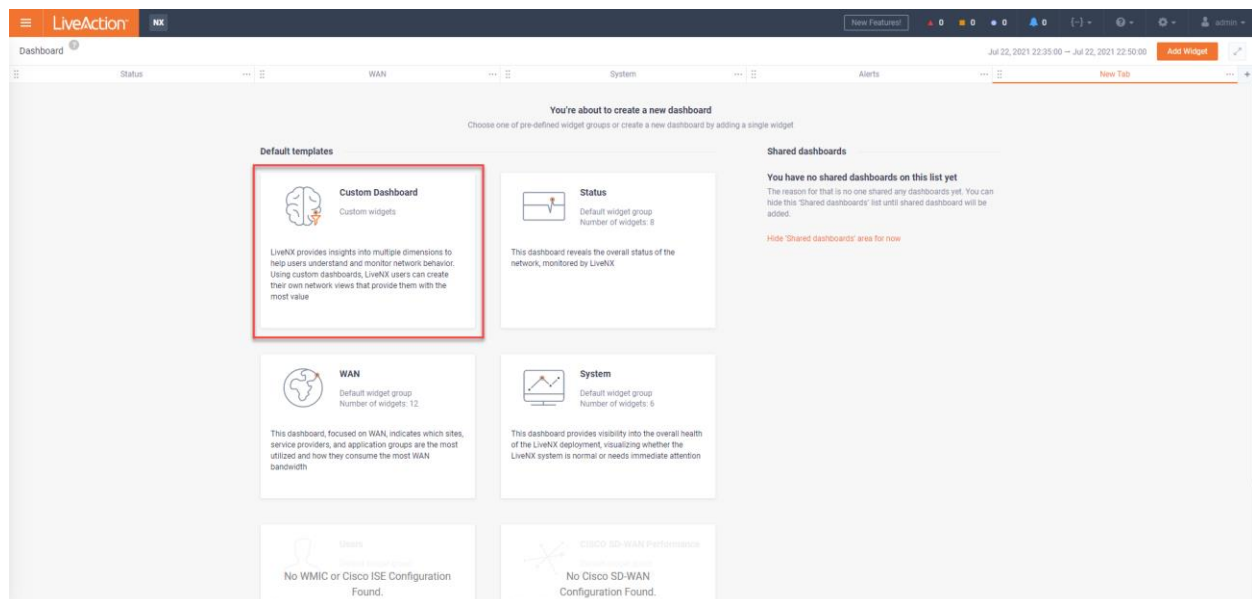
In this Lab you will Create and Modify your own Custom Dashboard.

Lab Steps:

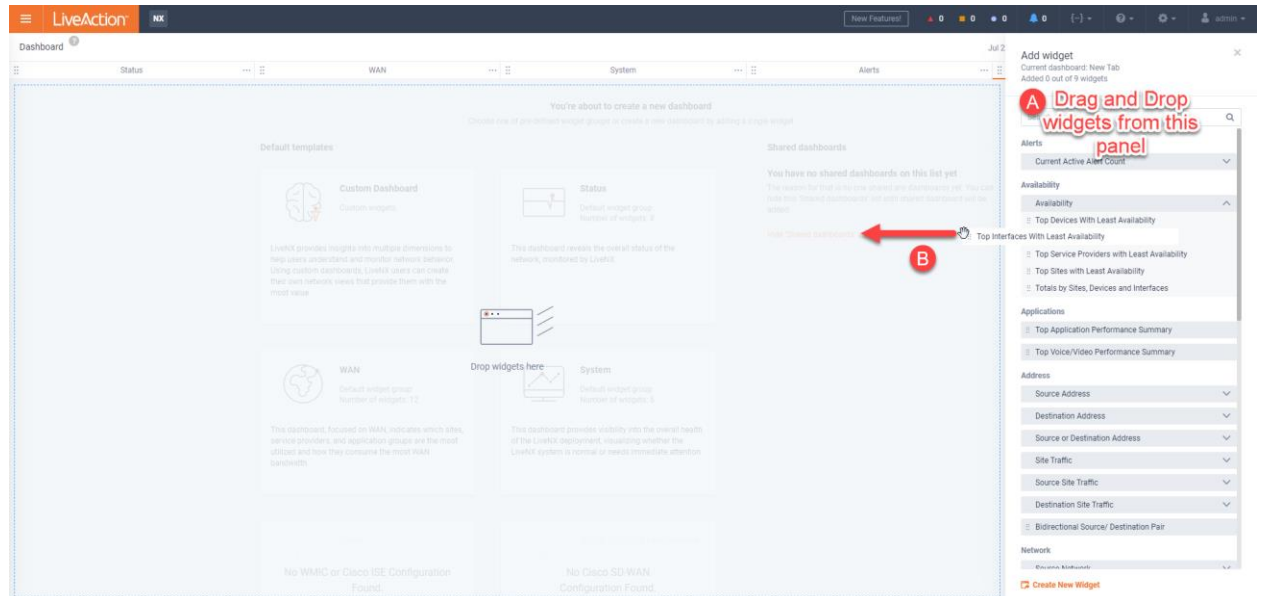
1. From the **Main** menu, click on **Dashboard** (1), then click on the **+** icon (2) to create a new tab in the dashboard space Dashboard. This will appear as “New Tab”.



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

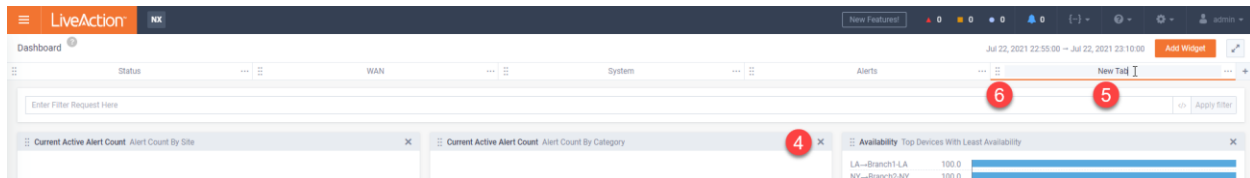


- Some options can be expanded to show more details, while others can be directly dragged to the dashboard. Drag-and-drop (A) or click + to add Widgets to your custom dashboard.



**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.

- Delete** un-wanted Widgets by clicking the **X** at top right of the widget.
- To give the dashboard tab a more appropriate name, simply select the **New Tab** text and rename your dashboard.
- You can also change the order



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

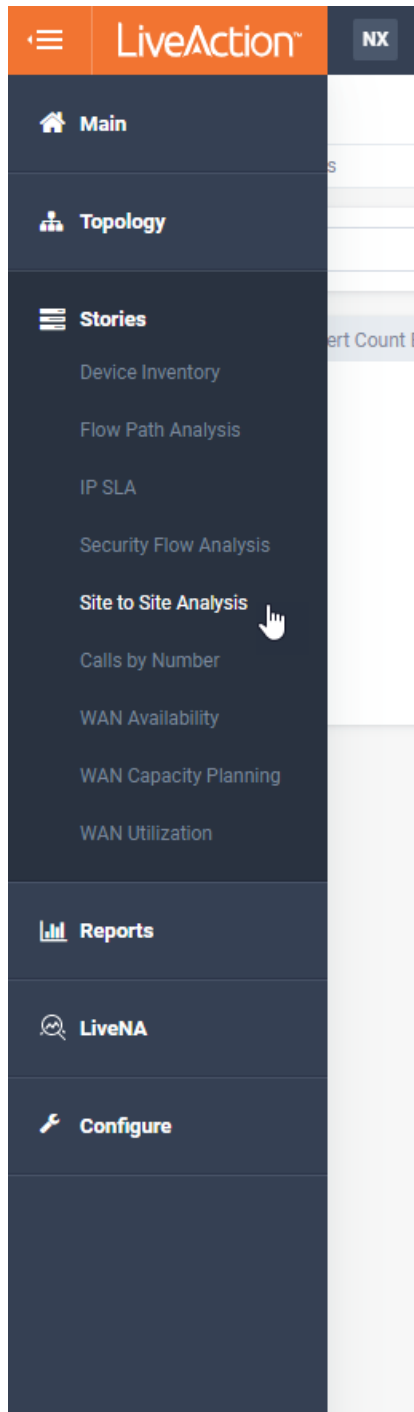
**Note:** Since LiveNX stores *breadcrumbs* it will retain a trail of the last page you've visited in the WebUI, based-upon your individual login credentials. Unless shared... Your custom Dashboard will not be visible to others.

## 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**.



---

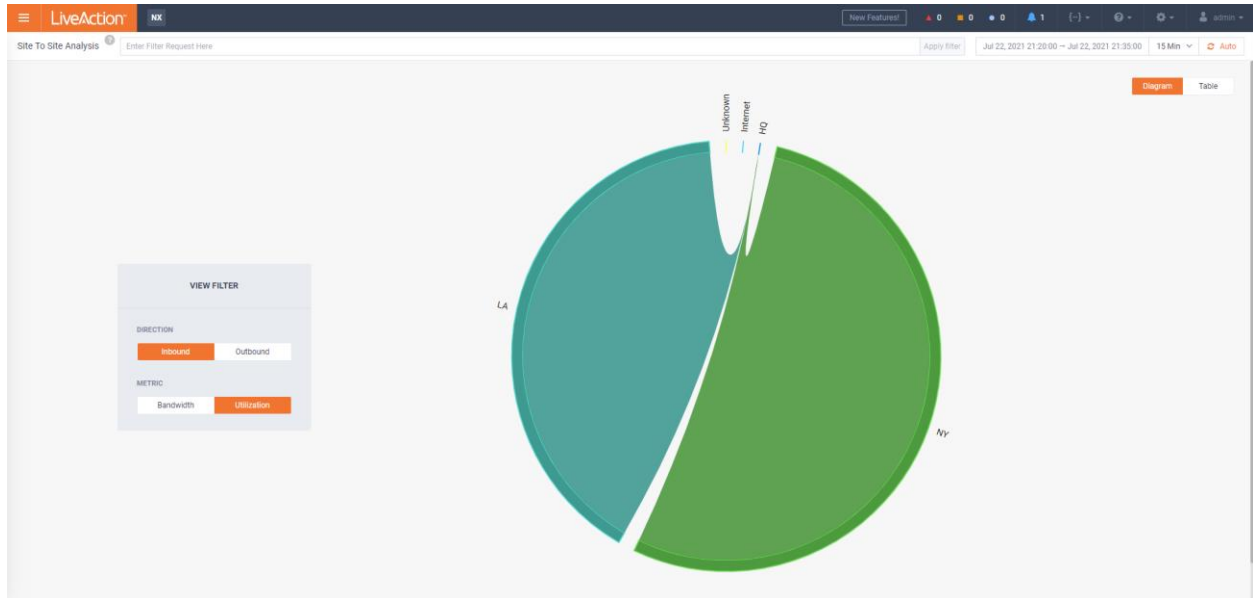
**Note:** Diagrams are for illustration purposes and may not reflect the data in your Training Pod. These labs are meant to illustrate *how* to get at the information.

---

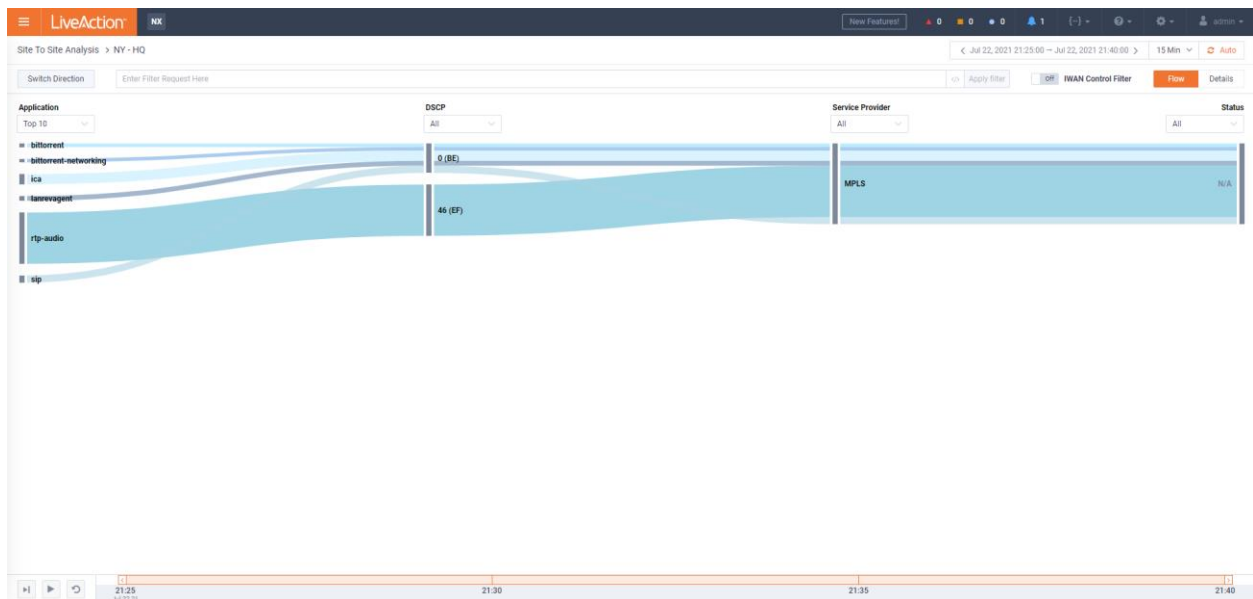


### 3. Select **Direction > Inbound**.

#### DIAGRAM



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



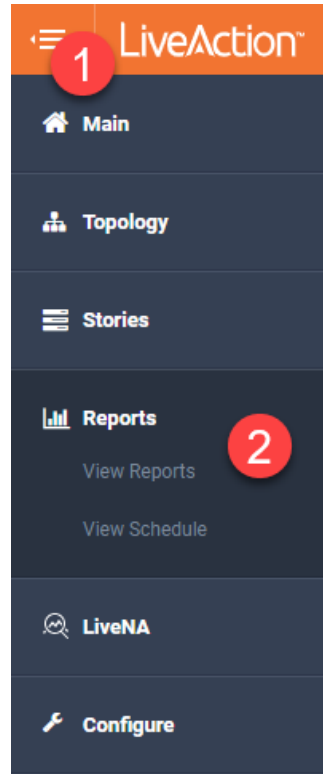
View the other pre-configured Stories to discover how they may help you with Capacity Planning, Inventory, and Network Management.

# 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**

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 conversations, 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/Runt/Overruns, etc.) per the specified filter.
Top Class Bandwidth	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/ Runt/ 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.

**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

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

**Bin Duration**  
1 Minute

**Display Filter**  
No Display Filtering

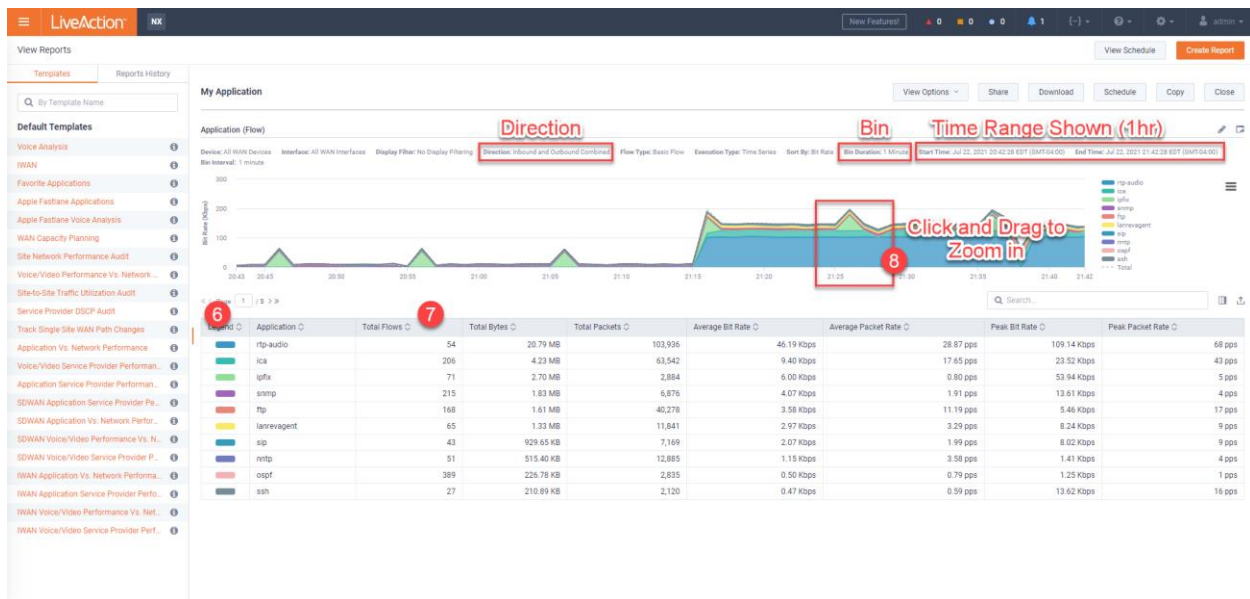
**Direction**  
Inbound and Outbound Combined

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

Cancel Save As Template Execute

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.



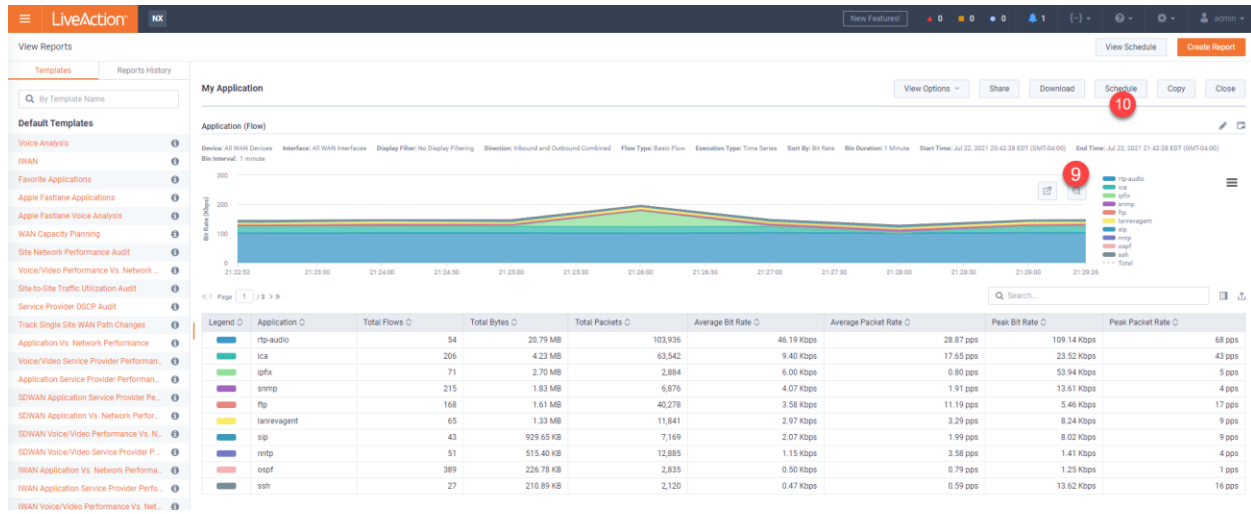
This report displays all the applications transiting the network in the **past hour**, in table format, with color references for the top 10 items by Total Bytes. All reports display 10 metrics per display page.

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.



SCHEDULE REPORT

Name

MY Application

Run Report

Hourly

Reports will be created on the hour for the previous hour

Schedule Ends

Never

Time Zone

(GMT-05:00) America/New York

DST

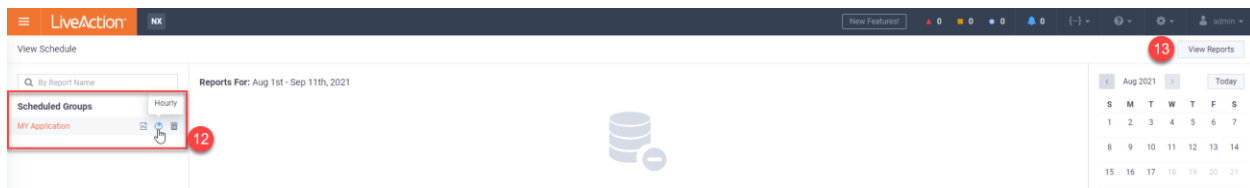
Cancel

Schedule

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



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

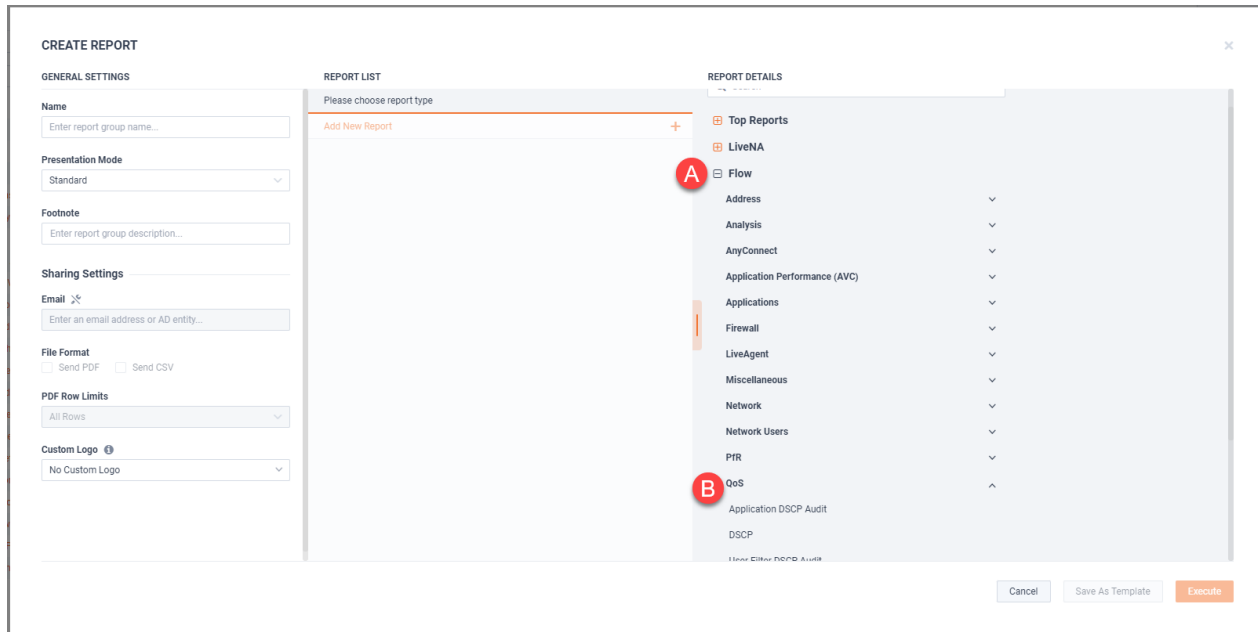


Lets have a look at creating a **Custom Report**

13. Navigate back to reports by clicking **Reports > View Reports**.

14. Click **Create Report** (top right of screen)

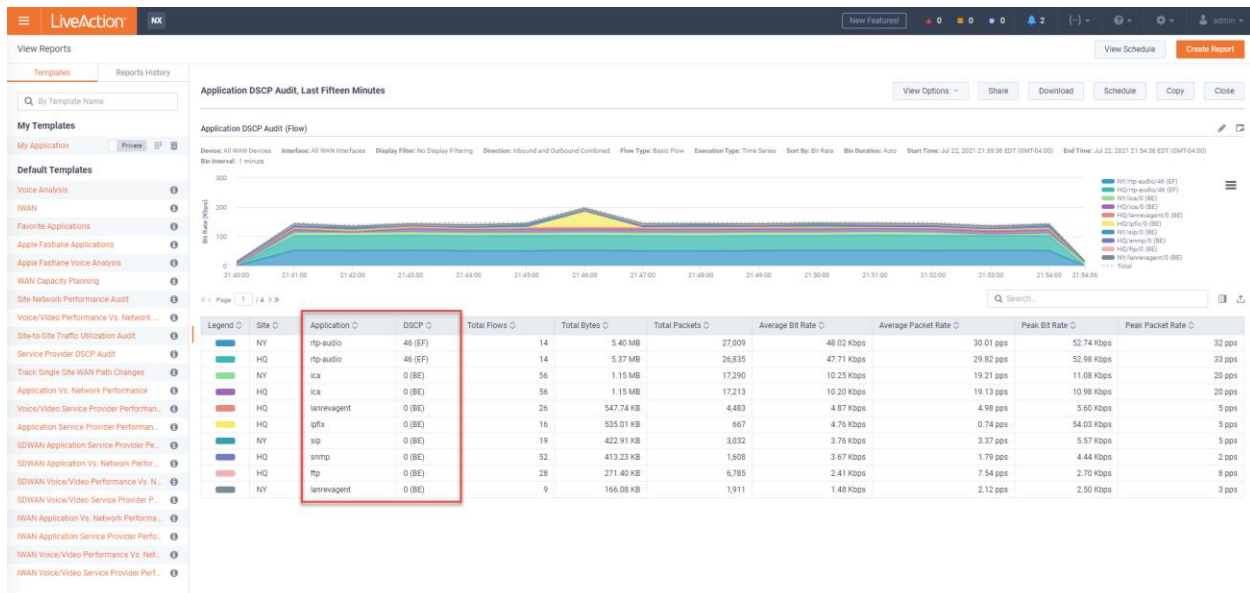
15. Expand (A) **Flow** and then expand (B) **QoS**.



16. Select **Application DSCP Audit**.

17. Click **Execute**.

18. Verify the Application to DSCP values



# 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**.

<input type="checkbox"/>	QoS Class Drop	Device, Interface	Warning	Qos Class VOICE Drop Rate > 20 kbps for at ...	Web UI
<input type="checkbox"/>	QoS Interface Drop	Device, Interface	Warning	Drop Rate > 2500 pps for at least > 0 minutes	Web UI
<input type="checkbox"/>	Routing Adjacency State Change	Network	Critical	for at least > 0 minutes	Web UI
<input type="checkbox"/>	Routing Polling Error	Network	Critical	for at least > 0 minutes	Web UI
<input type="checkbox"/>	Site Reachability	Network	Info	for at least > 5 minutes	Web UI
<input type="checkbox"/>	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 \*** For at Least \*

0 kbps > 0 min

**QoS Class \***

☒ VOICE

**Drop Rate \*** For at Least \*

20 kbps > 0 min

**QoS Class \***

☒ VIDEO

**Drop Rate \*** For at Least \*

50 kbps > 1 min

Add Specific QoS Class Alert

**Sharing**

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".

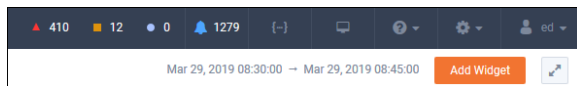
---

**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).

LiveAction NX

Alert Management

LiveNX Alerts

Enable Disable

Click this box to enable all Alerts

ALERT TYPE	SEVERITY	ENABLED	THRESHOLDS	SHARING
<input checked="" type="checkbox"/> All Type	All	All	Thresholds	Sharing
<input checked="" type="checkbox"/> IPSLA Voice/Jitter Test	Network	Critical	Total Test Errors > 3 Errors for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Line Card Operational State	Device, Interface	Multiple	Multiple	Multiple
<input checked="" type="checkbox"/> LiveNX CPU Utilization	System	Critical	Local/Server >= 40 % for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> LiveNX Disk Utilization	System	Critical	Local/Server >= 60 % for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> LiveNX Memory Utilization	System	Critical	Local/Server >= 40 % for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> LiveNX Node Connectivity	System	Critical	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Low WAN Interface Utilization	Device, Interface	Multiple	Multiple	Multiple
<input checked="" type="checkbox"/> Power Supply Operational State	Device, Interface	Multiple	Multiple	Multiple
<input checked="" type="checkbox"/> OGP Throughput Level	Device, Interface	Multiple	Multiple	Multiple
<input checked="" type="checkbox"/> QoS Class Default Drop	Device, Interface	Critical	Drop Rate > 0 kbps for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> QoS Class Drop	Device, Interface	Warning	Multiple	Web UI
<input checked="" type="checkbox"/> QoS Interface Drop	Device, Interface	Warning	Drop Rate > 2500 pps for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Routing Adjacency State Change	Network	Critical	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Routing Polling Error	Network	Critical	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Site Reachability	Network	Multiple	Multiple	Multiple
<input checked="" type="checkbox"/> Spanning Tree Topology Change	Network	Critical	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Voice Traffic Classification and Marking	Application	Critical	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Voice/Video Applications Performance	Application	Critical	Multiple	Web UI
<input checked="" type="checkbox"/> Voice/Video Performance - Jitter Avg	Application	Critical	Jitter Avg >= 30 ms for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Voice/Video Performance - Jitter Max	Application	Critical	Jitter Max >= 50 ms for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Voice/Video Performance - Packet Loss	Application	Critical	Packet Loss >= 1 % for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> VRRP Operational State	Network	Multiple	Multiple	Multiple

Rows: 44 / 44 Selected: 23

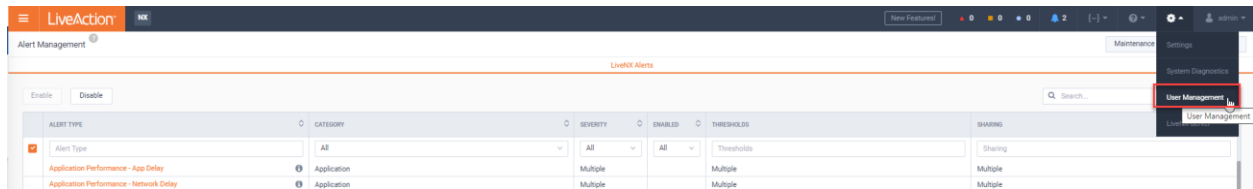


# Lab 1.6: Add a User Account

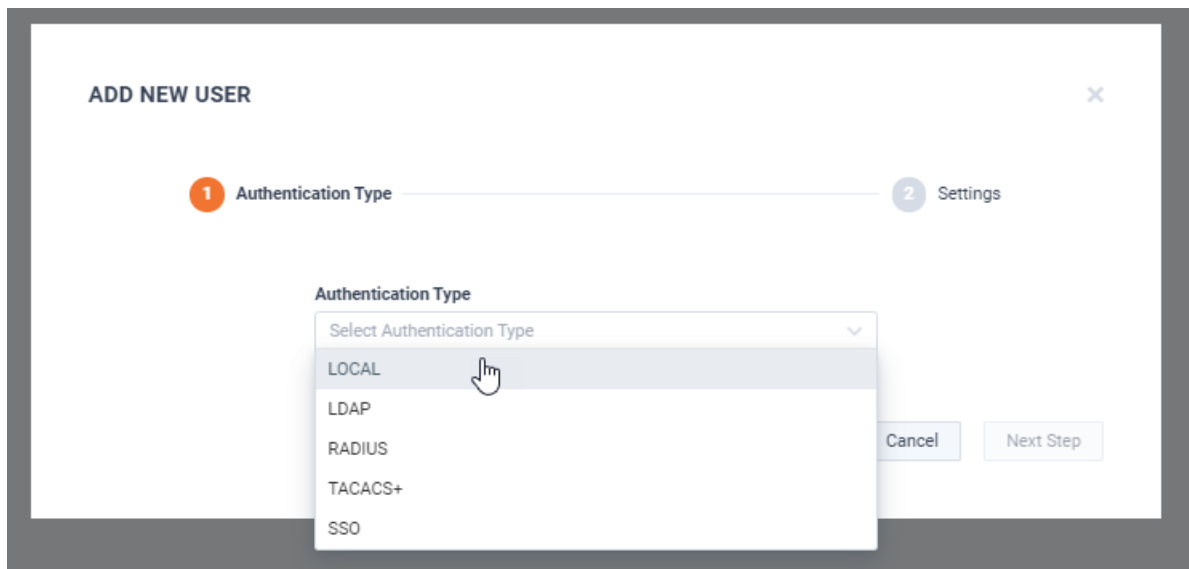
One of the first things to do after installing LiveNX is to grant additional user access, as well as to ensure that if you lose the credentials for the initial admin account, you will be able to login with appropriate privileges with a backup account.

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.

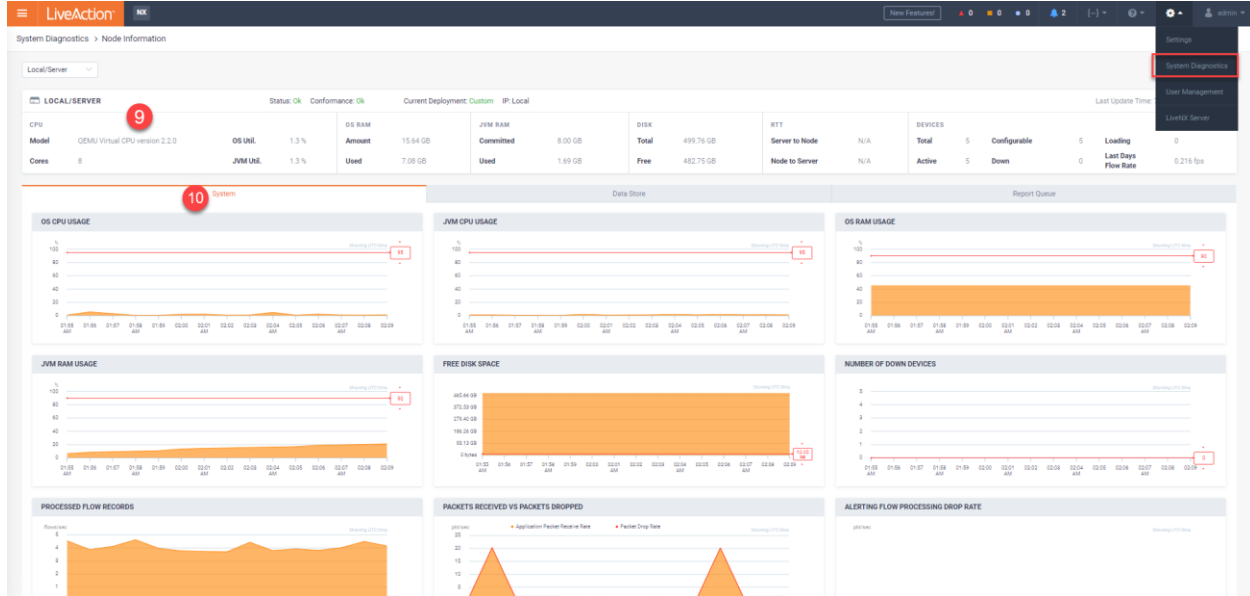
---

# Lab 1.7: View and Navigate System Diagnostics

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

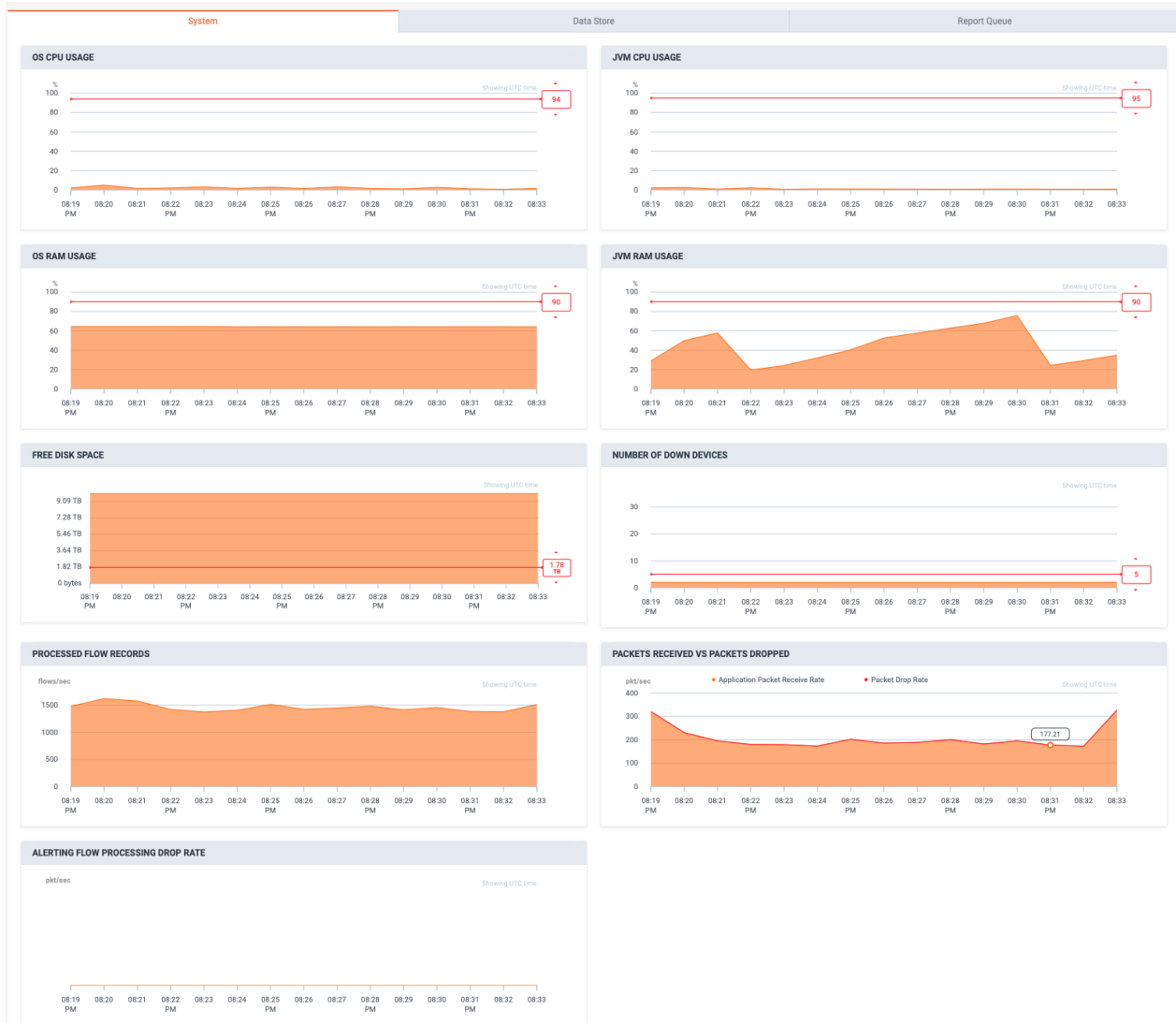
Lab Steps:

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.

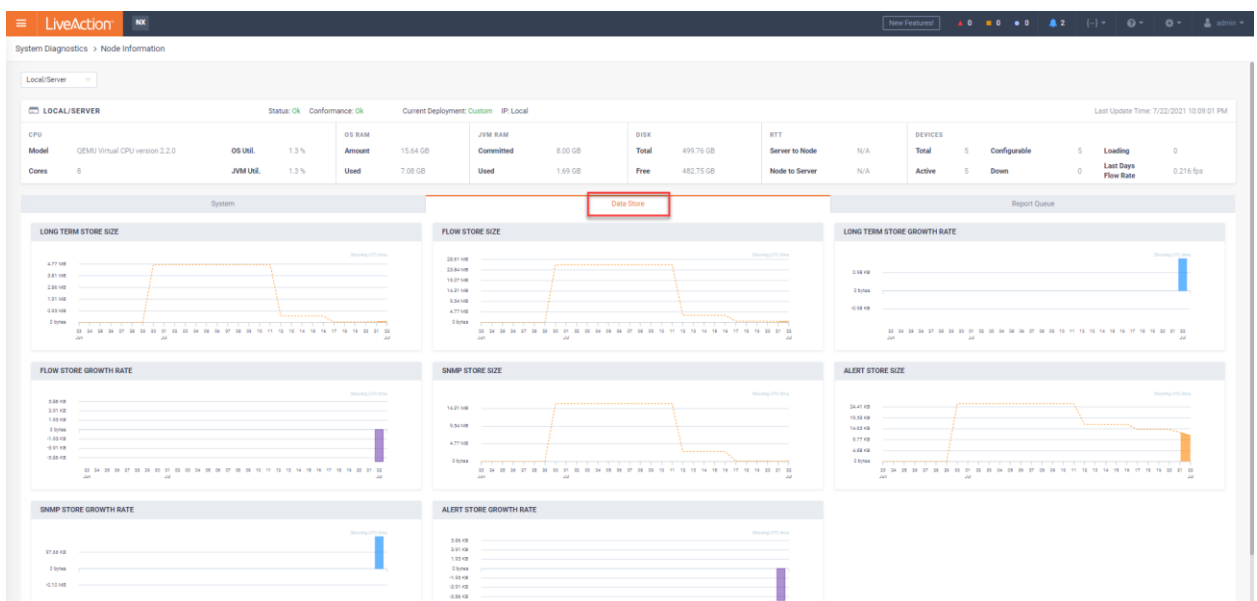


**Note:** If you have additional nodes, there will be multiple entries for each additional node and the details for those nodes can be seen as well.

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.



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

LiveAction

NEW

New Features

2

admin

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 Util.		OS RAM		JVM RAM		DISK		MTT		SERVICES					
Model	QEMU Virtual CPU version 2.2.0	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 State	0.216 f/s

System

Data Store

Report Queue

Report Queues

Cancel Cancel All

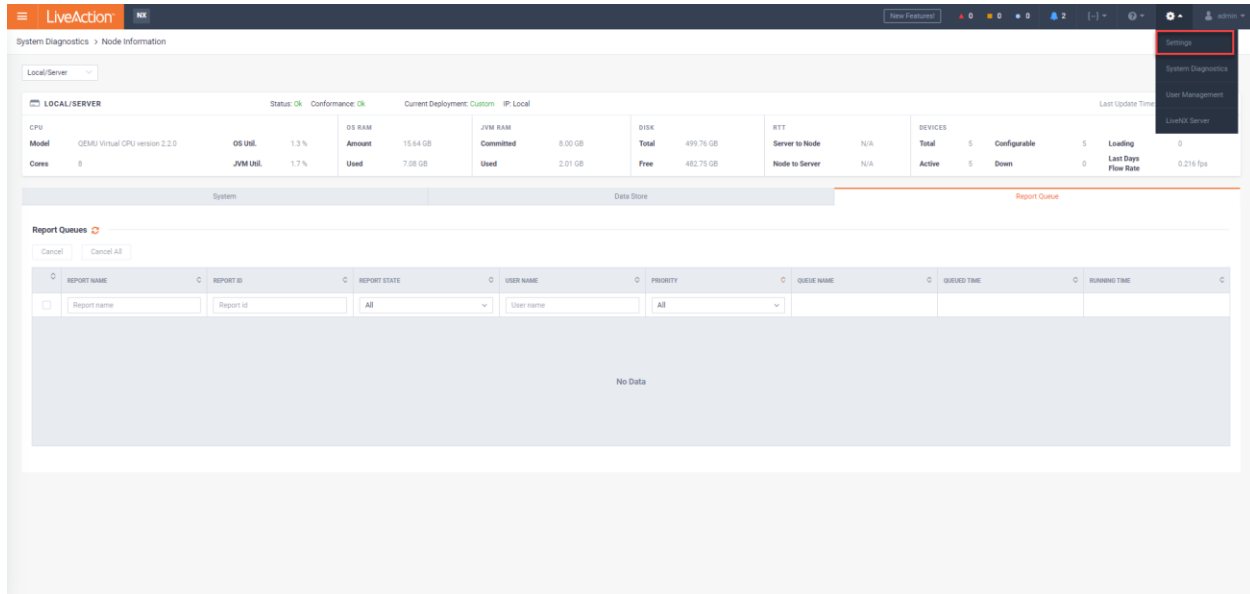
	REPORT NAME	REPORT ID	REPORT STATE	USER NAME	PRIORITY	QUEUE NAME	QUEUED TIME	RUNNING TIME
<input type="checkbox"/>	Report name	Report id	All	User name	All			

No Data

# Lab 1.8: Support and Troubleshooting

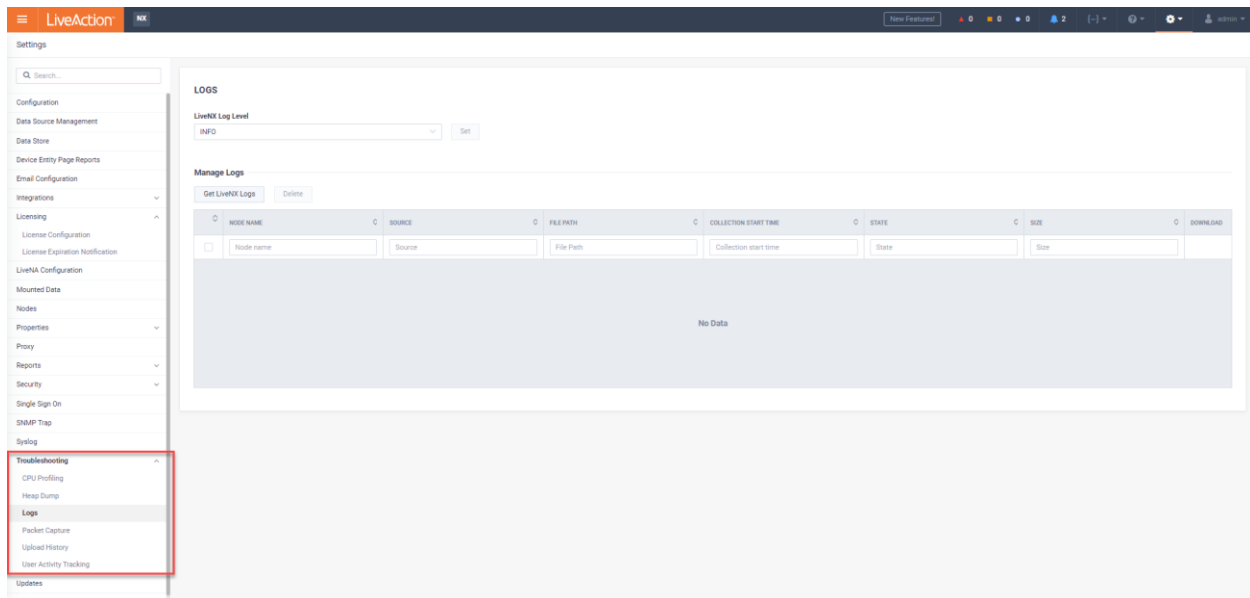
If support is needed, logs will need to be generated and collected.

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



The screenshot shows the LiveAction Node Information page. The top navigation bar includes the LiveAction logo and a user profile icon. A dropdown menu is open, showing options: Settings, System Diagnostics, User Management, and LiveNX Server. The main content area displays system information for a Local/Server node, including CPU, OS, RAM, and disk usage. Below this, there is a section for Report Queues, which is currently empty and shows 'No Data'.

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



The screenshot shows the LiveAction Settings page. The left sidebar contains a list of settings categories, with 'Troubleshooting' expanded and 'Logs' selected. The main content area displays the 'LOGS' section, which includes a 'LiveNX Log Level' dropdown set to 'INFO' and a 'Get LiveNX Logs' button. Below this, there is a table for 'Manage Logs' with columns for Node Name, Source, File Path, Collection Start Time, State, Size, and Download. The table is currently empty and shows 'No Data'.

**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.

Select All

Select None

☐ Local/Server

Cancel

Get Logs

---

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

---

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

The screenshot shows the LiveAction web interface. On the left is a sidebar with a search bar and a navigation menu. The 'Packet Capture' option under the 'Troubleshooting' section is highlighted with a red box. The main content area is titled 'PACKET CAPTURE' and contains a sub-header 'Capture Packets' with a 'Delete' button. Below this is a table with the following columns: NODE NAME, FILE NAME, COLLECTION START TIME, STATE, SIZE, and DOWNLOAD. The table is currently empty, showing 'No Data' in the center. The top of the interface has a 'LiveAction' header and a 'New Environment' button.

- 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.

<b>Interface*</b>	<b>Device</b>
<input type="text" value="eth0"/>	<input type="text" value="Other"/>
<b>Node</b>	<b>Protocol</b>
<input type="text" value="Local/Server"/>	<input type="text" value="None"/>
<b>Host</b>	<b>Duration*</b>
<input type="text" value="eg: x.x.x.x"/>	<input type="text" value="sec"/>
<b>Port</b>	
<input type="text" value="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

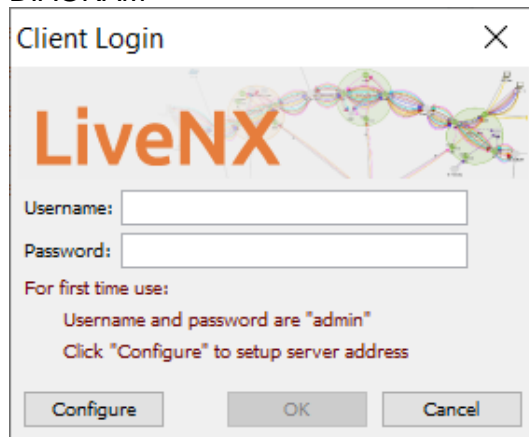
The LiveNX Client is a Java application which may be loaded and launched on your local workstation. In this class you may alternatively run the Client on the virtual workstation connected via Remote Desktop Connection. The Client may be downloaded at <https://cloudkeys.liveaction.com/downloads>, and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

A Mac version is also available for install if needed.

Lab Steps:

1. **Launch** the LiveNX Client.

DIAGRAM



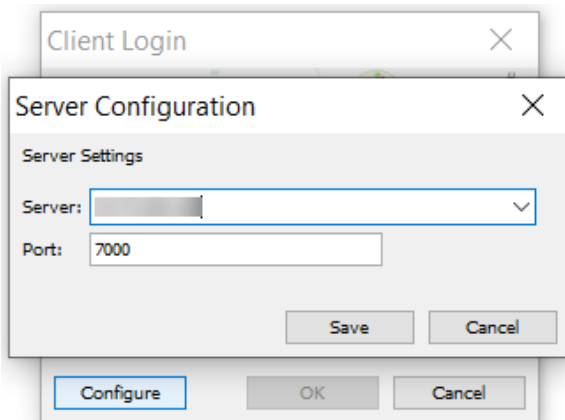
2. Click **Configure** to verify server settings.

---

**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.

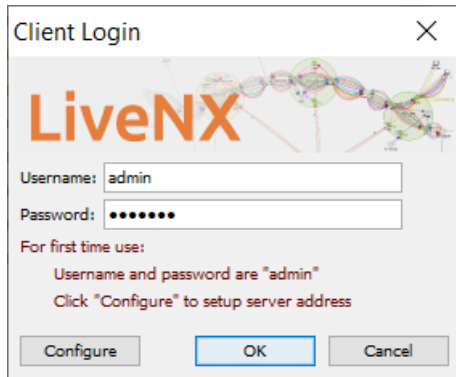
---

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



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

Password: Student (note the capital S)



Client Login

Username:

Password:

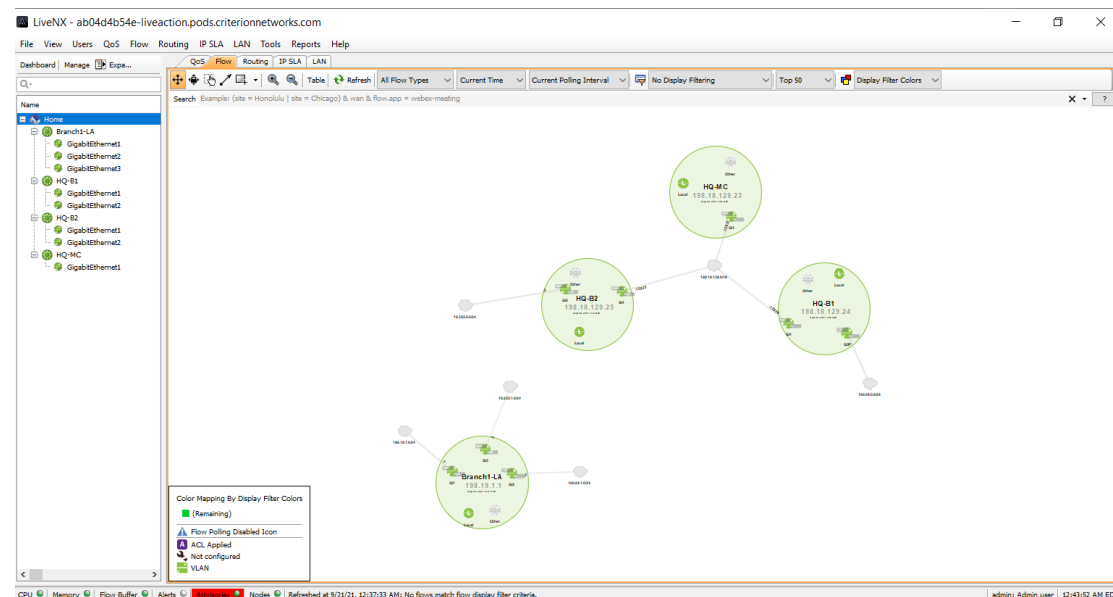
For first time use:  
Username and password are "admin"  
Click "Configure" to setup server address

6. Click **OK**

The Client will launch...



... and will open showing the current configured Topology.



**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

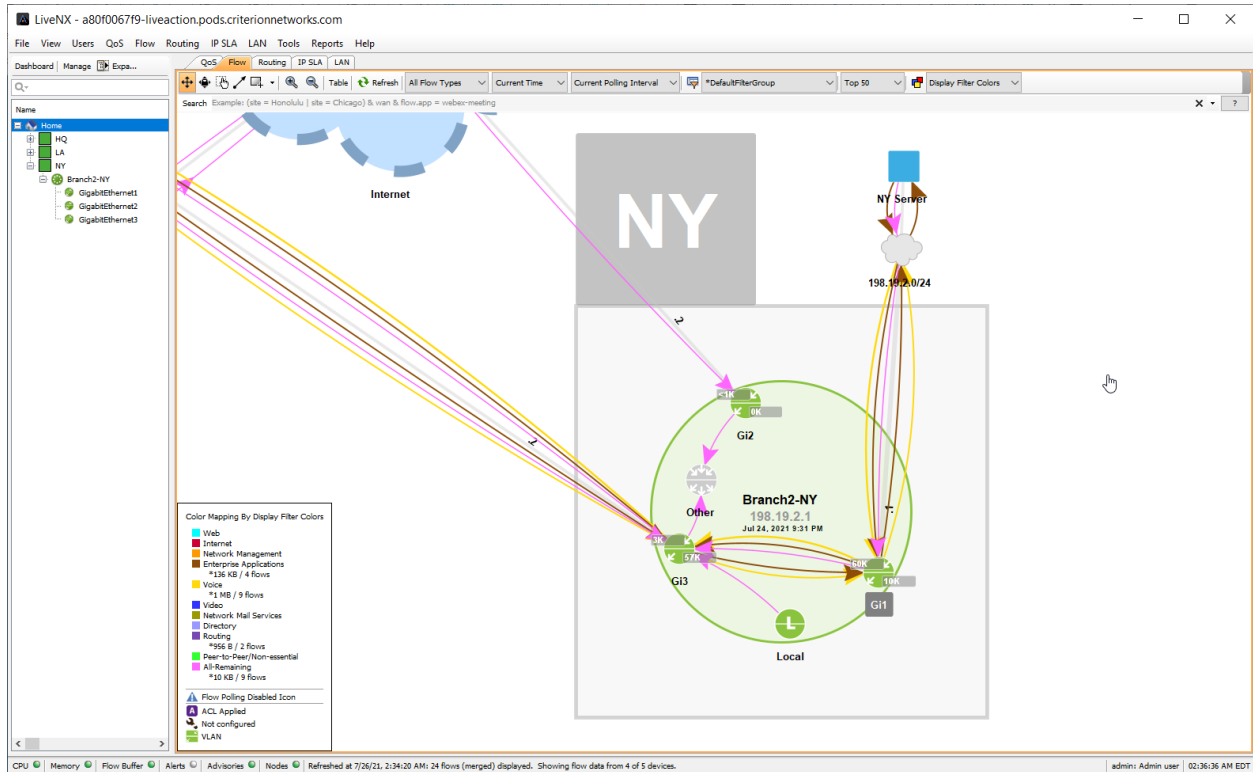
## Lab 2.2: Explore the LiveNX Client

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

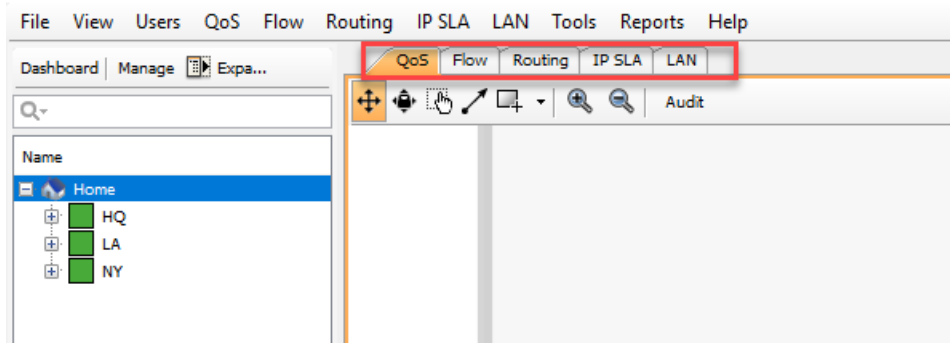


**Note:** Your topology may be different from the screenshot above.

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.

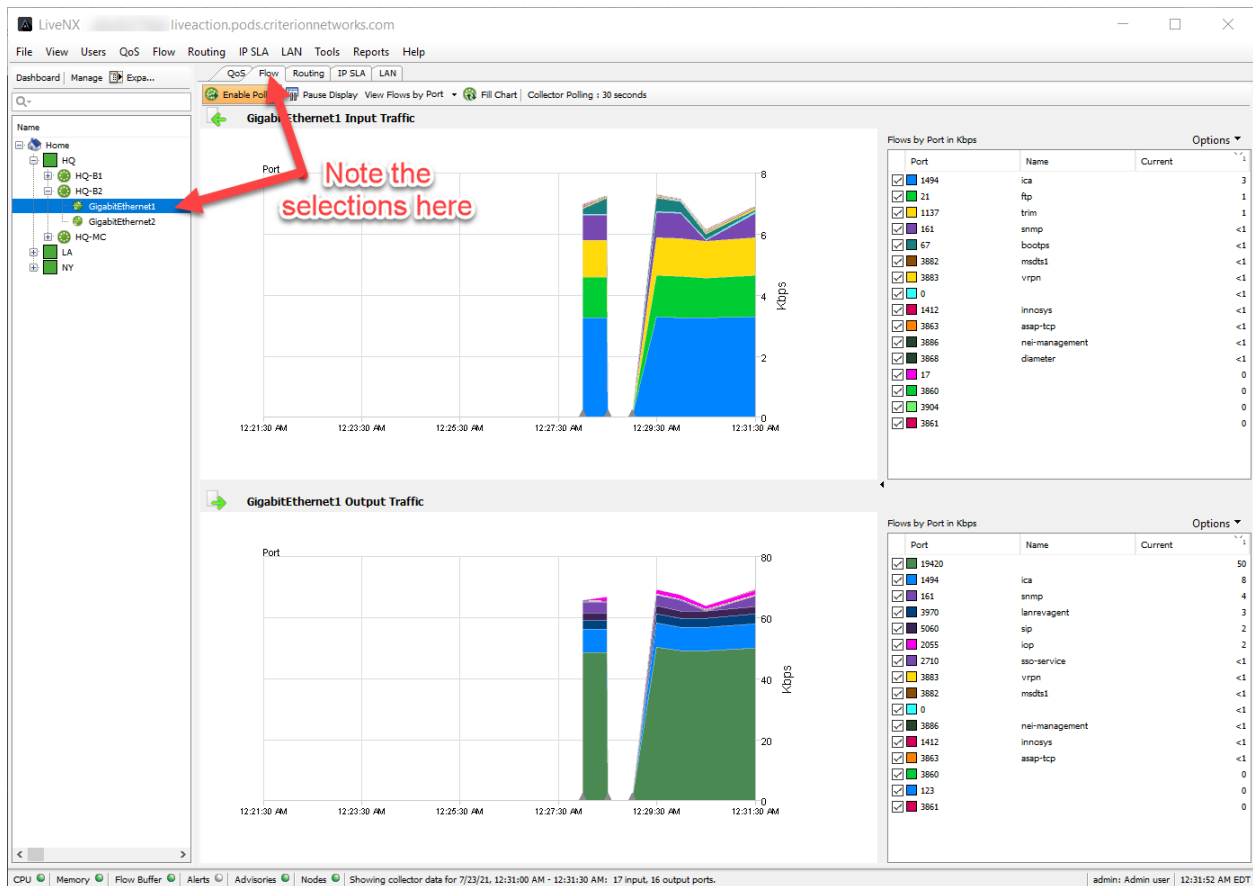
- Note the 5 Module Tabs to the top-left of the Topology Pane.

## DIAGRAM



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

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



**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

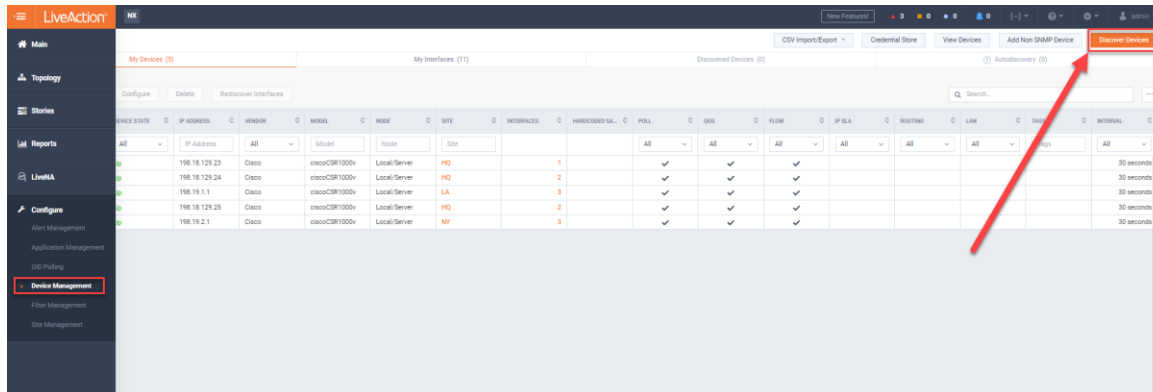
# Lab 3.1: Add Device

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**



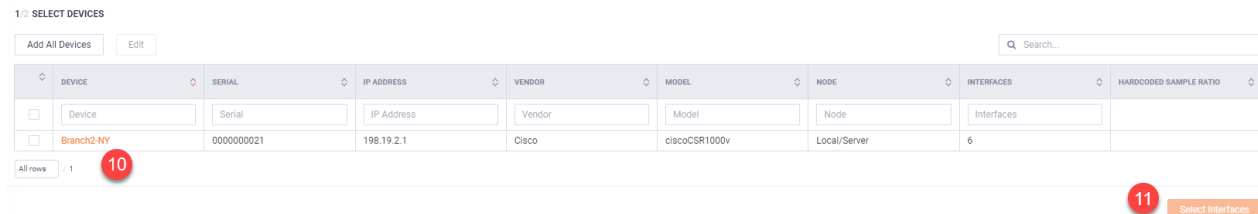
3. Click **Discover Devices**.

A screenshot of the 'DISCOVER DEVICES' form. The form has three tabs: '1. What to scan' (selected), '2. SNMP Settings', and '3. Node'. Step 4 points to the 'SPECIFY IP RANGES' section where '198.19.2.1' is entered in the 'IP Address' field. Step 5 points to the '2. SNMP Settings' tab. Step 7 points to the '3. Node' tab. Step 9 points to the 'Discover' button. Other fields include 'Choose a site' (dropdown), 'Add More' (button), 'SPECIFY SEED DEVICE TO SCAN' (radio button), 'IP address' (192.168.1.1), 'Hops' (empty field), 'Save & Next' (button), and 'Cancel' (button).

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**.

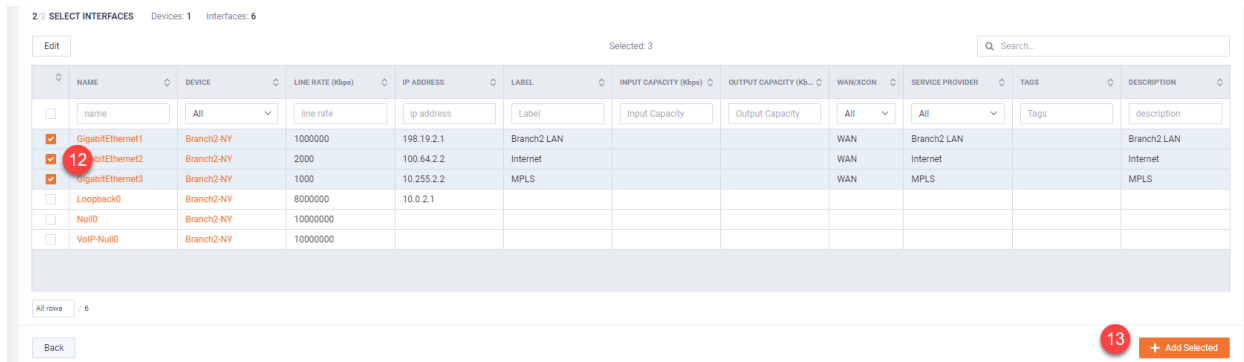


**Note:** Discovery may take a minute or two. If you've specified a large subnet to scan, and Discovery seems to take too long... click Stop.



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

11. Click **Select Interfaces**.

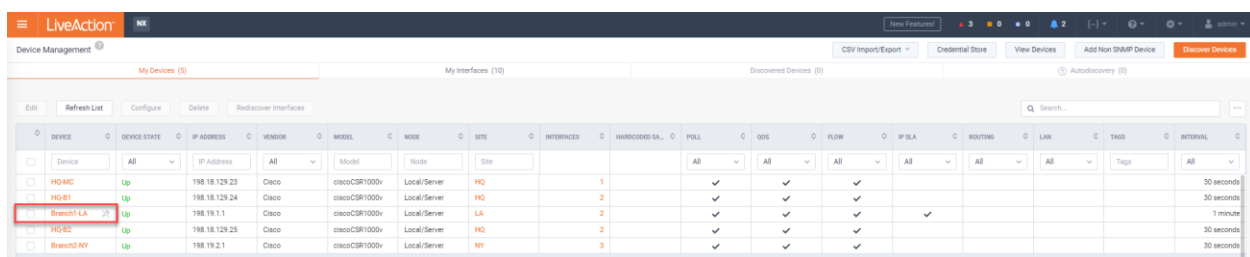


12. Select **GigabitEthernet1**, **GigabitEthernet2** & **GigabitEthernet3**.

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.



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

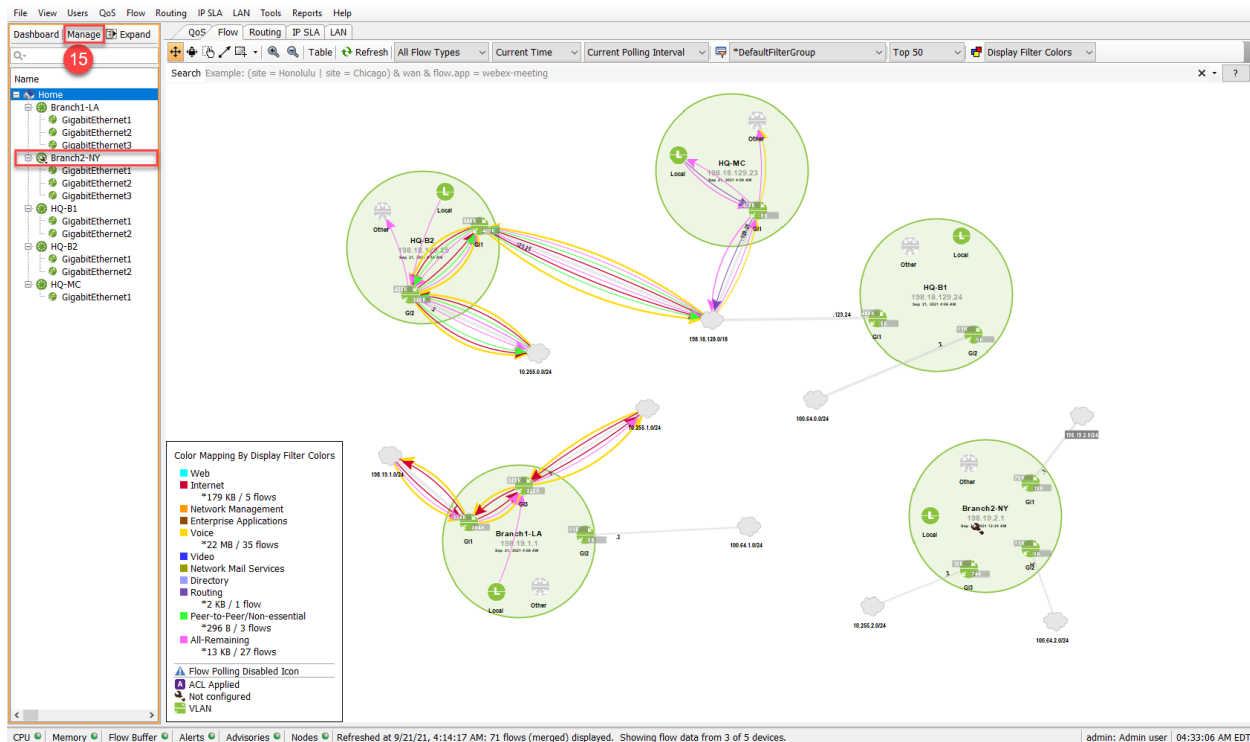
You may perform many management tasks via the WebUI... but since we'll need to go to the LiveNX Client to configure Flow Collection in the next lab... let's complete our Device Configuration in the Console.

**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**.



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
<input type="checkbox"/>	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 sec...	Configured
<input checked="" type="checkbox"/>	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1 minute	Not Config...
<input type="checkbox"/>	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 sec...	Configured
<input type="checkbox"/>	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 sec...	Configured
<input type="checkbox"/>	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 sec...	Configured

\* LAN polling occurs every 15 minutes

Number of Devices: 5

Device Configurations

**21** Configure

Remove

Add To Group

Remove From Group

Edit Groups

Configure QoS, Flow, and IP SLA

Select devices in the table and click the configure button.

Remove selected device(s).

<New Group>

Removes selected devices from their groups

Edit the groups

Global Device Settings

Edit Default SNMP Settings

Edit Default CLI Monitoring Settings - Not Set

Edit Default CLI Configuration Settings

Clear

Clear

**20** 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

☐ 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 devices

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

☒ Use my default Configuration CLI connection settings

☐ Enter connection settings for this device

Connection Type: SSH Port\*: 22

User name on Device:

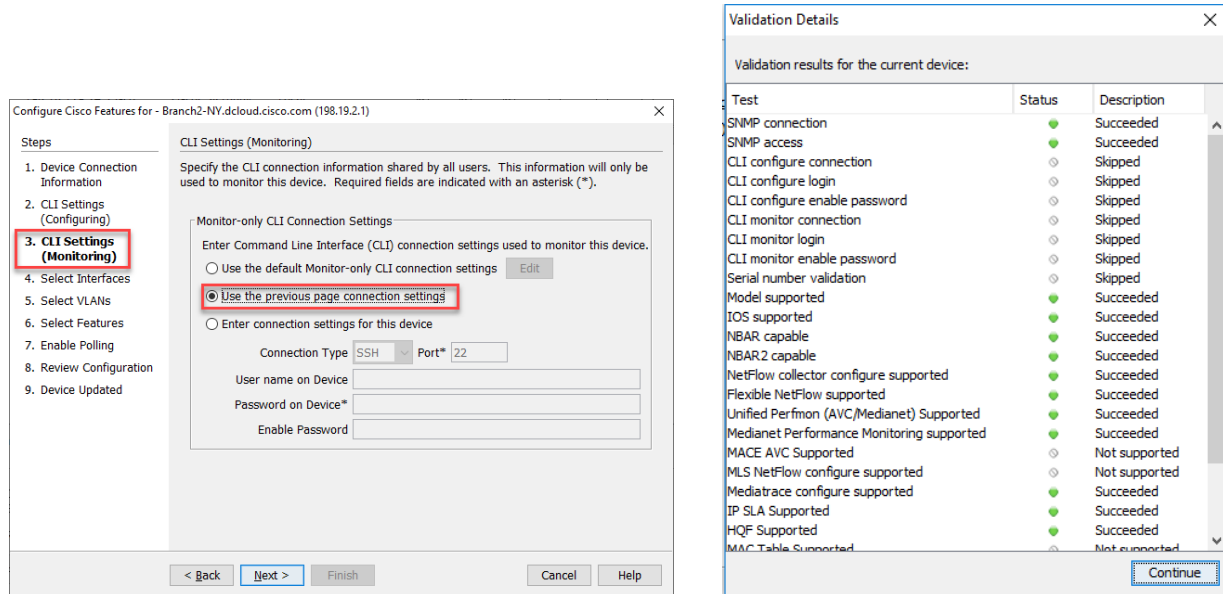
Password on Device\*:

Enable Password:

☐ Also use these credentials for monitor mode.

< Back Next > Finish Cancel Help

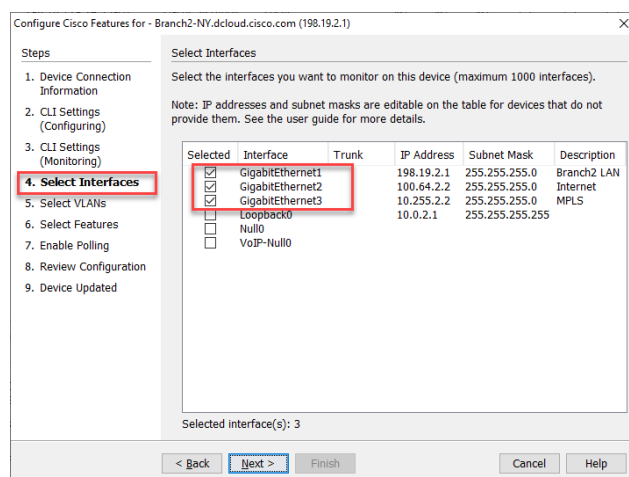
24. Step 3: Check Use the **Previous Page Connection Settings** ... Click **Next**. You will be shown a list of configuration elements to verify. Click Continue.



**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**

- You will want to include all GE interfaces
- You can include Loopback, but not necessary. The point is to understand you can choose both logical and physical interfaces.



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	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

< Back   **Next >**   Finish   Cancel   Help

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.

< 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

**Review Configuration**

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

```
configure terminal
  collect transport top 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.

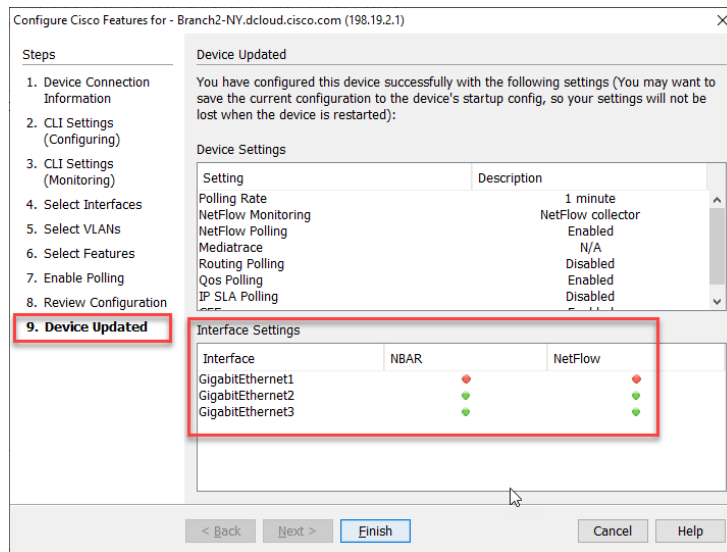
☐ I will manually configure the device myself.

< Back   **Next >**   Finish   Cancel   Help

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**.



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.

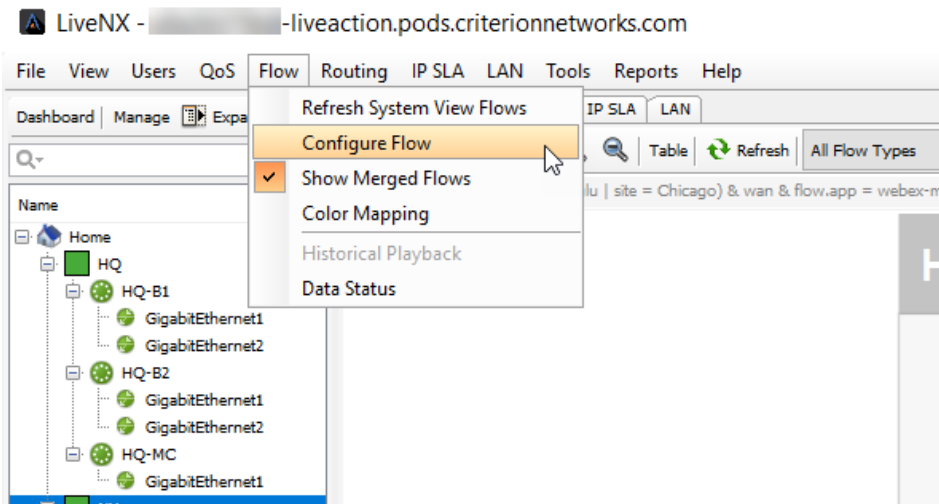
---

## Lab 3.3: Configure Flow on Devices

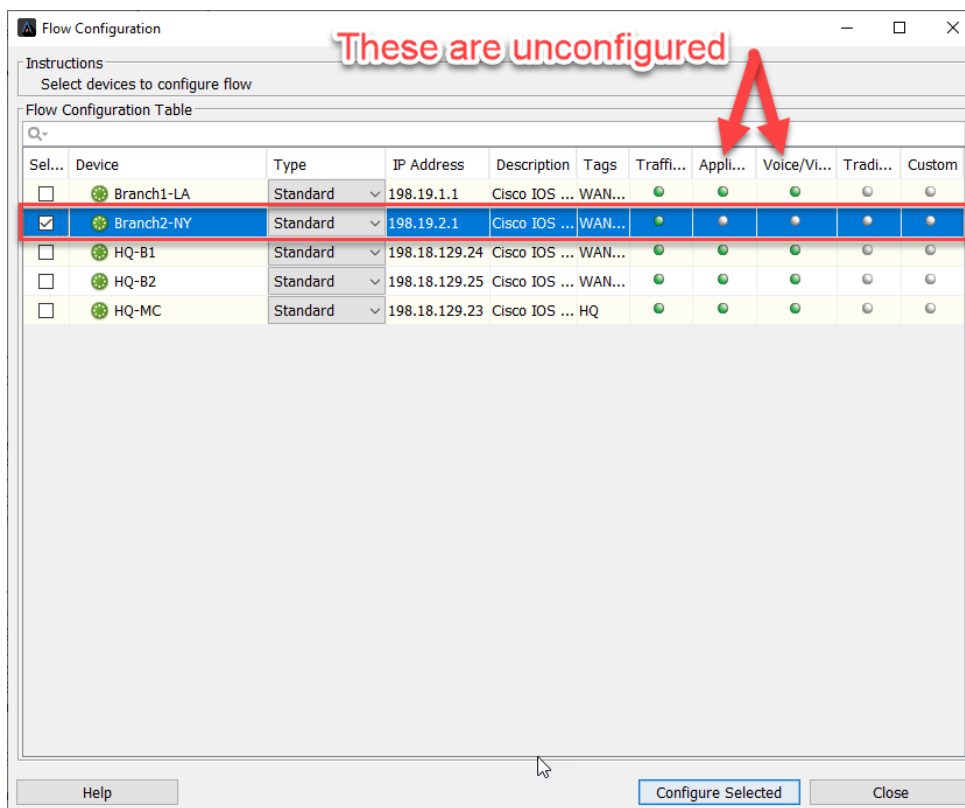
Before removing unwanted interfaces, you should remove any existing flow configurations those interfaces have been configured with... this will avoid any issues when writing new configuration data to the device.

Lab Steps:

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



34. Select **Branch2-NY**, click **Configure Selected**.



**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.

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,...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet1	-	198.19.2.1	Branch2 LAN	WAN,...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	-	100.64.2.2	Internet	WAN,...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet3	-	10.255.2.2	MPLS	WAN,...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Semantics are important

Flow Export Destination

☐ Configure Flow Export Destination

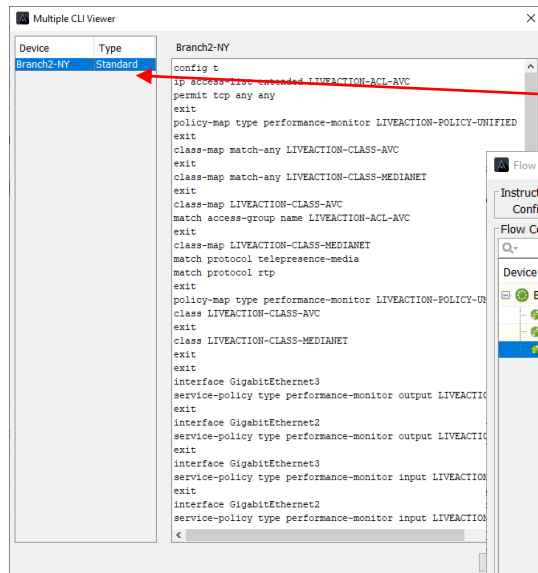
☒ LiveNX node

☐ LiveNX node flow replicator at port 9991

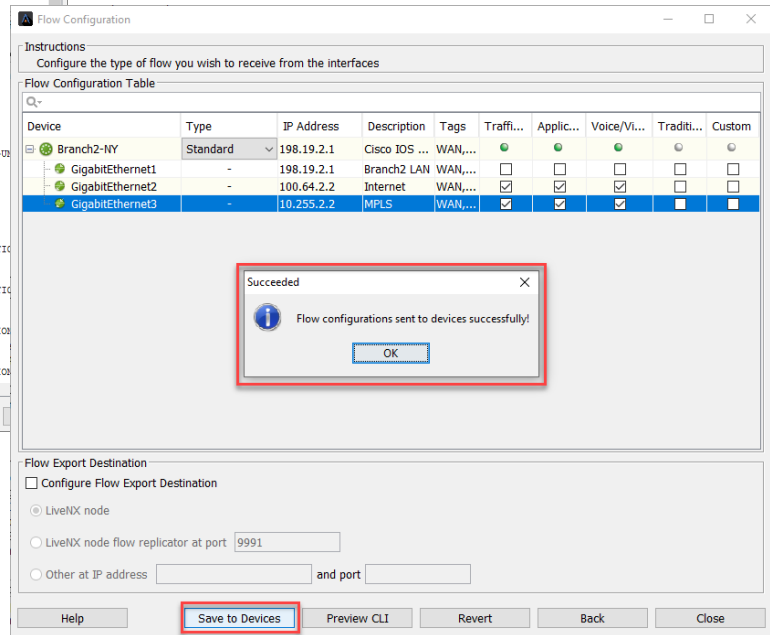
☐ Other at IP address and port

Help Save to Devices Preview CLI Revert Back Close

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.



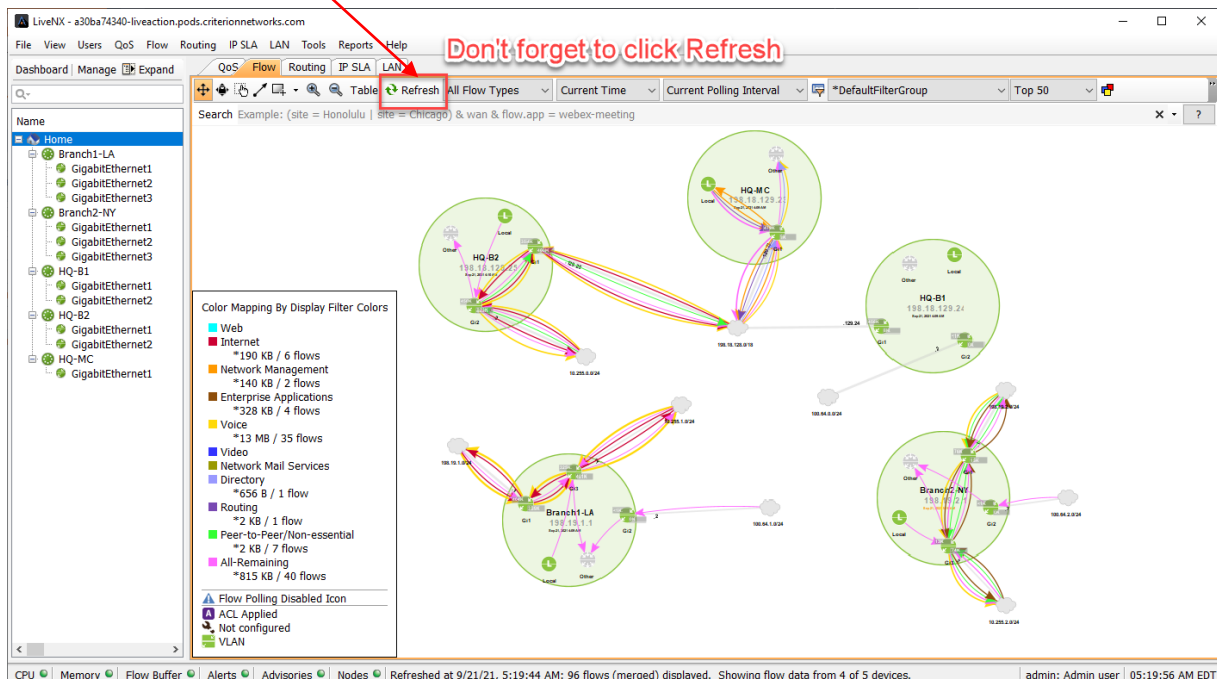
37. Click **Close**.

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.



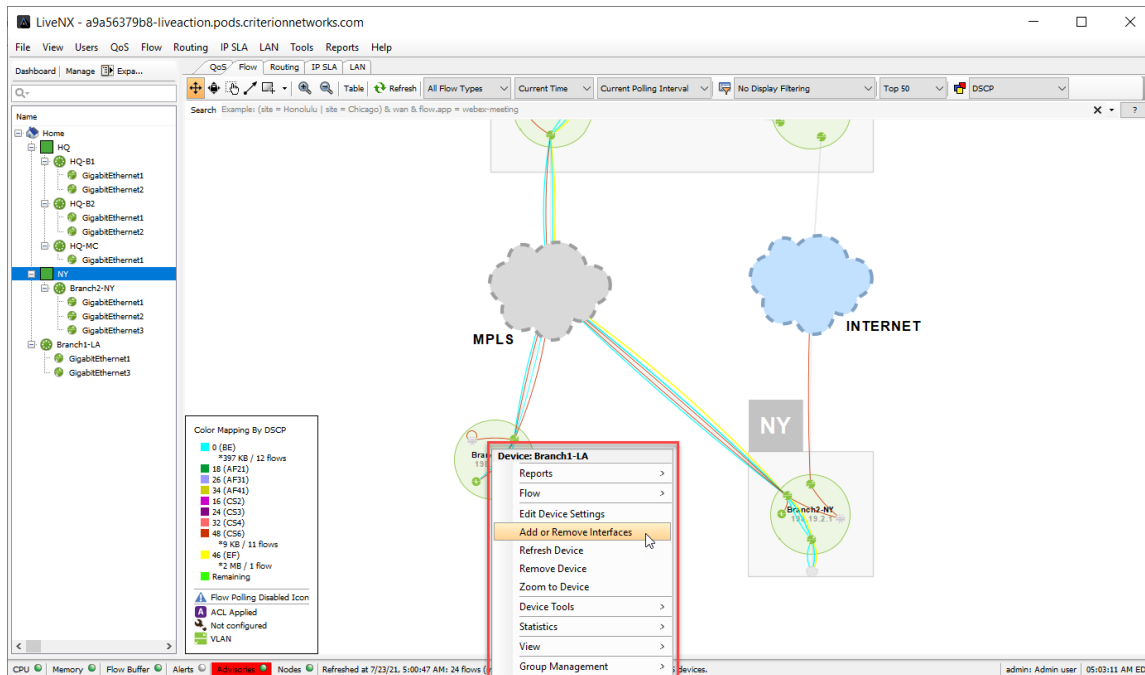
## Lab 3.4: Add/Remove Interfaces

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
<input checked="" type="checkbox"/>	GigabitEthernet1		198.19.1.1	255.255.255.0	Branch1 LAN
<input checked="" type="checkbox"/>	GigabitEthernet2		100.64.1.2	255.255.255.0	Internet
<input checked="" type="checkbox"/>	GigabitEthernet3		10.255.1.2	255.255.255.0	MPLS
<input type="checkbox"/>	Loopback0		10.0.1.1	255.255.255.255	
<input type="checkbox"/>	Null0				
<input type="checkbox"/>	VoIP-Null0				

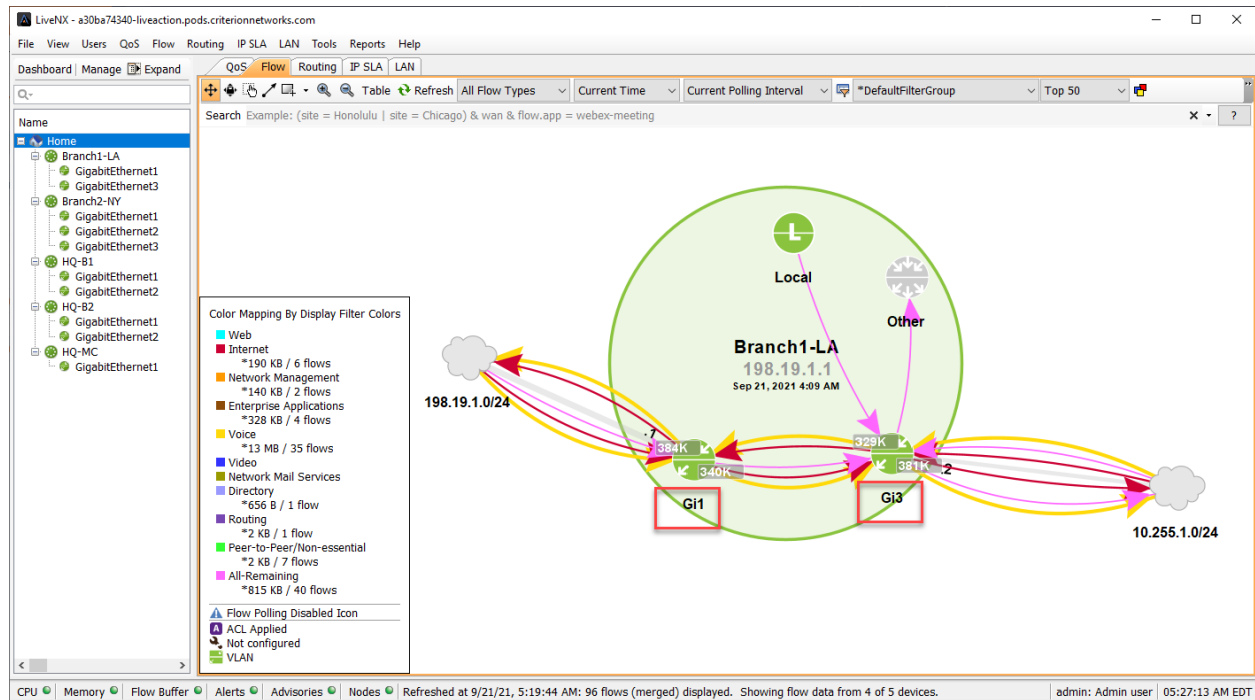
Selected interface(s): 2

< Back Next > Finish Cancel Help



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 **GigabitEthernet3**

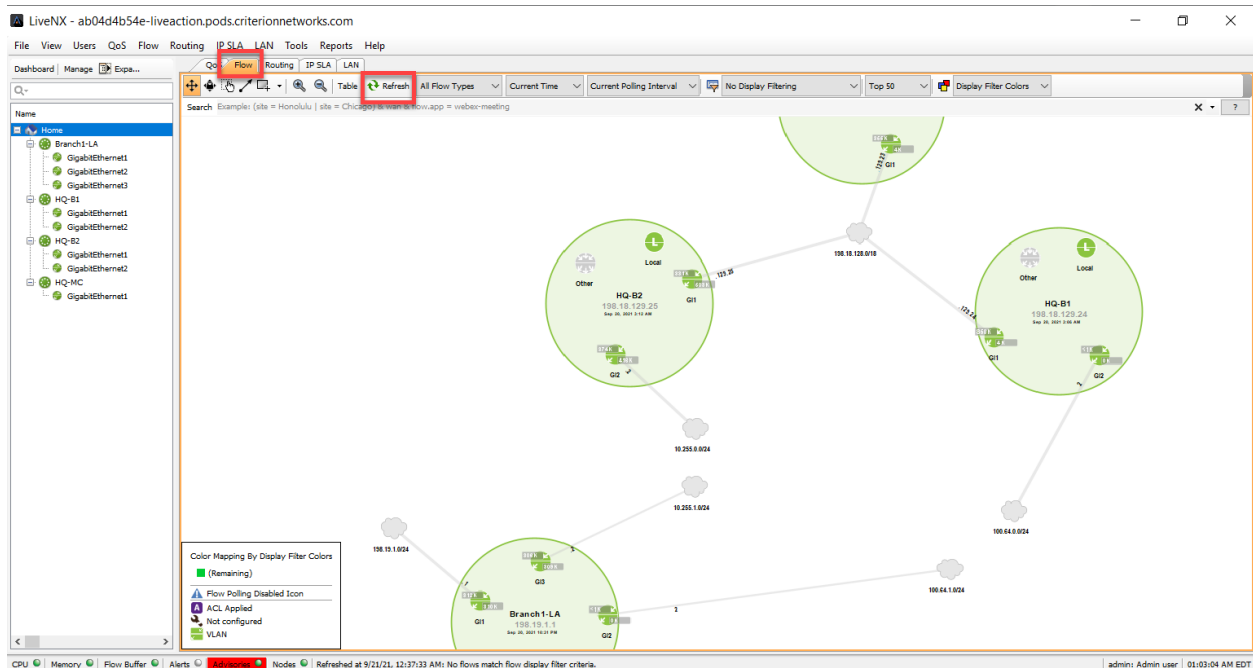


45. Repeat from Lab Step 1 above to perform interface addition/removal on **Branch2-NY** (as needed).

**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.

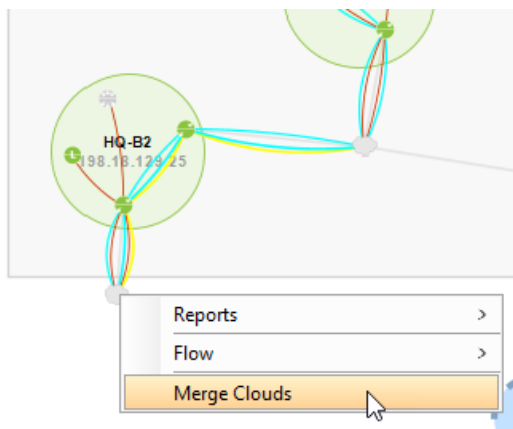


Notice on your topology that the **network clouds** are not connecting between devices. Since these clouds are across a service provider it is necessary to merge the clouds so that NetFlow can be properly visualized across the topology.

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

Lab Steps:

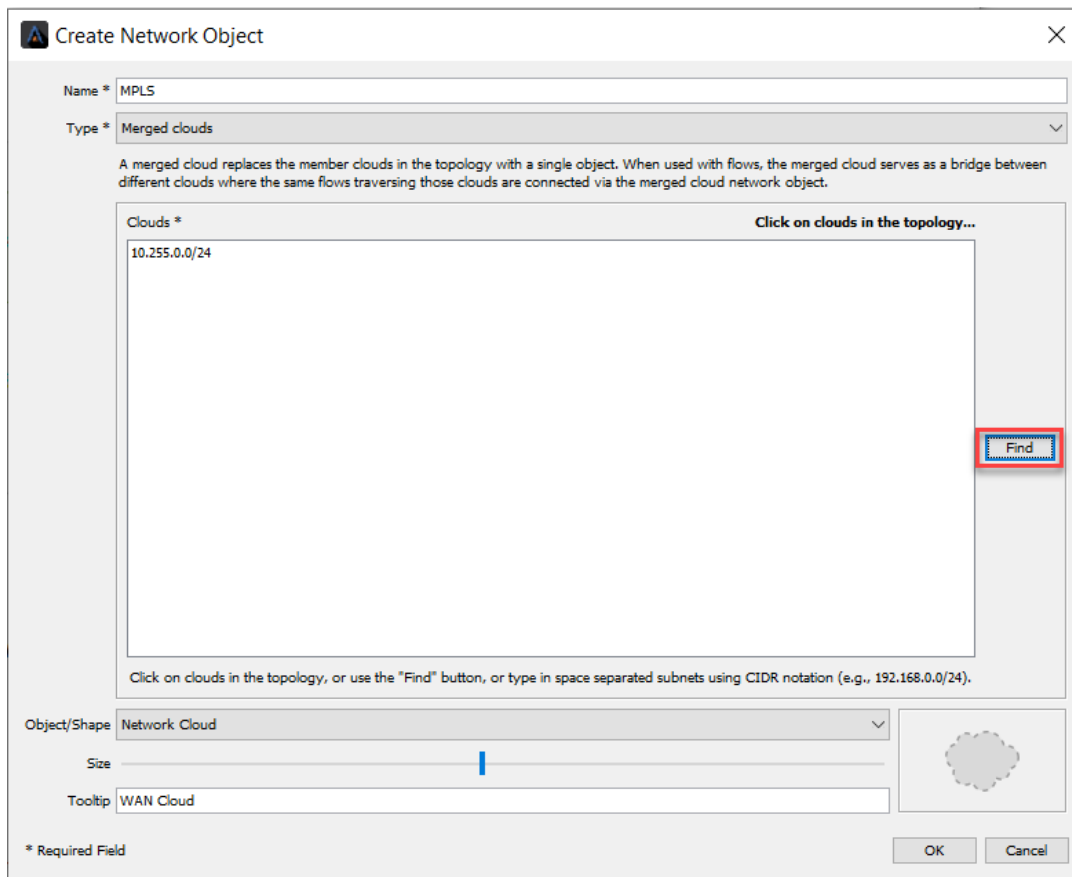
46. Right-click on the HQ-B2 Device's **GigabitEthernet2** 10.255.0.0/24 network cloud and select Merge Clouds.



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.



The "Create Network Object" dialog box is shown. The "Name" field is set to "MPLS". The "Type" is set to "Merged clouds". A description states: "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." The "Clouds" list contains "10.255.0.0/24". A "Find" button is highlighted with a red box. Below the list, instructions say: "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)." The "Object/Shape" is "Network Cloud", "Size" is a slider, and "Tooltip" is "WAN Cloud". "OK" and "Cancel" buttons are at the bottom right.

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 \*

10.255.0.0/24

Click on clouds in the topology...

Find

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

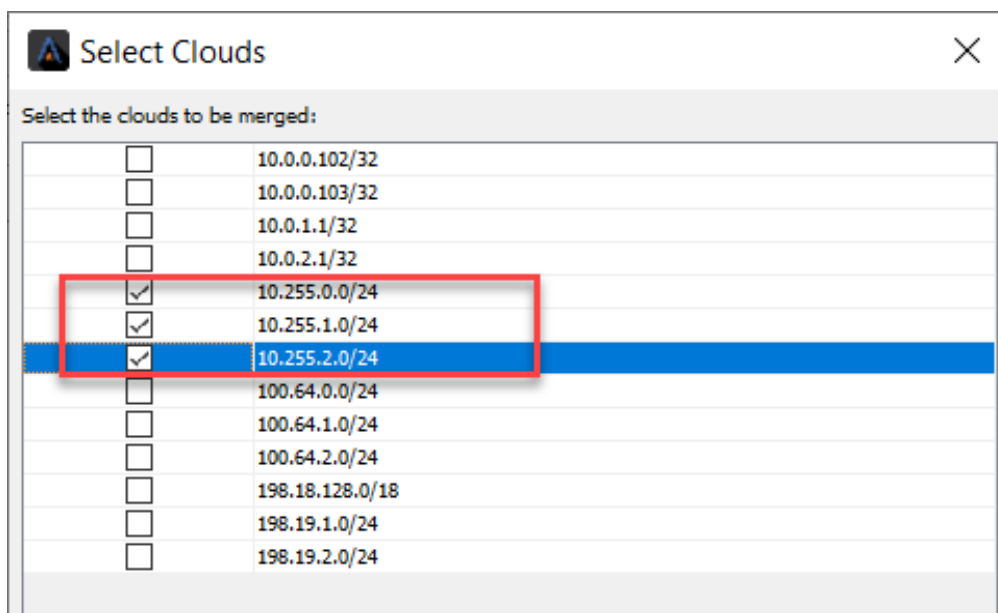
Tooltip WAN Cloud

\* Required Field

OK Cancel

50. Select the following networks and then select ok:

10.255.0.0/24  
10.255.1.0/24  
10.255.2.0/24



The "Select Clouds" dialog box is shown. It lists various IP ranges with checkboxes. A red box highlights the first three rows, which are also highlighted in blue: 10.255.0.0/24, 10.255.1.0/24, and 10.255.2.0/24. The "OK" button is highlighted with a red box.

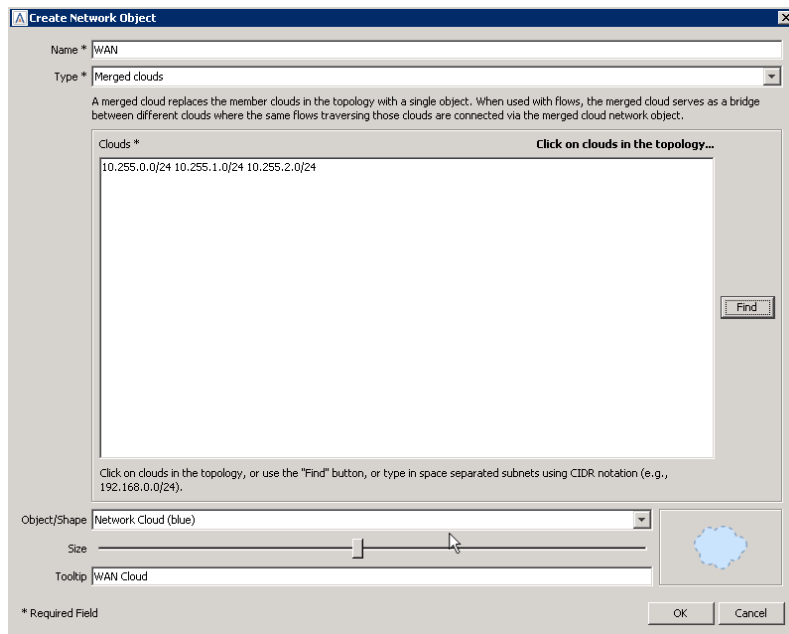
Select the clouds to be merged:

<input type="checkbox"/>	10.0.0.102/32
<input type="checkbox"/>	10.0.0.103/32
<input type="checkbox"/>	10.0.1.1/32
<input type="checkbox"/>	10.0.2.1/32
<input checked="" type="checkbox"/>	10.255.0.0/24
<input checked="" type="checkbox"/>	10.255.1.0/24
<input checked="" type="checkbox"/>	10.255.2.0/24
<input type="checkbox"/>	100.64.0.0/24
<input type="checkbox"/>	100.64.1.0/24
<input type="checkbox"/>	100.64.2.0/24
<input type="checkbox"/>	198.18.128.0/18
<input type="checkbox"/>	198.19.1.0/24
<input type="checkbox"/>	198.19.2.0/24

OK

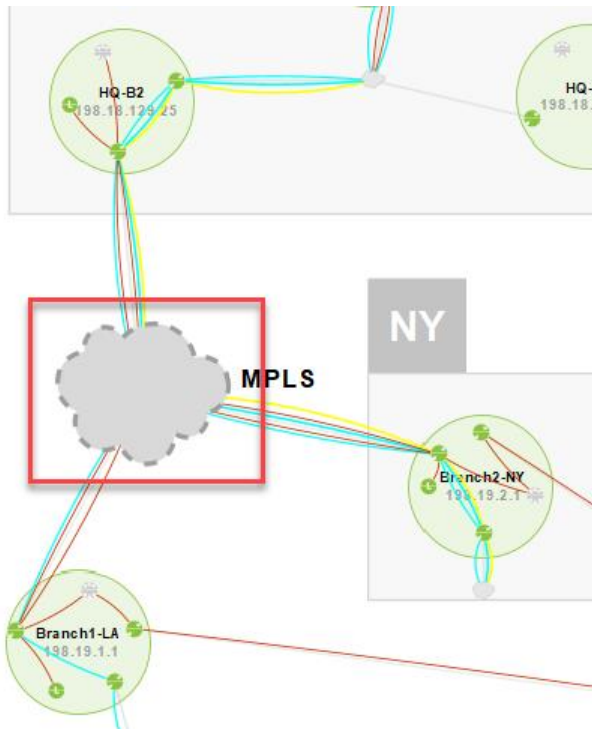
51. Click **OK**.

52. Click **OK** to finish.



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

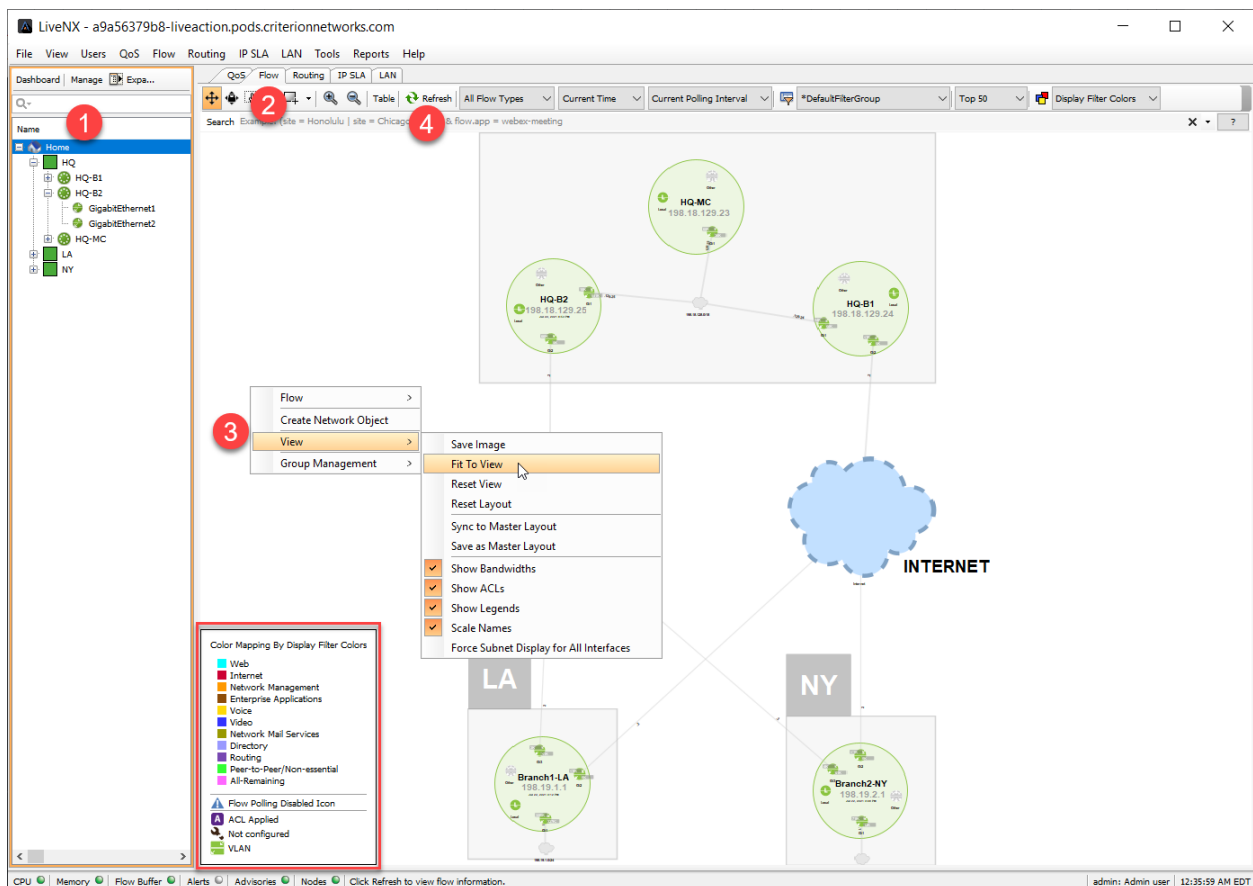
## Lab 4.1: Discover Flows

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.



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

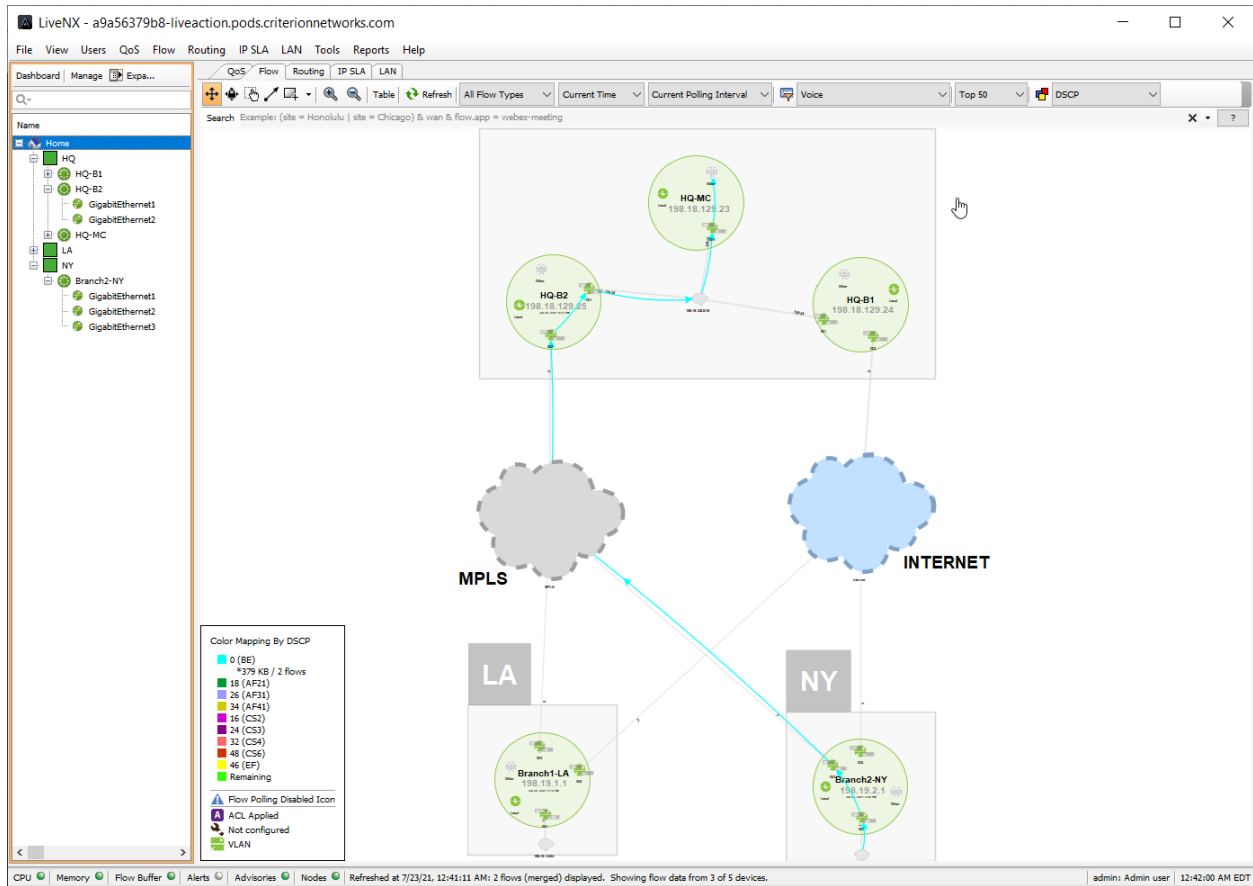
5. Set the filters to match:

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



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

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



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.

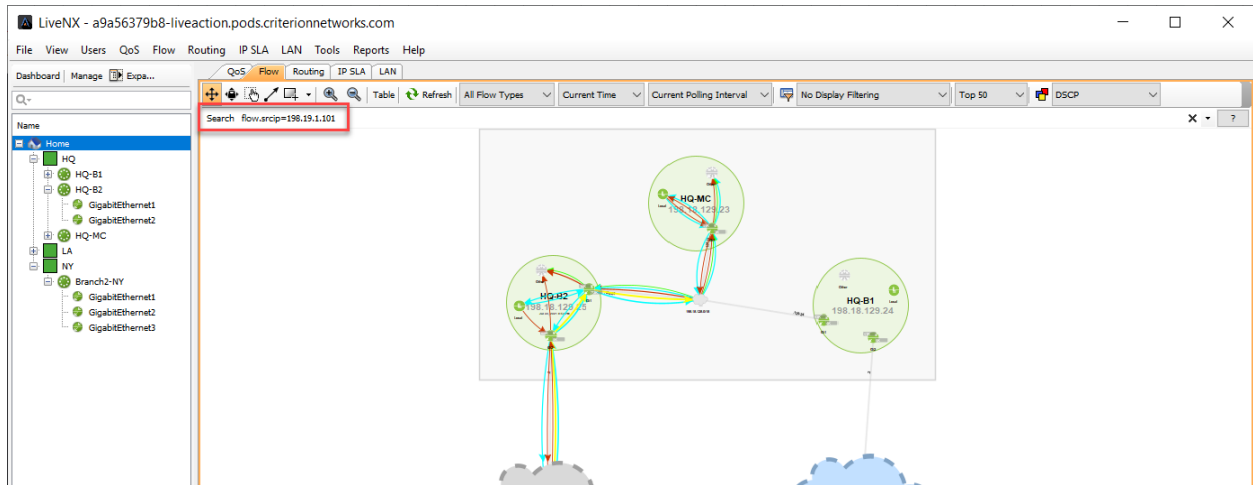
What other applications can you identify across our network?

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.



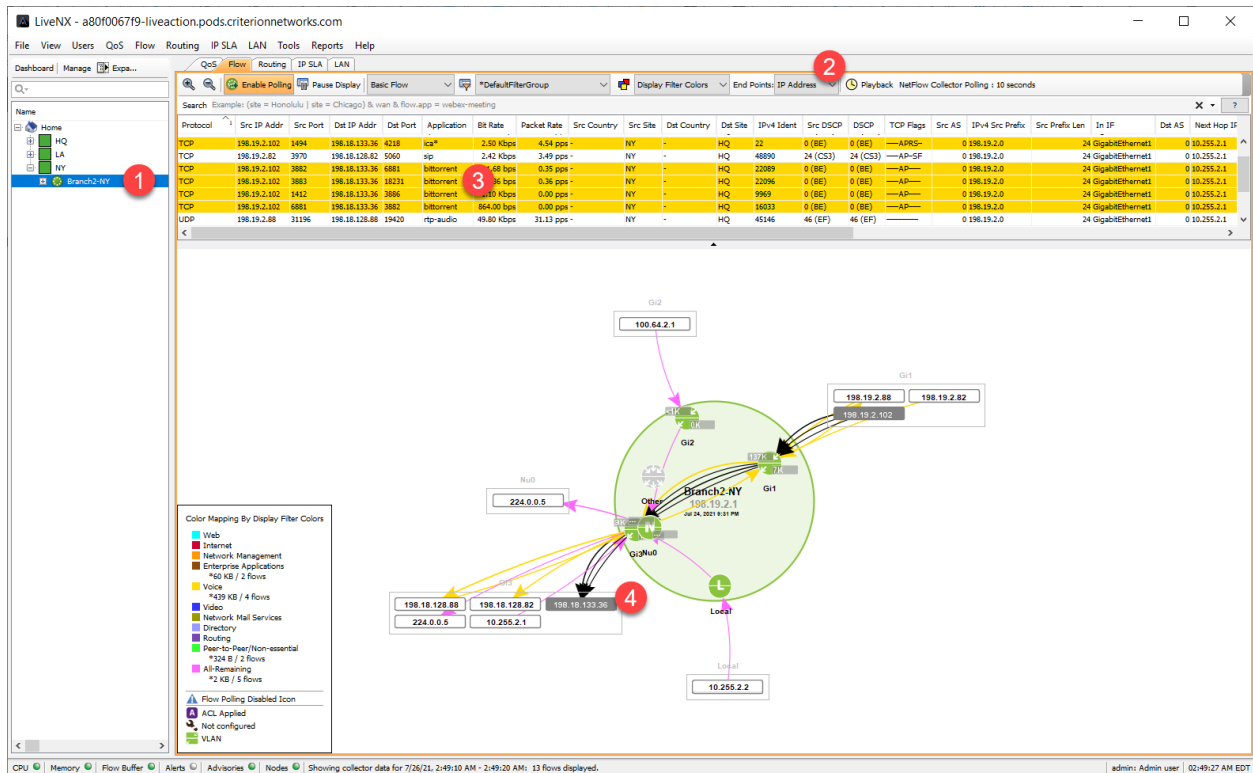
Notice that LiveNX has identified one or more *end-to-end* flows across the network.



## 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.

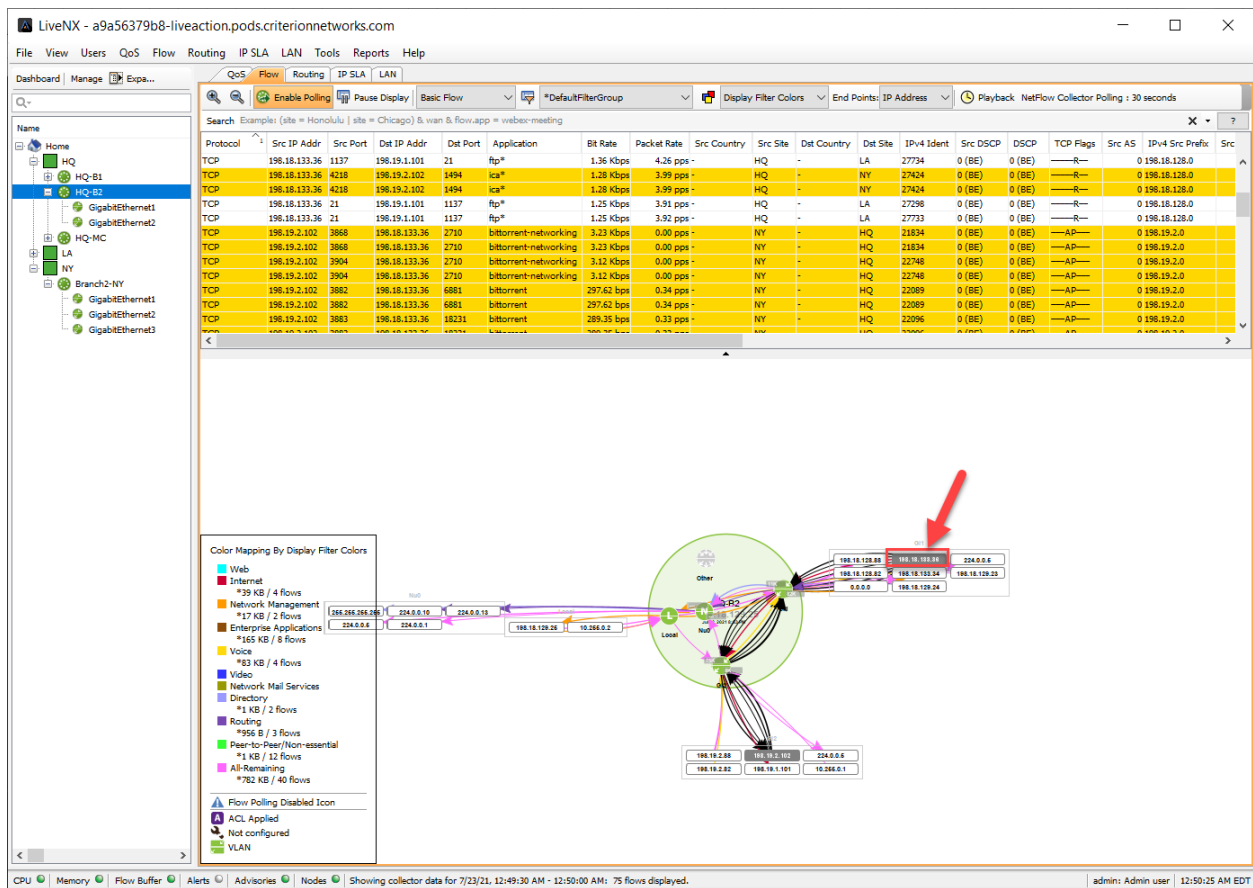
1. Double-click on the Branch2-NY Device or select it on the Home Tree.
2. Select **IP Addresses** as the endpoint display type



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.



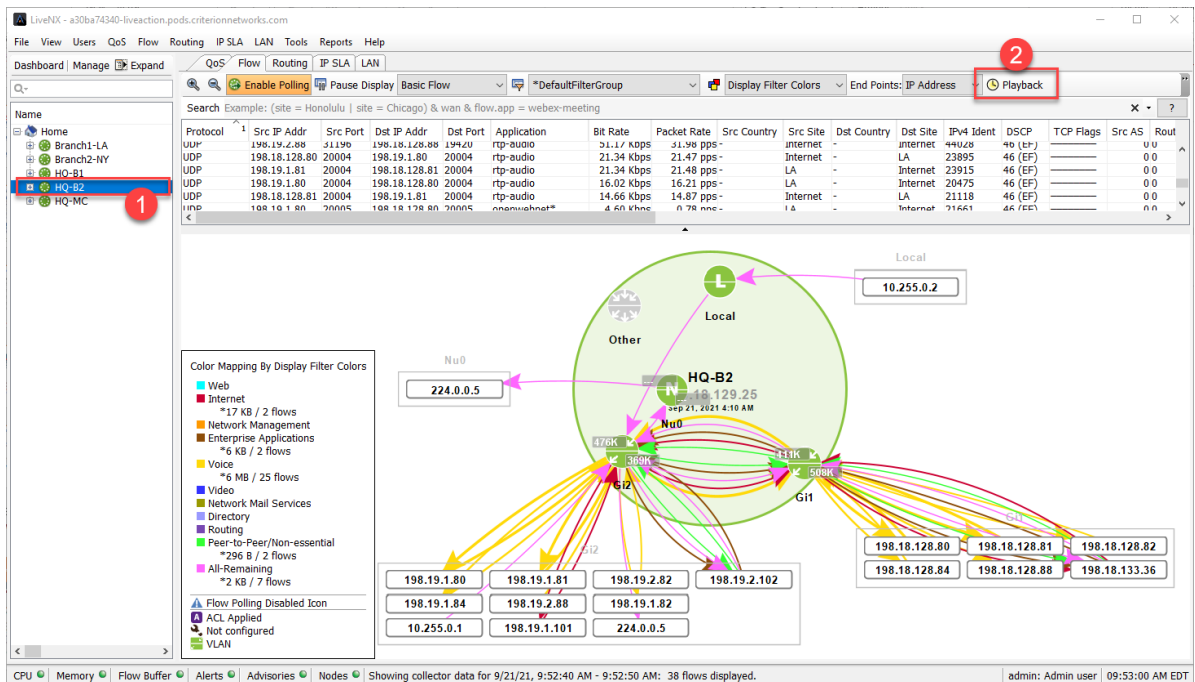
There is some other traffic, such as rtp, sip, and Citrix... but these 2 IPs are mostly generating BitTorrent. Make sure there isn't a ghost server in your network serving movies and such!

## Lab 4.4: Troubleshoot Issues

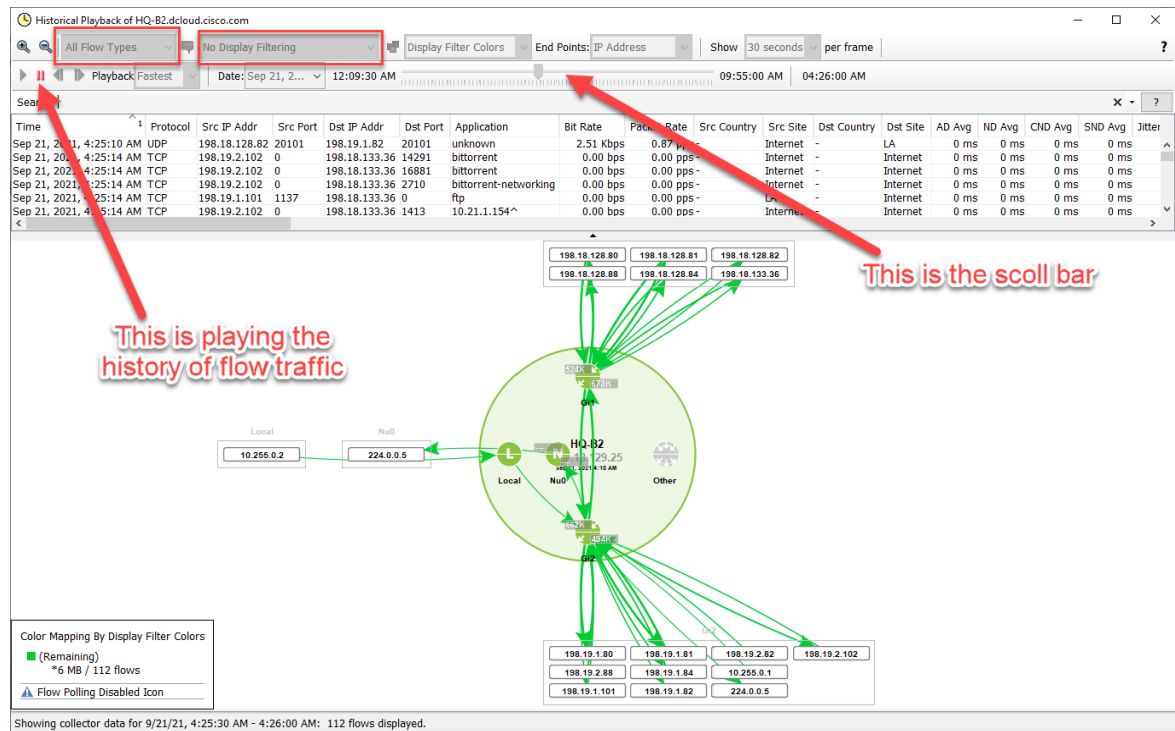
Users in the Marketing Department at our San Jose Headquarters have been complaining that their workstations seem to be “slowing down” numerous times a day. A pattern is developing that this happens about 4x per hour!

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**.



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



**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

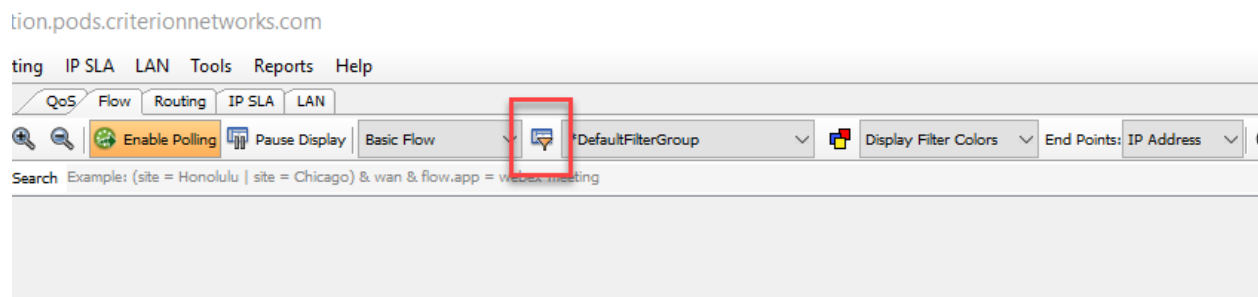
## Lab 5.1: Creating Custom Filters

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.

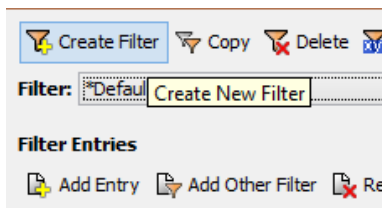
- In this lab you'll create a custom filter based-upon given ports to identify SIP and RTP traffic and verify their markings. Ports being used for the filters in this lab are:
  - SIP Ports: 5060 5061 5062
  - RTP Ports: 16384–32767

Lab Steps:

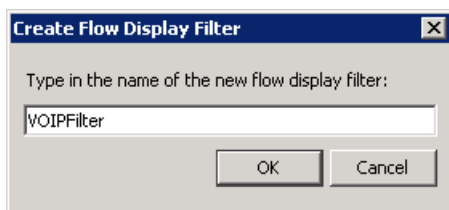
1. Select **HQ-B1**, and then click the **Filter** icon (looks like a funnel) to Open the Flow Display Filters Set-Up.



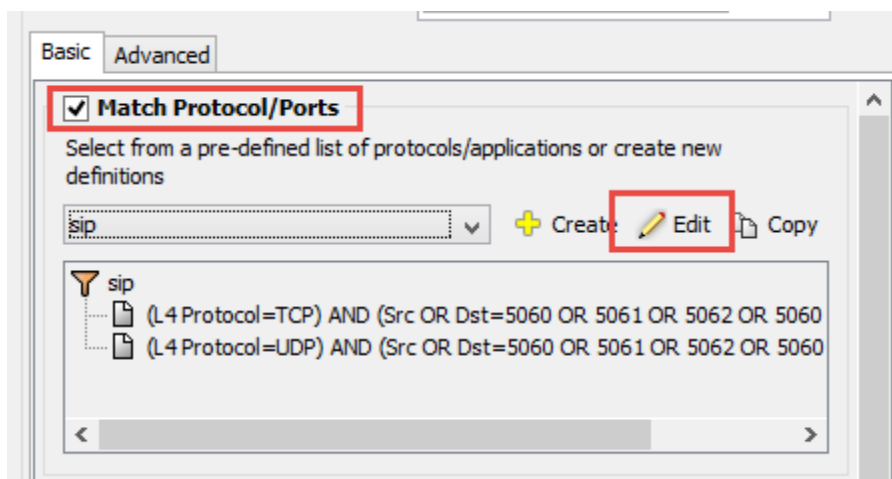
2. Click **Create Filter** on the top right of the Flow Display Filters Set-Up.



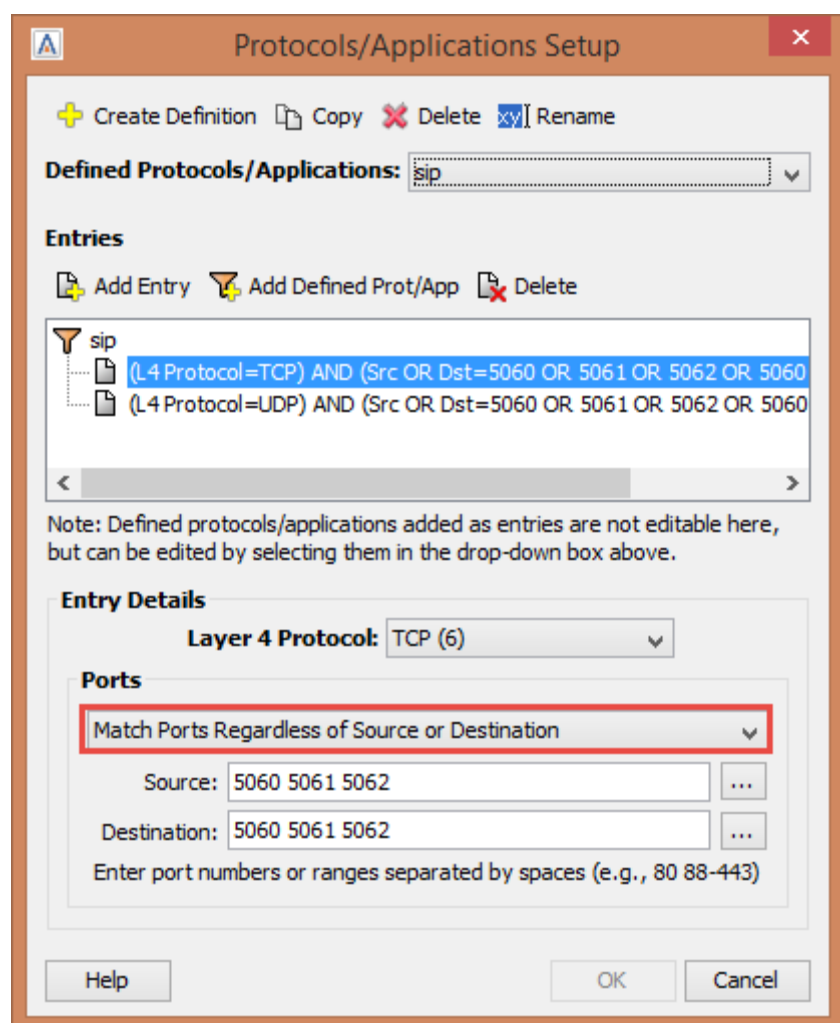
3. Enter a Name label:



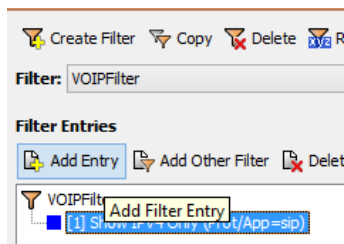
4. On the **Basic** Tab, check **Match Protocol/Ports** and select the **SIP** Protocol.
5. Click Edit.



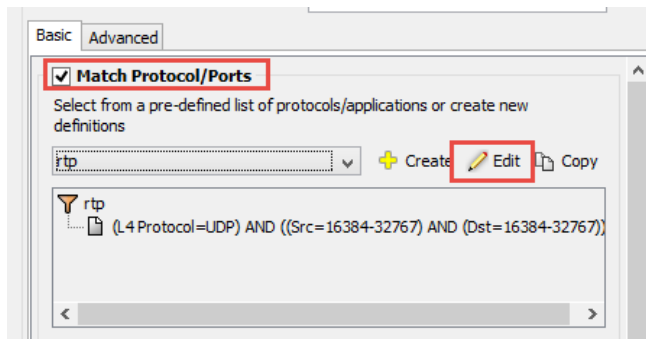
6. Edit both entries, for TCP and UDP, to match the ports provided.
7. Select to **"Match Ports Regardless of Source and Destination"** for both TCP and UDP.



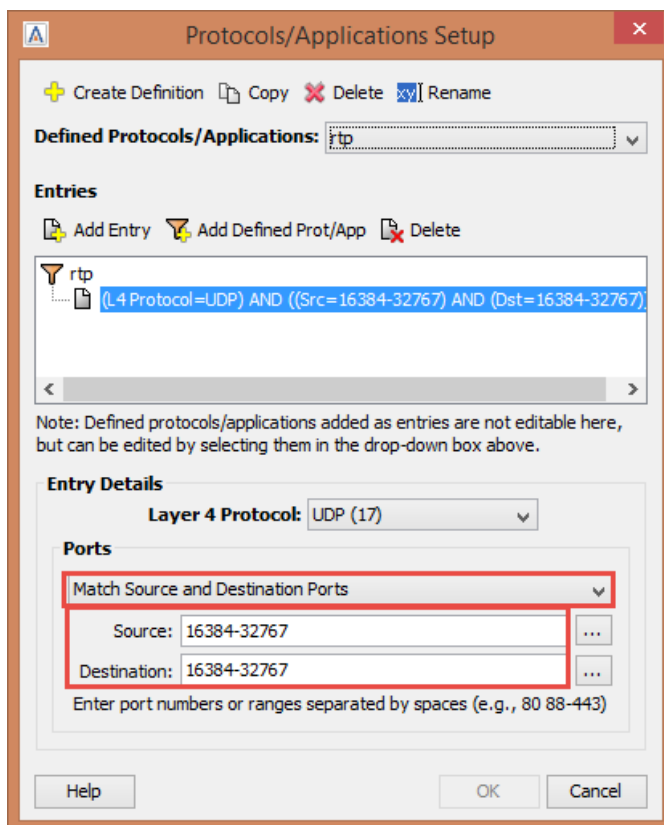
8. Click **OK**
9. Click **Add Entry**.



10. Select the “**rtp**” Protocol and **Edit** the ports.



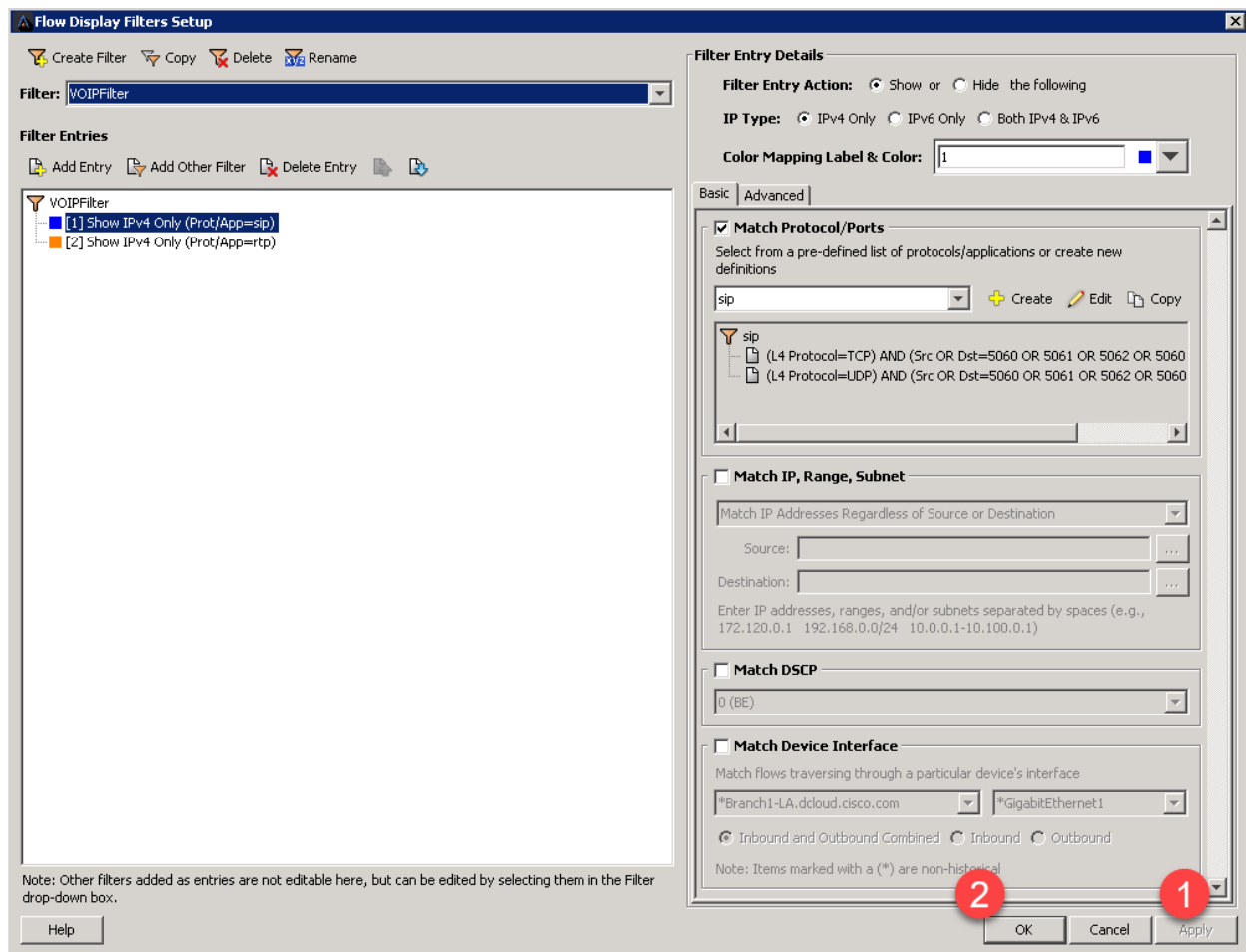
11. Edit the UDP Entry to “**Match Source and Destination Ports**” to 16384-32767 for both **source and destination**.



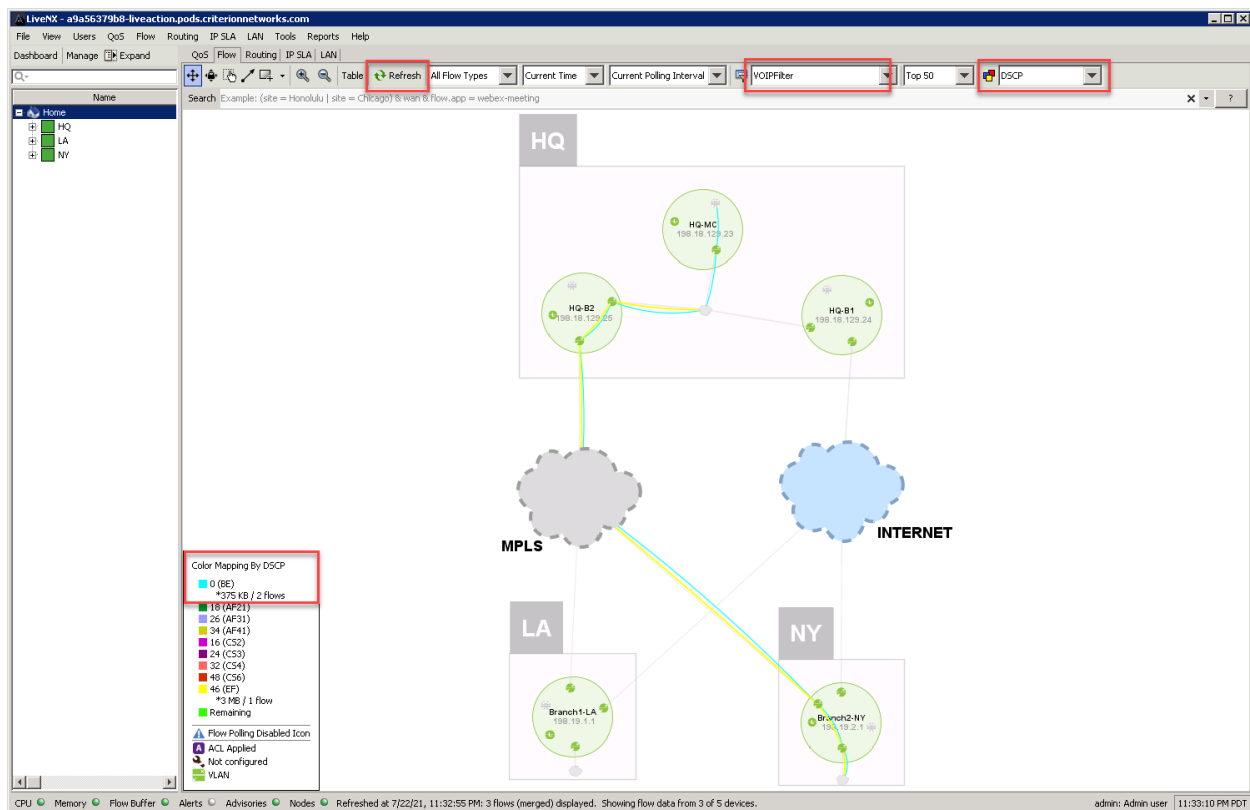
12. Click **OK**

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





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



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.

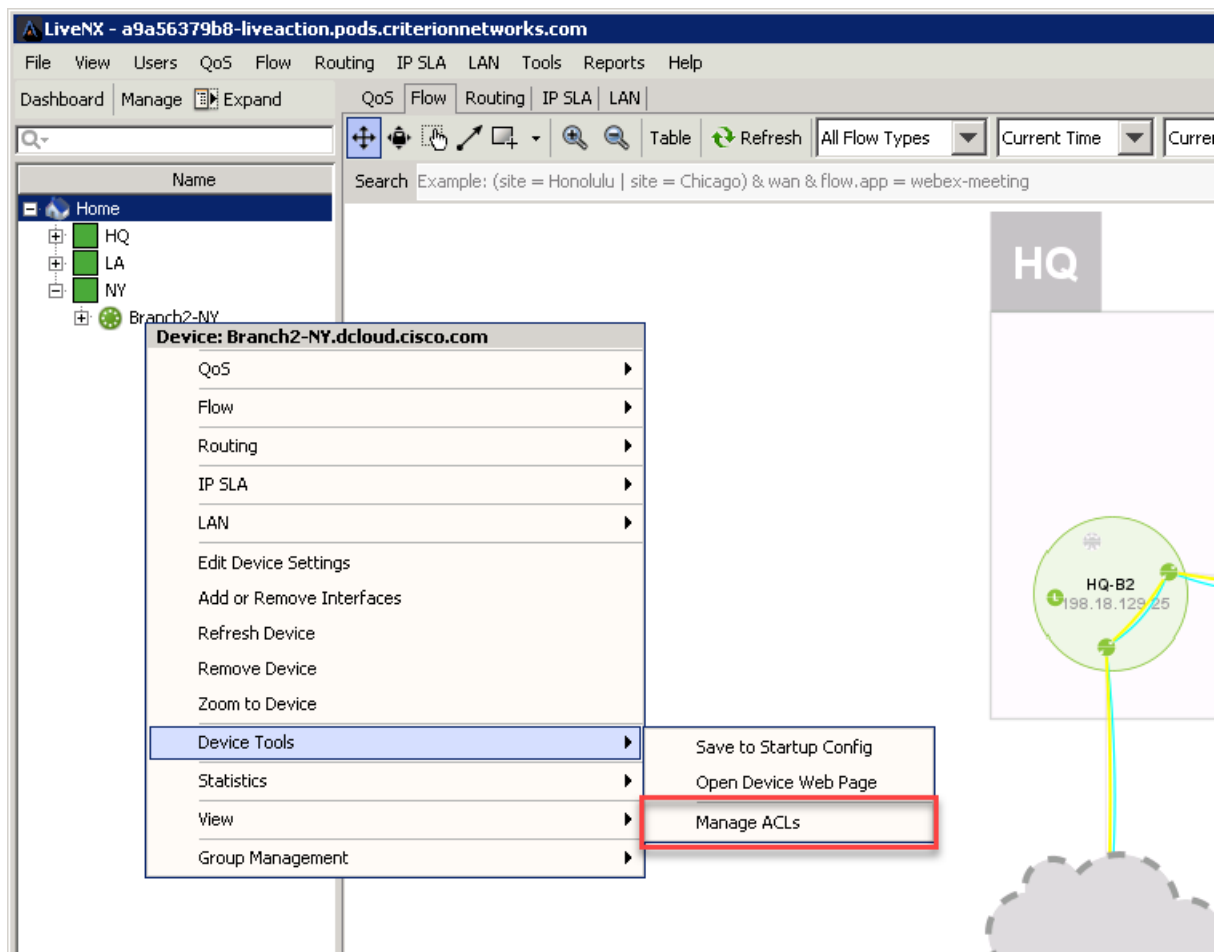
## Lab 5.2: ACL Creation

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**.



2. Select **Create ACL**

ACL Management for Branch2-NY

Current RouterBranch2-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)	

Create ACL

Edit ACL

Delete ACL

Copy ACL

Apply / Remove ACL

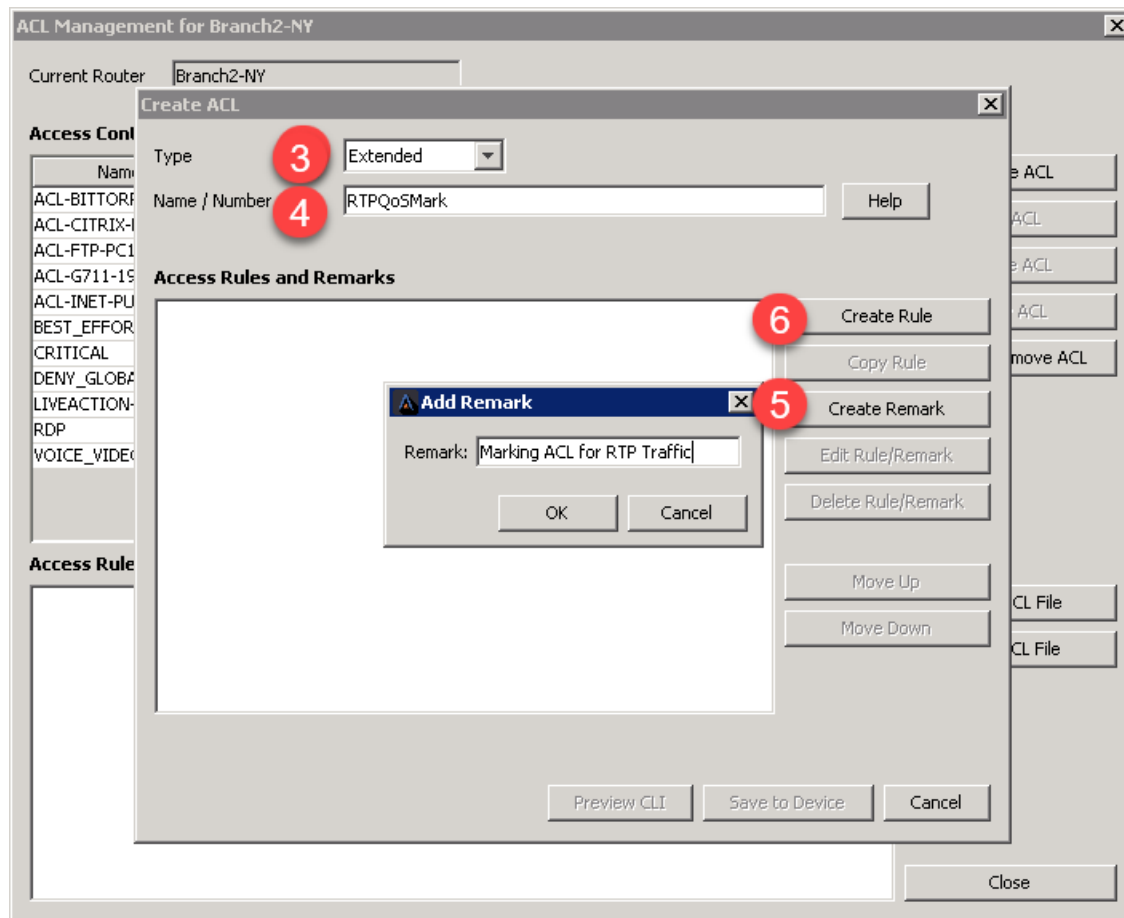
Access Rules and Remarks

Save ACL File

Load ACL File

Close

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 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.

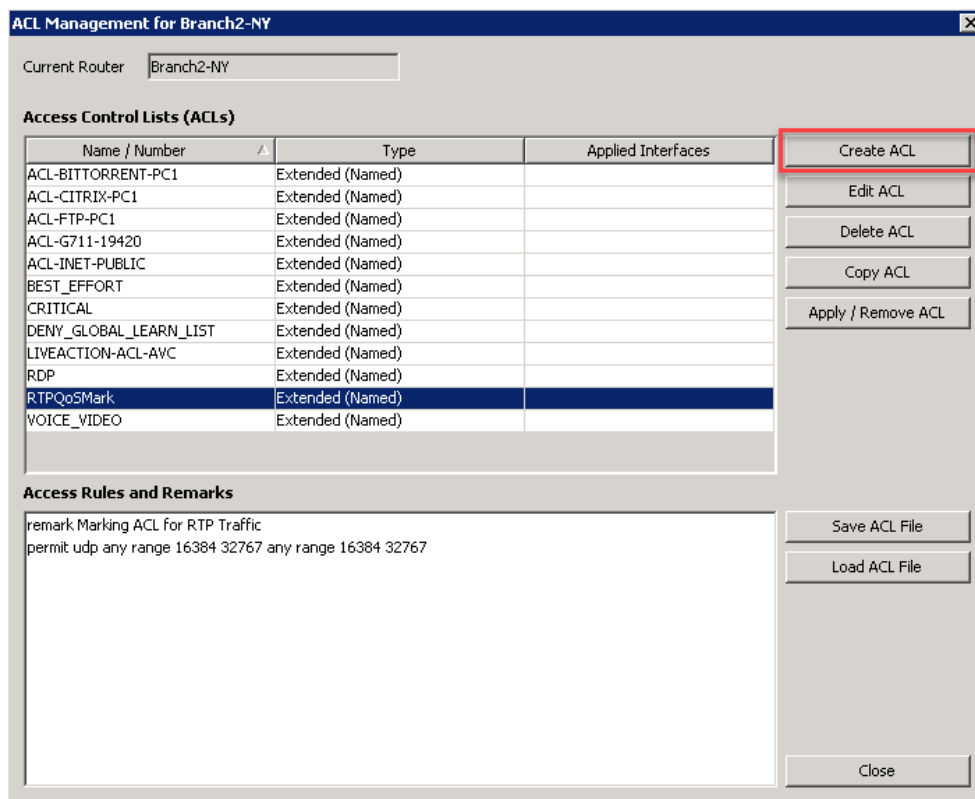
The screenshot shows the 'Add Extended Rule Entry for RTPQoSMark' dialog box. The 'UDP' protocol is selected. Both Source and Destination are configured with 'by Port' selected, 'Between' as the operator, and '16384 32767' as the port range. The 'Match' checkbox is unchecked, and 'Log Rule' is set to 'Log'.

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

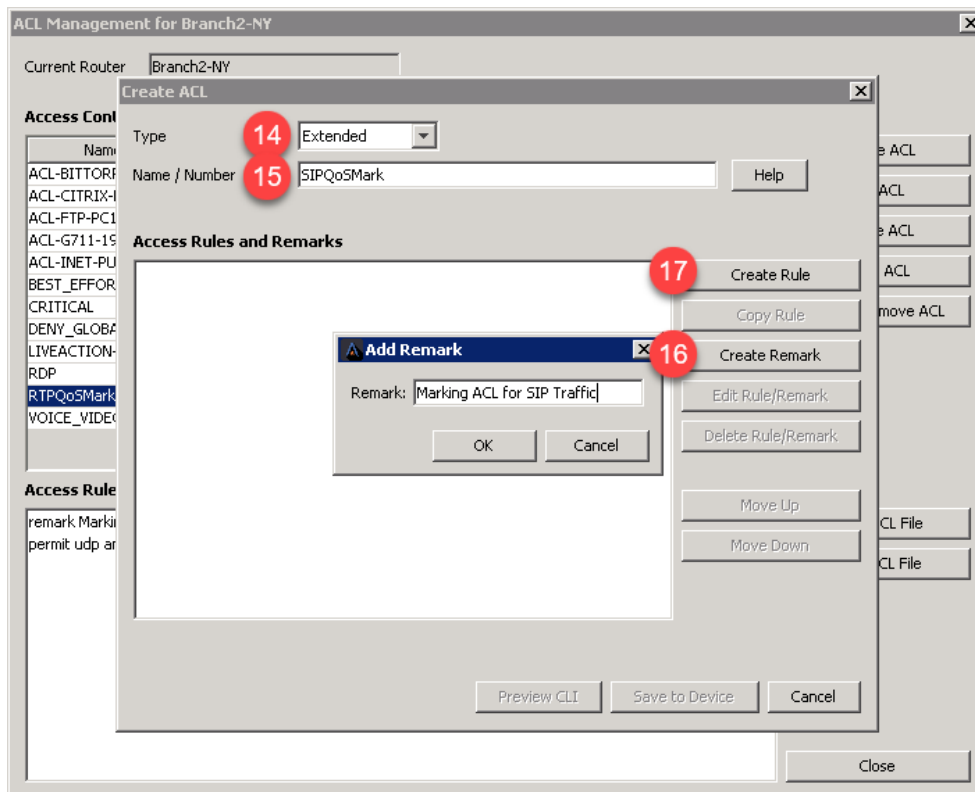
12. Click **Save to Device**.

The screenshot shows the 'Edit Extended ACL RTPQoSMark' dialog box. The 'Type' is 'Extended' and the 'Name / Number' is 'RTPQoSMark'. The 'Access Rules and Remarks' section shows a rule: 'permit udp any range 16384 32767 any range 16384 32767'. The 'Preview CLI' and 'Save to Device' buttons are highlighted with a red box.

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



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**.



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.

The screenshot shows the 'Add Extended Rule Entry for SIPQoSMark' dialog box. The 'Source' section is configured with 'TCP' as the protocol, 'any' as the source, and 'by Port' checked with the operator 'Between' and the port range '5060 5062'. The 'Destination' section is configured with 'any' as the destination. The 'Match' checkbox is unchecked, and the 'Log Rule' checkbox is checked with 'Log' selected. The 'OK' and 'Cancel' buttons are at the bottom right.

Next create another rule for destination SIP Ports.



**Edit Extended ACL SIPQoSACL**

Type:

Name / Number:

**Remarks**

**Access Rules**

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  ☐ Other

**Source**

☒ any ☐ by Network or IP  ☐ by Object-Group

☐ by Port

☐ Match

☐ Log Rule

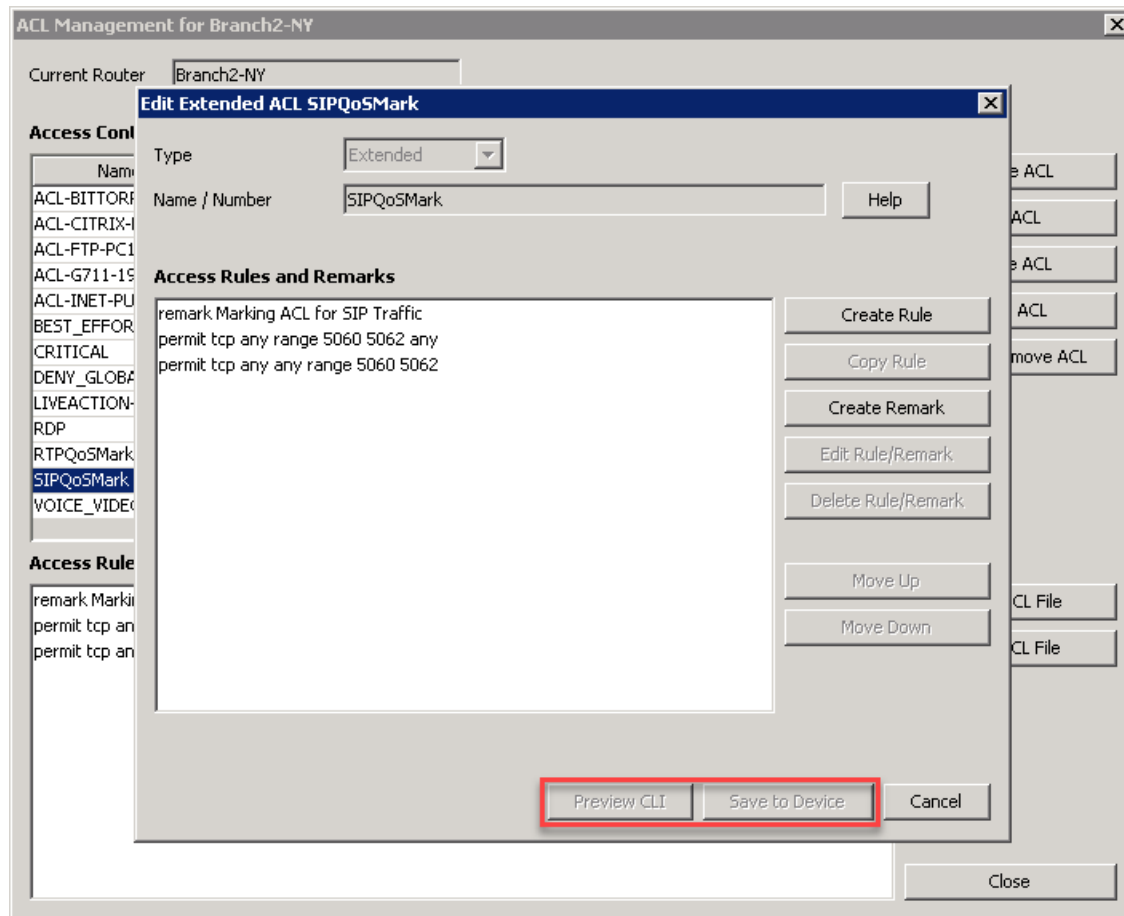
**Destination**

☐ any ☐ by Network or IP  ☐ by Object-Group

☒ by Port

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

31. Click **Save to Device**.



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

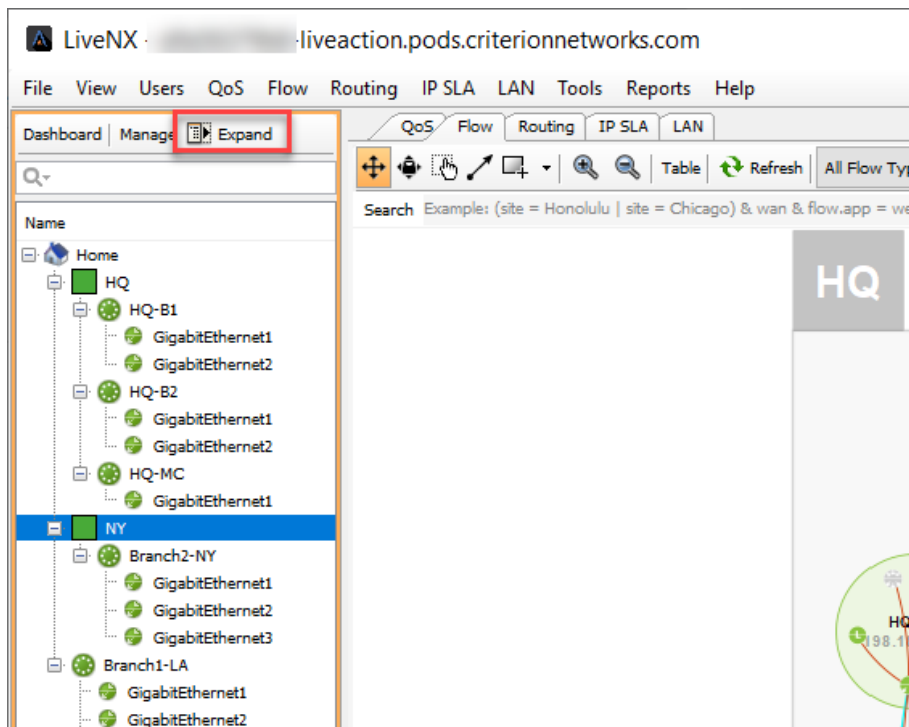
**Note:** Semantics may have already been configured on most of the devices in this Lab. You need to ensure that all the devices have their semantics entered.

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.

The screenshot shows the LiveNX interface with a network topology table. The table lists various network devices and their configurations. The 'Branch1-LA' device is highlighted in blue. A red box highlights the 'Details' sidebar on the right, which shows the configuration for the selected device. A red text overlay in the center of the table says 'Branch1-LA has been selected'.

Name	IP Address	Node	Label	Input Capacity	Output Capacity	WAN/XCon	Service Provider	Site	Site IP
HQ									
HQ-B1	198.18.129.24	Local						HQ	10.0.0.102.10.25
GigabitEthernet1	198.18.129.24								
GigabitEthernet2	100.64.0.2			4.0 Mbps	4.0 Mbps	WAN	Internet	HQ	10.0.0.102.10.25
HQ-B2	198.18.129.25	Local						HQ	10.0.0.102.10.25
GigabitEthernet1	198.18.129.25								
GigabitEthernet2	10.255.0.2					WAN	Default Service Provider		
HQ-MC	198.18.129.23	Local						HQ	10.0.0.102.10.25
GigabitEthernet1	198.18.129.23								
NY								NY	198.19.2.0/24
Branch2-NY	198.19.2.1	Local							
GigabitEthernet1	198.19.2.1			2.0 Mbps	2.0 Mbps	WAN	Internet		
GigabitEthernet2	100.64.2.2			2.0 Mbps	2.0 Mbps	WAN	MPLS		
GigabitEthernet3	10.255.2.2			2.0 Mbps	2.0 Mbps	WAN	MPLS		
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1.198.19.1.0/24
GigabitEthernet1	198.19.1.1		Branch1 LAN	2.0 Mbps	2.0 Mbps	WAN	Branch1 LAN		
GigabitEthernet2	100.64.1.2					WAN	Internet		
GigabitEthernet3	10.255.1.2		MPLS			WAN	MPLS		

**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 **LAN** Collapse

Q-

Name	IP Address	Node	Label	Input Capacity	Output Capacity	WAN/Con	Service Provider	Site	Site IP
Home									
HQ									
HQ-B1	198.18.129.24	Local							
GigabitEthernet1	198.18.129.24								
GigabitEthernet2	100.64.0.2			4.0 Mbps	4.0 Mbps	WAN	Internet	HQ	10.0.0.102.10.255
HQ-B2	198.18.129.25	Local							
GigabitEthernet1	198.18.129.25						Default Service Provider	HQ	10.0.0.102.10.255
GigabitEthernet2	10.255.0.2		HQ	2.0 Mbps	2.0 Mbps	WAN	MPLS	HQ	10.0.0.102.10.255
HQ-MC	198.18.129.23	Local							
GigabitEthernet1	198.18.129.23								
NY									
Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24
GigabitEthernet1	198.19.2.1								
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								
GigabitEthernet2	100.64.1.2		Branch1 LAN	2.0 Mbps	2.0 Mbps	WAN	Branch1 LAN		
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\_comacd

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**

The screenshot shows the LiveNX dashboard with a network topology on the left and a details panel on the right. The topology includes HQ, NY, and Branch1-LA sites. The details panel for Branch1-LA shows CPU and memory usage, device details, and site information. Red arrows indicate the flow from the table row to the details panel.

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

Details for Branch1-LA:

- CPU and Memory Usage:** CPU 33%, 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. Table with columns: ✓, Tag, Used.

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.

The screenshot shows the LiveNX dashboard with the 'Dashboard' tab selected. The topology view shows HQ, NY, and Branch1-LA sites. The details panel for Branch1-LA is visible, showing site information and tags.

Name	IP Address
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.

The screenshot shows the 'Flow' tab selected in the dashboard. The 'Flow Alerts - 24 Hours' section displays a graph with the message 'There is no data to display for the given time period'. Below the graph, the 'Flow source' is set to 'wan | xcon'. The 'Basic Flow' section shows data for the time period '07/23/21, 05:45:00 AM to 07/23/21, 06:00:00 AM'. It includes four tables: 'Top 10 Source Addresses', 'Top 10 Destination Addresses', 'Top 10 Source Countries', and 'Top 10 Destination Countries'. Each table lists IP addresses or countries, bytes transferred, and the number of flows.

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

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

Src Country	Bytes	Flows
Unknown	3 MB	500

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.



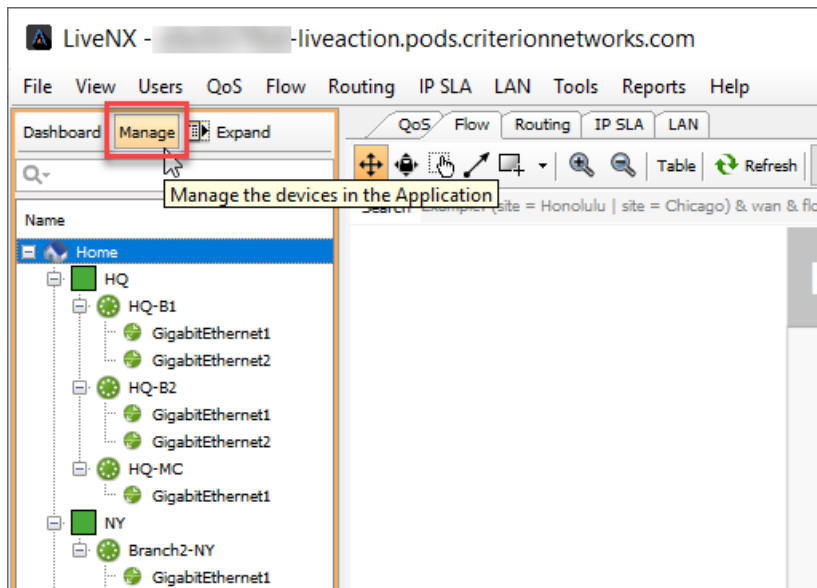
## Lab 6.2: Adding Devices to Groups

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.



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**”

Device Management

Filter by:
Filter
Clear

Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval	Status
<input type="checkbox"/>	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 seconds	Configured
<input type="checkbox"/>	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local	NY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 seconds	Configured
<input type="checkbox"/>	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 seconds	Configured
<input type="checkbox"/>	HQ-B2	198.18.129.25	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 seconds	Configured
<input type="checkbox"/>	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local	HQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10 seconds	Configured

\* LAN polling occurs every 15 minutes
Number of Devices: 5

Device Configurations

Configure
Remove
Add To Group
Remove From Group
Edit Groups

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

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
Edit
Edit

Default SNMP Settings
Default CLI Monitoring Settings - Not Set
Default CLI Configuration Settings

Clear
Clear
Clear

Apply
Close

### 3. Click Add

Edit Groups

Groups

Name	Size	
HQ	3	<input checked="" type="checkbox"/>
NY	1	<input type="checkbox"/>

Add
Edit
Remove

Close

4. Enter **LA** in the Name field.

5. Select **Branch1-LA** from the **All Other Devices** list

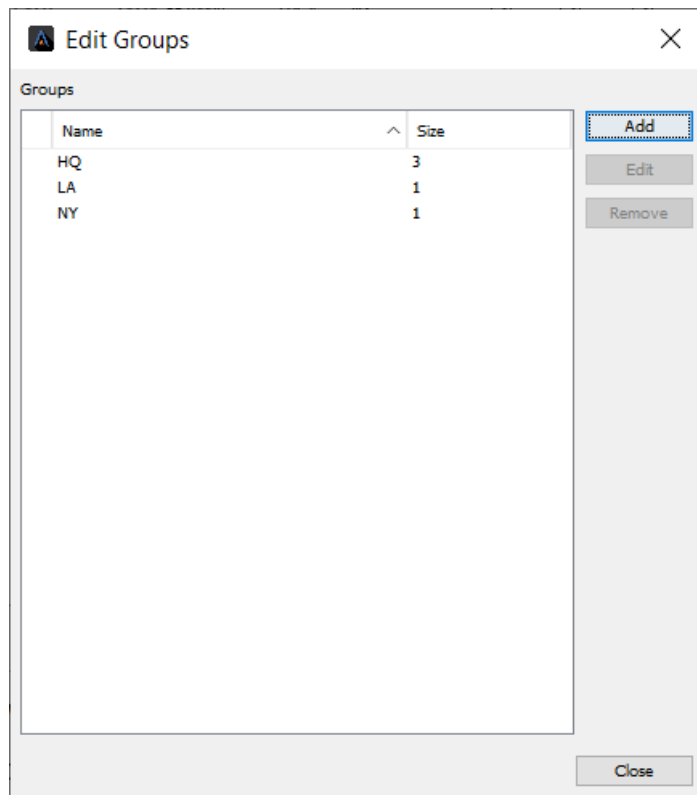
6. click the green **Right** arrow.
7. Click **Add**.
8. Repeat the steps above to create any other groups as necessary.

The screenshot shows the 'Add Group' dialog box. At the top, there is a 'Name (\*)' field containing 'LA' (marked with a red circle 4) and a 'Description' field. Below these are two list boxes: 'All Other Devices' (marked with a red circle 5) and 'Current Group of Devices' (marked with a red circle 6). The 'All Other Devices' list contains '(NY) Branch2-NY' (highlighted), '(HQ) HQ-B1', '(HQ) HQ-B2', and '(HQ) HQ-MC'. The 'Current Group of Devices' list contains 'Branch1-LA'. Between the lists are green right and left arrows. At the bottom right, there is an 'Add' button (marked with a red circle 7), a 'Done' button, and a 'Cancel' button. A note at the bottom left states 'Asterisks (\*) indicate required fields.'

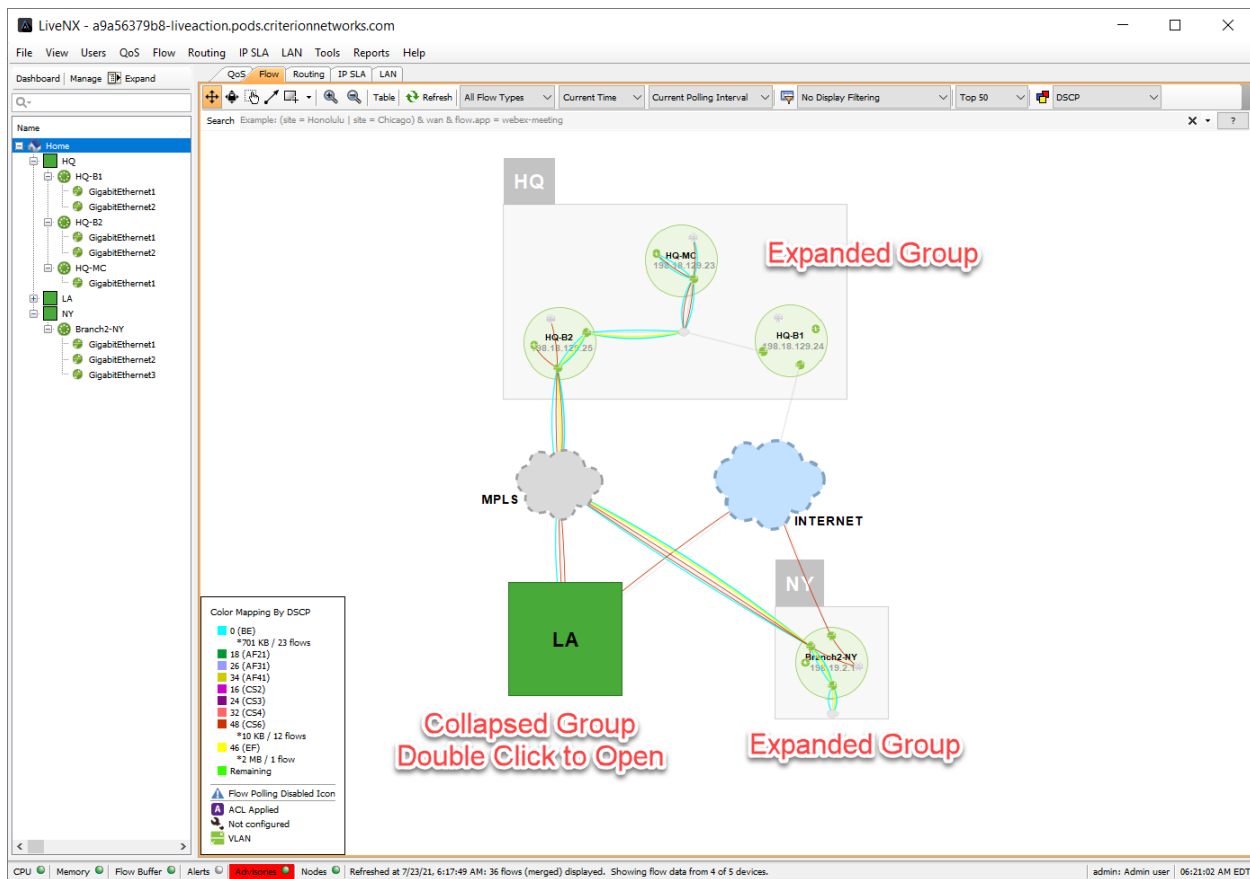
9. Once all groups have been created and devices correctly added, select **Done**.

Once completed your groups should look like the one below.

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



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.



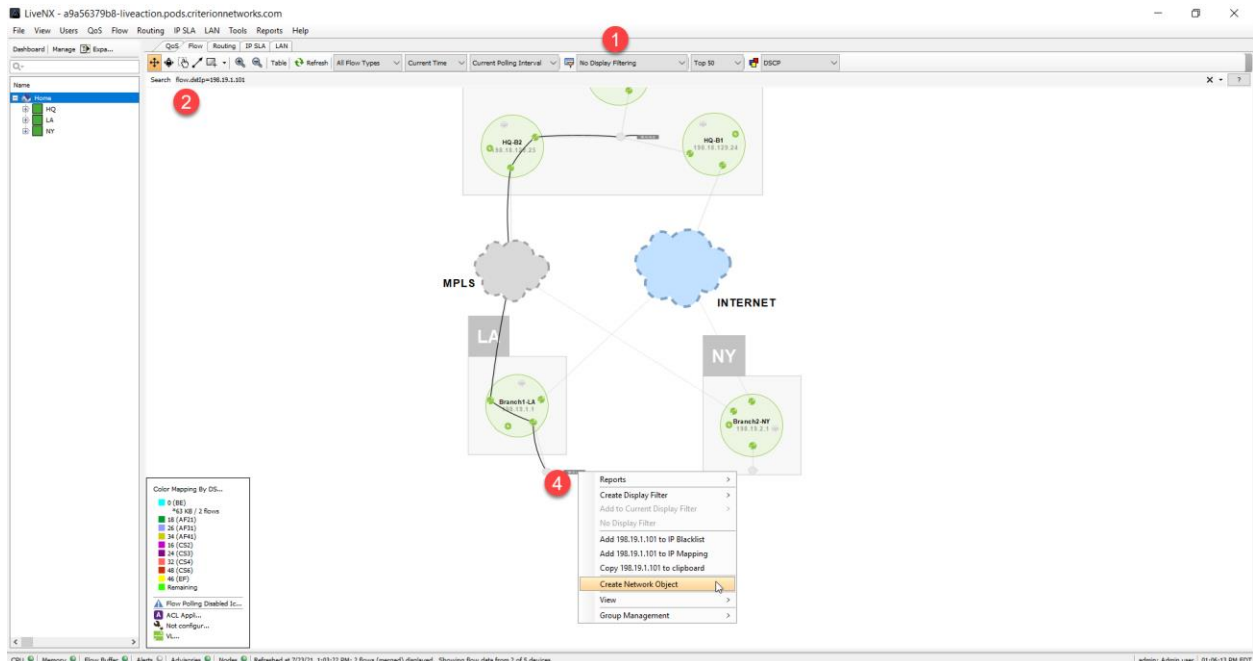
## Lab 6.3: Creating Network Objects

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**



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 ▼

Size IP Phone

Size Laptop

Tooltip Network Cloud


Tooltip Network Cloud (blue)

\* Required File PC

Router

Switch Processor

Custom... ▼



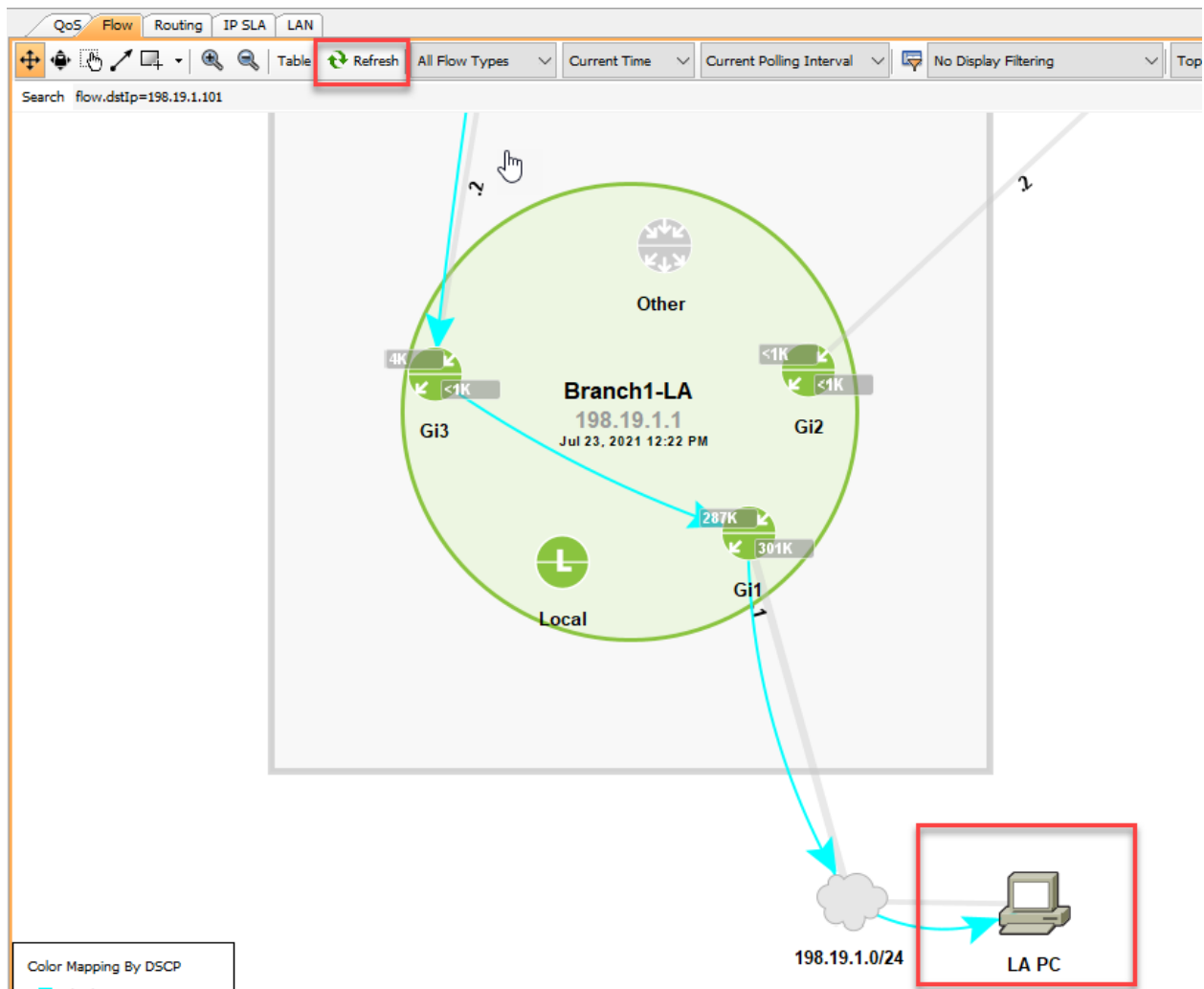
OK Cancel

**5**

**6**

7. Click Refresh.

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



**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.

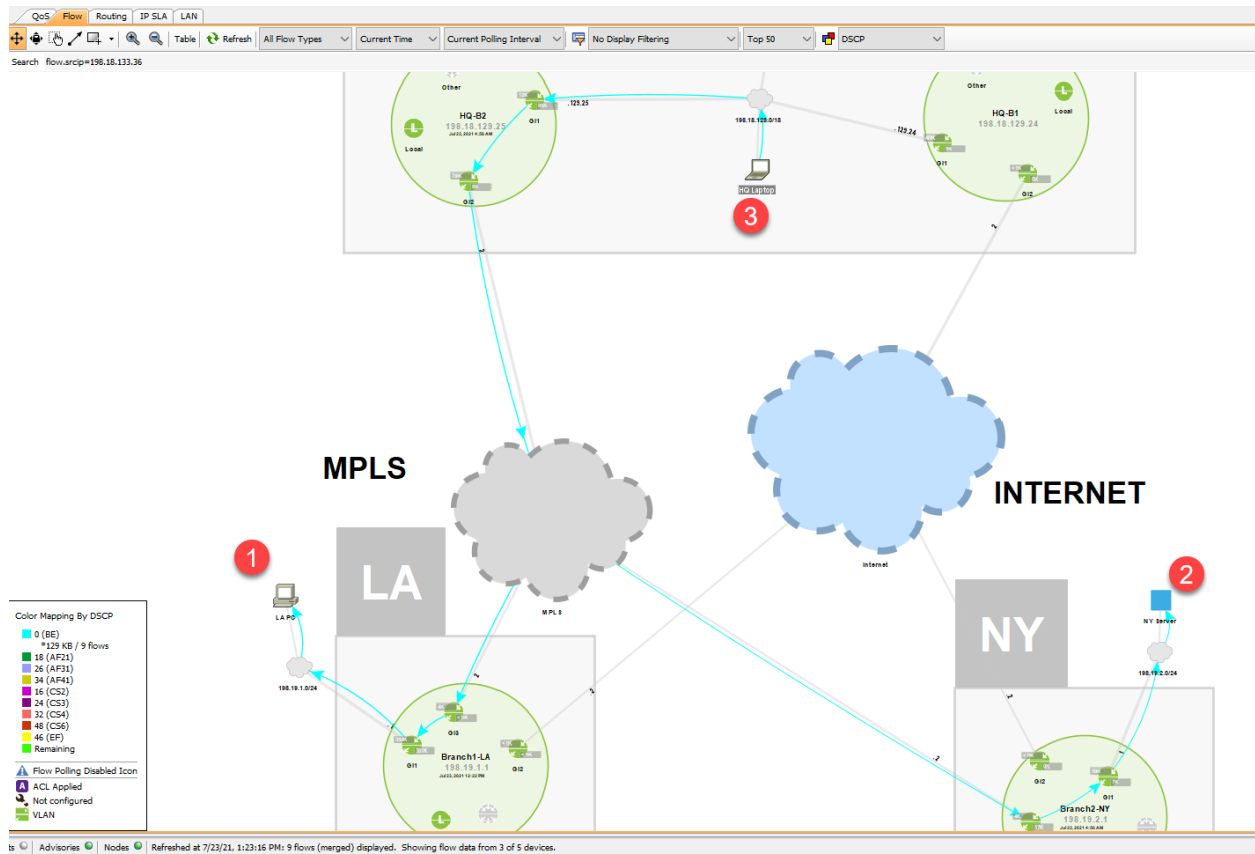
Object/Shape

- Generic Square
- IP Phone
- Laptop
- Network Cloud
- Network Cloud (blue)
- PC
- Router
- Switch Processor

OK Cancel

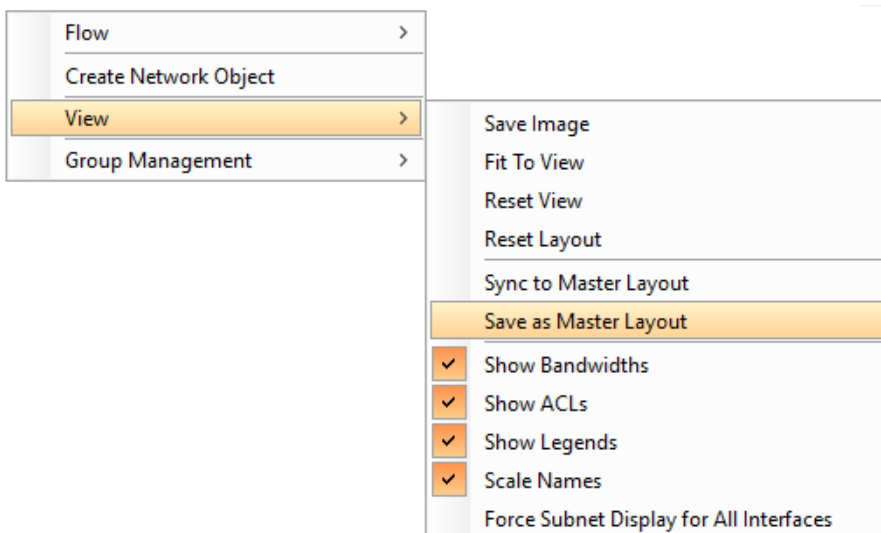
11. Select an Object/Shape as **"File Server"**.
12. Click **OK**. This will add the device to the diagram
13. Next, add a Laptop in HQ.
14. Enter the search string: flow.srcip=198.18.133.36
15. Select the flow (it will be near the HQ-B1 and HQ-B2 routers), right click on the IP Address endpoint.
16. 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.



**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

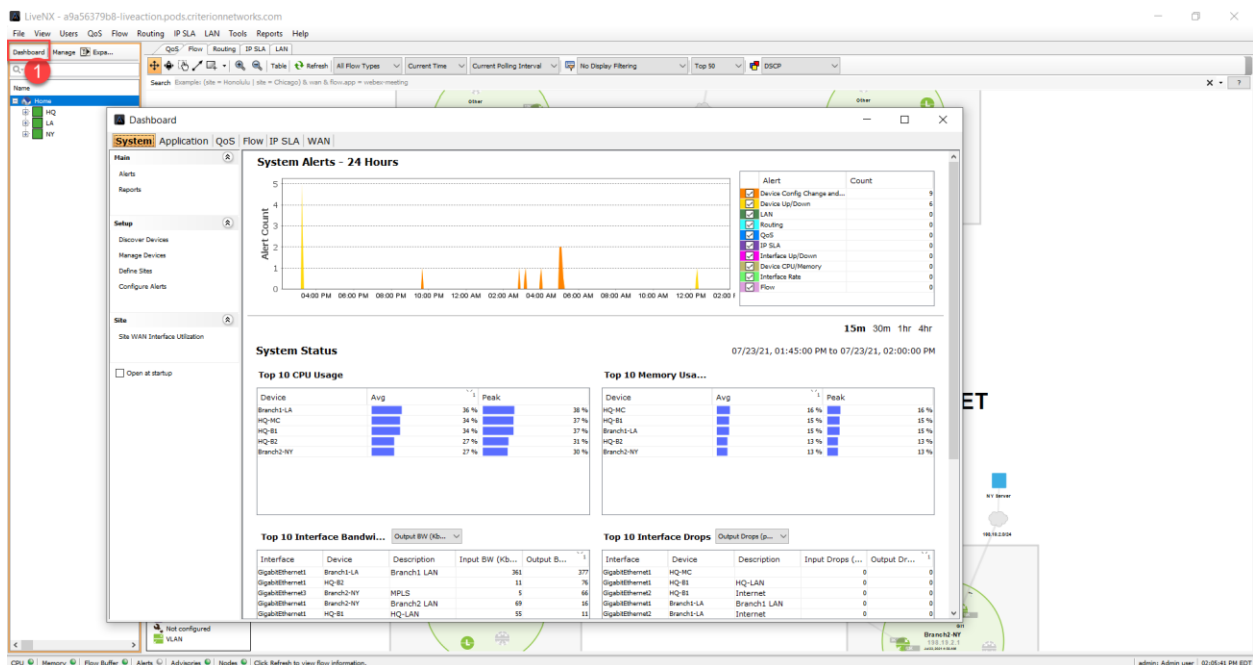
# Lab 7.1: The Dashboard

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.

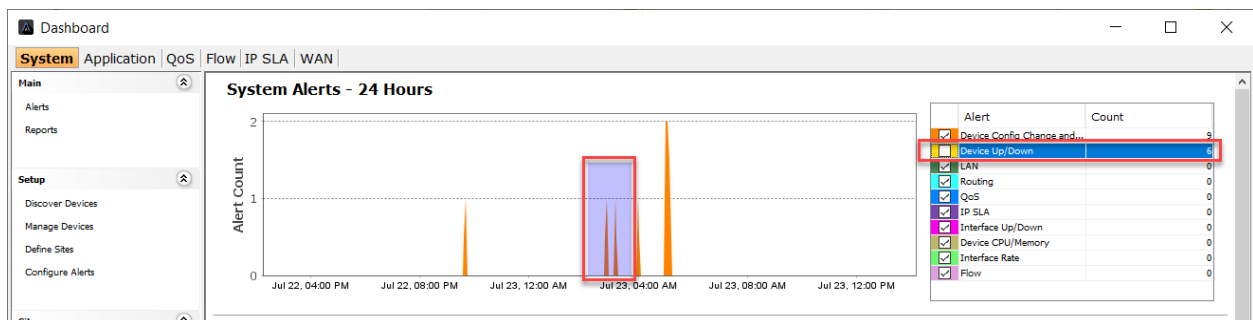
## Lab Steps:

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



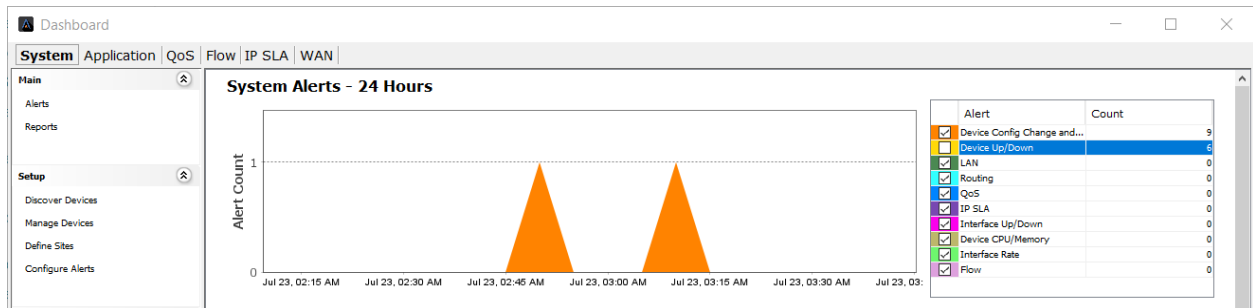
The Dashboard displays, showing a time-series of Alert Counts for the past 24-hours. To the right of the time-series note the Alert Type and Count.

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.

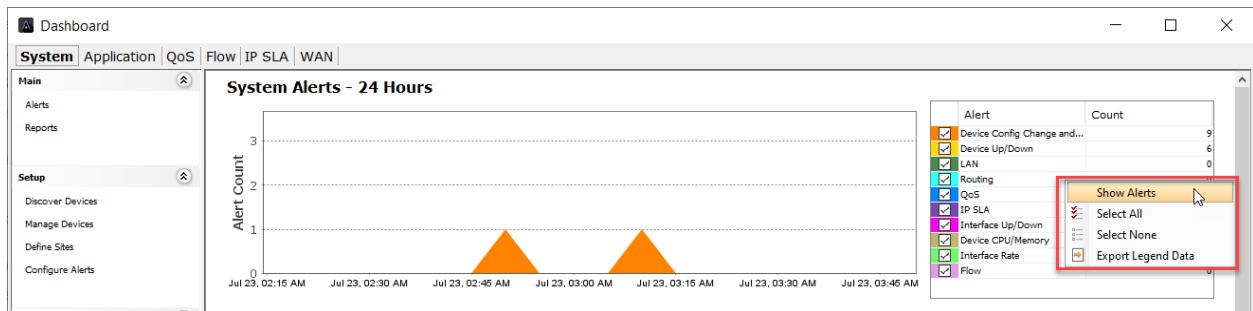


**Note:** Your results may not look the same as the images in this Lab. These images are for example purposes only.

**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!



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



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	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 08:44:30 PM	Warning	HQ-SJ	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 09:04:02 PM	Warning	HQ-SJ	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 11:01:01 PM	Warning	HQ-SJ	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 01:35:02 PM	Warning	Branch1-LA	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 05:49:30 PM	Warning	Branch1-LA	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 09:04:02 PM	Warning	Branch1-LA	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 11:01:01 PM	Warning	Branch1-LA	Flow	High media packet loss percent...	High media packet loss percent...
2016/05/13 01:00:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; ...
2016/05/13 01:01:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; ...
2016/05/13 01:06:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; ...
2016/05/13 01:07:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; ...
2016/05/13 01:11:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; ...
2016/05/13 01:12:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; ...
2016/05/13 01:17:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; ...
2016/05/13 01:17:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; ...
2016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0; ...
2016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1; ...
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; ...

☒ Filter by Time  
Start Time: 05/13/16 12:00:00 PM  
End Time: 05/14/16 12:00:00 PM

☐ 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.

Flow Reports

Q- Type here to filter reports.

Reports

- Interface Bandwidth
- Top Analysis**
- IPs and Ports
- Address
- Applications
- QoS
- Network
- Medianet
- Applications (AVC)
- NSEL
- PR
- Wireless
- AnyConnect
- Miscellaneous
- Custom Reports

Report Actions

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

Top Analysis

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

Execute Report

Source

HQ-SJ

All Interfaces

Filter

\*DefaultFilterGroup

Inbound

Number of flows: 1

CSV File Results

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=6284274599932723200

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

< Previous

Flows 1 - 1

Next >

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.

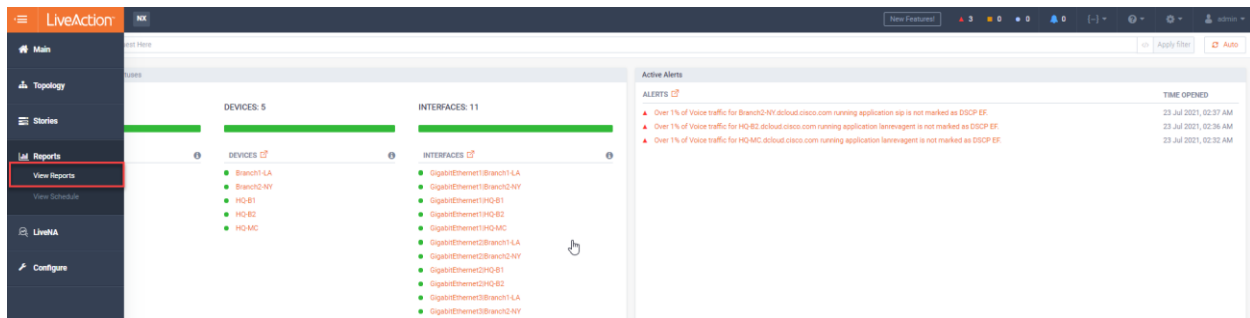
## Lab 7.2: Viewing Reports

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? ;-).

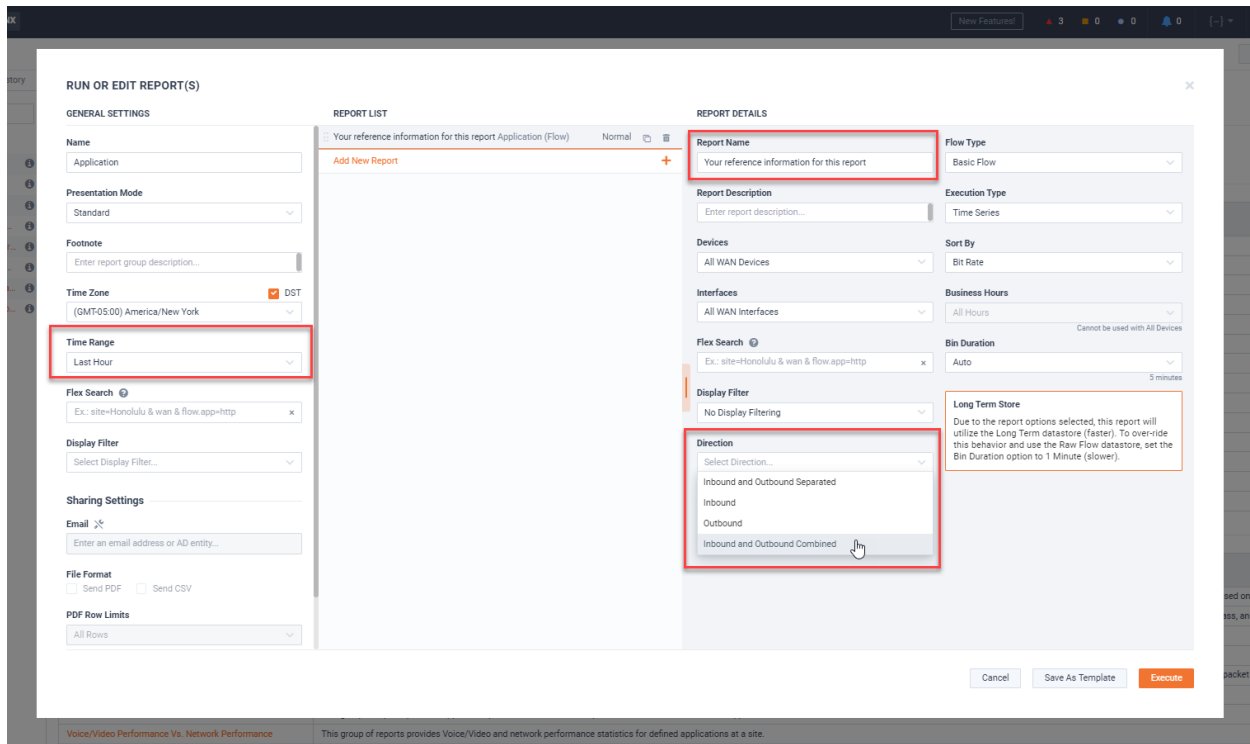
Lab Steps:

### 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.



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.



6. Click **Execute**.





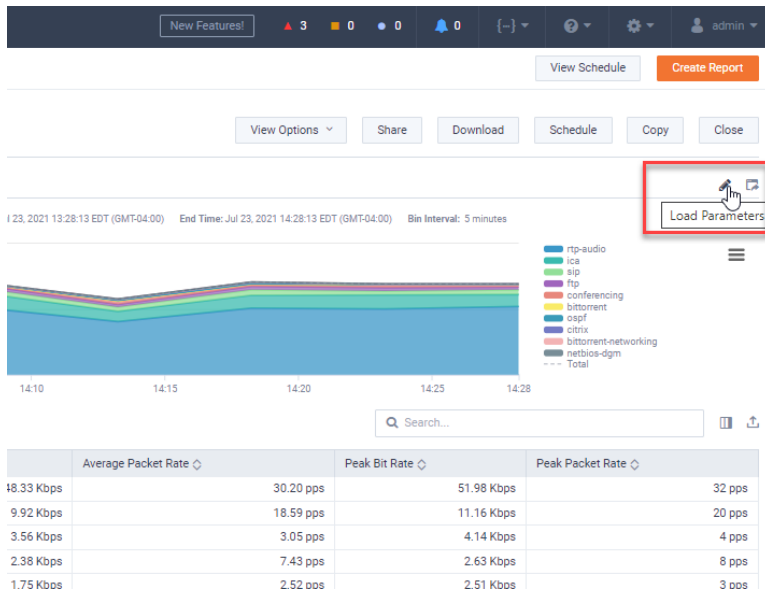
**Note:** Your results may not look the same as the images in this Lab. These images are for example purposes only.

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).

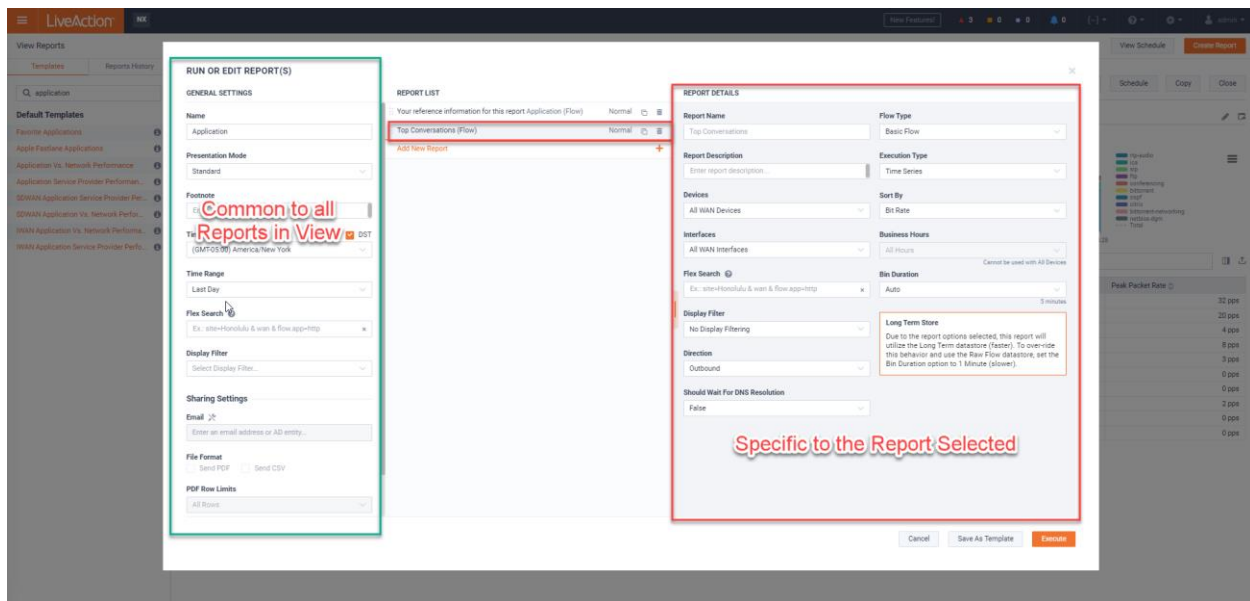
When you run a report... try to do filtering and searching so the system only needs to pull appropriate data to answer your question. LEAVE THE REPORT OPEN!

## 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.

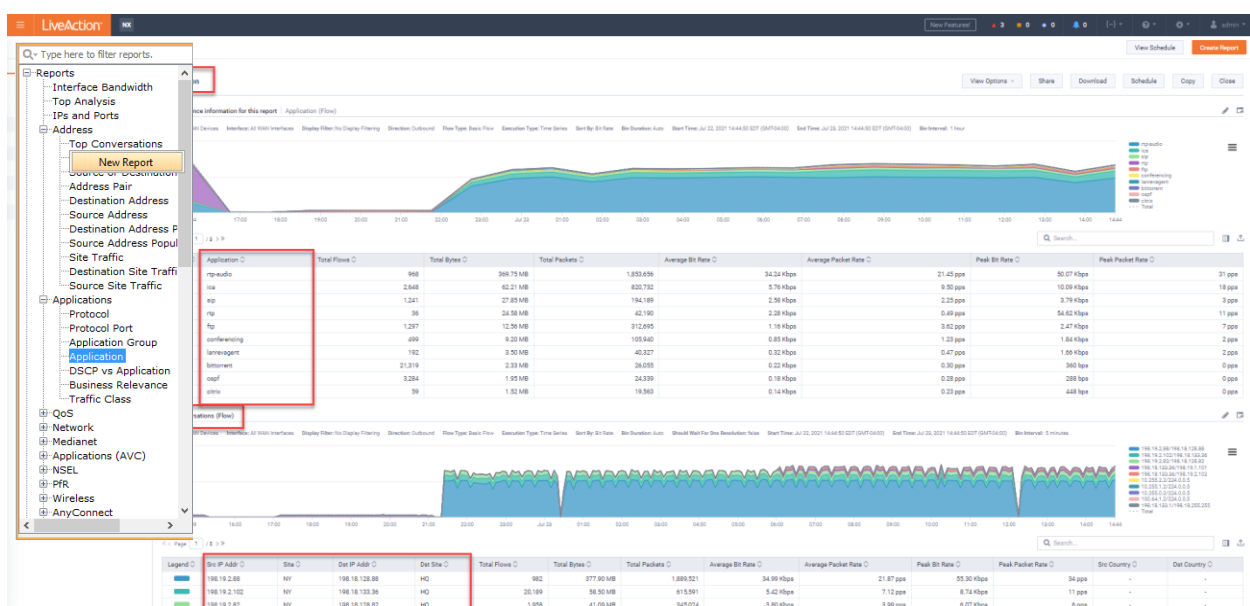


2. Click **Add New Report**, and then select **Top Conversations**.
3. You will be able to configure parameters that will affect both reports, and certain parameters specifically for the **Top Conversations** report. These parameters are independent of the original **Applications** report.



#### 4. Click **Execute**.

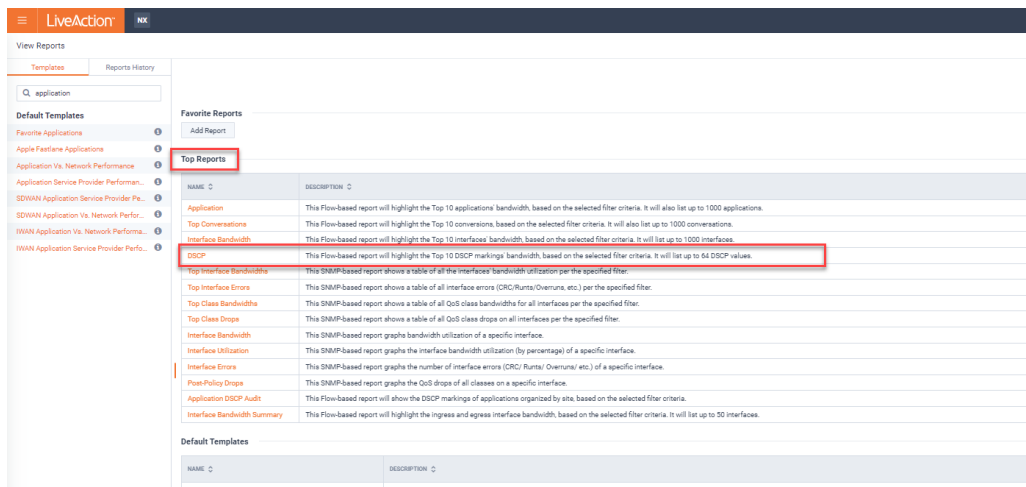
**Note:** Your results may not look the same as the images in this Lab. These images are for example purposes only.



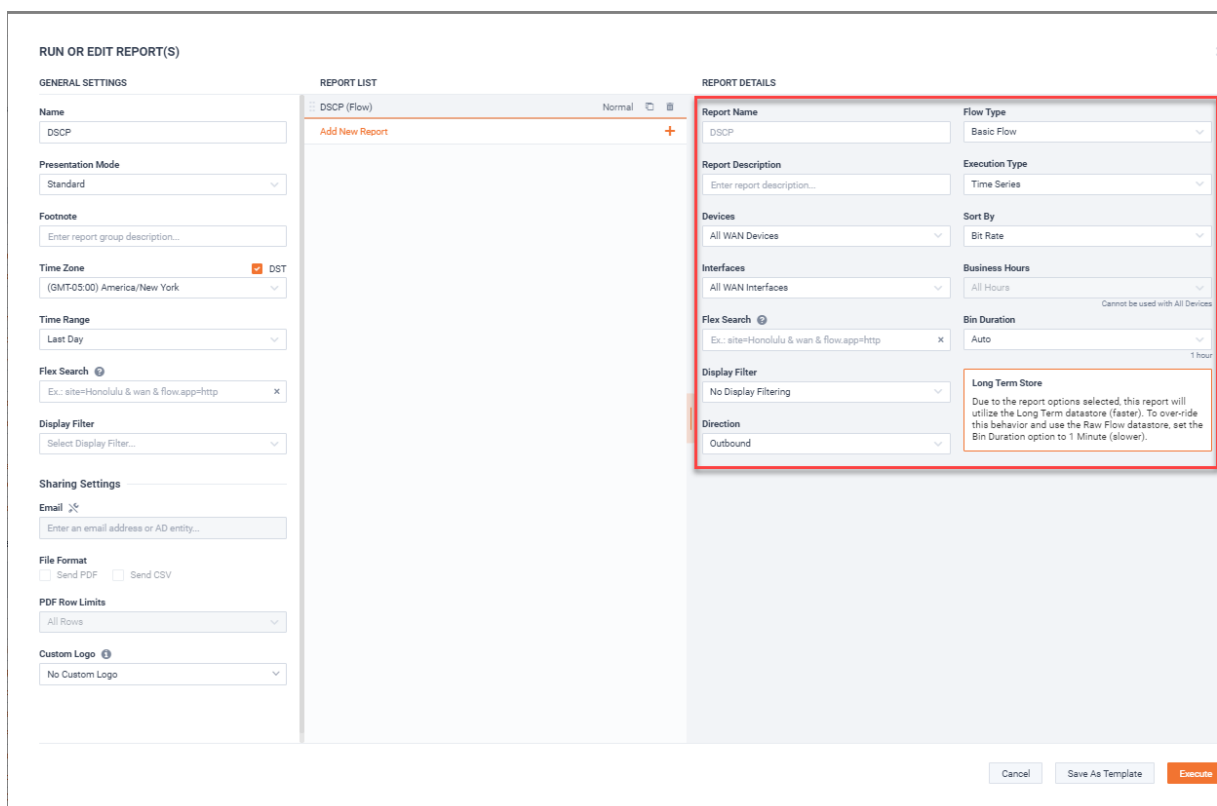
This **Top Conversations** report has been appended to the **Applications** report. in the selected time period including Source address, Destination address, total flows, etc.... a good way to see who is using the bandwidth, and what for... All that BitTorrent may not be good for business! Right-clicking 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**.



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



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		
<input checked="" type="checkbox"/>	0 (BE)	40,832	5 GB	16,556,237	49 Mbps	18396 pps	49.8 Mbps	18641 pps		
<input checked="" type="checkbox"/>	46 (EF)	366	250 MB	1,604,622	2 Mbps	1783 pps	2.3 Mbps	1833 pps		
<input checked="" type="checkbox"/>	26 (AF31)	131	33 MB	460,629	291 Kbps	512 pps	344.9 Kbps	607 pps		
<input checked="" type="checkbox"/>	34 (AF41)	230	27 MB	40,823	240 Kbps	45 pps	301.4 Kbps	56 pps		
<input checked="" type="checkbox"/>	8 (CS1)	197	17 MB	118,117	147 Kbps	131 pps	163.5 Kbps	144 pps		
<input checked="" type="checkbox"/>	48 (CS6)	125	6 MB	28,982	51 Kbps	32 pps	53.2 Kbps	33 pps		
<input checked="" type="checkbox"/>	16 (CS2)	2,368	979 KB	2,368	9 Kbps	3 pps	9.6 Kbps	2 pps		
<input checked="" type="checkbox"/>	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

- 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: 07/22/2021 Start Time: 15:10 End Date: 07/23/2021 End Time: 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: Min. 100x100px

**REPORT LIST**

DSCP (Flow) Normal

Please choose report type

Add New Report

**REPORT DETAILS**

Search

\* Only Time Range report types displayed

**Top Reports**

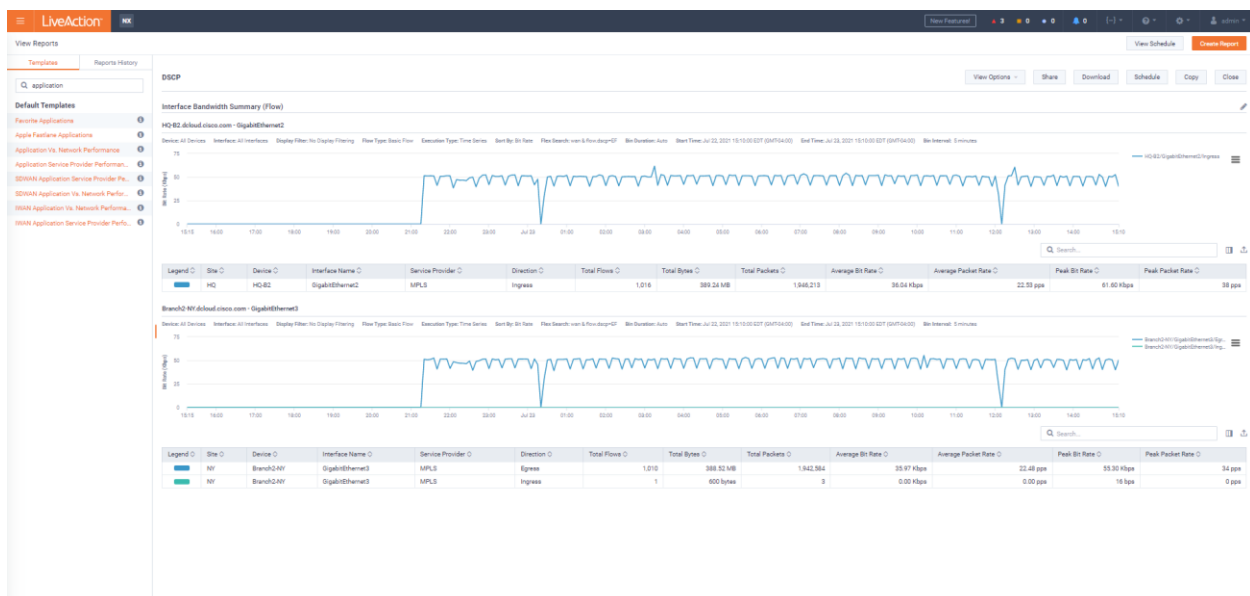
- Application (Flow)
- Top Conversations (Flow)
- Interface Bandwidth (Flow)
- DSCP (Flow)
- Top Interface Bandwidths (SNMP)
- Top Interface Errors (SNMP)
- Top Class Bandwidths (SNMP)
- Top Class Drops (SNMP)
- Interface Bandwidth (SNMP)
- Interface Utilization (SNMP)
- Interface Errors (SNMP)
- Post-Policy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

**LiveNA**

- Flow
- SNMP
- Cisco SD-WAN
- Alerts

Cancel Save As Template Execute

- Enter a Search String: **wan & flow.dscp=EF** (note upper-case).
- Select **All** devices.
- Click **Execute**.



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 & 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 & Ports**. Name your report.
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.

The screenshot displays the 'RUN OR EDIT REPORT(S)' interface, which is divided into three main sections: GENERAL SETTINGS, REPORT LIST, and REPORT DETAILS.

**GENERAL SETTINGS:**

- Name:** 'IPs and Ports, Last Fifteen Minute'
- Presentation Mode:** 'Standard'
- Footnote:** 'Enter report group description...'
- Time Zone:** '(GMT-05:00) America/New York' (DST is checked)
- Time Range:** 'Custom'
- Start Date:** '07/23/2021', **Start Time:** '15:29', **End Date:** '07/23/2021', **End Time:** '15:44'
- Flex Search:** 'Ex.: site=Honolulu & wan & flow.app=http' (with a clear 'x' button)
- Display Filter:** 'Select Display Filter...'
- Sharing Settings:**
  - Email:** 'Enter an email address or AD entity...'
  - File Format:** 'Send PDF' and 'Send CSV' are both unchecked.
  - PDF Row Limits:** 'All Rows'
  - Custom Logo:** 'No Custom Logo' (with a clear 'x' button)

**REPORT LIST:**

- Shows a list with one report: 'IPs and Ports (Flow)'.
- Buttons: 'Add New Report' (orange), 'Fast', and a trash icon.

**REPORT DETAILS:**

- Report Name:** 'IPs and Ports'
- Flow Type:** 'Basic Flow'
- Report Description:** 'Enter report description...'
- Execution Type:** 'Time Series'
- Devices:** 'HQ-B2' (highlighted with a red box)
- Sort By:** 'Bit Rate'
- Interfaces:** 'All Interfaces'
- Business Hours:** 'All Hours'
- Flex Search:** 'wan & flow.dscp=BE' (highlighted with a red box)
- Bin Duration:** 'Auto' (1 minute)
- Display Filter:** 'No Display Filtering'
- Direction:** 'Inbound and Outbound Combined' (highlighted with a red box)
- Should Wait For DNS Resolution:** 'False'
- Raw Flow Data:** A warning box states: 'Due to the options selected, this report will utilize the Raw Flow datastore (slower).'

At the bottom right, there are three buttons: 'Cancel', 'Save As Template', and 'Execute' (orange).



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



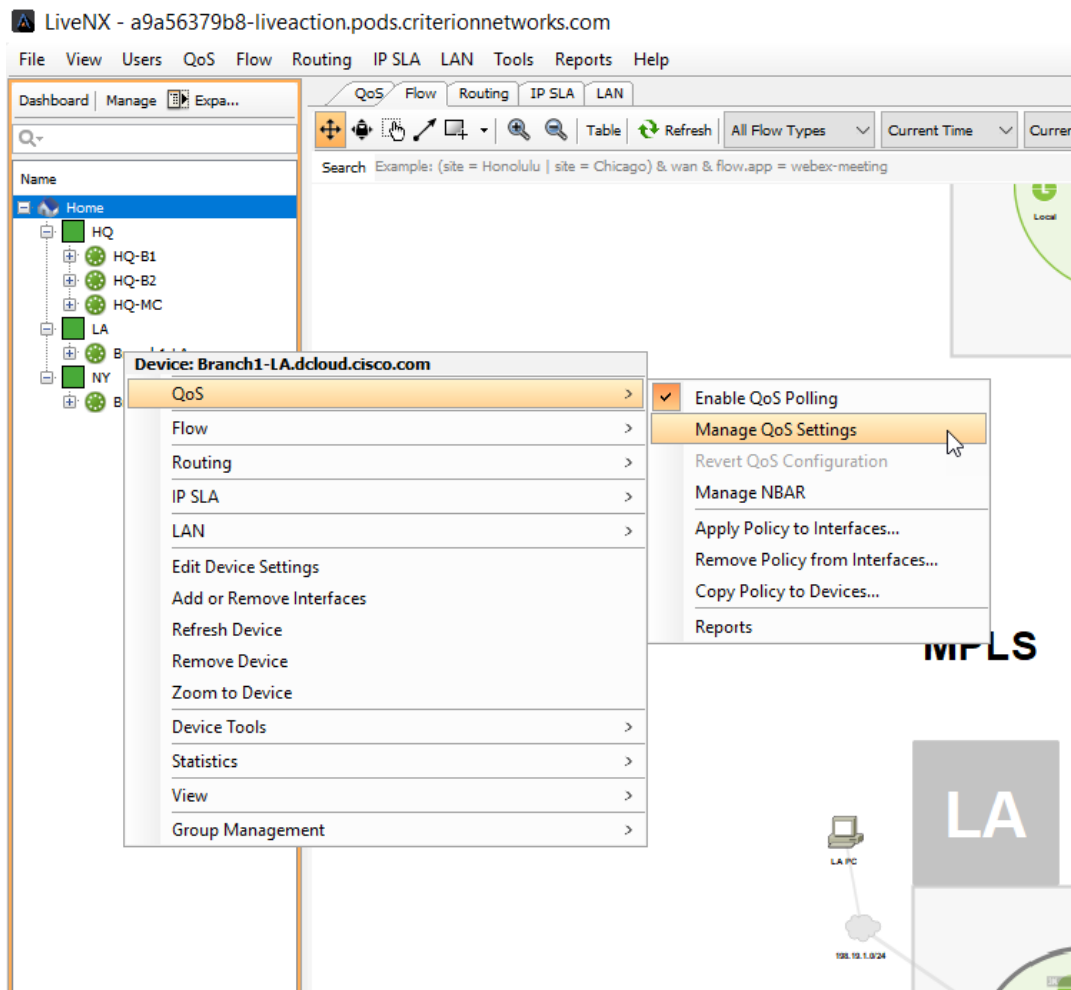
## Lab 8.1: QoS Marking Policy

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.

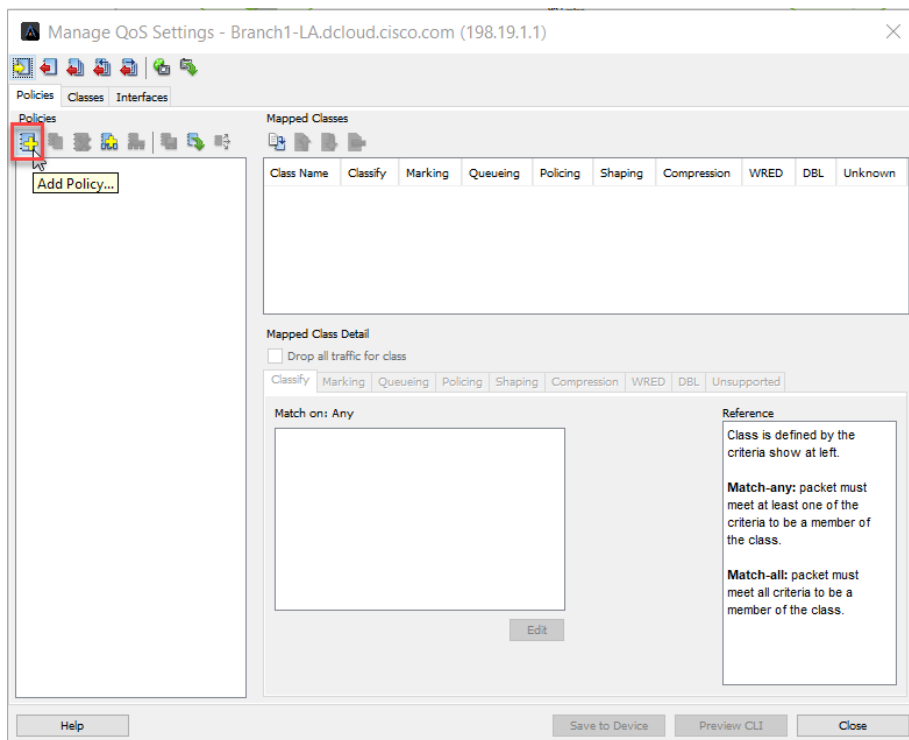
Since you've installed ACLs to use in your INGRESS marking policy, let's create the QoS marking policy using the **LiveNX client**.

Lab Steps:

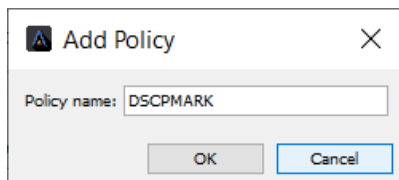
7. From the Home menu location (top-left of screen) right click on the "**Branch1-LA**" device.
8. Highlight QoS and select Manage QoS Settings.



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

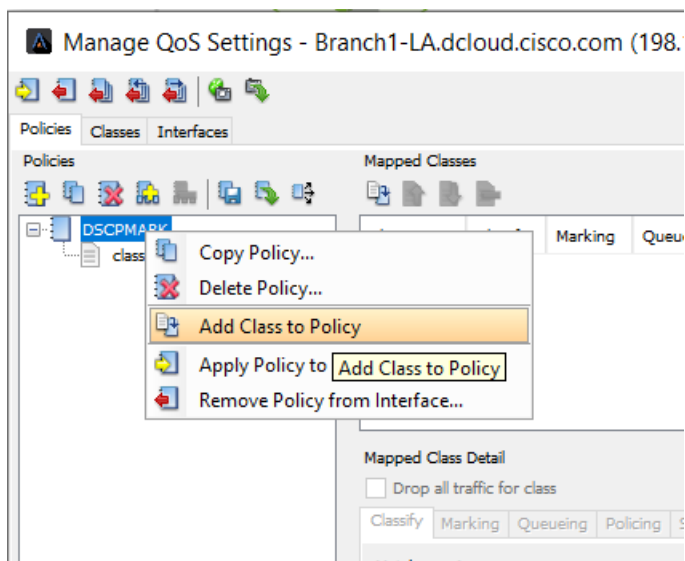


10. Give the new Policy a name, such as “DSCPMARK”



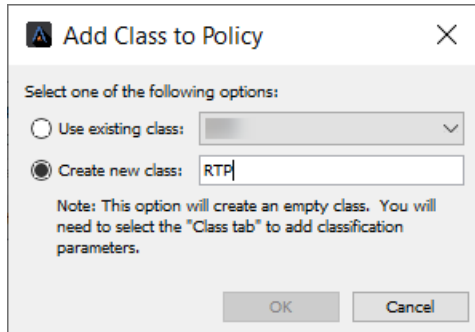
11. We are going to add two classes to this policy: **RTP** and **SIP**

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

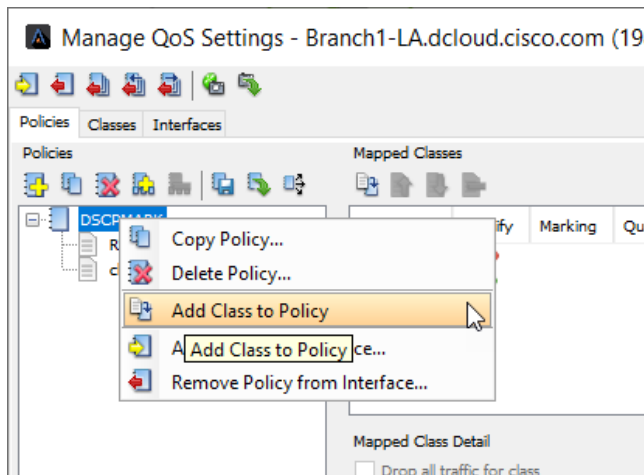


13. Select “Create a new class” and give the class a name RTP.

14. Click **OK**

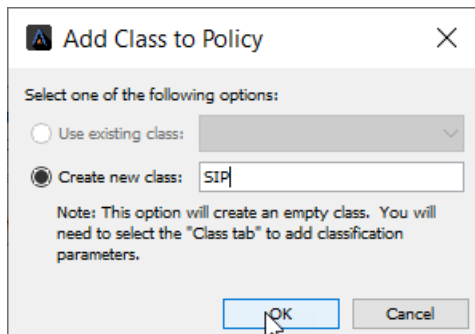


15. Select "Add Class to Policy"

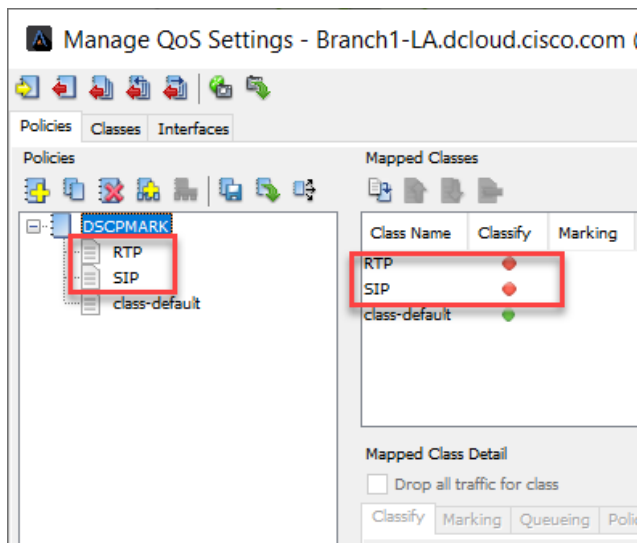


16. Click Create new class, Label it SIP.

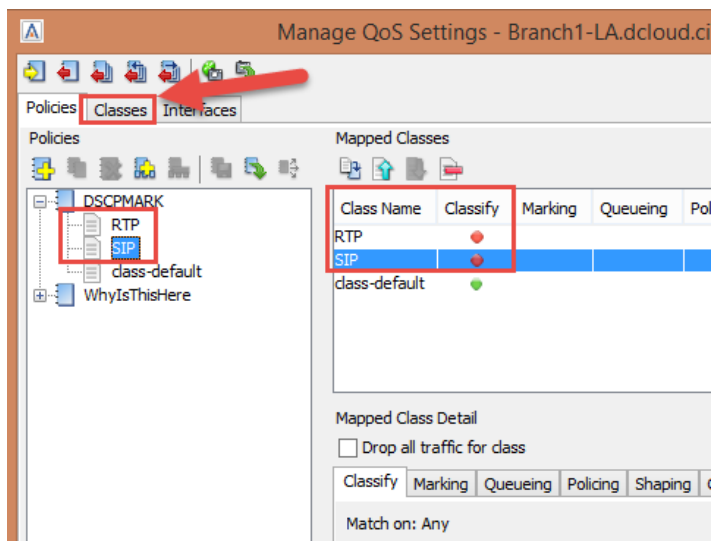
17. Click OK.



You should now see your two new classes added to the "DSCPMARK" policy.

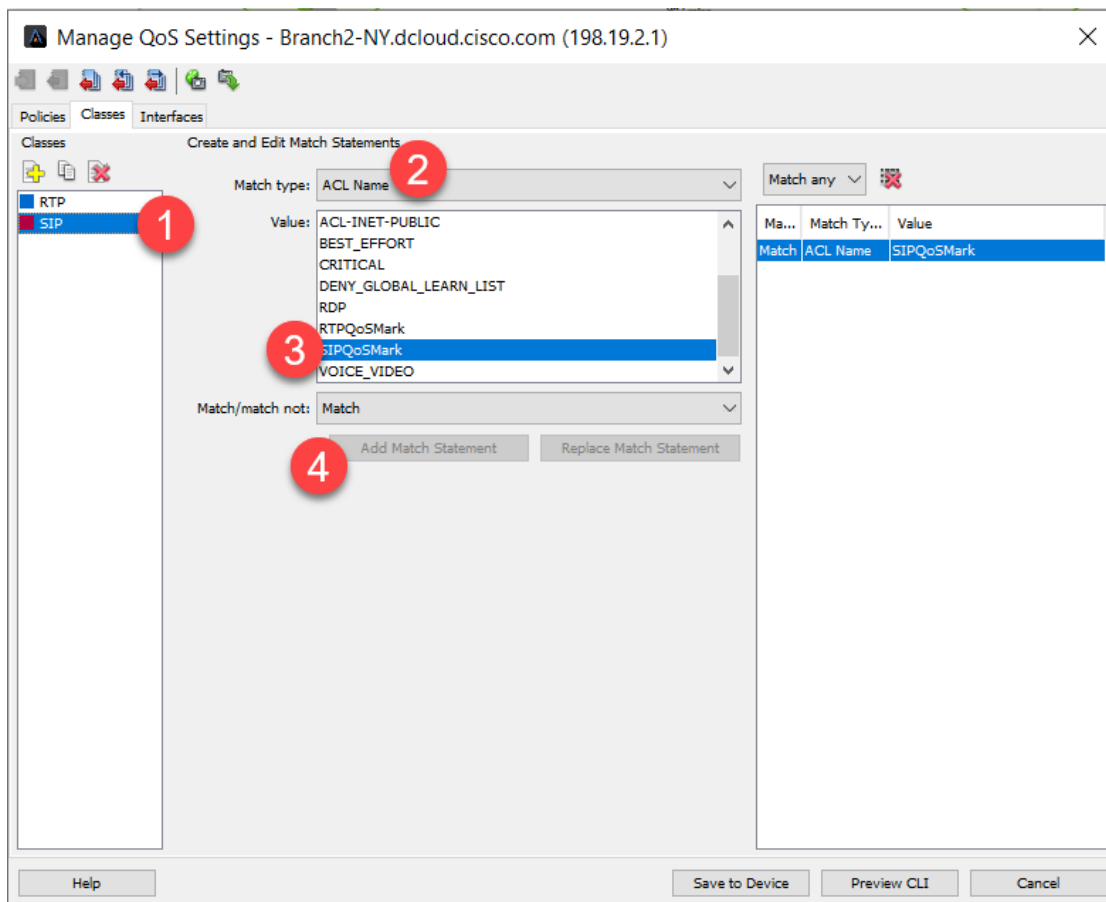


18. Select the “**Classes**” tab to match them to the created ACL’s.



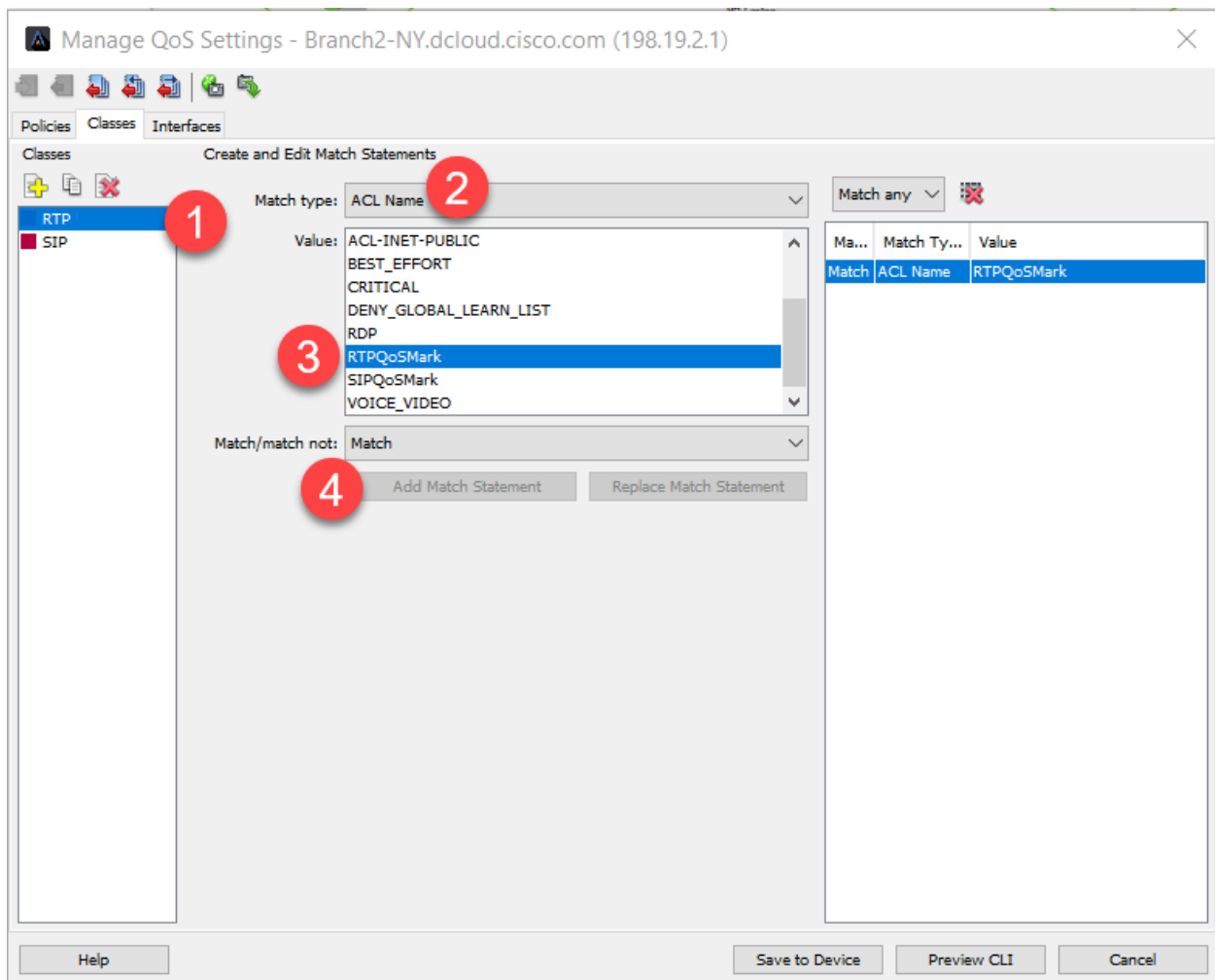
Select and match the SIP class...

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

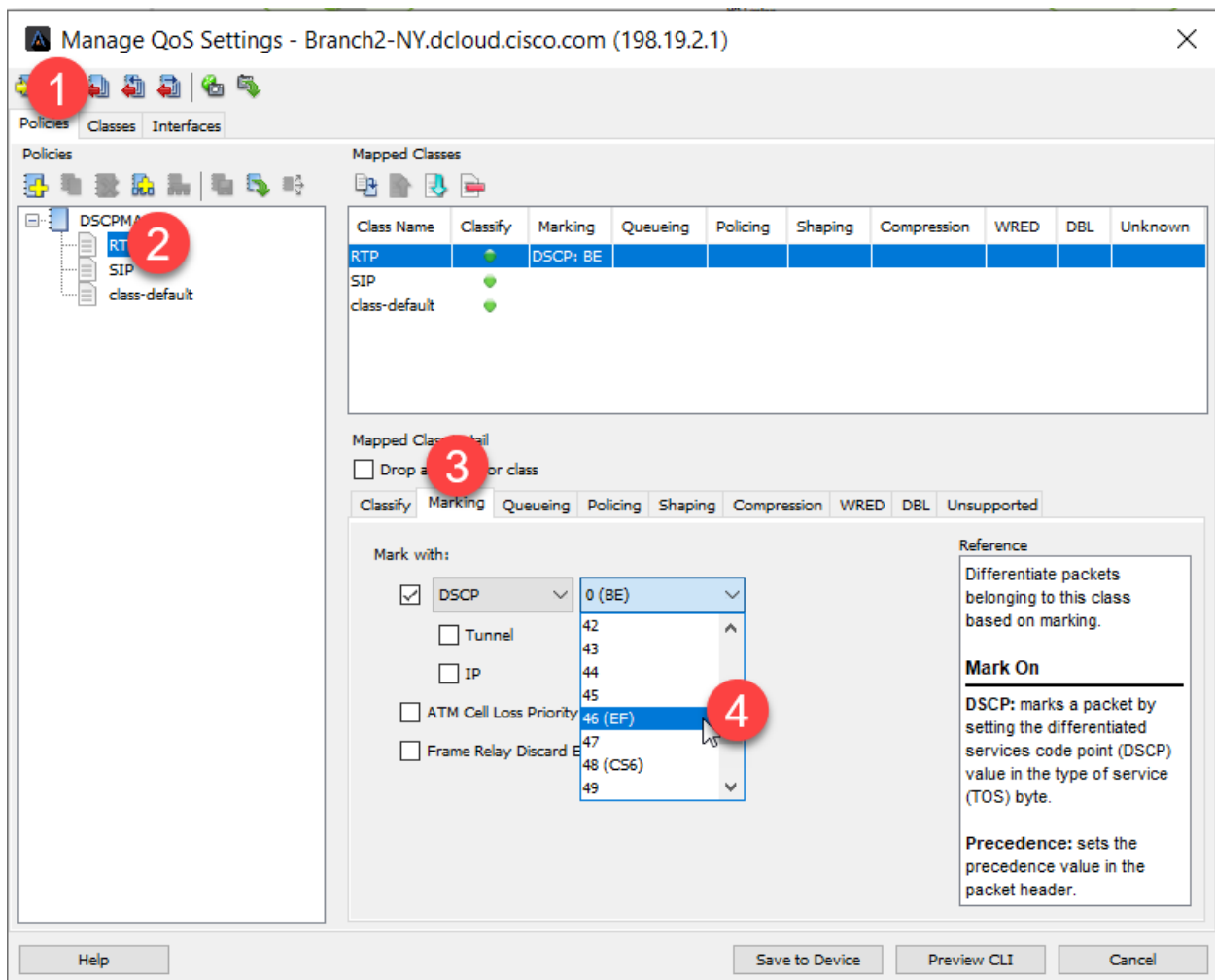


Next select the RTP Class and do the same...

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

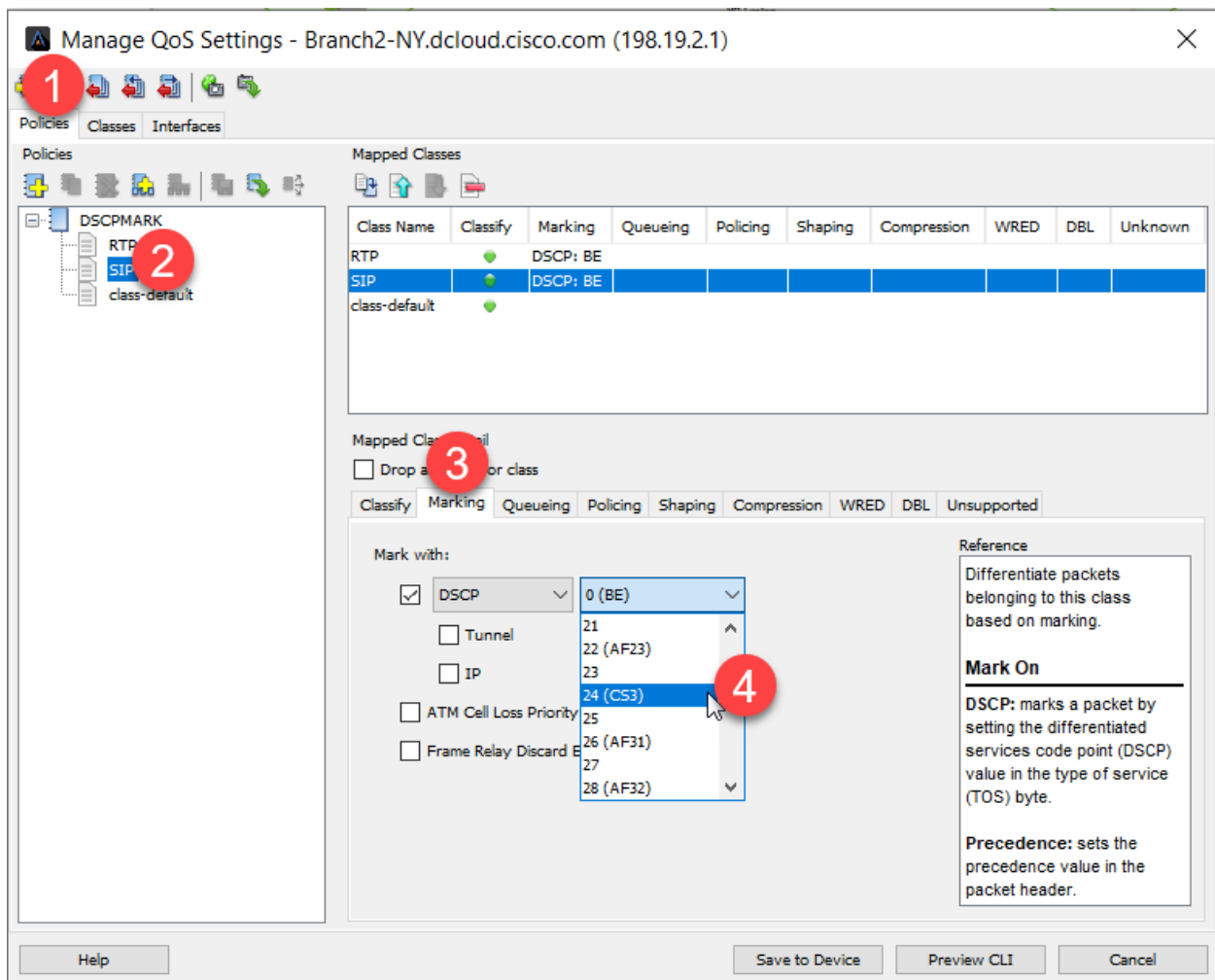


27. Select the **Policies** Tab.
28. Select the **RTP** Class.
29. Select the **Marking** Tab
30. Choose to mark the RTP Traffic with DSCP **46 (EF)**.



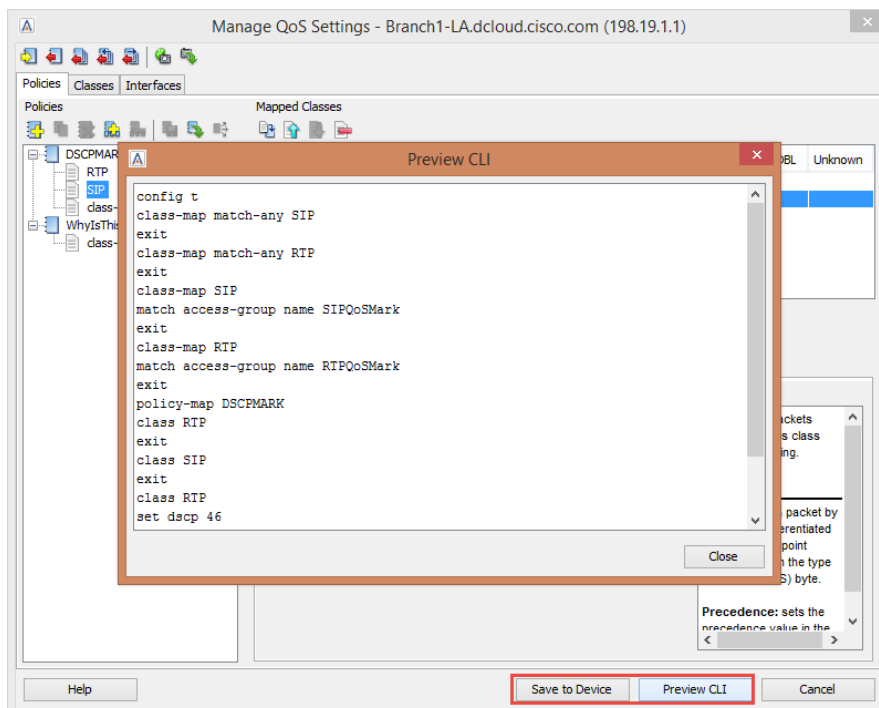
Next it is necessary to set the DSCP Markings for the SIP Class.

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



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

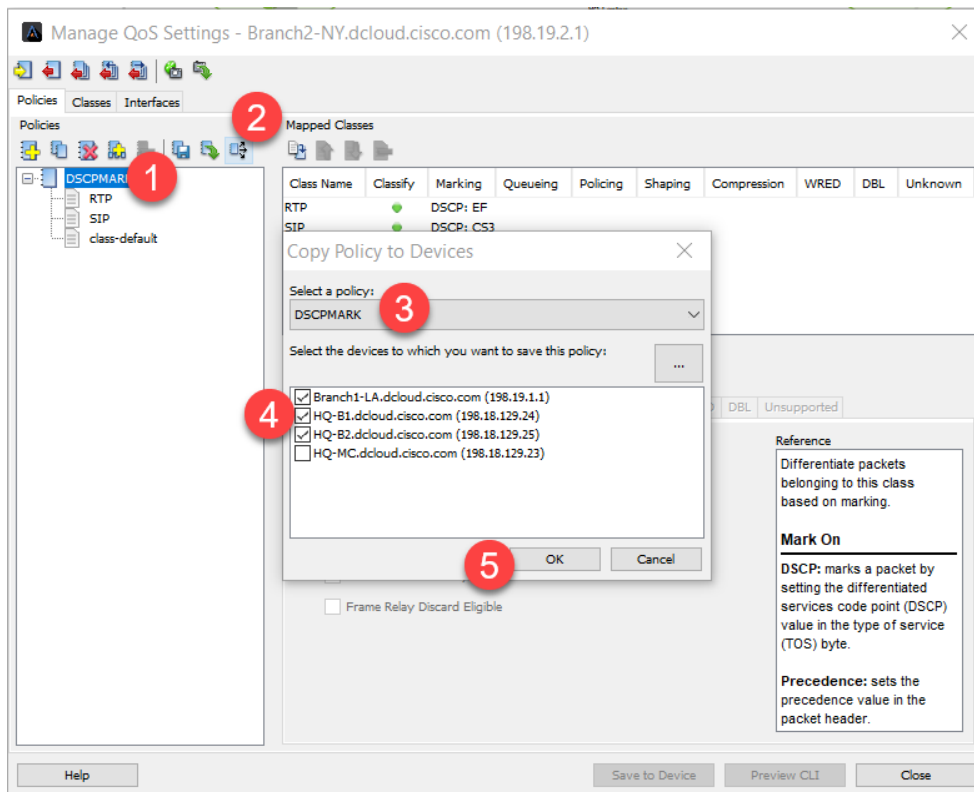
35. Click **Save to Device** if satisfied.





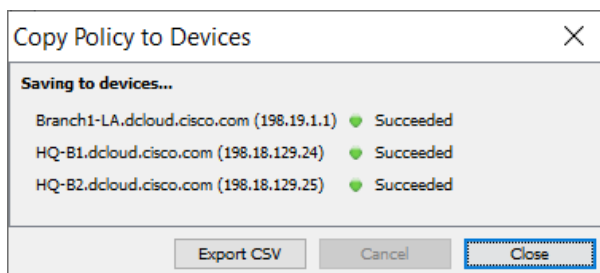
We can now push our newly created polices to *multiple* devices.

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**



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.

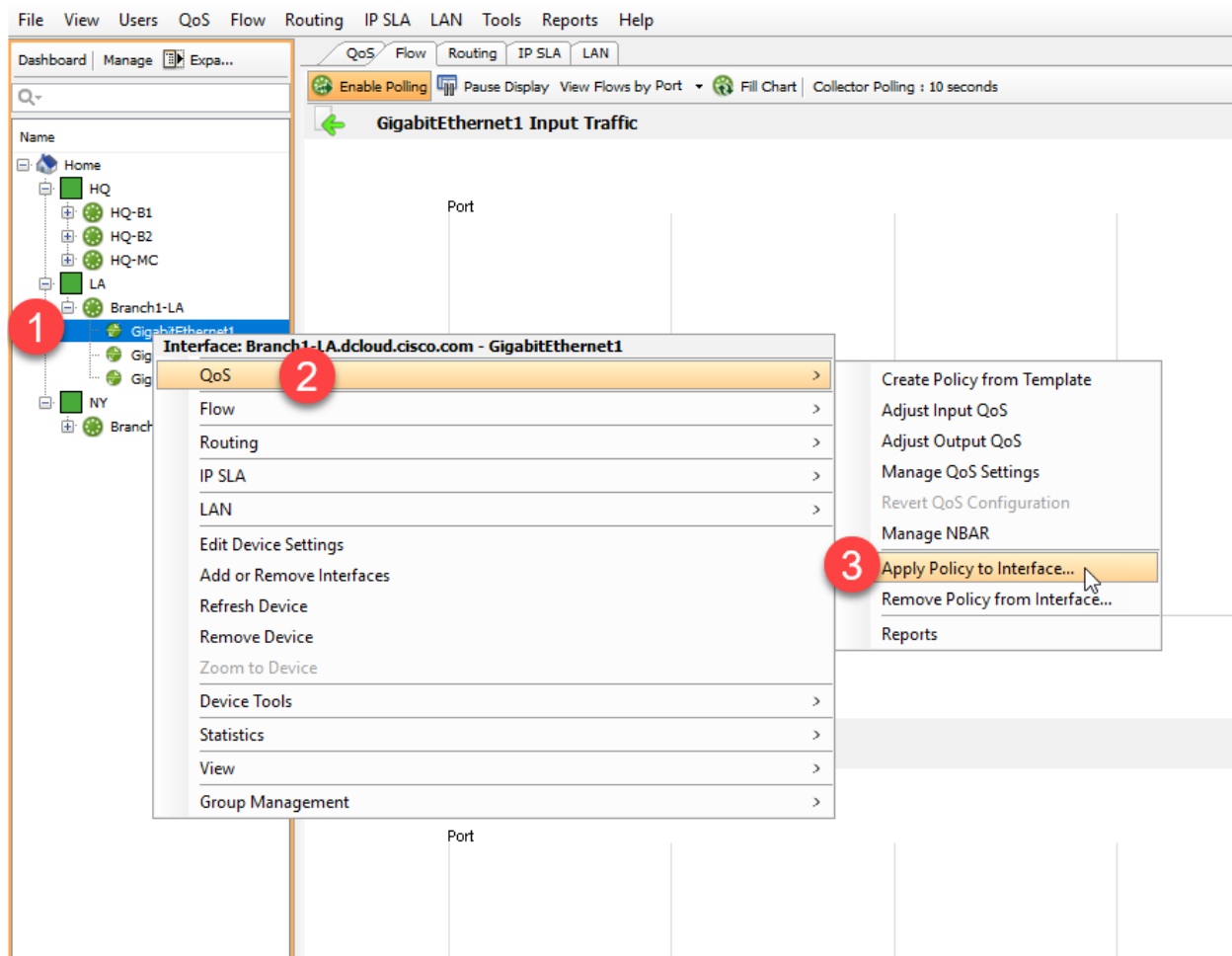


**Note:** You want to apply marking policies as close as possible to where traffic enters the network.

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.

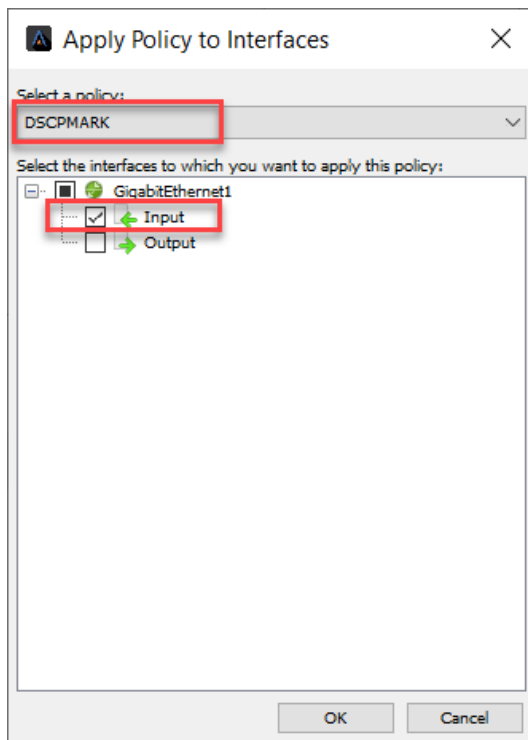
42. In the main device menu on the top-left, right-Click on the appropriate interface.

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



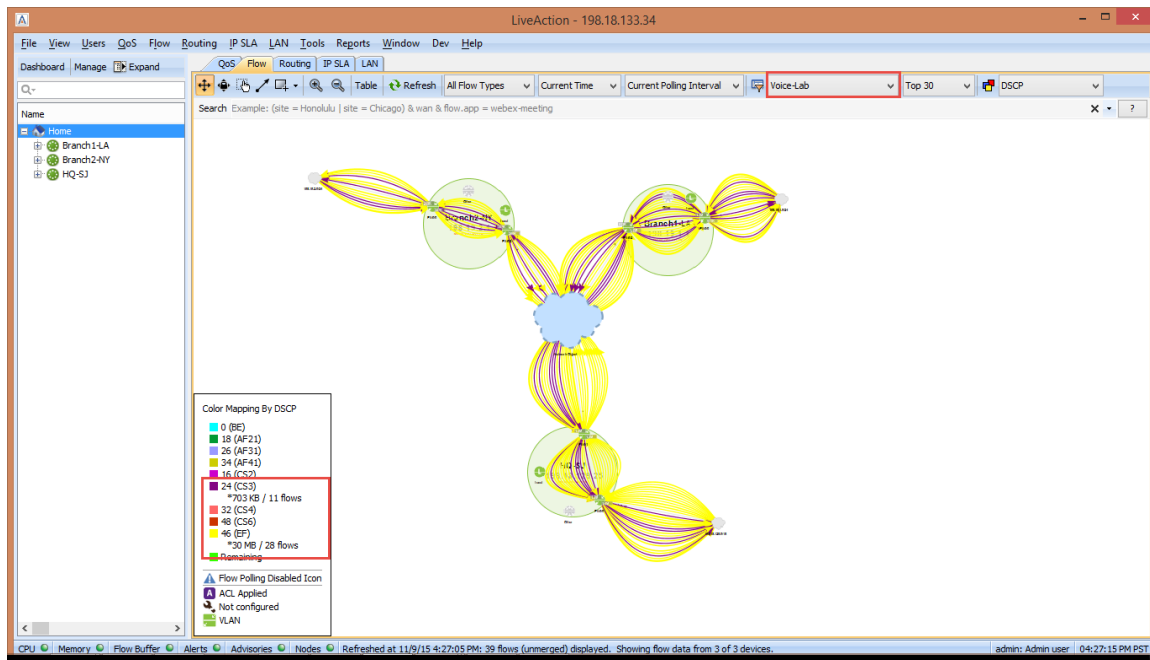
44. Select the “**DSCPMARK**” policy.

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



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.



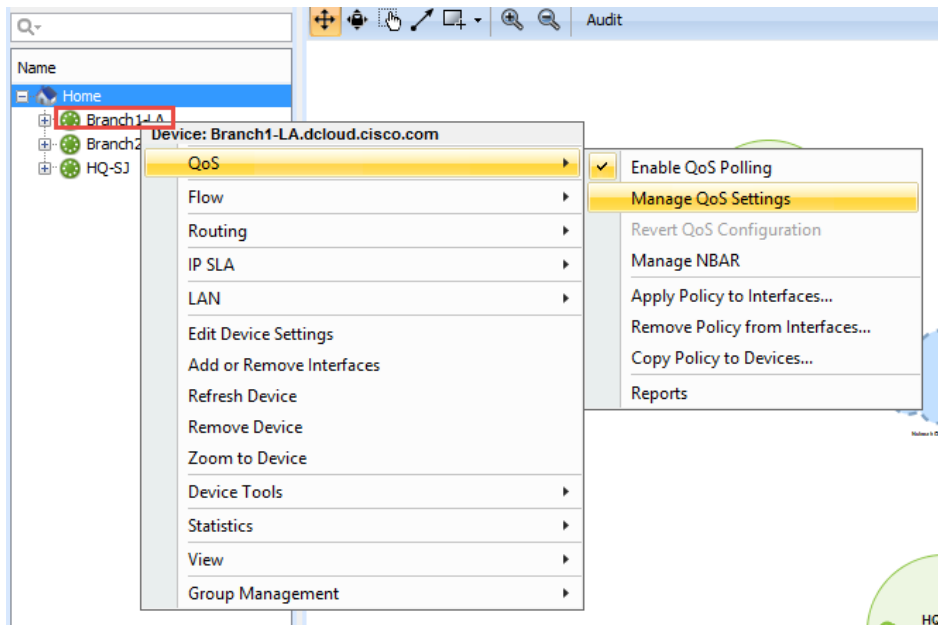
## Lab 8.2: QoS Queueing Policy

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.

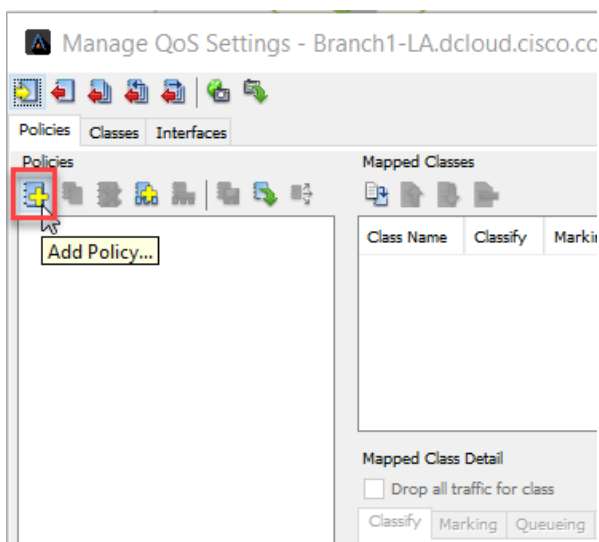
Lab Steps:

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

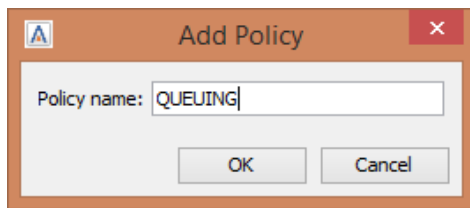


47. Select the **Policies** Tab.

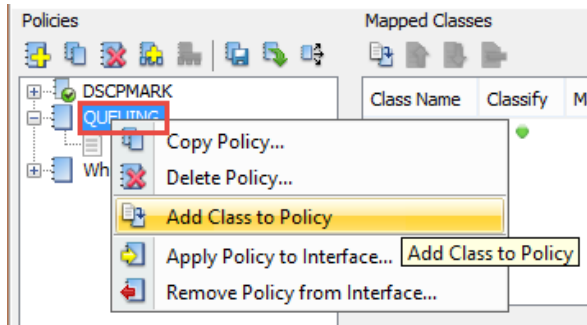
48. Click **Add Policy** to create a queuing policy.



49. Name the new policy QUEUEING.

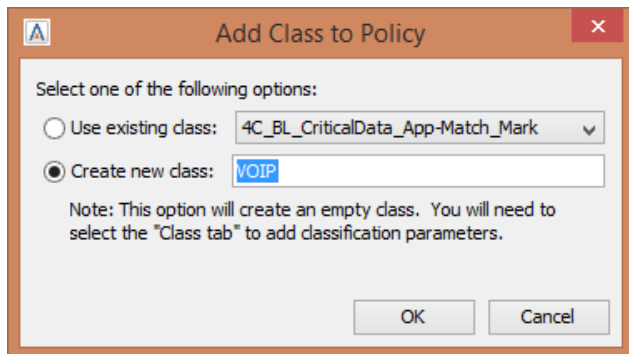


50. Right-click on the new QUEUEING Policy, select Add Class to Policy.

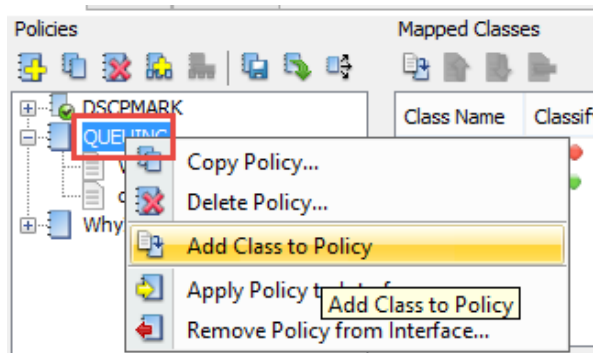


51. Create a new class labeled VOIP.

52. Click OK.

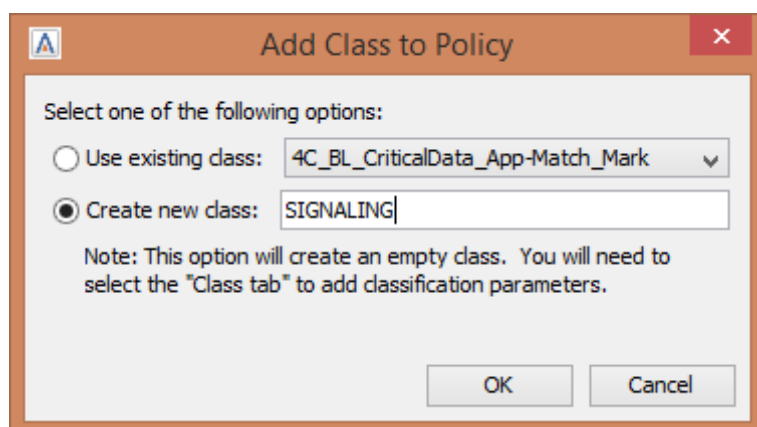


53. Right-click, again, on the QUEUEING Policy, select Add Class to Policy.



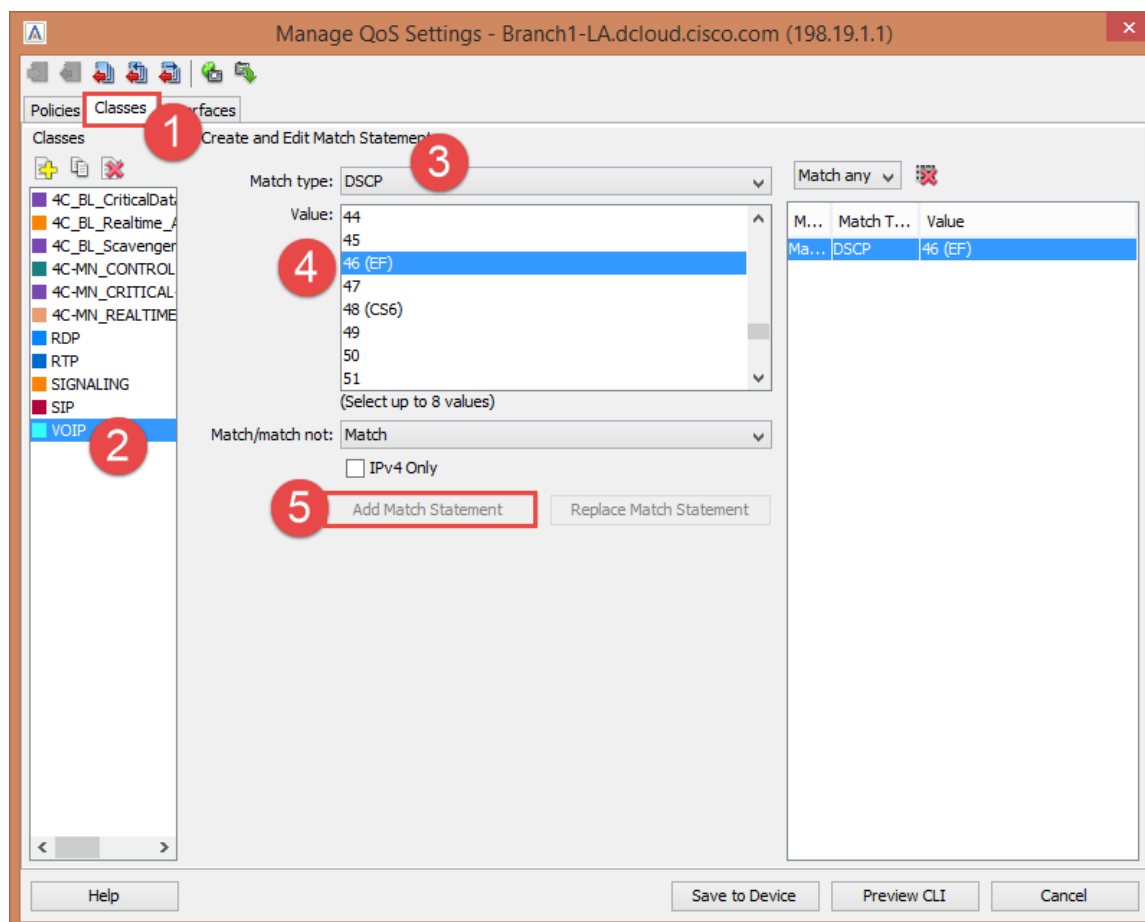
54. Create a new class and label it SIGNALING.

55. Click OK



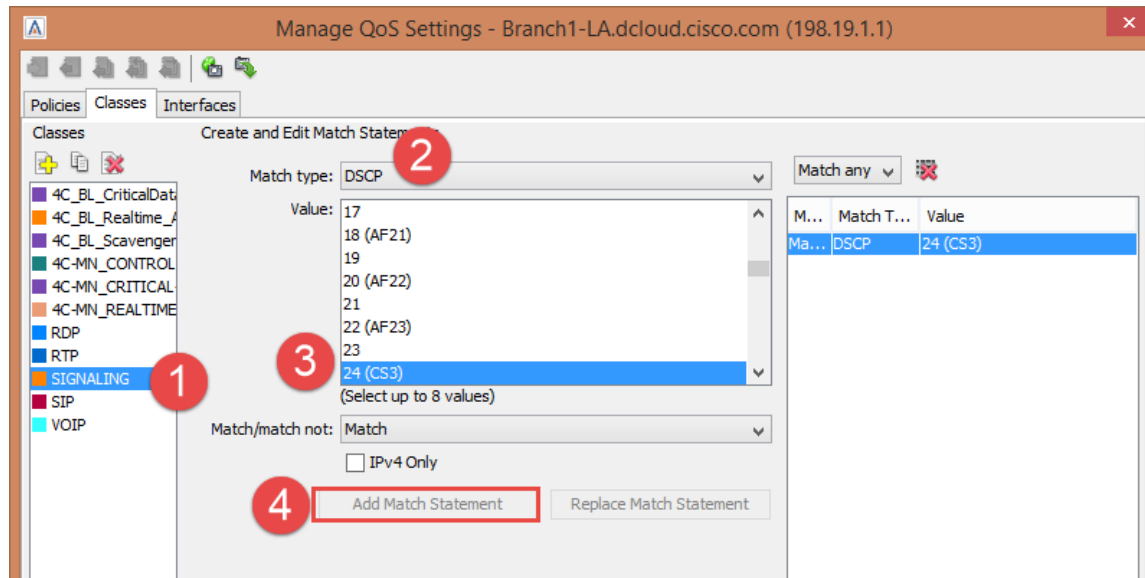
Configure VOIP Class:

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



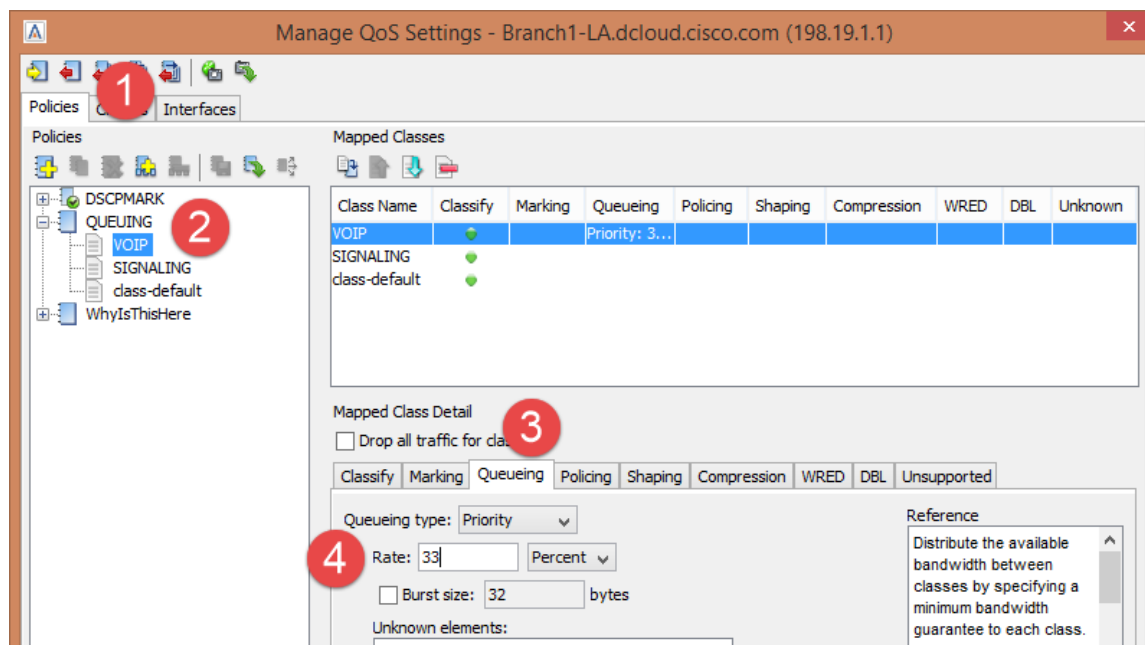
Configure SIGNALING Class:

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



Setup VoIP Priorities:

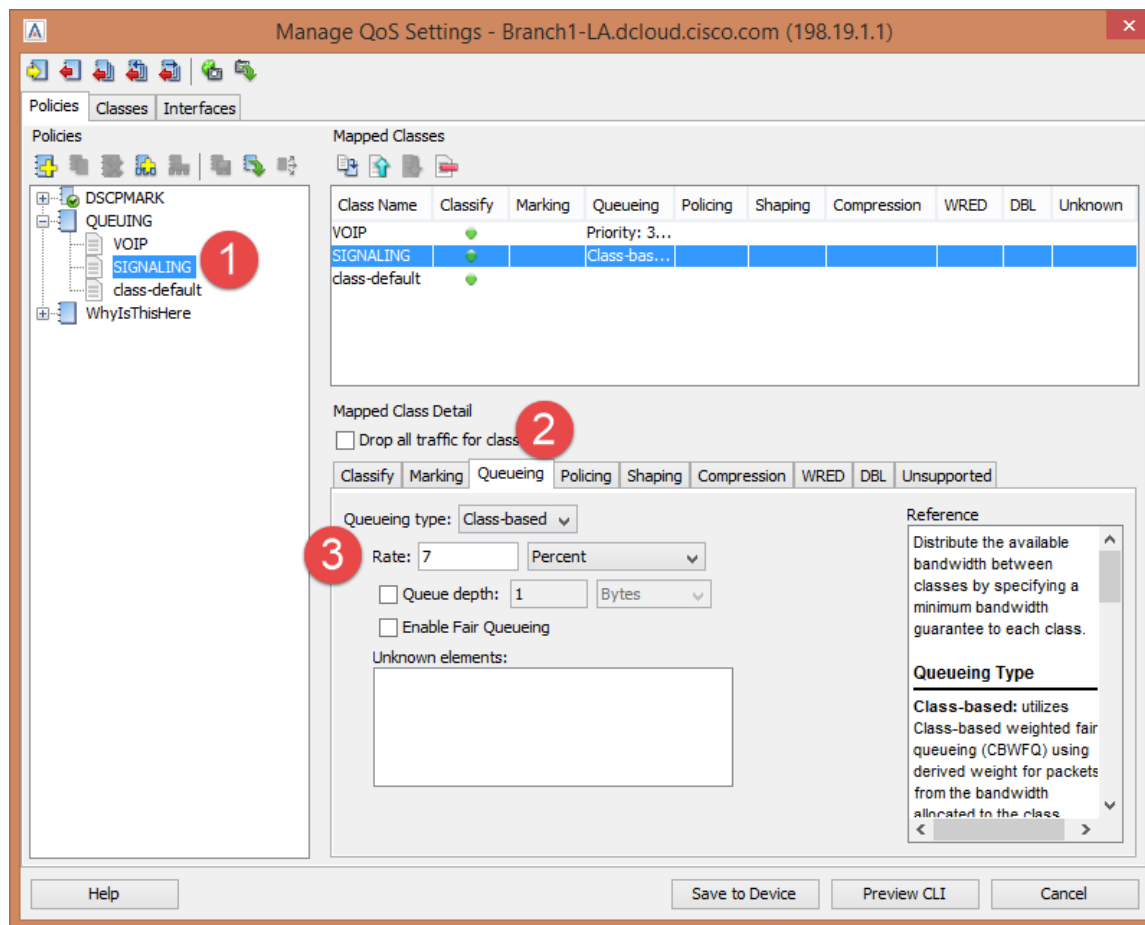
60. Select the Policies Tab.
61. Select the VOIP Class.
62. Select the Queuing Tab.
63. Select Priority Queuing, enter a rate of 33%.





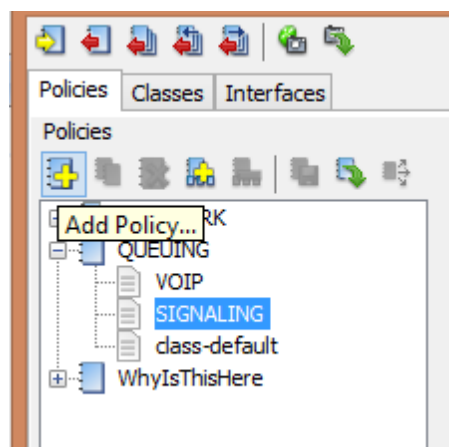
Setup Signaling Priorities:

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

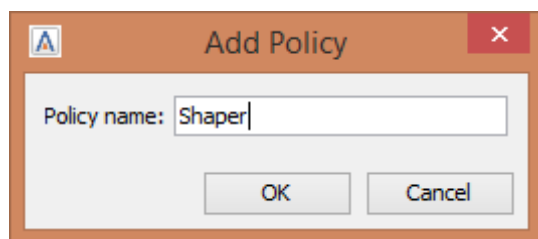


Create a Shaping Policy:

67. Click Add Policy.



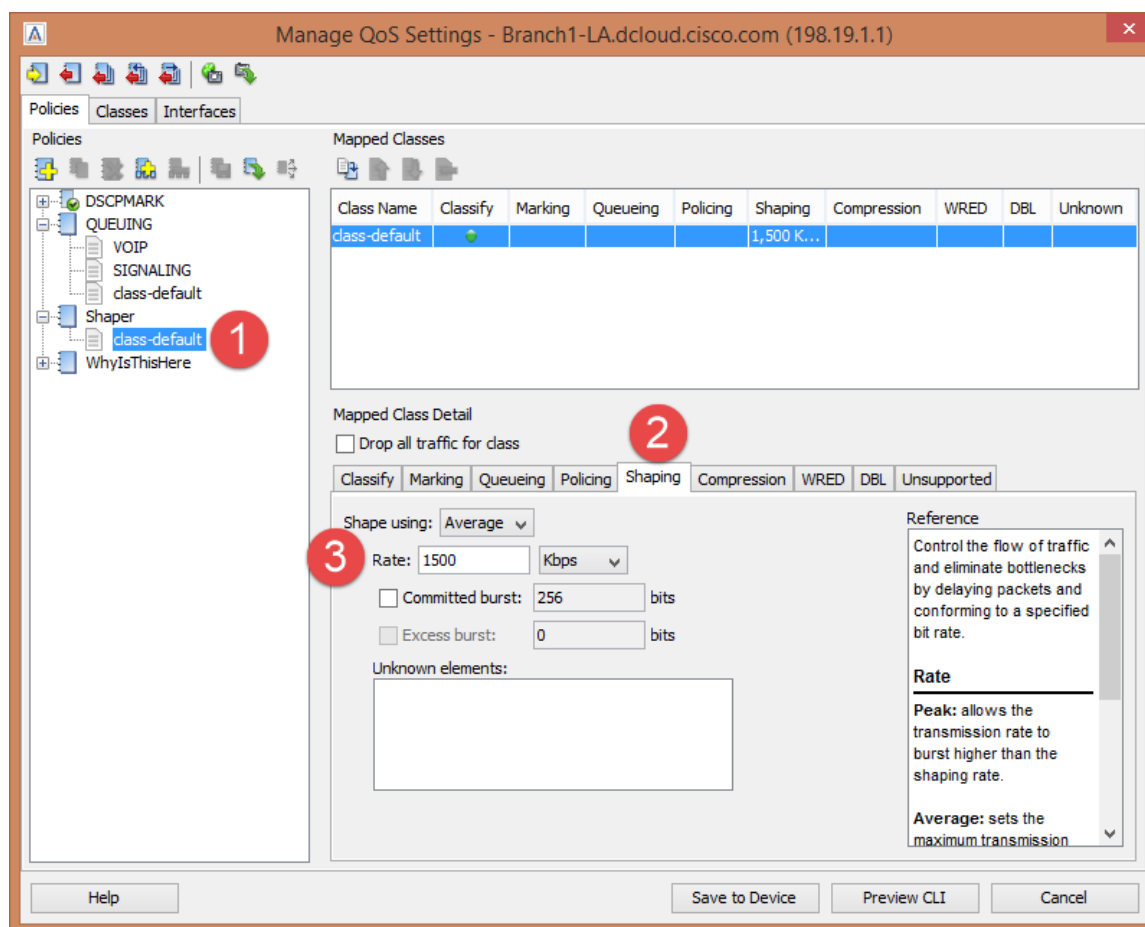
68. Give the Policy a name of Shaper.



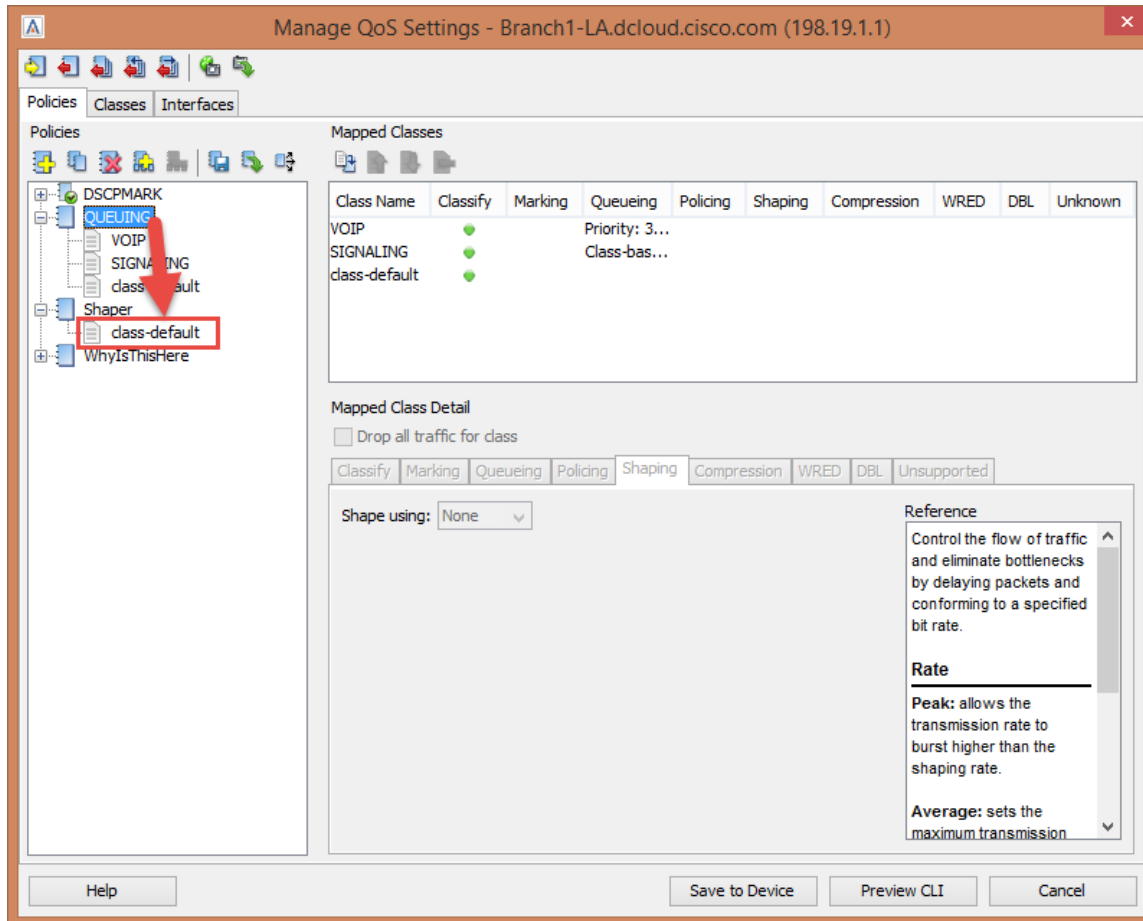
69. Select the **class-default** class under Shaper.

70. Select the Shaping tab.

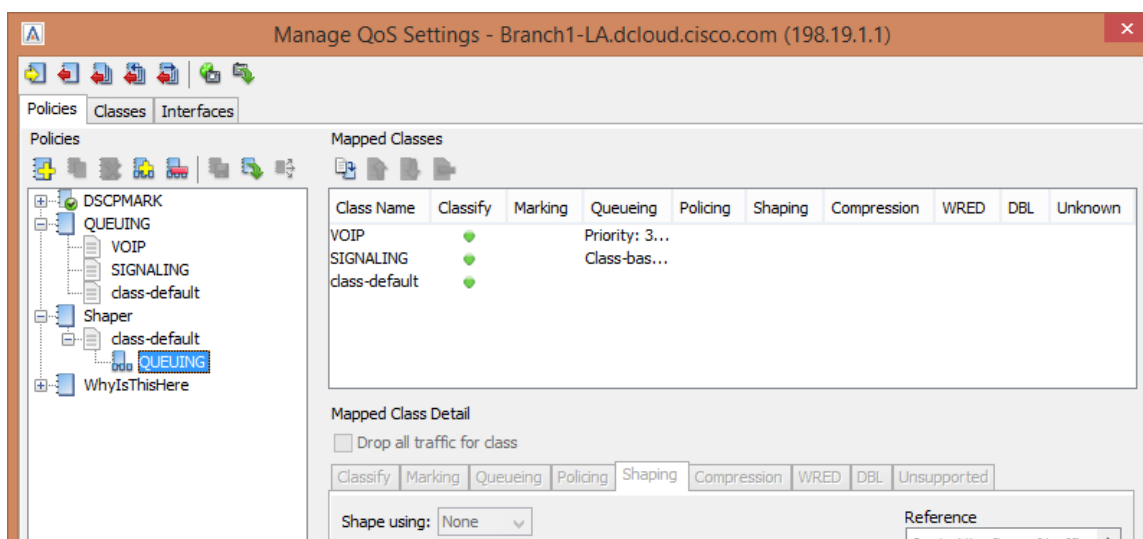
71. Select Average, enter 1500 Kbps.



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

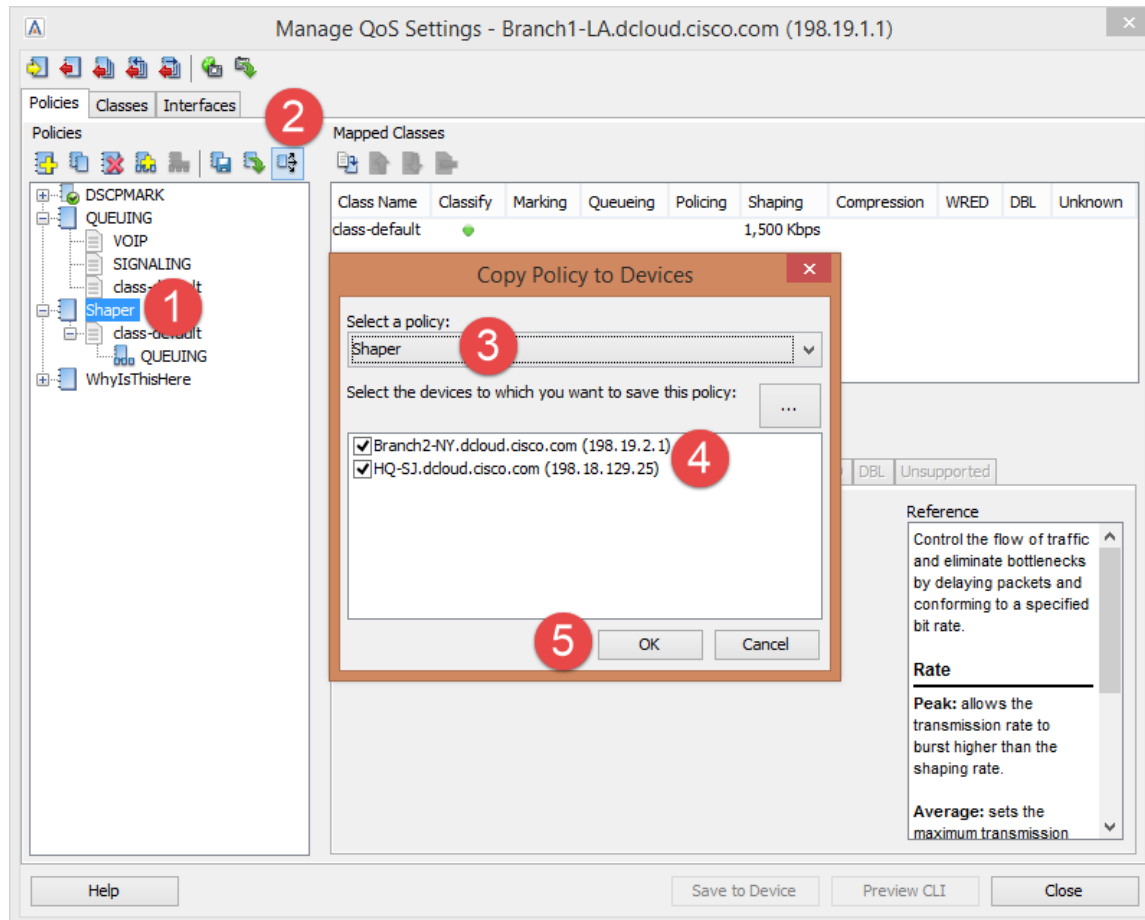


Now you should see the QUEUEING Policy as part of the shaper. This allows you to reserve the percentage of BW in the shaping policy!

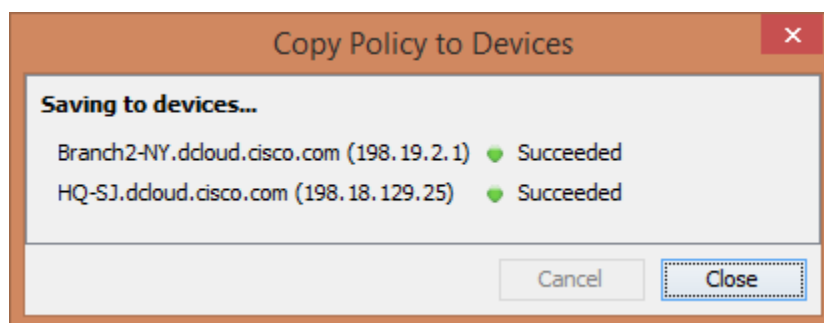


Copy the shaping policy to the other devices:

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.

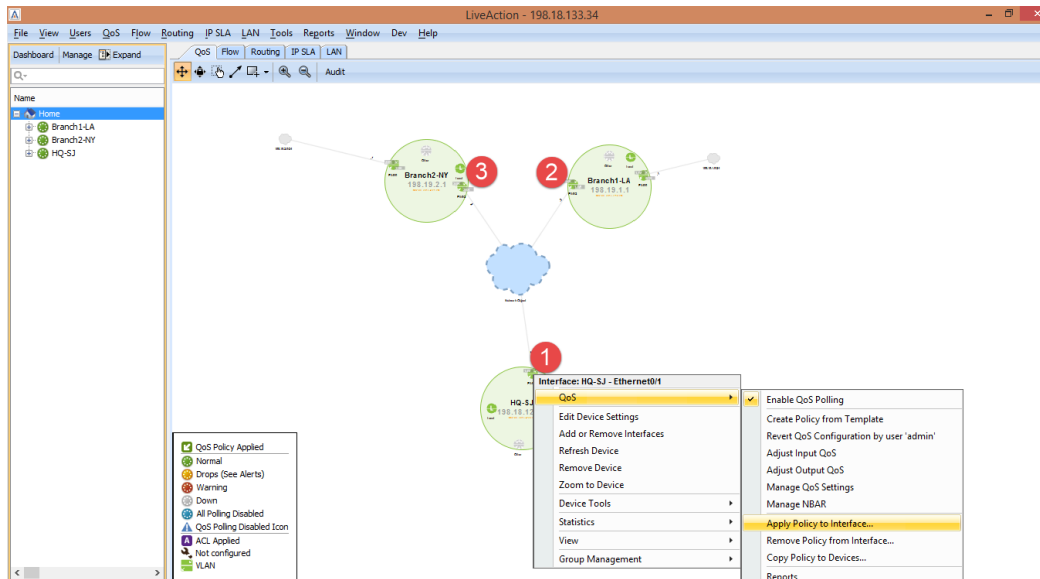


78. Click Close.
79. Click OK.

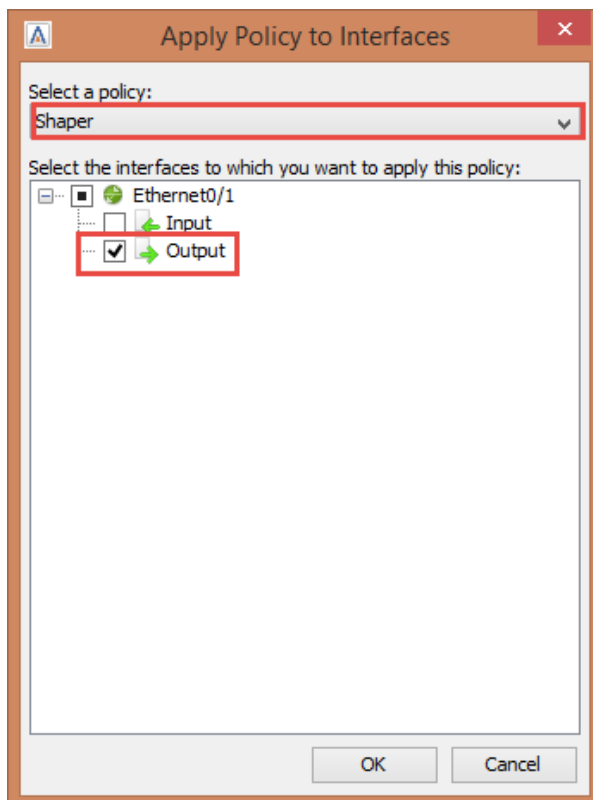


We still need to apply the policy to the WAN interfaces. Do the following steps on EACH of the 3 devices.

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

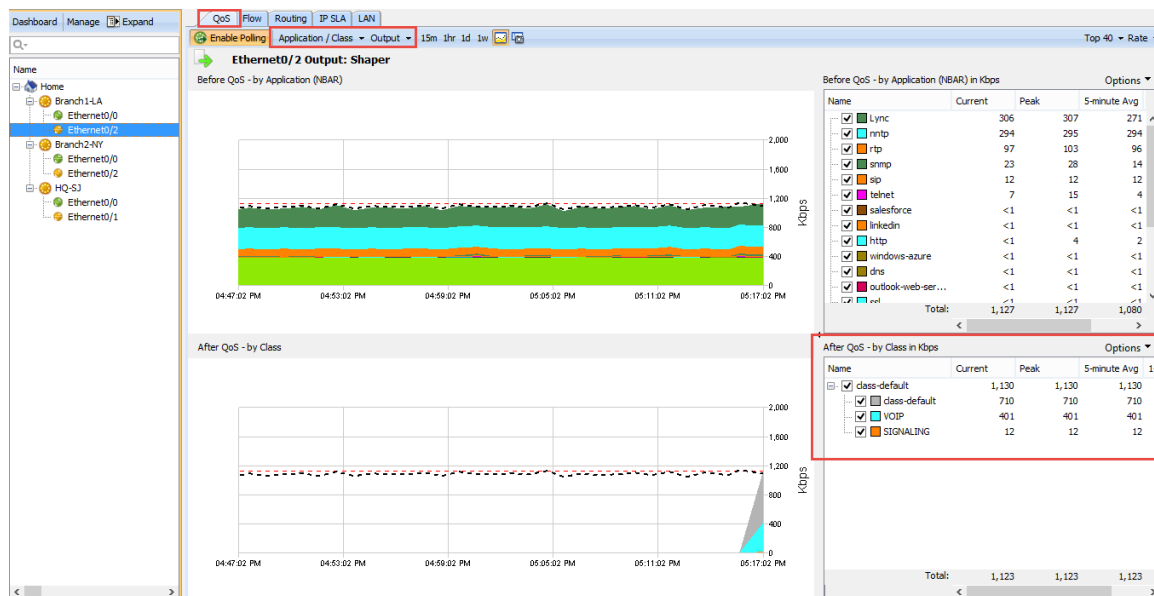


81. Select the Shaper Policy and the Output for the WAN interface.



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.



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.

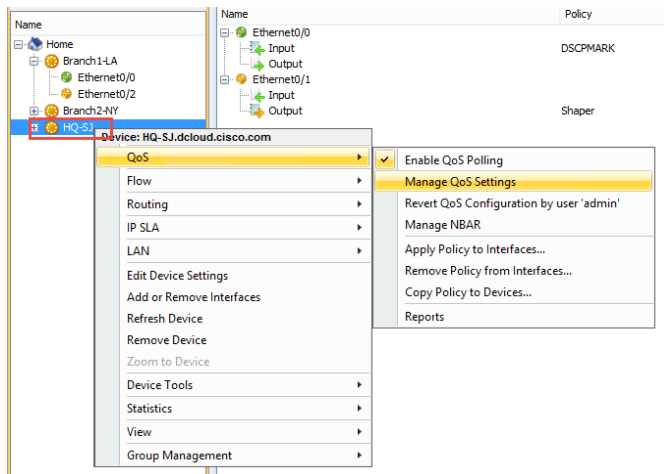
## Lab 8.3: QoS Verification

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:

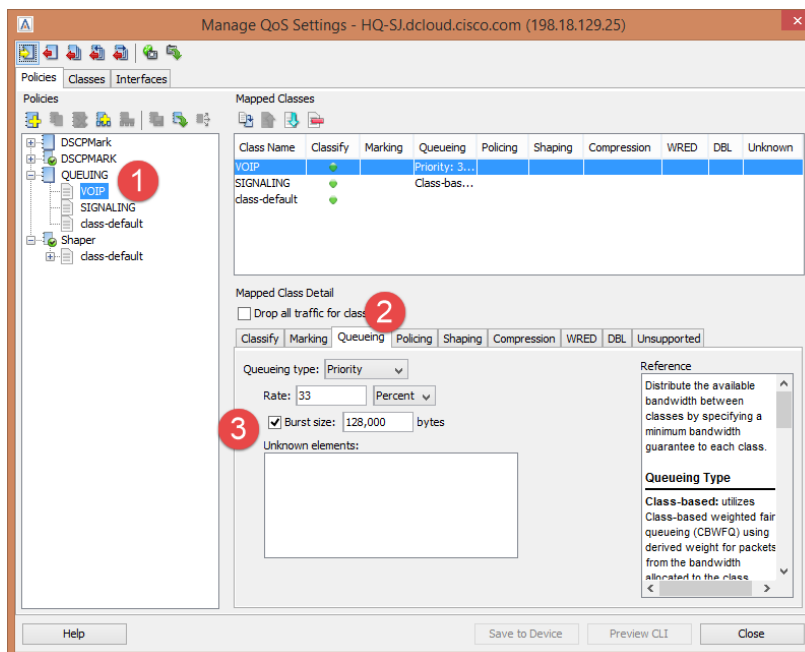
Select a device and select **QoS** and **Manage QoS Settings**.



83. Select the **VOIP** Class.

84. Click the **Queueing** Tab.

85. Select **Burst Size** of **128000**.



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/qcfcplsh.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfcplsh.html)

An excerpt about the math behind deciding the burst rate would be:

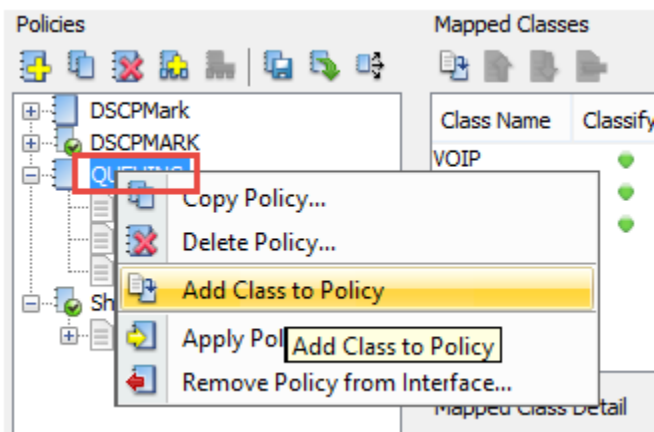
Cisco recommends the following values for the normal and extended burst parameters:

normal burst = configured rate \* (1 byte) / (8 bits) \* 1.5 seconds

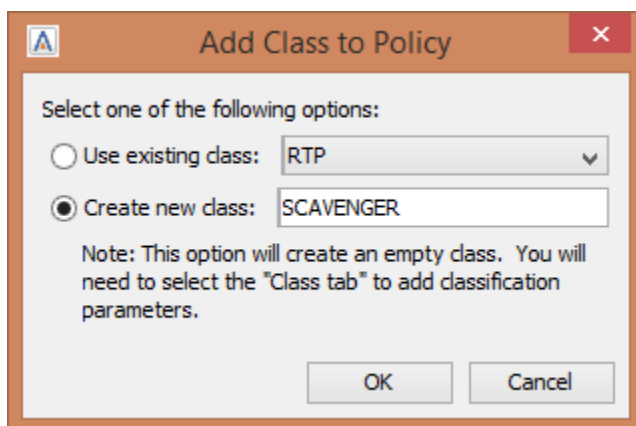
extended burst = 2 \* normal burst

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

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

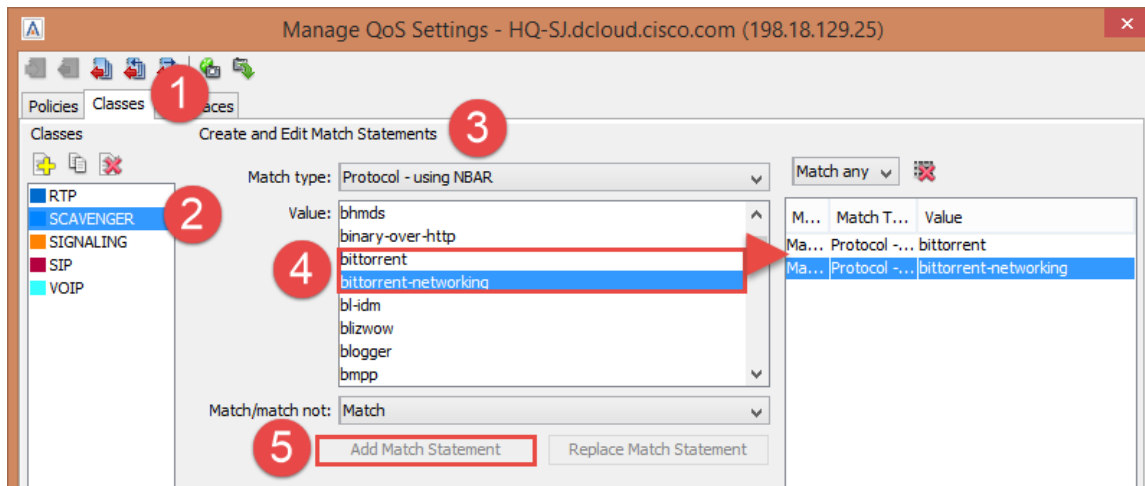


88. Give the new class a label of **SCAVENGER**.

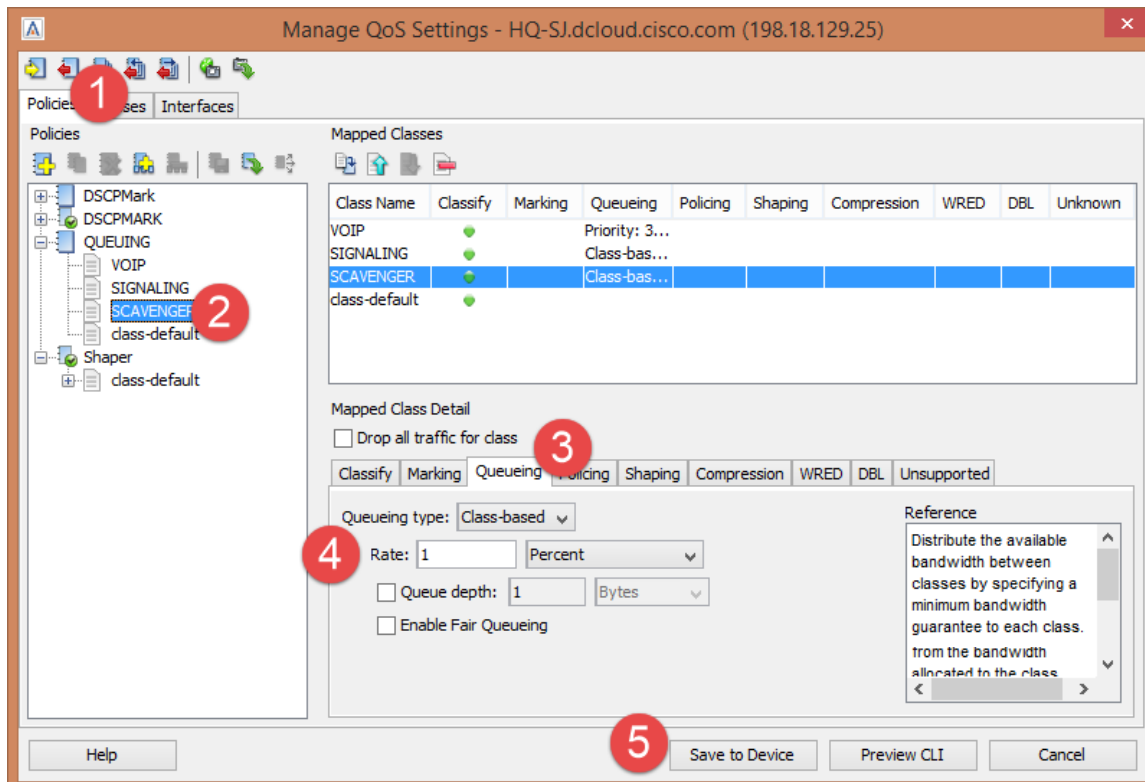




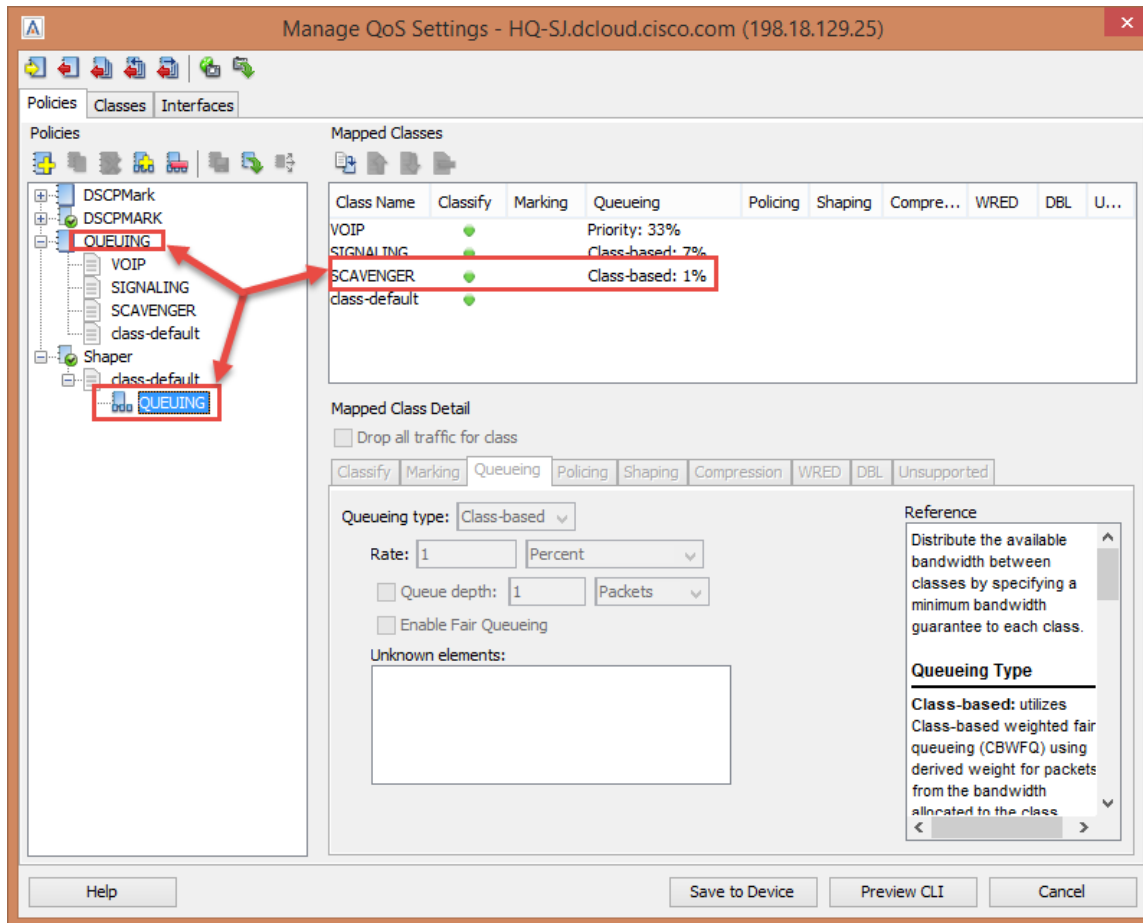
89. Select the **Classes** Tab.
90. Select the **Scavenger** Class.
91. For Match Type select **Protocol – Using NBAR**.
92. Select **both** “bittorrent” and “bittorrent-networking”.
93. Click **Add Match Statement** for both Applications.



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**

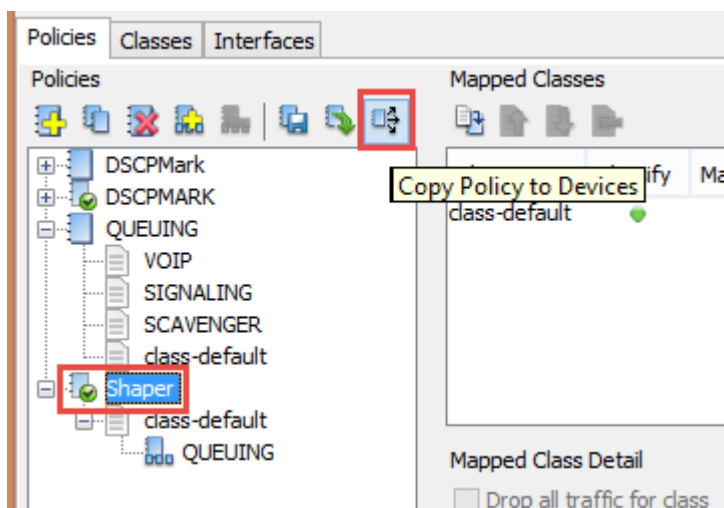


When making changes to the **QUEUEING** Policy it will also affect the Shaping Policy.

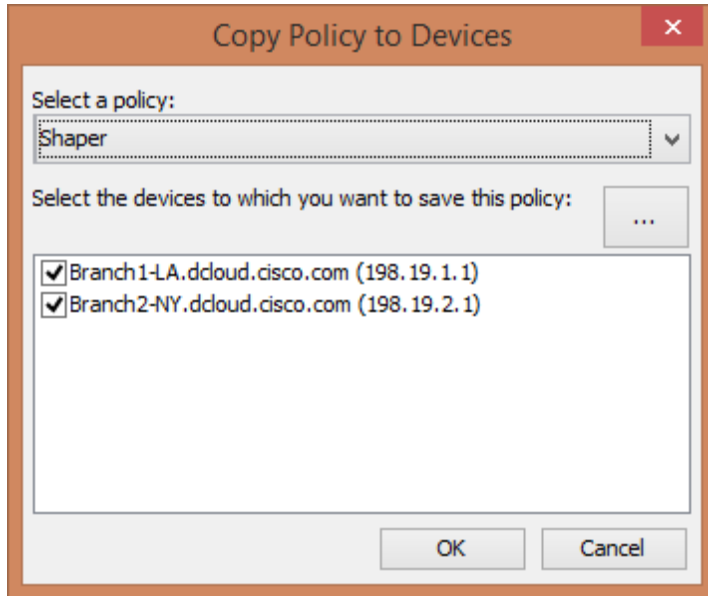


Copy the updated policy to other devices in the topology.

99. Select the **Shaper** Policy
100. Click the **Policy to Devices** button.

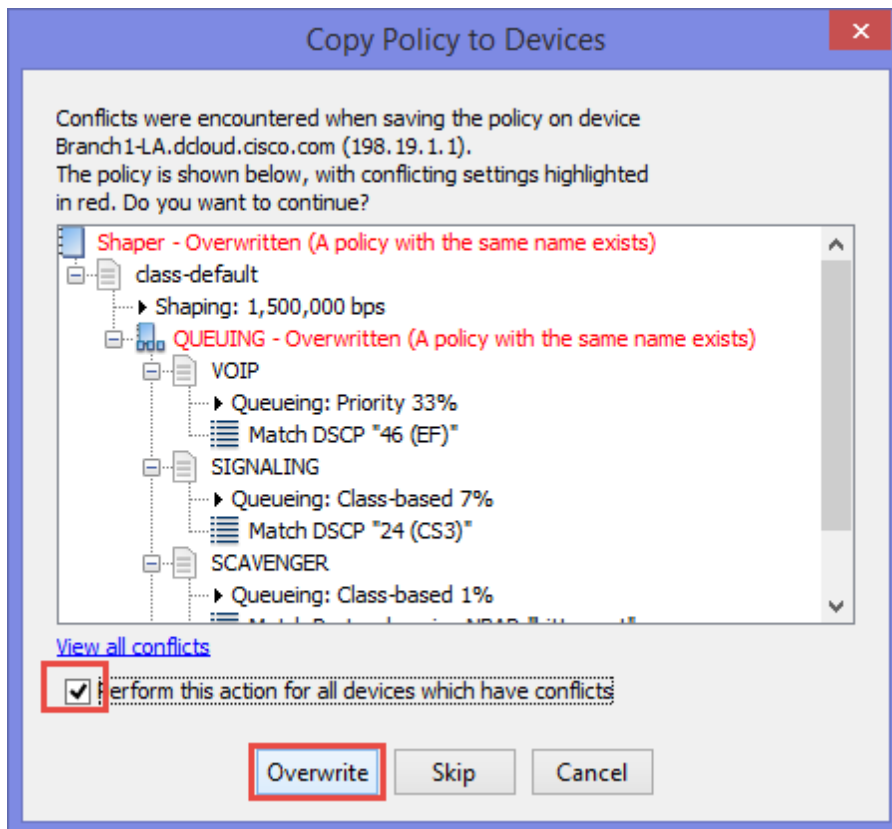


101. Select **Shaper** and select the other devices.



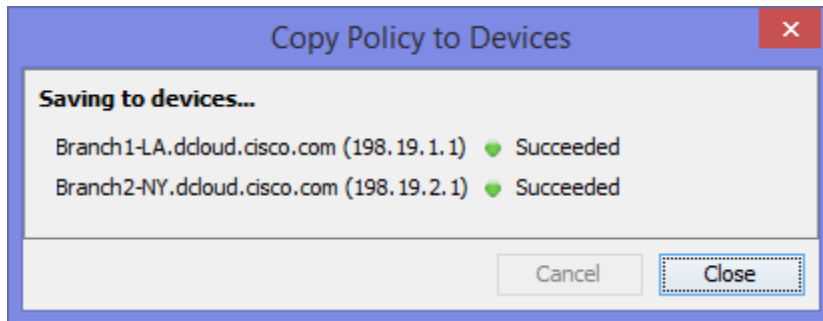
You are given a warning that you are overwriting a policy on both devices. This is what we want to do!

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

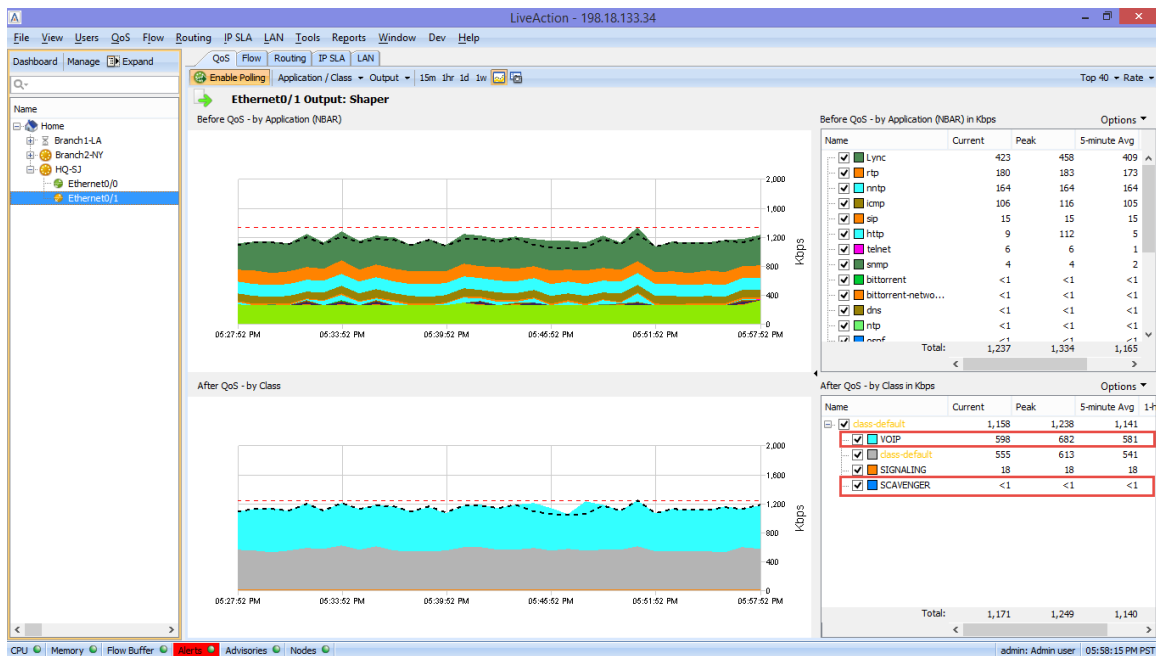


Ensure the copy is successful.

104. Click **Close**.



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



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

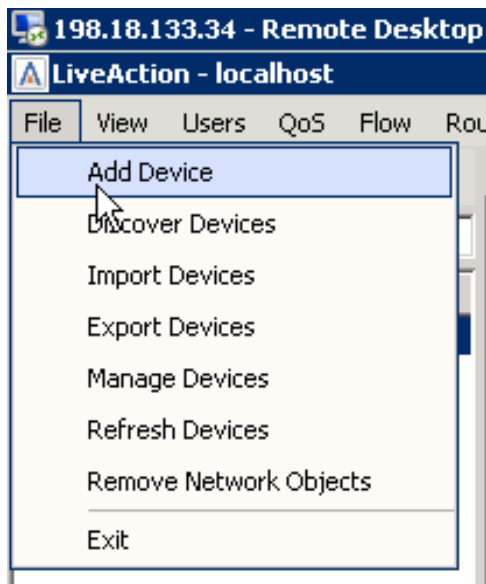
Lab A: Appendix

# 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”.

4. Click Next.

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

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

☐ 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

6. Click Next.

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:

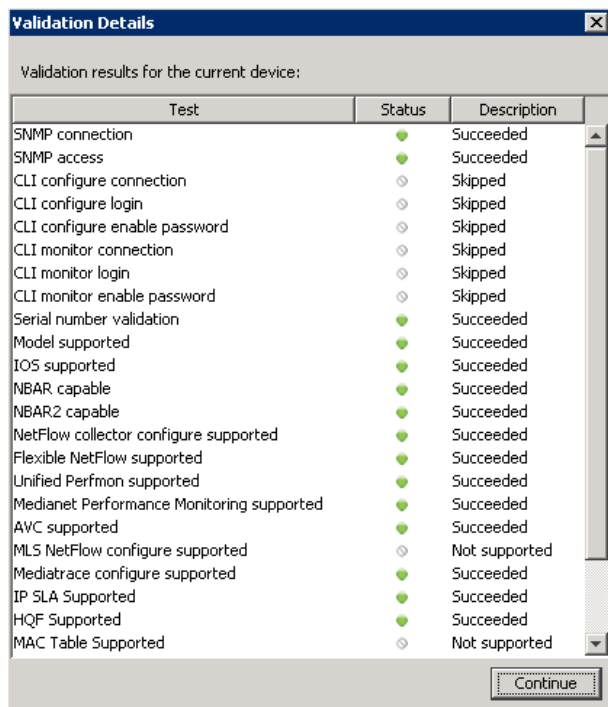
< Back Next > Finish Cancel Help

7. Select “Use the previous page connection settings”.

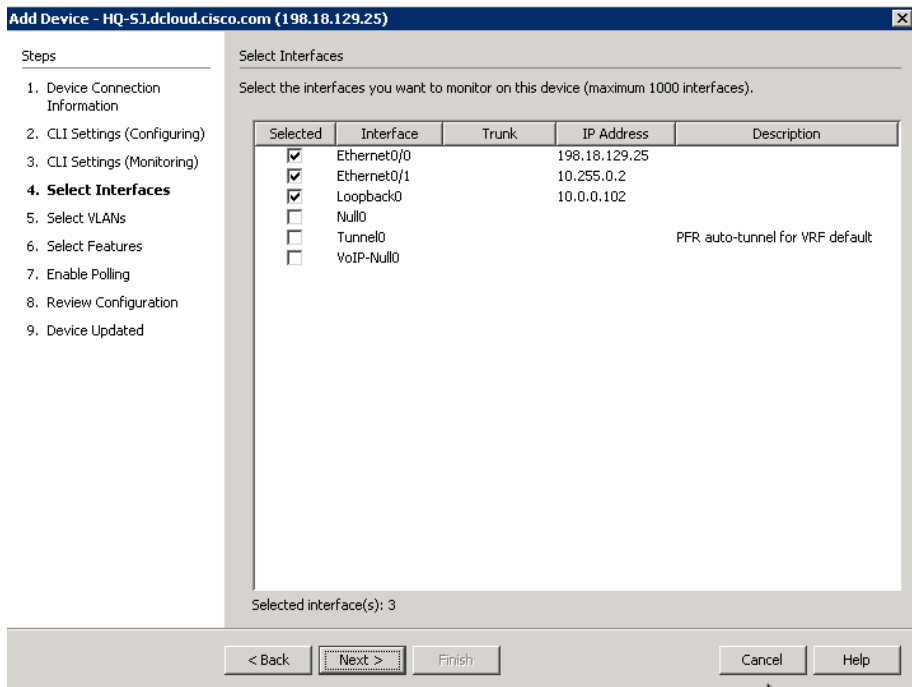
8. Click Next.

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

9. Click Continue.



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



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-S3.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 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.

< Back   Next >   Finish   Cancel   Help

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-S3.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 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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ethernet0/0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Loopback0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

< Back   Next >   Finish   Cancel   Help

12. Click Next.

13. Change the polling rate to 30 seconds.

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

The screenshot shows the 'Add Device' dialog box for HQ-S1.dcloud.cisco.com (198.18.129.25). The 'Steps' list on the left includes: 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, and 9. Device Updated. The main area is titled 'Enable Polling' and contains the instruction: '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.' Below this, the 'Polling Rate' is set to '30 seconds' in a dropdown menu. Under 'Poll the following features', the checkboxes for 'Flows', 'QoS', 'IP SLA', and 'Routing' are checked, while 'LAN\*' is unchecked. A note at the bottom states: '\* LAN polling occurs every 15 minutes' and '\* For SNMP v3, please see the User Guide on configuring LAN polling.' At the bottom of the dialog are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**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.

The screenshot shows the 'Add Device' dialog box for HQ-S1.dcloud.cisco.com (198.18.129.25) at the 'Review Configuration' step. The 'Steps' list on the left is the same as in the previous screenshot, with '8. Review Configuration' now selected. The main area is titled 'Review Configuration' and contains the instruction: 'The following commands will be sent to the device. Or you can choose to manually configure the device yourself.' Below this is a text area displaying the following configuration commands:

```
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
```

At the bottom, there are two radio buttons: 'Send the configuration commands to device.' (which is selected) and 'I will manually configure the device myself.' At the bottom of the dialog are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

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	●	●

< Back   Next >   **Finish**   Cancel   Help

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).

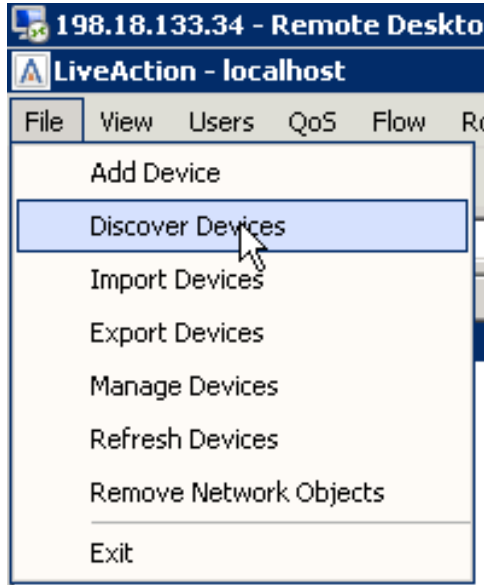
## Lab A.2: Client Device Discovery

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:

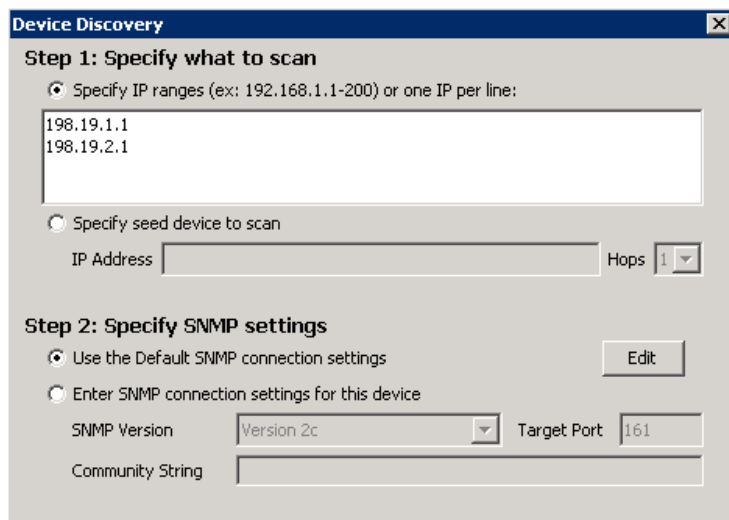
Adding several devices at once is as easy as adding a single device at a time. To do this:

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.

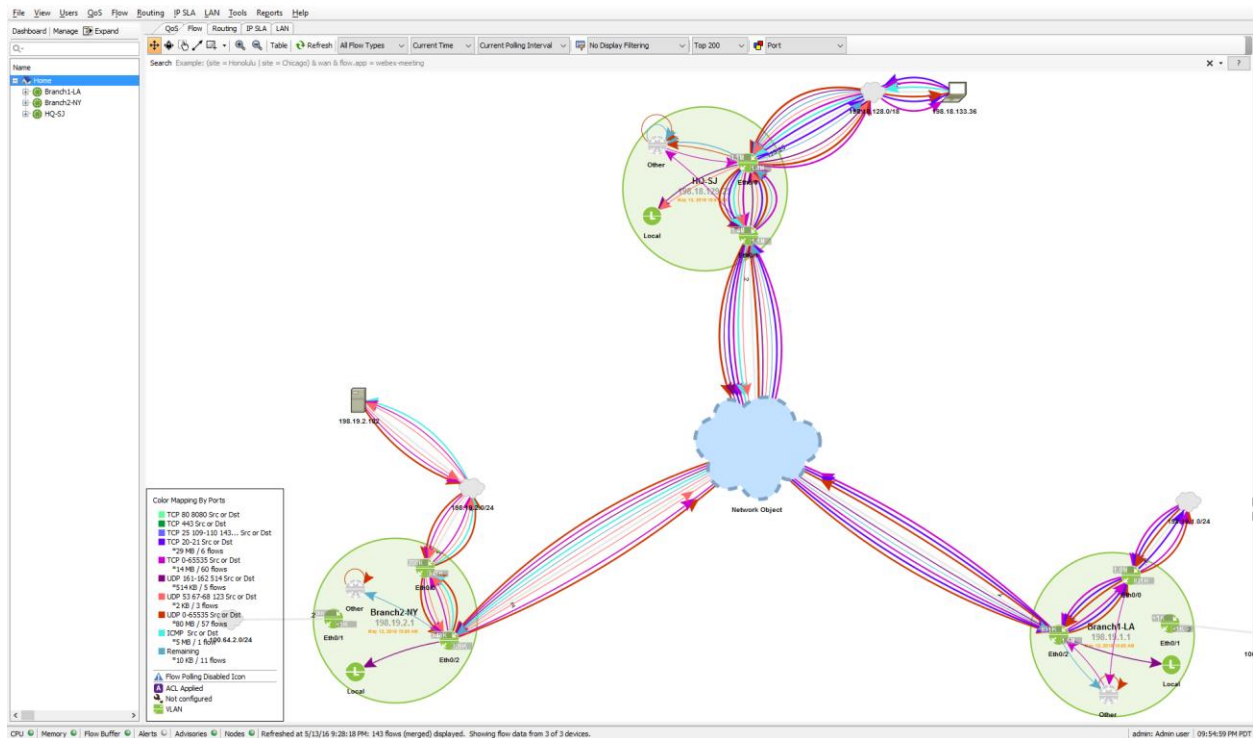


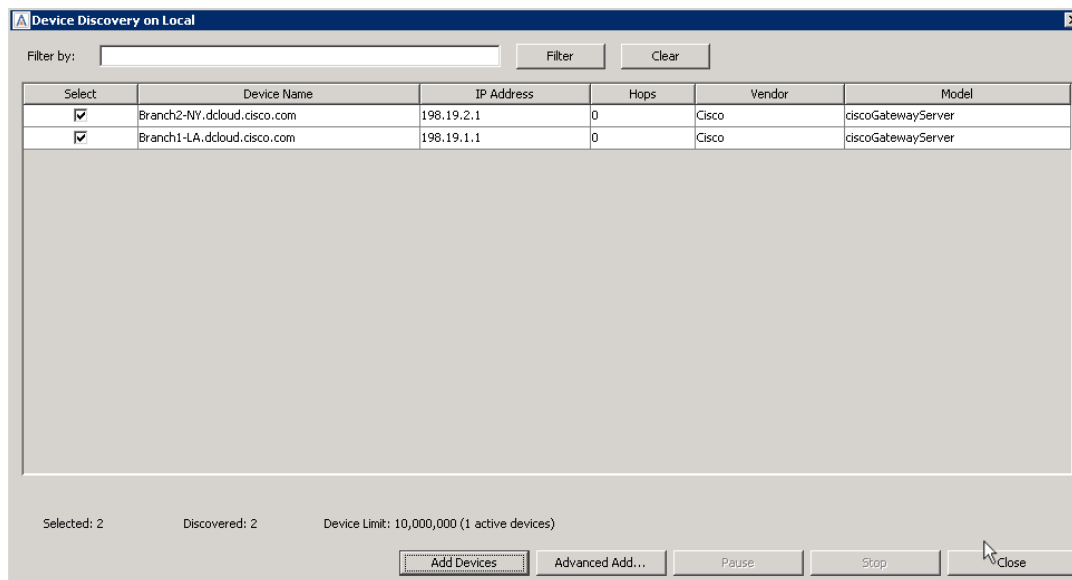
**Note:** In the Lab infrastructure we are utilizing the Local LiveNX Node included with the Server installation. If you require access to a Remote Node to access the subnets or addressing in “Step 1: Specify what to scan” you would use the Specify node drop-down at the bottom of this dialog box.



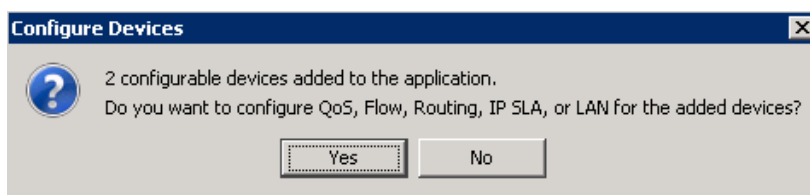
4. Click OK.
5. Verify that both devices were found, and then select Add Devices.

**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.





6. Select Yes on the configure devices dialog.



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.

The screenshot shows the 'Configure Cisco Devices' wizard window. On the left, a 'Steps' list shows '1. SNMP Settings' as the current step, followed by '2. CLI Settings (Configuring)', '3. CLI Settings (Monitoring)', '4. Validating Devices', '5. Select Features', '6. Enable Polling', '7. Update Device', and '8. Devices Configured'. The main area is titled 'SNMP Settings' and contains the instruction: 'Enter the SNMP connection information used for monitoring the selected devices.' There are two radio buttons: 'Use the Default SNMP connection settings' (which is selected) and 'Enter SNMP connection settings for this device'. An 'Edit' button is next to the first option. Below the radio buttons, there are fields for 'SNMP Version' (set to 'Version 2c') and 'Target Port' (set to '161'). A 'Community String' field is also present but empty. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

8. Select Use my default Configuration CLI connection settings.
9. Click next.

The screenshot shows the 'Configure Cisco Devices' wizard window at Step 2: 'CLI Settings (Configuring)'. The 'Steps' list on the left now highlights '2. CLI Settings (Configuring)'. The main area is titled 'CLI Settings (Configuring)' and contains the instruction: 'Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (\*).' There is a section titled 'Configuration CLI Connection Settings' with the sub-instruction: 'Enter Command Line Interface (CLI) connection settings used to configure these devices.' There are two radio buttons: 'Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp)' and 'Use my default: Configuration CLI connection settings' (which is selected). An 'Edit' button is next to the second option. Below the radio buttons, there is a section titled 'Enter connection settings for this device' with fields for 'Connection Type' (set to 'SSH'), 'Port\*' (set to '22'), 'User name on Device', 'Password on Device\*', and 'Enable Password'. A checkbox labeled 'Also use these credentials for monitor mode.' is at the bottom of this section. At the bottom of the window, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

10. Select Use the previous page connection settings.

The screenshot shows the 'Configure Cisco Devices' window with the 'CLI Settings (Monitoring)' tab selected. The left sidebar lists steps 1 through 8, with '3. CLI Settings (Monitoring)' highlighted. The main area contains instructions to specify CLI connection information. A sub-section titled 'Monitor-only CLI Connection Settings' offers three options: 'Use the default Monitor-only CLI connection settings' (with an 'Edit' button), 'Use the previous page connection settings' (which is selected), and 'Enter connection settings for this device'. Below these options are input fields for 'Connection Type' (set to SSH), 'Port\*' (set to 22), 'User name on Device', 'Password on Device\*', and 'Enable Password'. At the bottom are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

11. Click Next

12. After verifying that the device validation is successful, Click Next.

The screenshot shows the 'Configure Cisco Devices' window with the 'Validating Devices' tab selected. The left sidebar highlights step '4. Validating Devices'. The main area displays a message: '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.' Below this is a table with three columns: 'Device', 'Status', and 'Description'. The table contains two rows, both with a green status indicator and a 'Succeeded: click for details...' description. An 'Export Validation Details...' button is located below the table. The bottom navigation bar shows '< Back', 'Next >' (highlighted with a mouse cursor), 'Finish', 'Cancel', and 'Help'.

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Branch2-NY.dcloud.cisco.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

< Back   Next >   Finish   Cancel   Help

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	30 seconds
Branch2-NY.dcloud.cisco.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	30 seconds

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

< Back   Next >   Finish   Cancel   Help

**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.

**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

**Update Device**

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 **Send**

☐ Manually Configure Devices

Export Update Commands...

< Back Next > Finish Cancel Help

17. Once the updates are pushed successfully, 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

**Update Device**

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

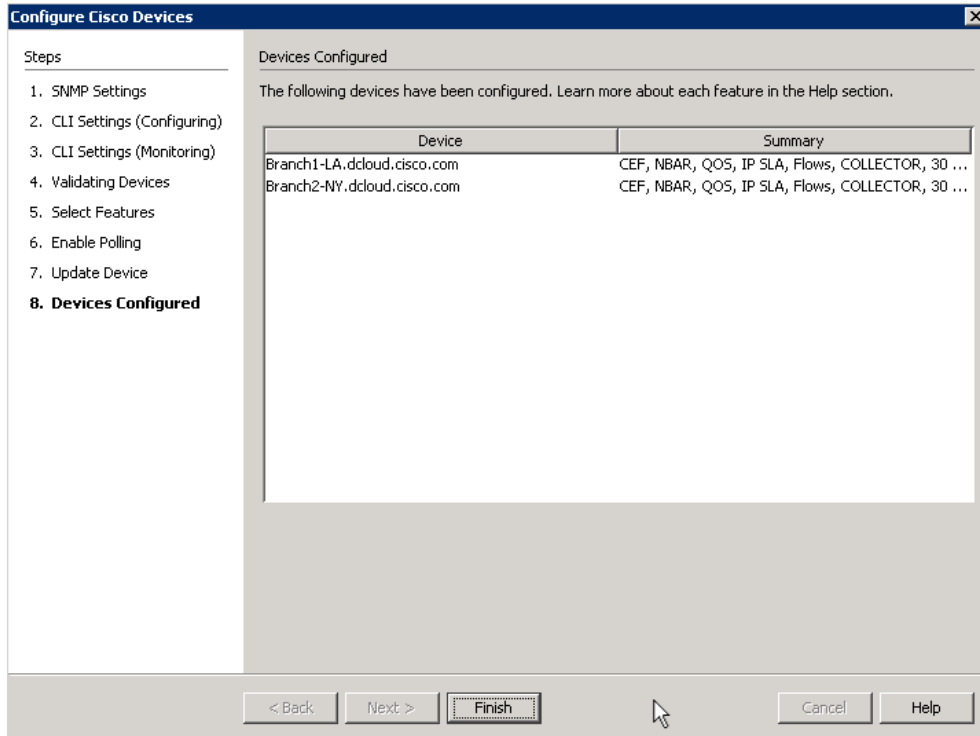
☒ Send Updates to Devices **Send**

☐ Manually Configure Devices

Export Update Commands...

< Back **Next >** Finish Cancel Help

18. Click finish to add the devices into the topology.

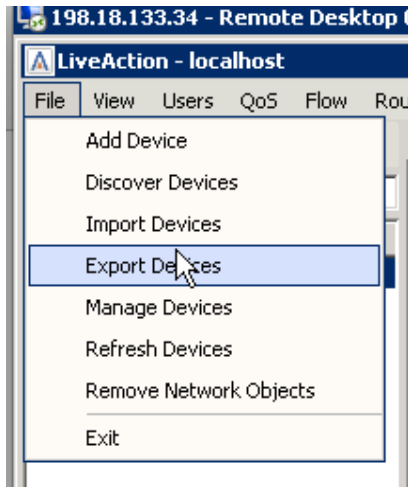


Now that you have added three devices to the topology, they should look familiar to the image below. What is important to remember is that you should only bring in interfaces that will have interesting traffic, to you, traversing them. We will not need all the interfaces that have been included, so in 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.



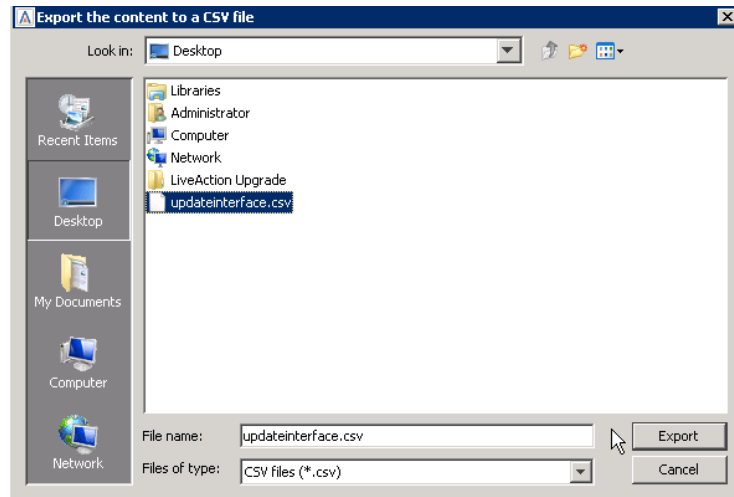
2. Deselect **GigabitEthernet2** and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

A screenshot of the 'Export Devices' dialog box. It features a search bar at the top right and a table of network devices. The table has columns for 'Add/Up...', 'Name', 'Type', 'Device Serial', 'IP Address', 'Vendor', 'Model', 'IOS Version', 'Description', 'Line Rate (Kb...', 'Node', 'Site', 'Site CIDR', and 'Data Cen...'. The table lists three routers: 'Branch1-LA.dcloud.cisco.com' (Serial 101), 'HQ-B1.dcloud.cisco.com' (Serial 2), and 'HQ-MC.dcloud.cisco.com' (Serial 1). Each router has several interfaces listed, including GigabitEthernet1, GigabitEthernet2, Loopback0, Null0, and VoIP-Null0. Checkmarks in the 'Add/Up...' column indicate which interfaces are selected for export. In this view, GigabitEthernet2 and Loopback0 are deselected for the first two routers. At the bottom right, there are 'Export to CSV' and 'Close' buttons.

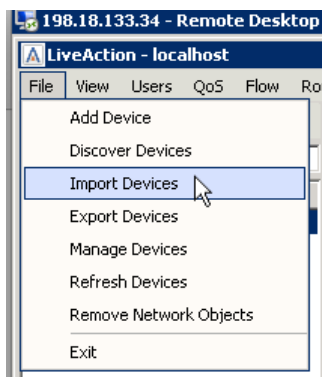
Add/Up...	Name	Type	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (Kb...	Node	Site	Site CIDR	Data Cen...
<input checked="" type="checkbox"/>	Branch1-LA.dcloud.cisco.com	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...	1,000,000	Local	LA	10.0.1.1, 198.19.1...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	2,000				
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		100.64.1.2				Internet	1,000				
<input checked="" type="checkbox"/>	GigabitEthernet3	Interface		10.255.1.2				MPLS	8,000,000				
<input type="checkbox"/>	Loopback0	Interface		10.0.1.1					10,000,000				
<input type="checkbox"/>	Null0	Interface							10,000,000				
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000				
<input checked="" type="checkbox"/>	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...	1,000,000	Local	HQ		<input type="checkbox"/>
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000				
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		100.64.0.2				Internet	8,000,000				
<input type="checkbox"/>	Loopback0	Interface							10,000,000				
<input type="checkbox"/>	Null0	Interface							10,000,000				
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000				
<input checked="" type="checkbox"/>	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...	1,000,000	Local	HQ		<input type="checkbox"/>
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.25					1,000,000				
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		10.255.0.2					8,000,000				
<input type="checkbox"/>	Loopback0	Interface		10.0.0.102					10,000,000				
<input type="checkbox"/>	Null0	Interface							10,000,000				
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000				
<input checked="" type="checkbox"/>	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...	1,000,000	Local	HQ		<input type="checkbox"/>
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.23					8,000,000				
<input type="checkbox"/>	Loopback0	Interface		10.0.0.103					10,000,000				
<input type="checkbox"/>	Null0	Interface							10,000,000				
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000				

3. Select Export to csv.

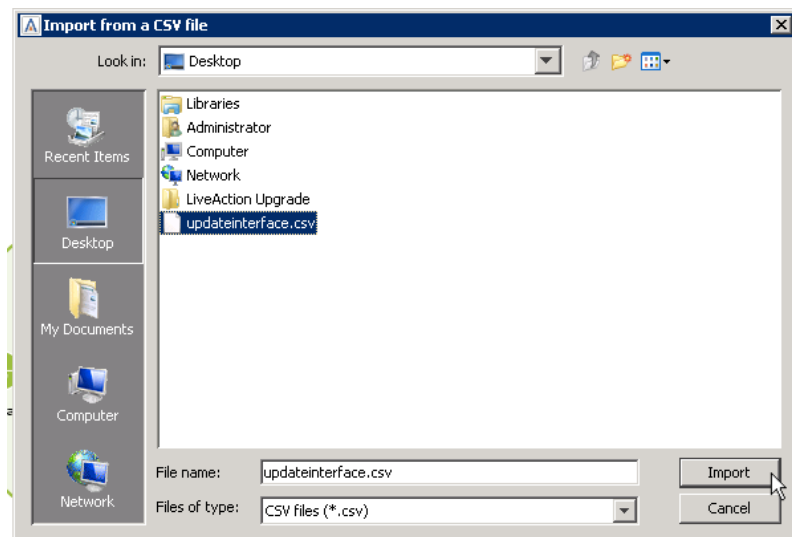
4. On the Export window give the file a name.
5. Export the csv to the desktop, or appropriate directory.



6. Close the export devices window.
7. Select File and Import Devices.



8. Select the file you previously exported.

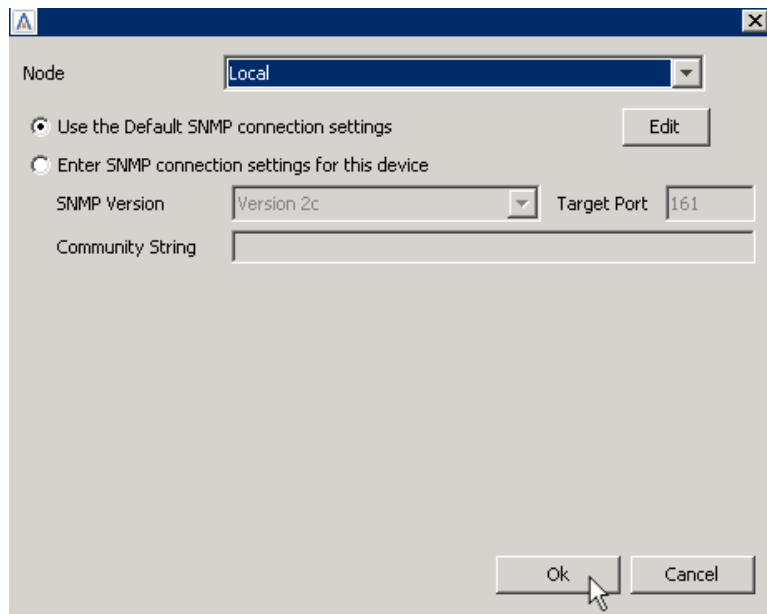


9. Click Add/Update Devices.

Add/Upd...	Name	Type	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K...	Node	Site	Site CIDR	Data Ce...	W
<input checked="" type="checkbox"/>	Branch1-LA.dcloud.cisco.com	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	LA	10.0.1.1, 198.1...	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000					
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		100.64.1.2				Internet	2,000					
<input checked="" type="checkbox"/>	GigabitEthernet3	Interface		10.255.1.2				MPLS	1,000					
<input type="checkbox"/>	Loopback0	Interface		10.0.1.1					8,000,000					
<input type="checkbox"/>	Null0	Interface							10,000,000					
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000					
<input checked="" type="checkbox"/>	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000					
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000					
<input checked="" type="checkbox"/>	Loopback0	Interface							8,000,000					
<input type="checkbox"/>	Null0	Interface							10,000,000					
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000					
<input checked="" type="checkbox"/>	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.25					1,000,000					
<input checked="" type="checkbox"/>	GigabitEthernet2	Interface		10.255.0.2					1,000,000					
<input checked="" type="checkbox"/>	Loopback0	Interface		10.0.0.102					8,000,000					
<input type="checkbox"/>	Null0	Interface							10,000,000					
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000					
<input checked="" type="checkbox"/>	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	HQ		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	GigabitEthernet1	Interface		198.18.129.23					1,000,000					
<input checked="" type="checkbox"/>	Loopback0	Interface		10.0.0.103					8,000,000					
<input type="checkbox"/>	Null0	Interface							10,000,000					
<input type="checkbox"/>	VoIP-Null0	Interface							10,000,000					

Add/Update Devices Import from CSV Export to CSV Close

10. Click OK to use the Default SNMP settings.



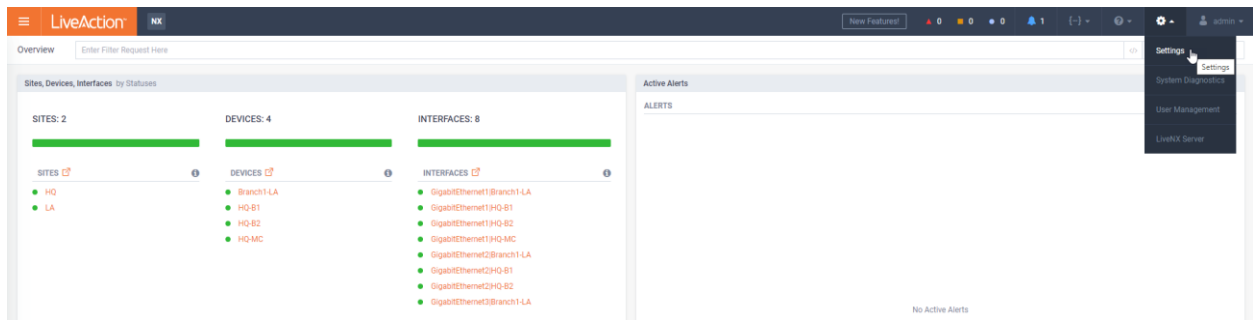
Your Topology Pane will now show the appropriate devices/configurations.

# Lab A.4: Saving Server Configurations

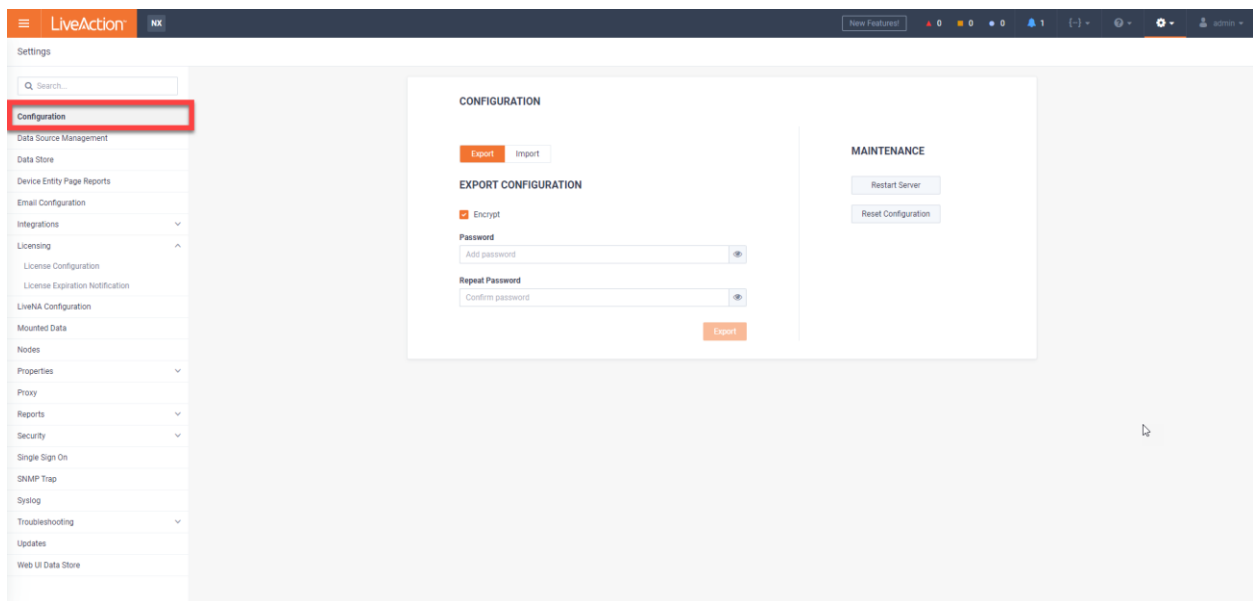
Prior to upgrading the LiveAction Software, or to retain existing Server configuration for use in the case of a hardware failure or misconfiguration, the current configuration file may be Exported to a local or network drive.

Lab Steps:

1. Open the LiveNX WebUI, select **Settings**.

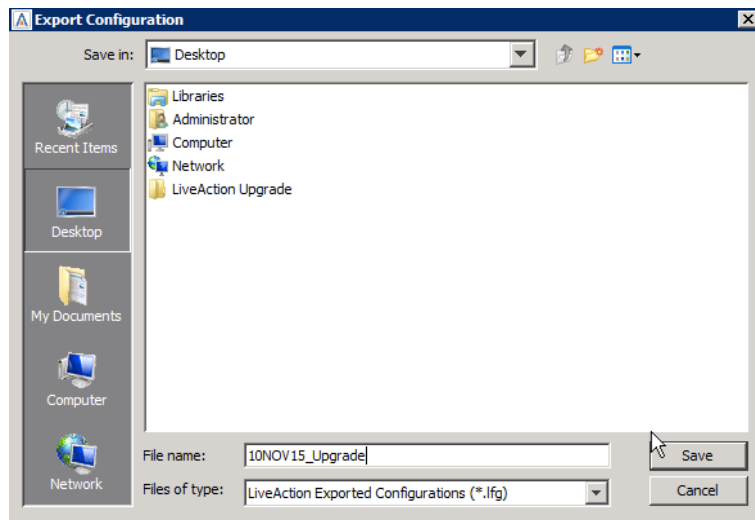


2. Select **Configuration**.



3. Click **Export**.
4. Enter encryption password if preferred.





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.

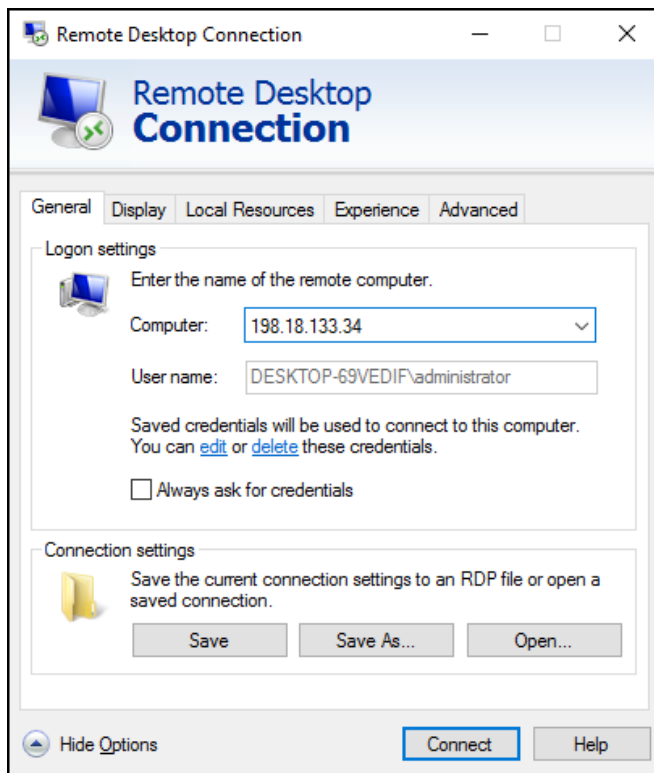
---

### 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.)

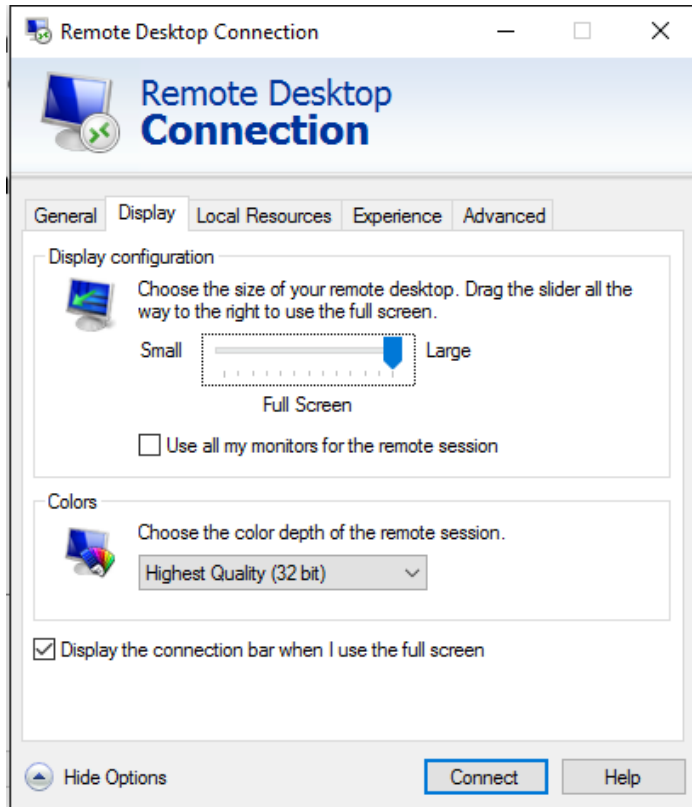
### DIAGRAM



- 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.

✓

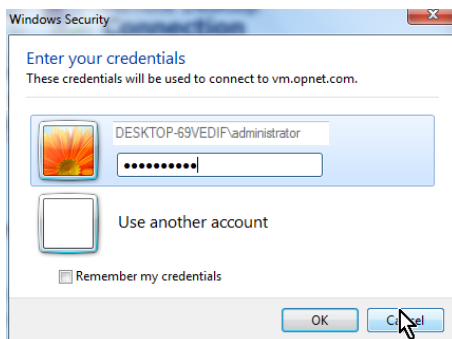
## DIAGRAM



9. Select Connect.

10. Enter the workstation password: **C1sco12345** (or otherwise defined by instructor).

## DIAGRAM



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.

---