LiveAction Training

Lab Workbook Pt. 1

4/8/2022
© Copyright 2022, 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.
March 2022.

Table of Contents

© Copyright LiveAction 2022

4/8/2022

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.

© Copyright LiveAction 2022

Lab .0

Lab 0: Setup and Get Connected

 © Copyright LiveAction 2022

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

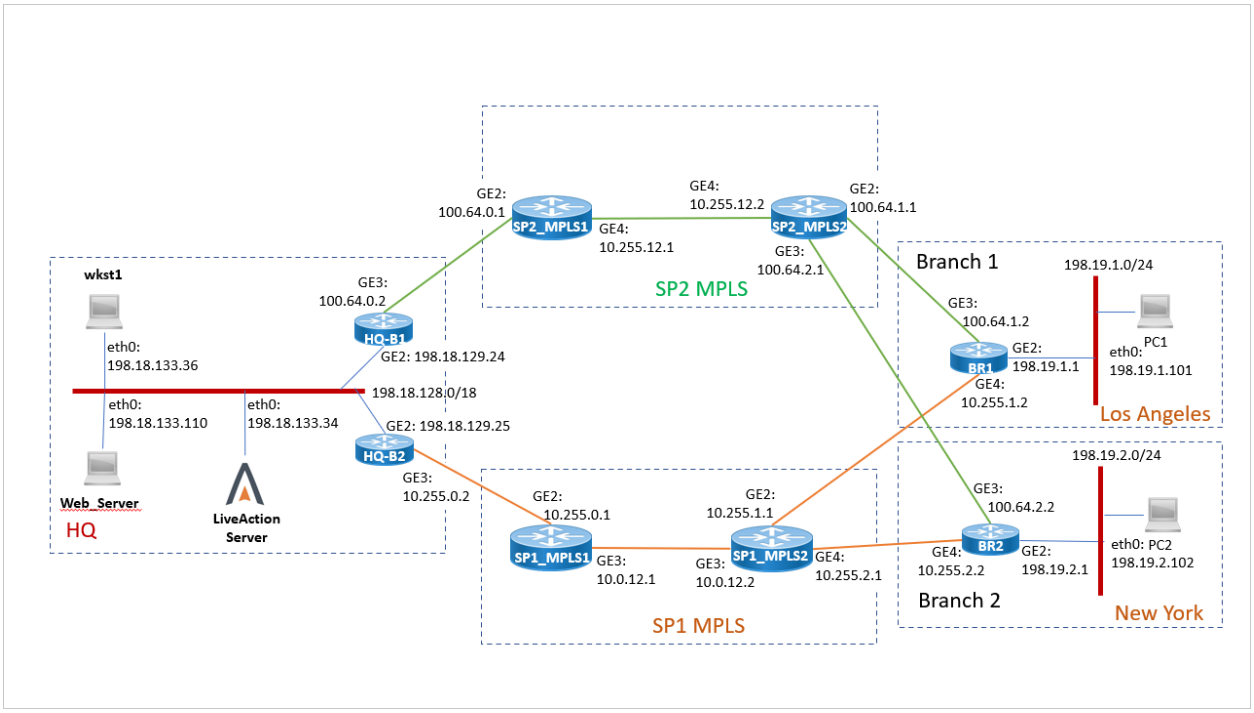


Figure 1

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 fully reflect the parameters of your pod.

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

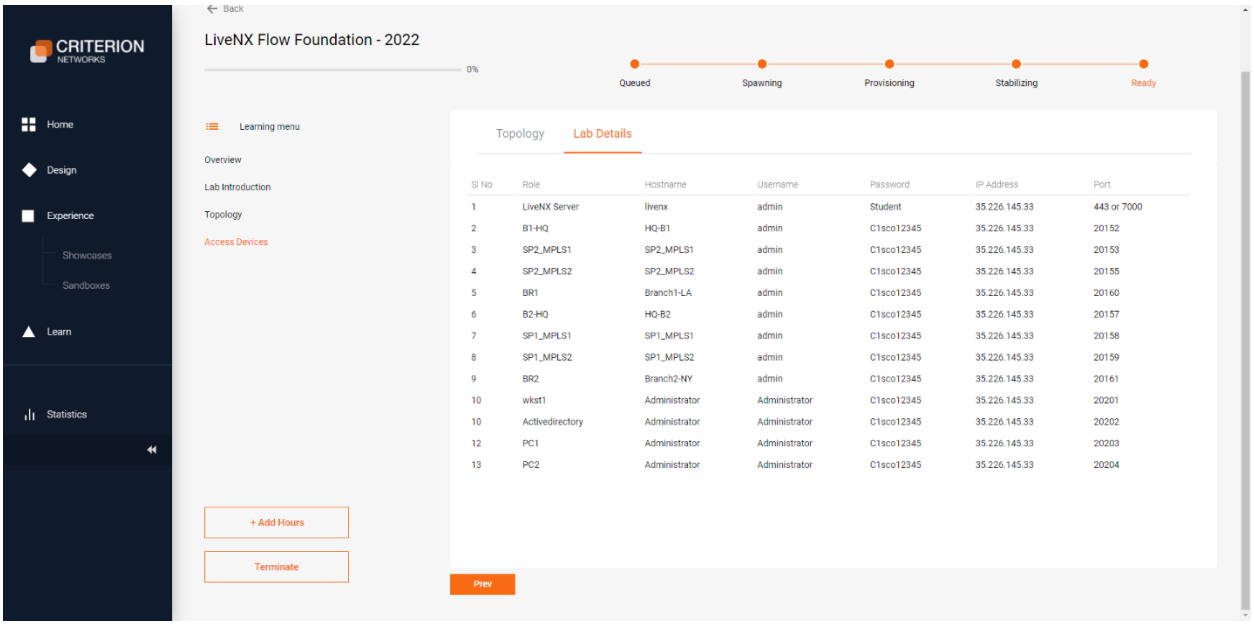


Figure 2

Lab Steps:

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

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

Lab 0.2: Connecting to Your Training Pod

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

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

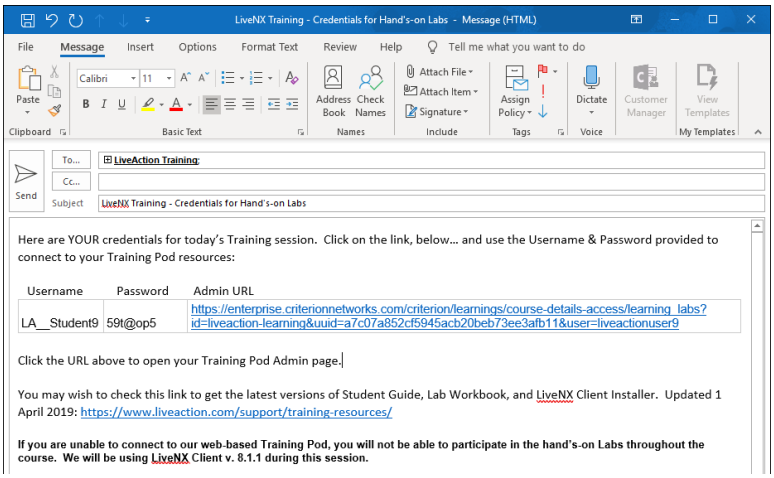


Figure 3

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**.

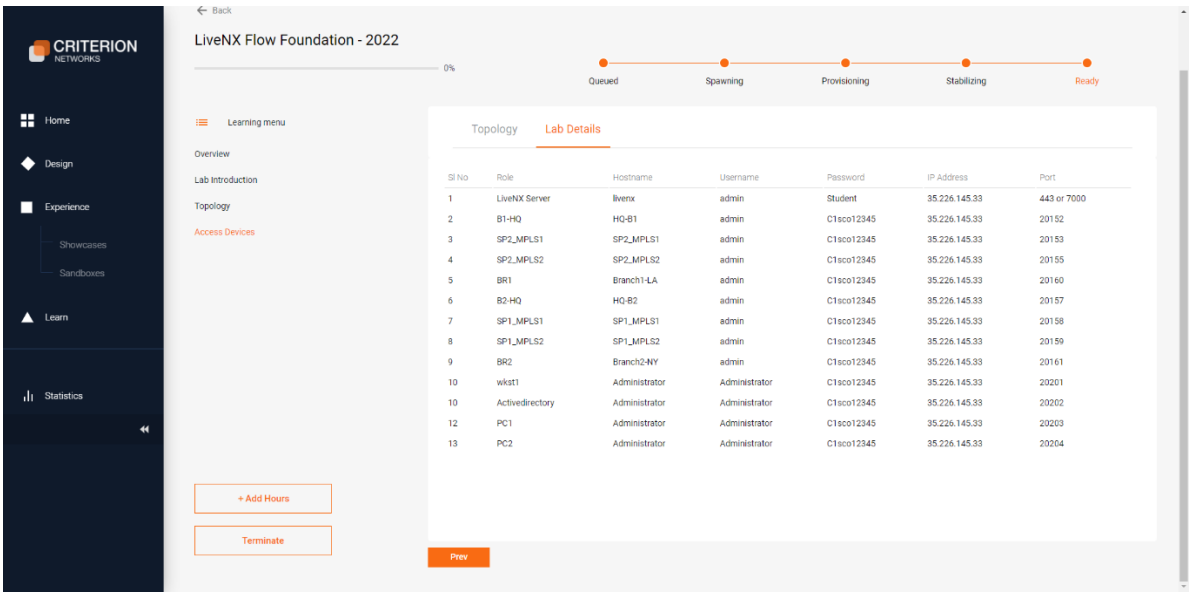


Figure 4

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.

 © Copyright LiveAction 2022

Lab 1

Lab 1: The LiveNX Web UI

© Copyright LiveAction 2022

Lab 1.1: Explore the Web UI

<u>These Labs uses the WebUI exclusively.</u>

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**

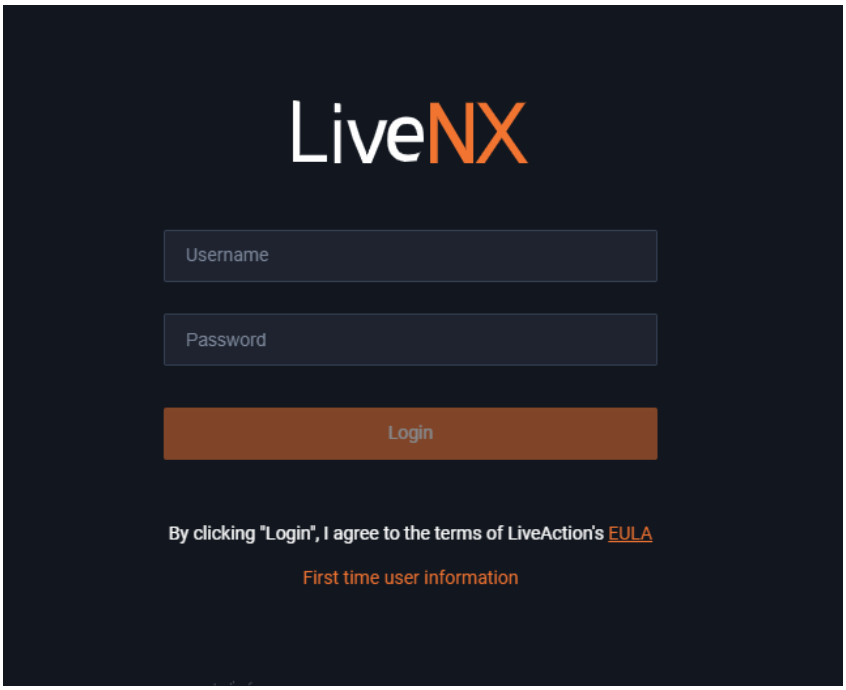


Figure 5

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!

 © Copyright LiveAction 2022

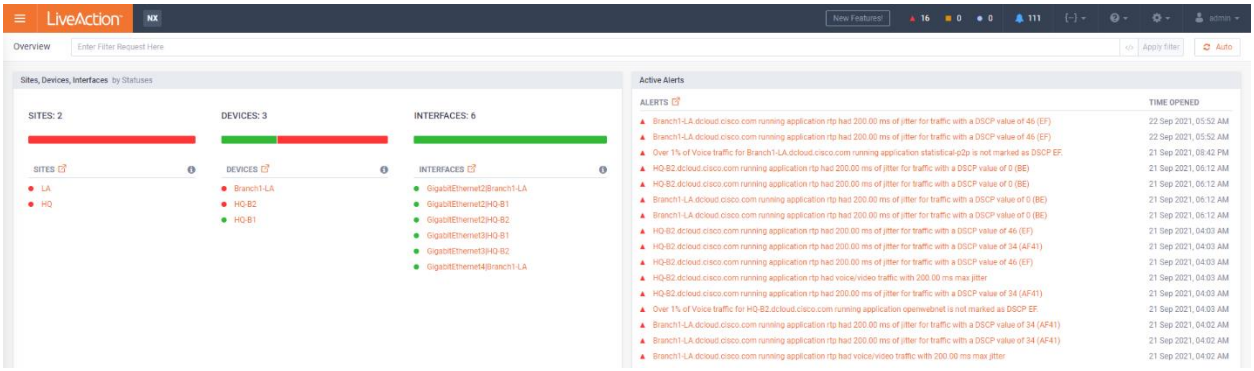


Figure 6

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

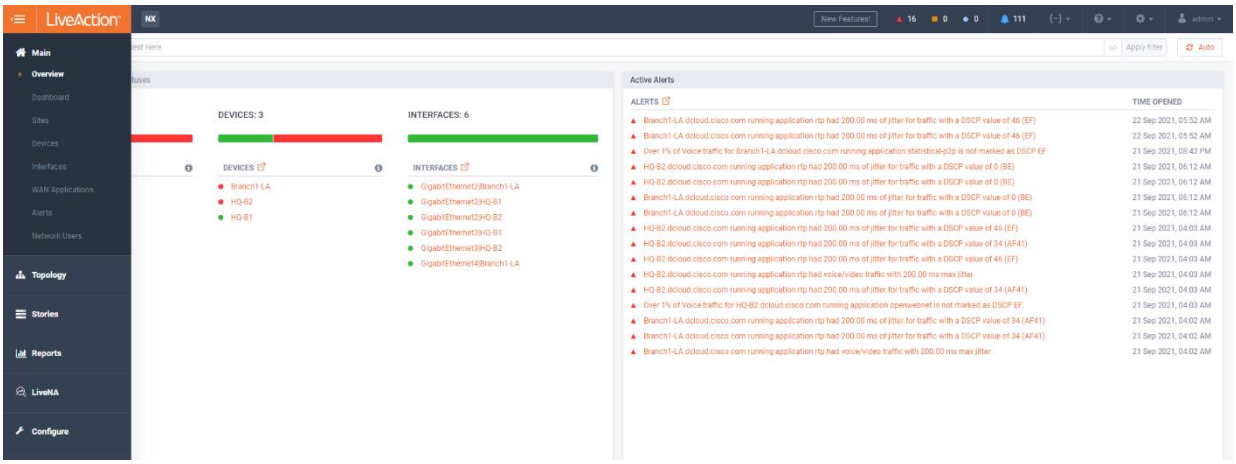


Figure 7

5. Select **Sites.**

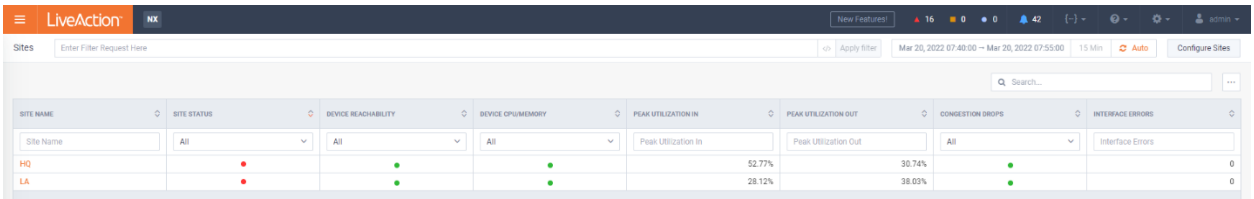


Figure 8

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

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

---

6. Note: Status, Utilization, Drops, Errors, etc.…
7. Toggle the **Auto Update** to ON.
8. Click on the link to **LA** 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).

 © Copyright LiveAction 2022

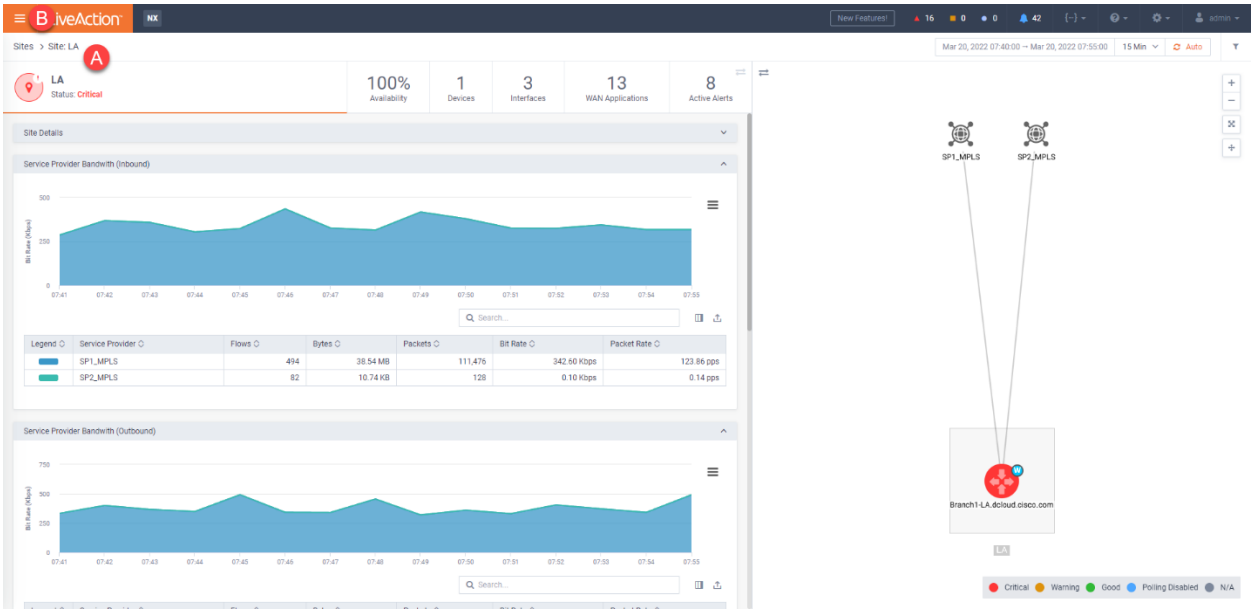


Figure 9

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

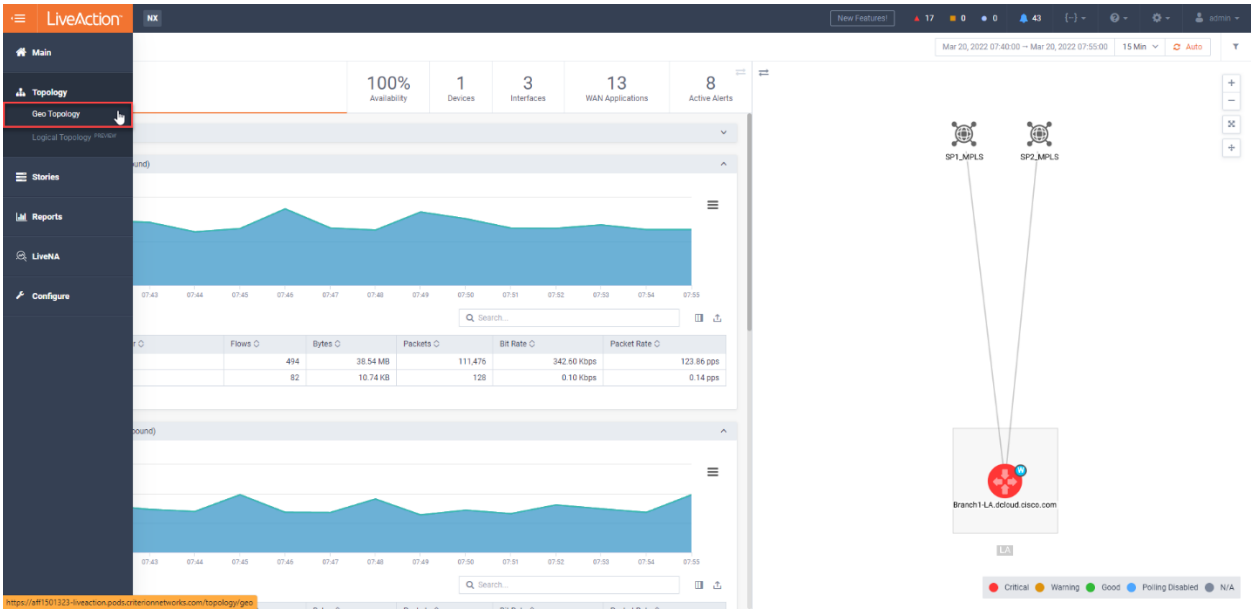


Figure 10

10. Click on a Site to see additional information & pivot points to other views/details.

 © Copyright LiveAction 2022

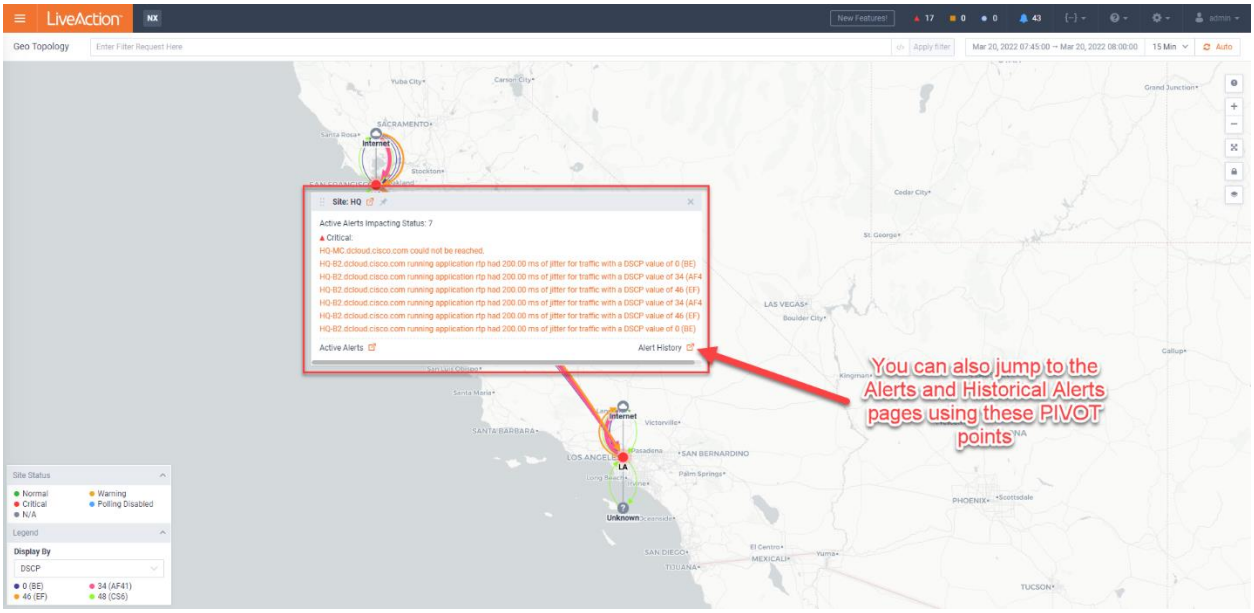


Figure 11

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

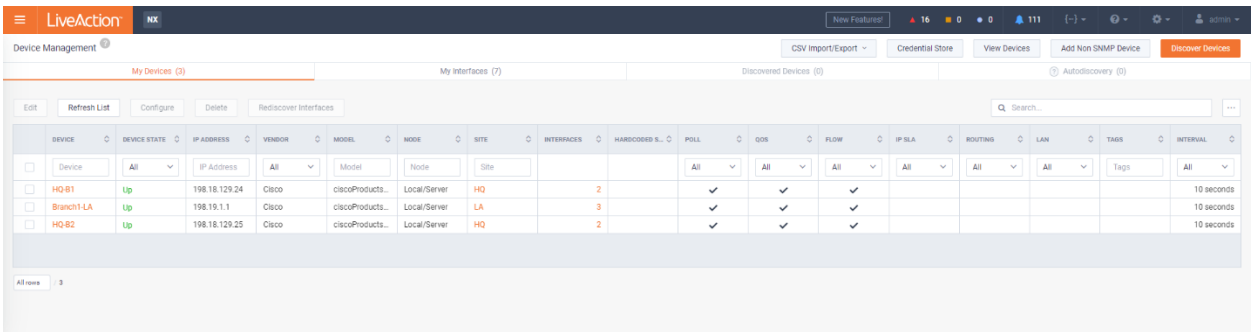


Figure 12

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

 © Copyright LiveAction 2022

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".

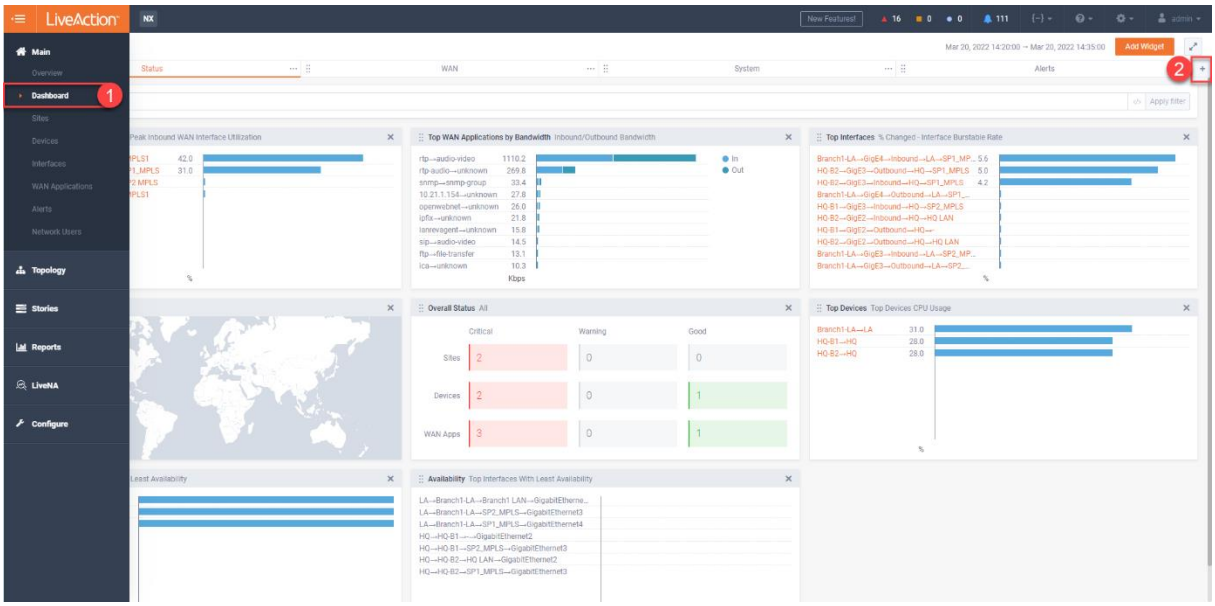


Figure 13

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

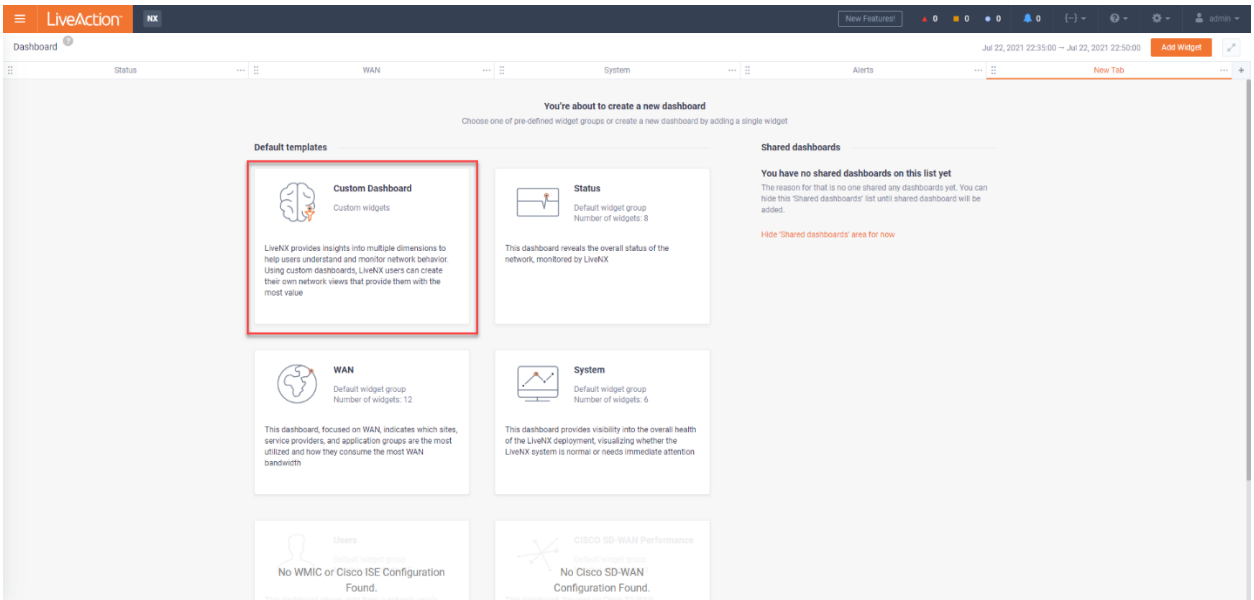


Figure 14

 © Copyright LiveAction 2022

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

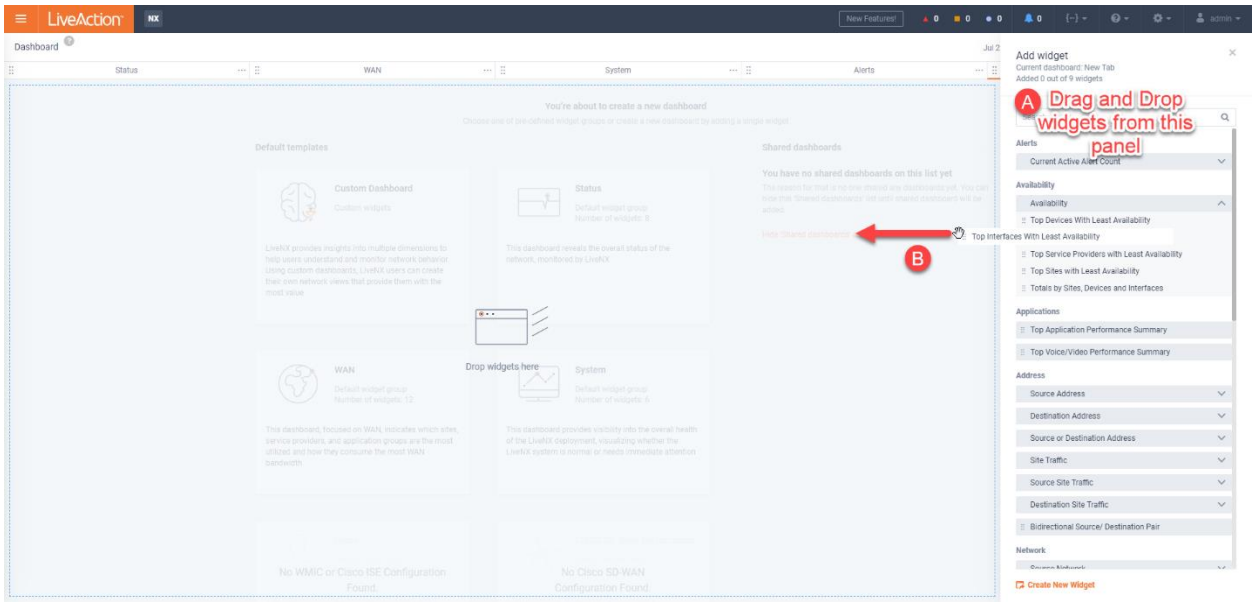


Figure 15

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

4. **Delete** un-wanted Widgets by clicking the **X** at top right of the widget.
5. To give the dashboard tab a more appropriate name, simply select the **New Tab** text and rename your dashboard.
6. You can also change the order Click the **6-Dots** and drag to the location you wish to move it too – much like a browser tab.

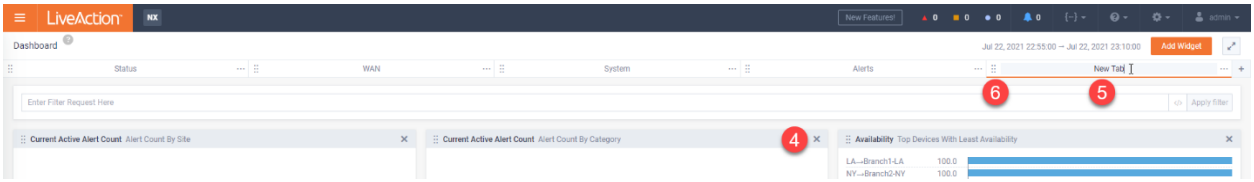


Figure 16

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.

 © Copyright LiveAction 2022

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**.

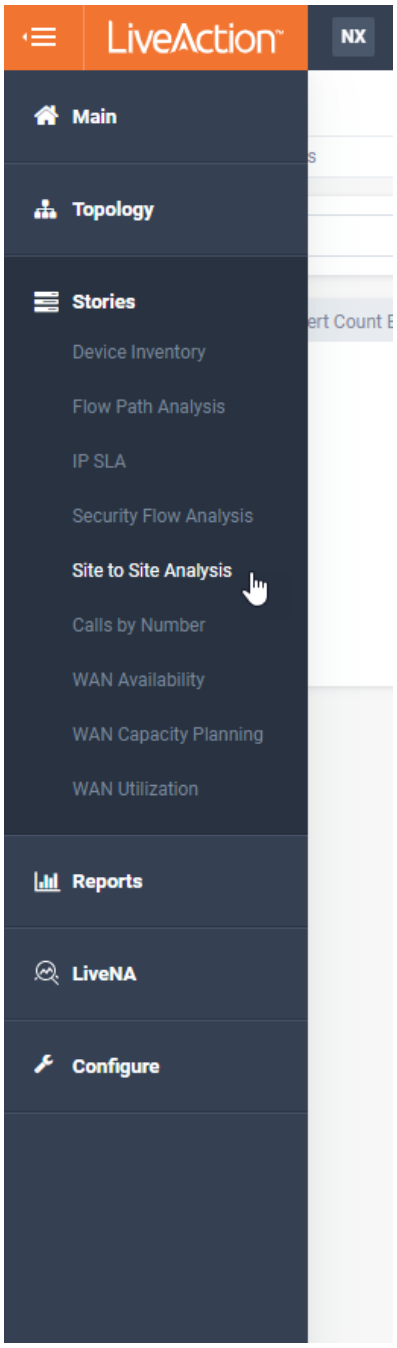


Figure 17

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.**

 © Copyright LiveAction 2022

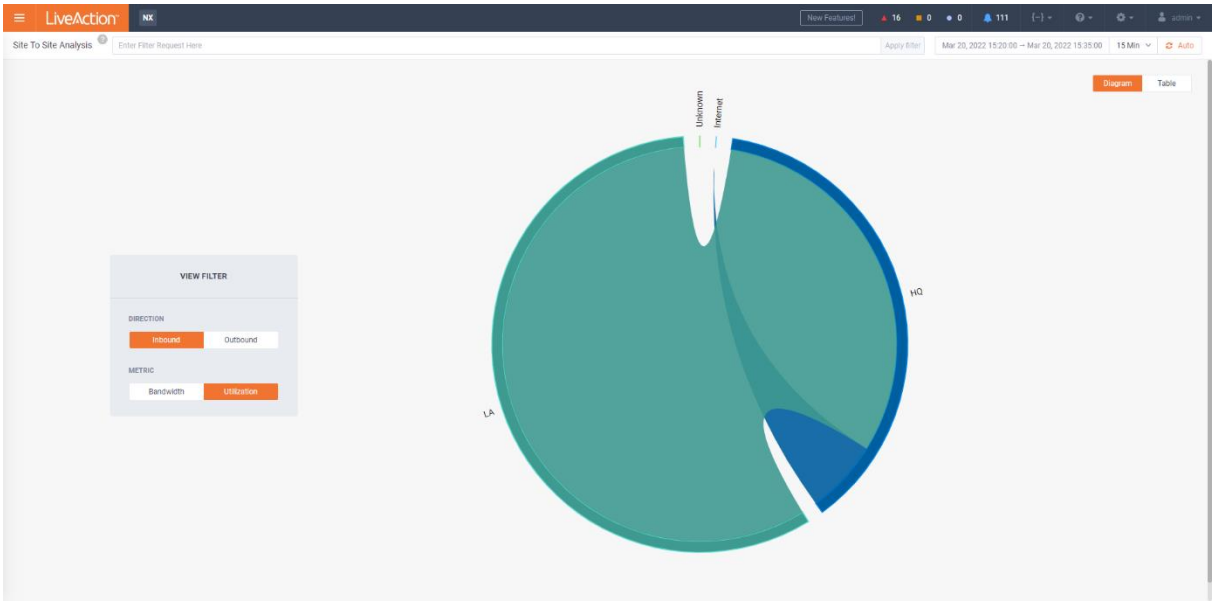


Figure 18

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

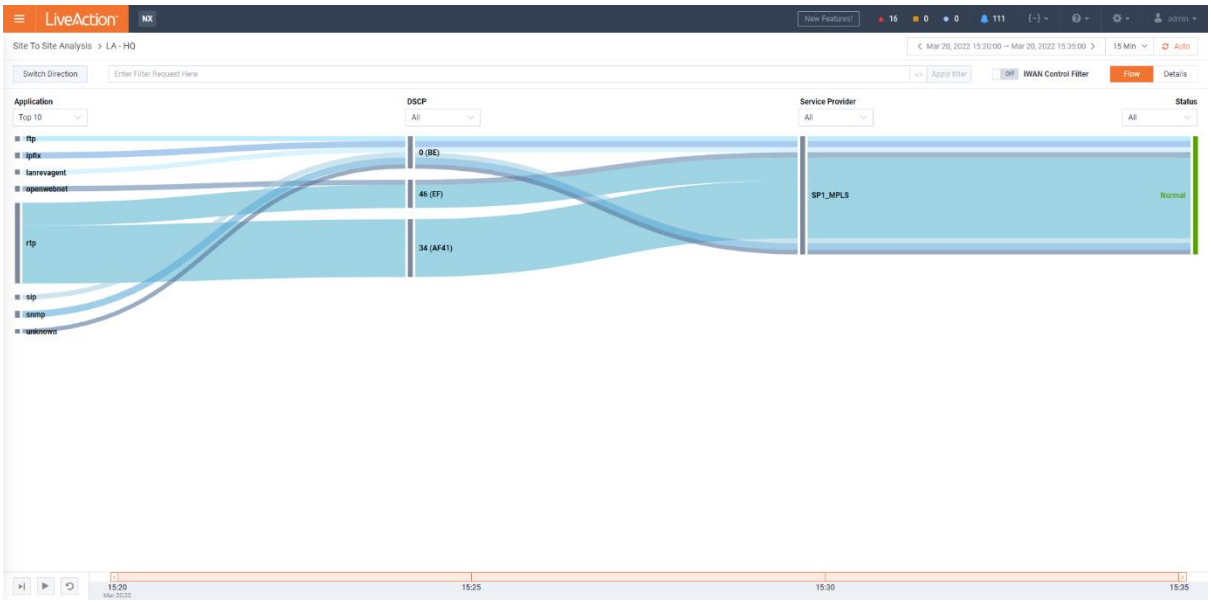


Figure 19

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

 © Copyright LiveAction 2022

Lab 1.4: WebUI

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.

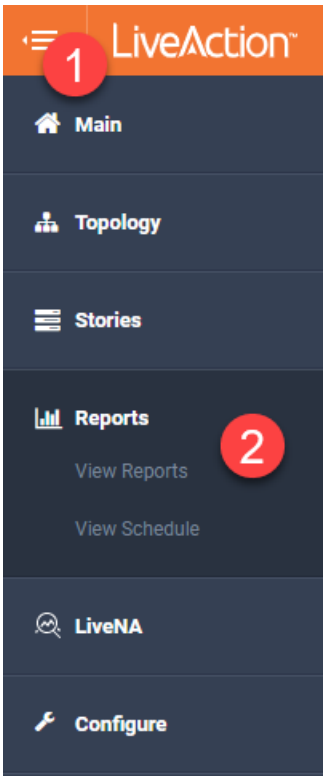


Figure 20

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

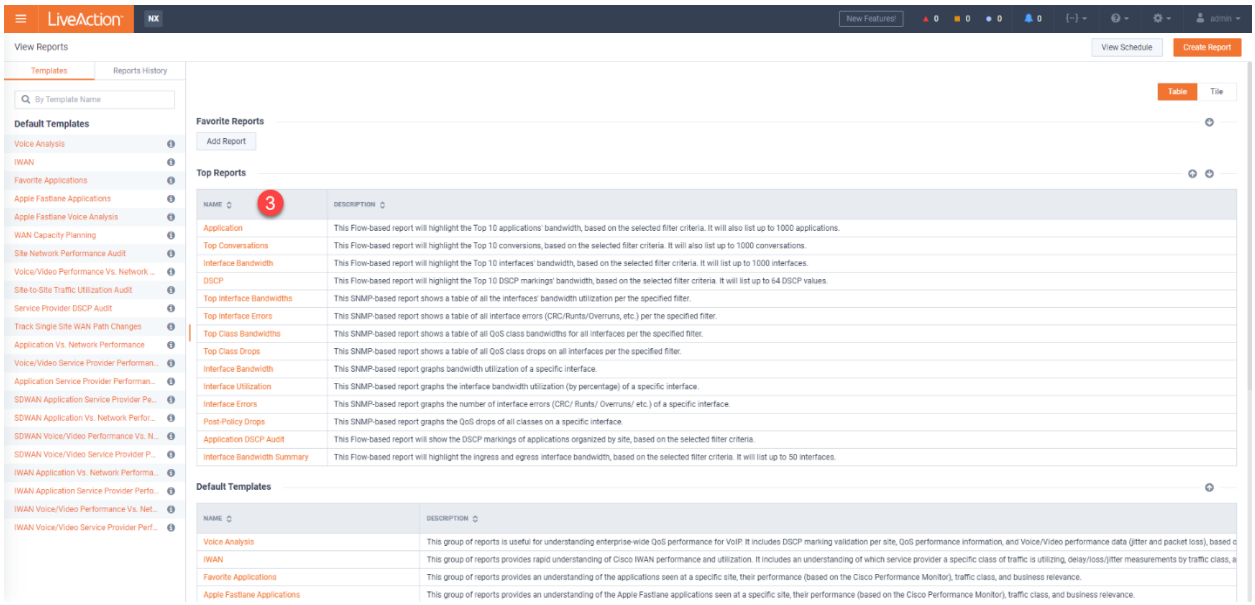


Figure 21

© Copyright LiveAction 2022

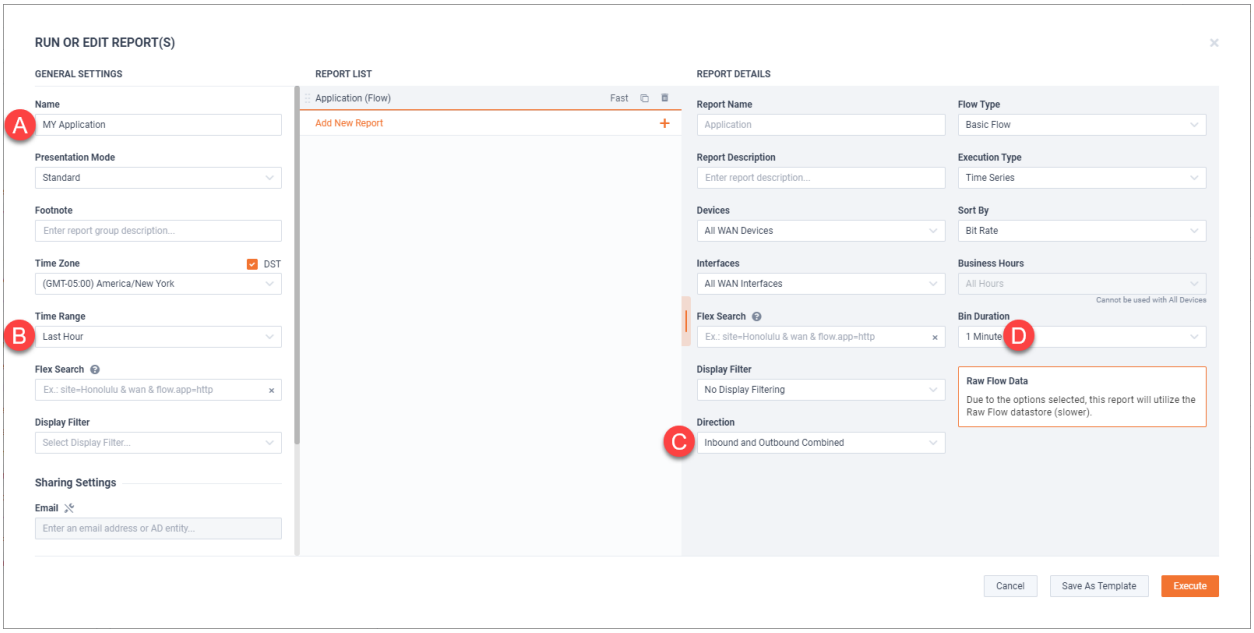


Figure 22

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.

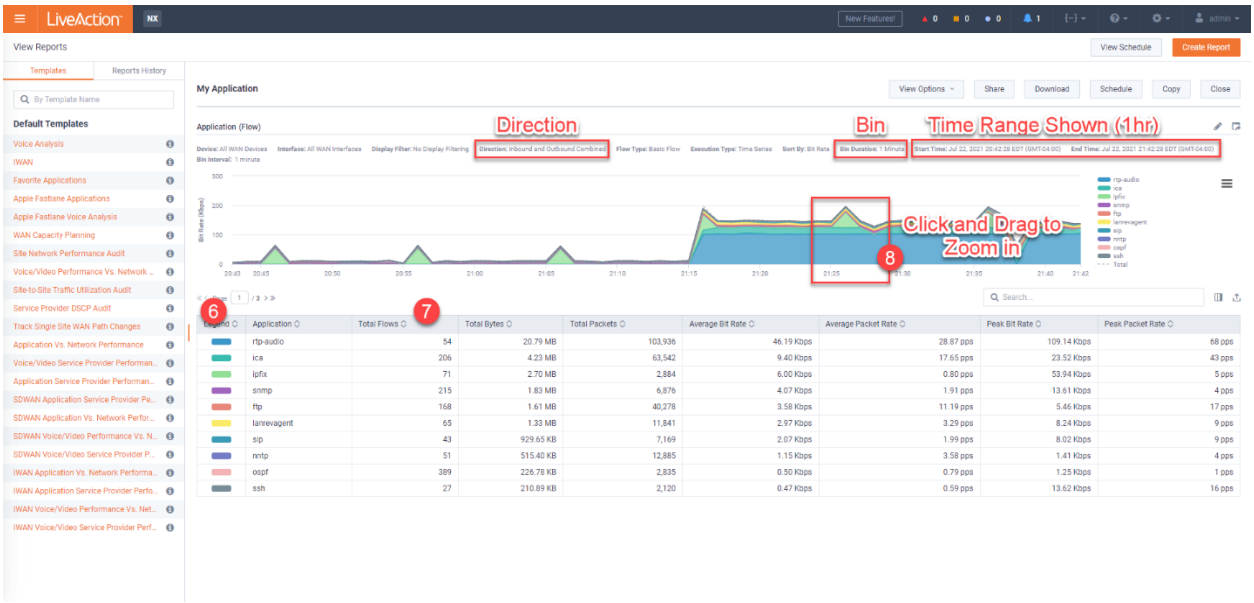


Figure 23

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.

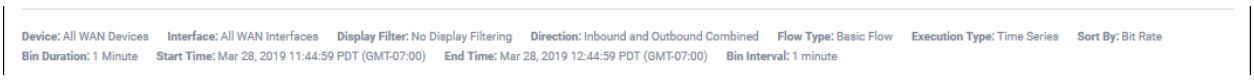


Figure 24

© Copyright LiveAction 2022

6. **Hide** a metric by clicking on the Legend (in the table, or on right of chart).
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.

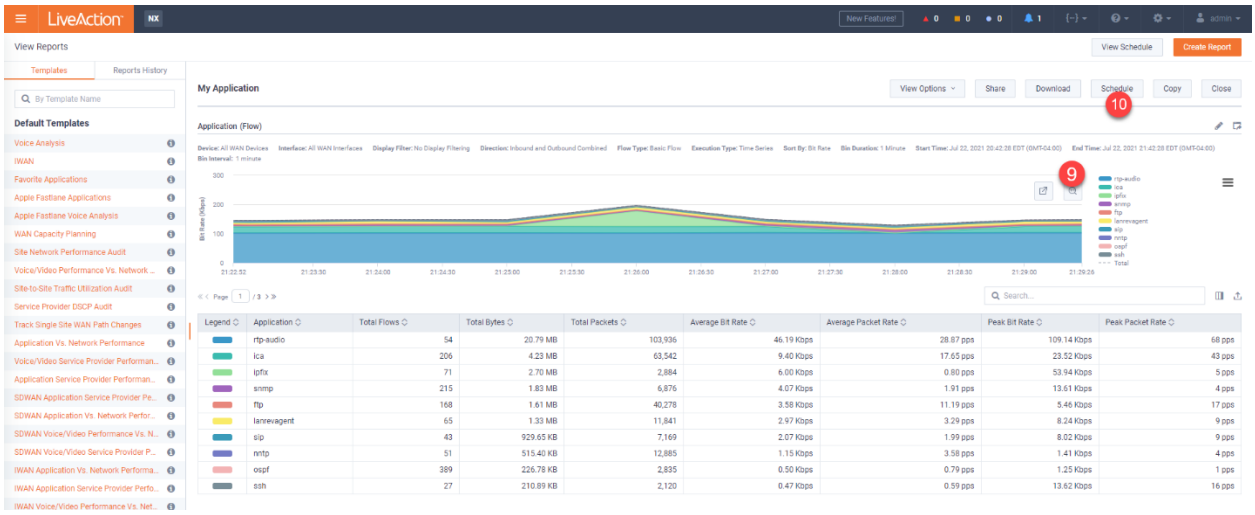


Figure 25

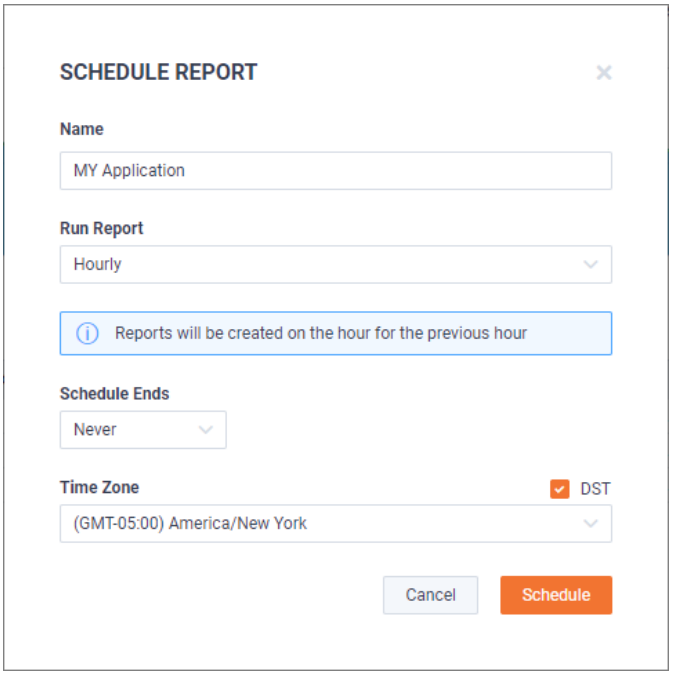


Figure 26

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

Figure 27

© Copyright LiveAction 2022

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

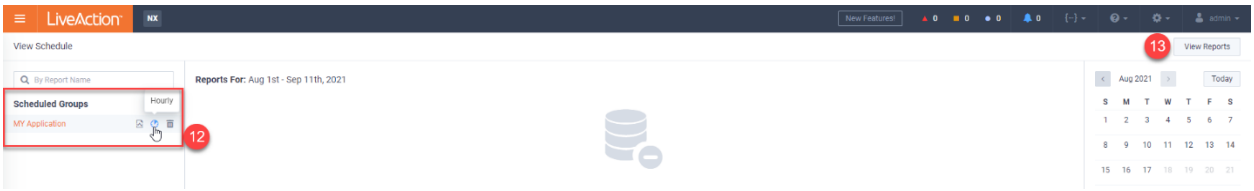


Figure 28

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.**

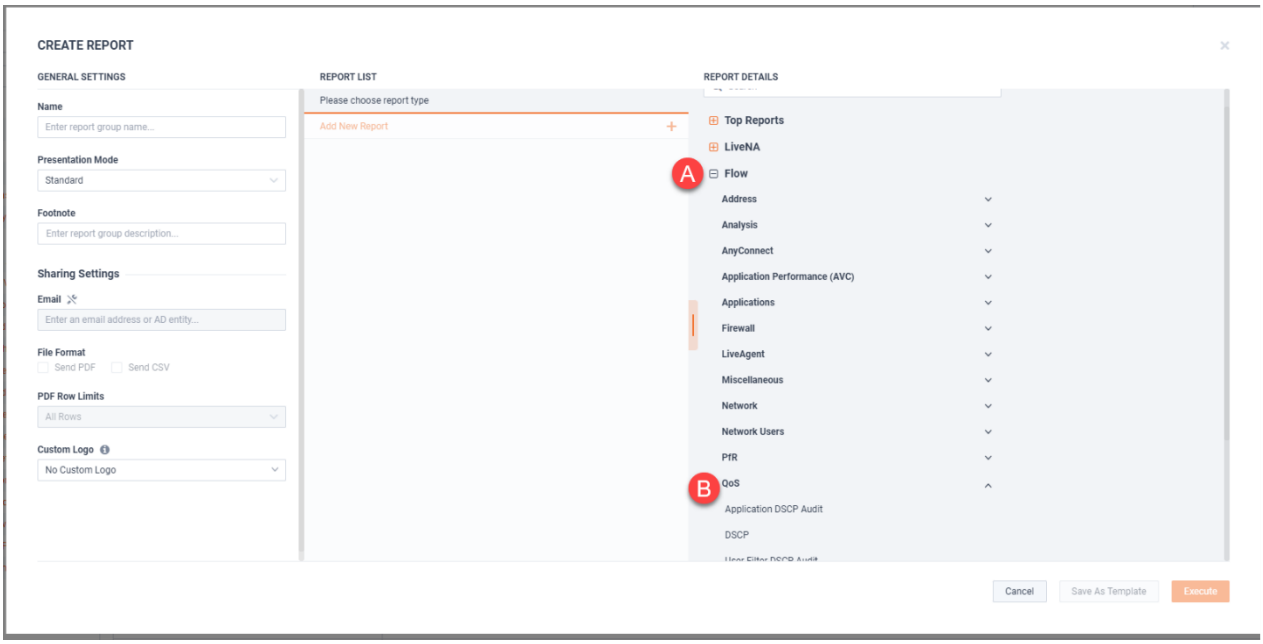
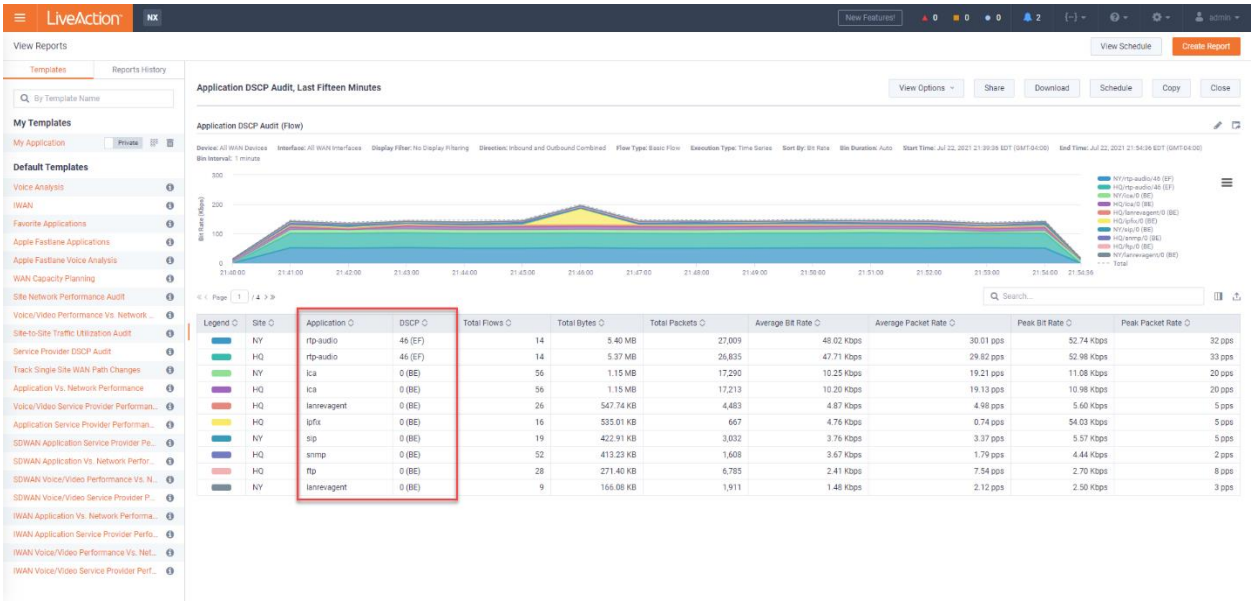


Figure 29

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

© Copyright LiveAction 2022



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

Figure 30

© Copyright LiveAction 2022

Lab 1.5: Enable / Customize Alerts

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

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

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

Lab Steps:

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

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

Figure 31

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

 © Copyright LiveAction 2022

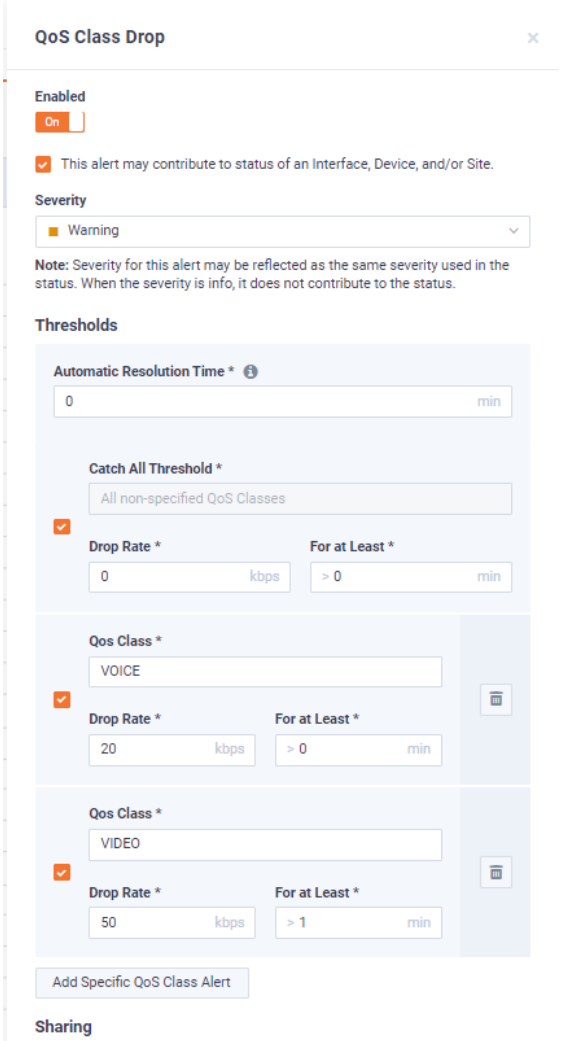


Figure 32

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.

 © Copyright LiveAction 2022

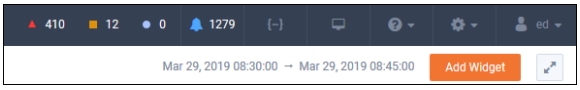


Figure 33

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

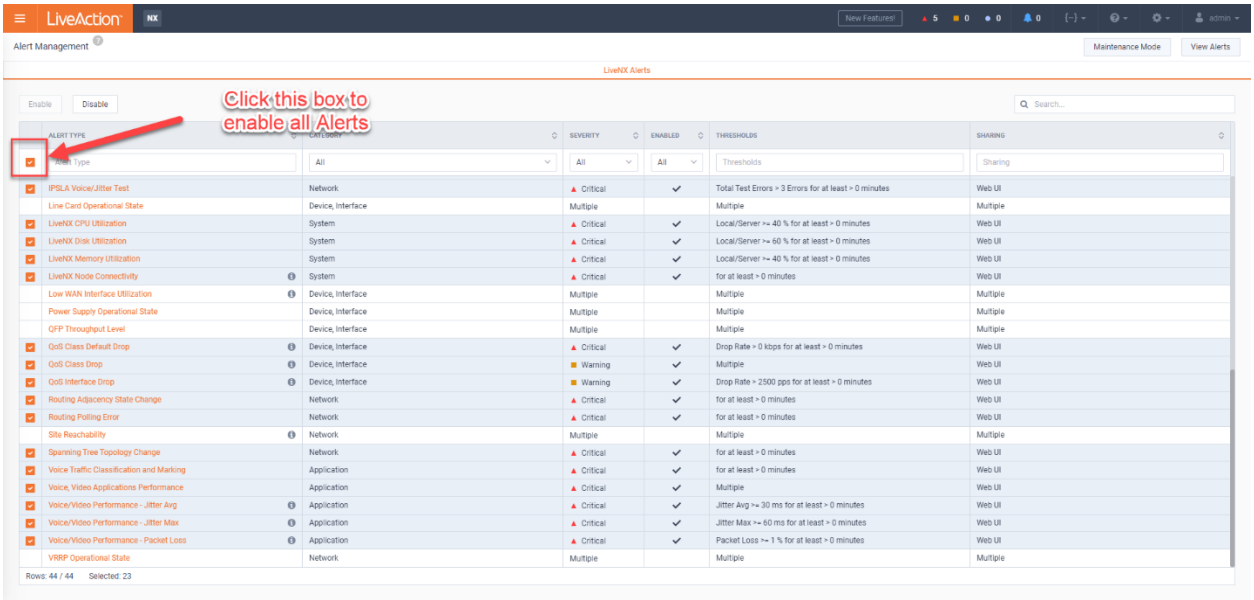


Figure 34

 © Copyright LiveAction 2022

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

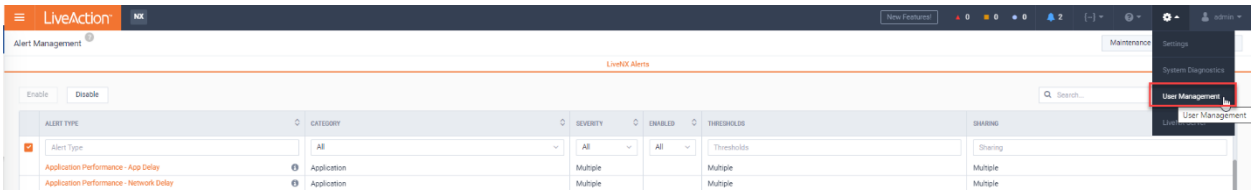


Figure 35

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

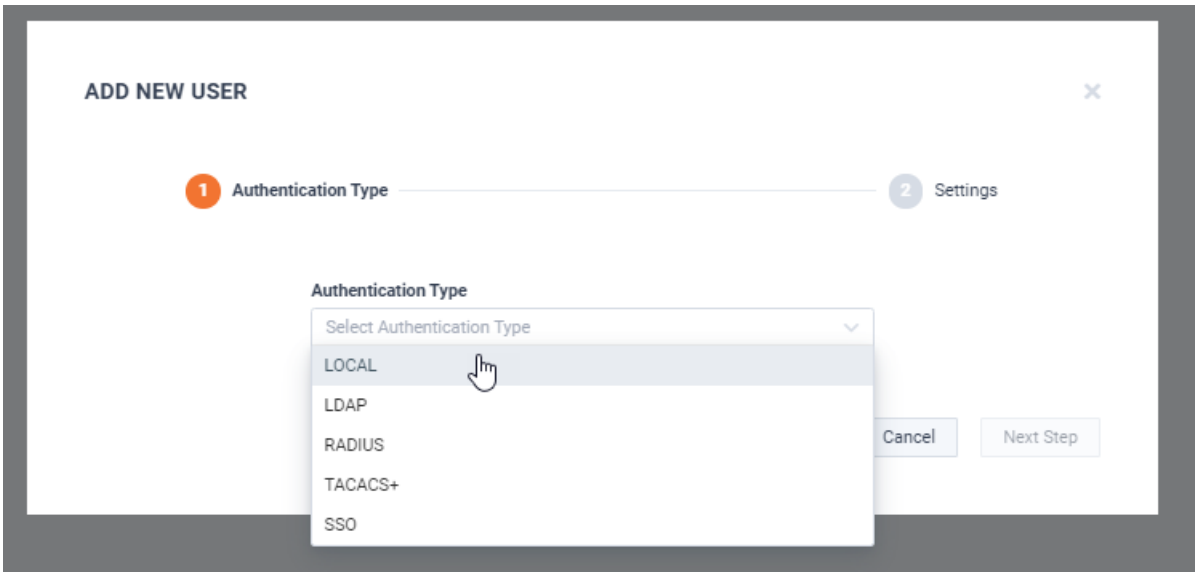


Figure 36

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.

 © Copyright LiveAction 2022

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.

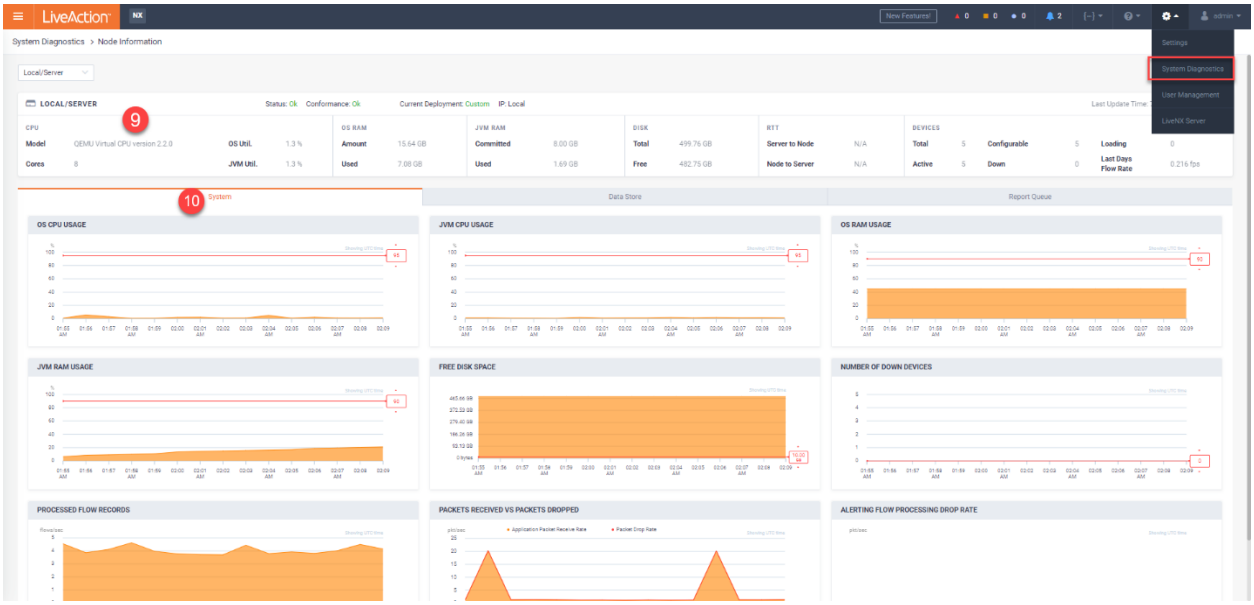


Figure 37

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.

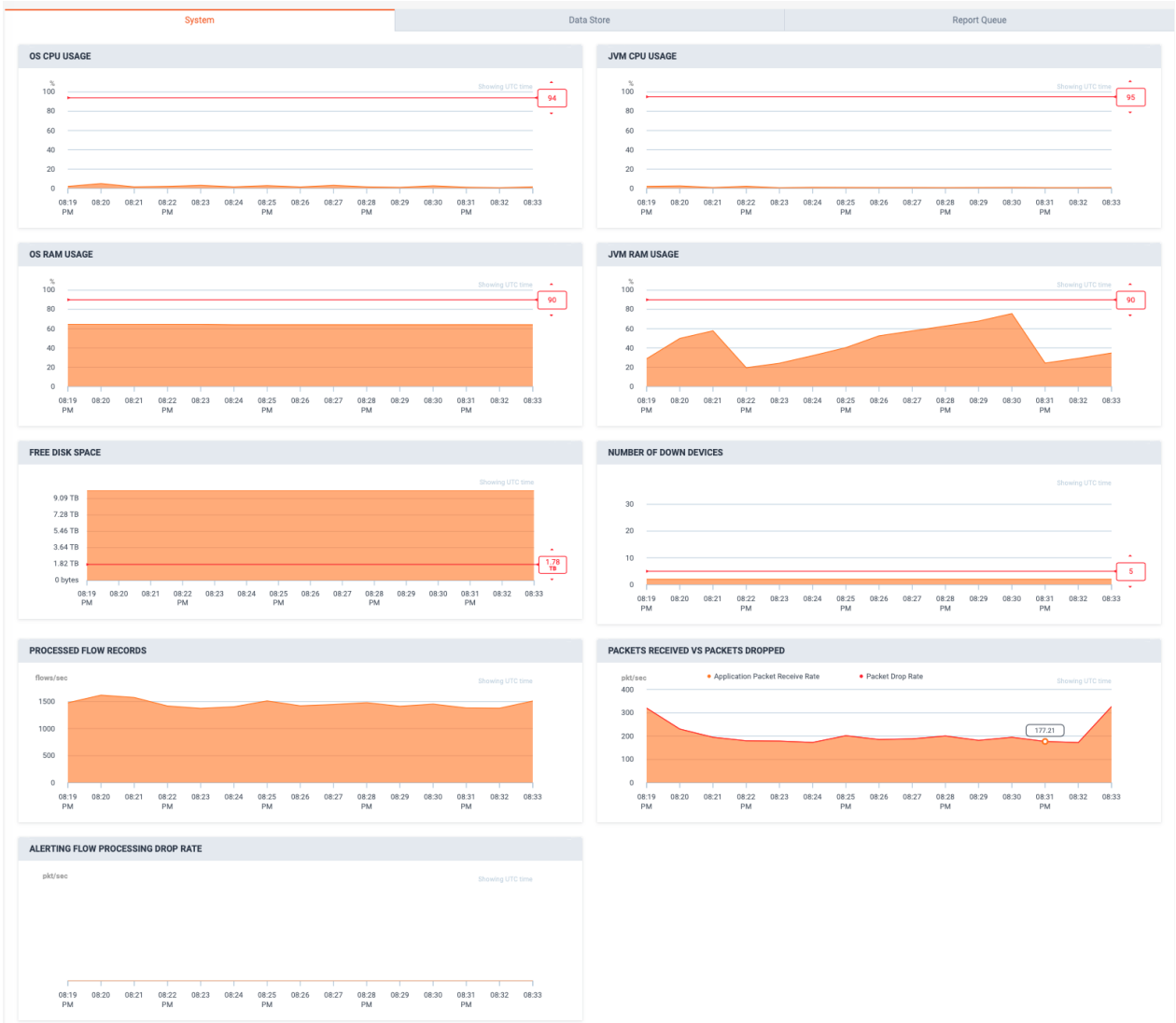


Figure 38

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

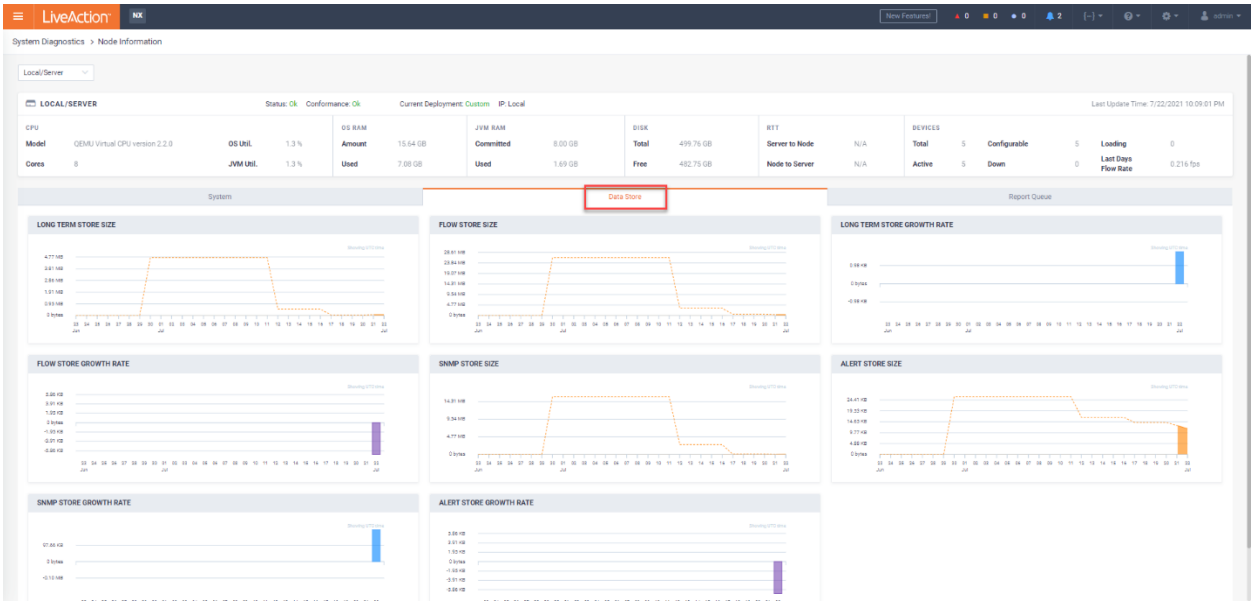


Figure 39

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

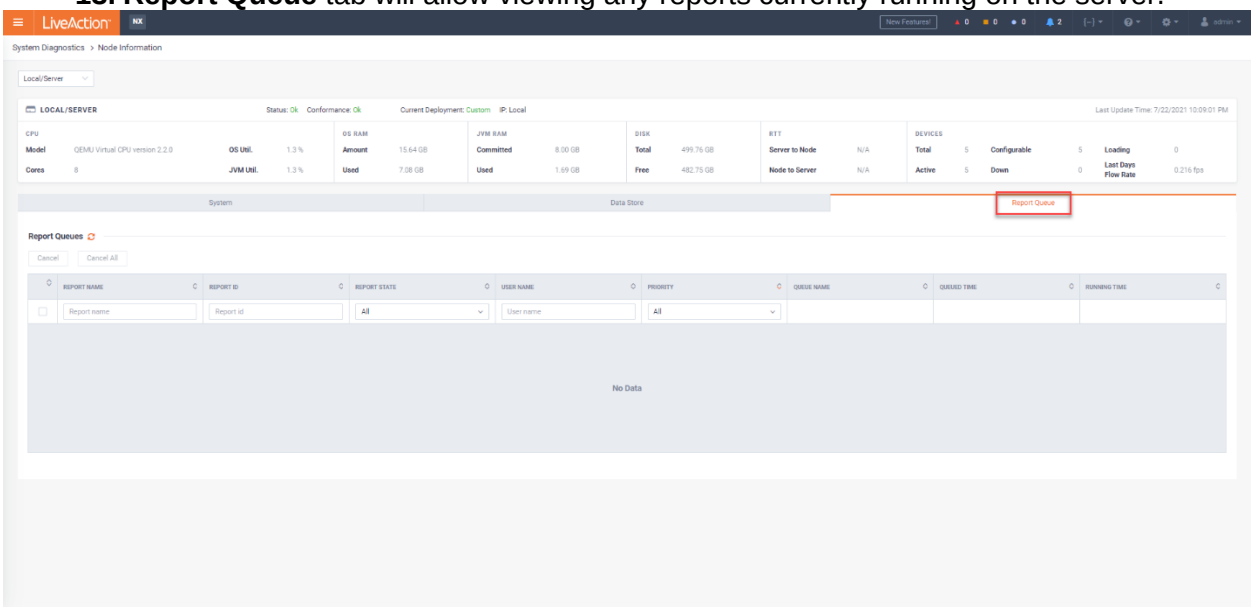


Figure 40

Lab 1.8: Support and Troubleshooting

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

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

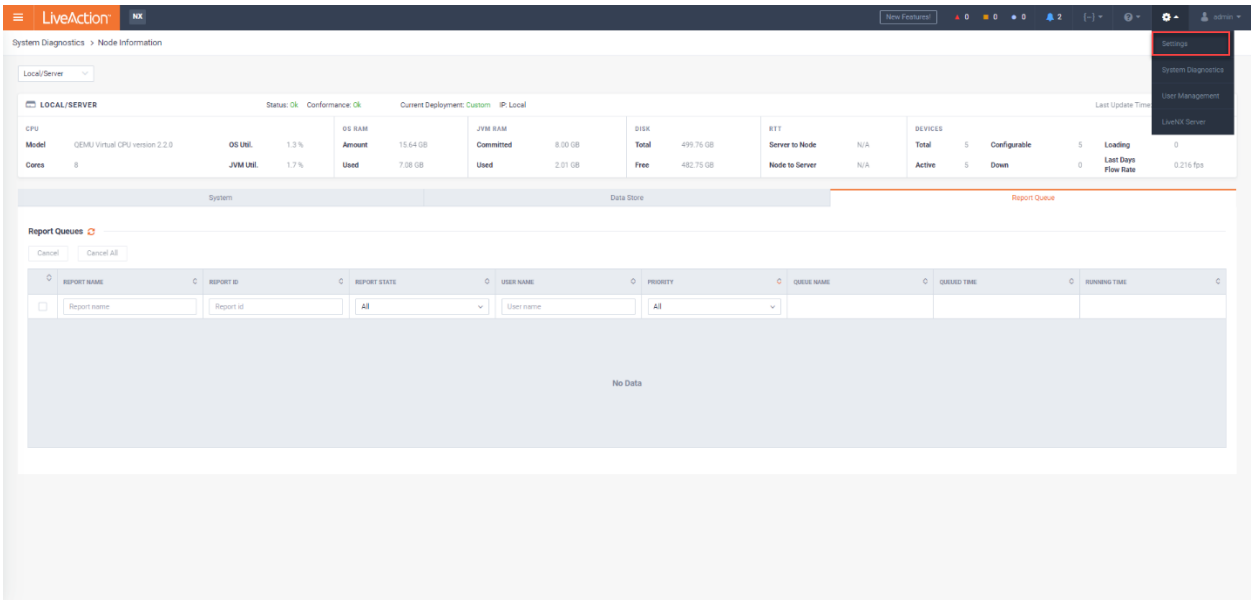


Figure 41

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

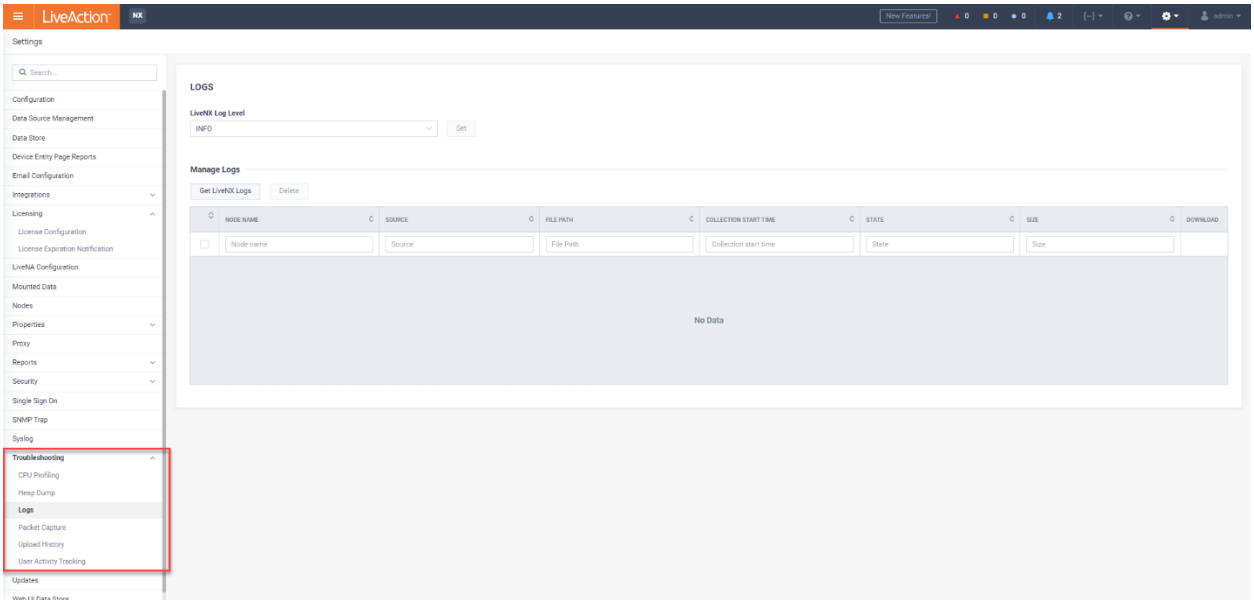


Figure 42

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**.

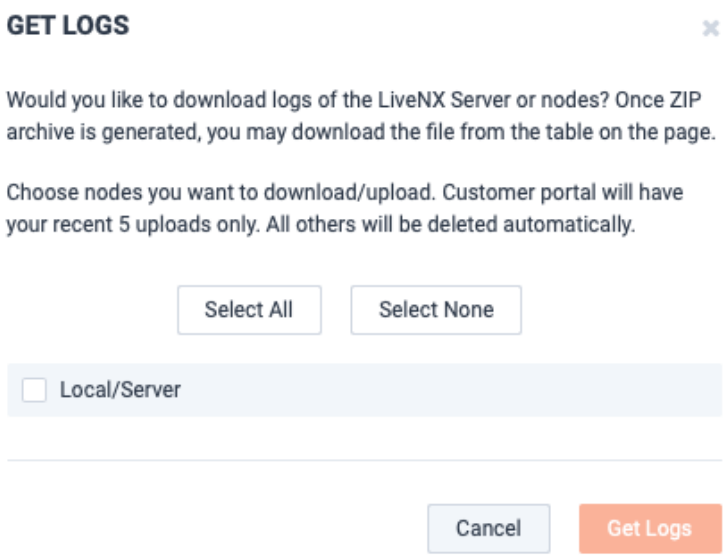


Figure 43

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

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

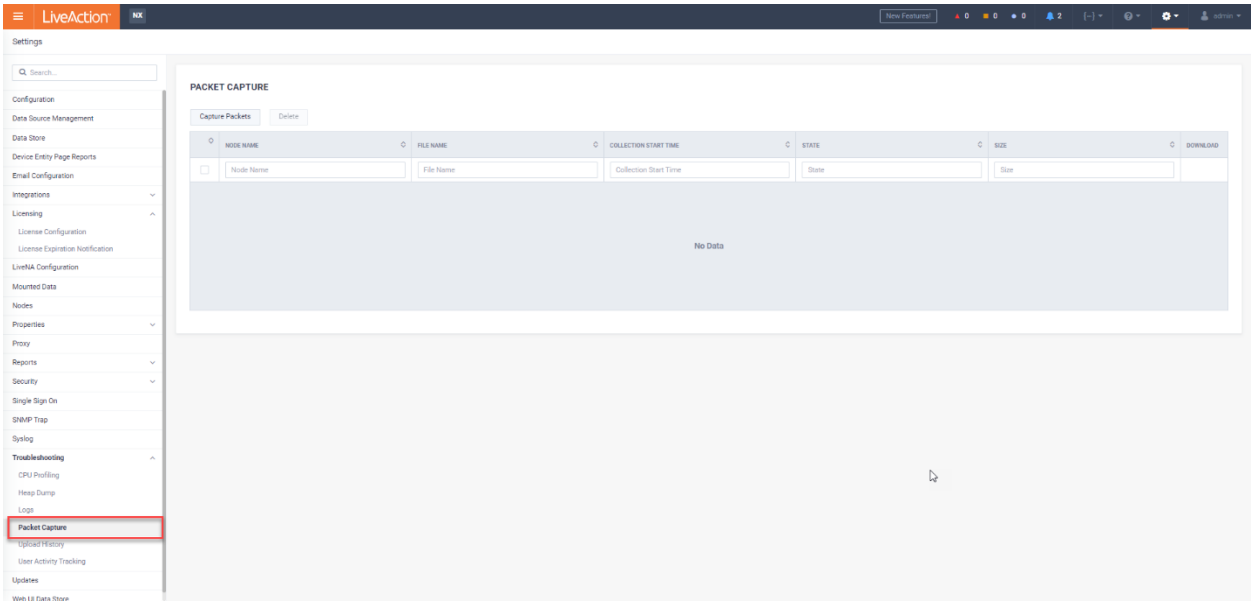


Figure 44

6. Click **Capture Packets.**

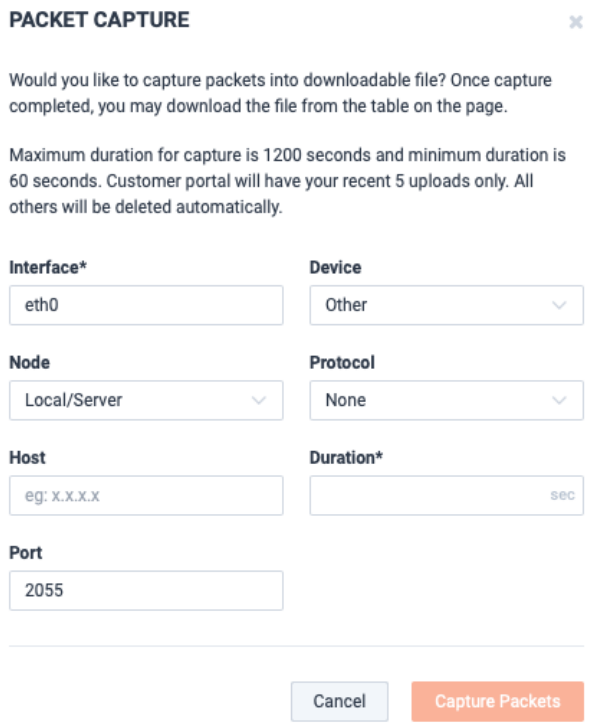


Figure 45

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

<u>These Labs uses the Engineering Console exclusively.</u>

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

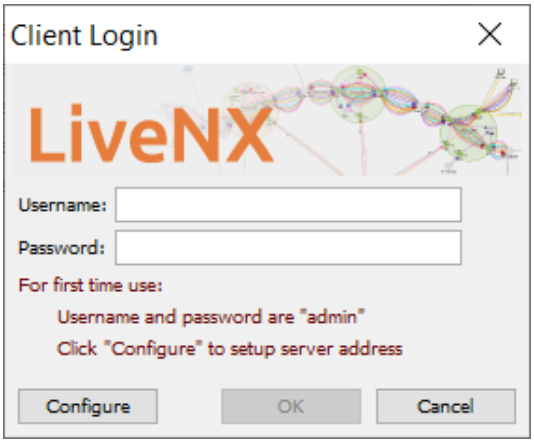


Figure 46

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

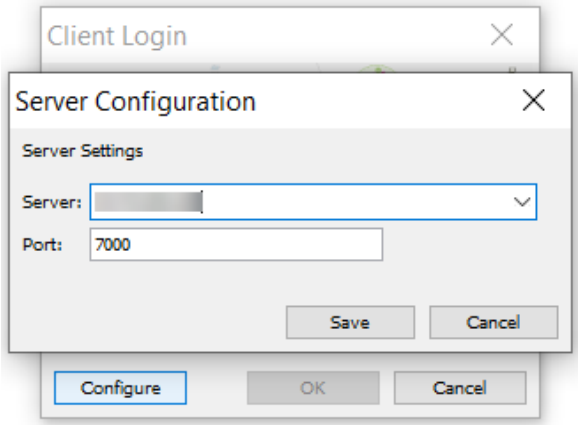


Figure 47

 © Copyright LiveAction 2022

4. **Click** Save
5. Enter the **Username** & **Password**.
   Username: admin
   Password: Student (note the capital S)

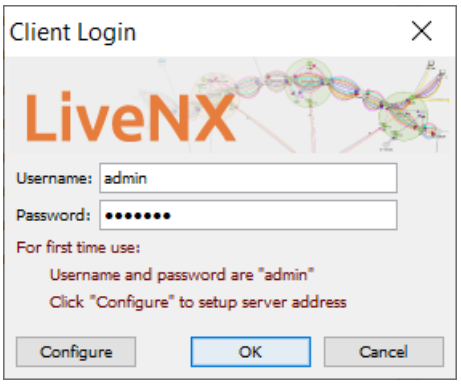


Figure 48

6. Click **OK**

The Client will launch…

Figure 49

… and will open showing the current configured Topology.

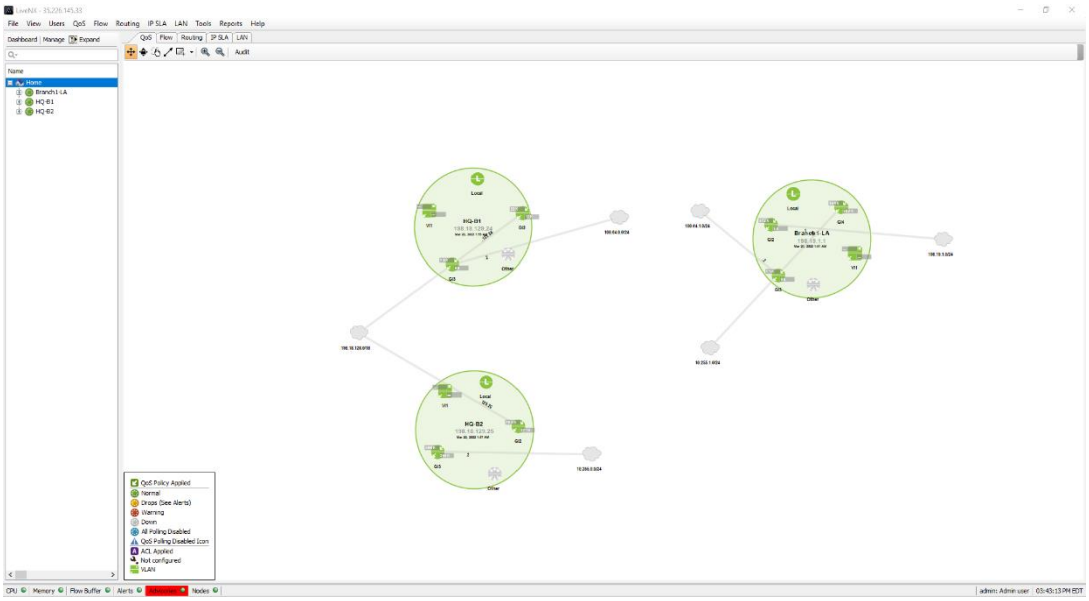


Figure 50

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

 © Copyright LiveAction 2022

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.

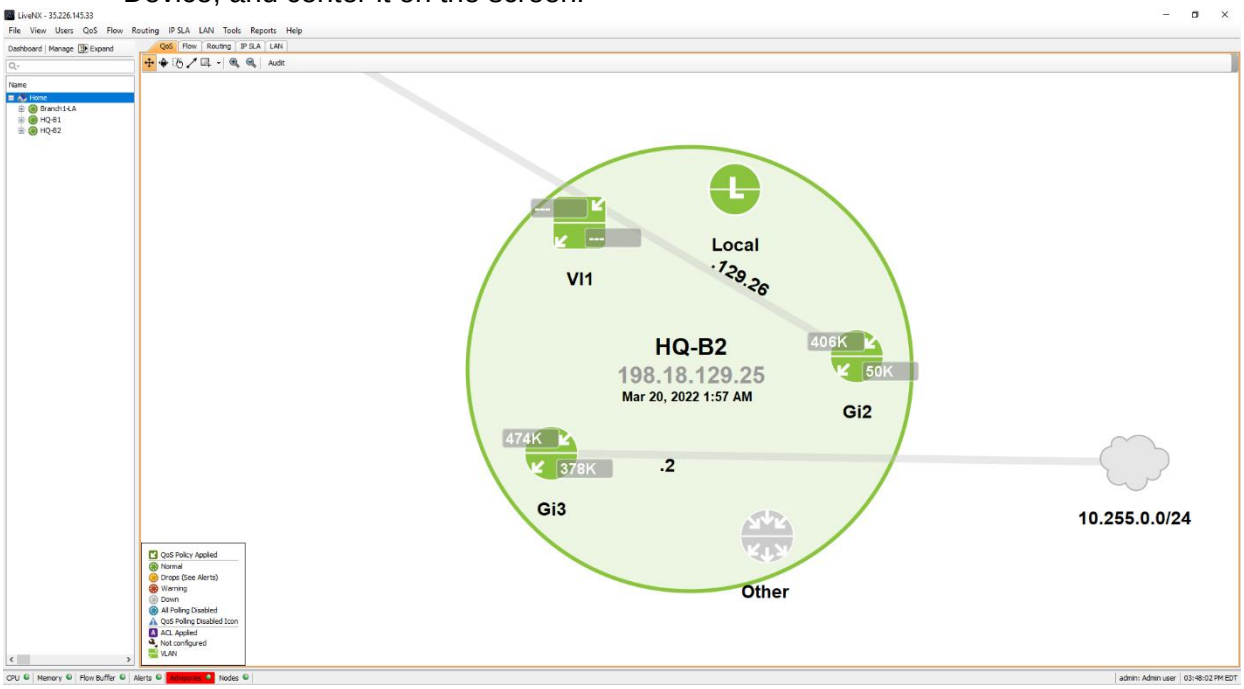


Figure 51

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.

 © Copyright LiveAction 2022

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

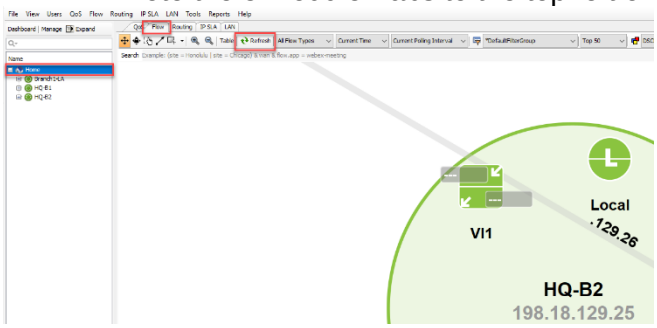


Figure 52

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

---

5. Click on **Flow** tab and then on **Refresh**. This will bring up all the flows that LiveNX is seeing from the router

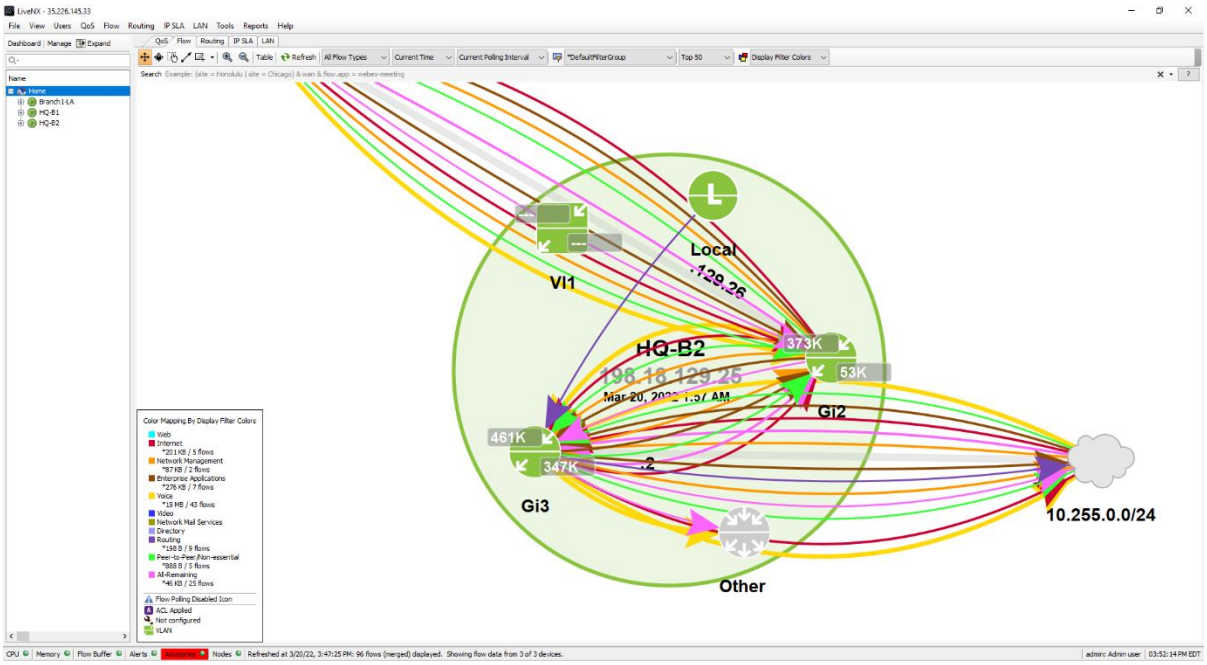


Figure 53

.

6. **Expand** the **HQ-B2** device in the **Home** Tree View.
7. Click on one of the interfaces… note how the information displayed in the Topology Pane changes.

 © Copyright LiveAction 2022

Figure 54

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!

 © Copyright LiveAction 2022

Lab 3

Lab 3: Configuring Devices

 © Copyright LiveAction 2022

Lab 3.1: Add Device

<u>This Lab uses the WebUI.</u>

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:

8. Login to the LiveNX WebUI
9. Select **Configure** > **Device Management**

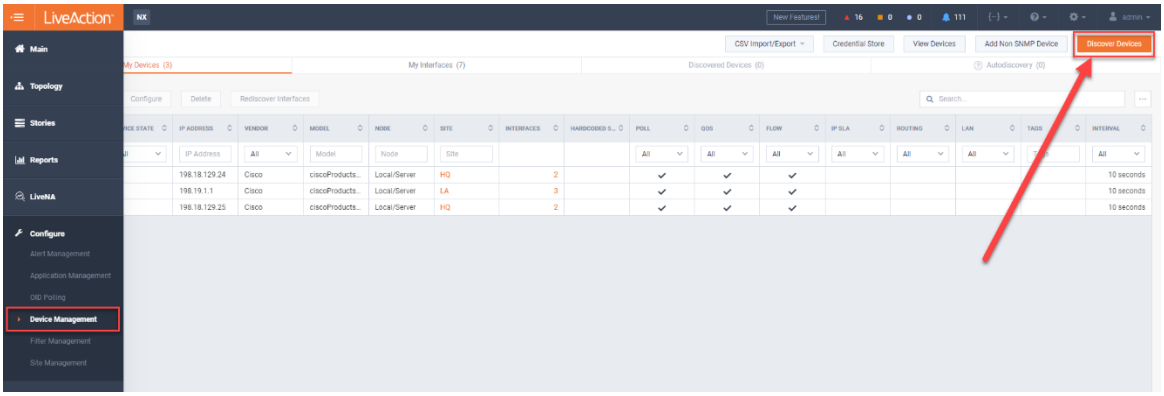


Figure 55

10. Click **Discover Devices**.

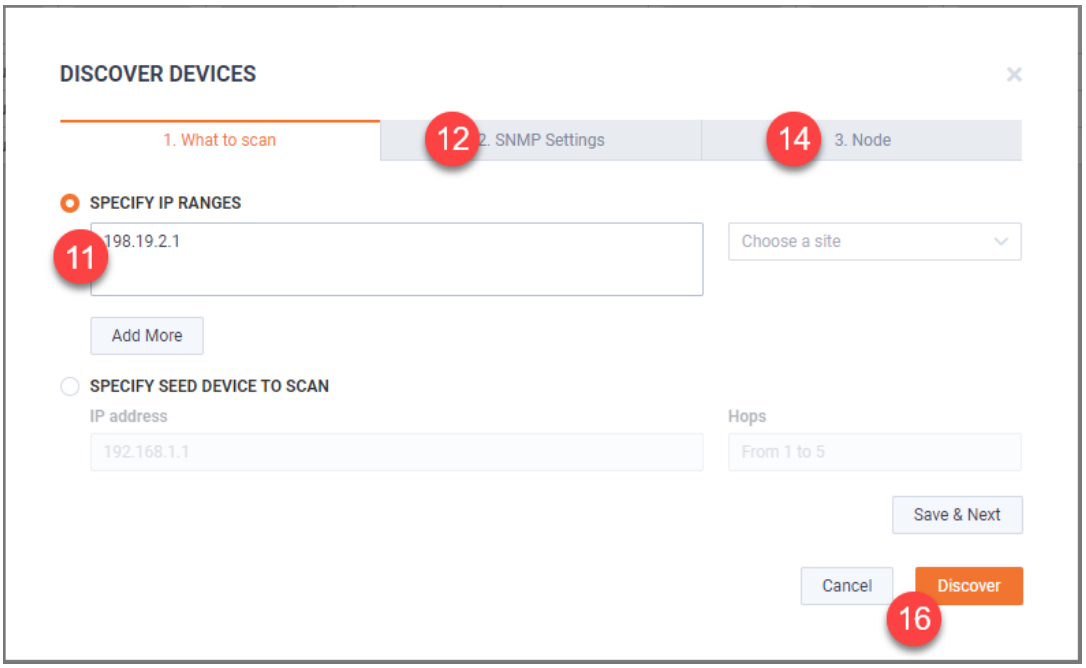


Figure 56

11. Enter **198.19.2.1**, in the IP Address field.
12. Select the **SNMP Settings** tab.
13. Click "**Default SNMP connection settings**".

 © Copyright LiveAction 2022

14. Select the **Node** tab.
15. Select **Local/Server**.
16. Click **Discover**.

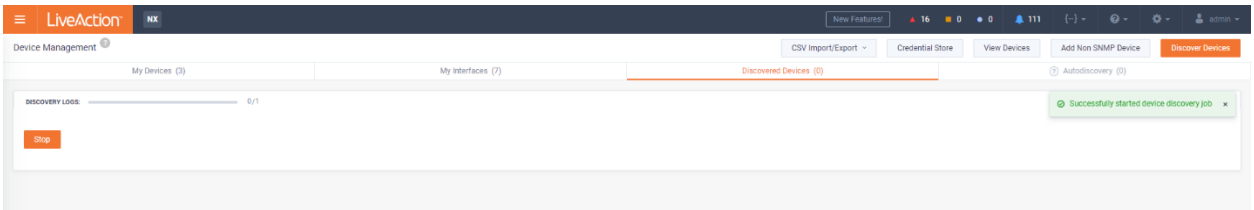
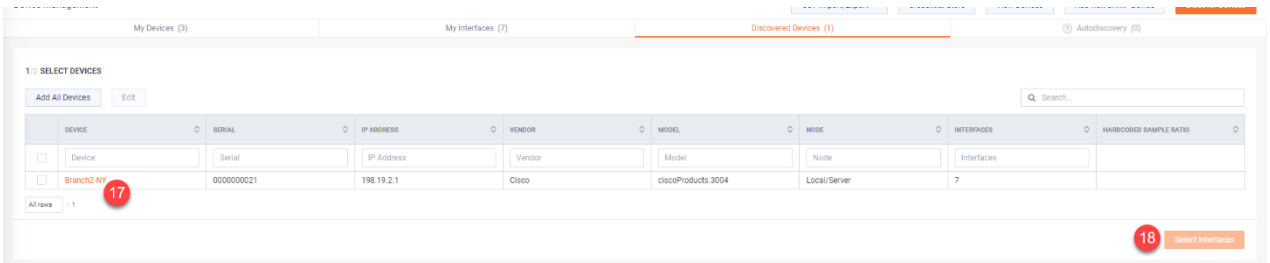


Figure 57

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.



17. Tick the box next to **Branch2-NY**.
18. Click **Select Interfaces**.

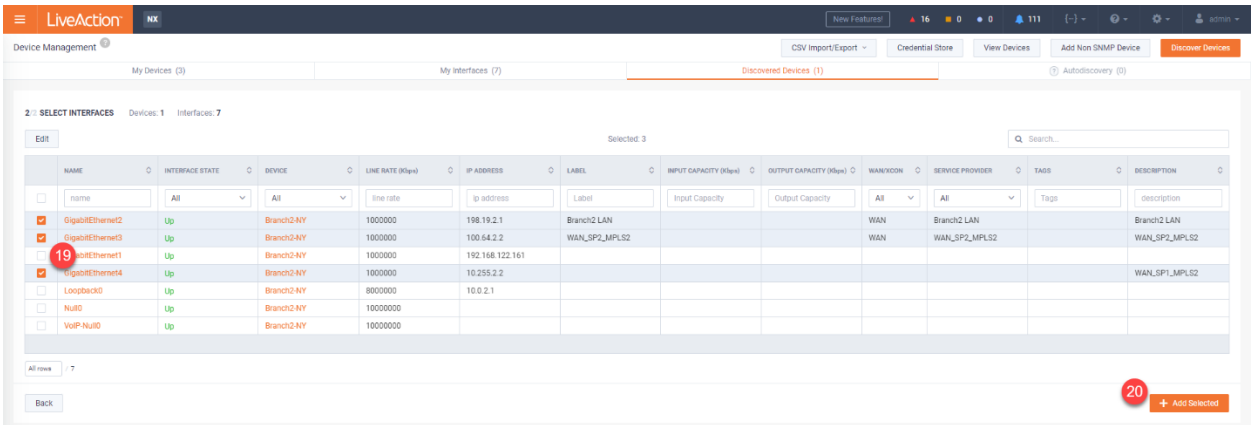


Figure 58

19. Select **GigabitEthernet2**, **GigabitEthernet3** & **GigabitEthernet4**.
20. 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.

 © Copyright LiveAction 2022

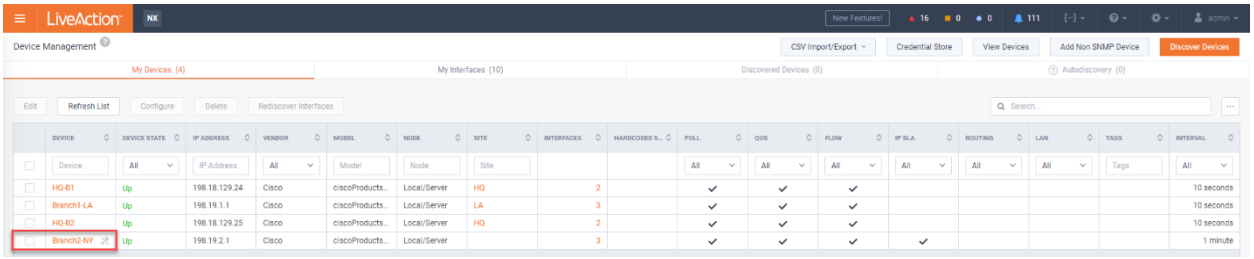


Figure 59

21. In the **Devices** Tab, click on the newly added **Branch2-NY** device. This will bring up the configuration page.

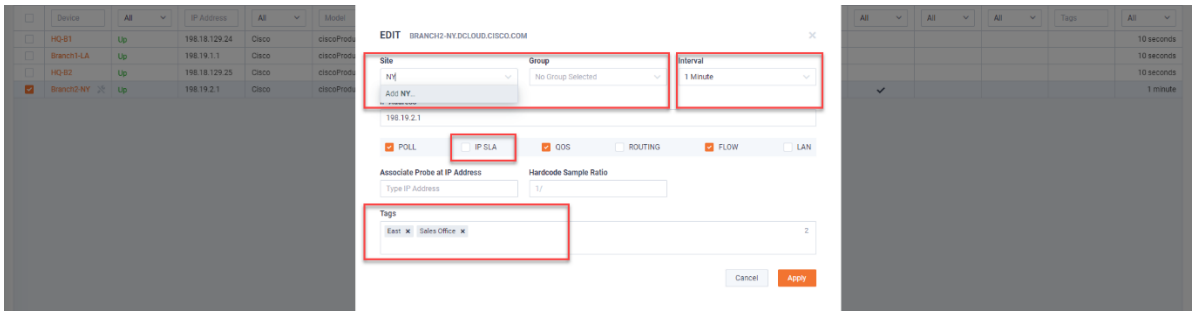


Figure 60

22. In the **Site** box, click and type **NY** assign the device to the site NY and do the same for **Group** (We will meet **Groups** in the Engineering Console).
23. Set the polling **Interval** to 10 seconds
24. Uncheck the **IPSLA** check box (this is not covered in this course)
25. Add **Tags** into the Tag box. Use something creative and descriptive for this site. We have used **East**, **Sales Office**, and **Branch**.

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.

26. Next we must give the site some additional information to ensure our reporting and monitoring work correctly. We must define the **Site** geographically. To do this, go to **Site Management** from the **Main Menu**.

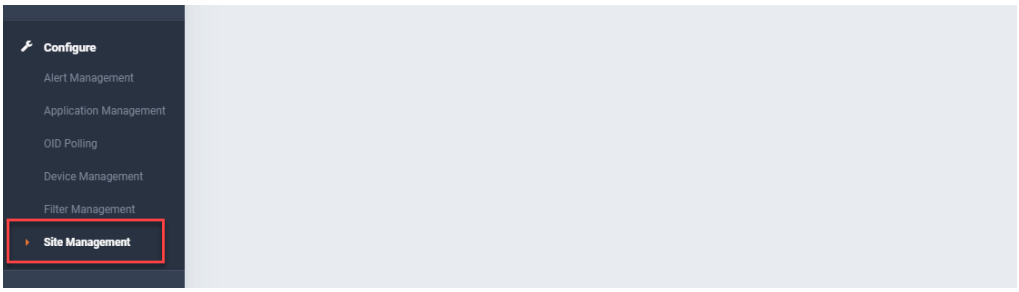


Figure 61

27. You will notice that NY does not have some of its **Site Semantic Info**. Here we can add what's missing.

 © Copyright LiveAction 2022

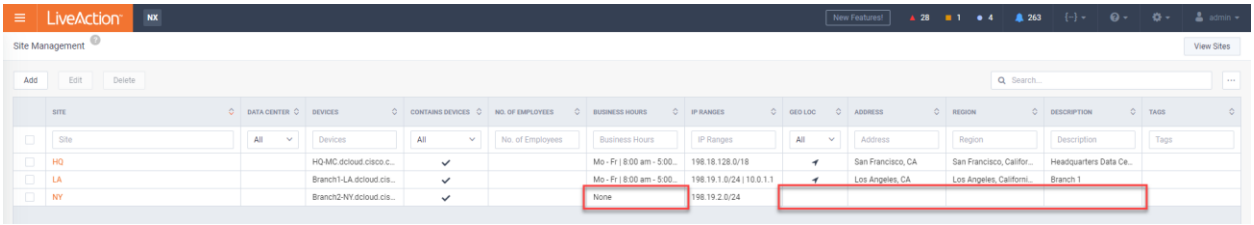


Figure 62

28. To open the **Site Configuration** pop-up, click on **NY** in the left column.

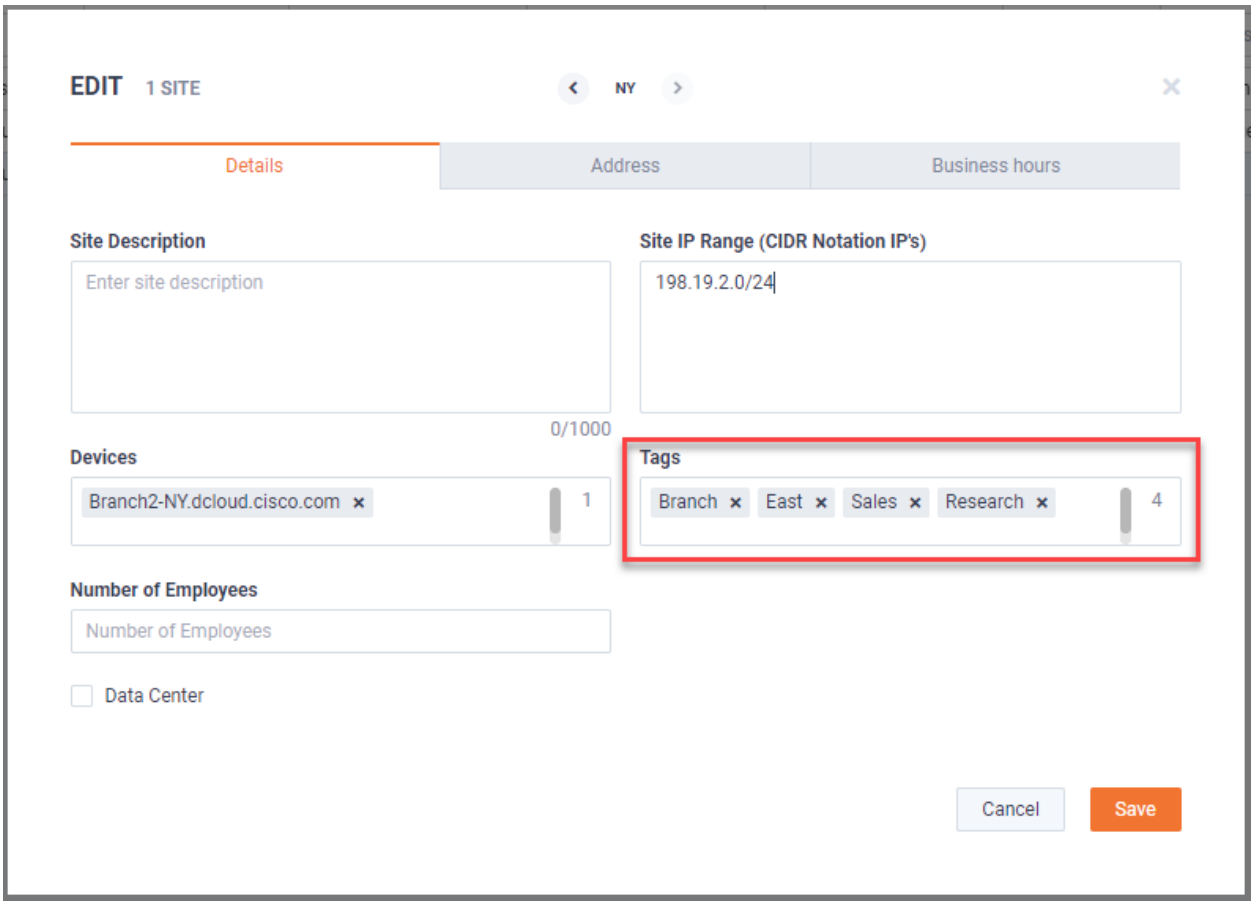


Figure 63

29. In the Tags box, enter **East**, **Branch**, and any others you want to add. We've added **Sales** and **Research.**

 © Copyright LiveAction 2022

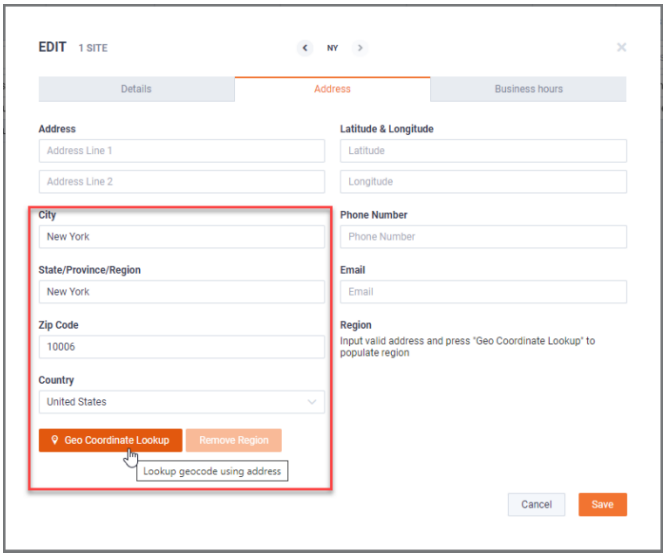


Figure 64

30. Enter some information in the City/State/Zip Code/Country fields (We have used zip code 10006 for central New York City). Then, click on the **Geo Coordinate Lookup**.

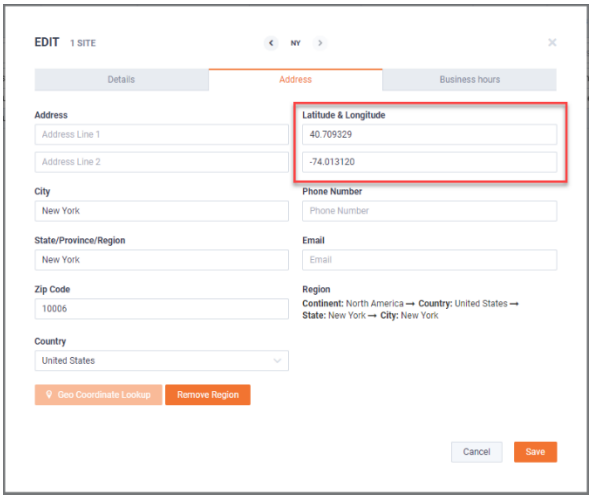


Figure 65

31. This calculates the position (as accurately as possible – if you put a street address too it improves the accuracy) and enters that information in the **Longitude** and **Latitude** cells. This is used to place the site on the **Geo Topology Map**.

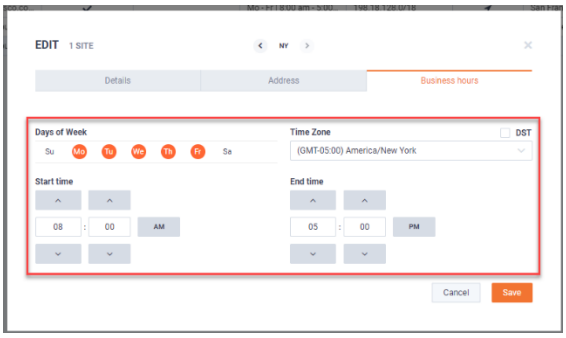


Figure 66

32. Next, click on the **Business Hours** tab, and complete the days of the week, and typical start and end times of people's workday. This is used on the **WAN Capacity Planning** and **WAN Utilization** calculations.

 © Copyright LiveAction 2022

33. Then Click **Save**.

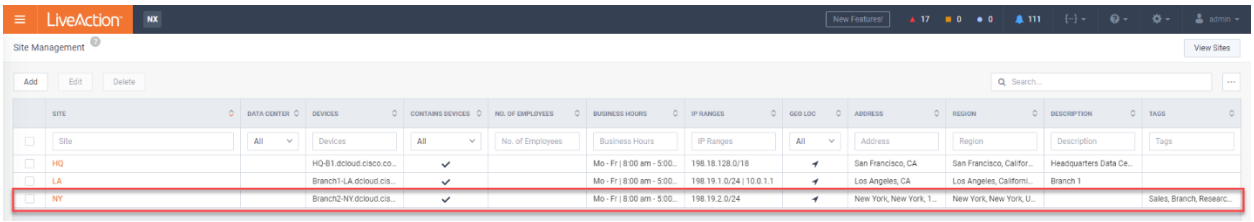


Figure 67

34. You'll see the table now completed with the new information for the Site New York. (Note, if you added information in the **Description** box, you would see that here too.

 © Copyright LiveAction 2022

Lab 3.2: Manage & Configure Devices

<u>This Lab uses the Engineering Console.</u>

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:

35. Login to the LiveNX Client.
36. Right-click on **Home** and **Expand All.**
37. The **NY** site now appears as we configured it from the WebUI. In the Engineering Console this is referred to as a **Group**. To use **Sites** in the WebUI and **Groups** in the Engineering Console you must configure both.

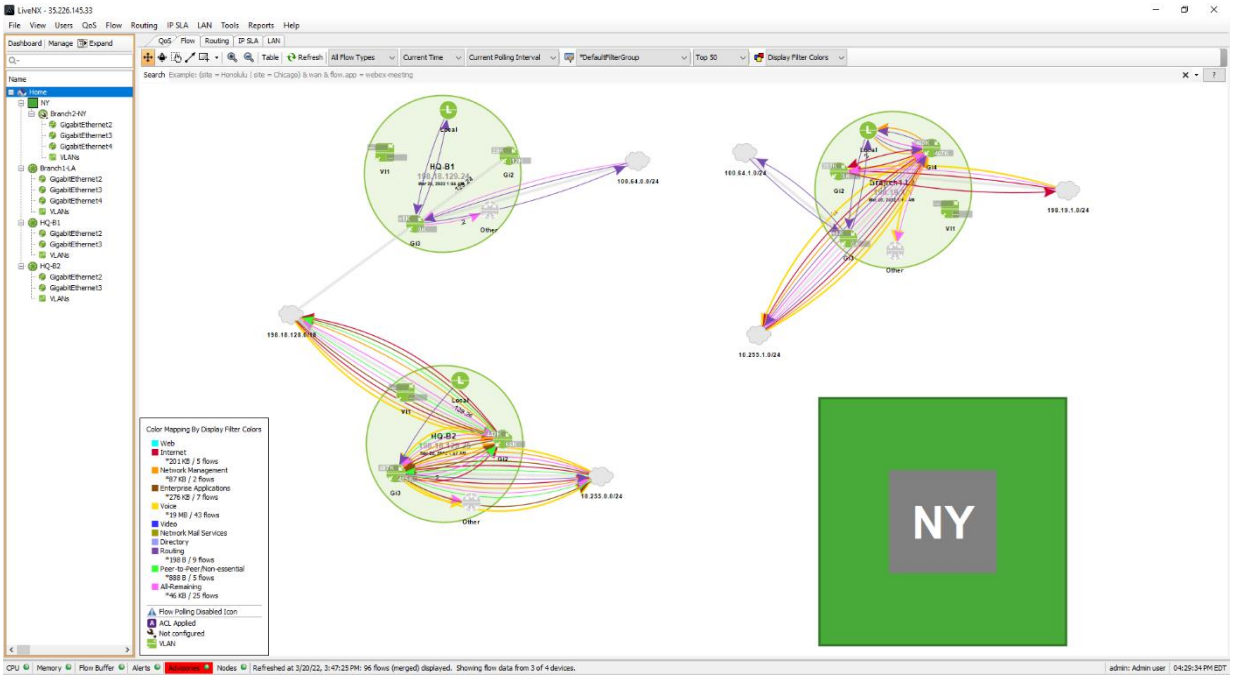


Figure 68

Double click on the **NY** Group to expand it, then right click on white space to reveal the **View Options** dialog, hover over **View**, and select **Fit to View**.

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, indicated by the wrench image.

---

38. Click **Manage** (Above the Home Tree). A **Device Management** dialogue will open.
39. Select only **Branch2-NY**

 © Copyright LiveAction 2022

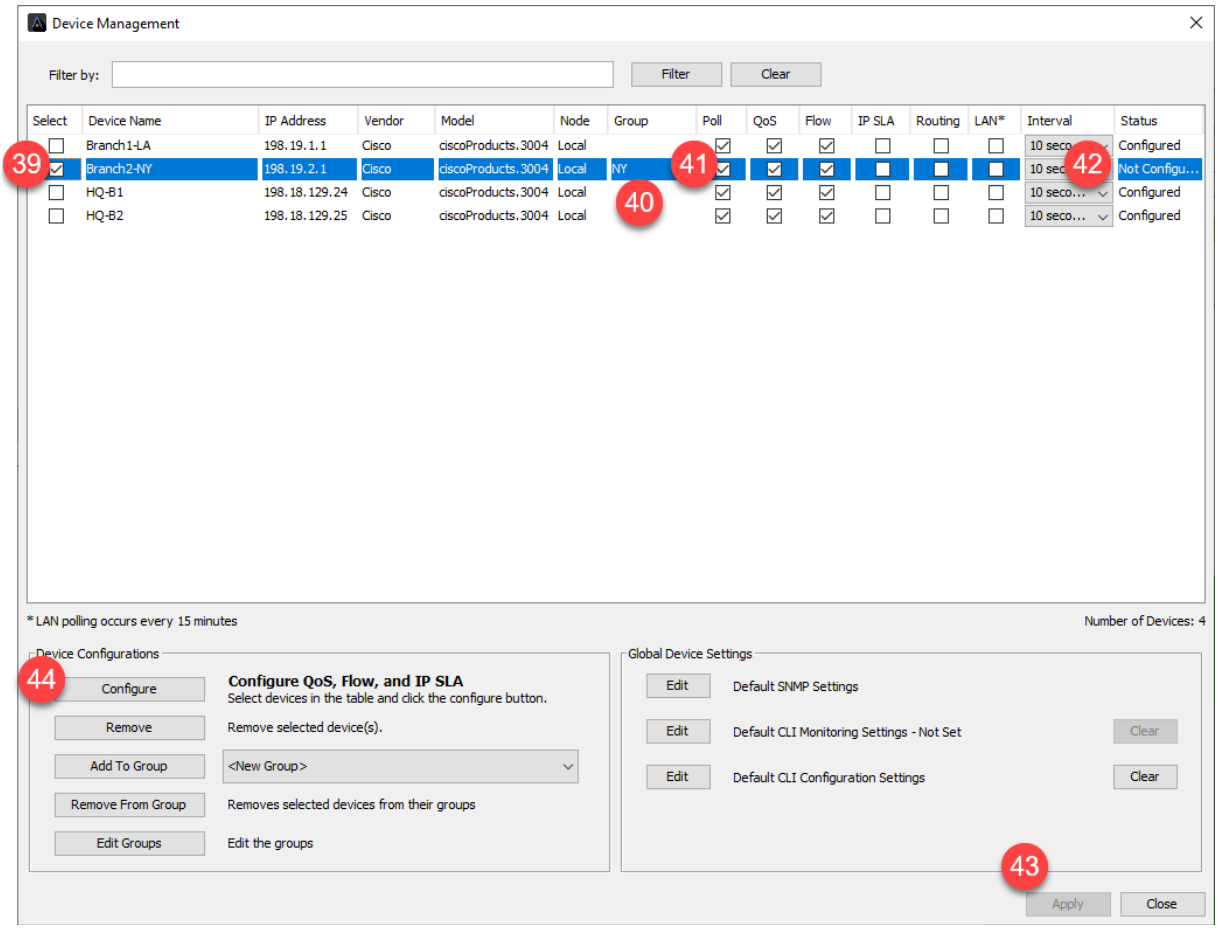


Figure 69

40. Here you will see the Group that we have already created for our new device.
41. Check ONLY **Poll, QoS** and **Flow**.
42. Verify the Interval on the device is **10 seconds**.
43. Click **Apply**.
44. Click **Configure**.

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

45. Step1: Use the **Default SNMP**… Click Next
46. Step2: Use **My Default Configuration CLI**… Click Next

 © Copyright LiveAction 2022

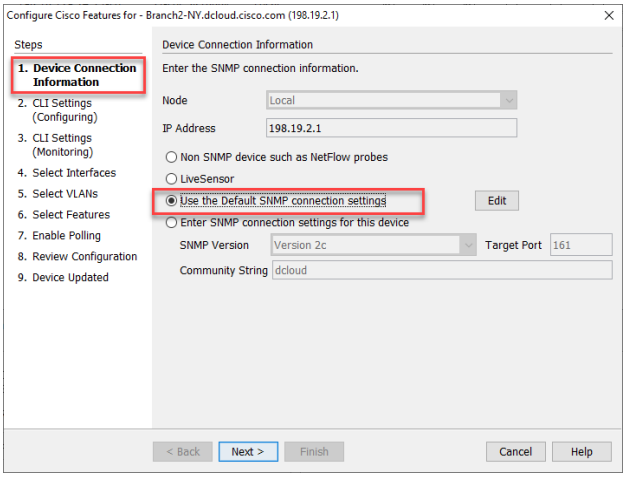


Figure 70

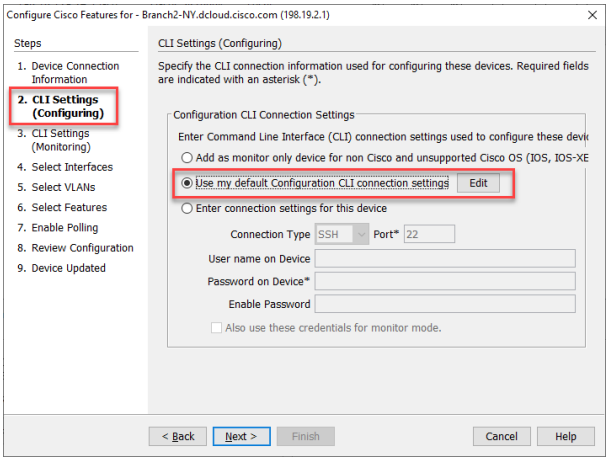


Figure 71

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

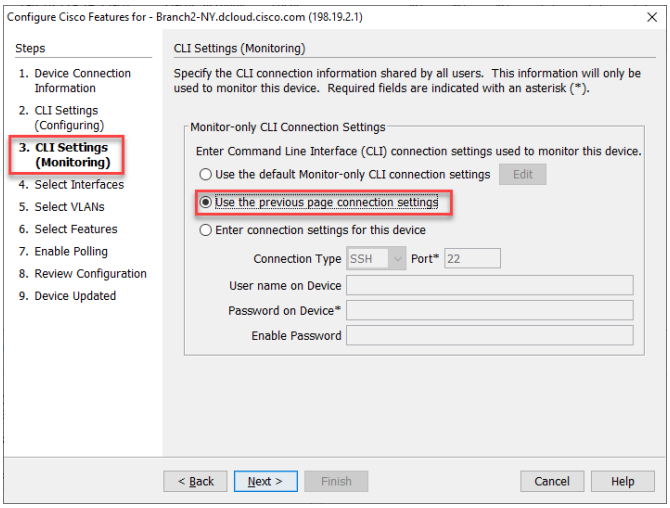


Figure 72

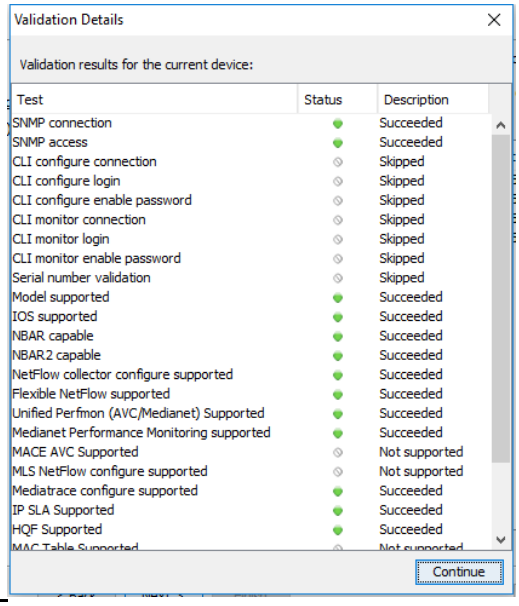


Figure 73

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.

48. Step 5: Ensure the correct interfaces are selected…**GigabitEthernet2, Gigabit Ethernet3, and GigabitEthernet4.** Click **Next**
    a. You can include Loopback, but not necessary. The point is to understand you can choose both logical and physical interfaces.

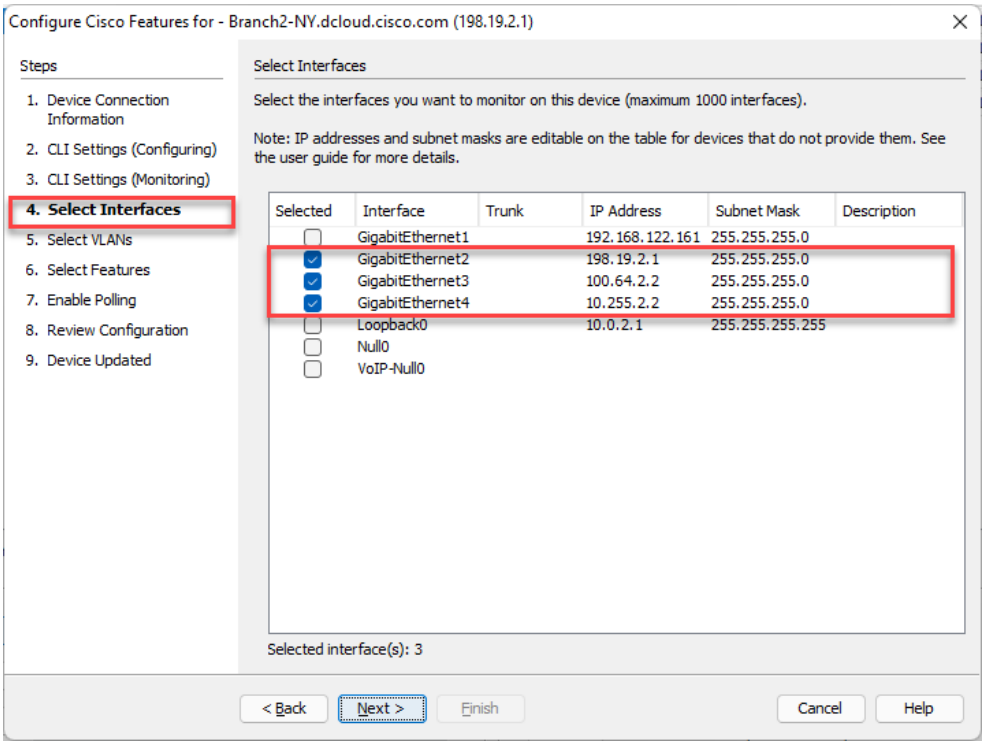


Figure 74

49. Step 5: Since there are no active VLANs configured on this exercise, skip past this option if one is shown. You may monitor up to 25 configured VLANs on each device. Click **Next.**

50. 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 **GigabitEthernet3** and **GigabitEthernet4 (WAN interfaces only)**. Click **Next**.

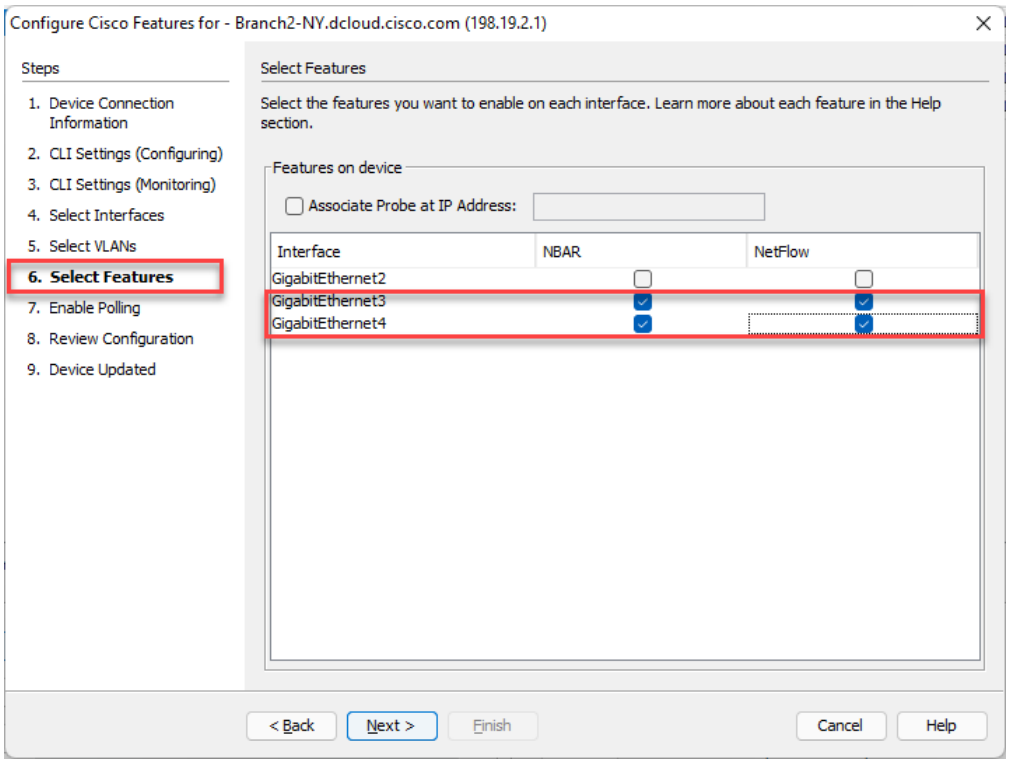


Figure 75

51. Step 7: Verify **Polling** is set for **10 Seconds** and ensure **Flows** and **QoS** are selected. These should be selected from our previous work for the NY Branch Router.

52. Click Continue

 © Copyright LiveAction 2022

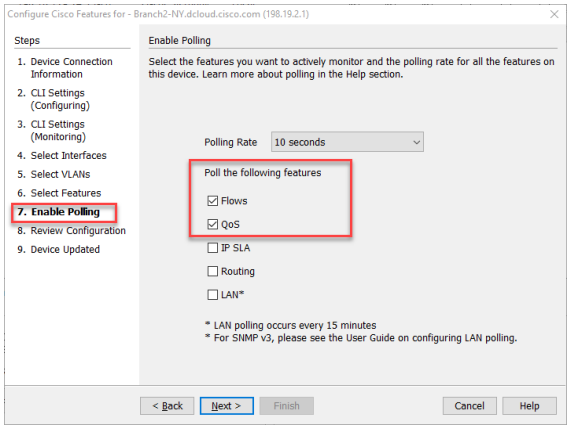


Figure 76

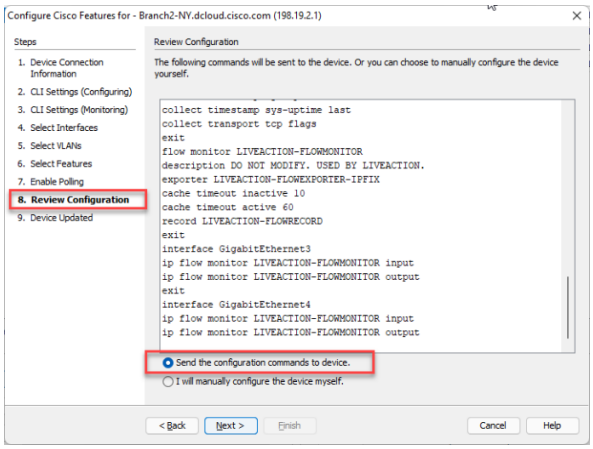


Figure 77

53. 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 can send the config instructions if you wish.
54. Click **Next**. Wait for the configuration process to finish.
55. Click **Finish**.

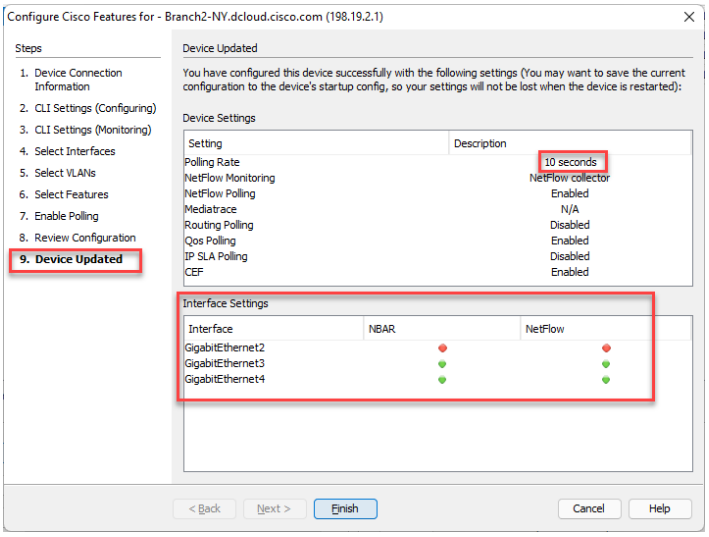


Figure 78

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

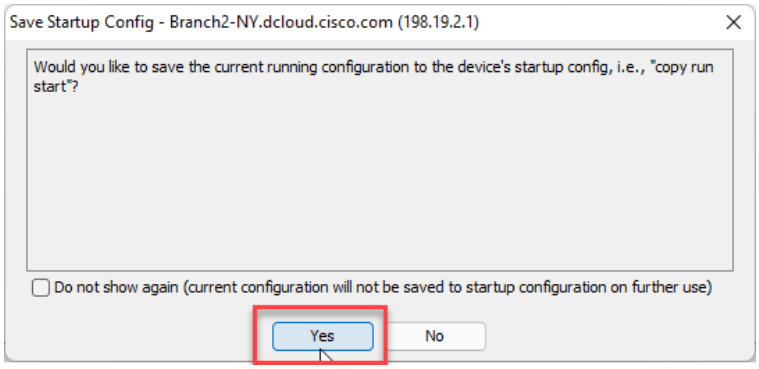


Figure 79

57. You will be prompted to save the current config to the startup config. For our exercise click **Yes**.

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.

58. Click **Close** to close the dialog box.

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.

 © Copyright LiveAction 2022

Lab 3.3: Configure Flow on Devices

<u>This Lab uses the Engineering Console.</u>

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

Lab Steps:

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

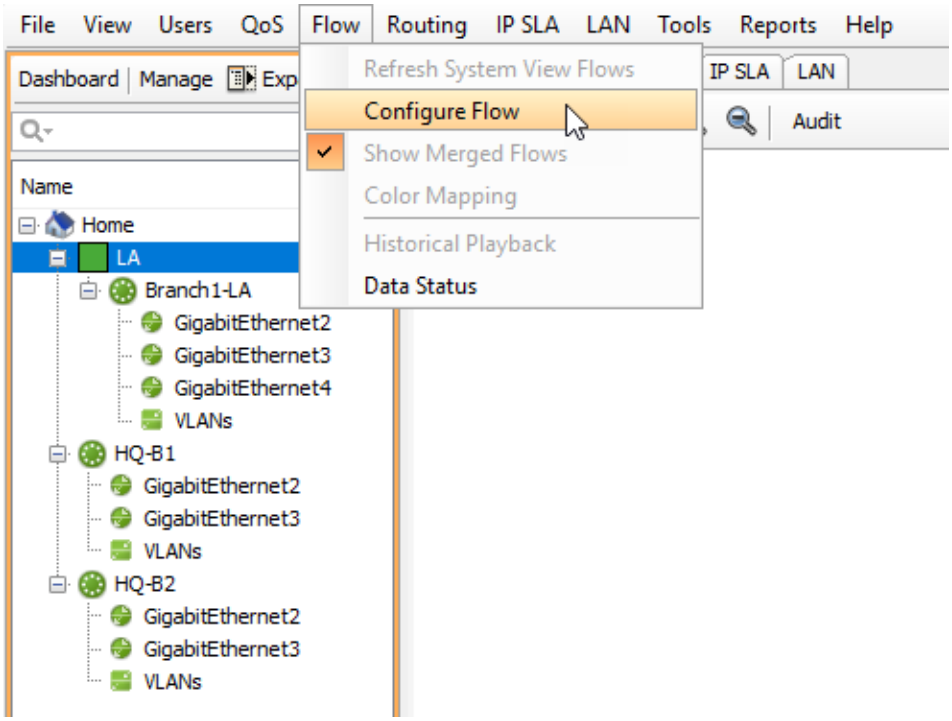


Figure 80

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

 © Copyright LiveAction 2022

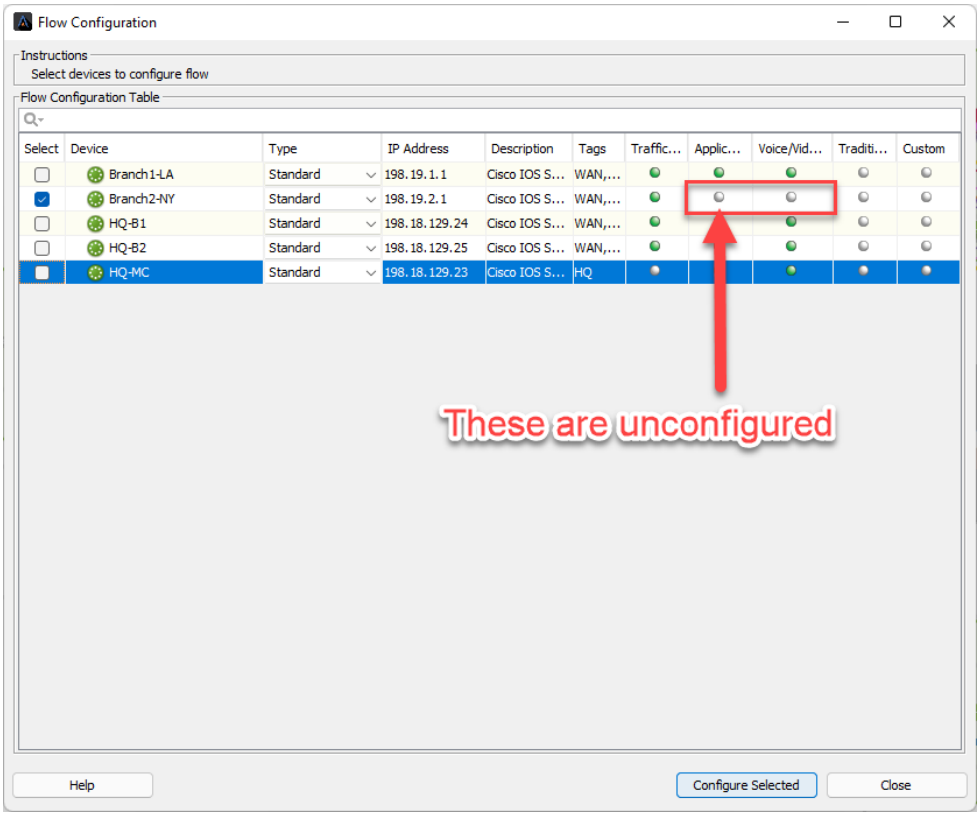


Figure 81

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 see in your Training Pod.

61. **Select** Traffic Statistics (FNF), Application Performance (AVC), and Voice/Video (Medianet) on **Branch2-NY** interfaces **GigabitEthernet2**, **GigabitEthernet3** and **GigabitEthernet4**.

Note: Semantics are important. Note that we have a WAN interface tag on a LAN interface – GigabitEthernet2. This needs to be corrected later..

 © Copyright LiveAction 2022

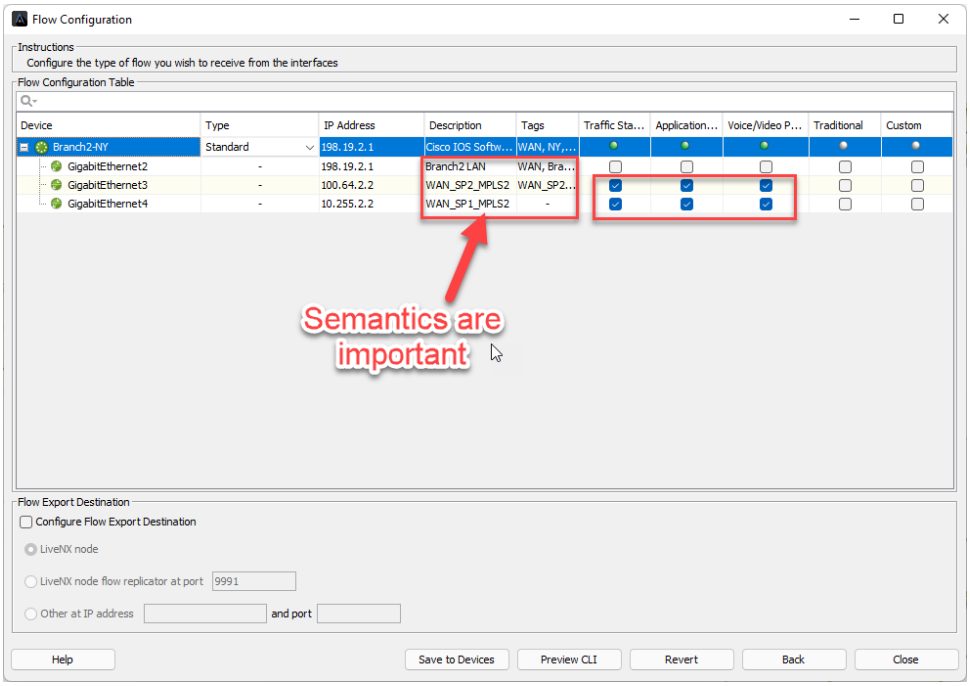
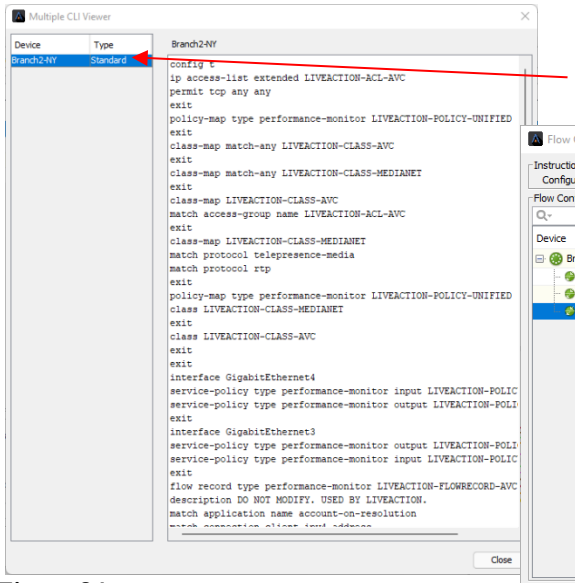


Figure 82

62. **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.

Figure 84

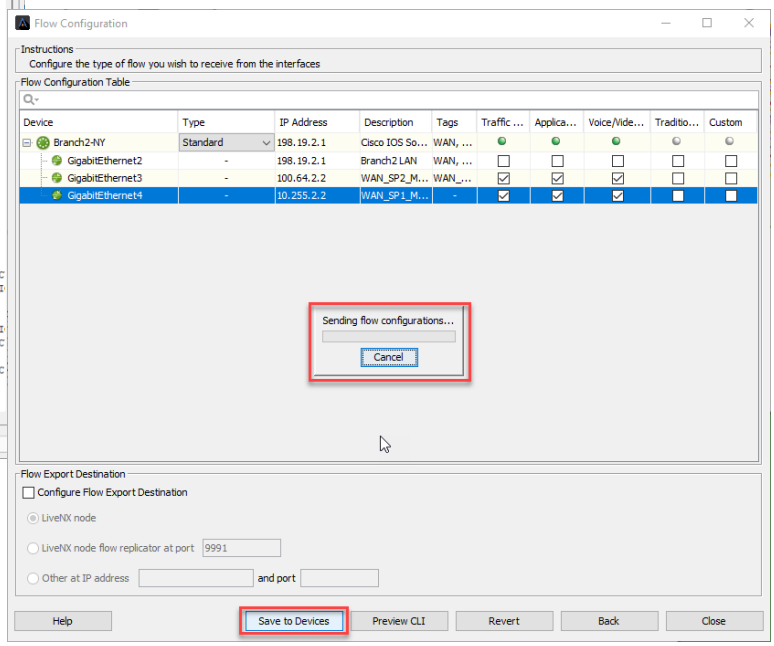


Figure 834

63. Click **Close**.
64. Click **Save to Devices**.
65. Again, **save the current running config to the startup config**.
66. Click **Close**.

 © Copyright LiveAction 2022

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!

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

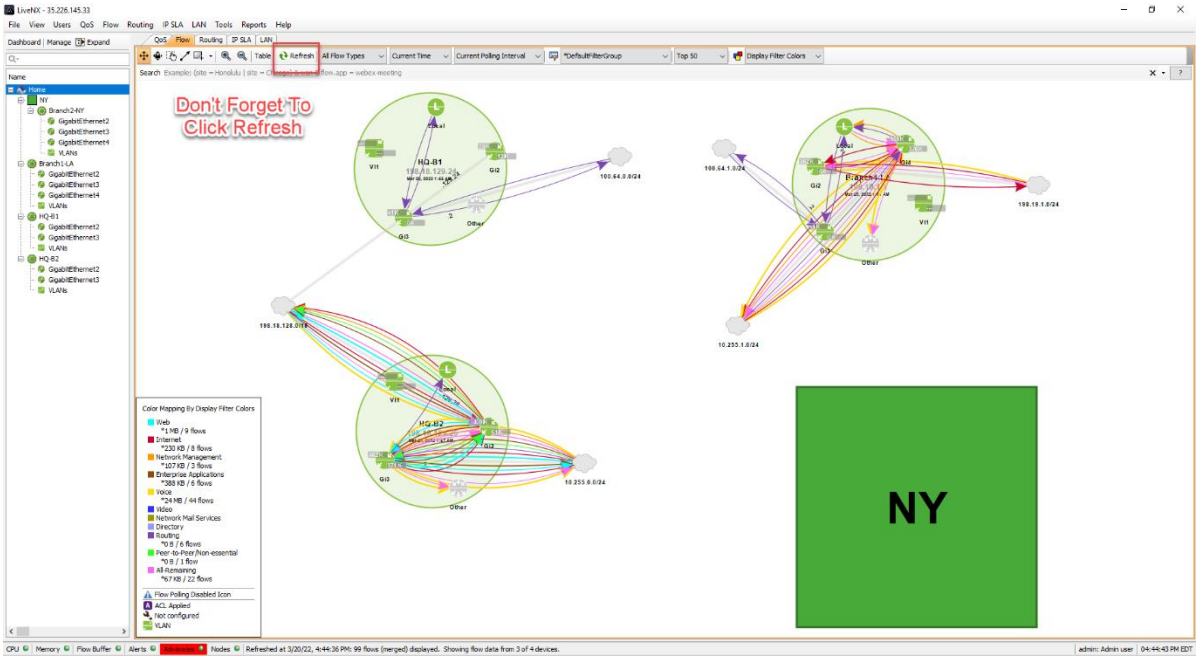


Figure 85

Lab 3.4: Add/Remove Interfaces

<u>This Lab uses the Engineering Console.</u>

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:

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

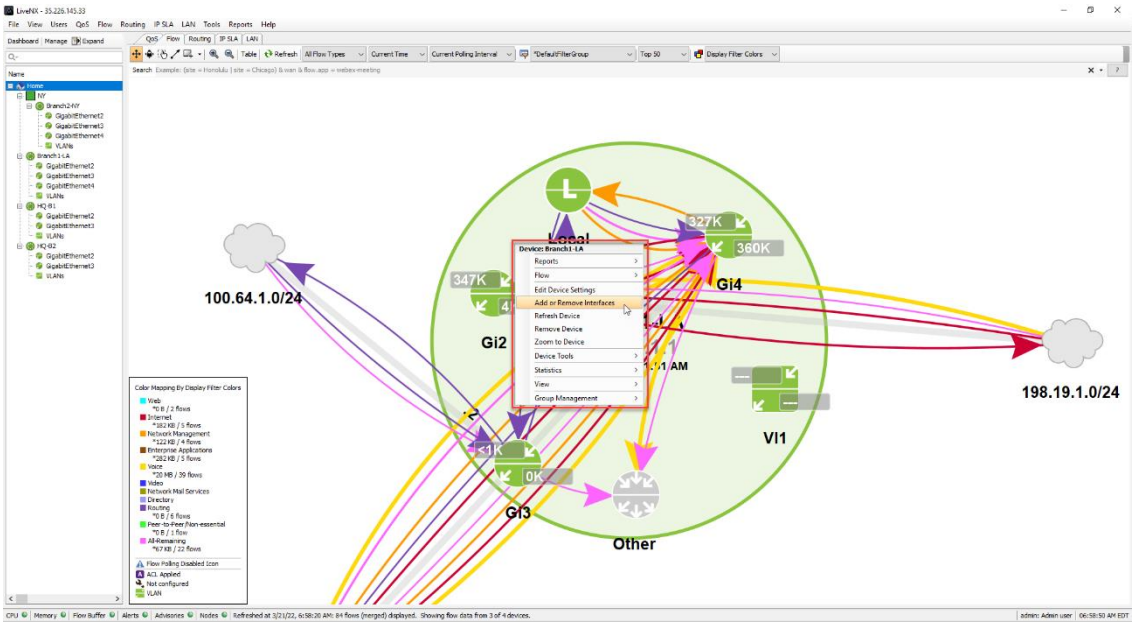


Figure 86

69. Deselect **GigabitEthernet3**.

 © Copyright LiveAction 2022

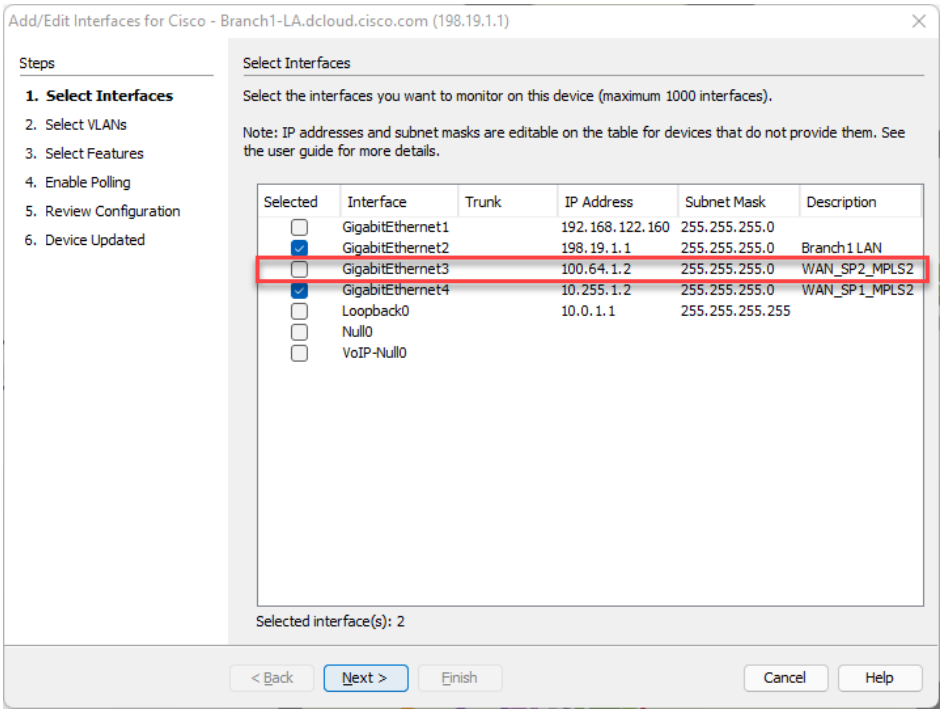


Figure 87

70. Select **Next** until the **Device Updated** window is displayed. Save the config to the device and save to startup config.

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

Notice that the device now has 2 active interfaces, represented by **GigabitEthernet2** and **GigabtEthernet4**

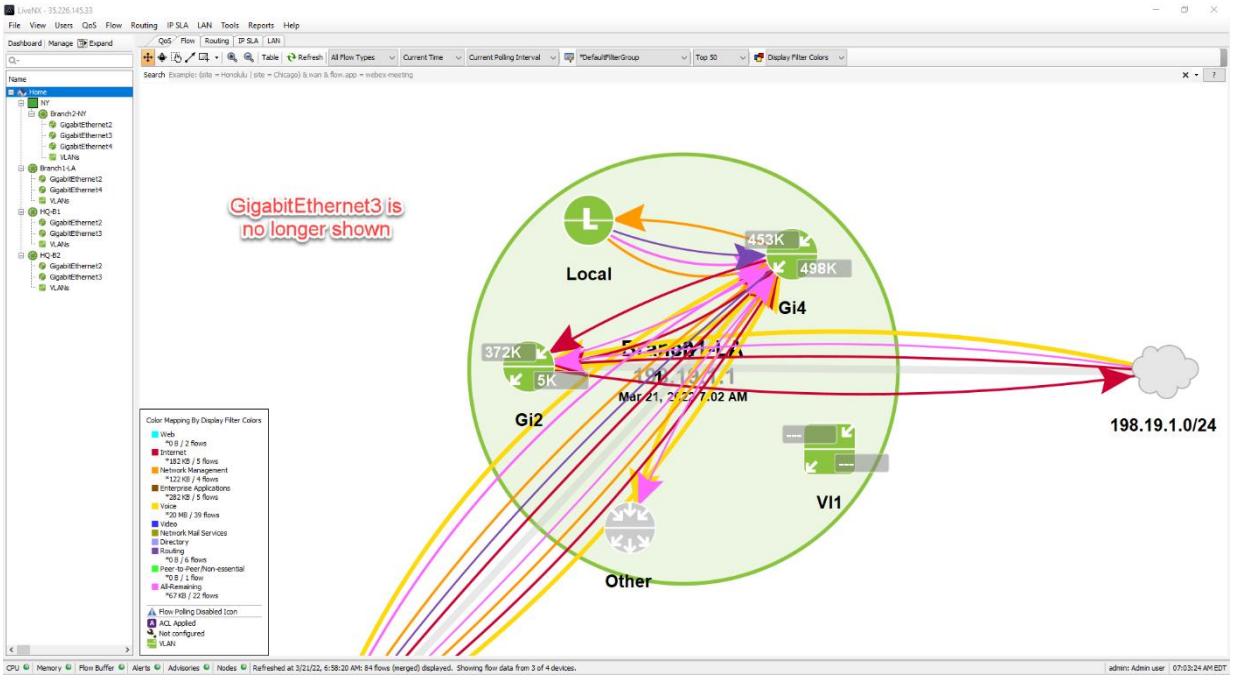


Figure 88

72. 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.

 © Copyright LiveAction 2022

Lab 3.5: Merge Clouds in Topology

<u>This Lab uses the Engineering Console.</u>

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.

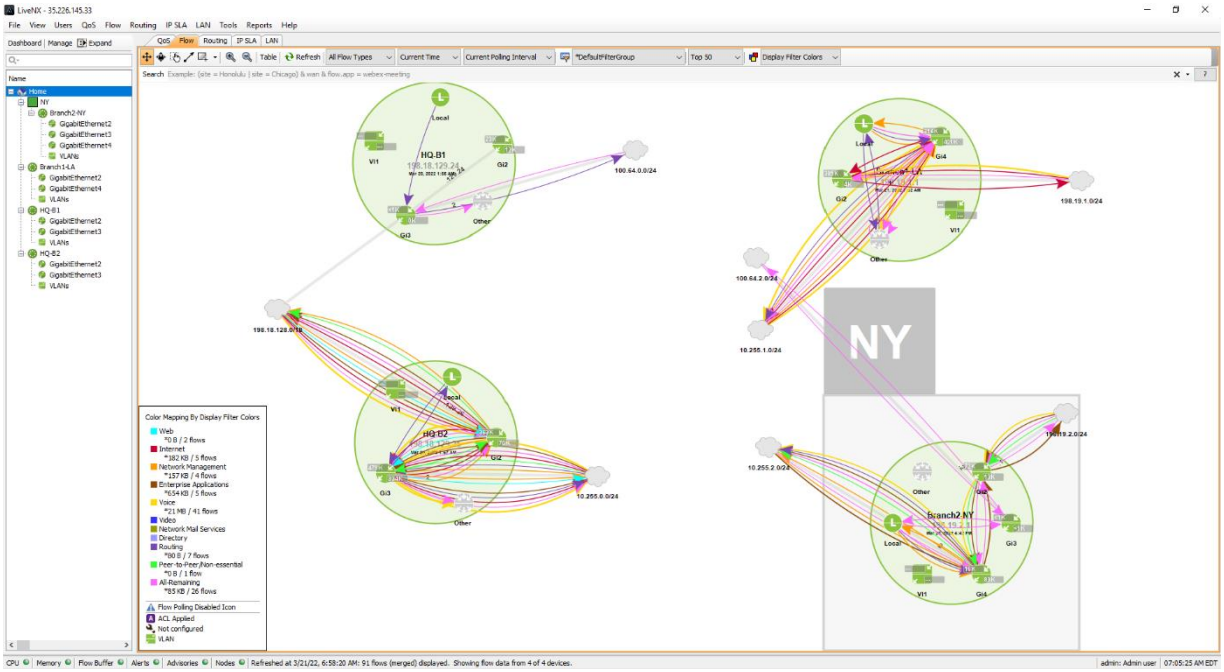


Figure 89

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:

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

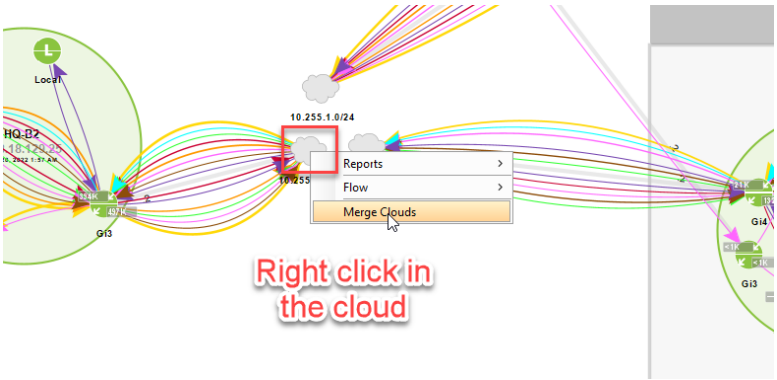


Figure 90

 © Copyright LiveAction 2022

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

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

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

76. Select "**Find**" to add more networks.

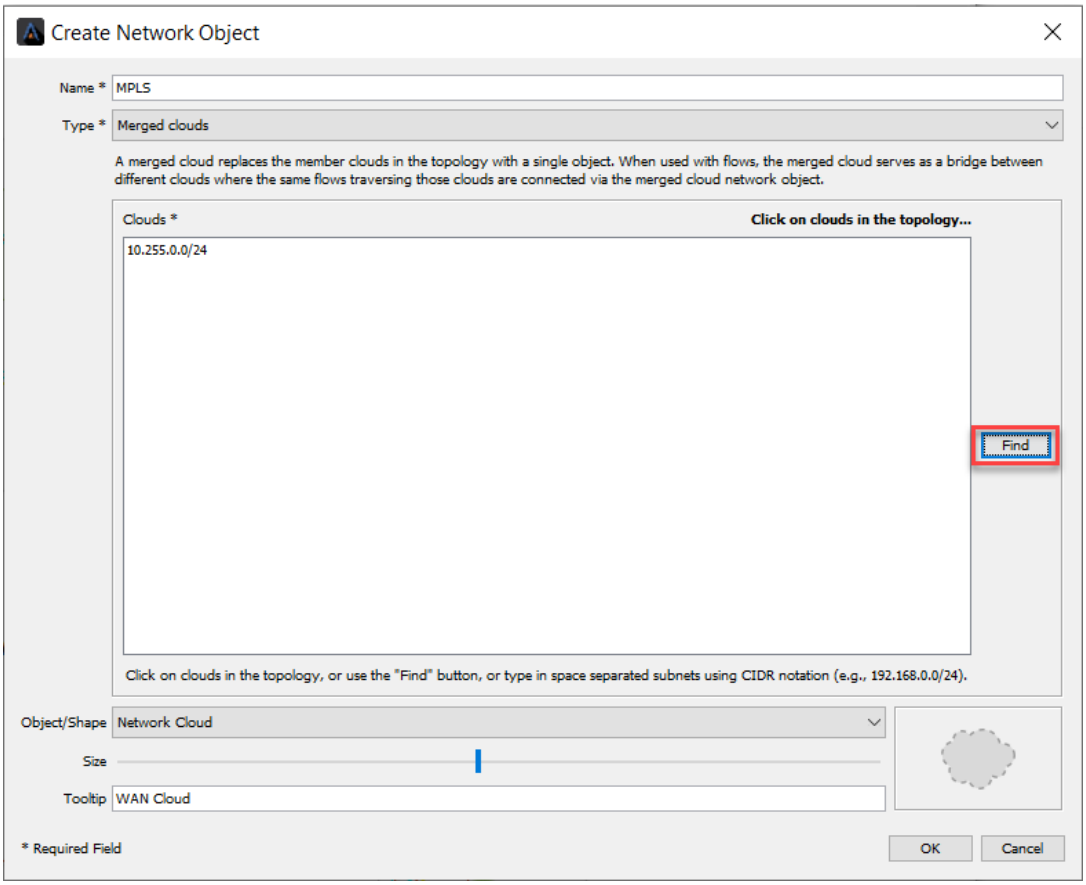


Figure 91

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

 © Copyright LiveAction 2022

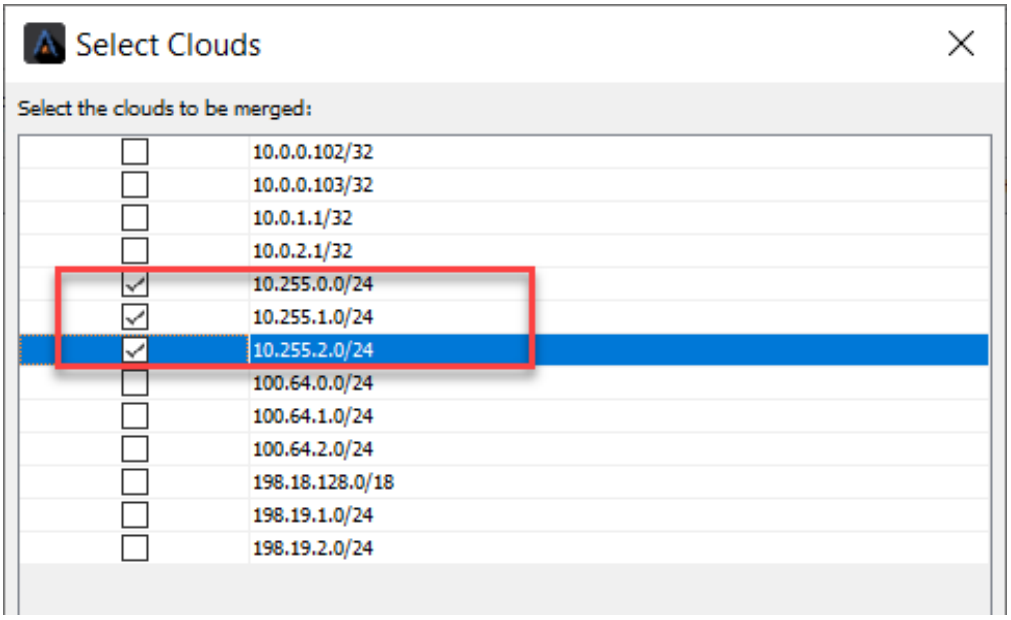


Figure 92

78. Click **OK**.
79. Click **OK** to finish.

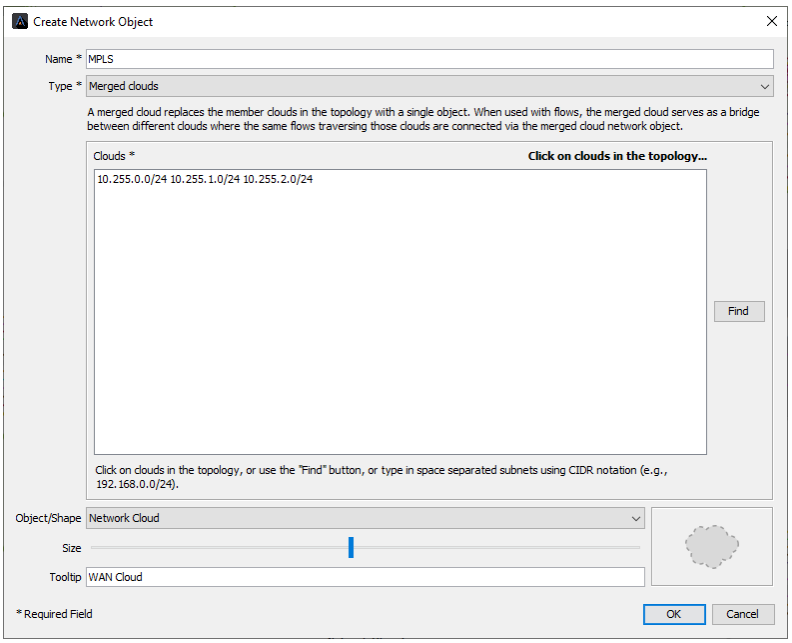


Figure 93

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.

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

 © Copyright LiveAction 2022

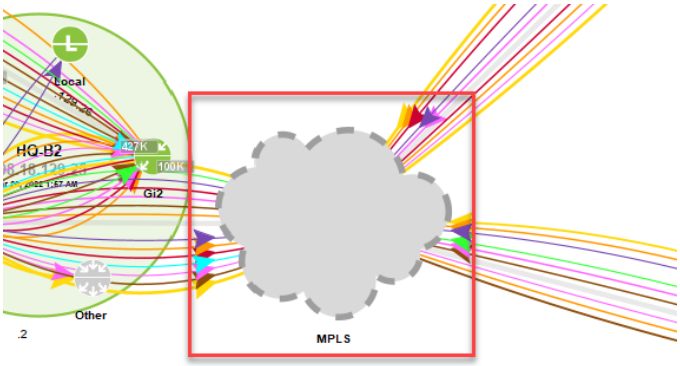


Figure 94

81. Now complete this for the second cloud, using IP addresses **100.64.0.1**, **100.64.1.0**, and **100.64.2.0**.

 © Copyright LiveAction 2022

Lab 4

Lab 4: Traffic Flows

 © Copyright LiveAction 2022

Lab 4.1: Discover Flows

<u>These Labs uses the Engineering Console exclusively.</u>

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.

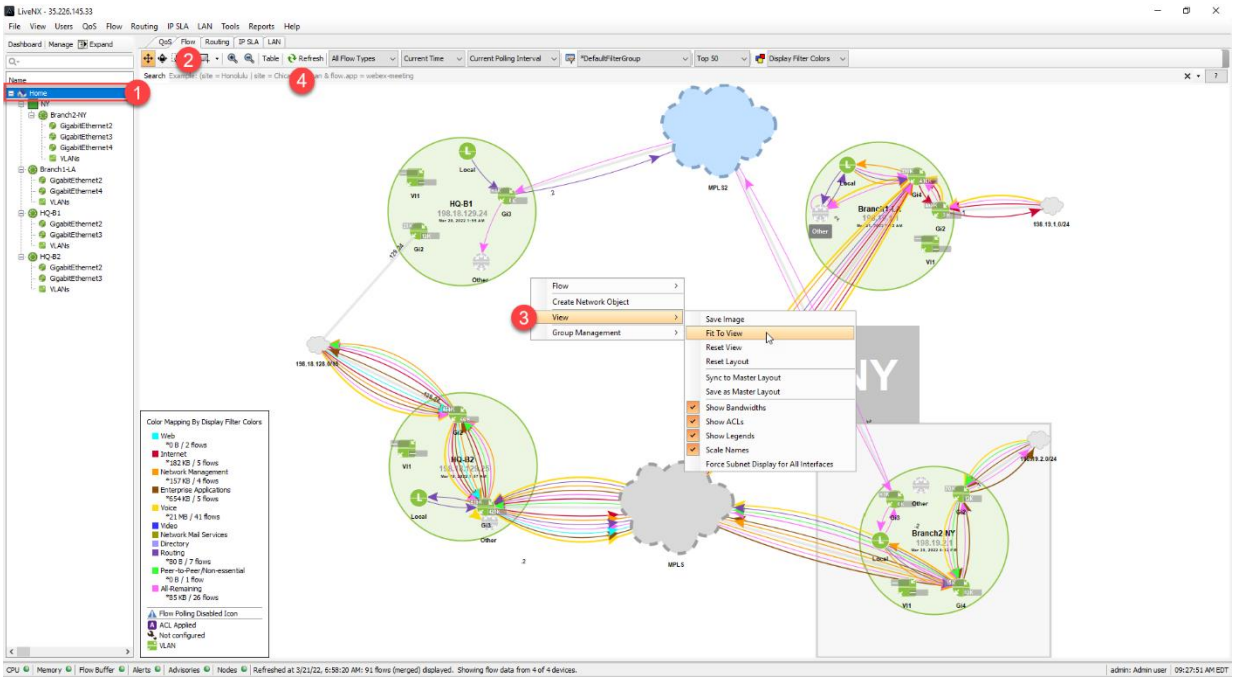


Figure 95

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: **Voice**, and **DSCP**.
6.

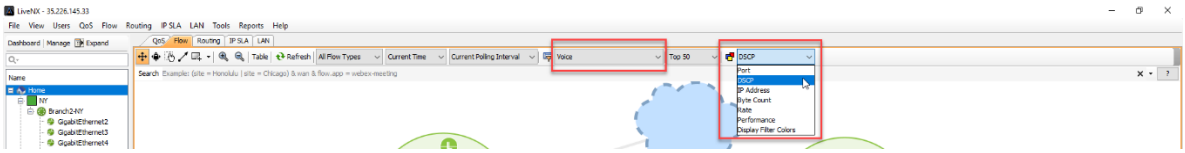


Figure 96

 © Copyright LiveAction 2022

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

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

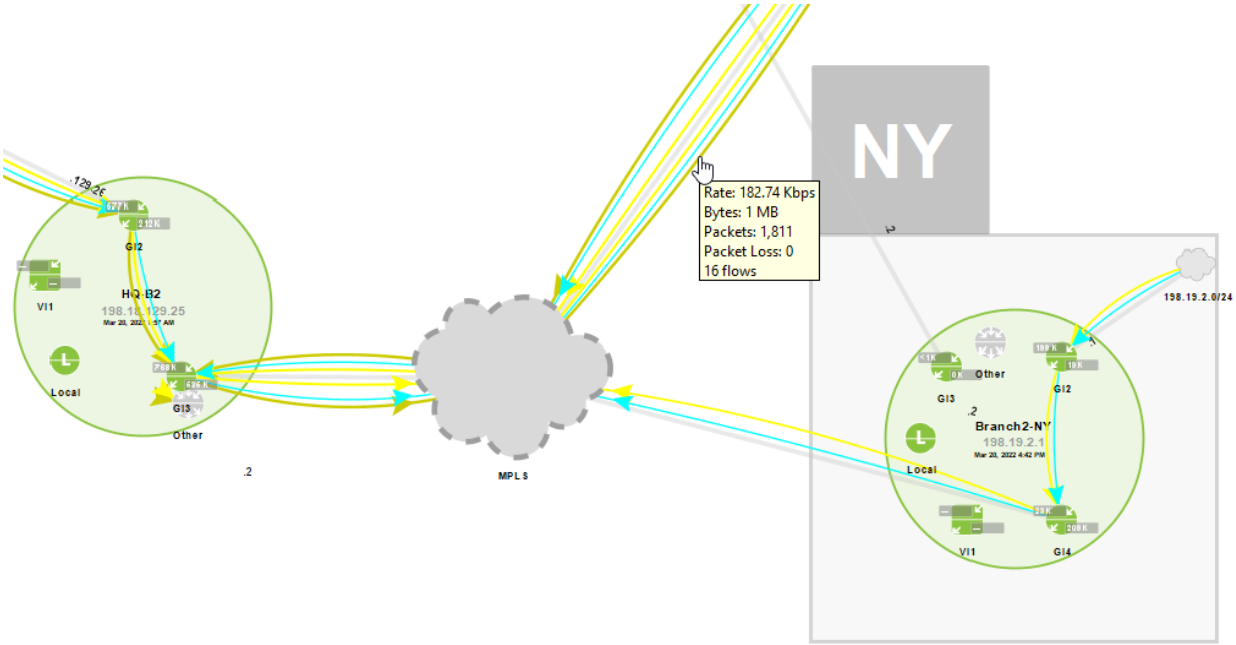


Figure 97

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

What other applications can you identify across our network?

Application	Port#	IP Pairs
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

 © Copyright LiveAction 2022

Lab 4.2: Discover Specific Flows

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

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

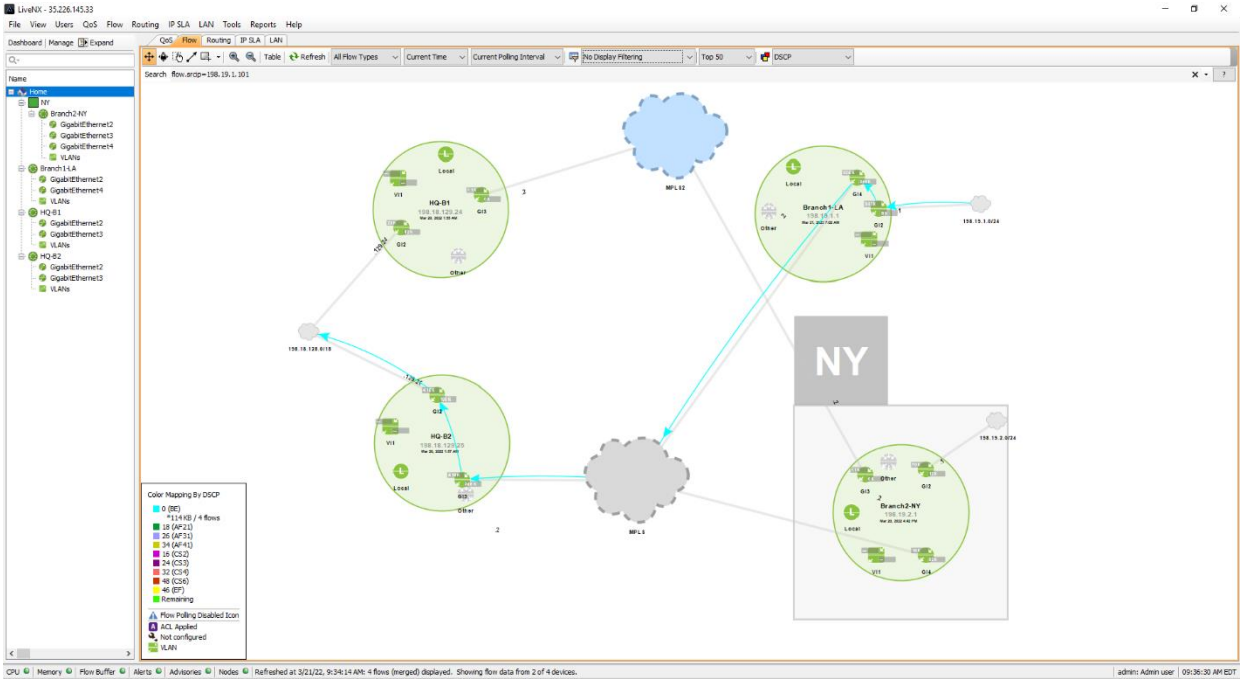
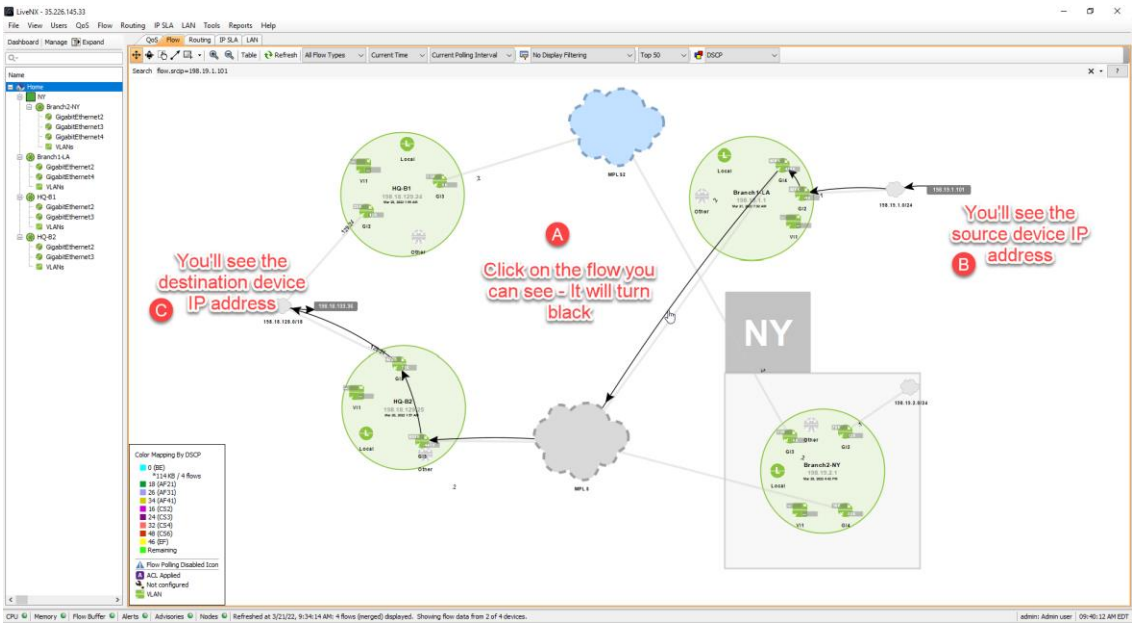


Figure 98

Notice that LiveNX has identified one or more *end-to-end* flows across the network. This flow originates from 198.19.1.101.



 © Copyright LiveAction 2022

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
3. Click on one of the rows relating to **Bittorrent**.

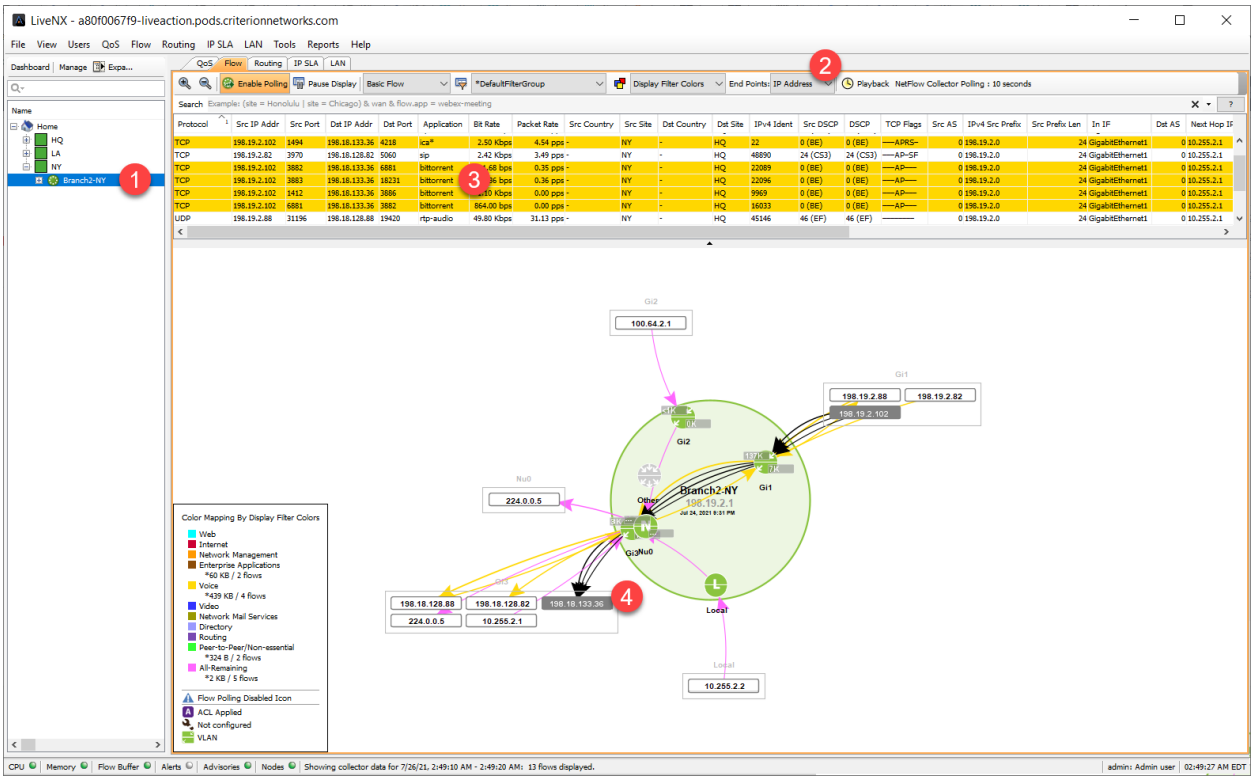


Figure 99

4. Click on one of the endpoints, and then click **Pause Display**. This stops the polling refresh from changing the information displayed in the table.

Almost too easy, wasn't it? What are the IP endpoints of all that BitTorrent traffic? You can expand the top window by dragging on the bottom edge.

_____ to/from _____

_____ to/from _____

 © Copyright LiveAction 2022

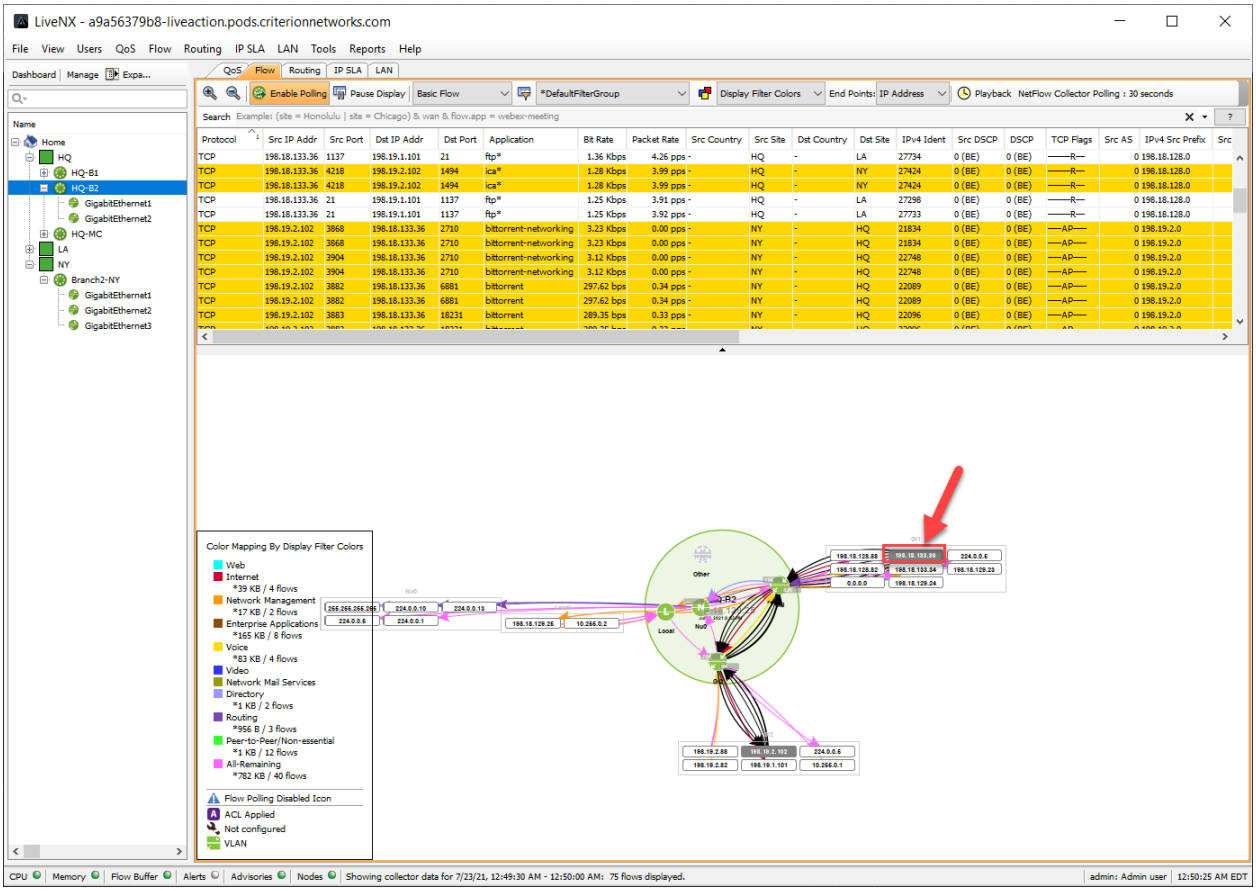


Figure 100

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!

 © Copyright LiveAction 2022

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**.

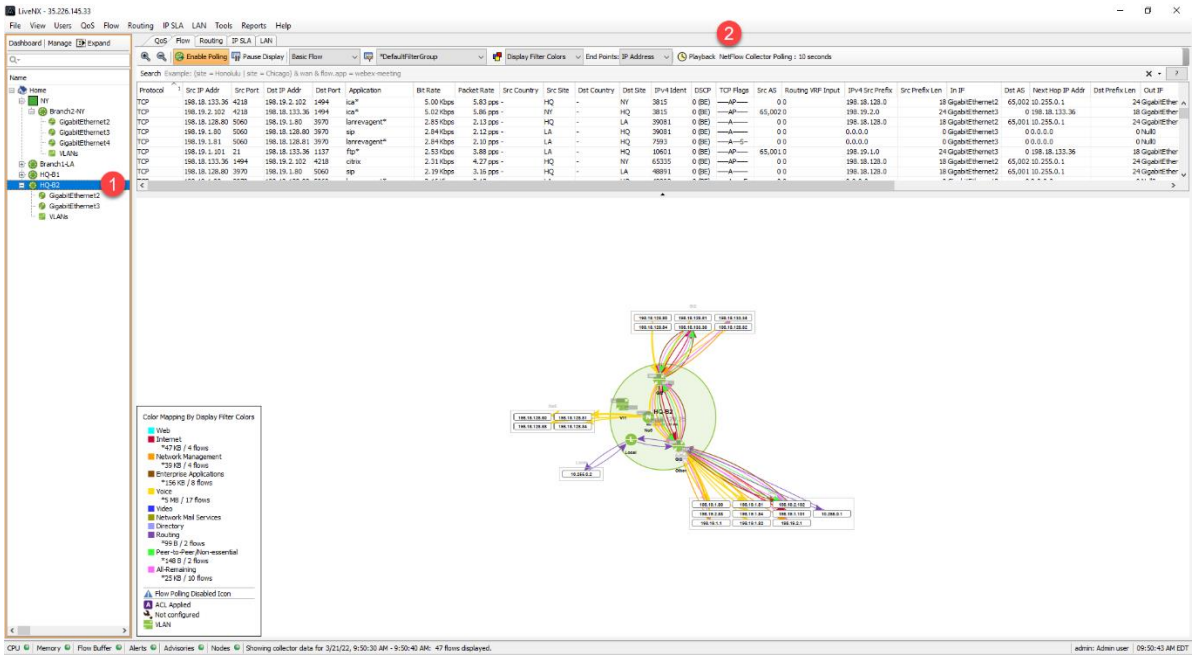


Figure 101

 © Copyright LiveAction 2022

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

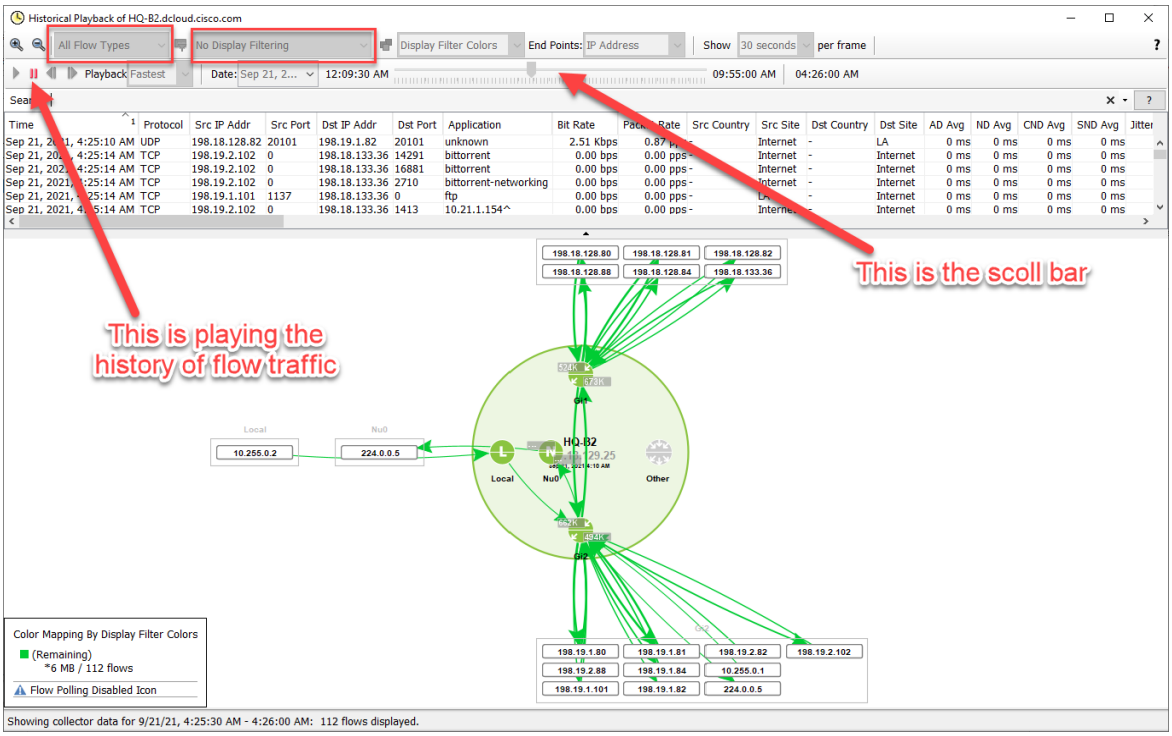


Figure 102

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.

Look for higher bandwidth utilization – This will be over 1Mbps.

 © Copyright LiveAction 2022

Lab 5

Lab 5: Custom Filters

© Copyright LiveAction 2022

Lab 5.1: Creating Custom Filters

<u>These Labs uses the Engineering Console exclusively.</u>

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

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

Lab Steps:

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

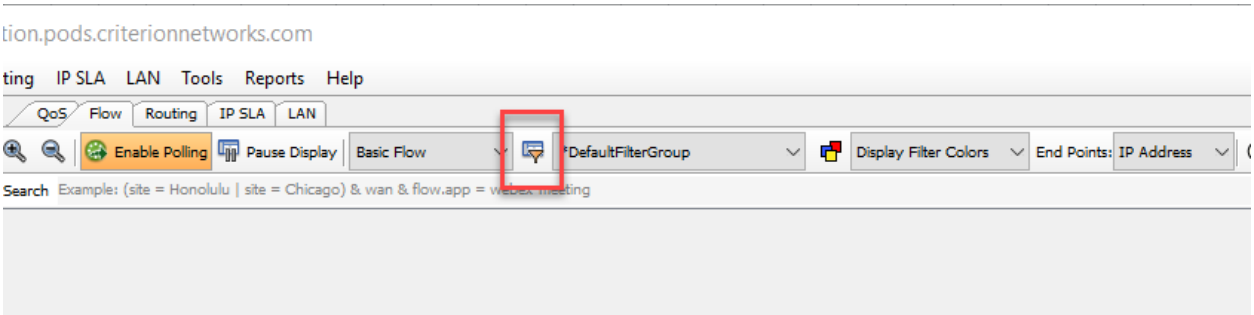


Figure 103

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

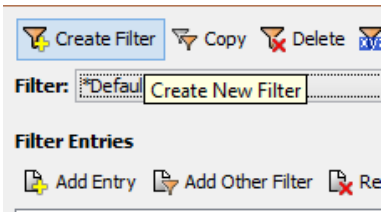


Figure 104

3. Enter a Name label: Use something that you will easily recognize. We have used **TRG-VoIP**.

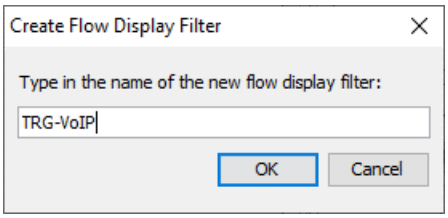
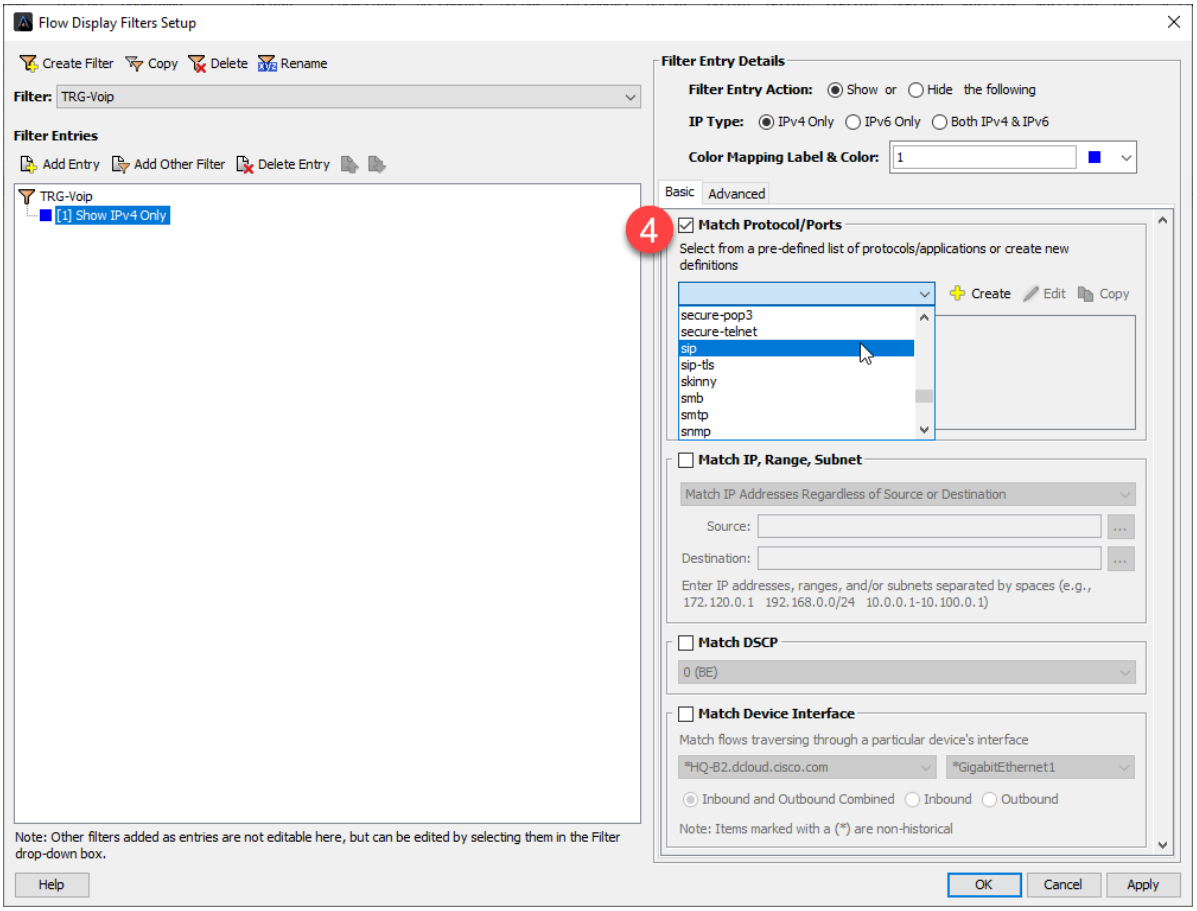


Figure 105

4. With the filter selected, look at the left of the window, and in the **Basic** Tab, check **Match Protocol/Ports** and select the **SIP** Protocol.

 © Copyright LiveAction 2022



5. Click **Edit** to the right of the SIP selection.

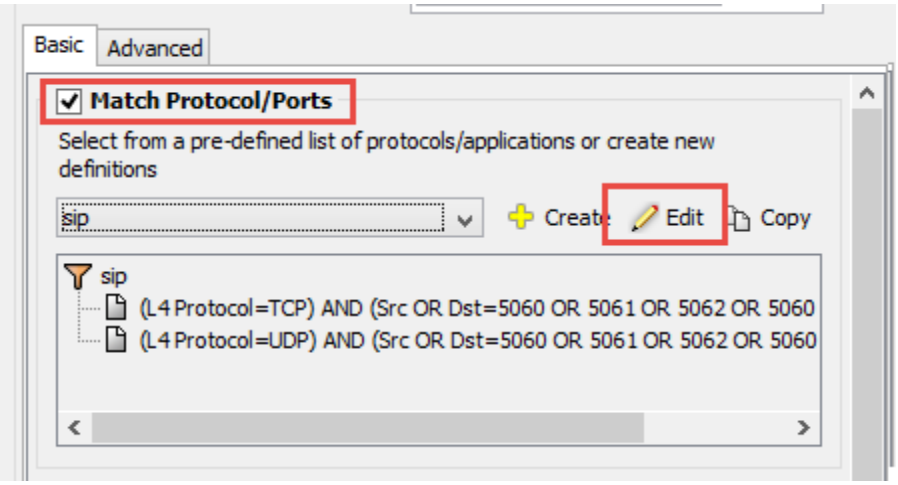


Figure 106

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.

 © Copyright LiveAction 2022

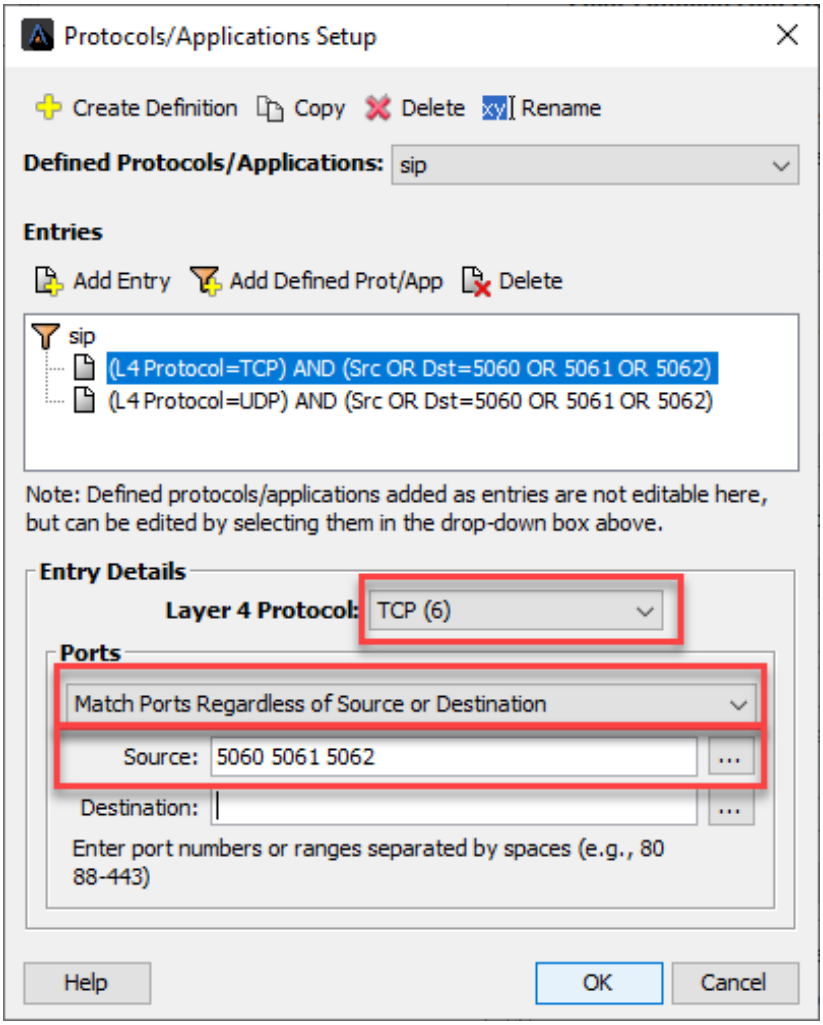


Figure 107

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

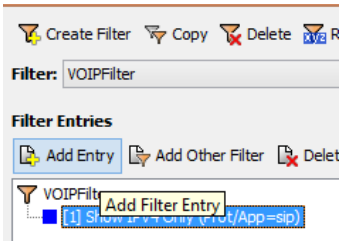


Figure 108

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

 © Copyright LiveAction 2022

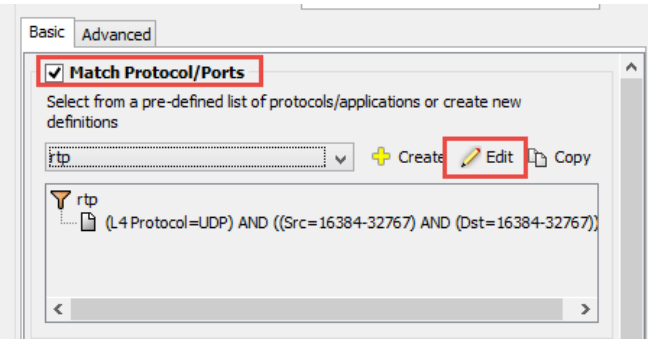


Figure 109

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

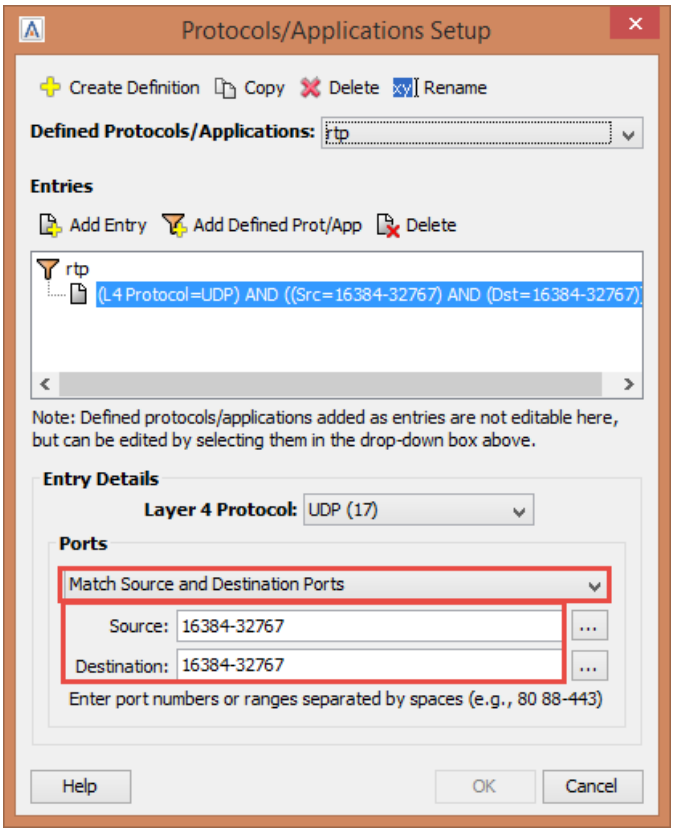


Figure 110

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

 © Copyright LiveAction 2022

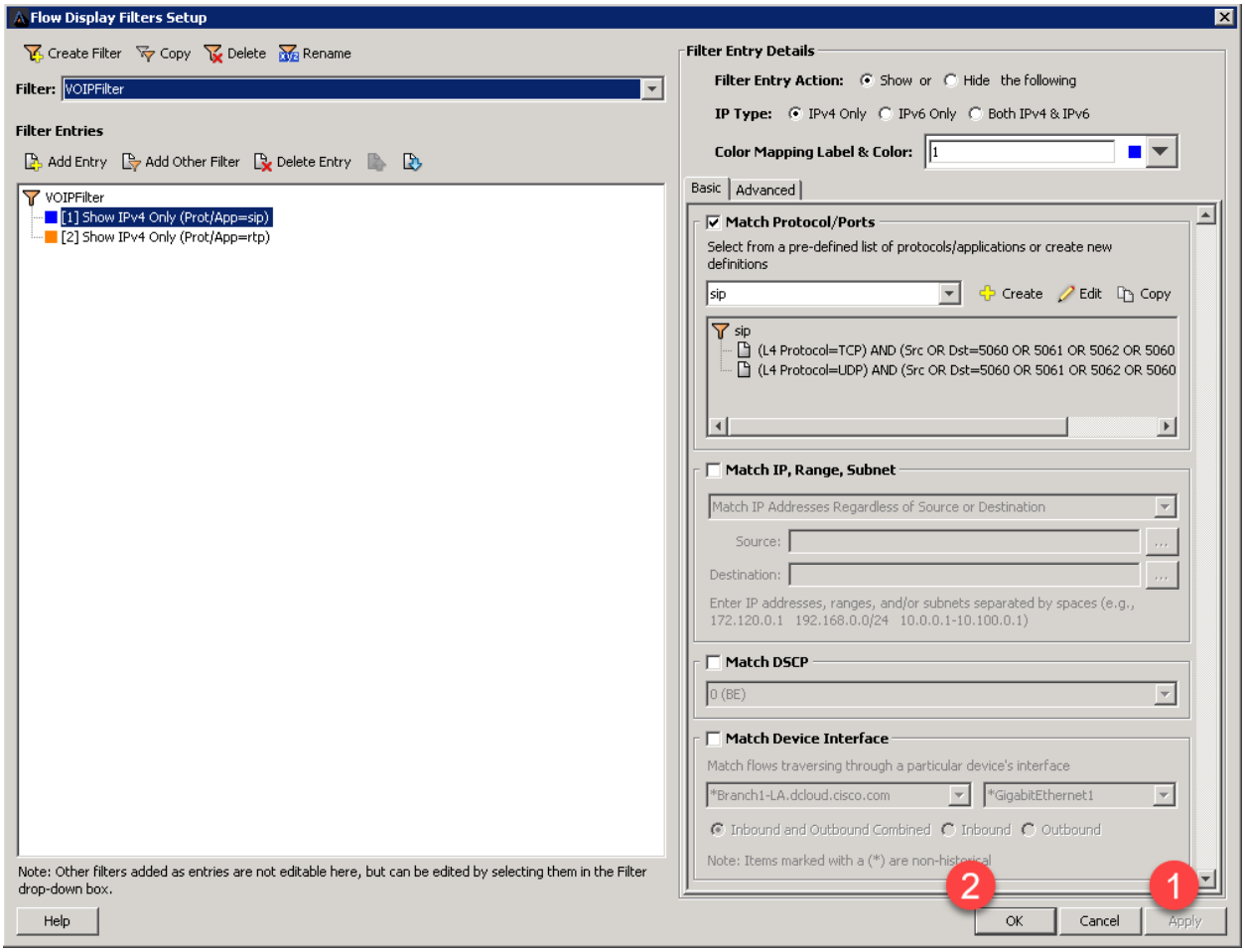


Figure 111

 © Copyright LiveAction 2022

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

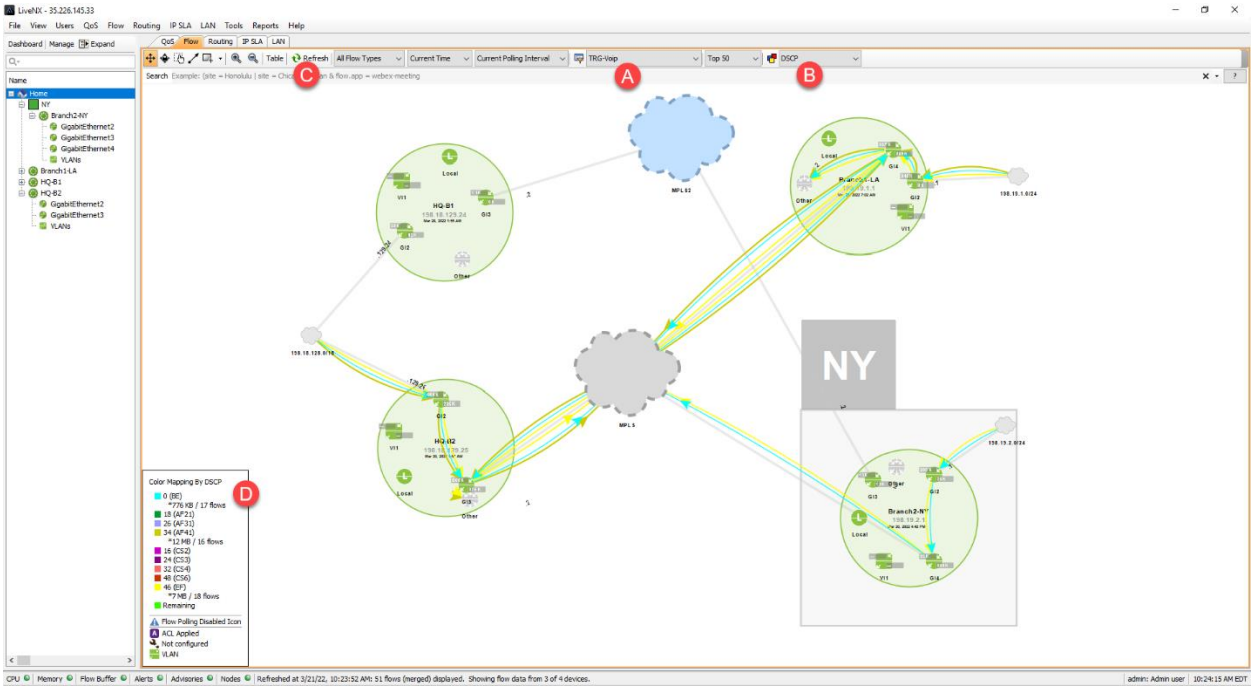


Figure 112

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

 © Copyright LiveAction 2022

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**.

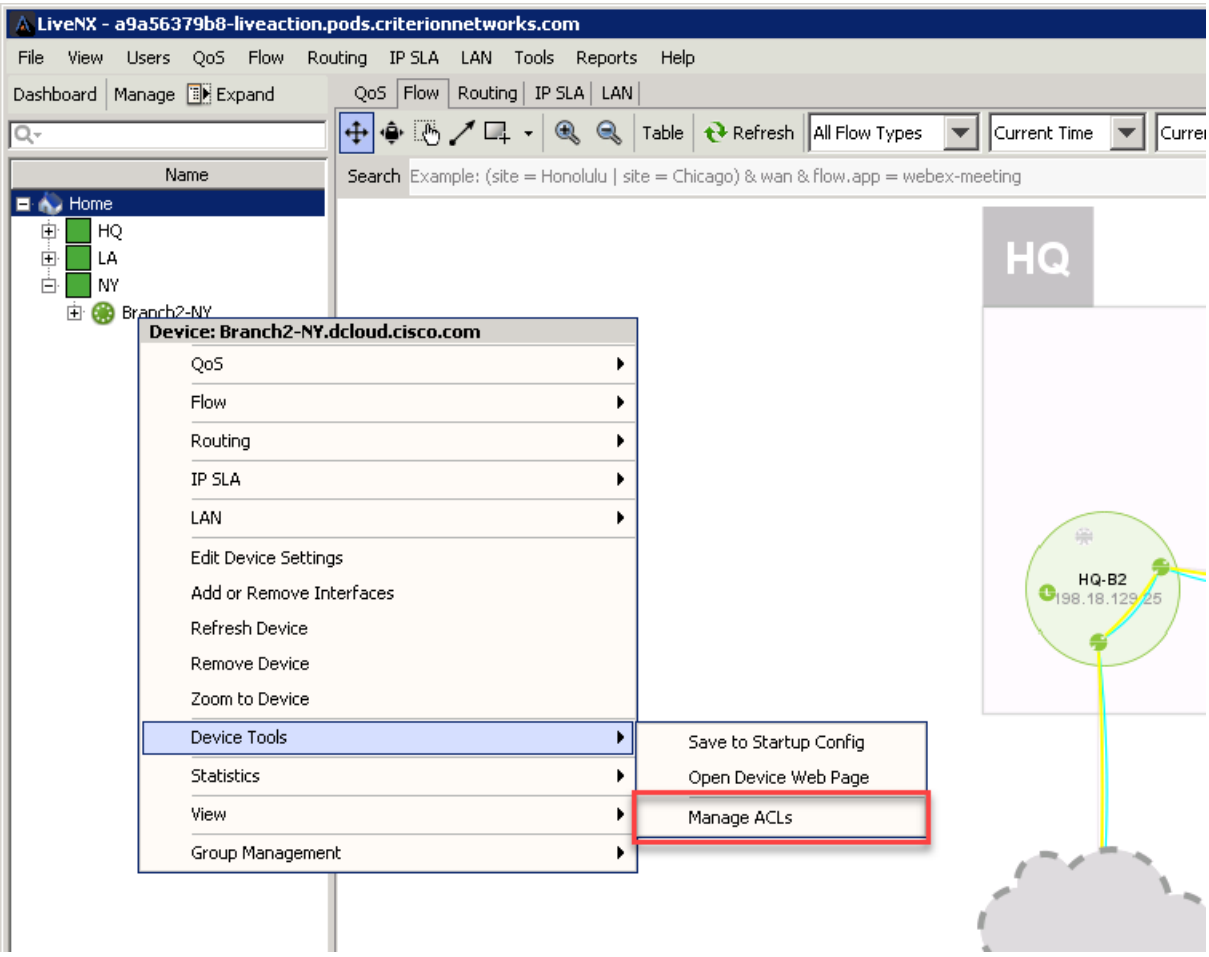


Figure 113

2. Select "**Create ACL**"

 © Copyright LiveAction 2022

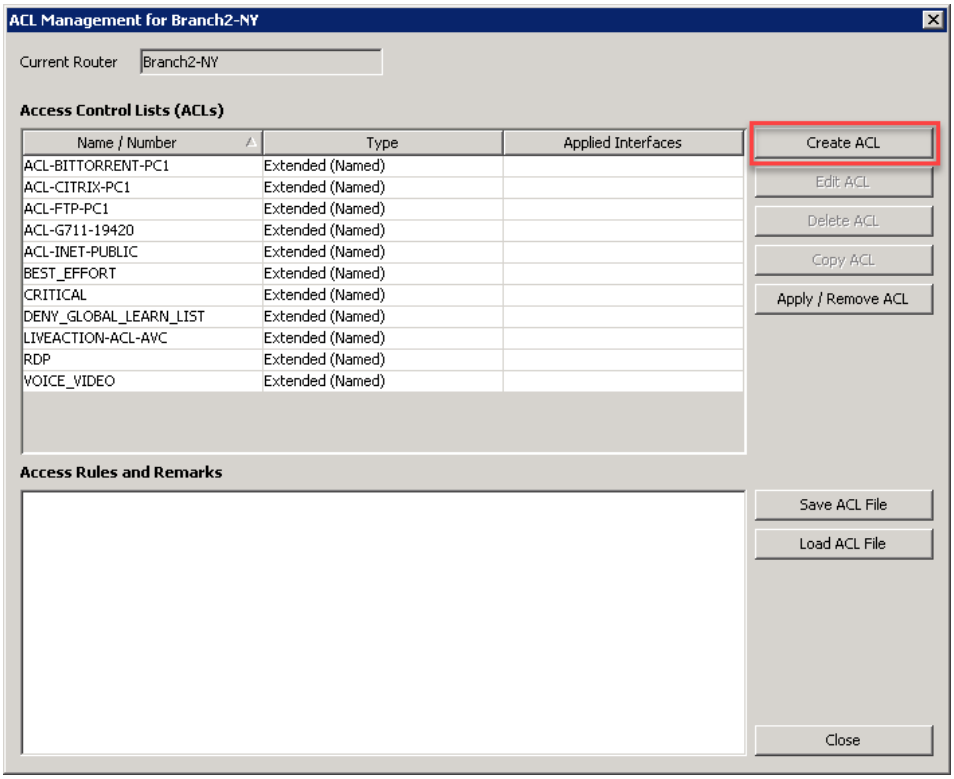


Figure 114

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**.

 © Copyright LiveAction 2022

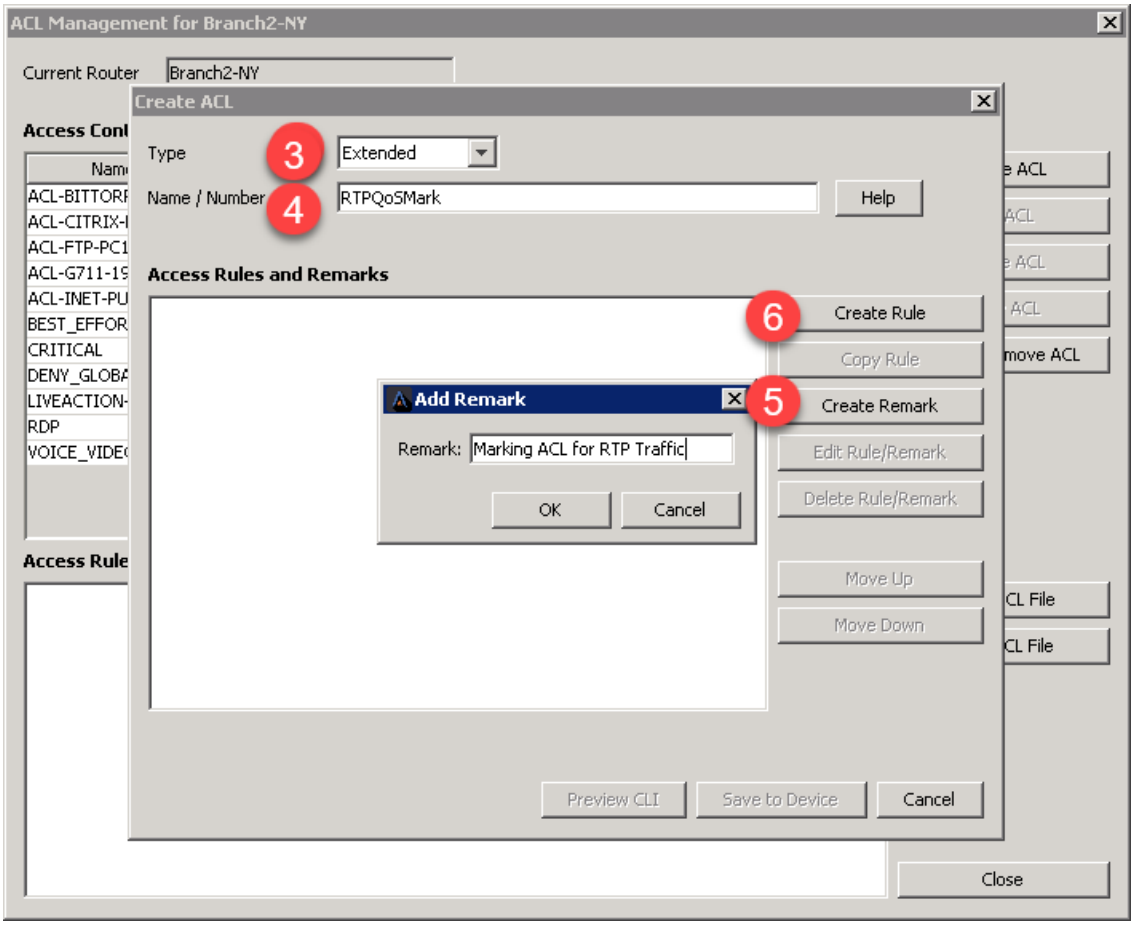


Figure 115

 © Copyright LiveAction 2022

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.

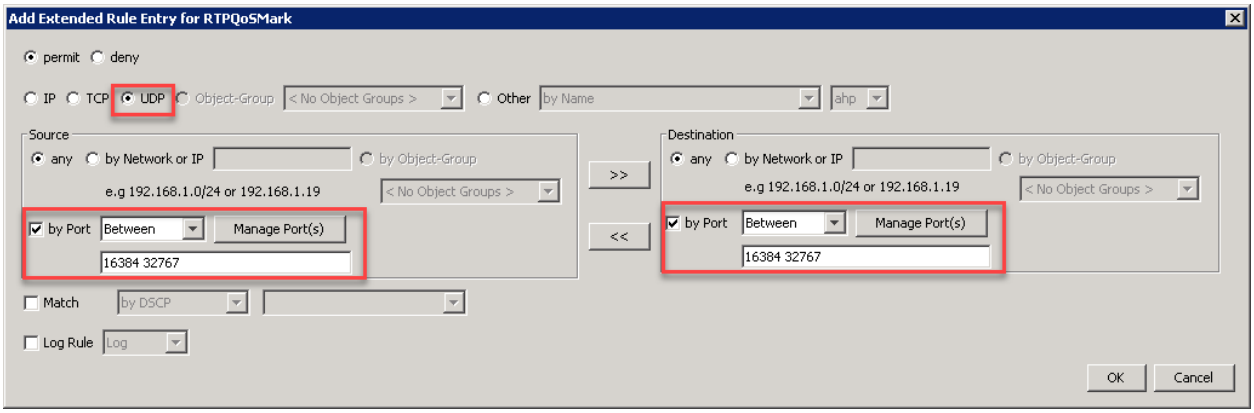


Figure 116

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

12. Click **Save to Device**.

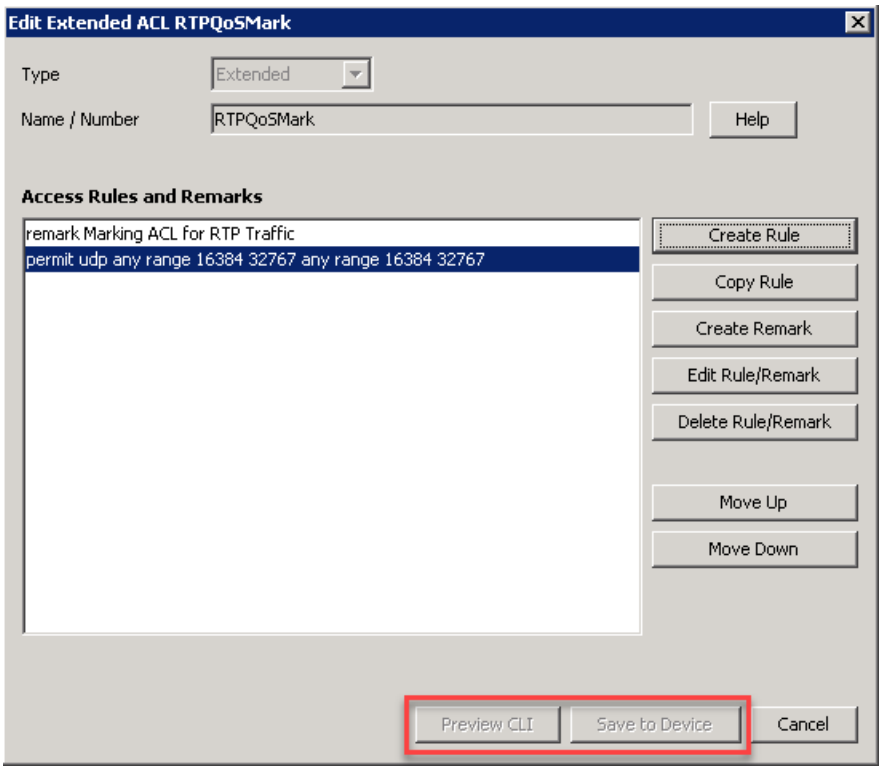


Figure 117

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

 © Copyright LiveAction 2022

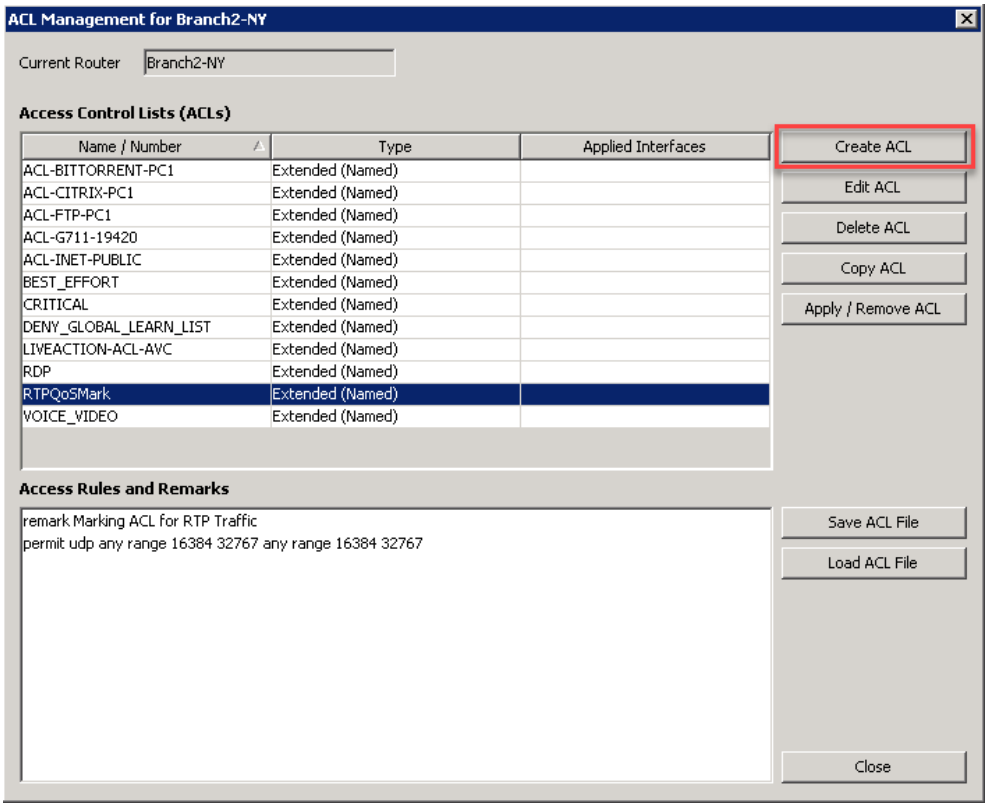


Figure 118

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**.

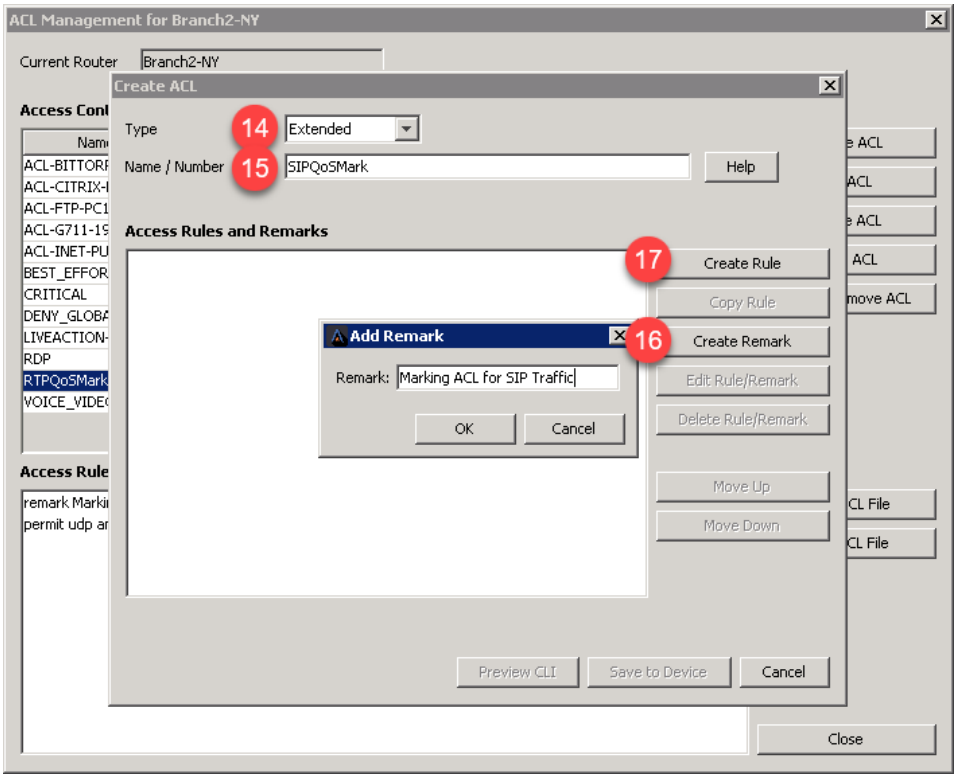


Figure 119

 © Copyright LiveAction 2022

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.

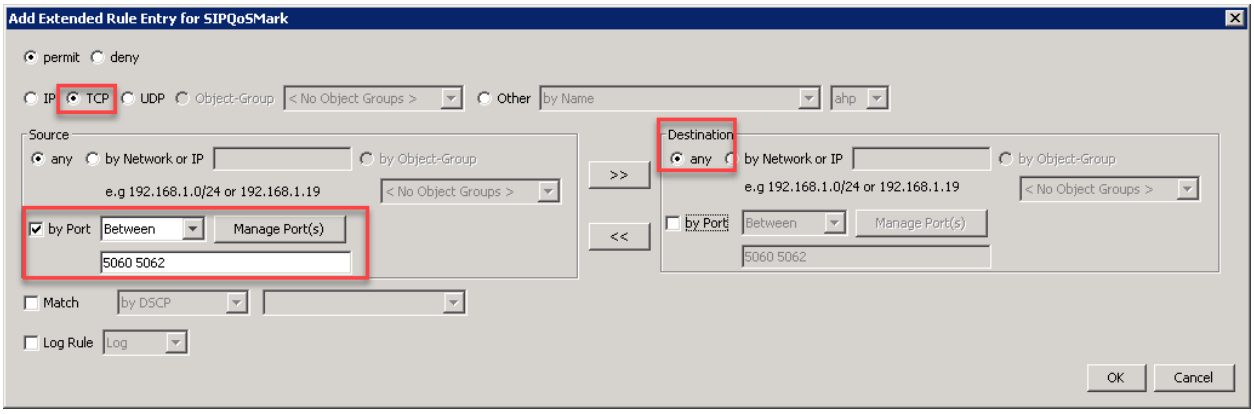


Figure 120

Next create another rule for destination SIP Ports.

 © Copyright LiveAction 2022

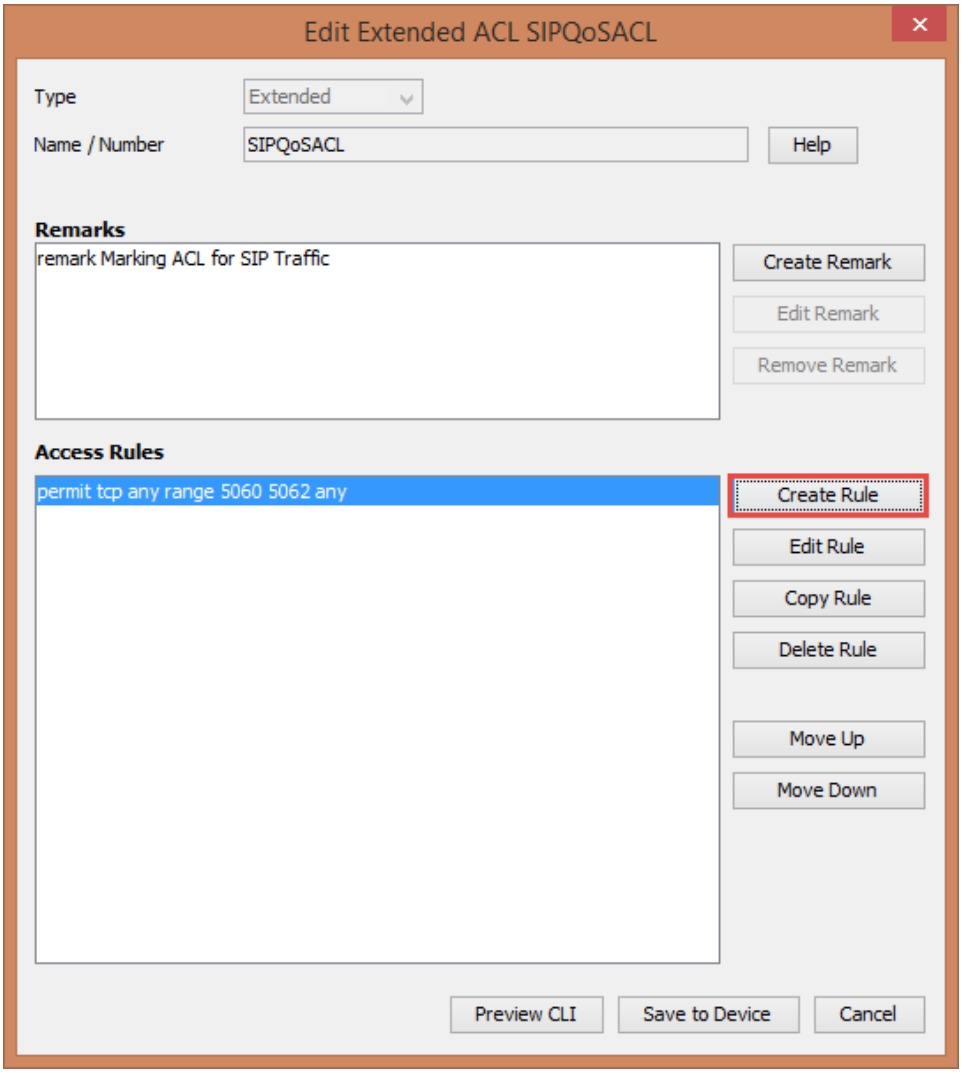


Figure 121

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

 © Copyright LiveAction 2022

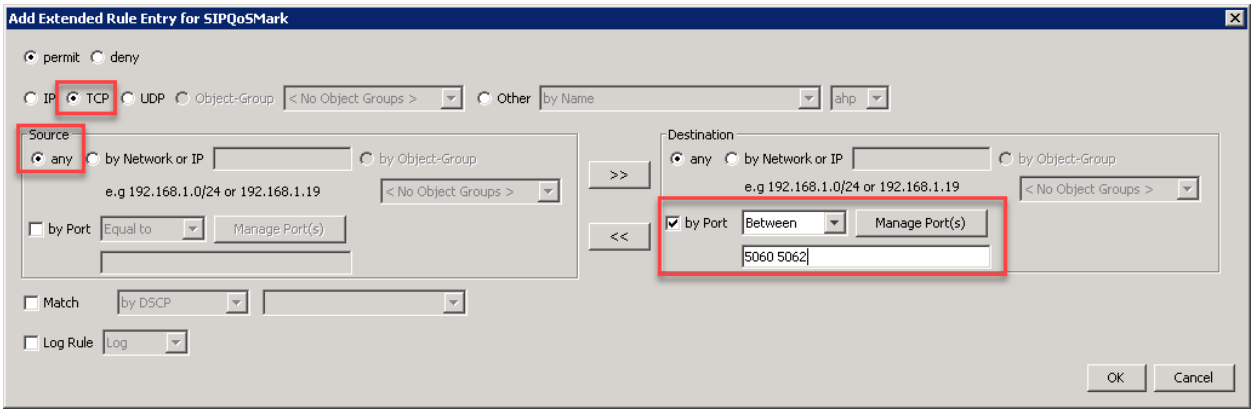


Figure 122

30. Click **Preview CLI** to review the configuration to push.
31. Click **Save to Device**, and then **Close**.

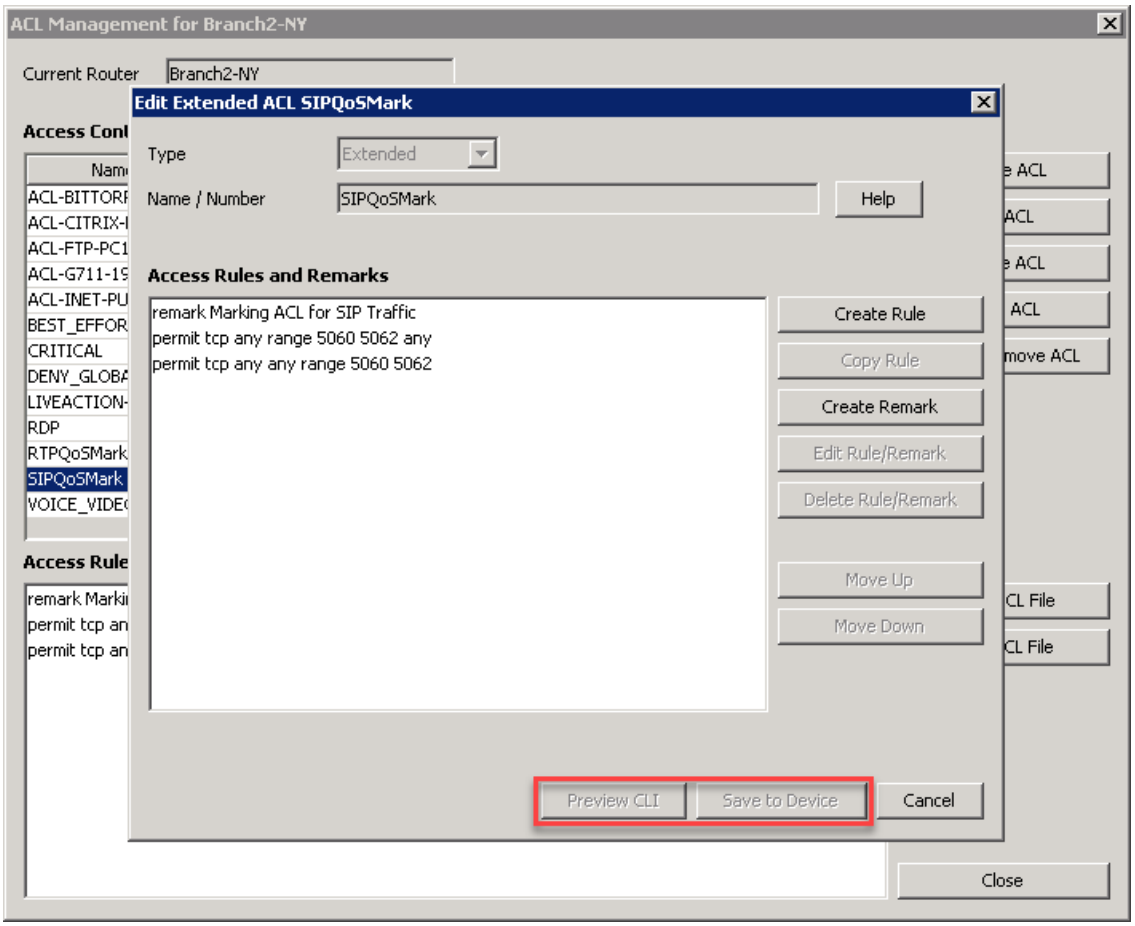


Figure 123

32. Now copy these ACL's to **Branch1-LA** router.
33. From **Branch2-NY**, go to Device Tools – Manage ACLs

 © Copyright LiveAction 2022

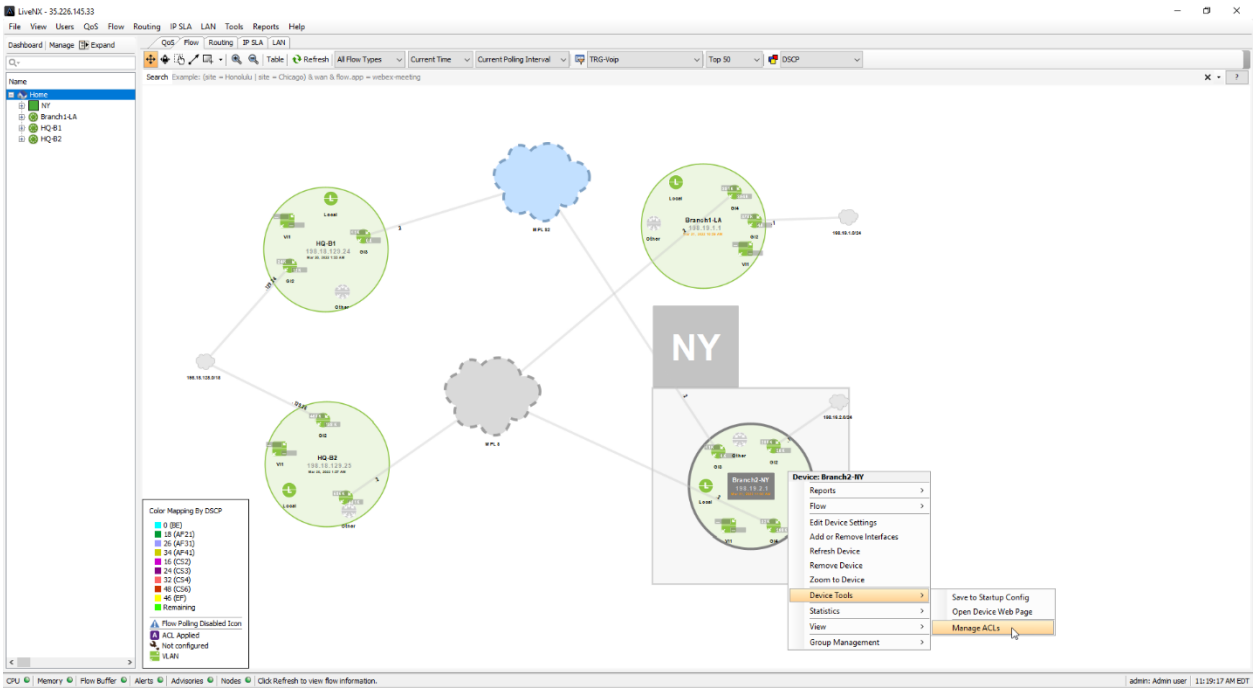


Figure 124

Next, you will save the **RTP and SIP Marking** ACLs to a file so you can apply on other devices. Click the **Save ACL File** button.

 © Copyright LiveAction 2022

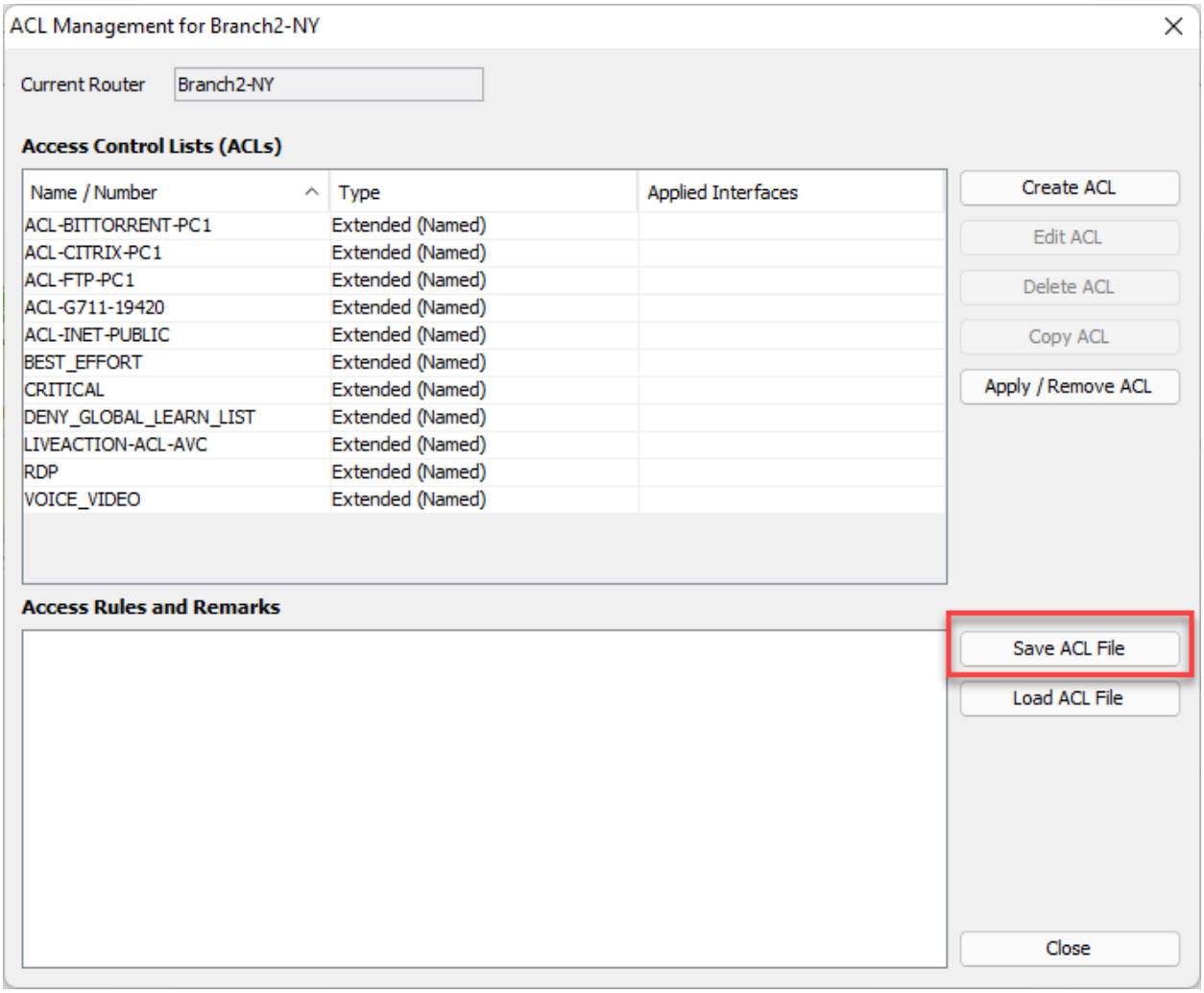


Figure 125

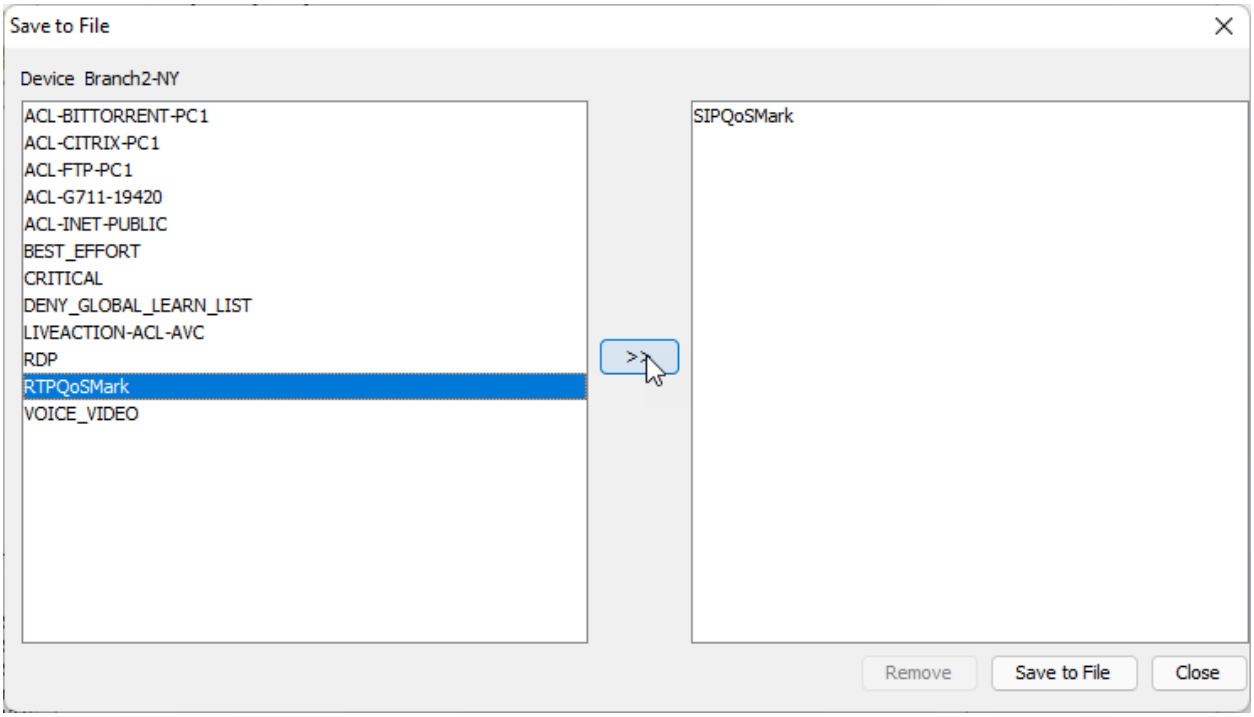


Figure 126

 © Copyright LiveAction 2022

4/8/2022

Select the ACLs to save one-by-one, and add them to the list on the right (**RTPQoSMark**, and **SIPQoSMark**).

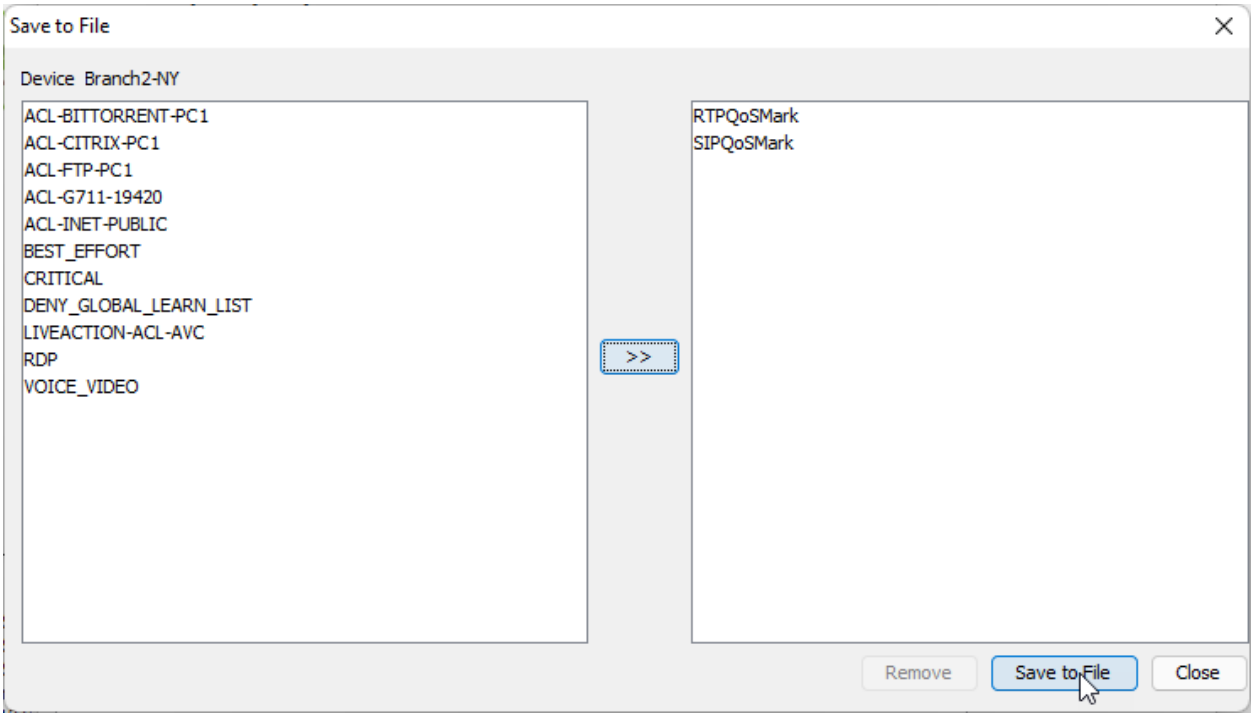


Figure 127

Name the file and save to a known location (I saved to Desktop)

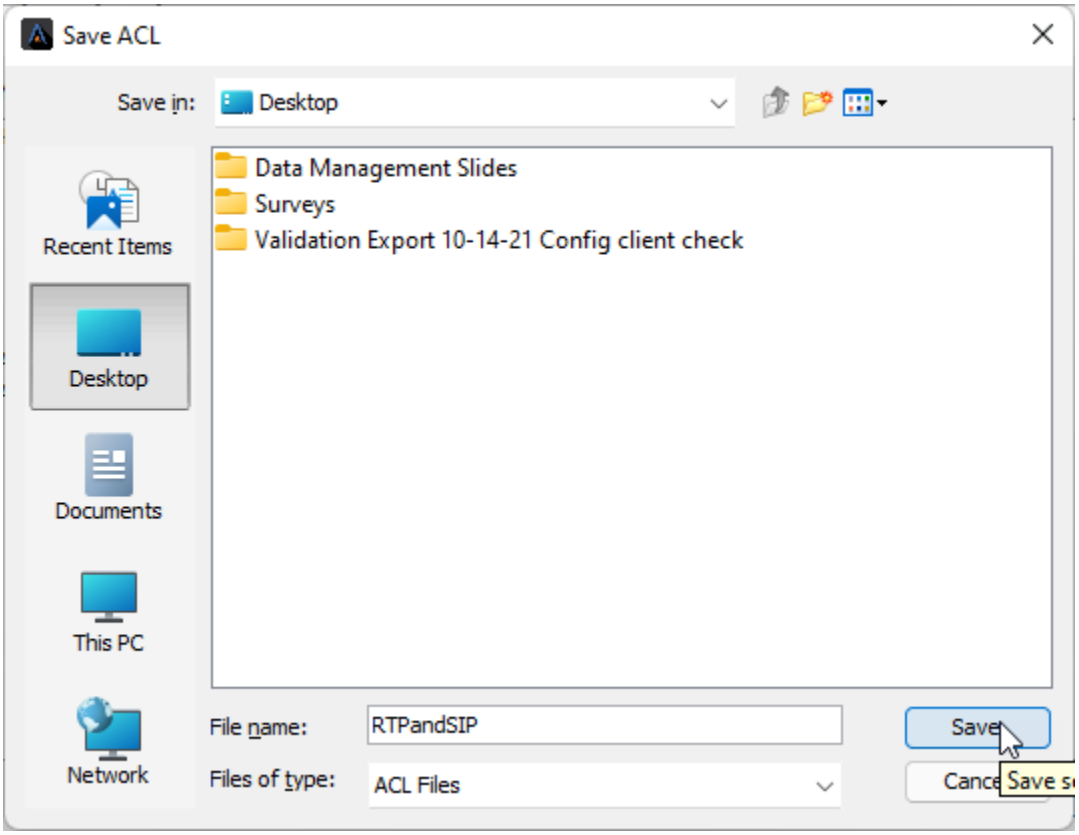


Figure 128

Go to **Branch1-LA** – Manage ACL's

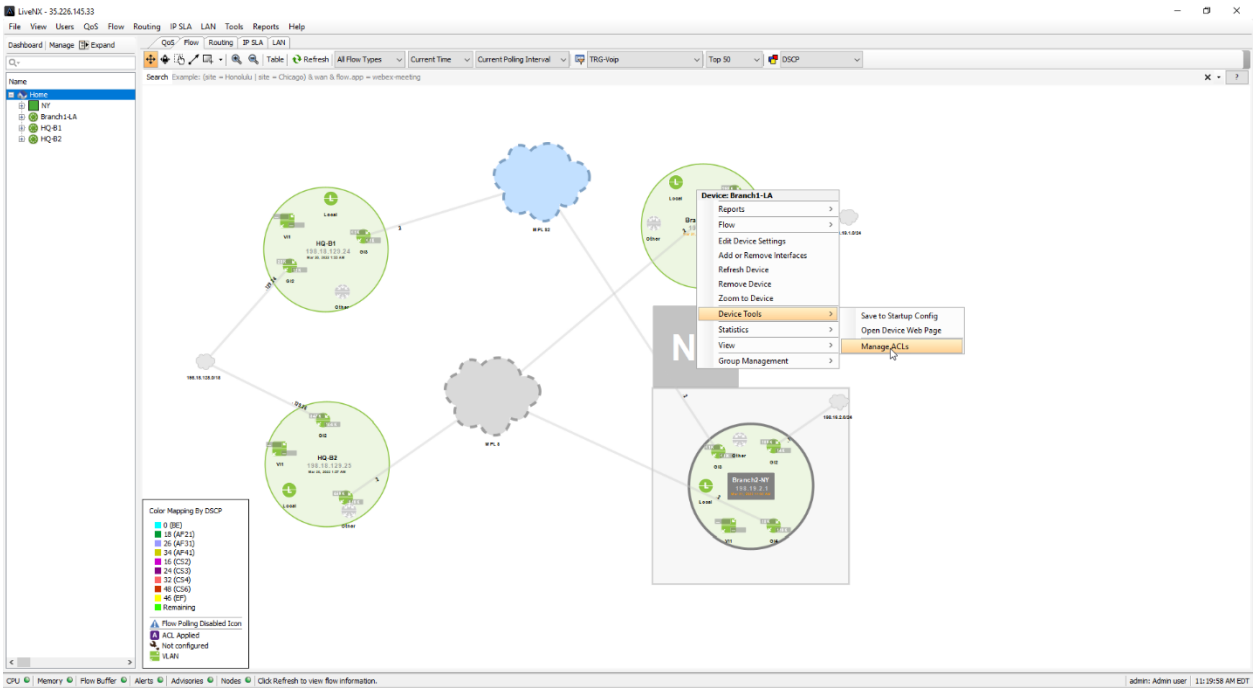


Figure 129

Select **Load ACL File**

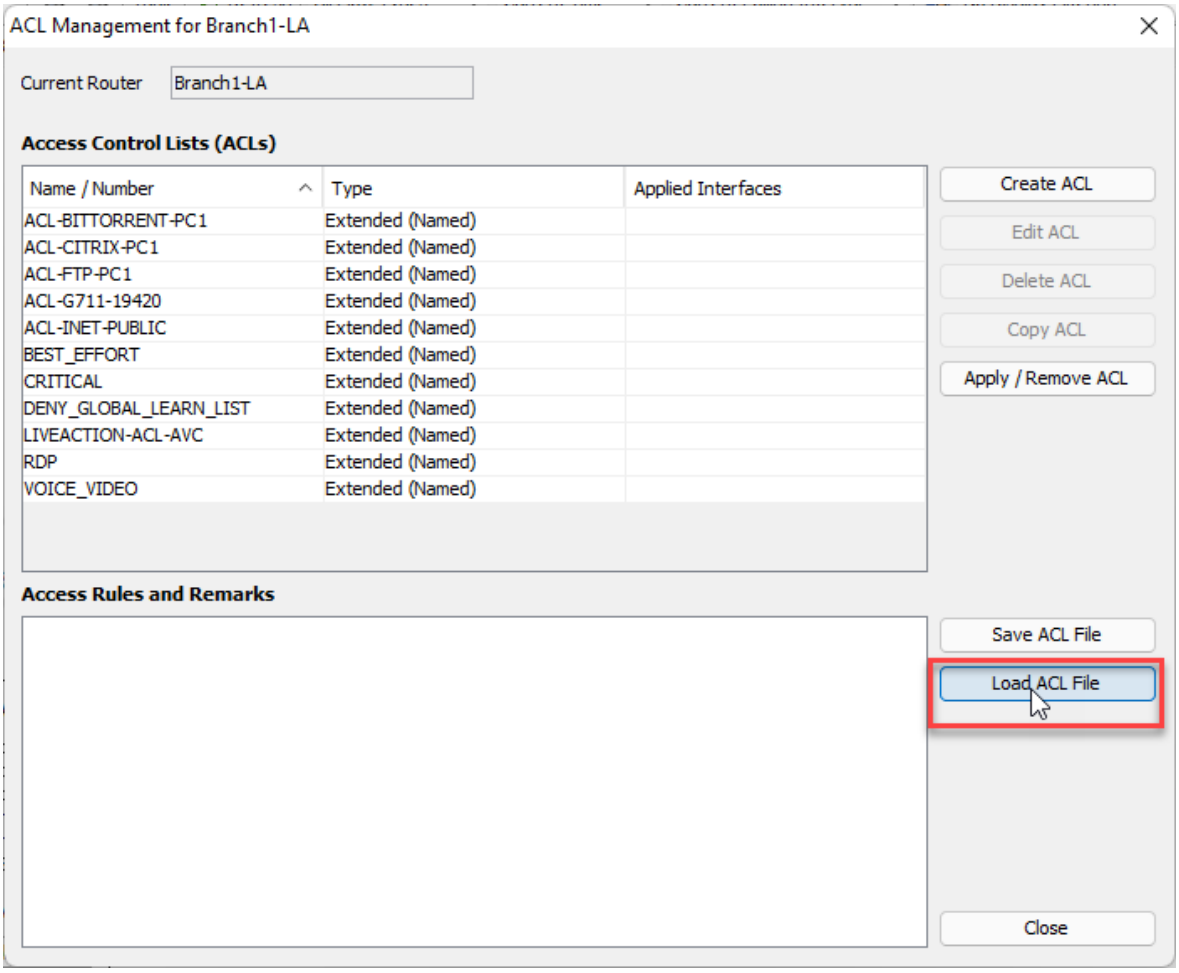


Figure 130

 © Copyright LiveAction 2022

4/8/2022

Select the saved ACL file from above (mine is on Desktop)

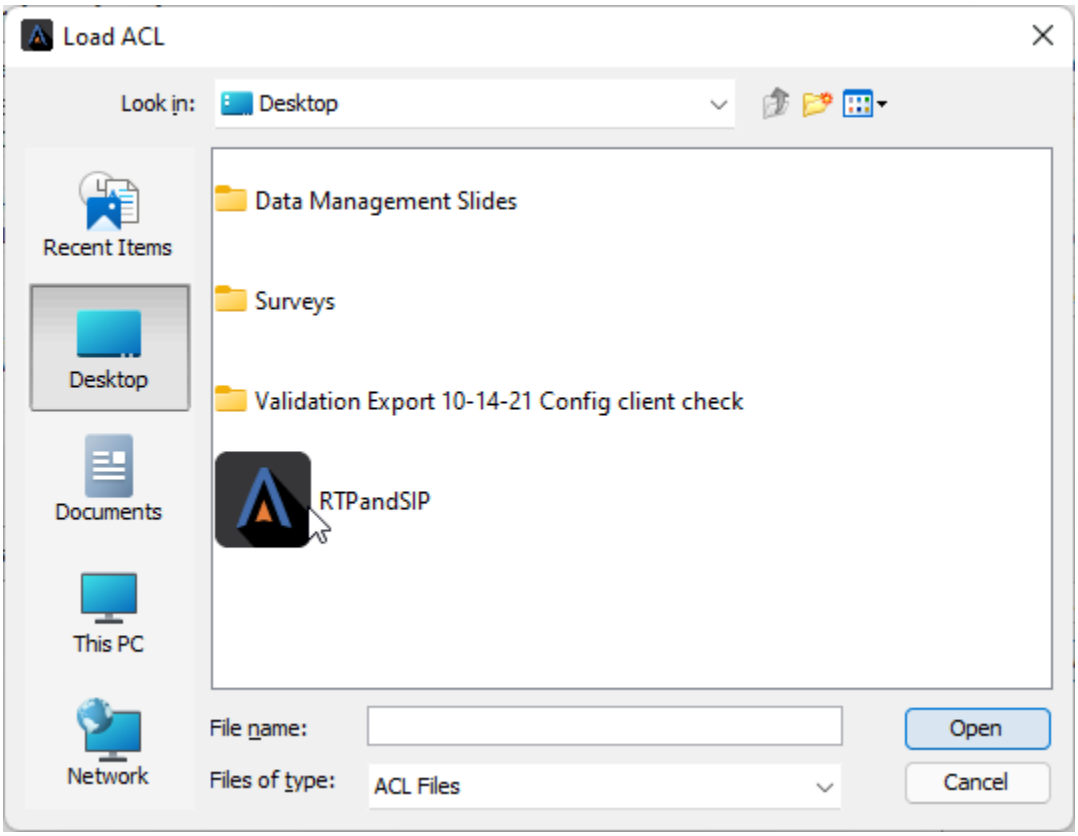


Figure 131

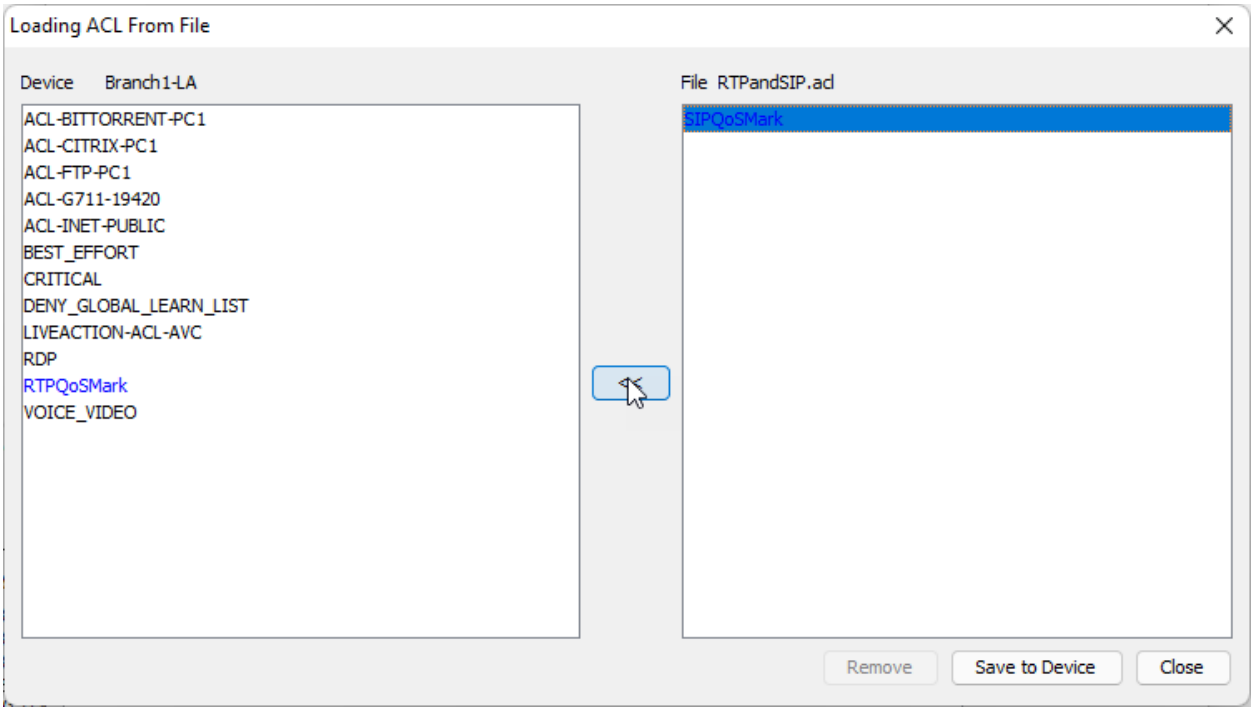


Figure 132

Move the ACLs one-by-one to the left and **Save to Device**

Verify they appear on the ACL list.

© Copyright LiveAction 2022

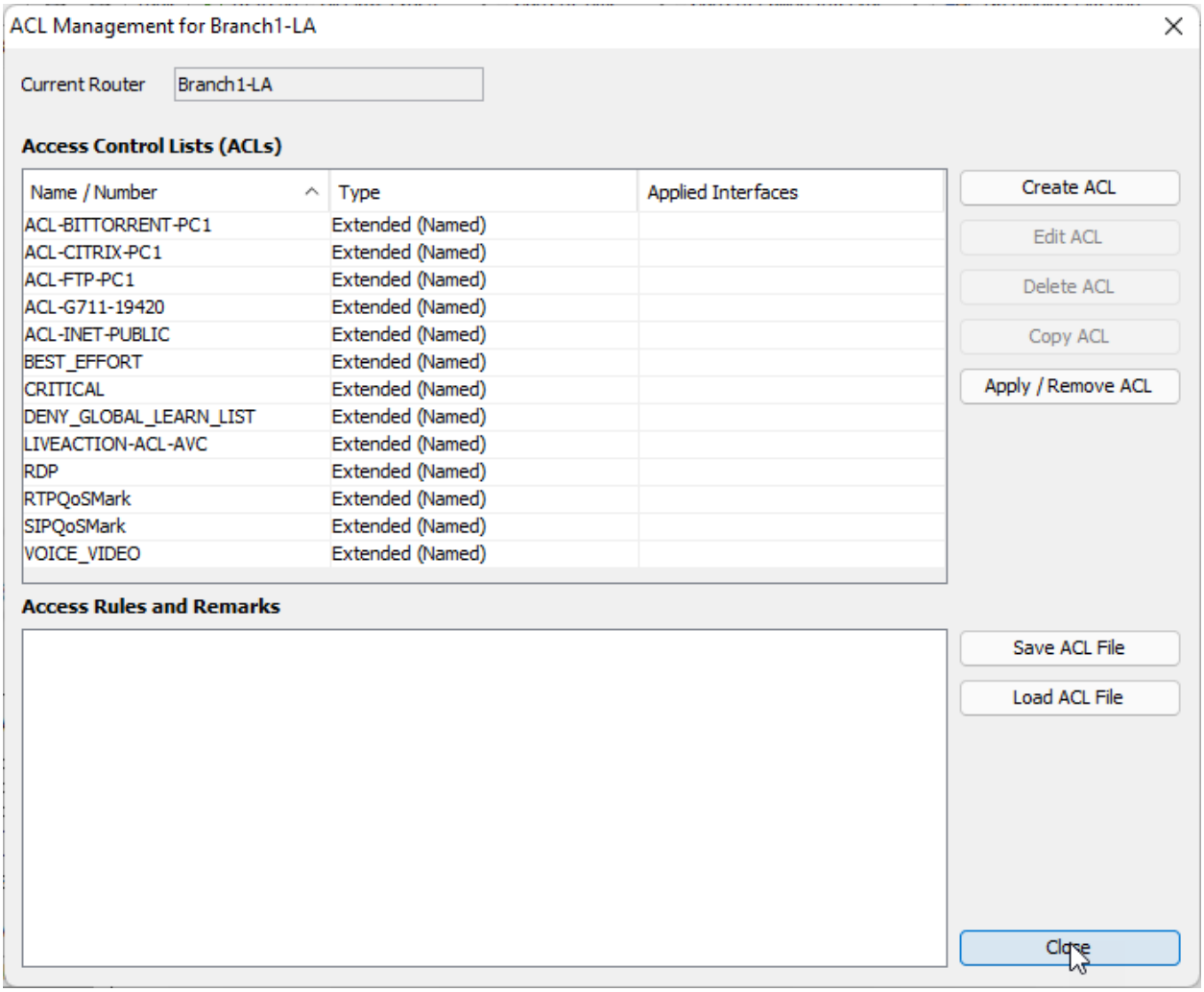


Figure 133

Close the **ACL Management for Branch1-LA** window.

You've now created an Access Control List (ACL) via the LiveNX Console **on both Branch routers**. 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.

 © Copyright LiveAction 2022

Lab 6

Lab 6: Making the Topology Work

© Copyright LiveAction 2022

Lab 6.1: Setting Device Semantics

<u>These Labs uses the Engineering Console exclusively.</u>

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.

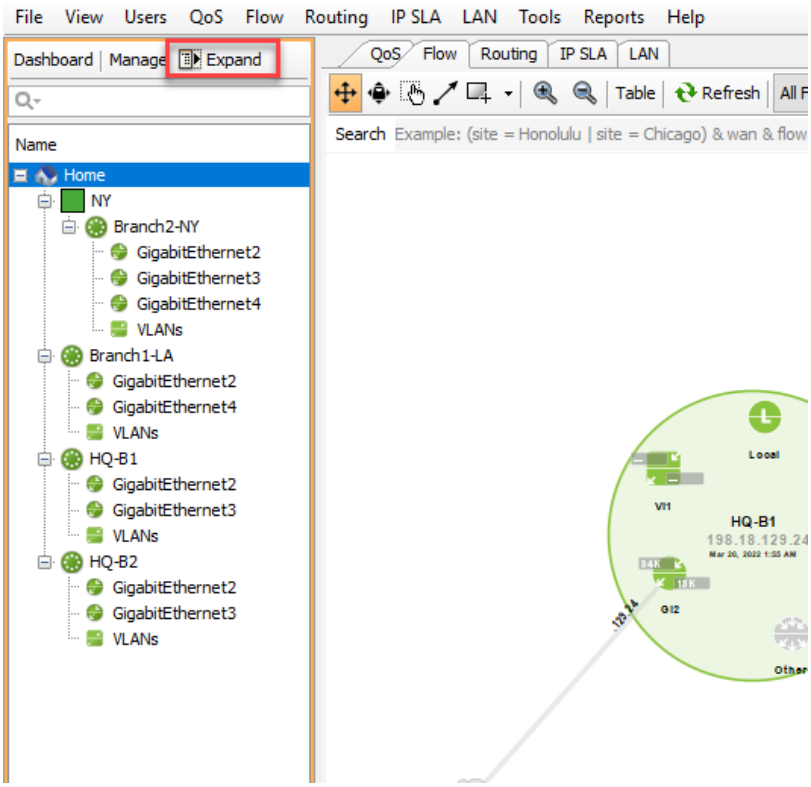


Figure 134

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

 © Copyright LiveAction 2022

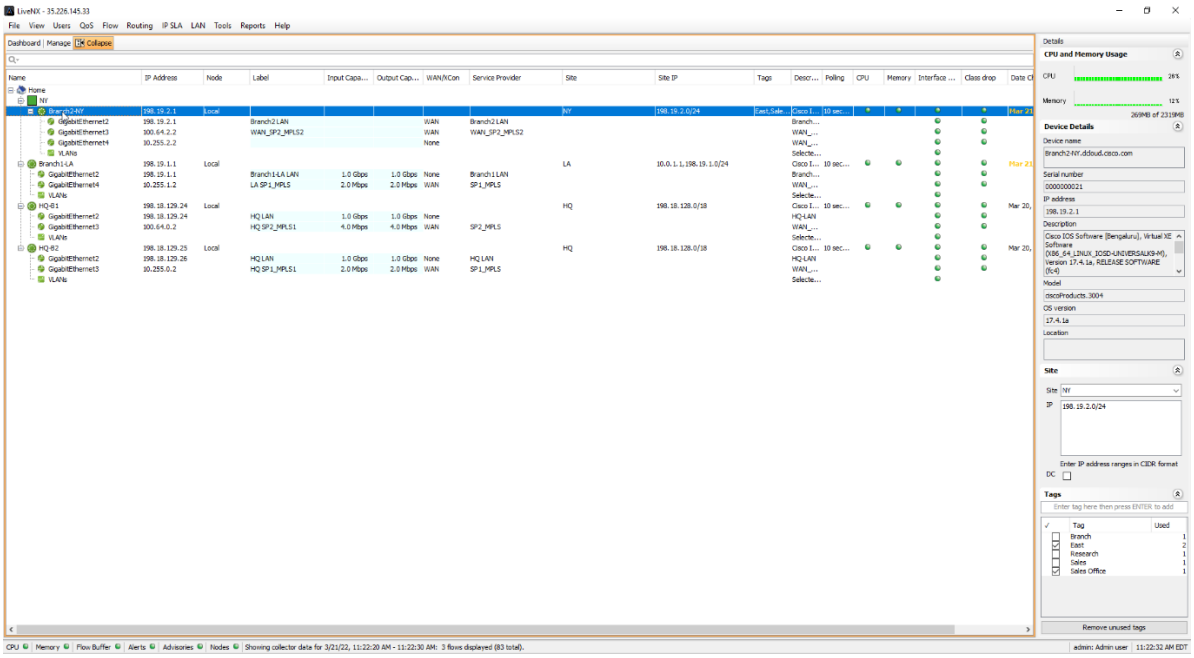


Figure 135

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. Clicking an interface or a device will bring up the Semantic config panel on the right of the screen.

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

Device	Interface	Site	Input Capacity	Output Capacity	WAN	Service Provider
Branch1-LA	GigabitEthernet2	LA			**NONE**	
Branch1-LA	GigabitEthernet3	LA	2000kbps	2000kbps	WAN	SP2_MPLS
Branch1-LA	GigabitEthernet4	LA	2000kbps	2000kbps	WAN	SP1_MPLS
Branch2-NY	GigabitEthernet3	NY	2000kbps	2000kbps	WAN	SP2_MPLS
Branch2-NY	GigabitEthernet4	NY	2000kbps	2000kbps	WAN	SP1_MPLS
HQ-B1	GigabitEthernet3	HQ	2000kbps	2000kbps	WAN	SP2_MPLS
HQ-B2	GigabitEthernet3	HQ	2000kbps	2000kbps	WAN	SP1_MPLS

Add the **Site IP** range to NY Router - **198.19.2.0/24**
Add the **Branch** Tag to LA Router (not one of the interfaces) and add the new tags of **West** and **Engineering**.

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

 © Copyright LiveAction 2022

4/8/2022

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.

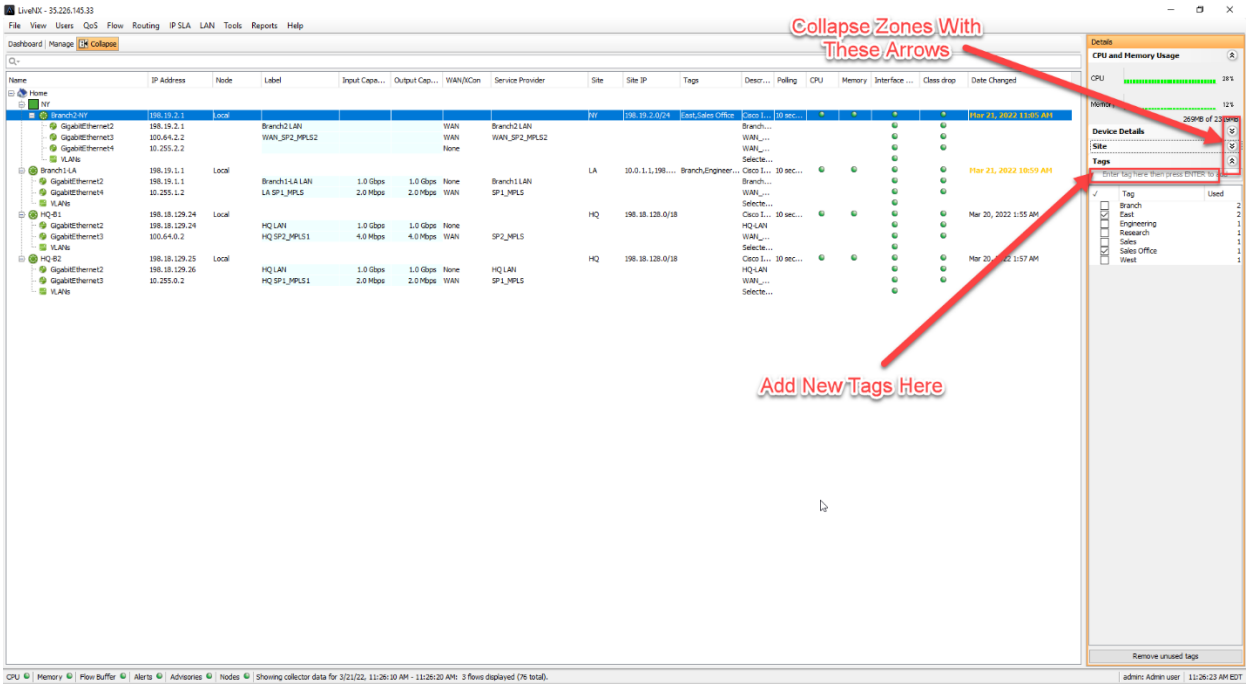


Figure 136

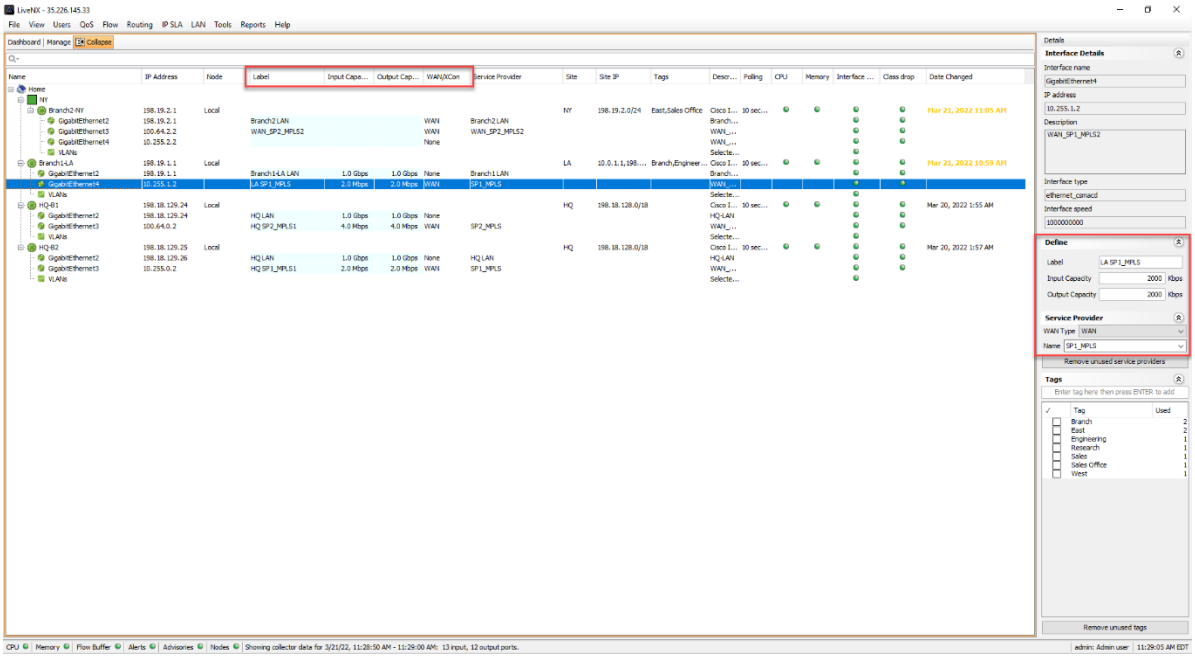


Figure 137

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 if it is not already done:

   a. **Branch1-LA** Device as **LA**

b. **Branch2-NY** Device as **NY**

c. **HQ-B2** Device as **HQ**

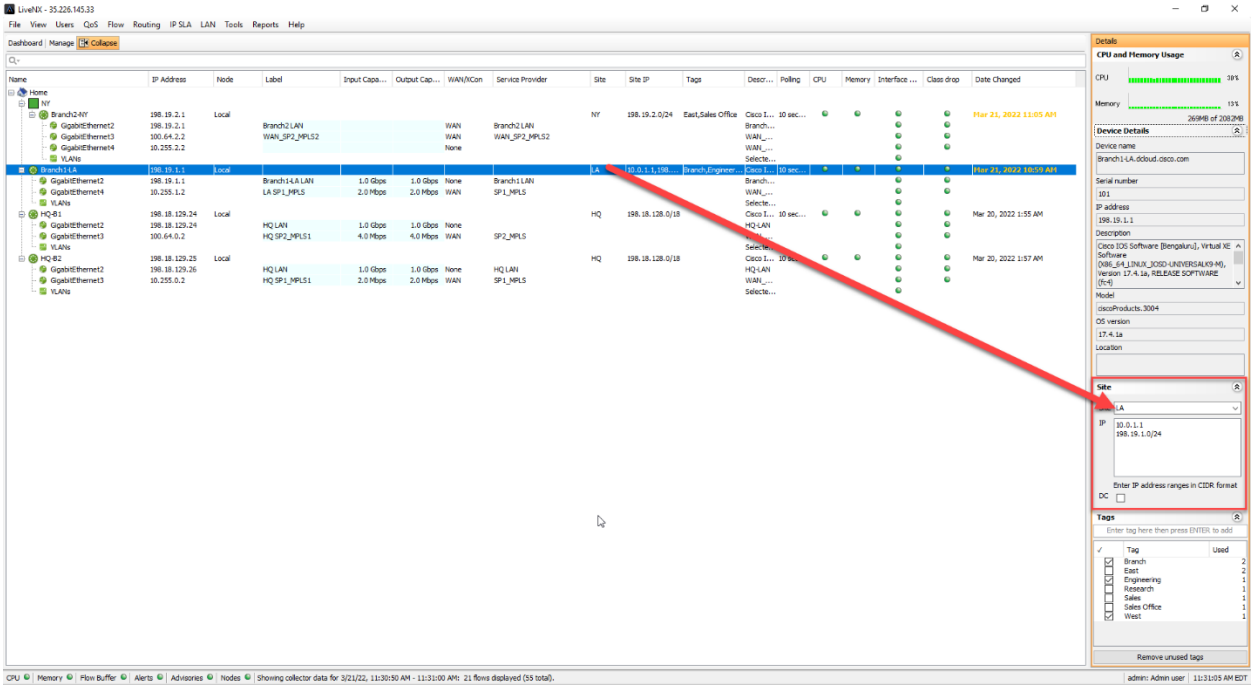


Figure 138

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.

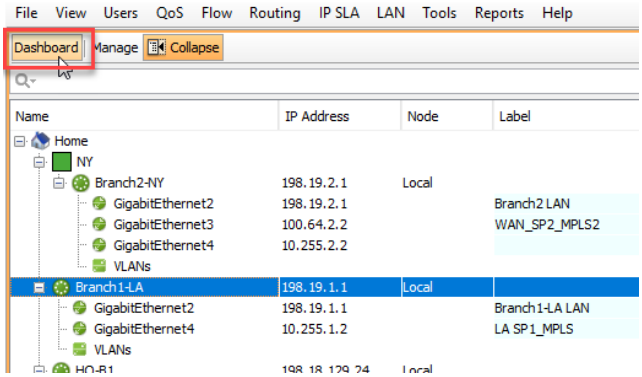


Figure 139

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 **site semantics** correctly.

 © Copyright LiveAction 2022

Site WAN Interface Utilization

Site	Interface L...	Input Capa...	Output Ca...	Input Avg	Input Peak	Output Avg	Output Peak	CPU Avg	CPU Peak	Memory Avg	Memory Pe...
HQ	HQ SP1_MPLS1	2,000	2,000,000	25 %	59 %	0 %	0 %	31 %	32 %	12 %	12 %
HQ	HQ SP2_MPLS1	4,000	4,000,000	0 %	0 %	0 %	0 %	29 %	30 %	13 %	13 %
LA	LA SP1_MPLS	2,000	2,000,000	18 %	29 %	0 %	0 %	30 %	32 %	13 %	13 %
NY	Branch2 LAN							27 %	29 %	12 %	12 %
NY	WAN_SP2_MP...							27 %	29 %	12 %	12 %

Figure 140

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.

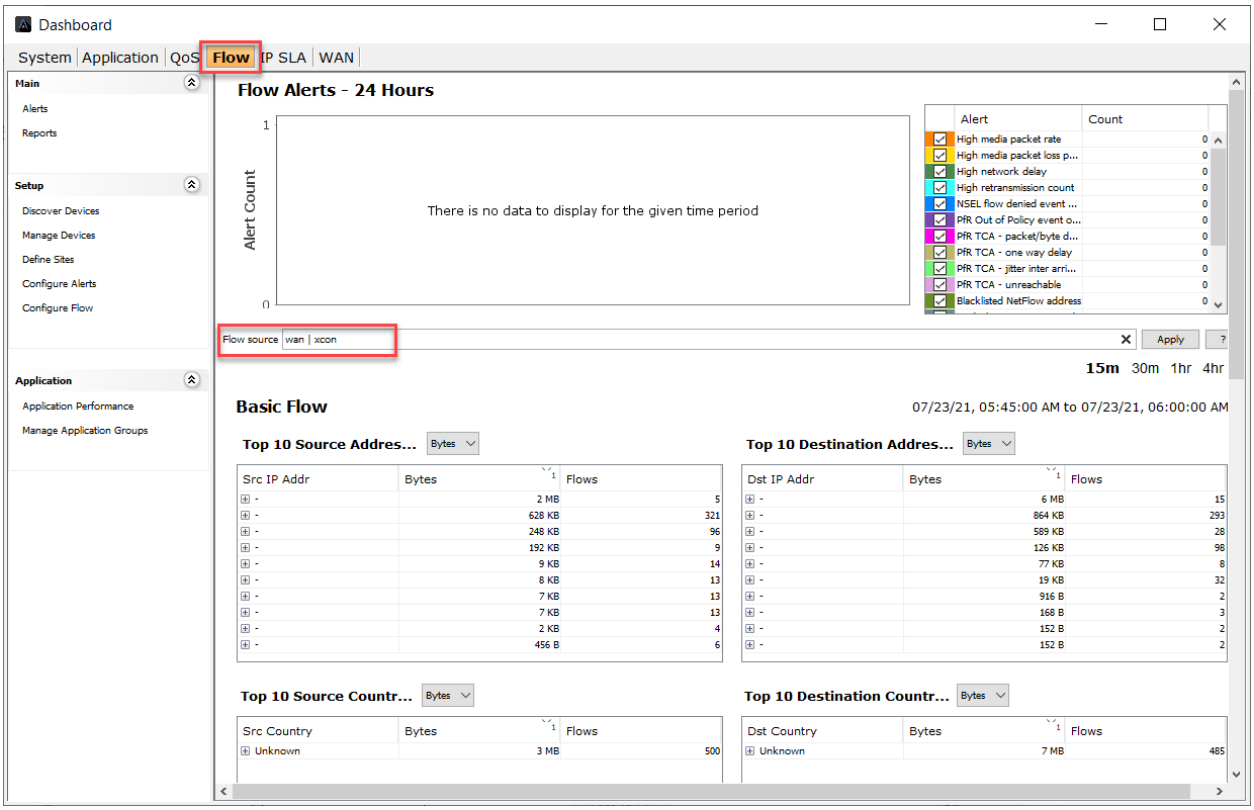


Figure 141

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

 © Copyright LiveAction 2022

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.

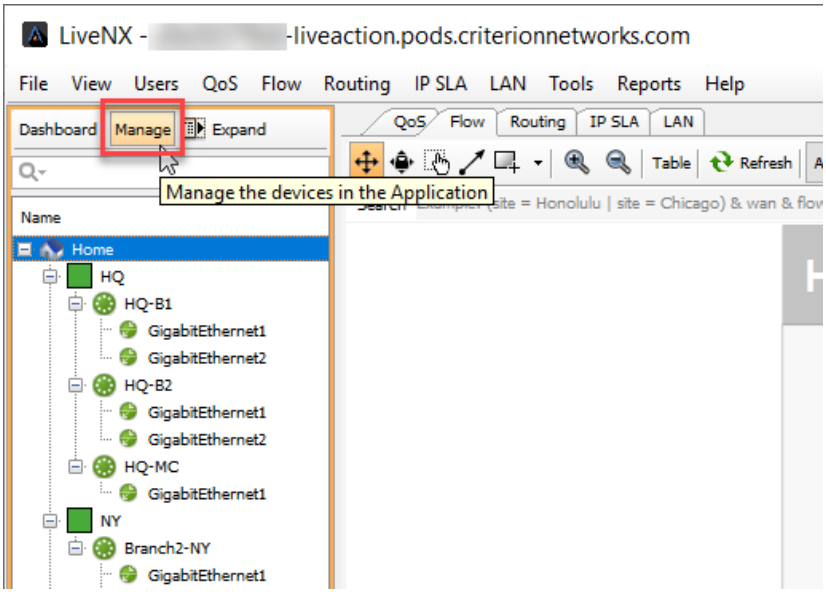


Figure 142

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**"

 © Copyright LiveAction 2022

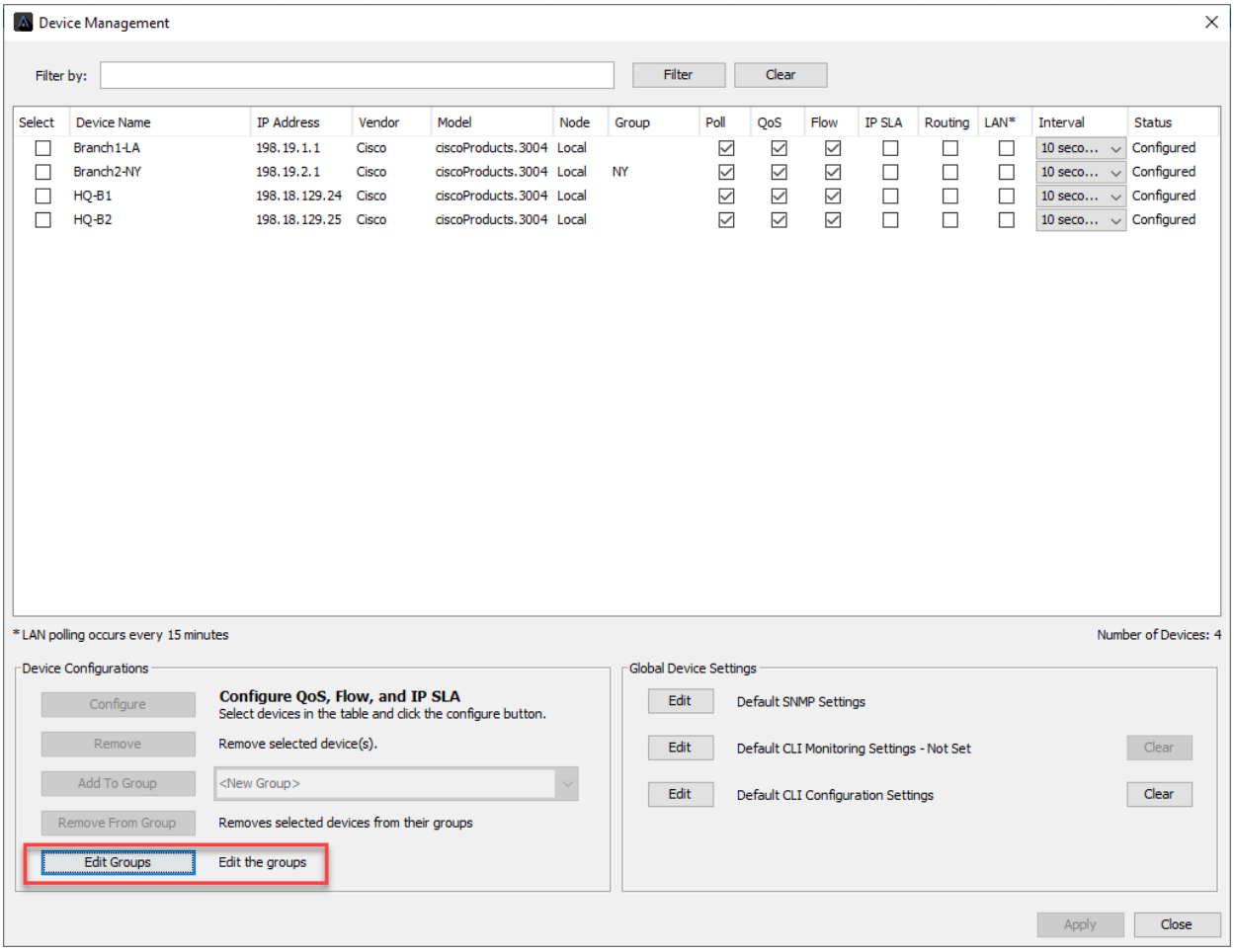


Figure 143

As we have only configured NY to be a group, we need to create **Groups** for the other sites in the Engineering Console (This can be achieved in the WebUI, but we've already seen how that's done)

3. Click **Add** to create a new group.

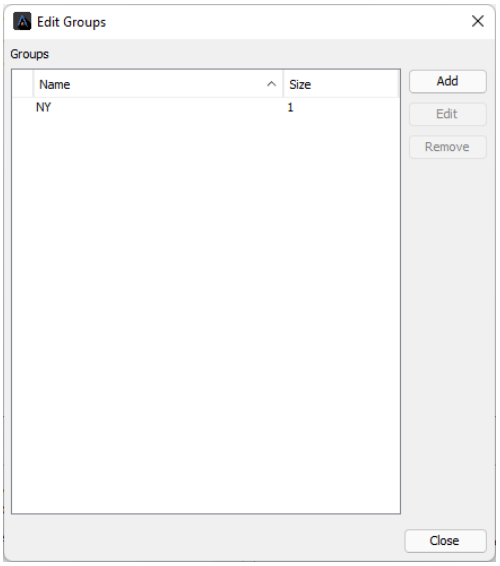


Figure 144

 © Copyright LiveAction 2022

4. Enter **LA** in the Name field.
5. Select **Branch1-LA** from the **All Other Devices** list
6. click the green **Right** arrow (or double click the device)
7. Click **Add**.
8. Repeat the steps above to create the **HQ** group.

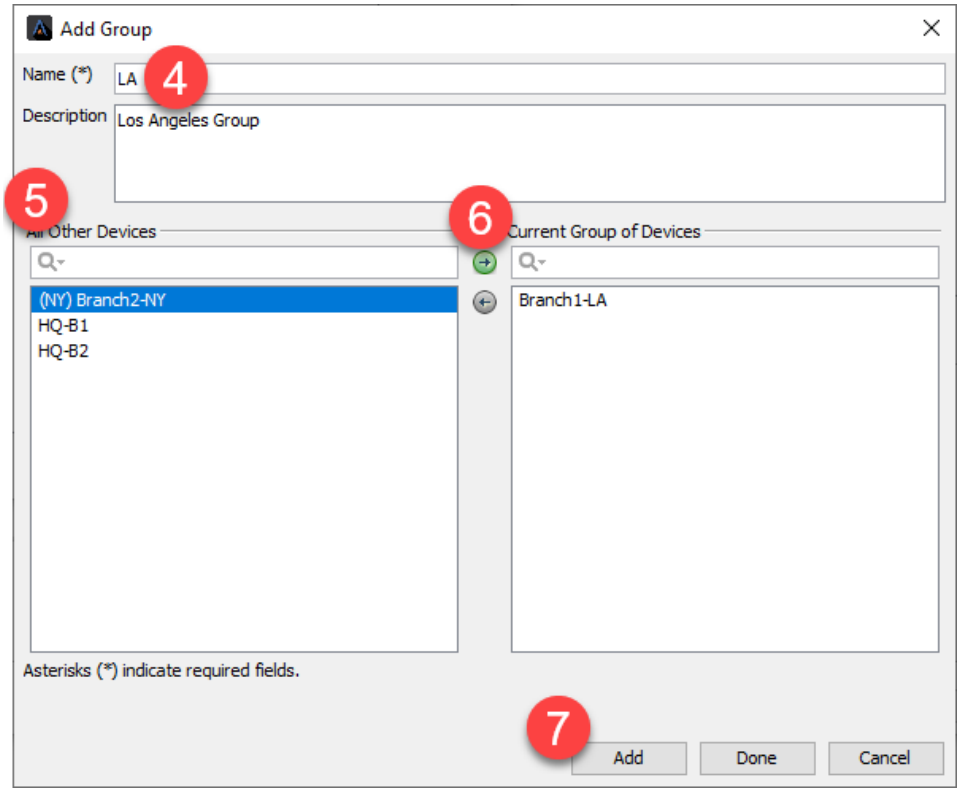


Figure 145

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.

 © Copyright LiveAction 2022

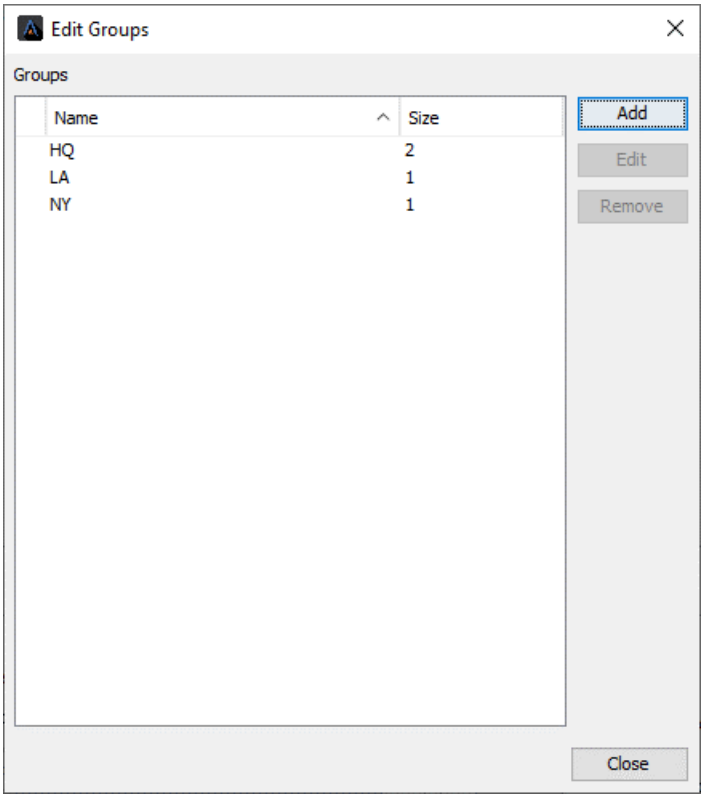


Figure 146

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.

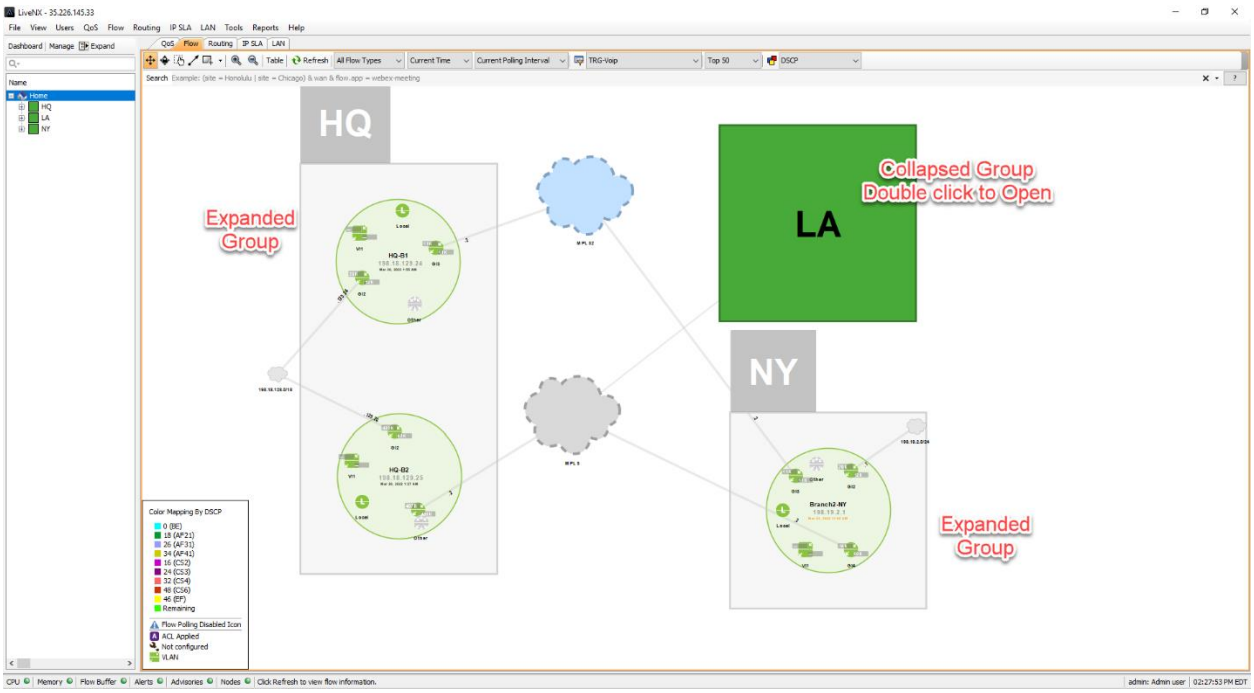


Figure 147

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 flex-search string: **flow.dstip=198.19.1.101**
3. Click on the **Flow line** that appears 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**

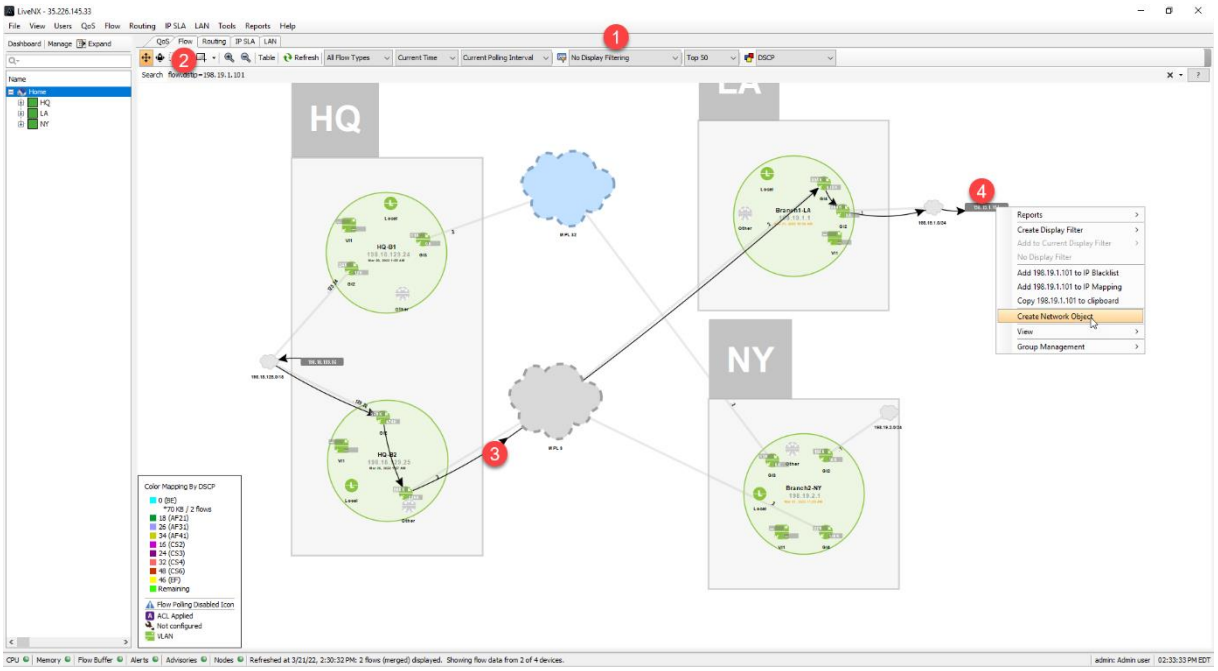


Figure 148

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

 © Copyright LiveAction 2022

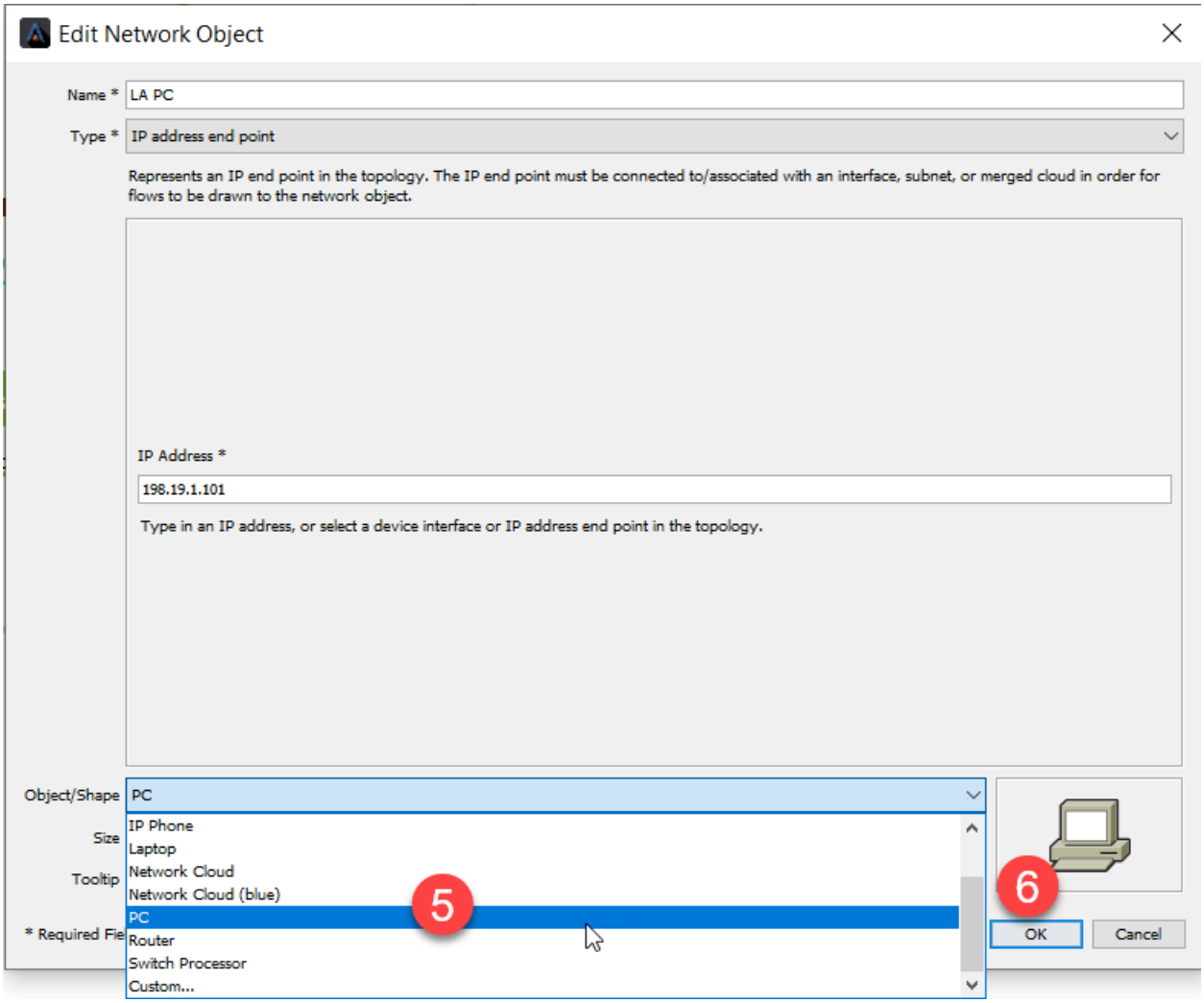


Figure 149

7. Click Refresh.

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

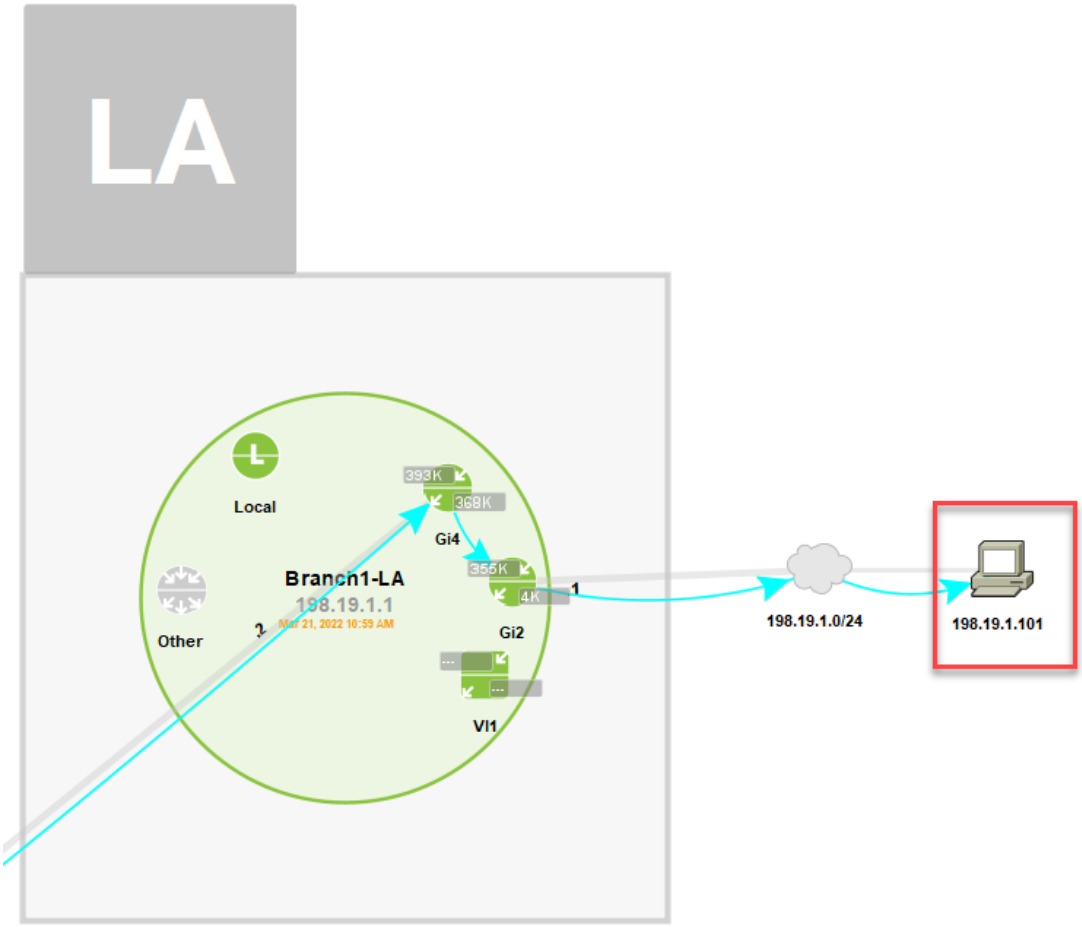


Figure 150

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**

 © Copyright LiveAction 2022

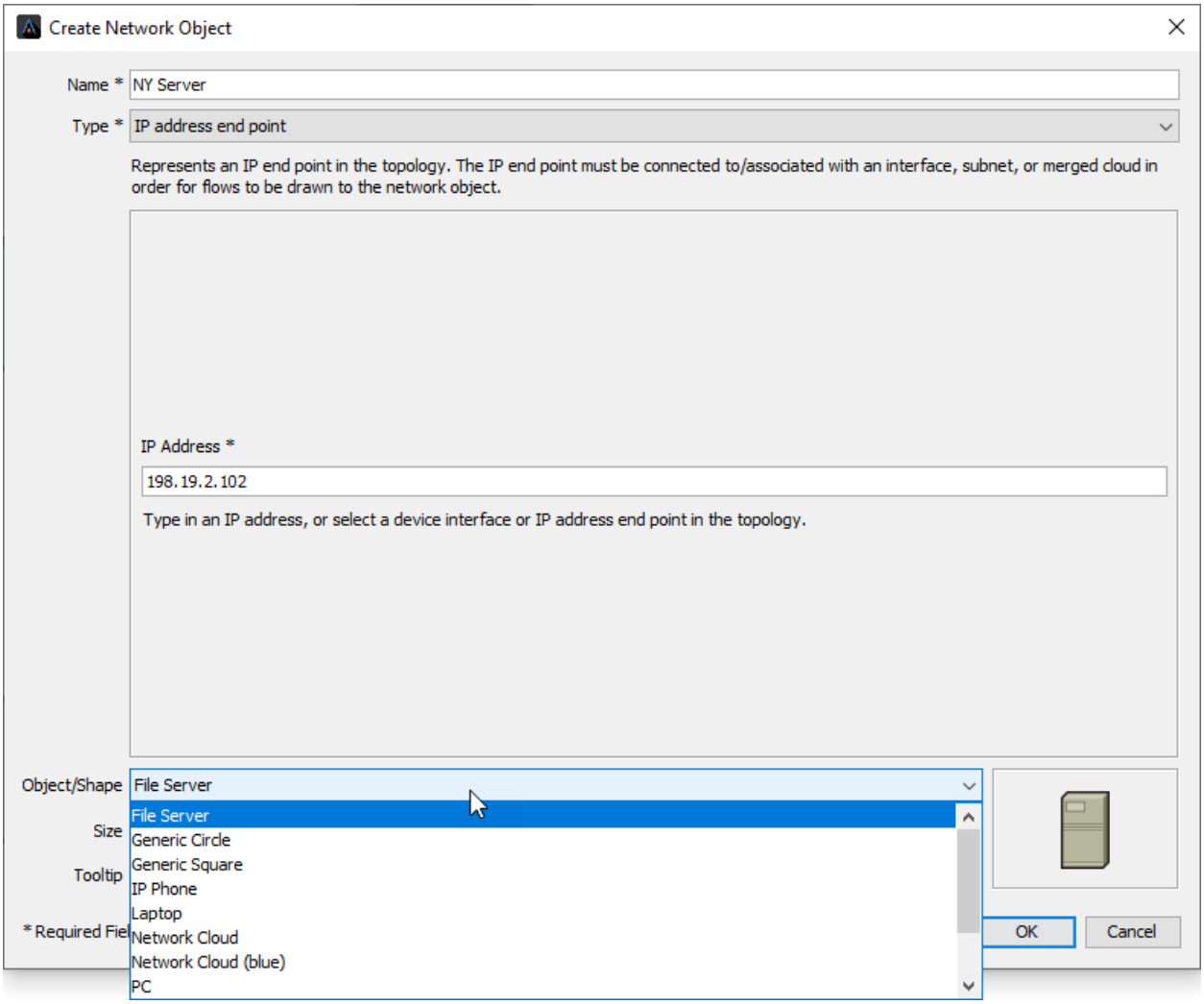


Figure 151

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.

 © Copyright LiveAction 2022

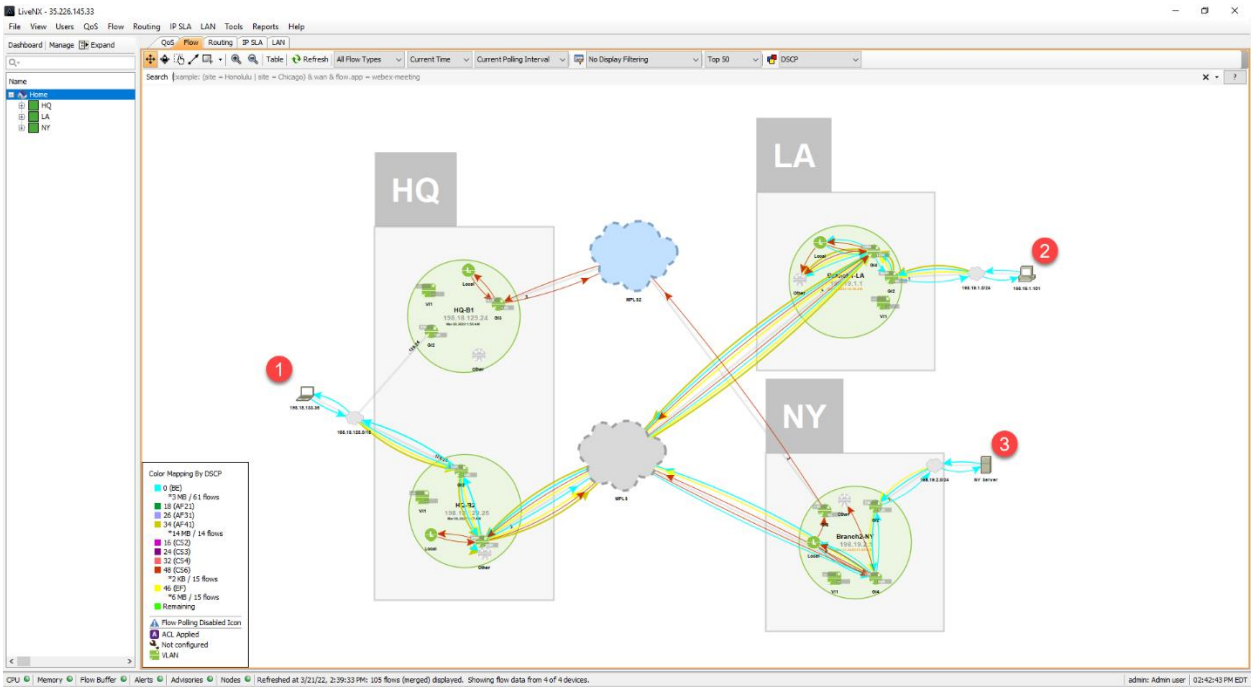


Figure 152

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**.

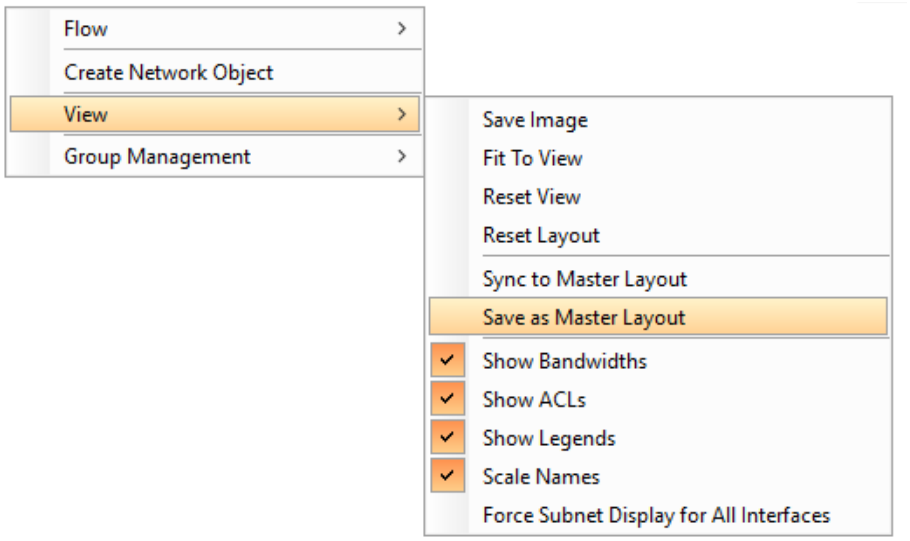


Figure 153

 © Copyright LiveAction 2022

Lab 7

Lab 7: Dashboards & Reports

 © Copyright LiveAction 2022

Lab 7.1: The Dashboard

<u>This Lab uses the Engineering Console.</u>

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.

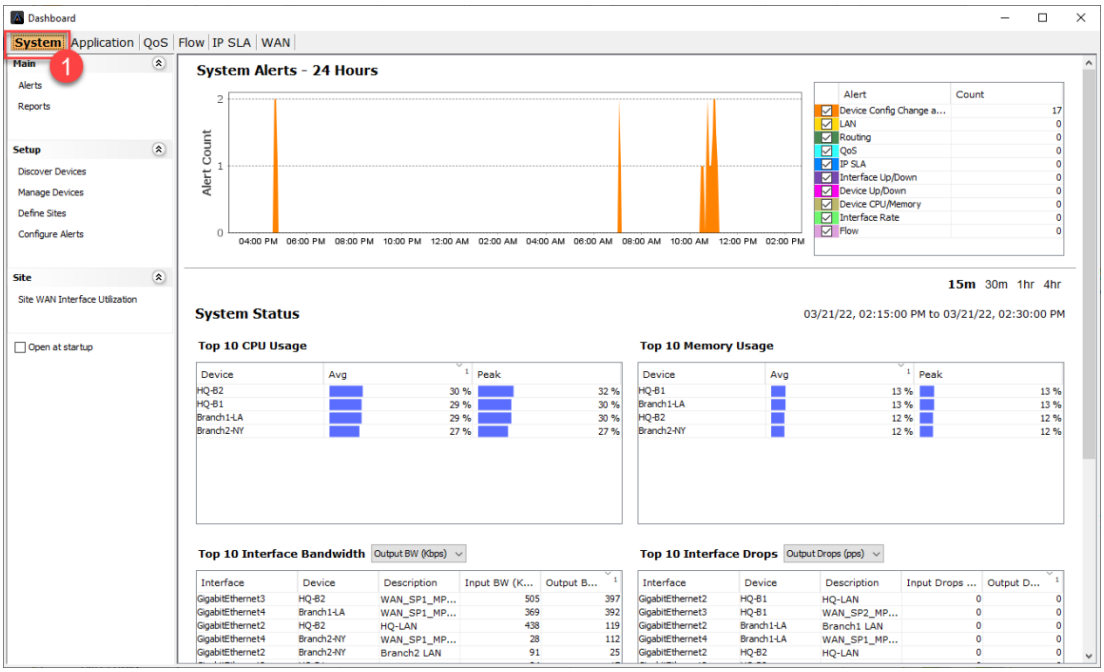


Figure 154

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.

 © Copyright LiveAction 2022

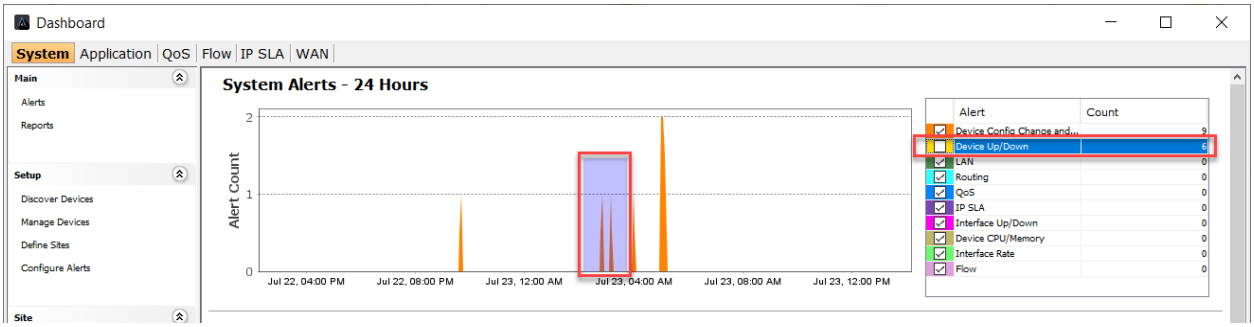


Figure 155

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 results you see may be different. What you see depends upon specific traffic being present at the specific time you are viewing. The *process* is important here… not the trace!

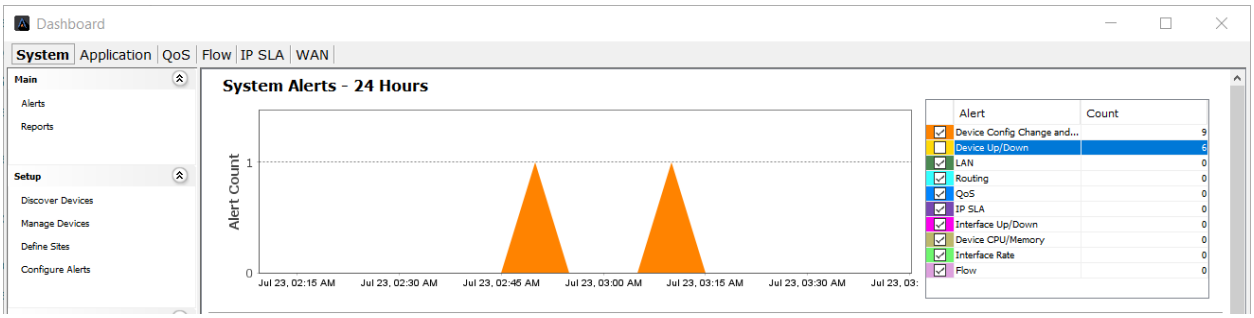


Figure 156

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

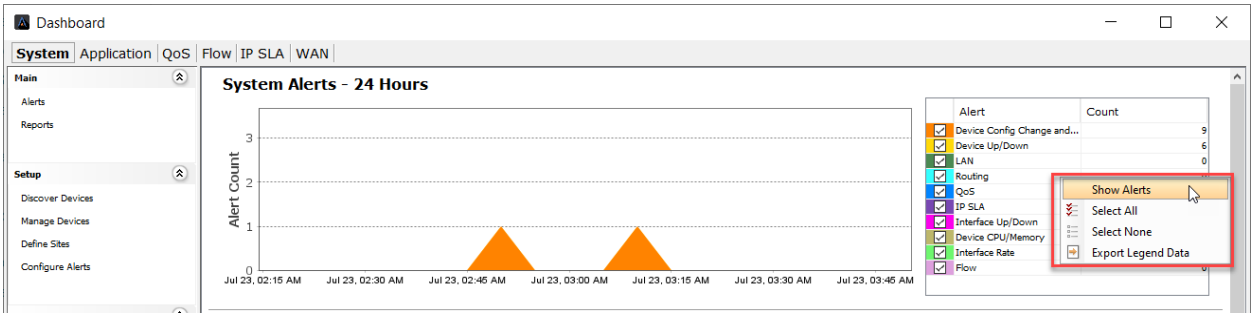


Figure 157

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

 © Copyright LiveAction 2022

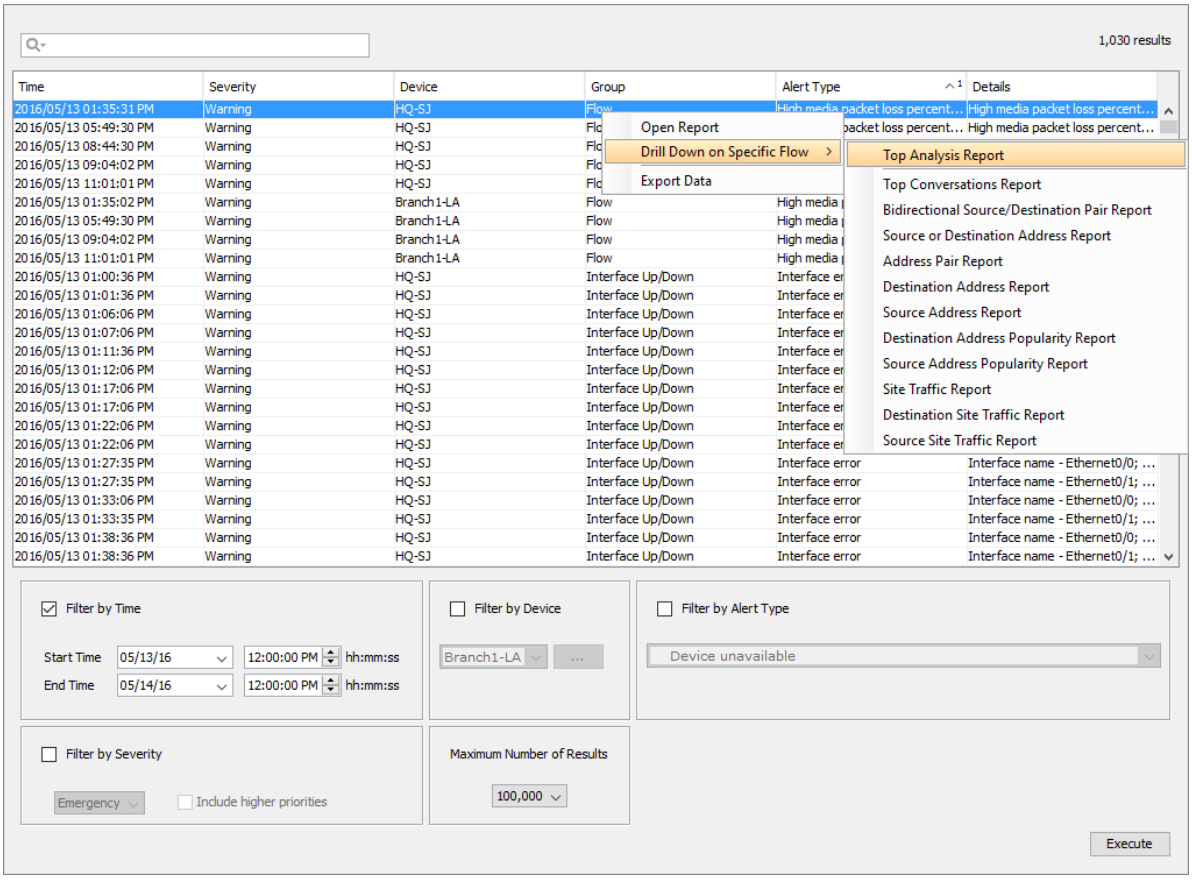


Figure 158

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.

 © Copyright LiveAction 2022

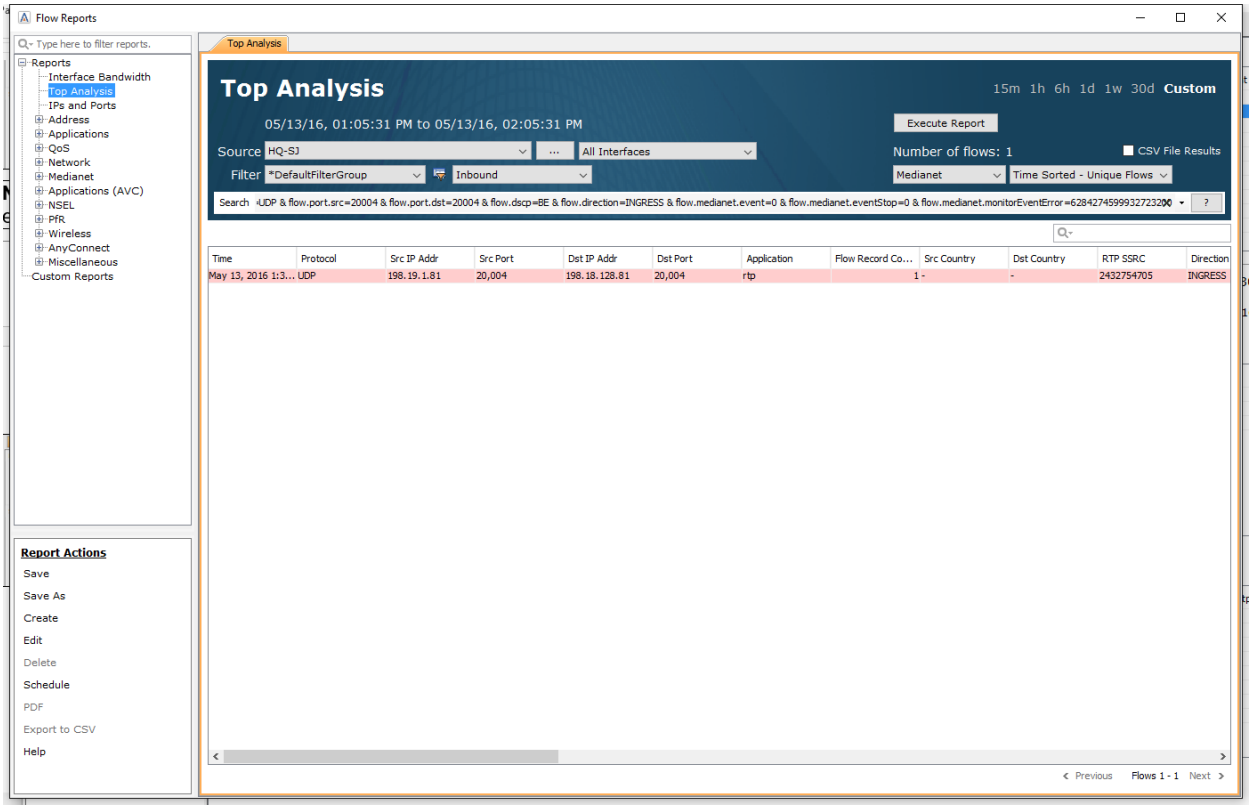


Figure 159

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.

 © Copyright LiveAction 2022

Lab 7.2: Viewing Reports

<u>This Lab uses the WebUI.</u>

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.

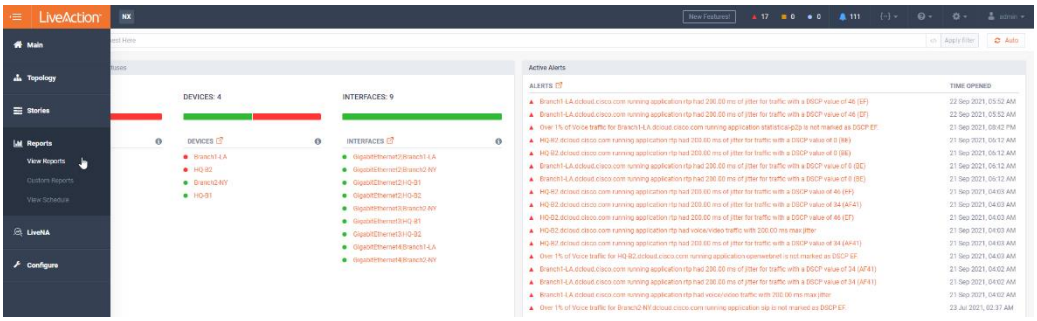


Figure 160

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.

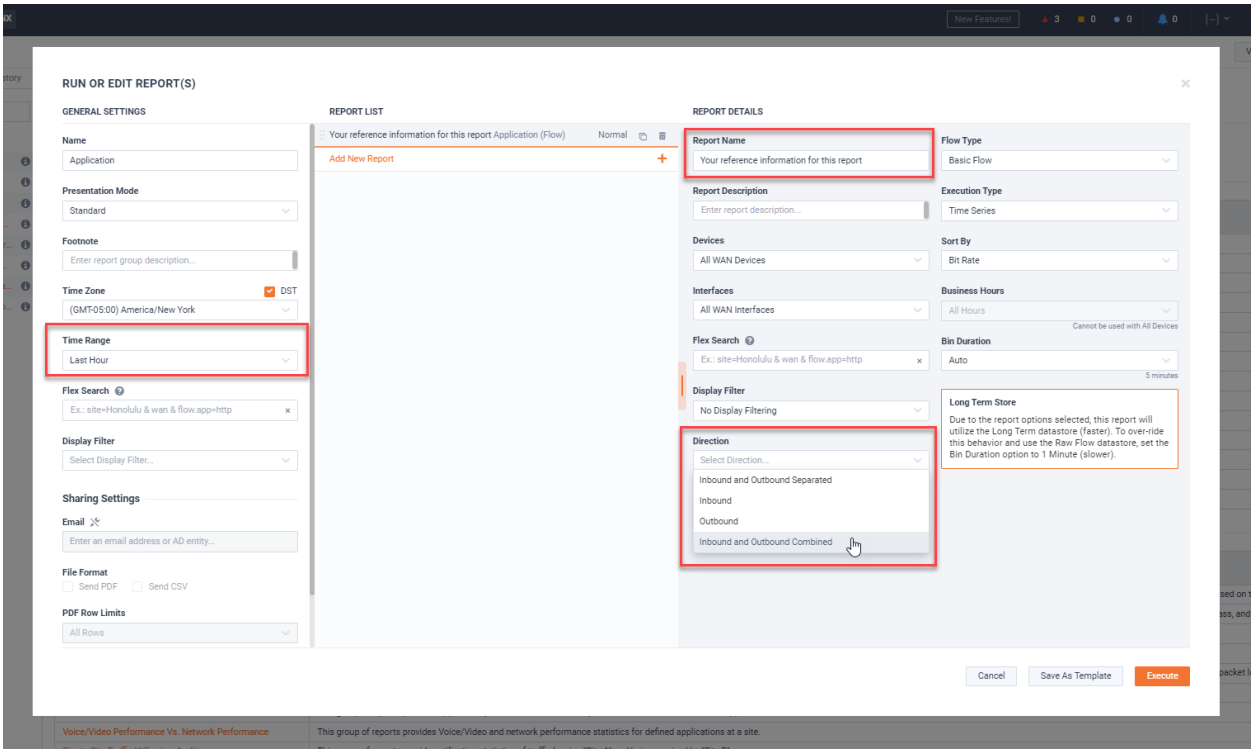


Figure 161

 © Copyright LiveAction 2022

6. Click **Execute**.

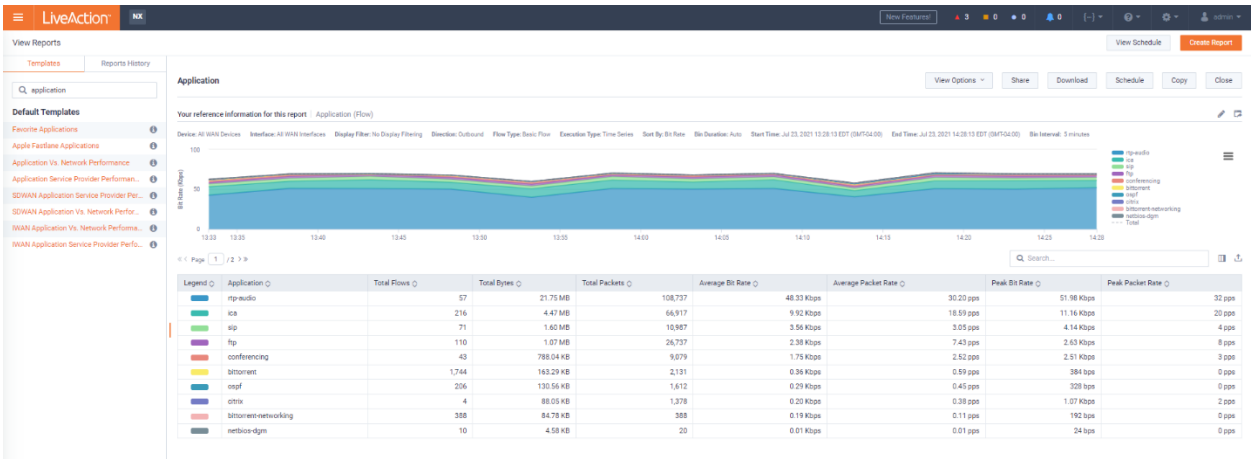


Figure 162

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.

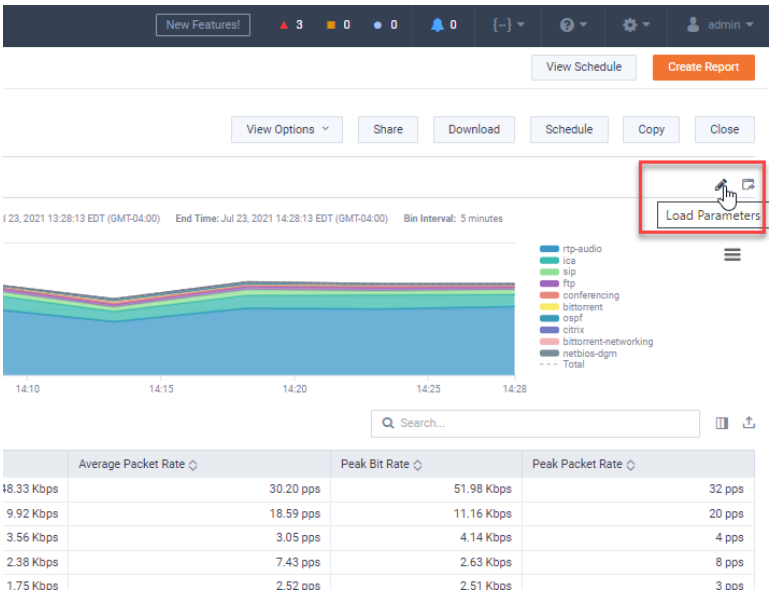


Figure 163

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.

 © Copyright LiveAction 2022

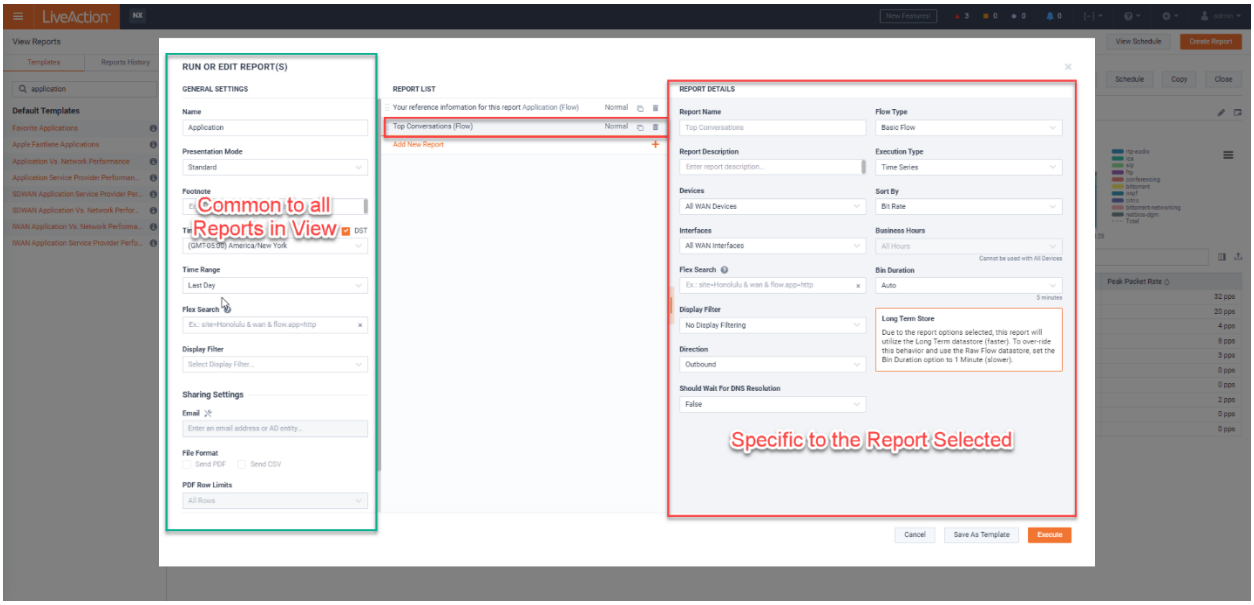


Figure 164

4. Click **Execute**.

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

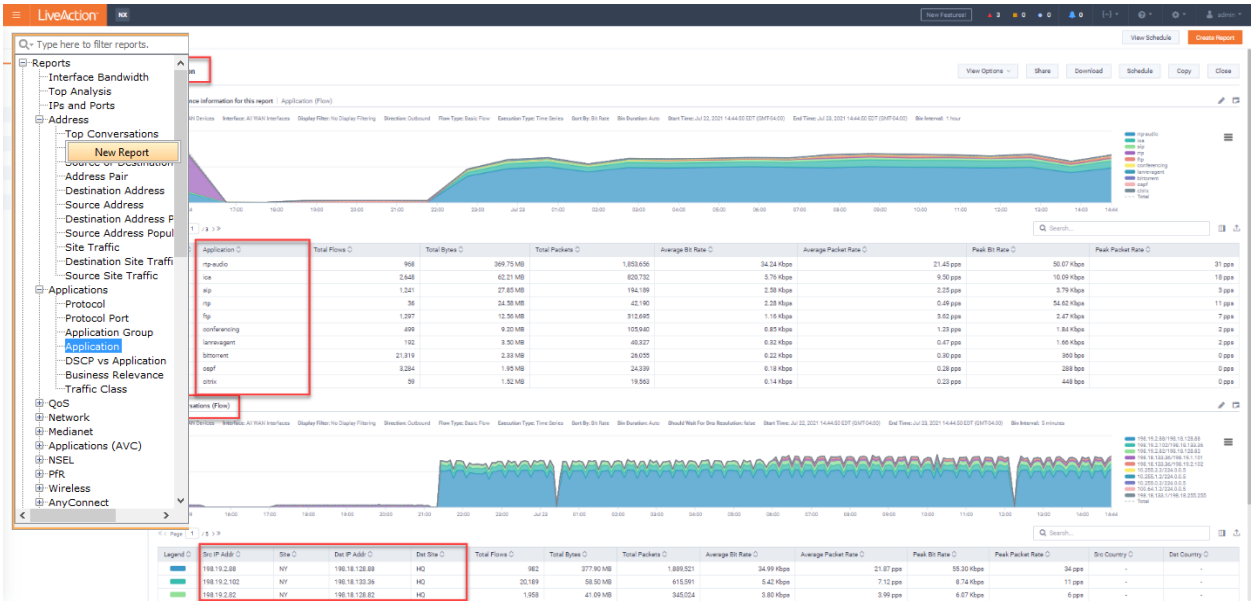


Figure 165

This **Top Conversations** report has been appended to the **Applications** report. in the selected time-range 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**.

 © Copyright LiveAction 2022

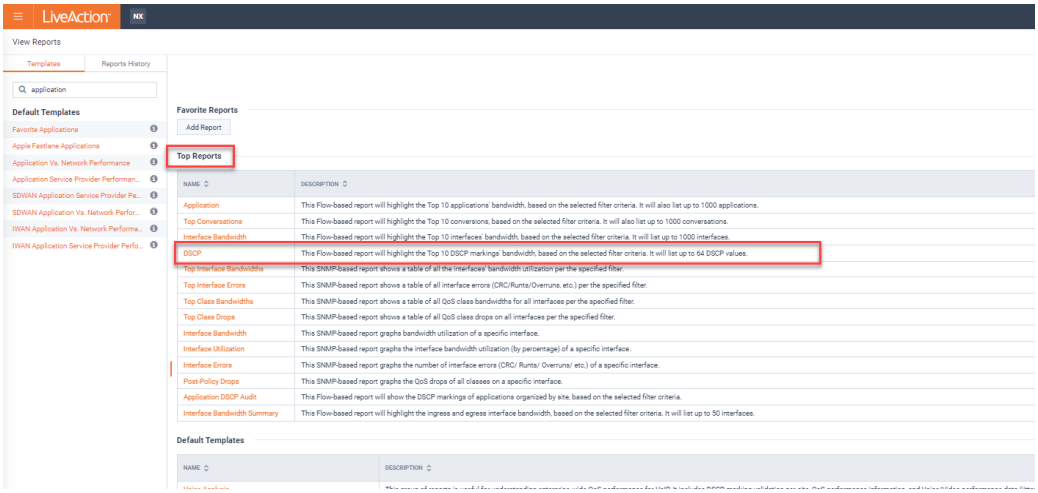


Figure 166

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

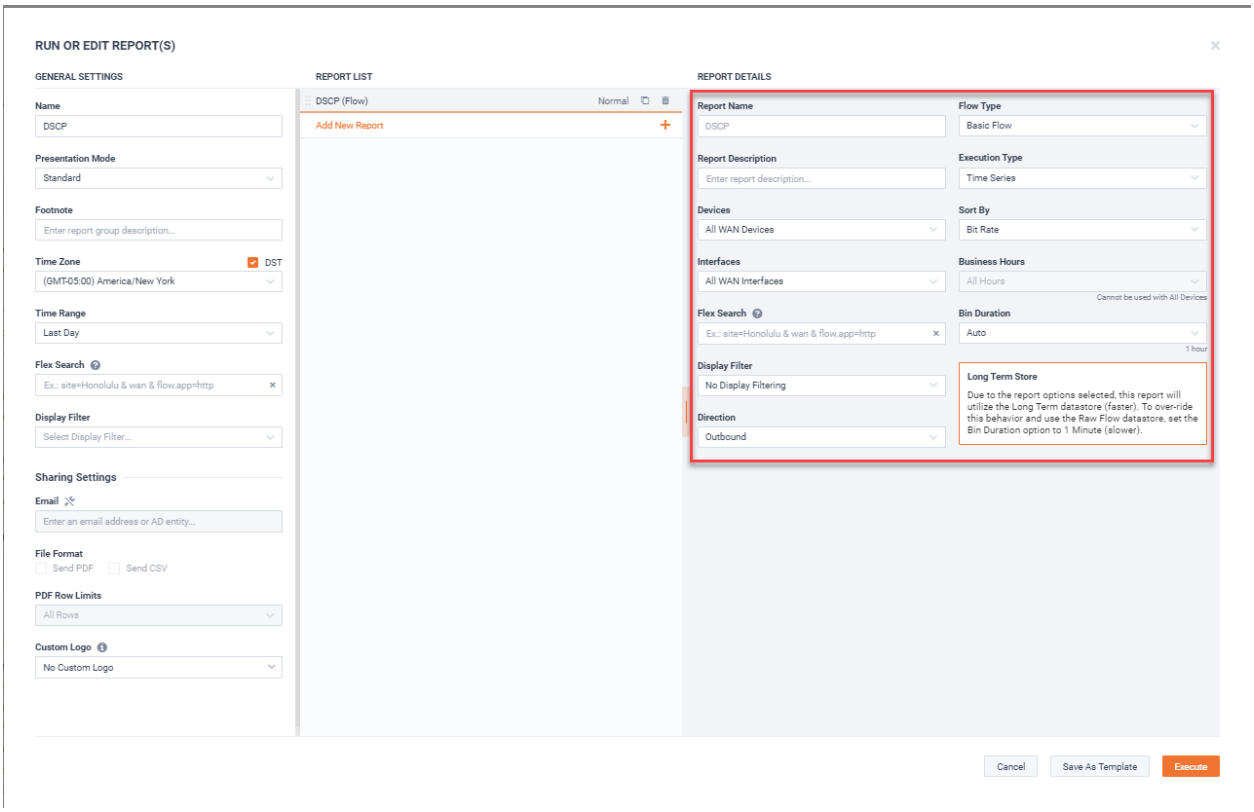


Figure 167

4. Click **Execute**.

 © Copyright LiveAction 2022

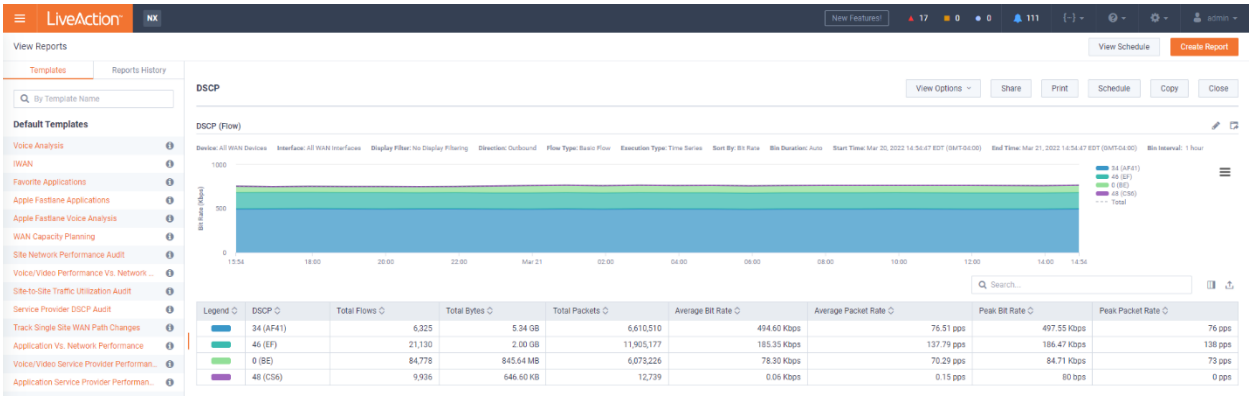


Figure 168

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

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

Bandwidth by Flow Type

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

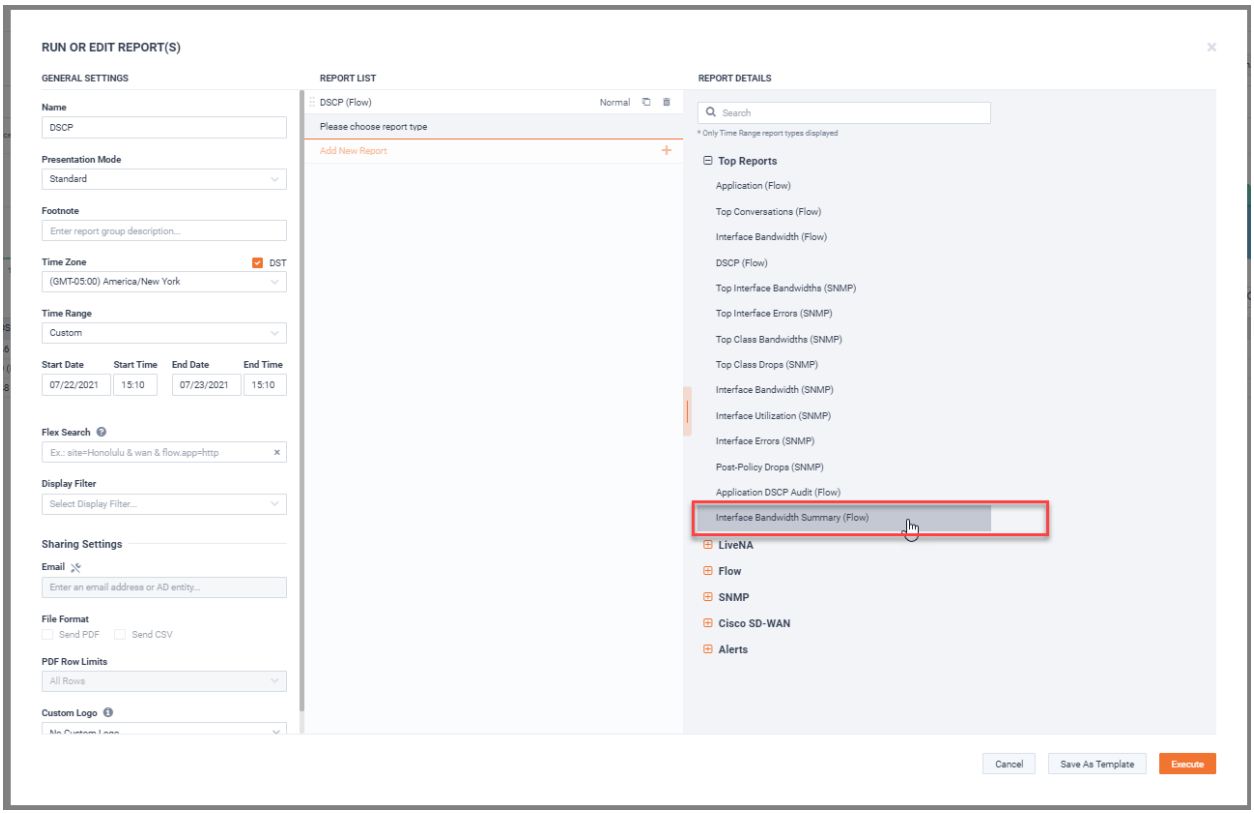


Figure 169

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

 © Copyright LiveAction 2022

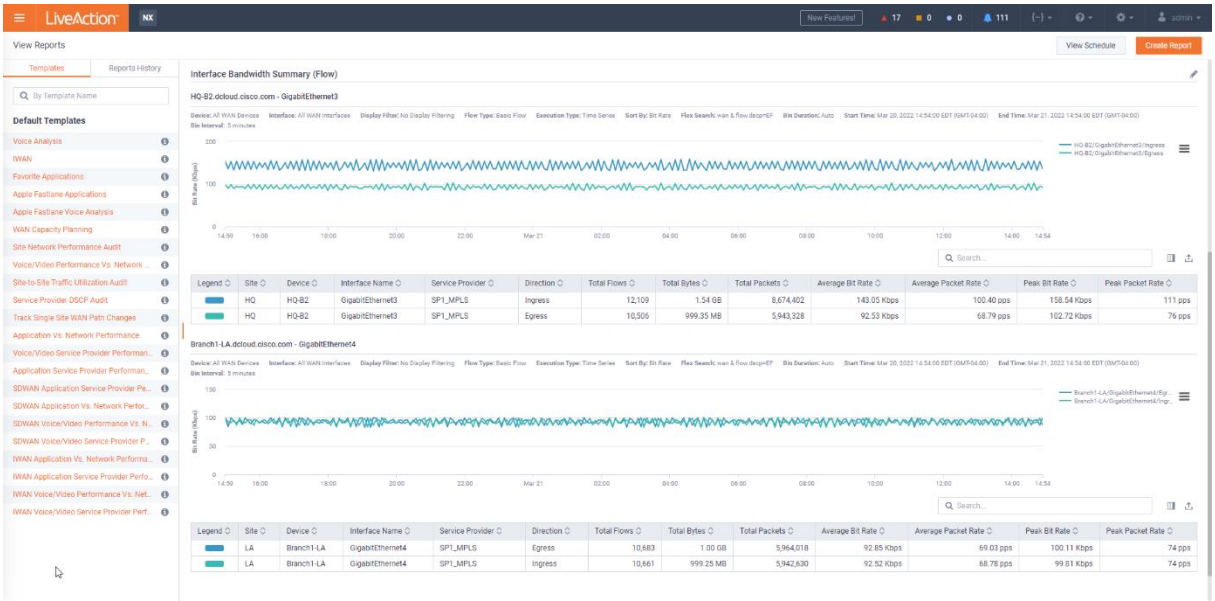


Figure 170

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.

 © Copyright LiveAction 2022

Lab 7.3: Create a Custom Report

<u>This Lab uses the WebUI.</u>

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

Lab Steps:

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

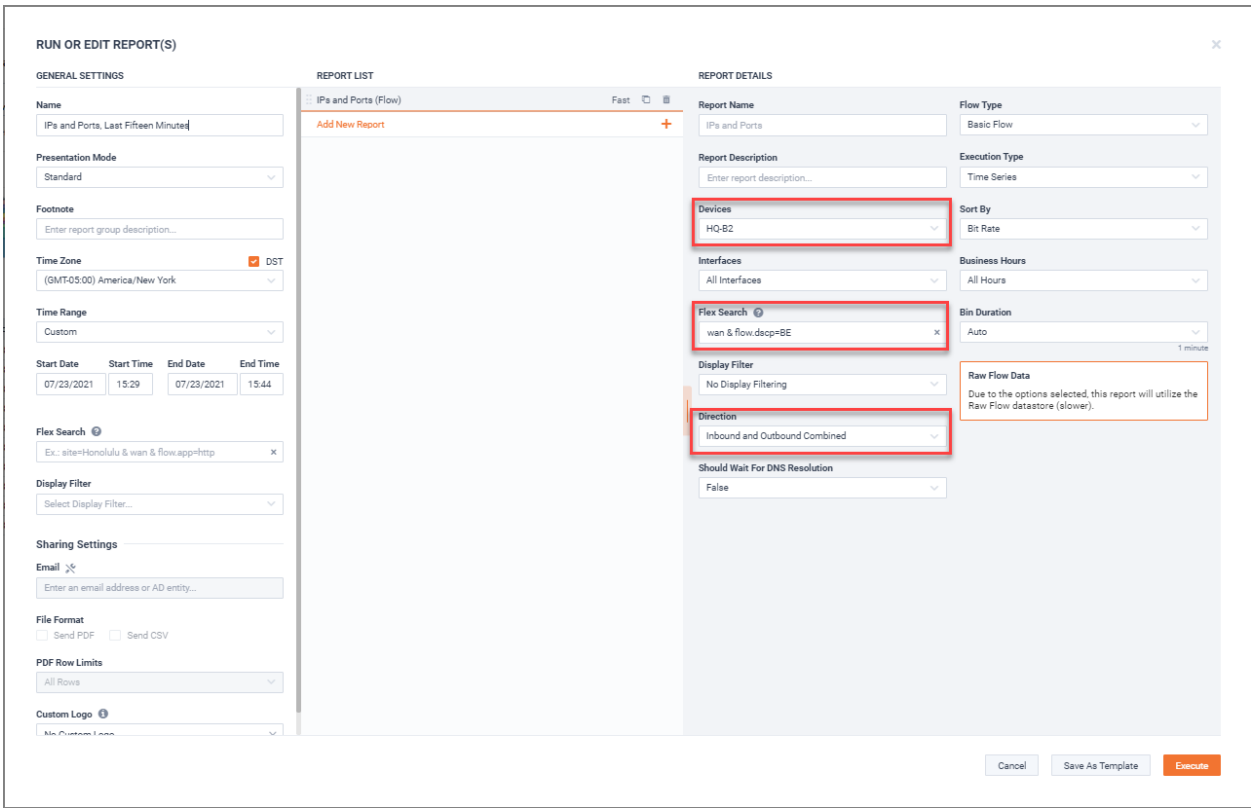


Figure 171

 © Copyright LiveAction 2022

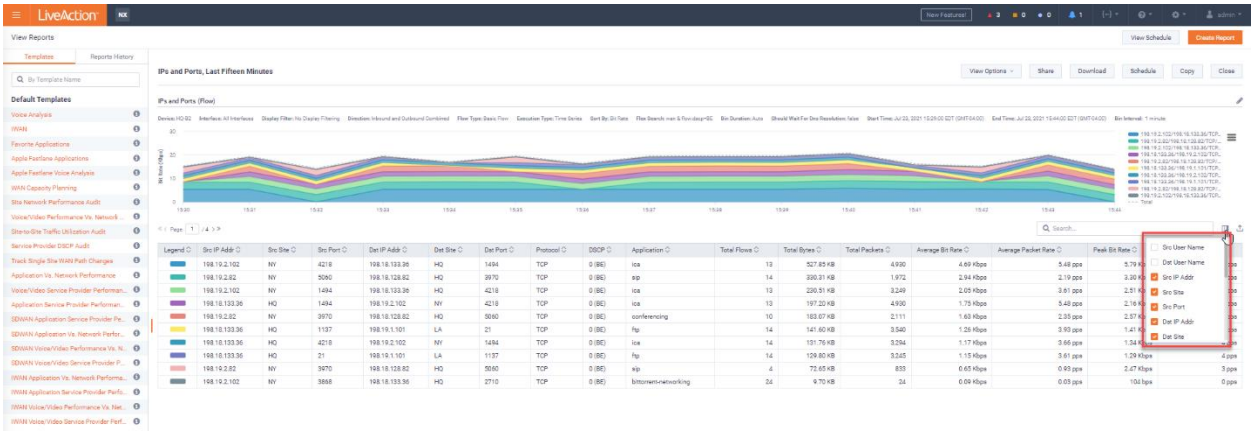


Figure 172

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**.

 © Copyright LiveAction 2022

Lab 8

Lab 8: QoS

© Copyright LiveAction 2022

Lab 8.1: QoS Marking Policy

<u>These Labs uses the Engineering Console exclusively.</u>

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.

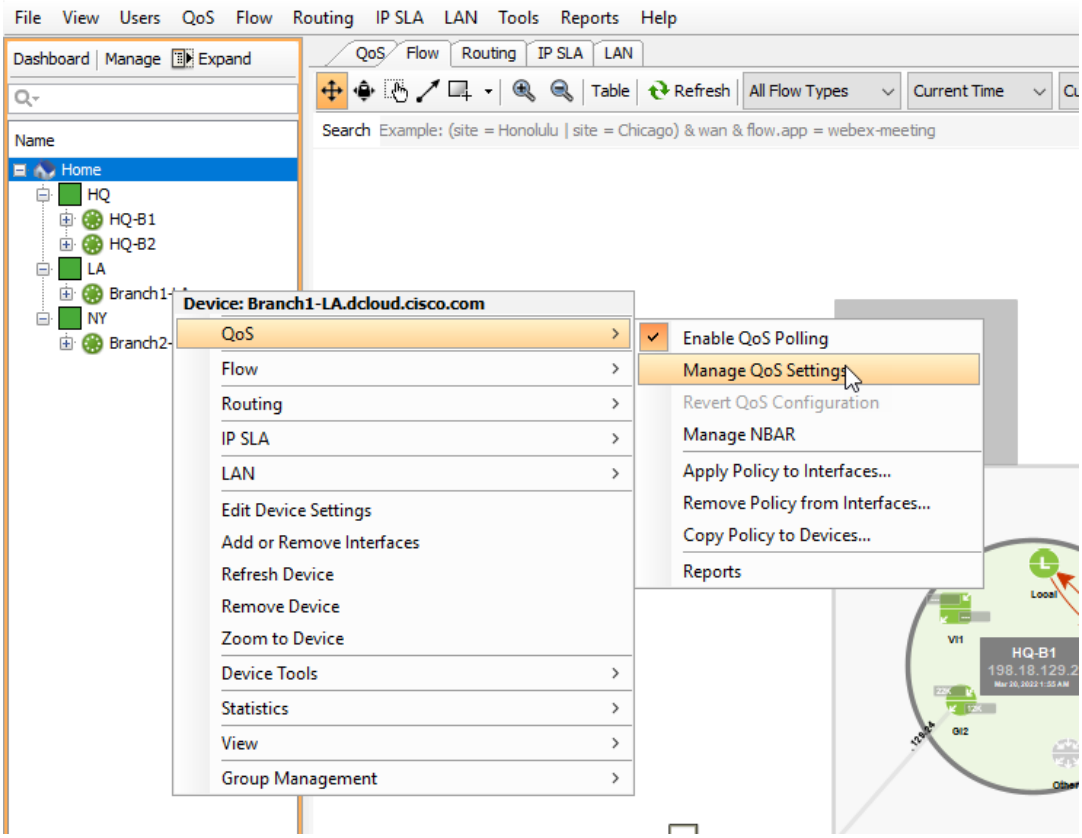


Figure 173

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

 © Copyright LiveAction 2022

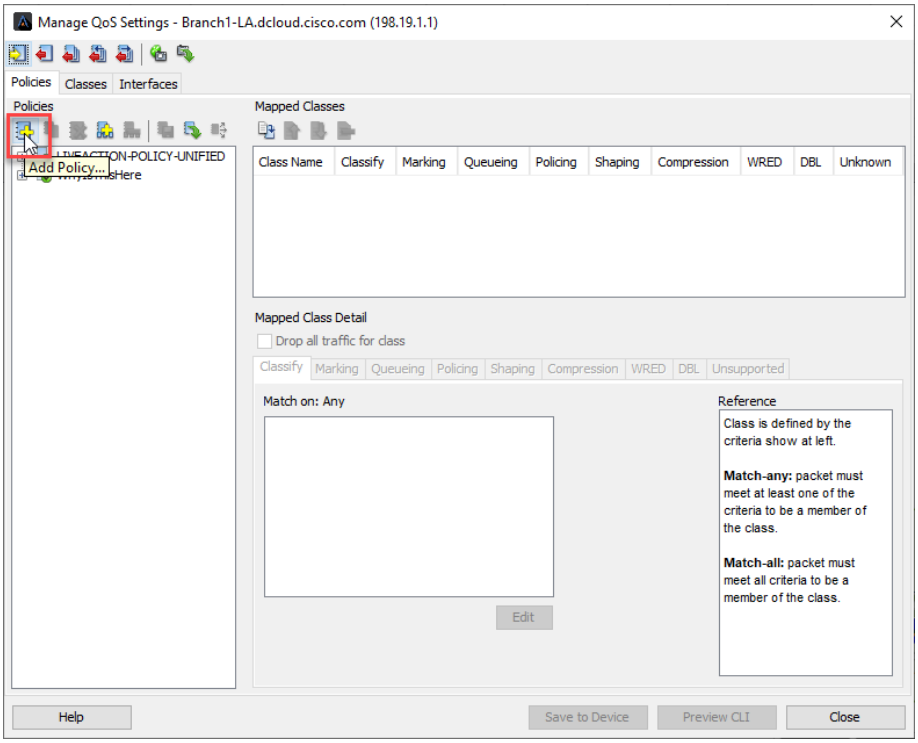


Figure 174

10. Give the new Policy a name, such as "**DSCPMARK**"

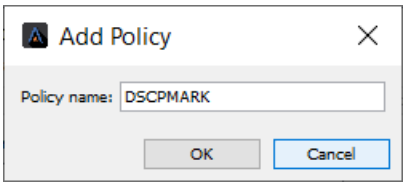


Figure 175

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**"

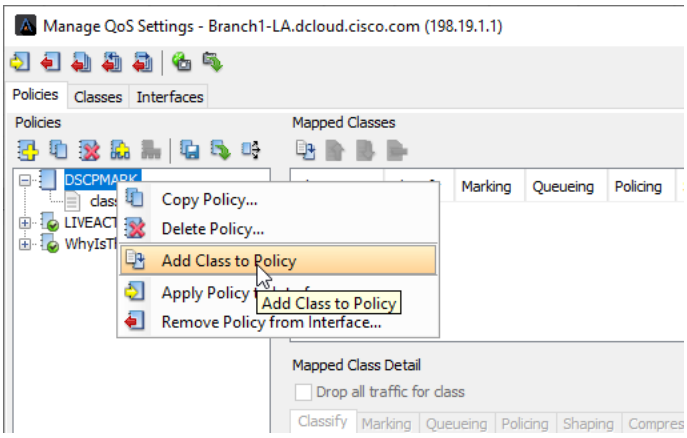


Figure 176

13. Select "**Create a new class**" and give the class a name **RTP**.
14. Click **OK**

 © Copyright LiveAction 2022

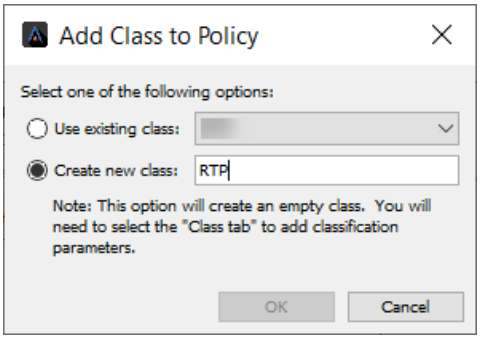


Figure 177

15. Right click **DSCPMark** again
16. Select "**Add Class to Policy**"

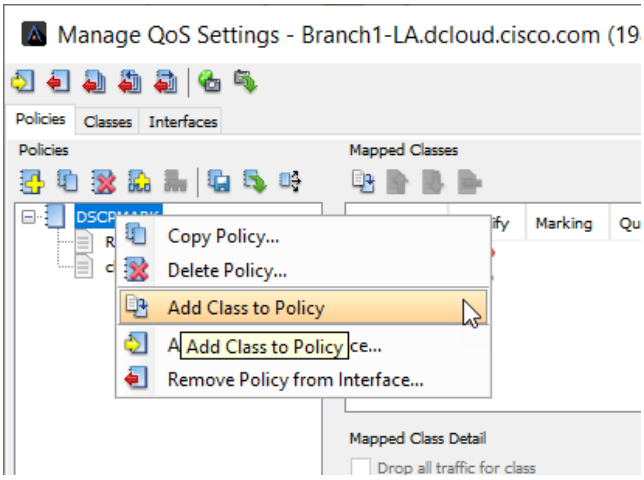


Figure 178

17. Click Create new class, Label it **SIP**.
18. Click OK.

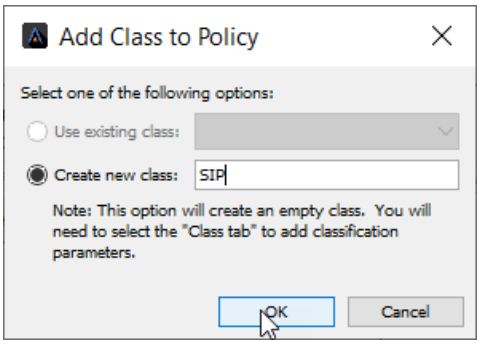


Figure 179

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

 © Copyright LiveAction 2022

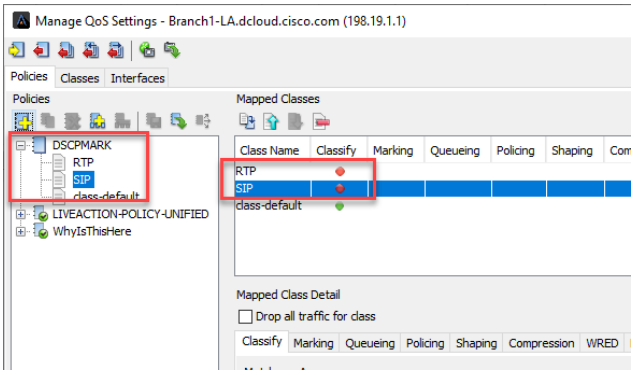


Figure 180

19. Select the "**Classes**" tab to match them to the created ACL's.

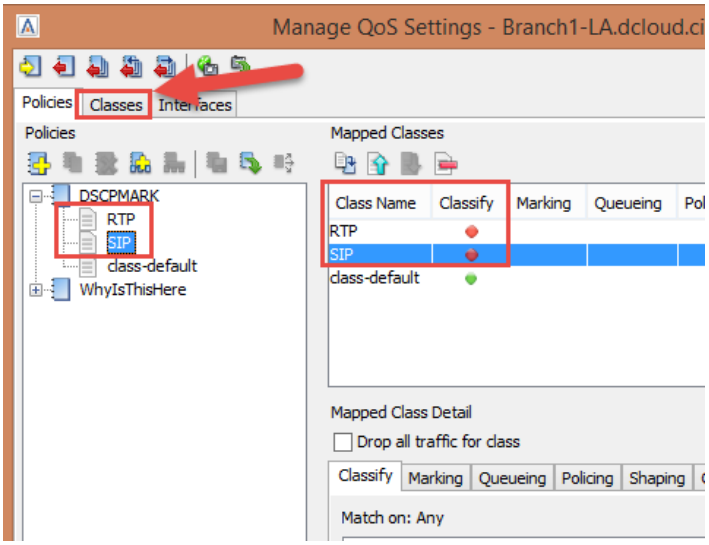


Figure 181

Select and match the SIP class…

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

 © Copyright LiveAction 2022

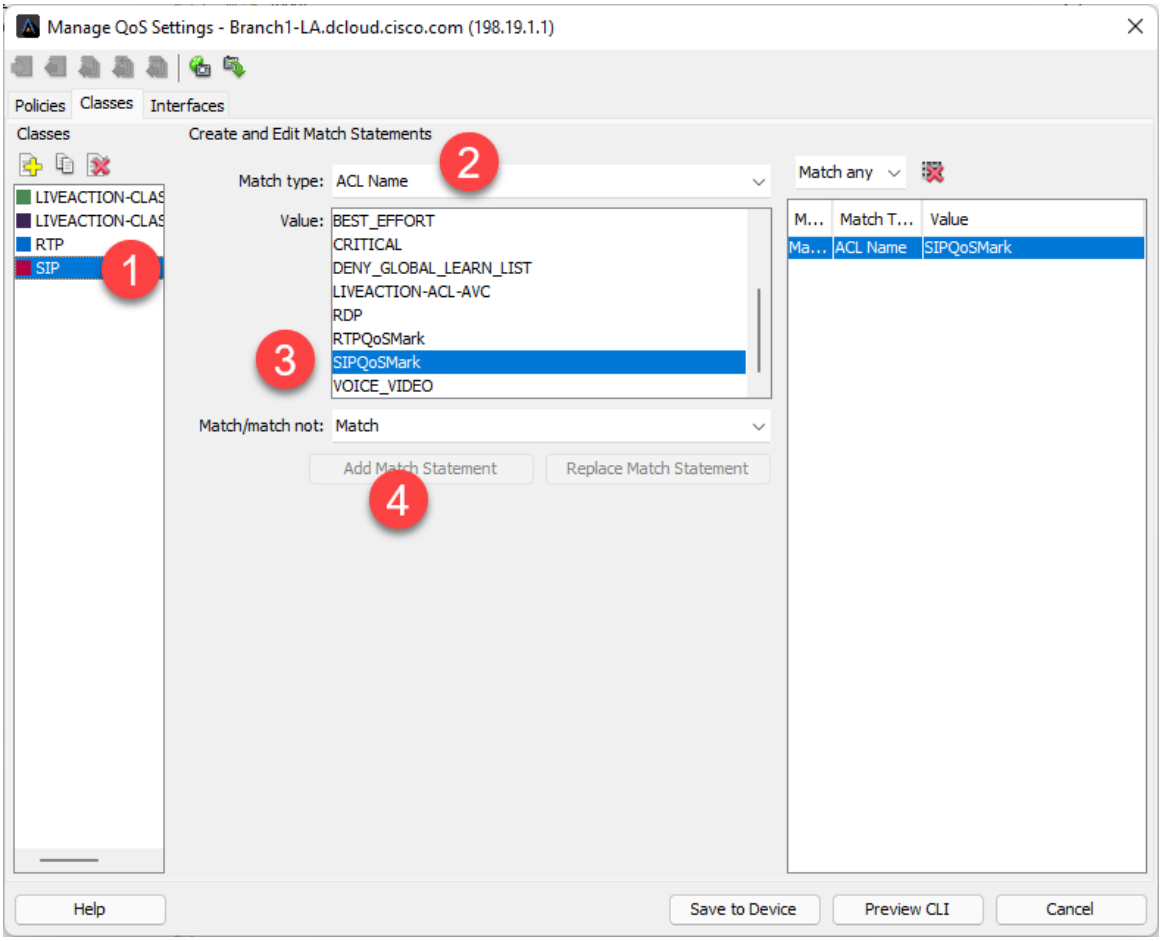


Figure 182

Next select the RTP Class and do the same…

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

 © Copyright LiveAction 2022

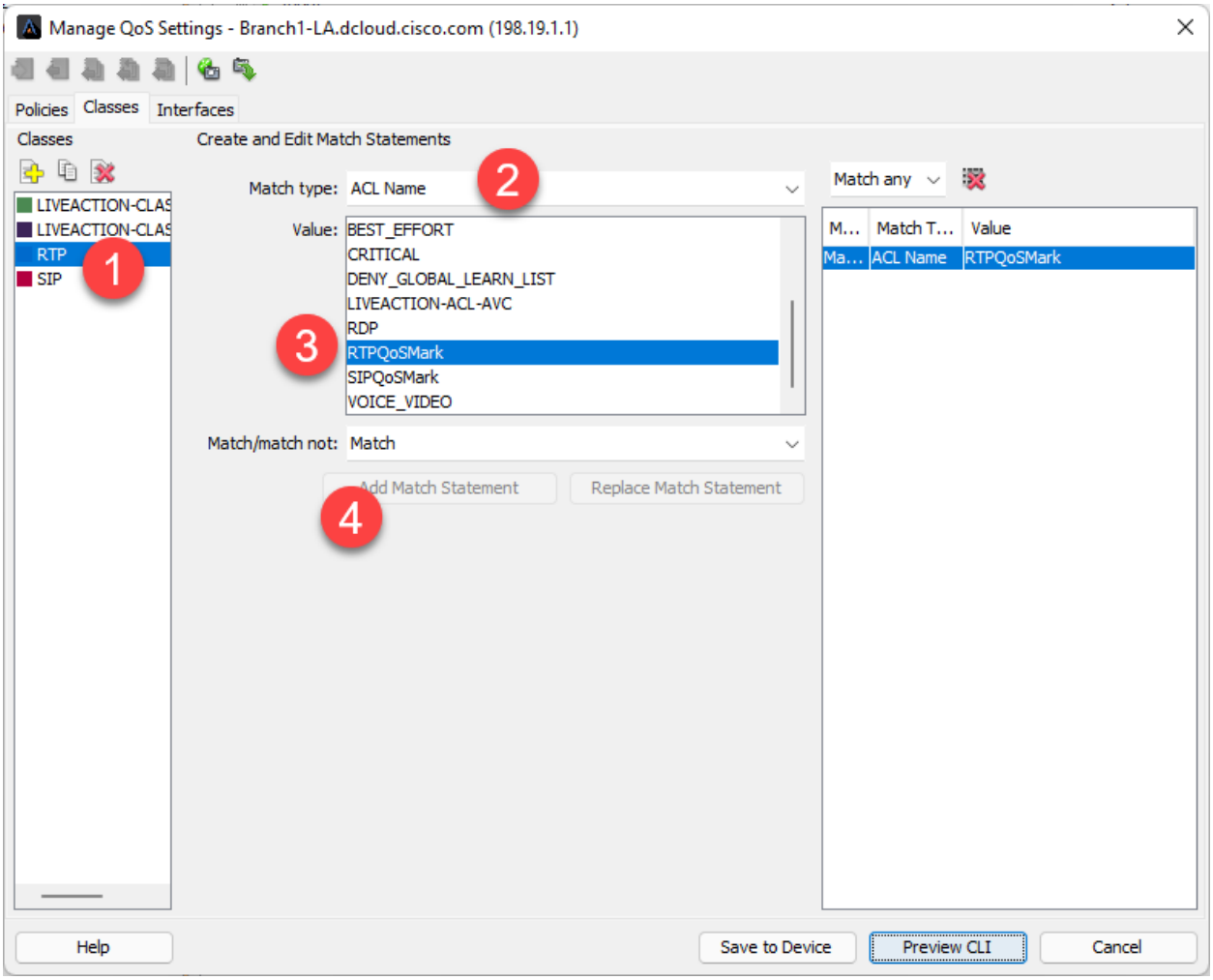


Figure 183

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

 © Copyright LiveAction 2022

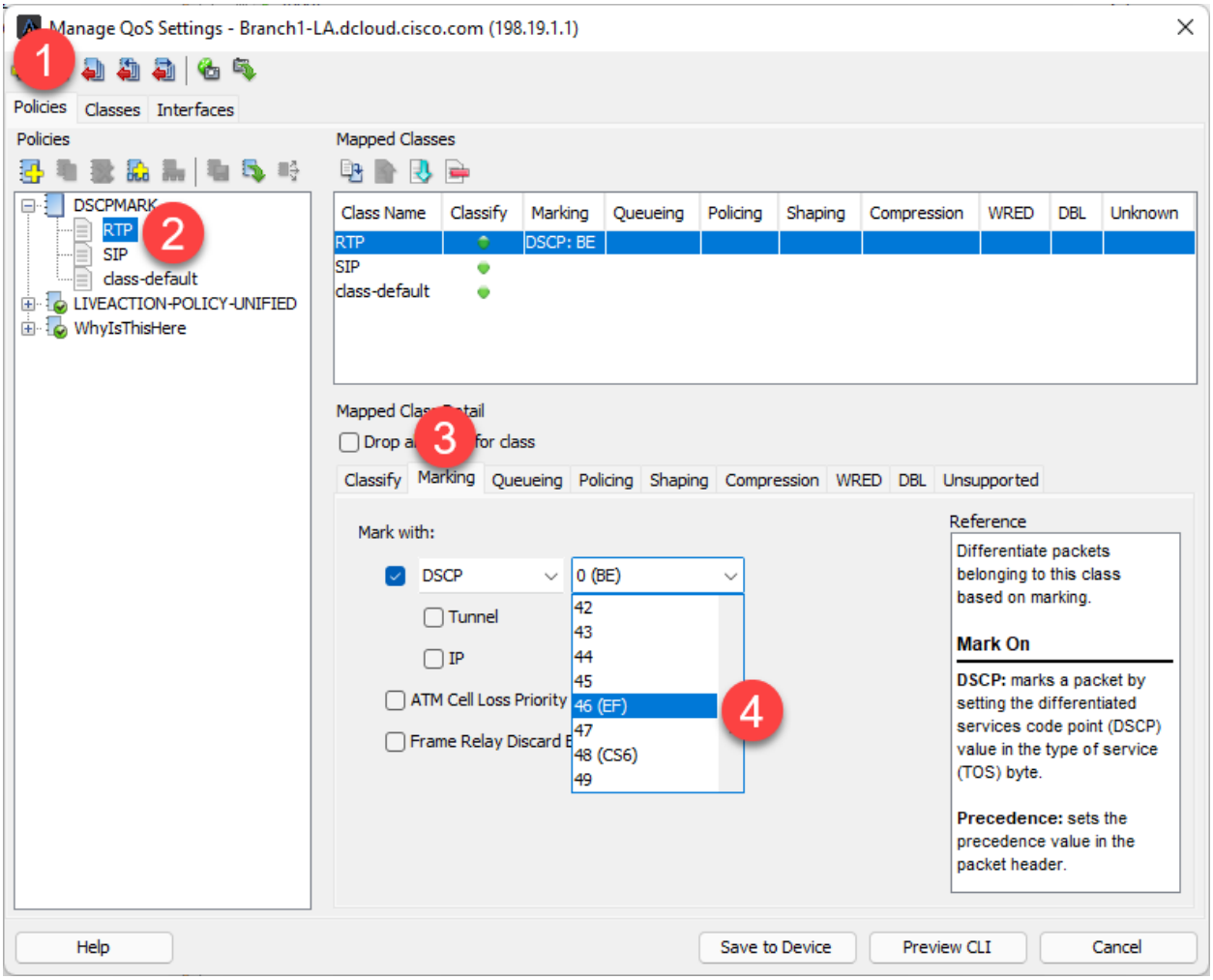


Figure 184

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

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

 © Copyright LiveAction 2022

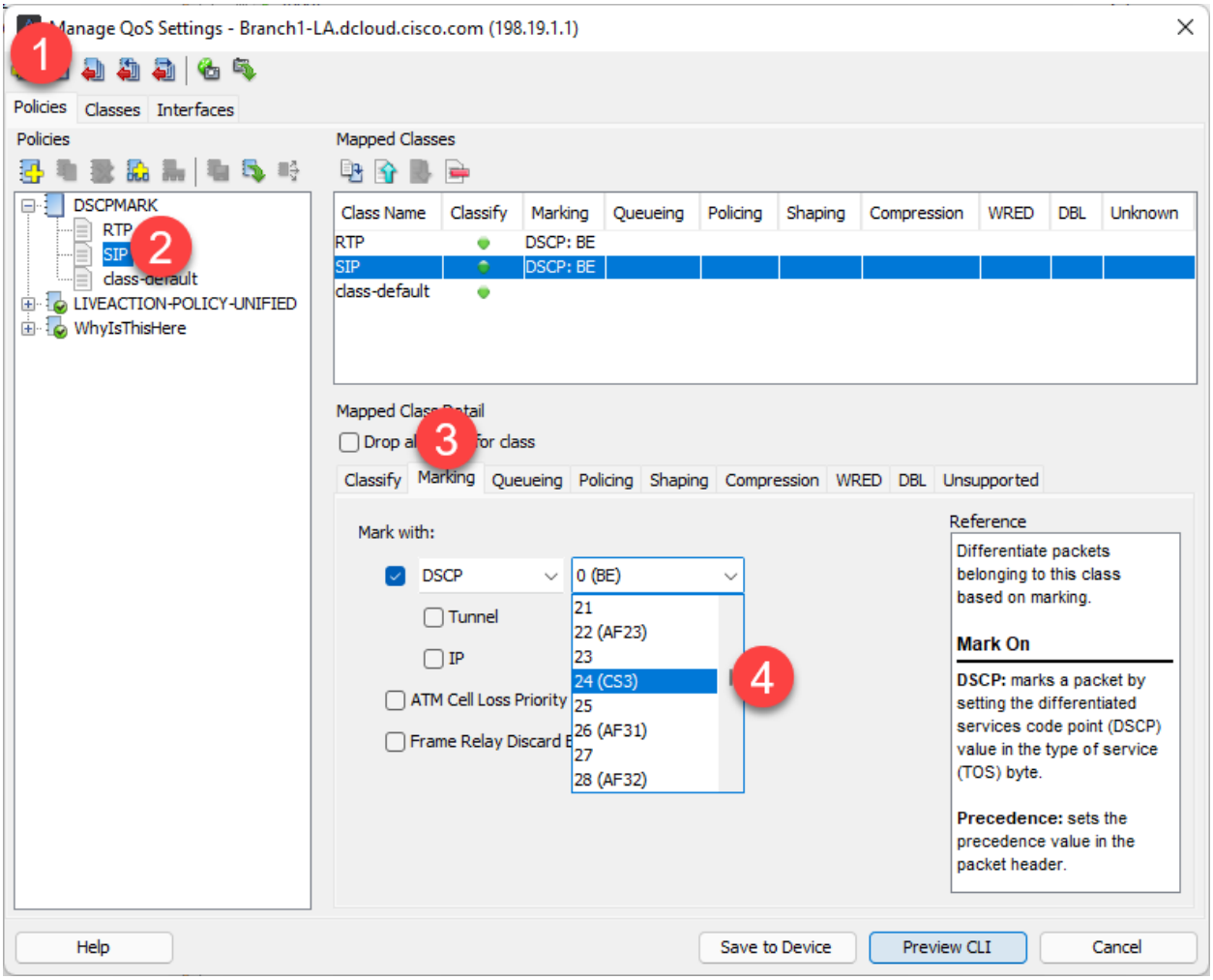


Figure 185

35. Click **Preview CLI** to see the policy you have created.
36. Click **Save to Device** if satisfied.

 © Copyright LiveAction 2022

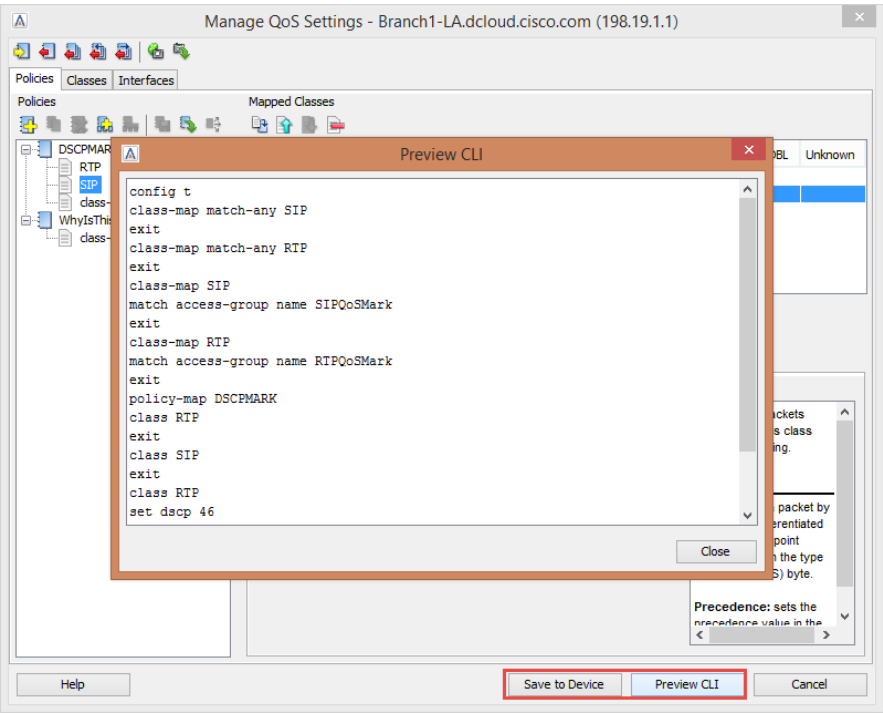


Figure 186

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

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

 © Copyright LiveAction 2022

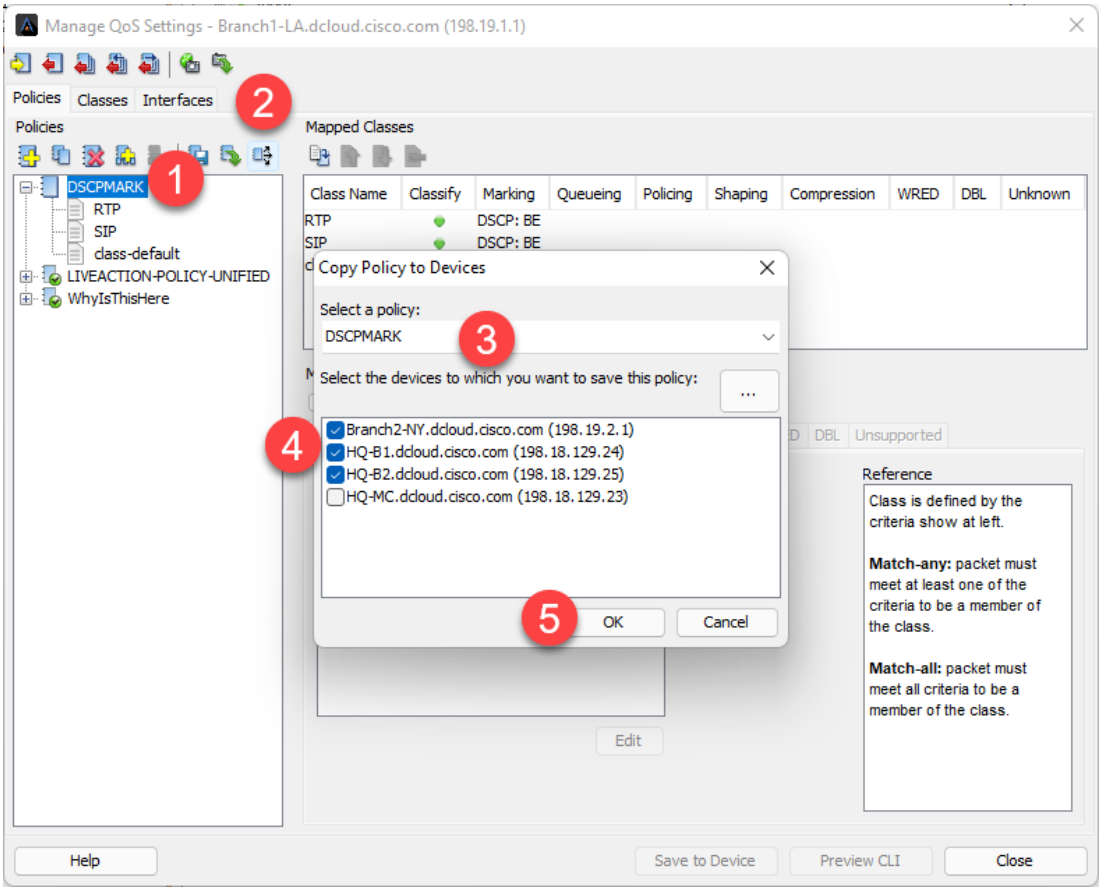


Figure 187

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

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

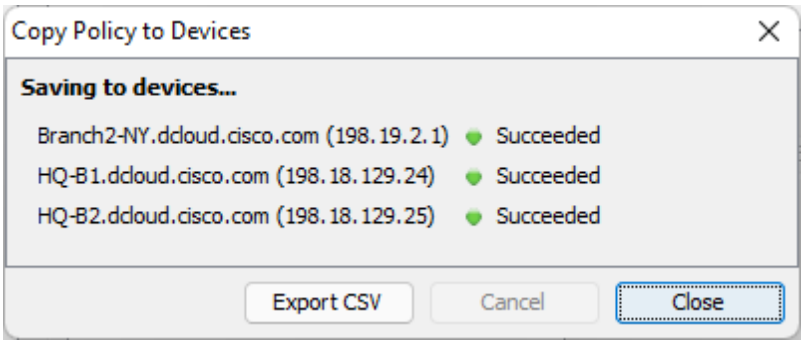


Figure 188

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.

43. In the main device menu on the top-left, right-Click on the appropriate interface.
44. Select **QoS**, and then **Apply Policy to Interface**.

 © Copyright LiveAction 2022

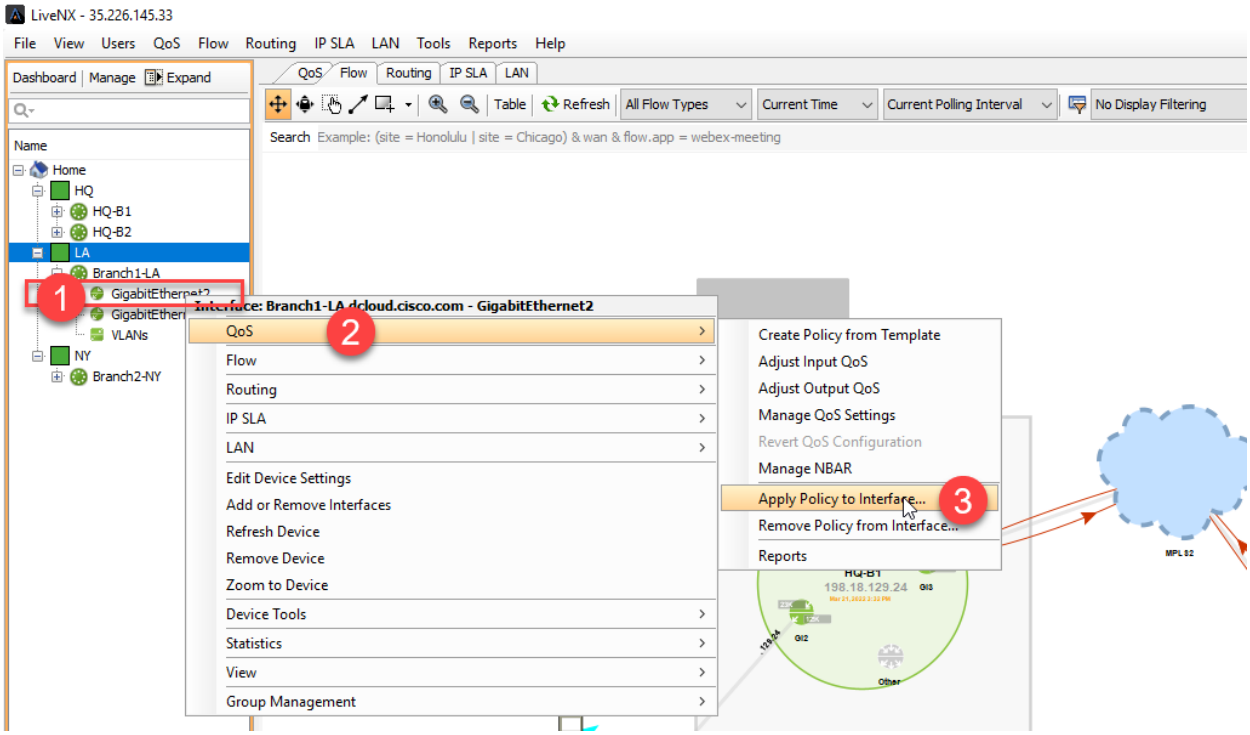


Figure 189

45. Select the "**DSCPMARK**" policy.
46. Click the **Input** of the **LAN Interface**

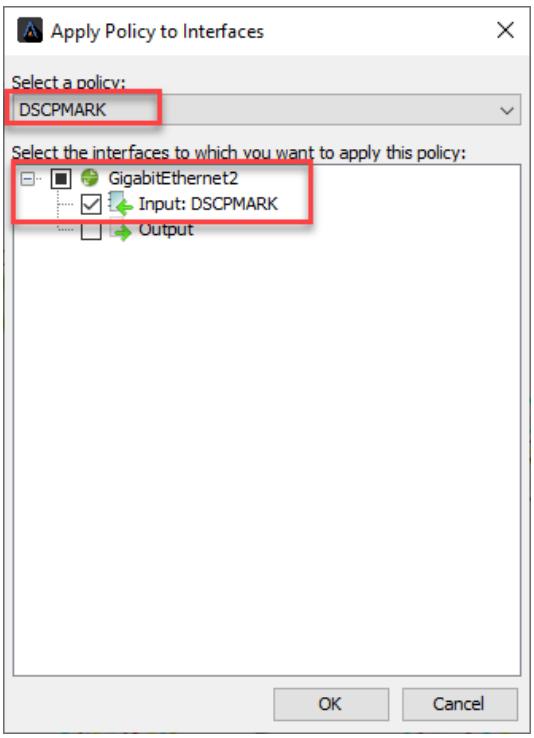


Figure 190

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

4/8/2022

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.

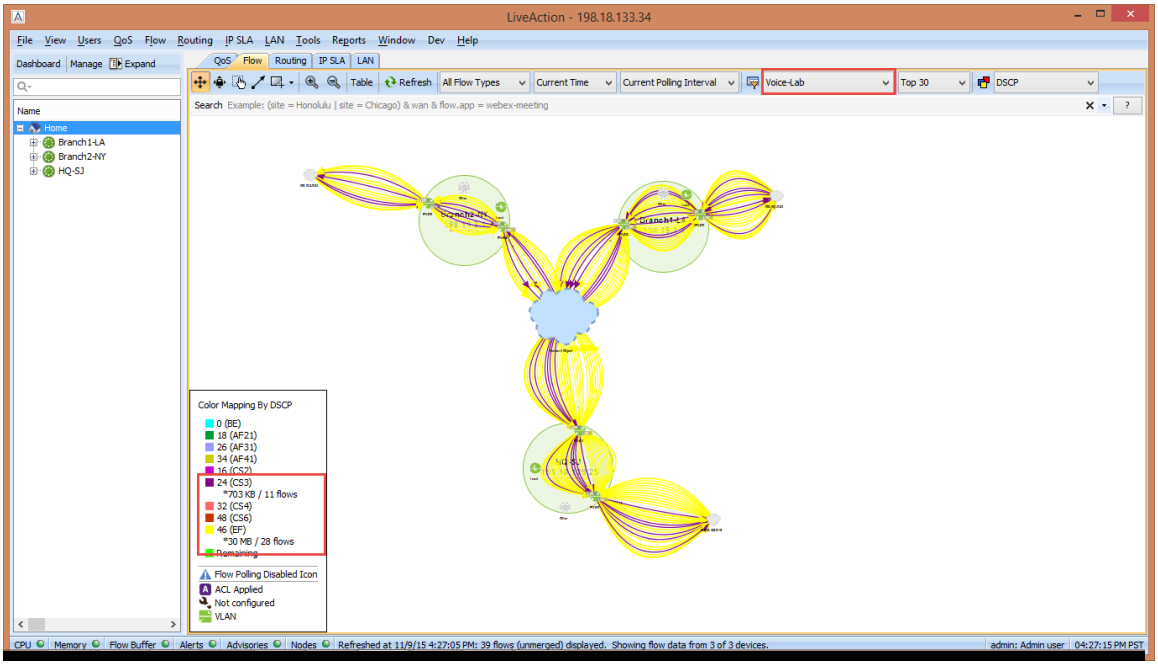


Figure 191

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:

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

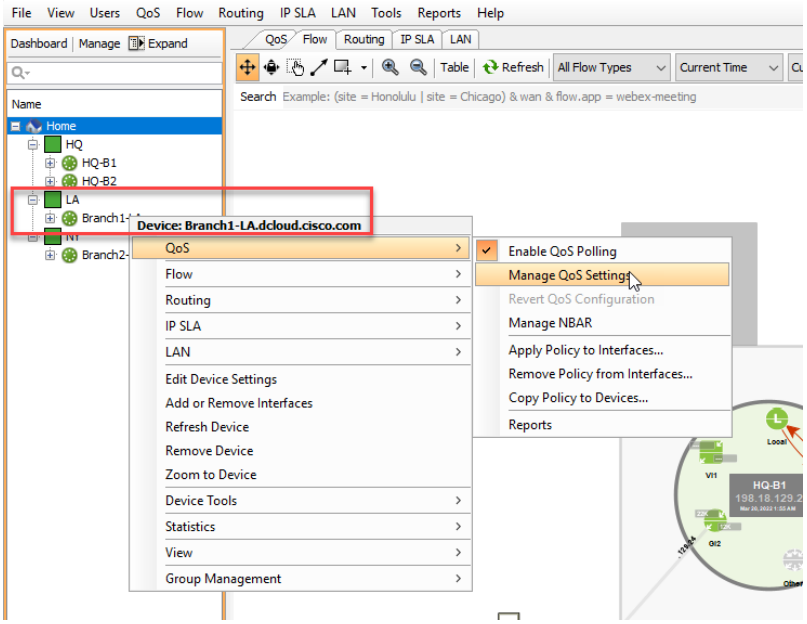


Figure 192

48. Select the **Policies** Tab.
49. Click **Add Policy** to create a queuing policy.

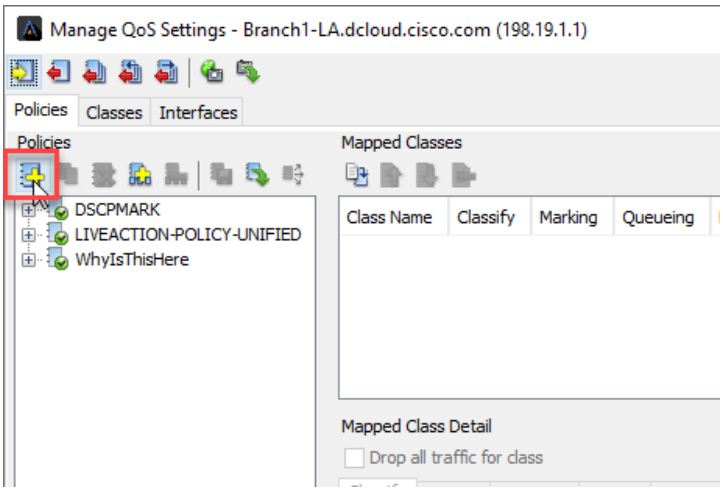


Figure 193

 © Copyright LiveAction 2022

50. Name the new policy QUEUEING.

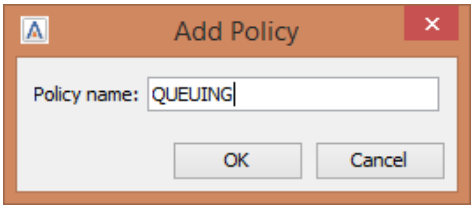


Figure 194

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

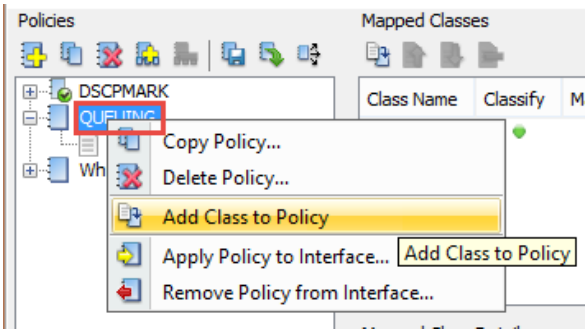


Figure 195

52. Create a new class labeled VOIP.

53. Click OK.

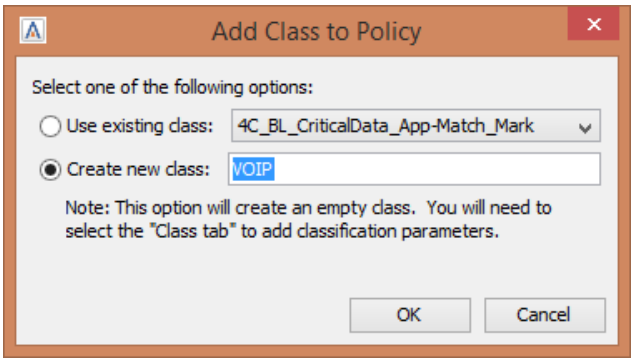


Figure 196

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

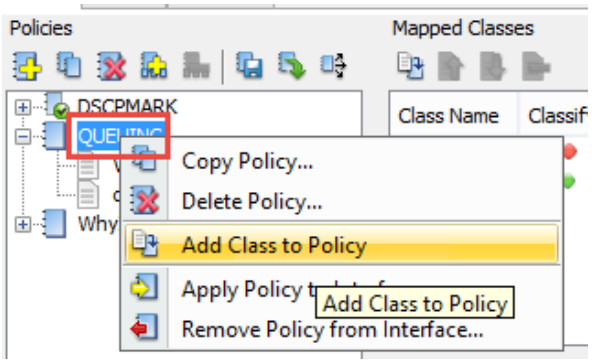


Figure 197

55. Create a new class and label it **SIGNALING**.

 © Copyright LiveAction 2022

56. Click OK

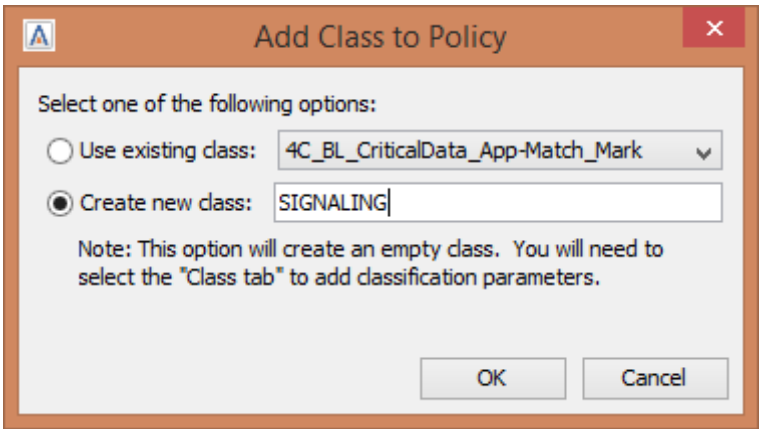


Figure 198

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**

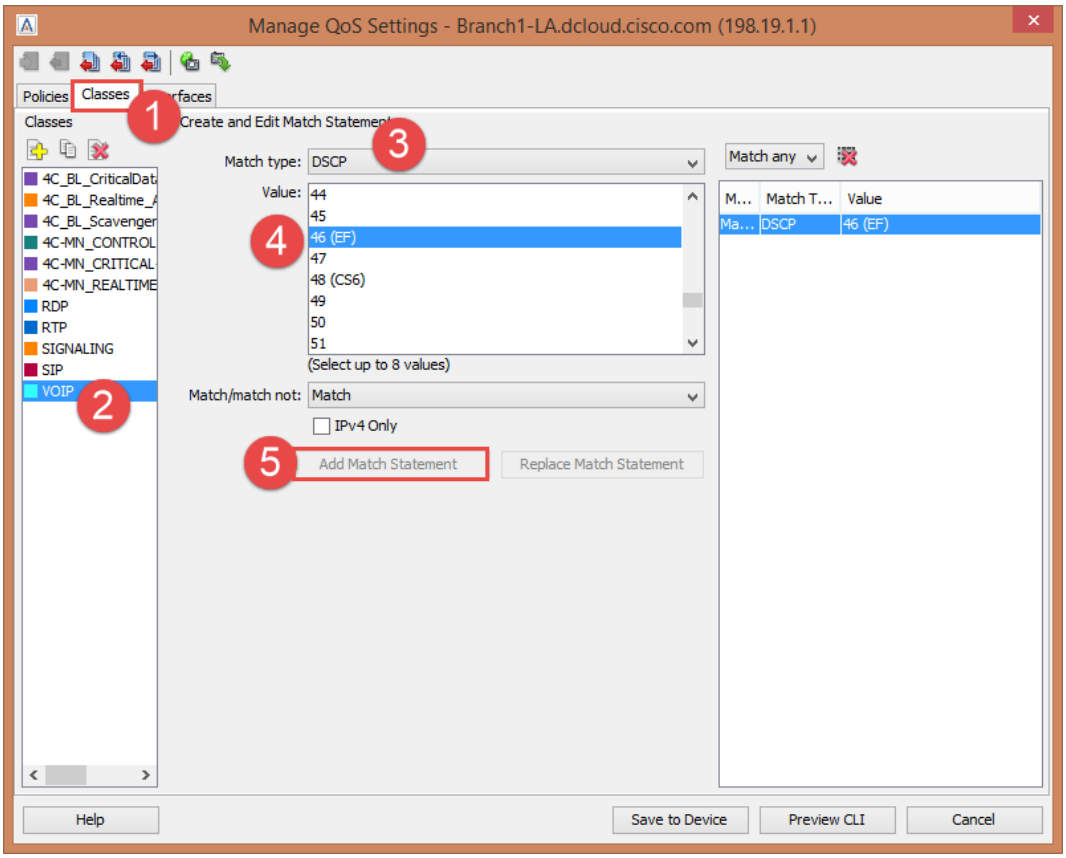


Figure 199

 © Copyright LiveAction 2022

4/8/2022

Configure SIGNALING Class:

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

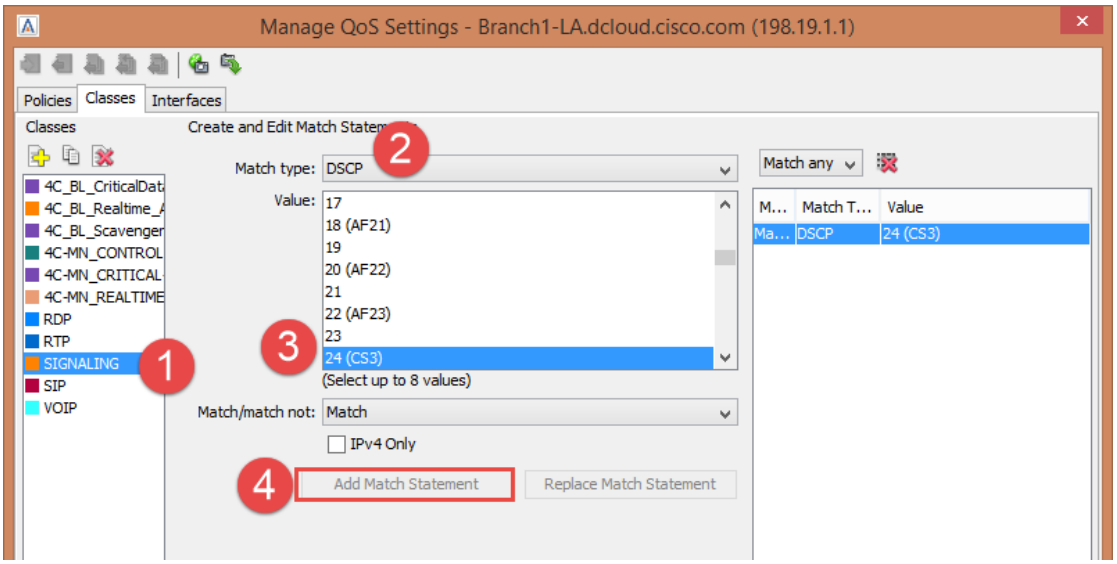


Figure 200

Setup VoIP Priorities:

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

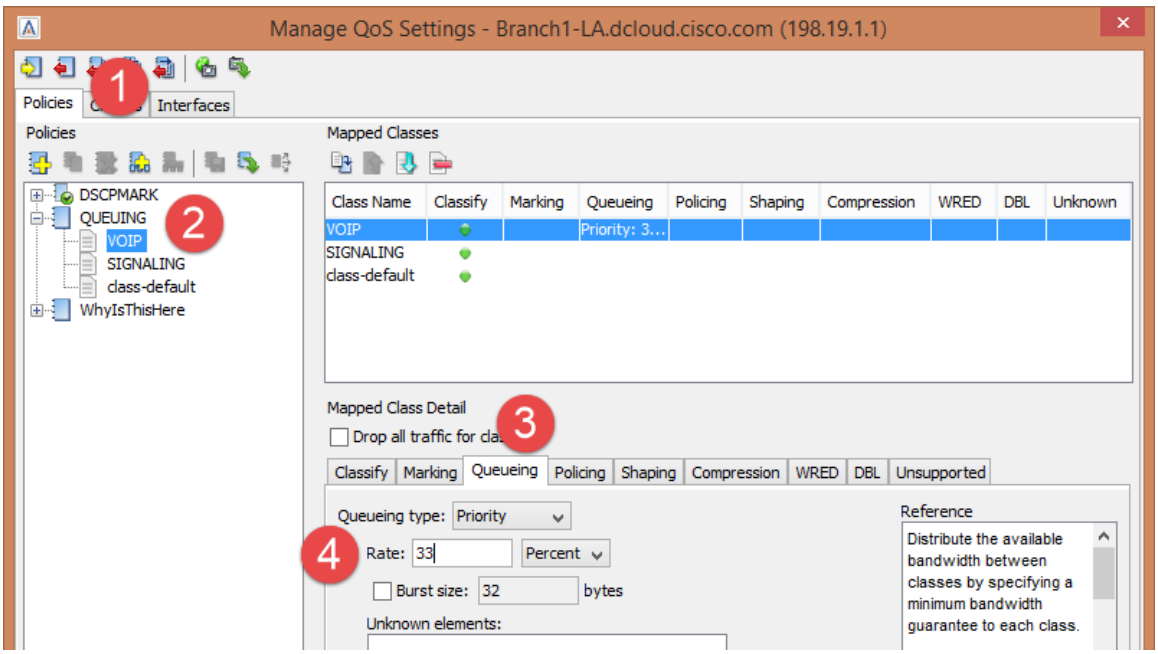


Figure 201

Setup Signaling Priorities:

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

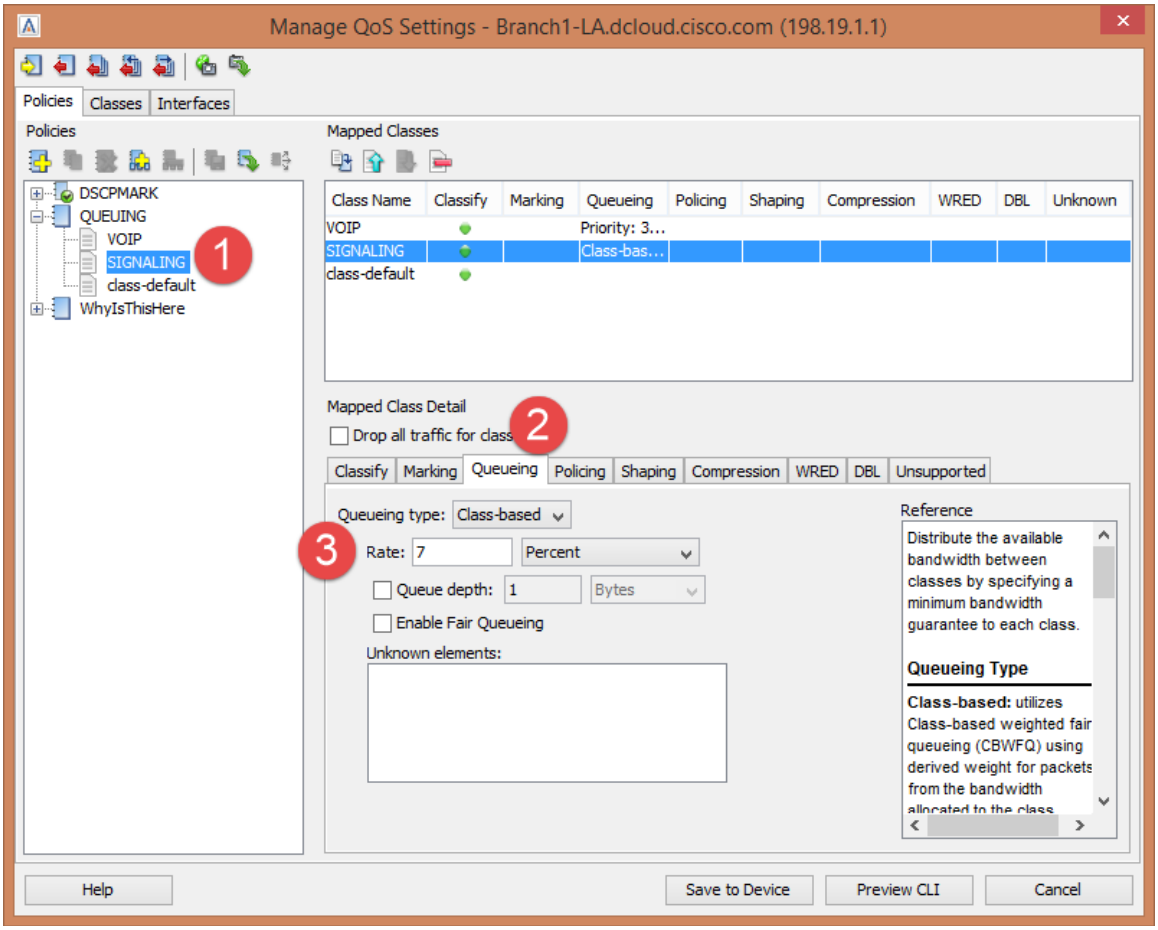


Figure 202

Create a Shaping Policy:

68. Click **Add Policy**.

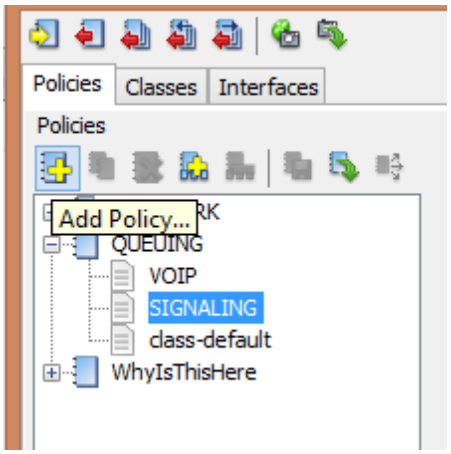


Figure 203

 © Copyright LiveAction 2022

69. Give the Policy a name of Shaper.

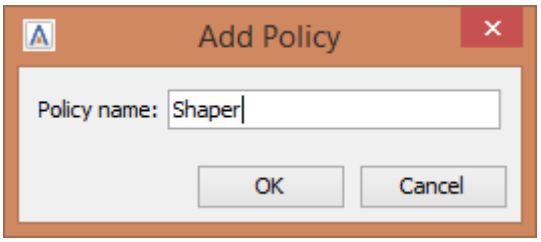


Figure 204

70. Select the **class-default** class under Shaper.
71. Select the Shaping tab.
72. Select Average, enter 1500 Kbps.

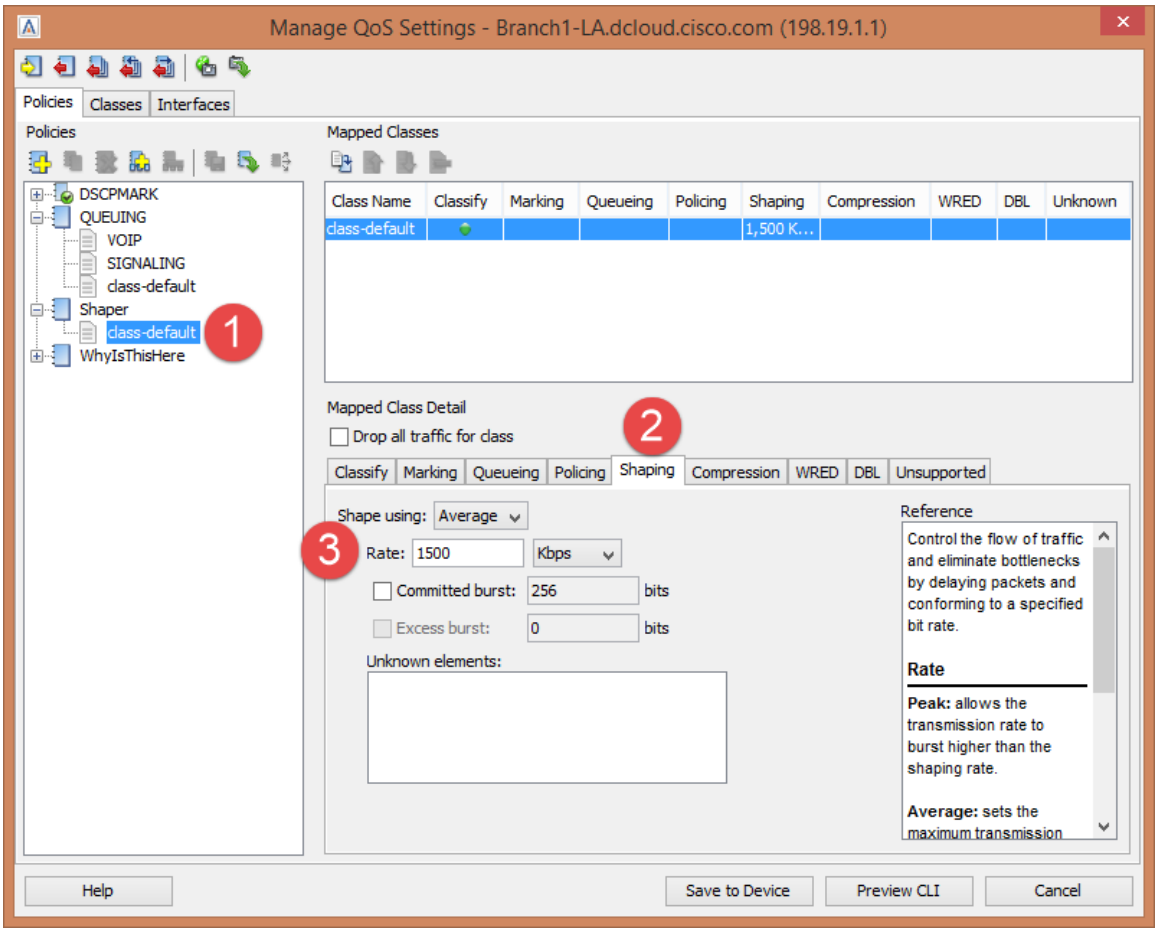


Figure 205

 © Copyright LiveAction 2022

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

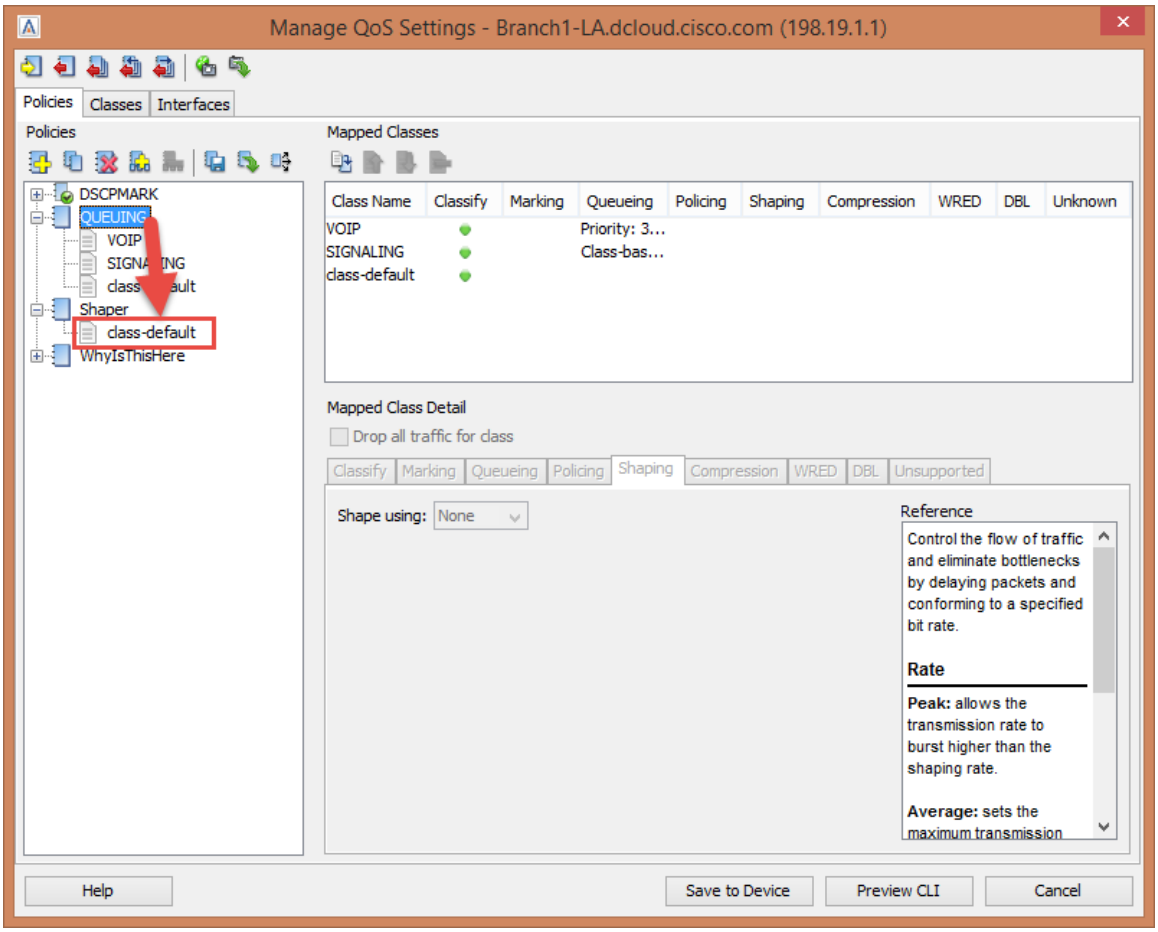


Figure 206

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!

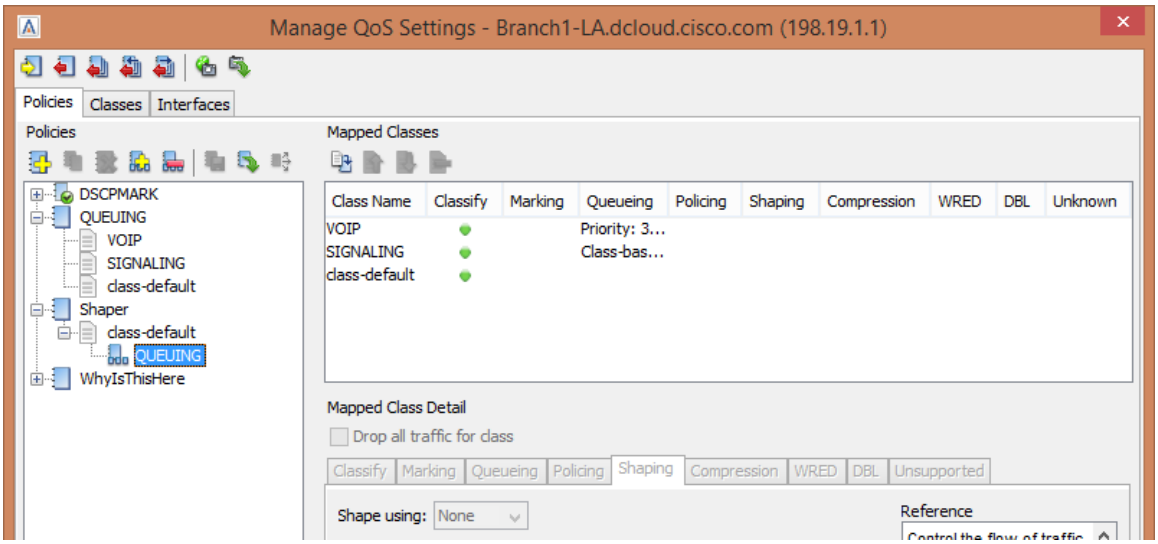


Figure 207

 © Copyright LiveAction 2022

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 devices.
77. Click OK to push the policy.

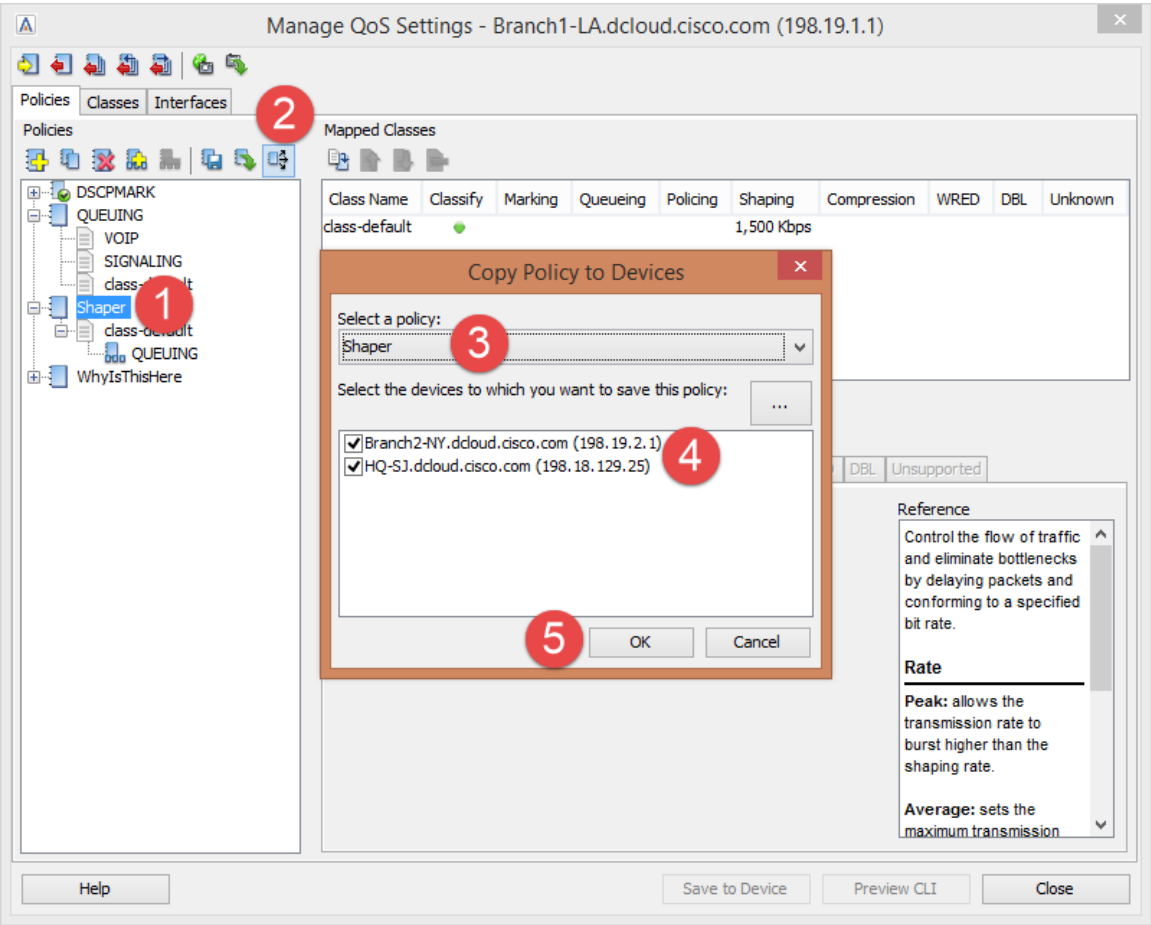


Figure 208

78. Click **Close**.
79. Click **OK**.

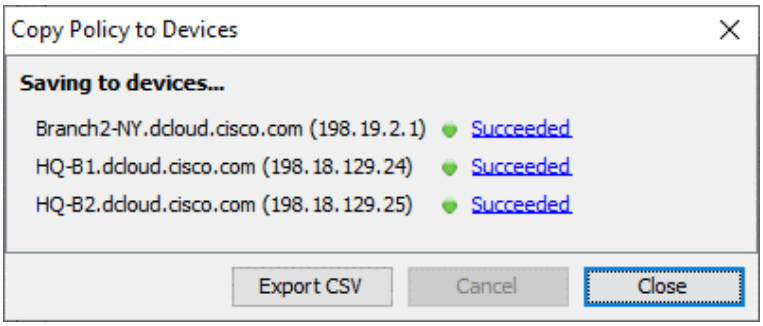


Figure 209

 © Copyright LiveAction 2022

We still need to apply the policy to the WAN interfaces. **Do the following steps on EACH of the 4 devices.**

80. Right-click on the WAN interface in the device list on the left and select **QoS** and **Apply Policy to Interface**.

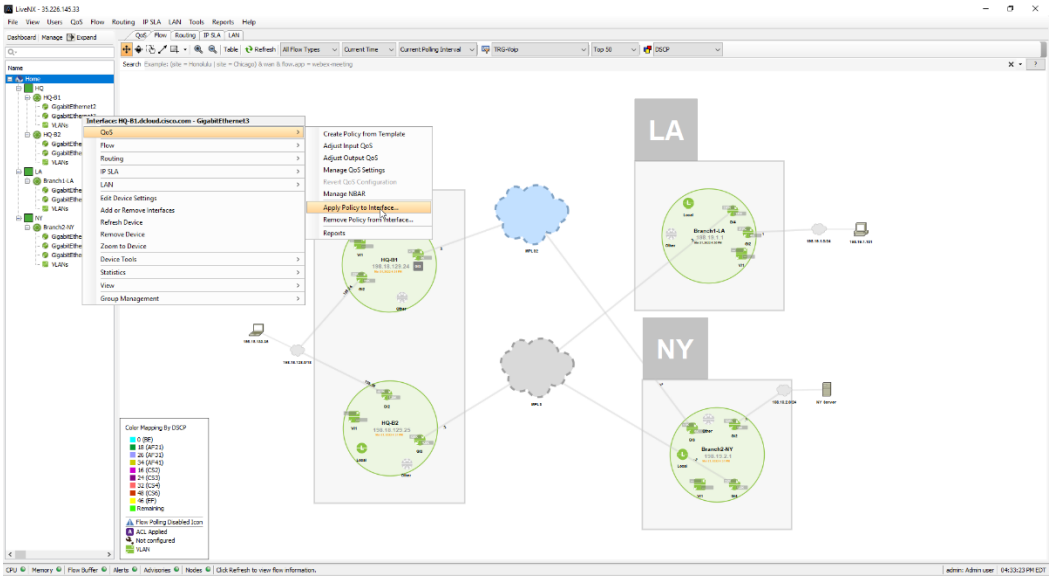


Figure 210

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

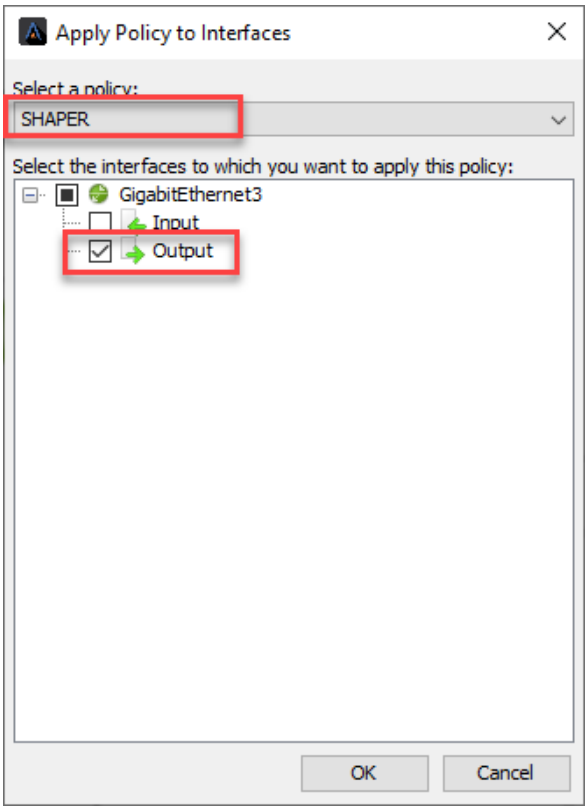


Figure 211

 © Copyright LiveAction 2022

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.

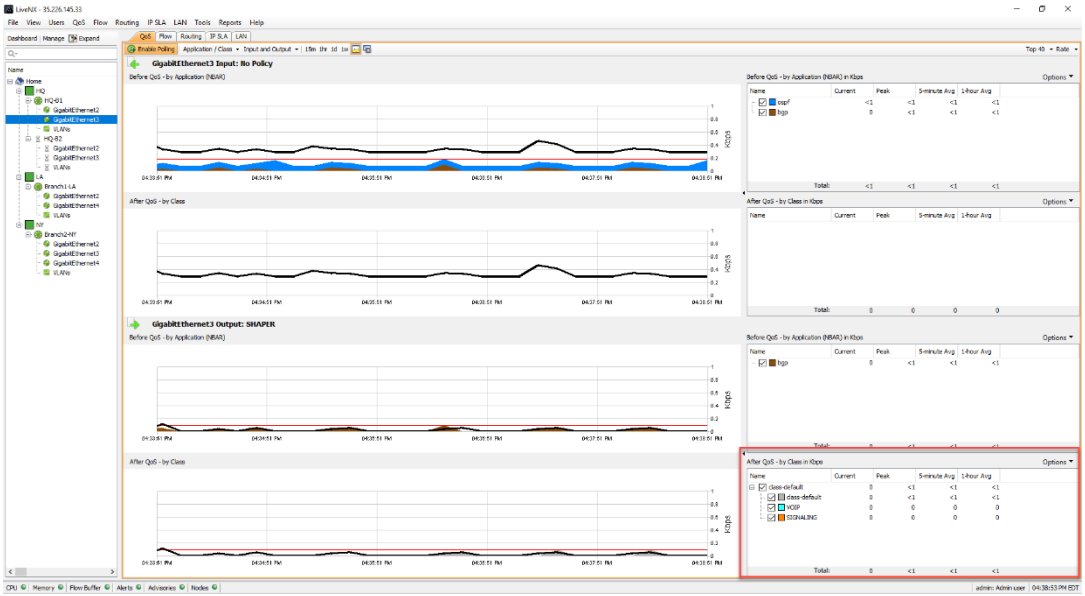


Figure 212

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.

 © Copyright LiveAction 2022

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**.

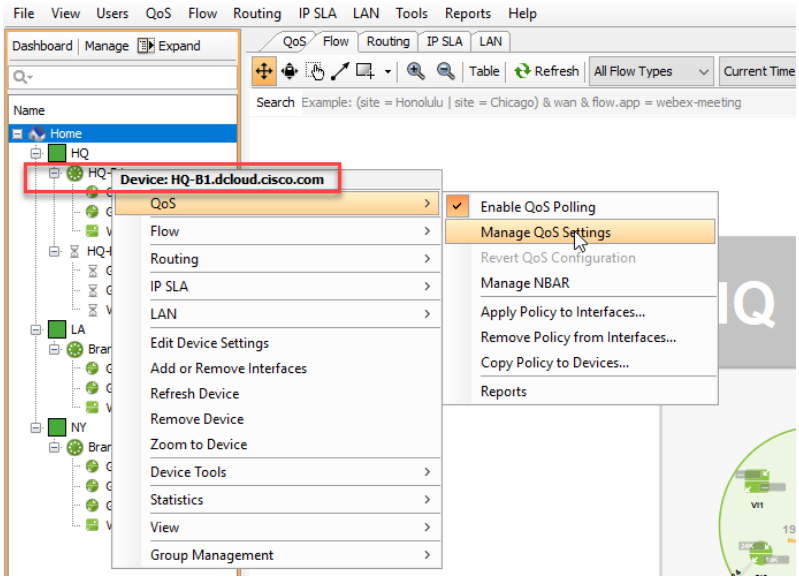


Figure 213

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

 © Copyright LiveAction 2022

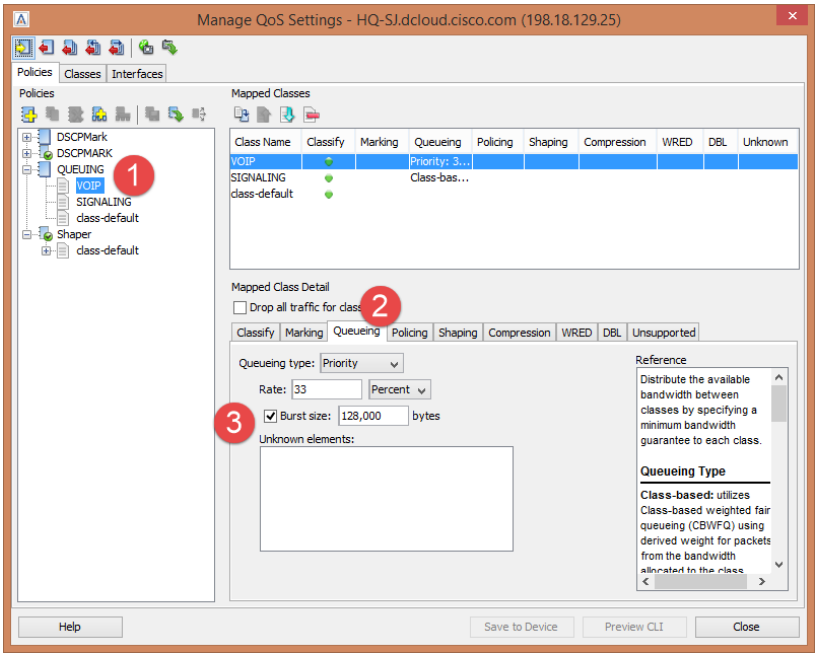


Figure 214

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.

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**.

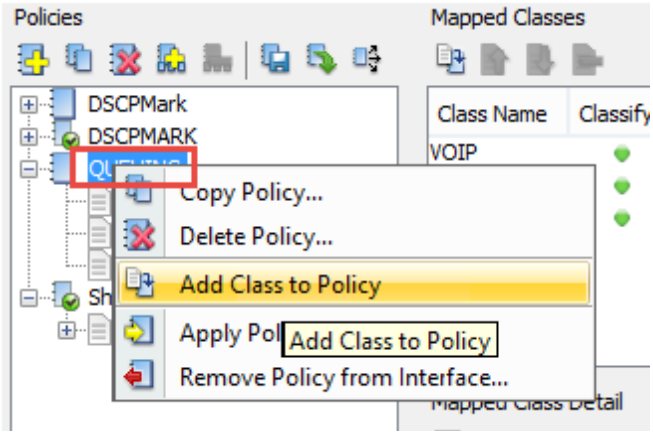


Figure 215

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

 © Copyright LiveAction 2022

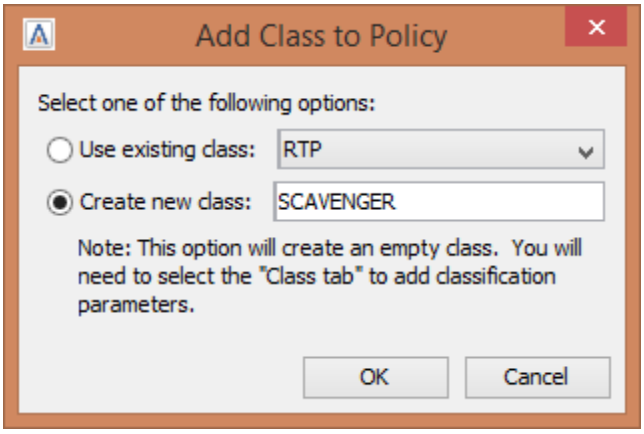


Figure 216

 © Copyright LiveAction 2022

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.

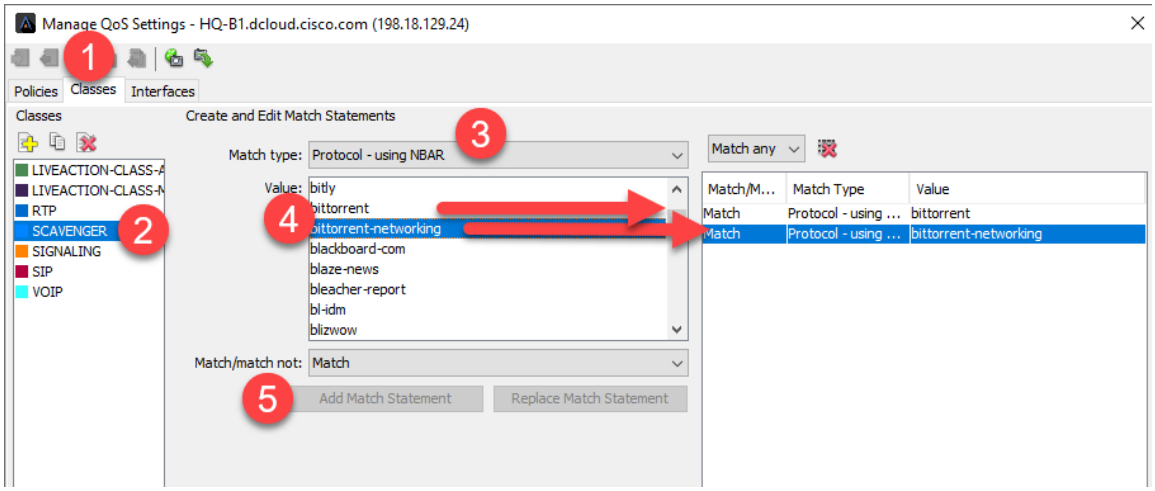


Figure 217

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

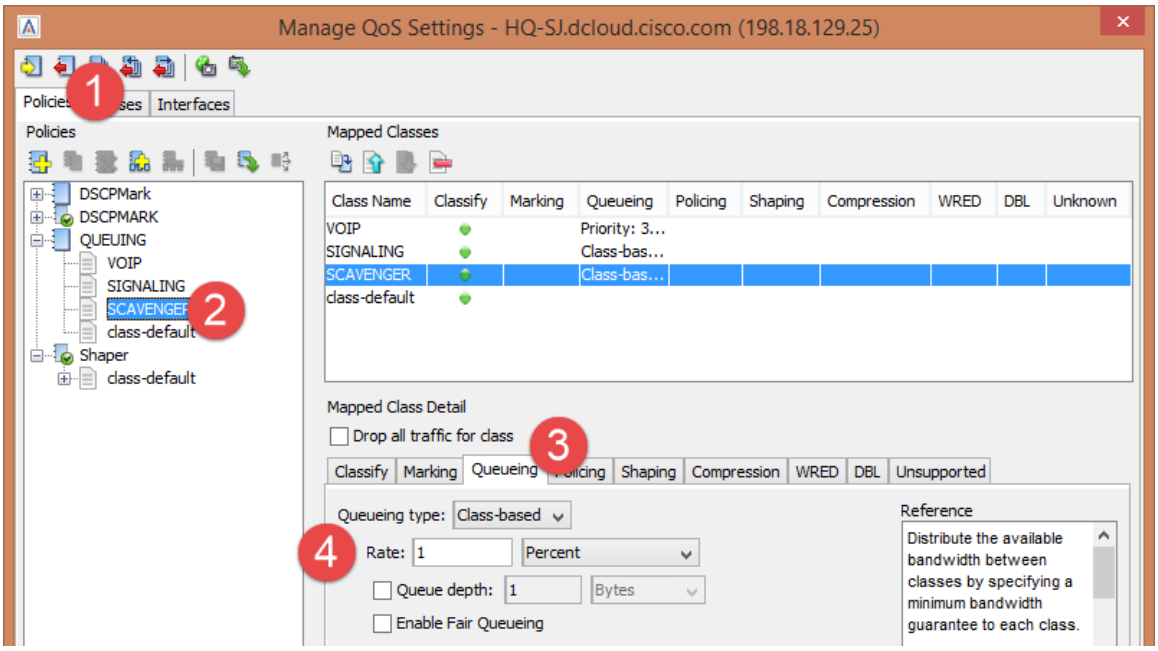


Figure 218

 © Copyright LiveAction 2022

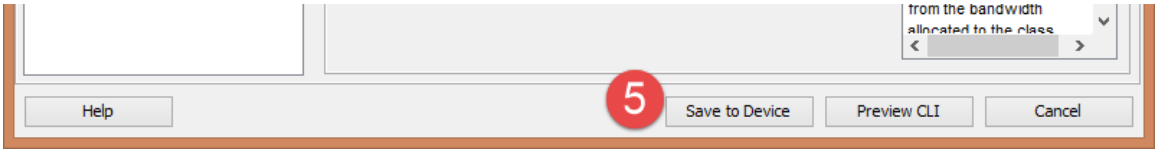


Figure 219

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

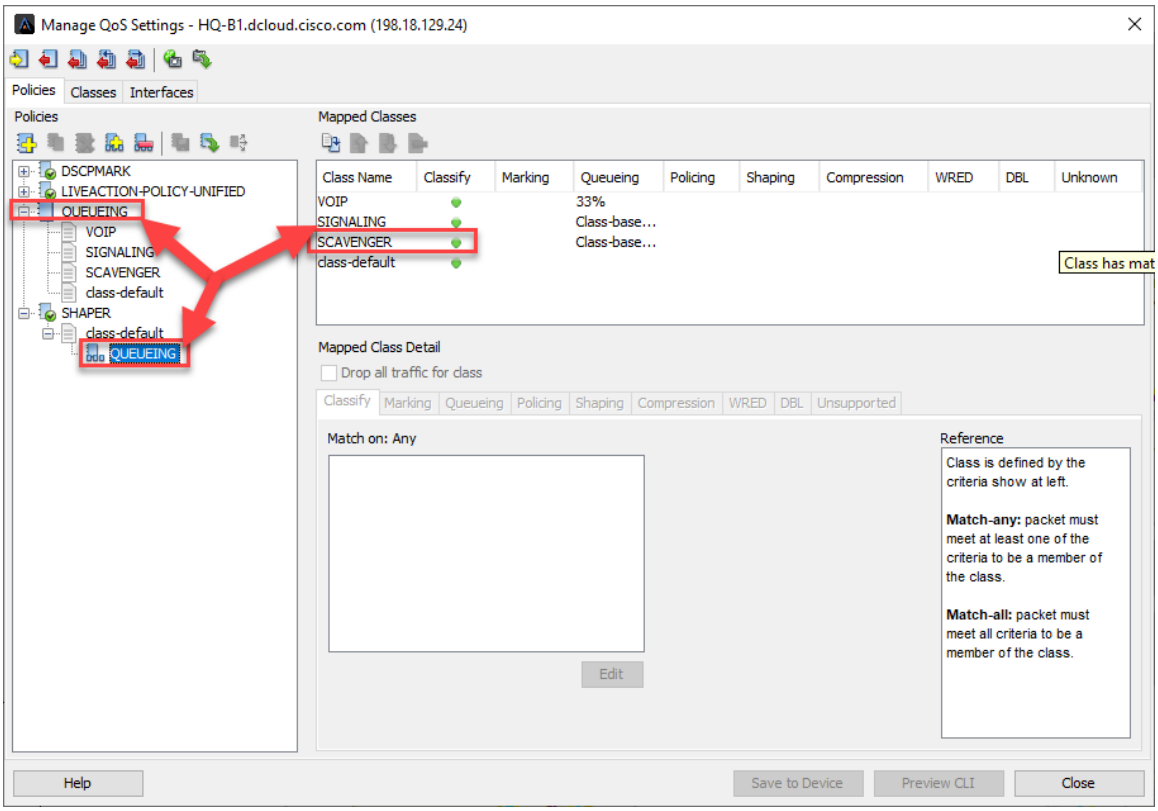


Figure 220

Copy the updated policy to other devices in the topology.

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

 © Copyright LiveAction 2022

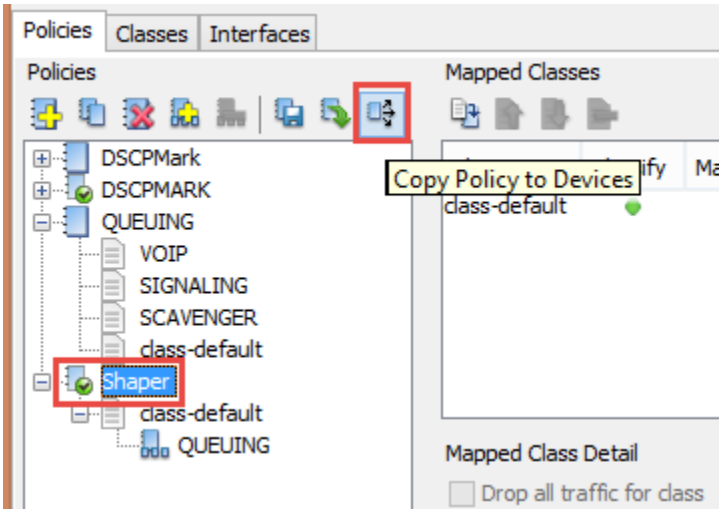


Figure 221

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

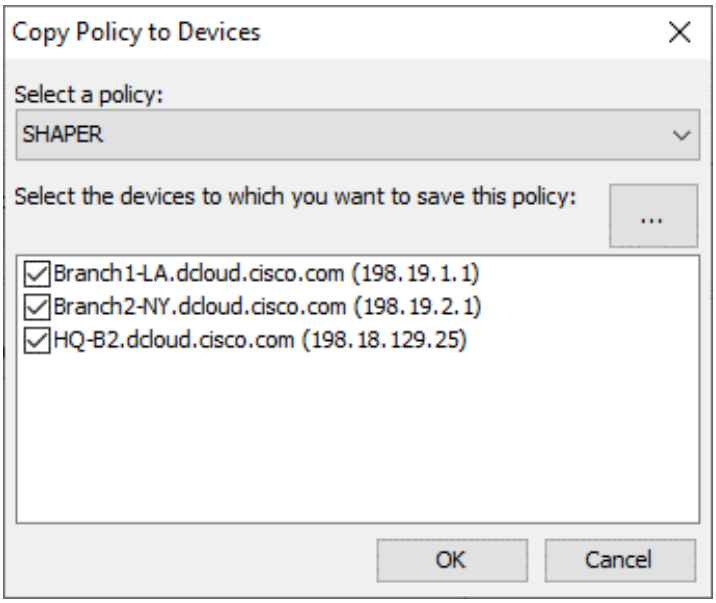


Figure 222

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**.

 © Copyright LiveAction 2022

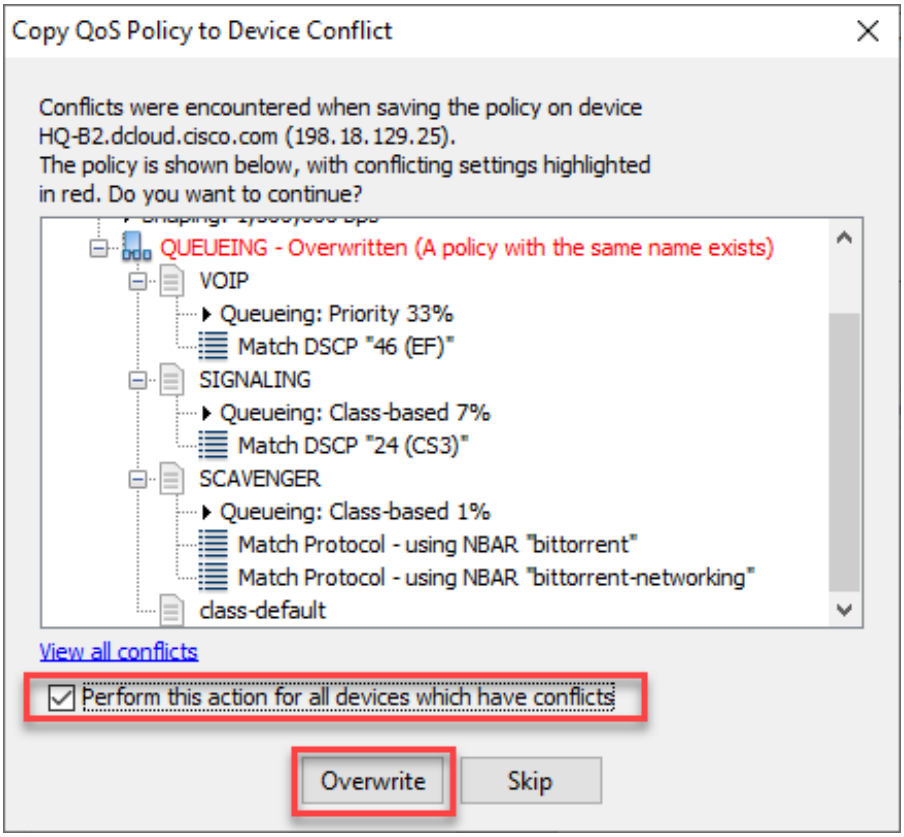


Figure 223

Ensure the copy is successful.

104. Click **Close**.

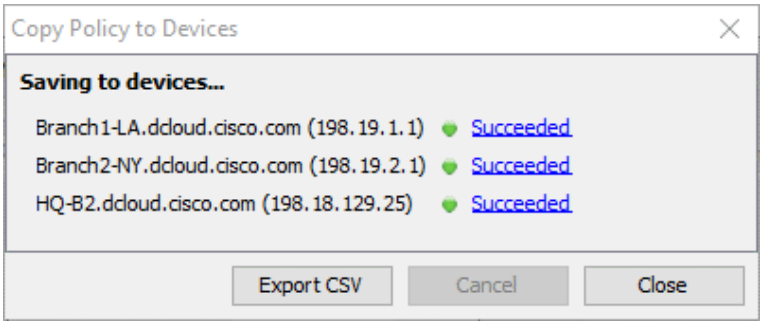


Figure 224

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

 © Copyright LiveAction 2022

Figure 225

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.

 © Copyright LiveAction 2022

Lab A

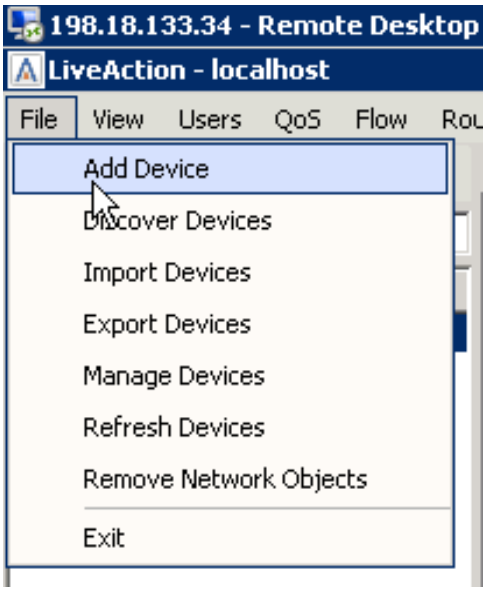
Lab A: Appendix

Lab A.1: Add Device

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

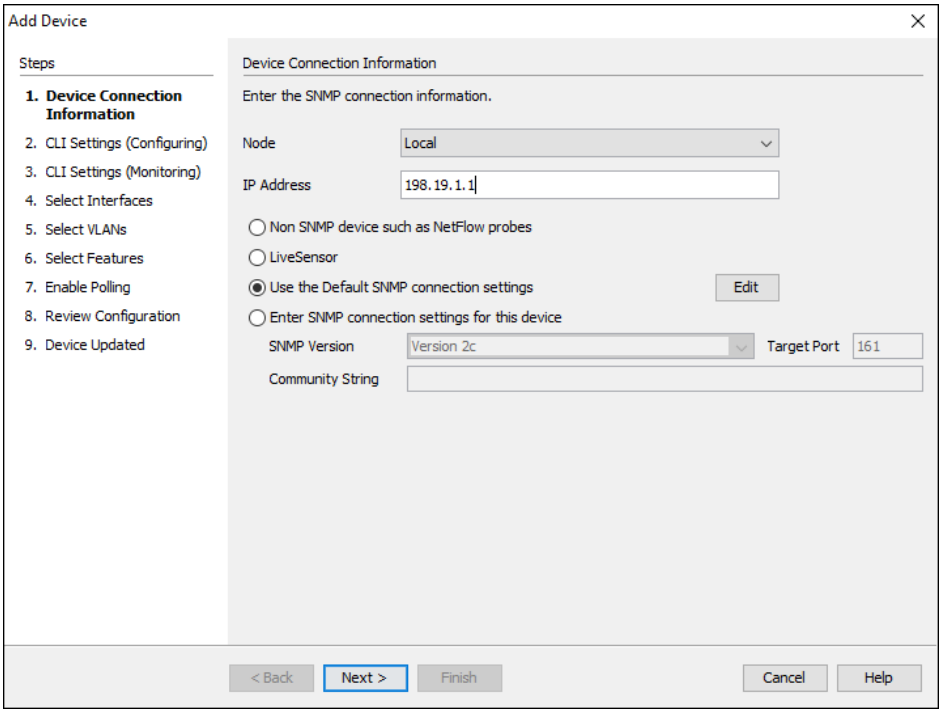
Lab Steps:

1. Select File, **Add Device**



A 1

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

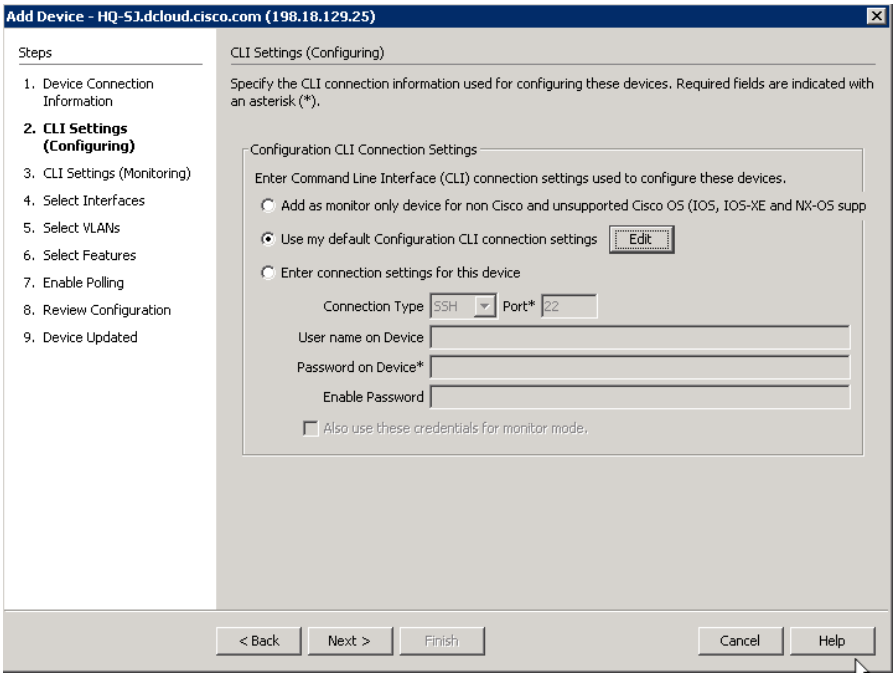


A 2

 © Copyright LiveAction 2022

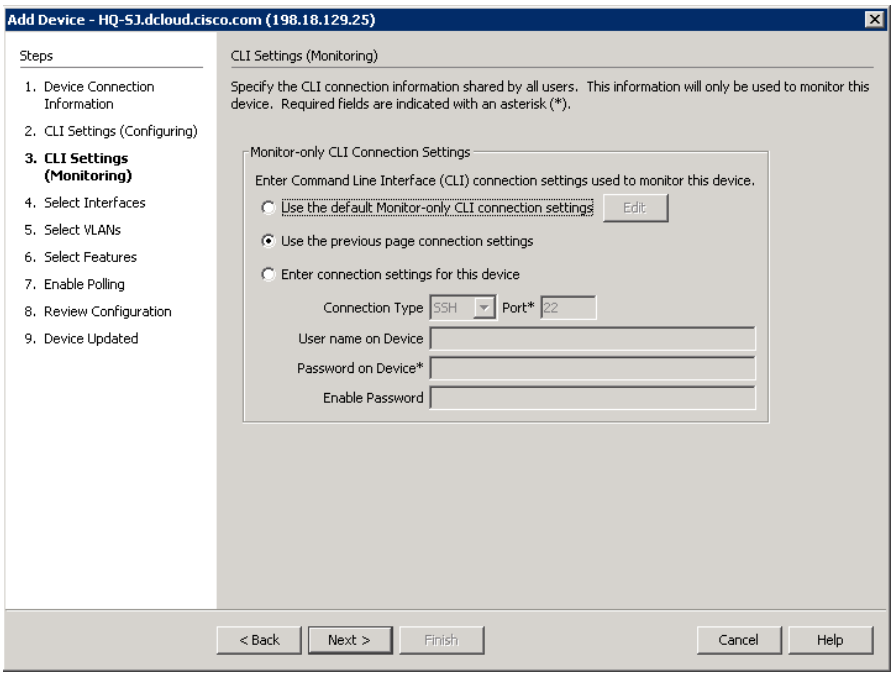
4. Click Next.

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



A 3

6. Click Next.



A 4

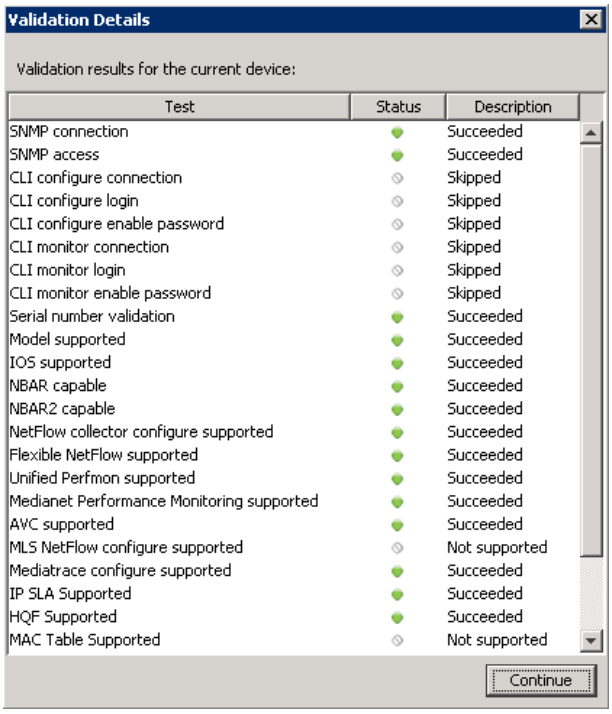
7. Select “Use the previous page connection settings”.
8. Click Next.

 © Copyright LiveAction 2022

4/8/2022

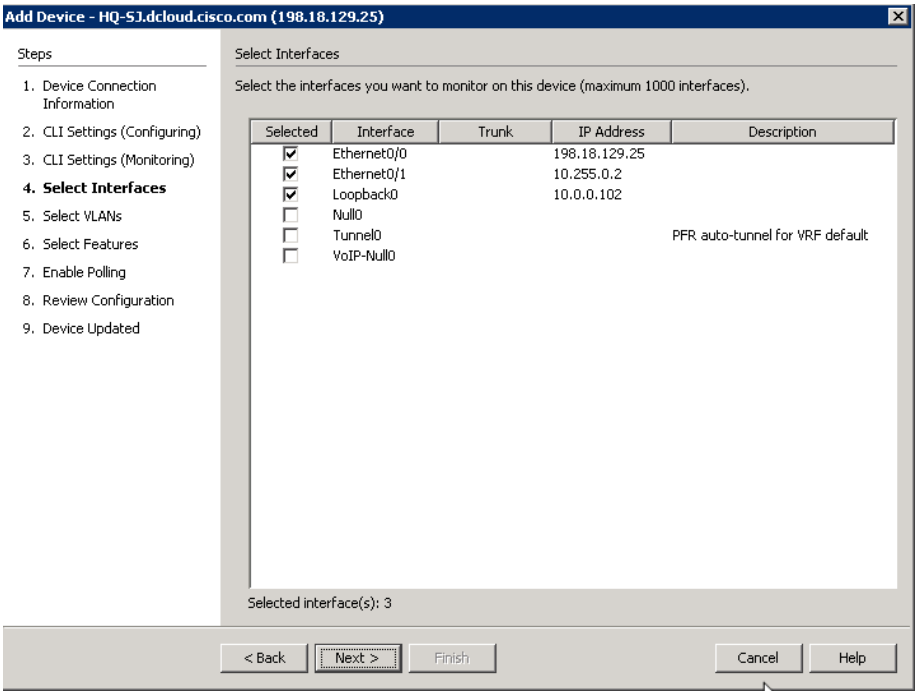
You can verify what capabilities LiveAction is able to interact with the device.

9. Click Continue.



A 5

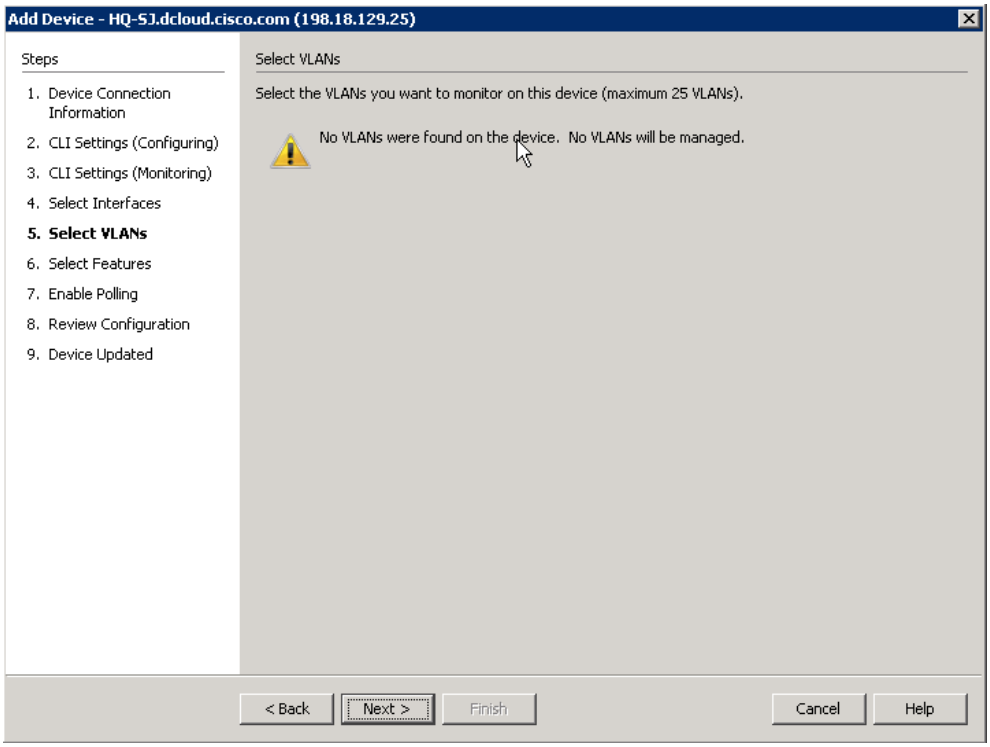
On the select interfaces window you may notice 3 interfaces are already selected. LiveAction automatically selects the interfaces based on the highest bit rate.



A 6

10. Click Next.

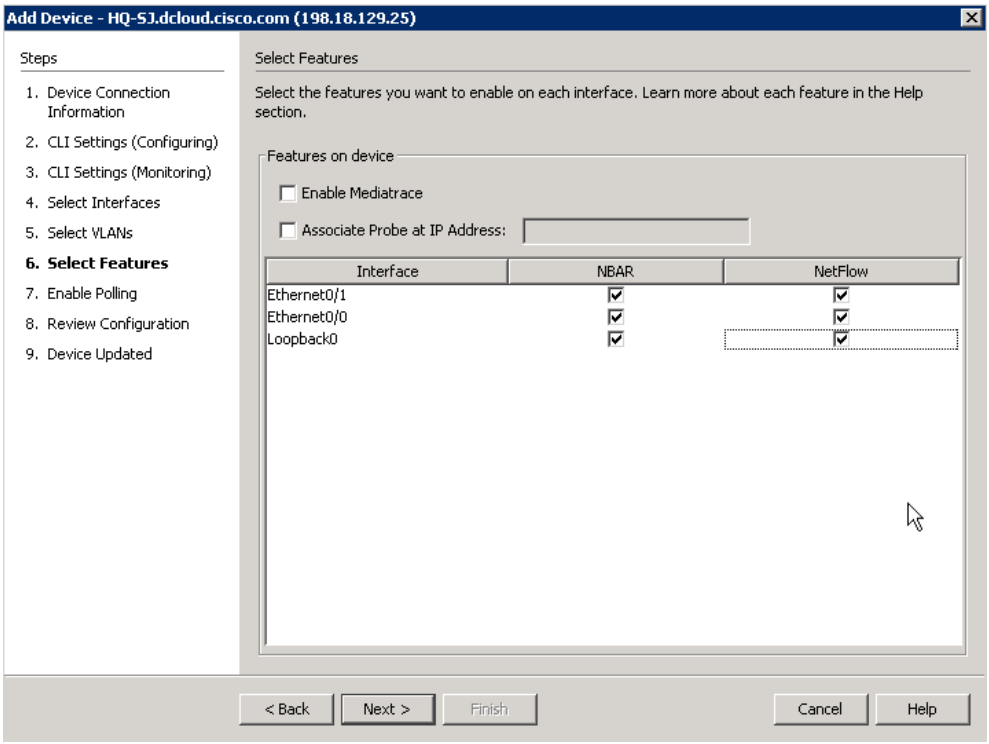
Note: Since there are no VLANs configured on this device, none will be displayed. You may monitor up to 25 configured VLANs on each device.



A 7

11. Click Next.

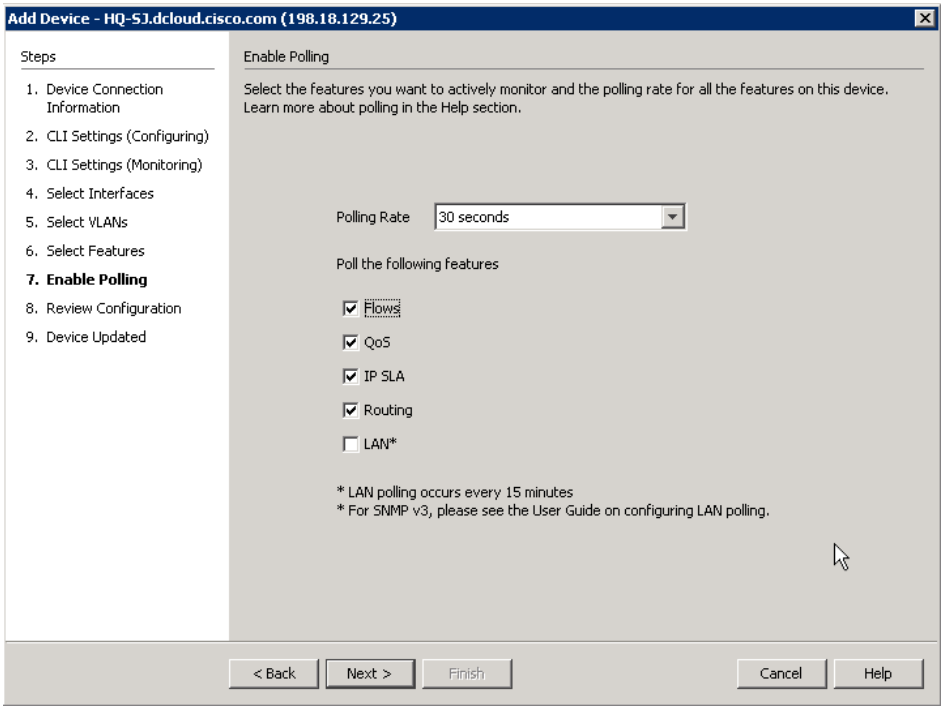
The **Select Features** dialog allows you to turn-on specific Cisco technologies using the templates included in LiveNX. This dialog displays the current IOS configuration of the device you are currently viewing. Leave this screen **AS-IS**.



A 8

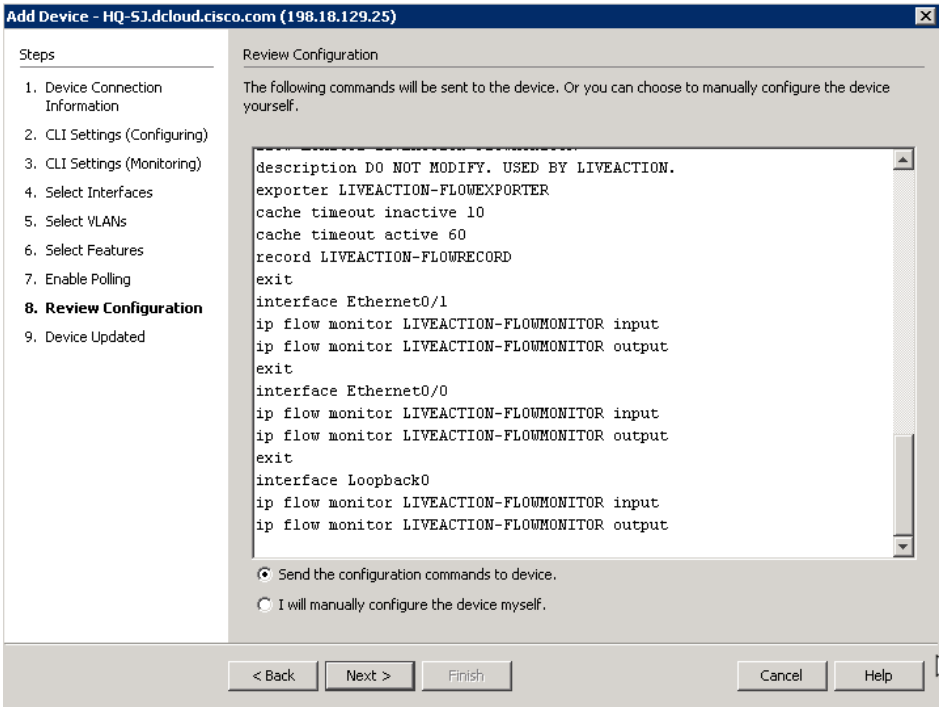
 © Copyright LiveAction 2022

12. Click Next.
13. Change the polling rate to 30 seconds.
14. Verify that ONLY the **Flow** & **QoS** boxes remain checked.



A 9

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.

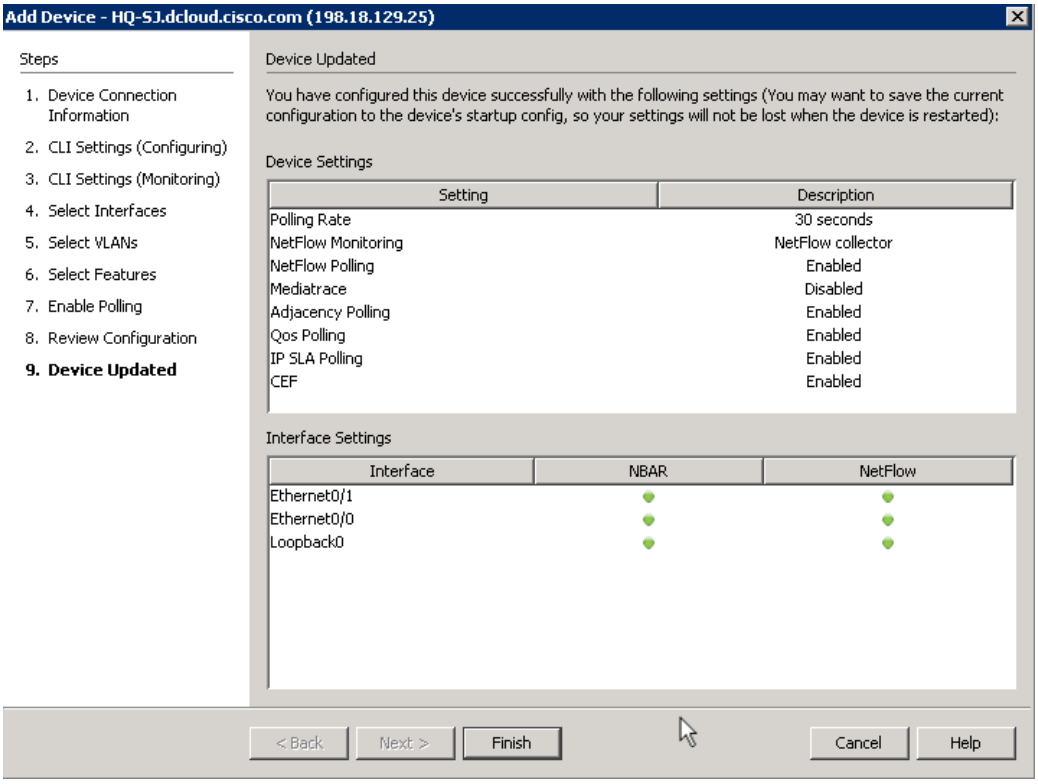


A 10

 © Copyright LiveAction 2022

15. Select “Send the configuration…” radio button, if available.
16. Click Next.

17. Click Finish.



A 11

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).

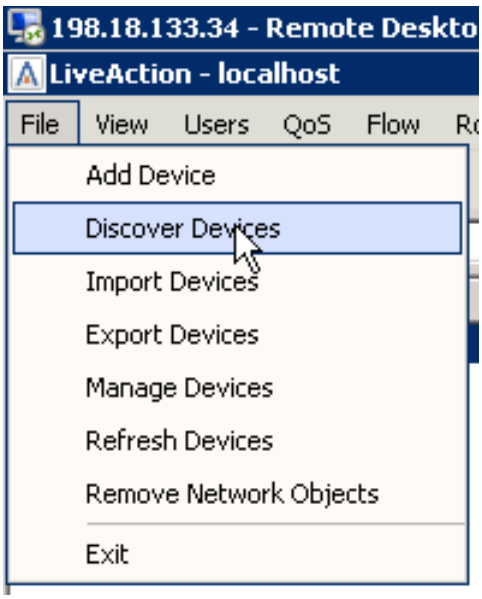
 © Copyright LiveAction 2022

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:

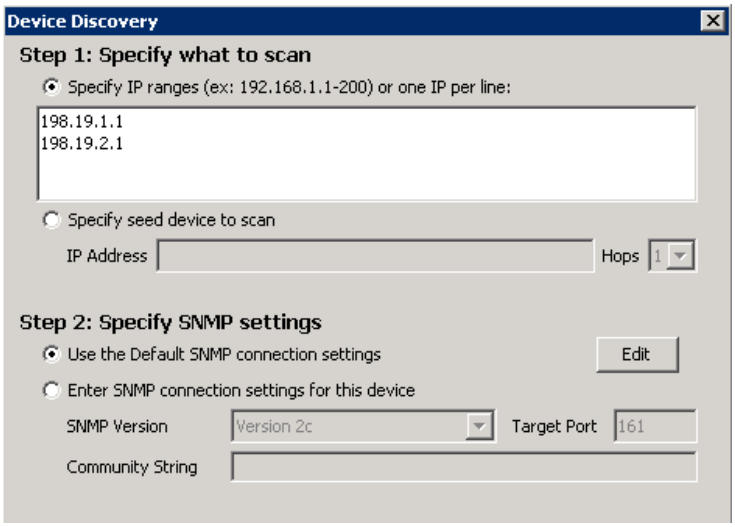
1. Select File and Discover Devices.



A 12

2. Specify the following IP addresses:
   198.19.1.1
   198.19.2.1

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



A 13

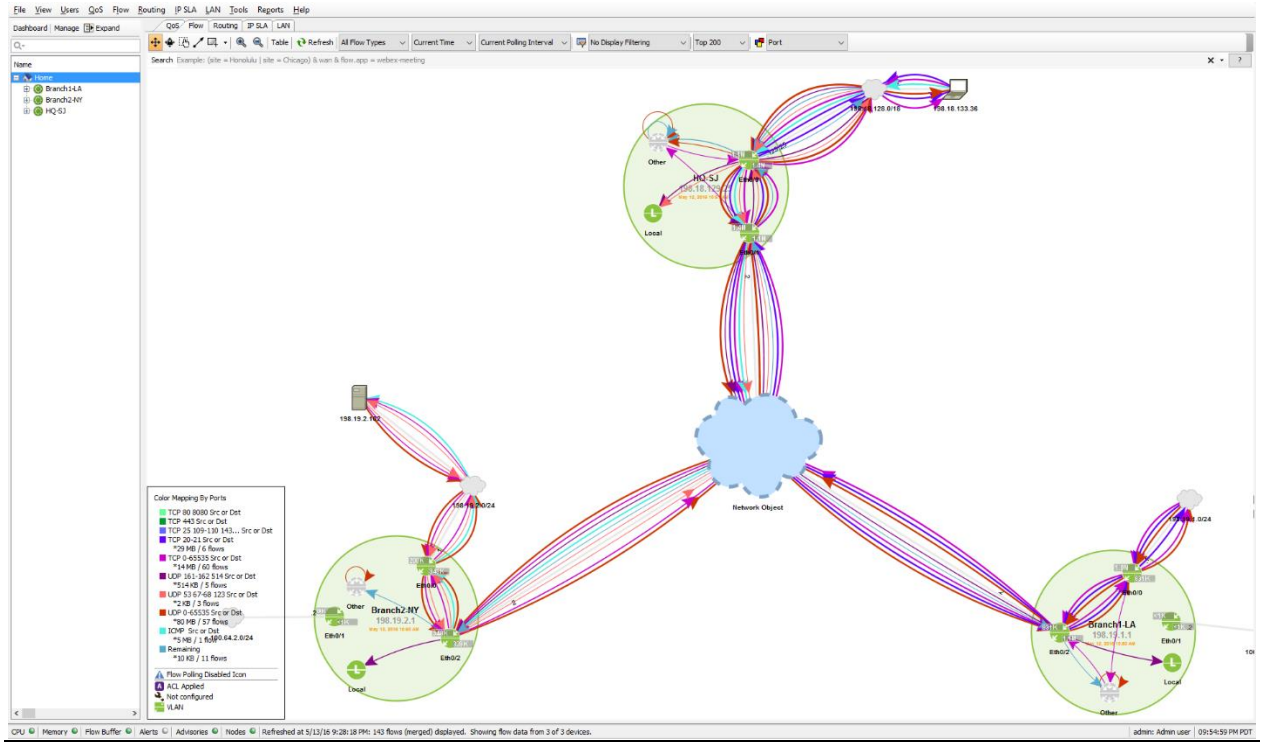
 © Copyright LiveAction 2022

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.

A 14

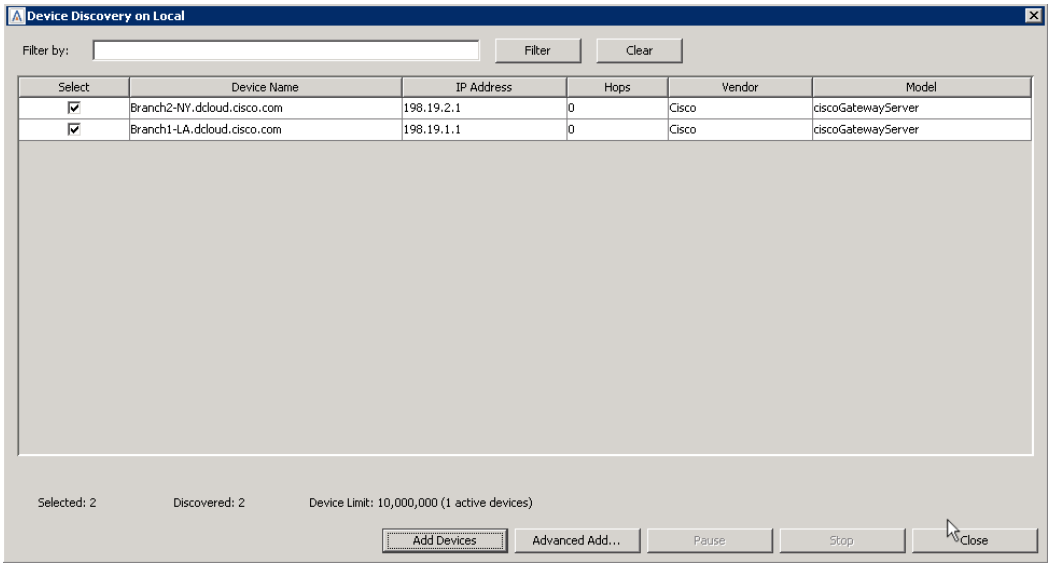
4. Click OK.
5. Verify that both devices were found, and then select Add Devices.

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.



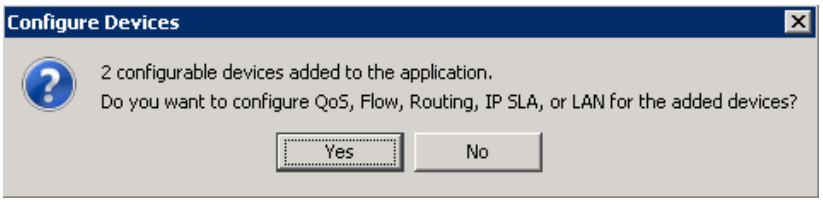
A 15

 © Copyright LiveAction 2022



A 16

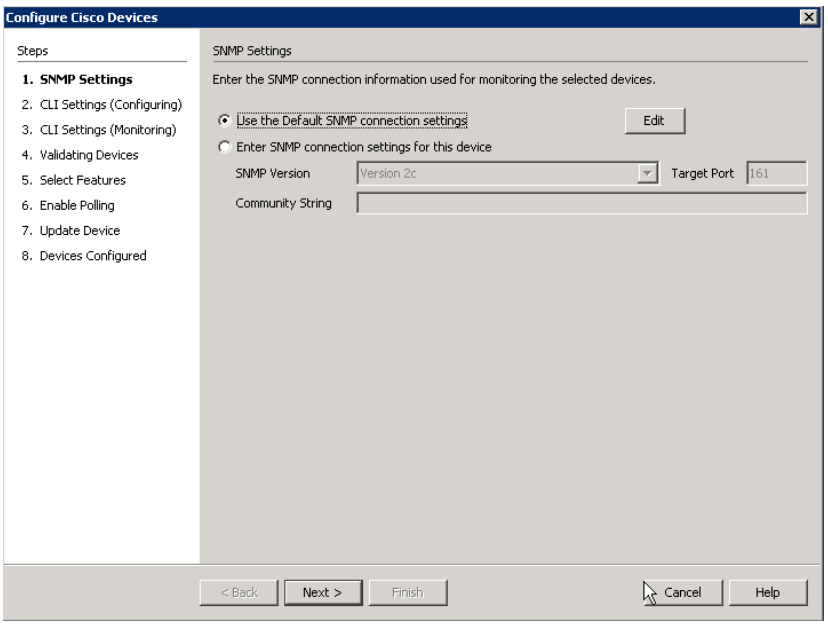
6. Select Yes on the configure devices dialog.



A 17

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

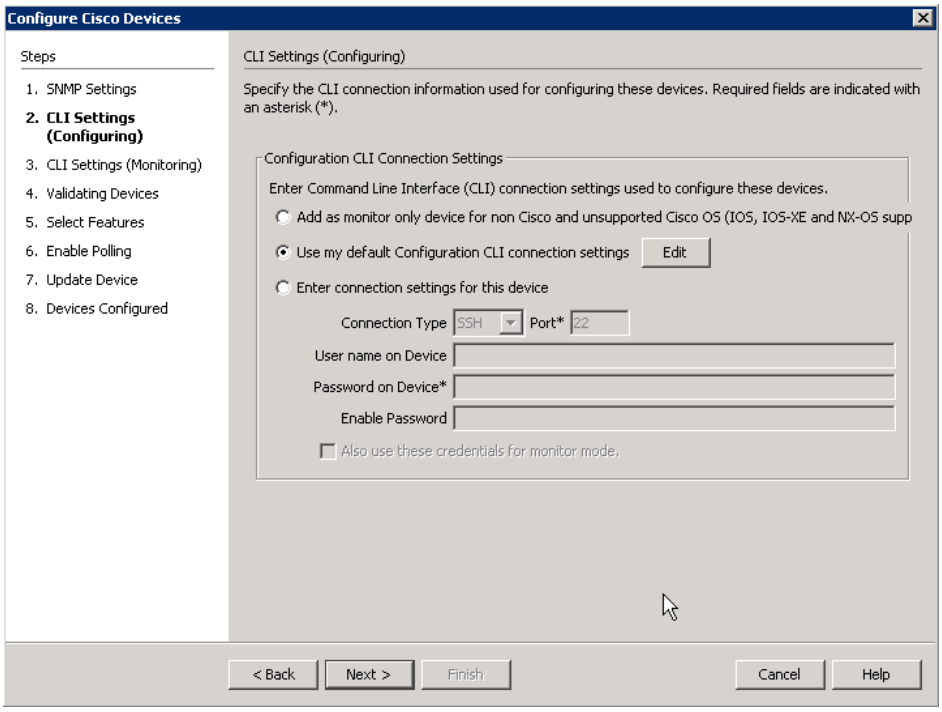
Note: You must be logged-in as the original admin user so that the LiveNX Wizard will inherit the appropriate credentials. Ask your instructor for clarification on this, if desired.



A 18

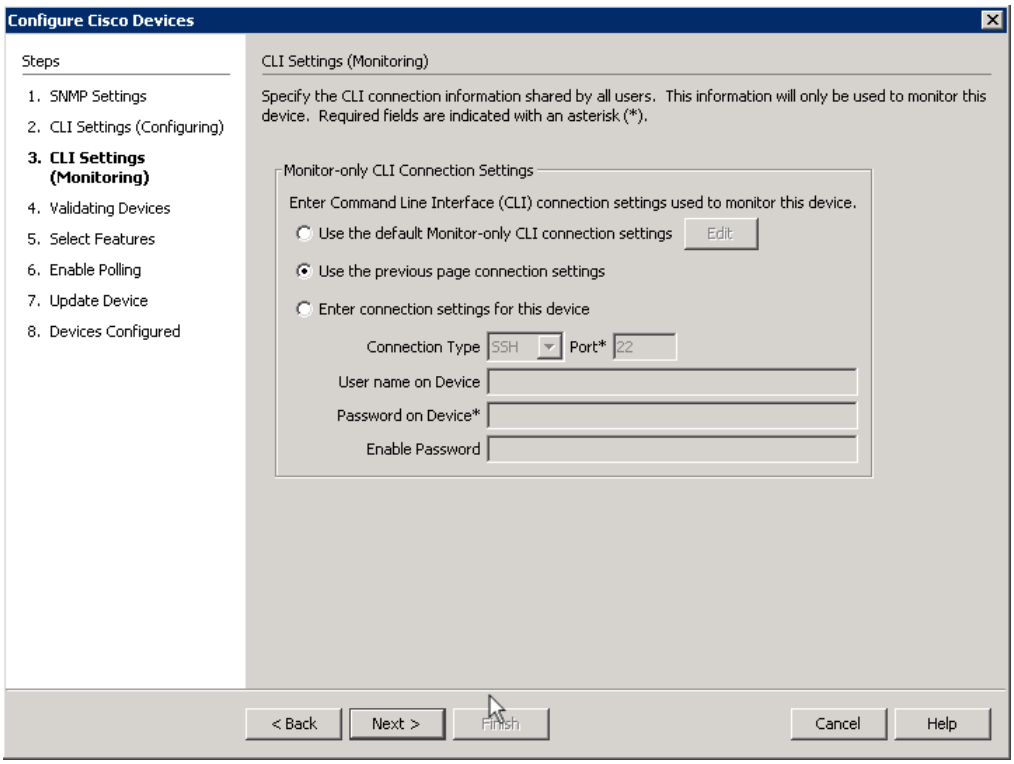
 © Copyright LiveAction 2022

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



A 19

10. Select Use the previous page connection settings.

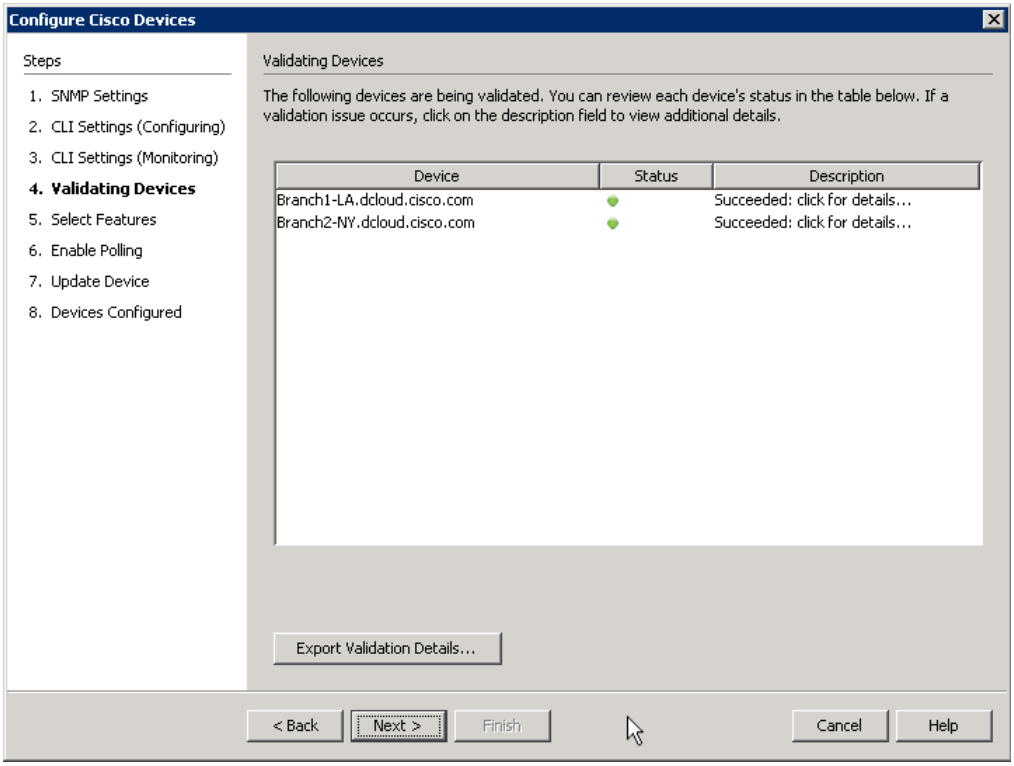


A 20

11. Click Next

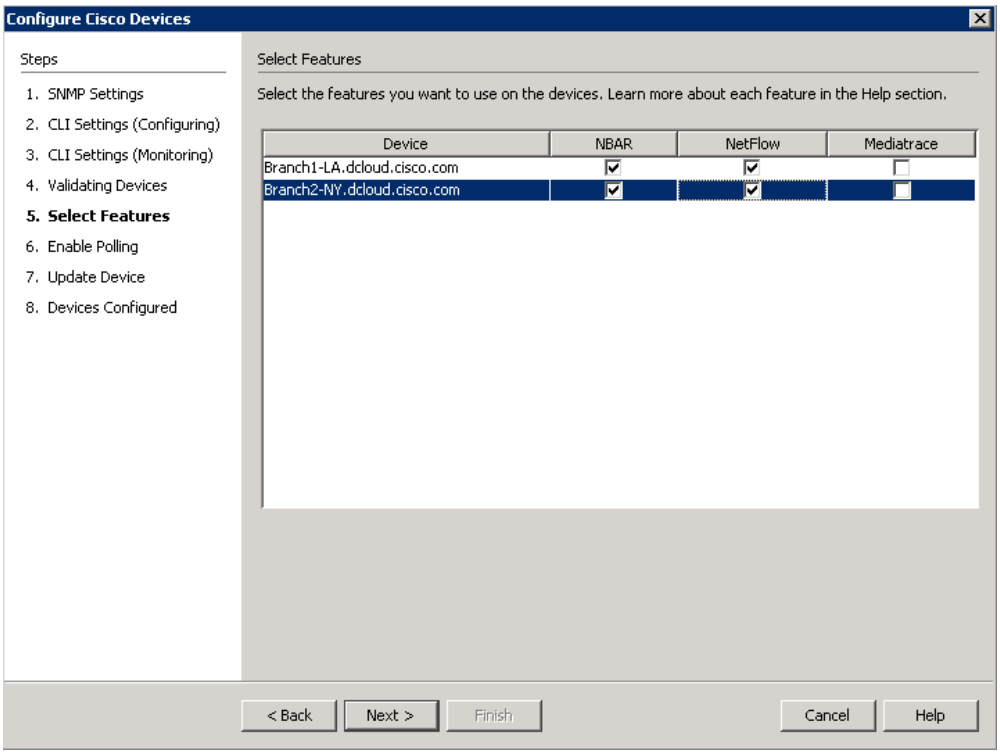
 © Copyright LiveAction 2022

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



A 21

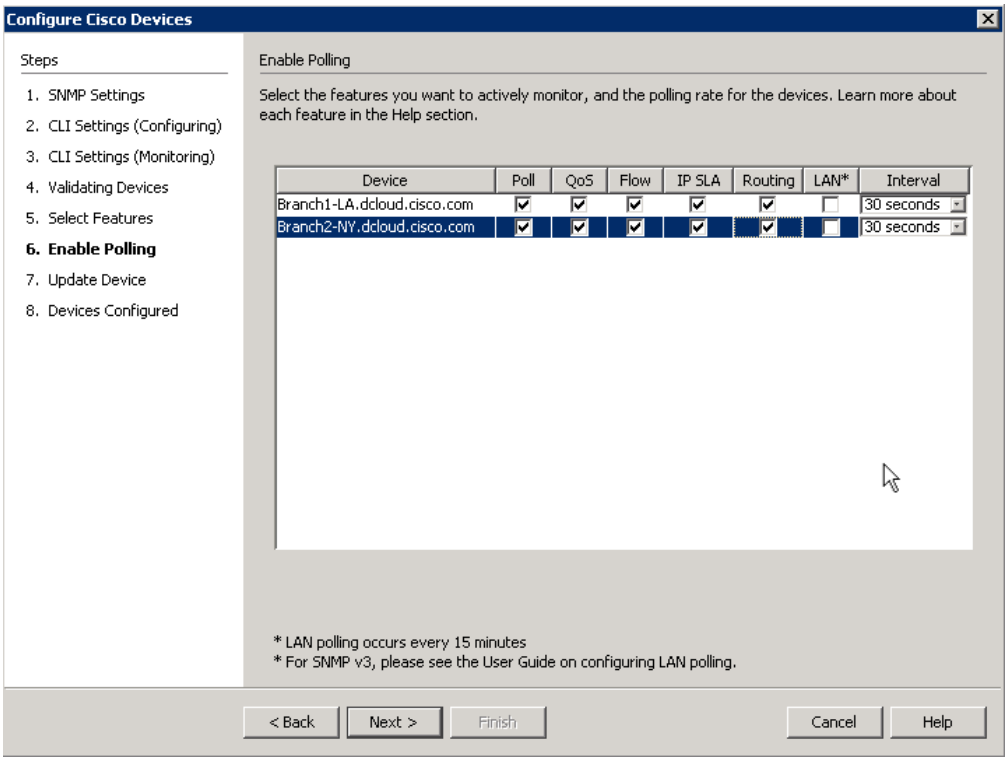
13. Select NBAR and NetFlow for both devices, Click Next.



A 22

14. Select all technologies excepting LAN.
15. Set the interval to 30 seconds for each device, Click Next.

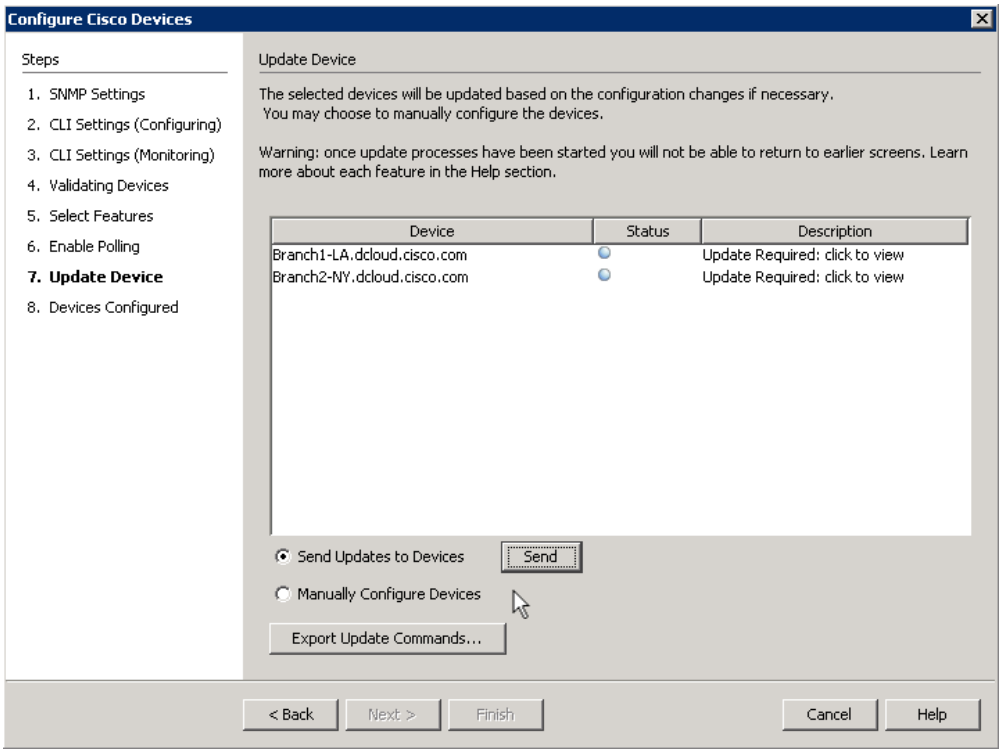
 © Copyright LiveAction 2022



A 23

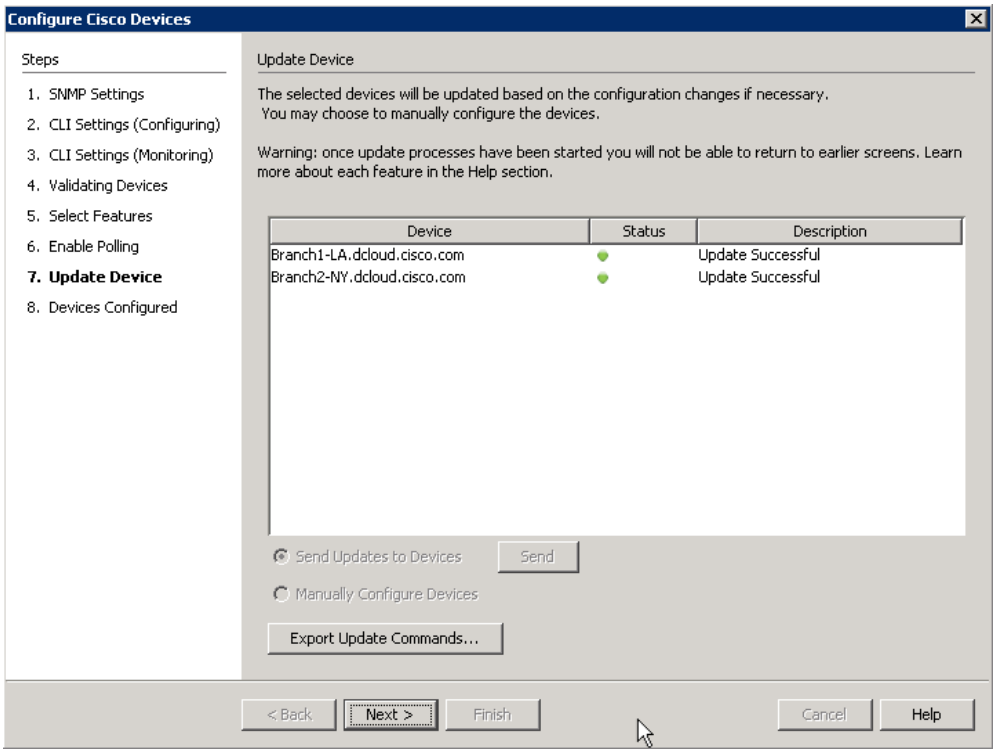
Note: For our class Labs we are gathering data every 30 seconds to reduce wait time when we make changes. In a production environment this may generate more network traffic than desired.

16. Select Send Updates to Devices and click Send.



A 24

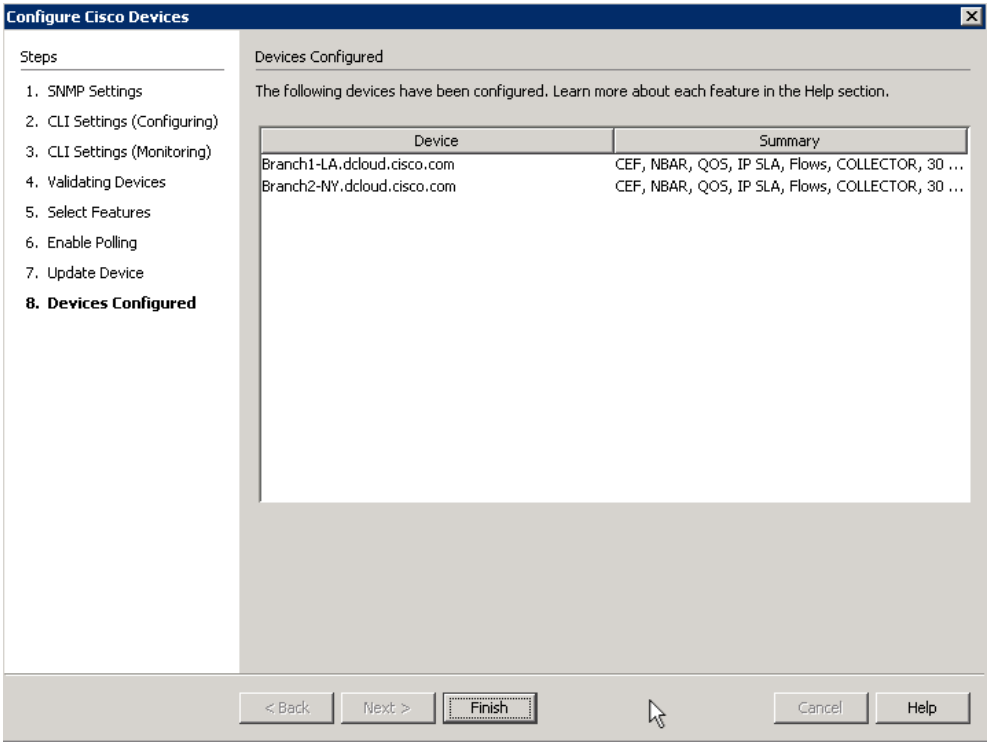
17. Once the updates are pushed successfully, click next.



A 25

 © Copyright LiveAction 2022

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



A 26

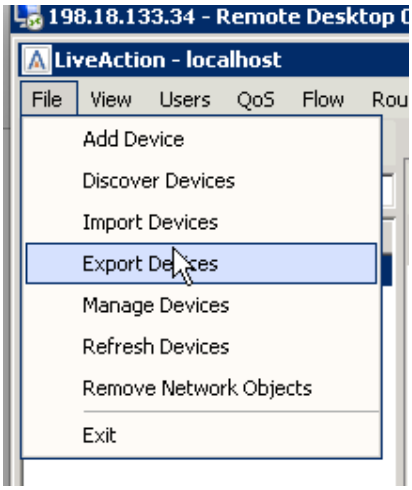
Now that you have added three devices to the topology, they should look familiar to the image below. What is important to remember is that you should only bring in interfaces that will have interesting traffic, to you, traversing them. We will not need all the interfaces that have been included, so in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

 © Copyright LiveAction 2022

Lab A.3: Export/Import Device Configuration

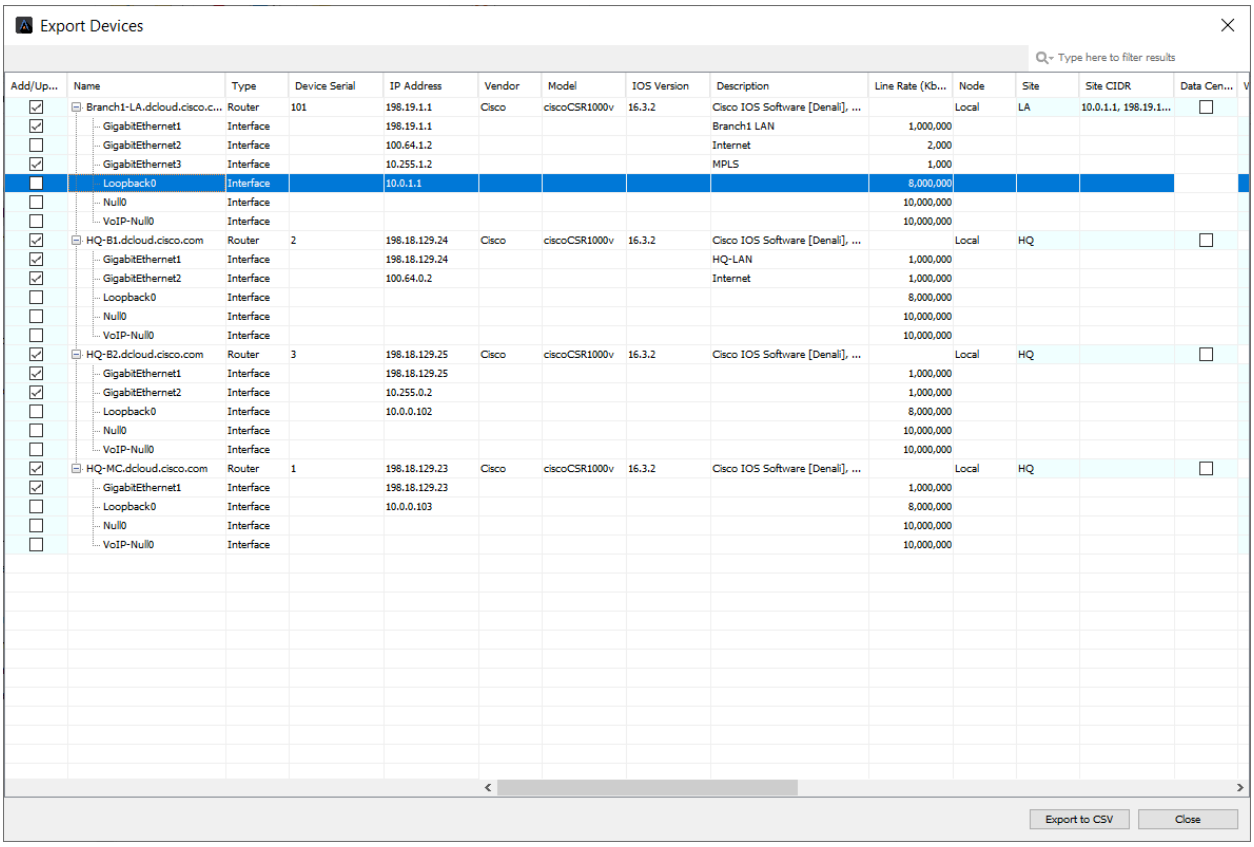
Lab Steps:

1. From the File Menu select Export Devices.



A 27

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

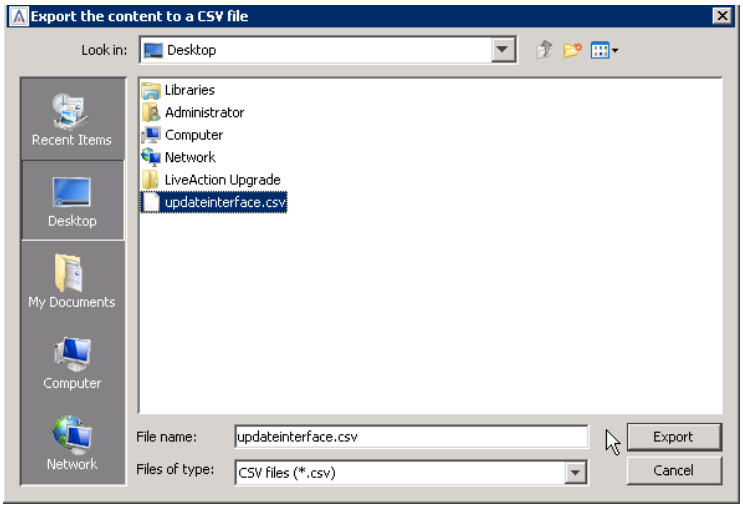


Add/Up...	Name	Type	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (Kb...	Node	Site	Site CIDR	Data Cen...
☑	Branch1-LA.dcloud.cisco.c...	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali], ...		Local	LA	10.0.1.1, 198.19.1...	☐
☑	GigabitEthernet1	Interface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

A 28

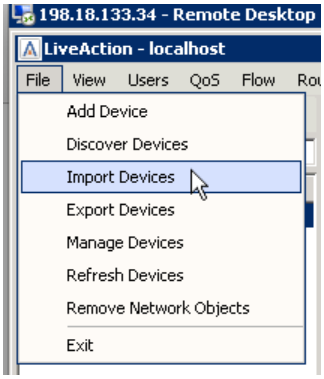
3. Select Export to csv.

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



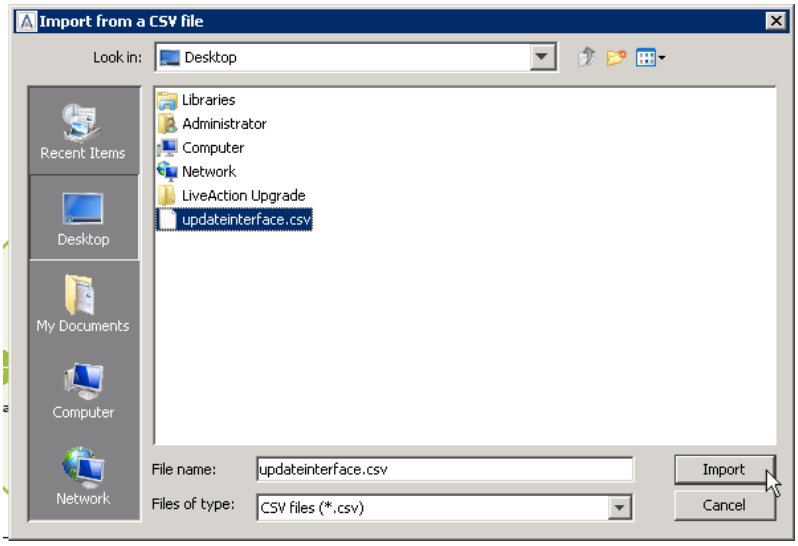
A 29

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



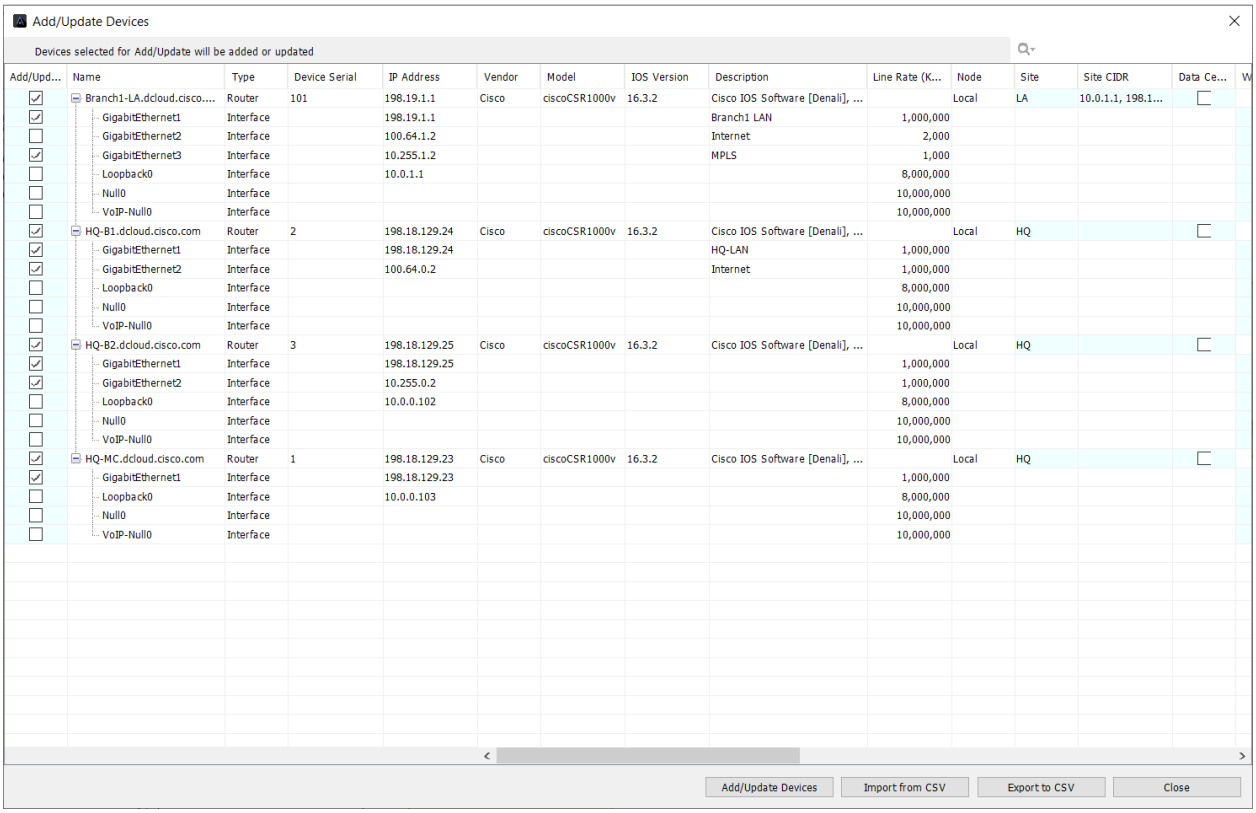
A 30

8. Select the file you previously exported.



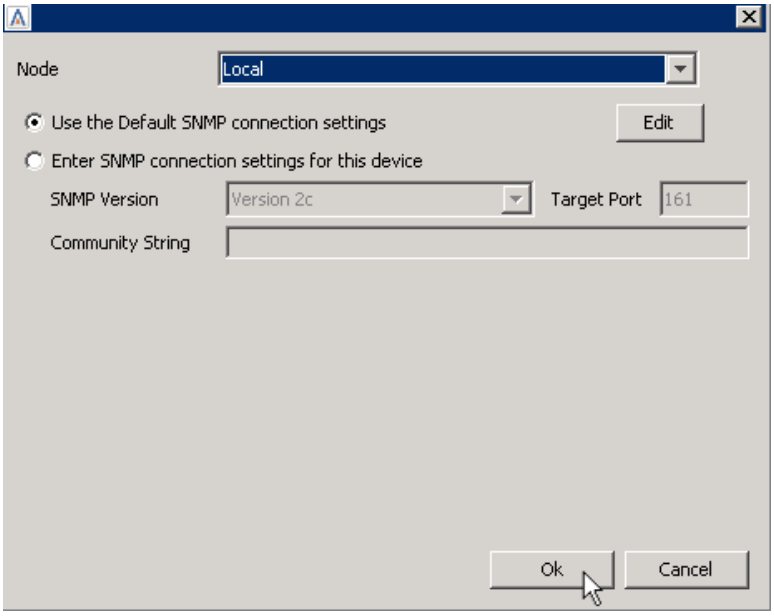
A 31

9. Click Add/Update Devices.



A 32

10. Click OK to use the Default SNMP settings.



A 33

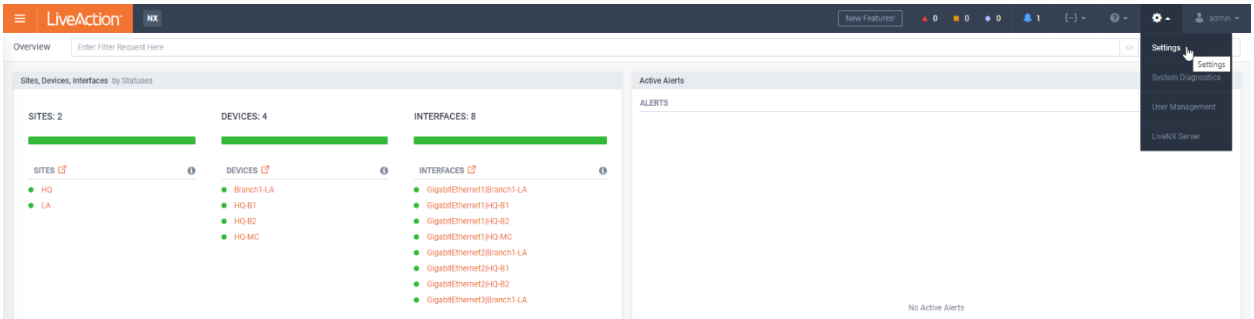
Your Topology Pane will now show the appropriate devices/configurations.

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.

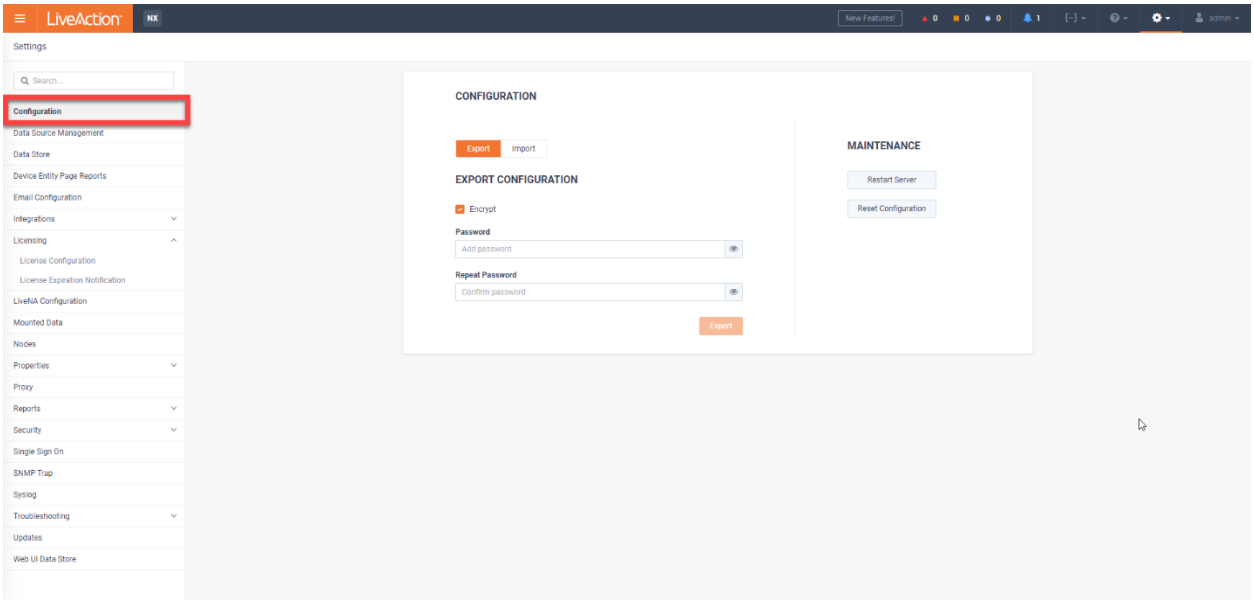
Lab Steps:

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



A 34

2. Select **Configuration**.

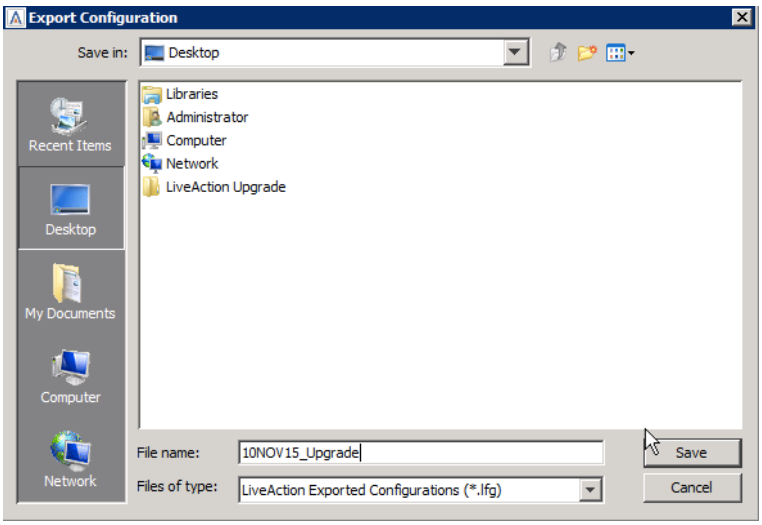


A 35

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

 © Copyright LiveAction 2022

4/8/2022



A 36

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.

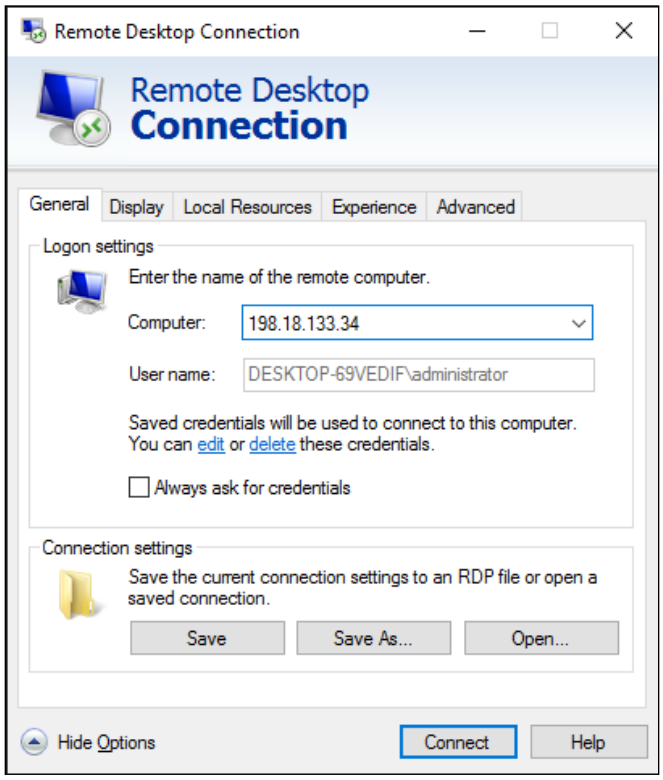
Note: Use the information from the Lab Details table to connect to the desired device.

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 37

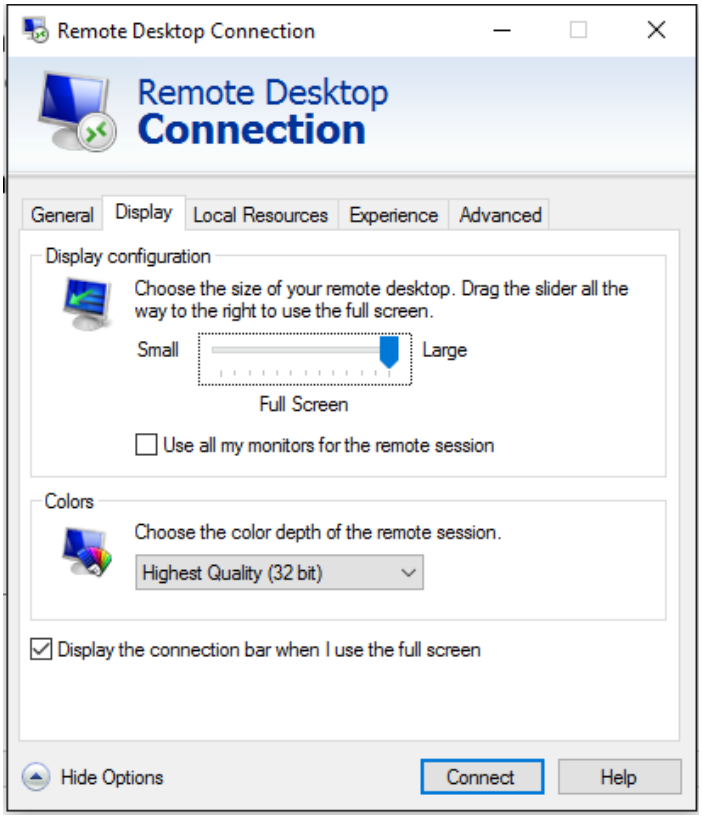
a. Enter the following fields:
   •Computer: **<ipaddress> :20201**
   (From your Lab Access worksheet)
   •Username: **administrator** (or otherwise defined by instructor)

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.

4/8/2022

✓

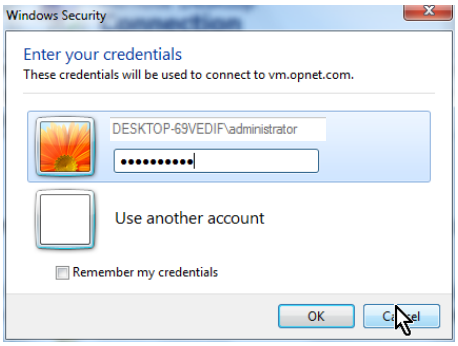
DIAGRAM



A 38

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

DIAGRAM



A 39

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 not lose any work.