LiveAction Training

Lab Workbook Pt. 1

July 2022.

Table of Contents

IMPORTANT INFORMATION – Please Read!

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

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

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

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

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

Lab .0

Lab 0: Setup and Get Connected

Lab 0.1: Connect to the Lab Network

For this class, each attendee or Student will connect to and manage their own LiveNX installation hosted by Criterion Networks. In this lab you will login to the hosting portal and connect to the lab environment.

You have been assigned a dedicated environment or "Pod", and this document provides you with information to help you login and run the hands-on labs. Your **Username** and **Password** should have been sent to you ahead of the course.

To login, go to https://portal.criterionnetworks.com/ and enter the username and password that the instructor has shared with you. (Make sure to click the Terms and Conditions Check Box).

Each Student will manage:

Local:
1 x PC Workstation to be used as a Management PC (Your Laptop)
1 x Installed LiveNX Client (installation performed in the class)
1 x Browser (Chrome or Firefox recommended)

Remote Student Pod
1 x LiveNX OVA Linux install
    1 LiveNX Server
    1 LiveNX Node (installed on LiveNX Server)
1 x Network topology (shown below)
1 x Windows Workstation (May be accessed via RDC but not required) and Browser
2 x Remote PC's located in Branches (may be accessed via RDC but not required)

DIAGRAM

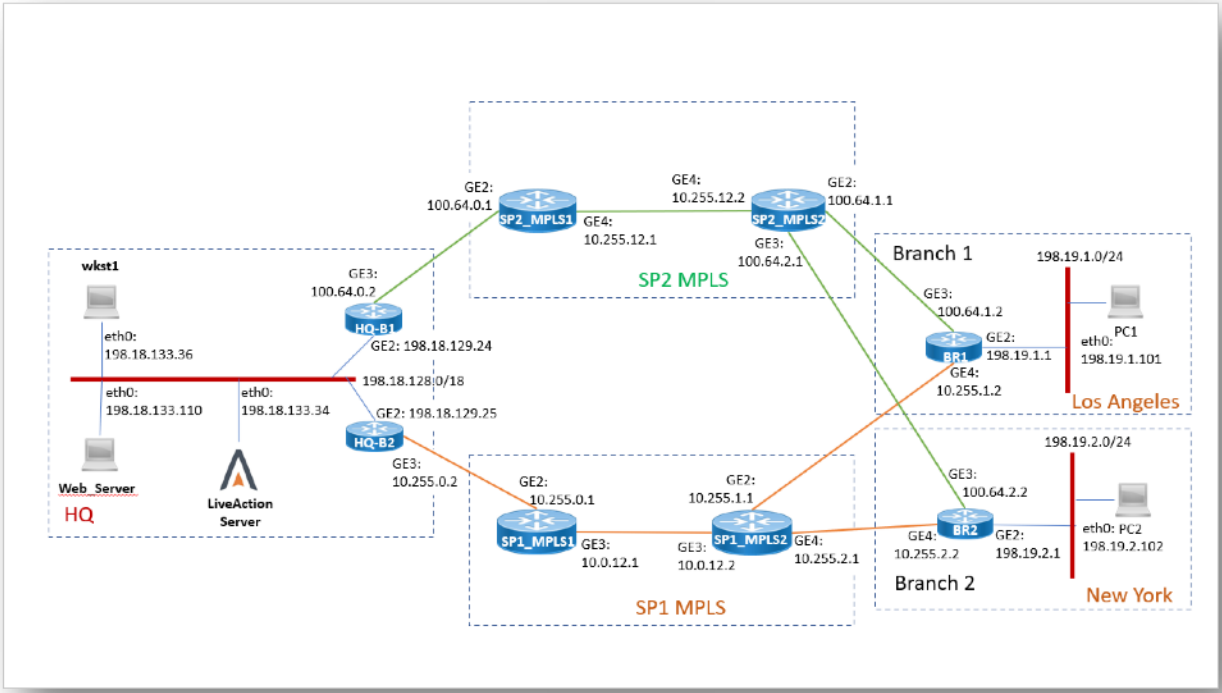


Figure 1 – Training Pod Topology

Lab Steps:

1. Connect your computer to the Internet.
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 by the Access Devices page in the Training Lab Portal.

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

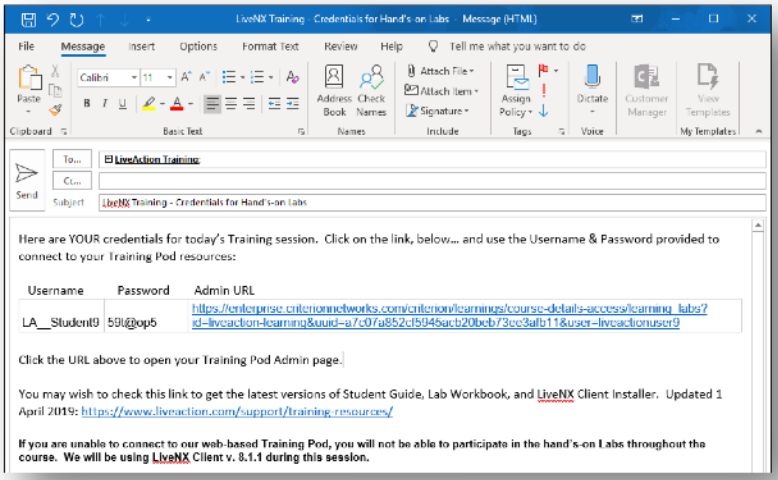


Figure 2

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. You will be taken to the **Home Screen**, where you will see Learning Options. Your Labs will be found in the **Learning Center** tile on the right.

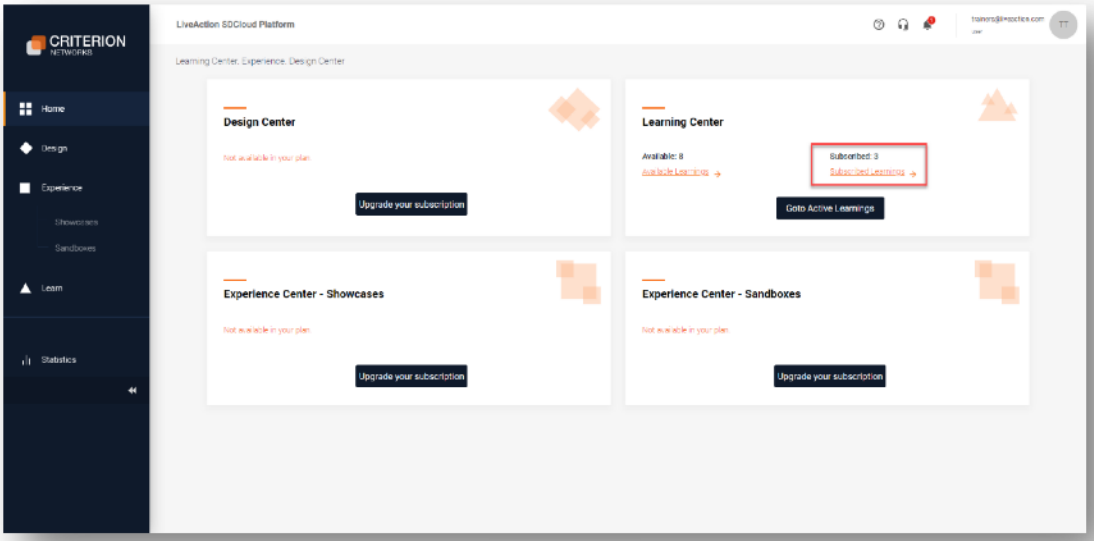


Figure 3

6. To find your Labs, click on the **Subscribed** option in the **Learning Center** tile.

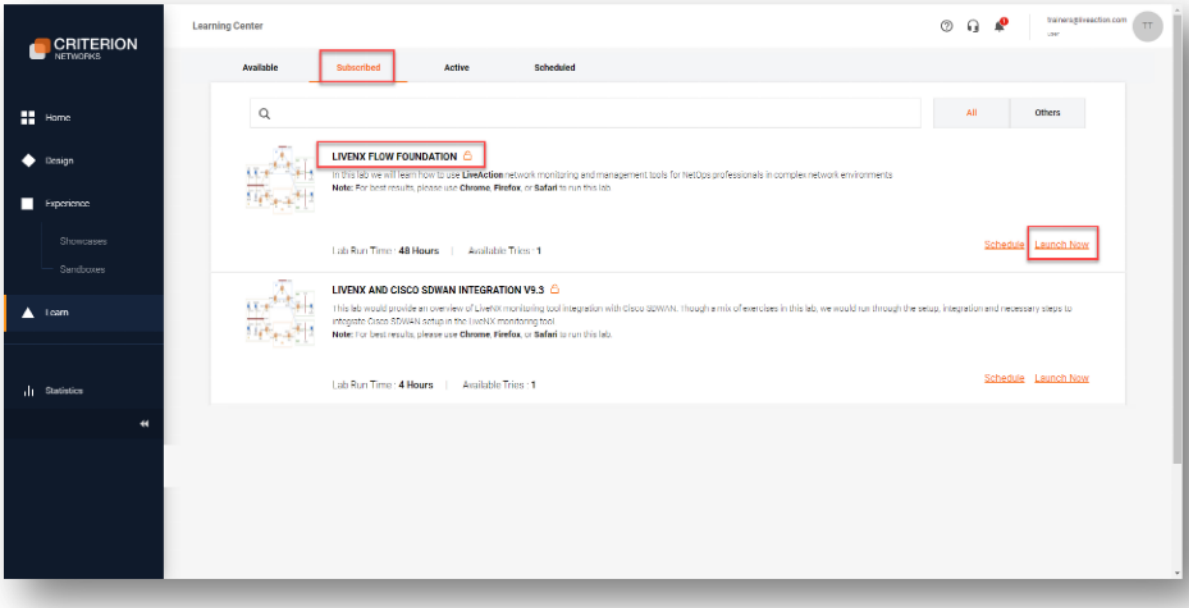


Figure 4

7. The Lab Pod may or may not be running already. You can check this status by looking to the right of the panel of the LiveNX Flow Foundations lab. If it says **Launch Now**, you should launch the lab by clicking **Launch Now**. If it says **Access Lab,** then it is already launched, and you can access it by clicking the **Access Lab** link.
8. Once in the lab menu click **Access Devices**.

9. Here you have two tabs: Topology, which is a live **Topology** map (click devices to access them), and **Lab Details**, which lists the IP addresses and ports of the devices. You can Remote Desktop Connect to the workstation and PC's in the labs.

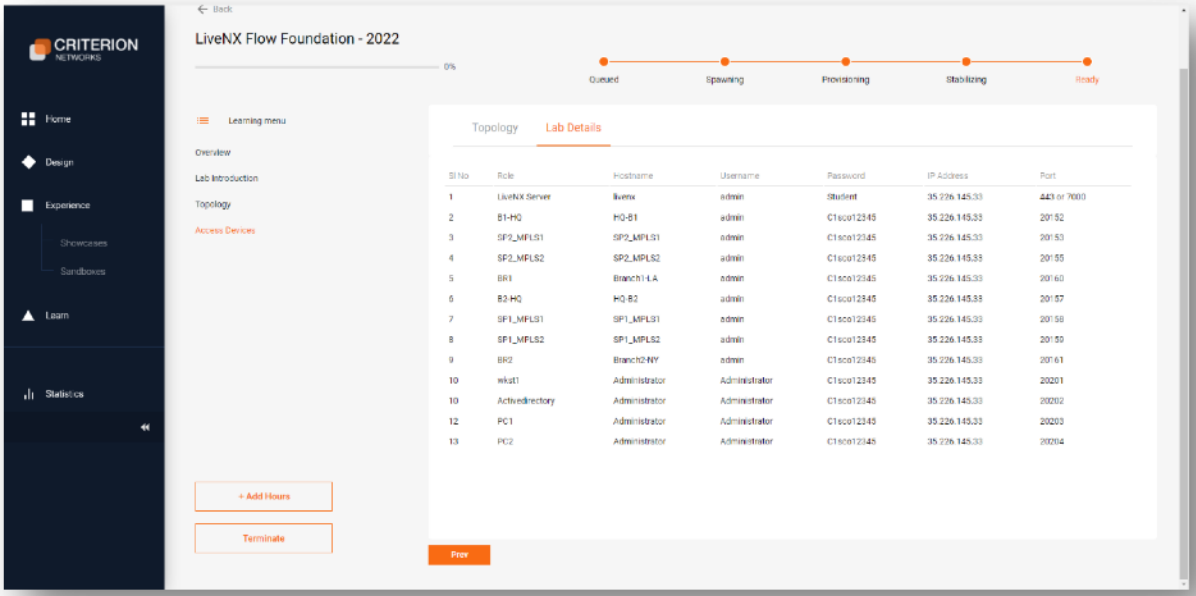


Figure 5

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:

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

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

Lab 1

Lab 1: The LiveNX Web UI

Lab 1.1: Explore the Web UI

<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:

13. Open your Browser and navigate to the LiveNX Server at https://<ipaddress>

14. Login to the WebUI using: Username: **admin** Password: **Student**

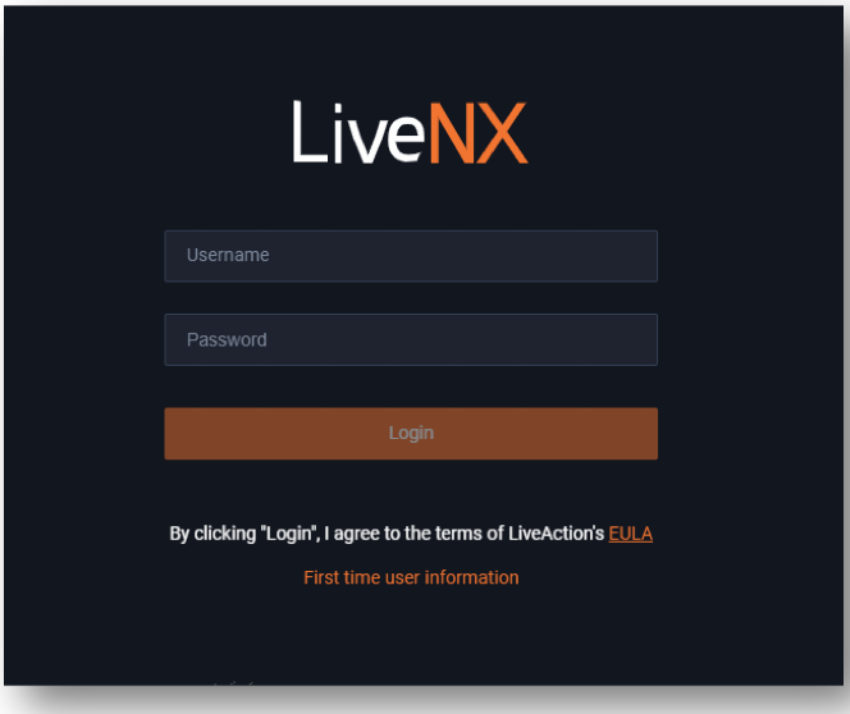


Figure 6

The Overview screen will appear.

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

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

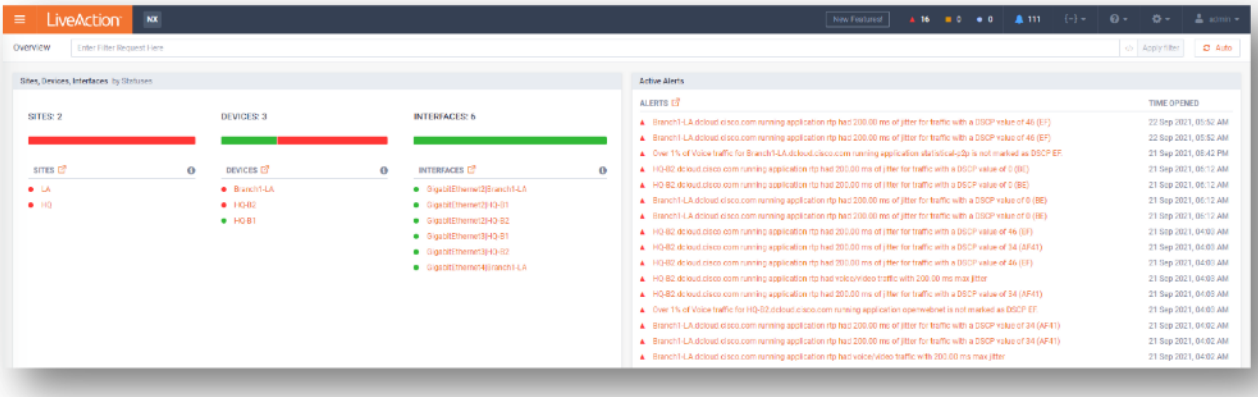


Figure 7

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

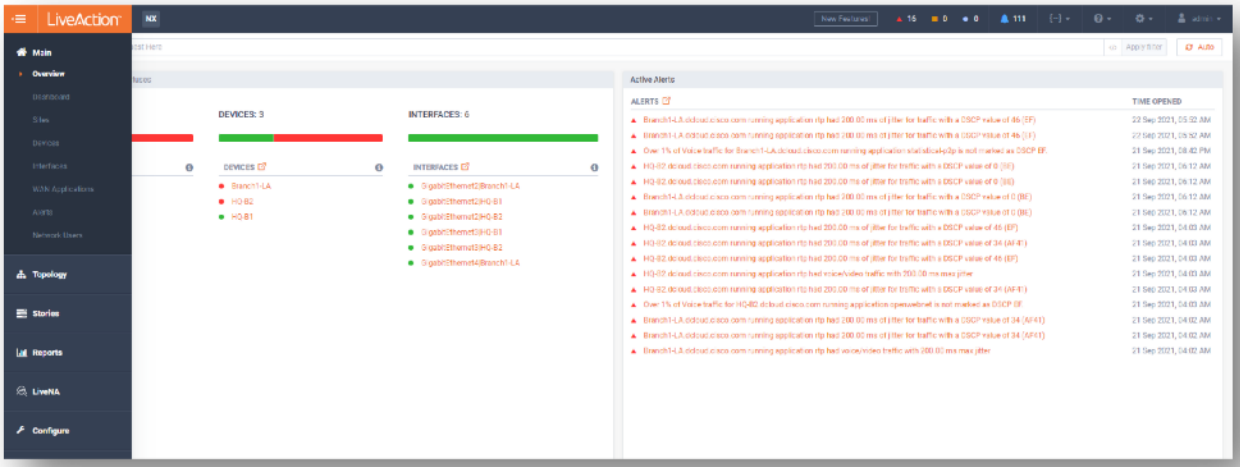


Figure 8

17. Select **Sites.**

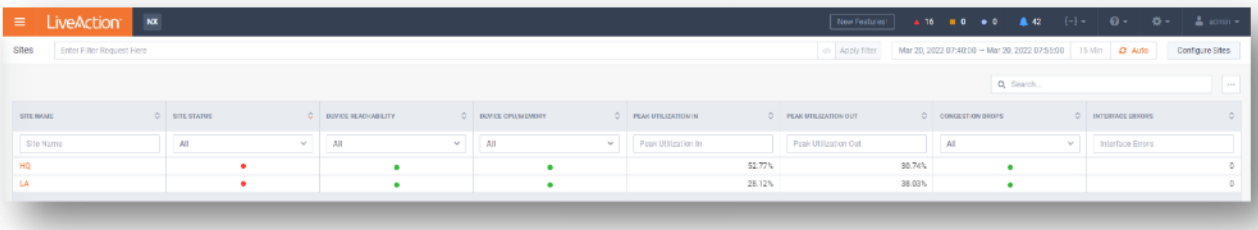


Figure 9

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

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

18. Note: Status, Utilization, Drops, Errors, etc.…

19. Toggle the **Auto Update** to ON.

20. 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).

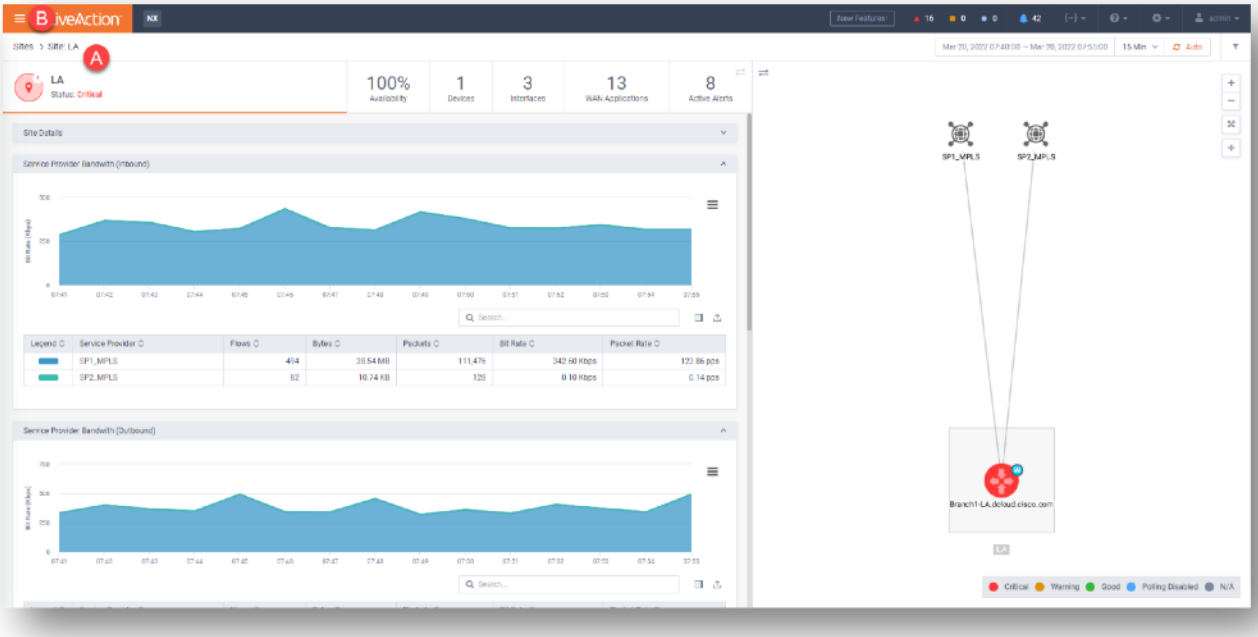


Figure 10

21. Select **Topology** > **Geo Topology**

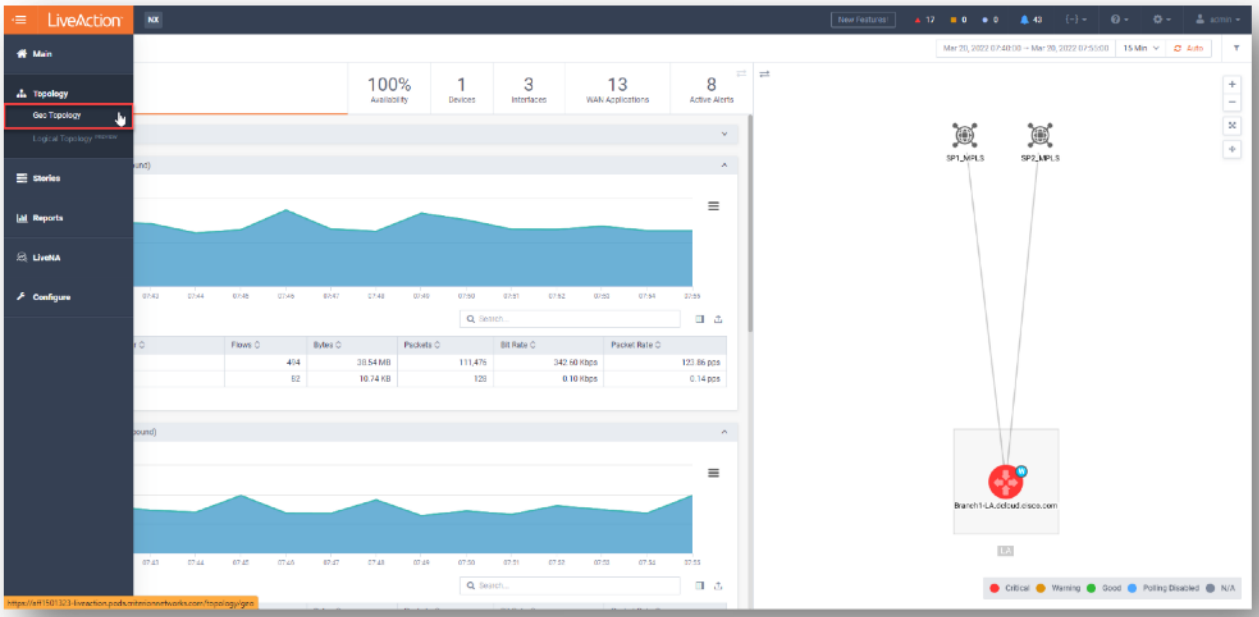


Figure 11

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

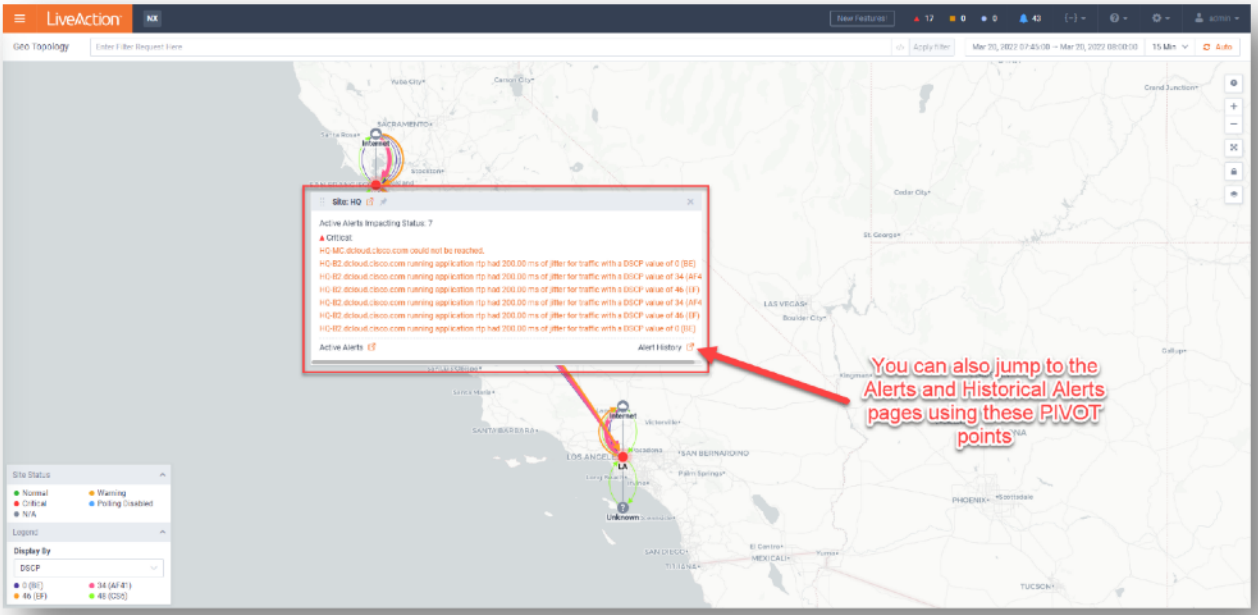


Figure 12

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

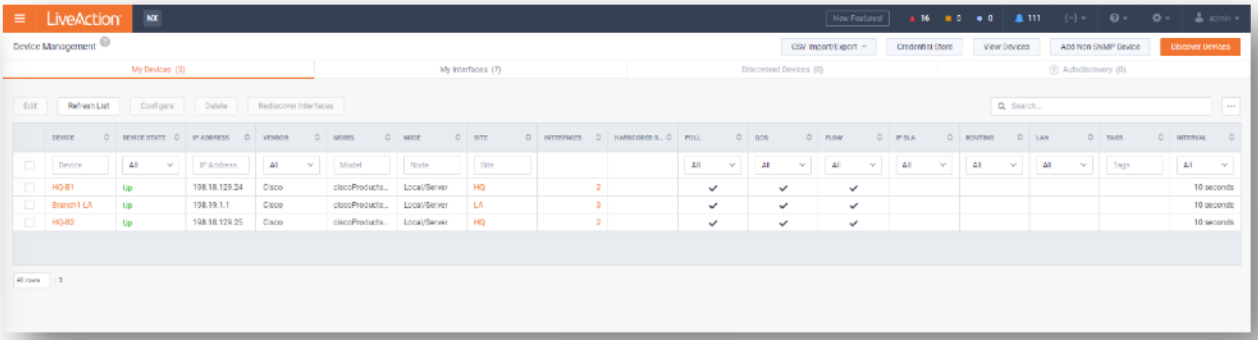


Figure 13

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

Lab 1.2: Dashboard Overview

Note: 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:

25. 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”.

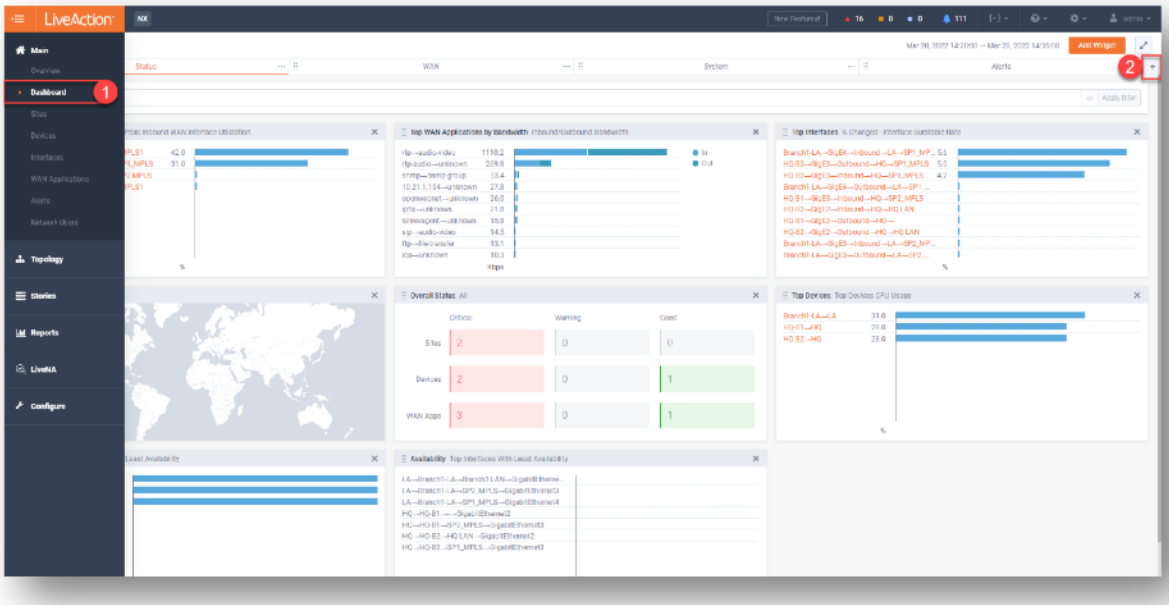


Figure 14

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

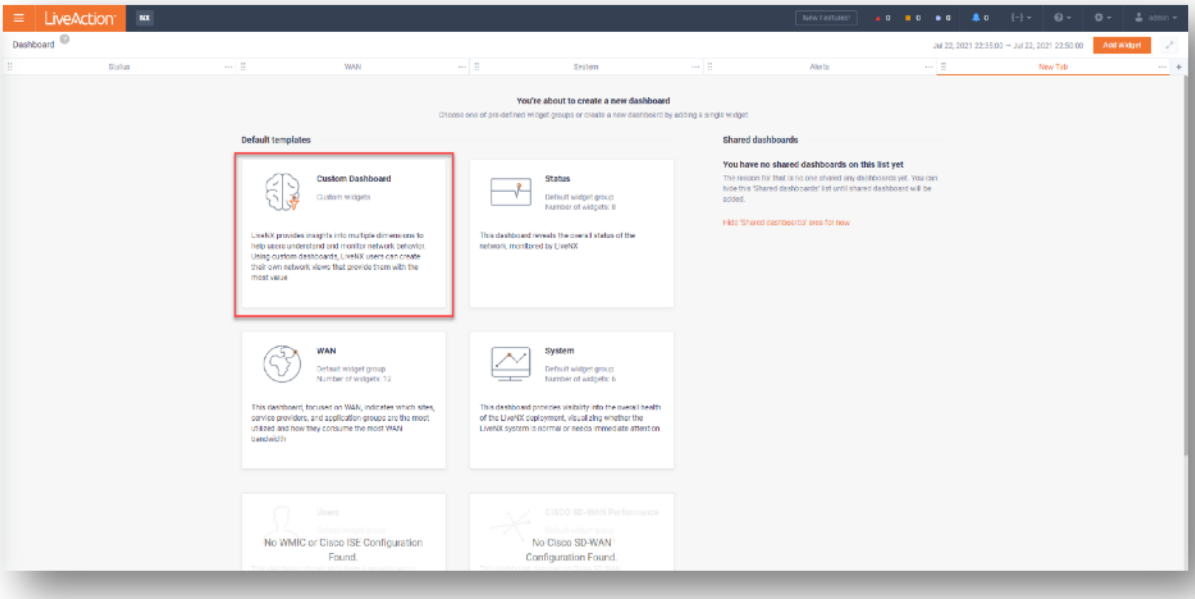


Figure 15

27. 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.

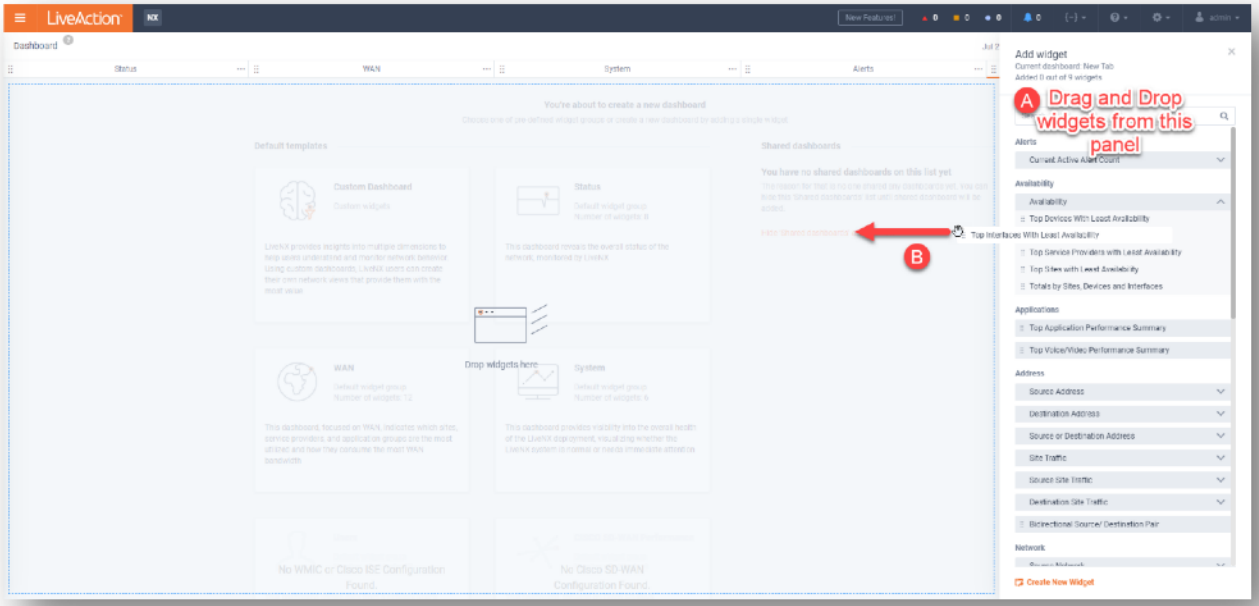


Figure 16

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.

28. **Delete** un-wanted Widgets by clicking the **X** at top right of the widget.
29. To give the dashboard tab a more appropriate name, simply select the **New Tab** text and rename your dashboard.
30. 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.

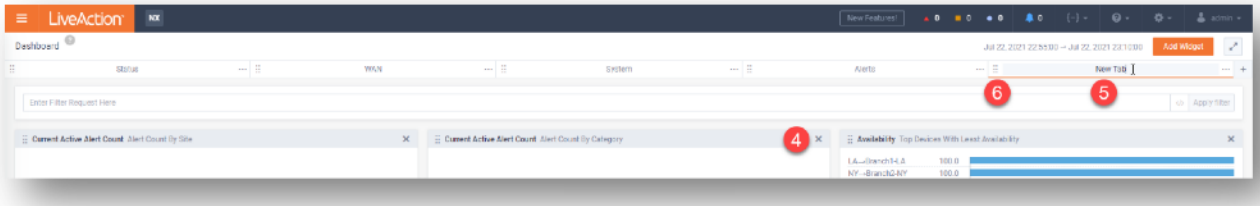


Figure 17

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

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

Lab 1.3: Pre-Configured Stories

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

Lab Steps:

31. Click the **Menu** icon.

32. Select **Stories**, and **Site-to-Site Analysis**.

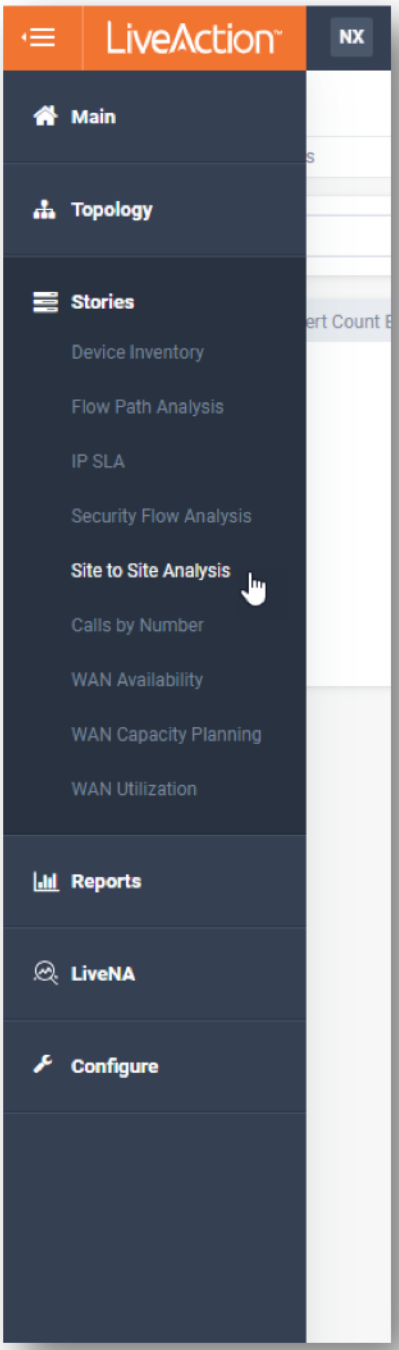


Figure 18

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.

33. Select **Direction > Inbound.**

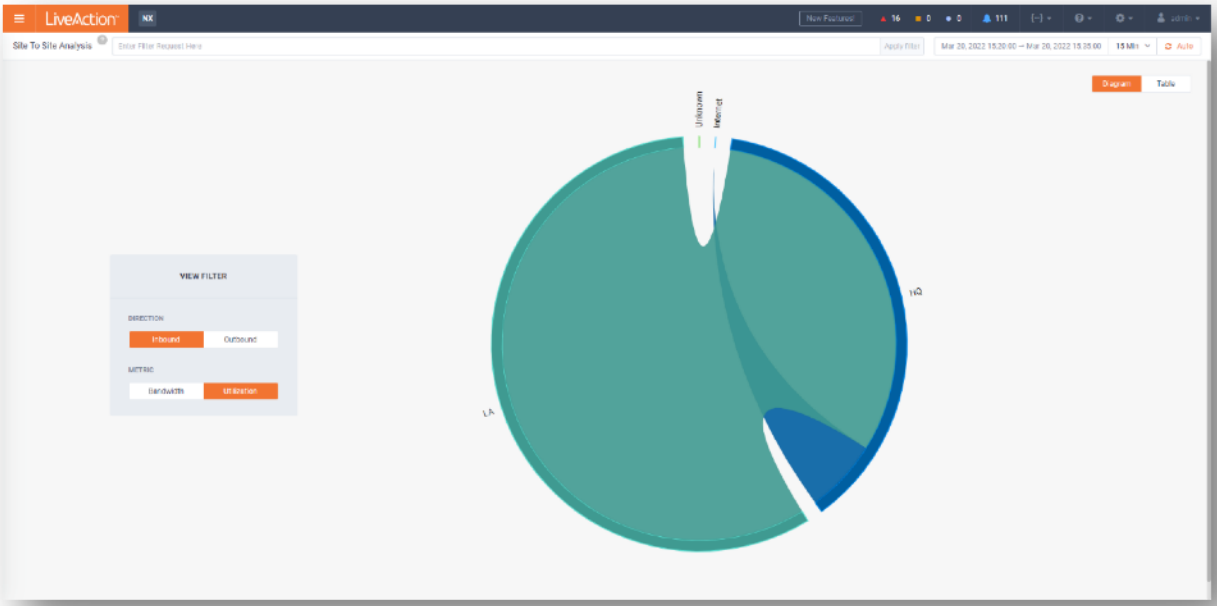


Figure 19

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

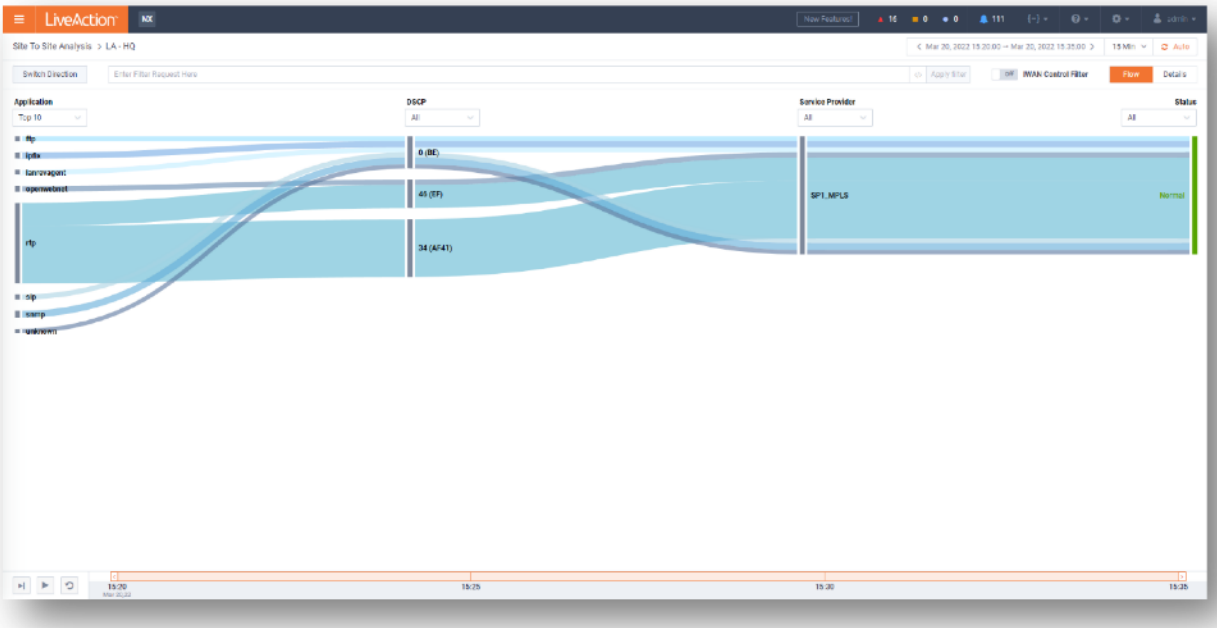


Figure 20

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

Lab 1.4: WebUI Reports

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

Lab Steps:

35. Click the **Menu** icon.

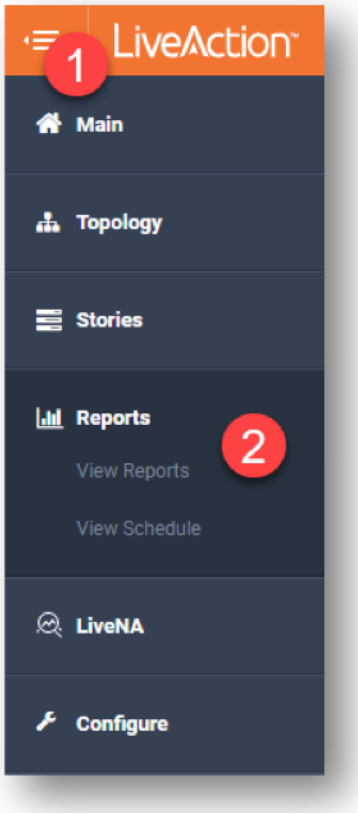


Figure 21

36. Select **Reports**, and **View Reports**.

37. From the Top Reports section, select **Application**

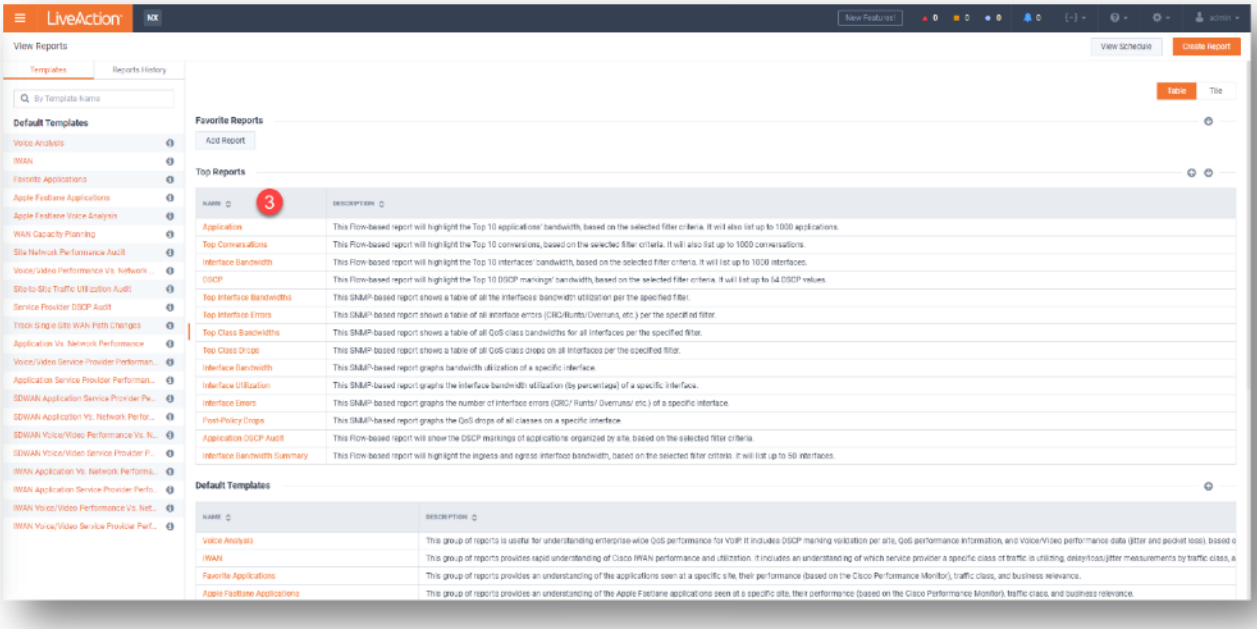


Figure 22

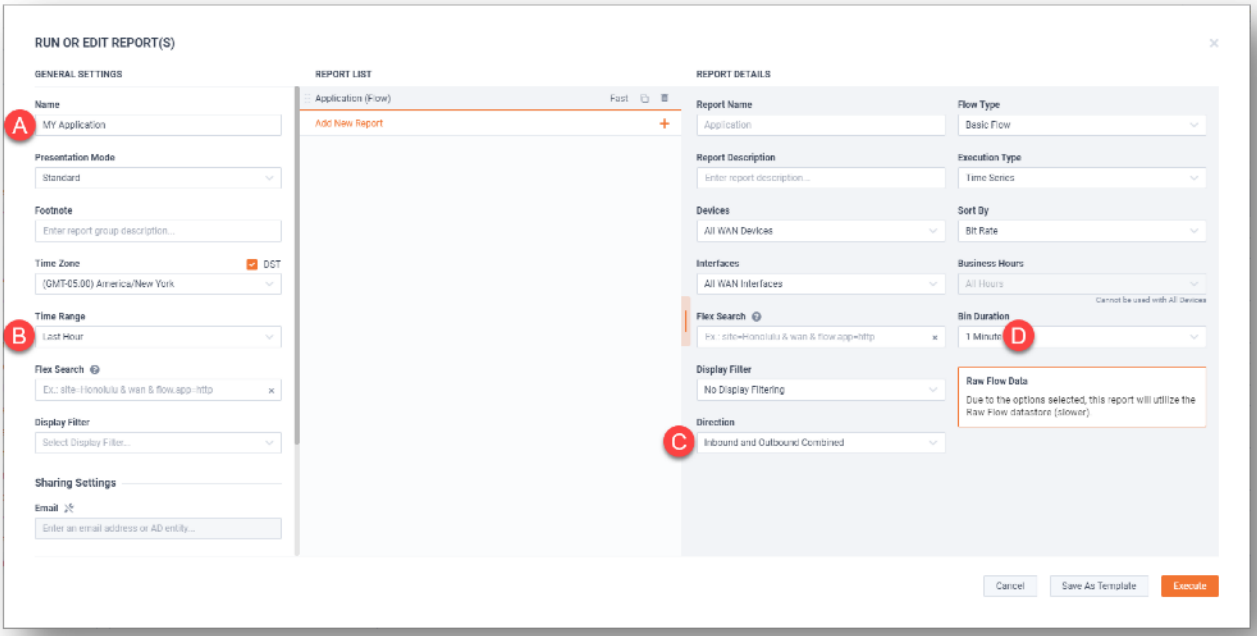


Figure 23

38. Select Options.
    - **Name**: My Application
    - **Time Range**: Last Hour
    - **Direction**: Inbound and Outbound Combined
    - **Bin Duration**: 1 Minute

39. Click Execute.

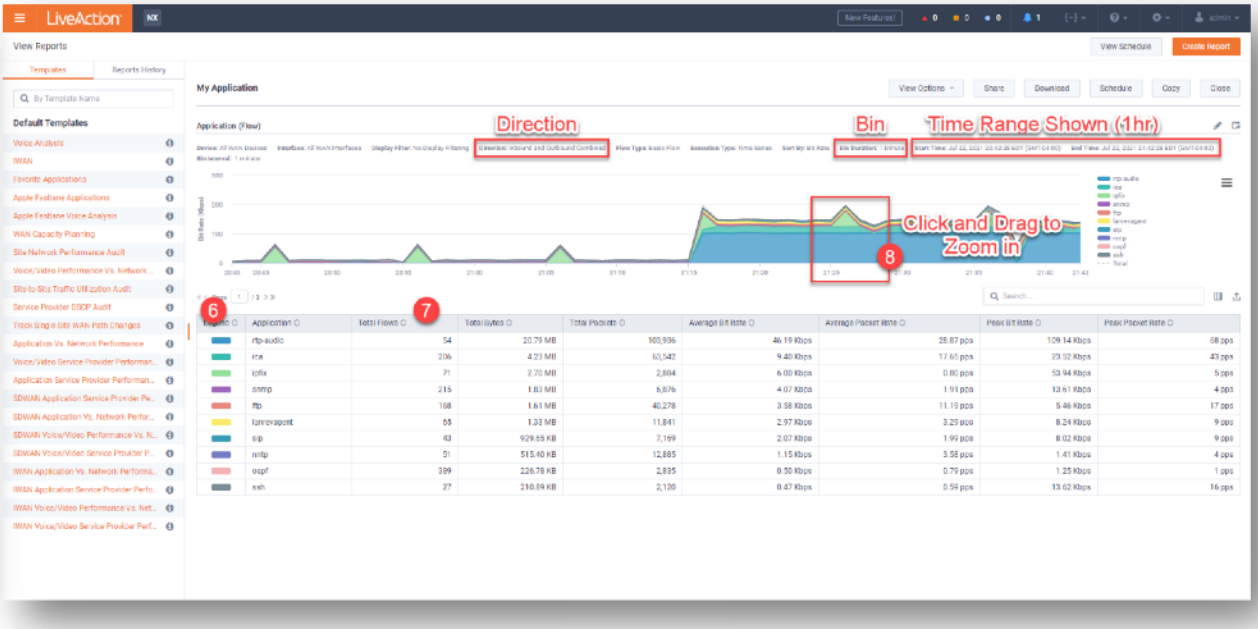


Figure 24

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.

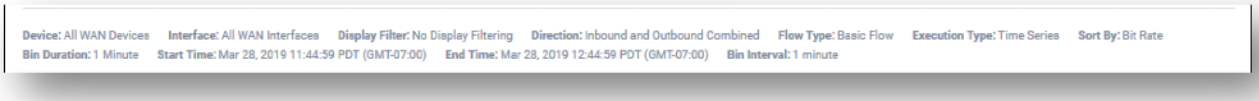


Figure 25

40. **Hide** a metric by clicking on the Legend (in the table, or on right of chart).
41. Re-sort by clicking on the **Sort Arrows**.
42. **Zoom-in** by Left-click-drag a portion of the chart.
43. **Reset** Zoom to normal.

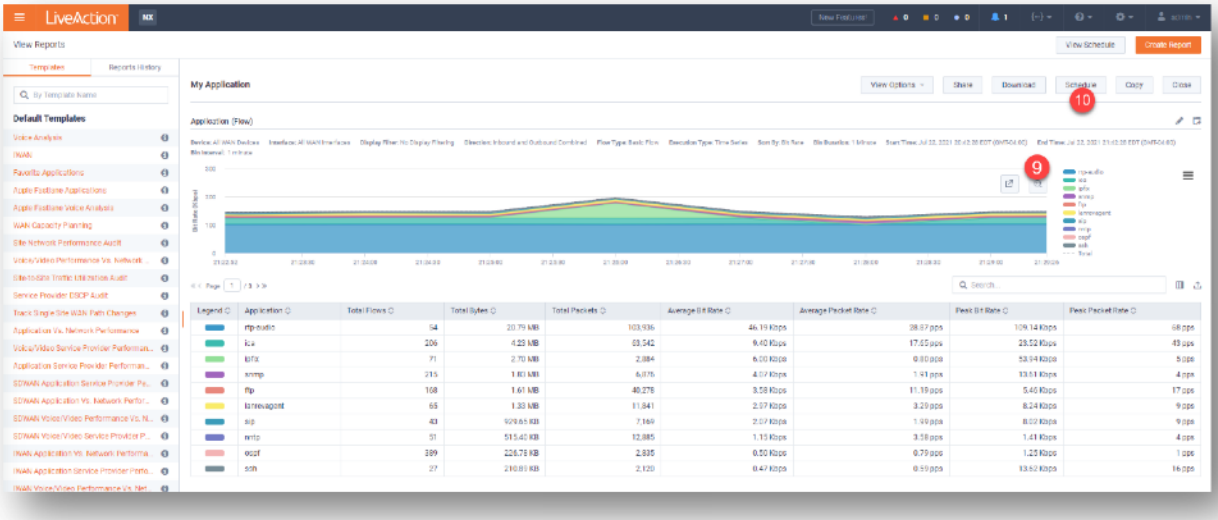


Figure 26

44. **Schedule** the Report to run Hourly.

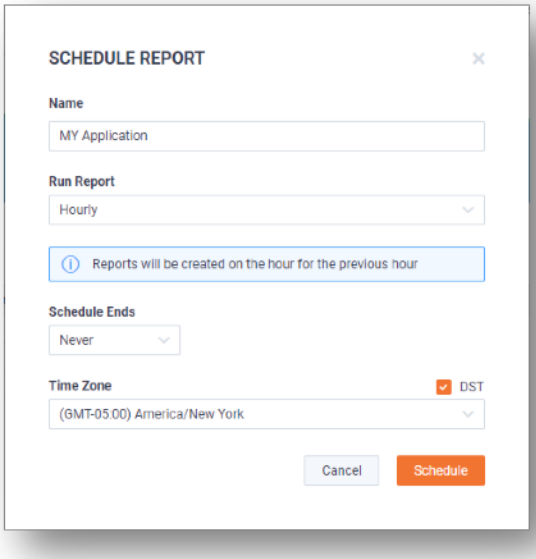


Figure 27

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

Figure 28

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

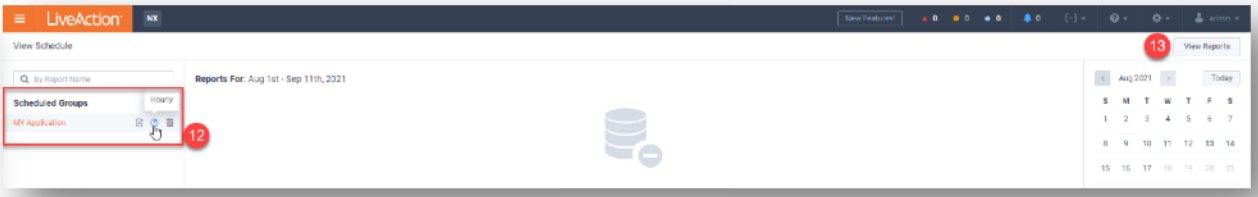


Figure 29

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

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

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

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

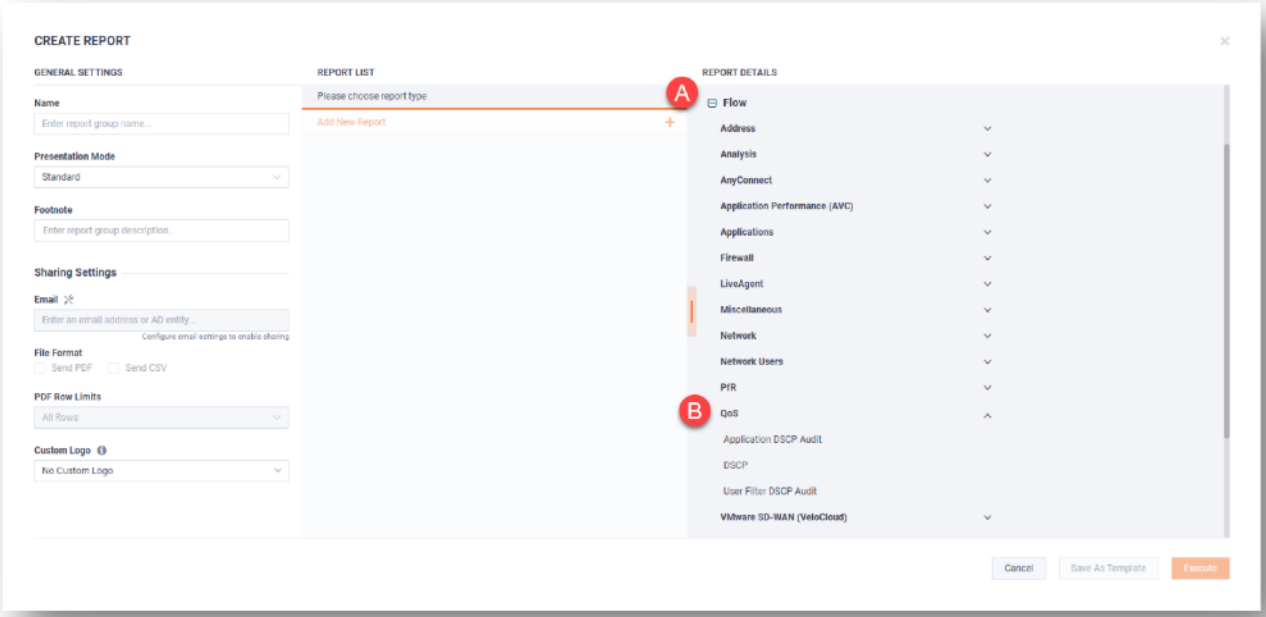


Figure 30

50. Select **Application DSCP Audit.**

51. Click **Execute**.

52. Verify the Application to DSCP values

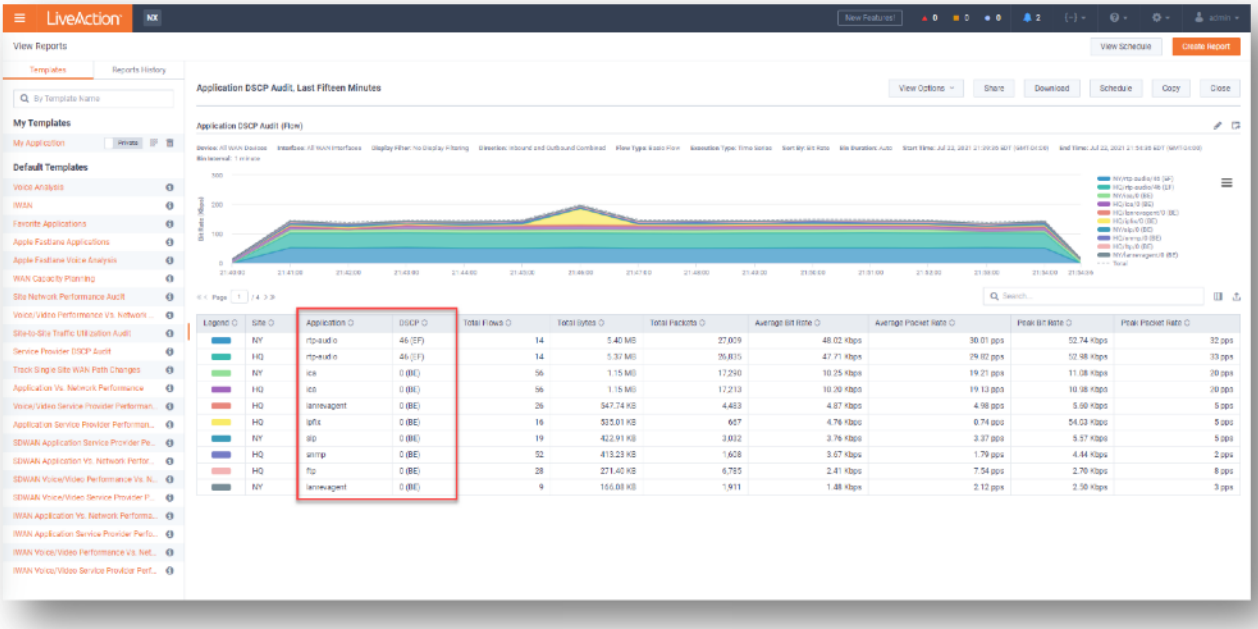


Figure 31

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.

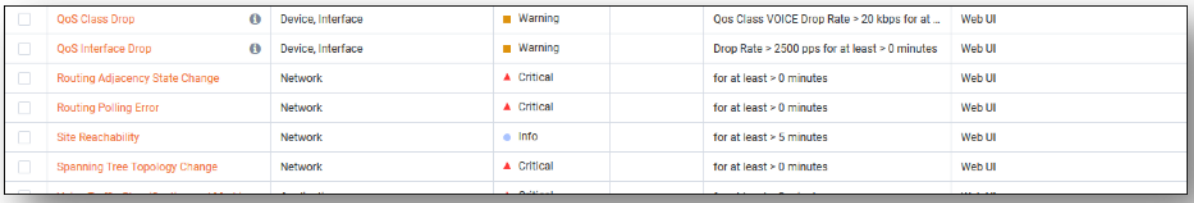
Note: By default, no alerts are enabled during initial LiveNX installation. It is up to the administrator to turn on alerts & notifications.

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

Lab Steps:

53. Click the **Menu** icon.

54. 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 32

55. Click on **QoS Class Drop**.

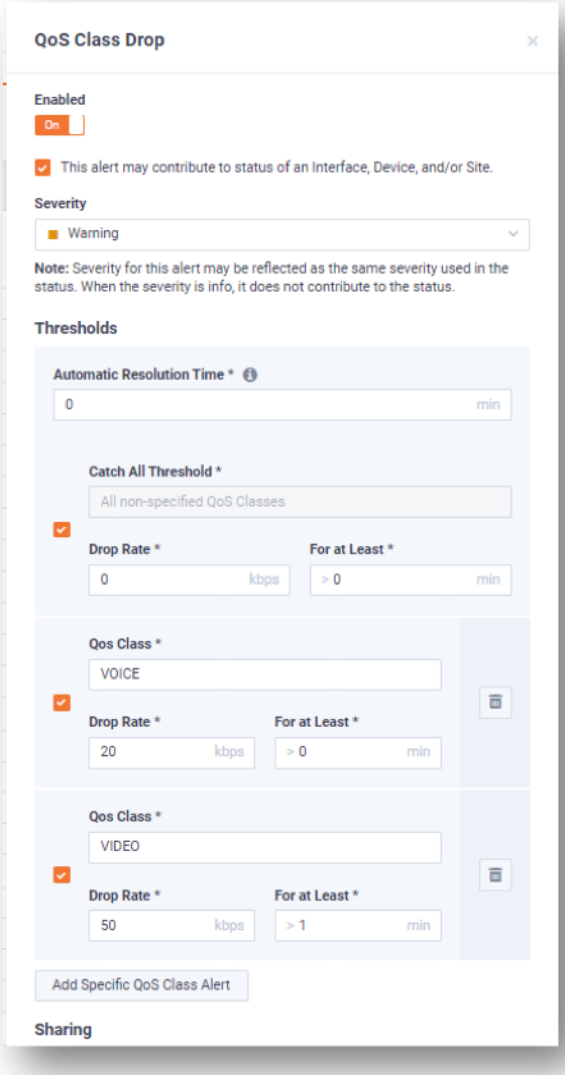


Figure 33

56. Select to **Enable** this alert.
57. Change the Severity if desired.
58. **Enter** QoS Class “VOICE”.
59. **Define** a DROP RATE of 20.
60. Leave FOR AT LEAST of “0”.

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

61. Click **Add More**
62. Enter **QoS Class** “VIDEO”.
63. Define a **DROP RATE** of “50”.
64. **Define** the interval of “1” min.
65. 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.

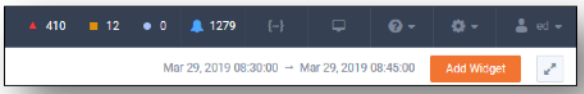


Figure 34

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

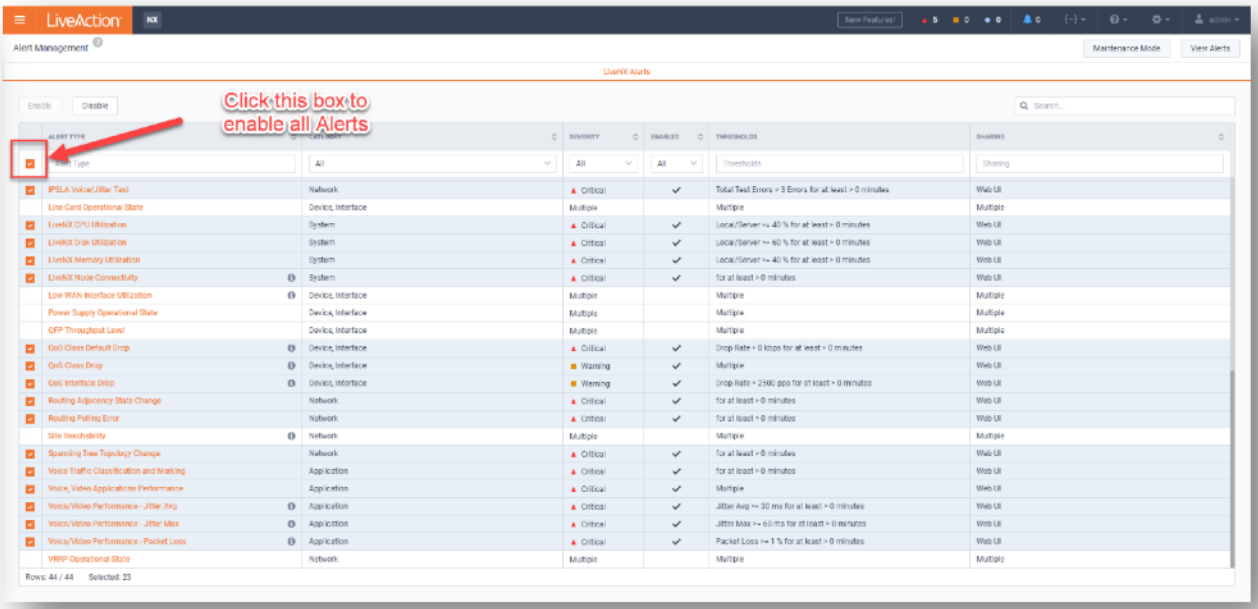


Figure 35

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:

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

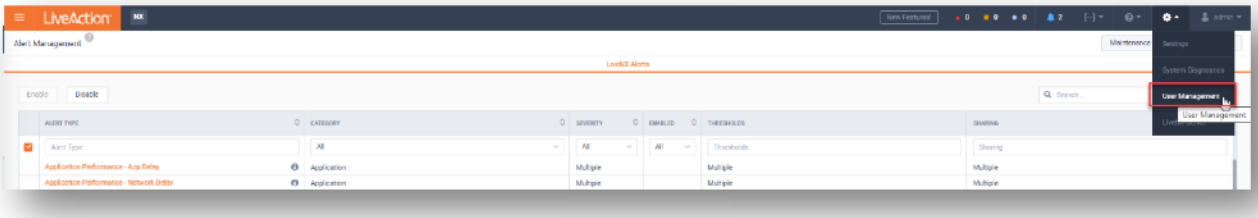


Figure 36

68. Click Add User.
69. For this exercise we will add a **Local** user.

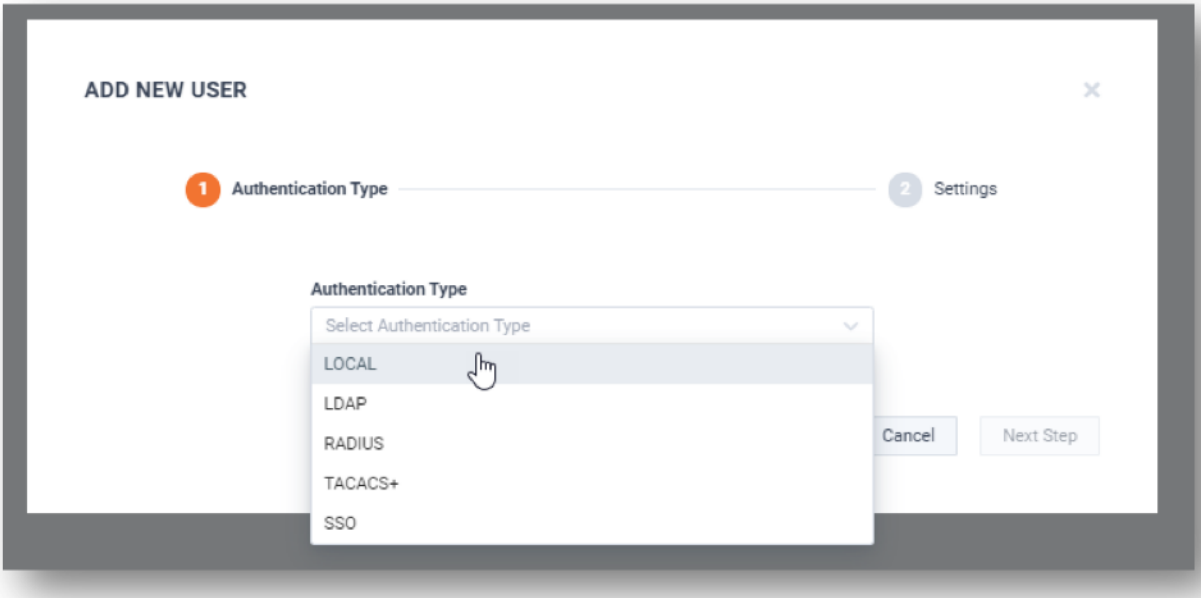


Figure 37

70. Enter a **username** and a **Display Name** (something you'll remember).
71. Select the **Admin** role from the **Group** drop-down, and a **Session Timeout** value.
72. 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.

73. Click **Add User**.

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

Lab 1.7: View and Navigate System Diagnostics

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

Lab Steps:

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

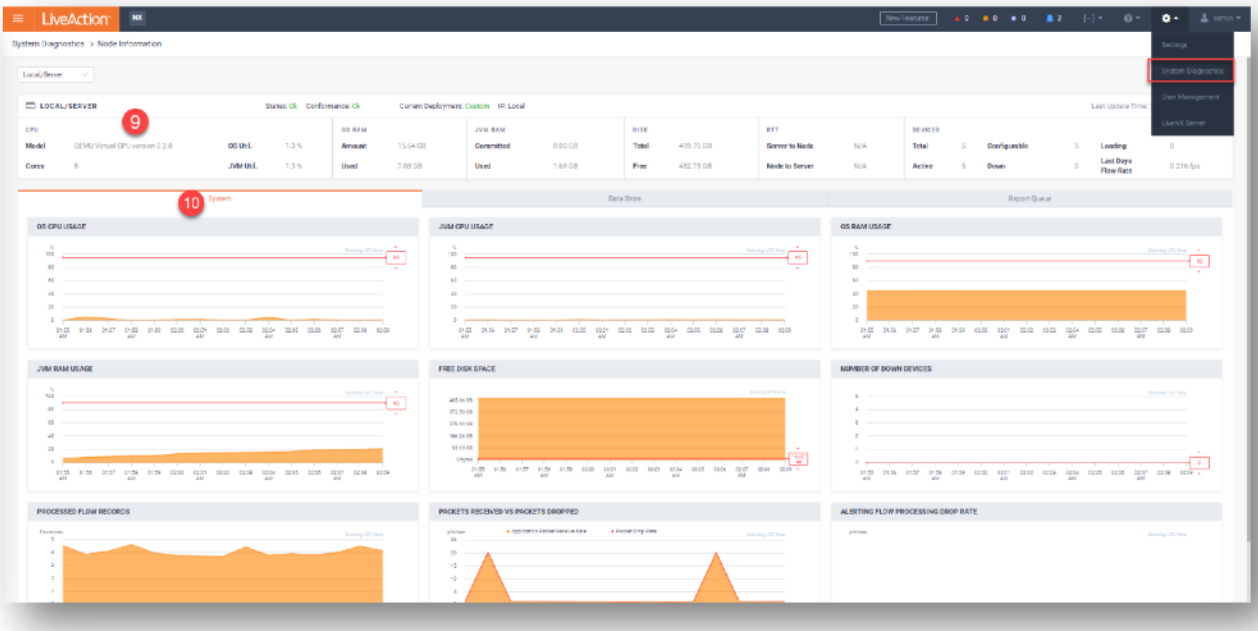


Figure 38

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.

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

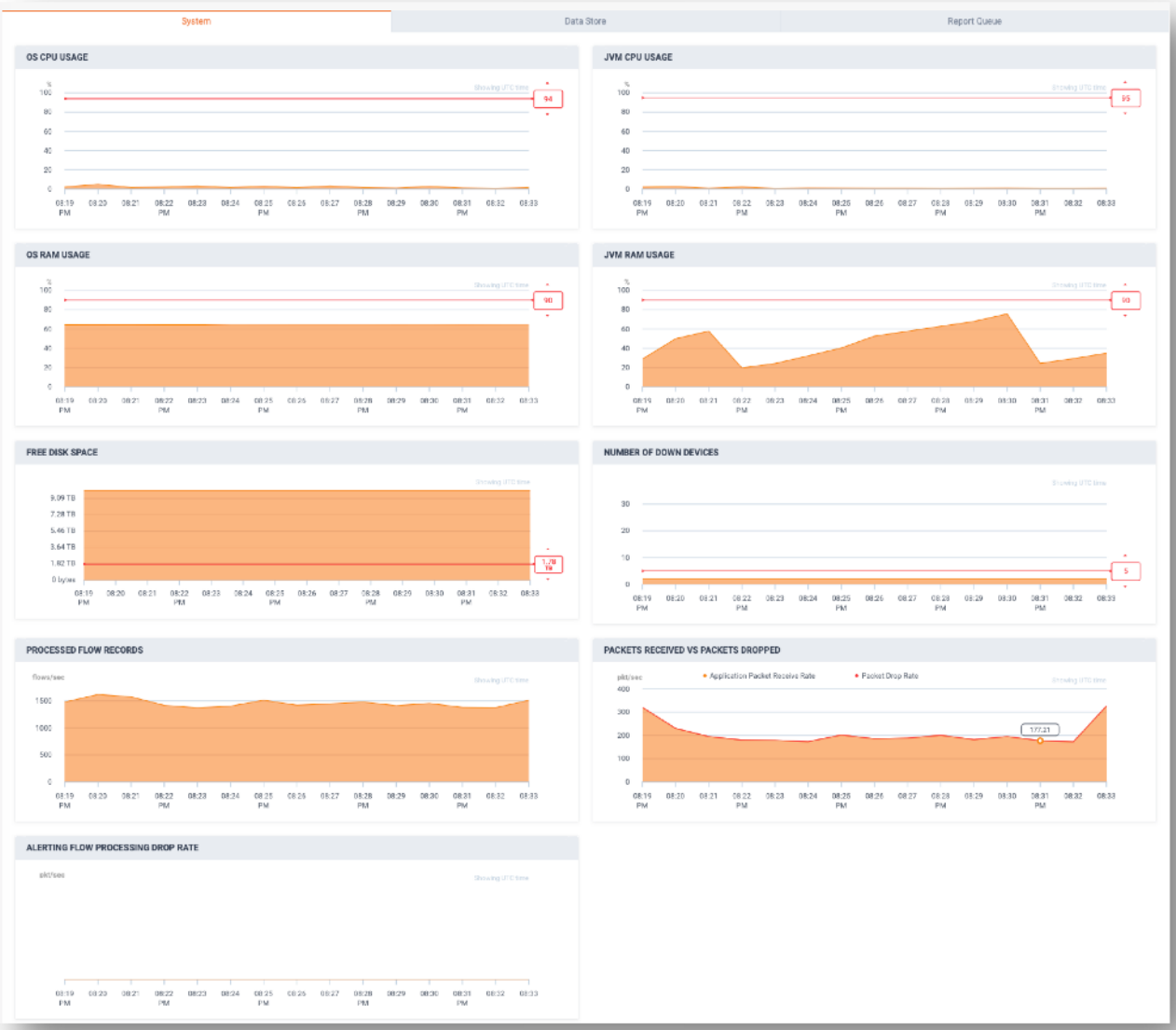


Figure 39

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

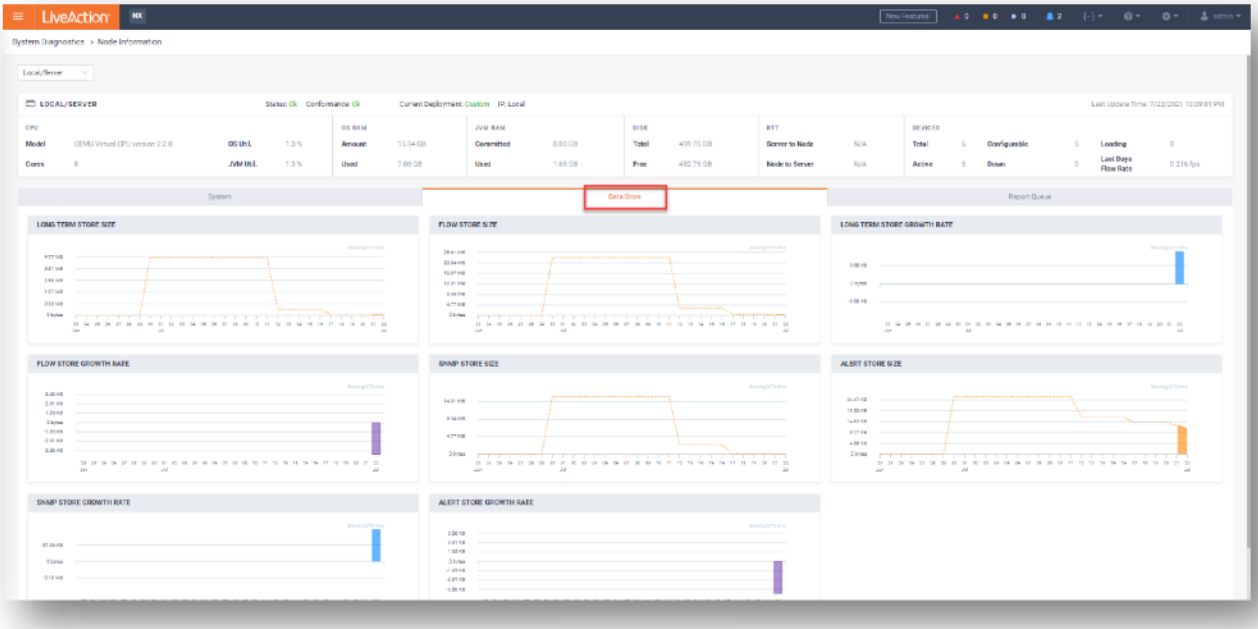


Figure 40

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

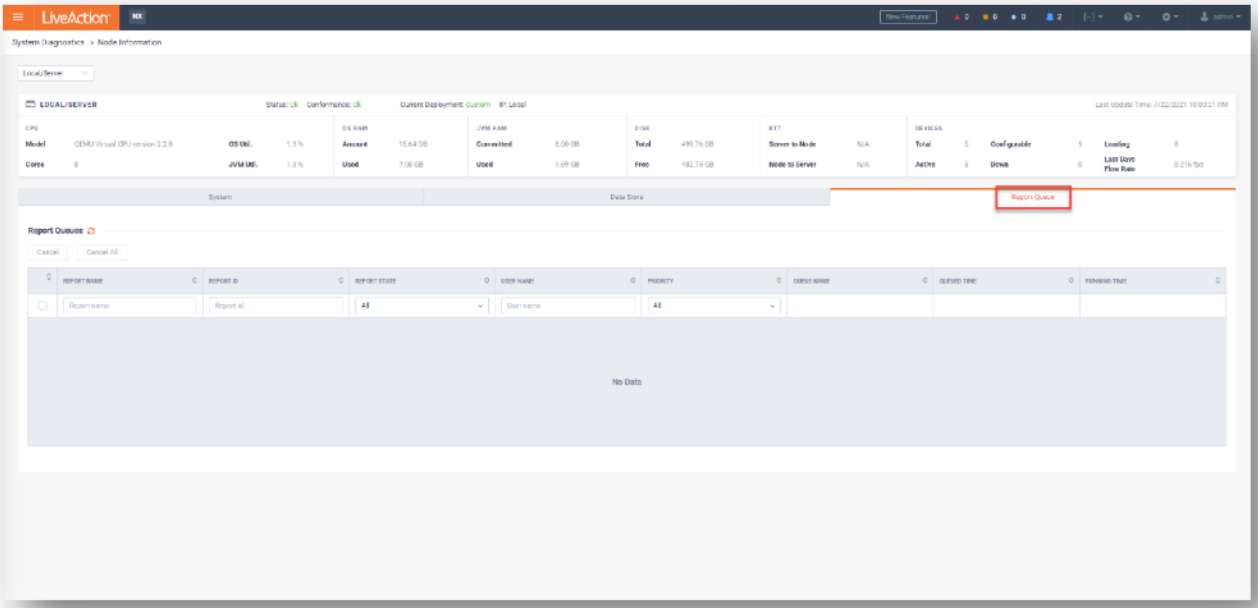


Figure 41

Lab 1.8: Support and Troubleshooting

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

80. Navigate to the **Settings** menu.

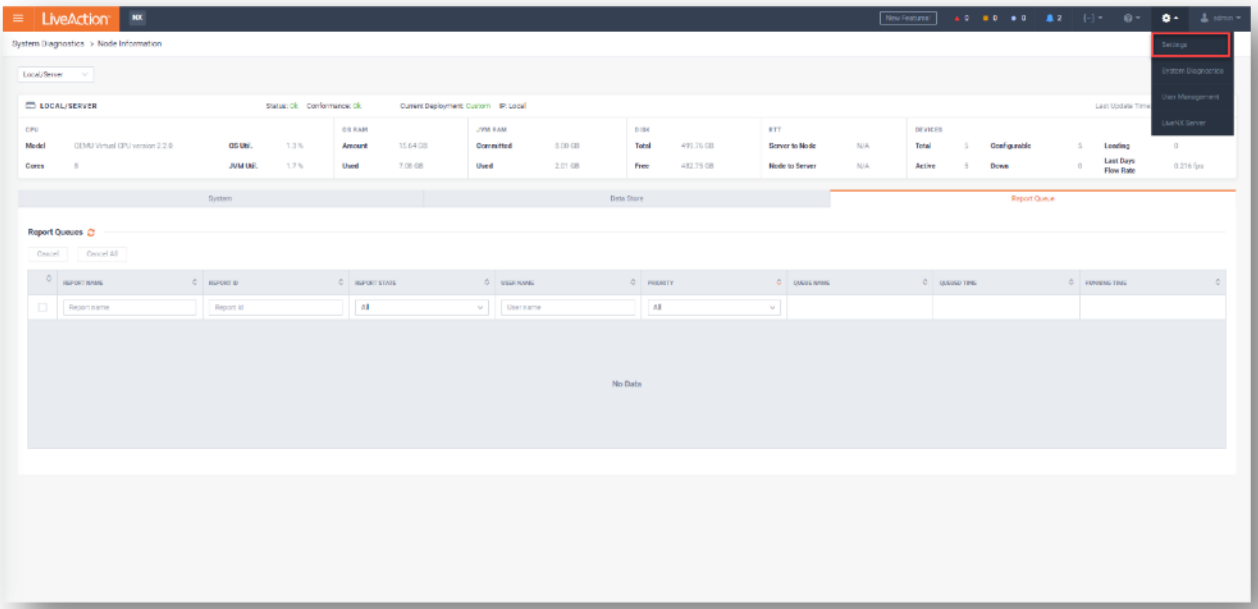


Figure 42

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

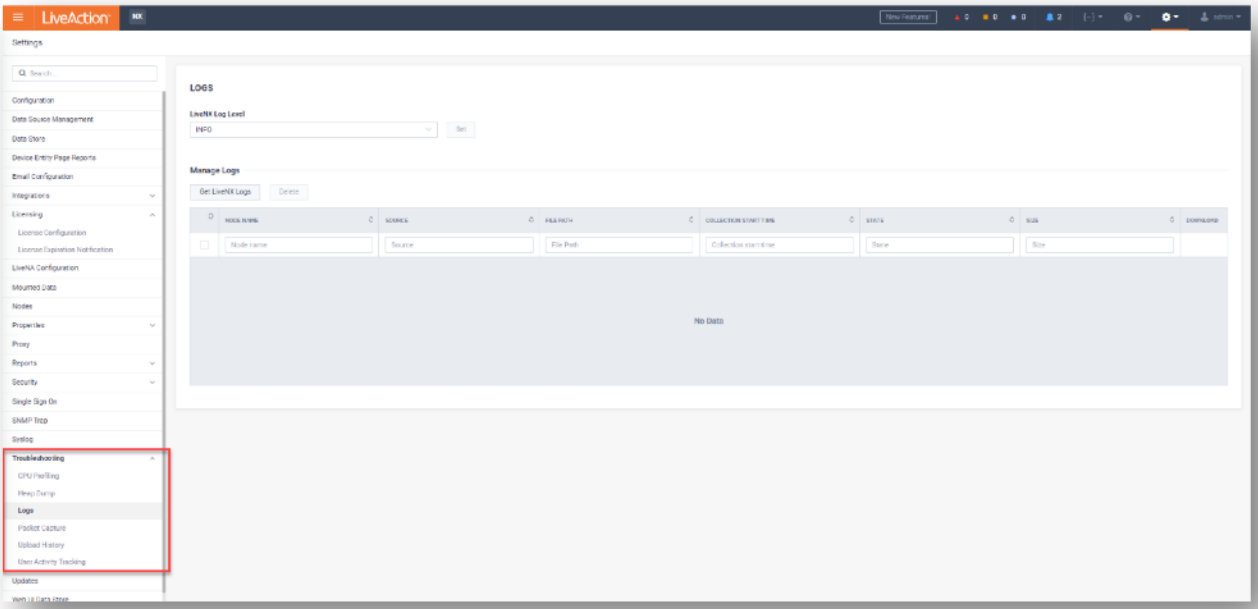


Figure 43

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

82. Click **Get LiveNX Logs**.

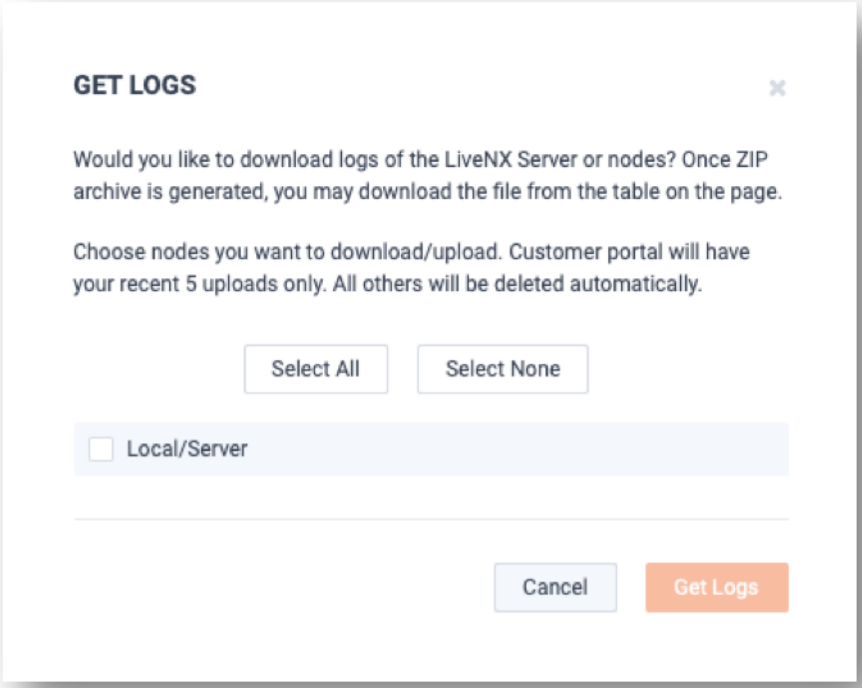


Figure 44

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

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

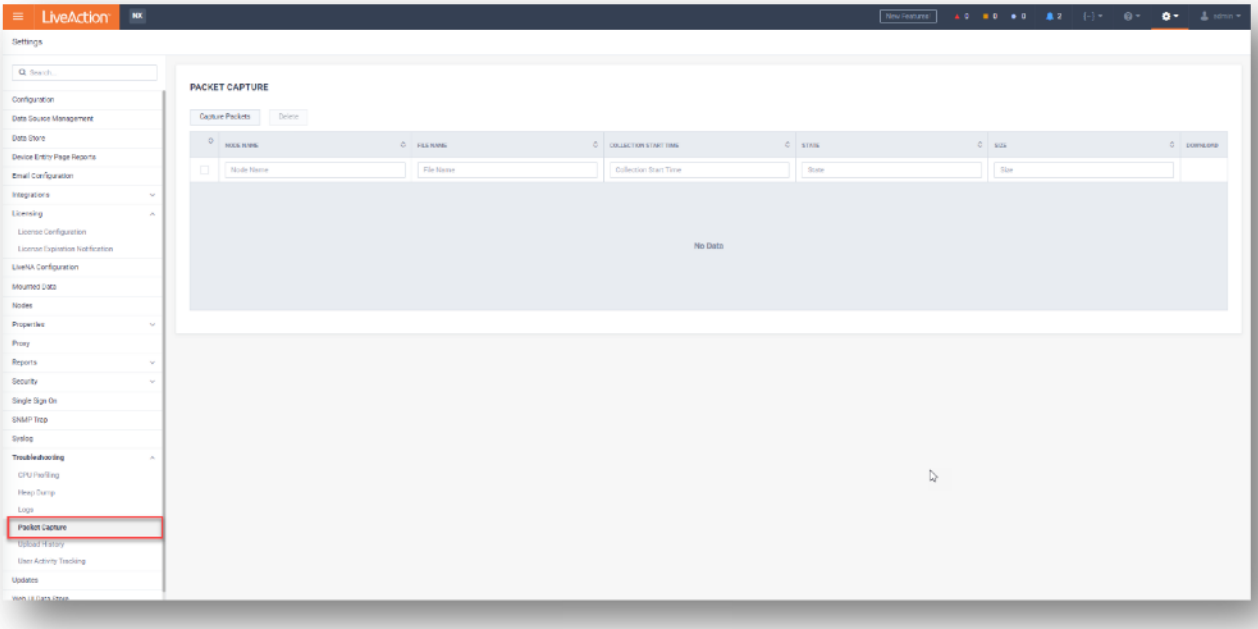


Figure 45

85. Click **Capture Packets.**

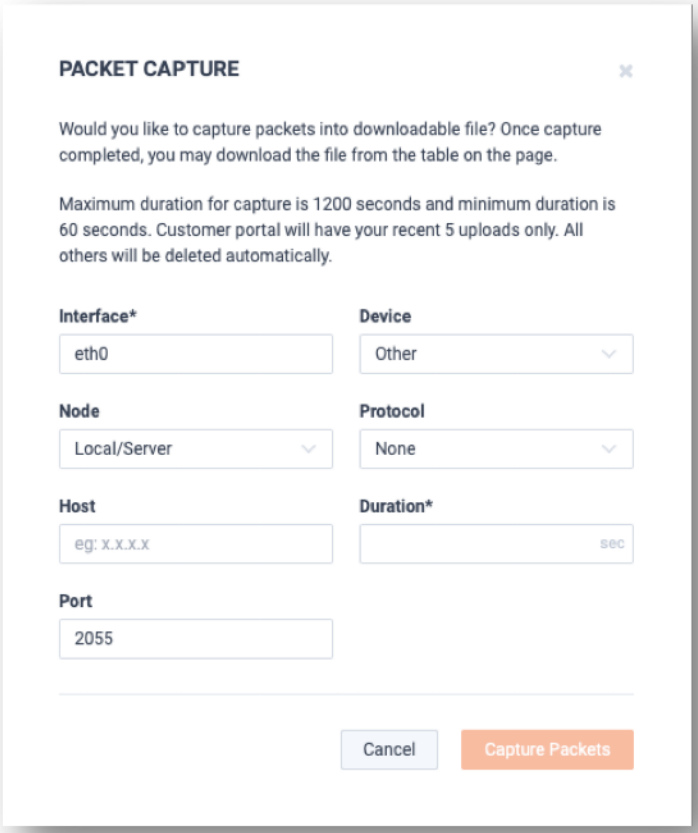


Figure 46

86. 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.

87. 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

These Labs uses the Engineering Console exclusively.

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:

88. **Launch** the LiveNX Client.

DIAGRAM

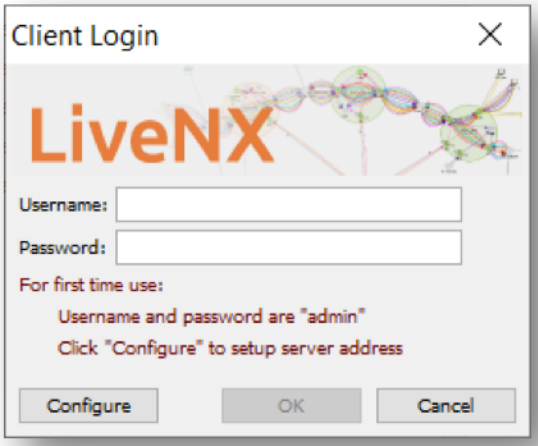


Figure 47

89. 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.

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

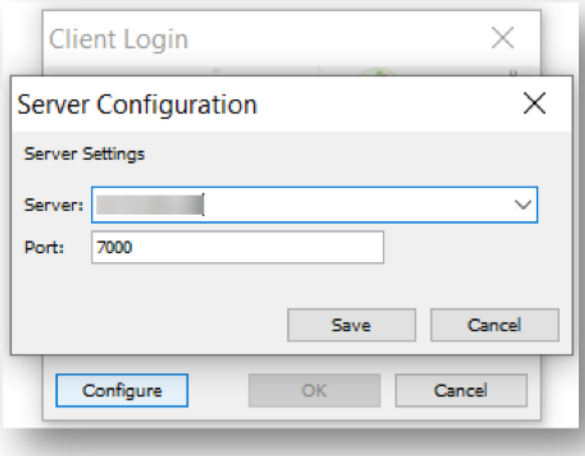


Figure 48

91. **Click** Save

92. Enter the **Username** & **Password**.
    Username: admin
    Password: Student (note the capital S)

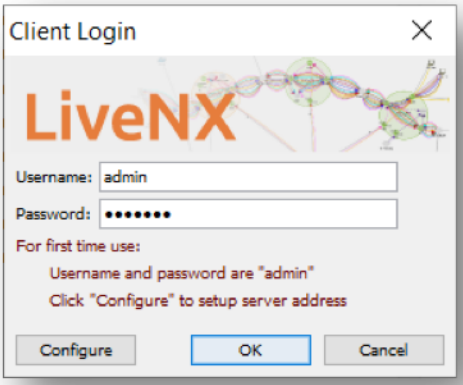


Figure 49

93. Click **OK**

The Client will launch…

Figure 50

… and will open showing the current configured Topology.

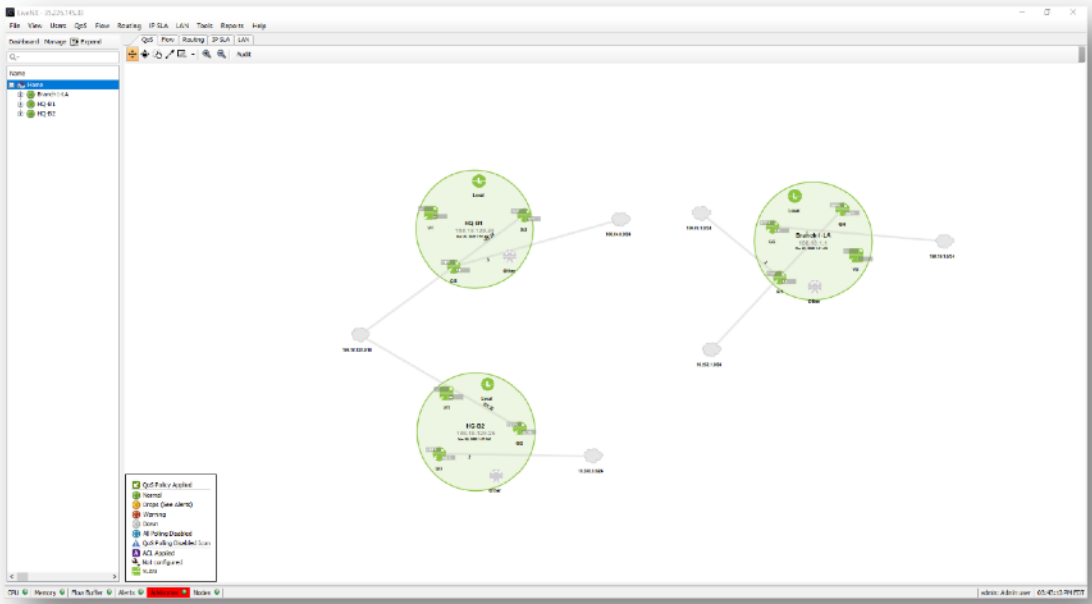


Figure 51

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

Lab 2.2: Explore the LiveNX Client

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

Lab Steps:

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

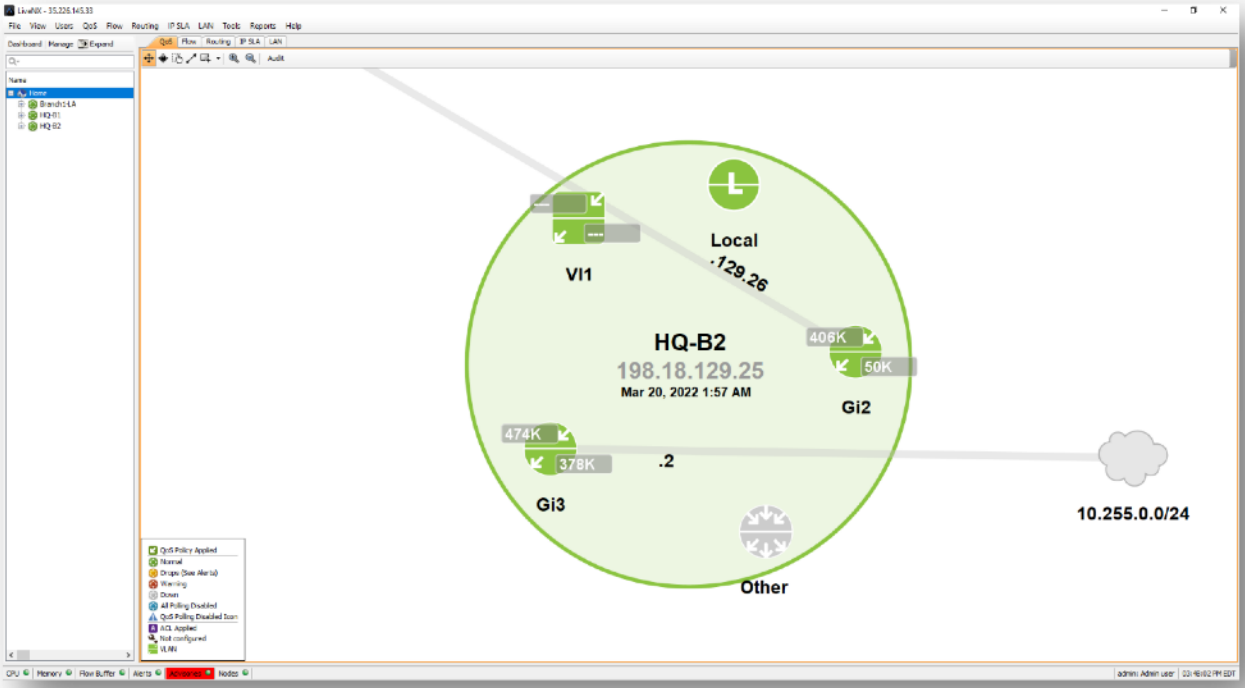


Figure 52

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

95. Left click anywhere in the white area and move the mouse to re-position the device(s) in the window.

96. Use the mouse scroll-wheel to zoom in & out.

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

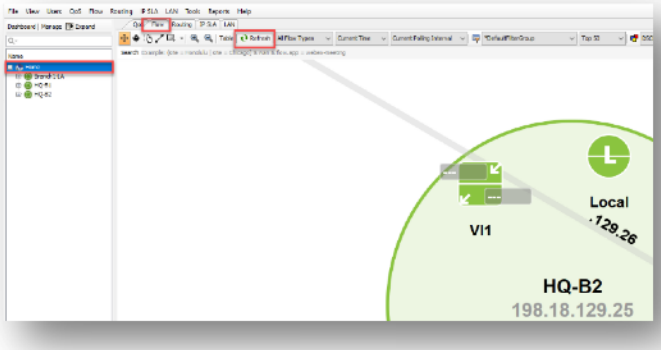


Figure 53

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

---

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

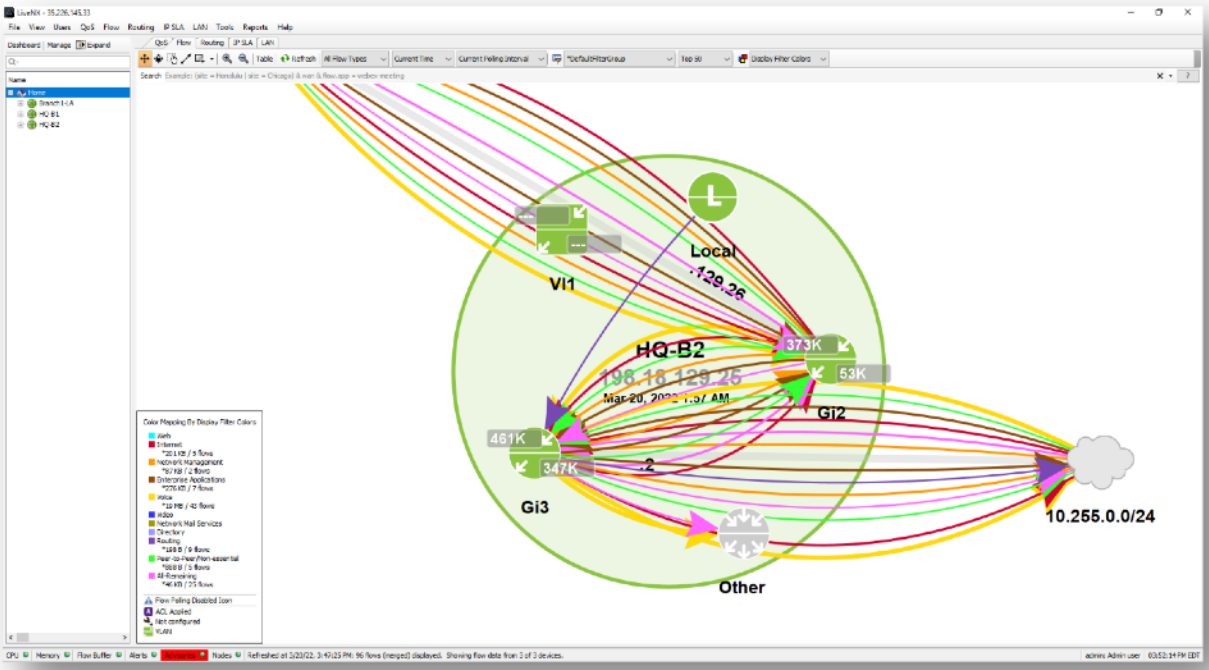


Figure 54

99. **Expand** the **HQ-B2** device in the **Home** Tree View.

100. Click on one of the interfaces… note how the information displayed in the Topology Pane changes.

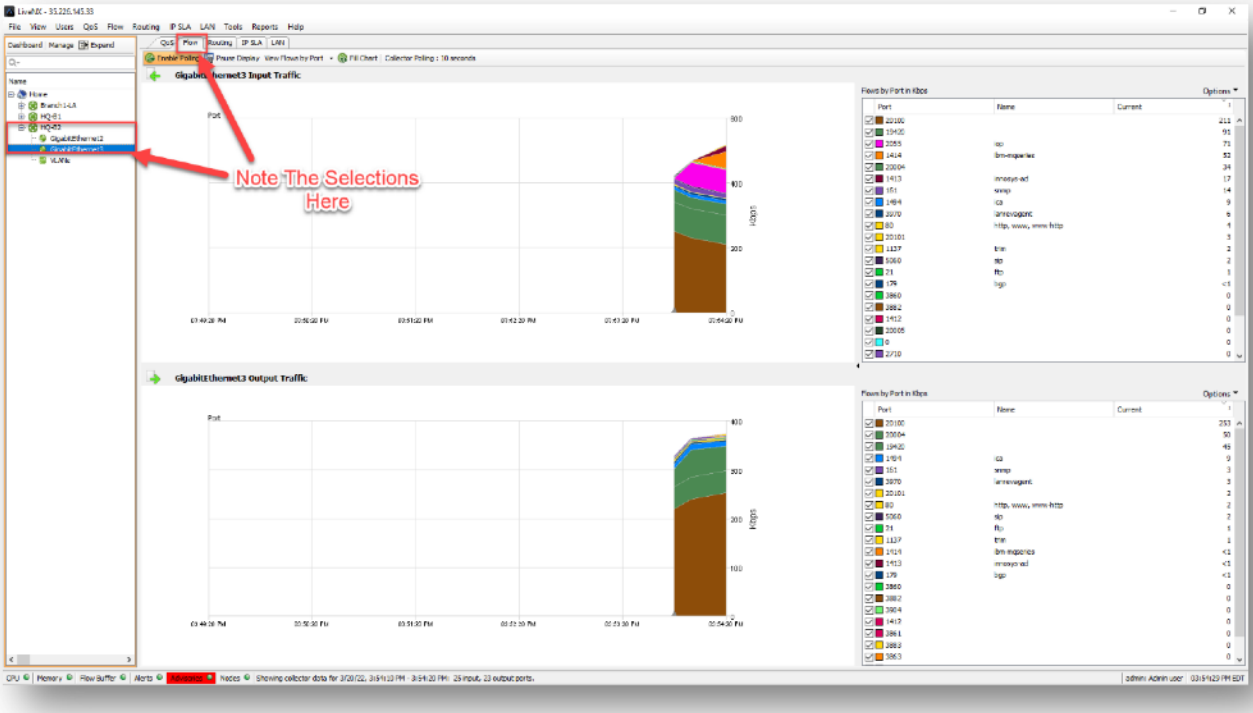


Figure 55

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

Lab 3

Lab 3: Configuring Devices

Lab 3.1: Add Device

This Lab uses the WebUI.

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:

101. Login to the LiveNX WebUI
102. Select **Configure** > **Device Management**

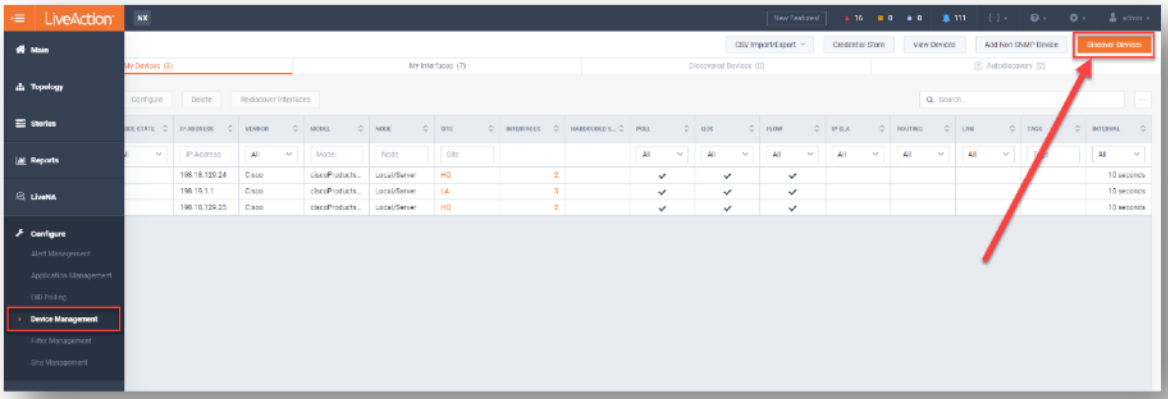


Figure 56

103. Click **Discover Devices**.

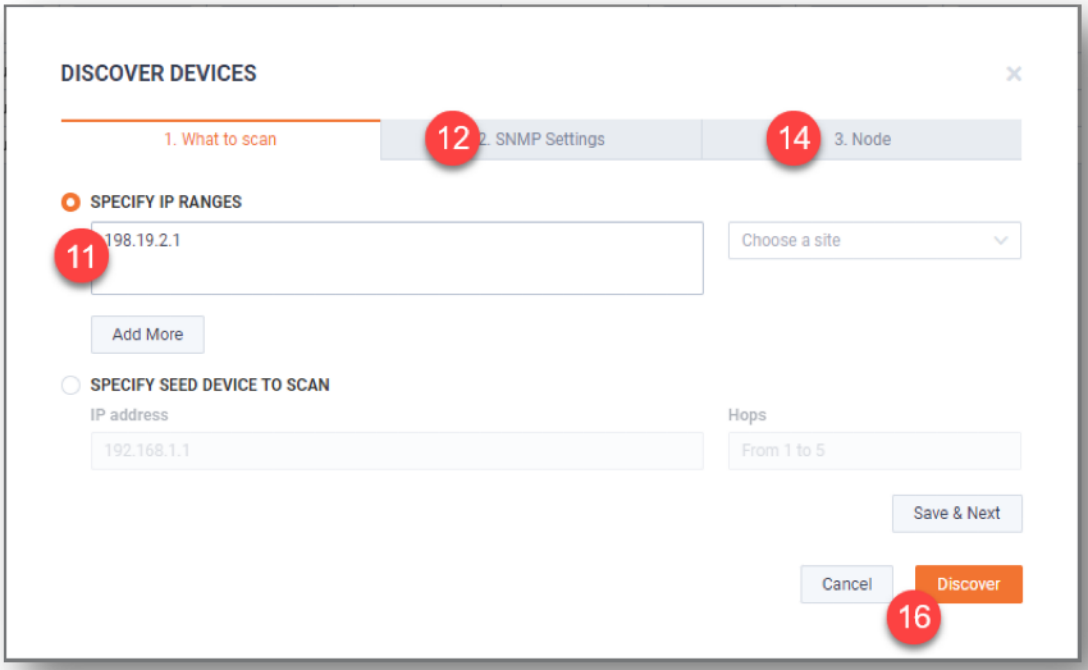


Figure 57

104. Enter **198.19.2.1**, in the IP Address field.

105. Select the **SNMP Settings** tab.

106. Click "**Default SNMP connection settings**".

107. Select the **Node** tab.

108. Select **Local/Server**.

109. Click **Discover**.

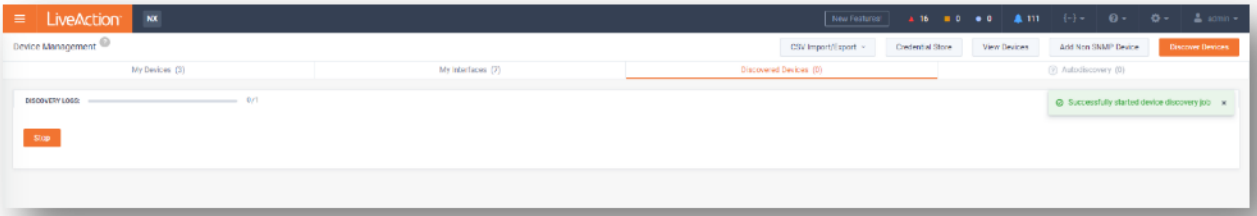


Figure 58

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.

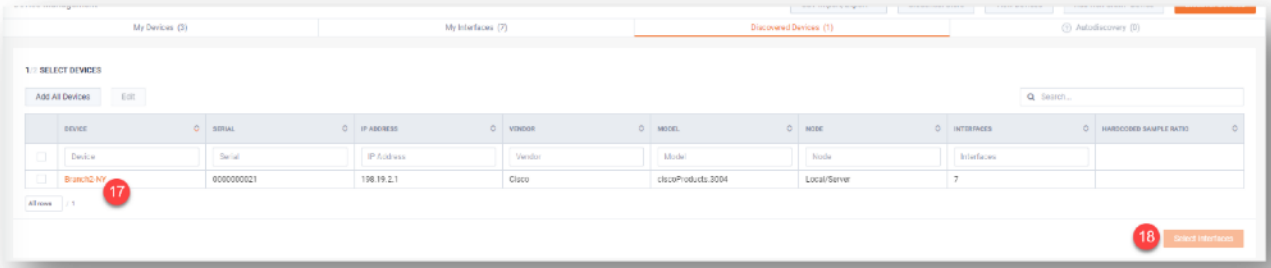


Figure 59

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

111. Click **Select Interfaces**.

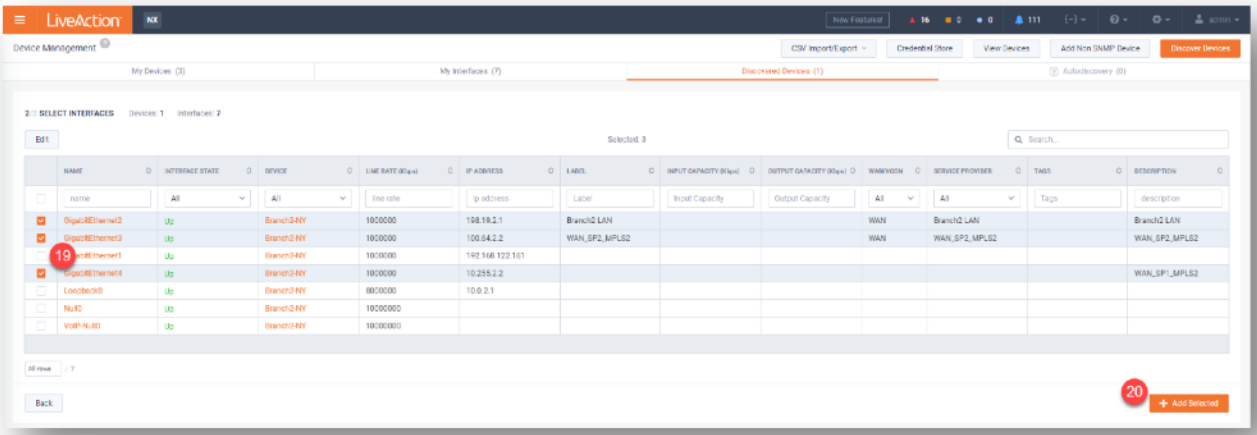


Figure 60

112. Select **GigabitEthernet2**, **GigabitEthernet3** & **GigabitEthernet4**.

113. 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.

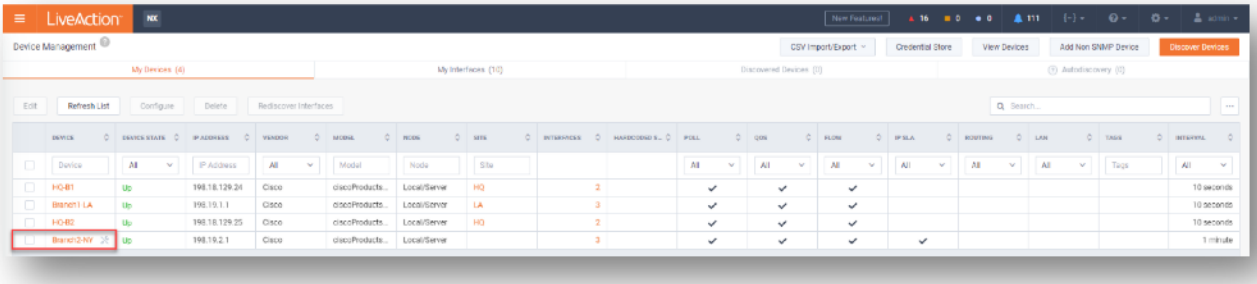


Figure 61

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

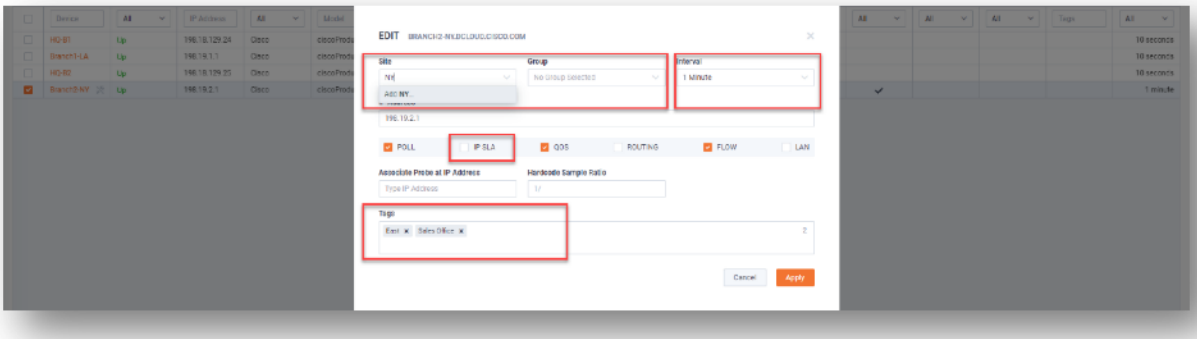


Figure 62

115. 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).

116. Set the polling **Interval** to 10 seconds

117. Uncheck the **IPSLA** check box (this is not covered in this course)

118. 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.

119. 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**.

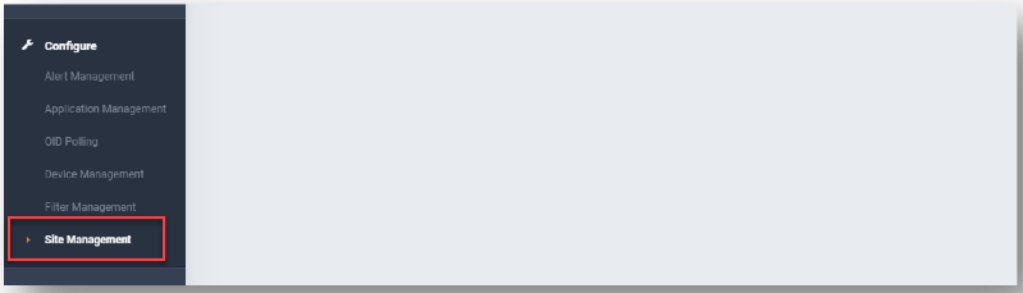


Figure 63

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

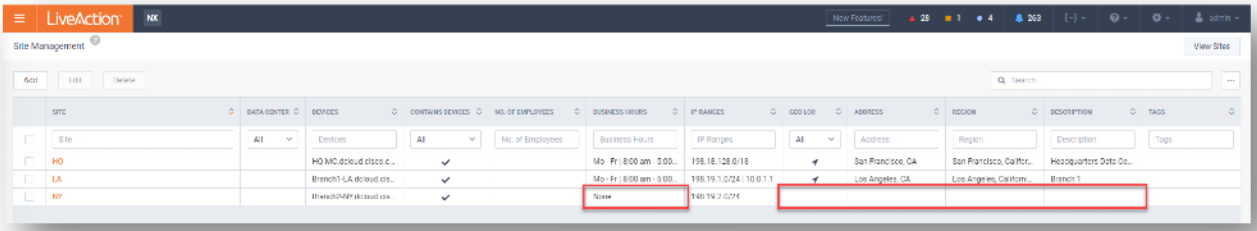


Figure 64

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

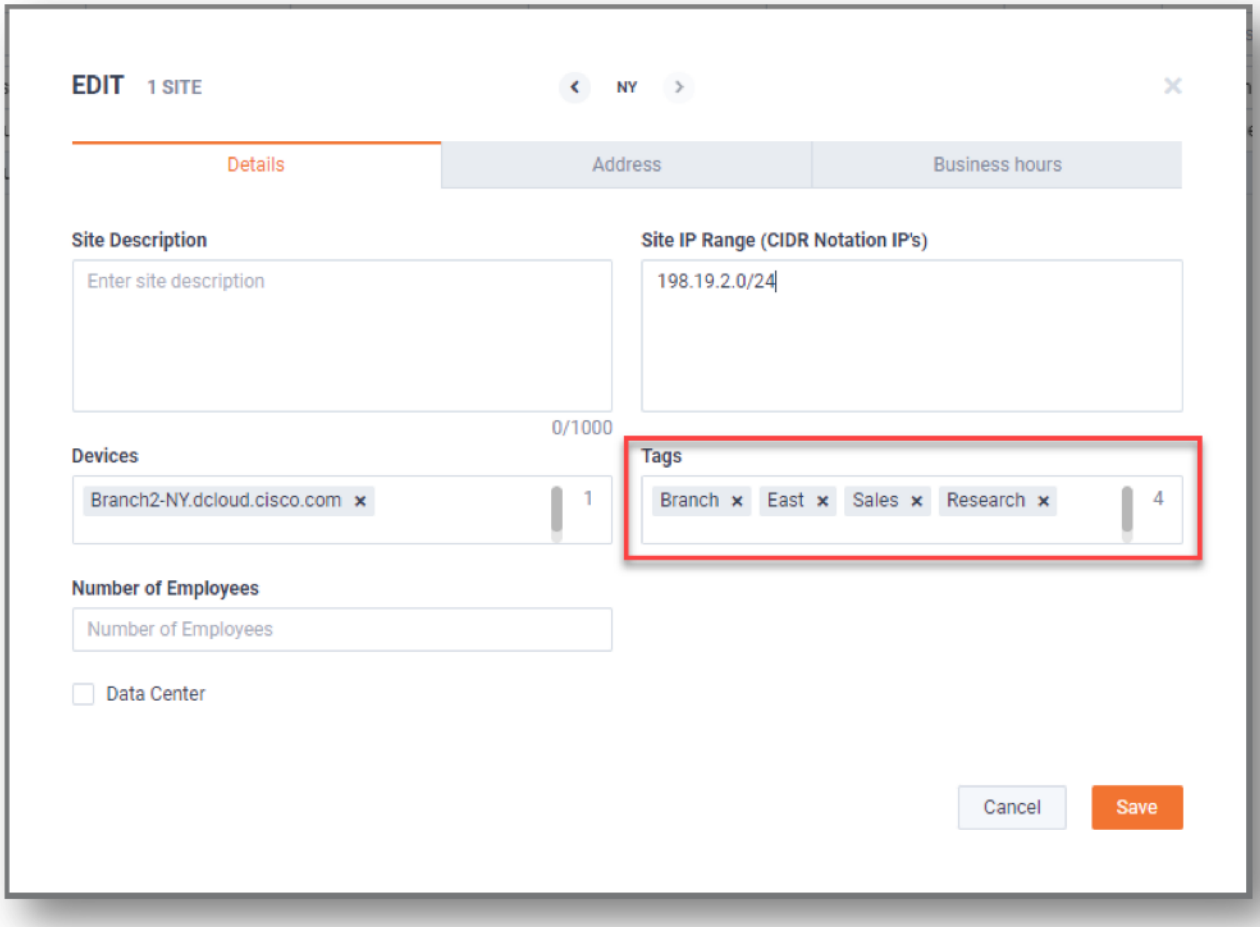


Figure 65

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

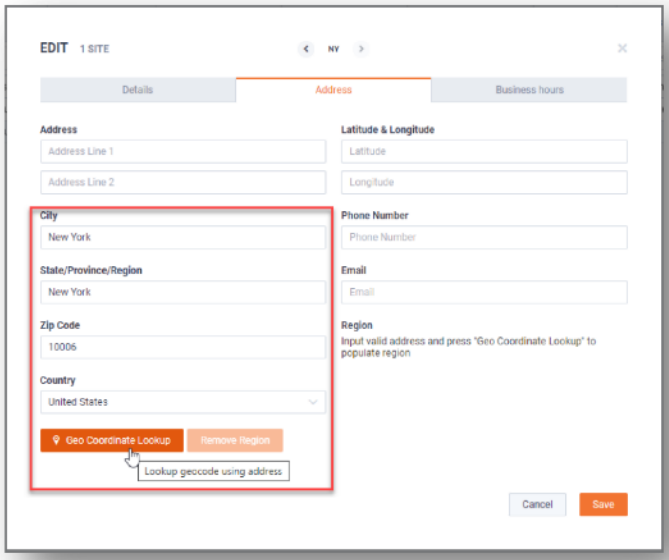


Figure 66

123. 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**.

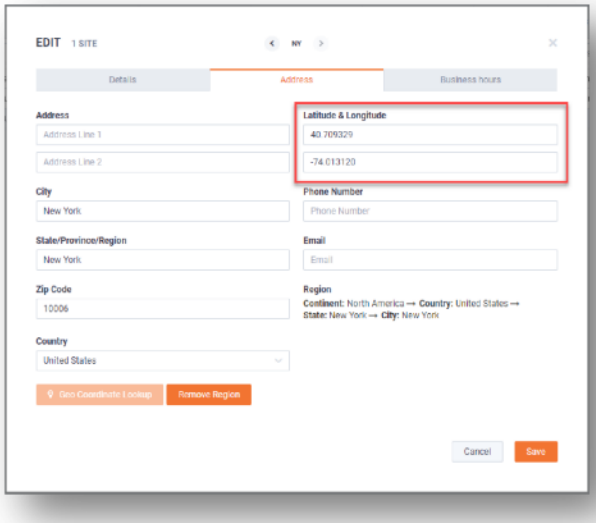


Figure 67

124. 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**.

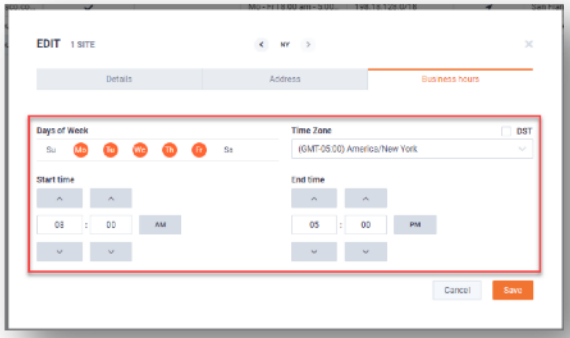


Figure 68

125. 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.

126. Then Click **Save**.

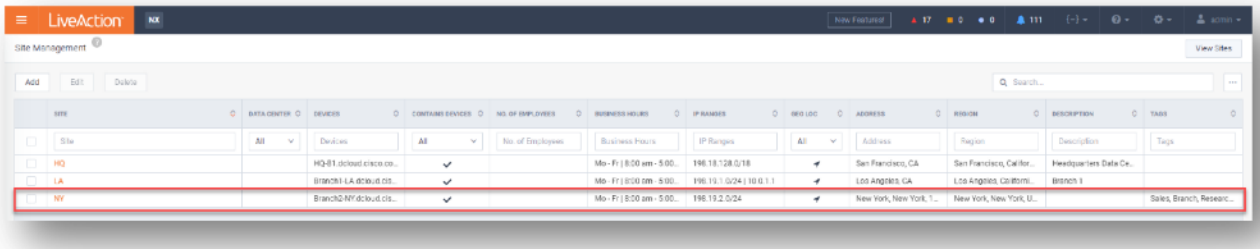


Figure 69

127. 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.

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:

128. Login to the LiveNX Client.

129. Right-click on **Home** and **Expand All.**

130. 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.

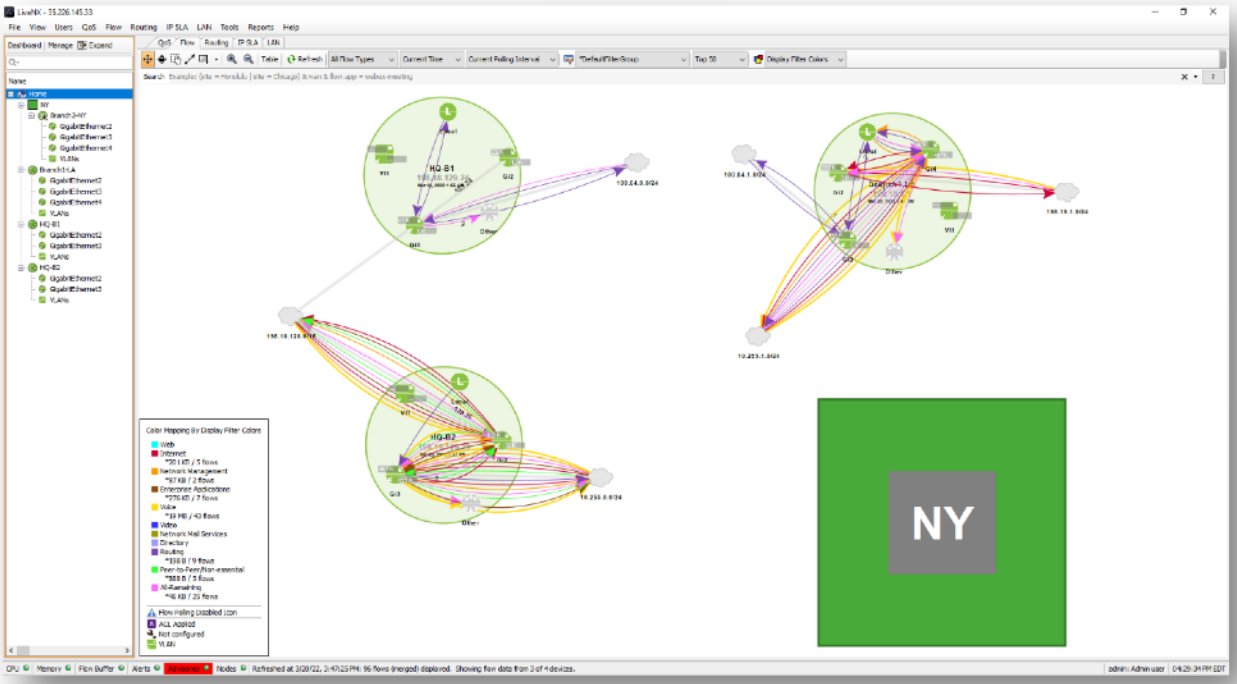


Figure 70

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.

---

131. Click **Manage** (Above the Home Tree). A **Device Management** dialogue will open.

132. Select only **Branch2-NY**

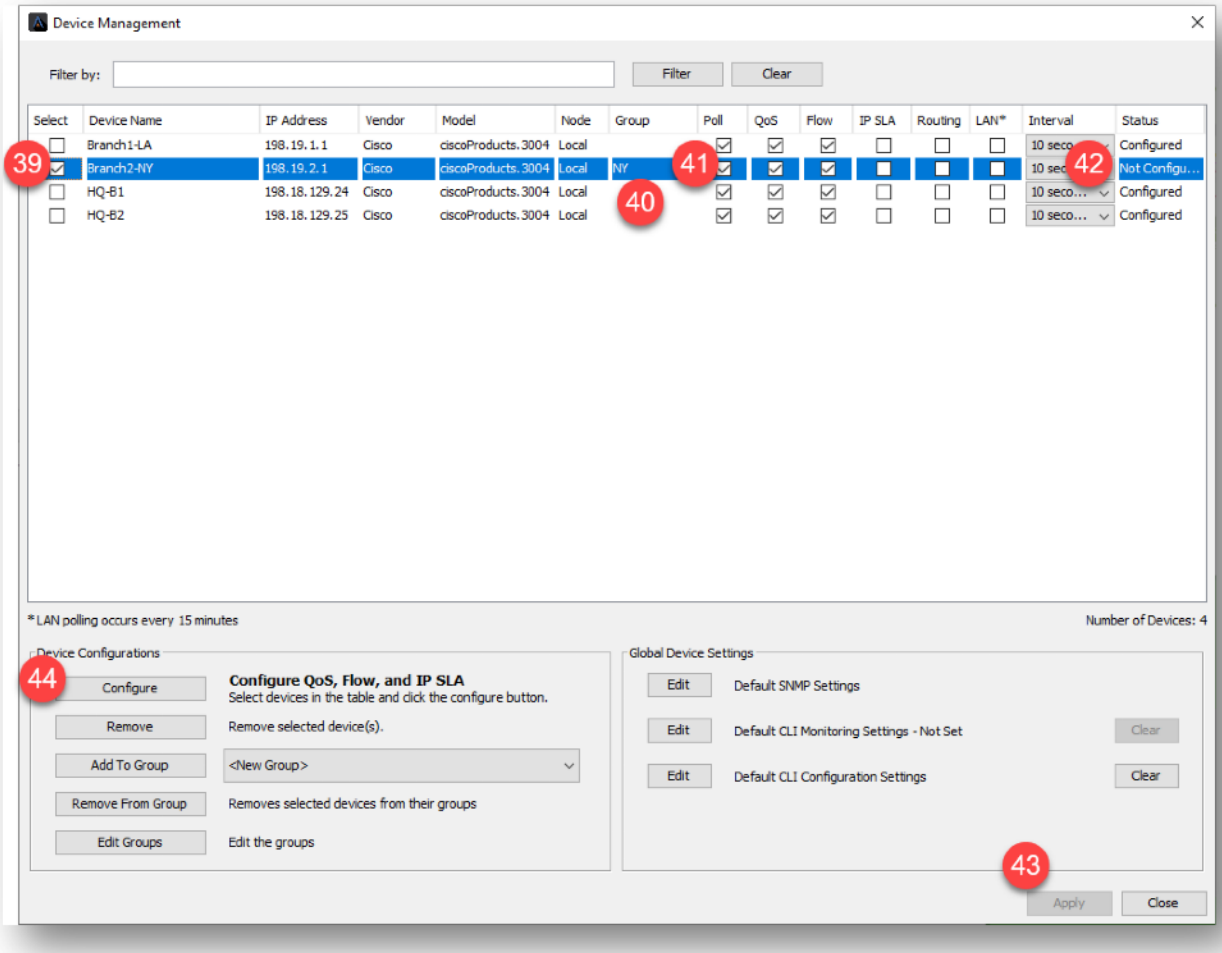


Figure 71

133. Here you will see the Group that we have already created for our new device.

134. Check ONLY **Poll, QoS** and **Flow**.

135. Verify the Interval on the device is **10 seconds**.

136. Click **Apply**.

137. Click **Configure**.

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

138. Step1: Use the **Default SNMP**… Click Next

139. Step2: Use **My Default Configuration CLI**… Click Next

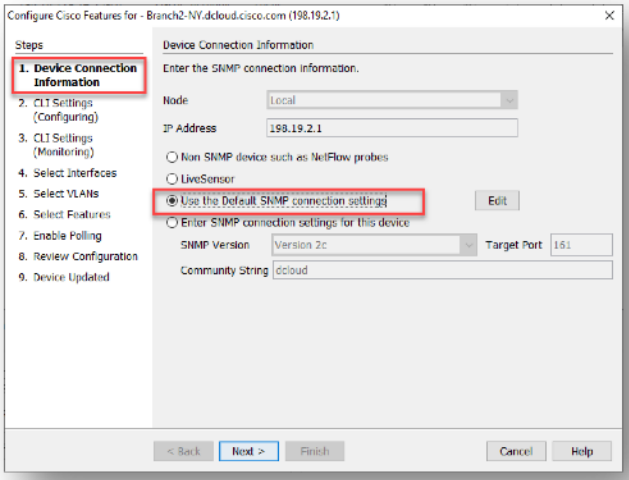


Figure 72

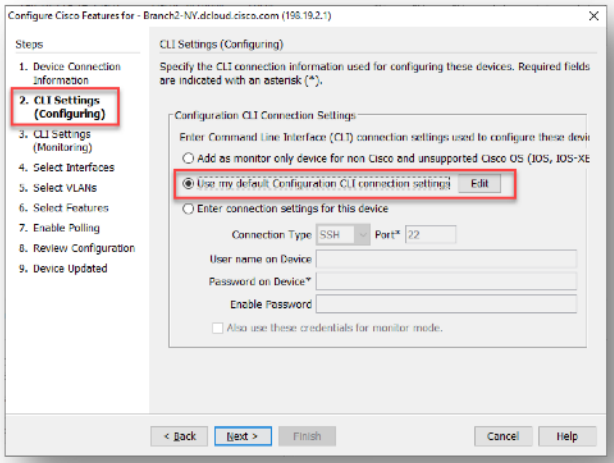


Figure 73

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

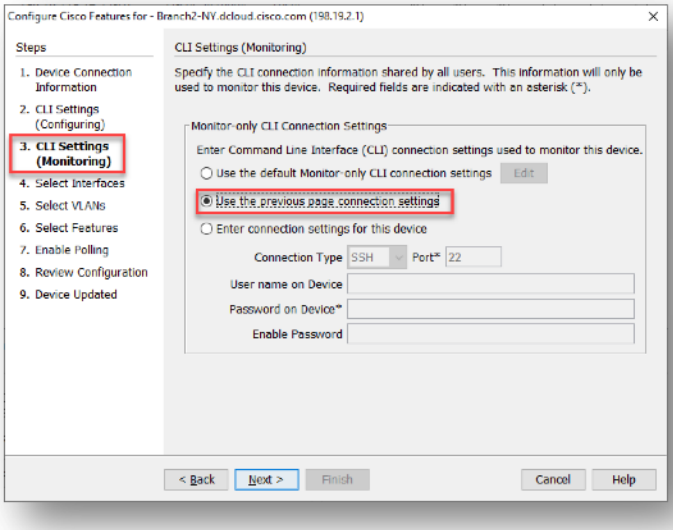


Figure 74

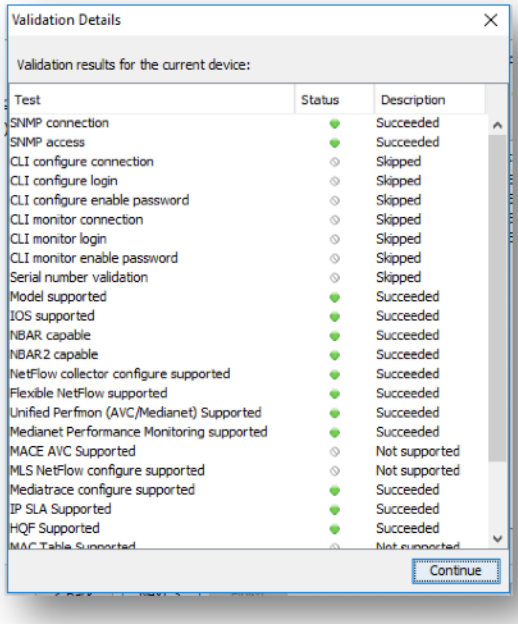


Figure 75

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.

141. Step 5: Ensure the correct interfaces are selected…**GigabitEthernet2, Gigabit Ethernet3, and GigabitEthernet4.** Click **Next**

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

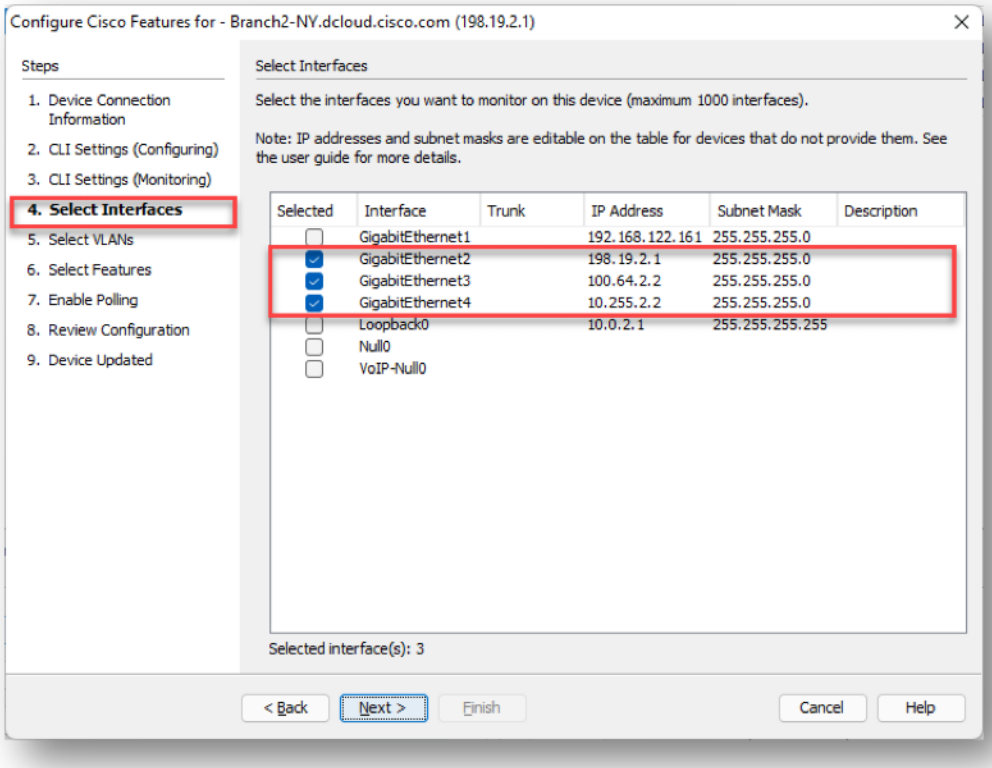


Figure 76

142. 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.**

143. 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**.

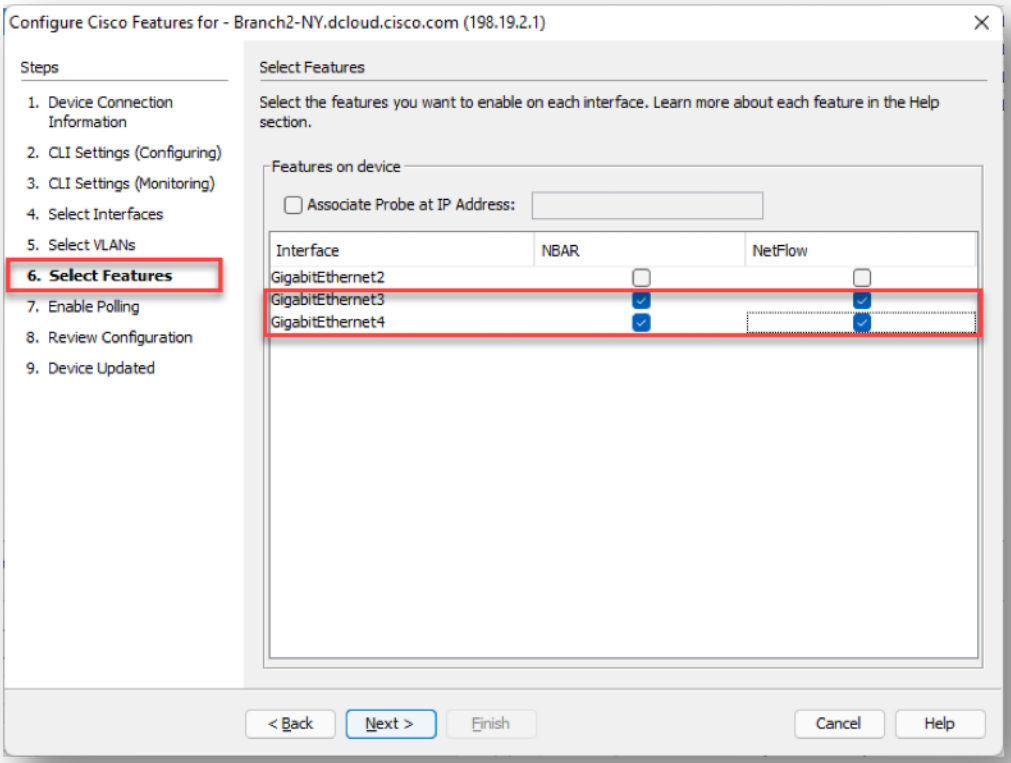


Figure 77

144. 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.

145. Click Continue

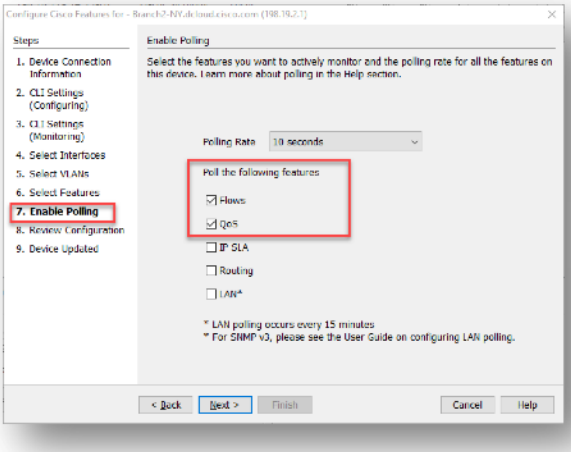


Figure 78

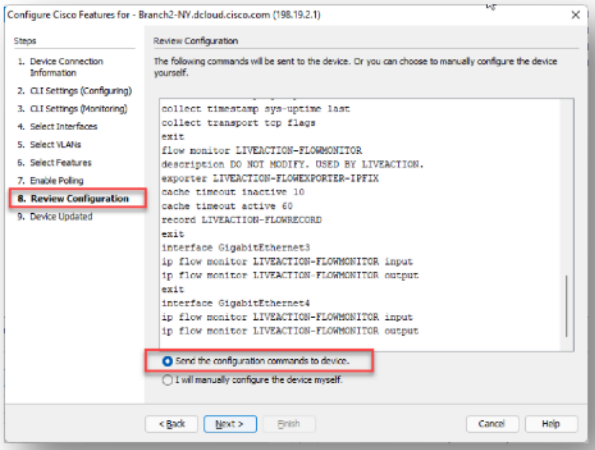


Figure 79

146. 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.

147. Click **Next**. Wait for the configuration process to finish.

148. Click **Finish**.

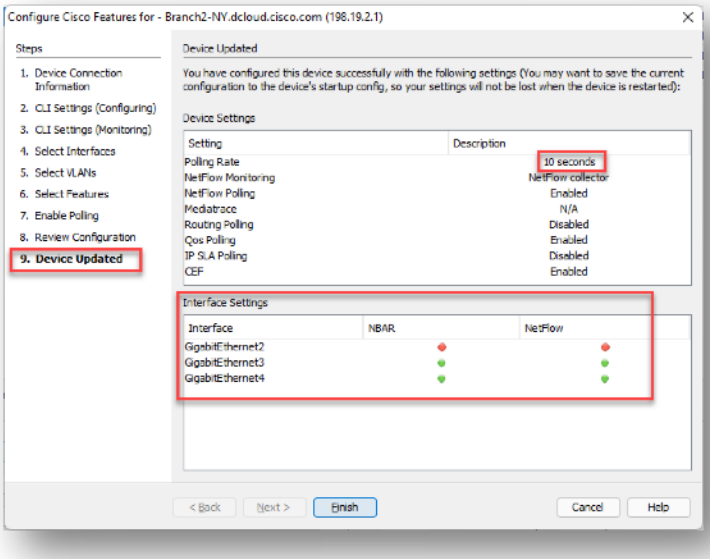


Figure 80

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

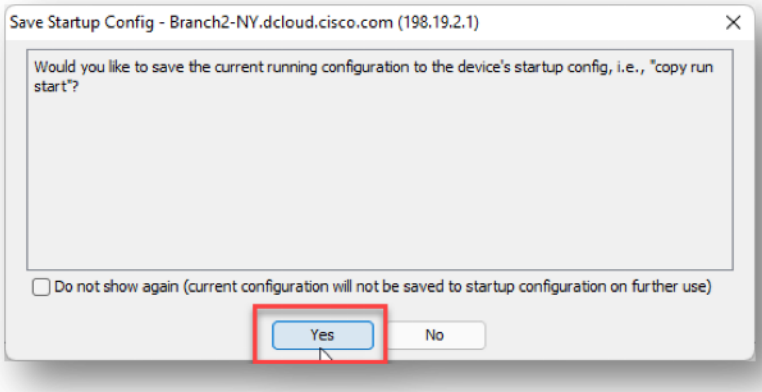


Figure 81

150. 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.

151. 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.

Lab 3.3: Configure Flow on Devices

This Lab uses the Engineering Console.

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:

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

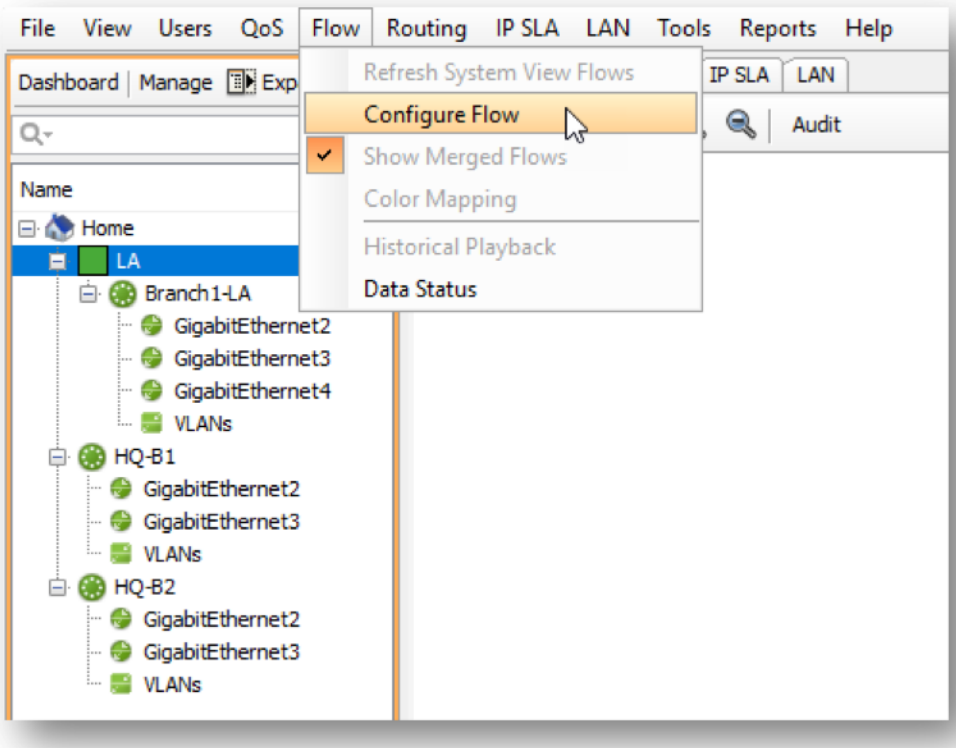


Figure 82

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

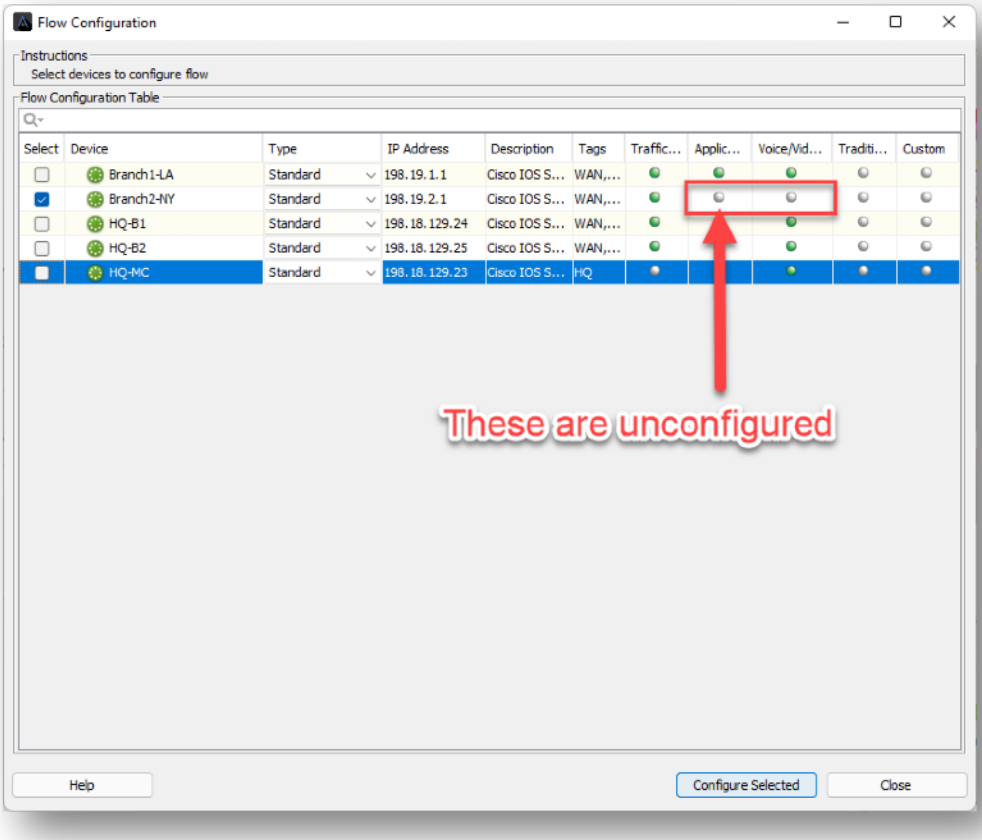


Figure 83

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.

154. **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..

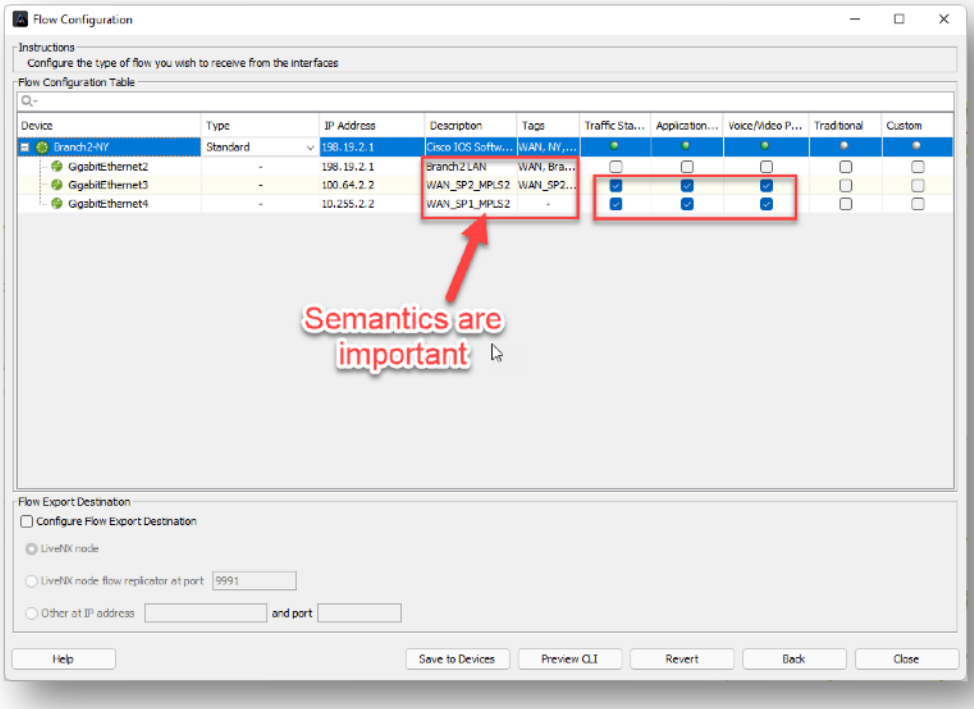
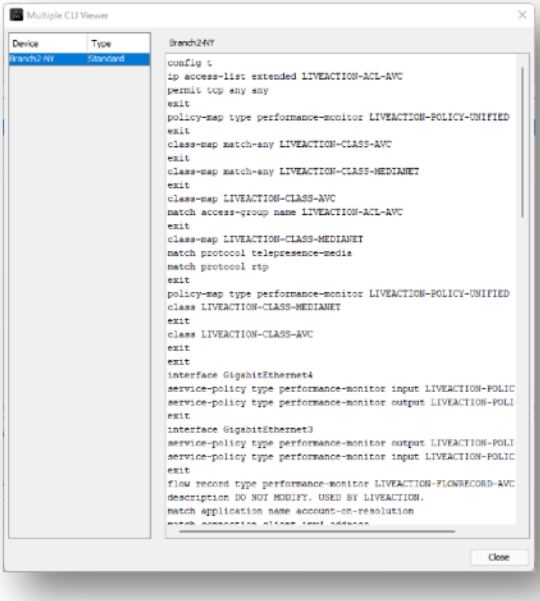


Figure 84

Click Preview CLI.



If you are working on more than one device, the configuration for each will be available to view here. Select a device in the list to view individual CLI file.

Figure 85

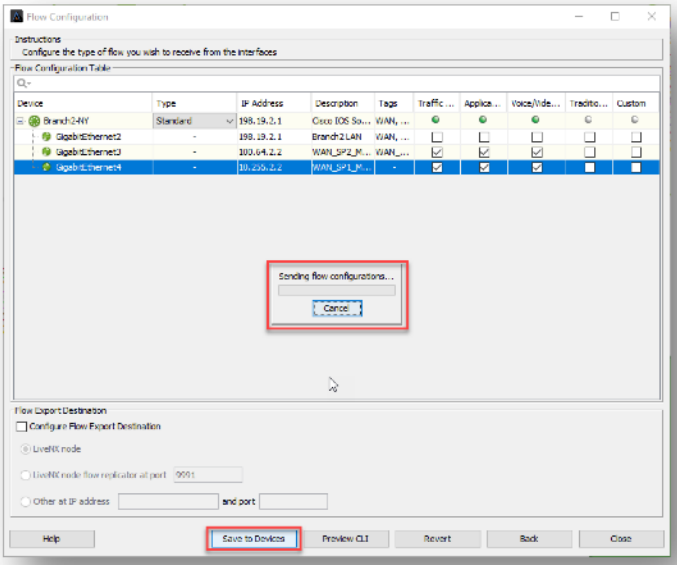


Figure 86

155. Click **Close**.

156. Click **Save to Devices**.

157. Again, **save the current running config to the startup config**.

158. Click **Close**.

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

---

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

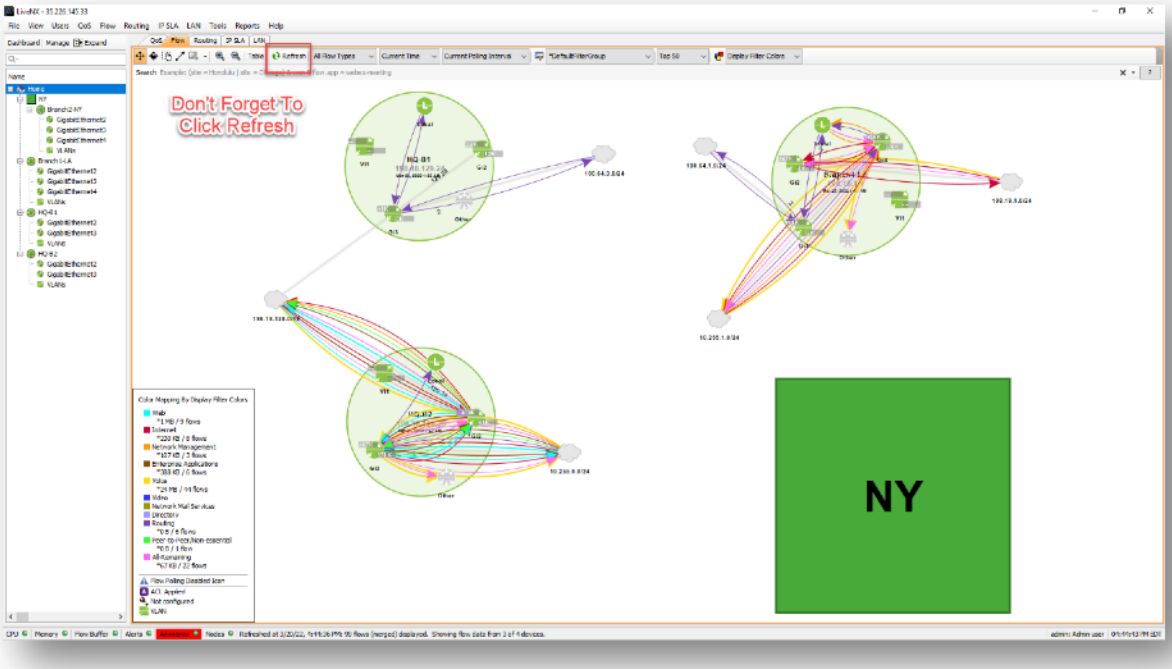


Figure 85

Lab 3.4: Add/Remove Interfaces

<u>This Lab uses the Engineering Console. Results can also be achieved in the WebUI.</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:

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

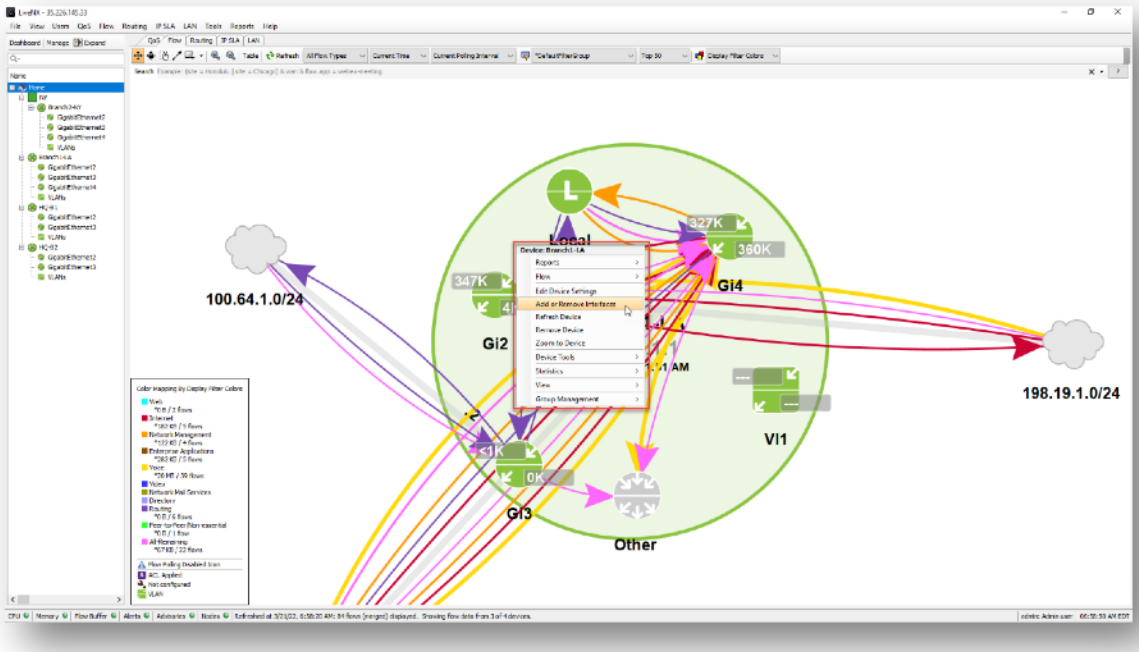


Figure 86

161. Deselect **GigabitEthernet3**.

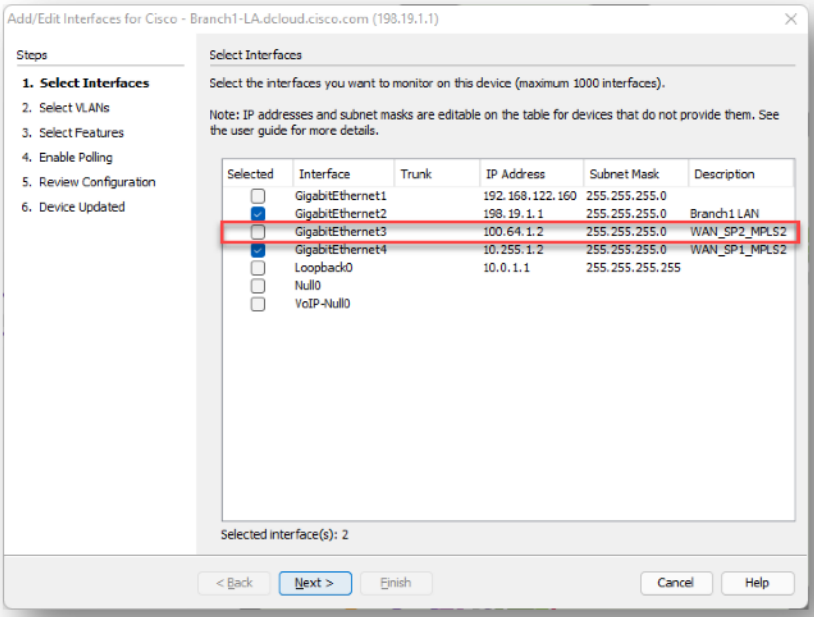


Figure 87

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

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

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

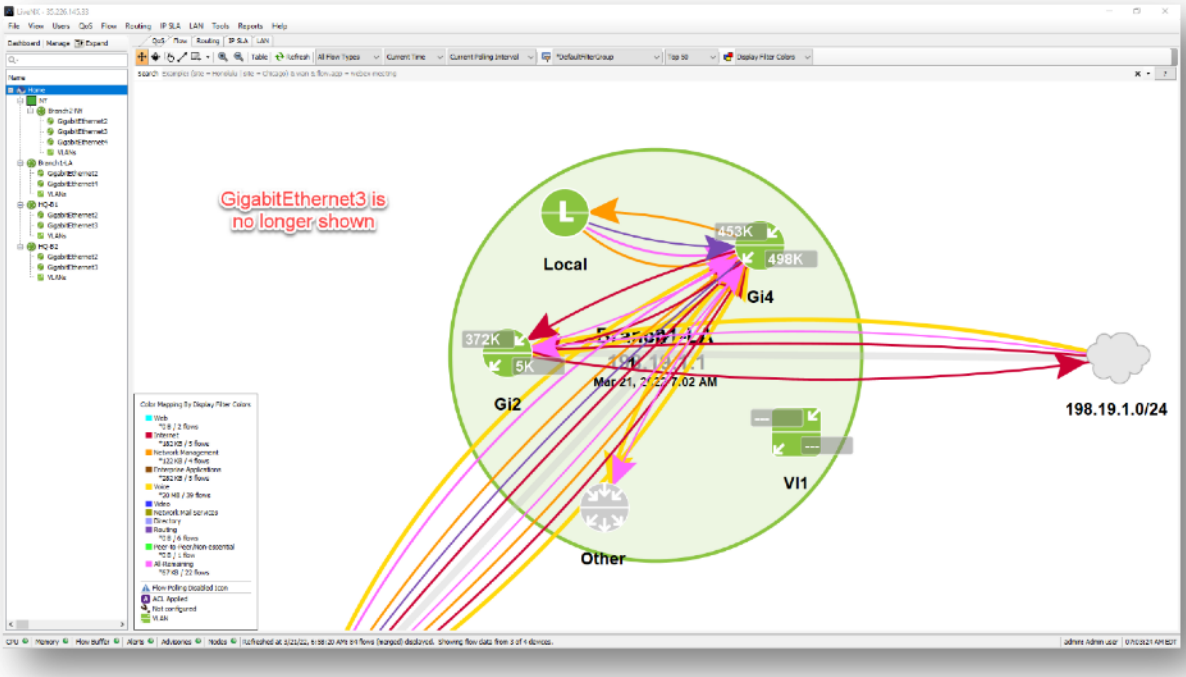


Figure 88

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

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

Lab 4

Lab 4: Making the Topology Work

Lab 4.1: Setting Semantics

<u>This Labs uses the Web UI.</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:

165. Device Semantic Settings can be viewed in the WebUI using the Story **Device Inventory**. You can also verify that all devices have their semantic information configured.

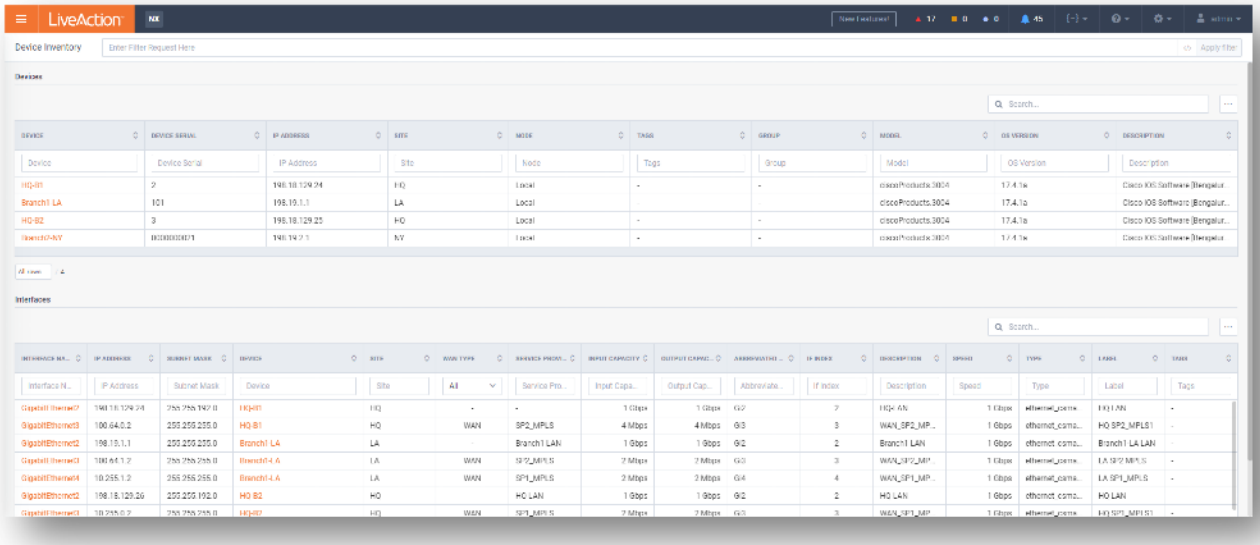


Figure 89

166. To configure semantics for Sites, Devices, and Interfaces you will need to visit the relevant **Configuration** pages. **Configuration** pages can be found under the **Main Menu**.

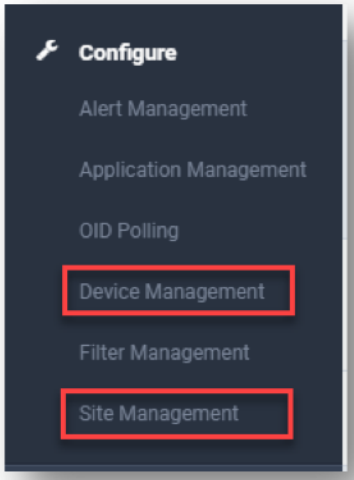


Figure 90

167. Let's start with Site semantics. Which will be in **Site Management**.

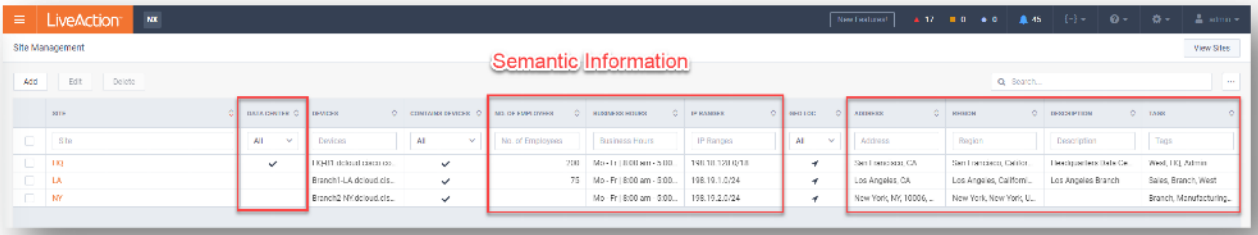


Figure 91

Within the **Site Semantics** page, you will begin to see the importance of **Semantic Data**. Each of the blocks of information highlighted in the boxes above are examples of **Semantic Data**. Semantic data allows you to view, or create views, of your network and its activity to help you understand, monitor, and troubleshoot more effectively.

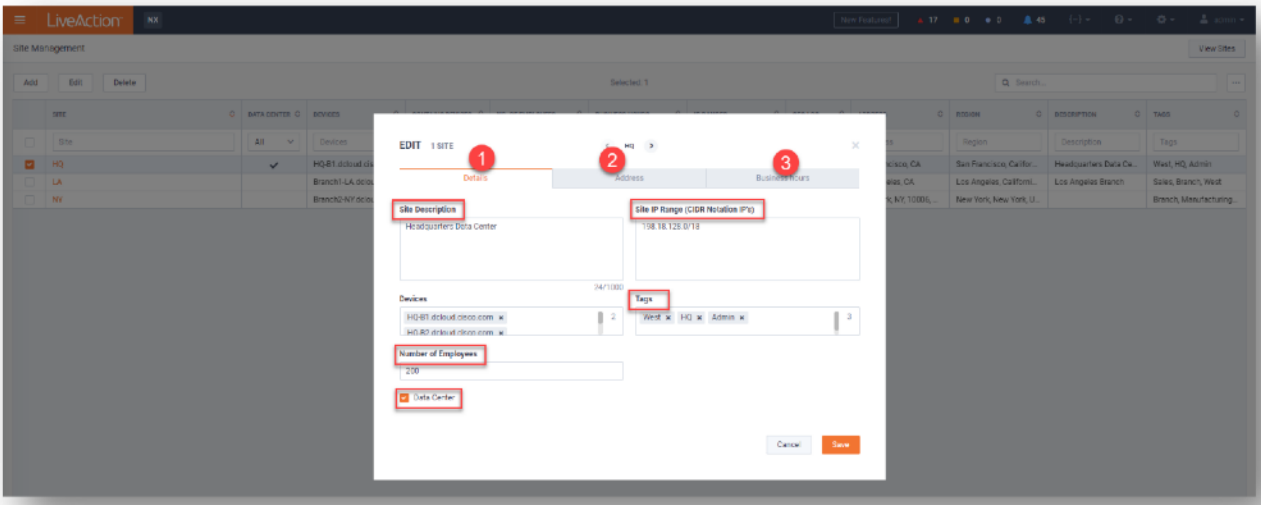


Figure 92

To edit the semantic data for a site, click on the site name, or select the check box and click **Edit**. The **Edit Site** pop-up window will appear and offers three tabs for editing the semantic information. These are **Details**, **Address**, and **Business Hours**. You can move between sites by clicking the arrows wither side of the site name in the middle top of the window.

Make sure you configure the **NY** site added earlier to complete the semantic data entries. You might even want to give it some tags that you can use later for creating a report, or in the Geo-Topology view.

Check the **Site Semantics** against this table, especially the NY branch settings:

Sites	Tags	Site IP Range	Description	Data Center	# Employees	Hrs Operation	City	State
HQ	West, Admin, HQ,	198.18.128.0/18	Headquarters Data Center	Yes	200	8am - 5pm	San Francisco	CA
LA	West, Sales, Branch	198.19.1.0/24	Los Angeles Branch	No	75	8am - 5pm	Los Angeles	CA
NY	**East, Manufacturing, Branch**	**198.19.2.0/24**	**New York Branch**	**No**	**125**	**3am – 10pm**	**New York**	**NY**

Let's now look at Device Semantics, found under **Device Management** in the Configure menu.

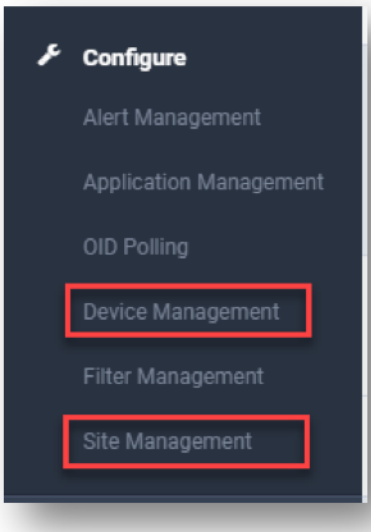


Figure 93

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.

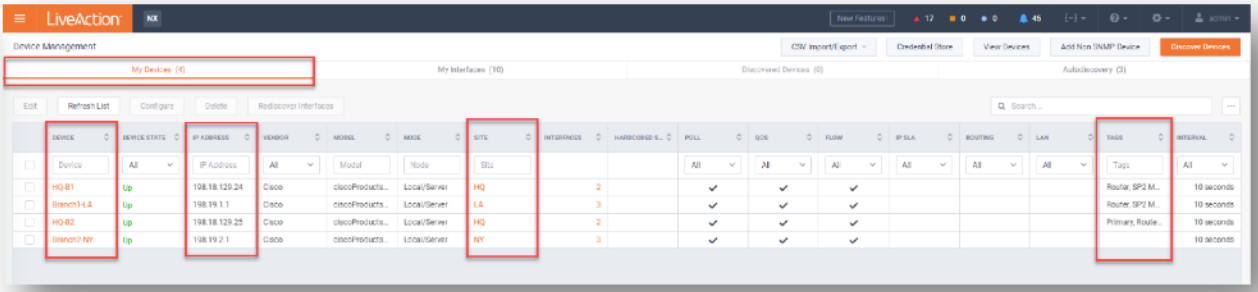


Figure 94

This screen shows the devices that LiveNX is monitoring, along with important semantic data. You can edit this information by clicking on the device name or selecting it with the check box and clicking **Edit**.

As discussed previously, these devices inherit semantic information from above (Site level), and will cascade their accumulated semantic information down to the interfaces.

Check the **Device Semantics** against this table, especially the NY branch settings:

Device	IP Address	Tags	Site	Group
HQ-B1	198.18.129.24	Router, SP2 MPLS, Secondary, DeviceTypeA	HQ	HQ
HQ-B2	198.18.129.25	Router, SP1 MPLS, Primary, DeviceTypeB	HQ	HQ
Branch1-LA	198.19.1.1	Router, SP1 MPLS, SP2 MPLS, DeviceTypeB	LA	LA
Branch2-NY	**198.19.2.1**	**Router, SP1 MPLS, SP2 MPLS, DeviceTypeB**	**NY**	**NY**

Finally, let's check the Interface Semantics that will make using LiveNX more accurate, and seamless.

Interface	Device	Site	Service Provider	Label	WAN/X-Con	Tags
GigabitEthernet2	HQ-B1	HQ	HQ LAN	HQ LAN	None	GE
GigabitEthernet3	HQ-B1	HQ	SP2_MPLS	SP2_MPLS	WAN	ATT, MPLS
GigabitEthernet2	HQ-B2	HQ	HQ LAN	HQ LAN	None	GE
GigabitEthernet3	HQ-B2	HQ	SP1_MPLS	SP1_MPLS	WAN	Verizon, MPLS
GigabitEthernet2	Branch1-LA	LA	Branch1 LAN	Branch1 LAN	None	GE
GigabitEthernet3	Branch1-LA	LA	SP2_MPLS	SP2_MPLS	WAN	ATT, MPLS
GigabitEthernet4	Branch1-LA	LA	SP1_MPLS	SP1_MPLS	WAN	Verizon, MPLS
GigabitEthernet2	**Branch2-NY**	**NY**	**Branch2 LAN**	**Branch2 LAN**	**None**	**GE**
GigabitEthernet3	**Branch2-NY**	**NY**	**SP2_MPLS**	**SP2_MPLS**	**WAN**	**ATT, MPLS**
GigabitEthernet4	**Branch2-NY**	**NY**	**SP1_MPLS**	**SP1_MPLS**	**WAN**	**Verizon, MPLS**

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

Now, when you look at the **Device Inventory Story** you should see a full complement of semantic data for the devices (including the Sites they belong to) as well as the interfaces.

Lab 4.2: Adding Devices to Groups

This Labs uses the Engineering Console.

Within the Engineering Console, having devices in groups makes it easier to manage the topology. You can also use group tags in reports and topology searches.

As you have created the groups in the WebUI lab earlier, this is a review of how the same result can be achieved in the **Engineering Console**. In this Lab you will create three groups, one called **LA**, one called **NY**, one called **HQ**.

Lab Steps:

168. Open the Device Management window by selecting Manage.

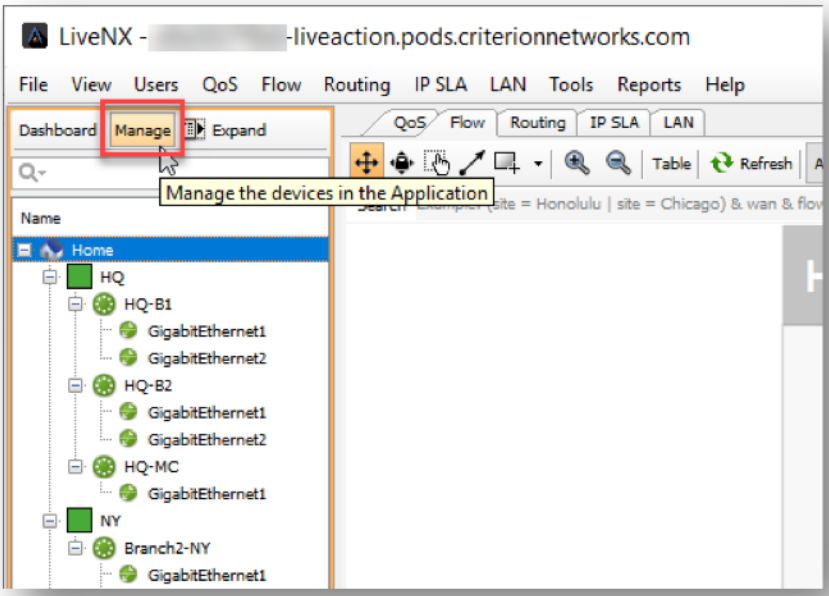


Figure 95

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.

169. Select "**Edit Groups**"

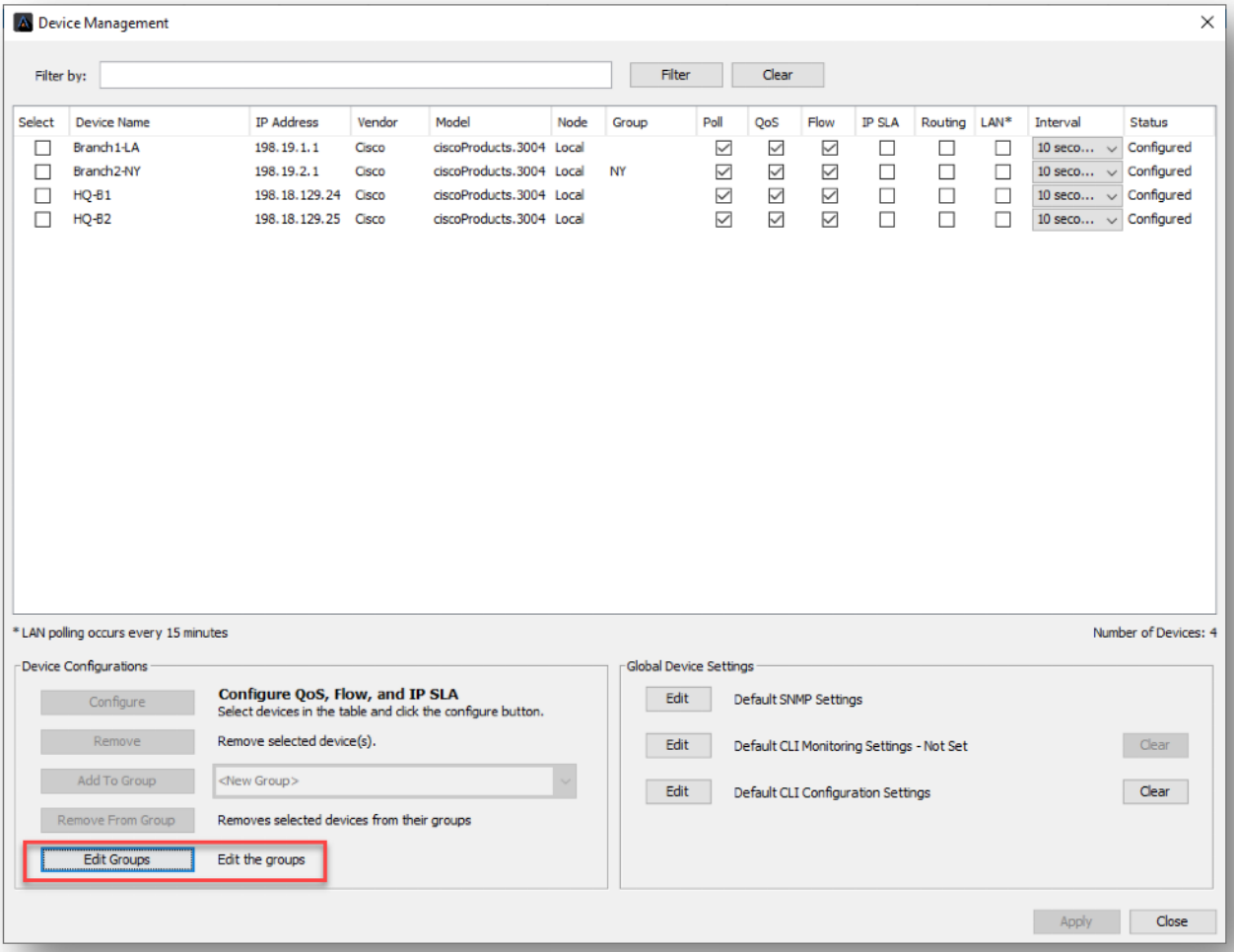


Figure 96

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)

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

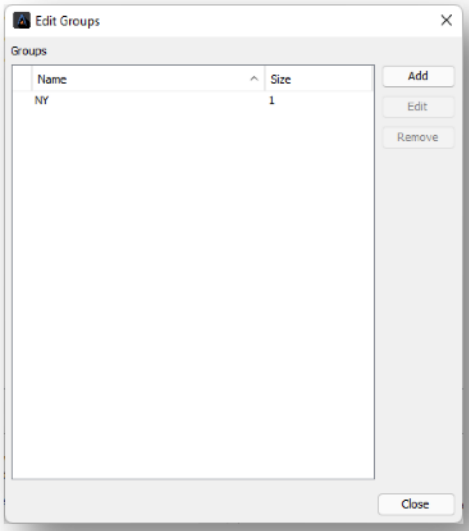


Figure 97

171. Enter **LA** in the Name field.
172. Select **Branch1-LA** from the **All Other Devices** list
173. click the green **Right** arrow (or double click the device)
174. Click **Add**.
175. Repeat the steps above to create the **HQ** group.

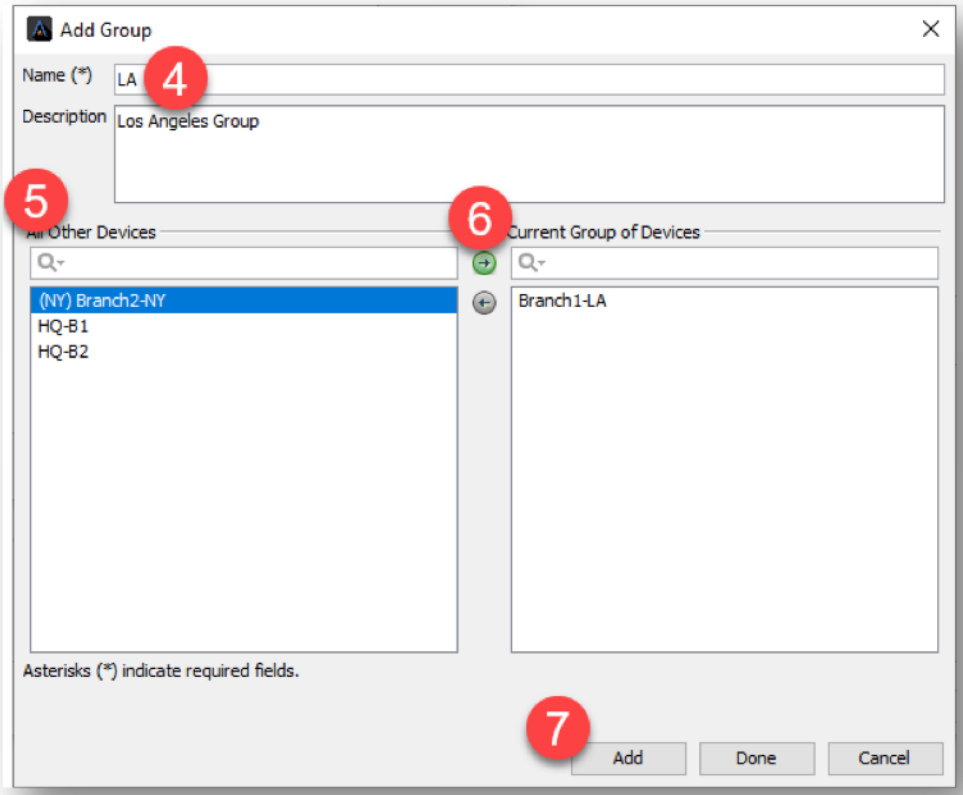


Figure 98

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

Once completed your groups should look like the one below.

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

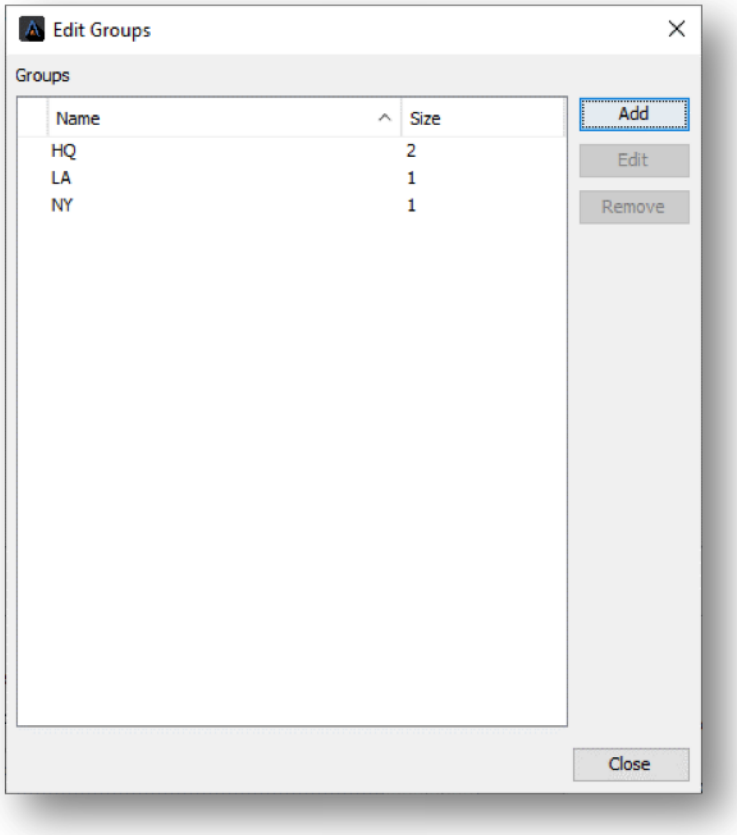


Figure 99

178. You may need to exit out of the previous windows to return to the **Device Management** window.

179. Double-click on the group to expand.

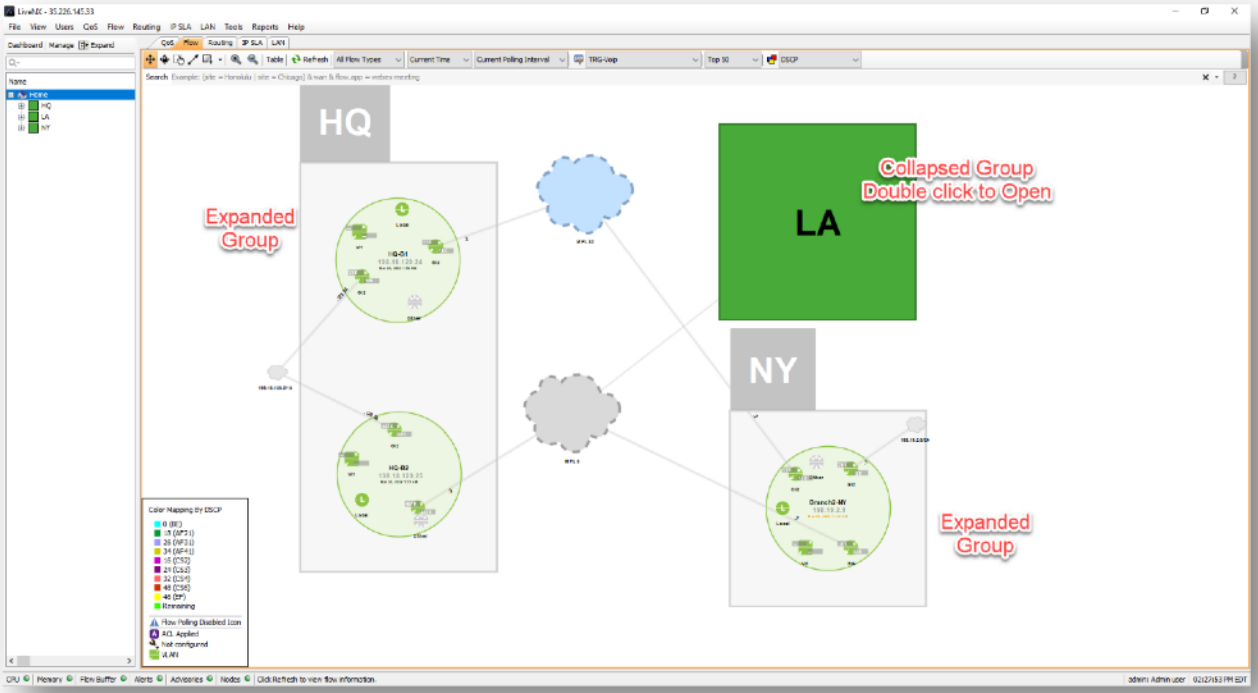


Figure 100

Lab 4.3: Merge Clouds in Topology

This Lab uses the Engineering Console.

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.

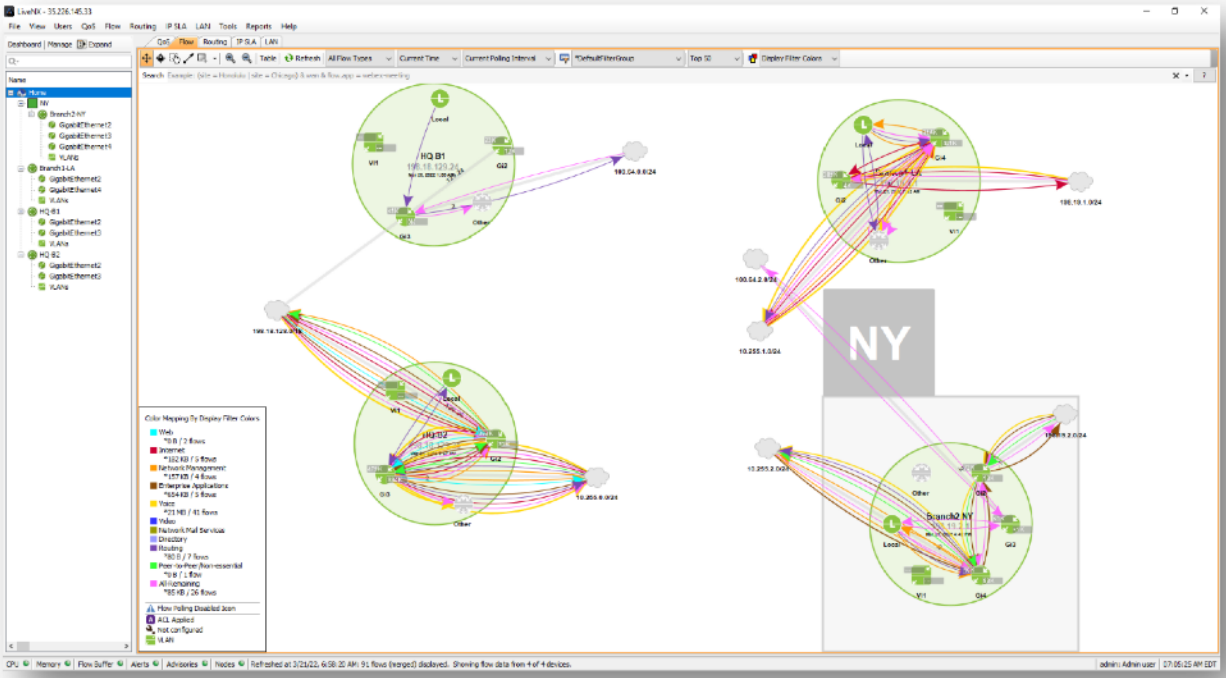


Figure 101

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:

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

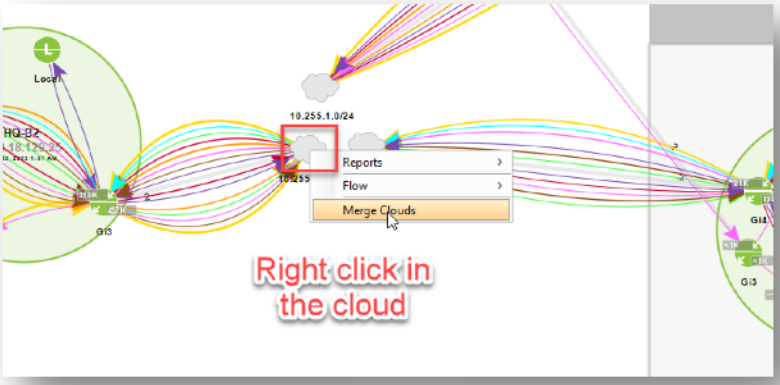


Figure 102

181. On the Create Network Object dialog and configure the **Network Name** (This could be your Service Provider, or Transport ID) We have used **MPLS1**.

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

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

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

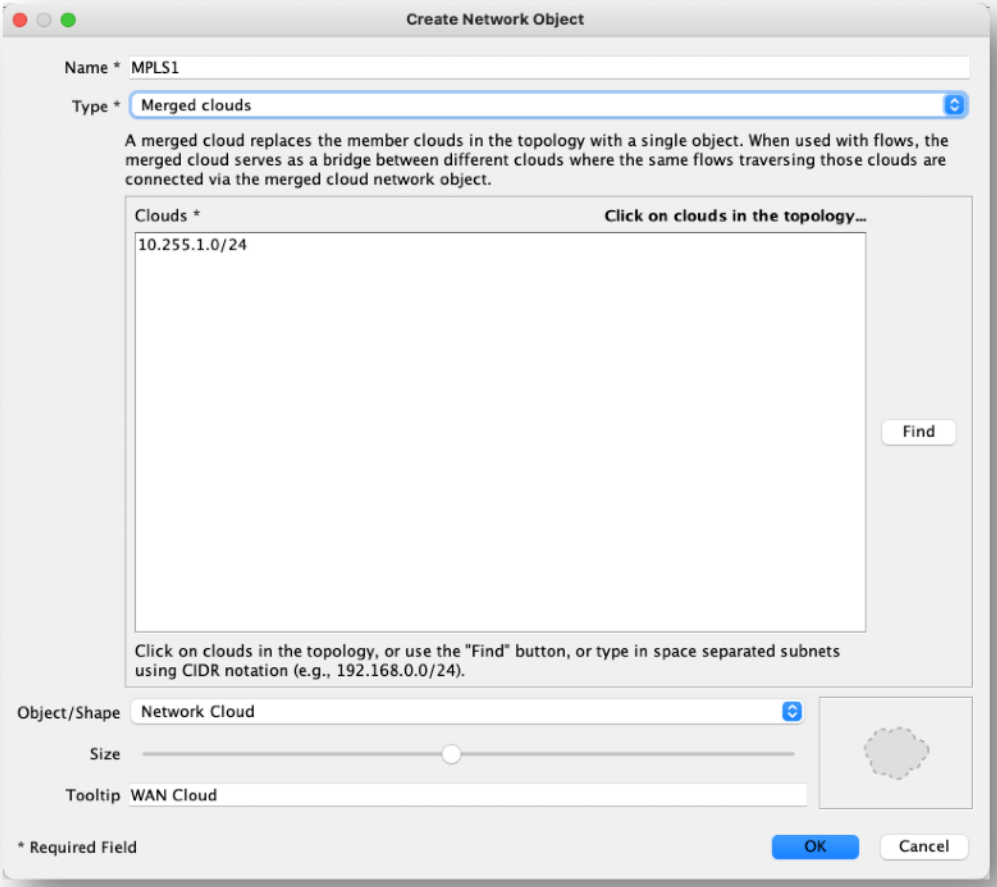


Figure 103

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

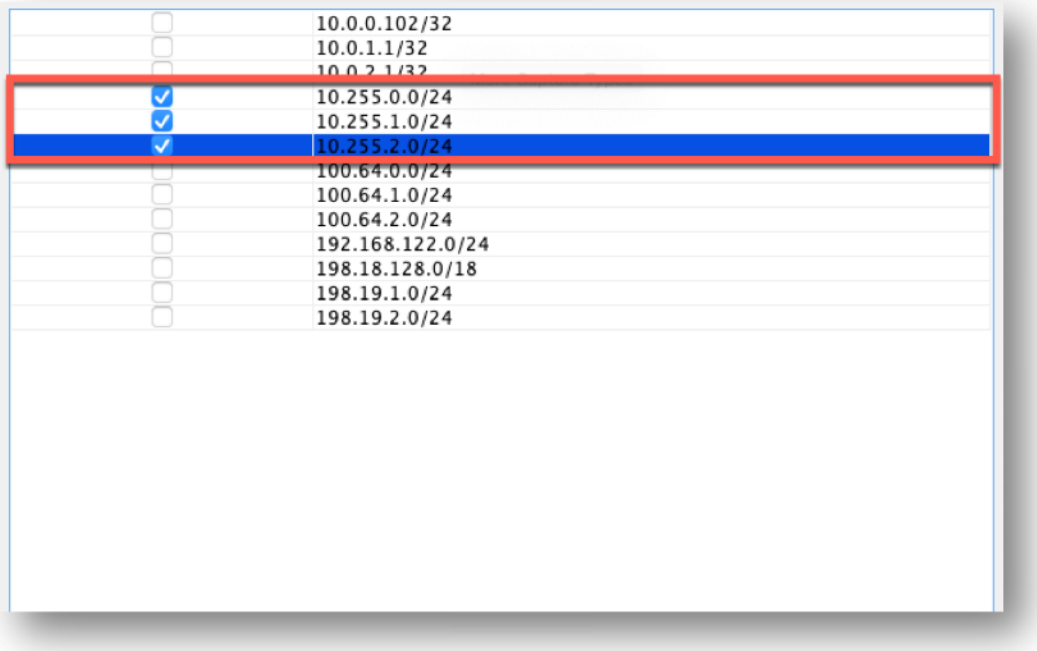


Figure 104

185. Click **OK**.

186. Click **OK** to finish.

Figure 105

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.

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

Figure 106

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

Lab 4.4: 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:

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

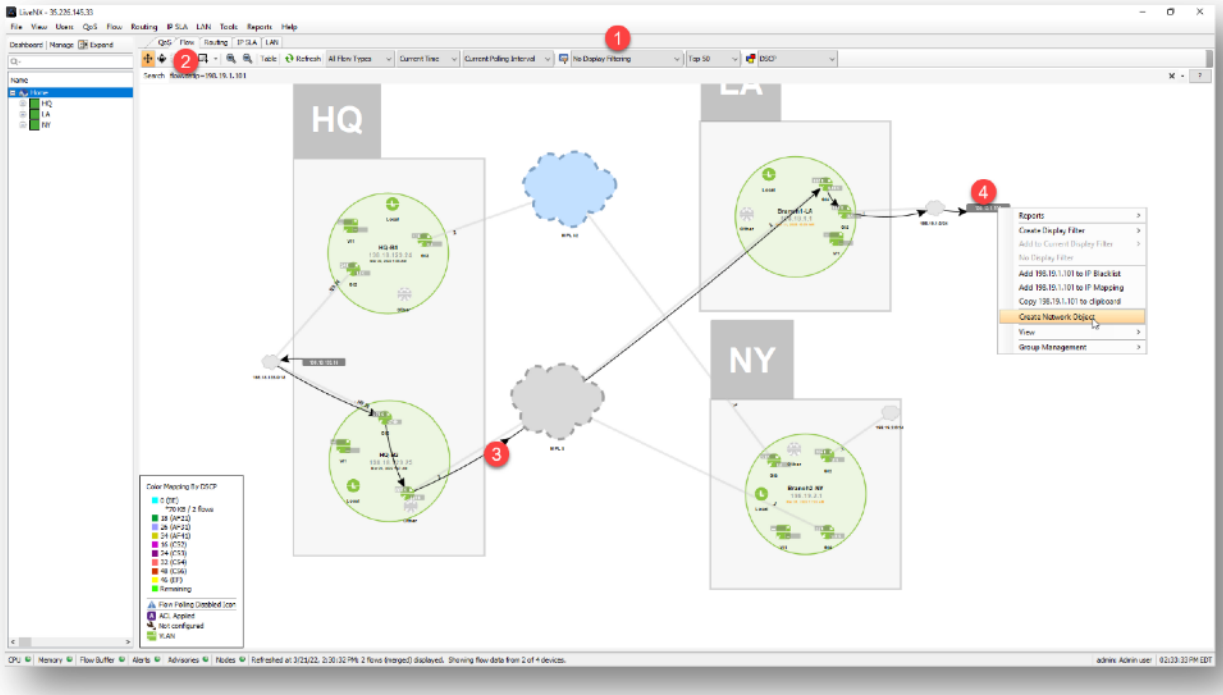


Figure 107

193. Select an **Object/Shape** as "PC".
194. Click **OK**.

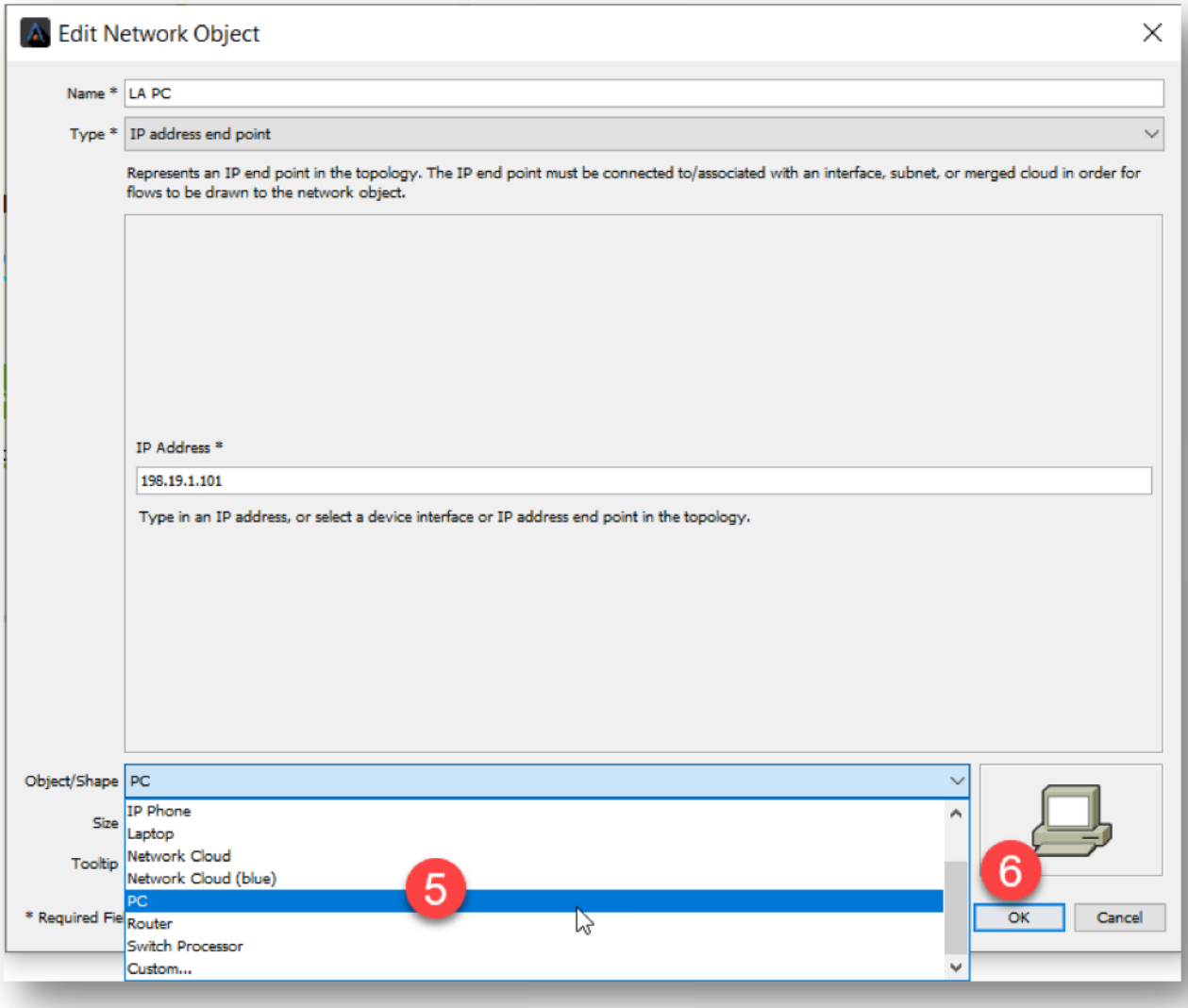


Figure 108

195. Click Refresh.

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

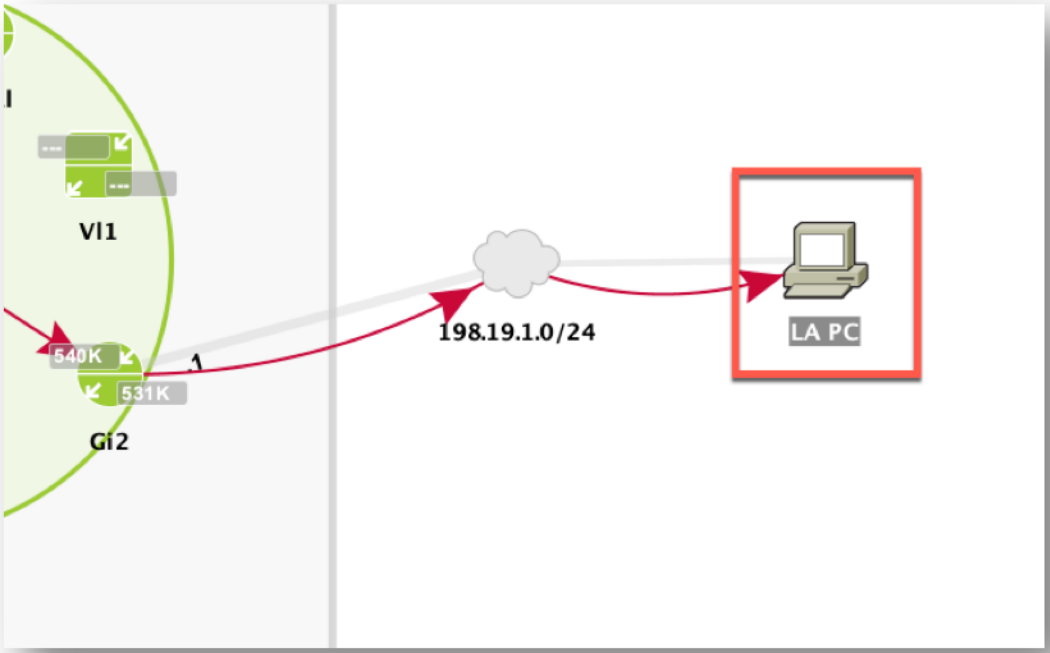


Figure 109

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

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

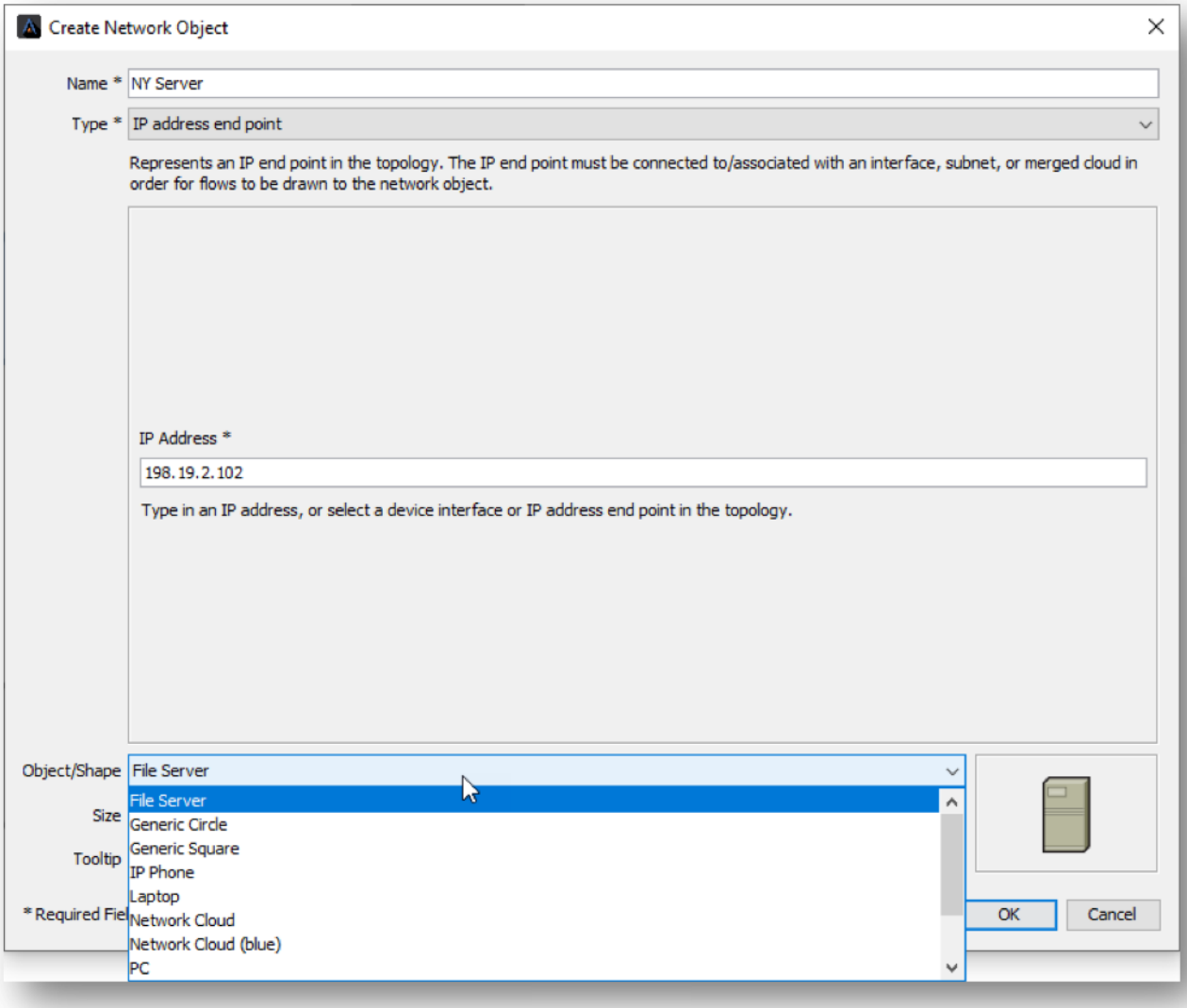


Figure 110

199. Select an Object/Shape as "**File Server**".
200. Click **OK**. This will add the device to the diagram

201. Next, add a Laptop in HQ.
202. Enter the search string: flow.srcip=198.18.133.36
203. Select the flow (it will be near the HQ-B1 and HQ-B2 routers), right click on the IP Address endpoint.
204. Select **Create Network Object**.
205. Select an Object/Shape as "**Laptop**".
206. Click **OK**.
207. Click **Refresh**.

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

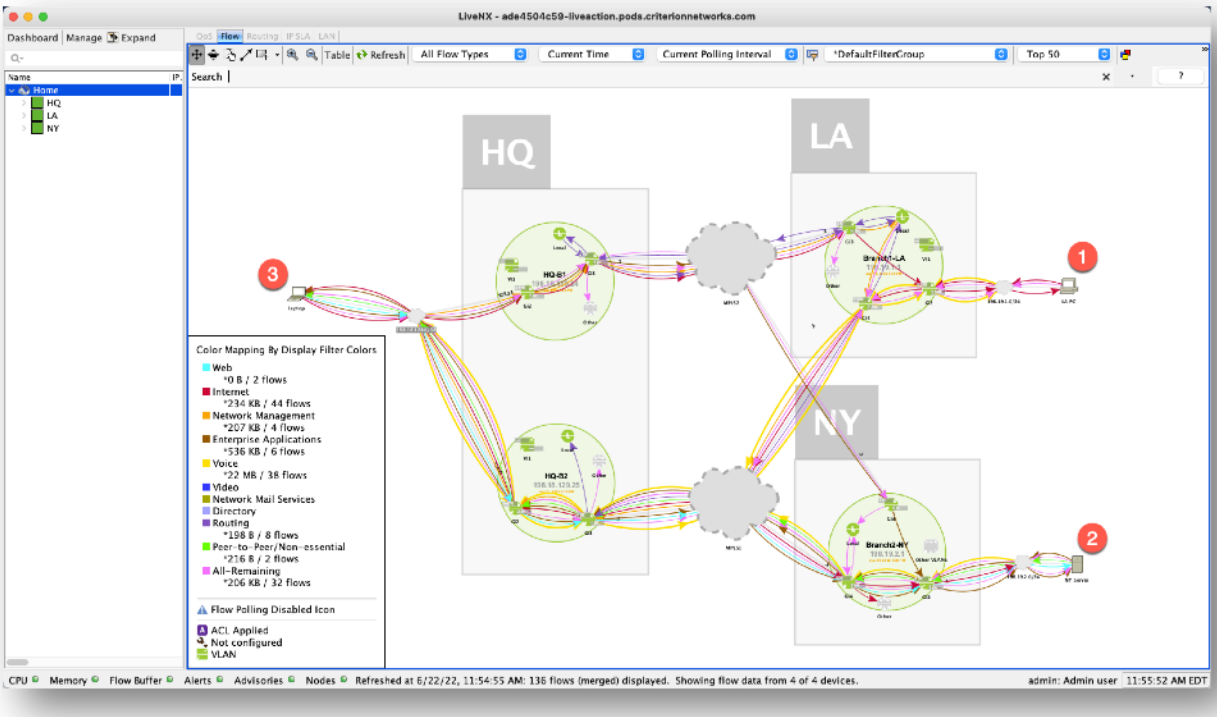


Figure 111

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.

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

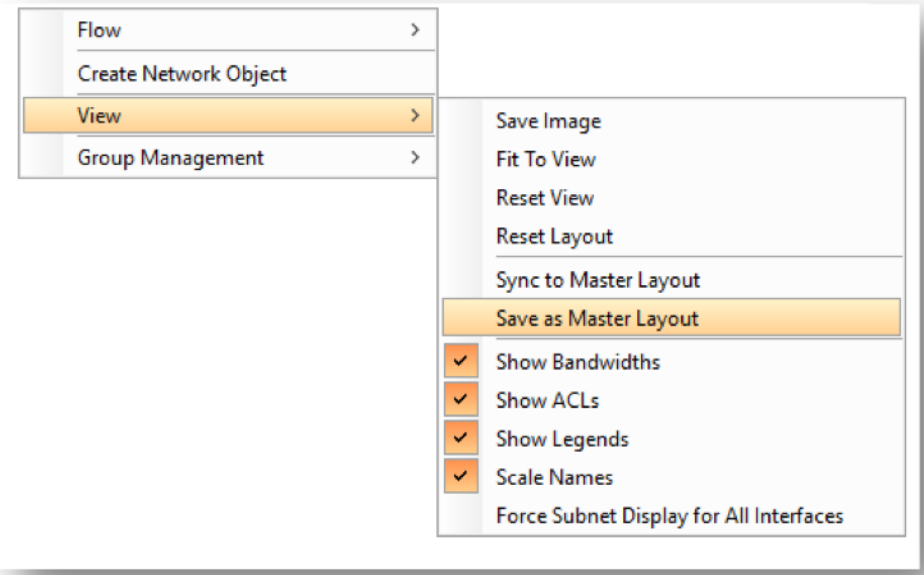


Figure 112

Lab 5

Lab 5: Dashboards & Reports

Lab 5.1: The Dashboard

This Lab uses the WebUI.

The LiveNX Dashboard is your first stop to view overall network health. There are some Default Templates already available, and you have the option to add more dashboards, delete any you don't want, or change them too.

In this Lab you'll examine the data provided within the Dashboard views and learn how to create your intelligence center for key views and information that LiveNX provides.

Lab Steps:

209. Click the Main Menu hamburger, and then click on Dashboard

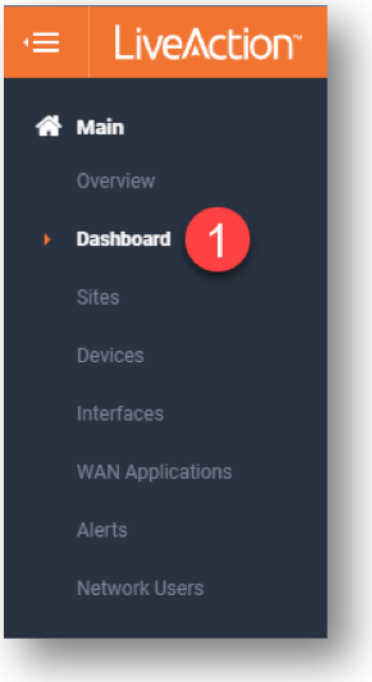


Figure 113

The Dashboard display is laid out with Tabs (2), and “Widgets”, also called Display panels (3).

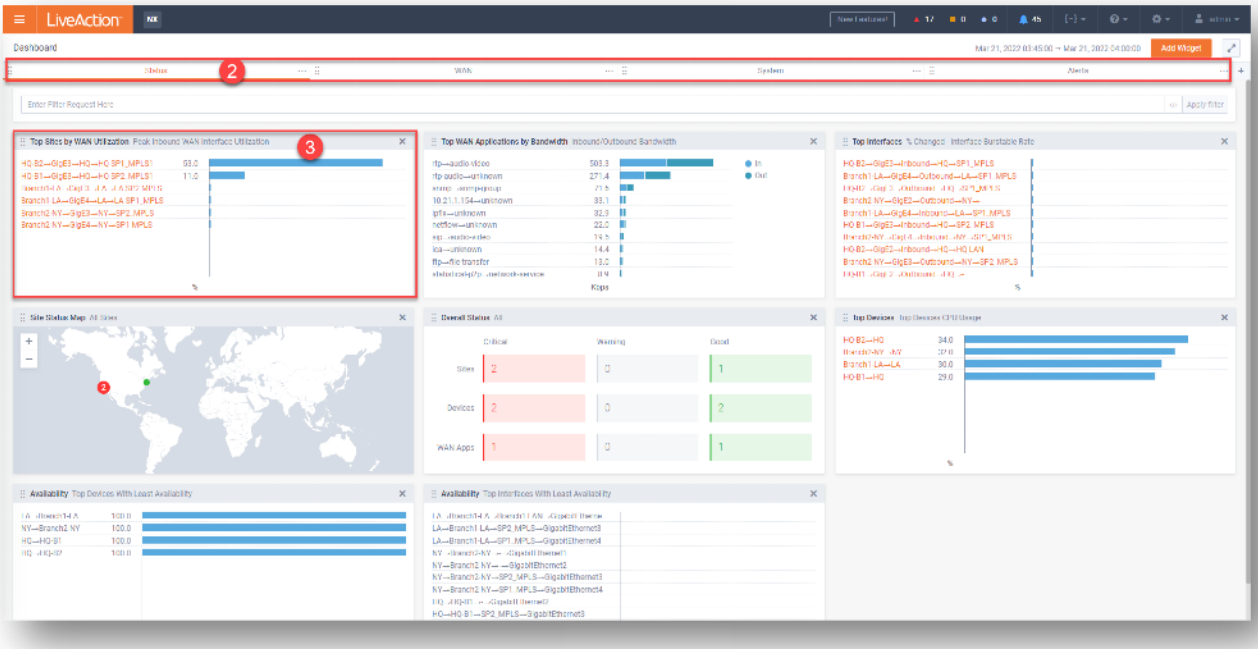


Figure 114

210. You can click any Widget heading, or orange text in the widgets for further drilldowns. Many of the charts and graphs will reveal more insight when you mouse-over them.

211. When you click these items, a new browser tab will open.

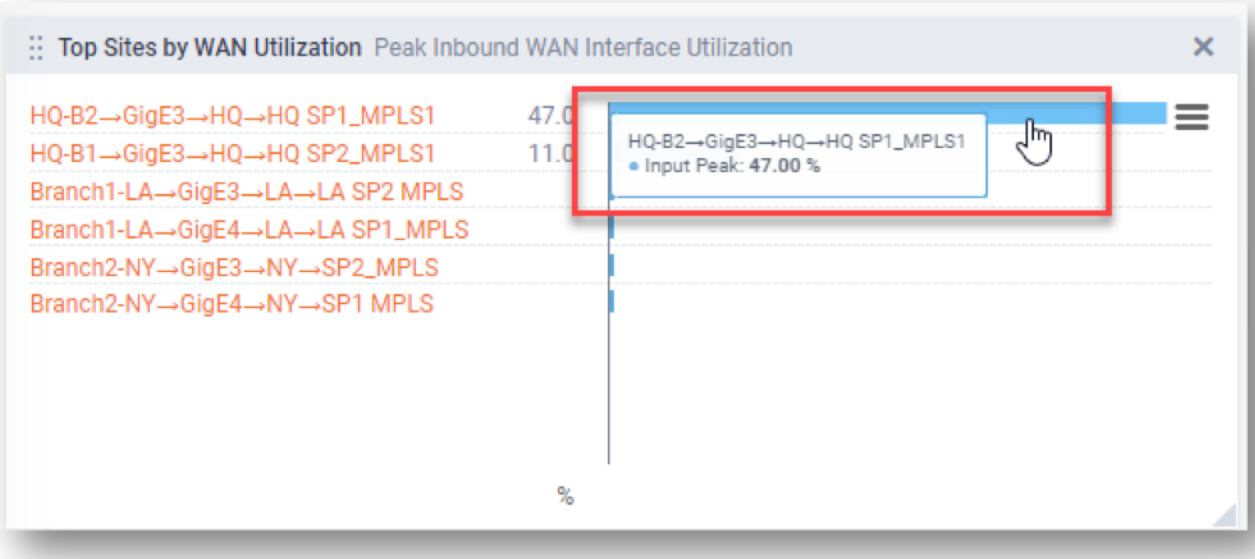


Figure 115

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

212. Click on the **WAN** tab.

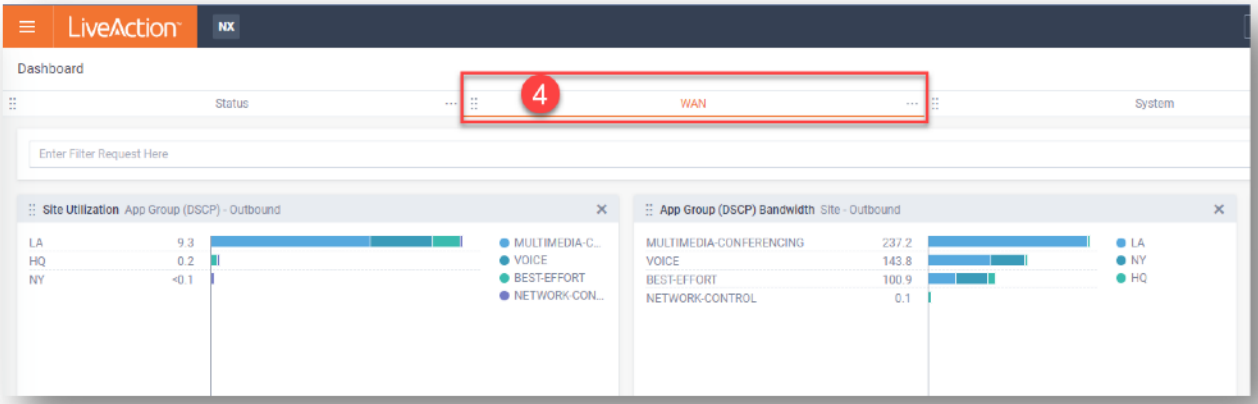


Figure 116

213. We are going to use this dashboard that shows all data in each of its widgets, and change it to only **rtp** data.In the **Search Bar** (5), click and select **Application** (6) from the dropdown options.

214. This will bring the **Application Pick** list (7), where you can specify which application you want to filter. Type **rtp**, and click on **rtp** from the list that appears.

215. Finally, click **Apply** to enact the filter.

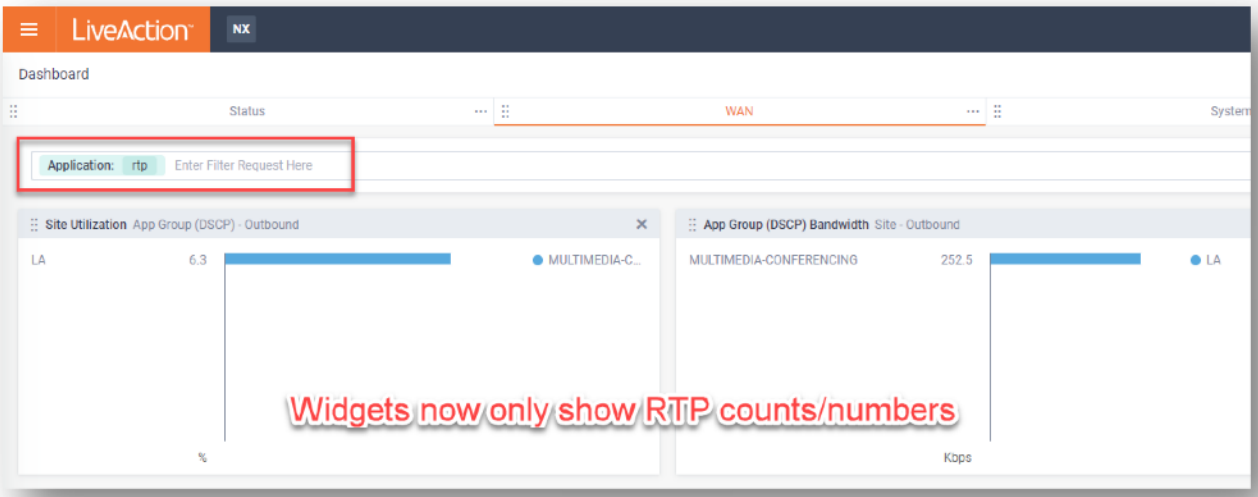


Figure 117

216. Next, we will create a new Dashboard, and populate it with specific reports.

217. Click on the + sign on the right side of the Dashboard Tab Bar.

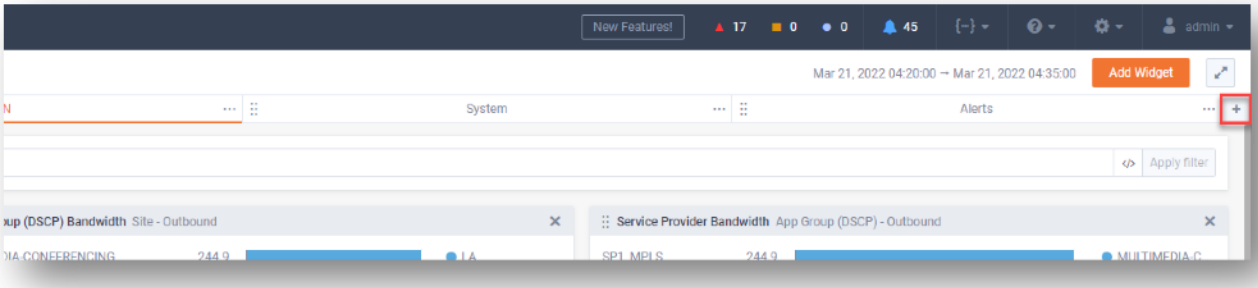


Figure 118

218. This will bring up a New Tab, which can be renamed by clicking in the text in the tab. We called our **TRAINING TAB**. Use any name you wish for your tab.

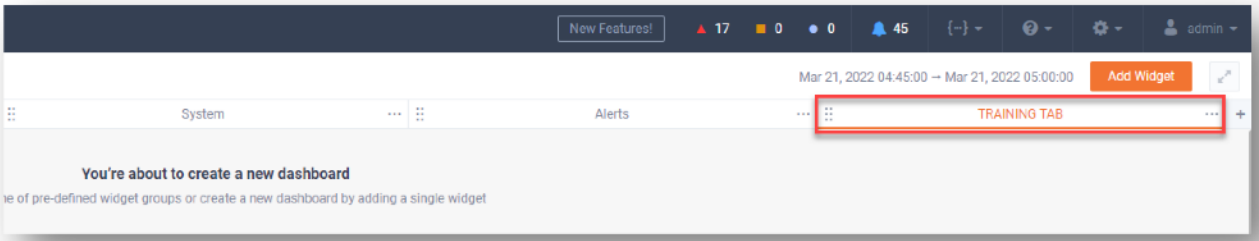


Figure 119

219. In the main body of the page, you'll find options of standard Dashboard layouts that can be modified, or the choice to build a custom dashboard. Click on **Custom Dashboard**.

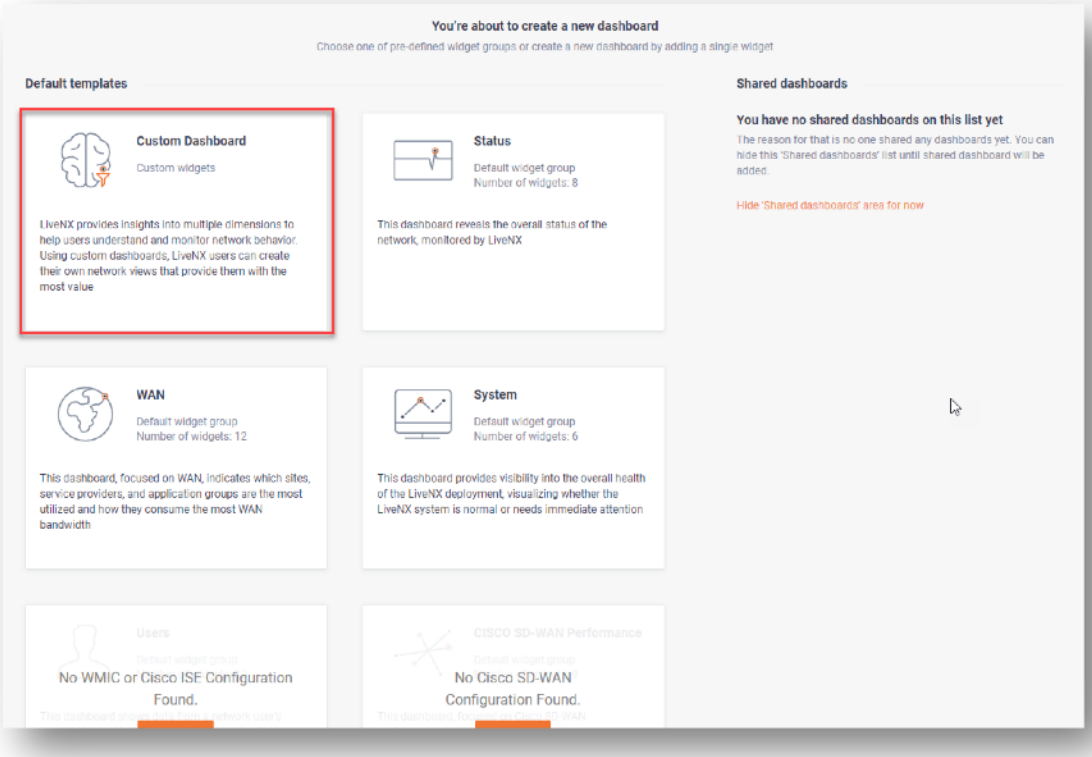


Figure 120

220. This will open a panel on the right where you can select standard reports to use as a standard widget or create your own widget from a custom report.

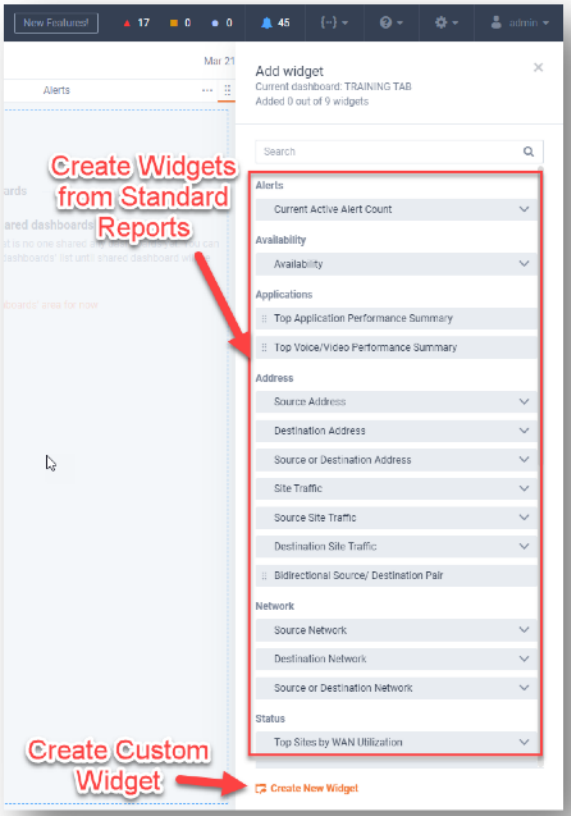


Figure 121

221. To add standard widgets to the Dashboard, either drag and drop items with the **Drag Handle** or open the category stacks to reveal options

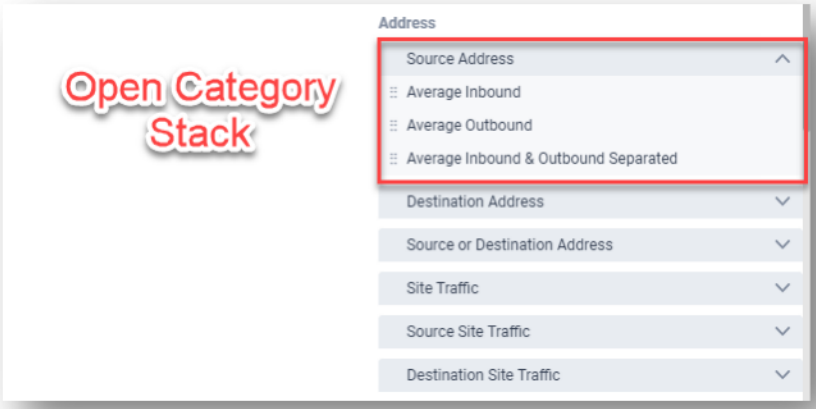


Figure 122

222. Drag any combination (up to 9 in total) onto a Custom Dashboard.

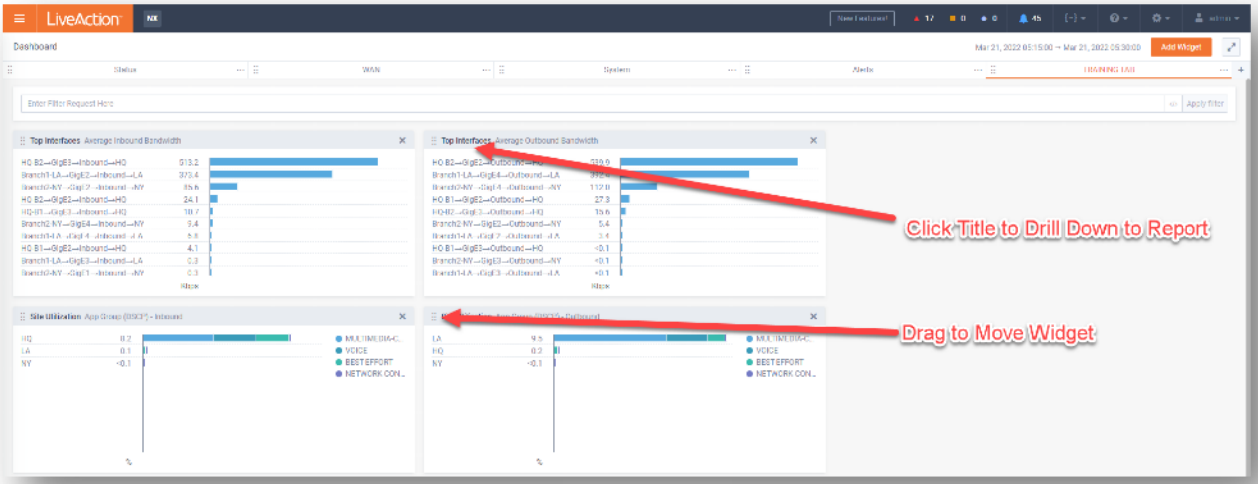


Figure 123

223. Congratulations. You've created a Custom Dashboard, and learned how to filter data within the view, as well as drilldown to detailed information.

Lab 5.2: 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

224. You will be using the **WebUI** for this part of the lab.

225. Select **View Reports** from the menu on the left.

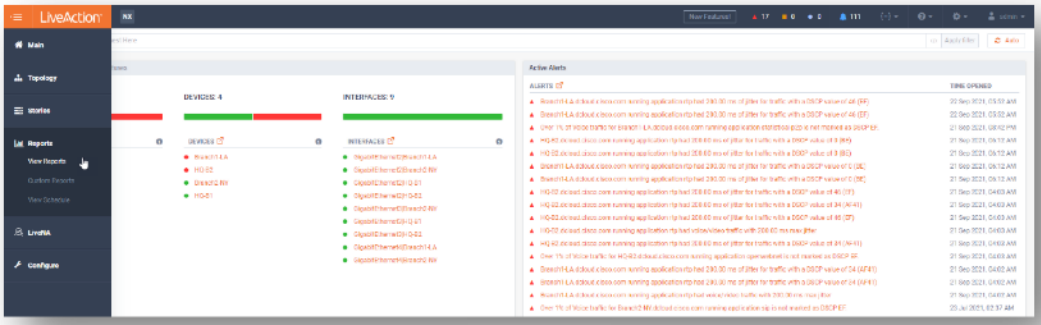


Figure 124

226. Select the **Application** report from **Top Reports**.

227. 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.

228. Select the **Inbound and Outbound Combined** filter.

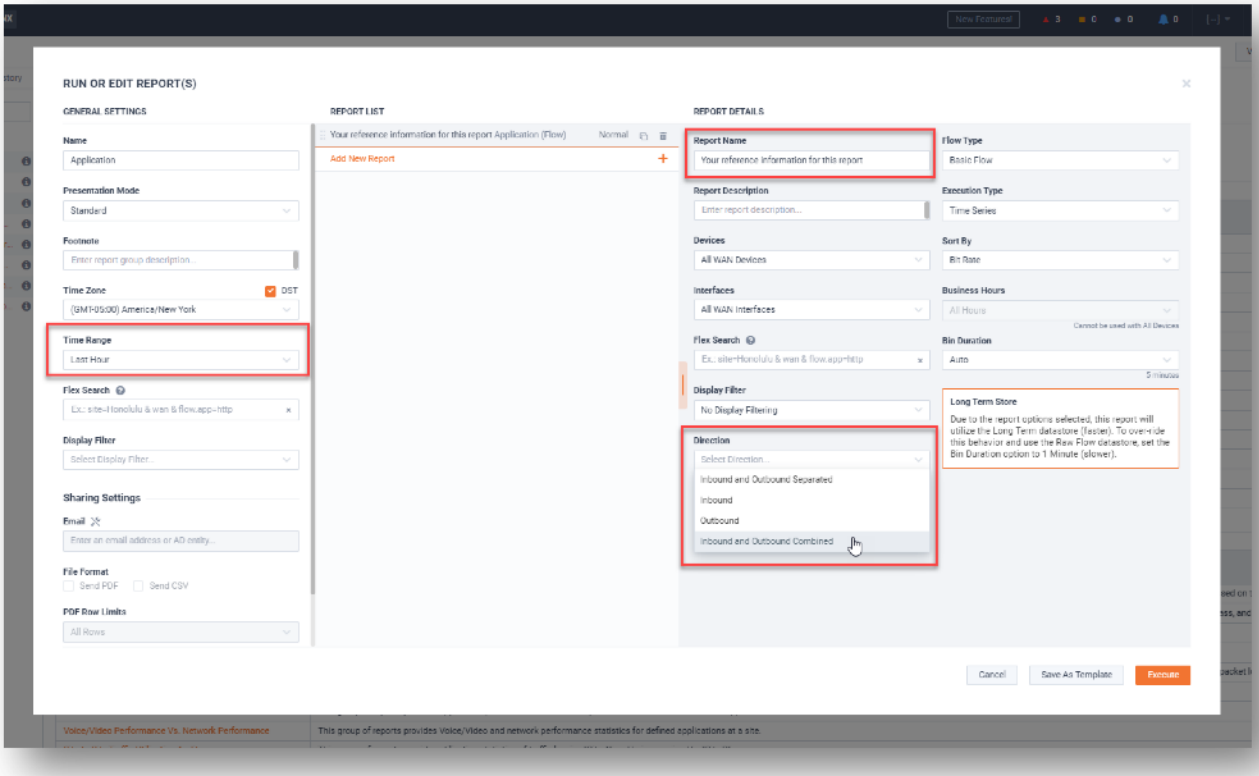


Figure 125

229. Click **Execute**.

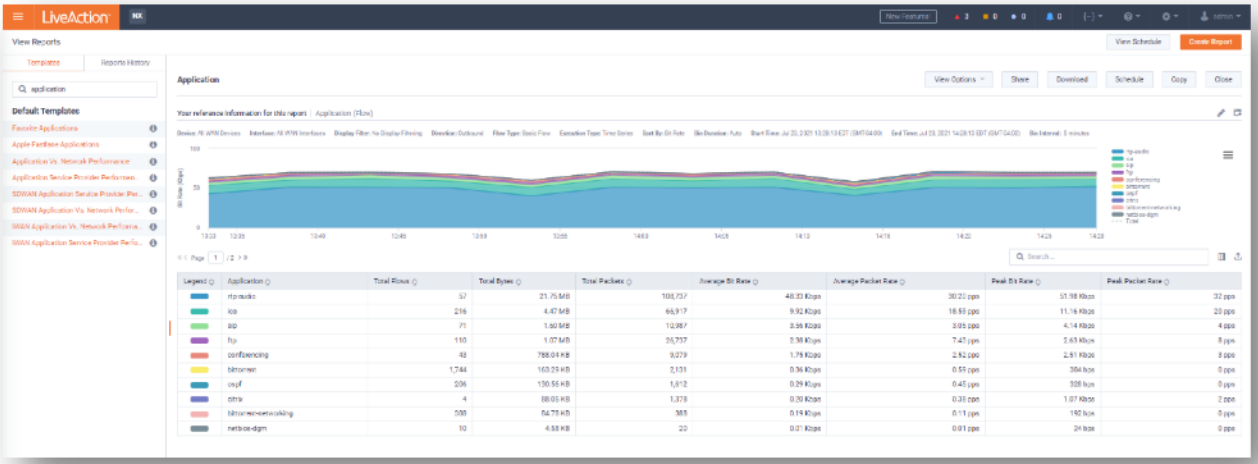


Figure 126

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

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

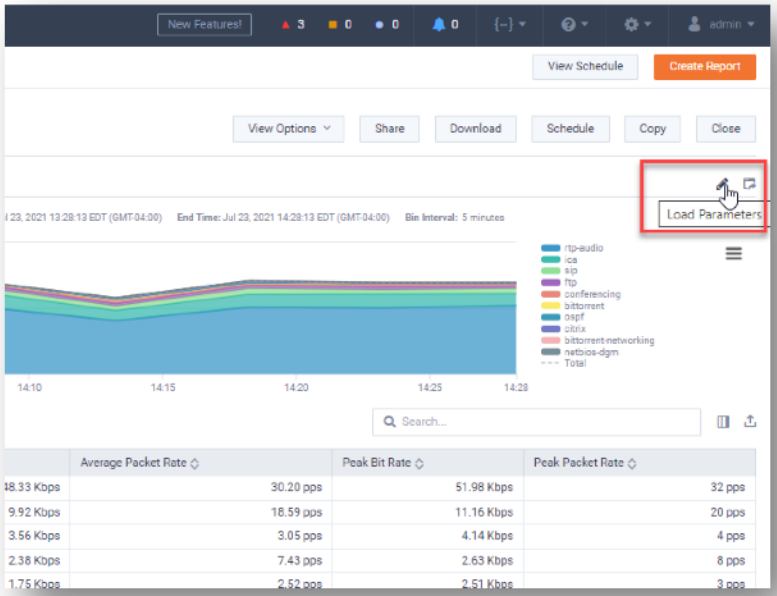


Figure 127

231. Click **Add New** Report, and then select **Top Conversations**.

232. 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.

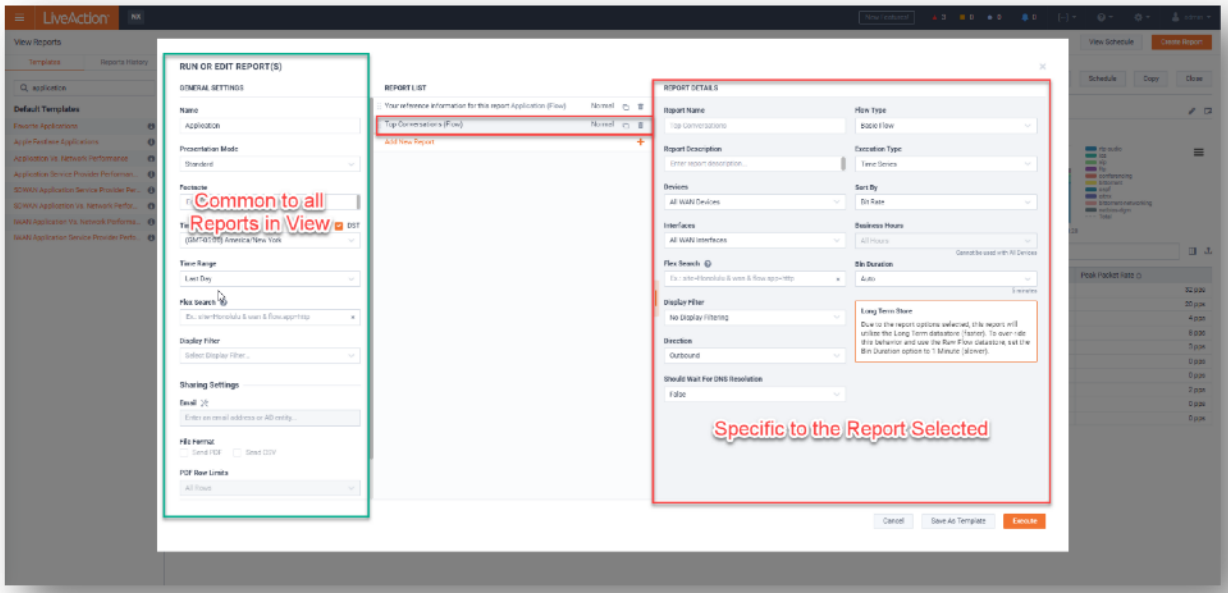


Figure 128

233. Click **Execute**.

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

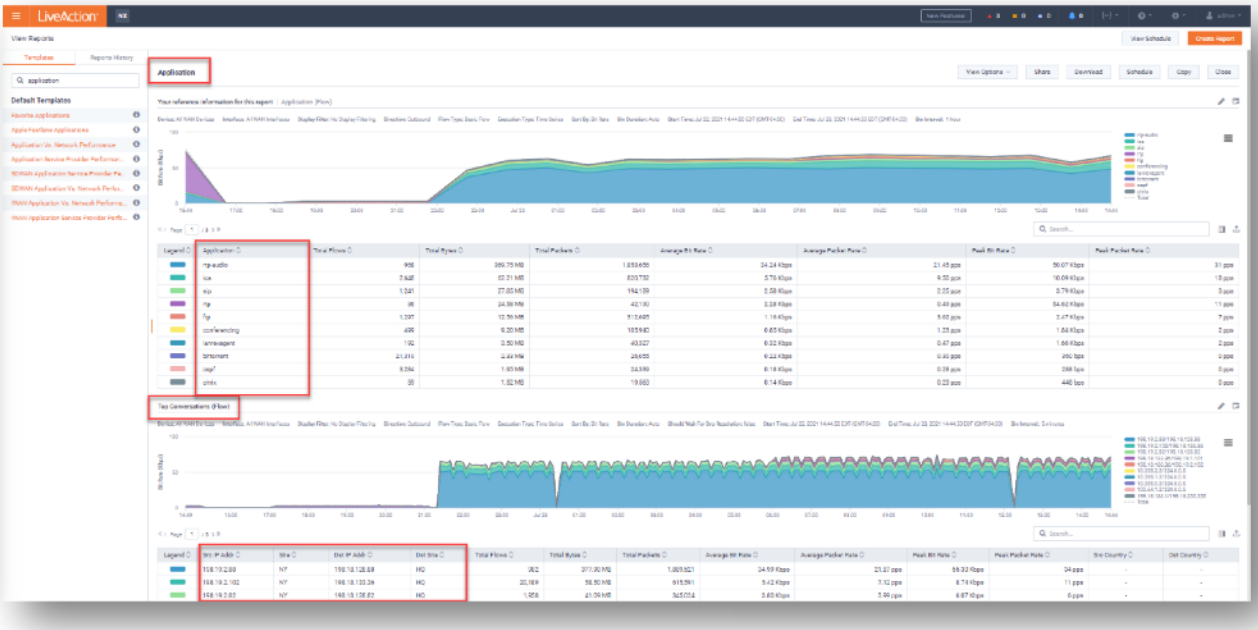


Figure 129

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

234. Close the report view. Next, we will look at QoS information by **DSCP** value.

235. On the report menu, click **DSCP**.

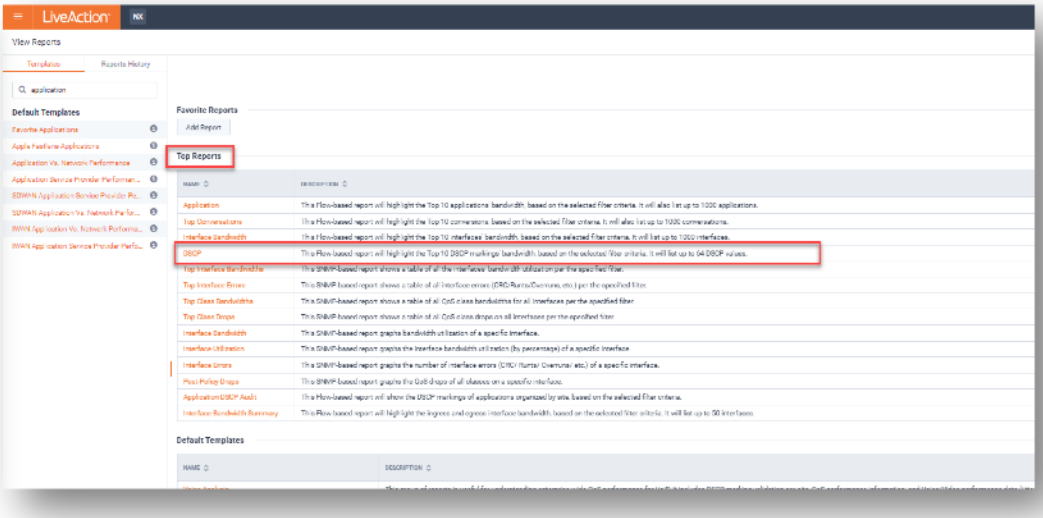


Figure 130

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

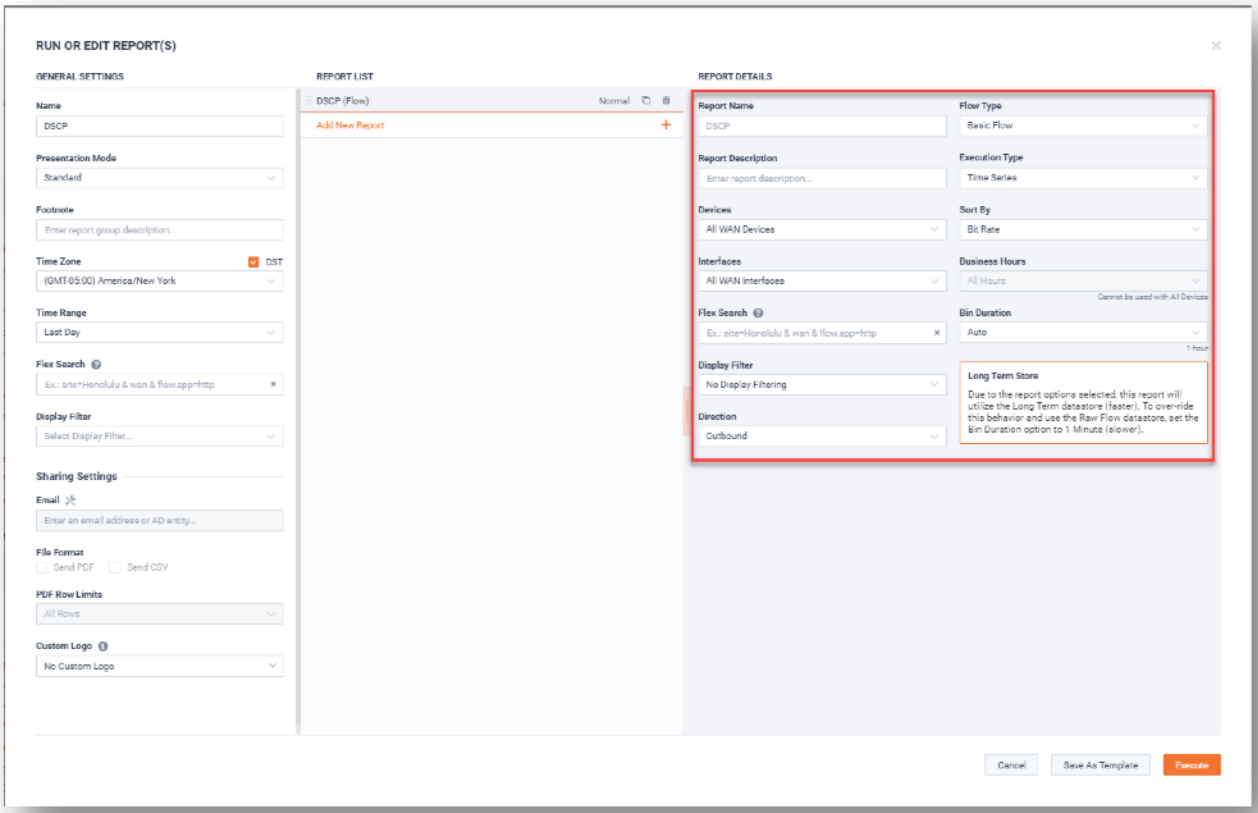


Figure 131

237. Click **Execute**.

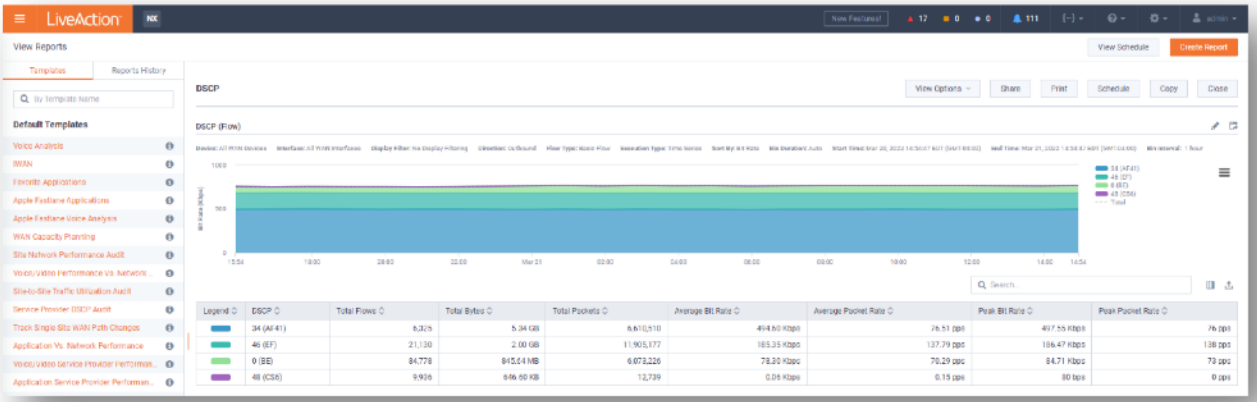


Figure 132

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 BEST EFFORT to route it. This **may** be a candidate for marking so that QoS may use priority routing.

Bandwidth by Flow Type

238. Let's add some more information to our page.

239. Click the **Load Parameters** pen icon and add **Interface Bandwidth Summary** from the Top Reports section.

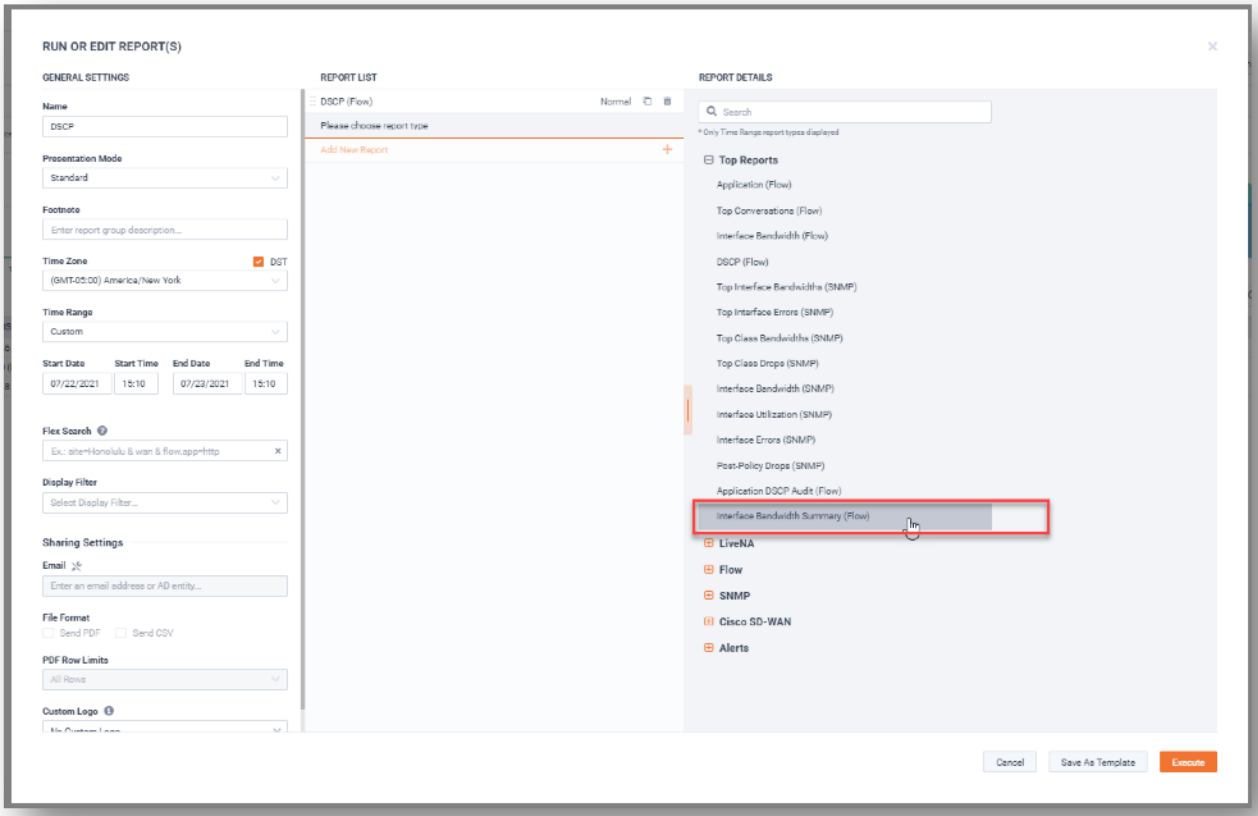


Figure 133

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

241. Select **All** devices.

242. Click **Execute**.

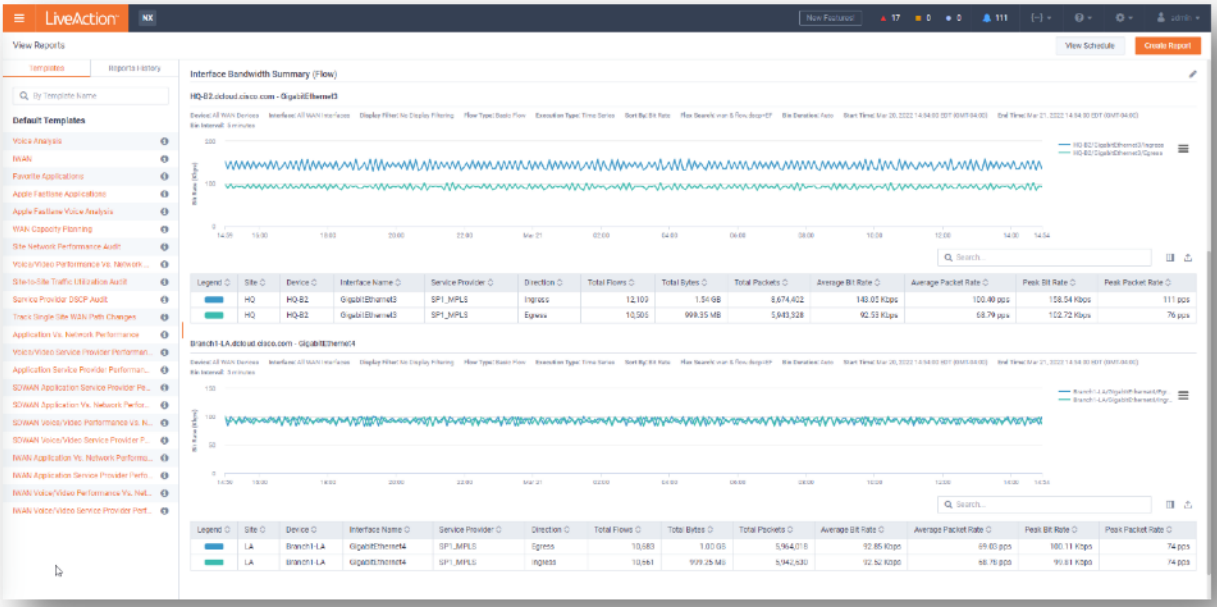


Figure 134

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

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

Lab 5.3: 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:

243. In the **View Reports** page, click on **Create Report** at the top-right of the screen.

244. Click on **Flow**, then **Analysis**, and select **IPs and Ports**.

- Name your report. (**Do not use "&"**)

245. Select **HQ-B2** device.

246. Enter **wan & flow.dscp=EF** in the Flex Search field.

247. Set the **Direction** as **Inbound and Outbound Combined**. the Fields as indicated in the diagram, below.

248. Click Execute Report.

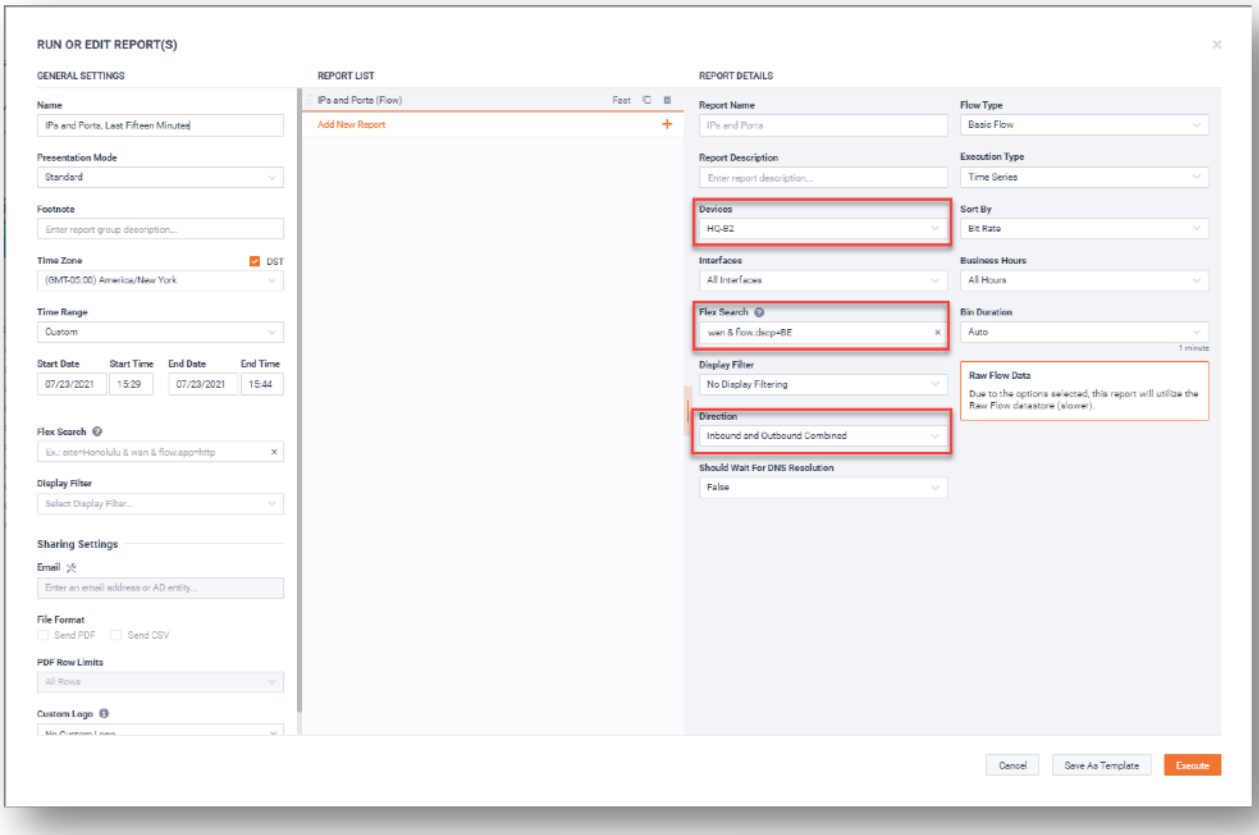


Figure 135

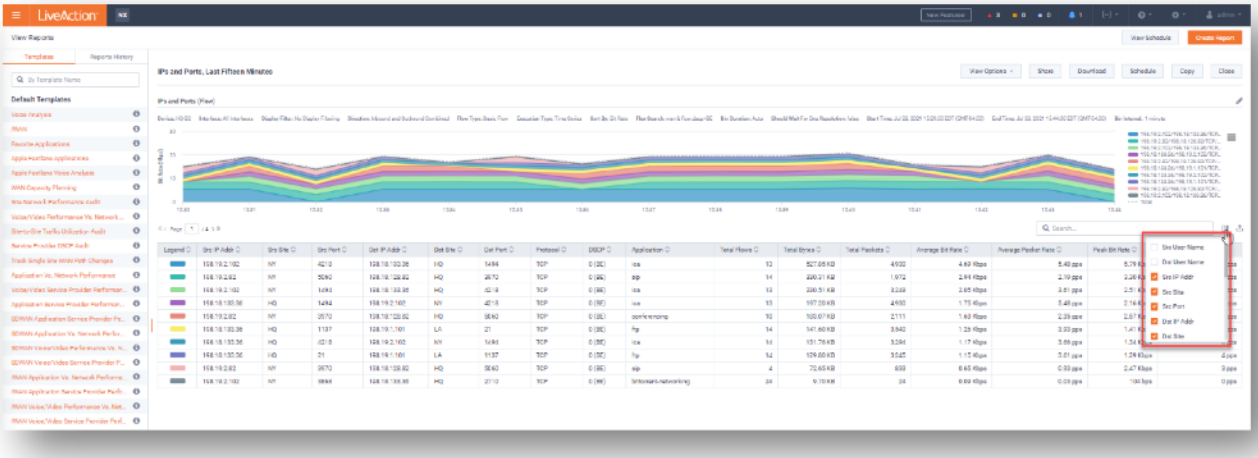


Figure 136

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

Lab 6

Lab 6: Traffic Flows

Lab 6.1: Discover Flows

These Labs uses the WebUI exclusively.

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 **Logical Topology** and **Geo-Topology** Pane.

In this Lab we need to find the address pair which has been generating **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:

249. Select Logical Topology from the Main Menu.

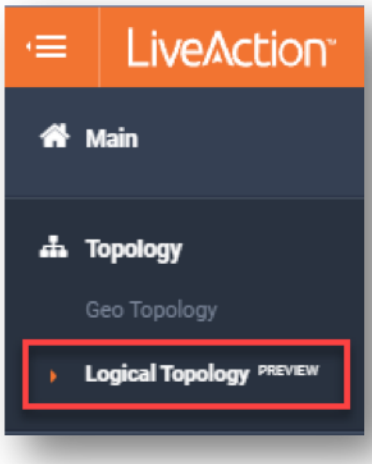


Figure 137

250. You should see all sites in the view, but if **NY** is missing add it to the view.

251. On the left side of the screen, if you see just HQ and LA listed, click the **Edit** button at the top of the panel.

252. Select **NY** so all three sites are checked.

253. Click **Save.**

254. To arrange the entities as you'd like to see them, unlock the view using the **View Lock** button on the right.

Figure 138

255. Click in the Filter Bar.

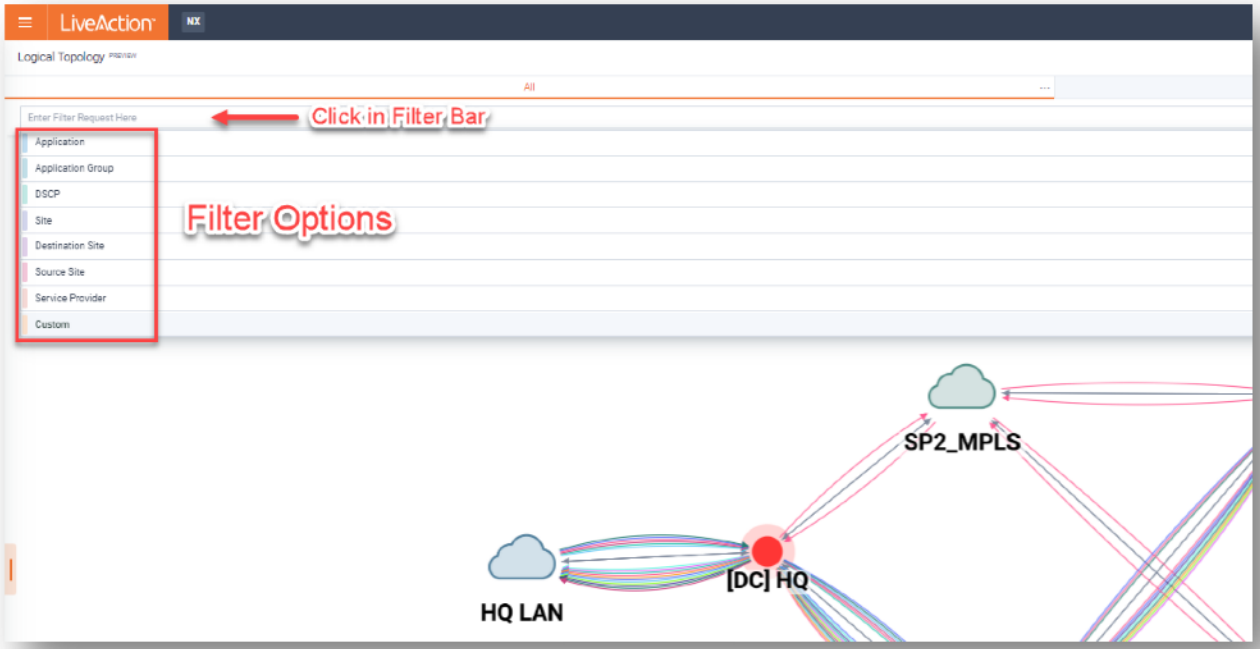


Figure 139

256. For this exercise, we are going to look for **FTP**, which is an application. Click on Application. This will bring up the applications to choose from.

257. You can select the application by scrolling down the list (only the top 50 are shown), or type in the application name. As **FTP** is far down the list, type the letters slowly to see the list change. Click **FTP** when you see it in the list.

258. Click **Apply Filter**.

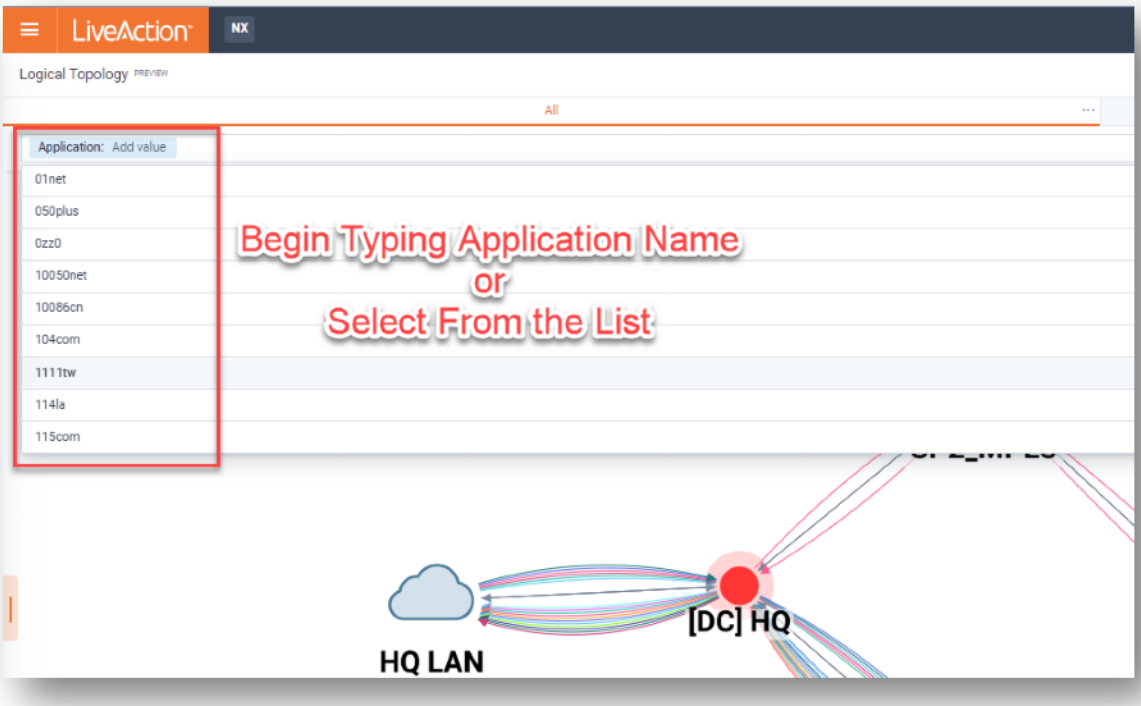


Figure 140

You'll see all FTP traffic flowing across the network, but even referring to the legend at the bottom-left corner may not help identify the **specific** flows!

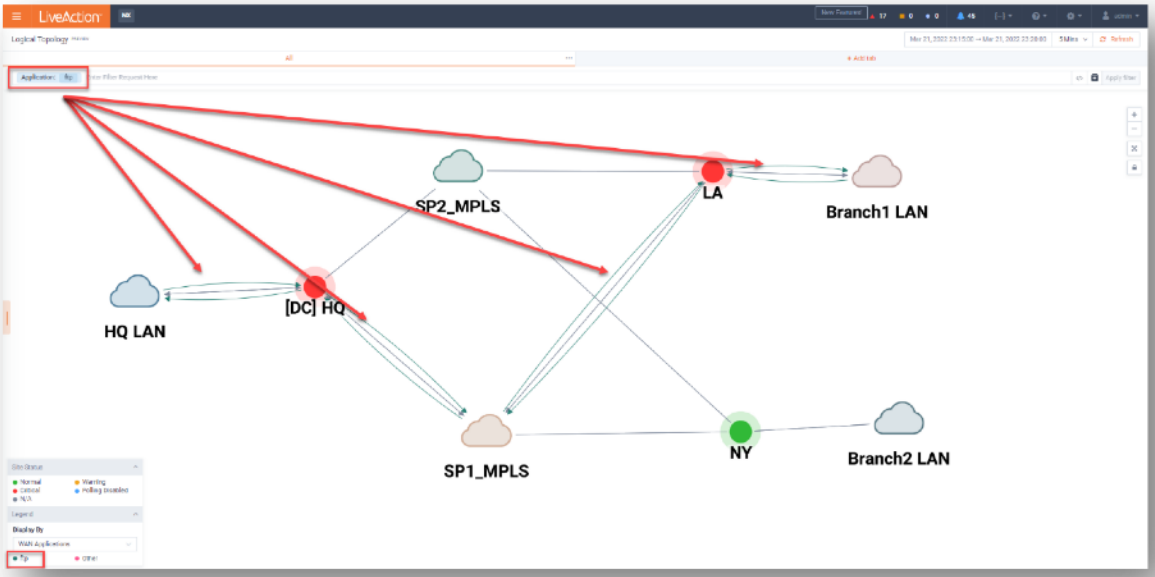


Figure 141

259. To get into the specific flows, down to the IP addresses of source and destination, click on one of the flow lines now visible. This brings up an information window that details the Application Name, the segment and direction of the flows, as well as bytes and bandwidth stats. There is also a **Pivot Point** ( )that will take you to a Report of the flow lines you have selected.

260. Click the **Pivot Point**.

Figure 142

261. You will be taken to the report page where details of the application, including source and destination IP addresses and DSCP Mapping are available.

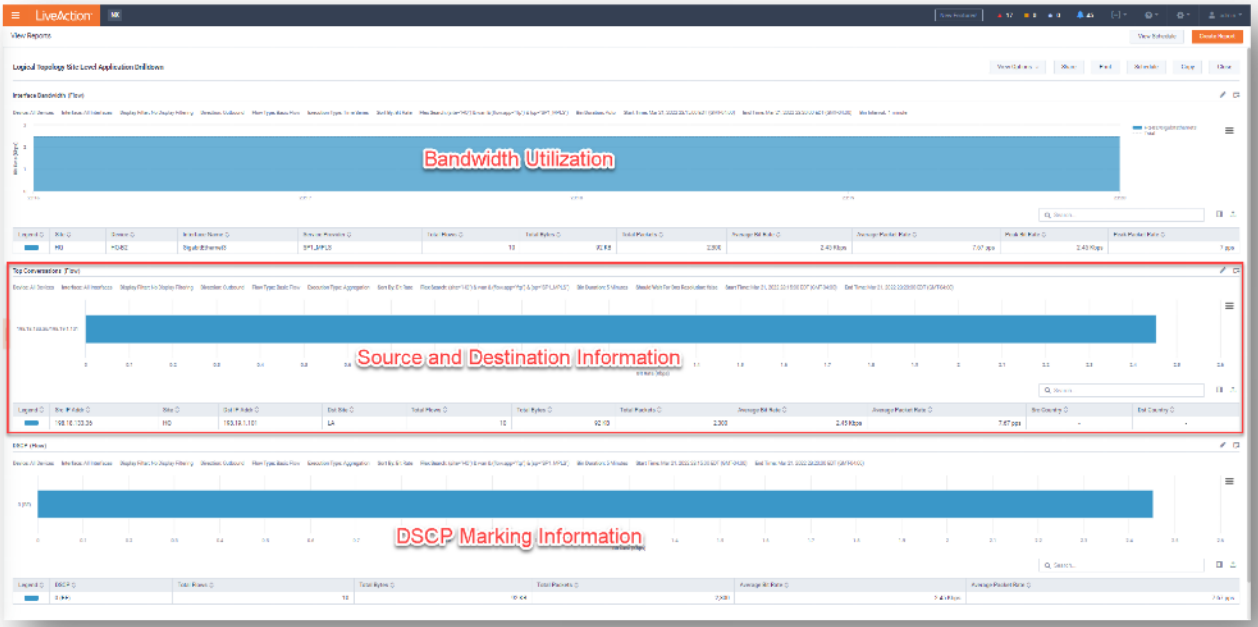


Figure 143

262. You can further drill down into detailed reports by right clicking on various cells. A pop-up box of detailed search filters and drill-downs will appear.

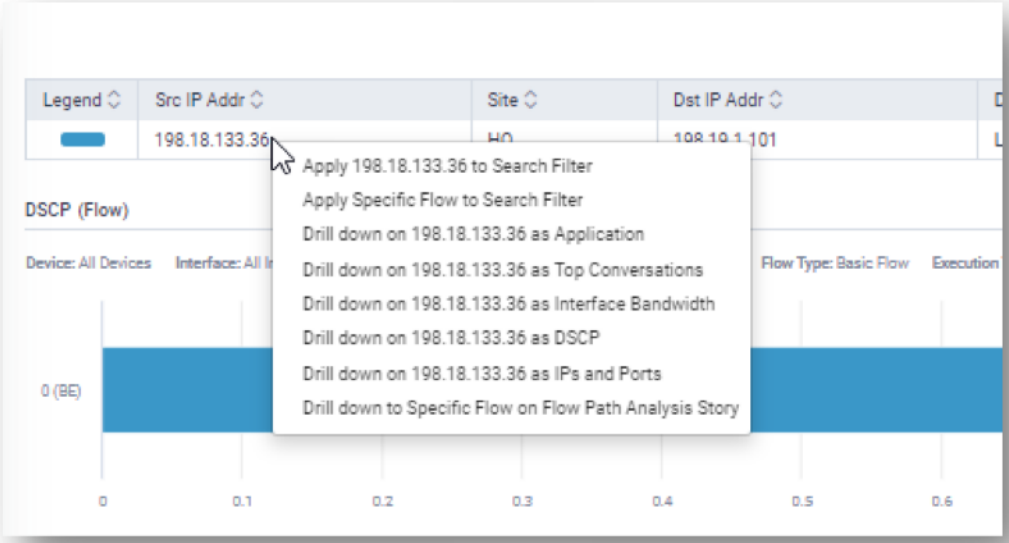


Figure 144

263. In this exercise, right click the SRC IP Address and select **Drill Down on 198.18.133.36 as IPs and Ports**.

264. This will bring up a report of the IP's and Ports being used. This can be further used to drill down to troubleshoot further if needed.

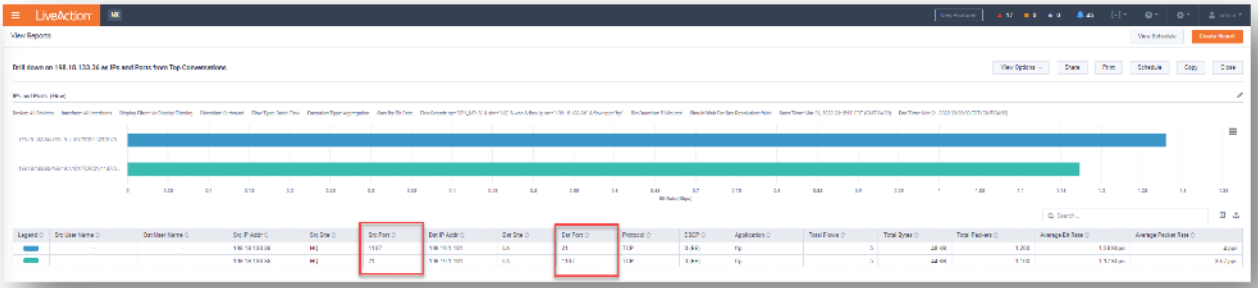


Figure 145

See how easy that was?

Using the **Logical Topology**, what other applications can you identify across our network?

Hint: By selecting **FTP** you are looking at ONLY **FTP**. What do you see if you remove that filter?

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

Lab 6.2: Discover Specific Flows

Note: This exercise will use the Flow Path Analysis story.

265. From the **Main Menu**, click on **Stories**, and then **Flow Path Analysis**.

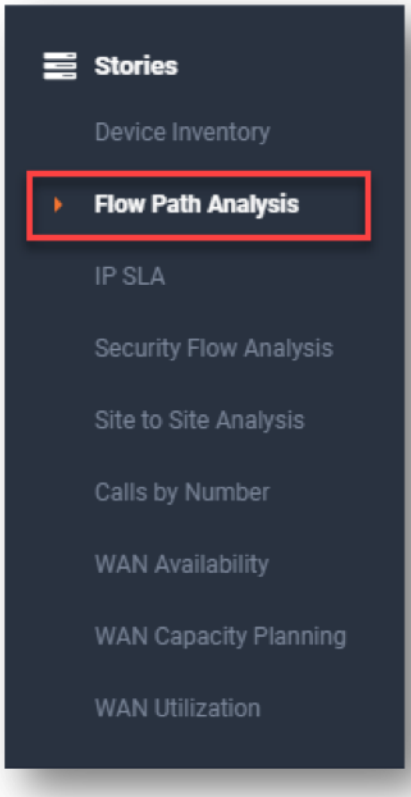
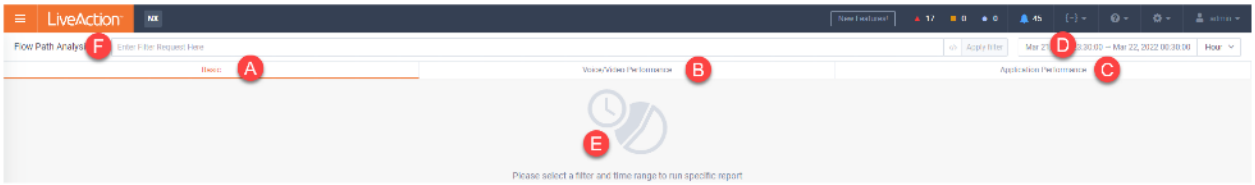


Figure 146

266. In the Flow Path Analysis home page, you are offered three Tabs: **Basic** (A), **Voice/Video Performance** (B), and **Application Performance** (C). Voice/Video Performance provides specific information on RTP/streaming media, such as packet loss and jitter. **Application Performance** provides information on bandwidth use, response time and latency for TCP data flows. For this exercise we will use the basic tab.



267. Note also that you can look back in time by adjusting the date/time (D) and duration of view in the upper right corner. The display (E) remains clear until you provide filter parameters in the **Page Filter** (F).

268. Click in the **Page Filter** and from the drop down, scroll and find **Src IP**, and click it. Note the other options here as there are many and can be used according to your need at any time. In the **Src IP** field type the IP address of the PC in Los Angeles **198.19.1.101**.

269. In the screen that populates you will see all traffic that originated at the Los Angeles PC (198.19.1.101), regardless of protocol, application, DSCP marking, or destination. You can add elements to the filter bar to refine your search.

270.

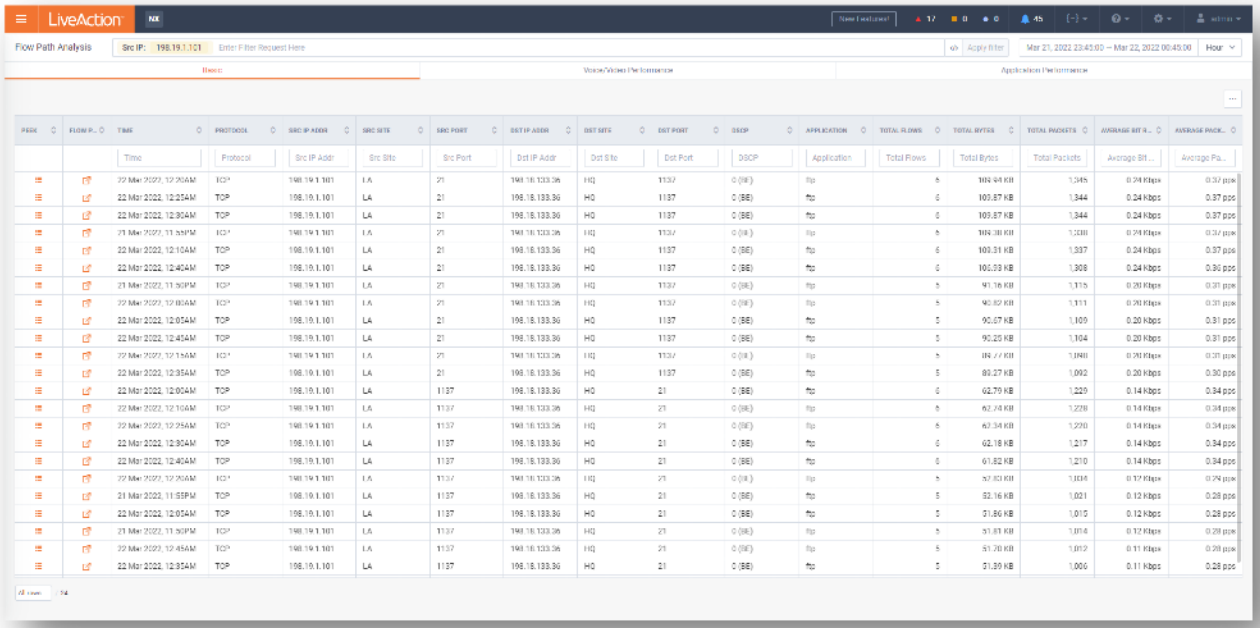


Figure 147

271. You can use column filters to further clarify/find the flow you are interested in. In our exercise the flows are very consistent, so click the **Flow Path Analysis** pivot point of the first flow on the list

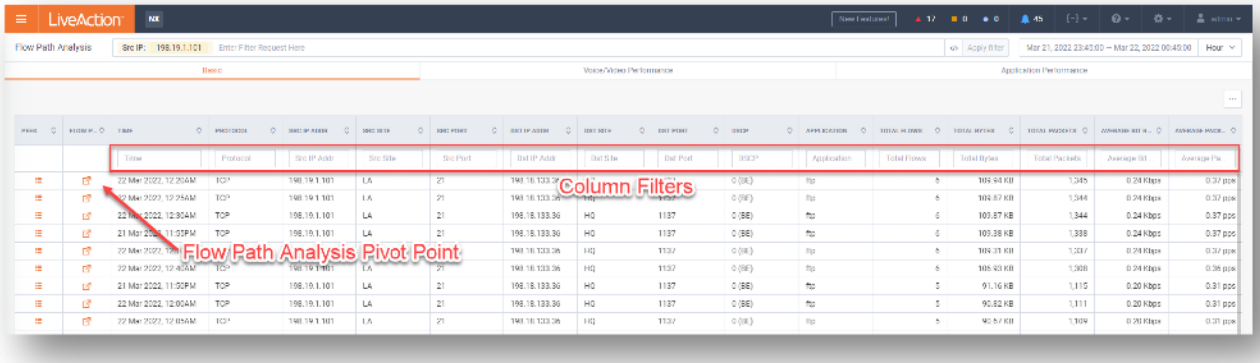


Figure 148

In this exercise you have located many flows relevant to a specific parameter – Source IP Address, 198.19.1.101. You can use this method to find flows relevant to other parameters even combining different parameters to

Lab 6.3: Examine Specific Traffic

Let's look at how to find a specific flow amongst the data on the network. Let's see how the **Voice Signaling (SIP)** traffic is performing in our NY Branch.

272. Navigate to the **Flow Path Analysis** page and clear out any page filters that may be left there. Make sure you are looking at the **Basic** tab too.

273. Let's now add site **NY**, and the Voice Signaling application, **SIP**.

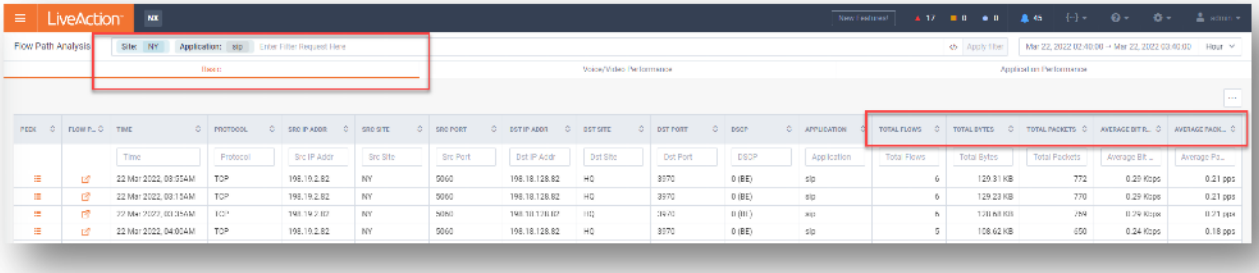


Figure 149

274. You'll see that for each identified flow the information provided relates to basic information – source/destination information, as well as DSCP/Application, network utilization. But we want to see more to understand the performance.

275. Now click on the **Application Performance** tab.

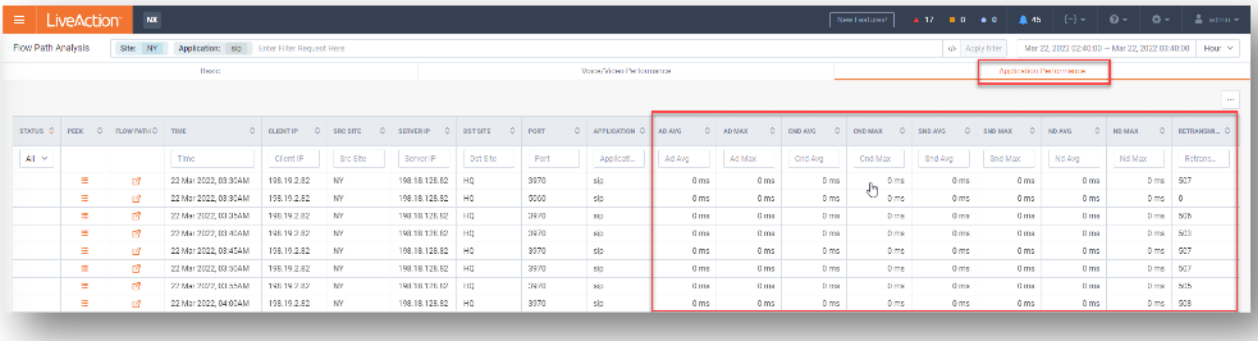


Figure 150

276. In this view you will see more detailed information related to TCP performance – including **Application Delay** (AD), **Network Delay** (ND), as well as retransmissions.

277. You can sort the results by clicking on a column heading. Each subsequent click on the same column heading reveres the sort order of the sort (smallest to largest vs largest to smallest)

278. You can also filter the table further by entering values in the column filters underneath the headings. This can be faster and more easily reversible than adding to the page filter at the top.

279. While we now have details on many flows that fit the parameters we searched for, and can single out subsets, we still want to drill-down on a specific flow to identify potential areas of trouble.

280. Click on the **Flow Path Analysis** pivot point on one of the flows.

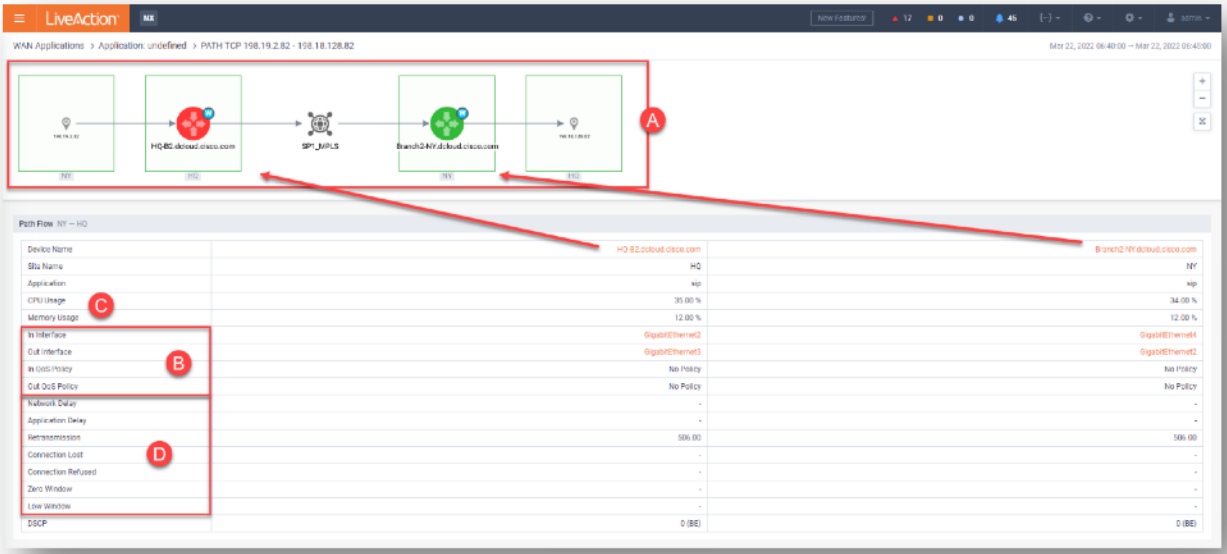


Figure 151

281. In the table that appears you will see the path through the network that this flow takes (A). You will see ingress and egress ports on each device through which it traverses, along with any applied In or Out Policies that are applied (B). The CPU and memory usage of the devices is shown for reference to aid in troubleshooting (C).

282. As we arrived at this page from the Application Performance overview, you will also see the TCP statistics that were seen at each device in the flow (D). This can be very valuable information when troubleshooting.

Almost too easy, wasn't it? What other information can you gather on other applications through the network? Try gathering the following information on other applications.

Bittorrent-Networking

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Bittorrent

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

Src Site_____ Src IP_____ Dst Site_____ Dst IP_____ Port_____

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

Lab 6.4: Troubleshooting Issues

Scenario: Users in the Marketing Department at our New York site have been complaining that their workstations seem to be “slowing down” numerous times a day. This only happens when they are connected to the intranet. A pattern is developing where this happens approximately every 5 minutes. We need to investigate.

The user is on 198.19.2.128, which is in the New York Office. First, let’s see what traffic is hitting our user. We will use the Analysis report that shows IP and Applications.

283. Go to Reports and create a new report.

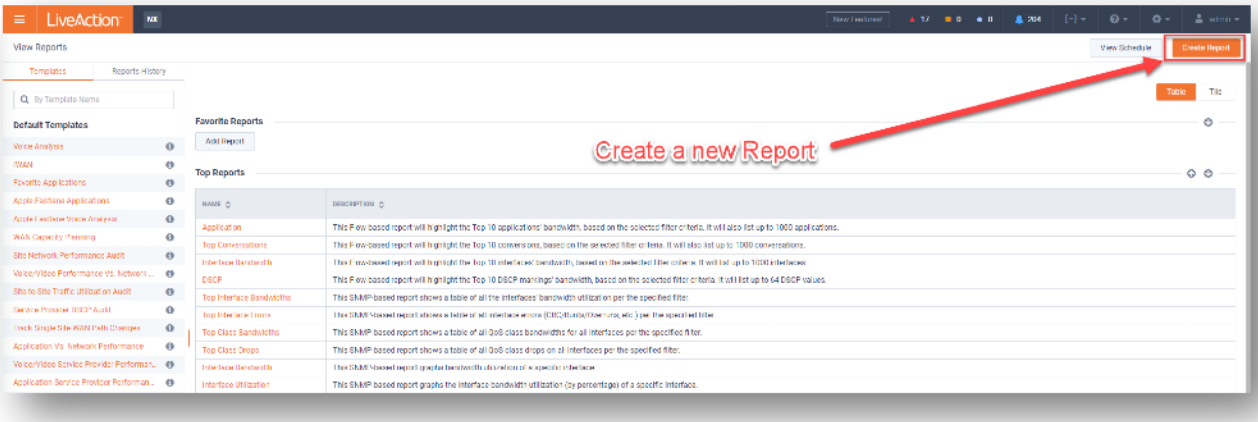


Figure 152

284. In the **Report Details** section (A), type **IP**, and click the **IP and Application** report in the **Analysis** section (B).

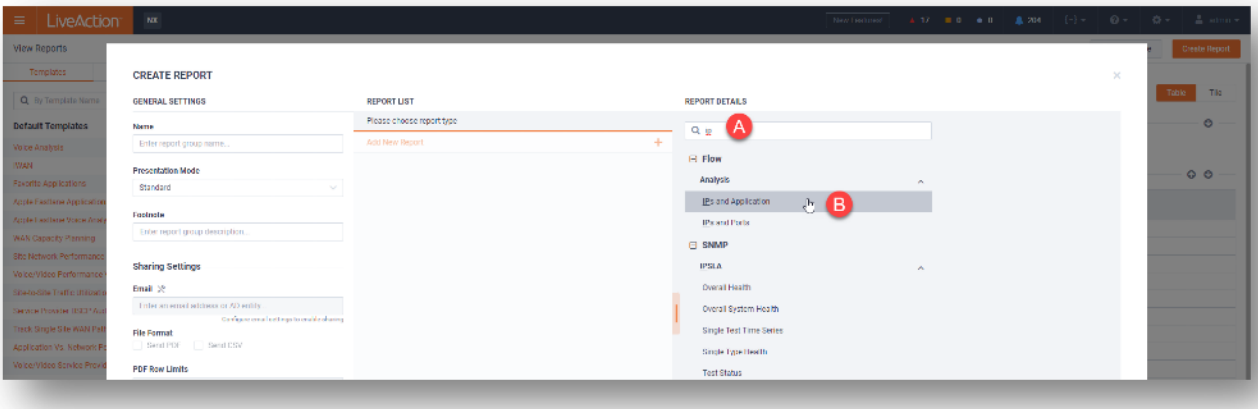


Figure 153

285. There are three key parameters that we want to review to give us the best view of the problem. These are characterized by:

- When are we looking? (Recently, and for 1 hour) **(1)**
- What are we looking for? (IP addresses and Applications) **(2)**
- Where are we looking? (NY site) **(3)**

286. The problem occurs approximately every 5 minutes. As we want to view all the traffic hitting 198.19.2.128, we will use Flex Search to focus on that destination IP address.

- flow.ip.dst=198.19.2.128 **(4)**

Flex Search can be entered in the Report Details section, or in the General Settings section. When used in General Settings for with a Report Template (multiple reports in one) the Flex Search affects ALL reports equally.

---

287. The traffic we are looking for happens every 5 minutes (approx.). It helps if you have the **No Display Filtering (5)** and **Flow Filter** set to **Basic Flow (6)**.

288. To see as much resolution on this time frame as possible we will force the **Bin Duration** (granularity of data) to 1 minute (7).

Beware: Forcing the Bin Duration to 1 minute for large time ranges can cause report slowness. We should be OK in this case as our search is quite simple.

---

289. Click **Execute**.

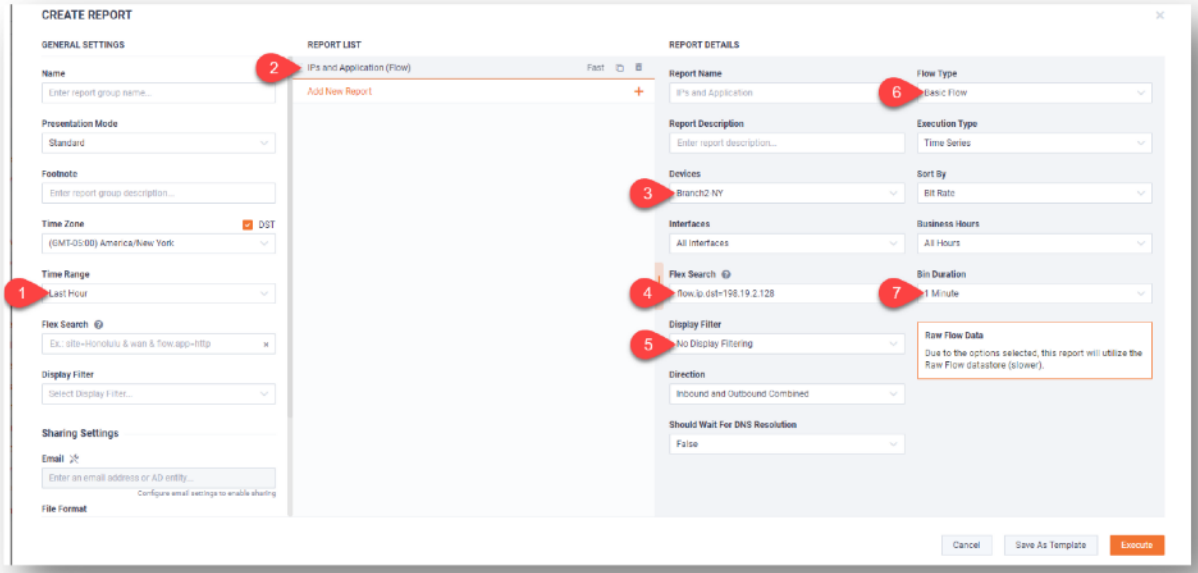


Figure 154

290. The report will provide a view of traffic with a destination IP address of 198.19.2.128. As you should see, there are clear peaks of data coming in, with TWO bursts separated by 2 minutes, followed by a 5-minute pause (8).

291. If you look in the table below you will see all the traffic is coming from 198.18.133.36 (9) and that it is sending a variety of applications (10).

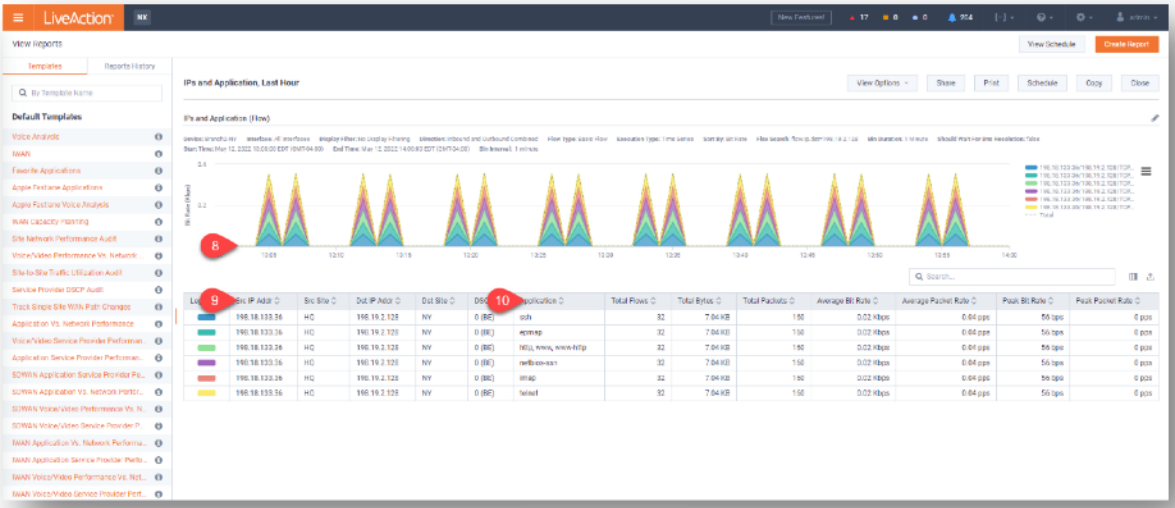


Figure 155

292. It would be recommended to check out the 198.18.133.36 device (the Workstation on HQ) and determine if it is infected with a virus looking for vulnerabilities.

Lab 7

Lab 7: Custom Filters

Lab 7.1: Creating Custom Display Filters

This Lab uses the Engineering Console.

Customizing LiveNX makes it more relevant. Creating and using **Custom Display Filters** will help you in your day-to-day use of LiveNX. Custom Display Filters allow you to quickly see a specific view of your network traffic as defined by the filter which includes Application (or group), IP Addresses (src, dst, either, or both), DSCP settings, Site (src, dst, either, or both), or Service Provider. Custom applications can also be used to define a Display Filter.

It is recommended that you create custom filters for common or frequently used views of your network to help monitor or troubleshoot.

In this lab you'll create a custom filter based-upon 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:

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

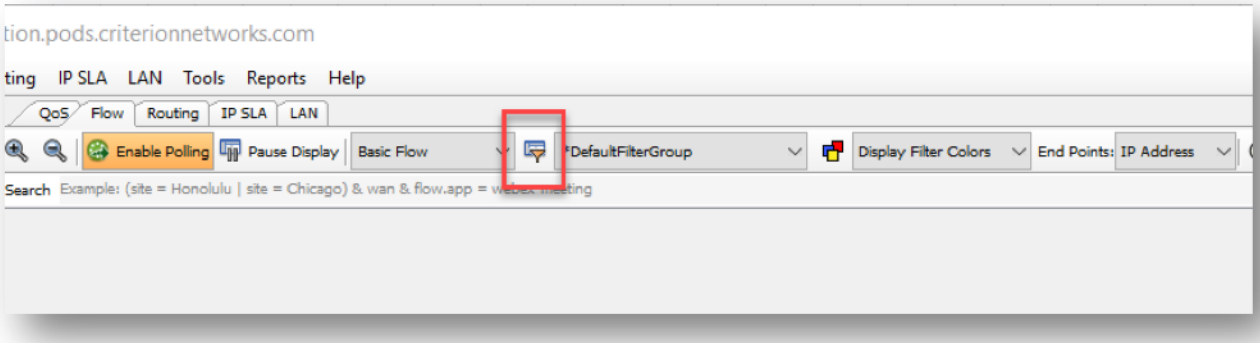


Figure 156

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

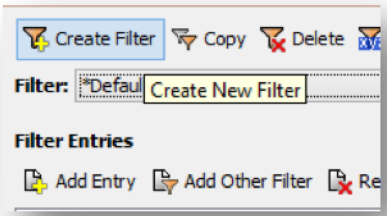


Figure 157

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

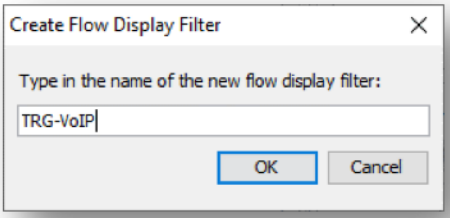


Figure 158

296. Give the label color a meaningful name – in this case **SIP**.

297. 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.

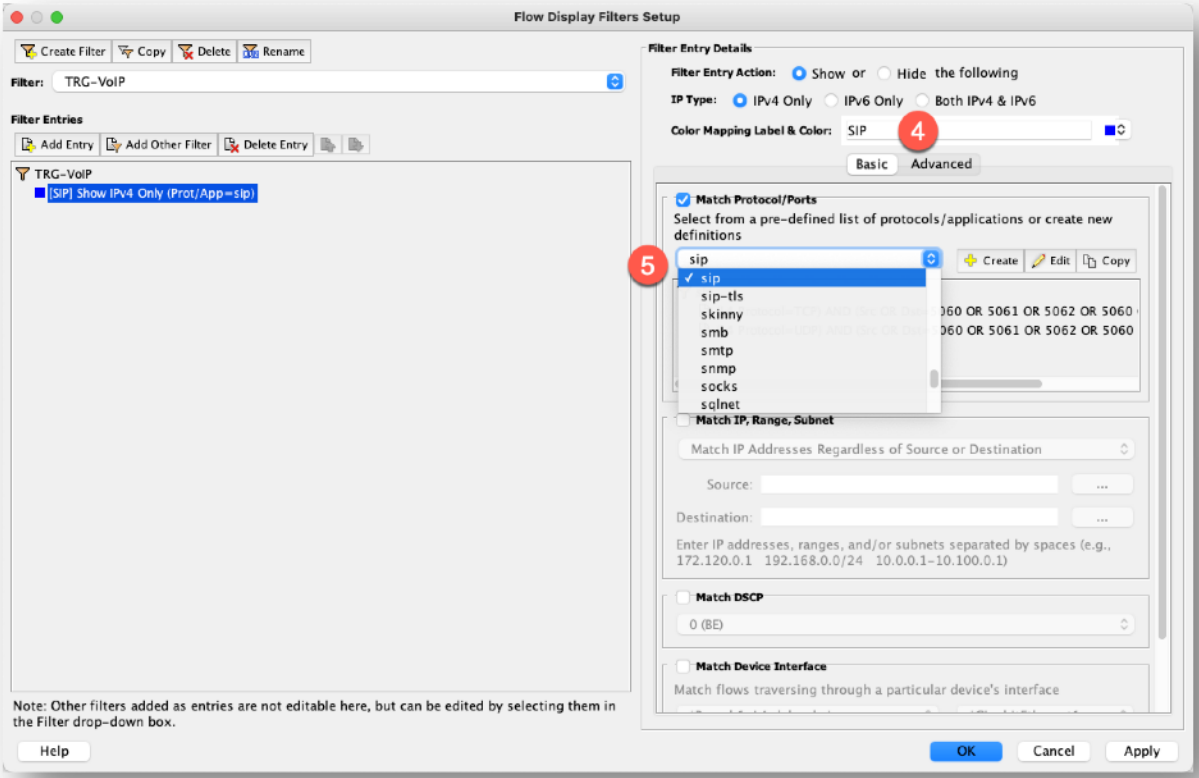


Figure 159

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

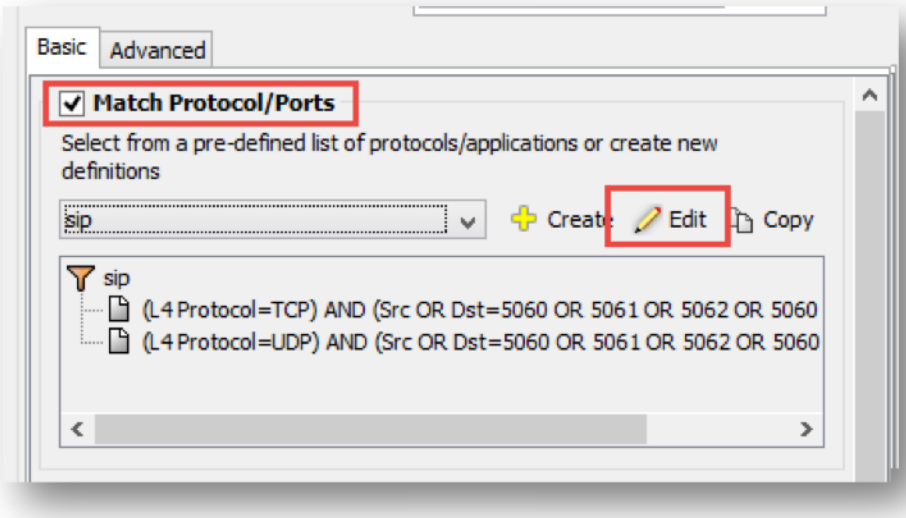


Figure 160

299. Edit both entries, for TCP and UDP, to match the ports provided.

300. Select to "**Match Ports Regardless of Source and Destination**" for both TCP and UDP.

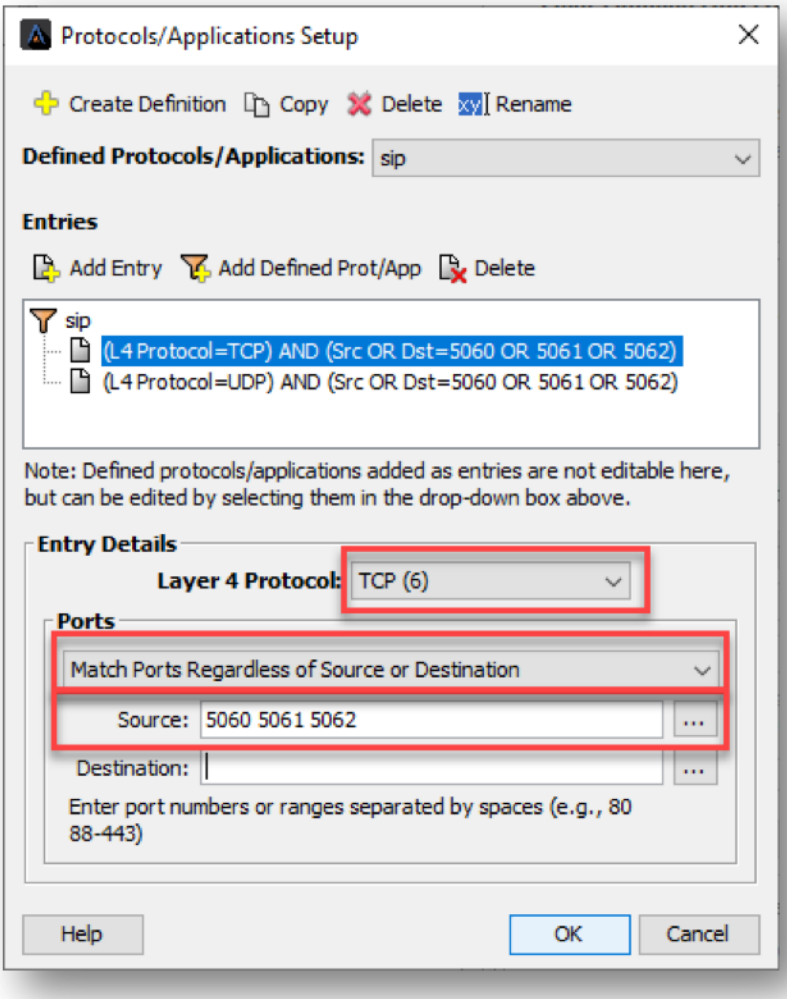


Figure 161

301. Click **OK**.

302. Then click **Apply**.

303. Create a new filter entry by clicking **Add Entry** under **Filter Entries**.

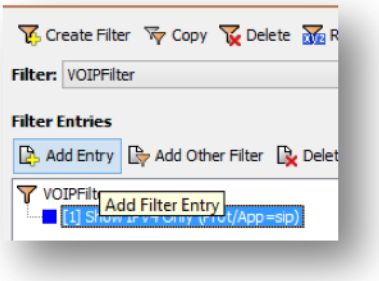


Figure 162

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

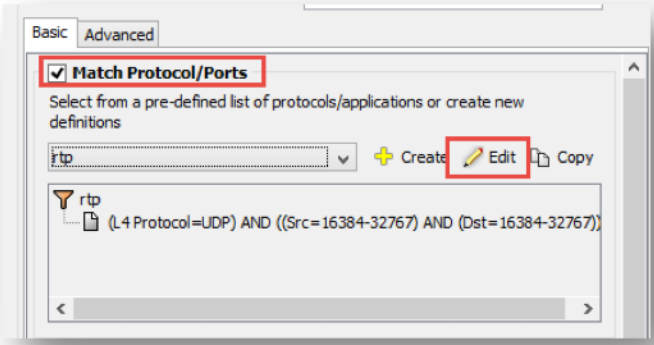


Figure 163

305. Name the color label again, this time **RTP**.

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

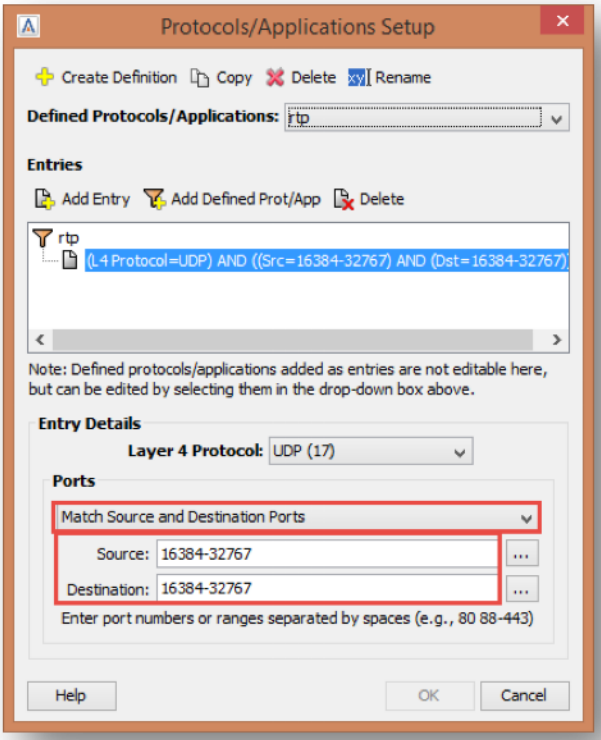


Figure 164

307. Click **OK.**

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

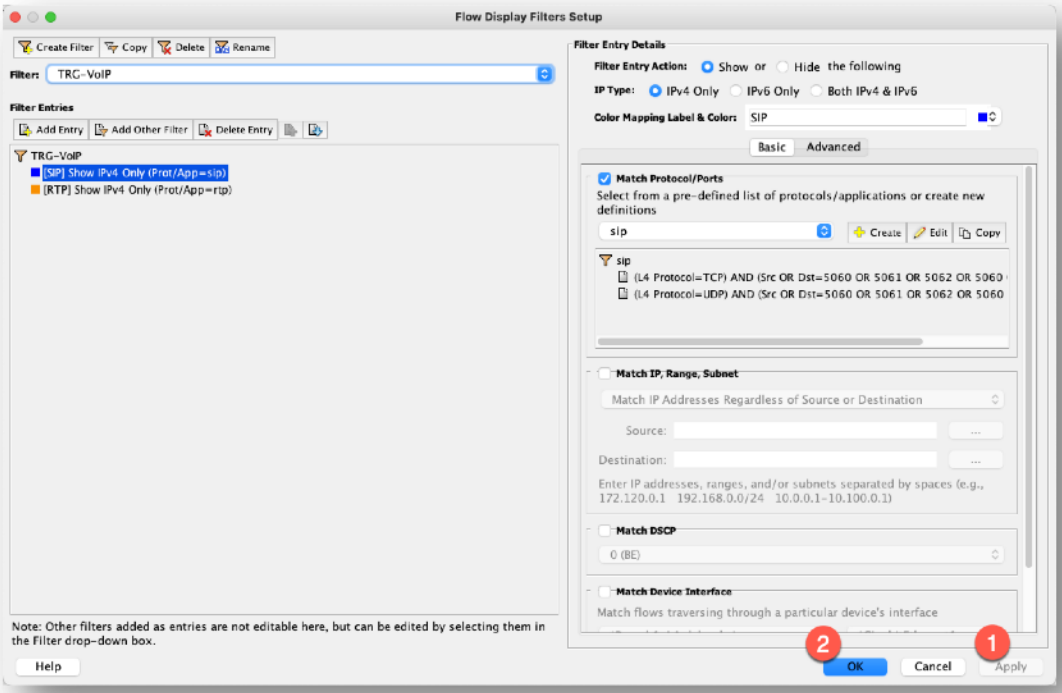


Figure 165

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

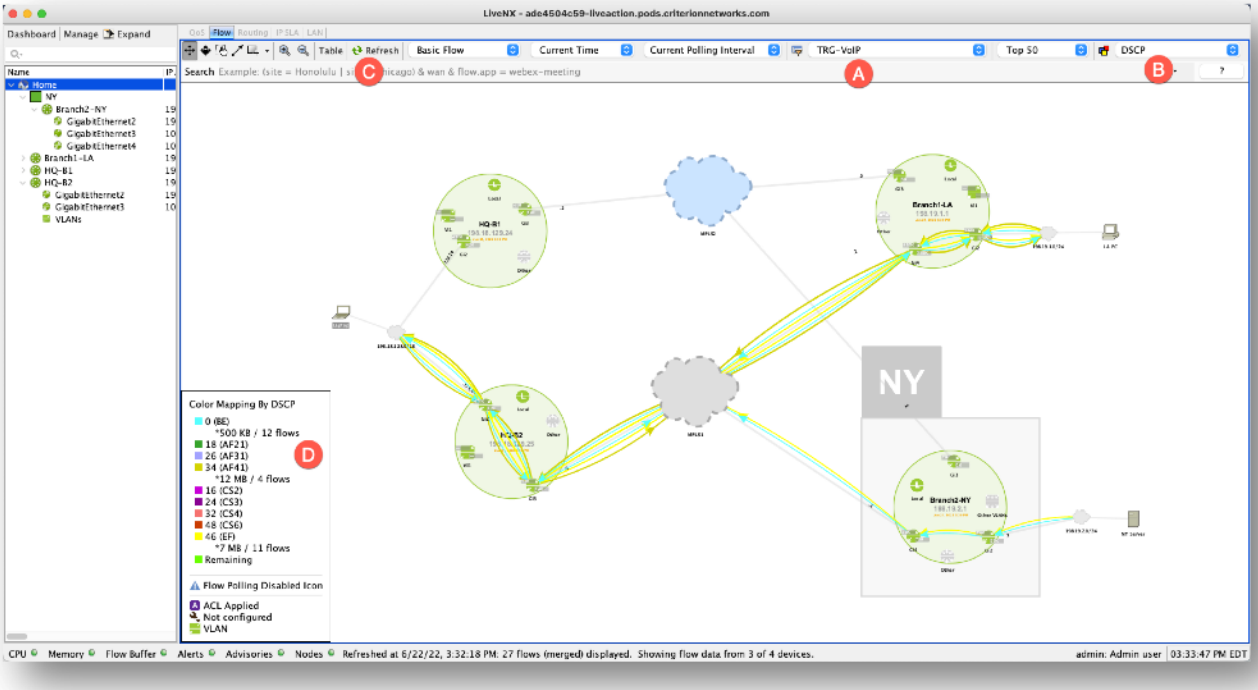


Figure 166

All the traffic should be Voice Traffic. Do you notice any traffic that is being treated incorrectly? Look for traffic marked with DSCP 0 (BE).

Lab 7.2: Creating Custom Applications

This Lab uses the WebUI.

Many times, either the network devices are not able to provide application recognition, or the application definitions provided by NetFlow don't always match the needs of your monitoring and troubleshooting. For this reason, LiveNX allows you to define **Custom Applications** and **Custom Application Groups**. Being able to create customized applications and groups provides for much clearer segmentation of traffic flows, and more powerful insights without manually filtering. **Custom Applications** and **Application Groups** can be applied in many places in LiveNX and are useful to provide flexibility and precision when monitoring and troubleshooting. Let's look at **Custom Applications** and **Custom Application Groups** and how to create them. This is a way of giving "unknown" applications a name.

310. To create a Custom Application, go to Main Menu > Configure > Application Management.

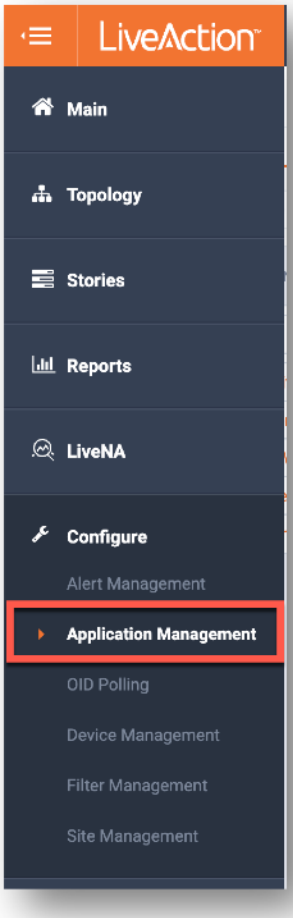


Figure 167

The Application management screen has three major areas. **Custom Applications** (1) where you can configure custom applications, **Application Groups** (2) where you configure multiple applications into a group, and the option to **View WAN Applications** (3).

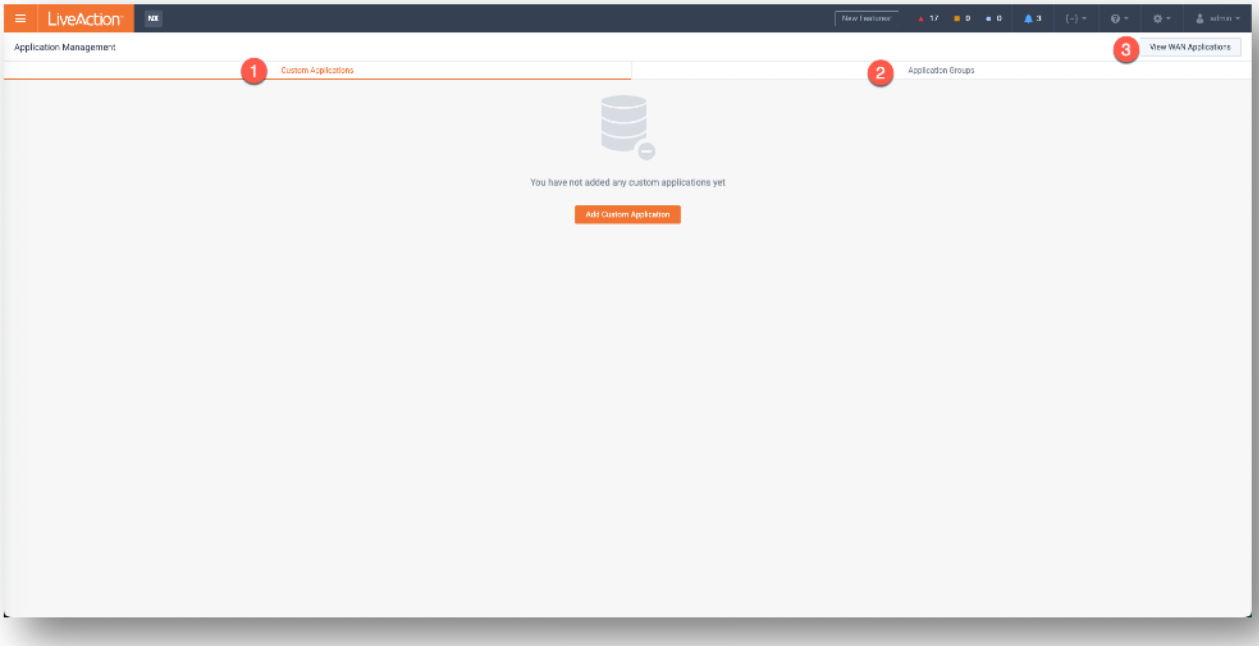


Figure 168

311. Click on **View WAN Applications** to list the applications that LiveNX is seeing in the network.

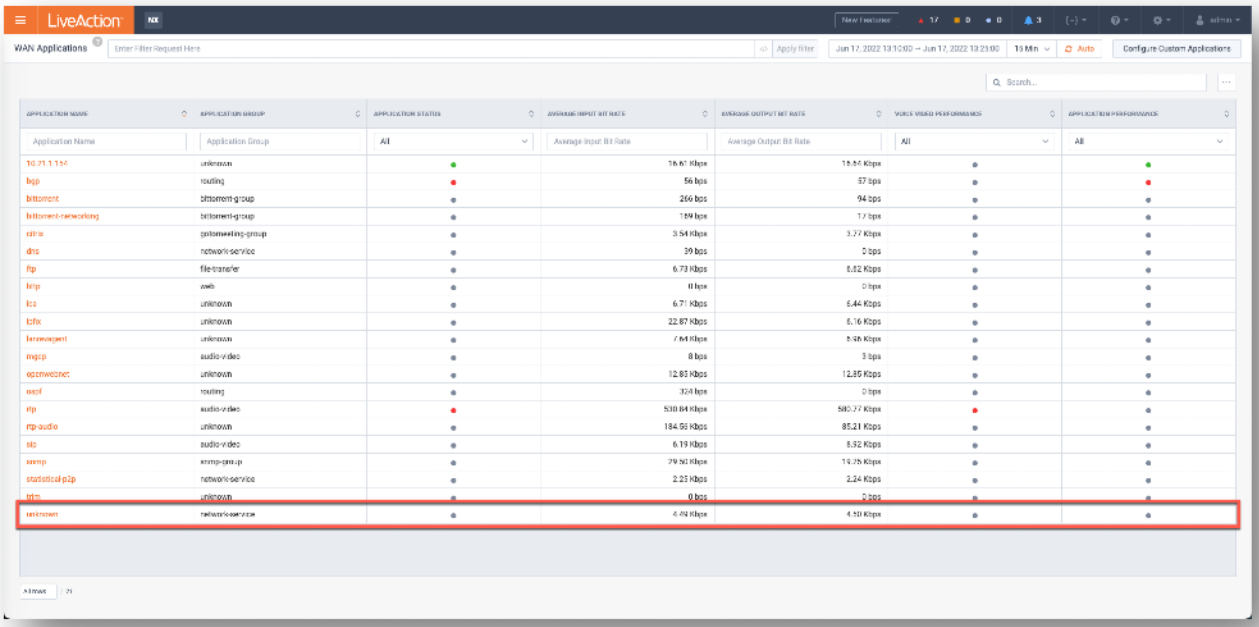


Figure 169

Here we reveal an application called **Unknown** running on our network. Let's give it a real name; but to do that, we must know exactly what we are naming so we don't accidentally name anything else.

312. Let's run a report to find out more about it. Go to **View Reports** and find **IPs and Ports** in the search bar.

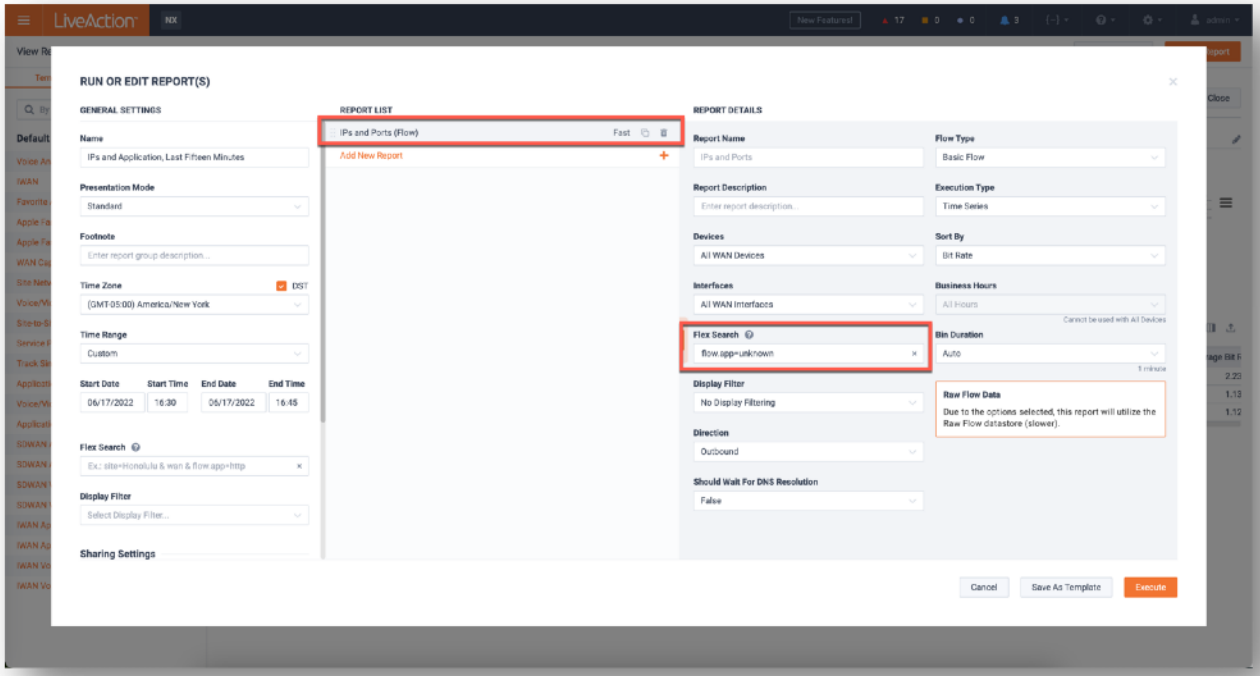


Figure 170

313. In the Flex Search field lets specify the application **unknown** using the flex search term:
   - flow.app=unknown
   - Click **Execute**.

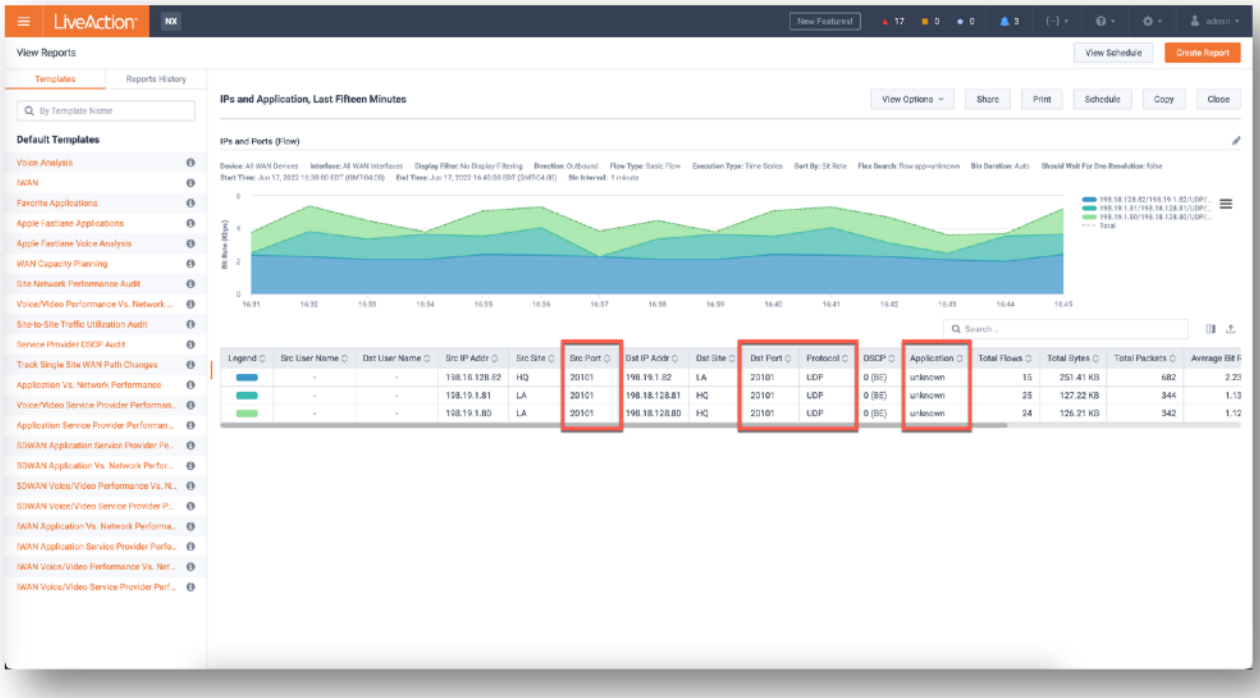


Figure 171

In the resulting report, you should see information regarding the application **unknown** listed.

314. We can see that this application has specific attributes that help define it

The information regarding application **unknown** is:
Protocol: UDP
Port: 20201

Now we know how to define **unknown**, we can ask LiveNX to give it a more useful name.

315. Jump back to the **Application Management** page in **Configure**.

316. In **Custom Application**, click **Add Custom Application**.

317. A pop-up window will appear asking for the parameters that are needed to define the custom application.

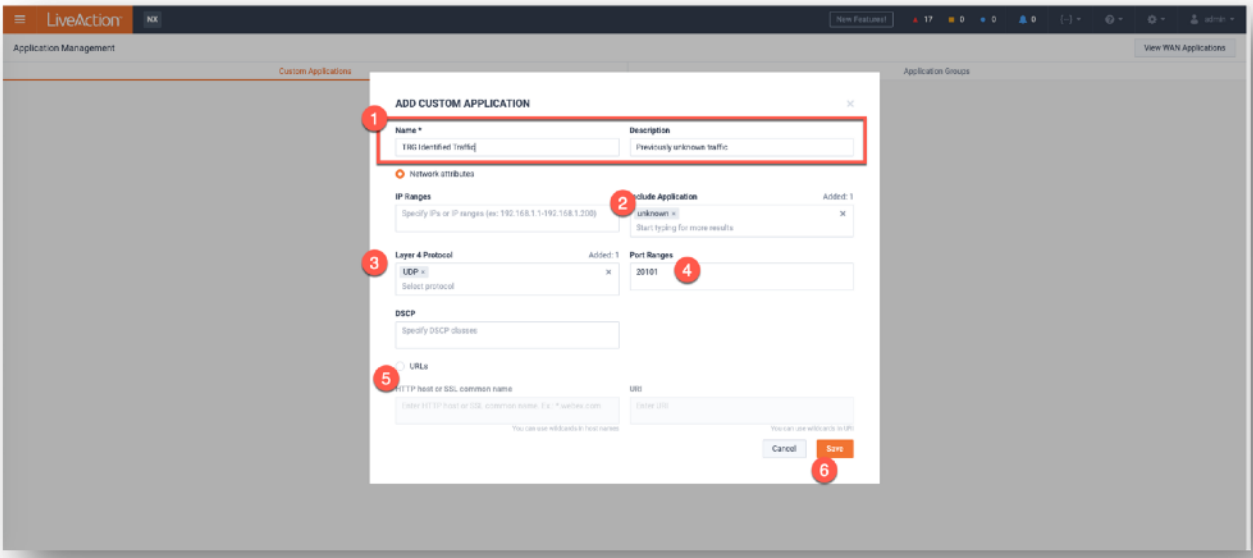


Figure 172

318. Give the application a new name and description (1) – usually something meaningful but you can get creative here.

319. Complete fields as necessary. The only mandatory field is the **Name** field. In our example you should focus on **Include Application** (2), **Layer 4 Protocol** (3), and **Port Ranges** (4).

320. Note that you can define a custom application by URL or URI strings (5).

321. Click **Save** (6) when you have completed the above steps.

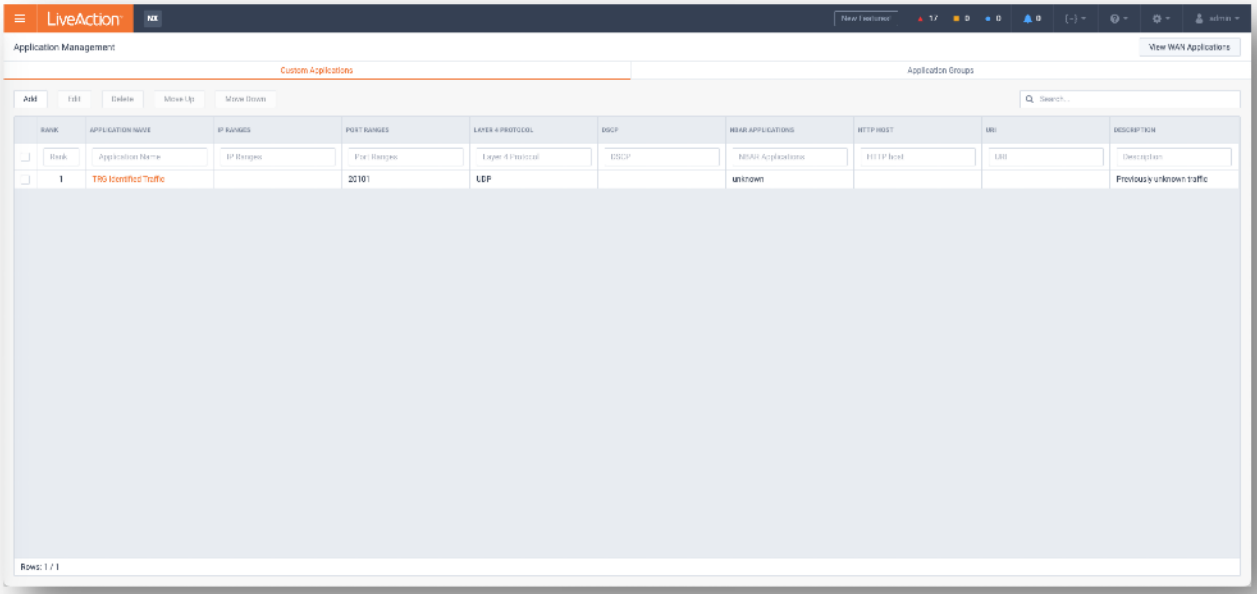


Figure 173

322. Looking at the **Geo-Topology** to verify the custom application will allow you to see the previously **unknown** traffic as the name you selected for it.

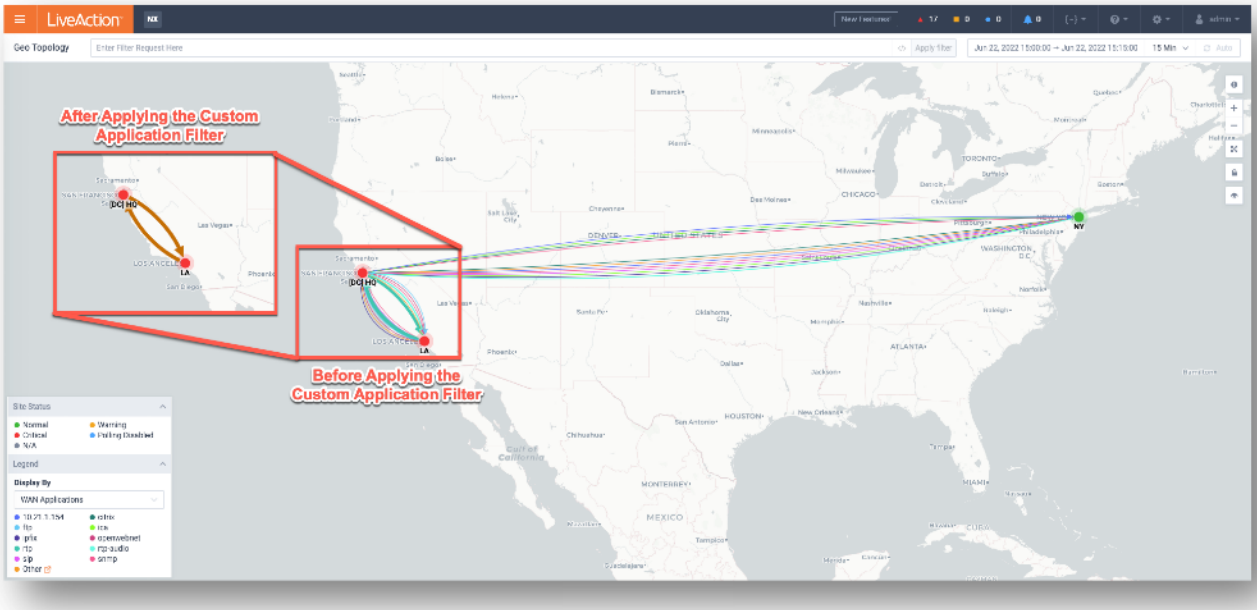


Figure 174

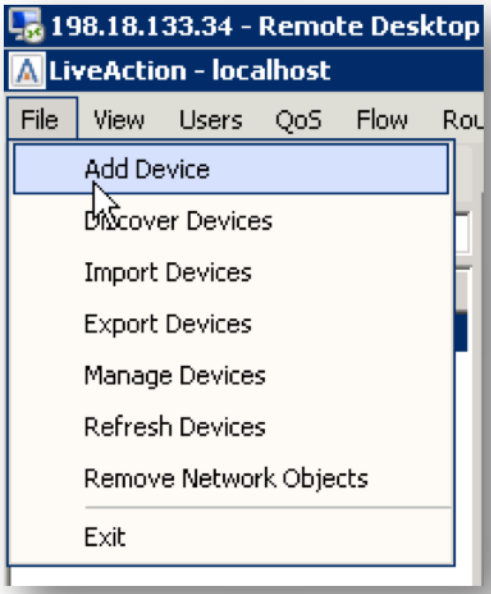
Appendices

Appendix 1: Add Device

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

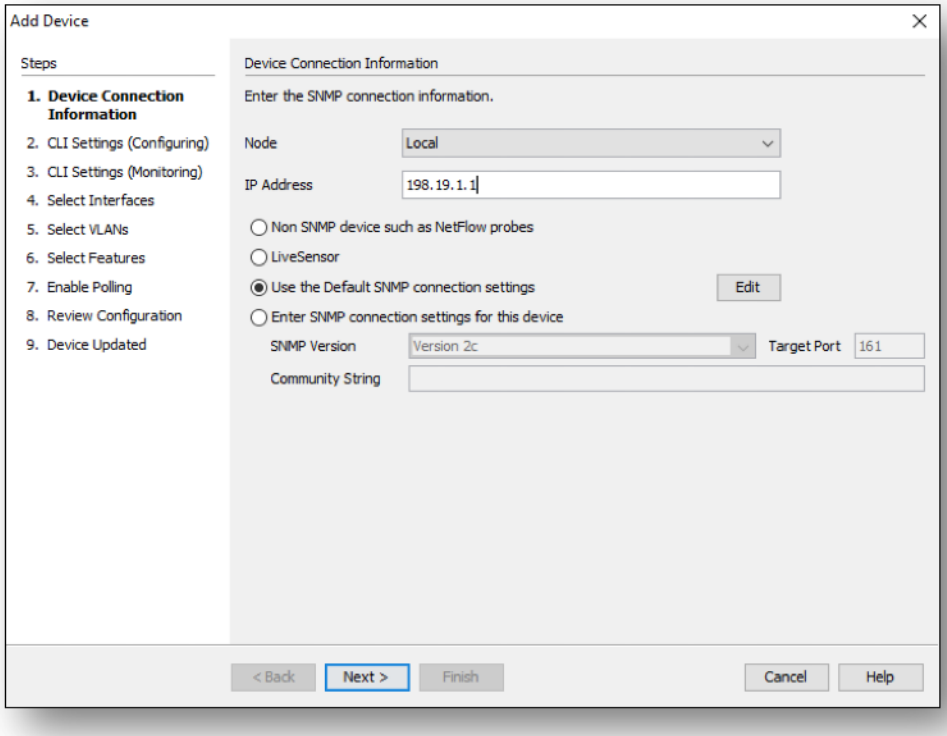
Lab Steps:

1. Select File, **Add Device**



A 1

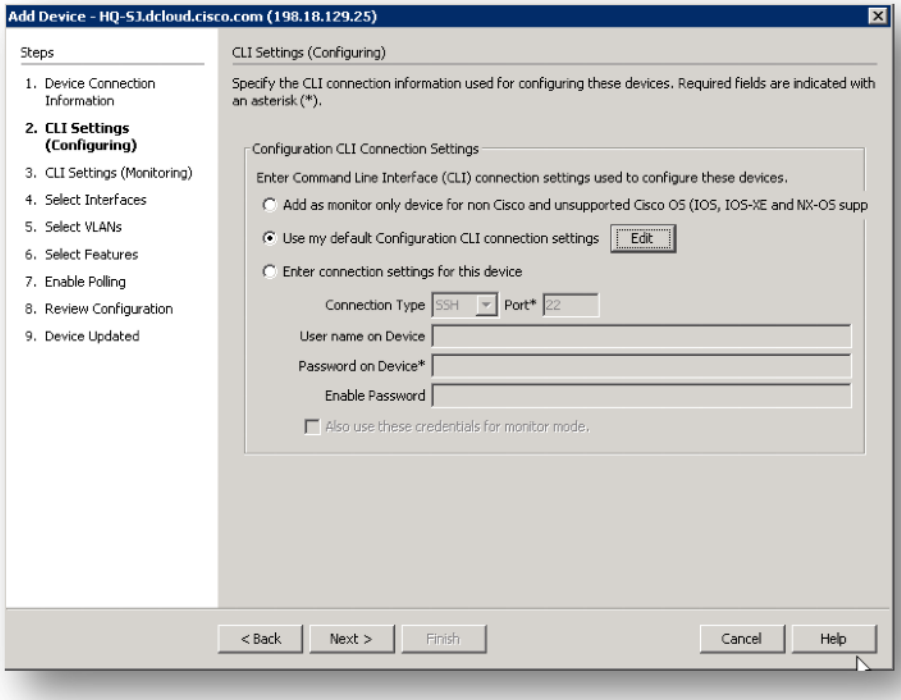
2. Enter 198.19.1.1 in the IP Address field.
3. Select “Use the Default SNMP connection settings”.



A 2

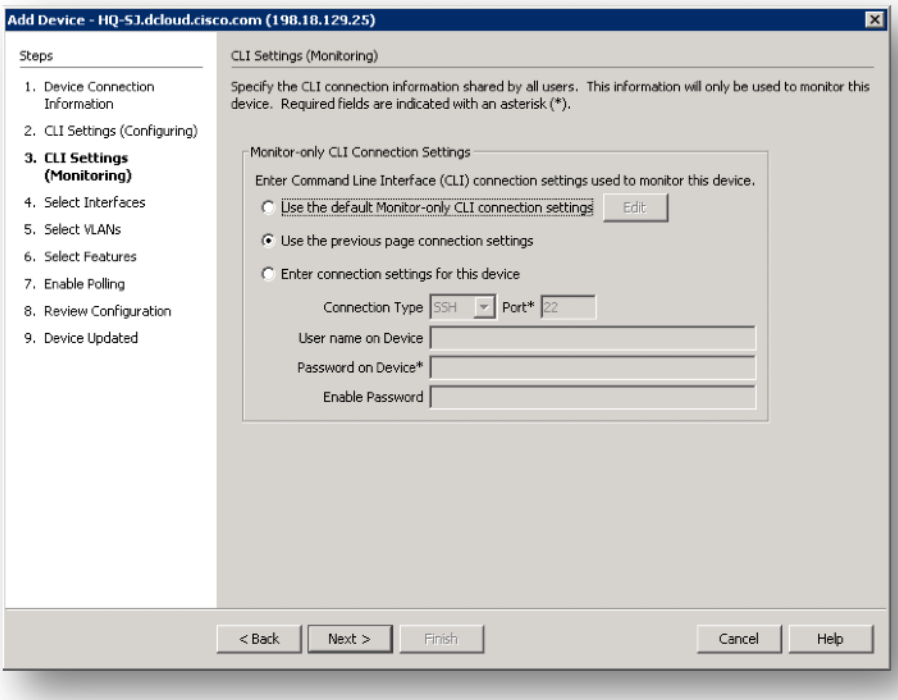
4. Click Next.

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



A 3

6. Click Next.

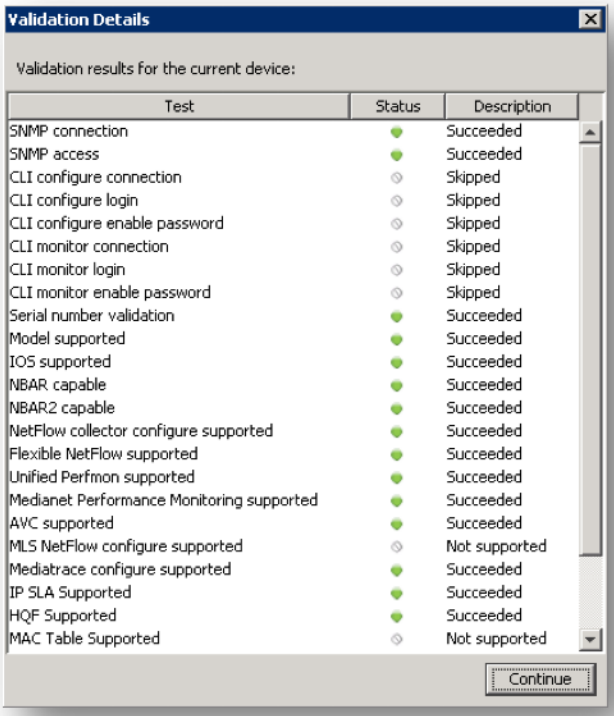


A 4

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

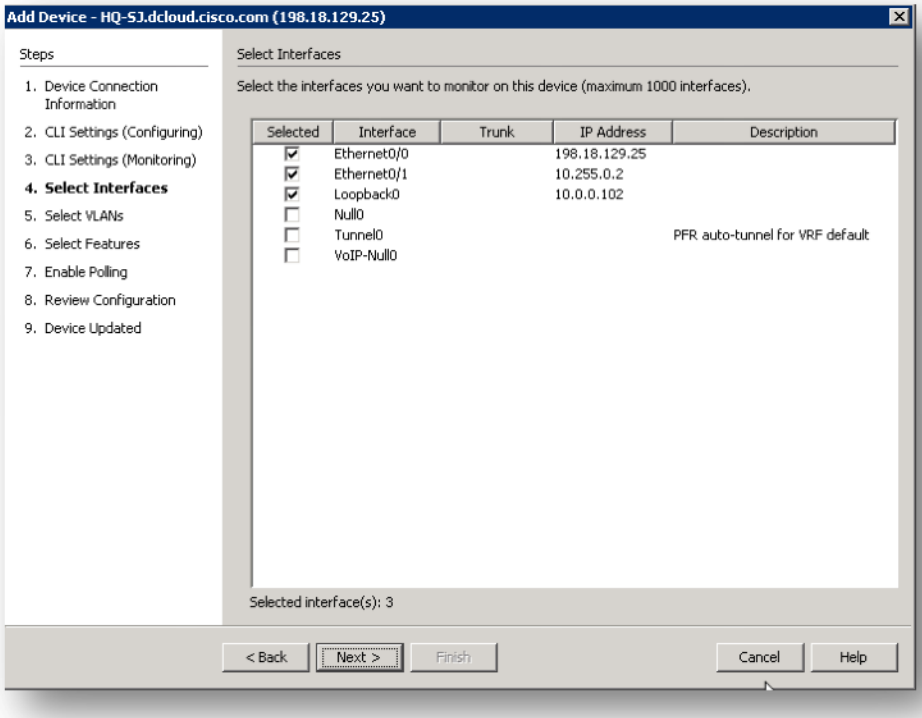
You can verify what capabilities LiveAction is able to interact with the device.

9. Click Continue.



A 5

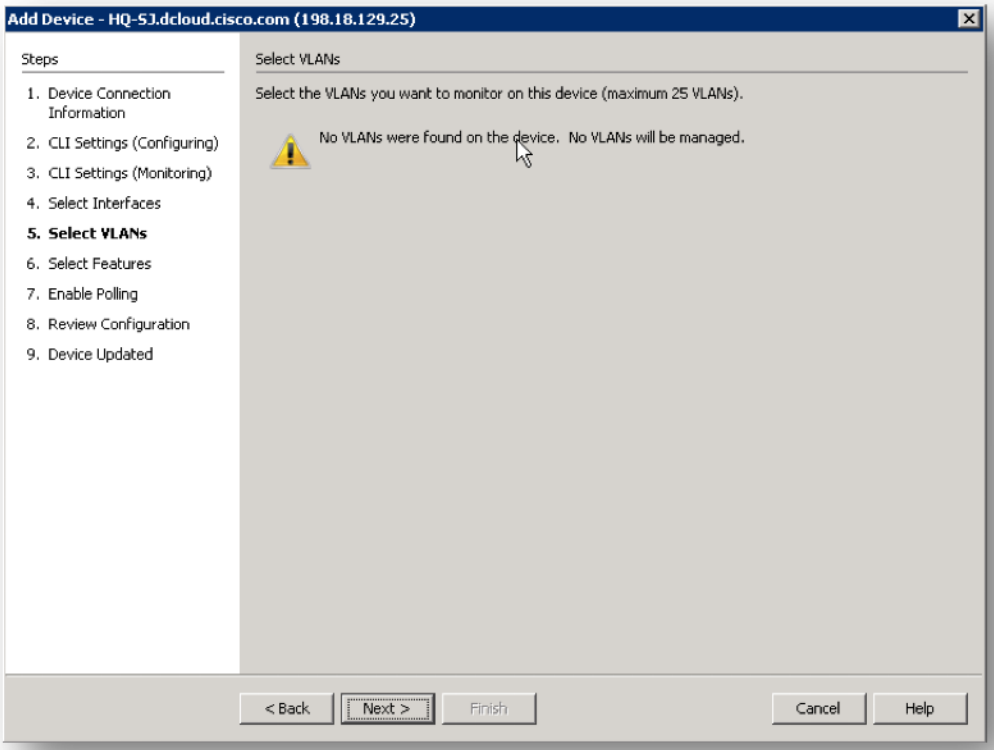
On the select interfaces window you may notice 3 interfaces are already selected. LiveAction automatically selects the interfaces based on the highest bit rate.



A 6

10. Click Next.

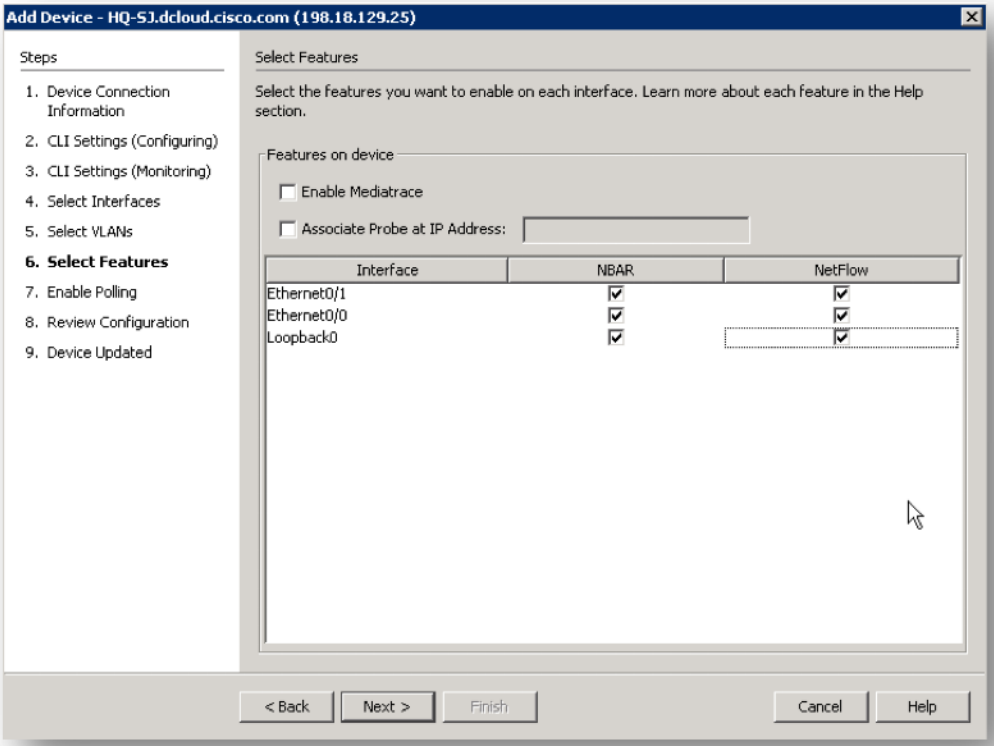
Note: Since there are no VLANs configured on this device, none will be displayed. You may monitor up to 25 configured VLANs on each device.



A 7

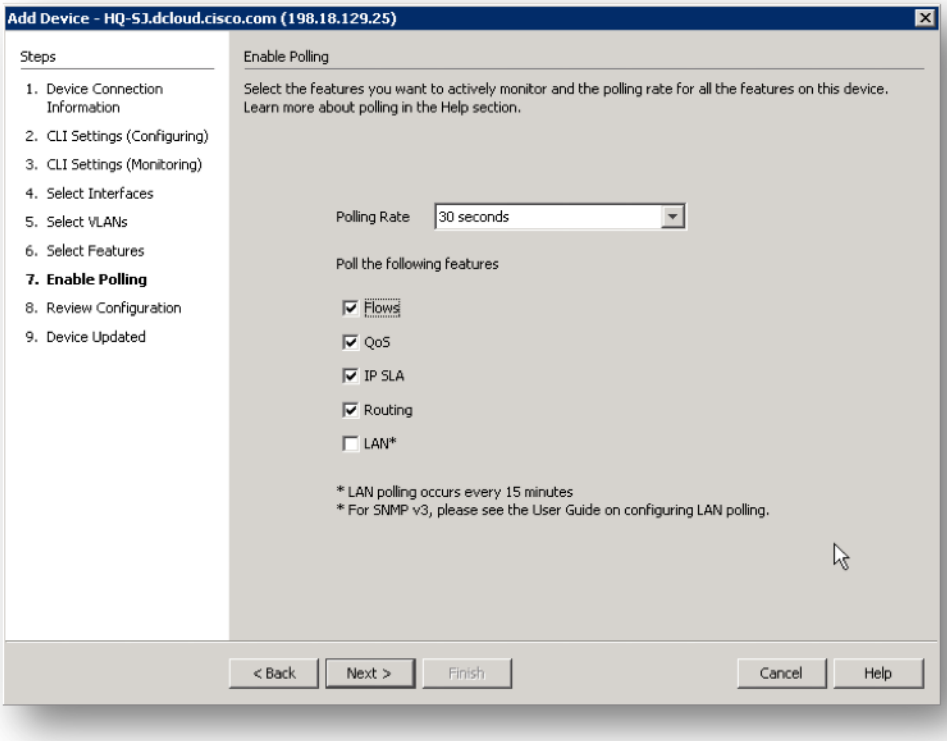
11. Click Next.

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**.



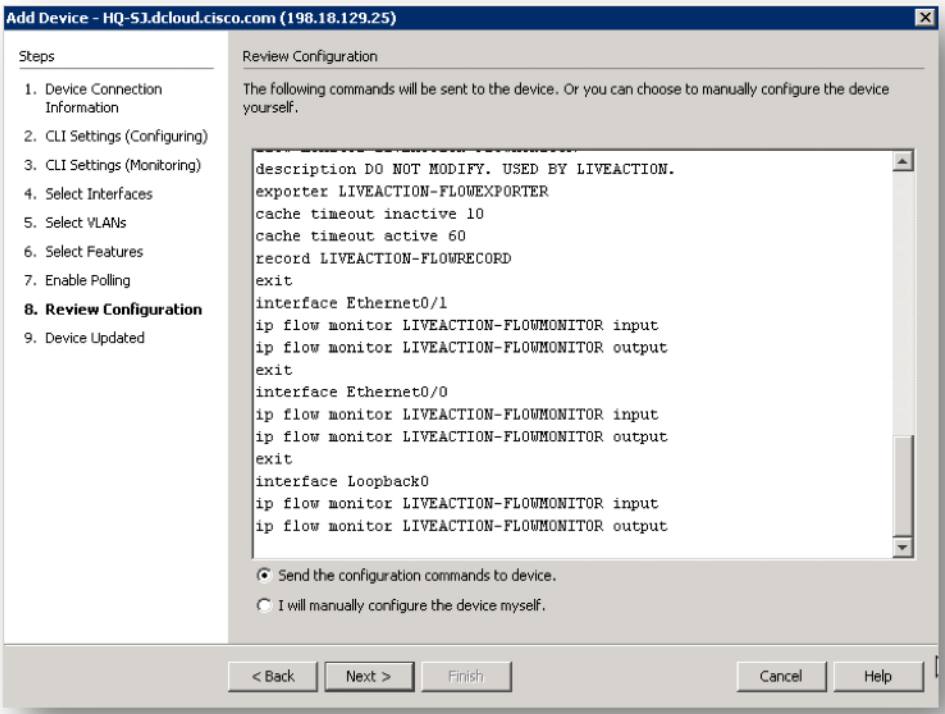
A 8

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



A 9

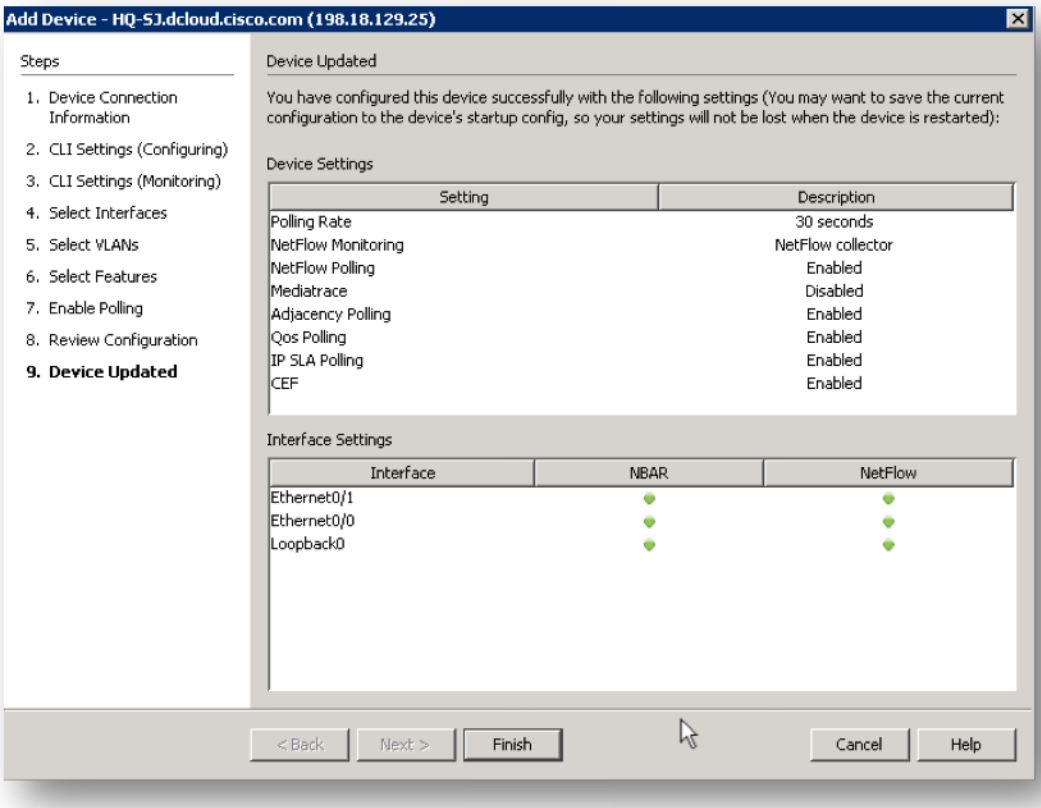
Note: Any changes to the Select Features dialog will generate a CLI push to update the current configuration. Before sending the NetFlow configurations to the device, you can verify the configurations that LiveAction created.



A 10

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

17. Click Finish.



A 11

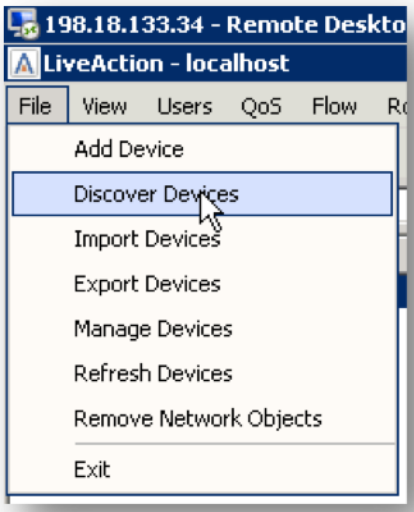
The device will be added to the Topology Pane in LiveNX. Note that LiveNX will not automatically position a new device with reference to any existing devices… you may need to scroll-about in the Topology Pane to locate your new device(s).

Appendix 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:

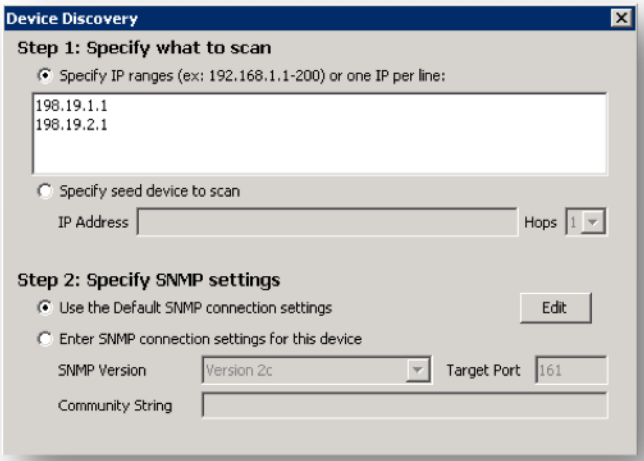
1. Select File and Discover Devices.



A 12

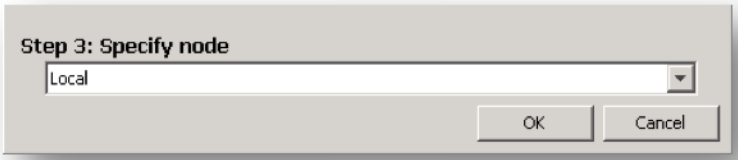
2. Specify the following IP addresses:
   198.19.1.1
   198.19.2.1

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



A 13

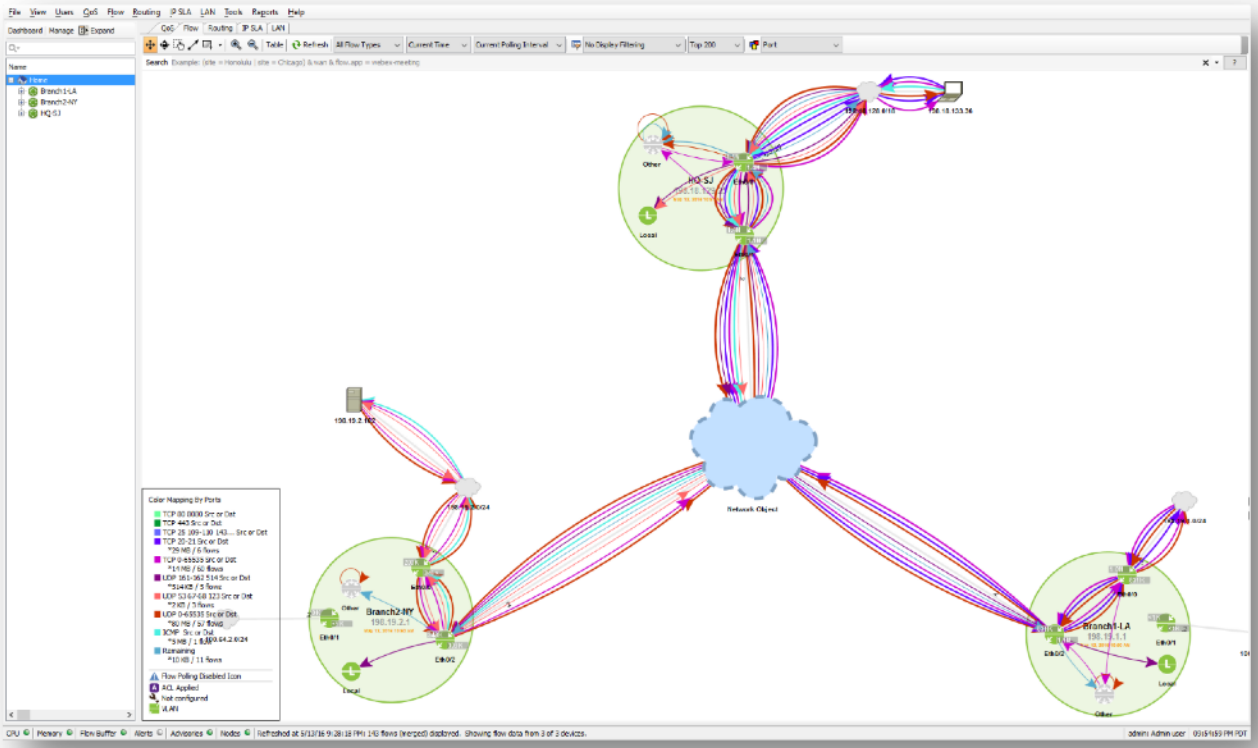
Note: In the Lab infrastructure we are utilizing the Local LiveNX Node included with the Server installation. If you require access to a Remote Node to access the subnets or addressing in "Step 1: Specify what to scan" you would use the Specify node drop-down at the bottom of this dialog box.



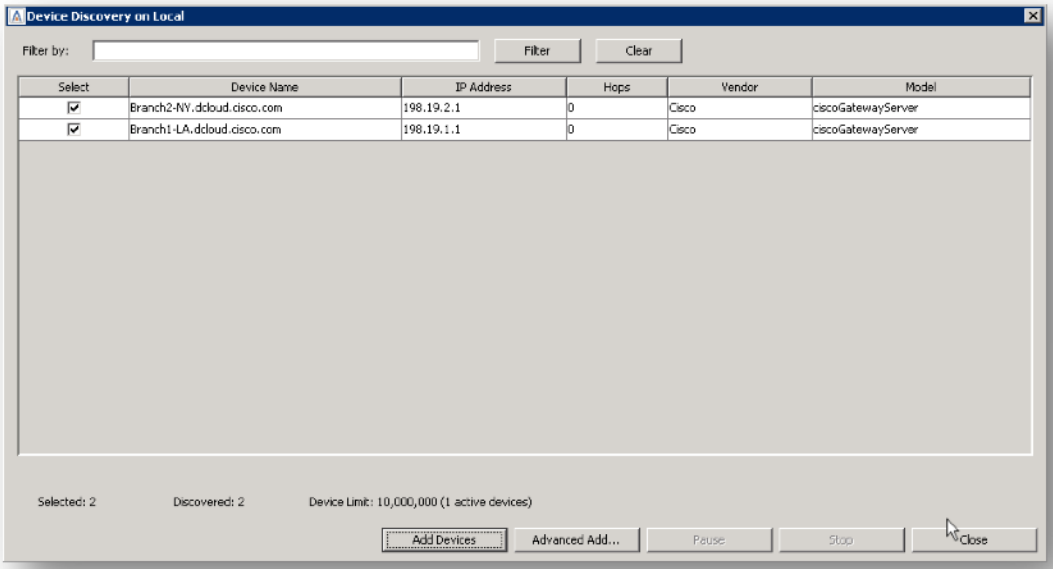
A 14

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.

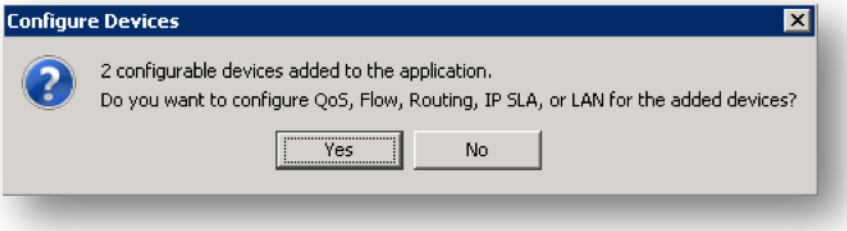


A 15



A 16

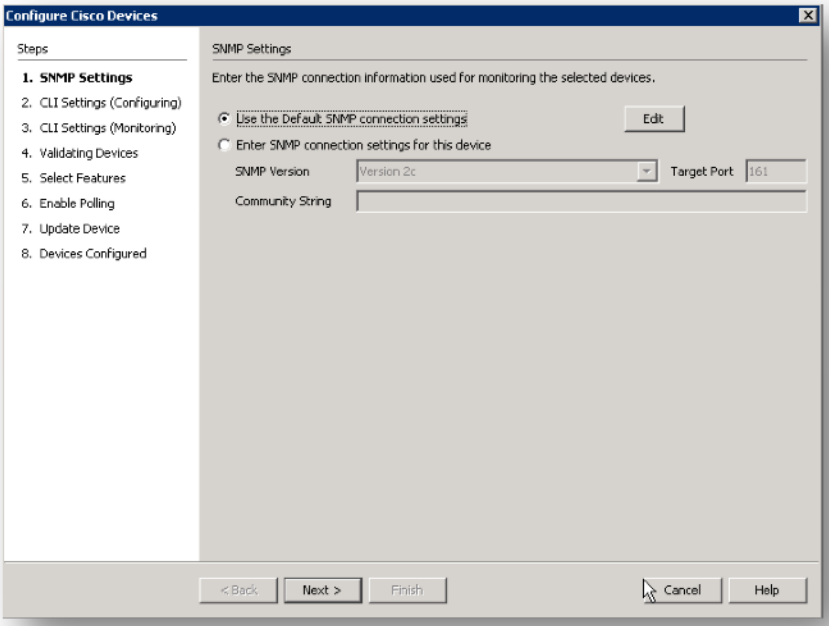
6. Select Yes on the configure devices dialog.



A 17

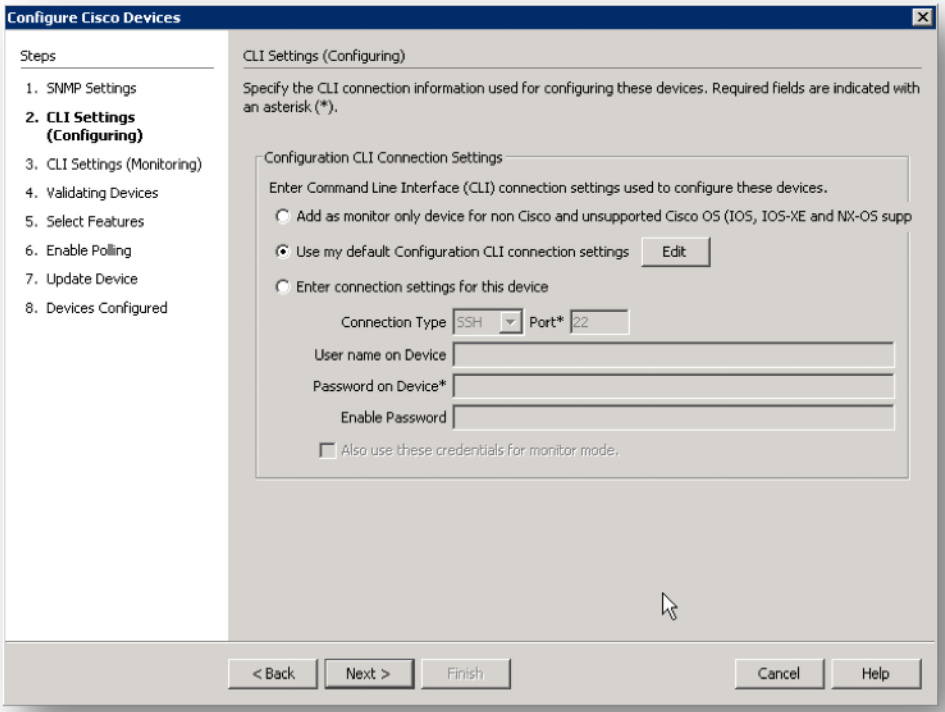
7. Use the default SNMP connection settings and then select Next

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.



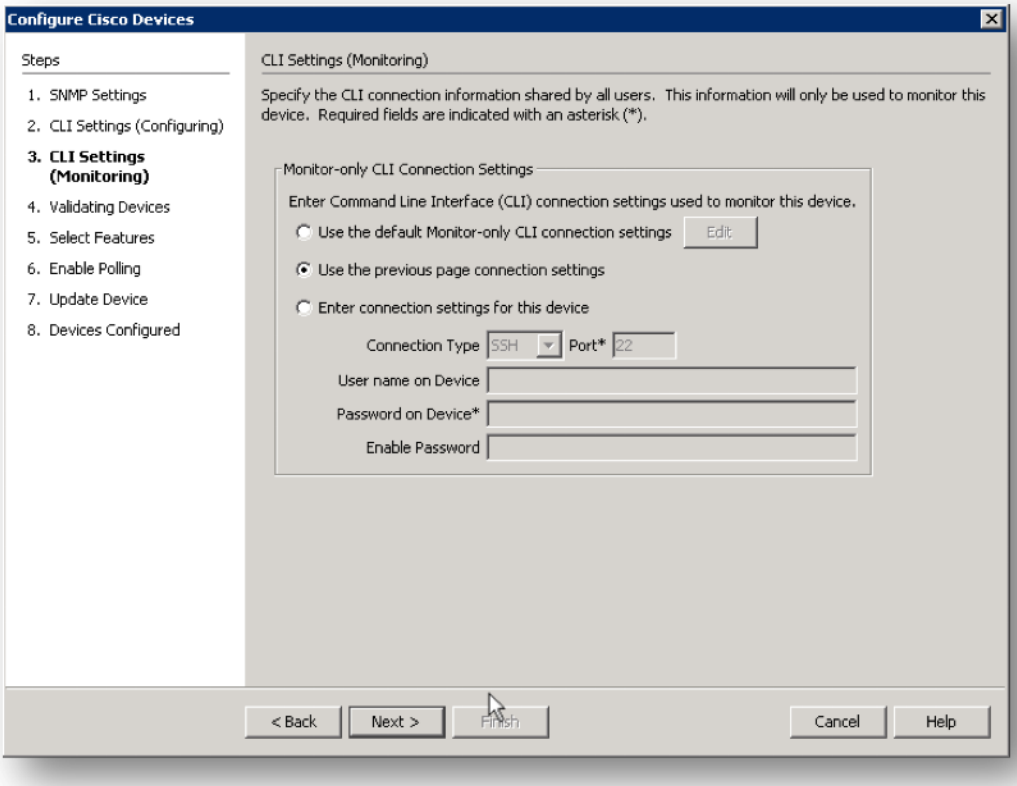
A 18

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



A 19

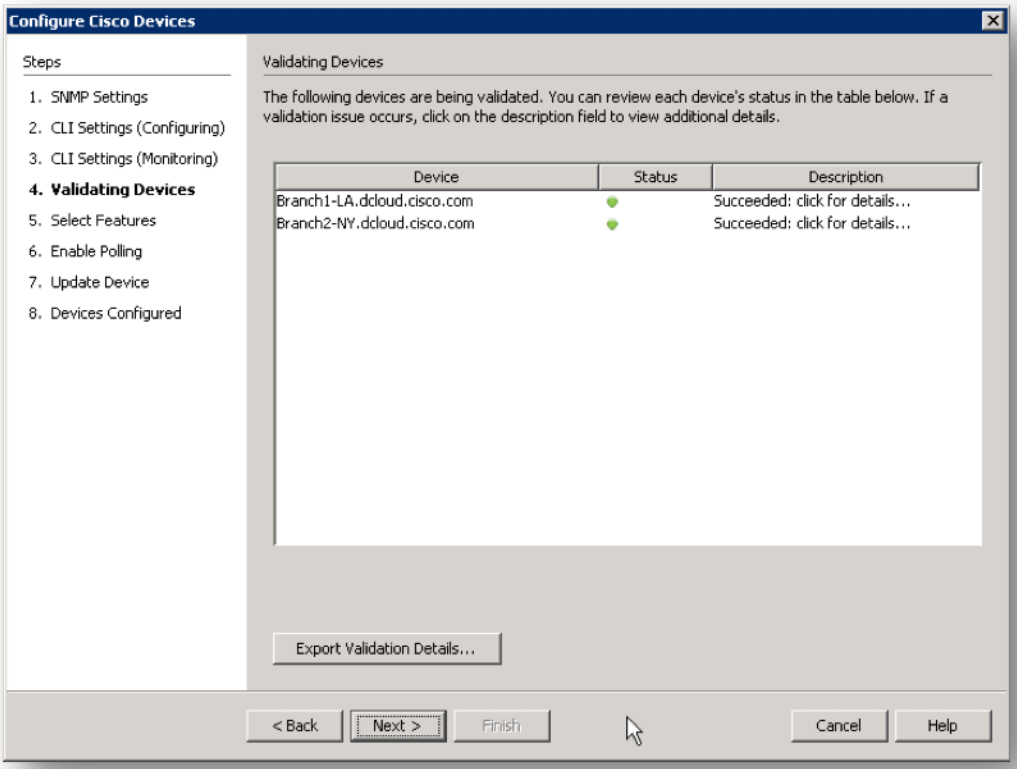
10. Select Use the previous page connection settings.



A 20

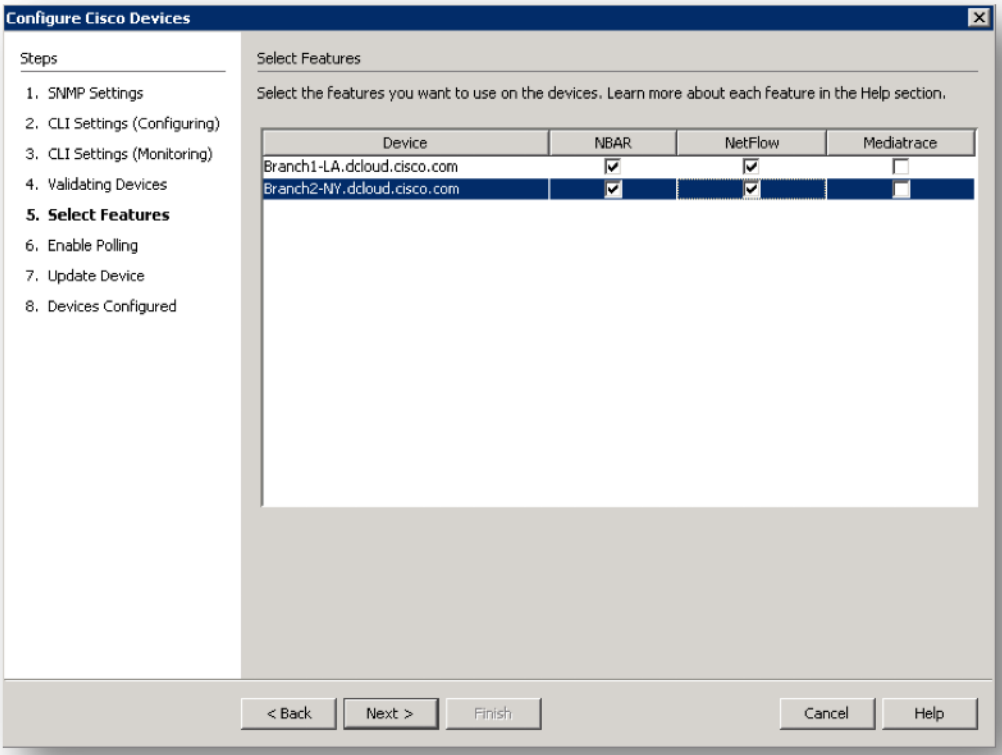
11. Click Next

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



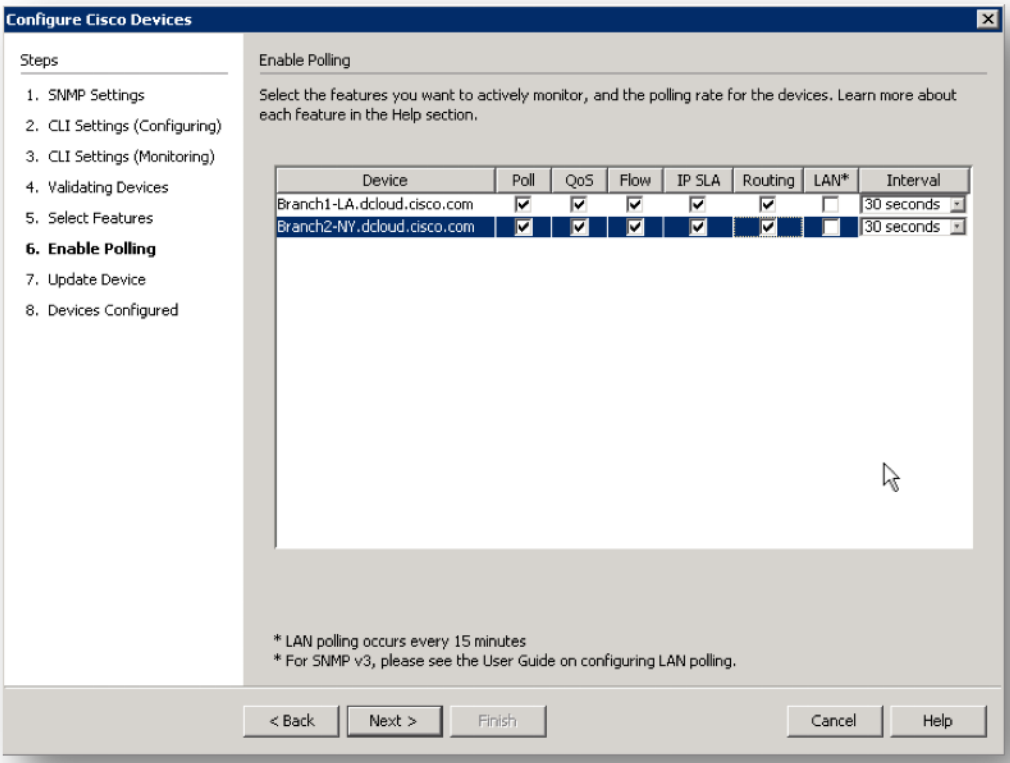
A 21

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



A 22

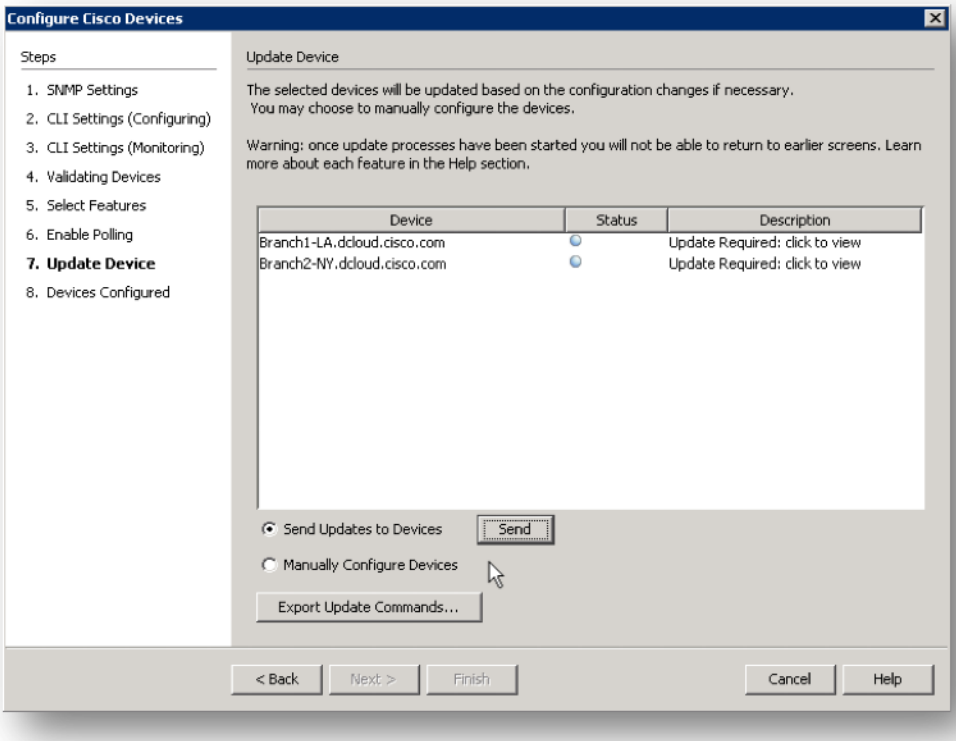
14. Select all technologies excepting LAN.
15. Set the interval to 30 seconds for each device, Click Next.



A 23

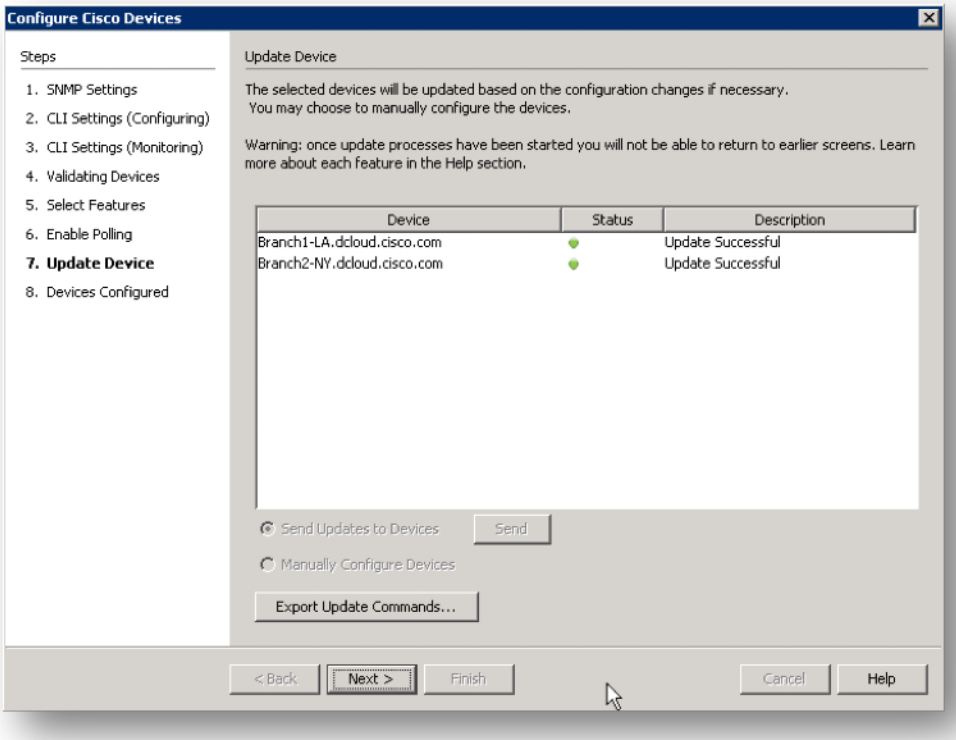
Note: For our class Labs we are gathering data every 30 seconds to reduce wait time when we make changes. In a production environment this may generate more network traffic than desired.

16. Select Send Updates to Devices and click Send.



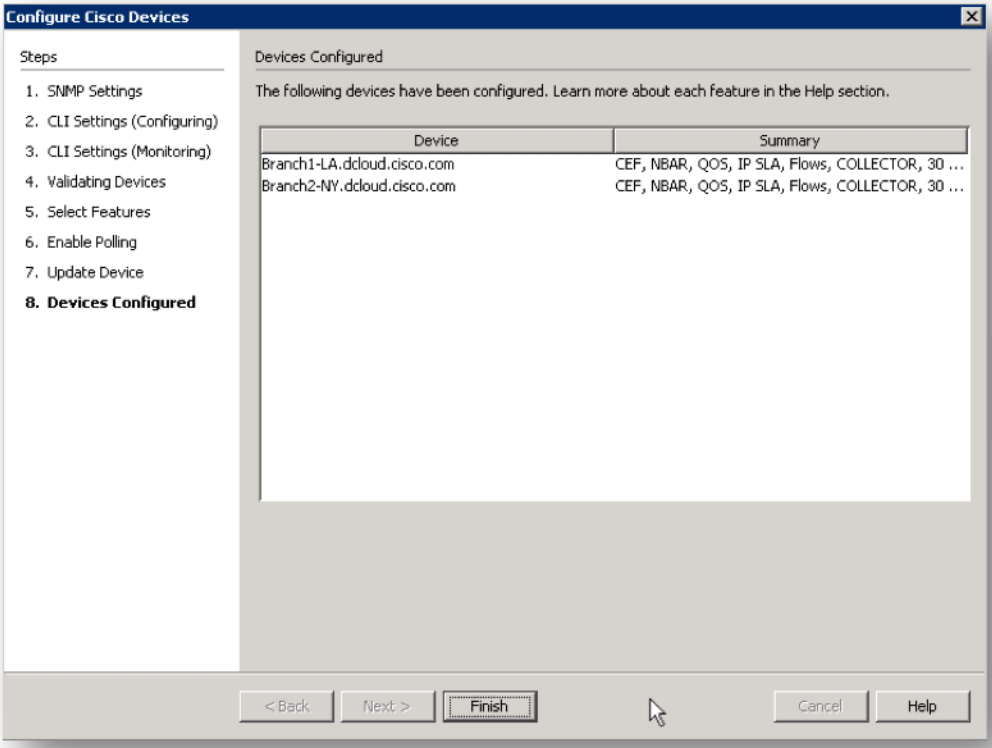
A 24

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



A 25

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



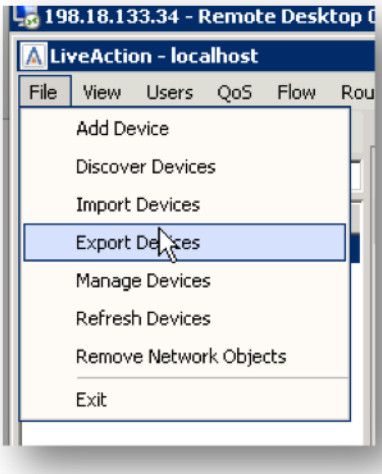
A 26

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.

Appendix 3: Export/Import Device Configuration

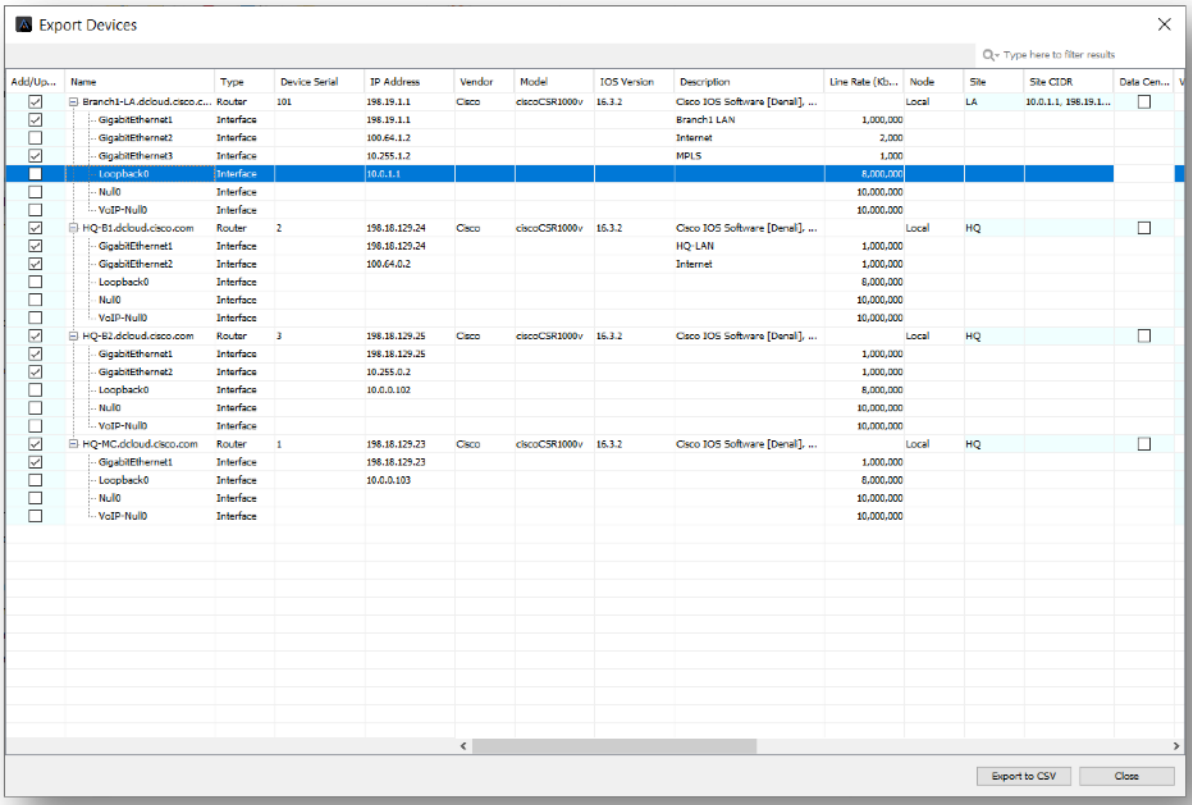
Lab Steps:

1. From the File Menu select Export Devices.



A 27

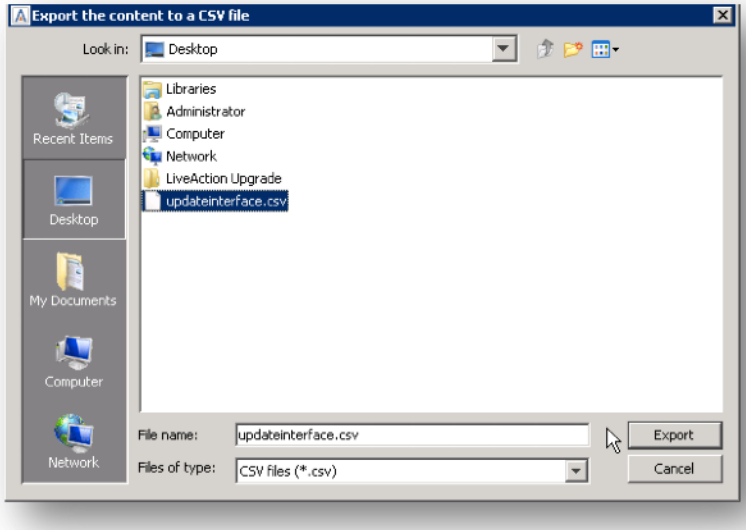
2. Deselect **GigabitEthernet2** and **Loopback0** from the 198.19.1.1 and 198.19.2.1 devices.



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				

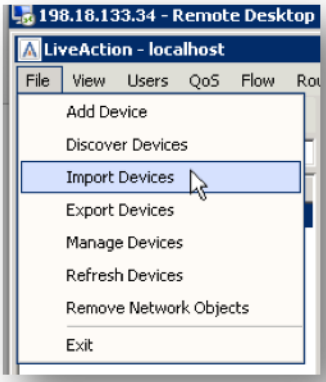
A 28

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.



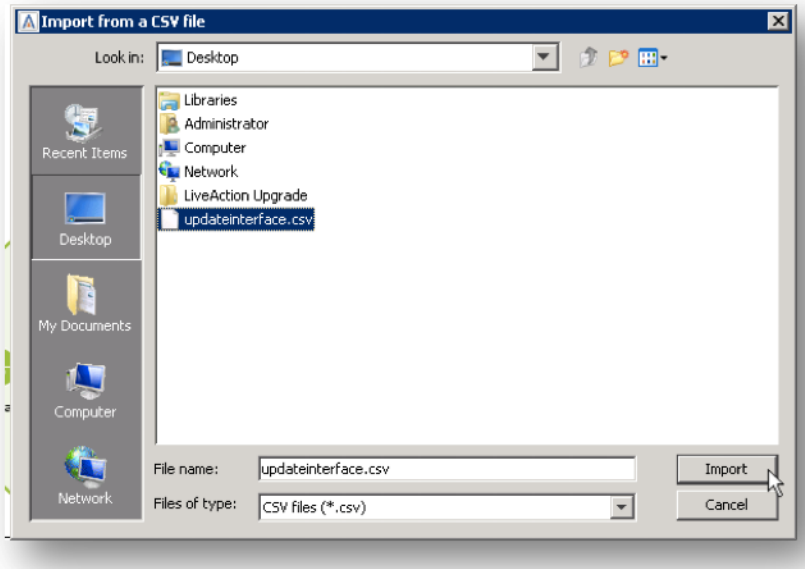
A 29

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



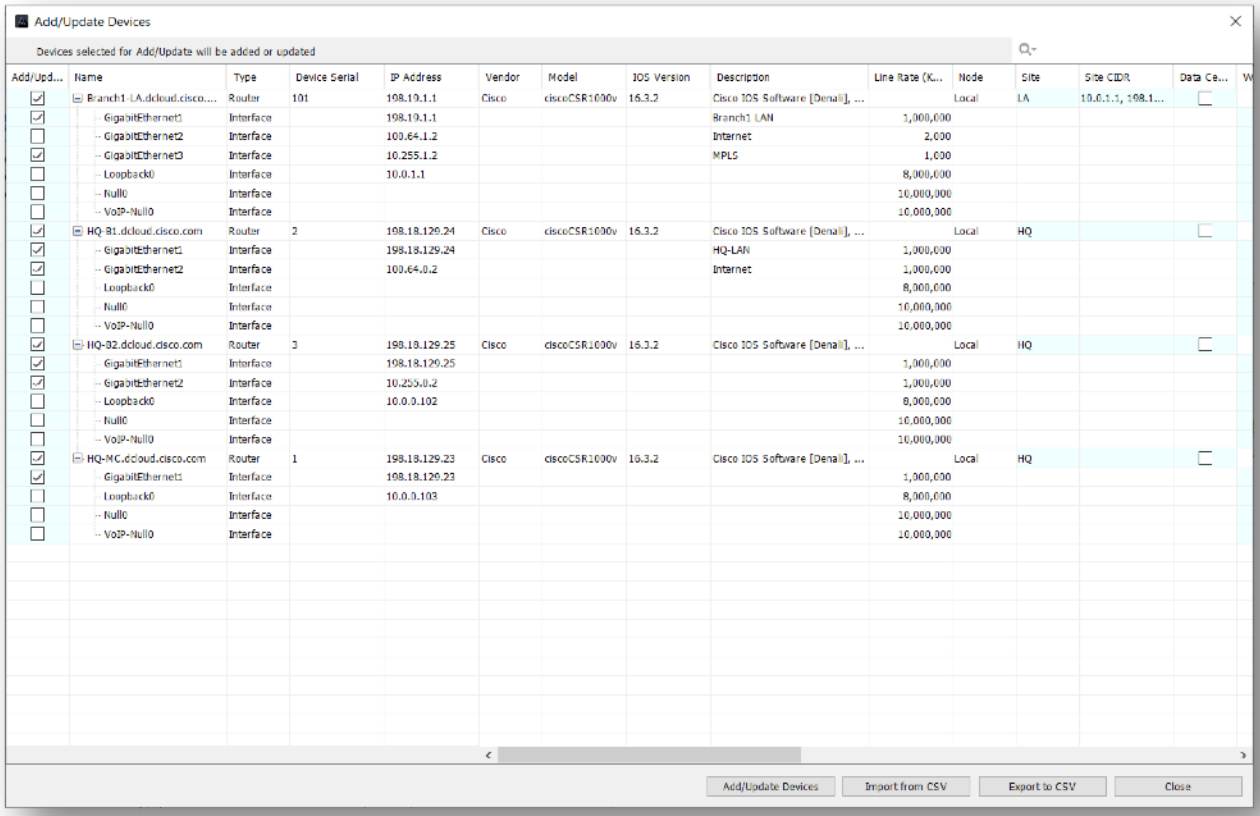
A 30

8. Select the file you previously exported.



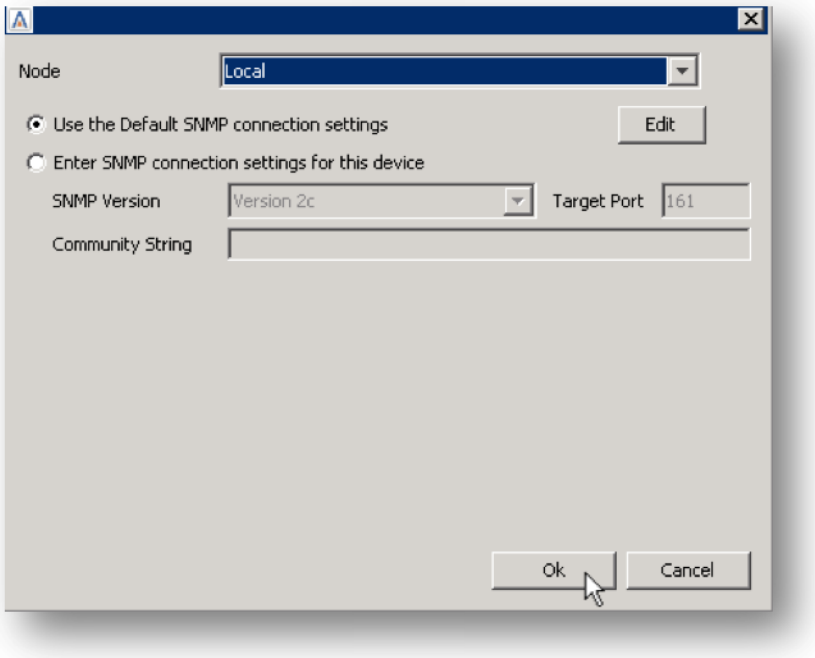
A 31

9. Click Add/Update Devices.



A 32

10. Click OK to use the Default SNMP settings.



A 33

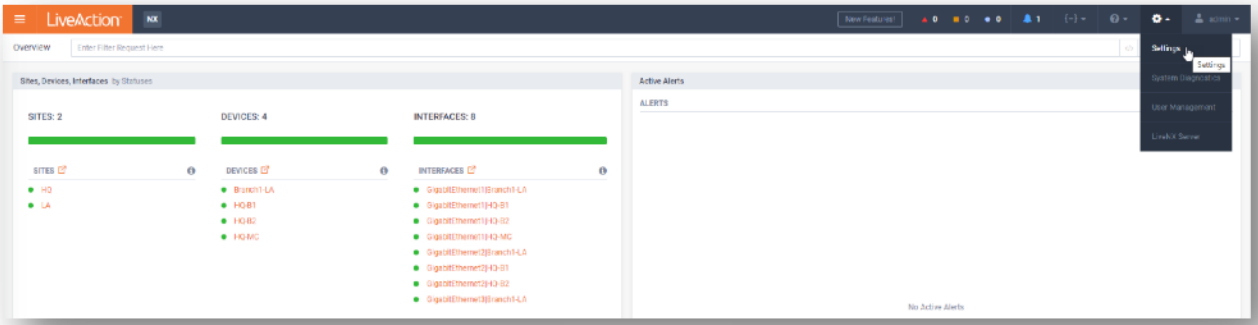
Your Topology Pane will now show the appropriate devices/configurations.

Appendix 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.

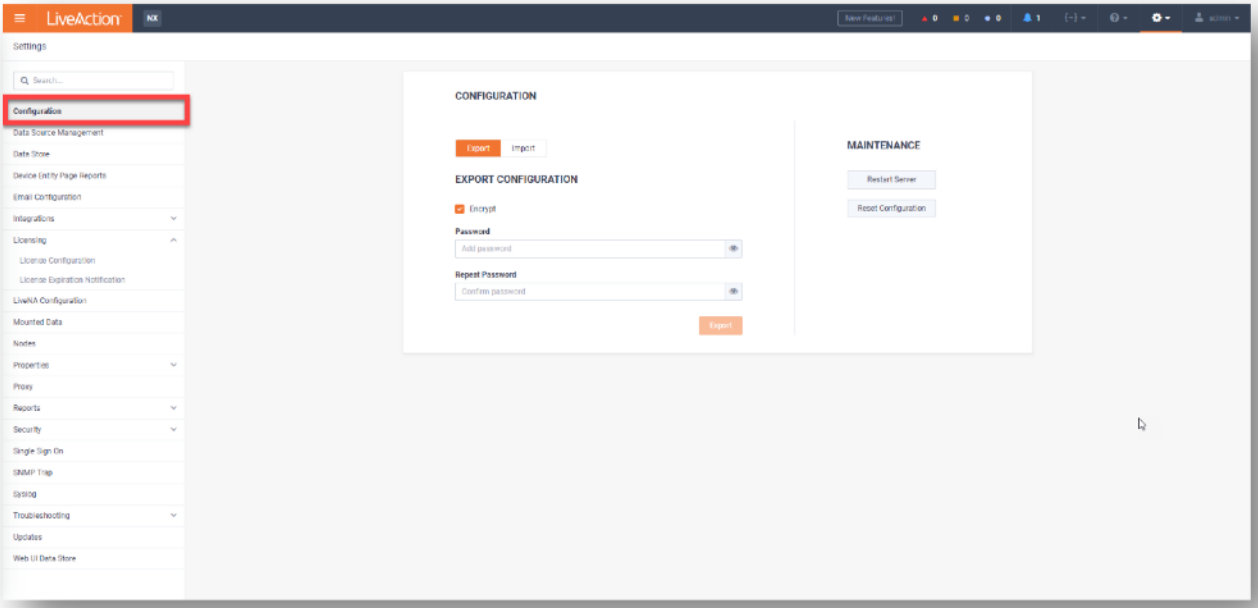
Lab Steps:

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



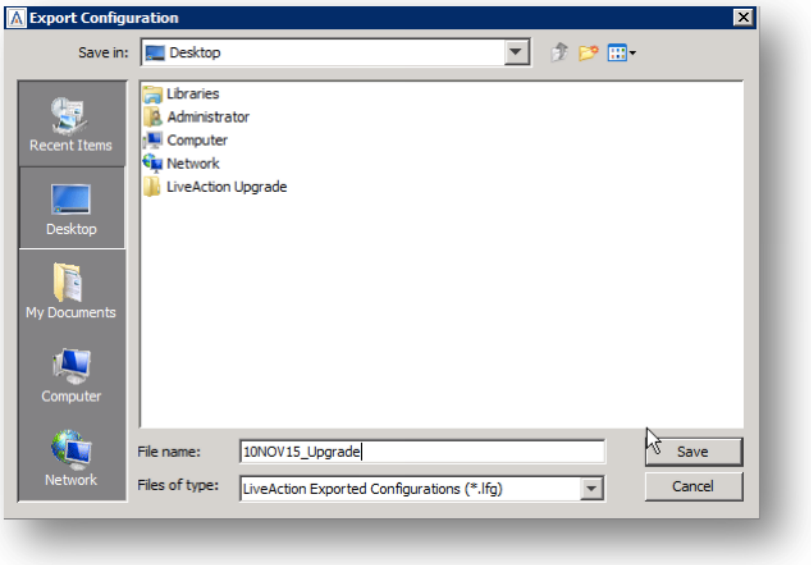
A 34

2. Select **Configuration**.



A 35

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



A 36

5. Select an appropriate place to save the file, give the file a name, then click Save.

Appendix 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.

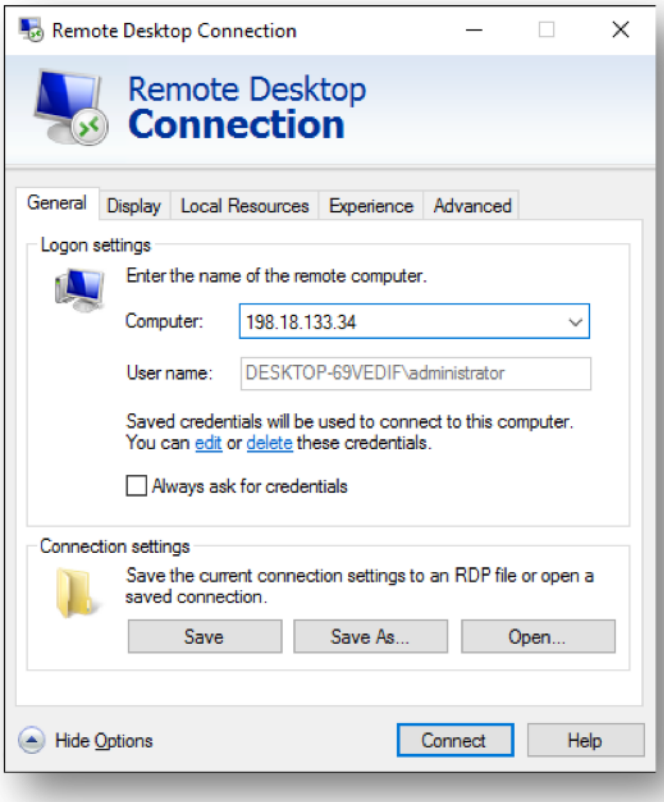
Note: Use the information from the Lab Details table to connect to the desired device.

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



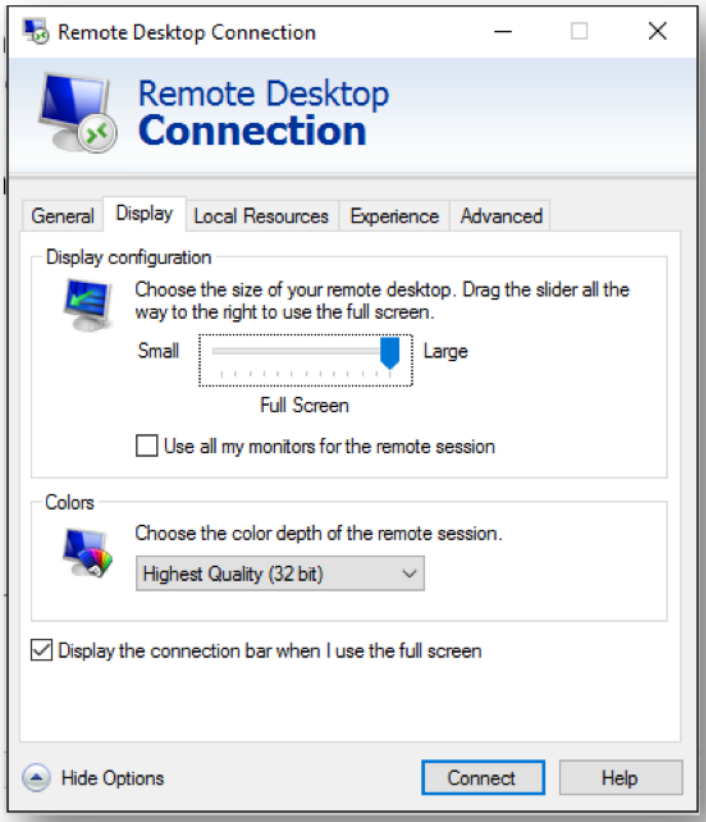
A 37

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

8. Set the RDC session properties on the Display tab so that your video is a minimum of 1200x800 resolution… this may NOT be changed once the connection is active. See next page for example.

✓

DIAGRAM

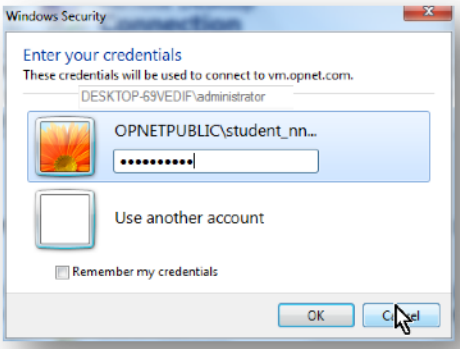


A 38

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.