

LiveAction Training Lab Workbook Pt. 1

#### © Copyright 2021, LiveAction, Inc.

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

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

#### Trademarks:

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

All other products or services mentioned herein are trademarks or registered trademarks of their respective owners. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark. 2021-Aug.

## **Table of Contents**

	Contents	
	etup and Get Connected	
	Connect to the Lab Network	
Lab 0.2: (	Connecting to Your Training Pod	. 9
Lab 0.3: I	Install the LiveNX Client	11
Lab 1: Th	he LiveNX Web UI	12
	Explore the Web UI	
Lab 1.2: (	Create a Custom Dashboard	18
Lab 1.3: F	Pre-Configured Stories	20
	WebUI Reports	
Lab 1.5: E	Enable / Customize Alerts	26
	Add a User Account	
Lab 1.7: \	View and Navigate System Diagnostics	30
Lab 1.8: \$	Support and Troubleshooting	33
	he LiveNX Client	
	Launch the LiveNX Client	
	Explore the LiveNX Client	
	onfiguring Devices	
	Add Device	
	Manage & Configure Devices	
	Configure Flow on Devices	
	Add/Remove Interfaces	
Lab 3.5: I	Merge Clouds in Topology	54
	raffic Flows	
	Discover Flows	
	Discover Specific Flows	
	Examine Specific Traffic	
	Troubleshoot Issues	
	Itering, Identifying, Marking	
	Creating Custom Filters	
	ACL Creation	
Lab 6: M	aking the Topology Work	79
	Setting Device Semantics	
	Adding Devices to Groups	
	Creating Network Objects	
	ashboards & Reports	
	The Dashboard	
	Viewing Reports1	
	Create a Custom Report1	
	oS	80
	QoS Marking Policy	
	QoS Queueing Policy	
	QoS Verification	
	ppendix	
	Add Device	
	Client Device Discovery	
	Export/Import Device Configuration	
	Saving Server Configurations	
Lab A.5: 0	Connect via Remote Desktop Connection1	58

#### **IMPORTANT INFORMATION – Please Read!**

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

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

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

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

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

# Lab.0

Lab 0: Setup and Get Connected

## Lab 0.1: Connect to the Lab Network

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

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

Local:

1 x PC Workstation to be used as a Management PC (Your Laptop)

1 x Installed LiveNX Client

1 x Browser

Remote Student Pod

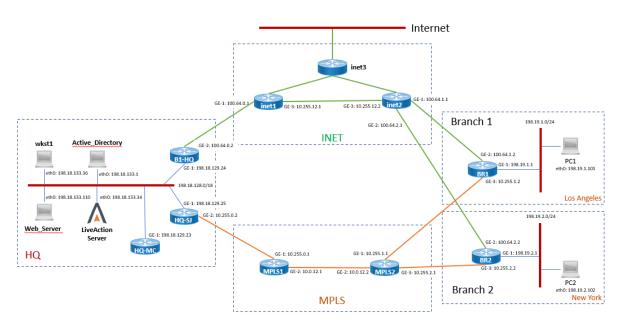
1 x Windows Workstation accessed via RDC (optional) with an installed LiveNX Client and Browser

1 x LiveNX OVA Linux install

1 LiveNX Server

1 LiveNX Node (installed on LiveNX Server)





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

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

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

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

Learning Labs Menu	0	Lab Status :	✓ READY		Time Lef	E: 8 DAYS 4 HOURS		
英 Overview		Topology	Lab Details					
Labs Introduction		SI No	Role	Hostname	Username	Password	IP Address	Port
		1	Liveaction	livenx	admin	Student	35.231.127.249	443
Access Devices		2	B1-HQ	HQ-B1	admin	C1sco12345	35.231.127.249	20019
		3	inet1	INET1	admin	C1sco12345	35.231.127.249	20018
		4	inet2	INET2	admin	C1sco12345	35.231.127.249	20020
		5	inet3	INET3	admin	C1sco12345	35.231.127.249	20021
		6	BR1	Branch1-LA	admin	C1sco12345	35.231.127.249	20001
		7	B2-HQ	HQ-B2	admin	C1sco12345	35.231.127.249	20022
		8	MPLS1	MPLS1	admin	C1sco12345	35.231.127.249	20010
		8	MPLS2	MPLS2	admin	C1sco12345	35.231.127.249	20009
		9	BR2	Branch2-NY	admin	C1sco12345	35.231.127.249	20000
		10	wkst1	Administrator	Administrator	C1sco12345	35.231.127.249	20201
		11	Activedirectory	Administrator	Administrator	C1sco12345	35.231.127.249	20202
		12	PC1	Administrator	Administrator	C1sco12345	35.231.127.249	20203
		13	PC2	Administrator	Administrator	C1sco12345	35.231.127.249	20204

DIAGRAM

Lab Steps:

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

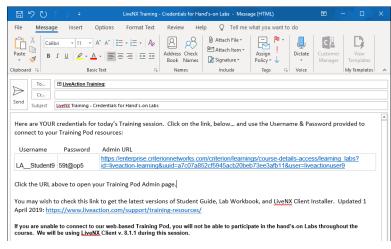
**Note:** Make sure to consult the Infrastructure Diagram and worksheets, as well as specific classroom instructions for names, IP addresses, and other parameters. **The screen shots in this Lab Workbook are examples** which may not reflect the appropriate parameters for the classroom and/or your specific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

## Lab 0.2: Connecting to Your Training Pod

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

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

#### DIAGRAM



#### Lab Steps:

1. Click the URL provided in the email.

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

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

Learning Labs Menu	Lab St	atus :	✓ READY		Time Le	eft : 8 DAYS 4 HOURS		
ର୍ଷ୍ଟ Overview	т	opology	Lab Details					
Labs Introduction	s	l No	Role	Hostname	Username	Password	IP Address	Port
Access Devices	1		Liveaction	livenx	admin	Student	35.231.127.249	443
Access Devices	2		B1-HQ	HQ-B1	admin	C1sco12345	35.231.127.249	20019
	3		inet1	INET1	admin	C1sco12345	35.231.127.249	20018
	4		inet2	INET2	admin	C1sco12345	35.231.127.249	20020
	5		inet3	INET3	admin	C1sco12345	35.231.127.249	20021
	6		BR1	Branch1-LA	admin	C1sco12345	35.231.127.249	20001
	7		B2-HQ	HQ-B2	admin	C1sco12345	35.231.127.249	20022
	8		MPLS1	MPLS1	admin	C1sco12345	35.231.127.249	20010
	8		MPLS2	MPLS2	admin	C1sco12345	35.231.127.249	20009
	9		BR2	Branch2-NY	admin	C1sco12345	35.231.127.249	20000
	10	D	wkst1	Administrator	Administrator	C1sco12345	35.231.127.249	20201
	1	1	Activedirectory	Administrator	Administrator	C1sco12345	35.231.127.249	20202
	12	2	PC1	Administrator	Administrator	C1sco12345	35.231.127.249	20203
	1:	3	PC2	Administrator	Administrator	C1sco12345	35.231.127.249	20204

## Lab 0.3: Install the LiveNX Client

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

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

To install the LiveNX Client:

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

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

# **Lab** 1

Lab 1: The LiveNX Web UI

## Lab 1.1: Explore the Web UI

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

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

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

Lab Steps:

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

LiveNX
Password
Login
By clicking "Login", I agree to the terms of LiveAction's EULA First time user information

The Overview screen will appear.

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

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

LiveAction <sup>-</sup>	NX							🌲 o 🛛 {-} ·	· 0 · 1	🕽 👻 👗 admin
Enter Filter Re	quest Here								<> App	ly filter 🛛 🛱 Aut
tes, Devices, Interfaces by S	tatuses					Active Alerts				
						ALERTS			т	ME OPENED
SITES: 3		DEVICES: 5		INTERFACES: 11						
SITES 🖸	0	DEVICES 2	0	INTERFACES 🖸	0					
HQ		Branch1-LA		GigabitEthernet1 Branch1-LA						
• LA		Branch2-NY		GigabitEthernet1 Branch2-NY						
NY		HQ-81		<ul> <li>GigabitEthernet1(HQ-B1</li> </ul>						
		HQ-MC		<ul> <li>GigabitEthernet1(HQ-MC</li> </ul>						
		HQ-SJ		<ul> <li>GigabitEthernet1/HQ-SJ</li> </ul>						
				GigabitEthernet2/Branch1-LA						

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

·≡ LiveAction №	ж		New Featurest 🔥 🔺 🖷 0 🔹 0	🜲 0 🗧 -} 🚱 😂 🚨 - admin
🕂 Main 🛛 👘	iere			
Overview     tuses			Active Alerts	
Dashboard			ALERTS 1	TIME OPENED
Sites	DEVICES: 5	INTERFACES: 11	Over 1% of Voice traffic for HQ-82.dcloud.cisco.com running application unknown is not marked as DSCP E	EF. 24 Jul 2021, 10:27 AM
Devices			Over 1% of Voice traffic for Branch1-LA.dcloud.cisco.com running application sip is not marked as DSCP EF	
Interfaces	O DEVICES 2	INTERFACES ☑	Over 1% of Voice traffic for Branch2-NY.dcloud.cisco.com running application sip is not marked as DSCP EF     Over 1% of Voice traffic for HQ-MC dcloud.cisco.com running application lanrevagent is not marked as DSC	
	Branch1-LA	GigabitEthernet1lBranch1-LA	Oren has of value name for reprint solution control and approximation namenagement of market as back	e en ao su ava i, va sa nu
WAN Applications	<ul> <li>Branch2-NY</li> </ul>	<ul> <li>Gigabitcherret (Branch1-LA</li> <li>GigabitEthernet1(Branch2-NY</li> </ul>		
Alerts	<ul> <li>HQ-B1</li> </ul>	<ul> <li>GigabitEthernet1[HQ-B1</li> </ul>		
Network Users	<ul> <li>HQ-B2</li> </ul>	<ul> <li>GigabitEthernet1 HQ-B2</li> </ul>		
	HQ-MC	<ul> <li>GigabitEthernet1[HQ-MC</li> </ul>		
Topology		<ul> <li>GigabitEthernet2(Branch1-LA</li> <li>GigabitEthernet2(Branch2-NY</li> </ul>		
		GigabitEthernet2[HQ-B1		
Stories		<ul> <li>GigabitEthernet2[HQ-B2</li> </ul>		
_		<ul> <li>GigabitEthernet3(Branch1-LA</li> </ul>		
Lal Reports		<ul> <li>GigabitEthernet3(Branch2-NY</li> </ul>		
@ LiveNA				
✗ Configure				

#### 5. Select Sites.

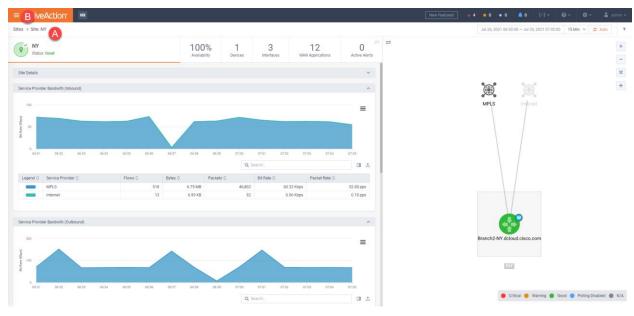
E LiveAction <sup>™</sup>									4 = 0 4	• 0 🐥 0 {} •		
Enter Filter Request Here	0								t021 06:50:00 →	Jul 26, 2021 07:05:00	5 Min 😂 Auto	Configure Sites
										Q Search		
SITE NAME	\$ITE STATUS	٥	DEVICE REACHABILITY	0	DEVICE CPU/MEMORY	0	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION D	ROPS O	INTERFACE ERRORS	
Site Name	All	~	All	~	All ~		Peak Utilization In	Peak Utilization Out	All	~	Interface Errors	
HQ	•		•				4.65%	34.28%		•		
LA	•		•		•		27.22%	0.01%		•		
NY	•						4.57%	10.13%				

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

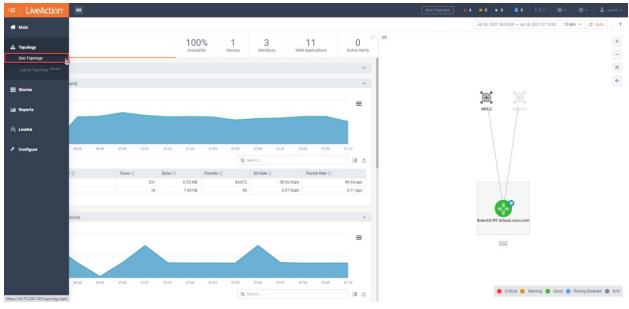
Note: Detailed site information is specified in the Device Semantics Lab.

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

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



9. Select Topology > Geo Topology



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



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

	Management 😨	My Devices (4)				My Interfaces	(0)			Discovered E	awicas (0)				() A	utorlino	overy (1)		
		my bences (4)				My interfaces	(0)			Discovered L					() A	utouisc	overy (1)		
Edit	Refresh List	t Configure	Delete	Rediscove	r Interfaces								Q S	earch					
0	DEVICE 🗘	DEVICE STATE 🗘	IP ADDRESS 🗘	VENDOR	MODEL O	NODE 🗘	SITE (	INTERFACES 🗘	HARDCODED _ 🗘	POLL 0	qos (	FLOW	) IP SLA	0	ROUTING	0	LAN	0	TAGS
	Device	All V	IP Address	All ~	Model	Node	Site			All ~	All V	All ~	All	~	All	~	All	~	Tags
	HQ-MC	Up	198.18.129.23	Cisco	ciscoCSR10	Local/Server	HQ	1		~	~	~							
	HQ-B1	Up	198.18.129.24	Cisco	ciscoCSR10	Local/Server	HQ	2		~	~	~							
	Branch1-LA	Up	198.19.1.1	Cisco	ciscoCSR10	Local/Server	LA	3		~	~	~							
	HQ-B2	Up	198.18.129.25	Cisco	ciscoCSR10	Local/Server	HQ	2		~	~	~							

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

## Lab 1.2: Create a Custom Dashboard

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

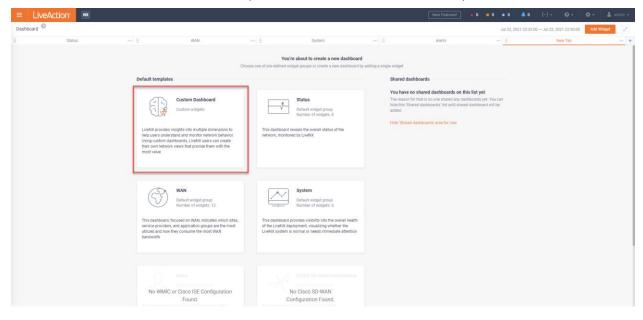
In this Lab you will Create and Modify your own Custom Dashboard.

Lab Steps:

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

·≡ LiveAction <sup>~</sup>	NX					New Features!         A         0         #         0         4         0         {-}         -	0· 0·	- 🛔 admin -
👫 Main						Jul 22, 2021 22:30:00 - Jul 22,	2021 22:45:00 A	dd Widget 🥜
Overview	Status … II	WAN			System	II Alerts	1	
Dashboard								Apply filter
Sites								
Devices	Peak Inbound WAN Interface Utilization	E Top WAN	Applications by Bandwidth In	bound/Outbound Bandwidth	×	Top Interfaces % Changed - Interface Burstable Rate		×
Interfaces	1	ospf-routing		0.3	o In	Branch1-LAGigE2InboundLAInternet 0		
WAN Applications		netbios-dgm- ntpnetwork	netbios-group k-service	<0.1	<ul> <li>Out</li> </ul>	HQ-MC→GigE1→Inbound→HQ→ 0 HQ-SJ→GigE2→Inbound→HQ→MPLS 0		
Alerts						Branch2-NY→GigE3→Inbound→NY→MPLS 0 H0-SJ→GigE1→Inbound→H0→- 0		
Network Users						HQ-B1→GigE2→Inbound→HQ→Internet 0 HQ-B1→GigE2→Outbound→HQ→Internet 0		
Network Users						Branch1-LAGigE2OutboundLAInternet 0		
a Topology						Branch1-LA->GigE3->Outbound->LA->MPLS 0 Branch1-LA->GigE1->Inbound->LA->- 0		
				Kbps				
Stories	×	🗄 Overall Sta	itus All		×	Top Devices Top Devices CPU Usage		×
			Critical	Warning	Good	HQ-MCHQ 35.0 HQ-B1HQ 35.0		
Lill Reports		Sites	0	0	3	Branch1-LALA 34.0		
<u>.</u>						Branch2-NY→NY         29.0           HQ-SJ→HQ         25.0		
C. LiveNA		Devices	0	0	5			
€ Configure								
• compare		WAN Apps	0	0	0			
	1 / J / J					<u>`</u>		
	Least Availability X	: Availability	Top Interfaces With Least A	wailability	×			
			-LA→-→GigabitEthernet1 -LA→Internet→GigabitEthern	100.0				
			-LA→Internet→GigabitEthernel					
		NY-Branch2	-NY→-→GigabitEthernet1	100.0				
			-NY-Internet-GigabitEthen					
			NY→MPLS→GigabitEtherne +→GigabitEthernet1	100.0				
		HQ→HQ-B1-	++orgabitEtheffet1	100.0				

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



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

oard  Status	WAN		System	Alerts	Jul 2	Add widget Current dashboard: New Tab	
						Added 0 out of 9 widgets	
						A Drag and Drop	
						widgets from this	5
						Alerts panel	
						Availability	
						Availability	
					105	E Top Devices With Least Availability	
				and the set of sector the sector of the sect	C: Top Inter	faces With Least Availability	
				В		Top Service Providers with Least Availability Top Sites with Least Availability	
						E Totals by Sites, Devices and Interfaces	
						Applications	
		1				E Top Application Performance Summary	
						Top Voice/Video Performance Summary	
	WAN	Drop widgets here				Address	
						Source Address	
						Destination Address	
						Source or Destination Address	
						Site Traffic	
						Source Site Traffic	
						Destination Site Traffic	
						Bidirectional Source/ Destination Pair	
						Network	
						Country Kinturnely	
						Create New Widget	

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

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

6. You can also change the order

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

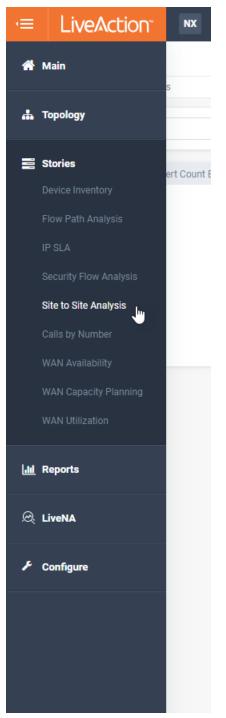
**Note:** Since LiveNX stores *breadcrumbs* it will retain a trail of the last page you've visited in the WebUI, based-upon your individual login credentials. Unless shared... Your custom Dashboard will not be visible to others.

## Lab 1.3: Pre-Configured Stories

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

Lab Steps:

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



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

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

DIAGRAN	NX	New Feature:         A 0         E         O         A 1         (-)         O         -         A           Apply film         Jad 22, 2021 21:2000 – Jad 22, 2021 21:3000         15 Min         15 Min <td< th=""><th></th></td<>	
		Dupor To	able
	VIEW FILTER	4	
	BIRCCTION Recound Outbound METRIC Bandwidth Utblication		

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

LiveAction 💌		New Features 0 = 0 = 0 + 1 {-} -	• 😔 • 🕹 admi
te To Site Analysis > NY · HQ		≤ Jul 22, 2021 21:25:00 → Jul 22, 203	21 21:40:00 > 15 Min ~ C Aut
Switch Direction Enter Filter Request Here		👳 Apply filter 🛛 🕅 IWAN C	Control Filter Flow Details
plication	DSCP	Service Provider	Sta
op 10 🗸	All 🗸	All	All
bittorrent-networking	0 (BE)		
		MPLS	N/A
ica tannevagent			
	46 (EF)		
rtp-audio			
ip			
lφ.			
φ.			
49			
9			
ap			
49			
49			
49			
49			
49			
49			
49			

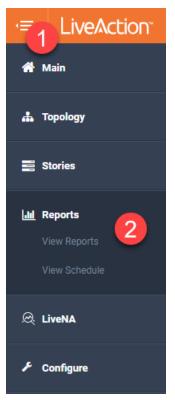
View the other pre-configured Stories to discover how they may help you with Capacity Planning, Inventory, and Network Management.

### Lab 1.4: WebUI Reports

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

Lab Steps:

1. Click the Menu icon.



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

E LiveAction №							<b>A</b> 0			
iew Reports								View	Schedule	Create Report
Templates Reports History										
Q By Template Name										Table Tile
efault Templates	Favorite Reports									0
ice Analysis	Add Report									
IAN (C										
vorite Applications	Top Reports									0 0
ble Fastiane Applications										
ole Fastlane Voice Analysis	NAME C	DESCRIPTION \$								
N Capacity Planning	Application	This Flow-based report	will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.							
Network Performance Audit	Top Conversations	This Flow-based report	will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.							
e/Video Performance Vs. Network 6	Interface Bandwidth	This Flow-based report	will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.							
to-Site Traffic Utilization Audit	DSCP	This Flow-based report	will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.							
ice Provider DSCP Audit	Top Interface Bandwidths	This SNMP-based report	t shows a table of all the interfaces' bandwidth utilization per the specified filter.							
k Single Site WAN Path Changes	Top Interface Errors	This SNMP-based report	t shows a table of all interface errors (CRC/Runts/Overruns, etc.) per the specified filter.							
lication Vs. Network Performance	Top Class Bandwidths	This SNMP-based report	t shows a table of all QoS class bandwidths for all interfaces per the specified filter.							
e/Video Service Provider Performan	Top Class Drops		t shows a table of all QoS class drops on all interfaces per the specified filter.							
ication Service Provider Performan	Interface Bandwidth	This SNMP-based repor	t graphs bandwidth utilization of a specific interface.							
VAN Application Service Provider Pe	Interface Utilization		t graphs the interface bandwidth utilization (by percentage) of a specific interface.							
AN Application Vs. Network Perfor	Interface Errors		t graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.							
AN Voice/Video Performance Vs. N	Post-Policy brops		t graphs the QoS drops of all classes on a specific interface.							
-	Application back Addit		vill show the DSCP markings of applications organized by site, based on the selected filter criteria.							
(AN Voice/Video Service Provider P	interface partoniaur oprinting y	This Flow-based report	will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.							
N Application Vs. Network Performa	Default Terrelates									0
N Voice/Video Performance Vs. Net										
N Voice/Video Service Provider Perf.	NAME O		DESCRIPTION \$							
The second control of the control control of the co	Voice Analysis		This group of reports is useful for understanding enterprise-wide QoS performance for VoIP. It includes DSCP marking validation	n per site, QoS perf	formance infor	mation, and	1 Voice/Video p	erformance da	ta (jitter and p	acket loss), bas
	IWAN		This group of reports provides rapid understanding of Cisco IWAN performance and utilization. It includes an understanding of w	which service prov	ider a specific	class of tra	ffic is utilizing,	delay/loss/jitte	r measuremen	its by traffic cla
	Favorite Applications		This group of reports provides an understanding of the applications seen at a specific site, their performance (based on the Cisc	co Performance M	onitor), traffic (	class, and b	usiness releva	nce.		
	Apple Fastiane Applications		This group of reports provides an understanding of the Apple Fastlane applications seen at a specific site, their performance (ba	and on the Class	Derformance k	donitor) tra	fic class and	huelnase ralaus	000	

GENERAL SETTINGS		REPORT LIST		REPORT DETAILS		
Name		Application (Flow)	Fast 🗈 🔳	Report Name	Flow Type	
MY Application		Add New Report	+	Application	Basic Flow	
Presentation Mode				Report Description	Execution Type	
Standard				Enter report description	Time Series	
Footnote				Devices	Sort By	
Enter report group description				All WAN Devices	✓ Bit Rate	
Time Zone	🔽 DST			Interfaces	Business Hours	
(GMT-05:00) America/New York				All WAN Interfaces	✓ All Hours	
Time Range				Flex Search 👔	Bin Duration	Cannot be used with All Device
Last Hour				Ex.: site=Honolulu & wan & flow.app=http	× 1 Minute D	
Flex Search 🔞				Display Filter	-	
Ex.: site=Honolulu & wan & flow.app=http	×			No Display Filtering	Raw Flow Data     Due to the options selected, th	in report will utilize the
Display Filter				Direction	Raw Flow datastore (slower).	iis report win dunze the
Select Display Filter			C	Inbound and Outbound Combined		
Sharing Settings				r		
Email X						
Enter an email address or AD entity						

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

Templates Reports Hi	istory										
Q By Template Name		My Applic	ation					View Options ~	Share Download	Schedule Copy	Clo
efault Templates		Application	Plant		Directio	20		Bin Time	Range Show	(1br)	1
olce Analysis	0	Application	(Plow)		Directio	200		Contraction Contraction	"a "second address" "second at a fight	maker "the "articlemeder"	_
	0	Device: All WA Bin Interval: 1		erfaces Display Filter: No Display Fi	haring Direction: Inbound and Outb	ound Combined Flow Type: Basic Flow	Execution Type: Time Series Sort By: Bit	Rate Bin Duration: 1 Minute Start Time: Jul 22, 20	21 20 42 28 EDT (0MT-04:00) End Tim	w: Jul 22, 2021 21:42:28 EDT (GM7	104:00)
YAN	-	300									
avorite Applications	0									tp-sudio	
pple Fastiane Applications	0	Ĵ 200 -								ipfix snmp	
pple Fastiane Voice Analysis	0	X						Clicktan	d Drag to-	ftp Iannevagent	
AN Capacity Planning	0	100								sp mtp	
ite Network Performance Audit	0				/			<u>a</u> Zoo		ash	
oice/Video Performance Vs. Network	- 0	20.4	20.45 20.50	20.55	21.00 21.03	21:10	21.15 21.20	21.25 21.90 21.5		Total	
ite-to-Site Traffic Utilization Audit	0						and and the				÷.,
ervice Provider DSCP Audit	0	6	1 / 3 > 3+						Q Search		1
rack Single Site WAN Path Changes	0	Levend O	Application 0	Total Flows 0	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate C	Average Packet Rate 0	Peak Bit Rate 🗘	Peak Packet Rate 🗘	
oplication Vs. Network Performance			rtp-audio	54	20.79 MB	103,936	46.19 Kbps	28.87 pps	109.14 Kbps		68
pice/Video Service Provider Performa		-	ica	206	4.23 MB	63,542	9.40 Kbps	17.65 pps	23.52 Kbps		43
Not have beinger forten i cristing	-		ipfox	71	2.70 MB	2,884	6.00 Kbps	0.80 pps	53.94 Kbps		5
minution Comins Desuider Deformer			snmp	215	1.83 MB	6,876	4.07 Kbps	1.91 pps	13.61 Kbps		4
		-	πρ	168	1.61 MB	40,278	3.58 Kbps	11.19 pps	5.46 Kbps		17
pplication Service Provider Performan DWAN Application Service Provider Pe		-	lanrevagent	65	1.33 MB	11,841	2.97 Kbps	3.29 pps	8.24 Kbps		5
DWAN Application Service Provider Pe DWAN Application Vs. Network Perfor			sip	43	929.65 KB	7,169	2.07 Kbps	1.99 pps	8.02 Kbps		.9
DWAN Application Service Provider Pe			and the second se	51	515.40 KB	12,885	1.15 Kbps	3.58 pps	1.41 Kbps		24
WAN Application Service Provider Pe WAN Application Vs. Network Perfor	N. 0	-	nntp		225.78 KB	2.835	0.50 Kbps	0.79 pps	1.25 Kbps		1
WAN Application Service Provider Pe OWAN Application Vs. Network Perfor OWAN Voice/Video Performance Vs. I OWAN Voice/Video Service Provider P	N. 0	-	ospf	389	220.76 NB						
WAN Application Service Provider Pe WAN Application Vs. Network Perfor WAN Voice/Video Performance Vs. M	N. 0	_		389 27		2,120	0.47 Kbps	0.59 pps	13.62 Kbps		16

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

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

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

- 6. Hide a metric by clicking on the Legend.
- 7. Re-sort by clicking on the Sort Arrows.

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

<pre>spect vertice is an intervert vertice is an inter</pre>																
Templates Reports History																
By Template Name	ly Application										View Options	~ S	Share Dov	vnload		ру
															10	
- testuis																
Devi		erface: All WAN Inter	faces Display Filter: 1	Io Display Filteri	ing Direction: Inbound an	nd Outbound Combine	ed Flow Type: Basic Flow	Execution Type: Time Se	eries Sort By: Bit	Rate Bin Duration: 1	Minute Start Time:	Jul 22, 2021 2	20:42:28 EDT (0MT-04	1.00) End Time	e: Jul 22, 2021 21:42:28 ED	T (0MT-04:00
	300														e rtp-audio	
Eastiana Applications	200												e	a	ica ipfix	
															ftp lanrevagent	
	100														elp mntp	
	Image: Sector of Yord       My Application         Application (Thor)       Image: Sector of Yord         Image: Sector of Yord       The Application (Thor)         Image: Sector Photoe Preformance (Y)       Image: Sector of Yord         Y Application       Image: Sector of Yord         Image:											ssh Total				
	21:22:52	21:23:30	21:24:00	21:24:30	21:25:00	21:25:30	21:26:00	21:26:30 21	:27:00	21:27:90	1:28:00	1.28:30	21:29:00	21:29:26		
	< Page 1 / 3 >>												Q Search			
	Legend C Applicat	n Ó.	Total Flows O		Total Bytes O	Total Par	ckets O	Average Bit Rate O		Average Packet	Rate O		Peak Rit Rate 🗅		Peak Packet Rate O	
				54					46.19 Kbps					109.14 Kbps		
-	ipfx															
N Application Service Provider Pe																
		-1														
		TIL.														
	ospf															
Application Service Provider Perfo ()	ssh ssh			27	210.8	89 KB	2,120		0.47 Kbps		0	59 pps		13.62 Kbps		
Number         Numer         Numer         Numer <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>																
	RT					×										
Name	ORT					×										
Name MY Application	IRT					×										
Name MY Application Run Report	RT															
Name MY Application Run Report	PRT															
<pre>spect</pre>																
Name MY Application Run Report Hourly () Reports will be o	<pre>verify intermed intermed</pre>															
Name MY Application Run Report Hourly () Reports will be o Schedule Ends																
Name MY Application Run Report Hourly (j) Reports will be of Schedule Ends Never																
Reports  require requi	the hour	for the p	revious		DST											
Name MY Application Run Report Hourly   Reports will be o Schedule Ends Never Time Zone	created on	the hour	for the p	revious		DST										
Name MY Application Run Report Hourly  Reports will be o Schedule Ends Never Time Zone	created on	the hour				DST										
Name MY Application Run Report Hourly   Reports will be o Schedule Ends Never Time Zone	created on	the hour				DST										
Name MY Application Run Report Hourly  Reports will be o Schedule Ends Never Time Zone	created on	the hour				DST										

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

≡ LiveAction		New Feature: A 0 10 0 0 A 2 (-)+ 0+ 4 amm-
View Reports		11 View Schedua Count Magnet
C, By Template Name	listory	My Application View Options ~ Share Download Schedule Copy Cose
Default Templates		Application (Flow)
Voice Analysis IWAN	0	Descent All INIX Devices Implant All NAXI Institutes Display Filter No Display Filter No Display Filter No Display Filter Ad Display Filter No Display Filter Ad Display Filter No Display Filter No Display Filter Ad Display Filter No Display Filte
Favorite Applications	0	300
Apple Fastiane Applications	0	
Apple Fastiane Voice Analysis	0	d - fo
WAN Capacity Planning	0	20 mm
Citis Mahandi Dadarmana Audit		ee ool

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

≡	LiveAction 💌		New Features!	<b>▲</b> 0 <b>■</b> 0	• 0 🧍	<b>0</b> {-} -	0.	•	- 4	🛔 admin 👻
View	Schedule							13	Viev	w Reports
Q	By Report Name	Reports For: Aug 1st - Sep 11th, 2021					< Au	g 2021	>	Today
Sche	duled Groups Hourt						S M	ти	ν т	F S
MY A	pplication 🖂 😭 🗓						1 2	3 4	4 5	6 7
_	3						8 9	10 1	1 12	13 14
							15 16	5 17 1		

Lets have a look at creating a Custom Report

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

ENERAL SETTINGS	REPORT LIST	REPORT DETAILS	
ame	Please choose report type		
Enter report group name	Add New Report	+ Top Reports	
resentation Mode		LiveNA	
Standard	×	A = Flow	
potnote		Address	×
Enter report group description		Analysis	~
		AnyConnect	~
haring Settings		Application Performance (AVC)	~
nail 🔀		Applications	~
Enter an email address or AD entity		Firewall	~
le Format		LiveAgent	~
Send PDF Send CSV		Miscellaneous	~
OF Row Limits	_	Network	~
	~	Network Users	~
ustom Logo 🚯		PfR	~
No Custom Logo	<u>×</u>	Boos	^
		Application DSCP Audit	
		DSCP	
		Liear Eiter DCCD Audit	

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

/iew Reports													View Schedule	Creat	te Report
Templates Reports Histor	У														
Q By Template Name		Application	DSCP Audit	, Last Fifteen Minutes						View Options ~	Share	Download	Schedule	Сору	Close
fy Templates		Application D	SCP Audit (Flo	w)											1
ly Application		Device: All MAN	Desinan Interd	ane All WAN Interfaces Di	alas Elbar No Dianlas	Eductors Binartine Inhound and C	Schound Combined Flow Tene	Basic Dirac - Execution Tene To	ne Series Sort By: Bit Rate Bin Duratio	er Acco Start Time: 31/22	2021 21 20 26 27	T (SMT.04.05) End Tim	ar 3,1 22 2021 21 54 56 F	DT (DATO) OF	6
Default Templates		Bin Interval: 1 m													
loice Analysis	0												NV/rtp-sudio/4	8 (EF) 18 (EF)	=
WAN	0	J 200 -											<ul> <li>NV/ida/0 (BE)</li> <li>HQ/ida/0 (BE)</li> <li>HQ/ida/0 (BE)</li> </ul>	-10 (05)	
avorite Applications	0	-	1										HQ/lpfu/0 (BE)		
upple Fastiane Applications	0	100 III											HQ/anrap/0 (8 HQ/ftp/0 (8E)		
lople Fastlane Voice Analysis	0	. 🛋				and have a sub-sure			Anne and the second				NY/larvevagen	1/0 (BE)	
VAN Capacity Planning	0	21:40:00	21:41	00 21,42,00	21:43:00	21:44:00 21:45:00	21.46.00 21.471	21.46.00 3	149.00 21.50.00 21.5	1.00 21:52:00	21:53:00	21.54.00 21.54	1.26		
ate Network Performance Audit	0	< < Page 1	14 3 20								Q S	earch			
/olce/Video Performance Vs. Network	0	Legend C	Cite A	Application ©	DSCP C	Total Flows 🗘	Total Bytes C	Total Packets C	Average Bit Rate 🗘	Average Packet Rate 🗘		Peak Bit Rate O	Peak Pack	of Ento A	
lite-to-Site Traffic Utilization Audit	0	Leyena o	NY	rtp-audio	46 (EF)	14	5.40 MB	27,009	48.02 Kbps	Arelage Facket Nate 🖓	30.01 pps		4 Kbps	er nate 🥹	32 pp:
Service Provider DSCP Audit	0	-	HQ	rtp-audio	46 (EF)	14	5.37 MB	26,835	47.71 Kbps		29.82 pps		8 Kbps		33 pp
Irack Single Site WAN Path Changes	0	-	NY	ica	0 (BE)	56	1.15 MB	17,290	10.25 Kbps		19.21 pps		8 Kbps		20 pp
opplication Vs. Network Performance	0	-	HQ	ica	0 (BE)	56	1.15 MB	17,213	10.20 Kbps		19.13 pps	10.9	6 Kbps		20 pp
/olce/Video Service Provider Performan.	0	-	HQ	lanrevagent	0 (BE)	26	547.74 KB	4,483	4.87 Kbps		4.98 pps	5.6	0 Kbps		5 pp
application Service Provider Performan	0	-	HQ	lpfix	0 (BE)	16	535.01 KB	667	4.76 Kbps		0.74 pps	54.0	3 Kbps		5 pp
OWAN Application Service Provider Pe.	0		NY	sip	0 (BE)	19	422.91 KB	3,032	3.76 Kbps		3.37 pps	5.5	7 Kbps		5 pp
DWAN Application Vs. Network Perfor_	0		HQ	snmp	0 (BE)	52	413.23 KB	1,608	3.67 Kbps		1.79 pps		4 Kbps		2 pp
OWAN Voice/Video Performance Vs. N.	0	-	HQ	ftp	0 (BE)	28	271.40 KB	6,785	2.41 Kbps		7.54 pps		0 Kbps		8 pp
DWAN Voice/Video Service Provider P_	0		NY	lanrevagent	0 (BE)	9	166.08 KB	1,911	1.48 Kbps		2.12 pps	2.5	0 Kbps		3 pp
WAN Application Vs. Network Performa.	0														
WAN Application Service Provider Perfo.	0														
WAN Voice/Video Performance Vs. Net.															

### Lab 1.5: Enable / Customize Alerts

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

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

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

Lab Steps:

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

	QoS Class Drop (1	Device, Interface	Warning	Qos Class VOICE Drop Rate > 20 kbps for at	Web UI
	QoS Interface Drop (1	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
_		A	1. Orikinal		

3. Click on QoS Class Drop.

QoS (	Class Drop				×
Enable On Thi Severit	] is alert may contribute	e to status	of an Interface, I	Device, and/or	Site.
	arning				~
	Geverity for this alert n When the severity is i <b>holds</b>				d in the
Auto	omatic Resolution Tin	ne* 🚯			min
	Catch All Threshold All non-specified C Drop Rate * 0		For at Leas	it *	min
	Qos Class * VOICE Drop Rate * 20	kbps	For at Least *	min	
	Qos Class * VIDEO Drop Rate *		For at Least *		
٨٩٩	50 Specific QoS Class A	kbps	> 1	min	
Sharir		iert			

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

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

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

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

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



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

LiveAction 💌								New Features!	▲ 5	• • •	<b>\$</b> 0	{} ~	Ø •	o
Management 🖗													Maintenance M	lode View
				Liv	eNX Aler	rts								
	Click this	s boxito												
nable Disable	CICKUI										Q Searc			
ALERT TYPE	enable a	II Alerts	ó	SEVERITY	0	ENABLED	0	THRESHOLDS		SHARING				
	*						*							
And Type		All	~	All	~	All	~	Thresholds		Sharing				
IPSLA Voice/Jitter Test		Network		A Critical		~		Total Test Errors > 3 Errors for at least > 0 minutes		Web UI				
Line Card Operational State		Device, Interface		Multiple				Multiple		Multiple				
LiveNX CPU Utilization		System		Critical		~		Local/Server >= 40 % for at least > 0 minutes		Web UI				
LiveNX Disk Utilization		System		Critical		~		Local/Server ≻= 60 % for at least > 0 minutes		Web UI				
LiveNX Memory Utilization		System		A Critical		~		Local/Server >= 40 % for at least > 0 minutes		Web UI				
LiveNX Node Connectivity	0	System		A Critical		~		for at least > 0 minutes		Web UI				
Low WAN Interface Utilization	0	Device, Interface		Multiple				Multiple		Multiple				
Power Supply Operational State		Device, Interface		Multiple				Multiple		Multiple				
QFP Throughput Level		Device, Interface		Multiple				Multiple		Multiple				
QoS Class Default Drop	0	Device, Interface		Critical		~		Drop Rate > 0 kbps for at least > 0 minutes		Web UI				
QoS Class Drop	0	Device, Interface		<ul> <li>Warning</li> </ul>		~		Multiple		Web UI				
QoS Interface Drop	0	Device, Interface		<ul> <li>Warning</li> </ul>		~		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	0	Network		Multiple				Multiple		Multiple				
Spanning Tree Topology Change		Network		Critical		~		for at least > 0 minutes		Web UI				
Voice Traffic Classification and Marking		Application		Critical		~		for at least > 0 minutes		Web UI				
Voice, Video Applications Performance		Application		Critical		~		Multiple		Web UI				
Voice/Video Performance - Jitter Avg	0	Application		Critical		~		Jitter Avg >= 30 ms for at least > 0 minutes		Web UI				
Voice/Video Performance - Jitter Max	0	Application		Critical		~		Jitter Max >= 60 ms for at least > 0 minutes		Web UI				
Voice/Video Performance - Packet Loss	0	Application		Critical		~		Packet Loss ≻= 1 % for at least > 0 minutes		Web UI				
VRRP Operational State		Network		Multiple				Multiple		Multiple				

## Lab 1.6: Add a User Account

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

Lab Steps:

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

≡	LiveAction 💌							New Features!	• •	•••	<b>\$</b> 2	{-} -} -	0 -	۰۰	💄 admin •
Alert	Management <sup>©</sup>												Maintenance		
				LiveN	X Alerti	8									agnostica
Er	Disable										Q, Sea	rch	- (	User Mana;	Lu,
	ALERT TYPE	CATEGORY	0	SEVERITY	0	ENABLED	C THRESHOLDS		SHARE	15				Livet	r Managemer
	Alert Type	All		All		All	Thresholds		Sha	ing					
	Application Performance - App Delay	Application		Multiple			Multiple		Multip	le					
	Application Performance - Network Delay	Application		Multiple			Multiple		Multip	le					

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

ADD NEW USER		×
1 Authentic	ation Type	2 Settings
	Authentication Type	
	Select Authentication Type  V LOCAL	
	LOCAL In Inc.	
	RADIUS	Cancel Next Step
	TACACS+	
	SSO	

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

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

7. Click Add User.

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

## Lab 1.7: View and Navigate System Diagnostics

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

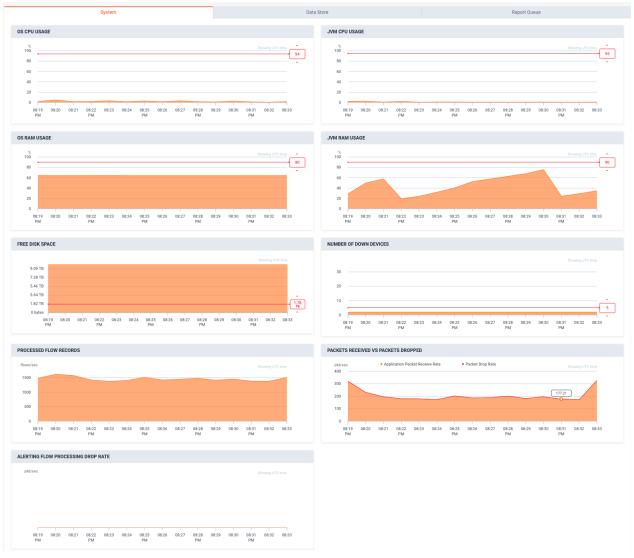
Lab Steps:

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

≡ Live	Action										New	Features	A0 80 •	0 🐥 2	{-} - 6	🗸 🔹 🕹 admin
System Diagno	ostics > Node Information															Settings
Local/Server																System Disgnostics
C LOCAL		ş	itatus: Ok Conforr	mance: Ok	Current Deplo	oyment: Custom IP: Local									Last Update	User Management
CPU Model	9 QEMU Virtual CPU version 2.2.0	OS KAM JVIN KAM DISK KT						N/A	DEVICES Total	5 Configura	ble	5 Loading	LiveNX Server 0			
Cores	8	JVM Util.	1.3 %	Used	7.08 GB	Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5 Down		0 Last Days Flow Rate	
_	10 System Data Store										Reg	port Queue				
OS CPU	USAGE				J	JVM CPU USAGE					OS RAM USAGE					
80 - 60 - 40 - 20 -	15 01-05 01-05 01-05 02-05 02-05 201-05 01-05 01-05 02-05 02-05 201 201 201 201 201 201 201 201 201 201	45 -														
JVM RAI	M USAGE				F	FREE DISK SPACE					NUMBER OF DOWN	DEVICES				
60 60 40 20 0 0 0 0 0																
PROCES	SED FLOW RECORDS				F	PACKETS RECEIVED VS PACKE	TS DROPPED				ALERTING FLOW P	ROCESSING D	ROP RATE			
forsite:				Browing UTO time		Application 25 15 5 5	Pecket Receive Rate	'ecket Drop Rate		Beening L/TC Bee	phtyset					

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

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



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

≡ LiveAction <sup>•</sup>	NX										Nex	w Features!	۵ 🔺	• • • •	<b>a</b> 2	{-} -	0 -	0- 4	admin 🕶
System Diagnostics > Node Info	rmation																		
Local/Server V																			
C LOCAL/SERVER		Status: Ok Confor	mance: Ok	Current De	eployment: Cu	ustom IP: Local										Last Updi	ste Time: 7/	22/2021 10:09:0	01 PM
CPU Model QEMU Virtual CPU	version 2.2.0 OS Util.	1.3 %	OS RAM	15.64 GB		JVM RAM	8.00 GB	DISK Total	499.76 GB	RTT Server to Node	N/A	DEVICES Total	5	Configurable		5 Loadir	Ng	0	
Cores 8	JVM Util.	1.3 %	Used	7.08 G8		Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5	Down		0 Last D		0.216 fps	
	System			_				Data Store						Repor	t Queue				
LONG TERM STORE SIZE					FLOW STO	ORE SIZE					LONG TERM STOP	RE GROWTH RA	TE						
4.77 MB 3.81 MB 2.84 MB 0.33 MB 0.35 M			Daning 177 day		28.81 MB 22.84 MB 19.27 MB 14.21 MB 9.54 MB 4.77 MB 0.34 MB			1 2 1 2 1 24 27 24 25 10	H 12 12 14 14 19 19	Denning UTC des	0.58 KB 0 bytes -0.58 KB 201 201	24 24 25 27 28 1	28 90 04 0 24	0 00 04 04 04 0	27 08 09 10 11	12 12 14 58 19		20 21 23 JM	
FLOW STORE GROWTH RATE					SNMP STO	ORE SIZE					ALERT STORE SIZ	E							
3.64 498 3.05 498 4.05 4.05 498 4.05 4.05 4.05 4.05 4.05 4.05 4.05 4.05	8 19 19 19 19 19 19 19 19 19 19 19 19 19	11 12 12 14 19 19 17	Renig 172 free									28 28 27 28 28							
SNMP STORE GROWTH RATE					ALERT ST	ORE GROWTH RATE													
97.66 KB 0 bytes -0.70 MB			Dentra University		5.89 KB 2.91 KB 1.95 KB 0 bytes -1.95 KB 0.91 KB 0.91 KB					Sharing 1772 894									

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

QEMU Virtual CP 8	PU version 2.2.0 OS Util.	0.5 RAM	JVM RAI 15.64 GB Commit		DISK	RTT	DEVICES		
		1.3 % Amount	15.64 GR Commit						
8						Server to Node N/A	Total 5 Configurable		0
		1.3 % Used	7.08 GB Used	1.69 GB	Free 482.75 GB	Node to Server N/A	Active 5 Down	0 Flow Rate	0.216 fps
	System			Data Sto	ore		Report Queue	1	
								-	
rt Queues 😷									
Cancel All									
C REPORT NAME	C REPORT ID	C REPORT	STATE 0	USER NAME O	PRIORITY	QUEUE NAME	0 QUEUED TIME	O RUNNING TIME	0
Report name	Report id	All	~	User name	All	~			
Report name	Report id	All	v	User name	All	~			
				No Da	ıta				

## Lab 1.8: Support and Troubleshooting

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

- EiveAction<sup>™</sup>
   C LOCAL/SERVER Amount Committee 8.00 GB Total Total OS Util. 499.76 GB Loading Last Days Flow Rate Used Used Free 482 75 GR Active Down ues 😋 Report Que
- 1. Navigate to the **Settings** menu.

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

≡ LiveAction <sup>™</sup>						0 🐥 2 {-} = 🖓 = 🕐	🕶 🚢 admi
Settings							
Q Search							
Configuration	LOGS						
Data Source Management	LiveNX Log Level						
Data Store	INFO	✓ Set					
Device Entity Page Reports							
Email Configuration	Manage Logs						
Integrations ~	Get LiveNX Logs Delete						
Licensing ^	NODE NAME	C SOURCE C	FILE PATH C	COLLECTION START TIME O	STATE C	SIZE	O DOWNLOAD
License Configuration	Node name	Source	File Path	Collection start time	State	Size	
iveNA Configuration							
lounted Data							
iodes							
roperties ~			1	No Data			
haxy							
leports ~							
ecurity ~							
ingle Sign On NMP Trap							
lyslog							
roubleshooting							
CPU Profiling							
Heap Dump							
Logs							
Packet Capture Upload History							
User Activity Tracking							
lpdates							
lieb Lii Data Store							

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

3. Click Get LiveNX Logs.

#### GET LOGS

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

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

	Select All	Select None	
Local/Server			
		Cancel	Get Logs

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

4. Once logs are generated, you can Download the zip file. Once downloaded locally, the logs can be shared with the LiveAction support team.

×

5. Navigate to Packet Capture under Troubleshooting.

≡ LiveAction <sup>™</sup>	x						{-} • O • O • & «
Settings							
Q. Search							
		PACKET CAPTURE					
Configuration	- 11						
ata Source Management	- 11	Capture Packets Delete					
ata Store	- 11	O NODE NAME	0 FILE NAME	O COLLECTION START TIME	C STATE	C SIZE	C DOWNLOAD
evice Entity Page Reports		Node Name	File Name	Collection Start Time	State	Size	
ail Configuration		Node Name	File Name	Collection start 1 ime	State	Size	
egrations	~						
censing	^						
License Configuration							
License Expiration Notification				No Data			
eNA Configuration							
ounted Data							
odes							
roperties	~						
DXY							
ports	~						
ecurity	~						
ngle Sign On							
NMP Trap							
slog							
roubleshooting	~						
CPU Profiling						la la	
Heap Dump							
Logs	_						
Packet Capture							
Upload History							
User Activity Tracking							
odates							

6. Click Capture Packets.

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

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

Interface*		Device	
eth0		Other	~
Node		Protocol	
Local/Server	$\sim$	None	~
Host		Duration*	
eg: x.x.x.x			Sec
Port			
2055			
		Cancel	Capture Packets

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

×

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

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

## Lab 2

Lab 2: The LiveNX Client

## Lab 2.1: Launch the LiveNX Client

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

A Mac version is also available for install if needed.

Lab Steps:

1. Launch the LiveNX Client.

DIAGRA	Μ	
Client Lo	gin	$\times$
Liv	veNX	
Username:		]
Password:		]
For first time	e use:	
Userna	me and password are "admin"	
Click "(	Configure" to setup server address	
Configu	re OK Cano	el

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

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

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

Clie	ent Login		×
Server	Configuration		×
Server 9	iettings		
Server:			$\sim$
Port:	7000		
		Save	Cancel
	Configure	ОК	Cancel

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

Password: Student (note the capital S)

Client Lo	ogin X
Liv	veNX
Username:	admin
Password:	•••••
For first tim	e use:
Userna	me and password are "admin"
Click "	Configure" to setup server address
Configu	re OK Cancel

6. Click OK

The Client will launch...



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

Image: Second	Manage De Expa QoS Flo	LAN Tools Reports Help						
Relative Geologicalities 19 Geologicalities 20 Geologicalities Contregeng By Daplay Filer Color (Including) Contregeng By Daplay Filer Color (Including) Con		' 🖳 + 🔍 🤍 Table 🛟 Re	fresh All Flow Types V Current Time	e v Current Polling Interval	V 😽 No Display Filtering	✓ Top 50 <	📑 Display Filter Colors 🗸 🗸	
Gestifiend: Gesti	Search Example	(site = Honolulu   site = Chicago) & vi	ran & flow.app = webex-meeting					×
Gestifiend: Gesti								
Gestellmard: egestellmard: gestellmard: gestellmard: G	ranch1-LA GrabitEthemat1							
GadeBrind GadeBrindt ea GadeBrindt GadeBrindt GadeBrindt GadeBrindt GadeBrindt GadeBrindt GadeBrindt Cor Mapping By Daplay Flar Color (Remaining) From Fingh Dabled Itam (Remaining) From Fingh Dabled Itam	GigabitEthernet2							
GgeldBiftwrd: Rig GgeldBiftwrd: G								
P2 BigeNtBrendt BigeNtBrendt BigeNtBrendt Corr Mepping By Diplay Filer Color ■ (Memping) ■ No. Copying By Diplay Filer Color ■ (Memping) ■ (Memping)	GigabitEthernet1				HQ-MC 198.18.129.23	)		
Digetetitierendi Gigetetitierendi Gigetetitierendi Gigetetitierendi Color Magning By Digbury Filter Color (Rewarding) Filter Filter Digetetitieren A. Actophysical M. A. Actophysical								
Vic Ggobbithmed Color Mopping By Daplay Filar Color	GigabitEthernet1				for the			
GgeldEthened:								
Color Magning By Dipley Filer Colors Mexanine Mexa							0	
Color Mapping By Otoplay Plar Colors Resulting A free reling Databati Ion We want with the second					1000		Local	
Color Magong By Diplay Filer Color				HQ-B2 198.18.129.25	91	HQ-B	1 29.24	
Color Hogong By Diglay Filer Colors ■ (kenning) ■ Free Folip Dabled Ion ● Free Folip Dabled Ion ● Folip Dabled Ion ● Naconfigured			102052024					
Color Magoling By Diplay Filar Colors Color Magoling By Diplay Filar Colors						*	w	
Color Hopping By Diplay Filter Colors								
Color Mapping By Dipulay Filar Colors								
Color Mapping By Dipby Filter Colors Color Mapping By Dipby Filter Colors Color Mapping Databal Ison A From Filling Databal Ison A From Filling Databal Ison A Fort Policy Colors Market Bandward State Market Bandward Marke							100.04.0.004	
Color Mapping By Dipby Filter Colors Color Mapping By Dipby Filter Colors Color Mapping Databal Ison A From Filling Databal Ison A From Filling Databal Ison A Fort Policy Colors Market Bandward State Market Bandward Marke								
Color Mapping By Digalay Filter Colors (Remaining) From Volting Databild Icon V Not configurad								
Color Mapping By Dapity Filter Colors								
Color Magong By Dipley Rar Colors  Color Magong By Dipley Rar Colors  Color Magong By Dipley Rar Colors  A free veloging Databation  A free ve								
(Semaining)     A Four Poling Disabled Icon     A Four Poling Disabled Icon     A Actorpied     Accordgand			× • • •					
A For-Foring Outside Icon     Such Applied     Vice Configurad			Branch1-LA 198.19.1.1					
C A.C. Applied Net Configured			Branch1-LA	02 VOC641684				
4 Not configured	(Remaining		* * Branchi LA * 1981.19.1.1	02 VOC641684				
	(Remaining     A Flow Polin	) Disabled Icon	* * Branchi LA * 1981.19.1.1	02 VOC641684				

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

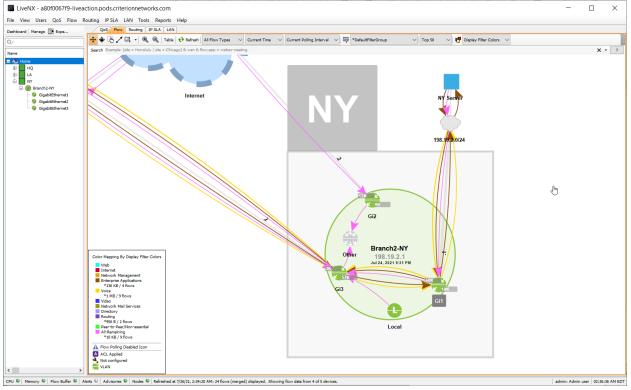
## Lab 2.2: Explore the LiveNX Client

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

Lab Steps:

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

#### DIAGRAM



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

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

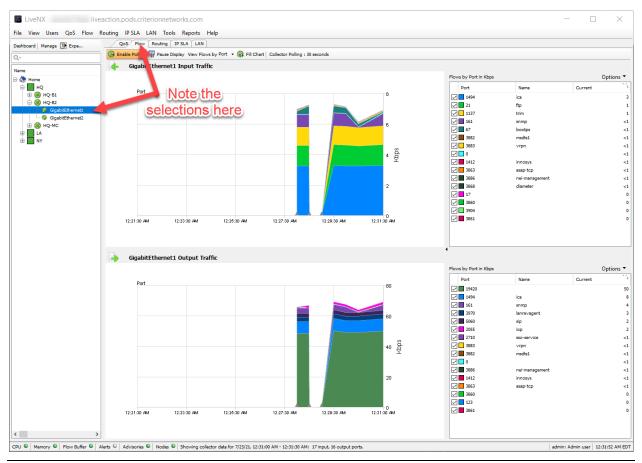
4. Note the 5 Module Tabs to the top-left of the Topology Pane.

#### DIAGRAM

File View Users QoS Flow	Routing IP SLA LAN Tools Reports Help
Dashboard Manage 🗈 Expa	Qos Flow Routing IP SLA LAN
Q,-	🕂 🗣 🖑 🖍 🗐 🔹 🍭 🔍 Audit
Name	
🖃 🟠 Home	
HQ	
LA LA	

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

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



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

# Lab 3

Lab 3: Configuring Devices

## Lab 3.1: Add Device

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

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

Lab Steps:

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

·≡ LiveAction <sup>~</sup>	NX																[	New Feature	tsl 🔺	a 🗖	• •	۵ 🐥	{} -	· 0-	٥-	& adv	nin <del>-</del>
👫 Main																CS	(Import/Ex	port ~	Credenti	ial Store	View	Devices	Add No	on SNMP Devic	× .	iscover Device	
	My Device	s (5)					My Ir	nterfaces (11)						Discovered	Devices (0	3)							Autodiscov	ery (0)	•		_
🚠 Topology																											
	Configure	D	elete Red	iscover Im	terfaces																٩	Search					
≣i Stories	EVICE STATE	0	P ADDRESS	VEND	on O	MODEL C	NODE	sitte	0 INTE	ERFACES C	HARDCODED SA 0	POLL	c	QOS	0	FLOW	0	IP SLA	0	ROUTING	0	LAN	0	14.05	0 10	TERVAL	c
Lat Reports	Al	-	IP Address	All	~	Model	Node	Site				All	×	All	×	All	~	All	~	All	×	All	×	6.21		All -	×
	lo ol		198.18.129.23	Cisco		ciscoCSR1000v	Local/Server	HQ		1		~			/		~									30 secor	inds
R. LiveNA	ap .		198.18.129.24	Cisco		ciscoCSR1000v	Local/Server	HQ		3		~			·		~									30 secor	
	ap.		198.19.1.1	Cisco		ciscoCSR1000v	Local/Server	LA		3		~			/		~									30 secor	
Configure	ap.		198.18.129.25 198.19.2.1	Cisco		ciscoCSR1000v ciscoCSR1000v	Local/Server	HQ		3		~			·		~ ~									30 secor	
Alert Management Application Management O/D Pulling Porket Management Filter Management Site Management																						′					

#### 3. Click Discover Devices.

1. What to scan	5	2. SNMP Settings		- 0	3. Node	
SPECIFY IP RANGES						
198.19.2.1			Choose a sit	e	~	
Add More						
SPECIFY SEED DEVICE TO SCAN						
IP address				Hops		
						Save & Next
						Save & Mexi

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

Device Management		Credential Store View Devices	Add Non SNMP Device Discover Devices
My Devices (2)	My Interfaces (4)	Discovered Devices (0)	(?) Autodiscovery (3)
DISCOVERY LOGS:	4/5		

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

Add A	I Devices Edit										Q Search		
0	DEVICE	SERIAL	0	IP ADDRESS	0	VENDOR	\$ MODEL.	>	NODE	INTER	FACES 🗘	HARDCODED SAMPLE RATIO	
	Device	Serial		IP Address		Vendor	Model		Node	Inte	rfaces		
	Branch2-NY	00000000	21	198.19.2.1		Cisco	ciscoCSR1000v		Local/Server	6			

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

#### 11. Click Select Interfaces.

0	NAME 🗘	DEVICE 0	LINE RATE (Kbps)	IP ADDRESS 🗘	LABEL	٥	INPUT CAPACITY (Kbps) 💲	ОИТРИТ САРАСІТУ (КЬ 🗘	WAN/XCC	N ¢	SERVICE PROVIDER	٥	TAGS 🗘	DESCRIPTION
	name	All V	line rate	ip address	Label		Input Capacity	Output Capacity	All	~	All	~	Tags	description
	GigabitEthernet1	Branch2-NY	1000000	198.19.2.1	Branch2 LAN				WAN		Branch2 LAN			Branch2 LAN
•	2 abitEthernet2	Branch2-NY	2000	100.64.2.2	Internet				WAN		Internet			Internet
	GigabitEthernet3	Branch2-NY	1000	10.255.2.2	MPLS				WAN		MPLS			MPLS
	Loopback0	Branch2-NY	8000000	10.0.2.1										
	Null0	Branch2-NY	10000000											
	VoIP-Null0	Branch2-NY	10000000											

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

#### 13. Click Add Selected.

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

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

	LiveAction <sup>®</sup>																			
wice N	Management ®											CSV Import/Ex	cred	ential Store	View [	Devices	Add Non SNMP D	evice	Discover D	levices
		My Devices (				My Int	terfaces (10)				Discovered Devices	0)				(7) Auto	odiscovery (0)			
Edit	Refresh List	Configure	Delete Redis	cover Interfaces											Q	Search				
٥	DEVICE 0	DEVICE STATE 0	IP ADDRESS 0	VENDOR 0	MODEL C	NODE O	SITE O	INTERFACES C	HARDCODED SA 0	POLL 0	qos C	FLOW Ô	IP SLA	CROUTING	0	LAN	C TAGS	0	INTERVAL	
	Device	All ~	IP Address	All ~	Model	Node	Site			All v	All ~	All ~	Al ~	All	~	Al	✓ Tags		All	
	HQ-MC	Up	198.18.129.23	Cisco	ciscoCSR1000v	Local/Server	HQ	1		~	~	~							30 1	secor
	HQ-B1	Up	198.18.129.24	Cisco	ciscoCSR1000v	Local/Server	HQ	2		~	~	~							30 r	secon
	Branch1-LA 🕺 💥	Up	198.19.1.1	Cisco	ciscoCSR1000v	Local/Server	LA	2		~	~	~	~						7	1 minu
	HQ-82	Up	198.18.129.25	Cisco	ciscoCSR1000v	Local/Server	HQ	2		~	~	~							30 r	secor
	Branch2-NY	Up	198.19.2.1	Cisco	ciscoCSR1000v	Local/Server	NY	3		~	~	~							30 /	secon

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

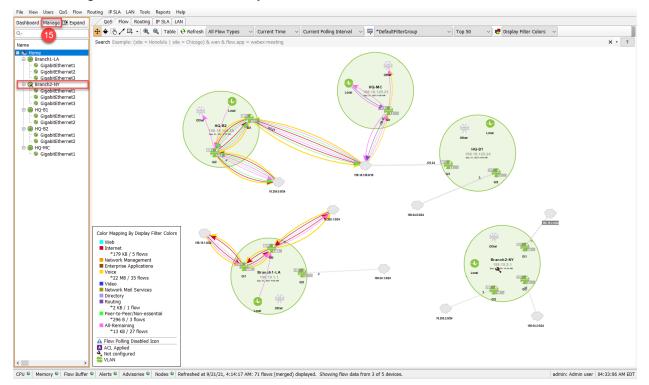
### Lab 3.2: Manage & Configure Devices

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

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

Lab Steps:

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



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

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

Devic	ce Management													>
Filter	r by:					Filter	(	Clear	]					
Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routi	LAN*	Interval	Status
	Branch1-LA	198.19.1.1	Cisco	ciscoCSR1000v	Local		$\checkmark$		$\checkmark$				10 sec	Configured
	Branch2-NY	198.19.2.1	Cisco	ciscoCSR1000v	Local	18							1 minute	9 t Config
	HQ-B1	198.18.129.24	Cisco	ciscoCSR1000v	Local	-	$\checkmark$	$\checkmark$	$\checkmark$				10 sec 🗸	Configured
	HQ-B2	198.18.129.25		ciscoCSR1000v	Local		$\checkmark$	$\checkmark$	$\checkmark$				10 sec $\sim$	Configured
	HQ-MC	198.18.129.23	Cisco	ciscoCSR1000v	Local		$\checkmark$	$\checkmark$	$\checkmark$				10 sec $\lor$	Configured
⊧ LAN p	olling occurs every 15 minu	utes											Numb	er of Devices: !
	Configurations					⊂Global Device	a Sattin	00						
		Configure QoS, Fl	ow and I				_	-						
2				d click the configure	button.	Edit	De	fault SNI	MP Setti	ngs				
	Remove	Remove selected d	evice(s).			Edit	De	fault CLI	Monitor	ing Settin	igs - Not	Set		Clear
	Add To Group	<new group=""></new>			~	Edit	De	fault CLI	Configu	ration Se	ttings			Clear
F	Remove From Group	Removes selected	devices fro	m their groups										
	Edit Groups	Edit the groups												
											_	-	20	

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

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

22. Step1: Use the Default SNMP... Click Next

23. Step2: Use My Default Configuration CLI... Click Next

Configure Cisco Features for -	Branch2-NY.dcloud.cisco.com (198.19.2.1) X		
Configure Cisco Features for - Steps      Device Connection Information      Cut Settings (Configuring)     Cut Settings (Monitoring)     Select Interfaces     Select VAINs     Select Treatures     Features     Features     Enable Polling     Review Configuration     Device Updated	Branch2-NV. deloud.cisco.com (198.19.2.1)     X       Device Connection Information	Information         are indicated with an asteris           2. CL1 Settings (Configuration CLI Connect (Monitoring)         Configuration CLI Connect Enter Command Line Int (Monitoring)           3. Selet Interfaces         Add as monitor only	formation used for configuring these devices. Required fields (*).  Ion Settings  arface (CLJ) connection settings used to configure these devic device for non Cisco and unsupported Cisco OS (IOS, IOS-XE guration CLI connection settings) Edit  args for this device  breve  br
		8. Review Configuration 9. Device Updated 9. Device Updated 9. Also use these	ice

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

		Validation Details		×
		Validation results for the current device:		
Configure Cisco Features for - B	ranch2-NY.dcloud.cisco.com (198.19.2.1) X	Test	Status	Description
configure elseo reacares for b		SNMP connection	•	Succeeded 🔺
Steps	CLI Settings (Monitoring)	SNMP access	•	Succeeded
1. Device Connection	Specify the CLI connection information shared by all users. This information will only be	CLI configure connection	$\odot$	Skipped
Information	used to monitor this device. Required fields are indicated with an asterisk (*).	CLI configure login	$\odot$	Skipped
2. CLI Settings		CLI configure enable password	$\odot$	Skipped
(Configuring)	Monitor-only CLI Connection Settings	CLI monitor connection	$\odot$	Skipped
3. CLI Settings	Enter Command Line Interface (CLI) connection settings used to monitor this device.	CLI monitor login	$\odot$	Skipped
(Monitoring)	O Use the default Monitor-only CLI connection settings Edit	CLI monitor enable password	$\odot$	Skipped
<ol> <li>Select Interfaces</li> </ol>		Serial number validation	$\odot$	Skipped
5. Select VLANs	Use the previous page connection settings	Model supported	•	Succeeded
6. Select Features	O Enter connection settings for this device	IOS supported	٠	Succeeded
7. Enable Polling		NBAR capable	•	Succeeded
8. Review Configuration	Connection Type SSH V Port* 22	NBAR2 capable	•	Succeeded
5	User name on Device	NetFlow collector configure supported	•	Succeeded
9. Device Updated	Password on Device*	Flexible NetFlow supported	•	Succeeded
		Unified Perfmon (AVC/Medianet) Supported	•	Succeeded
	Enable Password	Medianet Performance Monitoring supported	•	Succeeded
		MACE AVC Supported	$\odot$	Not supported
		MLS NetFlow configure supported	$\odot$	Not supported
		Mediatrace configure supported	•	Succeeded
		IP SLA Supported	•	Succeeded
		HQF Supported	•	Succeeded
		MAC Table Supported	0	Not supported
	< <u>Back</u> Finish Cancel Help			Continue

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

25. Step 5: Ensure the correct interfaces are selected... Click Next

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

Steps	Select Interf	aces				
1. Device Connection Information 2. CLI Settings (Configuring)	Note: IP add		masks are	editable on the	maximum 1000 inte table for devices ti	
<ol> <li>CLI Settings (Monitoring)</li> <li>Select Interfaces</li> <li>Select VLANS</li> <li>Select Features</li> <li>Fable Polling</li> <li>Review Configuration</li> <li>Device Updated</li> </ol>	Selected	Interface GigabitEthernet1 GigabitEthernet2 GigabitEthernet3 Loopback0 Null0 VoIP-Null0	Trunk	IP Address 198.19.2.1 100.64.2.2 10.255.2.2 10.0.2.1	Subnet Mask 255.255.255.0 255.255.255.0 255.255.255.255.0 255.255.255.255.255	Description Branch2 LAN Internet MPLS
	Selected in	iterface(s): 3				

- 26. Step 5: Since there are no VLANs configured on this device, none will be displayed. You may monitor up to 25 configured VLANs on each device. Click **Next.**
- 27. Step 6: The **Select Features** dialog allows you to turn-on specific Cisco technologies per device interface using the templates included in LiveNX. This dialog displays the

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

onfigure Cisco Features for -	Branch2-NY.dcloud.cisco.com (198.19.2.1)	)
Steps	Select Features	
1. Device Connection Information	Select the features you want to enable on each interface. Learn more about each featur in the Help section.	re
<ol> <li>CLI Settings (Configuring)</li> </ol>	Features on device	
<ol> <li>CLI Settings (Monitoring)</li> </ol>	Associate Probe at IP Address:	
4. Select Interfaces	Interface NBAR NetFlow	
5. Select VLANs	GiqabitEthernet1	
6. Select Features	GigabitEthernet2  GigabitEthernet3  V	
	GigabitEthernet3	i
7. Enable Polling		
8. Review Configuration		
9. Device Updated		
	< <u>Back</u> <u>Next</u> > Finish Cancel Help	

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

		Configure Cisco Features for -	Branch2-NY.dcloud.cisco.com (198.19.2.1) X
Configure Cisco Features for - E	Branch2-NY.dcloud.cisco.com (198.19.2.1)	Steps	Review Configuration
Steps 1. Device Connection Information 2. CLI Settings (Configuring) 3. CLI Settings (Monitoring) 4. Select Interfaces 5. Select VLANs 6. Select VLANs 6. Select Peatures 7. Enable Poling 8. Review Configuration 9. Device Updated	Enable Polling Enable Polling Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section. Polling Rate 10 seconds Poll the following features Poll th	Device Connection Information     Cut Settings (Configuring)     Cut Settings (Monitoring)     Select Interfaces     Select Treatures     Select Treatures     Tenable Polling     S. Review     Configuration     9. Device Updated	The following commands will be sent to the device. Or you can choose to manually configure the device yoursef.
	< <u>Back</u> <u>Next</u> Finish Cancel Help		< gack Next > Finish Cancel Help

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

Steps	Device Updated				
Device Connection Information     CLI Settings (Configuring)     CLI Settings	You have configured this of save the current configura lost when the device is res Device Settings	tion to the device's			
(Monitoring)	Setting		Description		
<ol> <li>Select Interfaces</li> <li>Select VLANs</li> <li>Select Features</li> <li>Enable Polling</li> <li>Review Configuration</li> </ol>	Polling Rate NetFlow Monitoring NetFlow Polling Mediatrace Routing Polling Qos Polling IP SLA Polling		1	1 minute NetFlow collector Enabled N/A Disabled Enabled Disabled	
9. Device Updated	Interface Settings				
	Interface GigabitEthernet1 GigabitEthernet2 GigabitEthernet3	NBAR	:	NetFlow	

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

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

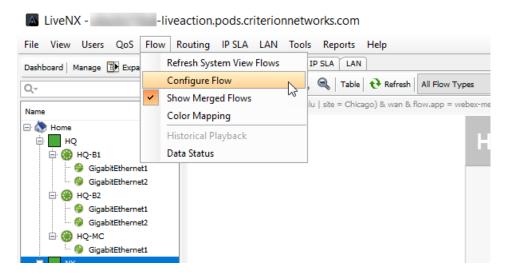
**Note:** Your new device may not be immediately visible. Use the **View > Fit to View** command to include all devices in the main view. Arrange as required.

## Lab 3.3: Configure Flow on Devices

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

Lab Steps:

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



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

	tions ct devices to configure fl		ese ar			gane		λ		
	Configuration Table						_	1		
2-										
Sel	Device	Туре	IP Address	Description	Tags	Traffi	Appli	Voice/Vi	Tradi	Custor
	🛞 Branch1-LA	Standard 🗸	198.19.1.1	Cisco IOS	WAN	۲	۲	۲	۵	۵
	Branch2-NY	Standard 🕓	198.19.2.1	Cisco IOS	WAN	•	•	•	•	•
	🛞 HQ-B1	Standard 🕓	198.18.129.24	Cisco IOS	WAN	۵	۵	۵	0	0
	🛞 HQ-B2	Standard v	198.18.129.25	Cisco IOS	WAN	۲	۲	•		۵
	🛞 HQ-MC	Standard v	198.18.129.23	Cisco IOS	HQ	۵	•	•		

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

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

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

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

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

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

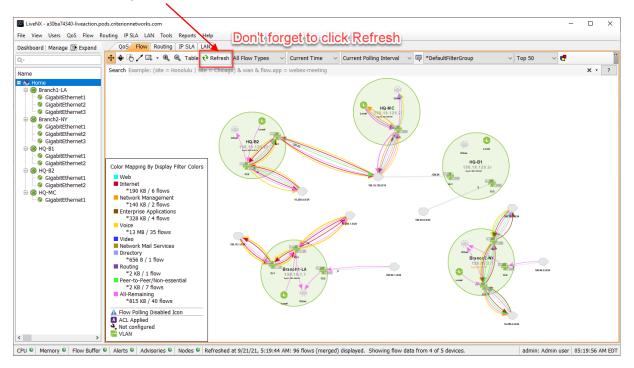
K Flow Configuration								-	o ×
Instructions									
Configure the type of flow	you wish to receive	from the inter	faces						
Flow Configuration Table									
Q-									
Device	Туре	IP Address	Description	Tags	Traffi	Applic	Voice/Vi	Traditi	Custom
🖃 🛞 Branch2-NY	Standard $\sim$	198.19.2.1	Cisco IOS	WAN,	۲	۲	۲		
- 🤤 GigabitEthernet1	-	198.19.2.1	Branch2 LAN	WAN,					
- 😔 GigabitEthernet2	-	100.64.2.2	Internet	WAN,					
└ 🚭 GigabitEthernet3	-	10.255.2.2	MPLS	WAN,					
	areir	nporta							
Flow Export Destination									
Configure Flow Export De	estination								
LiveNX node									
$\bigcirc$ LiveNX node flow replica	ator at port 9991								
Other at IP address		and po	ort						
Help	Save to Device	s Prev	iew CLI	Rev	ert	E	Back	C	lose

36. Click Preview CLI.

Multiple CLI Viewer Device Type Branch2-NY Standard	Branch2-NY config t parmit top any any exit policy-map type performance-monitor LIVEACTION-POLICY-U exit class-map match-any LIVEACTION-CLASS-AVC exit class-map match-any LIVEACTION-CLASS-MEDIANET exit class-map match-any LIVEACTION-CLASS-AVC match access-group name LIVEACTION-ACL-AVC exit class-map LIVEACTION-CLASS-MEDIANET class-map LIVEACTION-CLASS-MEDIANET	for e	ach w ce to v	e more ti ill be ava view indi	ailable vidual	to ۱	view	her		lect	
	<pre>match protocol true match protocol true exit policy-mmp type performance-monitor LIVEACTION-POLICY-U class LIVEACTION-CLASS-AVC exit class LIVEACTION-CLASS-MEDIANET exit interface GigabitEthernet3 service-policy type performance-monitor output LIVEACTI exit interface GigabitEthernet3 service-policy type performance-monitor input LIVEACTI exit interface GigabitEthernet3 service-policy type performance-monitor input LIVEACTI exit interface GigabitEthernet3 service-policy type performance-monitor input LIVEACTIO exit</pre>	GigabitEthernet1     GigabitEthernet2     GigabitEthernet3	Type Standard -	IP Address           ✓         198.19.2.1           198.19.2.1         100.61.2.1           100.61.2.1         100.22           101.255.2.2         10.255.2.2           Succeeded           Flow config	Cisco IOS Branch2 LAN Internet	WAN, WAN, WAN,	Cccessfully!	Applic	Voice/Vi	Traditi	Custom
38. C	ick <b>Close</b> . ick <b>Save to Devices</b> . ick <b>Close</b> .	Flow Export Destination Flow Export Destination Configure Flow Export De LiveNX node LiveNX node flow replica Other at IP address Help		and por	t	Reve	ert	E	lack	C	lose

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

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



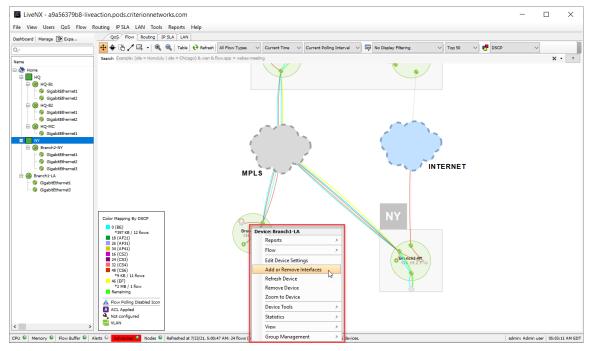
## Lab 3.4: Add/Remove Interfaces

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

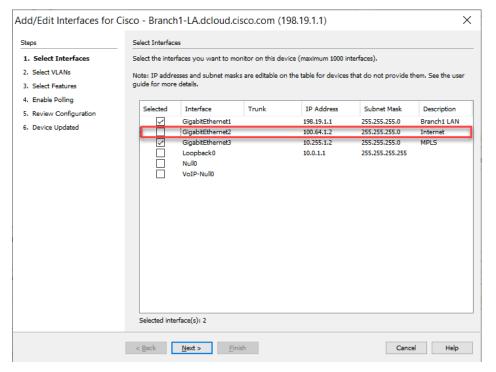
**Note:** Your Instructor may have already performed this process when they configured your Training Pod.

Lab Steps:

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

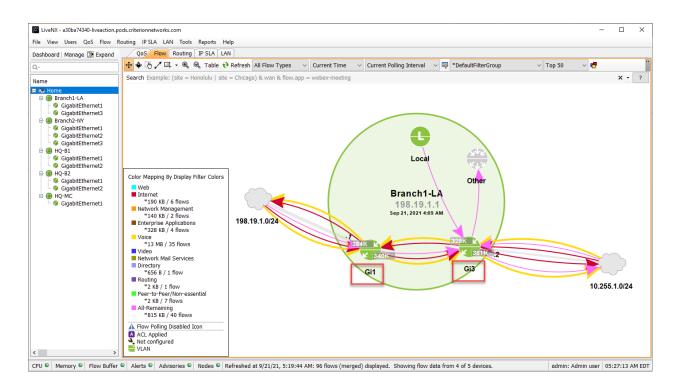


42. Deselect GigabitEthernet2.



- 43. Select Next until the Device Updated window is displayed.
- 44. Select Finish to update the device.

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

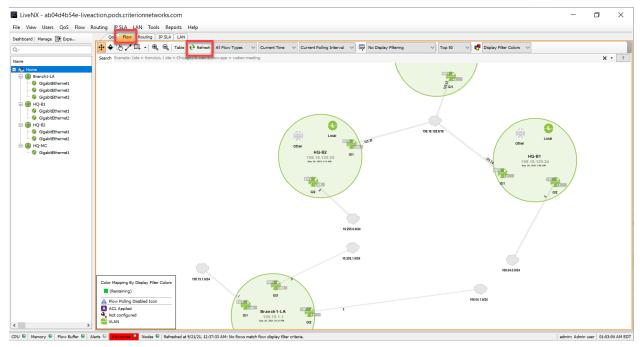


45. Repeat from Lab Step 1 above to perform interface addition/removal on **Branch2-NY** (as needed).

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

## Lab 3.5: Merge Clouds in Topology

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



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

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

Lab Steps:

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



- 47. On the Create Network Object dialog and configure the **Network Name** (This could be your Service Provider, or Transport ID) We have used **MPLS**.
- 48. Select the **Object/Shape** as appropriate and useful for simple visual recognition.

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

49. Select "Find" to add more networks.

🚺 Create	Network Object	×
Name *	MPLS	
Type *	Merged clouds	~
	A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serv different clouds where the same flows traversing those clouds are connected via the merged cloud network object.	ves as a bridge between
	Clouds * Click on clouds in the	topology
	10.255.0.0/24	Find
	Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.	168.0.0/24).
Object/Shape	Network Cloud ~	500
Size		
Tooltip	WAN Cloud	
* Required Fie	d	OK Cancel

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

	Select Cloud	ls	×
5	elect the clouds to be m	nerged:	
Γ		10.0.0.102/32	
		10.0.0.103/32	
		10.0.1.1/32	
		10.0.2.1/32	
	✓	10.255.0.0/24	
	$\checkmark$	10.255.1.0/24	
	✓	10.255.2.0/24	
		100.64.0.0/24	
		100.64.1.0/24	
		100.64.2.0/24	
		198.18.128.0/18	
		198.19.1.0/24	
		198.19.2.0/24	

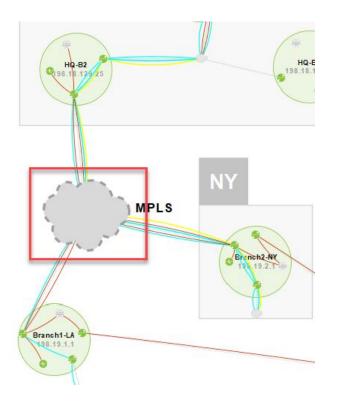
#### 51. Click **OK**.

52. Click **OK** to finish.

Name * WAN				
Type * Merged clouds				
			. When used with flows, the merged clou nected via the merged cloud network ob	
Clouds *			Click on clouds in the t	opology
10.255.0.0/2	10.255.1.0/24 10.255.2.0/24			
Click on clouds	in the tonology on use the "Eind"	within or hune in share sense	arated subnets using CIDR. notation (e.g	Find
Click on clouds 192.168.0.0/2		outton, or type in space sepa	arated subnets using CIDR notation (e.g	,
t/Shape Network Cloud	(blue)		<b>•</b>	
Size		k		
Tooltip WAN Cloud				100

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

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



# Lab 4

Lab 4: Traffic Flows

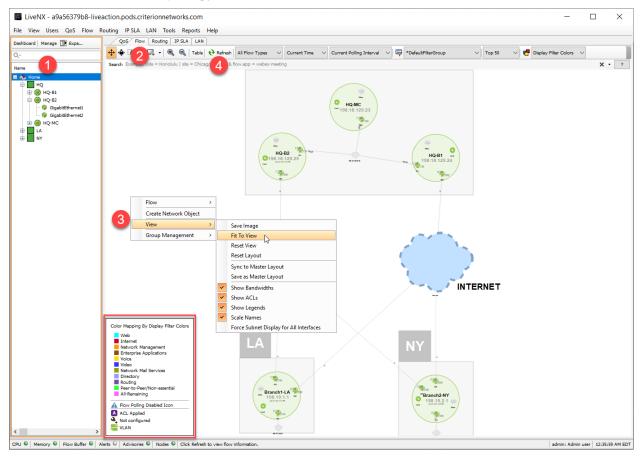
### Lab 4.1: Discover Flows

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

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

Lap Steps:

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



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

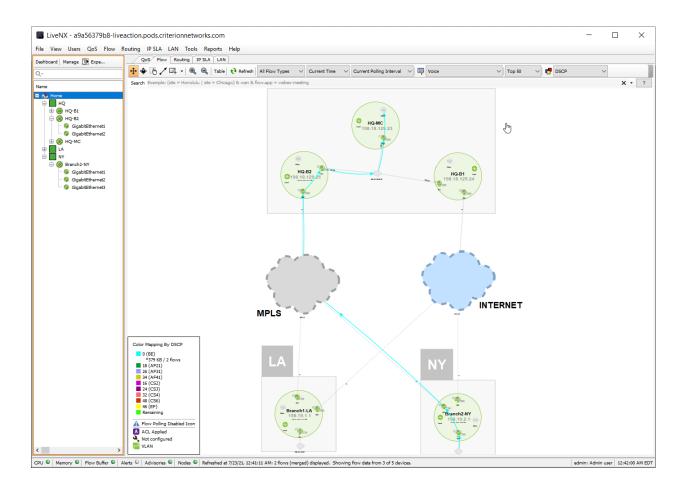
5. Set the filters to match:

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

🔁 Refresh 🛛 All Flow Types 🗸 Current Time 🗸 Current Polling Interval 🗸 🥰 Voice	/oice 🗸 Top 50 🗸 🗗 DSCP 🗸
--	---------------------------

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

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



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

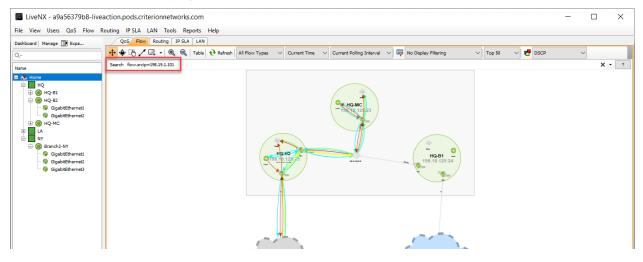
What other applications can you identify across our network?

Application	Port#	IP Pairs

### Lab 4.2: Discover Specific Flows

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

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

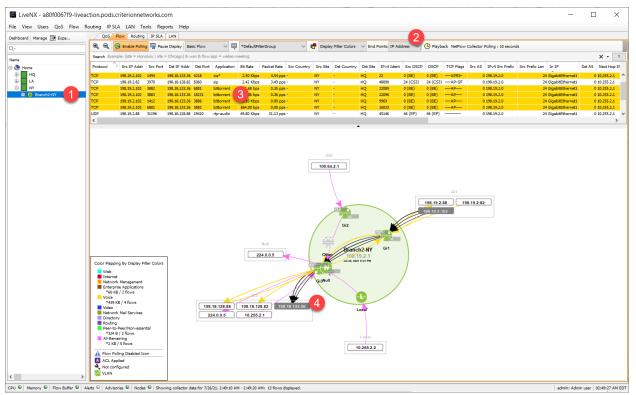


Notice that LiveNX has identified one or more end-to-end flows across the network.

## Lab 4.3: Examine Specific Traffic

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

1. Double-click on the Branch2-NY Device or select it on the Home Tree.

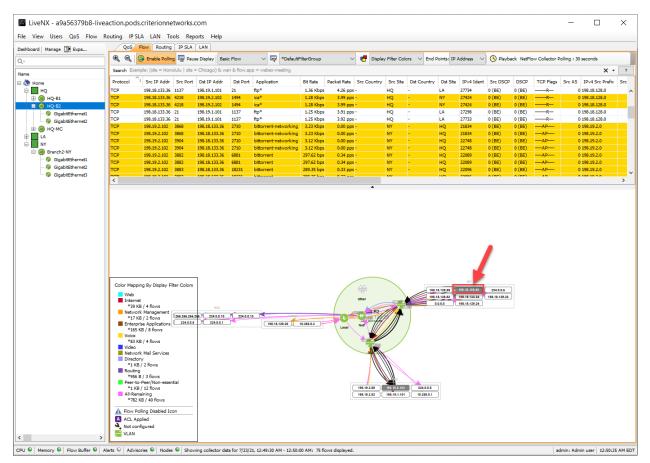


2. Select IP Addresses as the endpoint display type

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

\_ to/from \_\_

3. Click on one of the endpoints.



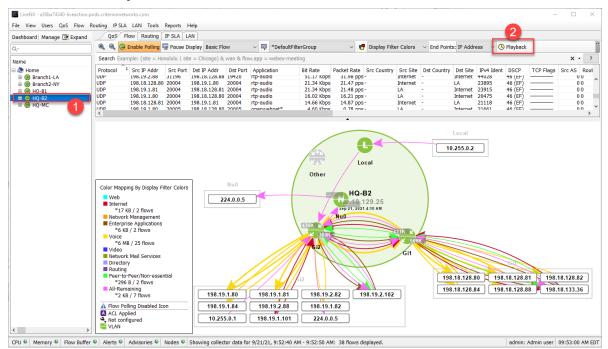
There is some other traffic, such as rtp, sip, and Citrix... but these 2 IPs are mostly generating BitTorrent. Make sure there isn't a ghost server in your network serving movies and such!

## Lab 4.4: Troubleshoot Issues

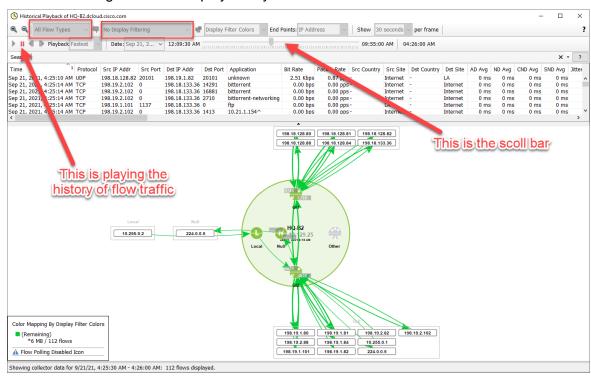
Users in the Marketing Department at our San Jose Headquarters have been complaining that their workstations seem to be "slowing down" numerous times a day. A pattern is developing that this happens about 4x per hour!

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

1. Open the HQ-B2 device. Double-click on it OR select from the Home Tree view.



2. Click the Playback button in the Filter Bar.



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

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

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

# Lab 5

Lab 5: Custom Filters

## Lab 5.1: Creating Custom Filters

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

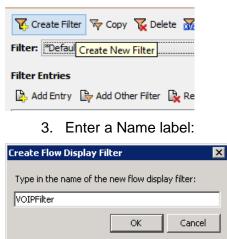
- In this lab you'll create a custom filter based-upon given ports to identify SIP and RTP traffic and verify their markings. Ports being used for the filters in this lab are:
  - SIP Ports: 5060 5061 5062
  - RTP Ports: 16384–32767

#### Lab Steps:

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

tion.pods.criterionnetworks.com					
ting IP SLA LAN Tools Reports Help					
Qo5 Flow Routing IP SLA LAN					
🔍 🔍 🔀 Enable Polling 🖙 Pause Display Basic Flow		<sup>t</sup> DefaultFilterGroup	× - 🗗	Display Filter Colors	 $\sim$ (
Search Example: (site = Honolulu   site = Chicago) & wan & flow.app = we	bex me	eting			

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



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

Match Pro	otocol/Ports				
elect from a p	ore-defined list (	of protocols/ap	plications or o	reate new	
efinitions					
ip		v	🕂 Create	🧷 Edit	Copy
_					
in Sip					
	otocol=TCP) AN	-			
🖳 💾 (L4 Pr	otocol=UDP) AN	ND (Src OR Dst	=5060 OR 50	61 OR 5062	OR 5060

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

Protocols/Applications Setup	×
🕂 Create Definition 🗋 Copy 💥 Delete 🕎 Rename	
Defined Protocols/Applications: sip	~
Entries	
🕒 Add Entry 🏾 🏹 Add Defined Prot/App 🛛 🙀 Delete	
Sip (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 506	50
🗋 (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 506	
<	>
Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.	
Entry Details	
Layer 4 Protocol: TCP (6) V	
Match Ports Regardless of Source or Destination	
Source: 5060 5061 5062	
Destination: 5060 5061 5062	
Enter port numbers or ranges separated by spaces (e.g., 80 88-443)	
Help OK Cancel	

- 8. Click OK
- 9. Click Add Entry.

🏹 Cr	eate Filte	er 🏹	Copy	Ҡ Del	ete	😿 R
Filter:	VOIPFilt	er				
Filter E	Entries					
🕒 Ad	ld Entry	B- /	Add Oth	er Filter	C <sub>×</sub>	Delet
VO	IPFilt Ac	ld Fil	ter Entr	y t/App	=sip)	

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

✓ Match Protocol/Ports	
Select from a pre-defined list of protocols/applications or create new	
definitions	
rtp. 🗸 🔶 Create 🖉 Edit 🗅 Ci	ору
(L4 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-327	767))
	.,,,
<	>

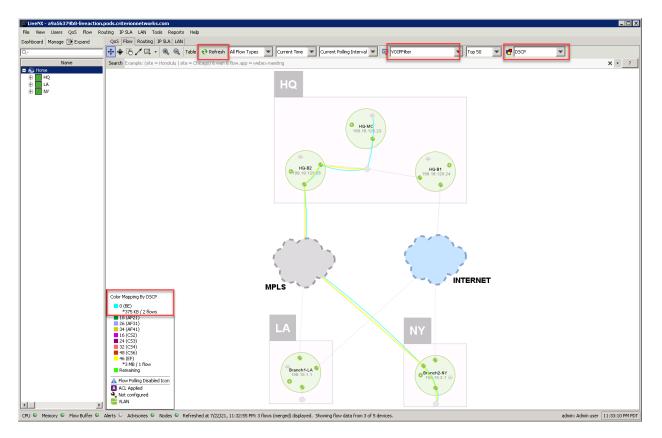
11. Edit the UDP Entry to "Match Source and Destination Ports" to 16384-32767 for both source and destination.

	Protocols/Applications Setup	×
🕂 Create Defini	ition 🗅 Copy 💥 Delete 🕎 Rename	
Defined Protoco	ols/Applications: rp	]•
Entries		
🔓 Add Entry 🥈	🌠 Add Defined Prot/App 🛛 🔓 Delete	
<b>r</b> tp	col=UDP) AND ((Src=16384-32767) AND (Dst=16384-32	767)
	COLEOPL) MIND ((2) (= 10204-25/01) MIND (D21-10204-25	.,07)
<		>
Note: Defined pro	tocols/applications added as entries are not editable her	
but can be edited	by selecting them in the drop-down box above.	
	yer 4 Protocol: UDP (17) v	
Ports		
Match Source	e and Destination Ports 🗸 🗸 🗸	
Source:	: 16384-32767	
Destination:	16384-32767	
Enter port nu	umbers or ranges separated by spaces (e.g., 80 88-443)	
Help	OK Cano	el

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

🛦 Flow Display Filters Setup	×
🏹 Create Filter 😽 Copy 🏹 Delete 😿 Rename	Filter Entry Details
Filter: VOIPFilter	Filter Entry Action:      Show or      Hide the following
,	IP Type:      IPv4 Only C IPv6 Only C Both IPv4 & IPv6
Filter Entries	Color Mapping Label & Color:
🔁 Add Entry 🕒 Add Other Filter 🕞 Delete Entry 🥼 🚯	Basic Advanced
VOIPFilter [1] Show IPv4 Only (Prot/App=sip)	Match Protocol/Ports
[2] Show IPv4 Only (Prot/App=rtp)	Select from a pre-defined list of protocols/applications or create new
	definitions
	sip 🚽 🔶 Create 🧷 Edit 🗅 Copy
	▼ sip □ (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
	□ (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
	🕝 🗖 Match IP, Range, Subnet
	Match IP Addresses Regardless of Source or Destination
	Source:
	Destination:
	Enter IP addresses, ranges, and/or subnets separated by spaces (e.g.,
	172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)
	Match DSCP
	0 (BE)
	Match Device Interface
	Match flows traversing through a particular device's interface
	*Branch1-LA.dcloud.cisco.com
	© Inbound and Outbound Combined C Inbound C Outbound
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter	Note: Items marked with a (*) are non-historical
drop-down box.	<u> </u>
Help	OK Cancel Apply

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



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

## Lab 5.2: ACL Creation

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

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

Lab Steps:

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

🛦 LiveNX - a9a56379b8-liveaction.	pods.criterionnetworks.com		
File View Users QoS Flow Ro	uting IP-SLA LAN Tools Report:	s Help	
Dashboard Manage 🗈 Expand	QoS Flow Routing IP SLA LAN		
Q-	🕂 🔶 🕭 🖊 🗔 🖌 🔍 🧠	Table 🔁 Refresh All Flow Types	Current Time 💌 Currei
Name	Search Example: (site = Honolulu   s	ite = Chicago) & wan & flow.app = web	pex-meeting
E 🔊 Home			
I III HQ IIII IIII IIIIIIIIIIIIIIIIIIIII			HQ
Branch2-NY     Device: Branch2-NY	dcloud.cisco.com	1	
QoS	•	1	
Flow	•	-	
Routing	•	-	
IP SLA	•	-	
LAN	•	-	
Edit Device Settin	gs	-	*
Add or Remove In	terfaces		HQ-B2 0198.18.129.25
Refresh Device			
Remove Device			
Zoom to Device			
Device Tools	•	Save to Startup Config	
Statistics	•	Open Device Web Page	
View	•	Manage ACLs	
Group Managemen	nt 🕨		
		-	and the second s
			1

2. Select "Create ACL"

CL-BITTORRENT-PC1       Extended (Named)         CL-CITRIX-PC1       Extended (Named)         CL-GITRIX-PC1       Extended (Named)         CL-GITRIX-PLBLIC       Extended (Named)         CL-INET-PUBLIC       Extended (Named)         CST_EFFORT       Extended (Named)         RITICAL       Extended (Named)         ENY_GLOBAL_LEARN_LIST       Extended (Named)         VEACTION-ACL-AVC       Extended (Named)         OP       Extended (Named)         OICE_VIDEO       Extended (Named)         OICE_VIDEO       Extended (Named)         Save ACL File       Load ACL File	Name / Number	∠ Type	Applied Interfaces	Create ACL
CL-CITRAPCI       Extended (Named)       Delete ACL         CL-G711-19420       Extended (Named)       Delete ACL         CL-INET-PUBLIC       Extended (Named)       Copy ACL         CST_EFFORT       Extended (Named)       Apply / Remove AC         RITICAL       Extended (Named)       Apply / Remove AC         VEACTION-ACL-AVC       Extended (Named)       Apply / Remove AC         DP       Extended (Named)       Delete ACL         DP       Extended (Named)       Apply / Remove AC         Streamed (Named)       Delete ACL       Apply / Remove AC         VEACTION-ACL-AVC       Extended (Named)       Delete ACL         DP       Extended (Named)       Delete ACL         Streamed (Named)       Delete ACL       Apply / Remove AC         Streamed (Named)       Delete ACL       Apply / Remove AC         Streamed (Named)       Delete ACL       Apply / Remove AC         Streamed (Named)       Delete ACL	L-BITTORRENT-PC1	Extended (Named)		
CL-G711-19420     Extended (Named)     Delete ACL       L-INET-PUBLIC     Extended (Named)     Copy ACL       ST_EFFORT     Extended (Named)     Apply / Remove ACL       VITICAL     Extended (Named)     Apply / Remove ACL       VEACTION-ACL-AVC     Extended (Named)     Apply / Remove ACL       OP     Extended (Named)     Apply / Remove ACL	L-CITRIX-PC1	Extended (Named)		Edit ACL
L-G/T1-19420       Extended (Named)         L-INET-PUBLIC       Extended (Named)         ST_EFFORT       Extended (Named)         RTICAL       Extended (Named)         NY_GLOBAL_LEARN_LIST       Extended (Named)         VEACTION-ACL-AVC       Extended (Named)         P       Extended (Named)         DICE_VIDEO       Extended (Named)	L-FTP-PC1	Extended (Named)		Delate LCL
IST_EFFORT       Extended (Named)       Image: Copy AcL         XITICAL       Extended (Named)       Apply / Remove AC         IST_GLOBAL_LEARN_LIST       Extended (Named)       Apply / Remove AC         VEACTION-ACL-AVC       Extended (Named)       Dice_video (Named)         P       Extended (Named)       Dice_video (Named)         DICE_VIDEO       Extended (Named)       Dice_video (Named)         Save ACL File       Save ACL File	L-G711-19420	Extended (Named)		Delete ACL
IST_EFFORT       Extended (Named)         RITICAL       Extended (Named)         RITICAL       Extended (Named)         INV_GLOBAL_LEARN_LIST       Extended (Named)         VEACTION-ACL-AVC       Extended (Named)         OP       Extended (Named)         DICE_VIDEO       Extended (Named)	L-INET-PUBLIC			Conv ACI
INY_GLOBAL_LEARN_LIST       Extended (Named)         VEACTION-ACL-AVC       Extended (Named)         VP       Extended (Named)         DICE_VIDEO       Extended (Named)         cess Rules and Remarks       Save ACL File				
VEACTION-ACL-AVC Extended (Named)  PP Extended (Named)  DICE_VIDEO Extended (Named)  Ccess Rules and Remarks  Save ACL File	ITICAL			Apply / Remove AC
DP       Extended (Named)         DICE_VIDEO       Extended (Named)				
CCESS Rules and Remarks Save ACL File				
cess Rules and Remarks Save ACL File				
Save ACL File	ICE_VIDEO	Extended (Named)		
Load ACL File	cess Rules and Remarks			
				Load ACL File

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

ACL Management	for Branch2-NY		_	×
Current Router	Branch2-NY			
	ate ACL		×	1
Access Conl Nam	e 😗 Ext	rended		∋ ACL
ACL-CITRIX-I	ne / Number 4	PQoSMark	Help	ACL
ACL-FTP-PC1 ACL-G711-19 Acc	cess Rules and Remar	der.		e ACL
ACL-INET-PU BEST_EFFOR	Less Rules and Remar	кэ	6 Create Rule	ACL
CRITICAL			Copy Rule	move ACL
DENY_GLOBA LIVEACTION- RDP		🛕 Add Remark 🛛 🗶	5 Create Remark	
VOICE_VIDE		Remark: Marking ACL for RTP Traffic	Edit Rule/Remark	
		OK Cancel	Delete Rule/Remark	
Access Rule			Move Up	CL File
			Move Down	CL File
		Preview CLI Save	e to Device Cancel	
				Llose
1				

ACL Rule Editor

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

Add Extended Rule Entry for RTPQo5Mark
⊙ permit C deny
C IP C TCP C UDP C Object-Group < No Object Groups > C Other by Name V ahp V
Source Destination
C any C by Network or IP C by Object-Group C by Network or IP C by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > < e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > <
Image Port(s)     Image Port(s)       Image Port(s)     Image Port(s)       Image Port(s)     Image Port(s)
Match by DSCP Y
Log Rule Log 💌
OKCancel

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

12. Click Save to Device.

Edit Extended ACL RT	PQoSMark			×
Туре	Extended			
Name / Number	RTPQoSMark			Help
Access Rules and Re	emarks			
remark Marking ACL fo				Create Rule
permit udp any range 1	.6384 32767 any range 163;	84 32767		Copy Rule
				Create Remark
				Edit Rule/Remark
				Delete Rule/Remark
				Move Up
				Move Down
			1	
1				
	_			
		Preview CLI	Save to	Device Cancel

13. Create ACLs for the SIP ports.

Current Router Branch2-NY			
ccess Control Lists (ACLs)			
Name / Number	🛆 Туре	Applied Interfaces	Create ACL
ACL-BITTORRENT-PC1	Extended (Named)		Edit ACL
ACL-CITRIX-PC1	Extended (Named)		
ACL-FTP-PC1	Extended (Named)		Delete ACL
ACL-G711-19420	Extended (Named)		
ACL-INET-PUBLIC	Extended (Named)		Copy ACL
BEST_EFFORT	Extended (Named)		
RITICAL	Extended (Named)		Apply / Remove ACL
ENY_GLOBAL_LEARN_LIST	Extended (Named)		
IVEACTION-ACL-AVC	Extended (Named)		
.DP	Extended (Named)		
RTPQoSMark	Extended (Named)		
/OICE_VIDEO	Extended (Named)		
ccess Rules and Remarks			
emark Marking ACL for RTP Tra			Save ACL File
ermit udp any range 16384 32	2767 any range 16384 32767		
			Load ACL File

- 14. Select "**Extended**" for the ACL Type.
- 15. Give a name to the ACL, such as "SIPQoSMark".
- 16. Click Create Remark to document your work!
- 17. Select Create Rule.

ACL Manageme	ent for Branch2-NY	×
Current Router	Branch2-NY	
G	ireate ACL	3
Nami	Type 14 Extended  Name / Number 15 SIPQoSMark Help	∋ ACL
ACL-FTP-PC1	-	
	Access Rules and Remarks	a ACL
ACL-INET-PU BEST_EFFOR	17 Create Rule	ACL
CRITICAL DENY_GLOBA	Copy Rule	move ACL
LIVEACTION-	Add Remark	
RTPQoSMark	Remark: Marking ACL for SIP Traffic Edit Rule/Remark	
VOICE_VIDE	OK Cancel Delete Rule/Remark	
Access Rule	Move Up	
remark Markii permit udp ar	Mave Dawn	
		CL File
	Preview CLI Save to Device Cancel	
	c	Llose
,		

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

Add Extended Rule Entry for SIPQoSMark
● permit C deny
O IP C Object:Group < No Object:Groups > Y O Other by Name
Source Destination
© any C by Network or IP C by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > < e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > <
by Port     Between     Manage Port(s)       5060 5062     5060 5062
9000 0002
Match by DSCP V
🔽 Log Rule 📃
OK Cancel

Next create another rule for destination SIP Ports.

	Edit Extended ACL SIPQoSACL	×
Туре	Extended 🗸	
Name / Number	SIPQoSACL	Help
Remarks		
remark Marking ACL for	SIP Traffic	Create Remark
		Edit Remark
		Remove Remark
Access Rules	060 5062	
permit tcp any range 5	060 5062 any	Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Marcalla
		Move Up
		Move Down
	Preview CLI Sav	ve to Device Cancel

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

Add Extended Rule Entry for SIPQoSMark	×
● permit C deny	
C IP C UDP C Object-Group < No Object Groups > V C Other by Name V ahp V	
Source	
💿 any 💿 by Network or IP 💦 C by Object-Group 👘 any 💿 by Network or IP 🔷 C by Object-Group	
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > > e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > >	
by Port Equal to V Manage Port(s)	
5060 5062	
Match by DSCP V	
🗖 Log Rule 🛛 💌	
OK Cancel	

- 30. Click **Preview CLI** to review the configuration to push.
- 31. Click **Save to Device**.

ACL Managem	ent for Branch2-NY					x
Current Router	r Branch2-NY					
	Edit Extended ACL SI	PQoSMark			I	×
Access Conl	Туре	Extended				e ACL
ACL-BITTORF ACL-CITRIX-I ACL-FTP-PC1	Name / Number	SIPQo5Mark			Help	ACL
ACL-G711-19	Access Rules and R	emarks				8 ACL
ACL-INET-PU BEST_EFFOR	remark Marking ACL fo				Create Rule	ACL
CRITICAL DENY_GLOBA	permit top any range 5 permit top any any rar				Copy Rule	move ACL
LIVEACTION- RDP					Create Remark	
RTPQoSMark					Edit Rule/Remark	
SIPQoSMark VOICE_VIDE(					Delete Rule/Remark	j
Access Rule					Move Up	
permit tcp an permit tcp an					Move Down	CL File
			Preview CLI	Save to	Device Cancel	1
						Close

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

## Lab 6

Lab 6: Making the Topology Work

## Lab 6.1: Setting Device Semantics

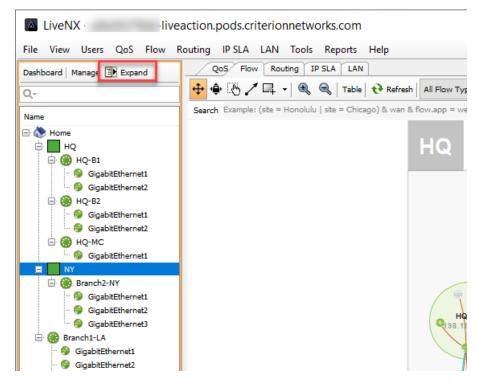
**Note:** Semantics may have already been configured on most of the devices in this Lab. You need to ensure that all the devices have their semantics entered.

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

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

Lab Steps:

1. Select Expand to set semantics for devices.



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

Image: State in the state i	oard Manage 💽 Collapse										Details	
Nome       HQ       10.0       Marce       HQ       10.0       Marce       Marce <ul> <li></li></ul>											CPU and Memory Usage	
None		IP Address	Node	Label	Input Capacity	Output Capa	WAN/XCon	Service Provider	Site	Site IP	CPU	
PG	Home	-										
P 0-91       194.1.102-3       Local       2009 0-91       100.0102.003       Percentation         P 0-92 0-92       194.1.102-3       100.0102.003       Percentation       Percentation <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Memory</td><td></td></t<>											Memory	
		198.18.129.24	Local						но	10.0.0.102.10.25		_
Control C		198.18.129.24					None					s of 2
Image: Service Provider       Image: Service Provider </td <td>GigabitEthernet2</td> <td>100.64.0.2</td> <td></td> <td></td> <td>4.0 Mbps</td> <td>4.0 Mbps</td> <td>WAN</td> <td>Internet</td> <td></td> <td></td> <td>Device Details</td> <td></td>	GigabitEthernet2	100.64.0.2			4.0 Mbps	4.0 Mbps	WAN	Internet			Device Details	
BiggladEthermad: 13255.12   BiggladEthermad: 195.13.12   BiggladEthermad: <td>E 🛞 HQ-B2</td> <td>198.18.129.25</td> <td>Local</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>HQ</td> <td>10.0.0.102,10.25</td> <td>Device name</td> <td></td>	E 🛞 HQ-B2	198.18.129.25	Local						HQ	10.0.0.102,10.25	Device name	
B       B	🛛 🤪 GigabitEthernet1	198.18.129.25					WAN	Default Service Provider			Branch1-LA.dcloud.cisco.com	
	- 🎯 GigabitEthernet2	10.255.0.2					None					
W       None       No       Padres       Padres         Image: Standback W       198.19.2.1       Local       No       No       No       Padres       Pa	🖮 🛞 но-мс	198.18.129.23	Local						HQ	10.0.0.102,10.25	Serial number	
Bendb-1-W 96.993.1 Local Non 96.993.1 Decorption   Cogabititiermet1 105.452.2 2.0 Mbps 2.0 Mbps VAN March March   Cogabititiermet2 105.452.2 2.0 Mbps 2.0 Mbps VAN March March   Cogabititiermet2 105.452.2 2.0 Mbps 2.0 Mbps VAN March March   Cogabititiermet2 105.452.2 MBIS VAN March March March   Cogabititiermet2 105.451.2 MBIS VAN March March March   Cogabititiermet2 10.255.12 MBIS VAN March March March   Cogabititiermet3 10.255.12 March March March March Mar		198.18.129.23					None				101	
											IP address	
Cogabititierend:     100.44.2     Cogabititierend:     10.255.2     Cogabititierend:     10.255.2     Cogabititierend:     10.255.1     Codd	🖻 🛞 Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24	198.19.1.1	
		198.19.2.1					None				Description	
Cogabitishered:     10.255.12     Cogabitishered:     1064.12     Cogabitishered:     1066.12     Cogabitishered:     1064.12     Cogabitishered:     1064.1     Cogabitishered:     1064.1     Cogabitishered:     1064.1     Cogabitishered:     1064.1     Cogabitishered:     Cogabitishe		100.64.2.2			2.0 Mbps	2.0 Mbps	WAN	Internet			Cisco 105 Software [Denali], CSR1000	/
GradetEthernet1 196.19.1.1     GradetEthernet2 100.64.1.2     GradetEthernet2 100.55.1.2     MPLS     VAN Branch1LAN     VAN Branch1LAN     VAN Branch1LAN     VAN MPLS     VAN MPLS     VAN MPLS     VAN MPLS     VAN MPLS     VAN MPLS     VAN     VAN     MPLS     VAN     VAN     MPLS     VAN					2.0 Mbps	2.0 Mbps	WAN	MPLS			Software	
Gigabeteritered Gigabeteritered Gigabeteritered 10.255.1.2 MPLS MP			Local						LA	10.0.1.1,198.19.1	(X86_64_LINUX_IOSD-UNIVERSALK9-	M),
Gigabitihiemet2 100.44.1.2 NPLS VAN Internet Gigabitihiemet3 10.355.1.2 MPLS VAN MPLS  Model  Mode				Branch1 LAN								(104)
Gepätelberned     10.255.1.2     MRLS     WAN     MRLS      Gepätelberned     10.255.1.2     MRLS     WAN     MRLS      Gepätelberned     10.255.1.2     MRLS     MRLS     Gepätelberned	GigabitEthernet2	100.64.1.2			2.0 Mbps	2.0 Mbps						
Ste LA Branch1-LA has been selected												
Branch1-LA has been selected       Image: Set of the presence of the p		10.255.1.2		MPLS			TO BE	MPLD			ciscoCSR1000v	
Branch1-LA has been selected  Ste  LA  Description  Enter IP address ranges in CIDR forme  C  Tags  Enter tag hars then press ENTER to address ranges ENTER to address then press ENTER to address the press ENTER		10.255.1.2		MPLS			WAN .	HPD .				
Branch1-LA has been selected  Ste  Ste  Ste  Ste  Ste  Ste  Ste		10.255.1.2		MPLS			WAR	HPD .			OS version	
Branch1-LA has been selected		10.255.1.2		MPLS				MPG.			OS version 16.3.2	
Branch1-LA has been selected		10.255.1.2		MPLS				NFG			OS version 16.3.2	
Branch1-LA has been selected		10.255.1.2		MPLS				mr G			OS version 16.3.2	
Branch1-LA has been selected		10.255.1.2		MPLS				MP G			OS version 16.3.2 Location	
Branch1-LA has been selected		10.255.1.2		MPLS							OS version 16.3.2 Location	
Enter IP address ranges in CIDR form C  Tags Enter to address ranges ENTER to ad		10.255.1.2		MPLS			WAN				OS version 16.3.2 Location	
Enter IP address ranges in CIDR form C  Tags Enter to address ranges ENTER to ad		10.255.1.2	-			0					05 version 16.3.2 Location Site Ste [A	
DC Tags Tags Enter tag here then press ENTER to ad		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site 19 10.0.1.1	
C     Tags     Enter tag here then press ENTER to ad		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site 19 10.0.1.1	
C Tags Enter tag here then press ENTER to ad		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site 19 10.0.1.1	
DC Tags Tags Enter tag here then press ENTER to ad		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site 19 10.0.1.1	
Tags Enter tag here then press ENTER to ad		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site LA IP 10.0.1.1 198.19.1.0/24	
Enter tag here then press ENTER to ad		10.255.1.2	E		-LA has	been					OS version 16.3.2 Location Site Site 10 119 100.1.1 198.15.1.0/24 Enter IP address ranges in CIDR.	orm
Enter tag here then press ENTER to ad		10.255.1.2	E		-LA has	been					OS version 16.3.2 Location Site Site 10 119 100.1.1 198.15.1.0/24 Enter IP address ranges in CIDR.	orma
		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site 10.0.1.1 196.19.1.0/24 Enter IP address ranges in CIDR I DC	orma
√ Tag Use		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site IP 100.1.1 198.15.1.0/24 Enter IP address ranges in CIDR I DC Tags	
		10.255.1.2	E		-LA has	been					OS version 16.3.2 Location Site Site Site IP 100.1.1 198.15.1.0/24 Enter IP address ranges in CIDR I DC Tags	
		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site Site IP 100.1.1 198.19.1.0/24 Enter IP address ranges in CIDR I OC Tags Enter ten press ENTER	to ad
		10.255.1.2	E		-LA has	been					OS version 16.3.2 Location Site Site Site Site IP 100.1.1 198.19.1.0/24 Enter IP address ranges in CIDR I OC Tags Enter ten press ENTER	to ad
		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site Site IP 100.1.1 198.19.1.0/24 Enter IP address ranges in CIDR I OC Tags Enter ten press ENTER	to ad
		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site Site IP 100.1.1 198.19.1.0/24 Enter IP address ranges in CIDR I OC Tags Enter ten press ENTER	to ad
		10.255.1.2	E		LA has	been					OS version 16.3.2 Location Site Site Site Site IP 100.1.1 198.19.1.0/24 Enter IP address ranges in CIDR I OC Tags Enter ten press ENTER	to ad

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

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

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

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

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

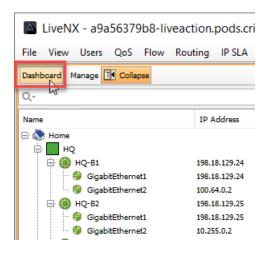
You can also tag individual or multiple devices that may belong to a site. This information can be used with the Dashboard, topology search, and reports.

coard Manage 🔣 Collapse										Details	
										Interface Details	
			_							Interface name	
	IP Address	Node	Label	Input Capacity	Output Capa	WAN/XCon	Service Provider	Site	Site IP	GigabitEthernet3	
Home			-				-			IP address	
HQ										10.255.1.2	
🖻 🛞 HQ-B1	198.18.129.24	Local						HQ	10.0.0.102,10.255	Description	
- 🤪 GigabitEthernet1 - 🤣 GigabitEthernet2	198.18.129.24 100.64.0.2			4.0 Mbps		None	Internet			MPLS	
GigabitEthernetz  HQ-B2	100.64.0.2 198.18.129.25	Local		4.0 MDps	4.0 Mbps	WAN	Internet	110	10.0.0.102,10.255	MPLS	
GigabitEthernet1	198.18.129.25	Local				WAN	Default Service Provider	HQ	10.0.0.102,10.255		
GigabitEthernet2	10.255.0.2		нQ	2.0 Mbps	2.0 Mbps		MPLS				
HQ-MC	198.18.129.23	Local	1102	210 11005	210 11005		ne co	HQ	10.0.0.102,10.255	Interface type	
GigabitEthernet1	198,18,129,23	coco				None			1010101202/201255		
NY										ethernet_csmacd	
- 🛞 Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24	Interface speed	
- 🤣 GigabitEthernet1	198.19.2.1					None				1000000	
- 🎯 GigabitEthernet2	100.64.2.2			2.0 Mbps	2.0 Mbps	WAN	Internet				
- 🊱 GigabitEthernet3	10.255.2.2		NY	2.0 Mbps	2.0 Mbps	WAN	MPLS			Define	
🛞 Branch1-LA	198.19.1.1	Local						LA	10.0.1.1,198.19.1.	Label LA	
🗝 🥪 GigabitEthernet1	198.19.1.1		Branch1 LAN			WAN	Branch1 LAN			Laber LA	
GigabitEthernet2	100.64.1.2			2.0 Mbps	2.0 Mbps		Internet			Input Capacity	2000
🦮 🚳 GigabitEthernet3	10.255.1.2		LA	2.0 Mbps	2.0 Mbps	WAN	MPLS			Output Capacity	2000
										Service Provider	
										WAN Type WAN	
										Name MPLS	
										Remove unused serv	ice providers
										Tags	
										Enter tag here then pres	is ENTER to ad
										√ Tag	Use

- 2. Select the device and then on the bottom right portion you will see a **Site** field.
- 3. Configure each device to a site as shown below:
  - a. Branch1-LA Device as LA
  - b. Branch2-NY Device as NY
  - c. HQ-B2 Device as HQ

nboard   Manage I Collapse													
										CPU and	Memory Usage		
					1	1							
e .	IP Address	Node	Label	Input Capacity	Output Capa	WAN/XCon	Service Provider	Site	Site IP	CPU			3
Home													
но										Memory			1
🕀 🛞 HQ-B1	198.18.129.24 198.18.129.24	Local	HQ LAN	1.0 Gbps	1.0 Gbps			HQ	10.0.0.102,10.255			323MB of	208
GigabitEthernet2	198.18.129.24		HQ LAN HQ Internet	4.0 Mbps	4.0 Mbps		Internet			Device D	etails		
Gigabitethemetz     HO-B2	198.18.129.25	Local	HQ Internet	4.0 Mbps	4.0 Mbps	WAN	Internet	но	10.0.0.102,10.255	Device nar	ne		
GigabitEthernet1	198.18.129.25	Local	HQ LAN	1.0 Gbps	1.0 Gbps	News	Default Service Provider	HQ	10.0.0.102,10.255		A.dcloud.cisco.com		
GigabitEthernet2	10.255.0.2		HQ MPLS	2.0 Mbps	2.0 Mbps		MPLS			Didition 1			
HQ-MC	198.18.129.23	Local	NQ MPLS	2.0 10005	2.0 Hops	1100	MPC5	HO	10.0.0.102.10.255	Serial num	ber		
GigabitEthernet1	198.18.129.23	Local				None			1010101102,101233	101			
NY	130.10.123.23					Hone				IP address			
Branch2-NY	198,19,2,1	Local						NY	198.19.2.0/24	198.19.1.1			
GigabitEthernet1	198.19.2.1	cocar	Branch2-NY LAM	1.0 Gbps	1.0 Gbps	None			130,13,2,0/24				
GigabitEthernet2	100.64.2.2		NY Internet	2.0 Mbps	2.0 Mbps		Internet			Description			
GigabitEthernet3	10.255.2.2		NY MPLS	2.0 Mbps	2.0 Mbps		MPLS			Cisco IOS Software	Software [Denali], C	CSR1000V	
Branch1-LA	198,19,1,1	Local		Lie Hops	Ele Hispo				10.0.1.1.198.19.1		INUX_IOSD-UNIVER	SALK9-M).	
GigabitEthernet1	198.19.1.1	COCU	Branch1-LA LAN	1.0 Gbps	1.0 Gbps	None	Branch1 LAN			Version 1	3.3.2, RELEASE SOFT	WARE (fc4	)
GigabitEthernet2	100.64.1.2		LA Internet	2.0 Mbps	2.0 Mbps		Internet			Technical	Support:		
GigabitEthernet3	10.255.1.2		LA MPLS	2.0 Mbps	2.0 Mbps		MPLS			Model			
g olgonication co	TOTESSTILE		2111122	210 11000	210 11000		100			ciscoCSR:	1000v		
										OS version	1		
										16.3.2			
										16.3.2			
										Location			
										Site			
									Y	Site			
									Y	Site Site LA			
									Y	Site LA	11		
									Y	Site LA	.1.1 19.1.0/24		
									Y	Site LA	1.1 19.1.0/24		
									Y	Site LA	1.1 19.1.0/24		
									Y	Site LA	.1.1 13.1.0/24		
									Y	Site LA IP 10.0 198.	19.1.0/24		
									Y	Site LA IP 10.0 198.	1.1 19.1.0/24 r IP address ranges in	n CIDR form	na
									Y	Site LA IP 10.0 198.	19.1.0/24	n CIDR form	n.a
									Y	Site LA IP 10.0 198. Ente DC	19.1.0/24	n CIDR form	
									X	Site LA IP 10.0 198. Ente DC	19.1.0/24 r IP address ranges in		
									Y	Site LA IP 10.0 198. Ente DC	19.1.0/24		
									Y	Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in		d
										Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in tag here then press l	ENTER to a	d
									Y	Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in tag here then press l	ENTER to a	d
									Y	Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in tag here then press l	ENTER to a	d
										Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in tag here then press l	ENTER to a	de
									X	Site LA IP 10.0 198. Ente DC Tags Enter	19.1.0/24 r IP address ranges in tag here then press l	ENTER to a	de

- 4. Open the dashboard to ensure that data is populating correctly.
- Note: It may take up to 15 minutes for the Dashboard to populate with data.



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

Site WAN Interface Utilizat...

15 %	15 0
13 %	17.0
	13 '
16 %	16 9
16 %	16 9
13 %	13 9
13 %	13 9
	16 %

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

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

Dashboard					- 🗆
ystem Application Q	OS Flow IP SLA WA	N			
ain	* Flow Alerts	- 24 Hours			
Alerts				Alert	Count
Reports	1			High media packet rate	0
				✓ High media packet loss p.	
				High network delay	0
ip	» Alert Count			High retransmission count	nt O
over Devices	8	There is no data to display f	or the given time period	NSEL flow denied event .	
	1 t	mere is no data to display i	si che given chile period	PfR Out of Policy event o	
age Devices	Ale			PfR TCA - packet/byte d.	
ne Sites				PfR TCA - one way delay	
e				PfR TCA - jitter inter arri.	
onfigure Alerts				PfR TCA - unreachable Blacklisted NetFlow addre	0
onfigure Flow	n 🗆 🗤			Black listed NetFlow addre	ess 0
pplication Performance	Flow source wan   xcon     Basic Flow     Top 10 Source	o Addres B∕tes ∨	Ton 10 Destin	07/23/21, 05:45:00 AM to	X Apply 15m 30m 1hr 4 0 07/23/21, 06:00:00
pplication Performance	Basic Flow     Top 10 Source	e Addres Bytes V		ation Addres Bytes V	15m 30m 1hr 4
plication Performance	Basic Flow     Top 10 Source     Src IP Addr	Bytes Flows	Dst IP Addr	Bytes V	15m 30m 1hr 4 o 07/23/21, 06:00:00
plication Performance	Basic Flow     Top 10 Source     Src IP Addr     B -	Bytes 1 Flows 2 MB	Dst IP Addr 5 🗷 -	Bytes 5 1	15m 30m 1hr 4 o 07/23/21, 06:00:00
plication Performance	Basic Flow     Top 10 Source     Src IP Addr     G -     G -	Bytes <sup>1</sup> Flows 2 MB 628 KB	5 221 2 -	Bytes 1 6 MB 864 KB	15m 30m 1hr 4 o 07/23/21, 06:00:00
plication Performance	Basic Flow     Top 10 Source     Src IP Addr     0     0     0	Bytes <sup>1</sup> Flows 2 MB 628 KB 248 KB	5 ₪ - 321 ₪ - 96 ₪ -	Bytes Bytes 6 MB 6 6 MB 6 6 4 KB 5 59 KB	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance	Basic Flow  Top 10 Source  Src IP Addr	Bytes <sup>1</sup> Flows 2 MB 628 KB	5 (B) - 321 (B) - 9 (B) -	Bytes 1 6 MB 864 KB	15m 30m 1hr 4 o 07/23/21, 06:00:00
plication Performance	Basic Flow     Top 10 Source     Src IP Addr     0     0     0	Bytes <sup>1</sup> 2 MB 628 KB 248 KB 192 KB	Dst IP Addr           5         10 -           321         10 -           96         10 -           9         10 -	Bytes 1 Bytes 1 Bytes 6 MB B64 KB B64 KB B65 KB 125 KB	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance	Basic Flow     Top 10 Source     Src IP Addr     0     0     0     0     0     0     0     0     0	Bytes <sup>1</sup> 1 Flows 2 MB 628 KB 192 KB 9 KB 9 KB	Dst IP Addr           5         fit           321         fit           96         fit           9         fit           14         fit	Bytes Viana Series Addres Bytes Viana Series Serie	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance	Basic Flow Top 10 Source Src IP Addr	Bytes 2 M8 2 M8 628 K8 248 K8 192 K8 9 K8 8 K8	Dst IP Addr           5         13           321         13           96         12           9         12           9         12           14         12           13         13	Bytes         1           Bytes         1           6 MB         864 KB           558 KB         125 KB           77 KB         19 KB	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance	Basic Flow Top 10 Source Src IP Addr  Src IP Addr  C  B  C  C  C  C  C  C  C  C  C  C  C	Bytes <sup>1</sup> 2 MB 628 KB 248 KB 192 KB 9 KB 8 KB 7 KB	Dst IP Addr           5         13 -           321         13 -           9         13 -           13         12 -           13         12 -           13         12 -           13         12 -           13         12 -           13         12 -           14         12 -	Bytes 1 Bytes 1 Bytes 6 6 MB 664 KB 589 KB 580 KB 560 KB 580 KB 5	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance		Bytes 1 Flows 2 MB 628 KB 192 KB 9 KB 8 KB 7 KB 7 KB	Dst IP Addr           5         Ø -           321         Ø -           96         Ø -           9         Ø -           14         Ø -           13         Ø -           13         Ø -	Bytes 1 Bytes 1 Bytes 1 6 MB 66 4KB 654 KB 559 KB 125 KB 125 KB 125 KB 19 KB 916 B 116 B	15m 30m 1hr 4 0 07/23/21, 06:00:00
plication Performance	<ul> <li>         Basic Flow         Top 10 Source         Src IP Addr         ∅ -</li></ul>	Bytes <sup>1</sup> 2 M8 628 K8 248 K8 192 K8 9 K8 8 K8 7 K8 7 K8 2 K8	Dst IP Addr           5         13 -           321         12 -           36         23 -           9         13 -           13         12 -           13         12 -           13         12 -           13         12 -           6         12 -	Bytes 1 Bytes	15m 30m 1hr 4 0 07/23/21, 06:00:00
pplication Performance	<ul> <li>         Basic Flow         Top 10 Source         Src IP Addr         ∅ -</li></ul>	Bytes 1 Flows 2 MB 628 KB 246 KB 9 KB 8 KB 7 KB 7 KB 7 KB 2 KB 456 B	Dst IP Addr           5         13 -           321         12 -           36         23 -           9         13 -           13         12 -           13         12 -           13         12 -           13         12 -           6         12 -	Bytes 1 Bytes 1 Byt	15m 30m 1hr 4 o 07/23/21, 06:00:00
pplication toplication Performance lanage Application Groups	Basic Flow Top 10 Source Src IP Addr  G G G G G G G G G G G G G G G G G G	Bytes 2 MB 2 MB 2 KB 2 48 KB 2 48 KB 192 KB 9 KB 8 KB 7 KB 2 KB 2 KB 456 B 2 KB 2 KB	Dst IP Addr           5         8           321         8           96         8           14         8           13         8           13         8           14         8           13         8           14         8           13         8           14         8           15         10           16         10           17         10           18         10           19         10           10         10           11         10           12         10           13         10           14         10           15         10           16         10           17         10           18         10           19         10           19         10           10         10	Bytes 1 Bytes 1 Byt	15m 30m 1hr 4 0 07/23/21, 06:00:00

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

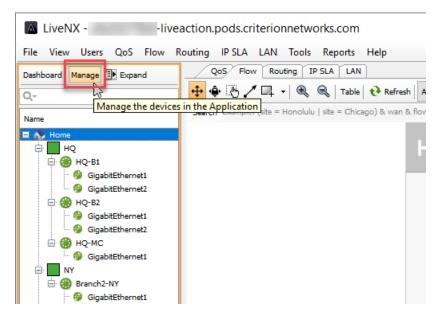
## Lab 6.2: Adding Devices to Groups

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

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

Lab Steps:

1. Open the Device Management window by selecting Manage.



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

2. Select "Edit Groups"

🔺 De	vice Managemen	it												×
Filter	by:						Filter		Clear					
Select	Device Name Branch1-LA Branch2-NY HQ-B1 HQ-B2 HQ-MC	IP Address 196.19.1.1 198.19.2.1 198.18.129.24 198.18.129.25 198.18.129.23	Vendor Cisco Cisco Cisco Cisco Cisco	Model ciscoCSR1000v ciscoCSR1000v ciscoCSR1000v ciscoCSR1000v ciscoCSR1000v	Node Local Local Local Local	Group NY HQ HQ HQ		Poll	Qos V V V	Flow Y		Routing	Interval 10 seconds × 10 seconds × 10 seconds × 10 seconds ×	Configured Configured Configured
* LAN po	ling occurs every 15 minu	utes											Nu	mber of Devices: 5
	Configurations Configure Remove Add To Group emove From Group Edit Groups	Configure QoS, FI Select devices in the tab Remove selected device <new group=""> Removes selected device Edit the groups</new>	le and click th (s).	ne configure button.	~		edit Edit Edit Edit	D	efault SNM efault CLI	Monitorin	s g Settings - ation Setting			Clear Clear
													Apply	Close

#### 3. Click Add

Edit Groups			×
oups			
Name	^	Size	Add
HQ		3	Edit
NY		1	
			Remove
			Close
			Close

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

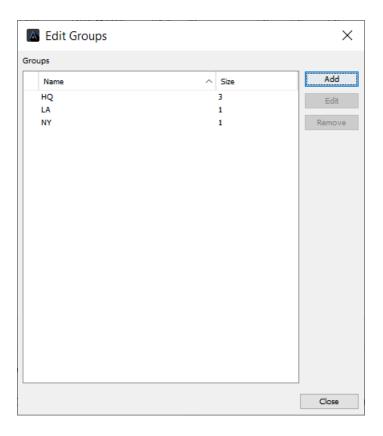
- 6. click the green **Right** arrow.
- 7. Click Add.
- 8. Repeat the steps above to create any other groups as necessary.

Add Group			Х
Name (*) LA 4 Description			
5 All Other Devices	6	Current Group of Devices	
Q-	$\ominus$	Q,-	
(NY) Branch2-NY (HQ) HQ-B1 (HQ) HQ-B2 (HQ) HQ-MC	•	Branch1-LA	
Asterisks (*) indicate required fields.			
		Add Done Canc	el

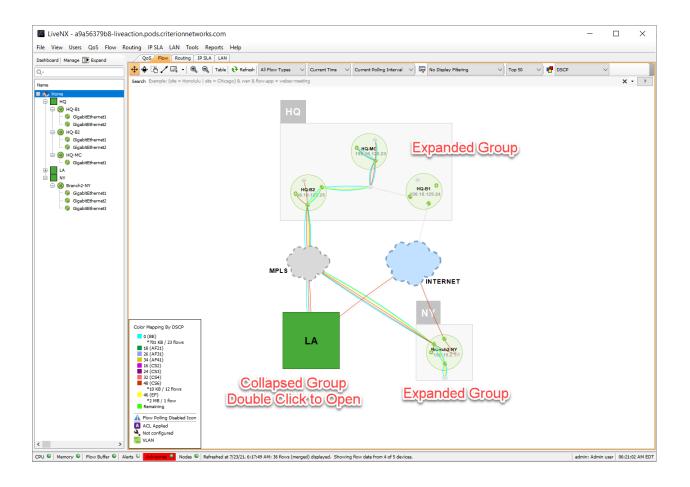
9. Once all groups have been created and devices correctly added, select **Done**.

Once completed your groups should look like the one below.

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



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



## Lab 6.3: Creating Network Objects

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

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

Lab Steps:

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

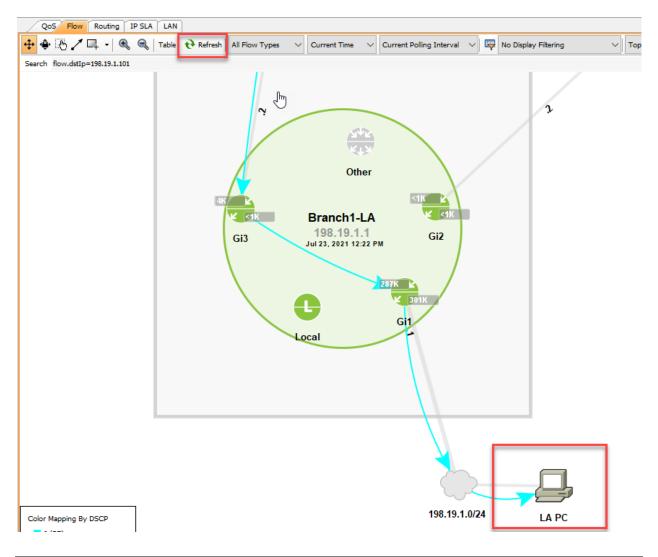


- 5. Select an Object/Shape as "PC".
- 6. Click OK.

🔼 Edit N	letwork Object	$\times$
Name *	LA PC	
Type *	IP address end point	$\sim$
	Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merged cloud in order flows to be drawn to the network object.	for
	IP Address *	
	198.19.1.101	
	Type in an IP address, or select a device interface or IP address end point in the topology.	
Object/Shape	PC V	
Size	IP Phone	
Tooltip	Network Cloud	
* Required Fie	e Router OK Car	icel
	Custom V	

7. Click Refresh.

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



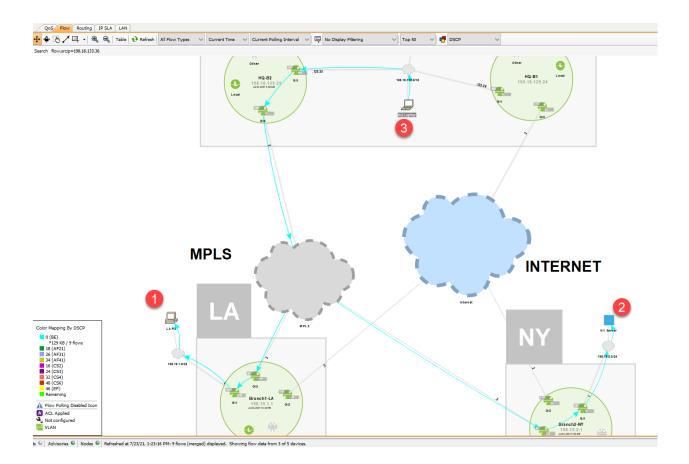
**Note:** Assigning representative icons to the flow endpoints makes it easier to locate potential trouble spots!

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

🔼 Create	Network Object	×
Name *	NY Server	
Type *	IP address end point	~
	Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, o flows to be drawn to the network object.	r merged cloud in order for
	IP Address *	
	198.19.2.102	
	Type in an IP address, or select a device interface or IP address end point in the topology.	
Object/Shape	Generic Square	×
Size	Generic Square 43 ,	<b>^</b>
Tooltip		
* Required Fie	Network Cloud (blue) PC	OK Cancel
	Router	
	Switch Processor	¥

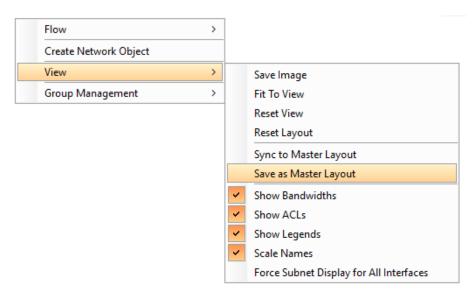
- 11. Select an Object/Shape as "File Server".
- 12. Click OK. This will add the device to the diagram
- 13. Next, add a Laptop in HQ.
- 14. Enter the search string: flow.srcip=198.18.133.36
- 15. Select the flow (it will be near the HQ-B1 and HQ-B2 routers), right click on the IP Address endpoint.
-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

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



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

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



## Lab 7

Lab 7: Dashboards & Reports

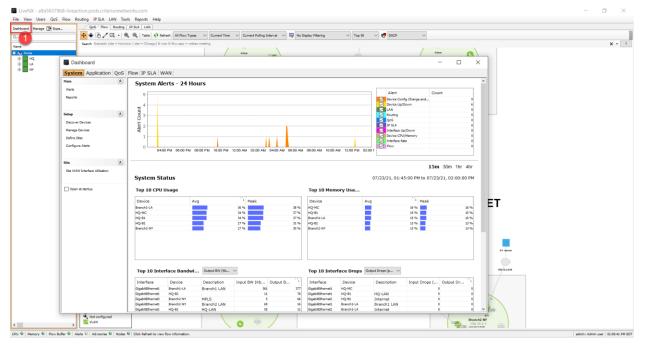
## Lab 7.1: The Dashboard

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

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

Lab Steps:

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



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

- 2. Un-check any alerts that are not relevant to your view (in this case, device up down as we have been working in a lab environment to build this course we know what those incidents are)
- Dashboard X System Application QoS Flow IP SLA WAN Main ۲ System Alerts - 24 Hours Alert Alert Count Report Count ۲ Routing QoS Discover Devices Alert P SLA Manage De Device CPU/Me Define S Configure Al Jul 22, 04:00 PM Jul 22, 08:00 PM Jul 23, 12:00 AM Jul 23, 08:00 AM Jul 23, 12:00 PM
- 3. Left-click-Drag to Zoom into a flow of interest.

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

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

System       Application       QoS       Flow       IP SLA       WAN         Main
Alerts Count Alert Count  Alert Count Device Config Change and 9 Device Lp/Down 6
Reports Alert Count Device Config Change and
Device Lipform     device Lipform     device Lipform     device Lipform
Setup (A) 7 Company Backing 0 V Qo5 0
Discover Devices USE Constraints Constrain
Define Chur Device CPU/Memory 0
Configure Alerts 0
Jul 23, 02:15 AM Jul 23, 02:30 AM Jul 23, 02:46 AM Jul 23, 03:00 AM Jul 23, 03:15 AM Jul 23, 03:00 AM Jul 23, 03:0

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

🔊 Dashboard			- 0	×
System Application QoS	Flow IP SLA WAN			
Main 🏾 🛞	System Alerts - 24 Hours			^
Alerts	Ale	ert Co	unt	
Reports		vice Config Change and		9
		vice Up/Down		6
Setup 🎗			now Alerts	
Discover Devices		-		4
Manage Devices		erface Up/Down	elect None	
Define Sites		erface Rate 🛛 🖻 Ex	port Legend Data	
Configure Alerts	U Fow Jul 23, 02:15 AM Jul 23, 02:30 AM Jul 23, 02:45 AM Jul 23, 03:00 AM Jul 23, 03:15 AM Jul 23, 03:30 AM Jul 23, 03:45 AM	N		

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

Time	Severity	Device	Group		Alert Type		<sup>1</sup> Details
016/05/13 01:35:31 PM	Warning	HQ-SJ	Flow				High media packet loss percent
1016/05/13 05:49:30 PM	Warning	HQ-SJ		Open Report	pa	acket loss percent.	High media packet loss percent
016/05/13 08:44:30 PM	Warning	HQ-SJ	Flo	Drill Down on Specifi	c Flow >	Top Analysi	s Report
016/05/13 09:04:02 PM	Warning	HQ-SJ	Flo	Export Data			•
016/05/13 11:01:01 PM	Warning	HQ-SJ		Export Data		Top Conver	sations Report
016/05/13 01:35:02 PM	Warning	Branch 1-LA Branch 1-LA	Flow		High media (	Bidirectiona	I Source/Destination Pair Report
016/05/13 05:49:30 PM	Warning Warning	Branch 1-LA Branch 1-LA	Flow		High media ( High media (	Source or D	estination Address Report
016/05/13 09:04:02 PM		Branch 1-LA Branch 1-LA	Flow				
016/05/13 11:01:01 PM 016/05/13 01:00:36 PM	Warning Warning	HO-SJ	Interface	Lip/Down	High media ( Interface er	Address Pai	r Report
016/05/13 01:00:36 PM	Warning	HQ-SJ HQ-SJ	Interface		Interface er	Destination	Address Report
016/05/13 01:06:06 PM	Warning	HQ-SJ HO-SJ	Interface		Interface er	Source Add	ress Report
016/05/13 01:07:06 PM	Warning	HQ-SJ HQ-SJ	Interface		Interface er		
016/05/13 01:11:36 PM	Warning	HQ-SJ	Interface		Interface er	Destination	Address Popularity Report
016/05/13 01:12:06 PM	Warning	HQ-SJ	Interface		Interface er	Source Add	ress Popularity Report
016/05/13 01:17:06 PM	Warning	HQ-SJ	Interface		Interface er	Site Traffic F	Report
016/05/13 01:17:06 PM	Warning	HO-SJ	Interface		Interface er		•
016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface		Interface er	Destination	Site Traffic Report
016/05/13 01:22:06 PM	Warning	HQ-SJ	Interface		Interface er	Source Site	Traffic Report
016/05/13 01:27:35 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro	or	Interface name - Ethernet0/0;
016/05/13 01:27:35 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro	or	Interface name - Ethernet0/1;
016/05/13 01:33:06 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro	or	Interface name - Ethernet0/0;
016/05/13 01:33:35 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro	or	Interface name - Ethernet0/1;
016/05/13 01:38:36 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro		Interface name - Ethernet0/0;
016/05/13 01:38:36 PM	Warning	HQ-SJ	Interface	Up/Down	Interface erro	or	Interface name - Ethernet0/1;
16/05/13 01:38:36 PM Filter by Time Start Time 05/13/16 05/14/16 Filter by Severity	Warning           ✓           12:00:00 PM ♀           ✓           12:00:00 PM ♀	hh:mm:ss Branch1-LA	Device	Up/Down Filter by Alert T Device unavail	уре	or	Interface name - Ethernet0/1;
Emergency 🗸	Include higher priorities	100,	000 🗸				Execute

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

7. Review the Top Analysis Report.

	sis	Ki da								
05/12/16 01:								15m 1h 6h 1	1d 1w 30d <b>(</b>	Custon
05/15/10, 01.	05:31 PM to 05/	13/16, 02:05	:31 PM			E	xecute Report			
Source HQ-SJ		~	··· All Interface	es	~	Nur	nber of flow	s: 1	CSV F	ile Resu
Filter *DefaultFilterGro	up 🗸 😽 🗄	Inbound	~			Med	lianet	V Time Sorted	- Unique Flows $\!$	
Search JUDP & flow.port.src=2	0004 & flow.port.dst=2	0004.8 flow.dscn=F	BE & flow.direction=ING	RESS & flow.media	anet.event=0.8 flow.u	nedianet.eventSton=0.4	& flow.medianet.m	onitorEventError=62	8427459993272320	
								Q		
Time Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application			Dst Country	RTP SSRC	Dire
May 13, 2016 1:3 UDP	198.19.1.81	20,004	198.18.128.81	20,004	rф		1-	-	2432754705	INGF
	Filter *DefaultFilterGro Search +UDP & flow.port.src=2	Filter *DefaultFilterGroup v *	Filter *DefaultFilterSroup v 💀 Inbound Search 4.DP & flow.port.src=20004 & flow.port.dst=20004 & flow.dsrp=	Fifter *DefaultFilterGroup     Inbound       Search 4JDP & flow.port.src=20004 & flow.port.dst=20004 & flow.dscp=BE & flow.drecton=2NG       Time     Protocol       Src IP Addr     Src Port     Dst IP Addr	Filter         *DefaultFilterGroup         Imbound           Search         4.DP & flow.port.src=20004 & flow.port.dst=20004 & flow.dscp=8E & flow.dsccton=INGRESS & flow.medd           Time         Protocol         Src IP Addr         Src Port         Dat IP Addr         Dst Port	Filter *DefaultFilterGroup     Inbound       Search *UDP & flow.port.stc=20004 & flow.port.dst=20004 & flow.drection=INGRESS & flow.medianet.event=0 & flow.n       Time     Protocol       Size IP Addr     Size P Addr	Filter         *DefaultFilterGroup         Isound         Mec           Search         4.DP & flow.port.src=20004 & flow.port.dst=20004 & flow.decp=8E & flow.decton=INGRESS & flow.medianet.eventStop=0         Mec           Time         Protocol         Src Part         Det IP Addr         Dst Part         Application         Flow Record Co	Filter     *DefaultFilterGroup     Image: Medianet       Search     4.DP & flow, port.src=20004 & flow, port.dst=20004 & flow, decp=BE & flow, drecton=DNGRESS & flow, medianet.event5top=0 & flow, medianet.event5	Filter     *DefaultFilterGroup     Image: Search     Medianet     Time Sorted       Search     4.DP & flow.port.src=20004 & flow.port.dst=20004 & flow.dexp=EE & flow.dexcton=INGRESS & flow.medanet.event50p=0 & flow.medan	Filter       *DefaultFilterGroup       Inbound       Medianet       Time Sorted - Unique Flows          Search       -UDP & flow.port.stc=20004 & flow.dstp=BE & flow.drecton=INGRESS & flow.medianet.event=0 & flow.medianet.eventStop=0 &

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

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

## Lab 7.2: Viewing Reports

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

#### Lab Steps:

#### **Run an Applications Report**

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

·≡ LiveAction <sup>®</sup>	NX					New Features!         ▲ 3         ■ 0         ▲ 0         {-} -	0- ¢-	💄 admin -
🖸 Main 😁	Here						<ul> <li>Apply filter</li> </ul>	🗗 Auto
	es					Active Alerts		
≣ Stories		DEVICES: 5		INTERFACES: 11		ALERTE (2) A Own 1% of Velos traffic for Revecto AV defoud citics com naving application sig is not marked at DSCP EF. A Own 1% of Velos traffic for ROEZ defoud citics com naving application havenagent is not marked at DSCP EF.	TIME OPEN 23 Jul 2021, 23 Jul 2021,	1, 02:37 AM 1, 02:36 AM
Lal Reports	0	DEVICES 2	0	INTERFACES	0	<ul> <li>Over 1% of Voice traffic for HQ-MC.doloud cisco.com running application lanrevagent is not marked as DSCP EF.</li> </ul>	23 Jul 2021	, 02:32 AM
View Reports		Branch1-LA     Branch2-NY		GigabitEthernet1 Branch1-LA				
View Schedule		<ul> <li>HQ-B1</li> </ul>		GigabitEthernet1 Branch2-NY     GigabitEthernet1 HQ-B1				
R. Livena		<ul> <li>HQ-B2</li> <li>HQ-MC</li> </ul>		GigabitEthernet1/HQ-B2     GigabitEthernet1/HQ-MC     GigabitEthernet2/Branch1-LA	Ŀ			
✗ Configure				GigabitEthernet2lBranch2-NY     GigabitEthernet2lHQ-B1     GigabitEthernet2lHQ-B2     GigabitEthernet2lHQ-B2     GigabitEthernet3lBranch1-LA				
				GigabitEthernet3(Branch2-NY				

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

GENERAL SETTINGS		REPORT LIST	REPORT DETAILS		
Name		🗄 Your reference information for this report Application (Flow) Normal 🛅	Report Name	Flow Type	
Application		Add New Report	Your reference information for this report	Basic Flow	
Presentation Mode			Report Description	Execution Type	
Standard	~		Enter report description	Time Series	
Footnote			Devices	Sort By	
Enter report group description			All WAN Devices	Bit Rate	
Time Zone	DST		Interfaces	Business Hours	
(GMT-05:00) America/New York	~		All WAN Interfaces	All Hours	
Time Range			Flex Search @	Cannot be used with Bin Duration	All De
Last Hour	~		Ex.: site=Honolulu & wan & flow.app=http	× Auto	
Flex Search			plaster films		5 mi
Ex.: site=Honolulu & wan & flow.app=http	×		Display Filter No Display Filtering	Long Term Store	
				Due to the report options selected, this report of utilize the Long Term datastore (faster). To over	r-rid
Display Filter Select Display Filter	~		Direction Select Direction	this behavior and use the Raw Flow datastore, Bin Duration option to 1 Minute (slower).	;et ti
Select Display Piller			Inbound and Outbound Separated		
Sharing Settings			Inbound		
Email 🔆			Outbound		
Enter an email address or AD entity			Inbound and Outbound Combined		
File Format Send PDF Send CSV			<u> </u>		
PDF Row Limits					
All Rows					
All Rows					
				Cancel Save As Template	Exe

5. Select the Inbound and Outbound Combined filter

6. Click **Execute**.

ew Reports									View Schedule Gre	eate Report
Templates Reports History										
Q application	Application						View Options	<ul> <li>Share Download</li> </ul>	Schedule Copy	Clos
U, application										
fault Templates	Your reference	e information for this report Application	(Flow)							/
orite Applications	Device: All WAN	Devices Interface: All WAN Interfaces Displa	Filter: No Display Filtering Direction: Out	bound Flow Type: Basic Flow Exec	ution Type: Time Series Sort By: Bit Rate	Bin Duration: Auto Start Time: Jul 23, 2021 13:	28:13 EDT (GMT-04:00) End Time: Jul 23, 2021 14:28:13 E	DT (GMT-04:00) Bin Interval: 5 minutes		
le Fastlane Applications ()	100								- rtp-audio	
lication Vs. Network Performance									ica sip	
ication Service Provider Performan									= trp conferencing	
N Application Service Provider Per	j 50								bittoment ospf	
AN Application Vs. Network Perfor	10								bittoment-networking netbios-dgm	
									Total	
N Application Vs. Network Performa									Total	
IN Application Vs. Network Performa	12.22	13:35 13:40	13.45	12.50 12.55	14.00	14:05 14:10	14.15 14.20	1425 14	Total	
IN Application Vs. Network Performa	12.22		13.45	12.50 12.55	14.00	1405 1410	14.15 14.20	1425 14 Q. Search		(
-	1233 << Page 1	/2 >>						Q Search	128	
-	1233 << Page 1	/2 >> Application ⊖	Total Flows 🔿	Total Bytes 🔿	Total Packets 🔿	Average Bit Rate 🔿	Average Packet Rate 🔿	Q, Search Peak Bit Rate $\diamondsuit$	Peak Packet Rate 🔿	
-	1233 << Page 1	/2 >> Application ⊖ rtp-audio	Total Flows 🔿 57	Total Bytes 🗘 21.75 MB	Total Packets 🔿 108,737	Average Bit Rate 🔿 48.33 Kbps	Average Packet Rate 🔿 30.20 pps	Q, Search Peak Bit Rate () \$1.98 Kbps	Peak Packet Rate 🔿	3
	12.33 « < Page 1 Legend 0	) /2 >> Application ⊘ rtp-audio ica	Total Flows () 57 216	Total Bytes $\diamondsuit$ 21.75 MB 4.47 MB	Total Packets () 108,737 66,917	Average Bit Rate () 48.33 Kbps 9.92 Kbps	Average Packet Rate $\bigcirc$ 30.20 pps 18.59 pps	Q, Search Peak Bit Rate () 51.98 Kbps 11.16 Kbps	Peak Packet Rate 🔿	3
-	1233 << Page 1	) /2 >> Application ⊜ rtp audio lice stp	Total Flows () 57 216 71	Total Bytes 21.75 MB 4.47 MB 1.60 MB	Total Packets () 108,737 66,917 10,987	Average Bit Rate () 48.33 Kbps 9.92 Kbps 3.56 Kbps	Average Packet Rate 30.20 pps 18.59 pps 3.05 pps	Q. Search Peak Bit Rate () 51.98 Kbps 11.16 Kbps 4.14 Kbps	Peak Packet Rate 🔿	3
-	12.33 « < Page 1 Legend 0	/2 >> Application ⊖ rp=uutio ica sip fip	Total Flows () 57 216 71 110	Total Bytes 21.75 MB 4.47 MB 1.60 MB 1.07 MB	Total Packets () 108,737 66,917 10,987 26,737	Average Bit Rate () 48.33 Kbps 9.92 Kbps 3.56 Kbps 2.38 Kbps	Average Packet Rate 30.20 pps 18.59 pps 3.05 pps 7.43 pps 7.43 pps	Q, Search Peak Bit Rate () 51.98 Kbps 11.16 Kbps 4.14 Kbps 2.63 Kbps 2.63 Kbps	Peak Packet Rate 🔿	3
-	1233 « < Page 1 Legend 0	/2 >> Application () rip-audio lica sip fb conferencing	Total Flows () 57 216 71 110 43	Total Bytes ○ 21.75 MB 4.47 MB 1.60 MB 1.07 MB 788.04 KB	Total Packets () 108,737 66,917 10,987 28,737 9,979	Average Bit Rate () 48.33 Kbps 9.92 Kbps 3.56 Kbps 2.38 Kbps 1.75 Kbps 1.75 Kbps	Average Packet Rate () 30.20 pps 18.59 pps 305 pps 7.43 pps 2.52 pps 2.52 pps	Q, Search Peak Bit Rate () 51.98 Kbps 11.16 Kbps 4.14 Kbps 2.43 Kbps 2.51 Kbps 2.51 Kbps	Peak Packet Rate 🔿	3
	12.33 « < Page 1 Legend 0	/2 3> Application () rtp-audio ica sip fip conferencing bitturent	Total Flows () 87 216 71 110 43 3 1,744	Total Bytes () 21.75 MB 4.47 MB 1.60 MB 1.07 MB 788.84 KB 163.29 KB	Total Packets © 100,737 66,917 10,947 28,737 90,799 2,131	Average Bit Rate () 48.33 Kbps 9.92 Kbps 2.38 Kbps 2.38 Kbps 1.75 Kbps 0.36 Kbps 0.36 Kbps	Average Packet Rate 50 20 pp 16 59 pp 30 59 pp 7 43 pp 2 52 pp 0 59 pp 0 59 pp	Q, Search	Peak Packet Rate 🔿	3
	1233 « < Page 1 Legend 0	/ 2 >> Application () rip-audio ice sip fip conferencing bibliorent conf	Total Flows 0 57 216 71 110 43 1,744 206	Total Bytes () 21.75 MB 4.47 MB 1.60 MB 7.86 04 KB 7.86 04 KB 7.86 32 KB 1.32 56 KB	Total Packets © 108,737 10,987 28,537 9,079 2,331 1,612	Average Bit Rate () 48.33 kbps 9.92 kbps 1.56 kbps 1.75 kbps 0.38 kbps 0.38 kbps 0.28 kbps	Average Packet Rate 30 20 pp 18,59 pp 74 30 2,52 pp 0,65 pp 0,65 pp 0,65 pp 0,65 pp 0,65 pp	Q, Search Peak Bit Rate () 51.98 Kbps 4.14 Kbps 4.14 Kbps 2.63 Kbps 2.63 Kbps 3.84 kps 3.84 kps 3.84 kps 3.28 kbps 3.28 kbp	22 Peak Packet Rate 🔿	3
-	1233 « < Page 1 Legend 0	/2 3> Application () rtp-audio ica sip fip conferencing bitturent	Total Flows () 87 216 71 110 43 3 1,744	Total Bytes () 21.75 MB 4.47 MB 1.60 MB 1.167 MB 788.04 KB 1.03.26 KK 88.05 KB	Total Packets © 100,737 66,917 10,947 28,737 90,799 2,131	Average Bit Rate () 48.33 Kbps 9.92 Kbps 2.38 Kbps 2.38 Kbps 1.75 Kbps 0.36 Kbps 0.36 Kbps	Average Packet Rate () 30.0 pps 10.59 pps 10.5	Q, Search Pesk Bit Rate () 51.99 K3pa 4.11 K5p 2.51 K5p 3.64 K5	22 Peak Packet Rate 🔿	3

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

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

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

#### Run a Top Talkers Report

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

	New Feature	:s! 🔺 3 🛛	0	• 0	<b>a</b> 0	{}	· • •	\$ <b>*</b>	💄 admin 👻
							View Scheo	lule	Create Report
		View Options ~		Share	Dov	vnload	Schedule	Сор	y Close
1 23, 2021 13:2	3:13 EDT (GMT-04:00) End Time: Ju	ul 23, 2021 14:28:13 EDT	r (GMT-04	:00) Bin I	iterval: 5	minutes			Load Parameters
							rtp-audio ica sip ftp conferenc bittorrent ospf citrix bittorrent etbios-d Total	networking	Ξ
14:10	14:15	14:20		14 Q Sear	:25 :h	14:2	3		1 ±
	Average Packet Rate 🛇		Peak B	Bit Rate 🖒			Peak Packet P	late 🗇	
18.33 Kbps		30.20 pps			51	98 Kbps			32 pps
9.92 Kbps		18.59 pps			11	16 Kbps			20 pps
3.56 Kbps		3.05 pps			4	.14 Kbps			4 pps
2.38 Kbps		7.43 pps			2	.63 Kbps			8 pps
1.75 Kbps		2.52 pps			2	.51 Kbps			3 DDS

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

= LiveAction ×				New Formares ( A 3 ( 0 ) + 0 ) ( A 0	[-] · • • • •	1
View Reports					Vew Schedule	Drester Report
Templates Reports History	RUN OR EDIT REPORT(S)			×		
Q, application	GENERAL SETTINGS	REPORT LIST	REPORT DETAILS		Schedule Copy	Close
Default Templates	Name	🗄 Your reference information for this report Application (Flow) Normal 🕒 🔳	Report Name	Flow Type		10
Favorite Applications 0	Application	Top Conversations (Flow) Normal 🐑 🗃	Top Conversations	Basic Flow ~		
Apple Pestiane Applications 0	Presentation Mode	Add New Report +	Report Description	Execution Type	= to solo	=
Application Vs. Network Performance 8	Standard		Enter report description	Time Series 🗠	0000 N2 0000 700	-
Application Bervice Provider Performan. 0 SCMAN Application Service Provider Per. 0	Footnote		Devices	Sort By	otherscore otherset	
COWAN Application Va. Network Perfor.	Common to all		All WAN Devices 🗸 🗸	Bit Rate 🔍	altria auto Sciences estructures	
INTERN Application Vis. Network Performa.	Reports in View B DET		Interfaces	Business Hours	restricte styre	
WAN Application Service Provider Perfo. 0	(GMT-05:00) America/New York		All WAN Interfaces	Al Hours v	10.	-
	Time Range		Flex Search	Carnot be used with AB Devices Bin Duration		0 2
	Last Day		Ex.: site+Hotolulu & wan & flow.app+http 8		Peak Packet Rate 😄	
	Flex Search		Display Filter	5 minutes		32 pps 20 pps
	Ex.: site=Honolulu & wan & flow.app=http *		No Display Filtering	Long Term Store Due to the report options selected, this report will		4 pps
	Display Filter		Direction	utilize the Long Term datastore (faster). To over-ride this behavior and use the Raw Flow datastore, set the		8 pps
	Select Display Filter		Outbound	Bin Duretion option to 1 Minute (slower).		3 pos 0 pps
			Should Wait For DNS Resolution			0 pps
	Sharing Settings		False 🗸			2 pps
	Enter an email address or AD entity					0 pps 0 pps
	File Format Bend PDP Send CSV PDF Rox Limits All Roxet		Specific to the	Report Selected		
				Cancel Save As Template Everyte		

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

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

LiveAction 💌								New Features A	3 80 00 4	6 (F) -	0· 0·	- <b>4</b> -
- Type here to filter reports.										Ve	iew Schedule	Create I
Reports	^											
Interface Bandwidth	in i							View Opti	ons - Share	Download Sch	hedule Copy	
Top Analysis												
IPs and Ports	nce information for this	report Application (Flow)										
Address	WilDevices Interface: Al 10	URN Interfaces Display Filter: No Displa	Filtering Direction: Outbound	Row Type: Dasic Flow Execution Typ	e: Time Deries Dont By: Bit Rate Bin Duration: A	luto Btart Time: Jul 22, 2021 14/44.50 EDT (GMT)	04:00) End Time: Jul 23, 2021 14:44:50 EDT (SMT04:0	0) BinInterval: 1 hour				
Top Conversations										=	rtp-audio	
New Report										=	nip Ha	
Source or Destination												
-Address Pair											larvevagent bittorrent	
- Destination Address										_		
Source Address	1 1700	18:00 19:00 2	21.00 22	0 28:00 34:28	01.00 02.00 03.00	0400 0500 0600	87.00 09.00 09.00	10.00 11.00	12:00 12:00	14.00 1444		
Destination Address									Q Search			
Source Address Popu	al 1/4>>								Q Search			
-Site Traffic	Application C	Total Flows O	Tota	I Bytes O	Total Packets C	Average Bit Rate O	Average Packet Rate C	Peak Bit	Rate O	Peak Packet Ra	ate O	
Destination Site Traff	tp-audio		968	369.75 MB	1,853,655	34:	14 Kbps	21,45 pps	50.07 K	bps		
Source Site Traffic	loa		2,648	62.21 MB	820,732	5.	76 Кара	9.50 pps	10.09 K	bpa		
Applications	sip		1,241	27.85 MB	194,189		58 Kbps	2.25 pps	3.79 K			
Protocol	np		36	24.58 MB	42,190		28 Kbps	0.49 pps	54.62 K			
Protocol Port	fp		1,297	12.56 MB	312,695		16 Kbps	3.62 pps	2.47 K			
Application Group	conferencing		499	9.20 MB	105,940		IS Kbpa	1.23 pps	1.84 K			
Application	lanrevagent bittorrent		192	3.50 MB 2.33 MB	40,327 26.055		32 Kbps 22 Kbps	0.47 pps 0.30 pps	1.66 K			
DSCP vs Application	ospf		3.284	2.33 MB	28,035		IS Kbos	0.30 pps	288			
Business Relevance	otrix		5,254	1.52 MB	19,563		la Kopa	0.23 pps	448			
Traffic Class	08%		59	1.04 MB	19,203	u.	a kops	0.23 pps	643	iba		
ii QoS	sations (Flow)											
Network	WOrvices Interface: All V	UN Interfaces Display Filter: No Displa	Fitering Direction Outbound	Flow Type: Rasic Flow Execution Type	e Time Series Sort By: Bit Rate Bin Duration: A	uto Should Walt For Drs Resolution: false Sta	rt Time: Jul 22, 2021 14:44:50 EDT (GMT-04:00) End T	Inne: Jul 23, 2021 14:44:50 EDT (SMT-04	00) Bin Interval: 5 minutes			
Medianet											198.19.2.88/198.18.128.8	
Applications (AVC)										=	198.19.2.102/198.18.122.1 198.19.2.82/198.18.128.8	2.26 92
B-NSEL				m		www.www	*****				198,18,123,36/198,19,1,1 198,18,123,36/198,19,2,1	.01 102
⊕ PfR											10.255.1.2/234.0.0.5 10.255.1.2/234.0.0.5 10.255.0.2/234.0.0.5	
Wireless									V		100.64.1.2/224.0.0.5	
AnyConnect	×				1				Y		Total	
>	9 16:00	17:00 18:00 19:00	20:00 21:00	22:00 22:00	Jul 23 01:00 02:00	12:03 04:00 05:00 04	100 07:00 08:00 09:00	10:00 11:00	12:00 12:00	14:00 14:44		
6.0	Page 1 / 5 > ≫								Q. Search			
L	igend O Sto IP Addr O	Site O Dat IP	4ddr O Det Site	O Total Flows O	Total Bytes 🗘 Total Pack	ets O Average Bit Rate O	Average Packet Rate O	Peak Bit Rate 0	Peak Packet Rate 🗘	Sire Country 🗘	Dat Countr	try O
	198,19,2,88	NY 198.18	128.88 HQ		82 377.90 MB	1,889,521 34.9	9 Kbps 21.87 pps	55.30 Kbps	34	ope -		
	100.10.0.00											

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

#### **Flow Identification**

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

≡ LiveAction <sup>™</sup>											
View Reports											
Templates Reports History											
Q, application											
Default Templates		Favorite Reports									
Favorite Applications	•	Add Report									
Apple Fastiane Applications											
Application Vs. Network Performance	L	Top Reports									
Application Service Provider Performan		NAME ©	DESCRIPTION \$								
SDWAN Application Service Provider Pe		Application	This Flow-based report v	will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.							
SDWAN Application Vs. Network Perfor		Top Conversations		This Flow-based report will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.							
IWAN Application Vs. Network Performa	•	Interface Bandwidth		will highlight the Top 10 interfaces' bandwidth, based on the selected filter oriteria. It will list up to 1000 interfaces.							
IWAN Application Service Provider Perfo		DSCP		wil highlight the Top 10 DSCP markings' bandwidth, based on the selected fifter criteria. It will list up to 64 DSCP values.							
		Top Interface Bandwidths	This SNMP-based report	t shows a table of all the interfaces' bandwidth utilization per the specified fiter.							
		Top Interface Errors	This SNMP-based report	t shows a table of all interface errors (CRC/Runts/Overuns, etc.) per the specified filter.							
		Top Class Bandwidths	This SNMP-based report	t shows a table of all QoS class bandwidths for all interfaces per the specified fitse.							
		Top Class Drops	This SNMP-based report	t shows a table of all QoS class drops on all interfaces per the specified filter.							
		Interface Bandwidth	This SNMP-based report	t graphs bandwidth utilization of a specific interface.							
		Interface Utilization	This SNMP-based report	t graphs the interface bandwidth utilization (by percentage) of a specific interface.							
	1	Interface Errors	This SNMP-based report	t graphs the number of interface errors (CRC/ Runta/ Overruns/ etc.) of a specific interface.							
	1	Post-Policy Drops	This SNMP-based report	t graphs the QoS drops of all classes on a specific interface.							
		Application DSCP Audit	This Flow-based report v	will show the DSCP markings of applications organized by site, based on the selected filter oriteria.							
		Interface Bandwidth Summary	This Flow-based report v	will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.							
		Default Templates									
		NAME 🗘		DESCRIPTION 🗘							

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

GENERAL SETTINGS	REPORT LIST		REPORT DETAILS	
Name	DSCP (Flow)	Normal 🖸 🗃	Report Name	Flow Type
DSCP	Add New Report	+	DSCP	Basic Flow
Presentation Mode			Report Description	Execution Type
Standard 🗸			Enter report description	Time Series
controte			Devices	Sort By
Enter report group description			All WAN Devices	Bit Rate
lime Zone 🔽 DST			Interfaces	Business Hours
(GMT-05:00) America/New York			All WAN Interfaces	All Hours
				Cannot be used with All Devi Bin Duration
Last Day			Flex Search @ Ex.: site=Honolulu & wan & flow.app=http	X Auto
				16
ilex Search 🔞			Display Filter	Long Term Store
Ex.: site=Honolulu & wan & flow.app=http ×			No Display Filtering	Due to the report options selected, this report will
Display Filter			Direction	utilize the Long Term datastore (faster). To over-ride this behavior and use the Raw Flow datastore, set the
Select Display Filter 🗸			Outbound	Bin Duration option to 1 Minute (slower).
Sharing Settings				
Email 🔆				
Enter an email address or AD entity				
File Format				
Send PDF Send CSV				
PDF Row Limits				
All Rows 🗸				
Custom Logo 🚯				
No Custom Logo 🗸 🗸				

4. Click **Execute**.

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

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

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

#### Bandwidth by Flow Type

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

ENERAL SETTINGS	REPORT LIST		REPORT DETAILS
lame	E DSCP (Flow) Norma	0.0	Q. Search
DSCP	Please choose report type		* Only Time Range report types displayed
resentation Mode	Add New Report	+	Top Reports
Standard $\sim$			Application (Flow)
ootnote			Top Conversations (Flow)
Enter report group description			Interface Bandwidth (Flow)
ime Zone 💆 DST			DSCP (Flow)
(GMT-05:00) America/New York			Top Interface Bandwidths (SNMP)
ime Range			i op interface Bandwidths (SNMP) Top Interface Errors (SNMP)
Custom v			
			Top Class Bandwidths (SNMP)
tart Date         Start Time         End Date         End Time           07/22/2021         15:10         07/23/2021         15:10			Top Class Drops (SNMP)
			Interface Bandwidth (SNMP)
lex Search 😡			Interface Utilization (SNMP)
Ex.: site=Honolulu & wan & flow.app=http ×			Interface Errors (SNMP)
isplay Filter			Post-Policy Drops (SNMP)
Select Display Filter			Application DSCP Audit (Flow)
			Interface Bandwidth Summary (Flow)
haring Settings			E LiveNA
mail 🔀			🗄 Flow
Enter an email address or AD entity			SNMP
ile Format			Cisco SD-WAN
Send PDF Send CSV			⊕ Alerts
DF Row Limits			
ustom Logo 🚯			
No Curtom Lono			

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

🗧 LiveAction 💌																			New Featureal	] • 3	• •	• • •	o {-} -	0.	0 · _ & (	admin *
View Reports																								View Schedule	Create R	leport
Templates Reports History Q. application	DSCP																			View Options	× 9	hare	Download	Schedule	Сору	Close
Default Templates	Interdence	Read wide t	Summary (Flov	->																						,
Fevorite Applications 0																										
Apple Fastiane Applications			- GigabitEtherne																							
Application Vs. Network Performance	Device: Al De	erices linterfac	e Al Interfaces I	Depley Filter: No Di	spley Filtering How I	ype: Sasic Flow	Execution Type: Tie	ne Series Sort By:	ot Kate P	lex Search: war	n & flow, dscp=62	An Duration: A	uto Start Time	Jul 22, 2021 16:	10:00 EDT (UM164)	(0) End Time:	36/28,202116/100	DEDT (GM1-64:00)	Bin Interval: 5 minute	5						
Application Service Provider Performan.																								HQ-82/Gipabi	(Dhemet2/Ingress	=
SDWAN Application Service Provider Pe 0	140						m-	vvv	5	NV	~~~	$\sim 1$	vvv	~~~	$\sim$	$\sim$	$\sim \sim \sim$	222	~~~~	VW /	$\sim$	w	vvv1			
SDWAN Application Va. Network Perfor 0										· · ·										· ·\/						
IWAN Application Vs. Network Performa	8								V											V						
MAN Application Service Provider Perfo 0	0	16:00	17:00	18:00	19.00 20.0	0 21.00	22.00	29.00	3.123	01.00	62.00	03.00	04.00	05:00	06.00	07:00	08.00	10	00 11.00	12:00	12:00	14.00	15:10			
			12,000	10.00	1900 200	0 2100	22.00	1000	10.10	01.00	12.00	08.00	0400	0000	08000	07.00	08.00	10		12,00			10.10			
																						Q Search				1
	Legend	Site 🗘	Device 🗘	inte	rface Name 🗘	Sen	vice Provider O	0	irection 🗘		Total Flows 🗘		Total Bytes 🗘		Total Packets 🗘		Average Bit Rat		Average Packs	rt Rate 🗘		Peak Bit	Rate 🗘	Peak Packs	t Rate 🗘	
	-	HQ	HQ-82	đig	abitEthernet2	MP	LS	li li	gress			1,016	1	189.24 MB		1,946,213		36.04 Kbj	28		22.53 pps		61.60 Kb	ра	1	38 pps
	Branch2-N	Y.deloud.cisco	.com · GigabitEt	hernet3																						
					splay Filtering Flow T	ype: Basic Flow	Execution Type: Tin	ne Series Sort By:	lit Rate F	lex Search: var	n & flow, datap=67	in Duration: A	uto Start Time:	Jul 22, 2021 15	10:00 EDT (GMT-04:	00) End Time:	Jul 23, 2021 15:10:0	(00:40T(QMT04:00)	Dis Internal: 5 minute							
	75																							Branchd-MUG	igabiliterreth Sp.	
																								Branch24000	igsbillherret3/ing	
	140 -						m	VVV	M	N	~~~~	VVV		$\sim$	~~~~	vvv	vvvv	~~~	\$~~~v	$\sqrt{1}$	VVV	222	$\sim$			
	8 8 25																			- V						
									V											V						
	0 15.15	5 16:00	17:00	18:00	19:00 20:00	0 21:00	22:00	22:00	3.6 23	01:00	62:00	03:00	04:00	osico	06:00	07:00	00.00	10	00 11.00	12:00	12:00	14:00	15:10			
																						Q Search.				± ⊞
	Legend C	Site 0	Device 0		Interface Name O		Service Provider	0	Direction	10	Total Flows C		Total Bytes		Total Packets		Average Bit R		Average Pack	ket Rate O		Peak Bit		Peak Packs		
		NY	Branch2-I Branch2-I		0igabitEthernet3 0igabitEthernet3		MPLS MPLS		Egress			1,010		388.52 MB 600 bytes		1,942,584		35.97 Ki 0.00 Ki			22.48 pps 0.00 pps		55.30 Ki			34 pps 0 pps
	_	No.	branch24	NT .	organizmemers		MPLS		ingress					oco byses				0.00 K	ipa -		0.00 pps		101	pa .		o ppa

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

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

## Lab 7.3: Create a Custom Report

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

Lab Steps:

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

GENERAL SETTINGS	REPORT LIST		REPORT DETAILS	
Name	IPs and Ports (Flow)	Fast 🕤 🗃	Report Name	Flow Type
IPs and Ports, Last Fifteen Minutes	Add New Report	+	IPs and Ports	Basic Flow 🗸
Presentation Mode			Report Description	Execution Type
Standard $\checkmark$			Enter report description	Time Series ~
Footnote			Devices	Sort By
Enter report group description			HQ-82	V Bit Rate V
Time Zone 🛛 🛃 DST			Interfaces	Business Hours
(GMT-05:00) America/New York $\sim$			All Interfaces	All Hours ~
Time Range			Flex Search 💿	Bin Duration
Custom V			wan & flow.dscp=BE	× Auto ~
Start Date         Start Time         End Date         End Time           07/23/2021         15:29         07/23/2021         15:44			Display Filter No Display Filtering	1 minu Raw Flow Data Due to the options selected, this report will utilize the Raw Flow datastore (slower).
Flex Search @ Ex.: site=Honolulu & wan & flow.app=http ×			Direction Inbound and Outbound Combined	V
Display Filter			Should Wait For DNS Resolution	
Select Display Filter			False	
Sharing Settings				
Email 🔆				
Enter an email address or AD entity				
File Format Send PDF Send CSV				
PDF Row Limits				
All Rows 🗸				
Custom Logo 📵				
No Pustom Loso V				

New Reports																- Vie	e Schedule Crewte I
Templates Reports History																	
Q. By Template Name	IPs and Po	rts, Last Fifteen Mi	nutes											View 0	Options - Share C	lownload Sch	edule Copy
fault Templates	IPs and Port	s (Flow)															
ice Analysis 0	Denice 110-22	Interfaces (1) interfaces	Dealer Filer No.2	anter Filmina - Direc	tion interact and Colored	Combined Flow To	or Bale Doy Law	ution Taxes Time Device	en last for its fare	Hen Describe ware & Stree descri-	-15 Bis Densities June 10	multi Weit For Den Benehrt	an false - Bart Timer Jul 21	2021 18/29 08 207 (647-64/0)	End Time: Jul 23, 2021 1544-00 827 0	WT-5401 Be beened	1.1.000
an 0	20																198 19 2 102/198 18 18 18 26/107
korite Applications 0																	198 19 2 85/198 18 128 82/70P
ple Fastiane Applications 0	140	-	-										Contraction of the local division of the loc			-	188 18 133 36/188 19 2 100/T07 188 19 3 80/198 18 128 83/T07
de Fastiane Voice Analysis 0	1 1		Contraction of the local division of the loc													Statement of the local division of the local	100 10 100 26/100 10.1 101/TCF 108 16 108 26/100 10.2 102/TCF
																	198.18.133.36/100.181.101/707
	ž 12																1988 19 7 87/1989 18 178 87 (YOR)
N Capacity Planning 0																	198,192,82/198,18,128,82/109/ 198,192,102/198,18,188,36/709 Tone
N Capacity Planning 0 Network Performance Audit 0	10.00	152		15.22	14	104	16.05		18	1627	1538	1529	1540	9649 (1864)	2 754		194 19.2 102/195 18 103 36/707
N Capacity Planning O National Performance Audh O ce/Video Performance Ve. Network O	t in the second			15.42	14	YEAR	1645		18	1827	159	539	9540	1541 1543	a 1644 Q Search .		194 19.2 102/195 18 103 36/707
N Capacity Planning O National Performance Audit O cerVideo Performance Vo. Network O			Sec Site C	1542 Sto Pen D	ntal. Det IP Addr C	1554 Det Site O	1645 Det Port C	Protocol C		1627 Application C	1534 Total Rows C	1529 Total Bytes C	1540 Total Packeta C	15.ct 15.ct Average Bit Rate C			194 19.2 102/195 18 103 36/707
N Capacity Plenning 0 Narionik Parformance Audit 0 De/Video Performance Va. Network. 0 eto-Site Treffic Unitation Audit 0 vice-Presider DSCP Audit 0	C < Page	14.58							DISC# C						Q. Search . Average Packet Rate C	1544 Peak Bit Rate C	Die 192 102/194 14:194 36:10
Nationalis Palenting     0       Nationalis Parliamance Audit     0       Individues Parliamance Val. Networks     0       Individues Tradition Unitization Audit     0       Inces Previdee DDDP Audit     0       Is Binglie Site XWAN Path Charges     0	C < Page	() /4 ⇒ ≫ Sec IP Adér C	She Site 0	Sec Port 0	Det IP Addr C	Det Site 🗘	Det Port 0	Protocol 0	0 (8E)	Application C	Total Plove C	Total Bytes C	Total Packets 0	Average Bit Rate C 1.69 Kbpe	Q. Search - Average Packet Rate C S-All ppr	15.44 Peak Bit Rate C 5.79 s	Die 192 102/194 14:194 36:10
I Capacity Planning 0 Nationik Planning Audit 0 Id/Udes Performance Vis Besuch 0 Id/Udes Performance Vis Besuch 0 Id/Udes Performance Vis Besuch 0 A Brigle Star WVA Planh Changes 0 Reation Vis Alessonk Performance 0	C < Page	74 ⇒ ≥ Sec IP Addr C 198,19,2,102	Sho She D NY	She Pert C 4218	Det IP Addr 0 198.18.133.36	Det She Q HQ	Det Port 0 1494	Protocol © TCP	050P C 0 (86) 0 (86)	Application C	Total Rove 0	Total Bytes C 527.85 KB	Total Packets 0 4900	Average Bit Rate C 4.69 Kbps 2.94 Kbps	Q. Teach. Average Packet Rate C 5.48 ppr 2.19 ppr	15.44 Peak Bit Rate C 5.76 s 3.30 s	Sto User Name
I Capacity Flaming 0 Ninoski Parlomance Audit 0 av/Video Performance Va Istetwork 0 av/Video Performance Va Istetwork 0 cos Pennide DDCP Audit 0 A. Braje Bas XVIV Palh Cherges 0 activity Istetwork Performance 0 av/Video Enrose Provider Performance 0	C < Page	0 /4 3.9 Set IP Addr 0 198.19.2.102 198.19.2.82	Site Site C NV NV	See Pert 0 4218 5050	Det IP Addr 0 198.18.133.36 198.18.128.82	Det Ste C HQ HQ	Det Part C 1494 3970	Protocol © TCP TCP	DBOP C 0 (BE) 0 (BE) 0 (BE)	Application C loa sip	Total Rove C 13	Total Bytes C 527.85 KB 830.31 KB	Total Packeta 0 4900 1,972	Average Bit Rate C 1.69 Kbps 2.94 Kbps 2.05 Kbps	Q, Teach Average Packet Rate D 5.48 pp 2.19 pp 3.61 pp	1544 Peak Bit Rate C 5.79 K 3.30 K 2.51 K	Sic User Name Dat User Name Sic Sic Size Sic Size
N Capachy Planning 0 Nancosk Parformance Audh 0 on/Video Parformance Va. Histwark. 0 vto-Site Traffic Unitization Audit 0 otcs-Provider DDDP Audit 0 ok Brogle Sta WANY Path Changes 0	C < Page	V /4 3.3 Sec IP Addr C 198,19,2,102 198,19,2,82 198,19,2,102	Sec Site C NV NV NV	Sho Port C 4218 5050 1494	Det IP Addr C 198.18.133.36 198.18.128.82 198.18.133.36	Dat Site C HQ HQ HQ	Det Port © 1494 3970 4218	Protocol C TCP TCP TCP	DSCP 0 0 (86) 0 (86) 0 (86) 0 (86)	Application C loa Bip loa	Total Plane C 13 14 13	Total Bytes C 827.85 ×8 830.31 ×8 230.51 ×8	Totel Packets 0 4900 1,972 3,249	Average Bit Rate C 4.69 Kbps 2.94 Kbps 2.05 Kbps 1.75 Kbps	Q. Search . Average Packet Refe C 5.40 pp 2.19 pp 3.61 pp 5.48 pp 5.48 pp	15.44	Sic User Name Bit Sic IP Addr Bits Site Bits Site Bits Port
Capazity Flering     0       National Pedismocina Audit     0       Volden Pedinamocina Audit     0       to Shariba DOCP Audit     0       Standard Pedinamocina Audit     0       to Shariba DOCP Audit     0       Standard Shariba Pedinamocina     0       Kolden Schwarzbeich Pedinamocina     0       Kolden Schwarzbeich Pedinamocina     0       Standard Shariba Pedinamocina     0       Kolden Schwarzbeich Pedinamocina     0	C < Page	5 /4 > 2 5 to IP Addr C 198 19 2.102 198 19 2.102 198 19 2.102 198 19 2.102 198 18 133.36	Sec Site C NV NV NV HQ	Site Pert C 4218 5050 1494 1494	Det IP Addr C 198 18.133.36 198 18.128.82 198 18.133.36 198 19.2.102	Dat Site 0 HQ HQ HQ NY	Det Port © 1494 9970 4218 4218	Protocol C TCP TCP TCP TCP	0000P C 0 (840) 0 (840) 0 (840) 0 (840) 0 (840) 0 (840)	Application C los los los	Total Plane 0 13 14 13 13	Total Bytes 0 527.85 KB 330.31 KB 230.51 KB 197.20 KB	Total Packets 0 4930 1,972 3,249 4,930	Average Bit Rate C 4.69 Kbps 2.94 Kbps 2.05 Kbps 1.75 Kbps 1.63 Kbps	Q, Seensh Average Packet Rate C 5.48 pps 3.61 pps 3.64 pps 5.48 pps 2.35 pps 2.35 pps	15.44 Peak Br Rate C 5.76 a 3.30 k 2.51 k 2.16 k 2.57 s	Sto User Name Bto IP Addr Bto Site Bto Site Bto Port Dto IP Addr
Classicy Flaving         0           Statistick Flavinssica Addit         0           Video Performance Addit         0           Video Performance Addit         0           Statistick Flavinssica Addit         0           Statistick Flavinssica Addit         0           Statistick Flavinssica Addit         0           Statistic Statistica Addit         0           Statistic Additiona Statistica Additiona Addi	C < Page	5 / 4 > 2 5 to 1P Addr C 198 19 2.102 198 19 2.102 198 19 2.102 198 19 2.102 198 18 133.36 198 19 2.82	Site Site C NV NV NV HO NV HO HQ HQ	See Part C 4218 5060 1494 1494 3970 1137 4218	Det IP Addr C 198.18.133.36 198.18.128.82 198.18.128.82 198.19.2.102 198.19.2.102	Det Ster 0 HQ HQ HQ HQ HQ LA NY	Det Port © 1494 9970 4218 4218 8060	Protect C TCP TCP TCP TCP TCP TCP TCP	080P C 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80)	Application C los los los conferencing	Total Hows 0 13 14 13 13 13 10 10 54 14	Total Bytes C 527.85 KB 330.31 KB 230.51 KB 197.20 KB 183.07 KB 141.60 KB 131.76 KB	Total Packets 0 4,930 1,972 3,249 4,930 2,111	Average Bit Rate C 4.69 Kbps 2.94 Kbps 2.05 Kbps 1.75 Kbps 1.63 Kbps	Q, Seenth. Average Racket Rate C 5.40 pp 3.61 pp 5.41 pp 5.41 pp 5.43 pp 5.43 pp 5.43 pp 5.43 pp 5.43 pp 5.43 pp 5.43 pp 5.43 pp 5.44	Peak Bit Rate C 9 8.309 9 2.59 9 2.59 9 2.59 1 4.418 1 344	No. 112. 2017 93. 13. 133. 26. 710 Terrer Det User Name Det User Name
Classicy Floring     0       March Arkbringsvari Juhan     0       March Stands Standsvari Juhan     0       March Standsvari Juhan     0	E c. Page	5 (4 ) 3 5 tr P Addr C 198,19,2,102 198,19,2,102 198,19,2,102 198,19,2,102 198,19,2,102 198,19,2,103 198,18,133,36 198,18,133,36 198,18,133,36	SPC Site C NV NV HQ HQ HQ HQ HQ	See Part C 4218 5060 1494 1494 9970 1137 4218 21	Det IP Add: 0 198.18.132.35 198.18.122.82 198.19.22.82 198.19.2102 198.19.2102 198.19.2102 198.19.2102 198.19.101	Det Ste 0 HQ HQ HQ HQ LA NY LA	Der Port © 1484 9970 4218 4218 5060 21 1494 1197	Protection TCP TCP TCP TCP TCP TCP TCP TCP TCP	080P C 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80)	Application C los alp los conferencing flip los flip	Tetal Pleve C 13 14 13 13 13 10 14 14 14	Total Bytes C 827.65 KB 830.31 KB 230.51 KB 107.20 KB 103.07 KB 141.60 KB 131.75 KB 129.60 KB	Total Packets 0 4,930 1,972 3,249 4,930 2,111 3,540 2,244 8,245	Amerage Bit Rate C 4.69 Köps 2.05 Köps 1.75 Köps 1.68 Köps 1.68 Köps 1.55 Köps 1.15 Köps 1.15 Köps	Q, Seeth- Average Packet Rete C 5.40 pp 3.61 pp 5.41 pp 5.41 pp 3.63 pp 3.63 pp 3.64 pp 3.64 pp 3.64 pp 3.64 pp 3.64 pp 3.61 pp	Peak Bic Rate C 9 5.76 # 9 2.01 # 9 2.05 # 9 2.05 # 9 2.05 # 1.41 # 9 1.34 # 9 1.34 #	No. 19.2. YEL
II Capachy Flaming 0 Nakiwak Performance Audit 0 os (Vidao Performance Va. Tetstoch 0 os Panalde DDCP Audit 0 dica Panalde DDCP Audit 0 dication Va. Tetstoch Performance 0 dication Va. Tetstoch Performance 0 dication Service Providee Performance 0	E < Page	5437 5437 198.19.2.102 198.19.2.102 198.19.2.102 198.19.2.102 198.19.2.82 198.19.2.82 198.19.2.82 198.18.133.36	Site Site C NV NV NV HO NV HO HQ HQ	See Part C 4218 5060 1494 1494 3970 1137 4218	Det IP Add: C 198.18.123.36 198.18.128.82 198.18.128.82 198.19.2.102 198.18.128.82 198.19.1.101 198.19.2.102	Det Ster 0 HQ HQ HQ HQ HQ LA NY	Det Port © 1494 9970 4218 4218 5060 21 1494	Protect C TCP TCP TCP TCP TCP TCP TCP	080P C 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80) 0 (80)	Application C los los los optimenoing fip los	Total Hows 0 13 14 13 13 13 10 10 54 14	Total Bytes C 527.85 KB 330.31 KB 230.51 KB 197.20 KB 183.07 KB 141.60 KB 131.76 KB	Total Packets () 4900 1,972 3,249 4,980 2,111 3,540 3,294	Average Bit Rate C 4.69 Kbps 2.04 Kbps 1.05 Kbps 1.75 Kbps 1.26 Kbps 1.26 Kbps 1.26 Kbps 1.26 Kbps 1.17 Kbps 0.17 Kbps 0.05 Kbps	Q Search. Average Packet Rev C 2/3 pp 2/3 cl pp 3/41 pp 3/41 pp 3/45 p	Peak Bit Rate C Peak Bit Rate C 5.79 s 2.51 s 2.51 s 2.51 s 1.24 s 1.34 s 1.34 s 1.34 s 2.24	Bro Over Name     Bro Over Name     Det Uver Name     Det Uver Name     Det Uver Name     Son IP Adde     Son Die     Son Die     Son Die     Det IP Adde     Det Ste      Det Ste      Des      Des

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

# Lab 8

Lab 8: QoS

# Lab 8.1: QoS Marking Policy

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

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

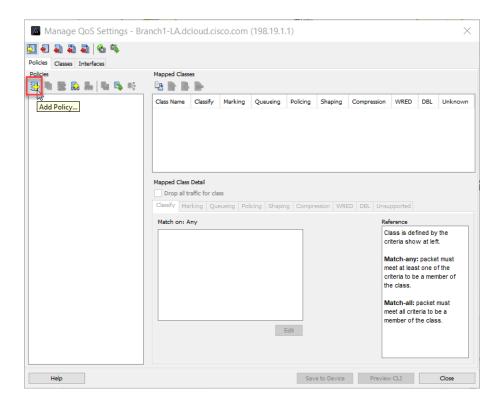
Lab Steps:

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

LiveNX - a9a56379b8-liveaction.pods.criterionnetworks.com

File View Use	rs QoS Flow Ro	outing IP SLA LAN Too	ols Reports H	elp		
Dashboard   Manag	e 🗈 Expa	QoS Flow Routing	IP SLA LAN			
Q-		🕂 🔶 🔀 🖊 🗔 📲	🗞 🔍 🛛 Table 🕇	🕑 Ref	resh All Flow Types 🗸 Current Time 🔨	Current
Name		Search Example: (site = Hono	lulu   site = Chicago	) & wa	an & flow.app = webex-meeting	
■ A Home	2			1		Local
⊡· NY	evice: Branch1-LA.do	cloud.cisco.com	>	~	Enable QoS Polling	
🕀 🛞 в	Flow		>		Manage QoS Settings	
	Routing		>		Revert QoS Configuration	
	IP SLA		>		Manage NBAR	
			>		Apply Policy to Interfaces	
					Remove Policy from Interfaces	
	Edit Device Setting Add or Remove Int	•			Copy Policy to Devices	
	Refresh Device	lenaces			Reports	
	Remove Device			-		S
	Zoom to Device					
	Device Tools		>			
	Statistics		>			
	View		>			
	Group Manageme	nt	>			
				1	LA RC 1921/02/1	

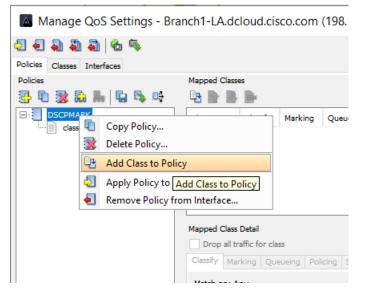
9. Click the Add Policy Icon.



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

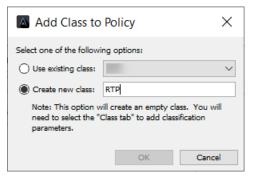
Add Policy ×						
Policy name: DSCPMARK						
ОК	Cancel					

- 11. We are going to add two classes to this policy: RTP and SIP
- 12. Right Click on your new "DSCPMARK" policy and select "Add Class to Policy"

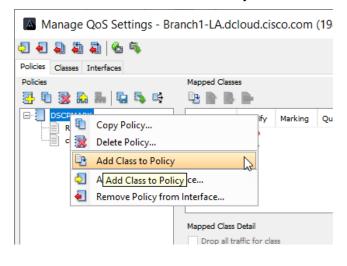


13. Select "Create a new class" and give the class a name RTP.

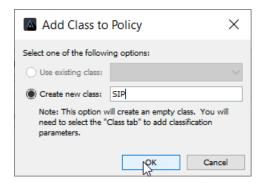
### 14. Click OK



#### 15. Select "Add Class to Policy"



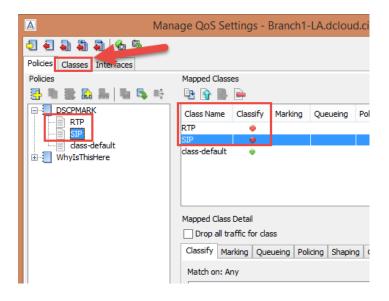
- 16. Click Create new class, Label it SIP.
- 17. Click OK.



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

Manage QoS Settings - Br	anch1-LA.dcloud.cisco.com (
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>	
Policies	Mapped Classes
📑 🗓 🖹 🔒 🐜 🗳 📑	
	Class Name Classify Marking
class-default	RTP SIP class-default
	Mapped Class Detail
	Drop all traffic for class
	Classify Marking Queueing Polic

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



Select and match the SIP class...

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

Manage QoS Settings -	Branch2-NY.dcloud.cisco.co	om (198.19.2.1)	~~~~~	×
4 4 4 4 4				
Policies Classes Interfaces				
Classes Create and Ed	lit Match Statements			
🔁 🖻 🕱 🐘	2		Match any 🗸 🐹	
RTP Match	type: ACL Name	$\sim$	match any 🗸 🦗	
	/alue: ACL-INET-PUBLIC	^	Ma Match Ty Value	
	BEST_EFFORT		Match ACL Name SIPQoSMar	k
	CRITICAL			
	DENY_GLOBAL_LEARN_LIST			
	RDP RTPQoSMark			
	3 SIPQoSMark			
	VOICE_VIDEO	¥		
Match/match	n not: Match	~		
	Add Match Statement	Replace Match Statement		
	<b>4</b>			
	-			
Help		Save to I	Device Preview CLI	Cancel

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

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

🛯 Manage QoS Settings - Bra	nch2-NY.dcloud.cisco.com (198.19.2.1)			$\times$
4 4 5 5 5				
Policies Classes Interfaces				
Classes Create and Edit Mat				
RTP Match type:	ACL Name 2	$\sim$	Match any \vee 🗱	
	ACL-INET-PUBLIC	~	Ma Match Ty Value	
	BEST_EFFORT CRITICAL		Match ACL Name RTPQoSMark	
	DENY_GLOBAL_LEARN_LIST			
	RDP	_		
3	RTPQoSMark SIPQoSMark			
	VOICE_VIDEO	¥		
Match/match not:	Match	$\sim$		
4	Add Match Statement Replace Match Stat	ement		
Help		Save to De	vice Preview CLI Cancel	

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

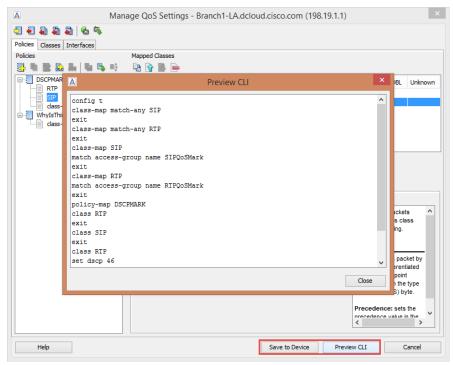
Manage QoS Settings - Bra	anch2-NY.dc	loud.ci	sco.com	(198.19.2	.1)					×
Policies Classes Interfaces										
Policies	Mapped Classe	s								
📴 🖷 🖹 🔝 🐜 🖷 🖏 🗠	Pe 🖹 🕓	<b>-</b>								
	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
SIP C	RTP		DSCP: BE							
class-default	SIP									
	class-default	•								
	Mapped Class	lief								
		3 or cla								
					-					
	Classify Mar	king Qu	eueing Pol	icing Shapir	ng Compre	ession WRI	ED DBL Unsu	pported		
	Mark with:						Ref	erence		
								fferentiate		
		5CP	~ O (E	3E)	~			elonging to		SS
		Tunnel	42 43		^		Da	ased on m	arking.	
		IP	43				м	ark On		
	_	_	45					SCP: mark		kat by
		1 Cell Loss	Priority 46 (	EF)	(4)			etting the d		
	Fran	me Relay D	Discard E		15			ervices co		
			48 ( 49	C56)	<b>v</b>			alue in the		service
			43		Ŧ		σ	OS) byte.		
							D	recedend	e cate	the
								ecedence		
							pa	cket head	ler.	
Help					<b>C</b>	e to Device	Preview	CIT		Cancel
Help					Save	e to Device	Preview			Cancer

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

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

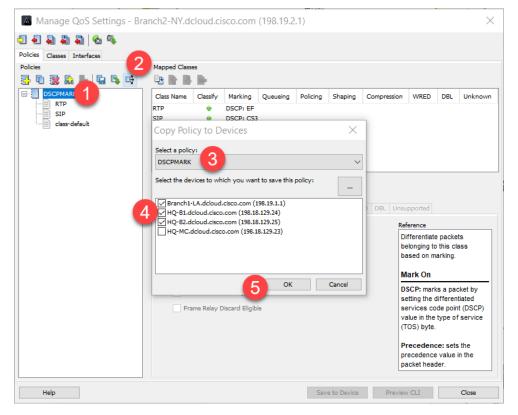
Manage QoS Settings - Bra	anch2-NY.dcloud.cisco.com (198.19.2.1)	$\times$
Policies Classes Interfaces		
Policies	Mapped Classes	
	Image: State of the s	Jnknown
	RTP DSCP: BE	
class-detault	SIP    DSCP: BE  class-default	
	Mapped Claring in Class	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Mark with: Reference	
	DSCP V 0 (BE) V Differentiate packets belonging to this class	3
	Tunnel 21 based on marking.	
	1P 23 Mark On DSC Pt marks a packa	
	ATM Cell Loss Priority 25	ted
	Frame Relay Discard E 26 (AF31) 27 28 (AF32) V (TOS) Index	
	(TOS) byte.	
	Precedence: sets th precedence value in t	
	packet header.	
Help	Save to Device Preview CLI Ca	ancel

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



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

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



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

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

Copy Policy to Devices	×
Saving to devices	
Branch1-LA.dcloud.cisco.com (198.19.1.1) 👳 Succeeded	
HQ-B1.dcloud.cisco.com (198.18.129.24) 💗 Succeeded	
HQ-B2.dcloud.cisco.com (198.18.129.25) 💗 Succeeded	
Export CSV Cancel Close	

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

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

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

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

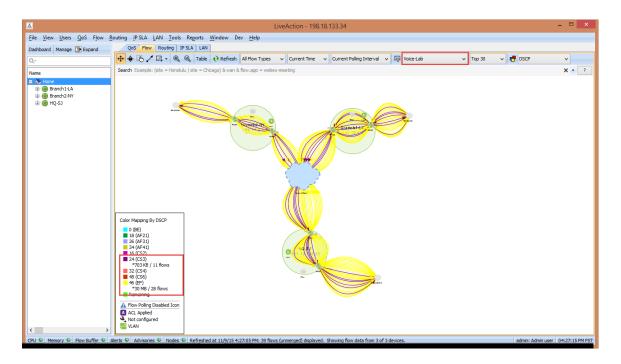
oard Manage		nable Polling 🕠 Pause Display Vie	w Flows by Port 👻 🎧 Fill Chart 🛛	Collector Polling : 10 seconds
		GigabitEthernet1 Input		
		olgabilization acti input	Turne	
Home				
но 🗄 🛞 но-в1		Port		
🕀 🛞 но-вг				
🗄 🛞 но-мс				
LA Branch1-L	•			
🤄 🌐 Gigabi	Ethernet1			
w Gig		Icloud.cisco.com - GigabitEthe		
🛛 🌍 Gig	Qos 2		>	
NY	Flow		>	
	Routing		>	
	IP SLA		>	
	LAN		>	
	Edit Device Settings			Manage NBAR
	Add or Remove Inte	rfaces		Apply Policy to Interface Remove Policy from Interface
	Refresh Device			Remove Policy from Interface
	Remove Device			Reports
	Zoom to Device			
	Device Tools		>	
	Statistics		>	
	View		>	—
	Group Management		>	
		Port		

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

Apply Policy to Interfaces	$\times$
Select a policy: DSCPMARK	$\sim$
Select the interfaces to which you want to apply this policy:	
🦾 🔲 🍐 Output	
OK Canc	
OK Cano	.ei

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

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



## Lab 8.2: QoS Queueing Policy

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

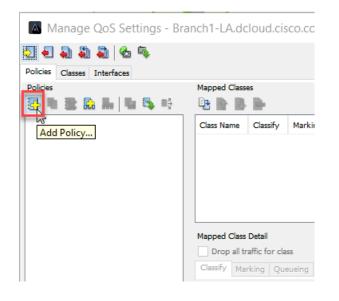
Now that you've verified your traffic is marked correctly through the network, using Netflow, you can create a queuing policy to protect the critical traffic.

Lab Steps:

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

me Home Home Branch 1 Branch 1	♦ ♦ ि / L +		
HQ-SJ	QoS		Enable QoS Polling
-	Flow	•	Manage QoS Settings
	Routing	+	Revert QoS Configuration
	IP SLA	•	Manage NBAR
	LAN	•	Apply Policy to Interfaces
	Edit Device Settings		Remove Policy from Interfaces
	Add or Remove Interfaces		Copy Policy to Devices
	Refresh Device		Reports
	Remove Device		4-14 1
	Zoom to Device		
	Device Tools	•	
	Statistics	•	
	View	•	
	Group Management	•	

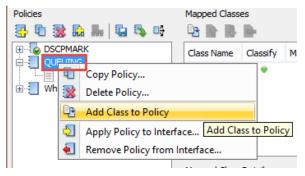
- 47. Select the **Policies** Tab.
- 48. Click Add Policy to create a queuing policy.



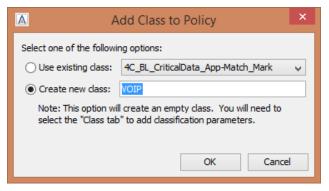
49. Name the new policy QUEUEING.



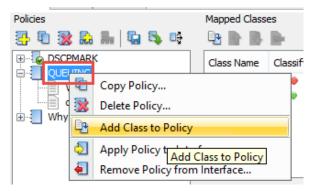
50. Right-click on the new QUEUEING Policy, select Add Class to Policy.



- 51. Create a new class labeled VOIP.
- 52. Click OK.



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



- 54. Create a new class and label it SIGNALING.
- 55. Click OK

Δ	Add Class to Policy								
Select one of the following options:									
O Use existing clas	ss: 4C_BL_CriticalData_App-Match_Mark	¥							
Oreate new class	s: SIGNALING								
Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.									
	OK Cance	1							

Configure VOIP Class:

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

	Manag	e QoS Settings - Branc	h1-LA.dcloud.cisco.com	(198.19.1.1)	×
	🏀 🖏				
Policies Classes	faces				
Classes	Create and Edit Mat				
📴 🖪 😥 🚩		3		Match any 🗸 🞇	
4C_BL_CriticalDat	Match type:		*	materiary v 🙀	
4C_BL_Realtime_/	Value:		^	M Match T Value	
4C_BL_Scavenger		45		Ma DSCP 46 (EF)	
4C-MN_CONTROL	(4)	46 (EF) 47			
4C-MN_CRITICAL 4C-MN_REALTIME	-	48 (CS6)			
RDP		49			
RTP		50			
SIGNALING		51 (Select up to 8 values)	×		
SIP					
	Match/match not:		¥		
		IPv4 Only			
	5	Add Match Statement	Replace Match Statement		
< >					
Help			Save to Devic	ce Preview CLI	Cancel

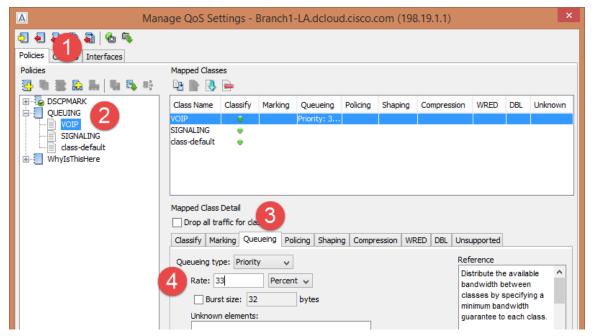
Configure SIGNALING Class:

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

Manag	ge QoS Settings - Branch1-LA.dcloud.cisco.com	ו (198.19.1.1)	×
44224			
Policies Classes Interfaces			
Classes Create and Edit Ma	tch Statem		
Match type:	DSCP 🗸	Match any 🗸 🐹	
4C_BL_CriticalDat 4C_BL_Realtime_A Value:	17 ^	M Match T Value	
4C_BL_Scavenger	18 (AF21)	Ma DSCP 24 (CS3)	
4C-MN_CONTROL	19		
4C-MN_CRITICAL	20 (AF22) 21		
4C-MN_REALTIME	22 (AF23)		
RDP	23		
SIGNALING 3	24 (CS3)		
SIP	(Select up to 8 values)		
VOIP Match/match not:	Match 🗸		
	IPv4 Only		
4	Add Match Statement Replace Match Statement		

Setup VoIP Priorities:

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



Setup Signaling Priorities:

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

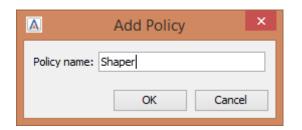
	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>		
Policies	Mapped Classes	
	. 🖷 📴 🐘 📄	
	Class Name Classify Marking Queueing Policing Shaping Compress	sion WRED DBL Unknown
	VOIP   Priority: 3	
	SIGNALING 🔶 Class-bas	
dass-default	class-default 👳	
WhyIsThisHere		
	Mapped Class Detail	
	Classify Marking Queueing Policing Shaping Compression WRED DBL	Unsupported
	Queueing type: Class-based v	Reference
	3 Rate: 7 Percent V	Distribute the available
	Rate: 7 Percent v	bandwidth between
	Queue depth: 1 Bytes V	classes by specifying a minimum bandwidth
	Enable Fair Queueing	guarantee to each class.
	Unknown elements:	
		Queueing Type
		Class-based: utilizes
		Class-based weighted fair
		queueing (CBWFQ) using derived weight for packets
		from the bandwidth
		allocated to the class
Help	Save to Device Previ	ew CLI Cancel

Create a Shaping Policy:

67. Click Add Policy.

친 🗐 🗿 🗿 🗿 🚳 🦻
Policies Classes Interfaces
Policies
🛃 🖲 🔡 🏫 🛼 🖏 🖏 🤫
Add Policy RK
VOIP
SIGNALING
dass-default
😟 🔄 WhyIsThisHere

68. Give the Policy a name of Shaper.



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

A Man	age QoS Settings - Branch1	-LA.dcloud.cisco.d	com (198.19.1.1)	×
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>				
Policies	Mapped Classes			
	Class Name Classify Marking class-default •	Queueing Policing	Shaping Compression	on WRED DBL Unknown
SIGNALING dass-default				
under the second secon				
	Mapped Class Detail	2		
	Classify Marking Queueing Po	licing Shaping Compre		Insupported
	Shape using: Average V			Reference Control the flow of traffic ^
	3 Rate: 1500 Kbps			and eliminate bottlenecks by delaying packets and
	Committed burst: 256	bits		conforming to a specified bit rate.
	Unknown elements:			Rate
				Peak: allows the transmission rate to burst higher than the shaping rate.
				Average: sets the maximum transmission
Help		Save to	Device Previe	w CLI Cancel

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

Mar	nage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>		
Policies	Mapped Classes	
Social and a second secon	Class Name     Classify     Marking     Queueing     Policing     Shaping     Compression     WRED     DBL     Unknown       VOIP     •     Priority: 3     SIGNALING     •     Class-bas       SIGNALING     •     Class-bas	
	Mapped Class Detail         Drop all traffic for class         Classify       Marking       Queueing       Policing       Shaping       Compression       WRED       DBL       Unsupported         Shape using:       None       V       Reference	
	Control the flow of traffic A and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.	
	Rate Peak: allows the transmission rate to burst higher than the shaping rate.	
	Average: sets the maximum transmission	
Help	Save to Device Preview CLI Cancel	

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

A Mar	nage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>		
Policies	Mapped Classes	
	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unkr	nown
VOIP SIGNALING dass-default Shaper dass-default WhyIsThisHere	VOIP Priority: 3 SIGNALING Class-bas dass-default	
	Mapped Class Detail	
	Drop all traffic for class	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Shape using: None v	

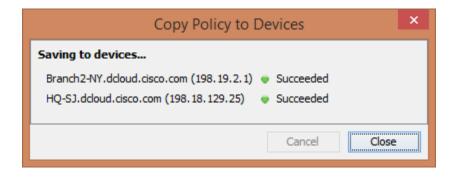
Copy the shaping policy to the other devices:

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

	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)
Image: Second system     Image: Second system       Policies     Classes       Policies       Image: Second system       Image: Second system	Apped Classes
OSCPMARK     QUEUING     VOIP     SIGNALING     dass-ouvolit     QUEUING     QUEUING     WhyIsThisHere	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown class-default • 1,500 Kbps Copy Policy to Devices Select a policy: Select the devices to which you want to save this policy:  PBL Unsupported Reference Control the flow of traffic ^ and eliminate bottlenecks by delaying packets and conforming to a specified bit rate. Rate Peak: allows the transmission rate to burst higher than the shaping rate. Average: sets the maximum transmission v
Help	Save to Device Preview CLI Close

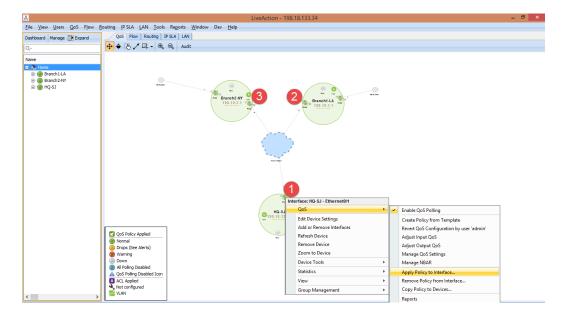
78. Click Close.

79. Click OK.



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

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

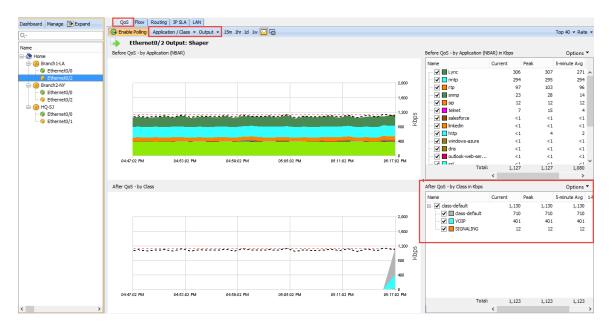


81. Select the Shaper Policy and the Output for the WAN interface.

Apply Policy to Interfaces	×
Select a policy:	
Shaper	~
Select the interfaces to which you want to apply this policy:	
OK Cancel	

82. Click **OK**.

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



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

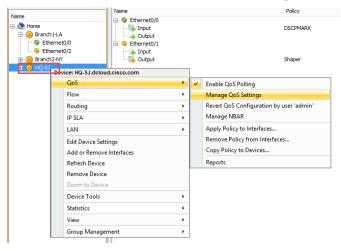
## Lab 8.3: QoS Verification

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

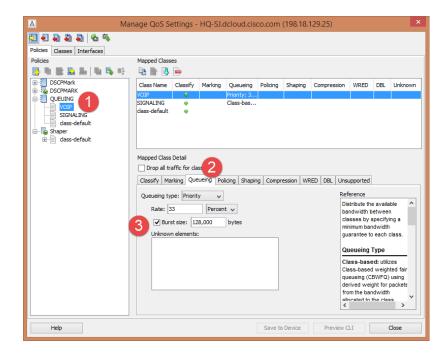
Since there seem to be drops on our device, let's investigate the drops and add a more granular QoS configuration.

Lab Steps:

Select a device and select QoS and Manage QoS Settings.



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

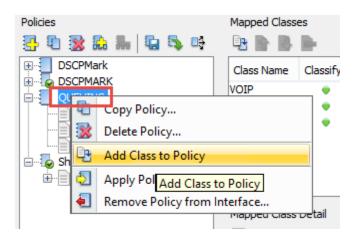


Note: Configuring a burst rate is something that is not always common and should be fully understood before looking to implement in your own network.

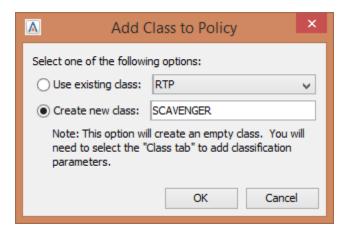
Read more about configuring a burst rate here: http://www.cisco.com/c/en/us/td/docs/ios/12\_2/qos/configuration/guide/fqos\_c/qcfpolsh.html

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

- 86. Right-click on the **QUEUEING** Policy.
- 87. Select Add Class to Policy.



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



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

	Mana	ge QoS Settings - HQ	-SJ.dcloud.cisco.com (198	8.18.129.25)	×
a a 🎝 🖏	- 6 5				
Policies Classes	aces				
Classes	Create and Edit Ma	ch Statements 3			
📑 🖻 🕱	Match type:	Protocol - using NBAR	¥	Match any 🖌 💥	
RTP SCAVENGER	2 Value:	bhmds	^	M Match T Value	
SIGNALING		binary-over-http bittorrent		Ma Protocol bittorrent	
SIP VOIP	4	bittorrent bittorrent-networking		Ma Protocol bittorrent-networking	
	· · · ·	bl-idm			
		blizwow			
		blogger bmpp	~		
	Match/match not:	Match	¥		
	5	Add Match Statement	Replace Match Statement		

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

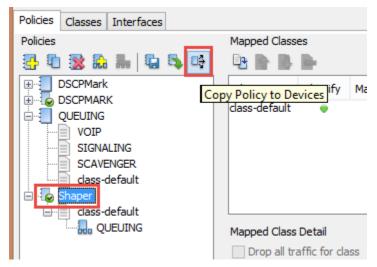
A	Ianage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)	×
<ul> <li>Policies</li> <li>ses</li> <li>Interfaces</li> </ul>		
Policies	Mapped Classes	
DSCPMark DSCPMARK UEUING VUEUING SIGNALING SCAVENCEF dass-default	Class Name       Classify       Marking       Queueing       Policing       Shaping       Compression       WRED       DBL       Unkn         VOIP       Priority: 3       Class-bas       Class-bas       SCAVENGER       Class-bas         SCAVENGER       Class-bas       Class-bas       Class-bas       Mapped Class Detail       Mapped Class Detail       Drop all traffic for class         Classify       Marking       Queueing       Shaping       Compression       WRED       DBL       Unsupported	own
	Queueing type:       Class-based v       Reference         Queue dept:       1       Percent v       Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. trom the bandwidth allocated to the class	~
Help	5 Save to Device Preview CLI Cancel	

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

A Ma	nage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)	×
<ul> <li>Policies</li> <li>Classes</li> <li>Interfaces</li> </ul>		
Policies	Mapped Classes	
DSCPMark DSCPMARK UUEUING SIGINALING SCAVENGER dass-default Shaper	Class Name Classify Marking Queueing Policing Shaping Compre WRED DBL VOIP Priority: 33% SIGNALING Class-based: 7% SCAVENGER Class-based: 1% class-default	U
Cueuring	Mapped Class Detail         Drop all traffic for dass         Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported         Queueing type:       Class-based          Rate:       1         Percent       V         Queue depth:       1         Packets       V         Classe by specifying a minimum bandwidth guarantee to each classe.	^
	Unknown elements: Class-based: utilizes Class-based: utilizes Cla	ts V
Help	Save to Device Preview CLI Cancel	

Copy the updated policy to other devices in the topology.

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



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

Copy Policy to Devices	×
Select a policy: Shaper	•
Select the devices to which you want to save this policy:	
<ul> <li>✓ Branch 1-LA.dcloud.cisco.com (198.19.1.1)</li> <li>✓ Branch 2-NY.dcloud.cisco.com (198.19.2.1)</li> </ul>	
OK Cance	

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

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

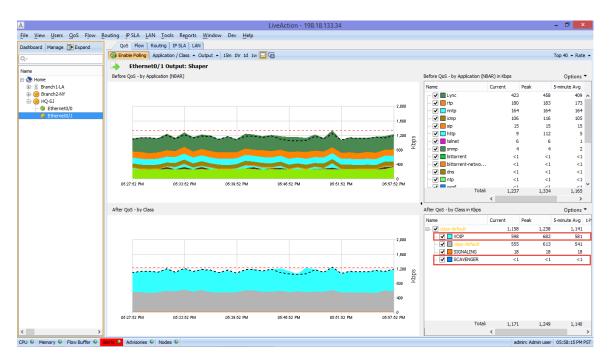
Copy Policy to Devices	×
Conflicts were encountered when saving the policy on device Branch 1-LA.dcloud.cisco.com (198.19.1.1). The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?	
Shaper - Overwritten (A policy with the same name exists) class-default Shaping: 1,500,000 bps QUEUING - Overwritten (A policy with the same name exists) VOIP VOIP VOIP Queueing: Priority 33% Match DSCP "46 (EF)" SIGNALING Queueing: Class-based 7% Match DSCP "24 (CS3)" SCAVENGER Queueing: Class-based 1% View all conflicts View all conflicts Overwrite Skip Cancel	< <

Ensure the copy is successful.

104. Click **Close**.

Copy Policy to Devices	×
Saving to devices Branch1-LA.dcloud.cisco.com (198.19.1.1) Succeeded Branch2-NY.dcloud.cisco.com (198.19.2.1) Succeeded	
Cancel	Close

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



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

# Lab A

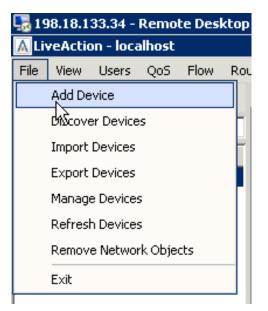
Lab A: Appendix

## Lab A.1: Add Device

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

Lab Steps:

1. Select File, Add Device



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

Add	Device			×
Ste	ps	Device Connection Inf	formation	
1.	Device Connection Information	Enter the SNMP conne	ection information.	
2.	CLI Settings (Configuring)	Node	Local	~
	CLI Settings (Monitoring) Select Interfaces	IP Address	198.19.1.1	
5.	Select VLANs	O Non SNMP device	such as NetFlow probes	
6.	Select Features	◯ LiveSensor		
7.	Enable Polling	Use the Default S	NMP connection settings	Edit
8.	Review Configuration	O Enter SNMP conne	ection settings for this device	
9.	Device Updated	SNMP Version	Version 2c	V Target Port 161
		Community String		
		< Back Next 3	> Finish	Cancel Help

5. Select "Use my default Configuration CLI connection settings".

Information         an asterisk (*).           2. CLI Settings (Configuring)         Configuration CLI Connection Settings           3. CLI Settings (Monitoring)         Enter Command Line Interface (CLI) connection settings used to configure these devices.	Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*). Configuration CLI Connection Settings Enter Command Line Interface (CLI) connection settings used to configure these devices. C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp C Use my default Configuration CLI connection settings C Enter connection settings for this device Connection Type SSH P Port* 22 User name on Device Password on Device* Enable Password	dd Device - HQ-SJ.dcloud.ci	sco.com (198.18.129.25)	
Information       an asterisk (*).         2. CLI Settings (Configuring)       Configuration CLI Connection Settings         3. CLI Settings (Monitoring)       Enter Command Line Interface (CLI) connection settings used to configure these devices.         4. Select Interfaces       C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and S. Select VLANs         6. Select Features       C Use my default Configuration CLI connection settings         7. Enable Polling       Enter connection settings for this device         8. Review Configuration       Connection Type         9. Device Updated       User name on Device         Password on Device*	an asterisk (*).  Configuration CLI Connection Settings Enter Command Line Interface (CLI) connection settings used to configure these devices.  Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp C Use my default Configuration CLI connection settings Edit C Enter connection settings for this device Connection Type SSH Port* Enable Password Enable Password	Steps	CLI Settings (Configuring)	
(Configuring)       Configuration CLI Connection Settings         3. CLI Settings (Monitoring)       Enter Command Line Interface (CLI) connection settings used to configure these devices.         4. Select Interfaces       C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and Configuration CLI Connection settings)         5. Select VLANs       C Use my default Configuration CLI connection settings)         6. Select Features       C Enter connection settings for this device         7. Enable Polling       C Enter connection Type SEH Port* 22         9. Device Updated       User name on Device         Password on Device*       Password on Device*	Enter Command Line Interface (CLI) connection settings used to configure these devices. Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp Use my default Configuration CLI connection settings Edit C Enter connection settings for this device Connection Type SSH P Port* 22 User name on Device Password on Device* Enable Password			with
Select Inter Commande Line Inter de (CL) connection settings Used to compare dises devices.     C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and     C Select Features     C Enter connection settings for this device     C Enter connection settings for this device     C Connection Type SSH P Port* 22     Device Updated     User name on Device     Password on Device*	C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp C Use my default Configuration CLI connection settings Edit C Enter connection settings for this device Connection Type SSH Port* 22 User name on Device Password on Device* Enable Password		Configuration CLI Connection Settings	
Select VLANs     C Add as monitor only device for hor Cisco and disapported cisco OS (105), 105-x2 and     C Select VLANs     C Use my default Configuration CLI connection settings     Edit     C Enter connection settings for this device     Review Configuration     Connection Type     SSH     Port*     Port*     Port*     Password on Device	Use my default Configuration CLI connection settings     Edit      Center connection settings for this device     Connection Type     SEH     Port*     Z2      User name on Device      Password on Device*      Enable Password	3. CLI Settings (Monitoring)	Enter Command Line Interface (CLI) connection settings used to configure these devices.	
Select Features     C Use my default Configuration CLI connection settings     Edit     C Enter connection settings for this device     Connection Type SSH  Port* 22      Device Updated     User name on Device     Password on Device*	C Enter connection settings for this device Connection Type SSH V Port* 22 User name on Device Password on Device* Enable Password	4. Select Interfaces	C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS s	ddr
Select Features     C Enter connection settings for this device     Enter connection Type SSH Point* 22     User name on Device     Password on Device*	C Enter connection settings for this device Connection Type SSH V Port* 22 User name on Device Password on Device* Enable Password		Use my default Configuration CLI connection settings     Edit	
7. Enable Polling     Connection Type       8. Review Configuration     Connection Type       9. Device Updated     User name on Device       Password on Device*	Connection Type SSH y Port* 22 User name on Device Password on Device* Enable Password			
9. Device Updated User name on Device Password on Device*	User name on Device Password on Device* Enable Password	-		
Password on Device*	Password on Device* Enable Password	-		
	Enable Password	5. Device opulated		-
Lilable Password	,			-
Also use these credentials for monitor mode.			,	
			< Back Next > Finish Cancel Help	

Steps       CLI Settings (Monitoring)         1. Device Connection Information       Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).         2. CLI Settings (Configuring)       Monitor-only CLI connection Settings (Monitoring)         3. CLI Settings (Configuring)       Monitor-only CLI connection Settings Enter Command Line Interface (CLI) connection settings used to monitor this device.         4. Select Interfaces       Use the previous page connection settings         5. Select VLANs       Enter connection settings for this device         6. Select Features       Enter connection settings for this device         7. Enable Polling       Connection Type SSH Port* 22         8. Review Configuration       User name on Device         9. Device Updated       User name on Device Password

- 7. Select "Use the previous page connection settings".
- 8. Click Next.

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

9. Click Continue.

Test	Status	Description	
SNMP connection		Succeeded	
SNMP access	•	Succeeded	Ī
CLI configure connection	0	Skipped	
CLI configure login	$\odot$	Skipped	
CLI configure enable password	0	Skipped	
CLI monitor connection	0	Skipped	
CLI monitor login	$\odot$	Skipped	
CLI monitor enable password	$\odot$	Skipped	
Serial number validation	•	Succeeded	
Model supported	•	Succeeded	
IOS supported	•	Succeeded	
NBAR capable	•	Succeeded	
NBAR2 capable	۲	Succeeded	
NetFlow collector configure supported		Succeeded	
Flexible NetFlow supported		Succeeded	
Unified Perfmon supported		Succeeded	
Medianet Performance Monitoring supported	•	Succeeded	
AVC supported	•	Succeeded	
MLS NetFlow configure supported	$\odot$	Not supported	
Mediatrace configure supported	•	Succeeded	
IP SLA Supported	•	Succeeded	
HQF Supported	•	Succeeded	
MAC Table Supported	0	Not supported	ľ

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

Add Device - HQ-SJ.dcloud.cis	co.com	(198.18.	129.25)			×
Steps	Select	Interface	is			
1. Device Connection Information	Select	the interf	aces you want to	monitor on this de	vice (maximum 100	0 interfaces).
2. CLI Settings (Configuring)	S	ielected	Interface	Trunk	IP Address	Description
3. CLI Settings (Monitoring)			Ethernet0/0		198.18.129.25	
4. Select Interfaces			Ethernet0/1 Loopback0		10.255.0.2 10.0.0.102	
5. Select VLANs			NullO			
6. Select Features			Tunnel0			PFR auto-tunnel for VRF default
7. Enable Polling			VoIP-NullO			
8. Review Configuration						
9. Device Updated						
	Sale	ucted inter	face(\$): 3			
	Dele	eceu incer	1000(5): 0			
	< Ba	ck	Next >	Finish		Cancel Help

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

Add Device - HQ-SJ.dcloud.cise	o.com (198.18.129.25)	×
Steps	Select VLANs	
Steps         1. Device Connection Information         2. CLI Settings (Configuring)         3. CLI Settings (Monitoring)         4. Select Interfaces         5. Select VLANS         6. Select Features         7. Enable Polling         8. Review Configuration         9. Device Updated	Select VLANs Select the VLANs you want to monitor on this device (maximum 25 VLANs). No VLANs were found on the device. No VLANs will be managed.	
	< Back Vext > Finish Cancel Help	

11. Click Next.

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

each feature in the Help
NetFlow
ব্ব
Ŀ\$

13. Change the polling rate to 30 seconds.

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

Steps	Enable Polling
1. Device Connection Information	Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section.
2. CLI Settings (Configuring)	
8. CLI Settings (Monitoring)	
. Select Interfaces	
. Select VLANs	Polling Rate 30 seconds
. Select Features	
. Enable Polling	Poll the following features
. Review Configuration	
. Device Updated	V Qo5
	IF SLA
	Routing
	LAN*
	* LAN polling occurs every 15 minutes
	* For SNMP v3, please see the User Guide on configuring LAN polling.
	k
	< Back Next > Finish Cancel Help

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

eps	Review Configuration	
eps   Device Connection Information  CLI Settings (Configuring)  Select Interfaces  Select VLANs  Select Features  Enable Polling  Review Configuration  Device Updated	Review Configuration The following commands will be sent to the device. Or you can choose to manually configure the yourself. description D0 NOT MODIFY. USED BY LIVEACTION. exporter LIVEACTION-FLOWEXPORTER cache timeout inactive 10 cache timeout active 60 record LIVEACTION-FLOWECORD exit interface EthernetO/1 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output exit interface EthernetO/0 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output exit interface Loopback0 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output	Jevice
		-
	Send the configuration commands to device.	
	C I will manually configure the device myself.	

- 15. Select "Send the configuration..." radio button, if available.
- 16. Click Next.

### 17. Click Finish.

iteps	Device Updated				
1. Device Connection Information	You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):				
2. CLI Settings (Configuring)	Device Settings				
3. CLI Settings (Monitoring)	Setting		Description		
4. Select Interfaces	Polling Rate		30 seconds		
5. Select VLANs	NetFlow Monitoring		NetFlow collector		
5. Select Features	NetFlow Polling		Enabled		
7. Enable Polling	Mediatrace		Disabled		
2	Adjacency Polling		Enabled		
<ol><li>Review Configuration</li></ol>	Qos Polling IP SLA Polling		Enabled Enabled		
9. Device Updated	CEF		Enabled		
	Interface Settings	1010	l Notelou		
	Interface Ethernet0/1	NBAR	NetFlow		
	Ethernet0/0				
	Loopback0	•	•		
	,				

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

## Lab A.2: Client Device Discovery

As we discovered in a prior Lab, the LiveNX Server in your topology has had device(s) preinstalled. 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.

🔜 198.18.133.34 - Remote Deskto							
🛦 LiveAction - localhost							
File	View	Users	QoS	Flow	Re		
Add Device							
	Discove	er Device	s				
	Import	Devices					
Export Devices							
Manage Devices					Γ		
Refresh Devices							
Remove Network Objects							
Exit							

- Specify the following IP addresses: 198.19.1.1 198.19.2.1
- 3. Select Use the default SNMP connection settings.

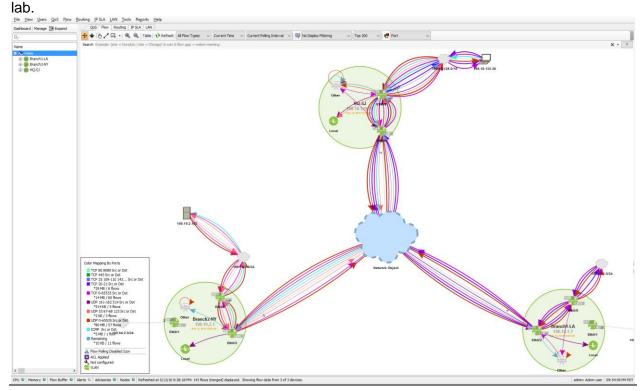
Device Discovery	×
Step 1: Specify v	vhat to scan
Specify IP range	es (ex: 192.168.1.1-200) or one IP per line:
198.19.1.1 198.19.2.1	
C Specify seed de	vice to scan
IP Address	Hops 1
Step 2: Specify S	NMP settings
Output Use the Default	SNMP connection settings Edit
C Enter SNMP con	nection settings for this device
SNMP Version	Version 2c Target Port 161
Community Strin	g 🛛

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

Step 3: Specify node		
Local		Ŧ
	ОК	Cancel

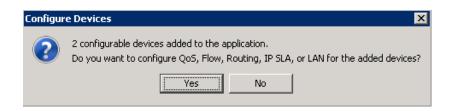
- 4. Click OK.
- 5. Verify that both devices were found, and then select Add Devices.

**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



🛦 Device Discove	ry on Local				×
Filter by:		Filter	Clear		
Select	Device Name	IP Address	Hops	Vendor	Model
	Branch2-NY.dcloud.cisco.com	198.19.2.1	0	Cisco	ciscoGatewayServer
V	Branch1-LA.dcloud.cisco.com	198.19.1.1	0	Cisco	ciscoGatewayServer
1					
Selected: 2	Discovered: 2 Device Limit: 10,	000,000 (1 active devices)			
		Add Devices Adva	nced Add	Pause	Stop

6. Select Yes on the configure devices dialog.



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

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

Configure Cisco Devices			×
Steps	SNMP Settings		
<ol> <li>SNMP Settings</li> <li>CLI Settings (Configuring)</li> <li>CLI Settings (Monitoring)</li> <li>Validating Devices</li> <li>Select Features</li> <li>Enable Polling</li> <li>Update Device</li> <li>Devices Configured</li> </ol>	SNMP Settings Enter the SNMP connection information used for monitoring the selected devi   Use the Default SNMP connection settings   C Enter SNMP connection settings for this device  SNMP Version Version Community String	Edit Target Port	161
	< Back Next > Finish	Cancel	Help

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

iteps	CLI Settings (Configuring)
1. SNMP Settings 2. CLI Settings (Configuring)	Specify the CLI connection information used for configuring these devices. Required fields are indicated wit an asterisk (*).
3. CLI Settings (Monitoring)	Configuration CLI Connection Settings
<ol> <li>Validating Devices</li> </ol>	Enter Command Line Interface (CLI) connection settings used to configure these devices.
5. Select Features	C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp
5. Enable Polling	Use my default Configuration CLI connection settings     Edit
7. Update Device	C Enter connection settings for this device
<ol> <li>Devices Configured</li> </ol>	Connection Type SSH Y Port* 22
	User name on Device
	Password on Device*
	Enable Password
	Also use these credentials for monitor mode.
	Ŗ
	< Back Next > Finish Cancel Help

10. Select Use the previous page connection settings.

Configure Cisco Devices								
Steps	CLI Settings (Monitoring)							
<ol> <li>SNMP Settings</li> <li>CLI Settings (Configuring)</li> </ol>	Specify the CLI connection information shared by all users. This information will only be used to monitor device. Required fields are indicated with an asterisk (*).							
<ol> <li>CLI Settings (Monitoring)</li> <li>Validating Devices</li> <li>Select Features</li> <li>Enable Polling</li> <li>Update Device</li> <li>Devices Configured</li> </ol>	Monitor-only CLI Connection Settings         Enter Command Line Interface (CLI) connection settings used to monitor this device.         Ise the default Monitor-only CLI connection settings         Enter connection spage connection settings         Enter connection settings for this device         Connection Type         SEM         Password on Device*         Enable Password							
	< Back Next > Finish Cancel Help							

### 11. Click Next

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

Steps	Validating Devices								
1. SNMP Settings	The following devices are being validated. Y								
2. CLI Settings (Configuring)	validation issue occurs, click on the descripti	on field to view addi	tional details.						
3. CLI Settings (Monitoring) Device Status Description									
4. Validating Devices	Branch1-LA.dcloud.cisco.com	Status	Description Succeeded: click for details						
5. Select Features	Branch2-NY.dcloud.cisco.com		Succeeded: click for details						
6. Enable Polling									
7. Update Device									
8. Devices Configured									
	1								
	Export Validation Details								
	< Back Next > Finish	R	Cancel Help						

Configure Cisco Devices				×							
Steps	Select Features										
<ol> <li>SNMP Settings</li> <li>CLI Settings (Configuring)</li> </ol>	Select the features you want to use on the devices. Learn more about each feature in the Help section.										
3. CLI Settings (Monitoring)	Device	NBAR	NetFlow	Mediatrace							
	Branch1-LA.dcloud.cisco.com		~								
<ol><li>Validating Devices</li></ol>	Branch2-NY.dcloud.cisco.com										
5. Select Features											
6. Enable Polling											
7. Update Device											
8. Devices Configured											
	1										
	e Back March >	1		need 1 state 1							
	<back next=""> Finish</back>		Ca	ncel Help							

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

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

Steps	Enable Polling								
1. SNMP Settings	Select the features you want to ac	tively mo	nitor, ar	nd the po	lling rate f	or the dev	ices. Lea	arn more abou	ıt
2. CLI Settings (Configuring)	each feature in the Help section.								
3. CLI Settings (Monitoring)									
4. Validating Devices	Device	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval	
5. Select Features	Branch1-LA.dcloud.cisco.com							30 seconds	
6. Enable Polling	Branch2-NY.dcloud.cisco.com							30 seconds	-
7. Update Device									
8. Devices Configured									
								R	
	,								
	<ul> <li>* LAN polling occurs every 15 mir</li> <li>* For SNMP v3, please see the U</li> </ul>			fian wie a I	AM colling				
	* For SNMP V3, please see the U	ser Guide	on con	nguring L	AN polling	•			
								1	
	< Back Next > Fit	nish					Cancel	Help	)

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

16. Select Send Updates to Devices and click Send.

onfigure Cisco Devices			
Steps	Update Device		
<ol> <li>SNMP Settings</li> <li>CLI Settings (Configuring)</li> <li>CLI Settings (Monitoring)</li> <li>Validating Devices</li> </ol>	The selected devices will be updated base You may choose to manually configure th Warning: once update processes have be more about each feature in the Help sect	e devices. en started you will not	i changes if necessary. : be able to return to earlier screens. Learn
5. Select Features	Device	Status	Description
6. Enable Polling	Branch1-LA.dcloud.cisco.com	•	Update Required: click to view
7. Update Device	Branch2-NY.dcloud.cisco.com		Update Required: click to view
	Send Updates to Devices	end	
	C Manually Configure Devices		
	Export Update Commands		
	<back next=""> Finish</back>		Cancel Help

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

eps	Update Device			
. SNMP Settings . CLI Settings (Configuring) . CLI Settings (Monitoring) . Validating Devices	The selected devices will be updated based You may choose to manually configure the Warning: once update processes have bee more about each feature in the Help sectio	e devices. En started you will no		ns. Lear
. Select Features	Device	Status	Description	
. Enable Polling	Branch1-LA.dcloud.cisco.com	•	Update Successful	
<ul> <li>Update Device</li> <li>Devices Configured</li> </ul>	Branch2-NY.dcloud.cisco.com	•	Update Successful	
	Send Updates to Devices Ser	nd		
	C Manually Configure Devices			
	Export Update Commands			

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

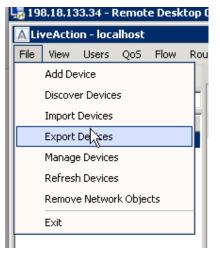
Configure Cisco Devices		×
Steps	Devices Configured	
1. SNMP Settings	The following devices have been configured. Lea	rn more about each feature in the Help section.
2. CLI Settings (Configuring)	Device	Summary
3. CLI Settings (Monitoring)	Branch1-LA.dcloud.cisco.com	CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30
<ol> <li>Validating Devices</li> </ol>	Branch2-NY.dcloud.cisco.com	CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30
5. Select Features		
6. Enable Polling		
7. Update Device		
8. Devices Configured		
	< Back Next > Finish	Cancel Help

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

# Lab A.3: Export/Import Device Configuration

Lab Steps:

1. From the File Menu select Export Devices.

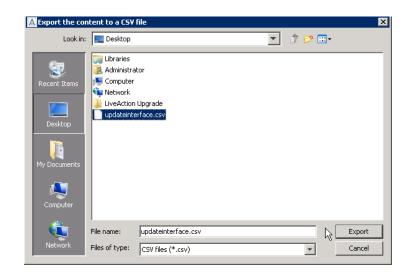


2. Deselect **GigabitEthernet2** and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

											Q	Type here to filter resul	ts
dd/Up	Name	Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (Kb	Node	Site	Site CIDR	Data Cen
$\checkmark$	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				
	Nullo	Interface							10,000,000				
	VoIP-Null0	Interface							10,000,000	1			
	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
		Interface		198.18.129.24				HQ-LAN	1.000.000				
		Interface		100.64.0.2				Internet	1,000,000				
		Interface							8,000,000				
		Interface							10.000.000	1			
	VoIP-Null0	Interface							10.000.000	1			
	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
		Interface		198.18.129.25					1,000,000				
	-	Interface		10.255.0.2					1,000,000				
	-	Interface		10.0.0.102					8,000,000				
		Interface							10,000,000				
		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		
		Interface		198.18.129.23					1,000,000				
	-	Interface		10.0.0.103					8,000,000				
		Interface							10,000,000				
		Interface							10,000,000				
					<								

3. Select Export to csv.

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



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



8. Select the file you previously exported.

2	\Lambda Import from a	1CS¥ file						×
	Look in:	🧮 Desktop			V	1 🖻	•	
2	Recent Items Desktop My Documents Computer	Computer Computer Network LiveAction	Upgrade					
		File name:	updateinterface.cs	,				Import
	Network	Files of type:	CSV files (*.csv)			T		Cancel

9. Click Add/Update Devices.

	Jpdate Devices													×
	s selected for Add/Update will b						1		1		Q.			_
dd/Upd		Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K	Node	Site	Site CIDR	Data Ce	
$\checkmark$	Branch1-LA.dcloud.cisco		101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	LA	10.0.1.1, 198.1		
1	- GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000					
	- GigabitEthernet2	Interface		100.64.1.2				Internet	2,000					
1	- 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					
1	🖶 HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ			
1	- GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000					
1	- GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000					
	Loopback0	Interface							8,000,000					
	- NullO	Interface							10,000,000					
	VoIP-Null0	Interface							10,000,000					
1	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ			
1	GigabitEthernet1	Interface		198.18.129.25					1,000,000					
1	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					
	- NullO	Interface							10,000,000					
	VoIP-Null0	Interface							10,000,000					
_					<									i
								Add/Update Devices	Import from CSV		Export to CSV	(	Close	

10. Click OK to use the Default SNMP settings.

Δ		×
Node	Local	
Use the Default SNI	MP connection settings	Edit
C Enter SNMP connect	tion settings for this device	
SNMP Version	Version 2c	Target Port 161
Community String		
	, 	
		Ok Cancel

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

### Lab A.4: Saving Server Configurations

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

Lab Steps:

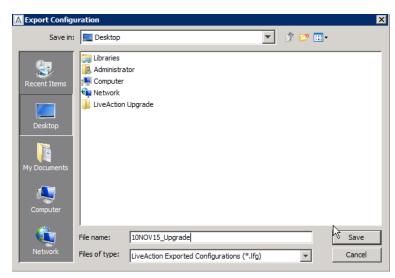
1. Open the LiveNX WebUI, select Settings.

≡ LiveAction <sup>™</sup> ™				New Features!	<u> </u>	• •	<b>A</b> 1	{} •	0 -	۰.	👗 admin
Overview Enter Filter Request Here									Φ	Settings	
Sites, Devices, Interfaces by Statuses			Active Alerts								Settings lagnostics
SITES: 2	DEVICES: 4	INTERFACES: 8	ALERTS						_	User Man	-
ыла (? 0 • но • LA	DEVICES (5) (0)	INTERFACES C <sup>2</sup> Image: Comparison of the second secon		Ne	o Active Alerts						

2. Select Configuration.

≡ LiveAction <sup>-</sup> NX	
Settings	
Q Search	
Configuration	
Data Source Management	
Data Store Device Entity Page Reports	
Email Configuration	
Integrations	~
Licensing License Configuration	^
License Expiration Notification	
LiveNA Configuration	
Mounted Data Nodes	
Properties	~
Proxy	
Reports	~
Security	~
Single Sign On SNMP Trap	
Syslog	
Troubleshooting	~
Updates	
Web UI Data Store	

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



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

## Lab A.5: Connect via Remote Desktop Connection

A direct connection from the LiveNX Client installed on your workstation is the most efficient method to connect, but you may use RDC as an *alternate* way to connect to your Student Pod. SKIP this Lab if directly connecting with the LiveNX Client on your local workstation.

To connect using Microsoft Remote Desktop on Windows, or a compatible Remote Desktop client on Linux and Macintosh, follow the steps below. On Windows you can typically find Remote Desktop in START > ALL PROGRAMS > ACCESSORIES.

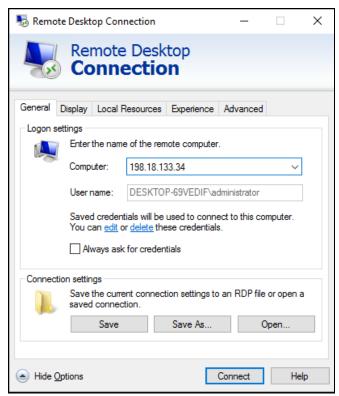
Note: Use the information from the Lab Details table to connect to the desired device.

Lab Steps:

Connect to the virtual Windows Workstation Desktop using the IP Address, username, and password pre-printed on the Class Worksheet, unless otherwise instructed.

- 6. Launch a Remote Desktop Connection.
- 7. BEFORE selecting Connect, click the General tab. (On Macintosh this will be the Preferences menu and Login tab.)

DIAGRAM



- a. Enter the following fields:
  •Computer: <ipaddress> :20201
  (From your Lab Access worksheet)
  •Username: administrator (or otherwise defined by instructor)
- 8. Set the RDC session properties on the Display tab so that your video is a minimum of 1200x800 resolution... this may NOT be changed once the connection is active. See next page for example.

#### DIAGRAM

퉣 Remo	ote Deskt	op Connection		—		$\times$
<b>A</b>		mote Desk Innectio				
General	Display	Local Resources	Experience	Advanced		
Display	configura	tion				
		se the size of your re the right to use the		). Drag the s	lider all th	ne
	Small	Full Scree		ge		
	Us	e all my monitors for	the remote se	ession		
Colors		e the color depth of est Quality (32 bit)	f the remote s	ession.		
🗹 Displa	y the con	nection bar when I	use the full sci	reen		
A Hide (	Options			Connect	Н	elp

9. Select Connect.

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

#### DIAGRAM

Windows Security	× •
Enter your These credenti	credentials als will be used to connect to vm.opnet.com.
	DESKTOP-69VEDIF\administrator
	Use another account
🕅 Reme	mber my credentials
	ОК Саде

11. Click OK.

Once successfully connected to your Pod you will see the Windows Desktop, and be able to access the LiveNX Server, Client, and other pod resources.

**Note**: Occasionally Remote Desktop may freeze its connection to the Pod workstation. If this happens, close the Remote Desktop window, and start again at Step 1 above. This will continue your lab session and will generally not lose any work.