

LiveAction Training Lab Workbook Pt. 1

© Copyright 2022, LiveAction, Inc.

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

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

Trademarks:

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

All other products or services mentioned herein are trademarks or registered trademarks of their respective owners. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark. March 2022.

Table of Contents

	•
Table of Contents	3
Lab 0: Setup and Get Connected	
Lab 0.1: Connect to the Lab Network	
Lab 0.2: Connecting to Your Training Pod	8
Lab 0.3: Install the LiveNX Client	9
Lab 1: The LiveNX Web UI	10
Lab 1.1: Explore the Web UI	11
Lab 1.2: Create a Custom Dashboard	
Lab 1.3: Pre-Configured Stories	
Lab 1.4: WebUI Reports	19
Lab 1.5: Enable / Customize Alerts	
Lab 1.6: Add a User Account	
Lab 1.7: View and Navigate System Diagnostics	
Lab 1.8: Support and Troubleshooting	
Lab 2: The LiveNX Client	
Lab 2.1: Launch the LiveNX Client	
Lab 2.2: Explore the LiveNX Client	38
Lab 3: Configuring Devices	
Lab 3.1: Add Device	
Lab 3.2: Manage & Configure Devices	48
Lab 3.3: Configure Flow on Devices	55
Lab 3.4: Add/Remove Interfaces	59
Lab 3.5: Merge Clouds in Topology	62
Lab 4: Traffic Flows	
Lab 4.1: Discover Flows	
Lab 4.2: Discover Specific Flows	
Lab 4.3: Examine Specific Traffic	
Lab 4.4: Troubleshoot Issues	
Lab 5: Custom Filters	
Lab 5.1: Creating Custom Filters	
Lab 5.2: ACL Creation	
Lab 6: Making the Topology Work	
Lab 6.1: Setting Device Semantics	
Lab 6.2: Adding Devices to Groups	
Lab 6.3: Creating Network Objects	
Lab 7: Dashboards & Reports	110
Lab 7.1: The Dashboard	111
Lab 7.2: Viewing Reports	115
Lab 7.3: Create a Custom Report	
Lab 8: QoS	
Lab 8.1: QoS Marking Policy	
Lab 8.2: QoS Queueing Policy	
Lab 8.3: QoS Verification	
Lab A: Appendix	
Lab A.1: Add Device	
Lab A.2: Client Device Discovery	101
Lab A.3: Export/Import Device Configuration	109
Lab A.4: Saving Server Configurations	1/3
Lab A.5: Connect via Remote Desktop Connection	175

4/8/2022 IMPORTANT INFORMATION – Please Read!

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

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

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

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

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

Lab.0

Lab 0: Setup and Get Connected

4/8/2022 Lab 0.1: Connect to the Lab Network

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

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

Local:

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

1 x Installed LiveNX Client

1 x Browser

Remote Student Pod

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

1 x LiveNX OVA Linux install

1 LiveNX Server

1 LiveNX Node (installed on LiveNX Server)

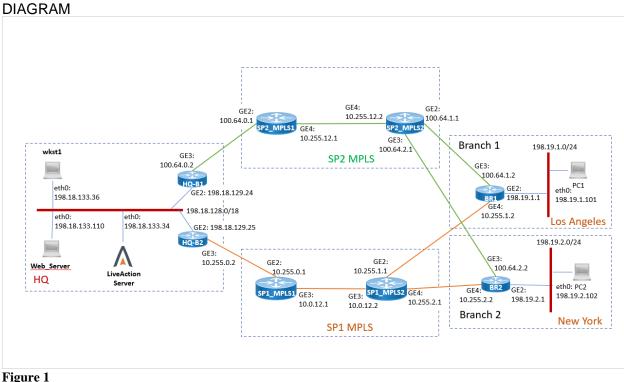


Figure 1

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

Note: Make sure to consult the Infrastructure Diagram, as well as specific classroom instructions for names, IP addresses, and other parameters. The screen shots in this Lab Workbook are *examples* which may NOT fully reflect the parameters of your pod.

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

	dation - 2022						
TERION LIVENX Flow Foun	0%		•	•	•	•	
	0%		Queued	Spawning	Provisioning	Stabilizing	Ready
:= Learning menu		Topology Lab	Details				
Overview							
Lab Introduction	SI N	o Role	Hostname	Username	Password	IP Address	Port
ce Topology	1	LiveNX Server	livenx	admin	Student	35.226.145.33	443 or 7000
	2	B1-HQ	HQ-B1	admin	C1sco12345	35.226.145.33	20152
Access Devices	3	SP2_MPLS1	SP2_MPLS1	admin	C1sco12345	35.226.145.33	20153
	4	SP2_MPLS2	SP2_MPLS2	admin	C1sco12345	35.226.145.33	20155
lboxes	5	BR1	Branch1-LA	admin	C1sco12345	35.226.145.33	20160
	6	B2-HQ	HQ-B2	admin	C1sco12345	35.226.145.33	20157
	7	SP1_MPLS1	SP1_MPLS1	admin	C1sco12345	35.226.145.33	20158
	8	SP1_MPLS2	SP1_MPLS2	admin	C1sco12345	35.226.145.33	20159
	9	BR2	Branch2-NY	admin	C1sco12345	35.226.145.33	20161
	10	wkst1	Administrator	Administrator	C1sco12345	35.226.145.33	20201
s	10	Activedirectory	Administrator	Administrator	C1sco12345	35.226.145.33	20202
**	12	PC1	Administrator	Administrator	C1sco12345	35.226.145.33	20203
	13	PC2	Administrator	Administrator	C1sco12345	35.226.145.33	20204
+ Add Hours							
Terminate							

Figure 2

Lab Steps:

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

^{4/8/2022} 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...

目 9 ひ 1	` ↓ Ŧ	L	iveNX Training -	Credentials for Har	nd's-on Labs - Messa	ige (HTML)		55 -		×
File Message	e Insert C	Options	Format Text	Review He	p Q Tell me v	what you want to	do			
Paste 3			- = - Ap = = =	Address Check Book Names	 Q Attach File ▼ Mttach Item ▼ Q Signature ▼ 	Assign Policy ▼ ↓	Dictate	Customer Manager	View Templates	
Clipboard 🕞	Basic	c Text	5	Names	Include	Tags 🗔	Voice		My Templates	^
Send To	E LiveAction Train		Hand's-on Labs							
connect to you Username	r Training Pod n Password	Admin U	IRL hterprise.crite	rionnetworks.co	ink, below and u m/criterion/learnin	igs/course-deta	ils-acces	s/learning	labs?	
April 2019: http	o check this link s://www.liveac	our Trainin k to get the <u>ction.com/</u> our web-ba	g Pod Admin e latest versio <u>'support/train</u> sed Training l	page. ons of Student G ning-resources/ Pod, you will not	iuide, Lab Workbo	ook, and LiveNX	ÇClient li	nstaller. U	pdated 1	
- Figure 3										

Lab Steps:

1. Click the URL provided in the email.

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

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

	← Back							
	LiveNX Flow Foundation - 2022							
NETWORKS		0%		•	•	•	•	•
				Queued	Spawning	Provisioning	Stabilizing	Ready
Home	Image: Learning menu							
TO TO	:= Ceaning menu	То	pology Lab D	etails				
🔶 Design	Overview							
	Lab Introduction	SI NO	Role	Hostname	Username	Password	IP Address	Port
Experience	Topology	1	LiveNX Server	livenx	admin	Student	35.226.145.33	443 or 7000
		2	B1-HQ	HQ-B1	admin	C1sco12345	35.226.145.33	20152
Showcases	Access Devices	3	SP2_MPLS1	SP2_MPLS1	admin	C1sco12345	35.226.145.33	20153
Sandboxes		4	SP2_MPLS2	SP2_MPLS2	admin	C1sco12345	35.226.145.33	20155
- Sandboxes		5	BR1	Branch1-LA	admin	C1sco12345	35.226.145.33	20160
		6	B2-HQ	HQ-B2	admin	C1sco12345	35.226.145.33	20157
Learn		7	SP1_MPLS1	SP1_MPLS1	admin	C1sco12345	35.226.145.33	20158
		8	SP1_MPLS2	SP1_MPLS2	admin	C1sco12345	35.226.145.33	20159
		9	BR2	Branch2-NY	admin	C1sco12345	35.226.145.33	20161
I Statistics		10	wkst1	Administrator	Administrator	C1sco12345	35.226.145.33	20201
		10	Activedirectory	Administrator	Administrator	C1sco12345	35.226.145.33	20202
*		12	PC1	Administrator	Administrator	C1sco12345	35.226.145.33	20203
		13	PC2	Administrator	Administrator	C1sco12345	35.226.145.33	20204
	+ Add Hours							
	Terminate	_	_					
		Prev						

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 0.3: Install the LiveNX Client

Lab 1.1: Explore the Web UI

These Labs uses the WebUI exclusively.

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>

LiveNX	
Username	
Password	
Login	
By clicking "Login", I agree to the terms of LiveAction's <u>EULA</u> First time user information	
igure 5	

2. Login to the WebUI using: Username: admin Password: Student

The Overview screen will appear.

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

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

LiveAction	NX					New Features! 🔺 16 💻 0 🔹 0 🌲 1111 {-} -	0- 0- 1
Enter Filter Requ	est Here						<> Apply filter C
ites, Devices, Interfaces by Stat	tuses					Active Alerts	
						ALERTS 📴	TIME OPENED
SITES: 2		DEVICES: 3		INTERFACES: 6		Branch1-LA.dcloud cisco com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	22 Sep 2021, 05:53
			_		_	Branch1-LA dcioud cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	22 Sep 2021, 05:53
						Over 1% of Voice traffic for Branch1-LA.dcloud.cisco.com running application statistical-p2p is not marked as DSCP EF.	21 Sep 2021, 08:42
SITES C	0	DEVICES C	0	INTERFACES 📴	0	HQ-B2.dcloud.cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	21 Sep 2021, 06:1
LA		Branch1-LA		GigabitEthernet2lBranch1-LA		HQ-82.dcloud.clsco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	21 Sep 2021, 06:12
HD		 HC-B2 		GigabitEthernet2IH0-B1		Branch1-LA debud cisco com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	21 Sep 2021, 06:12
		• HO-B1		 GigabiltEthernet2IH0-82 		Branch1-LA deloud cisco com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	21 Sep 2021, 05:1
				GigabilEtnemet3JH0-B1		 HQ-82 dcloud cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF) 	21 Sep 2021, 04:0
				 GigabitEthernet3IH0-B2 		HQ-82 dcioud cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 34 (AF41)	21 Sep 2021, 04:0
				GigabitEthernet4/Branch1-LA		 HQ-82.dcloud.cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF) 	21 Sep 2021, 04:0
						 HQ-82 dcloud cisco.com running application rtp had voice/video traffic with 200.00 ms max jitter 	21 Sep 2021, 04:0
						HQ-82.dcloud.cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 34 (AF41)	21 Sep 2021, 04:0
						Over 1% of Voice traffic for HQ-B2.dcloud.cisco.com running application openwebnet is not marked as DSCP EF.	21 Sep 2021, 04.0
						Branch1-LA.dcloud.cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 34 (AF41)	21 Sep 2021, 04:02
						Branch1-LA deloud cisco.com running application rtp had 200.00 ms of jitter for traffic with a DSCP value of 34 (AF41)	21 Sep 2021, 04:02
						Branch1-LA deloud cisco com running application rtp had voice/video traffic with 200.00 ms max jitter	21 Sep 2021, 04:02

Figure 6

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

🖶 Main							 Apply filter 	C Aut
• Overview						Active Alerts		
Deshooard						ALERTS 13	TIME OPENEI	D
Sites Sites Centrols Value Totale Autras Nationality Listers Startles Autras Autras Nationality Listers Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras Autras	θ	ремсез: 3 екисез (2 • такот) 4. • нов • нов	0	INTERFACES: 6 INTERFACES: 6 INTERFACES: 6 INTERFACES: 6 OpportStremet2broch: (A OpportStremet2broch: (A OpportStremet2broch: A OpportStremet2broch: A OpportStremet3broch: A	0	Beach14.Additud citize com numing agalication that 3000 m ed. piter for halfs: with a 000° value of 46.(F) Beach14.Additud citize com numing agalication static and 2000 m ed. piter for halfs: with a 000° value of 40.(F) Hold 2000 m ed. piter halfs: with a 000° value of 1800° related to 4800° value of 40.(F) Hold 2000 m ed. piter halfs: with a 000° value of 1800° related to 4800° value of 40.(F) Hold 2000 m ed. piter halfs: with a 000° value of 1800° related to 4800° value of 40.(F) Hold 2000 m ed. piter halfs: with a 000° value of 1800° value of	22 Gep 201, 22 Gep 2021, 21 Gep 201, 21 Gep 201,	05:52 Ah 08:42 Ph 06:12 Ah 06:12 Ah 06:12 Ah 04:03 Ah 04:03 Ah 04:03 Ah 04:03 Ah 04:03 Ah 04:03 Ah 04:03 Ah

Figure 7

5. Select Sites.

≡ LiveAction [•] ■											• 0 🐥 42			
Sites Enter Filter Request Here								Apply filter	Mar 20, 2	022 07:40:00	→ Mar 20, 2022 07:55:1	0 15 M	tin 🏾 🗢 Auto	Configure Sites
											Q Search			
SITE NAME	♀ SITE STATUS	٥	DEVICE REACHABILITY	0	DEVICE CPU/MEMORY	0	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	0	CONGESTION	I DROPS	0	INTERFACE ERRORS	\$
Site Name	All	~	All	~	All	~	Peak Utilization In	Peak Utilization Out		All		~	Interface Errors	
HQ	•		•		•		52.77%		30.74%		•			0
LA	•						28.12%		38.03%					0

Figure 8

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

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

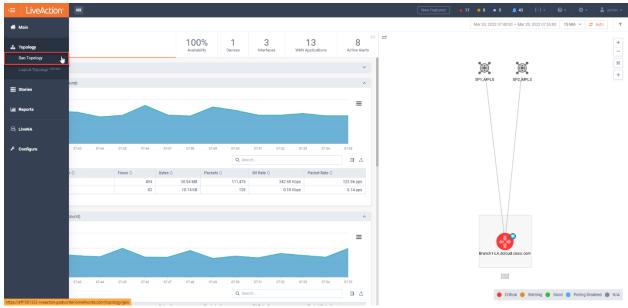
- 6. Note: Status, Utilization, Drops, Errors, etc....
- 7. Toggle the Auto Update to ON.
- 8. Click on the link to ${\bf LA}$ to see additional site info.

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

4/8/2022 ≡ B.iveAction[•] Sites > Site: LA A 3 Interfaces V LA 100% 13 8 1 Devices + - × ۲ ۲ = 11 ± Q SP1_MPLS SP2_MPLS 111,476 123.86 pps 0.14 pps 342.60 Kbp 10.74 KB ≡ LA 0 £ Q Search ● Critical ● Warning ● Good ● Poiling Disabled ● N/A

Figure 9

9. Select Topology > Geo Topology





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

<complex-block>



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

utice	Management 🎯										001	mport/Export ~	Credential Store	View Device	Addition	SNMP Device	Discover De
		My Devices (3)				My Inte	rfaces (7)			1	Discovered Devices	(0)			⑦ Autodisc	overy (0)	
Edit	Refresh List	Configure	Delete	Rediscover Interfa	ces									Q Sea	rch		
	DEVICE 0	DEVICE STATE	IP ADDRESS	VENDOR 0	MODEL 0	NODE 0	SITE 0	INTERFACES \$	HARDCODED S \$	POLL 0	QOS	FLOW Ô	IP SLA 🗘	ROUTING \$	LAN O	TAGS	0 INTERVAL
	Device	All ~	IP Address	All v	Model	Node	Site			All v	All ~	All ~	All 🗸	All 🗸	All ~	Tags	All
	HQ-B1	Up	198.18.129.24	Cisco	ciscoProducts	Local/Server	HQ	2		~	~	~					10 se
	Branch1-LA	Up	198.19.1.1	Cisco	ciscoProducts	Local/Server	LA	3		~	~	~					10 se
	HQ-B2	Up	198.18.129.25	Cisco	ciscoProducts	Local/Server	HQ	2		~	~	~					10 se

Figure 12

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

^{4/8/2022} Lab 1.2: Create a Custom Dashboard

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

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

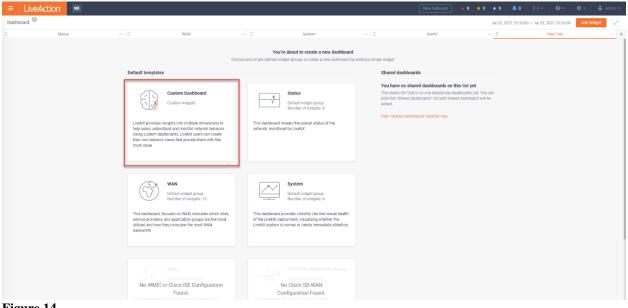
Lab Steps:

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

·≡ LiveAction [.]	NX			[New Features! 🔺 16 🔳 0 🔹 0 🌲 11	1 {-} - @ -	• • 1 admin •
👫 Main					Mar 20, 2022 14:3	0:00 → Mar 20, 2022 14:35:00	Add Widget 🥜
Overview	Status	WAN	8	System	8	Alerts	2 *
Dashboard 1							 Apply filter
Sites							
Devices	Peak Inbound WAN Interface Utilization X	E Top WAN Applications by Bandwidth Inb	ound/Outbound Bandwidth	×	Top Interfaces % Changed - Interface Burstable Rate		×
Interfaces	PLS1 42.0	rtpaudio-video 1110.2 rtp-audiounknown 269.8		In Out	Branch1-LA->GigE4->Inbound->LA->SP1_MP5.6 H0-82->GigE3->Outbound->H0->SP1_MPLS_5.0		
WAN Applications	2 MPLS	snmp-snmp-group 33.4 10.21.1.154-unknown 27.8			HQ-82-GigE3-Inbound-HQ-SP1_MPLS 4.2 Branch1-LA-GigE4-Outbound-LA-SP1_		
Alerts	(FCS)	openwebnetunknown 26.0			HQ-B1GigE3InboundHOSP2_MPLS		
Network Users		ipfixunknown 21.8 Ianrevagentunknown 15.8			HQ-B2GigE2InboundHQHQ LAN HQ-B1GigE2OutboundHQ		
		sip-audio-video 14.5 Rpfile-transfer 13.1			HQ-82GigE2OutboundHQHQ LAN Branch1-LAGigE3InboundLASP2_MP		
🚓 Topology		ica→uniktown 10.3 Kbps			Branch1-LA-+GigE3-+Outbound-+LA-+SP2		
and the second se	2241						
Stories	×	: Overall Status A/I		×	Top Devices Top Devices CPU Usage		×
A Reports		Critical	Warning	Good	Branch1-LA→LA 31.0 HQ-B1→HQ 28.0		_
	and the second	Sites 2	0	0	HQ-82HQ 28.0		
.C. LiveNA							
		Devices 2	0	1			
F Configure		WAN Apps 3	0	1			
					5		
	Leest Availability	Availability Top Interfaces With Least Av	allability	×			
		LA-Branch1-LA-Branch1 LAN-GigabitEt					
		LA-+Branch1-LA-+SP2_MPLS-+GigabitEthe	rnet3				
		LA-Branch1-LA-SP1_MPLSGigabitEthe HQHQ-81GigabitEthernet2	mel4				
		HQ→HQ-B1→SP2_MPLS→GigabitEthernet3	3				
		HQ-HQ-82-HQ LAN-GigabitEthernet2 HQ-HQ-82-SP1_MPLS-GigabitEthernet3					
		ing and a company of the second					

Figure 13

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.

Dashboard	ve/Action [®]							Jul 2					
	Status	8 WAN		System		Alerts		1	Add widge Current dashi Added 0 out o	board: New			
											and D s from		0
											anel	(Sectored as	-
									Availability Availabili		Count		~
						-	a a a a a a a a a a a a a a a a a a a	2 Top Intert	: Top Devia		ast Availability		
							B		 Top Servi Top Sites 	ice Provider s with Least	rs with Least Av		
									Applications				
									🗉 Top Appl	lication Perf	ormance Summ	iary	
									I Top Voice	e/Video Per	formance Sum	mary	
		(R) WAN	Drop widgets here						Address				
									Source A	ddress			\sim
									Destination	ion Address			~
									Source or	r Destinatio	n Address		~
									Site Traff	hc			~
									Source S	ite Traffic			~
									Destinati	ion Site Traf	fic		~
									E Bidirectio	onal Source	/ Destination Pa	ir	
									Network				
									Course Al	loðunel:			
									Create Ne	w Widget			

Figure 15

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

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

≡ LiveAction [™]					New Features!	0 0 0 0	{} • • • •	🕸 🚽 👗 admin 🤊
Dashboard						Jul 22, 2021 22:55:	:00 → Jul 22, 2021 23:10:00	Add Widget 🥜
Status	WAN		System		Alerts		New Tab	
Enter Filter Request Here						6	5	4 Apply filter
:: Current Active Alert Count Alert Count By Site	×	E Current Active Alert Count Alert	Count By Category	4 ×	Availability Top Devi	ces With Least Availability		×
				-	LA→Branch1-LA NY→Branch2-NY	100.0		

Figure 16

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

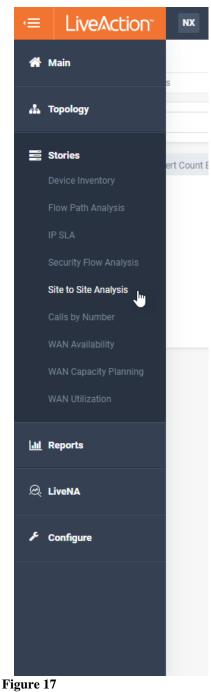
Note: Since LiveNX stores *breadcrumbs* it will retain a trail of the last page you've visited in the WebUI, based-upon your individual login credentials. Unless shared... Your custom Dashboard will not be visible to others.

^{4/8/2022} Lab 1.3: Pre-Configured Stories

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

Lab Steps:

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



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.**

4/8/2022	squest Here		New Featured		● 0 🜲 111 Mar 20, 2022 15 20 00 — M	lar 20, 2022 15:35:00	 C Auto
DESECTION METRIC Band	ound Outbound			нα			
		14					

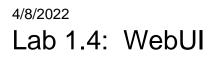
Figure 18

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

LiveAction 💌		
e To Site Analysis > LA - HQ		< Mar 20, 2022 15:20:00 - Mar 20, 2022 15:35:00 > 15 Min 🗸 😂 A
Switch Direction Enter Filter Request Here		4P Apply filter Off IWAN Control Filter Plow Deta
plication op 10 V	DSCP All	Service Provider S
ffp Ipftx	0 (BE)	
lanrevagent		
openwebnet	46 (EF)	SP1_MPLS Norm
rtp	34 (AF41)	
sip		
	1525	1530 15

Figure 19

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



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

Lab Steps:

1. Click the Menu icon.

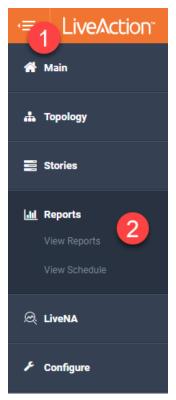


Figure 20

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

LiveAction [®]	×			New Fastures: 🔺 0 💻 0	• 0 🐥	<u> </u>	Ø -	🕸 – 🚢 adm
w Reports							View Schedule	Create Repo
Templates Reports Hist	tory							
								Table Tile
By Template Name								
fault Templates		Favorite Reports						0
ce Analysis	0	Add Report						
NN NN	0							
orite Applications	0	Top Reports						ତତ
le Fastiane Applications	0	NAME ©	DESCRIPTION C					
e Fastlane Voice Analysis	0	· · · ·						
I Capacity Planning	0	Application		will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications. will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.				
Network Performance Audit	0	Top Conversations		will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations. will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.				
e/Video Performance Vs. Network	0	DSCP		will highlight the Top To Interfaces bandwidth, based on the selected hiter criteria. It will list up to Tobo Interfaces.				
o-Site Traffic Utilization Audit	0	Top Interface Bandwidths		t shows a table of all the interfaces' bandwidth utilization per the specified filter.				
ice Provider DSCP Audit	0	Top Interface Errors		t shows a table of all interface errors (CRC/Runts/Overruns, etc.) per the specified filter.				
k Single Site WAN Path Changes	0	Top Class Bandwidths		t shows a table of all QOS class bandwidths for all interfaces per the specified filter.				
lication Vs. Network Performance	0	Top Class Drops		t shows a table of all QoS class drops on all interfaces per the specified filter.				
e/Video Service Provider Performan.	0	Interface Bandwidth		t graphs bandwidth utilization of a specific interface.				
ication Service Provider Performan	0	Interface Utilization	This SNMP-based repo	t graphs the interface bandwidth utilization (by percentage) of a specific interface.				
AN Application Service Provider Pe.	0	Interface Errors	This SNMP-based repo	t graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.				
AN Application Vs. Network Perfor	0	Post-Policy Drops	This SNMP-based repo	t graphs the QoS drops of all classes on a specific interface.				
AN Voice/Video Performance Vs. N.	. 0	Application DSCP Audit	This Flow-based report	will show the DSCP markings of applications organized by site, based on the selected filter criteria.				
AN Voice/Video Service Provider P	0	Interface Bandwidth Summary	This Flow-based report	will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.				
N Application Vs. Network Performa.	. 0							
N Application Service Provider Perfo.	0	Default Templates						0
N Voice/Video Performance Vs. Net.	0	NAME O		DESCRIPTION C				
Voice/Video Service Provider Perf.	0							
		Voice Analysis		This group of reports is useful for understanding enterprise-wide QoS performance for VoIP. It includes DSCP marking validation per site, QoS performance info				
		IWAN		This group of reports provides rapid understanding of Cisco IWAN performance and utilization. It includes an understanding of which service provider a specific			oss/jitter measure	iments by traffic c
		Favorite Applications Apple Fastlane Applications		This group of reports provides an understanding of the applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic This group of reports provides an understanding of the Apple Fastiane applications seen at a specific site, their performance (based on the Cisco Performance)				

GENERAL SETTINGS		REPORT LIST		REPORT DETAILS	
Name		Application (Flow)	Fast 🖻 🔳	Report Name	Flow Type
MY Application		Add New Report	+	Application	Basic Flow V
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	V All Hours V
Time Range				Flex Search 🚱	Cannot be used with All Device Bin Duration
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, this report will utilize the
Display Filter				Direction	Raw Flow datastore (slower).
Select Display Filter	~			Inbound and Outbound Combined	
Sharing Settings					
Email 🔀					
Enter an email address of AD entry					

Figure 22

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

View Reports										View Schedule Cr	eate Report
Templates Reports Hist	story										
Q By Template Name		My Applicat	ion					View Options ~	Share Download	Schedule Copy	Close
Default Templates		Application (F	low)		Directio	n		Bin Time	Range Show	n (1hr)	1
/olce Analysis	0	Device: All WAN I				~~	Received and the second second		21 20:42:28 EDT (0MT-04:00) End Tim	and the second se	_
VAN	0	Bin Interval: 1 m		orfaces Display Filter: No Display Filt	unection: Inbound and Outb	Flow Type: Basic Flow	Execution Type: Time Series Sort By: Bit	tate un puration: 1 Minute Start Time: Jul 22, 20	21 2092:28 ED1 (04/1-04:00) End Tim	98: 301 22, 2021 21:42:28 EDT (GM	PO4300)
avorite Applications	0	300								- rtp-audio	=
pple Fastiane Applications	0	î								ica ipfix	-
pple Fastiane Voice Analysis	0	ad 200							Duentes	ftp	
AN Capacity Planning	0	100							d Drag to	sip	
le Network Performance Audit	0	-							in in	espf	
										Total	
olce/Video Performance Vs. Network		20.43	20.45 20.50	20.55	21.00 21.05	21:10	21:15 21:20	21.25 21.90 21.5	15 21:40 21:42	Total	
oice/Video Performance Vs. Network Ite-to-Site Traffic Utilization Audit				20.55	21:00 21:05	21:10	21:15 21:20			tota	
	. 0	«/ 1	20.45 20.50]/3 >>>	20.55	21.00 21.05	21.10	21:15 21:20		5 21:40 21:42 Q Search	Iotai	
te-to-Site Traffic Utilization Audit Irvice Provider DSCP Audit	0			20.55 Total Flows 0	21.00 21.05 Total Bytes O	21:10 Total Packets O	21:15 21:20 Average Bit Rate O			Peak Packet Rate 🗘	
te-to-Site Traffic Utilization Audit trvice Provider DSCP Audit ack Single Site WAN Path Changes	0 0 0	«/ 1	/3>>>	Total Flows 0	Total Bytes O 20.79 MB	Total Packets O 103,936	Average Bit Rate C 46.19 Kbps	21.25 21.30 21.3 Average Packet Rate C 28.87 pps	Q Search Peak Bit Rate O 109.14 Kbps		68 p
te-to-Site Traffic Utilization Audit Invice Provider DSCP Audit ack Single Site WAN Path Changes splication Vs. Network Performance	. 0 0 0 0 0		/3 >> Application C rtp-audio ica	Total Flows 0 54 206	Total Bytes 0 20.79 MB 4.23 MB	Total Packets 0 103,936 63,542	Average Bit Rate C 46.19 Kbps 9.40 Kbps	2125 Clise 215 Average Packet Rate C 28.87 pps 17.65 pps	Q. Search Peak Bit Rate O 109.14 Kops 23.52 Kops		68 pj 43 pj
te-to-Site Traffic Utilization Audit nvice Provider DSCP Audit ack Single Site WAN Path Changes plication Vs. Network Performance ice/Video Service Provider Performan	- 0 0 0 0 0		/ a >≫ Application © rtp-audio ica Ipfix	Total Flows 0 54 206 71	Total Bytes 0 20.79 MB 4.23 MB 2.70 MB	Total Packets 0 103,936 63,542 2,884	Average Bit Rate 〇 46.19 KDps 9.40 KDps 6.00 KDps	2125 130 213 Average Packet Rate O 28.87 pps 17.65 pps 0.80 pps	Q. Search Peak Bit Rate O 109.14 Kbps 23.52 Kbps 53.94 Kbps		68 p 43 p 5 p
te-to-Site Traffic Utilization Audit rvice Provider DSCP Audit ack Single Site WAN Path Changes plication Vs. Network Performance ice/Video Service Provider Performan. plication Service Provider Performan.	 a a<) / s >≫ Application O rtp-audio ica ipfix snmp	Total Flows 0 54 206 71 215	Total Bytes 0 20.79 MB 4.23 MB 2.70 MB 1.83 MB	Total Packets © 103,936 63,542 2,884 6,876	Average Bit Rate O 46.19 Kops 6.00 Kops 4.07 Kops 4.07 Kops	2125 0150 215 Average Packet Rate C 28.87 pps 0.85 pps 0.85 pps 1.91 pps 1.91 pps	Q. Search Peak Bit Rate () 109.14 Kops 23.52 Kops 53.94 Kops 13.61 Kops		68 p 43 p 5 p 4 p
te-to-Site Traffic Utilization Audit	- 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)/3 >> Application 0 rtp-audio ica lipfix snmp ftp	Total Flows 0 7 54 206 711 215 168	Total Bytes O 20.79 MB 4.23 MB 2.70 MB 1.83 MB 1.61 MB	Total Packets © 103,936 63,542 2,884 6,876 40,278	Average Bit Rate C 46.19 KOps 6.00 Kops 6.00 Kops 4.07 Kops 3.58 Kops	2125 21 21 20 21 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 22 21 21	Q. Search Peak Bit Rate O 109.14 KDps 23.52 KDps 53.94 KDps 13.61 KDps 5.46 KDps 5.46 KDps		68 p
e to Site Traffic Utilization Audit nrice Provider DSCP Audit ack Single Site WAN Path Changes plication U. Network Performance ince/Video Service Provider Performance glication Service Provider Performance WAN Application Service Provider Perfor-	· · · · · · · · · · · · · · · · · · ·) / s >≫ Application O rtp-audio ica ipfix snmp	Total Flows 0 54 206 71 215	Total Bytes 0 20.79 MB 4.23 MB 2.70 MB 1.83 MB 1.61 MB 1.33 MB	Total Packets © 103,936 63,542 2,884 6,876	Average Bit Rate O 46.19 Kops 6.00 Kops 4.07 Kops 4.07 Kops	2125 0150 215 Average Packet Rate C 28.87 pps 0.85 pps 0.85 pps 1.91 pps 1.91 pps	Q. Search Peak Bit Rate () 109.14 Kops 23.52 Kops 53.94 Kops 13.61 Kops		68 p 43 p 5 p 4 p 17 p 9 p
e-to-Site Traffic UBIzation Audit rivice Provider DSCP Audit cs: Single Site WAN Path Changes glication V. Netwice Performance isol/Video Service Provider Performance WAN Application Service Provider Performance WWAN Application Service Performance Vs. N.	 a) (a) b) (a) c) (a) <lic) (a)<="" li=""> <lic)< td=""><td></td><td>)/3 >> Application ○ rtp-audio ica lofix sinnp ftp lanrevagent</td><td>Total Flows 0 54 206 711 215 168 65</td><td>Total Bytes 0 20.79 MB 4.23 MB 2.70 MB 1.83 MB 1.61 MB 1.33 MB 929 65 KB</td><td>Total Packets C 103,936 63,542 2,884 6,876 40,278 11,841</td><td>Average BIt Rate C 46.19 K0ps 6.00 K0ps 4.07 K0ps 3.58 K0ps 2.97 K0ps 2.97 K0ps</td><td>2125 2130 211 Average Packet Rate C 28.87 pps 0.85 pps 0.85 pps 11.9 pps 11.9 pps 11.9 pps 11.9 pps 11.3 pps 11.3 pps</td><td>Q. Search Peak Bit Rate C 109.14 Kops 23.52 Kops 53.94 Kops 13.61 Kops 5.46 Kops 8.24 Kops 8.24 Kops</td><td></td><td>68 pi 43 pi 5 pi 4 pi 17 pi 9 pi 9 pi</td></lic)<></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)></lic)>)/3 >> Application ○ rtp-audio ica lofix sinnp ftp lanrevagent	Total Flows 0 54 206 711 215 168 65	Total Bytes 0 20.79 MB 4.23 MB 2.70 MB 1.83 MB 1.61 MB 1.33 MB 929 65 KB	Total Packets C 103,936 63,542 2,884 6,876 40,278 11,841	Average BIt Rate C 46.19 K0ps 6.00 K0ps 4.07 K0ps 3.58 K0ps 2.97 K0ps 2.97 K0ps	2125 2130 211 Average Packet Rate C 28.87 pps 0.85 pps 0.85 pps 11.9 pps 11.9 pps 11.9 pps 11.9 pps 11.3 pps 11.3 pps	Q. Search Peak Bit Rate C 109.14 Kops 23.52 Kops 53.94 Kops 13.61 Kops 5.46 Kops 8.24 Kops 8.24 Kops		68 pi 43 pi 5 pi 4 pi 17 pi 9 pi 9 pi
le to Site Traffic Utilization Audit inice Provider DSCP Audit ack Single Site WAN Path Changes plication Vs. Network Performance ince/Video Service Provider Performan- plication Service Provider Performan- WAN Application Service Provider Per-	 e) <)/3 >> Application 0 rtp-audio ica ipfix snmp ftp iarrevagent sip	Total Flows 0 54 206 71 215 168 65 43	Total Bytes © 20.79 MB 4.22 MB 2.70 MB 1.83 MB 1.61 MB 1.33 MB 229 65 KB 515.40 KB	Total Packets ○ 103,936 63,542 2,884 6,876 40,278 11,841 7,169	Average BIR Rate C 46.19 Kops 6.00 Kops 6.00 Kops 3.58 Kops 2.97 Kops 2.97 Kops	2125 2120 2110 Average Packet Rate O 228 87 pois 0 30 pps 0 30 pps 0 119 pps 0 329 pps 0 329 pps 0 199 pps 0 329 pps	Q. Search Peak Bit Rate O 23.52 Kops 53.94 Kops 5.36 Kops 5.46 Kops 8.22 Kops 8.02 Kops		68 p 43 p 5 p 4 p 17 p

Figure 23

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

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

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 (in the table, or on right of chart).
- 7. Re-sort by clicking on the **Sort Arrows**.
- 8. **Zoom-in** by Left-click-drag a portion of the chart.
- 9. **Reset** Zoom to normal.

10. Schedule the Report to run Hourly.

≡ LiveAction [.]							New Features! A 0 B 0	• 0 🌲 1 {-} -	@ - ☆ - ≗ admin -
View Reports									View Schedule Create Report
Templates Reports History									
Q By Template Name	My Application						View Options ~	Share Download	Schedule Copy Close
Default Templates	Application (Flow))							- × ¤
Voice Analysis	Device: All WAN Devic	ces Interface: All WAN Interfa	ces Display Filter: No Display Filte	ring 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	к Jul 22, 2021 21:42:28 EDT (ОМТ-04:60)
IWAN Ø	Bin Interval: 1 minute								
Favorite Applications ()	300							9	ntp-audio
Apple Fastiane Applications	E 200								ipfx
Apple Fastiane Voice Analysis	te ()(2								ftp lenrevegent
WAN Capacity Planning (5)	2 100								aip ontp
Site Network Performance Audit									epf ssh
Voice/Video Performance Vs. Network 🕚	0 21:22:52	21:23:30	21:24:00 21:24:30	21:25:00 2	1 25:30 21:26:00	21:26:30 21:27:00	21:27:30 21:28:00 21:28:30	21:29:00 21:29:26	Total
Site-to-Site Traffic Utilization Audit	«< Page 1 /3							Q Search	0 ±
Service Provider DSCP Audit	N. C. Page [1] 7.3	1.7.0						G Search	u 15
Track Single Site WAN Path Changes ()	Legend O Ap	pplication O	Total Flows 🗘	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🗘	Average Packet Rate 🗘	Peak Bit Rate 🗘	Peak Packet Rate 🗘
Application Vs. Network Performance	- rt;	p-audio	54	20.79 MB	103,936	46.19 Kbps	28.87 pps	109.14 Kbps	68 pps
Voice/Video Service Provider Performan	ici		206	4.23 MB	63,542	9.40 Kbps	17.65 pps		43 pps
Application Service Provider Performan	ipt		71	2.70 MB	2,884	6.00 Kbps	0.80 pps	53.94 Kbps	5 pps
SDWAN Application Service Provider Pe ()		nmp	215	1.83 MB	6,876	4.07 Kbps 3.58 Kbps	1.91 pps 11.19 pps	13.61 Kbps 5.46 Kbps	4 pps 17 pps
SDWAN Application Vs. Network Perfor	- ft	p nrevagent	168	1.01 MB	40,278	2.97 Kbps	3.29 pps	5.46 KDps 8.24 Kbps	17 pps 9 pps
SDWAN Voice/Video Performance Vs. N			43	929.65 KB	7,169	2.97 Kbps	1.99 pps	8.02 Kbps	9 pps 9 pps
SDWAN Voice/Video Service Provider P			51	515.40 KB	12,885	1.15 Kbps	3.58 pps	1.41 Kbps	4 pps
IWAN Application Vs. Network Performa	- 05	spf	389	226.78 KB	2,835	0.50 Kbps	0.79 pps	1.25 Kbps	1 pps
IWAN Application Service Provider Perfo		sh	27	210.89 KB	2,120	0.47 Kbps	0.59 pps	13.62 Kbps	16 pps
IWAN Voice/Video Performance Vs. Net									

Figure 25

MY Application Run Report	
Run Report	
nun report	
Hourly	~
Never 🗸	
Time Zone	DS
(GMT-05:00) America/New York	~

Figure 26

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

View Reports					6	1 View Schedul	le Crea	ite Report
Templates Reports	History							
Q By Template Nome		My Application	View Options ~	Share	Download	Schedule	Сору	Close
Default Templates		Application (Flow)						1
Voice Analysis	0	Device: All WAN Devices Interface: All WAN Interfaces Display Filter: No Display Filter: No Display Filter: In Device: All WAN Devices Interface: File Type: Basic Flow Essentian Type: Time Series Sont By: Bit Rate	n Duration: 1 Minute Start Time: Jul 2	2021 20:42:28 ED	T (GMT-04:00) End	Time: Jul 22, 2021 21	42.28 EDT (GMT-	4.00)
	0	Device All AND Device Interface All WARTHINGS Display Files To Display Files To Display Files Type Tanks Month and Outhound and Outhound Combined Files Type Tanks File Tanks Store Bit Manual L Interna	n Duration: 1 Minute – Start Time: Jul 22	, 2021 20:42:28 ED	T (GMT-04:00) End	Time: Jul 22, 2021 21	42.28 EDT (GMT-	H-80)
IWAN			n Duration: 1 Minute Start Time: Jul 22	, 2021 20:42:28 ED		obue-gri	42.28 EDT (GMT-	
IWAN Favorite Applications	0	Enternal: Tennar 200	n Decision: 1 Minute — Start Time: Jul 2	, 2021 20-42-28 KD	т (6мт.ск. со) End	en rtp-suño en ca en pfo	A2:28 EDT (GMT-	
IWAN Favorite Applications Apple Fastiane Applications	0	Bis Interval: 1 minute	n Daration: 1 Minuta — Start Tima: Jul 2	2021 20-42-28 EG		rtp-suño ca pfx errop frp		
Voice Analysis IWAN Favorite Applications Apple Fastiane Applications Apple Fastiane Voice Analysis WAN Capacity Planning	0 0 0	Enternal: Tennae 200	n Durationi 1 Minuta — Start Timai Jul 22	. 2021 20:42:28 ED		rtp-sudio ca přo errro		



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

E LiveAction ■	New Features!	۵ 🔺	0 0	۵ 🐥	{} -	0 -	۰	🛔 admin 👻
View Schedule							13	View Reports
Q By Report Name Reports For: Aug 1st - Sep 11th, 2021						< Aug 2	2021 >	Today
Scheduled Groups Hourly						S M	т w	T F S
MY Application B B 12						1 2	3 4	5 6 7
						8 9	10 11	12 13 14
						15 16	17 18	

Figure 28

Lets have a look at creating a Custom Report

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

GENERAL SETTINGS	REPORT LIST	REPORT DETAILS	
Name	Please choose report type		
Enter report group name	Add New Report	+ Top Reports	
Presentation Mode		LiveNA	
Standard	7		
		Address	~
Footnote Enter report group description		Analysis	~
Enter report group description		AnyConnect	~
Sharing Settings	-	Application Performance (AVC)	~
Email 📯		Applications	~
Enter an email address or AD entity		Firewall	~
File Format		LiveAgent	~
Send PDF Send CSV		Miscellaneous	~
PDF Row Limits		Network	~
All Rows	*	Network Users	~
Custom Logo 🚯			
	~	PfR	~
		B ^{QoS}	^
		Application DSCP Audit	
		DSCP	
		Llear Eiltar DCCD Audit	

Figure 29

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

View Reports												View Schedu	le Crea	nte Report
Templates Reports History														
Q By Template Name	Application	DSCP Audit	, Last Fifteen Minute	s					View Options ~	Share	Download	Schedule	Сору	Close
Ay Templates	Application (SCP Audit (Fit	ow)											1
ly Application Private 📰 🛅	Device: All WAY	Devices Inter	face: All WAN Interfaces Di	isplay Filter: No Display F	Ritering Direction: Inbound and	Durbound Combined Flew Typ	Electric Flow Execution Type: Tr	ime Series Sort By: Bit Rete Bin Dura	tion: Auto Start Time: Jul 22, 20	21 21:39:36 EDT	(GMT-04:00) End Time:	(Jul 22) 2021 21:54:	36 EDT (0MT 04:0	(C)
Default Templates	Bin Interval: 1	minute												
oice Analysis O	300											 NY/rtp-aud HQ/rtp-aud 	5io/45 (EF)	=
NAN O	a 200											MQ/ice/0 (8 MQ/ice/0 (8 HQ/ice/0 (8	8K)	
	0									-		HQ/(pfix/0)	(BE)	
orite Applications 🚯	2	110												
	PU 100											HQ/anmp/0	0 (36) 0	
	100											HQ/errep/0 HQ/hp/0 (8	0 (8£) BE)	
ple Fastiane Applications O ple Fastiane Voice Analysis O	0 21.40.0	0 214	00 21.42.00	21.43.00	21.44.00 21.45.00	2140.00 2147	00 21.49,00 S	21:49:00 21:59:60 21	1.51.00 21.52.50	21.53.00	21.54.60 21.543	HQ/armp/C HQ/hp/0 (8 NY/latreva Total	0 (8£) BE)	
pple Fastiane Applications 0 sple Fastiane Voice Analysis 0 AN Capacity Planning 0	. 4		100 21.42.00	21.43.00	21:44:00 21:45:00	21:49.00 21:47	00 21.49.00 2	21 1/9 00 21 50 00 21	151.00 21.52.50	21.53.02 Q. Se		HQ/armp/C HQ/hp/0 (8 NY/latreva Total	0 (8£) BE)	
pple Fastiane Applications O ople Fastiane Voice Analysis O AN Capacity Planning O	0 21:40.0 4 < Page 1	/4>>									arch	HQ/anro/X HQ/hp/0 (8 NY/latevia Total	o (94) BE) Igens/O (BE)	
ple Fastiane Applications 0 ple Fastiane Voice Analysis 0 NI Capacity Planning 0 e Network Performance Audit 0 ice/Video Performance Vs. Network - 0	0	/4 >> Site 0	Application O	DSCP O	Total Flows C	Total Bytes 0	Total Packets 🗘	Average Bit Rate 🗘	IS1.00 21.52.00 Average Packet Rate C	Q Se	erch Peak Bit Rate C	HQ/somp/ HQ/sp/0 (0 NY/sp/0 (0 NY/screws Total 36	0 (8£) BE)	
ple Fastiene Applications 0 ple Fastiene Voice Analysis 0 AN Capacity Planning 0 le Network Performance Audit 0 uco/Video Performance Vs. Network - 0	0 21:40.0 4 < Page 1	/4 > ≫ Site 0 NY	Application © rtp-audio	DSCP O 46 (EF)	Total Flows 0	Total Bytes 0 5.40 MB	Total Packets Q 27,009	Average Bit Rate C 48.02 Kbps	Average Packet Rate 🗘	Q, Se 30.01 pps	Peek Bit Rate 0 52.74	HQ/somp/S HQ/spip 0 (NY/screars Total 56 Peak P	o (94) BE) Igens/O (BE)	32 pj
ele Fastane Applications of de Fastlane Voice Analysis of N Capacity Planning o s Network Petromance Audit o eu Volkoe Petromance Van Network O el-to-Sine Traffic XIII/zation Audit o vice Provider DSCP Audit o	0 21:40.0 4 < Page 1	/4 >> Site 0	Application O	DSCP O	Total Flows C	Total Bytes 0	Total Packets 🗘	Average Bit Rate 0 48.02 Kbps 47.71 Kbps	Average Packet Rate 🗘	Q Se	erch Peak Bit Rate O 52 74 52 98	HQ/somp/ HQ/sp/0 (0 NY/sp/0 (0 NY/screws Total 36	o (94) BE) Igens/O (BE)	32 p 33 p
pie Fastlane Applications o pie Fastlane Voice Analysis o Ni Capacity Planning o e Netroint Performance Audit o e Netrointe Performance Vis Network O e-to-Site Traffic Litization Audit o nrice Provider DSCP Audit o	0 21:000 <<< Page 1 Legend 0	/4 > 3 Site 0 NY HQ	Application C rtp-audio rtp-audio	DSCP 0 46 (EF) 46 (EF)	Total Flows 0 14 14	Total Bytes 0 5.40 MB 5.37 MB	Total Packets 27,009 26,835	Average Bit Rate 0 48.02 Kbps 47.71 Kbps 10.25 Kbps	Average Packet Rate 🗘	Q, Se 30.01 pps 29.82 pps	arch Peak Bit Rate 0 52.74 52.96 11.08	HQ/arrep/2 HQ//arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Arrep/2 NY/Ar	o (94) BE) Igens/O (BE)	
pie Fastane Applicators 0 pie Fastane Veice Analysis 0 N Capach: Planning 0 N Capach: Planning 0 N Morke Performance Audit 0 Lea Video Performance Audit 0 Nice Provider DRCP Audit 0 Nice Provider DRCP Audit 0 Charge Site WAN Plath Changes 0	0 21.000 C < Pope 1 Legend O	/4 > ≫ Site 0 NY HQ NY	Application C rtp-audio rtp-audio ica	DSCP 0 46 (EF) 46 (EF) 0 (BE)	Total Flows C 14 14 56	Total Bytes 0 5.40 MB 5.37 MB 1.15 MB	Total Packets 0 27,009 26,835 17,290	Average Bit Rate () 48.02 Kbps 47.71 Kbps 10.25 Kbps 10.20 Kbps	Average Packet Rate 🛇	Q, Se 30.01 pps 29.82 pps 19.21 pps	arch Peak Bit Rate O 52.74 52.98 11.08 10.98	Peak P Kbps Kbps Kbps Kbps	o (94) BE) Igens/O (BE)	32 p 33 p 20 p 20 p
ule Fastane Applications 0 Nei Fastane Applications 0 No Stacker Permin 0 A Opacher Permin Anno 0 In Nitrouiti, Performance Austit 0 In Nitrouiti, Performance Austit 0 In Nitrouiti, Performance Austit 0 In Orielle Traffer Uttration Austit 0 In Charlos Edition, Austit 0 In Call Traffer Uttration Austit 0 In Call Traffer Tr	0 21:00 << Page 1 Legend 0	/ ± > ≫ Site 0 NY HQ NY HQ	Application C rtp-audio rtp-audio Ica Ica	DSCP ○ 46 (EF) 46 (EF) 0 (BE) 0 (BE)	Total Flows 0 14 14 56 50	Total Bytes 0 5.40 MB 5.37 MB 1.15 MB 1.15 MB	Total Packets 27.009 26.835 17.290 17.213	Average Bit Rate C 48.02 KDps 47.71 Kbps 10.25 Kbps 10.20 Kbps 4.87 Kbps	Average Packet Rate 🛇	Q, Se 30.01 pps 29.82 pps 19.21 pps 19.13 pps	arch Peak Bit Rate O 52.74 52.98 11.08 10.98 5.60	Peak P Kbps Kbps Kbps Kbps Kbps	o (94) BE) Igens/O (BE)	32 p 33 p 20 p 20 p 5 p
the Fastann Applications.	0 21:00 << Pape 1 Legend C	/4 >> Site 0 NY HQ HQ HQ	Application © rtp-audio rtp-audio ica ica ianrevagent	DSCP 0 46 (EF) 46 (EF) 0 (BE) 0 (BE) 0 (BE)	Total Flows 0 14 14 56 50 26	Total Bytes C 5.40 MB 5.37 MB 1.15 MB 1.15 MB 547.74 KB 535.01 KB	Total Packets 27,009 26,835 17,290 17,213 4,483	Average Bit Rate C 48.02 KDps 47.71 Kbps 10.25 Kbps 10.20 Kbps 4.87 Kbps 4.76 Kbps	Average Packet Rate 🗘	Q, Se 30.01 pps 29.62 pps 19.21 pps 19.13 pps 4.98 pps	Peak Bit Rate 0 52.74 52.98 11.08 10.98 5.60 54.03	HQJampi (o (94) BE) Igens/O (BE)	32 p 33 p 20 p 20 p 5 p 5 p
HE Fashark Applications In N R Statlank Wolco Analysis In N Capacity Planning In N Capacity Planning In School Performance Audit In School Performance Performance In School Performance Performance In School Performance Performance In School Performance Performance In NAM Application Stervice Performance In NAM Application Stervice Performance In	0 21:00 << Pape 1 Legend C	/4 >> Site 0 NY HQ NY HQ HQ HQ	Application © rtp-audio rtp-audio ica ica lanrevagent ipfox	DSCP ○ 46 (EF) 46 (EF) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE)	Total Flows C 14 14 56 56 26 16	Total Bytes C 5.40 MB 5.37 MB 1.15 MB 1.15 MB 547.74 KB 535.01 KB	Total Packets © 27,009 26,835 17,290 17,213 4,483 667	Average BR Rate 0 48 02 Kbps 47 71 Kbps 10 25 Kbps 10 20 Kbps 4 87 Kbps 4 7 Kbps 3 76 Kbp5 3 76 Kbp5	Average Packet Rate 🔿	Q Se 30.01 pps 29.82 pps 19.21 pps 19.13 pps 4.98 pps 0.74 pps	arch Peek Bit Rate () 52.74 52.98 11.08 10.98 5.60 5.403 5.57	HQ/strengt H	o (94) BE) Igens/O (BE)	32 pj 33 pj 20 pj
pie Fastane Applications. 0 pie Fastane Voleo Andysis 0 Ni Capacity Planting 0 loce Video Performance Audit 0 loce Video Performance Vis Network 0 entos Northe Utilization Audit 0 nice Planting Utilization Audit 0 nice Planting Utilization Audit 0 piestellon Vis Network Performance 0	0 21 40 0 21 40 0 4 < Page 1 Legend 0	/4>> Site 0 NY HQ HQ HQ HQ NY	Application C rtp-audio rtp-audio ica ica ianrevagent ianrevagent ipfox sip	DSCP 0 46 (EP) 46 (EP) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE)	Total Flows 0 14 14 56 56 26 16 19	Total Bytes 0 5.40 MB 5.37 MB 1.15 MB 5.47 74 KB 5.35 01 KB 422.91 KB	Total Packets © 27,009 28,835 17,290 17,213 4,483 667 3,032	Average Bit Rate C 48.02 K0ps 47.71 Kbps 10.22 K0ps 10.22 K0ps 14.87 K0ps 14.77 K1ps 13.76 K0ps 3.67 K0ps 2.41 K0ps 2.41 K0ps	Average Packet Rate 🔿	Q, Se 30.01 pps 29.82 pps 19.21 pps 19.13 pps 4.98 pps 0.74 pps 3.37 pps	arch Peek Bit Rate 0 52.74 52.98 11.08 10.98 5.60 5.403 5.57 4.44	Peak P Kbps Kbps Kbps Kbps Kbps Kbps Kbps Kbps Kbps Kbps Kbps	o (94) BE) Igens/O (BE)	32 p 33 p 20 p 20 p 5 p 5 p

Video Performance Vs. Net... ideo Service Provider Perf.

0

Figure 30

^{4/8/2022} Lab 1.5: Enable / Customize Alerts

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

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

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

Lab Steps:

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

	QoS Class Drop (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
_		1	• O-W		

Figure 31

3. Click on QoS Class Drop.

QOSI	Class Drop							
Enable On	d							
	」 is alert may contri	ibuto to otot	us of an Interfac		Cito			
Severit		bute to stati	us or an internaci	e, Device, and/or	Site.			
	ry /arning				~			
Note: S	Severity for this ale When the severity				d in the			
		7 IS III 0, IL 00	Jes not contribut	e to the status.				
Thres	holds							
Aut	omatic Resolution	Time * 🚯						
0					min			
	Catch All Thres							
All non-specified QoS Classes Drop Rate * For at Least *								
	Qos Class *							
_	VOICE				_			
	Drop Rate *		For at Least *					
	20	kbps	> 0	min				
	Qos Class *							
	VIDEO							
	Drop Rate *		For at Least *					
		11	> 1	min				
	50	kbps						
	50	корз	~1					

Figure 32

- 4. Select to Enable this alert.
- 5. Change the Severity if desired.
- 6. Enter QoS Class "VOICE".
- 7. Define a DROP RATE of 20.
- 8. Leave FOR AT LEAST of "0".

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

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

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



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

								New Features A 5	0	• 0	a 0	{} -	0 -	¢-	👗 adr
rt M	anagement 💿												Maintenance	e Mode	View Ale
				Li	eNX Aler	rts									
Enal	Disable Click th	is box to									Q Search.				
		all Alerts									G Search.				
	ALERT TYPE	CATEGORY	0	SEVERITY	0	ENABLED	0	THRESHOLDS		SHARING					
-	Aven Type	All	~	All	~	AI	~	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		A 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	System		A Critical		~		for at least > 0 minutes		Web UI					
	Low WAN Interface Utilization	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	Device, Interface		Critical		~		Drop Rate > 0 kbps for at least > 0 minutes		Web UI					
•	QoS Class Drop	Device, Interface		 Warning 		~		Multiple		Web UI					
-	QoS Interface Drop	Device, Interface		 Warning 		~		Drop Rate > 2500 pps for at least > 0 minutes		Web UI					
~	Routing Adjacency State Change	Network		A Critical		~		for at least > 0 minutes		Web UI					
-	Routing Polling Error	Network		A Critical		~		for at least > 0 minutes		Web UI					
	Site Reachability	Network		Multiple				Multiple		Multiple					
2	Spanning Tree Topology Change	Network.		Critical		~		for at least > 0 minutes		Web UI					
•	Voice Traffic Classification and Marking	Application		A Critical		~		for at least > 0 minutes		Web UI					
•	Voice, Video Applications Performance	Application		A Critical		~		Multiple		Web UI					
~	Voice/Video Performance - Jitter Avg	Application		A Critical		~		Jitter Avg >= 30 ms for at least > 0 minutes		Web UI					
-	Voice/Video Performance - Jitter Max	Application		A Critical		~		Jitter Max >= 60 ms for at least > 0 minutes		Web UI					
2	Voice/Video Performance - Packet Loss	Application		A Critical		~		Packet Loss >= 1 % for at least > 0 minutes		Web UI					
	VRRP Operational State	Network.		Multiple				Multiple		Multiple					

Figure 34

^{4/8/2022} Lab 1.6: Add a User Account

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

Lab Steps:

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

									New Features!		0 = 0	• 0	🌲 2	{} -		۰۰	
Alert M	fanagement [©]														Maintenance	Settings	
Lado Ales												Diagnostics					
Ena	Disable												Q. Set	irch		User Mar	
	ALERT TYPE	0	CATEGORY C	0 s	VERITY	0	ENABLED	0	THRESHOLDS		SHARING					Liveture	ser Managerr
	Alert Type		All ~		All	~	All	~	Thresholds		Sharin	0					
	Application Performance - App Delay	0	Application		uhiple				Multiple		Multiple						- 1
	Application Performance - Network Delay	0	Application	0	utiple				Multiple		Multiple						

Figure 35

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

ADD NEW USER		×
1 Authenticatio	оп Туре	2 Settings
	thentication Type	
L	OCAL Jm	
	DAP RADIUS	Cancel Next Step
	ACACS+	

Figure 36

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

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

7. Click Add User.

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

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.

EiveAction ■		New Festures 4 0 = 0 + 0 4 2 (-) - 0 - 4 a sómin -				
System Diagnostics > Node Information		Settings				
Local/Server V		System Diagnostica				
Current Status: Ok Conformance: Ok Current	nt Deployment: Custom IP: Local	Last Update Time: 2				
CPU 05 KAM Model 0EMU Virtual CPU version 22.0 05 Ubil. 1.3 % Amount 156	JVM RAM DISK RTT 68 Committed 8.00.08 Total 4.99.76.08 Serier to Node	BEVICES LineNC Sorver N/A Total 5 Configurable 5 Loading 0				
Cores 8 JVM Util. 1.3 % Used 7.08	8 Used 1.69 GB Free 482.75 GB Node to Server	N/A Active 5 Down 0 Last Days 0.216 fps				
10 System	Report Queue					
OS CPU USAGE	JVM CPU USAGE	OS RAM USAGE				
JVM RAM USAGE	FREE DISK SPACE	NUMBER OF DOWN DEVICES				
	44.6 0 172.0 0 174.0 0 174.					
PROCESSED FLOW RECORDS	PACKETS RECEIVED VS PACKETS DROPPED	ALERTING FLOW PROCESSING DROP RATE				
Figure 37	state state in a lighter in hand lack all and the factor for the terms of ter	pilan Barang (17 In				

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

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

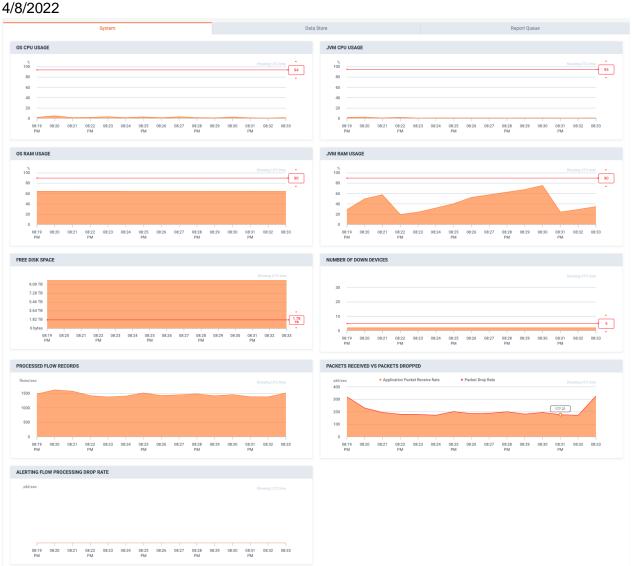
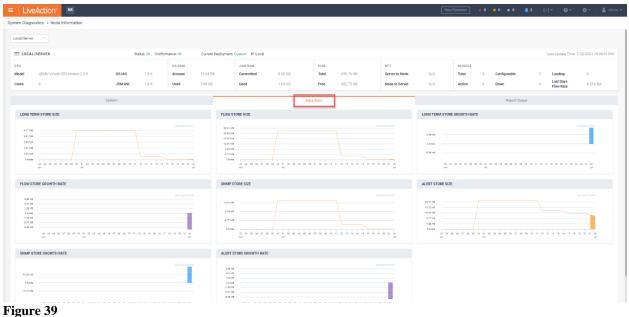


Figure 38

^{12.} Data Store tab will allow viewing the storage details applicable to the server.



1 igui (37

Lab 1.7: View and Navigate System Diagnostics© Copyright LiveAction 2022

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

LiveAction [®]									new	Features		•••	4 [−] *	.	0- 4-
Diagnostics > Node Information															
/Server V															
LOCAL/SERVER	Status: (0k Conformance: 0k	Current Deployr	ment: Custom IP: Local									Las	t Update Time:	7/22/2021 10:09:01
		OS RAM		JVM RAM		DISK		RTT		DEVICES					
el QEMU Virtual CPU version 2.2.0	OS Util. 1.	3% Amount	15.64 GB	Committed	8.00 GB	Total	499.76 GB	Server to Node	N/A	Total	5 (onfigurable	5 L	oading	0
13 8	JVM Util. 1.	3% Used	7.08 GB	Used	1.69 GB	Free	482.75 GB	Node to Server	N/A	Active	5 t	lown	0	Last Days Flow Rate	0.216 fps
	System				Det	Store		_				Report Queue	_		
	oyavem				Data	Store						Report Queux			
port Queues 😋															
Cancel All															
C REPORT NAME	C REPORT ID	0 REPORT	STATE	0 USER NAME		O PRIOR	Y	QUEUE NAME		0 qui	UED TIME		0 RUNNEN	IG TIME	
Report name	Report id	All		✓ User name		Al		~							
					No	Data									

Figure 40

Lab 1.8: Support and Troubleshooting

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

- Checkedor

 <
- 1. Navigate to the Settings menu.

Figure 41

LiveAction [®] N								0 • ≜ ∘
ttings								
Q. Search								
Q Search	LOG	iS						
onfiguration								
ta Source Management	Live	IX Log Level	✓ Set					
a Store	INP	0	✓ Set					
vice Entity Page Reports								
ail Configuration	Mar	age Logs						
egrations ~	G	et LiveNX Logs Delete						
ensing ^		O NODE MAME	C SOURCE O	FILE PATH C	COLLECTION START TIME 0	STATE C	51.75	C DOWNLOAD
icense Expiration Notification		Node name	Source	File Path	Collection start time	State	Size	
NA Configuration								
unted Data								
les								
perties v				,	io Data			
a,								
orts v								
uity ~								
gle Sign On								
/P Trap								
log								
bleshooting ^	•							
PU Profiling								
ap Dump								
28								
sket Capture	1							
load History								
ser Activity Tracking								
dates	T							
ah I II Data Store								

2. Navigate and expand Troubleshooting and then click Logs.

Figure 42

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

3. Click Get LiveNX Logs.

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	Sele	ct None	
Local/Server				
			Cancel	Get Logs

Figure 43

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

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

×

- 5. Navigate to Packet Capture under Troubleshooting.

- Figure 44
 - 6. Click Capture Packets.

PACKET CAPTURE		×
Would you like to capture packets int completed, you may download the file		
Maximum duration for capture is 120 60 seconds. Customer portal will hav others will be deleted automatically.		
Interface*	Device	
eth0	Other	\sim
Node	Protocol	
Local/Server V	None	\sim
Host	Duration*	
eg: x.x.x.x		Sec
Port		
2055		
	Cancel	re Packets

Figure 45

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

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

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

Lab 2

Lab 2: The LiveNX Client

^{4/8/2022} Lab 2.1: Launch the LiveNX Client

These Labs uses the Engineering Console exclusively.

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

A Mac version is also available for install if needed.

Lab Steps:

1. Launch the LiveNX Client.

DIAGRAM

Client Login X										
LiveNX										
Username:										
Password:										
For first time	e use:									
Userna	me and password are "admin"									
Click "Configure" to setup server address										
Configure OK Cancel										



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	Settings		
Server:			\sim
Port:	7000		
		Save	Cancel
	Configure	ОК	Cancel

Figure 47

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



6. Click **OK**

The Client will launch...



Figure 49

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

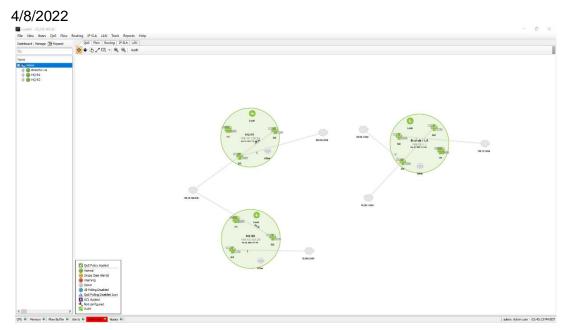


Figure 50

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

^{4/8/2022} Lab 2.2: Explore the LiveNX Client

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

Lab Steps:

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

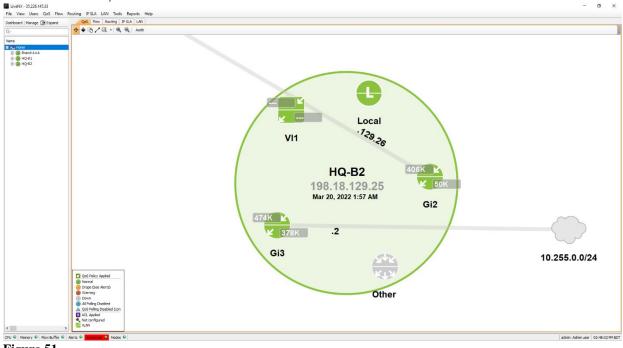


Figure 51

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

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

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

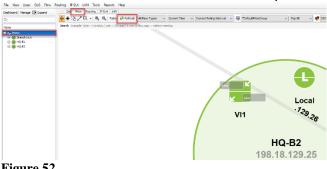


Figure 52

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

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

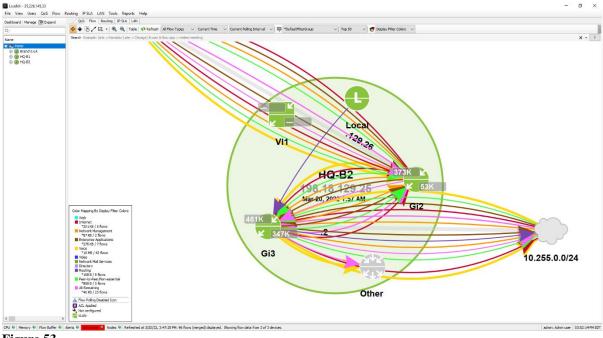
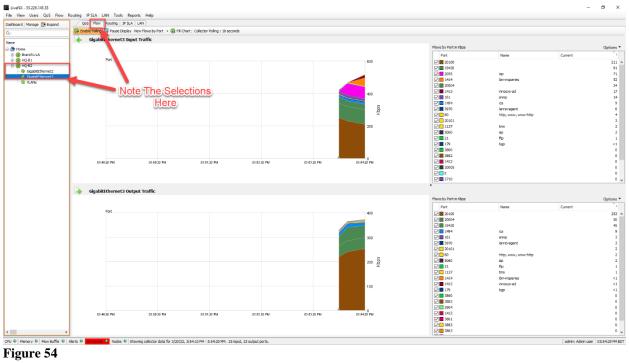


Figure 53

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



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



This Lab uses the WebUI.

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

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

Lab Steps:

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

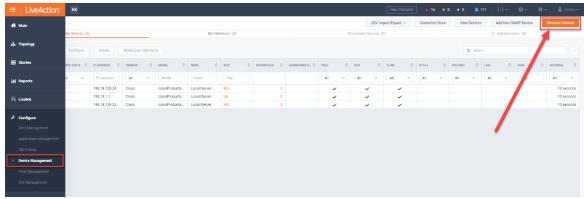


Figure 55

10. Click Discover Devices.

1. What to scan	12 2. SNMP Settings 14 3. Node
SPECIFY IP RANGES	
198.19.2.1	Choose a site
Add More	
Add Mole	
SPECIFY SEED DEVICE TO SCAN	
IP address	Hops
	Save & Nex

Figure 56

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

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

E LiveAction		New Features A 16	■ 0 • 0 🌲 111 {-} - 🖉 🛩	🕸 🚽 👗 admin 🚽
Device Management		CSV Import/Export ~ Credential S	tore View Devices Add Non SNMP Device	Discover Devices
My Devices (3)	My Interfaces (7)	Discovered Devices (0)	(7) Autodiscovery (0)	
DESCOVERY LOGS: 0/1			Successfully started	i device discovery job x
Stop				

Figure 57

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

	My Devices (3)		My Interfaces	(7)	Discovered D	levices (1)		(?) Auto	discovery (0)
2 SELE	ECT DEVICES								
Add A	Il Devices Edit							Q Search	
	DEVICE	SERIAL	0 IP ADDRESS 0	VENDOR	MODEL	NODE	INTERFACES	\$	HARDCODED SAMPLE RATIO
	Device	Serial	IP Address	Vendor	Model	Node	Interfaces		
	Branch2-NY	000000021	198.19.2.1	Cisco	ciscoProducts.3004	Local/Server	7		

17. Tick the box next to Branch2-NY.

18. Click Select Interfaces.

		My Der	rices (3)				M	v Int	terfaces (7)			Dis	cove	ered Devices (1)					 Autodiscovery (0) 		
SELE	CT INTERFACES	Davices	: 1 Interfaces: 7																		
dit											Selected: 3							Q	Search		
	NAME	0	INTERFACE STATE	0	DEVICE	0	LINE RATE (Kbps)	0	IP ADDRESS		LABEL O	INPUT CAPACITY (Kbps)		OUTPUT CAPACITY (Kbps) 🗘	WAN/XCC	N O	SERVICE PROVIDER	0	TAOS C	DESCRIPTION	
	name		All ~		All	-	line rate		ip address		Label	Input Capacity		Output Capacity	All	~	All	~	Tags	description	
2	GigabitEthernet2		Up		Branch2-NY		1000000		198.19.2.1	E	Branch2 LAN				WAN		Branch2 LAN			Branch2 LAN	
	GigabitEthernet3		Up		Branch2-NY		1000000		100.64.2.2	١	WAN_SP2_MPLS2				WAN		WAN_SP2_MPLS2			WAN_SP2_MPLS2	
- 6	19 abitEthernet1		Up		Branch2-NY		1000000		192.168.122.161												
2	GigabitEthernet4		Up		Branch2-NY		1000000		10.255.2.2											WAN_SP1_MPLS2	
	Loopback0		Up		Branch2-NY		8000000		10.0.2.1												
	NullO		Up		Branch2-NY		10000000														
	VoIP-Null0		Up		Branch2-NY		10000000														

Figure 58

19. Select GigabitEthernet2, GigabitEthernet3 & GigabitEthernet4.

20. Click Add Selected.

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

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

	LiveActio	nĩ 💌													111 {-} -			
vice N	Management 💿										CSV	mport/Export ~	Credential Store	View Devic	es Add Non	SNMP Device	Discover D	evices
		My Devices (4)				My Inter	faces (10)			D	liscovered Devices	(0)			() Autodisc	overy (0)		
Edit	Refresh List	Configure	Delete	Rediscover Interfa	ces									Q Se	arch			
	DEVICE 0	DEVICE STATE 0	IP ADDRESS	VENDOR 0	MODEL 0	NODE 0	SITE O	INTERFACES 0	HARDCODED S 0	POLL 0	qos (FLOW 0	IP SLA	ROUTING	LAN C	TABS	0 INTERVAL	
	Device	All 🗸	IP Address	All v	Model	Node	Site			All 🗸	All ~	Al v	All ~	All ~	All ~	Tags	All	,
	HQ-B1	Up	198.18.129.24	Cisco	ciscoProducts	Local/Server	HQ	2		~	~	~					10 s	secor
	Branch1-LA	Up	198.19.1.1	Cisco	ciscoProducts	Local/Server	LA	3		~	~	~					10 5	secor
	HQ-B2	Up	198.18.129.25	Cisco	ciscoProducts	Local/Server	HQ	2		~	~	~					10 s	secor
	Branch2-NY 💥	Up	198.19.2.1	Cisco	ciscoProducts	Local/Server		3		~	~	~	~				1	l minu

Figure 59

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

		All ~		All	Model	All V All V Tags	All ~
	HQ-81	Up	198.18.129.24	Cisco	ciscoProdu	EDIT BRANCH2-NYLDCLOUD.CISCO.COM X	10 seconds
	Branch1-LA	Up	198.19.1.1	Cisco	ciscoProdu	Site Group Interval	10 seconds
	HQ-B2	Up	198.18.129.25	Cisco	ciscoProdu	NM V No Group Selected V I Minute V	10 seconds
		Up	198.19.2.1	Cisco	ciscoProdu	Add NY	1 minute
l						191 192.1 POLL PSLA GOG ROUTING FLOW LAN Associate Probe all P Address Hardcodo Sample Ratio Type IP Address 1/ Tage Least Balax Office # 2 Cascel Apply	

Figure 60

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

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

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

ŗ	Configure
	Filter Management
•	Site Management

Figure 61

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

	LiveAction 🛛 💌															263 🔍				
Site Ma	nagement 🚳																			View Sites
Add	Edit Delete														Q	Search				
	smi O	DATA CENTER 🗘	DEVICES	0	CONTAINS DEVICES	O NO. OF EMPLOYEES O	0	BUSINESS HOURS	IP RANGES		SEO LOC	٥	ADDRESS 0		EGION	0	DESCRIPTION	Ô	TAGS	0
	Site	All ~	Devices		All ~	No. of Employees		Business Hours	IP Ranges		All	~	Address		Region		Description		Tags	
	HQ		HQ-MC.dcloud.ci	sco.c	~			Mo - Fr 8:00 am - 5:00	198.18.128.0/18		1		San Francisco, CA	1	an Francisco, Ca	lifor	Headquarters	Data Ce		
	LA		Branch1-LA.dclou	ud.cis	~			Mo - Fr 8:00 am - 5:00	198.19.1.0/24 10.0.1.1	_	1		Los Angeles, CA	1	os Angeles, Calif	orni	Branch 1		_	
	NY		Branch2-NY.dclou	ud.cis	~		T	None	198.19.2.0/24	Г										

Figure 62

in the

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

Details	Addres	SS		Business hours	
Site Description	:	Site IP Range (CIDR N	otation IP's)		
Enter site description		198.19.2.0/24			
	0/1000				
Devices		Tags			
Branch2-NY.dcloud.cisco.com ×	1	Branch × East ×	: Sales ×	Research ×	4
Number of Employees					
Number of Employees					
Data Center					

Figure 63

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

Details	Address	Business hours
Address	Latitude & Longitude	
Address Line 1	Latitude	
Address Line 2	Longitude	
City	Phone Number	
New York	Phone Number	
State/Province/Region	Email	
New York	Email	
Zip Code	Region	
10006	Input valid address and populate region	d press "Geo Coordinate Lookup" to
Country		
United States	~	
Geo Coordinate Lookup Remove Region		
2lm		
Lookup geocode using addr	ess	

Figure 64

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

Latitude & Longitude 40.709329
-74.013120
Phone Number
Phone Number
Email
Email
Region
Continent: North America → Country: United States → State: New York → City: New York

Figure 65

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

										_			
		Detai	Is				Add	Iress			Bu	isiness hours	
Days of	Week							Time Zone					DST
Su	Mo	Tu	We	Th	6	Sa		(GMT-05	00) A	kmerica/I	New York		
Start tir	ne							End time					
^		^						^		^			
08		00		AM				05		00	РМ		
~		~						~		~			

Figure 66

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

33. Then Click Save.

	LiveAction [®]									0 0 4 11			
te Mar	agement 💿												View Sites
Add	Edit Delete									Q, Search			
	SITE O	DATA CENTE	O DEVICES O	CONTAINS DEVICES 0	NO. OF EMPLOYEES	BUSINESS HOURS 0	IP RANGES O	GEO LOC 🗘	ADDRESS 0	REGION	DESCRIPTION 0	TAGS	
	Site	All	Devices	All 🗸	No. of Employees	Business Hours	IP Ranges	All v	Address	Region	Description	Tags	
	HQ		HQ-B1.dcloud.cisco.co	~		Mo - Fr 8:00 am - 5:00	198.18.128.0/18	1	San Francisco, CA	San Francisco, Califor	Headquarters Data Ce		
	LA		Branch1-LA.dcloud.cls	~		Mo - Fr 8:00 am - 5:00	198.19.1.0/24 10.0.1.1	1	Los Angeles, CA	Los Angeles, Californi	Branch 1		
	NY		Branch2-NY.dcloud.cls	~		Mo - Fr 8:00 am - 5:00	198.19.2.0/24	+	New York, New York, 1	New York, New York, U		Sales, Branc	ch, Researc

Figure 67

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

^{4/8/2022} Lab 3.2: Manage & Configure Devices

This Lab uses the Engineering Console.

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

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

Lab Steps:

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

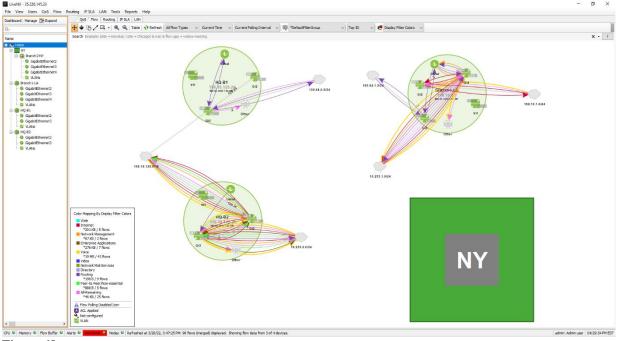


Figure 68

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

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

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

39. Select only Branch2-NY

in Der	vice Management													
Filte	r by:					F	ilter	Clear						
Select	Device Name	IP Address	Vendor	Model	Node	Group	Poll	QoS	Flow	IP SLA	Routing	LAN*	Interval	Status
	Branch 1-LA	198.19.1.1	Cisco	ciscoProducts.3004				\checkmark	\checkmark				10 seco	Configur
9	Branch2-NY	198.19.2.1	Cisco	ciscoProducts.3004		NY	41 🗖						10 sec 42	Not Cont
	HQ-B1	198.18.129.24		ciscoProducts.3004		(40)		\checkmark	\sim				10 seco ~	-
	HQ-B2	198.18.129.25	Cisco	ciscoProducts.3004	Local	$\mathbf{-}$	\checkmark	\checkmark	\checkmark				10 seco v	Configur

of Devices: 4 Select devices in the table and click the configure button. Remove selected device(s). Edit Clear Default CLI Monitoring Settings - Not Set Add To Group <New Group> \sim Edit Clear Default CLI Configuration Settings Remove From Group Removes selected devices from their groups Edit Groups Edit the groups Close

Figure 69

4/8/2022

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

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

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

 \times

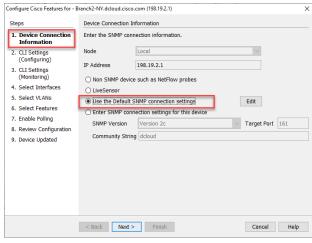


Figure 70

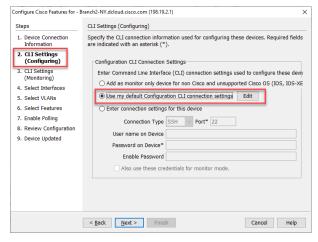


Figure 71

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

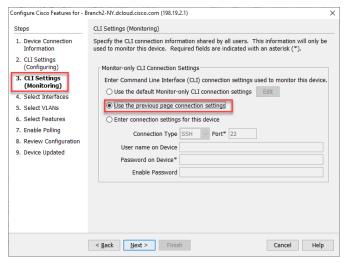


Figure 72

Test	Status	Description	
SNMP connection	•	Succeeded	۰,
SNMP access		Succeeded	
CLI configure connection	0	Skipped	
CLI configure login	0	Skipped	
CLI configure enable password	\odot	Skipped	
CLI monitor connection	\odot	Skipped	
CLI monitor login	\odot	Skipped	
CLI monitor enable password	\odot	Skipped	
Serial number validation	0	Skipped	
Model supported	•	Succeeded	
IOS supported		Succeeded	
NBAR capable		Succeeded	
NBAR2 capable		Succeeded	
NetFlow collector configure supported		Succeeded	
Flexible NetFlow supported		Succeeded	
Unified Perfmon (AVC/Medianet) Supported		Succeeded	
Medianet Performance Monitoring supported		Succeeded	
MACE AVC Supported	\odot	Not supported	
MLS NetFlow configure supported	\odot	Not supported	
Mediatrace configure supported	٠	Succeeded	
IP SLA Supported	•	Succeeded	
HQF Supported	•	Succeeded	
MAC Table Supported		Not supported	_

Figure 73

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

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

Configure Cisco Features for - B	ranch2-NY.dclo	oud.cisco.com (19	8.19.2.1)			×
Steps	Select Interfac	es				
1. Device Connection Information				s device (maximum 10		
2. CLI Settings (Configuring)		esses and subnet ma for more details.	asks are edital	ble on the table for de	evices that do not	provide them. See
3. CLI Settings (Monitoring)	and aber galae					
4. Select Interfaces	Selected	Interface	Trunk	IP Address	Subnet Mask	Description
5. Select VLANs		GigabitEthernet1		192.168.122.161	255.255.255.0	
6. Select Features		GigabitEthernet2		198.19.2.1	255.255.255.0	
		GigabitEthernet3		100.64.2.2	255.255.255.0	
7. Enable Polling		GigabitEthernet4		10.255.2.2	255.255.255.0	
8. Review Configuration		Loopback0		10.0.2.1	255.255.255.255	
9. Device Updated		Null0				
		VoIP-Null0				
	Selected inte	orface/a), 2				
	Selected inte	chace(s). 5				
	< <u>B</u> ack	<u>N</u> ext > Ei	nish		Can	cel Help

Figure 74

- 49. Step 5: Since there are no active VLANs configured on this exercise, skip past this option if one is shown. You may monitor up to 25 configured VLANs on each device. Click **Next.**
- 50. Step 6: The **Select Features** dialog allows you to turn-on specific Cisco technologies per device interface using the templates included in LiveNX. This dialog displays the current IOS configuration of the device you are currently viewing. Match the settings for **GigabitEthernet3** and **GigabitEthernet4 (WAN interfaces only)**. Click **Next**.

Configure Cisco Features for - B	ranch2-NY.dcloud.cisco.com (198.19.2	2.1)		×
Steps	Select Features			
Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Renable Polling	Select the features you want to enable section. Features on device Associate Probe at IP Address: Interface GigabitEthernet2 GigabitEthernet3 GigabitEthernet4	on each interface. Learn more	about each feature in the Help	
8. Review Configuration 9. Device Updated				
	< Back Next > Einish		Cancel Hel	Þ

Figure 75

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

52. Click Continue

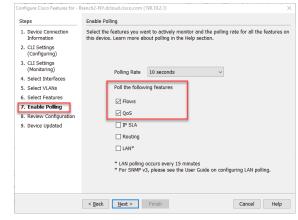


Figure 76

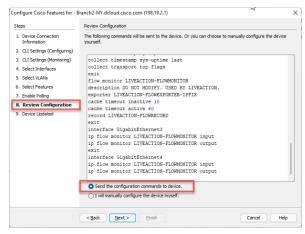


Figure 77

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

teps	Device Updated				
1. Device Connection Information	You have configured this devic configuration to the device's st				
2. CLI Settings (Configuring)	Device Settings				
3. CLI Settings (Monitoring)	Setting		Description		
 Select Interfaces 	Polling Rate			10 seconds	
5. Select VLANs	NetFlow Monitoring			NetFlow collector	
5. Select Features	NetFlow Polling			Enabled	
7. Enable Polling	Mediatrace			N/A	
-	Routing Polling			Disabled	
Review Configuration	Qos Polling			Enabled	
9. Device Updated	IP SLA Polling			Disabled	
	CEF			Enabled	
	Interface Settings				
	Interface Settings			1	-
	Interface	NBAR		NetFlow	
	GigabitEthernet2		٠	•	
	GigabitEthernet3		•	•	
	GigabitEthernet4		•	•	
	GigabitEthernet4		•	•	J

Figure 78

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

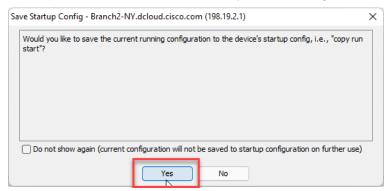


Figure 79

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

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

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

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

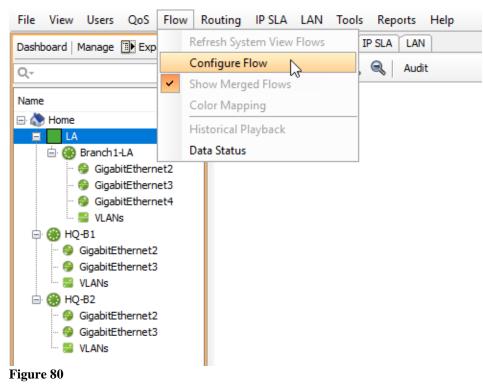
^{4/8/2022} Lab 3.3: Configure Flow on Devices

This Lab uses the Engineering Console.

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

Lab Steps:

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



60. Select Branch2-NY, click Configure Selected.

4/8/2	2022
-------	------

nstruct Select	tions t devices to configure flow										
	onfiguration Table										
Q											
Select	Device	Туре		IP Address	Description	Tags	Traffic	Applic	Voice/Vid	Traditi	Custom
	🛞 Branch 1-LA	Standard	\sim	198.19.1.1	Cisco IOS S	WAN,	۲	۵	۲	۵	
\checkmark	Branch2-NY	Standard	\sim	198.19.2.1	Cisco IOS S	WAN,	۲	•	۲	•	0
	🛞 HQ-B1	Standard	\sim	198.18.129.24	Cisco IOS S	WAN,	•		0	•	
	🛞 HQ-B2	Standard	\sim	198.18.129.25	Cisco IOS S	WAN,	۲	T	۲	0	0
	🛞 HQ-MC	Standard	\sim	198.18.129.23	Cisco IOS S	HQ	•		0	•	•
				T	nese a	re (unc	onfig	gured	J	
				TĽ	iese a	ire (unce	onfig	gured	J	

Figure 81

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

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

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

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

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

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

nstructions	and the second second second second								
Configure the type of flow you low Configuration Table	wish to receive from the i	Interfaces							
Device	Туре	IP Address	Description	Tags	Traffic Sta	Application	Voice/Video P	Traditional	Custom
🚯 Branch2-NY	Standard	√ 198.19.2.1	Cisco IOS Softw		•	•	•	•	•
- 🧐 GigabitEthernet2		198, 19, 2, 1	Branch2 LAN	WAN, Bra					
GigabitEthernet3	-	100.64.2.2	WAN_SP2_MPLS2						0
GigabitEthernet4		10.255.2.2	WAN_SP1_MPLS2						0
		Seman impo	tics are ortant ⊳						
		Seman impo	tics are						
	tion	Seman impo	tics are ortant ▷						
Configure Flow Export Destine		Seman impo	tics are ortant ▷						
Configure Flow Export Destine		Seman impo	tics are ortant ▷						
ow Export Destination Configure Flow Export Destina LiveNX node LiveNX node flow replicator a Other at IP address	t port 9991	Seman impo	tics are ortant						

Figure 82

62. Click Preview CLI.

Multiple CLI Viewer		If you I	nave m	ore tha	n one o	devi	ice t	he c	onfig	urati	on
Device Type Branch2-NY Standard	Branch2-NY	-	h will b						•		
oranich2+41 Standard •	config t ip access-list extended LIVEACTION-ACL-AWC permit top any any exit	1	to view			-					
	policy-map type performance-monitor LIVEACTION-FOLICY-UNIFIED exit class-map match-any LIVEACTION-CLASS-AVC	Flow Configuration								_	
	exit class-map match-any LIVEACTION-CLASS-MEDIANET	Instructions Configure the type of flow yo	u wish to receive fror	n the interfaces							
	exit class-map LIVEACTION-CLASS-AVC match access-group name LIVEACTION-ACL-AVC	Flow Configuration Table									
	exit class-map LIVEACTION-CLASS-MEDIANET	Device	Туре	IP Address	Description	Tags	Traffic				
	match protocol telepresence-media match protocol rtp exit policy-map type performance-monitor LIVEACTION-FOLICY-UNIFIED	Branch2-NY GigabitEthernet2 GigabitEthernet3	Standard	198.19.2.1 198.19.2.1 100.64.2.2	Cisco IOS So Branch2 LAN WAN_SP2_M	WAN,					
	class LIVEACTION-CLASS-MEDIAMET exit class LIVEACTION-CLASS-AVC exit exit inteface GigabitEthernet4	 OgebitEthernet4 	-	10.255.2.2	WAN_SP1_M	_					
	<pre>service-policy type performance-monitor input LIVEACTION-FOLT entitie-policy type performance-monitor output LIVEACTION-FOLT entit interface GigabitEthernet3 service-policy type performance-monitor output LIVEACTION-FOLT extit extit</pre>			Send	ding flow configurati	ions					
	flow record type performance-monitor LIVEACTION-FLOWRECORD-AVC description DO NOT MOIFY. USED BY LIVEACTION. match application name account-on-resolution										
	Close				B						
igure 84		Flow Export Destination Configure Flow Export Dest UiveNX node LiveNX node flow replicato Other at IP address		and port							
		Help		Save to Devices	Preview CLI		Revert		Back		Close

63. Click Close.



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

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

- <complex-block><complex-block><complex-block>
- 67. Don't forget to click **Refresh** in the Filter Bar.

Figure 85

^{4/8/2022} Lab 3.4: Add/Remove Interfaces

This Lab uses the Engineering Console.

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

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

Lab Steps:

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

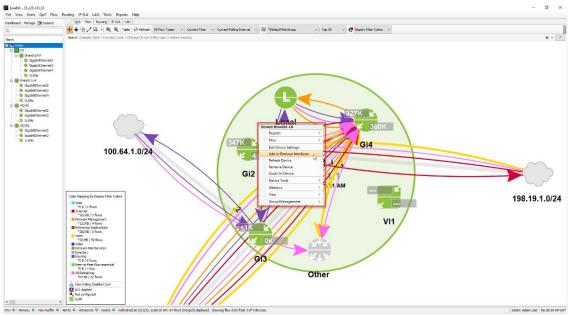


Figure 86

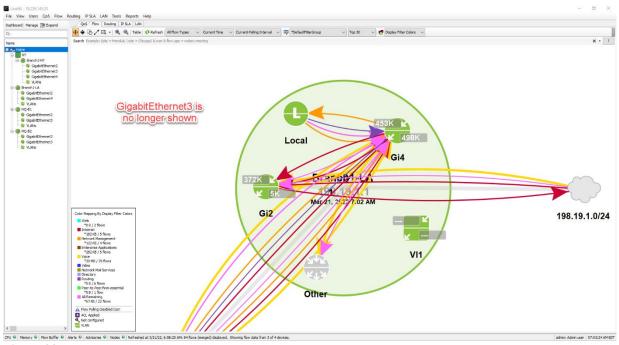
69. Deselect GigabitEthernet3.

Add/Edit Interfaces for Cisco	- Branch1-LA.dclo	oud.cisco.com (1	98.19.1.1)			>
Steps	Select Interfac	ces				
Steps	Select the inte	rfaces you want to	nasks are edit Trunk	this device (maximum 1 table on the table for d IP Address 192.168.122.160 198.19.1.1 100.64.1.2 10.255.12 10.0.1.1	evices that do not p Subnet Mask	Description Branch1LAN WAN_SP2_MPLS2 WAN_SP1_MPLS2
	Selected inte		inish		Canc	el Help

Figure 87

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

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





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

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

^{4/8/2022} Lab 3.5: Merge Clouds in Topology

This Lab uses the Engineering Console.

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

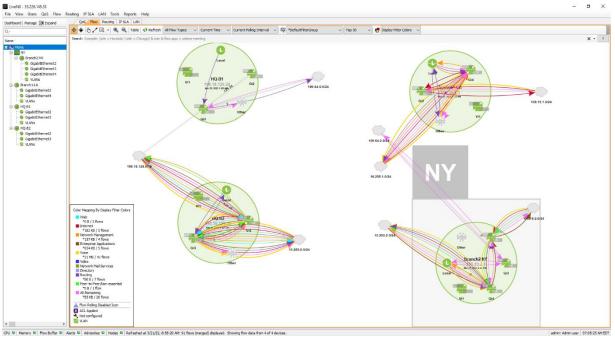


Figure 89

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

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

Lab Steps:

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

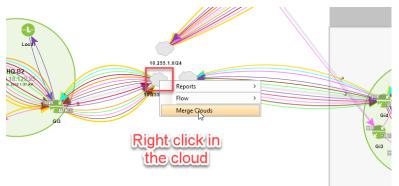


Figure 90

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

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

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

A n diff	PLS arged clouds merged cloud replaces the r ferent clouds where the san louds * 10.255.0.0/24					rves as a bridge b	~ petween
A n diff	rerged cloud replaces the r ferent clouds where the san louds *					rves as a bridge b	
diff	ferent clouds where the san					rves as a bridge b	etween
1	0.255.0.0/24				Click on clouds in the	e topology	
							Find
	*1 1 1 1 1						
C	Click on clouds in the topolo	ogy, or use the "Find" but	ton, or type in space se	eparated subnets using	CIDR notation (e.g., 192	.168.0.0/24).	
bject/Shape Ne	twork Cloud				\sim	<u>~</u> ~.	
Size —			1				2
Tooltip WA	AN Cloud						



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

📐 Sel	lect Clou	ds	\times
Select the	clouds to be	merged:	
		10.0.0.102/32	
		10.0.103/32	
		10.0.1.1/32	
		10.0.2.1/32	
	\checkmark	10.255.0.0/24	
	\checkmark	10.255.1.0/24	
	\checkmark	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	

| | Figure 92

- 78. Click OK.
- 79. Click OK to finish.

🔼 Create Ne	etwork Object	×
Name *	* MPLS	
Type *	6 Merged douds	~
	A merged doud replaces the member douds in the topology with a single object. When used with flows, the merged doud serves as a between different douds where the same flows traversing those douds are connected via the merged doud network object.	bridge
	Clouds * Click on clouds in the topology	
	10.255.0.0/24 10.255.1.0/24 10.255.2.0/24 Click on douds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.166.0.0/24).	Find
Object/Shape	Network Cloud	
Size		þ
Tooltip	WAN Cloud	
* Required Fie	eld OK I	Cancel

Figure 93

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

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

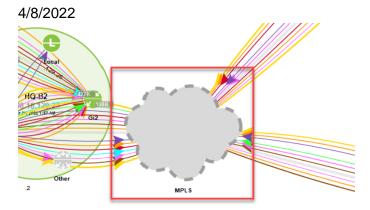


Figure 94

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

Lab 4

Lab 4: Traffic Flows

Lab 4.1: Discover Flows

These Labs uses the Engineering Console exclusively.

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

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

Lap Steps:

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

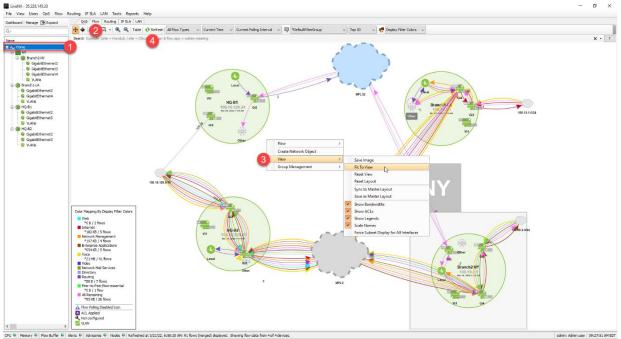


Figure 95

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

5. Set the filters to match: Voice, and DSCP.

6.			
LiveNX - 35.226.145.33			- a ×
File View Users QoS Flow R	outing IPSLA LAN Tools Reports Help		
Dashboard Manage I Expand	QoS Flow Routing IP SLA LAN		
Q.	🕂 🗣 🔀 🖍 🗔 📲 🧠 🔍 Table 🕹 Refresh 🛛 All Flow Types 🗸 Current Time 🗸 Current Poling Interval 🧹 🞼 Voice	🗸 Top 50 🗸 🛃 DSCP 🗸	
Name	Search Example: (site = Honolulu site = Chicago) & wan & flow.app = webex-meeting	Port 1502	× • ?
= 🔊 Hore		IP Address	
B NY Branch24VY		Byte Count	
Branch2-Wr GgabitEthernet2		Rate Performance	
- GgabitEthernet3		Display Filter Colors	
- 🤤 GgabitEthernet4			



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

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

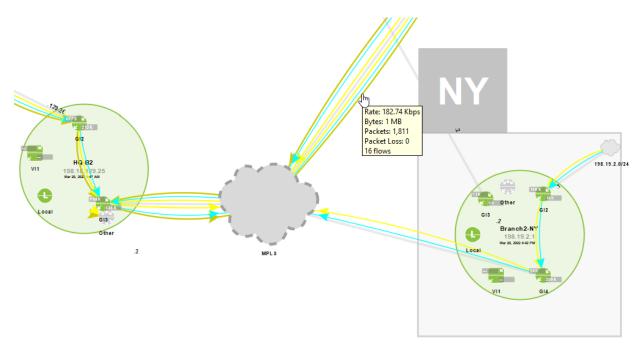
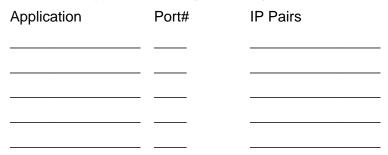


Figure 97

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

What other applications can you identify across our network?



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

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

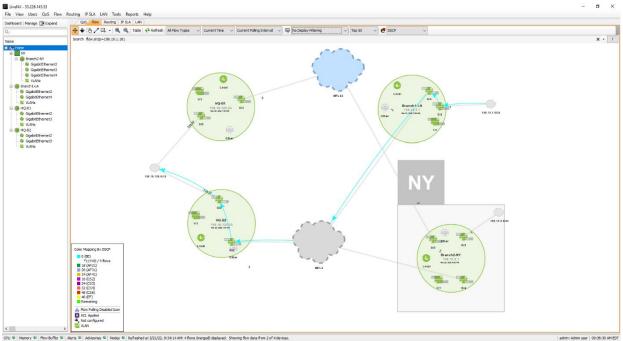
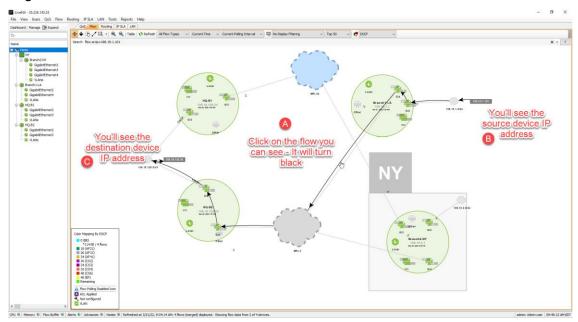


Figure 98

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



^{4/8/2022} Lab 4.3: Examine Specific Traffic

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

- 1. **Double-click** on the Branch2-NY Device or select it on the Home Tree.
- 2. Select IP Addresses as the endpoint display type
- 3. Click on one of the rows relating to Bittorrent.

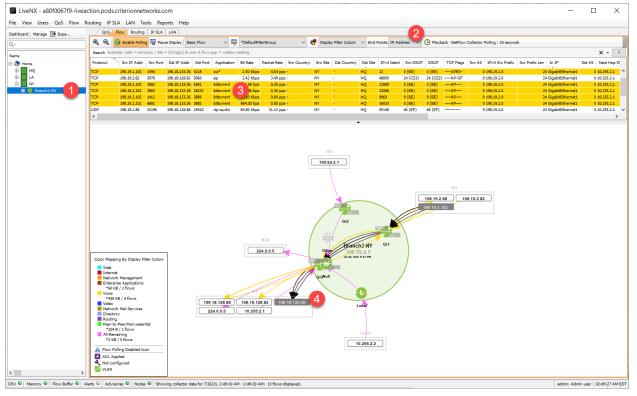


Figure 99

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

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

_____ to/from _____ _____ to/from _____

LiveNX - a9a56379b8-																	- 0
View Users QoS Flov				<u> </u>													
ard Manage 📴 Expa		Flow Routing	-		c Flow	✓ ↓ *Defaulti	EltorGroup	~	Dicelary	Eltor Cole	Frank Frank	Dointry TD	Address		hack NotEl	law Callector I	Polling : 30 seconds
						pp = webex-meeting	nieroroup		- Disbies	The Cold		-one. IF	Address •		Deck Web 1	iow conector P	X
		<u>^</u>			-												
lome	Protocol	¹ Src IP Addr				Application			Src Country		Dst Country		IPv4 Ident			-	Src AS IPv4 Src Pre
HQ	TCP TCP	198.18.133.36 198.18.133.36		198.19.1.101 198.19.2.102	21	ftp*	1.36 Kbps 1.28 Kbps	4.26 pps		HQ HQ	-	LA	27734	0 (BE) 0 (BE)	0 (BE) 0 (BE)		0 198.18.128.0
 HQ-B1 HQ-B2 	TCP	198.18.133.36		198.19.2.102	1494	ica*	1.28 Kbps	3.99 pps		HQ	-	NY	27424	0 (BE)	0 (BE)		0 198.18.128.0
GigabitEthernet1	TCP	198.18.133.36		198.19.1.101	1137	ftp*	1.25 Kbps	3.91 pps		нQ	-	LA	27298	0 (BE)	0 (BE)	R	0 198.18.128.0
GigabitEthernet2	TCP	198.18.133.36		198.19.1.101	1137	ftp*	1.25 Kbps	3.92 pps		HQ	-	LA	27733	0 (BE)	0 (BE)	R	0 198.18.128.0
но-мс	TCP	198.19.2.102		198.18.133.36	2710	bittorrent-networking		0.00 pps		NY	-	HQ	21834	0 (BE)	0 (BE)	AP	0 198.19.2.0
A	TCP TCP	198.19.2.102 198.19.2.102		198.18.133.36 198.18.133.36	2710 2710	bittorrent-networking bittorrent-networking	3.23 Kbps 3.12 Kbps	0.00 pps		NY NY	•	HQ HO	21834 22748	0 (BE) 0 (BE)	0 (BE) 0 (BE)	——AP——	0 198.19.2.0 0 198.19.2.0
Y	TCP	198.19.2.102		198.18.133.36	2710	bittorrent-networking		0.00 pps		NY		HQ	22748	0 (BE) 0 (BE)	0 (BE) 0 (BE)		0 198.19.2.0
Branch2-NY	TCP	198.19.2.102		198.18.133.36	6881	bittorrent	297.62 bps	0.34 pps		NY		HQ	22089	0 (BE)	0 (BE)	AP	0 198.19.2.0
👙 GigabitEthernet1	TCP	198.19.2.102	3882	198.18.133.36	6881	bittorrent	297.62 bps	0.34 pps		NY	-	HQ	22089	0 (BE)	0 (BE)	-AP	0 198.19.2.0
😌 GigabitEthernet2	TCP	198.19.2.102	3883	198.18.133.36	18231	bittorrent	289.35 bps	0.33 pps		NY	-	HQ	22096	0 (BE)	0 (BE)		0 198.19.2.0
GigabitEthernet3	<	100 10 2 102	2002	100 10 100 00	10001	Laternat	200 25 km	0.22.000		LIV.		100	22007	0 (PC)	0 (05)	40	0 100 10 2 0
														,			
		ping By Display F	iter Colors	7					<u></u>		188.	18.128.88	OC1 598.18.198.84	224.0.0.6			
	Veb Inter *39 Netw *17 Enter *16 Voice *83 Video	het KB / 4 flows ork Management KB / 2 flows prise Applications 5 KB / 8 flows KB / 4 flows	266 266 266	540) 2740) 2740.01 2240.01		13 10 10 10 10 10 10 10 10 10 10 10 10 10	16.266.0.2	O Lose	And		188	18.128.82	011 592 10.103.04 103.15.103.04 104.15.103.04 104.16.103.04	224.0.5.6 168.18.128.23			
	Web Intern 17 17 17 18 17 18 Volec 18 Volec 11 11 11 12 11 11 12 11 12 12 13 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 <	Net KB / 4 flows hrk Management KB / 2 flows orise Applications s KB / 8 flows s KB / 4 flows ory (B / 2 flows 10 s B / 3 flows to-Peer/Non-essee 18 / 12 flows	286 286 286 224 0.0.0	286 224.0.0.10			10.256.0.2	0	Other 		224.0.5	18.128.82	198.18.133.34				

Figure 100

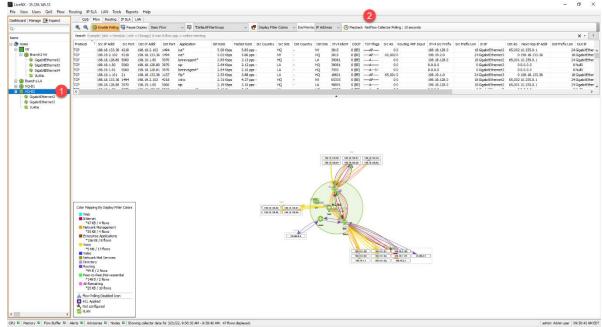
There is some other traffic, such as rtp, sip, and Citrix... but these 2 IPs are mostly generating BitTorrent. Make sure there isn't a ghost server in your network serving movies and such!

^{4/8/2022} Lab 4.4: Troubleshoot Issues

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

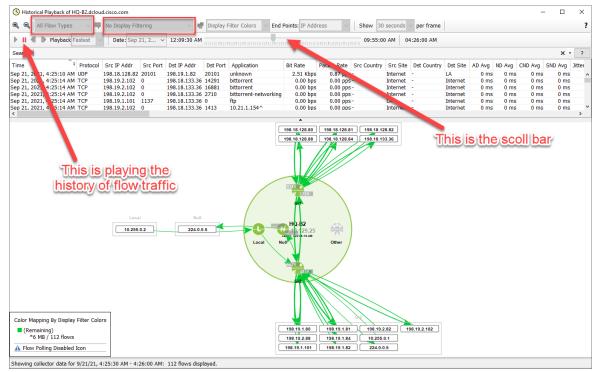
It looks as though we may have an infected PC on the HQ sub-net... we need to identify the source PC by IP Address so that we can re-load anti-virus software on the identified user's workstation.

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



2. Click the Playback button in the Filter Bar.

Figure 101



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

Figure 102

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

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

Lab 5

Lab 5: Custom Filters

^{4/8/2022} Lab 5.1: Creating Custom Filters

These Labs uses the Engineering Console exclusively.

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

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

Lab Steps:

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

tion.pods.criterionnetworks.com		
ting IP SLA LAN Tools Reports Help		
QoS Flow Routing IP SLA LAN		
🔍 🔍 🥵 Enable Polling 🌆 Pause Display Basic Flow	🗸 🖾 DefaultFilterGroup	✓ I Display Filter Colors ✓ End Points: IP Address ✓ (
Search Example: (site = Honolulu site = Chicago) & wan & flow.app = w	v ebex mee ting	

Figure 103

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

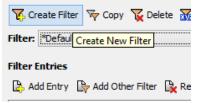


Figure 104

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

Create Flow Display Filter	×
Type in the name of the new flow display fill	ter:
TRG-VoIP	
ОК	Cancel

Figure 105

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

K Flow Display Filters Setup	×
🔀 Create Filter 😽 Copy 🏹 Delete 😿 Rename	Filter Entry Details
Filter: TRG-Voip 🗸	Filter Entry Action: Show or Hide the following
Filter Entries	IP Type: IPv4 Only IPv6 Only Obth IPv4 & IPv6 Color Mapping Label & Color:
💫 Add Entry 🛛 🔓 Add Other Filter 🙀 Delete Entry 🐘 🏬	
TRG-Voip	Basic Advanced
•	Select from a pre-defined list of protocols/applications or create new definitions
	secure-pop3
	secure-telnet
	skinny
	smb smtp
	snmp v
	Match IP, Range, Subnet
	Match IP Addresses Regardless of Source or Destination $\qquad \qquad \lor$
	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
	*HQ-B2.ddoud.cisco.com \vee *GigabitEthernet1 \vee
	Inbound and Outbound Combined Inbound Outbound
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.	Note: Items marked with a (*) are non-historical
Help	OK Cancel Apply

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

✓ Match Protocol/Ports	^
Select from a pre-defined list of protocols/applications or create new definitions	
sip 🗸 🔶 Create 🧷 Edit 🗅	Сору
▼ sip ↓ (L4 Protocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR	5060
(L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR	5060

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

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) □ (L4 Protocol=UDP) AND (Src OR Dst=5060 OR 5061 OR 5062)			
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)			
Match Ports Regardless of Source or Destination \checkmark			
Source: 5060 5061 5062			
Destination: Enter port numbers or ranges separated by spaces (e.g., 80 88-443)			
Help OK Cancel			

Figure 107

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

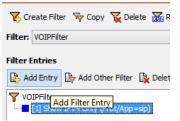


Figure 108

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

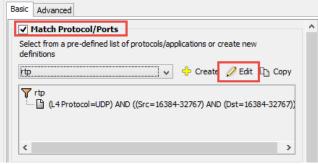


Figure 109

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

Δ	Protocols/Applications Setup			
🕂 Create Defini	tion 🗅 Copy 💥 Delete 쨌 Rename			
Defined Protoco	ls/Applications: rtp 🗸 🗸 🗸 🗸			
Entries				
	🗸 Add Defined Prot/App 🛛 🔒 Delete			
Trp				
	col=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767)			
<	>			
Note: Defined protocols/applications added as entries are not editable here,				
but can be edited by selecting them in the drop-down box above.				
Layer 4 Protocol: UDP (17)				
Ports				
Match Source	and Destination Ports 🗸 🗸			
Source:	16384-32767			
	16384-32767			
Enter port numbers or ranges separated by spaces (e.g., 80 88-443)				
Help	OK Cancel			

Figure 110

12. Click OK

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

🛦 Flow Display Filters Setup	X
🏹 Create Filter 😽 Copy 🏹 Delete 🚮 Rename	Filter Entry Details
Filter: VOIPFilter	Filter Entry Action: • Show or • Hide the following
	IP Type: 💿 IPv4 Only 🔘 IPv6 Only 🔘 Both IPv4 & IPv6
Add Entry By Add Other Filter Delete Entry Delete Entry	Color Mapping Label & Color:
	Basic Advanced
[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
	sip
	▼ sip □ (L4 Protocol=TCP) 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
	Match Device Interface
	Match flows traversing through a particular device's interface *Branch1-LA.dcloud.cisco.com *
	Informed and Outbound Combined Ontbound Outbound
	Note: Items marked with a (*) are non-historical
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.	2
Help	OK Cancel Apply

Figure 111

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

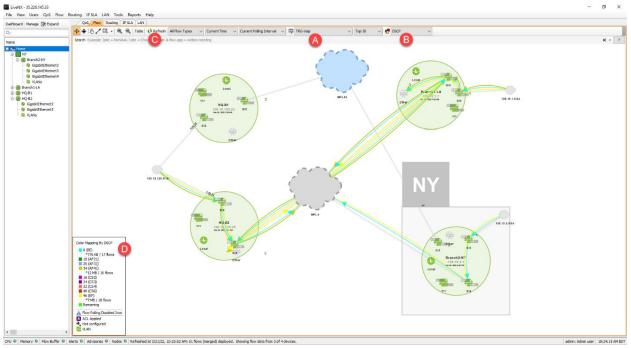


Figure 112

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

^{4/8/2022} Lab 5.2: ACL Creation

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

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

Lab Steps:

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

🛦 LiveNX - a9a56379b8-liveaction	.pods.criterionnetworks.com		
File View Users QoS Flow Ro	outing IP-SLA LAN Tools Re	eports Help	
Dashboard Manage 🗐 Expand	QoS Flow Routing IP SLA	LAN	
Q-	j 🕂 🔶 🔀 🖊 🗔 🔹 🔍	Refresh All Flow T	ypes 💌 Current Time 💌 Currei
Name	Search Example: (site = Honolu	ulu site = Chicago) & wan & flow.app	= webex-meeting
E 🔊 Home			
			HQ
Branch2-NY Device: Branch2-NY	/.dcloud.cisco.com		
Qo5		•	
Flow		•	
Routing		•	
IP SLA		•	
LAN		•	
Edit Device Settin	ngs		*
Add or Remove I	Interfaces		HQ-B2 0198.18.12925
Refresh Device			
Remove Device			
Zoom to Device			
Device Tools		Save to Startup Config	
Statistics		Open Device Web Page	
View		Manage ACLs	
Group Manageme	ent	•	
			1
	-		6

Figure 113

2. Select "Create ACL"

L-BITTORRENT-PC1		
	Extended (Named)	Edit ACL
L-CITRIX-PC1	Extended (Named)	CUICACL
L-FTP-PC1	Extended (Named)	Delete ACL
L-G711-19420	Extended (Named)	
L-INET-PUBLIC	Extended (Named)	 Copy ACL
5T_EFFORT	Extended (Named)	
ITICAL	Extended (Named)	 Apply / Remove ACL
NY_GLOBAL_LEARN_LIST	Extended (Named)	
EACTION-ACL-AVC	Extended (Named)	
P ICE_VIDEO	Extended (Named) Extended (Named)	
ess Rules and Remarks	5	
		Save ACL File
		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 Managem	ent for Branch2-NY			×
Current Route	r Branch2-NY			
	Create ACL		×	
Access Conl	Туре	Extended		e ACL
ACL-BITTORF ACL-CITRIX-I	Name / Number 4	RTPQoSMark	Help	ACL
ACL-FTP-PC1				e ACL
ACL-G711-19 ACL-INET-PU	Access Rules and Re			
BEST_EFFOR			6 Create Rule	ACL
CRITICAL DENY_GLOBA			Copy Rule	move ACL
LIVEACTION-		🛕 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	
	1			
		Preview CLI Save	to Device Cancel	
				Llose
,			· · · · · · · · · · · · · · · · · · ·	

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 > V C Other by Name
Destination
or any O by Network or IP O by Object-Group or any O by Network or IP O 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 Between Image Port(s) Image Port(s) Image Port(s) Image Port(s)
16384 32767
Match by DSCP V
Log Rule Log
OKCancel

Figure 116

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

12. Click Save to Device.

Edit Extended ACL RT	PQoSMark				×
Туре	Extended				
Name / Number	RTPQoSMark			Help	
Access Rules and Re	marks				
remark Marking ACL for				Create Rule	
permit udp any range 1	.6384 32767 any range 16	384 32767		Copy Rule	
				Create Remark	
				Edit Rule/Remark	
				Delete Rule/Remar	k
				Move Up	
			•		
				Move Down	
1					
		Preview CLI	Save to	Device Cance	9

Figure 117

13. Create ACLs for the SIP ports.

urrent Router Branch2-NY			
unencikouter joranchizhin			
ccess Control Lists (ACLs))		
Name / Number	🛆 Туре	Applied Interfaces	Create ACL
ACL-BITTORRENT-PC1	Extended (Named)		
CL-CITRIX-PC1	Extended (Named)		Edit ACL
CL-FTP-PC1	Extended (Named)		Delete ACL
CL-G711-19420	Extended (Named)		
CL-INET-PUBLIC	Extended (Named)		Copy ACL
EST_EFFORT	Extended (Named)		
RITICAL	Extended (Named)		Apply / Remove ACL
ENY_GLOBAL_LEARN_LIST	Extended (Named)		
IVEACTION-ACL-AVC	Extended (Named)		
DP	Extended (Named)		
(TPQoSMark	Extended (Named)		
OICE VIDEO	Extended (Named)		
OICE_VIDEO			
NICE_NDEO			
orce_noto			
ccess Rules and Remarks	5		Save ACL File
ccess Rules and Remarks	5		
ccess Rules and Remarks	s affic		Save ACL File
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		
ccess Rules and Remarks	s affic		

- 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.

Cess Conl		ixtended		× ACL
CL-CITRIX-I CL-FTP-PC1 CL-G711-19	Name / Number 15	JPQoSMark arks	Help	ACL 9 ACL
CL-INET-PU EST_EFFOR			7 Create Rule	ACL
RITICAL ENY_GLOBA			Copy Rule	move ACL
VEACTION-		🛦 Add Remark 🛛 🏹 1	6 Create Remark	i l
DP TPQoSMark		Remark: Marking ACL for SIP Traffic	Edit Rule/Remark	i l
OICE_VIDE		OK Cancel	Delete Rule/Remark	Ī
cess Rule			Move Up	1
emark Markiı ermit udp ar			Move Down	CL File
		Preview CLI Save	to Device Cancel	

- 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		×
C IP C UDP C Object:Group < No Object Groups > V C Other by N	Name	
Source	Destination	
any C by Network or IP C by Object-Group	💽 any 🥤 by Network or IP 🔅 by Object-Group	
e.g 192.168.1.0/24 or 192.168.1.19	>> e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >	
V by Port Between Manage Port(s)	Sofo Sofo Sofo Sofo Sofo Sofo Sofo Sofo	
5060 5062	0000 0002	
Match by DSCP		
Log Rule Log		
	OK Cancel	

Figure 120

Next create another rule for destination SIP Ports.

	Edit Extended ACL SIPQoSACL	×
Type Name / Number	Extended v SIPQoSACL	Help
Remarks remark Marking ACL fo	· CID Traffic	
Tellark Planning ACL TO		Create Remark Edit Remark
Access Rules		Remove Remark
permit tcp any range 5	060 5062 any	Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
	Preview CLI Save	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	x
● permit C deny	
C IP C CDP C Object:Group < No Object Groups > Y C Other by N	lame v Jahp v
Source	Destination
any by Network or IP O by Object-Group	any C by Network or IP C by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19	>> e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >
by Port Equal to Manage Port(s)	Image Port Manage Port(s) Soloo Soloo2
Match by DSCP V	
🗖 Log Rule 🛛 💌	
	OKCancel

Figure 122

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

L Managem	ent for Branch2-NY					
urrent Router	Branch2-NY					
	Edit Extended ACL SI	PQoSMark			>	۲.
ccess Conl						
Nami	Туре	Extended 🗾 💌				B ACL
CL-BITTORF	Name / Number	SIPQoSMark			Help	
CL-CITRIX-I		, .				ACL
CL-FTP-PC1						ACL
CL-G711-19	Access Rules and R	emarks				ACL
CL-INET-PU	remark Marking ACL fo	or SIP Traffic			Create Rule	ACL
EST_EFFOR RITICAL	permit top any range s					
ENY_GLOBA	permit top any any rar	nge 5060 5062			Copy Rule	move ACL
VEACTION-					Create Remark	
OP .					Create Kelliark	
TPQoSMark					Edit Rule/Remark	
IPQoSMark						
DICE_VIDE					Delete Rule/Remark	
cess Rule					Move Up	
mark Markii					Move op	CL File
ermit top an					Move Down	
ermit top an						CL File
	1					
			Preview CLI	Save t	o Device Cancel	
				-		
-						
						Close

Figure 123

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

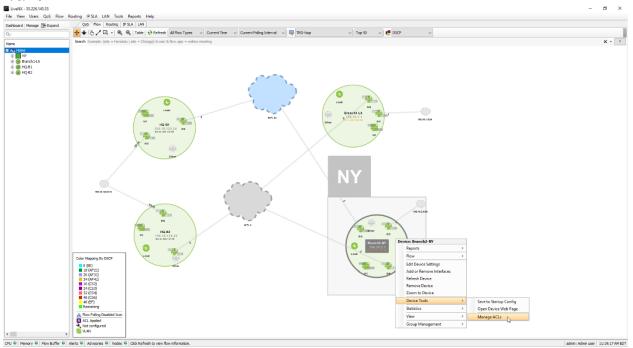


Figure 124

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

CL Manageme	nt for Branch2-I	NY			>
Current Router	Branch2-NY				
Access Contro	l Lists (ACLs)				
Name / Number		~ 1	Туре	Applied Interfaces	Create ACL
ACL-BITTORREN	T-PC1	E	xtended (Named)		Edit ACL
ACL-CITRIX-PC1	1	E	xtended (Named)		Edit ACL
ACL-FTP-PC1			xtended (Named)		Delete ACL
ACL-G711-1942	0		xtended (Named)		
ACL-INET-PUBLI	C		xtended (Named)		Copy ACL
BEST_EFFORT			xtended (Named)		
CRITICAL			xtended (Named)		Apply / Remove ACL
DENY_GLOBAL_I	_		xtended (Named)		
LIVEACTION-AC	L-AVC		xtended (Named)		
RDP			xtended (Named)		
VOICE_VIDEO		E	xtended (Named)		
Access Rules a	and Remarks				
					Save ACL File
					Load ACL File
					Close

Save to File	×
Device Branch2-NY	
ACL-BITTORRENT-PC1 ACL-CITRIX-PC1 ACL-FTP-PC1 ACL-G711-19420 ACL-INET-PUBLIC BEST_EFFORT CRITICAL DENY_GLOBAL_LEARN_LIST LIVEACTION-ACL-AVC RDP RTPQoSMark VOICE_VIDEO	SIPQoSMark
	Remove Save to File Close

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

Save to File					×
Device Branch2-NY					
ACL-BITTORRENT-PC1 ACL-CITRIX-PC1 ACL-FTP-PC1 ACL-FTP-PUBLIC BEST_EFFORT CRITICAL DENY_GLOBAL_LEARN_LIST LIVEACTION-ACL-AVC RDP VOICE_VIDEO	>>	RTPQoSMark SIPQoSMark			
			Remove	Save to File	Close

Figure 127

Save ACL				×
Save in:	📒 Desktop	~	🏂 📂 🛄 •	
Recent Items Desktop Documents	📒 Surveys	agement Slides Export 10-14-21 Config client check		
2	File <u>n</u> ame:	RTPandSIP		Save
Network	Files of type:	ACL Files	~	Cance Save s

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

Figure 128

Go to Branch1-LA - Manage ACL's

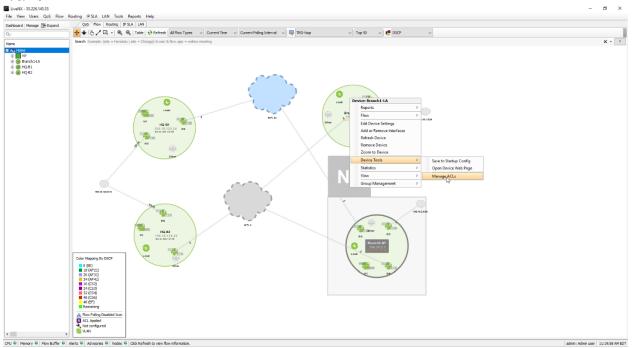


Figure 129

Select Load ACL File

ACL Managemer	nt for Branch1-I	A			×
Current Router	Branch 1-LA				
Access Contro	l Lists (ACLs)				
Name / Number		^ T)	ype	Applied Interfaces	Create ACL
ACL-BITTORREN	IT-PC1	Ex	tended (Named)		Edit ACL
ACL-CITRIX-PC1	L	Ex	tended (Named)		Edit ACL
ACL-FTP-PC1		Ex	tended (Named)		Delete ACL
ACL-G711-19420)	Ex	tended (Named)		
ACL-INET-PUBLI	С	Ex	tended (Named)		Copy ACL
BEST_EFFORT		Ex	tended (Named)		
CRITICAL			tended (Named)		Apply / Remove ACL
DENY_GLOBAL_L	EARN_LIST		tended (Named)		
LIVEACTION-AC	L-AVC	Ex	tended (Named)		
RDP			tended (Named)		
VOICE_VIDEO		Ex	tended (Named)		
Access Rules a	and Remarks				
					Save ACL File
					Load ACL File
					Close

4/8/2022 **Select** the saved ACL file from above (mine is on Desktop)

Load ACL					×
Look in:	📃 Desktop		~	🏂 📂 🛄 •	
Recent Items	📒 Data Mana	agement Slides			
Decker	📒 Surveys				
Desktop	Validation	Export 10-14-21 Confi	g client check	c	
Documents	RTP	andSIP			
This PC					
*	File <u>n</u> ame:				Open
Network	Files of type:	ACL Files		~	Cancel

Figure 131

Loading ACL From File		X
Device Branch1-LA ACL-BITTORRENT-PC1 ACL-CITRIX-PC1 ACL-G711-19420 ACL-INET-PUBLIC BEST_EFFORT CRITICAL DENY_GLOBAL_LEARN_LIST LIVEACTION-ACL-AVC RDP RTPQoSMark VOICE_VIDEO	File RTPandSIP.ad	
	Remove Save to Device Close	5

Figure 132

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

Verify they appear on the ACL list.

CL Manageme	nt for Branch1-	٠LA			
urrent Router	Branch 1-LA				
ccess Contro	l Lists (ACLs)				
Name / Number		~	Туре	Applied Interfaces	Create ACL
CL-BITTORREN	IT-PC1	E	Extended (Named)		Edit ACL
L-CITRIX-PC1	L	E	Extended (Named)		Lucher
L-FTP-PC1			Extended (Named)		Delete ACL
L-G711-1942	-		Extended (Named)		
L-INET-PUBLI	С		Extended (Named)		Copy ACL
ST_EFFORT			Extended (Named)		
ITICAL			Extended (Named)		Apply / Remove ACL
NY_GLOBAL_I			Extended (Named)		
EACTION-AC	L-AVC		Extended (Named)		
P .			Extended (Named)		
PQoSMark			Extended (Named)		
PQoSMark			Extended (Named)		
DICE_VIDEO		E	Extended (Named)		
ccess Rules a	and Remarks				
					Save ACL File
					Load ACL File
					C dtu
					Clase

Figure 133

Close the ACL Management for Branch1-LA window.

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

Lab 6

Lab 6: Making the Topology Work

© Copyright LiveAction 2022

^{4/8/2022} Lab 6.1: Setting Device Semantics

These Labs uses the Engineering Console exclusively.

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

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

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

Lab Steps:

1. Select Expand to set semantics for devices.

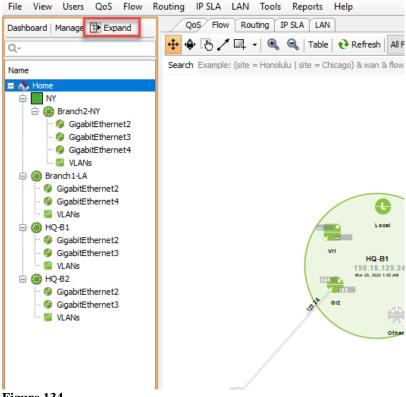


Figure 134

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

4/8/2022

shboard Manage 🔣 Collapse																	Details
																	CPU and Memory Usage
																-	
ne .	IP Address	Node	Label	Input Capa	Output Cap	WAN/XCon	Service Provider	Site	Site IP	Tags	Descr Poling	CPU	Memory	Interface	Class drop	Date C	CPU
Hone																	Menory
E 🛞 Brangh2-NY	198.19.2.1	Local						NY	198.19.2.0/24	East, Sale	Cisco I 10 sec		•	۲	۲	Har 21	269MB of
GebitEthernet2	198.19.2.1		Branch2 LAN			WAN	Branch2 LAN				Branch			•	•		
- 🧐 GigabitEthernet3	100.64.2.2		WAN_SP2_MPLS2			WAN	WAN_SP2_MPLS2				WAN			•	۲		Device Details
- 🧐 GigabitEthernet4	10.255.2.2					None					WAN			•	6		Device name
VLANS											Selecte			۲			Branch2-NY.ddoud.cisco.com
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1, 198, 19.1.0/24		Cisco I 10 sec	6	•	•	•	Mar 21	
GigabitEthernet2	198.19.1.1		Branch1-LA LAN	1.0 Gbps	1.0 Gbps		Branch1LAN				Branch			•	6		Serial number
 – GigabitEthernet4 	10.255.1.2		LA SP1_MPLS	2.0 Mbps	2.0 Mbps	WAN	SP1_MPLS				WAN			•	•		0000000021
- S VLANS											Selecte			•			IP address
9 🛞 HQ-81	198.18.129.24	Local						HQ	198.18.128.0/18		Cisco I 10 sec		۲	•	۲	Mar 20,	198, 19.2.1
- 9 GgabitEthernet2	198.18.129.24		HQ LAN	1.0 Gbps	1.0 Gbps						HQ-LAN			•	•		
 GgabitEthernet3 	100.64.0.2		HQ SP2_MPLS1	4.0 Mbps	4.0 Mbps	WAN	SP2_MPLS				WAN			•	۲		Description
- 🔛 VLANS											Selecte			۲			Cisco IOS Software (Bengaluru), Virtua
) 🛞 HQ-82	198.18.129.25	Local						HQ	198.18.128.0/18		Cisco I 10 sec	6	•	•	6	Mar 20,	Software (X86 64 LINUX IOSD-UNIVERSALK9-M
 GoabitEthernet2 	198.18.129.26		HQ LAN	1.0 Gbps	1.0 Gbps		HQ LAN				HQ-LAN			•	۵		Version 17.4 ta, RELEASE SOFTWARE
– SigabitEthernet3	10.255.0.2		HQ SP1_MPLS1	2.0 Mbps	2.0 Mbps	WAN	SP1_MPLS				WAN			•	6		(fc4)
- S VLANS											Selecte			•			Model
																	dscoProducts.3004
																	OS version
																	17.4.1a
																	Location
																	Site
																	Ste Nr
																	IP 198.19.2.0/24
																	Enter IP address ranges in CIDR f
																	DC
																	Tags Enter tag here then press ENTER to
																	√ Tag Us
																	Branch
																	Branch East Research
																	Sales
																	Sales Office
																	Remove unused tags

Figure 135

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

Adding semantic information to an interface allows you to more easily filter information to see exactly what you are looking for. Clicking an interface or a device will bring up the Semantic config panel on the right of the screen.

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

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

Add the Site IP range to NY Router - 198.19.2.0/24

Add the **Branch** Tag to LA Router (not one of the interfaces) and add the new tags of **West** and **Engineering**.

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

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.

ard Manage 🔣 Collapse													~	Zone			Details	
												1	nese	e Arro	WS 1		CPU a	nd Memory Usage
										_			L. 1				CPU	
ione	IP Address	Node	Label	Input Capa	Output Cap	WAN//(Con	Service Provider	Site	Site IP	Tags	Descr Poling	CPU	Memory	Interface	Class drop	Date Changed	0-0	
NY																	Memor	
Branch2-NY	198, 19, 2, 1	Local						N	198.19.2.0/24	East.Sales Office	Cisco I 10 sec.		•	•	•	Har 21, 2022 11:05 AM	menner	
GigabitEthernet2	198, 19, 2, 1	1000	Branch2 LAN			WAN	Branch2 LAN		ENGLES/ENGLEY	conçoares entre	Branch			0	0	THE LY LOLD LEGISLET		269//8
GigabitEthernet3	100.64.2.2		WAN_SP2_MPLS2			WAN	WAN_SP2_MPLS2				WAN				•			e Details
GigabitEthernet4	10.255.2.2					None					WAN			•	•		Site	
- S VLANS											Selecte			•			Tags	
Branch1-LA	198.19.1.1	Local						LA	10.0.1.1,198	Branch,Engineer.	Cisco I 10 sec.		۲	•	•	Mar 21, 2022 10:59 AM		er tag here then press ENTER
GigabitEthernet2	198.19.1.1		Branch1-LA LAN	1.0 Gbps	1.0 Gbps	None	Branch1LAN				Branch			•	•			er tøgnere tilen press birt b
GigabitEthernet4	10.255.1.2		LA SP 1_MPLS	2.0 Mbps	2.0 Mbps	WAN	SP1_MPLS				WAN			•	۲		1	Tag
S VLANS											Selecte			•				Branch
HQ-81	198.18.129.24	Local						HQ	198.18.128.0/18		Cisco I 10 sec.	😜	6	6	•	Mar 20, 2022 1:55 AM		East
GigabitEthernet2	198.18.129.24		HQ LAN	1.0 Gbps	1.0 Gbps						HQ-LAN			•	۲			Engineering Research
· 6 GigabitEthernet3	100.64.0.2		HQ SP2_MPLS1	4.0 Mbps	4.0 Mbps	WAN	SP2_MPLS				WAN			•	•		1 H	Research Sales
- 🔛 VLANS											Selecte			•				Sales Office
HQ-82	198.18.129.25	Local						HQ	198.18.128.0/18		Osco I 10 sec.	😐	•	•	۲	Mar 20, 22 1:57 AM	Ŭ	West
·	198.18.129.26		HQ LAN	1.0 Gbps	1.0 Gbps		HQ LAN				HQ-LAN			•	•			
 GigabitEthernet3 VLANs 	10.255.0.2		HQ SP1_MPLS1	2.0 Mbps	2.0 Mbps	WAN	SP1_MPLS				WAN Selecte				•			
											Add	Nev	y Ta	gs He	ere			
												Þ						
																		Remove unused tags
			Showing collector data f															admin: Admin user 11:2

oard Manage 💽 Collapse																Details
																Interface Details
		_									_					Interface name
	IP Address	Node	Label	Input Capa	Output Cap WAN	KCon Service Provider	Site	Site IP	Tags	Descr Po	iling CPU	Memory	Interface	Class drop	Date Changed	Gigabit[]thernet4
iome			-													IP address
NY Branch2-NY	198.19.2.1	Local					NY	100 10 2 0 00	East, Sales Office	Correct 10					Mar 21, 2022 11:05 AM	10.255.1.2
GigabitEthernet2	198.19.2.1	LOCA	Branch2 LAN		WAN	Branch2 LAN	N.	196, 19, 2, 0/24	East, sales office	Branch	bec		õ	ē	Har 21, 2022 11:05 MH	Description
GigabitEthernet3	100.64.2.2		WAN_SP2_MPL52		WAN	WAN_SP2_MPL52				WAN			•			WAN_SP1_MPLS2
- 🤤 GigabitEthernet4	10.255.2.2				None					WAN			•	•		
Branch1-LA	198.19.1.1	t and							Branch,Engineer.	Selecte					Mar 21, 2022 10:59 AM	
g branch1-LA	198.19.1.1 198.19.1.1	Local	Branch 1-LA LAN	1.0 Gbps	1.0 Gbps None	Branch1 LAN	LA	10.0.1.1,198	branch,brigneer.	Branch 10	sec				Mar 21, 2022 10:59 AM	
GgabiEthernet4	10.255.1.2		LA SP1_MPLS	2.0 Hbps	2.0 Mbps WAN	SP1_MPLS				WAN			•			Interface type
VLANS										Selecte			•			ethernet_csmacd
HQ-81	198.18.129.24	Local					HQ	198.18.128.0/18		Cisco I 10	sec (•	•		Mar 20, 2022 1:55 AM	Interface speed
GgabitEthernet2 GgabitEthernet3	198.18.129.24 100.64.0.2		HQ LAN HQ SP2_MPLS1	1.0 Gbps 4.0 Mbps		SP2_MPLS				HQ-LAN WAN				-		1000000000
VLANS	100.04.0.2		mg or a MPLS1	4.0 Mops	HUMPPS WAY	or a_NPL5				Selecte				•		-
HQ-82	198.18.129.25	Local					HQ	198.18.128.0/18		Osco I 10	sec (•	ē	۲	Mar 20, 2022 1:57 AM	Define
GgabitEthernet2	198.18.129.25		HQLAN	1.0 Gbps		HQ LAN				HQ-LAN			•	۲		Label LA SP 1_MPLS
GgabitEthernet3	10.255.0.2		HQ SP 1_MPLS 1	2.0 Mbps	2.0 Mbps WAN	SP1_MPLS				WANG			8	•		
VLANS										Selecte			•			Input Capacity 20
																Output Capacity 20
																Service Provider
																WAN Type WAN
																Name SP1_MPLS
																Remove unused service provid
																Tags
																Enter tag here then press ENTER
																√ Tag
																Branch East Engineering Research Sales Office West
																Engineering
																Research Sales
																Sales Office
																West Vest



- 2. Select the device and then on the bottom right portion you will see a **Site** field.
- 3. Configure each device to a site as shown below if it is not already done:

a. Branch1-LA Device as LA

b. Branch2-NY Device as NY

c. HQ-B2 Device as HQ

oard Manage 📑 Collapse																		Details	
																		CPU and	Memory Usage
	IP Address	Node	Label	Inc. A Cons.	Output Cap	WAN INCOM	Service Provider	Site	Site IP	Tacs	Owner	Polina (-		Interface	Chara dava	Date Changed	CPU	
Home	Dr Address	NUCLE	Laber	piput capa	Cuput cap	WWWWCon	Service Provider	Side	Side Dr	Tags	Dest	Poing C	10	Plentry	propriate	Class crop	bate changes		
NY																		Memory	
🗄 🛞 Branch2-NY	198.19.2.1	Local						NY	198.19.2.0/24	East,Sales Office	Cisco I	10 sec	•	•	•	•	Mar 21, 2022 11:05 AM		269MB
GigabitEthernet2	198.19.2.1		Branch2 LAN			WAN	Branch2 LAN				Branch				۲	۲		Device D	
- 🚱 GigabitEthernet3	100.64.2.2		WAN_SP2_MPL52			WAN	WAN_SP2_MPLS2				WAN				•	•		· · · · · · · · · · · · · · · · · · ·	
- 🚱 GigabitEthernet4	10.255.2.2					None					WAN				•	•		Device nam	
VLANs											Selecte				•			Branch1-L	A.dcloud.cisco.com
Branch1-LA GoabitEthernet2	198.19.1.1 198.19.1.1	Local	Branch 1-LA LAN	1.0 Gbps	1.0 Gbps	None	Branch 1 LAN	LA 🔍	10.0.1.1,198	Branch,Engineer.	Branch	10 sec	•	•	•	•	Har 21, 2022 10:59 AH	Serial num	
GgabitEthernet4	10.255.1.2		LA SP1_MPLS	2.0 Mbps	2.0 Mbos		SP1_MPLS				WAN							101	
VLANs	2012001212		010120100	2101000	21011000		0.19.00				Selecte					-		IP address	
HQ-81	198.18.129.24	Local						HQ	198.18.128.0/18		Cisco I	10 sec	•	•	•	•	Mar 20, 2022 1:55 AM		
GgabitEthernet2	198.18.129.24		HQ LAN	1.0 Gbps	1.0 Gbps	None					HQ-LAN				۲	۲		198.19.1.	
GgabitEthernet3	100.64.0.2		HQ SP2_MPLS1	4.0 Mbps	4.0 Mbps	WAN	SP2_MPLS				A				۲	۲		Description	
- 🔛 VLANs											Selecter.				6			Cisco IOS	Software [Bengaluru], Vir
HQ-82	198.18.129.25	Local						HQ	198.18.128.0/18	1	Osco I	10 96.	•	۲	۲	۲	Mar 20, 2022 1:57 AM	Software Orac 64	.INUX_JOSD-UNIVERSALK
GgabitEthernet2	198.18.129.26		HQ LAN	1.0 Gbps	1.0 Gbps		HQ LAN				HQ-LAN				•	۲		Version 13	.4.1a, RELEASE SOFTWA
GgabitEthernet3	10.255.0.2		HQ SP1_MPLS1	2.0 Mbps	2.0 Mbps	WAN	SP1_MPLS				WAN				•	•		(fc4)	
- 🖺 VLANs											Selecte				•			Model	
																		dscoProdu	acts.3004
																		OS version	
																		17.4.1a	
																		Location	
								2										Enter DC Tags Enter t V 1 V 8 S 5 S 7 S 7 S 8 S 7 S 7 S 8 S 7 S 7 S 7 S 7 S 7 S 7 S 7 S 7 S 7 S 7	11.1 19.10/24 19 address ranges in CED ag here then press ENTER 10 10 10 10 10 10 10 10 10 10
Memory C Flow Buffer C																			Remove unused tags

- Figure 138
 - 4. Open the dashboard to ensure that data is populating correctly.

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

File View Users QoS Flow F	Couting IPSLA I	AN Tools F	Reports Help
Dashboard Q VS			
Name	IP Address	Node	Label
Home i i Im NY			
⊟ ↔ Branch2-NY GigabitEthernet2	198.19.2.1 198.19.2.1 100.64.2.2	Local	Branch2 LAN
🚱 GigabitEthernet3 😌 GigabitEthernet4 🔜 VLANs	10.255.2.2		WAN_SP2_MPLS2
Branch1-LA	198.19.1.1	Local	
🛛 🔮 GigabitEthernet2	198.19.1.1		Branch1-LA LAN
- 😔 GigabitEthernet4	10.255.1.2		LA SP1_MPLS
Бigure 139	198 18 179 74	Local	

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



Site WAN Interface Utilization

u0	¹ Interface L	Input Capa	Output Ca	Input Avg	Input Peak	Output Avg	Output Peak	CPU Avg	CPU Peak	Memory Avg	Memory Pe
HQ	HQ SP1_MPLS1	2,000	2,000,000	25 %	59 %	0 %	0 %	31 %	32 %	12 %	12 %
HQ	HQ SP2_MPLS1	4,000	4,000,000	0 %	0 %	0 %	0 %	29 %	30 %	13 %	13 %
LA	LA SP1_MPLS	2,000	2,000,000	18 %	29 %	0 %	0 %	30 %	32 %	13 %	13 %
NY	Branch2 LAN							27 %	29 %	12 %	12 %
NY	WAN_SP2_MP							27 %	29 %	12 %	12 %

Figure 140

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

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

Dashboard							_	
System Application QoS	Flow IP SLA WAN	I						
Main 🄇	Flow Alerts -							^
Alerts						Alert	Count	
Reports	1						dia packet rate	0 ^
							dia packet loss p	0
Setup 🎗	Ξ					High ne		0
Setup (*)	Alert Count						ransmission count	0
Discover Devices	tc	There is r	io data to display for th	e given time pe	eriod		of Policy event o	0
Manage Devices	ler						- packet/byte d	0
Define Sites	<						A - one way delay	0
							A - jitter inter arri	0
Configure Alerts							4 - unreachable ed NetFlow address	0
Configure Flow	0					Diacking	ed Nethow address	• •
	Flow source wan xcon						×	Apply ?
Application (\$							15m 3	30m 1hr 4hr
Application Performance	Basic Flow					07/23/21, 05	5:45:00 AM to 07/23/21	, 06:00:00 AM
Manage Application Groups								
	Top 10 Source	Addres Bytes \vee			Top 10 Destinat	ion Addres Bytes	\sim	
	Src IP Addr	Bytes	¹ Flows		Dst IP Addr	Bytes	1 Flows	
	· -		2 MB	5	· -		6 MB	15
	± -		628 KB	321	± -		864 KB	293
	± -		248 KB	96 9	+ - + -		589 KB	28
	± -		192 KB 9 KB	9	± -		126 KB 77 KB	98
	· ·		8 KB	13	· ·		19 KB	32
	· •		7 KB	13	· -		916 B	2
	± -		7 KB	13	+ -		168 B	3
	· ·		2 KB	4	· ·		152 B	2
	± -		456 B	6	± -		152 B	2
	Top 10 Source (Countr Bytes ∨			Top 10 Destinati	on Countr Bytes		
	Src Country	Bytes	¹ Flows		Dst Country	Bytes	1 Flows	
	Unknown		3 MB	500	Unknown		7 MB	485
								~
	<							>

Figure 141

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

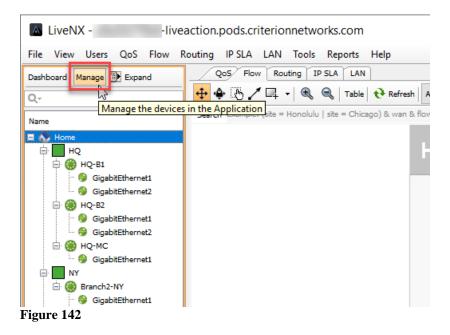
^{4/8/2022} Lab 6.2: Adding Devices to Groups

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

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

Lab Steps:

1. Open the Device Management window by selecting Manage.



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

2. Select "Edit Groups"

Filter	by:					Filter		Clear					
	Device Name Branch1-LA Branch2-NY HQ-B1 HQ-B2	IP Address 198.19.1.1 198.19.2.1 198.18.129.24 198.18.129.25		Model ciscoProducts.3004 ciscoProducts.3004 ciscoProducts.3004 ciscoProducts.3004	Local Local	Group	Poll	QoS V V V	Flow V V V	IP SLA	Routing		_
	ling occurs every 15 min	nutes					co Cottin					Nu	mber of Devices
-	ling occurs every 15 min Configurations	Configure QoS, Flo	ow, and I	PSLA		Global Devi Edit	_ `	gs	MP Settin	gs		Nu	mber of Devices
-	Configurations		able and click	P SLA the configure button.			D	efault SNI		-	s - Not Set	Nu	mber of Device:
	Configurations Configure	Configure QoS, Fl Select devices in the ta	able and click	P SLA the configure button.	~	Edit		efault SNI efault CLI	[Monitorii	-		Nu	
evice (Configurations Configure Remove	Configure QoS, Flo Select devices in the ta Remove selected device	able and click	the configure button.	~	Edit Edit		efault SNI efault CLI	[Monitorii	ng Settings		Nu	Clear
	Configurations Configure Remove Add To Group	Configure QoS, Fk Select devices in the ta Remove selected devic	able and click	the configure button.	~	Edit Edit		efault SNI efault CLI	[Monitorii	ng Settings		Nu	Clear

Figure 143

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

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

ps			
Name	^	Size	Add
NY		1	Edit
			Remove

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

🛕 Add Group		×
Name (*) LA 4		
Description Los Angeles Group		
5	6	
All Other Devices	<u> </u>	Current Group of Devices
Q,	•	Q_
(NY) Branch2-NY	÷	Branch1-LA
HQ-B1		
HQ-B2		
Asterisks (*) indicate required fields.		
		Add Done Cancel

Figure 145

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

Once completed your groups should look like the one below.

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

4/8/2022		
🔼 Edit Groups		×
Groups		
Name	^ Size	Add
HQ LA	2	Edit
NY	1	Remove
		Close

Figure 146

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

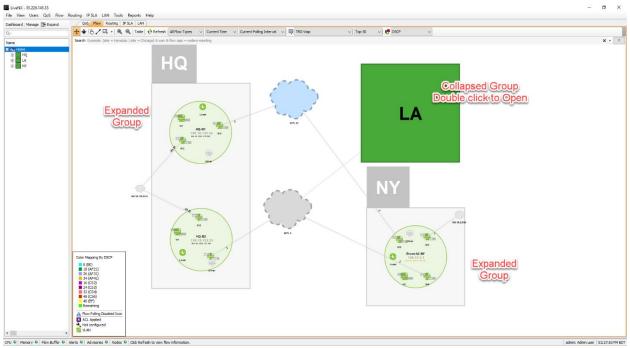


Figure 147

^{4/8/2022} Lab 6.3: Creating Network Objects

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

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

Lab Steps:

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

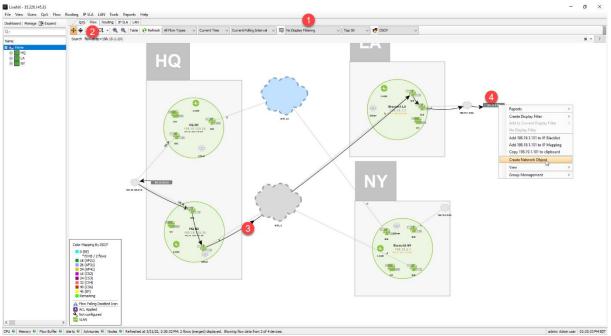


Figure 148

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

🔝 Edit N	etwork 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 for flows to be drawn to the network object.	л
	IP Address *	
	198.19.1.101	
	Type in an IP address, or select a device interface or IP address end point in the topology.	
Object/Shape	PC ~	
Size	IP Phone	
Tooltip	Network Cloud Network Cloud (blue)	
* Required Fie	Router Switch Processor	el
	Custom V	

Figure 149

7. Click Refresh.

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

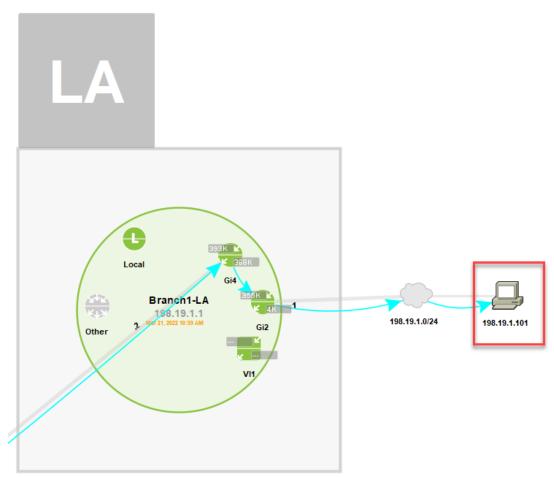


Figure 150

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

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

Create Ne	twork Object	×				
Name *	NY Server					
Type *	IP address end point	~				
Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merge order for flows to be drawn to the network object.						
	IP Address * 198.19.2.102 Type in an IP address, or select a device interface or IP address end point in the topology.					
Object/Shape	File Server ~					
Size	File Server					
	Generic Square IP Phone					
	lanton					
	Network Cloud	OK Cancel				
	Network Cloud (blue) PC V					
	ru 🗸					

Figure 151

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

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



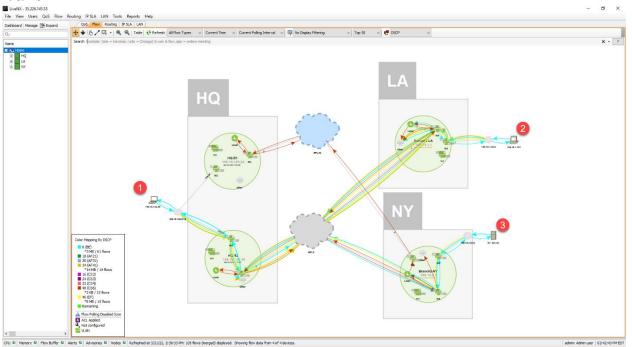


Figure 152

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

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

Flow	>		
Create Network Object			
View	>	Save Image	
Group Management	>	Fit To View	
		Reset View	
		Reset Layout	
		Sync to Master Layout	
		Save as Master Layout	
		 Show Bandwidths 	
		 Show ACLs 	
		 Show Legends 	
		 Scale Names 	
		Force Subnet Display for All Interface	s



Lab 7

Lab 7: Dashboards & Reports

^{4/8/2022} Lab 7.1: The Dashboard

This Lab uses the Engineering Console.

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:

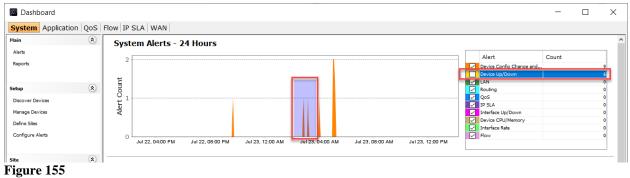
1. Click the **Dashboard** tab (above the Home Tree-view). You will first see the **System** Dashboard.

Dashboard										-	
System Application QoS	Flow IP SLA WAN	I I									
lain 1 ®	System Alert	s - 24 Hours									
	2							Alert	Cou	nt	
Reports	-							Device Config	Change a		17
								LAN			0
	Alert Count							Routing			0
tup 🛞	5							QoS			0
scover Devices	¥ 1							IP SLA			0
	l le l							Interface Up/D Device Up/Dow			0
anage Devices	<							Device Op/Dow			0
fine Sites								Interface Rate	emory		0
onfigure Alerts	0							Flow			0
-	04:00 PM 0	06:00 PM 08:00 PM	10:00 PM 12:00 A	M 02:00 AM 04:	00 AM 06:00 AM 0	8:00 AM 10:00 AM 1	2:00 PM 02:00 PM				
										30m 1hr	
									151	- 50m m	4111
te WAN Interface Utilization	Sucton Statu	16									
ite WAN Interface Utilization	System Statu	IS						03/21/22, 02:15:0	00 PM to 03/21	/22, 02:30:0	00 PN
te WAN Interface Utilization	System Statu Top 10 CPU Usa					Top 10 Memo		03/21/22, 02:15:0	0 PM to 03/21	/22, 02:30:0	00 PN
	Top 10 CPU Usa	ige				-	ry Usage	03/21/22, 02:15:0		/22, 02:30:0	00 Pf
	Top 10 CPU Usa			¹ Peak		Device			¹ Peak		
	Top 10 CPU Usa	ige	30	%	32 %	Device HQ-B1	ry Usage	13	1 Peak		13 9
	Top 10 CPU Usa Device HQ-82 HQ-81	ige	30 29	%	30 %	Device HQ-B1 Branch1-LA	ry Usage	13	1 Peak 3 %		13 9 13 9
	Top 10 CPU Usa Device HQ-82 HQ-81 Branch1-LA	ige	30 29 29	%	30 % 30 %	Device HQ-B1 Branch1-LA HQ-B2	ry Usage	15	1 Peak 3 % 3 %		13 9 13 9 12 9
	Top 10 CPU Usa Device HQ-82 HQ-81	ige	30 29	%	30 %	Device HQ-B1 Branch1-LA	ry Usage	15	1 Peak 3 %		13 9 13 9 12 9
	Top 10 CPU Usa Device HQ-82 HQ-81 Branch1-LA	Avg	30 29 29 27	%	30 % 30 %	Device HQ-B1 Branch1-LA HQ-B2	Avg	11 12 12 12 12 12	1 Peak 3 % 3 %		13 % 13 % 12 %
	Device HQ-82 HQ-81 Branch14A Branch2-NY	Avg	30 29 29 27 27 Nutput BW (Klops)	%	30 % 30 % 27 %	Device HQ-81 Branch1-LA HQ-82 Branch2-NY	Avg	11 12 12 12 12 12	1 Peak 3 % 3 %		13 % 13 % 12 %
	Top 10 CPU Use Device HQ-82 HQ-81 Branch14A Branch14A Branch24YY	Avg Avg ReBandwidth 0 Device	30 29 29 27 Dutput BW (Klops) ~ Description	96 96 96 96 96 96 96 96 96 96 96 96 96 9	30 % 30 % 27 %	Device HQ-81 Branch1-LA HQ-82 Branch2-NY Top 10 Interfa	Avg	11 11 12 12 12 12 12 12 12 12 12 12 12 1	1 Peak 3% 2% 2%		13 9 13 9 12 9 12 9
	Top 10 CPU Usa Device HQ-82 HQ-81 Branch14A Branch14A Branch24Yr	Avg	30 29 27 27 Nutput BW (Kdps) ↓ Description WAN_SP1_MP	4	30 % 30 % 27 % Output B 1 397	Device HQ-81 Brench1-LA HQ-82 Brench2-NY Top 10 Interfa	Avg	11 12 12 12 12 12 12 12 12 12 12 12 12 1	1 Peak 3 %	Output D	13 % 13 % 12 %
	Top 10 CPU Use Device HQ-82 HQ-81 Branch1-LA Branch1-LA Branch2-NY Top 10 Interface Interface GgabitEtherne13	Avg	30 29 27 Autput BW (Kbps) ~ Description WAN_SP1_MP	% % % % % % % % % % % % % % % % % % %	30 % 30 % 27 % Output B 1 397 392	Device HQ-81 Brench1-LA HQ-82 Brench2-NY Top 10 Interface GgabitEtherent2	Avg	ut Drops (pps) V Description HQ-LAN WAN, SP2_MP	1 Peak 3 %	. Output D	13 % 13 % 12 %
	Top 10 CPU Use Device HQ-82 HQ-81 Branch14A Branch24Yr Top 10 Interface GgabitEthernet3 GgabitEthernet3	Avg	30 29 27 27 27 27 27 27 27 27 27 27 27 27 27	96 % % % %	30 % 30 % 27 % Output B 1 397 392 119	Device HQ-81 Brench-LA HQ-82 Brench-LA HQ-82 Brench-LA MY Top 10 Interface GgabitEthernet2 GgabitEthernet3 GgabitEthernet3	Avg Avg Device HQ81 HQ81	11 11 12 12 12 12 12 12 12 12 12 12 12 1	I Peak 3% % 7%	. Output D 0	13 % 13 % 12 %
	Top 10 CPU Use Device HQ-82 HQ-81 Branch14A Branch24Yr Top 10 Interface GgabitEthernet3 GgabitEthernet3	Avg Avg Ee Bandwidth Device HQ-82 Branh1-KA HQ-82 Branh2-KY	30 29 27 Autput BW (Kbps) ~ Description WAN_SP1_MP	9% % % % % % % % % % % % % % % % % % %	0 % 30 % 27 % 0utput B 1 392 119 119	Device HQ-81 Branh1-LA HQ-82 Branh2-NY Top 10 Interfac Interface GgabitEthernet2 GgabitEthernet3	Avg Avg Avg Device HQ81 HQ81 Branh14A	ut Drops (pps) V Description HQ-LAN WAN, SP2_MP	1 Peak 36 37 38 38 38 39 39 39 39 39 39 39 39 39 39 39 39 39	- Output D 0 0	13 % 13 % 12 % 12 %

Figure 154

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

- 2. Un-check any alerts that are not relevant to your view (in this case, device up down as we have been working in a lab environment to build this course we know what those incidents are)
- 3. Left-click-Drag to Zoom into a flow of interest.



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

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

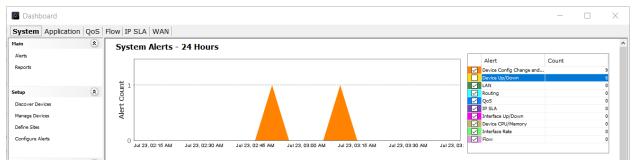


Figure 156

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

Dashboard		- 🗆	\times
System Application QoS	Flow IP SLA WAN		
Main	System Alerts - 24 Hours		^
Alerts	Alert	Count	
Reports	3		9
			0
Setup 🎗	ⁱ g 2 ⁱ g 2	Show Alerts	
Discover Devices Manage Devices	IPSLA ₹	Select All	15
Define Sites	Device CPU/Memory	Select None	
Configure Alerts	I Interface Rate	Export Legend Dat	a
	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		
0			

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

Time	Severity	Device	Group)	Alert Type	^1 Details
016/05/13 01:35:31 PM	Warning	HQ-SJ	Flow	_		t loss percent High media packet loss percent
016/05/13 05:49:30 PM	Warning	HQ-SJ	Flo	Open Report	packe	t loss percent High media packet loss percent
016/05/13 08:44:30 PM	Warning	HQ-SJ	Flo	Drill Down on Sp	pecific Flow	Top Analysis Report
016/05/13 09:04:02 PM	Warning	HQ-SJ	Flo			TOP Analysis Report
016/05/13 11:01:01 PM	Warning	HQ-SJ	Flo	Export Data		Top Conversations Report
016/05/13 01:35:02 PM	Warning	Branch 1-LA	Flow		High media (Bidirectional Source/Destination Pair Report
016/05/13 05:49:30 PM	Warning	Branch 1-LA	Flow		High media (
16/05/13 11:01:01 PM Warning I 16/05/13 01:00:36 PM Warning I 16/05/13 01:01:36 PM Warning I 16/05/13 01:01:36 PM Warning I		Branch 1-LA	Flow		High media (Source or Destination Address Report
		Branch 1-LA	Flow			Address Pair Report
		HQ-SJ	Interfa			
		HQ-SJ	Interfa			Destination Address Report
		HQ-SJ	Interfa	ace Up/Down	Interface er	Source Address Report
		HQ-SJ	Interfa	ace Up/Down	Interface er	Destination Address Popularity Report
016/05/13 01:11:36 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	1 2 1
016/05/13 01:12:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	Source Address Popularity Report
016/05/13 01:17:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	Site Traffic Report
016/05/13 01:17:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	Destination Site Traffic Report
016/05/13 01:22:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	
016/05/13 01:22:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface er	Source Site Traffic Report
016/05/13 01:27:35 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/0;
016/05/13 01:27:35 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/1;
016/05/13 01:33:06 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/0;
016/05/13 01:33:35 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/1;
016/05/13 01:38:36 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/0;
016/05/13 01:38:36 PM	Warning	HQ-SJ	Interfa	ace Up/Down	Interface error	Interface name - Ethernet0/1;
 ✓ Filter by Time Start Time 05/13/16 End Time 05/14/16 	 ✓ 12:00:00 PM			Filter by A Device una		×
Filter by Severity	Include higher priorities		mber of Results			

Figure 158

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

7. Review the Top Analysis Report.

	Top Analysis										
rts terface Bandwidth op Analysis s and Ports	Тор А	nalys	is	AT					15m 1h 6h	1d 1w 30d 9	Custom
ddress	05/1	3/16, 01:05	5:31 PM to 05/	13/16, 02:05	:31 PM			Execute Report			
oS	Source HQ-S	53		~	··· All Interfac	es	~	Number of flows	s: 1	CSV	File Result
etwork	Filter *Def	aultFilterGroup	o 🗸 🤿 i	Inbound	~			Medianet	✓ Time Sorted	- Unique Flows 🗸	/
oplications (AVC) SEL	Search JUDP & f	low port src=200	04.8 flow port dst=2	20004 & flow dscn=1	BE & flow direction=ING	RESS & flow media	anet event=0.8 flow	medianet.eventStop=0 & flow.medianet.m	nonitorEventError=60	28427459993272326	x • ?
R	bearen oor en	iomportiore-zoo									
ireless nyConnect									Q,-		
scellaneous	Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co Src Country	Dst Country	RTP SSRC	Direc
om Reports	May 13, 2016 1:3	. UDP	198.19.1.81	20,004	198.18.128.81	20,004	rtp	1 -	-	2432754705	INGRI
Actions											
s											
c Actions											
s											
s											
s											
is ile											
s											

Figure 159

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

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

^{4/8/2022} Lab 7.2: Viewing Reports

This Lab uses the WebUI.

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.

d Main	ere						ch Applyfilter C Au
Topology						Active Monts	
E Stories	DEVICE	S: 4		INTERFACES: 9		A List to CT A Branch 14 Added cisto con summa application to had 200,00 mc of jitter for traffic with a 1602P value of 49 (FF) A Branch 14 Added cisto con summa application to had 200,00 mc of titter for traffic with a 562P value of 49 (FT)	TIME OPENED 22 Sep 2021, 05:52 Ab 22 Sep 2021, 05:52 Ab
M Reports	O DEVICE	s 🗗	0	INTERFACES 2	0	Instrum - Exclusion costs com numma gaperation (or table 200 of the of pertine of sime with a boor value of exclusion) A one if the of vision traffice definition LLA disclusion com numma applications national statistica-p22b in efit marked as DDOP (0" HQ #12 dottous close com uniming application inplinal 200 D0 mol of lifet for Hartistica and DDOP value of 0 (16)	21 Sep 2021, 03:52 AV 21 Sep 2021, 03:52 AV 21 Sep 2021, 05:12 AV
View Reports	 Brand HQ B Brand 	2		GipabitEthernet2Branch14A GipabitEthernet2Branch2 NY GipabitEthernet2H0-B1		Hog 82 Activate class: come naming application in the lat 2020.01m or of latter for fulfile with a 2020 Hole of 0 (66) Drawth 4.4A closed, class community application to the 2020 AC more of the for traffic with a 5020 Hole of 0 (62) Eranch 1.4A closed class community application to the 2020 DF more of parts in traffic with a 5020 Hole of 0 (82)	21 Sep 2021, 06:12 AA 21 Sep 2021, 06:12 AA 21 Sep 2021, 06:12 AA
View Schedule	 Ho-8 	1		OlgebitEthernet2H0-82 GigebitEthernet2H0-82 GigebitEthernet2H0-81		High R2 dotated actions comminancing application right via 2018.00 million sof stifter for traffic with a USSRP values of 40 (FF) High R2 dotated actions comminancing application right via 2008.00 million of pitter for traffic with a DSRP values of 34 (AF41) High R2 dotated actions comminancing application right via 2008.00 million of pitter for traffic with a DSRP value of 64 (FT)	21 Sep 2021, 04:03 AM 21 Sep 2021, 04:03 AM 21 Sep 2021, 04:03 AM
3. LiveNA				GipsbitEthernet3H0-82 GipsbitEthernet4(Bratch1-LA		HiG-82 delosed citoso com running application rip had volce video traffic with 200.00 ms mar (Ber HiG-82 delosed citoso com running application rip had 200.00 ms of (Her ter traffic with a DSCP value of 34 (APAT)	21 Sep 2021, 04:03 AN 21 Sep 2021, 04:03 AN 21 Sep 2021, 04:03 AN
[#] Configure				 GigabitEthemat4Branch2-WY 		One 1% of Vice Italia for IHQ 24 debut case com unmarg application operandroli in rist market as DEPS FF Banchi-LA debut clicks com unmarg application to had 200.20 ms of PIHH for traffic with a DECP Visite of 24 (APR1) Banchi-LA debut clicks com unmarg application to had 200.20 ms of PIHH for traffic with a DECP visite of 24 (APR1) Banchi-LA debut clicks com unmarg application to had 200.20 ms of PIHH for traffic with a DECP visite of 24 (APR1)	21 Sep 2021, 04.02 AN 21 Sep 2021, 04.02 AN
						Branch14.A ddout cisco.com nunning application rtp had voice/ octor traffic with 202.00 ms max jitter Over 1% of Voice traffic for Branch2NV/dcout cisco.com running application sig is not marked as DBCP EF.	21 Sep 2021, 04/02 AN 23 Jul 2021, 02/37 AM

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

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 \vee	Bit Rate ~
Time Zone 🗹 DS	т	Interfaces	Business Hours
(GMT-05:00) America/New York		All WAN Interfaces \checkmark	All Hours ~
Time Range		Flex Search 🔞	Cannot be used with All Device Bin Duration
Last Hour V		Ex.: site=Honolulu & wan & flow.app=http 🔹 🗙	Auto
Flex Search 😡	-	Display Filter	5 minute
Ex.: site=Honolulu & wan & flow.app=http ×		No Display Filtering	Long Term Store 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 🗸		Select Direction V	Bin Duration option to 1 Minute (slower).
Sharing Settings		Inbound and Outbound Separated	
Email X		Inbound	
Enter an email address or AD entity		Inbound and Outbound Combined	
File Format			1
PDF Row Limits			
All Rows 🗸			



6. Click **Execute**.

≡ Live∧c	tion" 💌													
fiew Reports												View Sched	lule Cre	eate Report
Templates	Reports History													
Q application		Application						Vie	w Options 👻	Share	Download	Schedule	Сору	Clos
efault Templates		Your reference	e information for this report Applica	ation (Flow)										1
orite Applications	0	Device: AI WAN	Devices Interface: All WAN Interfaces D	Naslay Filter: No Display Filtering Direction: Ou	hourd Flow Type: David Flow Exec	ution Type: Time Series Sort By: Bit Rete	Bin Duration: Auto Start Time: Jul 23, 2021 13:2	28-13 EDT (0M7-04-00) End Time: Jul 23-202	21 14:28:13 EDT (0	(T-04:00) Bin I	sterval: 5 minutes			
ple Fastlane Applica	ations 🚯											_		
plication Vs. Networ	rk Performance 🛛 🚯											ica sip		-
lication Service Pro	ovider Performan 🚯											and the second s	ina	
(AN Application Se	ervloe Provider Per	0 State										bittorrent ospf oitrix		
(AN Application V)	s. Network Perfor.	-H										bittorrent-	networking	
	Network Performa											Total		
N Application Vs. N	Network Performa	13.33	12:35 13:40	13:45	13:50 13:55	14.00	1405 1410	14:15	14:20	1	425 1	Total 4:28		
N Application Vs. N	-	13.33		13.45	13:50 13:55	14.00	1405 1410	14.15	14:20	1 Q. Sear		Total		Ξ
Application Vs. N	-	13.33 < < Page 1		13:45 Total Flows 🔿	13:50 13:55 Tocal Bytes 🔿	1400 Total Packets 🔿	14:05 14:10 Average Bit Rate 🔿	14:15 Average Packet Rate 🔿			ch	Total		
Application Vs. N	-	13.33 < < Page 1]/2 >>		Total Bytes 🔿			Average Packet Rate 🔿		Q Sear	ch	428 Peak Packet R		
Application Vs. N	-	13.33 < < Page 1	/2 >> Application ♦	Total Flows 🔿	Total Bytes 🔿 21.75 MB	Total Packets 🔾	Average Bit Rate 🔿	Average Packet Rate 🔿	P	Q Sear	ch	428 Peak Packet R		32
Application Vs. N	-	13.33 < < Page 1	/2 >> Application ⊖ thp audio ica stp	Total Flows () 51 214 71	Total Bytes 0 21.75 MB 4.47 MB 1.60 MB	Total Packets () 108,737 66,917 10,987	Average Bit Rate () 46.33 Kbps 9.92 Kbps 3.56 Kbps	Average Packet Rate 🔿	90.20 pps 18.59 pps 3.05 pps	Q Sear	51.98 Kbps 11.16 Kbps 4.14 Kbps	Peak Packet R		32 20 4
N Application Vs. N	-	13.33 < < Page 1	/2 >> Application () rtp audio ica sip ftp	Tetal Flows () 55 216 71 116	Total Bytes () 21.75 MB 4.47 MB 1.60 MB 1.07 MB	Total Packets 108,737 66,917 10,887 26,737	Average Bit Rate () 46.33 Kbps 9.92 Kbps 3.56 Kbps 2.38 Kbps	Average Packet Rate 🔿	F 30.20 pps 18.59 pps 3.05 pps 7.43 pps	Q Sear	51.98 Kbp 11.16 Kbp 4.14 Kbp 2.63 Kbp	Peak Packet R		32 20 4 8
N Application Vs. N	-	13.33 < < Page 1	/2 > > Application ⊕ rtp-audio ice sip ftp conferencing	Total Flows () 51 216 71 111 43	Total Bytes ○ 21.75 MB 4.47 MB 1.60 MB 1.07 MB 788.04 KB	Total Packets 0 108,737 66,917 10,957 28,737 9,079	Avenage Bit Rate () 48.33 Klops 9.92 Klops 3.56 Klops 2.38 Klops 1.35 Klops 1.75 Klops	Average Packet Rate 🔿	90.20 pps 18.59 pps 3.05 pps 7.43 pps 2.52 pps	Q Sear	ch 51.98 Kbpr 11.16 Kbpr 4.14 Kbpr 2.63 Kbpr 2.51 Kbpr	Peak Packet R		32 20 4 8 3
Application Vs. N	-	13.33 < < Page 1	/2 >> Application O rtp-audio ice sip ftp conferencing bittoreent	Tetal Flows () 51 214 71 116 45 45 1,744	Total Bytes () 21.75 MB 4.47 MB 1.60 MB 1.07 MB 788.04 KB 163.29 KB	Total Packets () 108,737 66,917 10,987 26,737 9,079 2,131	Average Bit Rate () 48.33 Kbps 9.52 Kbps 2.38 Kbps 2.38 Kbps 1.75 Kbps 0.36 Kbps 0.36 Kbps	Average Packet Rate 🔿	90.20 pps 30.20 pps 3.05 pps 3.05 pps 2.52 pps 0.59 pps	Q Sear	ch 51.98 Kbpr 11.16 Kbpr 4.14 Kbpr 2.63 Kbpr 2.51 Kbpr 384 bpr	Peak Packet R		32 20 4 8 3 0
N Application Vs. N	-	13.33 < < Page 1	/2 >> Application ⊖ ripraudio ka sip fip conferencing biblioment copf	Total Flows () 55 214 71 71 114 43 1744 200	Total Bytes () 21 75 MB 4 47 MB 1 60 MB 1 107 MB 788,04 KB 1 82,9 KB 1 30,56 KB	Total Packets 0 108,737 10,837 28,737 9,079 2,131 1,612	Average Dt Rate () 48.33 Klops 9.92 Klops 3.56 Klops 2.38 Klops 1.75 Klops 0.39 Klops 0.39 Klops 0.29 Klops 0.29 Klops	Average Packet Rate 🔿	7.43 pps 0.59 pps 2.52 pps 0.59 pps 0.59 pps 0.45 pps	Q Sear	ch 51.98 Kbpr 11.16 Kbpr 4.14 Kbpr 2.63 Kbpr 2.51 Kbpr 384 bpr 328 bpr	Peak Packet R		32 20 4 8 3 0 0
N Application Vs. N	-	13.33 < < Page 1	/2 >> Application O rtp-audio ice sip ftp conferencing bittoreent	Tetal Flows () 51 214 71 116 45 45 1,744	Total Bytes ⊖ 21.75 MB 4.47 MD 1.00 MB 9.107 MB 788.04 KB 193.05 KR 88.05 KB	Total Packets () 108,737 66,917 10,987 26,737 9,079 2,131	Average Bit Rate () 48.33 Kbps 9.52 Kbps 2.38 Kbps 2.38 Kbps 1.75 Kbps 0.36 Kbps 0.36 Kbps	Average Packet Rate 🔿	90.20 pps 30.20 pps 3.05 pps 3.05 pps 2.52 pps 0.59 pps	Q Sear	ch 51.98 Kbpr 11.16 Kbpr 4.14 Kbpr 2.63 Kbpr 2.51 Kbpr 384 bpr	Peak Packet R		32 20 4 8 3 0

Figure 162

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

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

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

Run a Top Talkers Report

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

	New Feature	es! 🔺 3 I	0 • 0	🌲 0	{} ▼	9 -	Ø	💄 admin 🔫
						View Sched	lule	Create Report
		View Options ~	Share	Dow	nload	Schedule	Сору	Close
1 23, 2021 13:2	8:13 EDT (GMT-04:00) End Time: Ju	ul 23, 2021 14:28:13 ED	T (GMT-04:00)	Bin Interval: 5 r	ninutes			Load Parameters
						rtp-audio ica sip ftp conferenc bittorrent ospf citrix bittorrent- netbios-di Total	networking	=
14:10	14:15	14:20	QS	14:25 earch	14:28			11
	Average Packet Rate 🛇		Peak Bit Rate	• 🗘		Peak Packet R	late 🗇	
48.33 Kbps		30.20 pps		51.	98 Kbps			32 pps
9.92 Kbps		18.59 pps		11.	16 Kbps			20 pps
3.56 Kbps		3.05 pps			14 Kbps			4 pps
2.38 Kbps		7.43 pps			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 [.] ^{IX}				New Festures 4 3 8 0 • 0 4 0	{-} * · · · ·	🛔 admin 🕶
View Reports					View Schedule C	Treate Report
Templates Reports History	RUN OR EDIT REPORT(S)				c	
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		12
Favorite Applications	Application	Top Conversations (Flow) Normal 🕤 🖀	Top Conversations	Basic Flow ~		
Apple Fastlane Applications 0	Presentation Mode	Add New Report +	Report Description	Execution Type	- rtp-oudio	=
Application Vs. Network Performance	Standard ~		Enter report description	Time Series V	sip to	-
Application Service Provider Performan	Footnote		Devices	Sort By	conferencing costs bittoment	
SDWAN Application Service Provider Per	Common to all		All WAN Devices	Bit Rate	citrix	
SDWAN Application Vs. Network Perfor					netbios-dgm Total	
WAN Application Service Provider Perfo.	Reports in View st		Interfaces	Business Hours	28	
	(GMT-05:00) America/New York		All WAN Interfaces	All Hours V Cannot be used with All Devices		1 L
	Time Range		Flex Search 😧	Bin Duration		
	Last Day 🗸		Ex.: site+Honolulu & wan & flow.app+http x	Auto 🗸	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		4 pps
				Due to the report options selected, this report will utilize the Long Term datastore (faster). To over-ride		8 pps
	Display Filter Select Display Filter		Direction Outbound	this behavior and use the Raw Flow datastore, set the Bin Duration option to 1 Minute (slower).		3 pps
	Select Display Hiter V		Uutoouno			0 pps
	Sharing Settings		Should Wait For DNS Resolution			0 pps
	Email 2		False V			2 pps 0 pps
	Enter an email address or AD entity					0 pps
			Specific to the	Report Selected		
	File Format Send PDF Send CSV					
	PDF Row Limits					
	As holds					
				Cancel Save As Template Execute		
				Encourt		

Figure 164

4. Click Execute.

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

LiveAction 💌											New Festures!	.3 .0 .0			5- <u>8</u>
Type here to filter reports.														View Schedule	Create
eports	^														Сору
Interface Bandwidth	in in										View Op	stions - Share	Download	Schedule C	Сору
Top Analysis															
IPs and Ports		information for this rep													
Address	UN D	evices Interface: ATY(A)	Enterfaces Display	Filter: No Display Filtering Direct	tion: Outbourd Row Type	Easic Flow Execution Type	: Time Series Surt By: Bit Rate	Bin Duration: Auto Blant Time: J	22, 2021 14:44:50 EDT (SMT-04:00)	End Time: Jul 23, 2021 14:44:50 EDT (SMT-64:0	 Bieleterval: 1 hour 				
Top Conversations														mpeudio	
New Report														- sip	
Source or Desenation														to conferencing	
Address Pair														bittorent	
Destination Address														citrix	
Source Address		17:00	19:00 19	100 20-00 2	00 22:00	22-00 34/22	02.00 02.00	0202 0408	06:00 06:00	07.00 09.00 09.00	1000 1100	12:00 12:00	14-00 14-44		
Destination Address	P														
-Source Address Popu	ul 💾	/a⇒≫										Q, Sea	/ch		
-Site Traffic		Application 0	т	Fotal Flows 🗘	Total Bytes (Total Packets 🗘	Average Bit R	te 🗘	Average Packet Rate 🗘	Peak	Bit Rate 🗘	Peak Par	cket Rate O	
Destination Site Traff	fi	rtp-audio			968	369.75 MB		1,853,656	34.24 Kbpe		21.45 pps	50	0.07 Kbps		
Source Site Traffic		ica			2,648	62.21 M8		820.732	5.76 Kbps		9.50 pps	10	0.09 Kbps		
Applications		sip			1,241	27.85 MB		194,189	2.58 Kbps		2.25 pps	3	1.79 Kbps		
Protocol		np			36	24.50 MB		42,190	2.28 Kbps		0.49 pps	54	L62 Kbps		
Protocol Port		ftp			1,297	12.56 MB		312,695	1.16 Kbps		3.62 pps	2	1.47 Khps		
Application Group		conferencing			409	9.20 MB		105,940	0.85 Kbps		1.23 pps	1	.84 Kbps		
Application		lanrevagent			192	3.50 MB		40,327	0.32 Kbps		0.47 pps	1	.66 Kbps		
DSCP vs Application		bittorrent			21,319	2.33 MB		26,055	0.22 Kbps		0.30 pps		360 bps		
Business Relevance		cepf			3,284	1.95 MB		24,339	0.18 Kbps		0.28 pps		288 bps		
Traffic Class		oitrix			59	1.82 MB		19,563	0.14 Kbps		0.23 pps		448 bps		
QoS	-														
Network	5.40	ions (Flow)													
Medianet	1970	evices Interface: ATT(A)	i Interfacea Display	Filter: No Display Filtering Direct	tion: Outbound Row Type	Eleaic Flow Execution Type	: Time Dories Dort By: Bit Rate	Die Duration: Auto Dhould Wait	or Dro Resolution: false - Etart Time: J	Aui 22, 2021 14:44:50 EDT (DMT04:00) End Ti	we: Jul 23, 2021 14:44 50 EDT (SMT	04:00) Bis Interval: 5 minute			
Applications (AVC)														198.19.2.88/198.1	
NSEL														108.15.2.82/198.11 198.18.133.36/198	98,19,1,101
PfR					PV-	$\sim\sim\sim\sim\sim$					<u> </u>		****	10.255.2.2/224.0.0	
Wireless					· · ·							× / × × ×		10.255.1.2/224.0.5 10.255.0.2/224.0.5 100.64.1.2/224.0.5	10.5
AnyConnect	~													198.18.133.1/198.1	18.255.255
i Anyconnecc		16:00	17:00 18:00	19:00 20:00	21:00 22	22:00	Jui 23 0100 0	200 0200 040	0 000 0000	07:00 08:00 09:00	10:00 11:00	1200 1200	14:00 14:44		
	Page 1	/\$>>				-						Q, Sea	.ch		
L	egend O	Src IP Addr O	Site O	Det IP Addr O	Dat Site O	Total Flows O	Total Bytes O	Total Packets O	Average Bit Rate O	Average Patket Rate 0	Peak Bit Rate O	Peak Packet Rate O	Sre Court		n Country O
	_	198.19.2.88	NY	198.18.128.88	HQ		82 377.90 MB	1,889,521	34.99 Kbps	21.87 pps	55.30 Kbps		34 pps		
		198.19.2.102	NY	198.18.133.35	HQ	20.1	69 58.50 MB	615.591	5.42 Kbps	7.12 pps	8.74 Kbps		11 pps		

Figure 165

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

Flow Identification

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

≡ LiveAction [.] ■			
View Reports			
Templates Reports History			
Q application			
Default Templates	Favorite Reports		
Favorite Applications	Add Report		
Apple Fastlane Applications			
Application Vs. Network Performance	Top Reports		
Application Service Provider Performan	NAME O	DESCRIPTION C	
SDWAN Application Service Provider Pe	Application	This Eloushased report up	Il 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 0	Top Conversations		I highlight for to 10 conversions based on the selected filter orderia. It will also list up to 1000 conversations.
IWAN Application Vs. Network Performa 0	Interface Bandwidth		If highlight the Top 10 interfaces' bandwidth, based on the selected fifter criteria. It will list up to 1000 interfaces.
IWAN Application Service Provider Perfo 0	DSCP		If holds to the Top 10 DSCP marking's bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
	Top Interface Bandwidths		shows a table of all the interfaces' bandwidth utilization per the specified filter.
	Top Interface Errora	This SNMP-based report	shows a table of all interface errors (CRC/Punta/Overruna, etc.) per the specified fiter.
	Top Class Bandwidths	This SNMP-based report	shows a table of all QoS class bandwidths for all interfaces per the specified filter.
	Top Class Drops	This SNMP-based report	shows a table of all QoS class drops on all interfaces per the specified filter.
	Interface Bandwidth	This SNMP-based report	graphs bandwidth utilization of a specific interface.
	Interface Utilization	This SNMP-based report	graphs the interface bandwidth utilization (by percentage) of a specific interface.
	Interface Errora	This SNMP-based report	graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.
	Post-Policy Drops	This SNMP-based report	graphs the QoS drops of all classes on a specific interface.
	Application DSCP Audit	This Flow-based report w	ill show the DSCP markings of applications organized by site, based on the selected filter criseria.
	Interface Bandwidth Summary	This Flow-based report wi	Il highlight the ingress and egress interface bandwidth, based on the selected filter oriteria. It will list up to 50 interfaces.
	NAME \$		DESCRIPTION \$
			The server of second is useful for advanced by concerning of the product of the PPCP and the product of data and the product of the product o

Figure 166

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	
Footnote			Devices	Sort By	
Enter report group description			All WAN Devices	✓ Bit Rate	
Fime Zone 🛃 DST			Interfaces	Business Hours	
(GMT-05:00) America/New York 🗸			All WAN Interfaces	V All Hours	Cannot be used with All Devic
Fime Range			Flex Search @	Bin Duration	annot be used with All Devic
Last Day 🗸			Ex.: site=Honolulu & wan & flow.app=http	× Auto	
Flex Search 🚱			Display Filter		1 h:
Ex.: site=Honolulu & wan & flow.app=http ×			No Display Filtering	Long Term Store Due to the report options select	ted this report will
Display Filter			Direction	utilize the Long Term datastore this behavior and use the Raw	e (faster). To over-ride Flow datastore, set the
Select Display Filter 🗸			Outbound	Bin Duration option to 1 Minute	e (slower).
Sharing Settings					
Enter an email address or AD entity					
ile Format					
Send PDF Send CSV					
PDF Row Limits					
All Rows 🗸					
Custom Logo 🚯					
No Custom Logo $\qquad \lor$					

Figure 167

4. Click **Execute**.

= LiveAction 🛯 🕨									• 0 🐥 111 {-} ~		
View Reports									[View Schedule Create Re	Report
Templates Reports Hist	ory	DSCP						View Options	- Share Print	Schedule Copy C	Close
Default Templates		DSCP (Flow)									1
/oice Analysis	0	Device: All WAN	Devices Interface: All WA	N Interfaces Display Filter: No Disp	lay Filtering Direction: Outbound	Flow Type: Basic Flow Execution Type	Time Series Sort By: Bit Rate Bin Duration	6 Auto Start Time: Mar 20, 2022 14:54:47 EDT (0MT-04	100) End Time: Mar 21, 2022 14:54:47 8	DT (OMT-04:00) Bin Interval: 1 hour	
WAN	0	1000								— 34 (AF41)	=
worite Applications	0	-								46 (EF) 0 (8E)	=
ple Fastiane Applications	0	e (Khps								43 (CS6) Total	
pple Fastlane Voice Analysis	0	B SOO									
IAN Capacity Planning	0	8									
te Network Performance Audit	0	0	18.00	20.00	22.00 Mar 21	02.00	04.00 05.00	08.00 10.00 11	200 14.00 14.54		
ice/Video Performance Vs. Network	0	1.4.46	12.00	20.00	12.00	02.00	0.00				
te-to-Site Traffic Utilization Audit	0								Q Search	1	
ervice Provider DSCP Audit	0	Legend O	DSCP 🗘	Total Flows 🗘	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🗘	Average Packet Rate 🛇	Peak Bit Rate 🗘	Peak Packet Rate 🗘	
ack Single Site WAN Path Changes	0	. —	34 (AF41)	6,325	5.34 GB	6,610,510	494.60 Kbps	76.51 pps	497.55 Kbps	7	76 pp
plication Vs. Network Performance	0	-	46 (EF)	21,130	2.00 GB	11,905,177	185.35 Kbps	137.79 pps	186.47 Kbps	13	138 pp
plication vs. Network Performance						(070 00)		70.29 pps	A 4 74 10		
pplication vs. Network Performance olce/Video Service Provider Performan	0		0 (BE)	84,778	845.64 MB	6,073,226	78.30 Kbps	70.29 pps	84.71 Kbps	/	73 pp

Figure 168

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

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

Bandwidth by Flow Type

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

GENERAL SETTINGS	REPORT LIST		REPORT DETAILS	
Name	DSCP (Flow)	Normal 🗈 🛍	Q Search	
DSCP	Please choose report type		* Only Time Range report types displayed	
Presentation Mode	Add New Report	+	Top Reports	
Standard \sim			Application (Flow)	
Footnote			Top Conversations (Flow)	
Enter report group description			Interface Bandwidth (Flow)	
Time Zone 🗾 DST			DSCP (Flow)	
(GMT-05:00) America/New York			Top Interface Bandwidths (SNMP)	
Time Range			Top Interface Errors (SNMP)	
Custom V			Top Class Bandwidths (SNMP)	
Start Date Start Time End Date End Time			Top Class Drops (SNMP)	
07/22/2021 15:10 07/23/2021 15:10			Interface Bandwidth (SNMP)	
			Interface Utilization (SNMP)	
Flex Search 🚱			Interface Errors (SNMP)	
Ex.: site=Honolulu & wan & flow.app=http ×			Post-Policy Drops (SNMP)	
Display Filter			Application DSCP Audit (Flow)	
Select Display Filter 🗸			Interface Bandwidth Summary (Flow)	
Sharing Settings			E LiveNA	
Email 🔆			Flow	
Enter an email address or AD entity			SNMP	
File Format			Cisco SD-WAN	
Send PDF Send CSV			Alerts	
PDF Row Limits				
All Rows 🗸				
Custom Logo 📵				
No Custom Lono V				

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

and a second														
View Reports												View Sch	Creat	le Repor
Templates Reports Histor	y Interface B	andwidth	Summary (Flow	v)										
Q By Template Name	HQ-82.dclos	d.cisco.com	n - GigabitEtherne	rt3										
Default Templates	Device: All WAS Die Interval: S		aterface: All WAN Int	arlaces Display Filter: No Die	eplay Filtering Flow Type: Basi	Flow Execution Typ	e: Time Series Sort By: Bit	t Rate – Flex Search: war	n & flow deop=EF Bin Duratio	er: Auto Start Time: Mar 20, 2	222 14:54:00 EDT (GMT-04:00) Em	Time: Mar 21, 2022 14:54:00 E	DT (GMT-04:00)	
oice Analysis	O 200												appbt[themet3/ingress	_
IAN	0												SigabitEthernet3/Egrasa	=
vorite Applications	0 (Maga	~~~~~	~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	·/////////////////////////////////////	www.www	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	······	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	······	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~		
pole Fastiane Applications		~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	m		
pie Fastlane Voice Analysis	0													
W Capacity Planning	0 0	16:00	185	10 20:00	22.00	Mar 21	02:00	04.00	06-00 08:00	10:00	12:00 1	4.00 14.54		
e Network Performance Audit	0	16:00	185	10 20:00	22.00	Mar 21	0200	04:00	06:00 08:00	10:00		4.00 14.54		
ce/Video Performance Vs. Network	0										Q Search			11
to-Sile Traffic Utilization Audit	O Legend O	Site 🗘	Device O	Interface Name O	Service Provider ©	Direction C	Total Flows 0	Total Bytes O	Total Packets 🗘	Average Bit Rate C	Average Packet Rate 🗘	Peak Bit Rate O	Peak Packet Rate	0
vice Provider DSCP Audit	0	HQ	HQ-82	GigabitEthernet3	SP1_MPLS	Ingress	12,109	1.54 GB	8,674,402	143.05 Kbps	100.40 pp	158.54 Kbps		111 p
ck Single Site WAN Path Changes	0	HQ	HQ-82	GigabitEthernet3	SP1_MPLS	Egress	10,506	999.35 MB	5,943,328	92.53 Kbps	68.79 pp	s 102.72 Kbps		76 p
slication Vs. Network Performance	0													
ce/Video Service Provider Performan	0		o.com - GigabitEti											
plication Service Provider Performan	O Bin Interval: 5		sterface: All WAN Inte	erfaces Display Filter: No Dis	aplay Filtering Flow Type: Basis	Flow Execution Typ	e: Time Series Sort By: Bit	t Race – Flex Search: war	a flow deep+EF Bis Durwtie	ec. Auto Start Time: Mar 20, 2	222 14 54:00 EDT (0MT-04:00) En	Time: Mar 21, 2022 14:54:00 E	00 20-TMD) TO	
WAN Application Service Provider Pe	O 150 -											- Ratel	-LA/GigabitEthernet4/Ep	
WAN Application Vs. Network Perfor	0											- Branch	-LA/GigabitEthernet&/in	gr. =
WAN Voice/Video Performance Vs. N	0 14x 100 ¥	Monor	WANN MA	Arabamana	some source was	AMOUNTANA	ware ware and	Massar Martin	man manage	Annanannan	Mar warden and	Voovoox		
VAN Voice/Video Service Provider P.	0 50													
AN Application Vs. Network Performa	60													
W Application Service Provider Perfo	0	10.00	181	10 20'00	22.90	War 21	02.00	84.90	06.00 08.00	10:00	12.00 1			
		10.00	183	10. 20.00	22,90	Mar 21	62.00	64300	0630 0830	1000	1230	4.00 1.4.54		
											Q, Search			-
N Voice/Video Performance Vs. Net.	0								Total Packets C	Average Bit Rate C	Average Packet Rate C	0.000000		
W Voice/Video Performance Vs. Net.	O Legend 0	Site 🗘	Device 0	Interface Name O	Service Provider O	Direction Q	Total Flows O	Total Bytes 🗘	Total Packets		Average Facket hate -	Peak Bit Rate 🗘	Peak Packet Rate	0
AN Voice/Video Performance Vs. Net. AN Voice/Video Service Provider Perf.	and a second second	Site O	Device O Branch1-LA	Interface Name O GigabitEthernet4	Service Provider 0 SP1_MPLS	Direction C Egress	Total Flows 0 10,683			92.85 Kbps	Average Packet hate 5		Peak Packet Rate	₽ C. 74 p

Figure 170

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

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

^{4/8/2022} Lab 7.3: Create a Custom Report

This Lab uses the WebUI.

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.

SENERAL SETTINGS	REPORT LIST		REPORT DETAILS	
lame	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
ootnote		1	Devices	Sort By
Enter report group description			HQ-B2	V Bit Rate
ime Zone 🗸 DST			Interfaces	Business Hours
(GMT-05:00) America/New York			All Interfaces	All Hours
ime Range			Flex Search 👔	Bin Duration
Custom v			wan & flow.dscp=BE	× Auto
Start Date Start Time End Date End Time			et l. etc.	1 mi
			Display Filter	Raw Flow Data
07/23/2021 15:29 07/23/2021 15:44			No Display Filtering	Due to the options selected, this report will utilize th
			Direction	Raw Flow datastore (slower).
lex Search 🔞			Inbound and Outbound Combined	
Ex.: site=Honolulu & wan & flow.app=http ×		1	Inbound and Outbound Combined	
			Should Wait For DNS Resolution	
Display Filter			False	
Select Display Filter 🗸				
Sharing Settings				
imail 🔀				
Enter an email address or AD entity				
ile Format				
Send PDF Send CSV				
PDF Row Limits				
All Rows 🗸				
Custom Logo 📵				
No Oustan Lana				



ew Reports																	View Sched	dule Ore	ata Repo
Templatee Reports History																			
Q By Template Name	IPs and Por	rts, Last Fifteen Mir	nutes											Viaw	Optiona - Share	Download	Schedule	Сору	Cla
fault Templates	IPs and Ports	s (Flow)																	
ce Analysis 0	Device H2-92	Interface: All Interfaces	Display Filter: No C	agies Filtering Dire	tion. Introduction	Continued Revel	oper Danis Flow	cution Type: Time Dari	ies - Gent By: Dit For	te - Flex Dearch man & Flow days	-95 Bin Duration Auto	Droubl Wait For Dro Repolut	en false - Start Time Jul 23	2, 2021 15:29:00 52T (SMT04:00)	End Time: Jul 20, 2021 15-64	a (20.497.00) TG2 0	is letterval: 1 minut	-	
	30																	102/108/10.133.36	TOP
rhe Applications 0																		02/108.10.123.82/1 102/108.18.133.36	
e Fastiane Applications 0	10		and the second se			Concession of the local division of the loca		and in case of the local division of the loc								-	Mag 192.19.23	93.26/109.19.2.102 (82/109.18.128.82/1	109/-
Feetlene Voice Anelysis 0	1																· 198.18.10	33.56/108.19.1.101 23.56/108.19.2.102	TCP.
Cepecity Planning 0	2 1																amon (88,10.2)	22.26/198.19.1.131 82/198.18.129.82/1	TOP/.
																	#### 192.19.2.* Total	102/108.16.122.36	
envork Performance Audit																			
Verwork Performance Audit 0 eVideo Performance Ve. Network 0	0	15.31	3	15.92	19.28	1524	15,35		12.26	19.87	15.28	1528	1540	1041. 104	2 1943	13.4			
	0 1920 < (Page 1			15.82	1920	1524	15,35		12.26	15.27	15.39	1539	15,42	1541 154	2 1543 Q Se				1
Video Performance Ve. Network 0 Gite Treffic Ublication Audit 0	< C Page 1]/4.5.9													Q, 50	arth		Sito User Name	
Video Performance Vs. Network 0 dite Treffic Utilization Audit 0 e Provider DSCP Audit 0		/4 >> She IP Addr 0	She She C	Sto Port 🗘	Det IP Addr C	Det Ste C	Dat Port 0	Protocol C	DSCP 0	Application Q	Total Flows 0	Total Byres 0	Total Packeta 0	Average Bit Rate C	Q So Average Packet Rate C	Peak Bit I		Sro User Name Dot User Name	
Video Performance Va. Network 0 othe Traffic Utilization Audit 0 e Provider DSCP Audit 0 Single Ste WAN Path Charges 0	< C Page 1	/4 > > Sec IP Addr 0 198.10.2.102	Sho She C NY	Sto Port 0 4218	Det IP Add: 0 198.18.133.36	Det Ste 0 HQ	Dat Port © 1494	Protocol © TCP	DSCP 0 0 (BE)	Application ©		Total Bytes 0 527.85 KB	Total Packets 0 4930	Average Bit Rate 0 4.69 Kbp	Q, So Average Packet Rate C	Peek Bit I	Refer C	Dot Uper Name	
VUldeo Performance Ve, Network 0 NOSe Traffic Usitzetion Audit 0 e Provider DSCP Audit 0 Single She WARD Path Changes 0 ation Ve, Network Performance 0	< C Page 1	/4 >> She IP Addr 0	She She C	Sto Port 🗘	Det IP Addr C	Det Ste C	Dat Port 0	Protocol C	DSCP 0	Application Q	Total Rows 0	Total Bytes 0 527.85 KB 390.31 KB	Total Packeta 0	Average Bit Rate C 4.69 Kbp 2.94 Kbp	Q, So Average Packet Rate C	Peek Bit 1 148 pps 119 pps	Refe C C C C C C C C C C C C C C C C C C	Dot User Name Sro IP Addr	
VVdeo Performance Vs. Network O O O O O O O O O O O O O O O O O O O	< C Page 1	74 55 Sec IP Addr 0 108.10.2.102 198.19.2.82	She She C NV NV	Sto Port 0 4218 5060	Det IP Addr 0 198 18.133.36 198.18.128.82	Det Site C HQ HQ	Det Port 0 1494 3970	Protocol C TCP TCP	0 (BE) 0 (BE)	Application © Ica ap	Total Rows 0 13 14	Total Bytes C 527.85 KB 330.31 KB 230.51 KB	Total Packets () 4920 1.972	Average Bit Rate C 4.69 Kbp 2.94 Kbp 2.05 Kbp	Q Sa Average Packet Rate C	Peek Bit 1 148 ppe 19 pps 10 pps	Refe C 3.79 KG 3.30 KG 2.51 KG	Dot User Name Sro IP Addr Sro Sta	
Ander Perfamance Vr. Natural - 0 altra Talfic Utilization Audit 0 altra Talfic Utilization Audit 0 Single Stark UKAN Path Charges 0 Single Stark UKAN Path Charges 0 Under Service Provider Performance 0 caton Service Provider Performance 0	< (Page 1 Legend 0	74 >> Src IP Addr 0 198.19.2.102 198.19.2.82 198.19.2.102	Src Ster C NY NY NY	Sto Port 0 4218 5060 1494	Det IP Addr 0 198.18.133.36 198.18.128.82 198.18.133.36	Det Ste C HQ HQ HQ	Dat Port 0 1494 3970 4218	Protocol C TCP TCP TCP	0 (BE) 0 (BE) 0 (BE)	Application © los sp los	Total Flows C 13 14 13	Total Bytes © 527.85 KB 330.31 KB 230.51 KB 197.20 KB	Total Packata () 4920 1.972 3.249	Average Brt Rate © 4.69 Kbp 2.94 Kbp 2.05 Kbp 1.75 Kbp	Q Se Average Packet Rate C	Peek Bit 1 148 ppe 119 ppe 161 ppe 148 ppe	Rese C 5.79 Ko 2.30 Ko 2.51 Ko 2.16 Ko 2.16 Ko	Dot User Name Sro IP Addr Sro Sita Sro Port	
Video Perfimmance VN, Netsols 0 HSIN Traffic UNItation Audit 0 HSIN Traffic UNItation Audit 0 HSIN Traffic UNITATION AUDIT 0 HSIN TRAFFIC Provide Performance 0 HSIN Traffic UNITATION Provide Performance 0 Napplication Service Photolet Performance 0	< (Pege 1 Legend 0	/4 >> Siro IP Addr C 198.19.2.102 198.19.2.82 198.19.2.102 198.18.133.36	Src Ster C NY NY NY HQ	Sto Port © 4218 5060 1494 1494	Dat IP Addr C 198.18.133.36 198.18.128.82 198.18.133.36 198.19.2.102	Det Site C HQ HQ HQ NY	Det Port 0 1494 3970 4218 4218	Protocol C TCP TCP TCP TCP	060P 0 0 (86) 0 (86) 0 (86) 0 (86) 0 (86)	Application ica sp ica ica	Totel Flows © 13 14 13 13	Total Вузек © 527.65 КВ 390.31 КВ 290.51 КВ 197.20 КВ 183.07 КВ	Total Packets © 4930 1,972 3,249 4930	Average Bit Rate © 4.69 Kbp 2.94 Kbp 2.05 Kbp 1.75 Kbp 1.63 Kbp	Q Se Average Pedet Rate C	Peek Bit 1 148 ppe 119 ppe 161 ppe 148 ppe	Refe C 5.79 K5 3.30 K5 2.51 K5 2.16 K5 2.57 K5 1.41 K5	Dot User Name Sro IP Addr Sro Sita Sro Port Dat IP Addr	
Video Performances VN, Network U des Treffer Multication Audit des Treffer Multication Audit Dargie State WAR Performance Video Service Provider Performance Video Service Provider Performance Application Service Provider Performance NApplication Service Provider Performance	< (Page 1 Legend C	/4 >> Sirc IP Addr C 198.19.2.102 198.19.2.102 198.19.2.102 198.18.133.36 198.19.2.82	Site Site C NY NY NY HQ NY	Sto Port © 4218 5060 1494 1494 3970	Dat IP Addr C 198.18.133.36 198.18.128.82 198.18.133.36 198.19.2.102 198.18.128.82	Det Site C HQ HQ HQ NY HQ	Dat Port 0 1494 3970 4218 4218 4218 5060	Protocol C TCP TCP TCP TCP TCP TCP	COCP 0 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE)	Application loa sp loa ica conferencing	Total Flows 0 13 14 13 13 13	Total Вуне © 527 к5 к8 390.31 К8 290.51 К8 197.20 К8 183.07 К8 141.60 К8	Total Packets © 4920 1,972 3249 4930 2,111	Average Bit Rate C 4.69 Kbp 2.04 Kbp 1.73 Kbp 1.63 Kbp 1.25 Kbp 1.25 Kbp	Q Se	Peek Bit 1 148 ppe 19 ppe 10 ppe 148 ppe 35 ppe	Refe C 5.79 K5 3.30 K5 2.51 K5 2.16 K5 2.57 K5 1.41 K5	Dot User Name Sro IP Addr Sro Sita Sro Port	
Voldeo Pierfinnance VI, National VI dora Tolifol Ublaction Audit VI envolder 1021-Audit VI Struje Slav Hahl Changes VI Struje Slav Hahl Changes VI Struge Slav Pinder Pierforman. V Video Sence Pinder Pierforman. V Napitatoria VI: National Pinder Pind Napitatoria VI: National Pinder Pind Napitatoria VI: National Pinder Pind National Pinder Pinder Pinder VII. VII. VII.	C (Page 1	14 >> Sec IP Add: 0 198 19.2.102 198 19.2.102 198 19.2.102 198 18.133.36 198 18.133.36 198 18.133.36	Site She C NV NV HQ NV HQ HQ HQ HQ	Stra Port © 4218 5060 1494 1494 9970 1137 4218 21	Det IP Add: 0 198.18.132.86 198.19.128.82 198.19.128.82 198.19.2102 198.19.2102 198.19.101 198.19.2.102 198.19.101	Det Site C H2 H2 H2 H2 H2 H2 H2 H2 L4 L4	Der Port © 1494 3970 4218 4218 5060 21 1494 1137	Protocol © TCP TCP TCP TCP TCP TCP TCP TCP TCP	DBCP () 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE)	Application © loa sip loa loa conferencing fra	Total Flows © 13 14 13 13 13 10 14	Tetal Bytes 0 527.55 KB 330.31 KB 220.51 KB 197.20 KB 145.60 KB 147.60 KB 151.76 KB	Total Packets © 4 020 1 972 2 249 4 930 2 111 3 540 2 244 3 245	Average Bit Rate © 4.69 Kbp 2.04 Kbp 1.75 Kbp 1.68 Kbp 1.26 Kbp 1.27 Kbp 1.17 Kbp 1.15 Kbp	Q, tin Average Packet Rate C 3 3 3 3 4 3 4 3 4 5 4 5 5 5 5 5 5 5 5 5	Peek Bit 1 48 pps 19 pps 61 pps 38 pps 39 pps 65 pps 66 pps 66 pps 66 pps	Refe C 5.79 K0 2.51 K0 2.51 K0 2.51 K0 2.57 K0 2.57 K0 3.44 K0 1.24 K0 1.24 K0 1.29 Kbps	Dot User Name Sro IP Addr Sro Sita Sro Port Dat IP Addr	
Aldeo Performance Ve. Network 0 offer Traffic Utilization Audit 0 e Provider DSCP Audit 0 Single Stis WAN Path Charges 0	C (Page 1	74 >> Sec IP Addr C 198.19.2.102 198.19.2.82 198.19.2.102 198.18.133.36 198.18.133.36 198.18.133.36	Site She C NV NV HQ NV HQ HQ	Stra Port © 4218 5060 1494 1494 3970 1137 4218	Det IP Add: 0 198.18.128.26 198.18.128.82 198.18.128.82 198.19.2.102 198.18.128.82 198.19.1.101 198.19.2.102	Det Site C HQ HQ HQ NY HQ LA NY	Der Port © 1494 9970 4218 4218 5060 21 1494	Protocol C TCP TCP TCP TCP TCP TCP TCP TCP	DBCP () 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE) 0 (BE)	Application © ica ica ica ica conferencing fes ica	Total Flows © 13 14 13 13 10 14 14	Total Bytes © 527,85 KB 230,31 KB 230,51 KB 197,20 KB 163,07 KB 141,60 KB 131,76 KB 131,76 KB 129,80 KB 72,65 KB	Total Packets 0 4930 1,972 3,249 4930 2,111 3,540 3,294	Average Bit Rate © 4.69 Kbp 2.94 Kbp 1.75 Kbp 1.25 Kbp 1.25 Kbp 1.37 Kbp 1.37 Kbp 0.55 Kbp 0.65 Kbp	Q in Average Padvet Rate C	A48 ppa 119 ppa 10 ppa 148 ppa 148 ppa 148 ppa 148 ppa 148 ppa 149 ppa 149 ppa	Refe C 5.79 K0 2.51 K0 2.51 K0 2.51 K0 2.51 K0 2.57 K0 3.257 K0 3.2577 K0 3.25777 K0 3.25777 K0 3.25777 K0 3.25777 K0 3.25777777777777777777777777777777777777	Dot User Name Sro IP Addr Sro Sita Sro Port Dat IP Addr	

Figure 172

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

Lab 8

Lab 8: QoS

4/8/2022 Lab 8.1: QoS Marking Policy

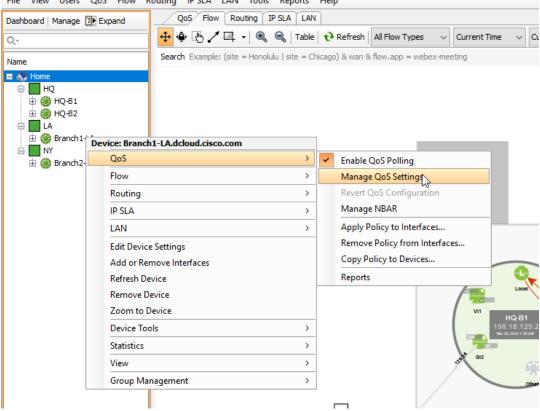
These Labs uses the Engineering Console exclusively.

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.



File View Users QoS Flow Routing IP SLA LAN Tools Reports Help

Figure 173

9. Click the Add Policy Icon.

Manage QoS Settings - Branch1	-LA.dcloud.cisco.com (198.19.1.1)	×
J 🖣 🎝 🎝 🖨 🗞 🍬		
Policies Classes Interfaces		
Policies	Mapped Classes	
R 🕨 🗟 🖦 🐜 🛸 🎭		
Add Policy	Class Name Classify Marking Queueing Policing Shaping Compression	WRED DBL Unknown
	Mapped Class Detail	
	Drop all traffic for dass	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Uns	upported
	Match on: Any Re	ference
		lass is defined by the
	cr	riteria show at left.
		latch-any: packet must eet at least one of the
		riteria to be a member of
	th	e class.
		latch-all: packet must
		eet all criteria to be a ember of the class.
	Edit	
Help	Save to Device Preview 0	CLI Close

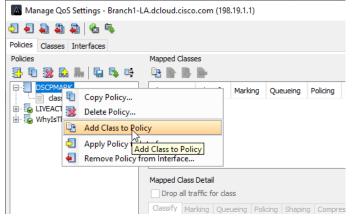
Figure 174

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

🔺 Add Policy	×		
Policy name: DSCPMARK			
ОК	Cancel		

Figure 175

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



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

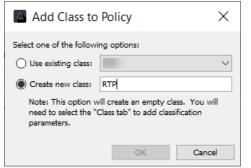
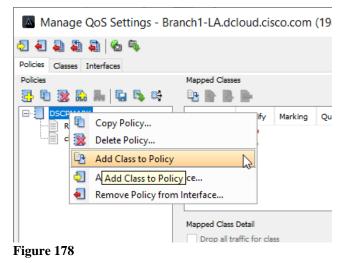


Figure 177

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



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

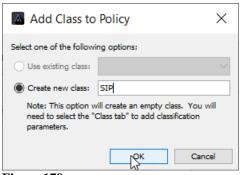


Figure 179

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

Manage QoS Settings - Bran	ich1-LA.dcloud.cisco.com (198.19.1.1)
🔄 🗐 🗿 🦓 🗿 🚱 🦠	
Policies Classes Interfaces	
Policies	Mapped Classes
	👳 🕒 🕞 🐘 🚔
DSCPMARK	Class Name Classify Marking Queueing Policing Shaping Com
RTP	RTP
dass-default	SIP 🔶
LIVEACTION-POLICY-UNIF	IED dass-default
🗄 🐻 WhyIsThisHere	
_	
	Mapped Class Detail
	Drop all traffic for class
	Classify Marking Queueing Policing Shaping Compression WRED
E! 100	

Figure 180

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

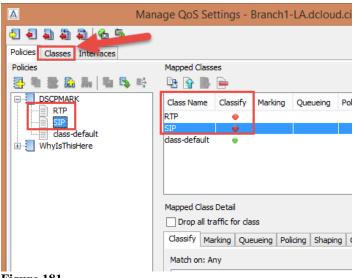


Figure 181

Select and match the SIP class...

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

🛕 Manage QoS Sett	ings - Branch1-LA.c	dcloud.cisco.com (198.19.1.1)	×
4422	🍓 🖏		
Policies Classes Inte	rfaces		
Classes	Create and Edit Mat		
LIVEACTION-CLAS	Match type:	ACL Name V Match any V 🕅	_
LIVEACTION-CLAS		BEST_EFFORT M Match T Value	
RTP SIP		CRITICAL Ma ACL Name SIPQoSMark DENY_GLOBAL_LEARN_LIST	
		LIVEACTION-ACL-AVC	
		RDP RTPQoSMark	
		SIPQoSMark	
	-	VOICE_VIDEO	
	Match/match not:	Match	
		Add Match Statement Replace Match Statement	
Help		Save to Device Preview CLI Cancel	\Box

Figure 182

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

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

🔼 Manage QoS Se	ttings - Branch1-LA.	.dcloud.cisco.com (198.19.1.1)	×
	🍪 🖏		
Policies Classes Int	terfaces		
Classes	Create and Edit Mat		
LIVEACTION-CLAS	Match type:	: ACL Name 2 Match any V	
SIP		: BEST_EFFORT CRITICAL DENY_GLOBAL_LEARN_LIST LIVEACTION-ACL-AVC RDP RTPQoSMark SIPQoSMark VOICE_VIDEO	
		Add Match Statement Replace Match Statement	
Help		Save to Device Preview CLI Cancel	

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

Manage QoS Settings - Branch1-L	A.dcloud.cisco.cor	n (198.19	9.1.1)							×
1 2 3 3 4 6 5										
Policies Classes Interfaces										
Policies	Mapped Classes									
📑 🕷 😹 🐜 🕷 🖏 🍕	🖳 🛃 📑									
	Class Name Cla	ssify M	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
SIP C	RTP		SCP: BE							
dass-default	SIP class-default	:								
LIVEACTION-POLICY-UNIFIED WhyIsThisHere										
	Mapped Class	-1]
		for class								
	Classify Marking			icing Shapir	on Compre	ession WR	ED DBI Unsi	innorted		
								erence		
	Mark with:							ferentiate	packet	s
	DSCP		~ O (E	BE)	~		be	longing to	this cla	
	🗌 Tur	nnel	42 43				Da	sed on ma	arking.	
			43				Ma	ark On		
		Loss Pric	45 arity 45					CP: mark tting the d		
			47	<u>E</u> F)	- (4		se	rvices co	de point	t (DSCP)
	Frame R	elay Disca	48 ((CS6)	_			lue in the DS) byte.	type of	service
			49				1			
								ecedence ecedence		
							pa	cket head	er.	
Help					Save to	Device	Preview C	u	C	Cancel

Figure 184

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

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

anage QoS Settings - Branch1-L	A.dcloud.cisco.com (19	98.19.1.1)					×	
📒 a a a 🕹 🐐 👘								
Policies Classes Interfaces								
Policies	Mapped Classes							
📑 🐂 🖹 🔓 🐂 🐂 👒 🗠	🖳 🔂 📑 📄							
	Class Name Classify	Marking Queueing	Policing	Shaping	Compression	WRED	DBL Unknown	
	RTP 🔶	DSCP: BE						
dass-oerault	SIP 🔶	DSCP: BE						
LIVEACTION-POLICY-UNIFIED WhyIsThisHere								
E. Wilysmishere								
	Mapped Class Dotail							
	Drop al 3 For d	lass						
	Classify Marking Qu	ueueing Policing Shap	ing Compr	ession WF	RED DBL Unsi	upported		
	Mark with:				Ref	erence		
		a (mm)					ntiate packets ng to this class	
	DSCP	✓ 0 (BE)	~	rking.				
	Tunnel	21 22 (AF23)					_	
	□ IP	23				ark On		
	ATM Cell Loss	24 (CS3) Priority 25	- 4				a packet by fferentiated	
		Discard E			se	rvices cod	e point (DSCP)	
		27 28 (AF32)				lue in the t OS) byte.	ype of service	
		28 (AF52)						
							e: sets the value in the	
					pa	cket heade	er.	
Help			Save to	Device	Preview C		Cancel	

Figure 185

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

36. Click Save to Device if satisfied.

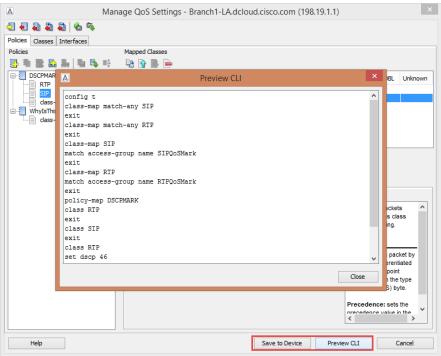


Figure 186

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

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

🛕 Manage QoS Settings - Branch1-L	A.dcloud.cisco	.com (19	8.19.1.1)							×		
5 J J J J J J K												
Policies Classes Interfaces												
Policies	Mapped Class	es										
📴 🗈 🖹 🔓 📂	9 🗈 🖪	B										
	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown		
RTP	RTP	٠	DSCP: BE							·		
dass-default	SIP	•	DSCP: BE									
E LIVEACTION-POLICY-UNIFIED	d Copy Polic	y to Devic	es			×						
🗄 🦢 WhyIsThisHere	Select a pol	icy:										
	DSCPMARK	c 🌔	3			~						
	N Select the d	levices to v	which you w	ant to save t	his policy:							
	C		,									
				(198.19.2.1)			D DBL Uns	upported				
4				. 18. 129. 24)			De					
				. 18. 129. 25) 3. 18. 129. 23)				Reference Class is defined by the				
								criteria show at left.				
								atab any	. na oko	must		
								Match-any: packet must meet at least one of the				
				5 ок		Cancel		iteria to be	e a men	nber of		
				UK		Cancer	th	e class.				
								atch-all:				
								eet all crite ember of t				
				Ed	it					.		
Help					Save to	Device	Preview (Close		

Figure 187

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

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

Copy Policy to Devices		×
Saving to devices		
Branch2-NY.dcloud.cisco.com (198.19.2.1) HQ-B1.dcloud.cisco.com (198.18.129.24) HQ-B2.dcloud.cisco.com (198.18.129.25)	 Succeeded Succeeded Succeeded 	
Export CSV	Cancel	Close
Export CSV	Carried	Ciuse

Figure 188

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

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

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

LiveNX - 35.226.145.33

nboard Manage 🔟 Exp	🕂 🕂 🖉 🖊 📮 🗸 🔍 🔍 Table 🔥 Refresh	All Flow Types	Current Time V Current Polling Interval V Current Polling Interval V Current Polling V Curr
e	Search Example: (site = Honolulu site = Chicago) & wan &	flow.app = webex-m	neeting
Home HQ HQ HQ-B1 HQ-B1 HQ-B2 LA D-M Branch1-LA		_	
GigabitEther	a+2 Enterface: Branch1-LA deloud.cisco.com - GigabitEthernet2		
VLANs	QoS 2	>	Create Policy from Template
NY	Flow	>	Adjust Input QoS
🗄 🛞 Branch2-NY	Routing	>	Adjust Output QoS
	IP SLA	>	Manage QoS Settings
	LAN	>	Revert QoS Configuration
	Edit Device Settings		Manage NBAR
	Add or Remove Interfaces		Apply Policy to Interface 3
	Refresh Device		Remove Policy from Interface
	Remove Device		Reports
	Zoom to Device		НQ-В1 198.18.129.24 ов
	Device Tools	>	221 Mar 24, 3022 3:32 PM
	Statistics	>	oft orz
	View		
			Other

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

Apply Policy to Interfaces	Х
Select a policy: DSCPMARK	~
Select the interfaces to which you want to apply this policy:	
····· · · · · · · · · · · · · · · · ·	
OK Cance	:
E'	

Figure 190

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.

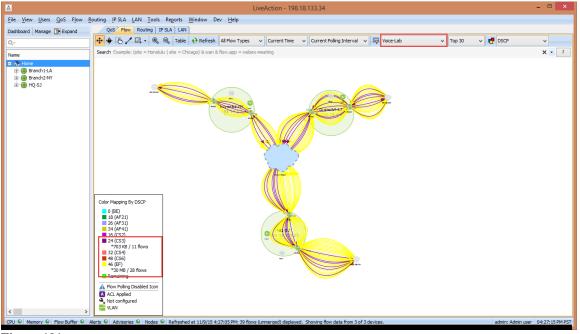


Figure 191

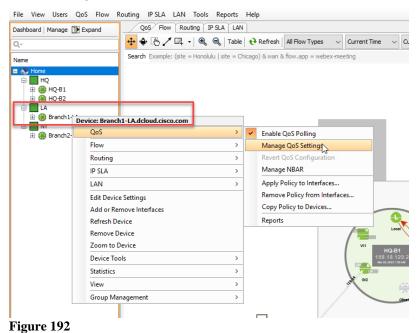
^{4/8/2022} Lab 8.2: QoS Queueing Policy

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

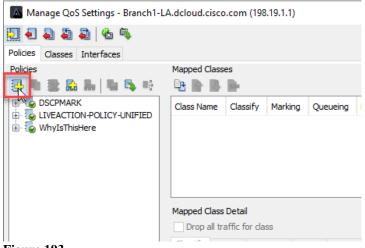
Now that you've verified your traffic is marked correctly through the network, using Netflow, you can create a queuing policy to protect the critical traffic.

Lab Steps:

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



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



50. Name the new policy QUEUEING.

Δ	Add Policy	×
Policy n	ame: QUEUING	
	OK	Cancel
Figure 1	94	

0

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

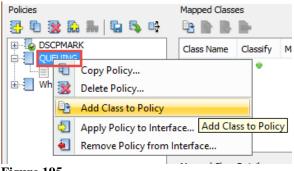


Figure 195

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

Add Class to Policy				
Select one of the follow	ving options:			
 Use existing class: 	4C_BL_CriticalData_App-Match_Mark	¥		
Oreate new class:	VOIP			
	vill create an empty class. You will need to b" to add classification parameters.			
	OK Cance			

Figure 196

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

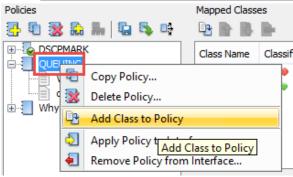


Figure 197

55. Create a new class and label it SIGNALING.

56. Click OK

Add Class to Policy					
Select one of the following options:					
O Use existing class: 4C_BL_CriticalData_App-Match_Mark	~				
Create new class: SIGNALING					
Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.					
OK Cancel					



Configure VOIP Class:

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

A Manag	ge QoS Settings - Branch1-LA.dcloud.cisco.com	n (198.19.1.1)	×
4 4 1 1 2 2			
Policies Classes			
Classes Create and Edit Mat			
🚯 🗈 😹 💦 Match trace		Match any 🗸 👯	
4C BL CriticalDat			
4C_BL_Realtime_4 Value:		M Match T Value	
4C_BL_Scavenger	45	Ma DSCP 46 (EF)	
4C-MN_CONTROL	46 (EF) 47		
4C-MN_CRITICAL	48 (CS6)		
4C-MN_REALTIME	49		
RTP	50		
SIGNALING	51 ~		
SIP	(Select up to 8 values)		
Match/match not:	Match v		
	IPv4 Only		
5	Add Match Statement Replace Match Statement		
< >			
Help	Save to Dev	ice Preview CLI	Cancel
· · · · · · · · · · · · · · · · · · ·			

Figure 199

Configure SIGNALING Class:

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

A N	Anage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
Policies Classes Interfaces		
Classes Create and E	tidit Match Statem	
4C_BL_CriticalDat 4C_BL_Realtime_A 4C_BL_Scavenger 4C-MN_CONTROL 4C-MN_CRITICAL 4C-MN_REALTIME RDP RTP SIGNALING	Match any V Match any V Value: 17 18 (AF21) M Match T Value 19 20 (AF22) 21 22 (AF23) 23 24 (CS3) (Select up to 8 values)	
VOIP Match/matc	ch not: Match v IPv4 Only	
Figure 200		

Setup VoIP Priorities:

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

A Mar	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)							×		
Policies										
Policies	Mapped Classe	S								
📴 🐂 📚 🛼 🐜 🐃 🛸 🔫	PB 📗 🔒	-								
DSCPMARK	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	VOIP			Priority: 3						
SIGNALING	SIGNALING	٠								
dass-default	class-default	•								
😟 🔄 WhyIsThisHere										
	Mapped Class [Detail								
	Drop all tra		3							
	Classify Mar		-	icing Shapir	- Comm	ession WF	RED DBL Uns	upported		
	Classify Man	king Que	Cocing Po	iong snapir	ig Compr	ession wr		upporteu		
	Queueing type: Priority V Reference									
	Distribute the available									
	Burst	t size: 32	2	bytes				nimum bar		
	Unknown	elements	:				gu	arantee to	each o	class.

Setup Signaling Priorities:

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

	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)								
Image: Second system Image: Second system Image: Second system Policies Classes Interfaces Policies Second system Image: Second system	Mapped Classes								
🛃 🕷 📚 🚵 🐜 🖏 🎭	Image: Class Name Classify Marking Oueueing Policing Shaping Compression WRED DBL Unknown								
OUEUING VOIP SIGNALING dass-default WhyIsThisHere	Class Halle Class Halle								
Help	Save to Device Preview CLI Cancel								

Figure 202

Create a Shaping Policy:

68. Click Add Policy.

친 원 위 위 위 생 책
Policies Classes Interfaces
Policies
📑 🖲 🖹 🚵 🐜 🐴 🖏 🕸
Add Policy, ^{RK} ☐ ··· ☐ QUEUING VOIP SIGNALING class-default ₩hyIsThisHere
Figure 203

69. Give the Policy a name of Shaper.

Δ	Add Policy	×
Policy name: Shaper		
	ОК	Cancel
	-	

Figure 204

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

A	Aanage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
 Policies Classes Interfaces 		
Policies	Mapped Classes	
ODSCPMARK QUEUING VOIP SIGNALING dass-default Shaper Class-default WhyIsThisHere	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unkno	wn
	Mapped Class Detail Drop all traffic for dass Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Shape using: Average Reference 3 Rate: 1500 Kbps Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate. Excess burst: 0 bits bits	^
	Unknown elements: 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	



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)	×
 Policies Classes Interfaces 		
Policies	Mapped Classes	
📑 🗓 🖹 🔝 🐜 🖷		
	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unkn	own
VOIP	VOIP Priority: 3 SIGNALING Class-bas	
SIGNA ING	dass-default	
Shaper		
ulass-default ⊕ √ WhyIsThisHere		
	Mapped Class Detail	
	Drop all traffic for dass	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Shape using: None V	
	Control the flow of traffic and eliminate bottlenecks	Â
	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	

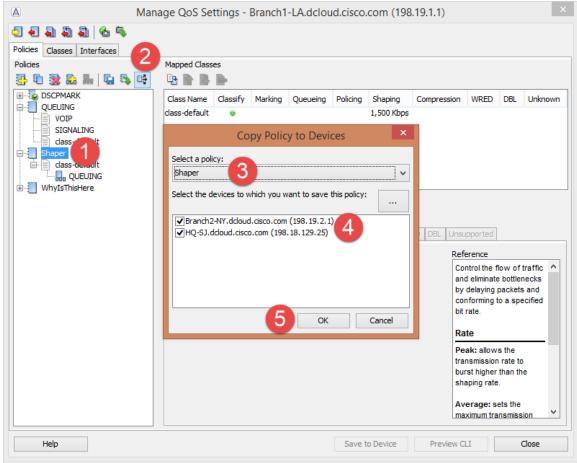
Figure 206

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

A N	Nanage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
Image: Second system Image: Second system Image: Second system Policies Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system	Mapped Classes	
DSCPMARK QUEUING VOIP SIGNALING dass-default dass-default dass-default whyIsThisHere	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL U VOIP • Priority: 3 SIGNALING • Class-bas dass-default •	Unknown
Figure 207	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shape using: None V Reference Control the flow of tree	affic A

Copy the shaping policy to the other devices:

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





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

Copy Policy to Devices	×
Saving to devices	
Branch2-NY.dcloud.cisco.com (198.19.2.1)	
HQ-B1.dcloud.cisco.com (198.18.129.24) 👳 Succeeded	
HQ-B2.dcloud.cisco.com (198.18.129.25) 👳 Succeeded	
Export CSV Cancel	Close

Figure 209

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

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

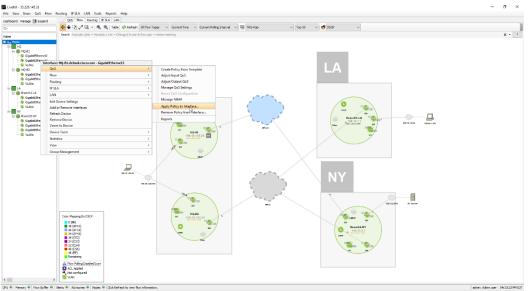


Figure 210

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

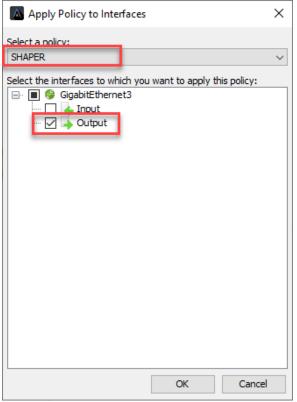


Figure 211

82. Click **OK**.

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

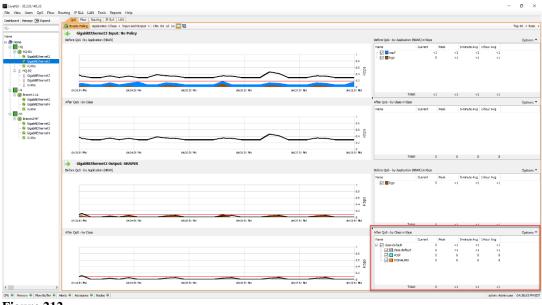


Figure 212

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

^{4/8/2022} Lab 8.3: QoS Verification

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

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

Lab Steps:

Select a device and select QoS and Manage QoS Settings.

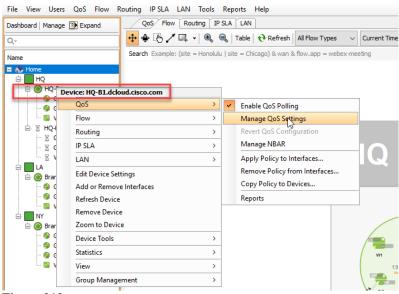


Figure 213

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

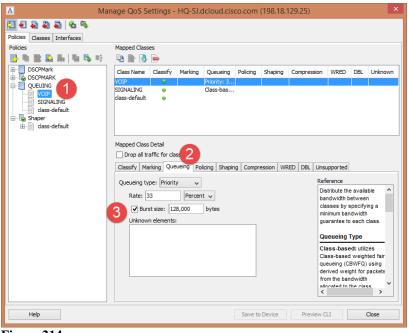


Figure 214

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

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

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

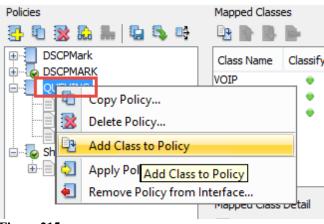


Figure 215

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

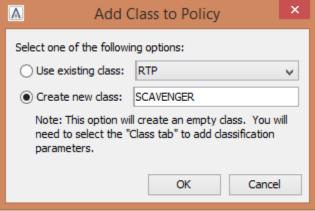


Figure 216

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

Manage QoS Settings - HQ-B1.dcloud	.cisco.com (198.18.129.24)					×
Policies Classes Interfaces						
Classes Create and Edit M	atch Statements : Protocol - using NBAR	~	Match any	~ X		
LIVEACTION-CLASS-4						
	: bitly	\uparrow	Match/M	Match Type	Value	
	bittorrent		Match	Protocol - using		
JCAVENOLK Z	bittorrent-networking		Match	Protocol - using	bittorrent-networking	
SIGNALING	blackboard-com	-				
SIP	blaze-news					
VOIP	bleacher-report					
	bl-idm					
	blizwow	Υ.				
Match/match no	: Match	\sim				
5	Add Match Statement Replace Match Statement	t				
T: 015						

Figure 217

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

M	anage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)	×
2 2 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
Policies	Mapped Classes	
DSCPMark	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unkn	own
	VOIP Priority: 3 SIGNALING Class-bas	
SIGNALING dass-default	SCAVENGER 💿 Class-bas	
	Mapped Class Detail	
	Drop all traffic for class	
	Classify Marking Queueing wincing Shaping Compression WRED DBL Unsupported	
E' 219	Queueing type: Class-based v Reference Queueing type: Class-based v Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. Queue depth: 1 Bytes v Enable Fair Queueing Guarantee to each class.	^



		trom the bandwidth allocated to the class
Help	5 Save to Dev	vice Preview CLI Cancel

Figure 219

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

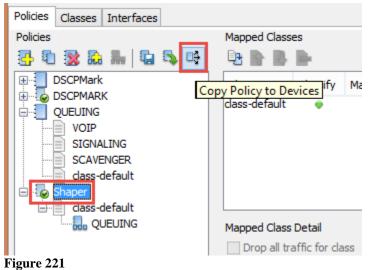
Manage QoS Settings - HQ-B1.dcloud.ci	sco.com (198.18.129.24)						×
친 🗐 🗿 🗿 🗿 🚳 👒								
Policies Classes Interfaces								
Policies	Mapped Classes							
DSCPMARK DEVENTION-POLICY-UNIFIED OUEUEING SIGNALING SCAVENCER dass-default dass-default dass-default dass-default dass-default	Class Name Classif VOIP SIGNALING SCAVENGER dass-default Mapped Class Detail Drop all traffic for d Classify Marking Qu	ass	Queueing 33% Class-base Class-base	Shaping	Compression	WRED	DBL	Unknown Class has mat
	Match on: Any		Edit			Criteria Match- meet at criteria the clas Match- meet all	a defined show at l any: pac least one to be a m	left. ket must of the mober of et must o be a
Help				Save to D	evice Pre	view CLI		Close

Figure 220

Copy the updated policy to other devices in the topology.

99. Select the **Shaper** Policy

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



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

Copy Policy to Devices	×
Select a policy: SHAPER	~
Select the devices to which you want to save this policy:	
Branch1-LA.dcloud.cisco.com (198.19.1.1) Branch2-NY.dcloud.cisco.com (198.19.2.1) HQ-B2.dcloud.cisco.com (198.18.129.25)	
ОК Са	ancel

Figure 222

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

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

Copy QoS Policy to Device Conflict	×
Conflicts were encountered when saving the policy on device HQ-B2.dcloud.cisco.com (198.18.129.25). The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?	
OUEUEING - Overwritten (A policy with the same name exists) OUEUEING - Overwritten (A policy with the same name exists) VOIP VOIP Queueing: Priority 33% Match DSCP "46 (EF)" SIGNALING VQueueing: Class-based 7% Match DSCP "24 (CS3)" SCAVENGER VQueueing: Class-based 1% Match Protocol - using NBAR "bittorrent" Match Protocol - using NBAR "bittorrent-networking" dass-default	<
View all conflicts	
Perform this action for all devices which have conflicts	
Overwrite Skip	

Figure 223

Ensure the copy is successful.

104. Click **Close**.

Copy Policy to Devices			×
Saving to devices			
Branch 1-LA.dcloud.cis	co.com (198.19.1.1) 👳 <u>Succeeded</u>	
Branch2-NY.dcloud.cis	co.com (198.19.2.1) 👳 <u>Succeeded</u>	
HQ-B2.dcloud.cisco.co	m (198.18.129.25)	Succeeded	
	Export CSV	Cancel	Close
	Export CSV	Cancel	Close

Figure 224

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



Figure 225

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

Lab A

Lab A: Appendix

^{4/8/2022} 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

519	98.18.1	33.34 -	Remo	te Desi	ktop
🔺 Liv	veActio	on - loca	alhost		
File	View	Users	QoS	Flow	Rou
	Add De	vice			
	DISCOVE	er Device	s		
	Import	Devices			H
	Export	Devices			
	Manag	e Device:	5		
	Refres	h Device:	5		
	Remov	e Networ	rk Obje	cts	
	Exit				
1					

Ā 1

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

Add Device			×
Steps	Device Connection Infor	mation	
1. Device Connection Information	Enter the SNMP connect	ion information.	
2. CLI Settings (Configuring)	Node	Local	\sim
3. CLI Settings (Monitoring)	IP Address	198.19.1.1	
4. Select Interfaces	1 /100 000		
5. Select VLANs	Non SNMP device su	uch as NetFlow probes	
6. Select Features	LiveSensor		
7. Enable Polling	Use the Default SNM	MP connection settings	Edit
8. Review Configuration	Enter SNMP connect	tion settings for this device	
9. Device Updated	SNMP Version	Version 2c	V Target Port 161
	Community String		
	< Back Next >	Finish	Cancel Help

- 4. Click Next.
- 5. Select "Use my default Configuration CLI connection settings".

×
e indicated with
d NX-OS supp

A 3

6. Click Next.

Add Device - HQ-SJ.dcloud.cise	co.com (198.18.129.25) 🛛 🗙
Steps	CLI Settings (Monitoring)
 Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Polling Review Configuration Device Updated 	Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*). Monitor-only CLI Connection Settings Enter Command Line Interface (CLI) connection settings used to monitor this device. © Use the default Monitor-only CLI connection settings © Enter connection settings for this device Connection Type 55H Port* 22 User name on Device Password on Device* Enable Password
	< Back Next > Finish Cancel Help



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

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

9. Click Continue.

atus • • • • • • • • • • • • • • • • • • •	Description Succeeded Succeeded Skipped Skipped Skipped	
0	Succeeded Skipped Skipped	
0	Skipped Skipped	
0	Skipped	
0		
0	Skipped	
~		
0	Skipped	
	Skipped	
0	Skipped	
•	Succeeded	
0	Not supported	
•	Succeeded	
•	Succeeded	
•	Succeeded	
0	Not supported	-
	• • • •	 Not supported Succeeded Succeeded Succeeded

A 5

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

Steps	Select Interface	es			
1. Device Connection Information	Select the inter	faces you want to	monitor on this de	evice (maximum 100	10 interfaces).
2. CLI Settings (Configuring)	Selected	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			
5. Select Features		Tunnel0 VoIP-Null0			PFR auto-tunnel for VRF default
7. Enable Polling		VOTH-INDIIO			
8. Review Configuration					
9. Device Updated					
	Selected inter	face(s): 3			
			. 1		
	< Back	Next >	Finish		Cancel Help

A 6

10. Click Next.

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

Steps	Select VLANs	
1. Device Connection Information	Select the VLANs you want to monitor on this device (maximum 25 VLANs).	
2. CLI Settings (Configuring)	No VLANs were found on the device. No VLANs will be managed.	
3. CLI Settings (Monitoring)	A 13	
4. Select Interfaces		
5. Select VLANs		
6. Select Features		
7. Enable Polling		
3. Review Configuration		
). Device Updated		
	< Back Next > Finish Cancel Help	

11. Click Next.

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

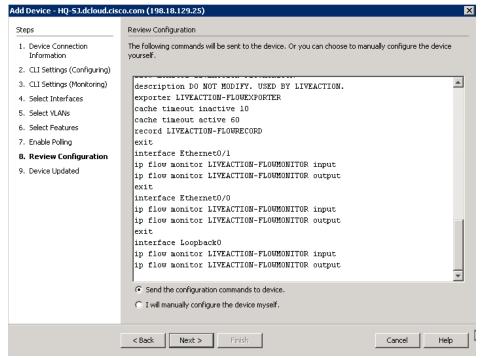
Information section. 2. CLI Settings (Configuring) 3. CLI Settings (Monitoring) 4. Select Interfaces 5. Select VLANs 6. Select Features 7. Enable Polling 8. Review Configuration Loopback0		NetFlow
 CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Mediatrace Select Features Interface Ethernet0/1 Review Configuration 	t IP Address: NBAR	<u>হ</u>
		<i>\</i> ₅

A 8

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

teps	Enable Polling
 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)	
3. CLI Settings (Monitoring)	
. Select Interfaces	
. Select VLANs	Polling Rate 30 seconds
. Select Features	Poll the following features
. Enable Polling	Poli the rollowing reacures
. Review Configuration	Flows
. Device Updated	🔽 QoS
	V IP SLA
	Routing
	LAN*
	* LAN polling occurs every 15 minutes * For SNMP v3, please see the User Guide on configuring LAN polling.
	R
	< 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.



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

17. Click Finish.

	(You may want to save the curren ost when the device is restarted):	
	Description	
	30 seconds	
	NetFlow collector	
	Enabled	
	Disabled Enabled	
	Enabled	
	Enabled	
	Enabled	
NBAR	NetFlow	
•	٠	
•	•	
•	•	

A 11

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

^{4/8/2022} 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					kto
🛕 Liv	veActio	on - loca	alhost		
File	View	Users	QoS	Flow	Ro
	Add De	vice			
	Discove	er Devrice	s		ᅡ
	Import	Devices			
	Export	Devices			
	Manage	e Device:	5		ſ
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: Specif	fy what to scan	
Specify IP r	anges (ex: 192.168.1.1-200) or one IP per line:	
198.19.1.1 198.19.2.1		
C Specify see	d device to scan	
IP Address		Hops 1 💌
Use the Def		Edit t 161



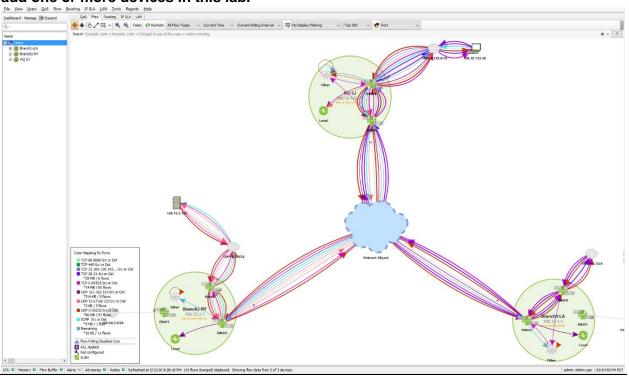
Note: In the Lab infrastructure we are utilizing the Local LiveNX Node included with the Server installation. If you require access to a Remote Node to access the subnets or addressing in "Step 1: Specify what to scan" you would use the Specify node drop-down at the bottom of this dialog box.

	*
ок	Cancel
	ОК

A 14

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

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



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

A 16

1/8/2022

6. Select Yes on the configure devices dialog.

Configur	e Devices 🛛 🗙
?	2 configurable devices added to the application. Do you want to configure Qo5, Flow, Routing, IP SLA, or LAN for the added devices?
	Yes No
A 17	

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

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

nfigure Cisco Devices		
eps	SNMP Settings	
I. SNMP Settings (LI Settings (Configuring) (LI Settings (Monitoring) Validating Devices Select Features Enable Polling Update Device Devices Configured	Enter the SNMP connection information used for monitoring the selected devices.	
	< Back Next > Finish Cancel He	lp

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

Steps	CLI Settings (Configuring)
1. SNMP Settings 2. CLI Settings (Configuring)	Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).
CLI Settings (Monitoring)	Configuration CLI Connection Settings
 Validating Devices 	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
6. Enable Polling	Use my default Configuration CLI connection settings Edit
7. Update Device	C Enter connection settings for this device
8. Devices Configured	Connection Type SSH Port* 22
	User name on Device
	Password on Device*
	Enable Password
	Also use these credentials for monitor mode,
	<i>v</i>
	< Back Next > Finish Cancel Help

10. Select Use the previous page connection settings.

iteps	CLI Settings (Monitoring)
1. SNMP Settings	Specify the CLI connection information shared by all users. This information will only be used to monitor this
2. CLI Settings (Configuring)	device. Required fields are indicated with an asterisk (*).
3. CLI Settings (Monitoring) 4. Validating Devices	Monitor-only CLI Connection Settings Enter Command Line Interface (CLI) connection settings used to monitor this device.
5. Select Features	C Use the default Monitor-only CLI connection settings Edit
5. Enable Polling	O Use the previous page connection settings
7. Update Device	C Enter connection settings for this device
Devices Configured	Connection Type SSH V Port* 22
	Password on Device*
	Enable Password

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

eps	Validating Devices				
1. SNMP Settings 2. CLI Settings (Configuring)	The following devices are being validated. validation issue occurs, click on the descrip				
3. CLI Settings (Monitoring)	Device	Status	Description		
4. Validating Devices	Branch1-LA.dcloud.cisco.com	•	Succeeded: click for details		
5. Select Features	Branch2-NY.dcloud.cisco.com	٠	Succeeded: click for details		
6. Enable Polling					
7. Update Device					
8. Devices Configured					
	Export Validation Details				
	< Back Next > Finish] 🗟	Cancel Help		

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

onfigure Cisco Devices				
Steps	Select Features			
1. SNMP Settings	Select the features you want to use on th	ne devices. Learn more	e about each feature	in the Help section.
 CLI Settings (Configuring) CLI Settings (Monitoring) Validating Devices 	Device Branch1-LA.dcloud.cisco.com Branch2-NY.dcloud.cisco.com	NBAR	NetFlow	Mediatrace
 Select Features Enable Polling Update Device Devices Configured 				
	< Back Next > Finish]	Ca	incel Help

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

nfigure Cisco Devices					
ōteps	Enable Polling				
 SNMP Settings CLI Settings (Configuring) 	Select the features you want to act each feature in the Help section.	ively monitor, ar	nd the polling rate I	or the devices	. Learn more about
3. CLI Settings (Monitoring)	Device	Poll QoS	Flow IP SLA	Routing LA	N* Interval
4. Validating Devices	Branch1-LA.dcloud.cisco.com				30 seconds 💽
5. Select Features	Branch2-NY.dcloud.cisco.com				30 seconds 🖃
6. Enable Polling					
7. Update Device					
					à
	* LAN polling occurs every 15 min * For SNMP v3, please see the Us < Back Next > Fin	er Guide on conf	iguring LAN polling		ncel 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.

teps	Update Device		
 SNMP Settings CLI Settings (Configuring) CLI Settings (Monitoring) Validating Devices 	The selected devices will be updated bas You may choose to manually configure to Warning: once update processes have be more about each feature in the Help sect	he devices. een started you will not	
5. Select Features	Device	Status	Description
. Enable Polling	Branch1-LA.dcloud.cisco.com	•	Update Required: click to view
. Update Device	Branch2-NY.dcloud.cisco.com		Update Required: click to view
	Send Updates to Devices	iend	
	C Manually Configure Devices		
	Export Update Commands		
	<back next=""> Finish</back>	1	Cancel He

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

iteps	Update Device			
 SNMP Settings 	The selected devices will be updated based You may choose to manually configure the		n changes if necessary.	
2. CLI Settings (Configuring)	You may choose to manually configure the	devices.		
. CLI Settings (Monitoring)	Warning: once update processes have beer more about each feature in the Help section		t be able to return to earlier screen	is. Learn
. Validating Devices	more about each reature in the help section			
. Select Features	Device	Status	Description	
. Enable Polling	Branch1-LA.dcloud.cisco.com		Update Successful	
. Update Device	Branch2-NY.dcloud.cisco.com	•	Update Successful	
	Send Updates to Devices Sen	d		
	C Manually Configure Devices			
	Export Update Commands			
	< Back Next > Finish		Cancel	Help

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

4. Validating Devices Branch2-NY.dcloud.cisco.com CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 5. Select Features Enable Polling 7. Update Device B. Devices Configured	×	
Steps	Devices Configured	
Steps 1. SNMP Settings 2. CLI Settings (Configuring) 3. CLI Settings (Monitoring) 4. Validating Devices 5. Select Features 6. Enable Polling 7. Update Device	The following devices have been configured. Learn Device Branch1-LA.dcloud.cisco.com	-
		igured devices have been configured. Learn more about each feature in the Help section. Device Summary deloud.cisco.com CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 deloud.cisco.com CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30
	< Back Next > Finish	Cancel Help

A 26

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

Lab A.3: Export/Import Device Configuration

Lab Steps:

1. From the File Menu select Export Devices.

	8.18.13	33.34 - F	Remot	e Desk	top (
🔥 Li	veActio	on - loca	alhost						
File	View	Users	QoS	Flow	Rou				
	Add De	evice							
	Discov	er Device	s						
	Import	Devices			F				
	Export	Dectes							
	Manag	e Device:	5						
	Refres	h Device:	5						
Refresh Devices Remove Network Objects									
	Exit								
27									

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

											Q- 1	ype here to filter result	25
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	
\checkmark	- GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000				
	- GigabitEthernet2	Interface		100.64.1.2				Internet	2,000				
\checkmark	- 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				
\checkmark	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
\checkmark	- GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000				
\checkmark	- GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000				
	- Loopback0	Interface							8,000,000				
	Null0	Interface							10,000,000				
	VoIP-Null0	Interface							10,000,000				
\checkmark	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
\checkmark	- GigabitEthernet1	Interface		198.18.129.25					1,000,000				
\checkmark	- GigabitEthernet2	Interface		10.255.0.2					1,000,000				
	- Loopback0	Interface		10.0.0.102					8,000,000				
	- NullO	Interface							10,000,000				
	VoIP-Null0	Interface							10,000,000				
\checkmark	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	НQ		
\checkmark	- 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				
					<								

A 28

3. Select Export to csv.

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

Export the co	ntent to a CSV	file			
Look in:	: 📃 Desktop		- Ø) 📂 🗄	•
Recent Items Desktop My Documents Computer	Computer Computer Computer LiveAction updateint				
	File name:	updateinterface.csv			Export
Network					

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



8. Select the file you previously exported.

🛕 Import from a	CS¥ file				×
Look in:	🧮 Desktop		•	1 📂 🖽	-
 Recent Items Desktop My Documents Computer	Ciparies Administra Computer Network LiveAction				
Network	File name:	updateinterface.csv			Import
	Files of type:	CSV files (*.csv)		•	Cancel

A 31

9. Click Add/Update Devices.

Device	pdate Devices selected for Add/Update will b	e added or u	pdated								Q-			×
dd/Upd	Name	Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K	Node	Site	Site CIDR	Data Ce.	
\checkmark	Branch1-LA.dcloud.cisco	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	LA	10.0.1.1, 198.1	Г	
2	- GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,00	0				
	- GigabitEthernet2	Interface		100.64.1.2				Internet	2,00	0				
2	- GigabitEthernet3	Interface		10.255.1.2				MPLS	1,00	0				
	- Loopback0	Interface		10.0.1.1					8,000,00	0				
	- Null0	Interface							10,000,00	0				
	VoIP-Null0	Interface							10,000,00	0				
	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		Г	
	- GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,00	0			_	
	- GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,00					
	- Loopback0	Interface							8,000,00					
	- Null0	Interface							10,000,00					
	VoIP-Null0	Interface							10,000,00					
	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ			
	GigabitEthernet1	Interface		198.18.129.25					1,000,00				_	
	- GigabitEthernet2	Interface		10.255.0.2					1,000,00					
Π	- Loopback0	Interface		10.0.0.102					8,000,00					
	NullO	Interface							10,000,00					
	VoIP-Null0	Interface							10,000,00					
	HO-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					1,000,00	0			_	
	- Loopback0	Interface		10.0.0.103					8,000,00					
	- NullO	Interface							10,000,00					
Π	VoIP-Null0	Interface							10,000,00					
									10/000/00					
					<									
								Add/Update Devices	Import from CSV		Export to (Close	

A 32

10. Click OK to use the Default SNMP settings.

		×
Node	Local	_
Ouse the Default SNM	P connection settings	Edit
C Enter SNMP connecti	ion settings for this device	
SNMP Version	Version 2c	Target Port 161
Community String		
		Ok Cancel
		v

A 33

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

^{4/8/2022} 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:

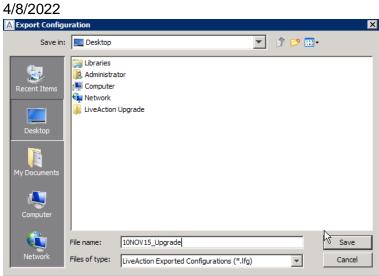
1. Open the LiveNX WebUI, select Settings.

≡ LiveAction ⁻	NX						New Features!	0 0	• 0 🐥 1	{} -	0- 0	🔺 👗 admin 🖣
Overview Enter Filter Reg	uest Here										♦ Se	tings Ju
Sites, Devices, Interfaces by Sta	atuses					Active Alerts					Sy	Settings item Diagnostics
SITES: 2		DEVICES: 4		INTERFACES: 8		ALERTS						er Management
SITES CÎ HQ LA	0	DEVICES (2) Branch1-LA HOB1 HOB2 HOMC	0	INTERACES C GigutiSthemat18/ach14.A GigutiSthemat18/0.81 GigutiSthemat19/0.82 GigutiSthemat19/0.4C GigutiSthemat19/0.4C GigutiSthemat28/0.81 GigutiSthemat29/0.82 GigutiSthemat29/0.82	0			No Active Alerts				
A 34												

2. Select Configuration.

≡ LiveAction ⁻	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	
A 35	

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



A 36

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

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.

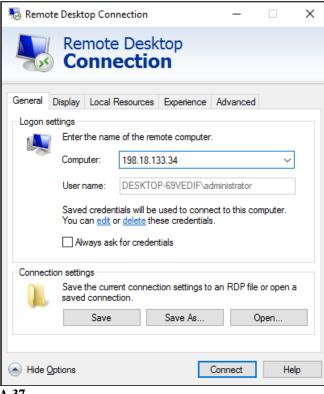
Note: Use the information from the Lab Details table to connect to the desired device.

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

Nemote Desktop Connection -		×			
Remote Desktop Connection					
General Display Local Resources Experience Advanced	I				
Display configuration					
Choose the size of your remote desktop. Drag the sway to the right to use the full screen. Small Full Screen	slider all th	e			
Use all my monitors for the remote session					
Choose the color depth of the remote session.					
Display the connection bar when I use the full screen					
Hide Options Connect	He	elp			

A 38

9. Select Connect.

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

DIAGRAM



A 39

11. Click OK.

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

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