LiveAction Training Lab Workbook Pt. 1

© Copyright 2019, 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. 2019Apr15

Table of Contents

Lab 0: S	Setup and Get Connected	. 5
	Connect to the Lab Network	
Lab 0.8:	Connecting to YOUR Training Pod	. 8
Lab 0.9:	Install the LiveNX Client	. 9
	he LiveNX Web UI	
Lab 1.1:	Explore the Web UI	11
	Create a Custom Dashboard	
Lab 1.3:	Pre-Configured Stories	17
	WebUI Reports	
Lab 1.5:	Enable / Customize Alerts	20
Lab 1.6:	Add a User Account	22
Lab 2: T	he LiveNX Client	23
	Launch the LiveNX Client	
Lab 2.2:	Explore the LiveNX Client	27
Lab 3: T	raffic Flows	29
	Discover Flows	
	Discover Specific Flows	
Lab 3.3:	Examine Specific Traffic	33
	Troubleshoot Issues	
Lab 4: F	iltering, Identifying, Marking	35
	Creating Custom Filters	
	ACL Creation	
Lab 5: C	Configuring Devices	47
	Add Device	
	Manage & Configure Devices	
	Configure Flow on Devices	
	Delete Unused Interfaces	
	Merge Clouds in Topology	
	laking the Topology Work	
	Setting Device Semantics	
	Adding Devices to Groups	
	Creating Network Objects	
	Console Dashboard & Reports	
	The Client Dashboard	
Lab 7.2:	Viewing Console Reports	79
	Create a Custom Report	
Lab 8: C	loS	83
Lab 8.1:	QoS Marking Policy	84
	QoS Queueing Policy	
	QoS Verification1	
	Appendix1	
	Add Device1	
	Client Device Discovery1	
	Export/Import Device Configuration1	
	Saving Server Configurations1	
Lab A.5:	Connect via Remote Desktop Connection1	29

IMPORTANT INFORMATION – Please Read!

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

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

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

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

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

Lab.0

Lab 0: Setup and Get Connected

Lab 0.7: Connect to the Lab Network

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

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

Local:

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

1 x Installed LiveNX Client

1 x Browser

Remote Student Pod

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

1 x LiveNX OVA Linux install

1 LiveNX Server

1 LiveNX Node (installed on LiveNX Server)





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

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

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

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

Lab Steps:

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

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

Lab 0.8: 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... similar to that below...

DIAGRAM



Lab Steps:

1. Click the URL provided in the email.

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

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

Learning Labs Menu	Lab Status :	✓ READY		Time Le	eft: 2 DAYS 17 H	OURS	
💢 Overview	Topolog	y Lab Details					
Labs Introduction	SI No	Role	Hostname	Username	Password	IP Address	Port
	1	Liveaction	livenx	admin	Student	104.196.66.177	443
Access Devices	2	B1-HQ	HQ-B1	admin	C1sco12345	104.196.66.177	20019
	3	inet1	INET1	admin	C1sco12345	104.196.66.177	20018
	4	inet2	INET2	admin	C1sco12345	104.196.66.177	20020
	5	inet3	INET3	admin	C1sco12345	104.196.66.177	2002
	6	BR1	Branch1-LA	admin	C1sco12345	104.196.66.177	2000
	7	B2-HQ	HQ-B2	admin	C1sco12345	104.196.66.177	20022
	8	MPLS1	MPLS1	admin	C1sco12345	104.196.66.177	2001
	8	MPLS2	MPLS2	admin	C1sco12345	104.196.66.177	20009
	9	BR2	Branch2-NY	admin	C1sco12345	104.196.66.177	2000
	10	wkst1	Administrator	Administrator	C1sco12345	104.196.66.177	2020
	11	Activedirectory	Administrator	Administrator	C1sco12345	104.196.66.177	20202
	12	PC1	Administrator	Administrator	C1sco12345	104.196.66.177	20203
	13	PC2	Administrator	Administrator	C1sco12345	104.196.66.177	20204

Lab 0.9: 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. http://www.liveaction.com/download/links/
 - 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.

If you DO decide to launch the Client now... you may be presented with a dialog to enter the LiveNX Server IP Address, Use the addressing from your Lab Details web page.

DIAGRAM

Server C	onfiguration X											
Server Settings												
Server:	198.18.133.34											
Port:	7000											
	Save Cancel											

Lab 1

Lab 1: The LiveNX Web UI

Lab 1.1: Explore the Web UI

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

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

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

Lab Steps:

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

LiveNX
admin
••••••
Login

The Main Dashboard 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 UX			New	eatures!	D 0	• 0	10	{}	Ģ	0 -	\$ -	💄 admir	-
Dashboa	ard 🔞								Mar 27, 201	9 12:00:00	→ Mar 27, 20	019 12:15:00	Add V	Vidget	e.
	Status			WAN			System					Alerts			+
	Filter Request Here												<	Apply filter	
E Top S	Sites by WAN Utilization	eak Inbound WAN In	terface Utilization 💙	Top WAN Applications by	y Bandwidth Ir	bound/Outbound B	andwidth 🕽	×	:: Top Interf	aces % Cha	nged - Interfa	ace Burstable	Rate	>	¢
	GigE0/1 San_Jose_DC -1. 2-NY GigE0/2 New_Yo1.			rtp voip-telephony unknown bulk-data	536.3 134.3	In Ou			Branch2-NY Branch2-NY						
	GigE0/0 San_Jose_DC -			ica unknown	51.5										
Branch	2-NY GigE0/0 New_Yo			sip signaling	43.7 I										
				citrix desktop-virtualization	10.1										
				snmp ops-admin-mgmt	9.6										
				openwebnet[unknown	6.8										
				nntp bulk-data	4.1										
				ftp file-sharing	2.7										

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

(≔ LiveAction	NX UX		New Features	▲ 0 ■ 0	• 0	4 0 {}	₽ 0 •	🌣 👻 💄 admin 🗸
A MAIN						Mar 27, 2019 12:00:00 →	Mar 27, 2019 12:15:00	Add Widget
Dashboard	=	WAN	··· 8	System		=	Alerts	+
Sites								Apply filter
Devices								
Interfaces	Peak Inbound WAN Interface Utilization 🗙	:: Top WAN Applications by I	Bandwidth Inbound/C	utbound Bandwidth	×	: Top Interfaces % Change	ed - Interface Burstable	Rate X
WAN Applications	.0 .0 0	unknown bulk-data	536.3 134.3 51.5	● In ● Out		Branch2-NY GigE0/2 Outbo Branch2-NY GigE0/2 Inbour		
Network Users	0		43.7 I 10.1 I 9.6 I 6.8 I					
A TOPOLOGY		nntp bulk-data ftp file-sharing bittorrent p2p-file-transfer	4.1 2.7 2.2 Kbps				36	
STORIES	-							
	×	:: Overall Status All			×	Top Devices Top Devices		×
	· Com	Critical	Warning	Good		Branch2-NY New_York HQ-SJ San_Jose_DC	59.0 40.0	
INSIGHT		Sites 0	0	2				
		Devices 0	0	2				
		WAN Apps 0	0	0			%	
							70	

5. Select Sites.

E LiveAct	ion	NX U						▲ 0 ■ 0 ●	0 🔔 0 {-}		
tes								Mar 27, 2019 11	:55:00 → Mar 27, 2019 12:	10:00 15 Min 🖉 Au	to Configure Sites
SITE NAME	\$	SITE STATUS	٥	IMPORTANCE	٥	DEVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION DROPS	INTERFACE ERRORS
Site Name		All	~	All	~	All v	All v		Peak Utilization Out	All ~	Interface Errors
New_York		•		Unspecified		•	•	1.09 %	15.46 %	•	0
San_Jose_DC		•		Unspecified		•	•	0.72 %	0.03 %	•	0
Unspecified				Unspecified		•	•	-		•	0

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

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

- 6. Note; Status, Utilization, Drops, Errors, etc...
- 7. Toggle the Auto Update to ON.
- 8. Change the display to Hour.
- 9. Click on the link to New_York to see additional device info.

Anytime you wish to return to a prior level, or the WebUI home, you can click the Menu icon.

10. Select Topology > Geo Topology

LiveAction Lab Workbook Pt. 1



Note: Anytime the Geo Topology is launched it defaults to filter for Status: Critical Alerts.

11. Delete Critical alerts by hovering over Critical button & click the "x", then click Apply

```
Geo Topology Status: Critical Enter Filter Request Here \Lambda Apply filter
```

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



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

My Inte	terfaces (4)		Discovered Devices	(0)			Autodisco	(2)	
							() Autodisco	overy (3)	
ces Configure	Delete				Q Sear				
					-				
♦ MODEL ♦ N	NODE 🗘 SITE	INTERFACES 🗘	POLL 🗘	QOS	\$ F	LOW	IP SLA	ROUTING	LA
✓ Model	Node Site		All 🗸	All	× .	Ali 🗸	All 🗸	Ali v	A
cisco3945 L	Local/Server San_Jose_DC	2	~	~		~			
cisco3945 L	Local/Server New_York	2	~	~		~	~	1	
	Model Cisco3945	Model Node Site cisco3945 Local/Server San_Jose_DC	Model Node Site cisco3945 Local/Server San_Jose_DC 2	✓ Model Node Site All ✓ cisco3945 Local/Server San_Jose_DC 2 ✓	✓ Model Node Site All ✓ All cisco3945 Local/Server San_Jose_DC 2 ✓ ✓	♦ MODEL ◆ NODE ◆ SITE ◆ INTERFACES ◆ POLL ◆ QOS ◆ F ✓ Model Node Site All ✓ All ✓ All ✓ I ✓ cisco3945 Local/Server San_Jose_DC 2 ✓ ✓ ✓	MODEL NODE SITE INTERFACES POLL QOS FLOW Model Node Site All All All All cisco3945 Local/Server San_Jose_DC 2 Z Z	♦ MODEL ♦ NODE ♦ SITE ♦ INTERFACES ♦ POLL ♦ QOS ♦ FLOW ♦ IPSLA ♦ • • Model Node Site • Interfaces • All • All • All • All • All • • •	Model Node Site Interfaces Poll Qos FLow IP SLA Routing Model Node Site All All All All All All All All All All All All All All All All All All All All All All All All All All </td

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

Lab 1.2: Create a Custom Dashboard

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

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

Lab Steps:

1. From the **Main>Dashboard** click on the **+** icon to create a new Dashboard.

Dashboard	0					Mar 27, 2019 12:10:00 → Mar	r 27, 2019 12:25:00 Add Wie	lget 🛃
	Status	#	WAN	11	System	=	Alerts	
2	2. Click C	ustom Dashb	ooard.					Ŭ
≡ Li	iveAction~	k UX		New Features!	▲ 0 💻 0 🔹	0 🐥 0 {-}		💄 admin 🗸
Dashboard	0					Mar 27, 2019 12:10:00 → Ma	ar 27, 2019 12:25:00 Add Wi	idget 🚽
=	Status	··· II WAN	··· 8	System	8	Alerts ii	New Tab	+
		с		e about to create a new dash get groups or create a new dasht		ridget		
	Default templates				s	nared dashboards		
	LiveNX provides insigh help users understand Using custom dashboi	ustom Dashboard istom widgets the into multiple dimensions to and monitor network behavior, ards, LiveNX users can create vs that provide them with the	This dashboard re network, monitore	Status Default widget group Number of widgets: 9 veals the overall status of the d by LiveNX	Th hid ad	u have no shared dashboards te reason for that is no one shared a de this 'Shared dashboards' list unti ided. de 'Shared dashboards' area for nov	any dashboards yet. You can I shared dashboard will be	
	This dashboard, focus service providers, and	AN Hault widget group Imber of widgets: 12 ed on WAN, indicates which sites, application groups are the most consume the most WAN	of the LiveNX depl	System Default widget group Number of widgets: 6 ovides visibility into the overall h oyment, visualizing whether the normal or needs immediate atten				
	No WM	ares fault where areas AIC or Cisco ISE juration Found. Configure areas there there? Configure areas there there		CISCO SD-WAN Performan Default works provo or Cisco SD-WAN Infiguration Found. Configure are service classes more performance leave epoyment	ice is In			

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

≡	LiveAction	NX UX			New Features!		0	• 0 🐥 0					
Dash	board ^②							Mar 27,	م دا دا بین دا د				×
::	Status	11	WAN	:	System	1		Alerts	Add widg Current das Added 1 ou	hboard: Nev			
E													Q
8									Alerts				^
										Active Alert	Count		~
									Availability Availab				~
									Application	s			
											formance Su erformance S		
									Address	00, 1100011			
									Source	Address			\sim
				,					Destina	tion Addres	s		~
			• •	72					Source	or Destinati	on Address		^
									Average				
			Drop widge	ts here						e Outbound	Outbound Co	mbined	
			5.0p								outbound co	Jinbined	
									Site Tra				~
									Source	Site Traffic			~
									Destina	tion Site Tra	iffic		\sim
									:: Bidirect	ional Source	e/ Destinatio	n Pair	
									Network				
									Source	Network			\sim
									Destina	tion Networ	k		~
									:: Average	e Inbound			
									:: Average	Outbound			
									:: Average	e Inbound &	Outbound Se	eparated	
									Source	or Destinati	on Network		~ ,
									🗔 Create N	lew Widget			

3. Drag-and-drop, or click + to add Widgets to YOUR Custom Dashboard.

Note: For the purposes of this Lab you may choose any combination of widgets to add to YOUR Custom Dashboard. You can add up to 12 widgets on a single Dashboard.

- 4. Delete un-wanted Widgets by clicking the Trash icons.
- 5. Select the **New Tab** text and rename your Dashboard.

Dashboard	- ⁻						Mar 27, 2019	9 12:15:00 → Mar 27, 2	019 12:30:00 Add Widget	2	
	Status	··· 8	WAN	··· 8	System	=	Alerts		New Tab)	+

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

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

Lab 1.3: Pre-Configured Stories

The LiveNX WebUI has a number of 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: 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.

3. Select Inbound.





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

Site To Site Analysis > Internet - New_York		$<\ {\rm Mar}\ 27,2019\ 12:25:00\ \rightarrow\ {\rm Mar}\ 27,2019\ 12:40:00\ >\ 15\ {\rm Min}$	✓ 🖉 Auto
Switch Direction Enter Filter Request Here		Apply filter IWAN CONTROL FILTER Off Flow	Details
APPLICATION Top 10 V	DSCP All	SERVICE PROVIDER	STATUS
= bittorrent = http ica	0 (BE)	MPLS	N/A
rtp	= 46 (EF)		
www-http			

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

Lab 1.4: WebUI Reports

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

Lab Steps:

- 1. Click the Menu icon.
- 2. Select Reports, and View Reports.

View Reports			View Schedule Create Re		
Templates Reports His	story		Table Tile		
Q By Template Name					
/ly Templates	Default Templates		0		
folce - Interface Bandwi Private		IWAN	Favorite Applications		
Default Templates	This group of reports is useful for understanding enterprise-wid QoS performance for VoIP. It includes DSCP marking validation per site, QoS performance information, and Voice/Video	 This group of reports provides rapid understanding of Cisco IWAN performance and utilization. It includes an understanding of which service provider a specific class of traffic is utilizing, 	This report template provides an understanding of the applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic class, and business		
Voice Analysis	 performance data (jitter and packet loss), based on the Cisco Performance Monitor. 	delay/loss/jitter measurements by traffic class, and corrected vs. uncorrected events.	relevance.		
WAN	0				
Favorite Applications	Apple Fastlane Applications	Apple Fastlane Voice Analysis	WAN Interface Capacity		
Apple Fastlane Applications	This report template provides an understanding of the Apple	This group of reports is useful for understanding enterprise-wide	This report template provides visibility into the performance of a		
Apple Fastlane Voice Analysis	Fastlane applications seen at a specific site, their performance	Apple Fastlane QoS performance for VoIP. It includes DSCP	WAN interface. It includes interface bandwidth, interface		
WAN Interface Capacity	 (based on the Cisco Performance Monitor), traffic class, and business relevance. 	marking validation per site, QoS performance information, and Voice/Video performance data (jitter and packet loss), based on the Cisco Performance Monitor.	utilization, interface errors, QoS performance, top applications, top talkers, and top DSCP reports.		
	Top Reports		0 0		
	Application	Top Conversations	Interface Bandwidth		
	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.	This Flow-based report will highlight the Top 10 conversions,	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.		
	DSCP	Top Interface Bandwidths	Top Interface Errors		
	This Flow-based report will highlight the Top 10 DSCP markings bandwidth, based on the selected filter criteria. It will list up to	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.	This SNMP-based report shows a table of all interface errors (CRC/Runts/Overruns. etc.) per the specified filter.		

3. From the Top Reports lower section, select Application

GENERAL SETTINGS	REPORT LIST		REPORT DETAILS	
NAME	Application (Flow)	Fast 💼	DEVICES	
MY Application	Add New Report	+	All WAN Devices	
PRESENTATION MODE			INTERFACES	
Standard			All WAN Interfaces	
OOTNOTE			FLEX SEARCH	
			Ex.: site=Honolulu & wan & flow.app=http	×
TIME ZONE	Ø DST		DISPLAY FILTER	
(GMT-08:00) America/Los Angeles			No Display Filtering	
TIME RANGE			DIRECTION	
Last Hour			Inbound and Outbound Combined	
SHARING	end PDF		FLOW TYPE	
Enter an email address or AD entity			Basic Flow	
Configure email settings to enable	sharing		EXECUTION TYPE	
Ex.: site=Honolulu & wan & flow.app=http	×		Time Series	
DISPLAY FILTER			SORT BY	
			Bit Rate	
			BUSINESS HOURS	
			All Hours	
			Cannot be used w	rith All Devices
			1 Minute	

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

LiveAction Lab Workbook Pt. 1



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

Note the Report Options on the image.

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

- 6. Hide a metric by clicking on the Legend.
- 7. Re-sort by clicking on the Sort Arrow.
- 8. Zoom-in by Left-click-drag a portion of the chart.
- 9. Reset Zoom to normal.
- 10. Schedule the Report to run Hourly.

MY Application	
RUN REPORT	
Hourly	
SCHEDULE ENDS	
Never	
	🔽 DST

Lab 1.5: Enable / Customize Alerts

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

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

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

Lab Steps:

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

QoS Class Drop (1	Device, Interface	Warning	Qos Class VOICE Drop Rate > 20 kbps for at	Web UI
QoS Interface Drop (1)	Device, Interface	Warning	Drop Rate > 2500 pps for at least > 0 minutes	Web UI
Routing Adjacency State Change	Network	Critical	for at least > 0 minutes	Web UI
Routing Polling Error	Network	Critical	for at least > 0 minutes	Web UI
Site Reachability	Network	Info	for at least > 5 minutes	Web UI
Spanning Tree Topology Change	Network	Critical	for at least > 0 minutes	Web UI
	A	1 Oriking		

3. Click on QoS Class Drop.

QoS Class Drop		×
On		
SEVERITY		
 Warning 		~
Note: Severity for this alert will be status. When the severity is info, it	reflected as the same severity used does not contribute to the status.	in the
THRESHOLDS		
QOS CLASS		
VOICE		
DROP RATE	FOR AT LEAST	â
> 20 kbps	> 0 min	
QOS CLASS		
VIDEO		
DROP RATE	FOR AT LEAST	Î
> 50 kbps	> 1 min	
Add More		
SHARING		
Email 💥	ServiceNow 🔆	
support@ × 1	SNMP trap	
	Syslog 💥	
(i) This alert may contribute to stat	tus of an Interface, Device, and/or S	ite.
Canc	el Save	

- 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.

▲ 410	1 2	• 0	🌲 1279					💄 ed 🗸
Mar 29, 2019 08:30:00 → Mar 29, 2019 08:45:00								et 🛃

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

veNX	Alert Management × +						
\rightarrow	🖄 🏠 🛈	tps://104.196.66.177/livenx/settings/ale	rting		♡☆ C'		🗊 III\ 🖶 »
lost Vi	sited						
					▲ 0 ■ 0 ● 0 ▲ 0 {]		
t Mar	nagement ^③						View Alerts
			LiveN	X Alerts			
Enable	Disable		Sele	cted: 31			
	ALERT TYPE	CATEGORY \$	SEVERITY	C ENABLED	THRESHOLDS	SHARING	\$
	Alert Type	All v	All	All	✓ Thresholds	Sharing	
	BGP Peer Connection Change	Network	Critical	~	for at least > 0 minutes	Web UI	
	Cisco IWAN Path Change	Network	Critical	~	for at least > 0 minutes	Web UI	
	Cisco IWAN Threshold Crossing	Network	Critical	~	for at least > 0 minutes	Web UI	
	Cisco SD-WAN SLA Class Path Change	Network	Critical	~	for at least > 0 minutes	Web UI	
	Critical Traffic Response Time	Application	Critical	~	Response Time >= 5 ms for at least > 0 min.	. Web UI	
	Device CPU Utilization ()	Device, Interface	Critical	~	Utilization >= 80 % for at least > 0 minutes	Web UI	
	Device Flow Stop	Device, Interface	Critical	~	for at least > 0 minutes	Web UI	
V	Device Memory Utilization (1)	Device, Interface	Critical	×	Utilization >= 90 % for at least > 0 minutes	Web UI	
	Device Reachability (1)	Device, Interface	Critical	~	for at least > 0 minutes	Web UI	
Z	Interface Errors (CRC, Frame, Overruns,	Device, Interface	Critical	~	Number of Errors >= 40 Errors for at least > .	Web UI	
V	Interface Reachability	Device, Interface	Warning	~	for at least > 0 minutes	Web UI	
v	IPSLA Test	Network	Critical	~	Total Test Errors > 3 Errors for at least > 0 m	Web UI	
~	IPSLA Voice/Jitter Test	Network	Critical	~	Total Test Errors > 3 Errors for at least > 0 m	Web UI	
V	LiveNX CPU Utilization	System	Critical	~	Local/Server >= 40 % for at least > 0 minutes	Web UI	
~	LiveNX Disk Utilization	System	Critical	~	Local/Server >= 60 % for at least > 0 minutes	web UI	
v	LiveNX Memory Utilization	System	Critical	~	Local/Server >= 40 % for at least > 0 minutes	Web UI	
~	LiveNX Node Connectivity	System	Critical	~	for at least > 0 minutes	Web UI	
v	Media Jitter Max	Application	Critical	~	Jitter Max >= 60 ms for at least > 0 minutes	Web UI	
v	Media Jitter Min	Application	Critical	1	Jitter Min >= 30 ms for at least > 0 minutes	Web UI	
Z	Media Packet Loss	Application	Critical	×	Packet Loss >= 1 % for at least > 0 minutes	Web UI	
-	Network Delay Per Connection	Network	Critical	1	Delay Time >= 40 ms for at least > 0 minutes	Web UI	

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

<u>File Edit View History Bookmarks</u>	Tools Help						- 🗆 🗙
🛗 Criterion Networks SDCloud Pla 🗙	🖾 LiveNX Dashboard 🛛 🗙 🕂	-					
$\overleftarrow{\bullet}$ \bigstar $\overleftarrow{\bullet}$	🛈 윮 https://35.231.127.249			🗵	D ☆ C'		© ∥\ 🖶 ≫ 😑
🌣 Most Visited							
≡ LiveAction •	NX UX			▲ 0 ■ 0 ●	• 0 🐥 0	(-) 🖵 💡 -	🌣 🔺 👗 adm 🤉 🗸
Dashboard					Mar 12, 2019 15	:35:00 → Mar 12, 2019 15:50:00	System Management
:: Status	··· -	WAN	··· II	System	1	Alerts	System Diagnostics
							Users Management
: Top Sites by WAN Utilization Peak	k Inbound WAN Interface Utilization	: Top WAN Applications	by Bandwidth Inbound/Out	oound Bandwidth 🗙	:: Top Interfaces %	Changed - Interface Burstavie Ra	LiveNX Server
HQ-SJ GigE0/1 San_Jose_DC - 1.0		rtp voip-telephony	528.4	• In	Branch2-NY GigE0/2	Outbound N0	

2. Click Add User

ADD NEW USER	
Local	LDAP
USERNAME *	DISPLAY NAME *
Add username	Display Name
ROLE *	SESSION TIMEOUT *
Select role V	15 Minutes V
Admin	REPEAT PASSWORD *
Clerk	Confirm password
Demo User	
Full Config	Cancel Add User
Monitor Only	
Monitor Only Partial Config	

- 3. Enter a username (something you'll remember).
- 4. Select the Admin role from the drop-down.
- 5. 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.

6. 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 2

Lab 2: The LiveNX Client

Lab 2.1: Launch the LiveNX Client

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

There is also a Mac client available.

Lab Steps:

1. Launch the LiveNX Client.

Java Web Start will begin to download and may take several minutes depending on your connection speed. You may be prompted with download warnings, or various save options, depending on your OS and security configuration.

DIAGRAM							
Client Logir	ı	×					
Live	Action						
Username:							
Password:							
For first time	e use:						
Usernar	me and password are "admir	1"					
Click "C	Click "Configure" to setup server address						
Configure	e 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.

Client on YOUR Workstation

Client	Login		×
Ļ	Server C	onfiguration	×
User	Server:	ettings (YourServerIP) v	
For f		7000	
-		Save	Cancel
Co	nfigure	ОК	Cancel

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

Client Logi	n X
Live	Action
Username:	admin
Password:	•••••
For first tim	e use:
Userna	me and password are "admin"
Click "C	onfigure" to setup server address
Configur	e OK Cancel

5. Click OK

The Client will launch...



... and eventually display the Client window showing the current configured Topology.



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

Lab 2.2: Explore the LiveNX Client

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

Lab Steps:

1. Right-click anywhere in the white area of the Topology Pane, and select View > Fit To View to zoom into the HQ-SJ Device, and center it on the screen.

DIAGRAM



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

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

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

DIAGRAM

File View Users QoS Flow	Routing IP SLA LAN Tools Reports Help
Dashboard Manage 🖹 Expand	QoS Flow Routing IP SLA LAN
Q_	₩ @ 10 / II + @ @ Audit
Name	
🗉 🕎 Home	
🗄 🛞 HQ-SJ	

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

- 5. Click on **Flow** tab, and on the **Home** icon in the tree-view pane to the left of the screen.
- 6. Expand the HQ SJ 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: Traffic Flows

Lab 3.1: Discover Flows

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

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

Lap Steps:

- 1. Select the Flow Tab.
- 2. Refresh the Topology Pane.



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

3. Set the filters to match:

🔁 Refresh	All Flow Types	~	Current Time	\sim	Current Polling Interval	~	ę	Voice	~	Top 50	~	T	DSCP	~

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

4. Refresh the Topology Pane, if needed.

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



- 5. Hover over the colored lines to see the volume of Voice transmissions.
- 6. **Click** on the colored flow line to see the IP end-points.

What other applications can you identify across our network?

Application	Port#	IP Pairs

Lab 3.2: Discover Specific Flows

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

- 1. Enter a search string of "flow.srcip=198.19.1.101".
- 2. Select No Display Filtering.
- 3. Click Refresh
- 4. Click on the displayed flow indicator.



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

Lab 3.3: 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.

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



2. Click on one of the end-points.

to/from

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

Lab 3.4: Troubleshoot Issues

Note: Your Instructor may direct you to skip this Lab, and will instead demonstrate these steps for the class.

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.

Lab Steps:

- 1. Open the SJ HQ device.
 - a. Double-click on it OR select from the Home Tree view.
- 2. Click the Playback button in the Filter Bar.
- 3. Scroll through the time display until you discover anomalous behavior.

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



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

Lab 4

Lab 4: Filtering, Identifying, Marking

Lab 4.1: Creating Custom Filters

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

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

Lab Steps:

1. Click the Filter ICON (looks like a funnel) to Open the Flow Display Filters Set-Up.

	SLA	LAN	<u>T</u> ools	Rep	orts	<u>W</u> ine	dow	Dev	<u>H</u> elp			
1	Flow	Rou	ting I	P SLA	LAN							
	🛞 E	nable P	olling	p Pau	se Disp	olay	Basic	Flow		Ģ	1	Def

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

🏹 Create Filter 😽 Copy 🏹 Delete 🚮	
Filter: *Defaul Create New Filter	
Filter Entries	
😫 Add Entry 🛛 🔓 Add Other Filter 🛛 🙀 Re	

3. Enter a Name label:

Create Flow Display Filter	×
Type in the name of the new flow display filter:	
OK Cance	

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

	tocol/Ports
elect from a p	re-defined list of protocols/applications or create new
efinitions	
ip	V 🔶 Create 🧷 Edit 🗅 Copy
_	
sip	
	tocol=TCP) AND (Src OR Dst=5060 OR 5061 OR 5062 OR 5060
[] (L4 Pr	tocol=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	k		
🕂 Create Definition 🗅 Copy 💥 Delete 📈 Rename			
Defined Protocols/Applications: sip			
Entries			
😩 Add Entry 🏾 🏹 Add Defined Prot/App 🔓 Delete			
Sip Image: Contract of the state of the sta			
< >			
Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.			
Entry Details			
Layer 4 Protocol: TCP (6) V			
Ports			
Match Ports Regardless of Source or Destination			
Source: 5060 5061 5062			
Destination: 5060 5061 5062			
Enter port numbers or ranges separated by spaces (e.g., 80 88-443)			
Help OK Cancel			

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



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



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

Protocols/Applications Setup	ł		
🕂 Create Definition 🗋 Copy 💥 Delete 🕺 Rename			
Defined Protocols/Applications:]		
Entries			
🕒 Add Entry 🏹 Add Defined Prot/App 🔓 Delete			
rtp 			
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) v			
Ports			
Match Source and Destination Ports 🗸 🗸			
Source: 16384-32767			
Destination: 16384-32767			
Enter port numbers or ranges separated by spaces (e.g., 80 88-443)			
Help OK Cancel]		

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

Create Filter Filter Entry Details Filter Entry Action:	A Flow Display Fi	ilters Setup
Color Mapping Label & Color. VOIPFiter I 1 Show IPv4 Only (Prot/App-sip) Color Mapping Label & Color. Match Protocol/Ports Select from a pre-defined list of protocols/applications or create new definitions It protocol It protoc	Filter: VOIPFilter	Filter Entry Action: Show or Hide the following
Select find a pre-defined list of protocols/applications or create new definitions	Add Entry By Add Other Filter By Delete Entry By By	
		Select from a pre-defined list of protocols/applications or create new definitions Ftp: Create Create Copy Ftp: Create Copy Ftp: Create Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp: Copy Ftp:
(o (BE) ~)		□ Match DSCP 0 (BE) v
Match Device Interface Match flows traversing through a particular device's interface Match flows traversing through a particular device's interface "Branch1-LA.ddoud.cisco.com Help OK Cancel Apply	the Filter drop-down box.	Match flows traversing through a particular device's interface Branch1-A.ddoud.disco.com Fethernet0/0

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

	LiveAction - 198.18.133.34	- 🗆 🗙
<u>File View Users QoS Flow R</u>	souting IPSLA LAN Iools Reports Window Dev Help	
Dashboard Manage 📑 Expand	Qos ² Flow Routing IP SLA LAN	
Q,	🕂 🕂 🥀 🥂 🛴 🔍 🍕 🍕 Table 🔁 Refresh. All Flow Types 🗸 Current Time 🗸 Current Poling Interval 🗸 🤤 Voice-Lab 🗸 Top 30 🗸 🦉 DSCP	¥
Name	Search Example: (ate = Honolulu ate = Chicago) & wan & flow.app = webex-meeting	× - ?
Hanie Pie @ Branch1LA Pie@ Branch2AYY Die @ HQ_SJ Pie @ HQ_SJ	Color Marping By DSCP 0 (B) 2 (S) 3 (K-13) 3 (K-13)	
		2:50 PM
	arts 🚅 dog e 🚰 togs 🖉 affe 🔼 11 g 10 🗞 17 g 🛃 ton g 💭 di dogla yed. Showing flow data from 3 of 3 devices. admin: Admin	user 02:11/9/2015 ST

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

Lab 4.2: ACL Creation

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

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

Lab Steps:

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



2. Select "Create ACL"

	ACL Management	for Branch1-LA	
Current Router Branch 1-LA			
Access Control Lists (ACLs)			
Name / Number	Туре	Applied Interfaces	Create ACL
ACL-BITTORRENT-PC1	Extended (Named)		Edit ACL
ACL-CITRIX-PC1	Extended (Named)		
ACL-FTP-PC1	Extended (Named)		Delete ACL
ACL-G711-19420	Extended (Named)		
ACL-INET-PUBLIC	Extended (Named)		Copy ACL
BEST_EFFORT	Extended (Named)		
CRITICAL	Extended (Named)		Apply / Remove ACL
DENY_GLOBAL_LEARN_LIST	Extended (Named)		
RDP	Extended (Named)		
RTPACL	Extended (Named)		
SIPQoS	Extended (Named)		
VOICE_VIDEO	Extended (Named)		
Access Rule Entries permit tcp host 198.19.1.101 eq	47309 host 198.18.133.36 eq 1044		Save ACL File
permit tcp host 198. 19. 1. 101 eq	1044 host 198.18.133.36 eq 47309		
			Load ACL File
			Close

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

	Create ACL	×
Type Name / Number	Extended v RTPQoSMark	Help
Remarks		
remark Marking ACL f	for RTP Traffic	Create Remark
		Edit Remark
		Remove Remark
Access Rules		
		Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
	Preview CLI Save	to Device Cancel

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 RTPQoSMark	×
fermit deny UDP Object-Group < No Object Groups > Other by Name ahp	
Source	
Match by DSCP v Log Rule Log v OK Cancel	

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

12. Click Save to Device.

	Create ACL	×
Туре	Extended 🗸	
Name / Number	RTPQoSMark	Help
Remarks		
remark Marking ACL fo	r RTP Traffic	Create Remark
		Edit Remark
		Remove Remark
Access Rules	16384 32767 any range 16384 32767	Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
	Preview CLI Save to D	Device Cancel

Create ACLs for the SIP ports.

	ACL Manage	ment for Branch1-LA	×
Current Router Branch 1	LA		
Access Control Lists (AC	Ls)		
Name / Number	Туре	Applied Interfaces	Create ACL
ACL-BITTORRENT-PC1	Extended (Named)		Edit ACL
ACL-CITRIX-PC1 ACL-FTP-PC1	Extended (Named) Extended (Named)		Delete ACL
ACL-G711-19420	Extended (Named)		
ACL-INET-PUBLIC	Extended (Named)		Copy ACL
BEST_EFFORT	Extended (Named)		
CRITICAL	Extended (Named)		Apply / Remove ACL
DENY_GLOBAL_LEARN_LIST	T Extended (Named)		
RDP	Extended (Named)		
RTPACL	Extended (Named)		
RTPQoSMark	Extended (Named)		
SIPQoS	Extended (Named)		
VOICE_VIDEO	Extended (Named)		
Access Rule Entries			
	01 eq 47309 host 198.18.133.36 eq 1		Save ACL File
permit top nost 198, 19, 1, 10	01 eq 1044 host 198.18.133.36 eq 47	203	Load ACL File

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

	Create ACL	×
Type Name / Number	Extended V SIPQoSMark Help	
Remarks		
remark Marking ACL	for SIP Traffic Create R	lemark
	Edit Re	mark
	Remove F	Remark
Access Rules		
	Create	Rule
	Edit R	tule
	Сору Р	Rule
	Delete	Rule
	Move	Un

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

Edit Extended Rule	Entry for SIPQoSACL ×
permit O deny	
○ IP	✓ ahp ✓
Source	Destination
any O by Network or IP by Object-Group	any O by Network or IP by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > v	> e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups > v
✓ by Port Between ✓ Manage Port(s)	< Dep Port Equal to V Manage Port(s)
5060 5062	
Match by DSCP v	
Log Rule Log V	
	OK Cancel

Next create another rule for destination SIP Ports.

	Edit Extended ACL SIPQoSACL	×
Туре	Extended 🗸	
Name / Number	SIPQoSACL	Help
Remarks remark Marking ACL for	SID Traffic	
remark Marking ACL for	SIP frame	Create Remark
		Edit Remark
		Remove Remark
Access Rules		
	000 5000	
permit tcp any range 5	060 5062 any	Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
	Preview CLI Save t	to Device Cancel

LiveAction Lab Workbook Pt. 1

● ○ ○ Edit Extend	led Rule Entry for SIPQoS
💿 permit 🛛 deny	
○ IP • TCP ○ UDP ○ Object-Group < No Object Gr ‡ ○ Other	by Name 💠 ahp 🛟
Source	Destination
any Object-Group	>> O by Network or IP O by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 <pre>< No Object Gr \$</pre>	e.g 192.168.1.0/24 or 192.168.1.19 <pre>< No Object Gr +</pre>
✓ by Port Between ÷ Manage Port(s)	by Port Equal to Manage Port(s)
5060 5062	
□ Match by DSCP ‡	
Log Rule	
	OK Cancel

- 22. Select "TCP" as the protocol type.
- 23. For Source check Any.
- 24. In Destination select by Port.
- 25. Select "Between" as the operator value.
- 26. In the entry box use "5060 5062" as the field entry.
- 27. Click OK when your fields match the diagram below

Edit Extended Ru	ule Entry for SIPQoSMark
Dermit O deny DP ODject-Group < No Object Groups > Other by Name	e v ahp v
Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Source Sou	Destination • any • by Network or IP • e.g 192.168.1.0/24 or 192.168.1.19 by Object-Group • e.g 192.168.1.0/24 or 192.168.1.19 • y • by Port Between • Manage Port(s) 5060 5062
Match by DSCP V Log Rule Log V	OK Cancel

- 28. Click Preview CLI to review the configuration to push.
- 29. Click Save to Device.

	Edit Extended ACL SIPQoSMark	×
Туре	Extended v	
Name / Number	SIPQoSMark	Help
Remarks remark Marking ACL for	SIP Traffic	Create Remark
		Edit Remark
		Remove Remark
Access Rules		
permit tcp any range 5		Create Rule
permit tcp any any ran	ge 5060 5062	Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
		Profe Domi
	Preview CLI Save to	Device Cancel

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

Lab 5

Lab 5: Configuring Devices

Lab 5.1: Add Device

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

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

Lab Steps:

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

	()	A https://104.1	96.66.177/liven:	<pre>k/settings/device</pre>	-management			•••	⊠ ☆ C				🗊 III\	+	»
Most Visited															
E LiveAction [™]	NX UX								• 0 🐥 0						
MAIN							Credential	Store	View Dev	ces /	Add Non SN	MP Device	Disco	ver Devic	ces
	2)		My	Interfaces (4)			Discovered D	evices	(0)		(Autodisc	overy (3)	4	
TOPOLOGY													1		
	Redis	cover Interfaces	Configure	Delete					Q						
STORIES	ADDRESS 🗘	VENDOR \$	MODEL \$	NODE 🗘	SITE 🗘	INTERFACES 🛟	POLL	٥	qos 🗘	FLOW	O IP S	LA 🗘	ROUTING	\$	LAN
III REPORTS	Address	All ~	Model	Node			All	~	All v	All	~ All	1	All	~	All
	8.18.129.25	Cisco	cisco3945	Local/Server	San_Jose_DC	2	~		~						
MINSIGHT	8.19.2.1	Cisco	cisco3945	Local/Server	New_York	2	~		~			~	~		
Site Management															
Device Management															

3. Click Discover Devices.

1. What to scan	2. SNMP Settings	3. Node	
SPECIFY IP RANGES			
198.19.1.1 198.19.2.1 198.18.129.23-25	Choose	e a site 🗸 🗸	
Add More			
SPECIFY SEED DEVICE TO SCAN IP ADDRESS		HOPS	
		Sav	e & Next

- 4. Enter 198.19.1.1, 198.19.2.1, and 198.18.129.23-25 in the IP Address field.
- 5. Select the SNMP Settings tab.

- 6. Click "Default SNMP connection settings".
- 7. Select the **Node** tab.
- 8. Select Local/Server.
- 9. Click **Discover**.

Device Management 🕝		Credential Store View Devices	Add Non SNMP Device Discover Devices
My Devices (2)	My Interfaces (4)	Discovered Devices (0)	② Autodiscovery (3)
DISCOVERY LOGS:	4/5 1		

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.

				Selected: 1		Q Search	
t.	DEVICE	SERIAL	IP ADDRESS	VENDOR \$	MODEL \$	NODE	INTERFACES
	Device	Serial			Model	Node	
	Branch1-LA	101	198.19.1.1	Cisco	cisco3945	Local/Server	5
	HQ-B1	2	198.18.129.24	Cisco	cisco3945	Local/Server	6
	HQ-MC	1	198.18.129.23	Cisco	cisco3945	Local/Server	3

10. Tick the box next to Branch1-LA.

11. Click Select Interfaces.

					Se	lected: 4		Q			
	NAME \$	DEVICE \$	LINE RATE (KBP 🗘	IP ADDRESS	LABEL \$		OUTPUT CAPAC 🗘	WAN (Kbps)	≎ servi ≎	TAGS 🗘	DESCRIPTION
	name	All ~	line rate	ip address			Output Capa	All	All 🗸		
1	GigabitEthernet	Branch1-LA	100000	198.19.1.1	Branch1 LAN	100000	100000	~	Branch		Branch1 LAN
	GigabitEthernet	Branch1-LA	2000	100.64.1.2	Internet	2000	2000	~	Internet		Internet
	GigabitEthernet	Branch1-LA	1000	10.255.1.2	MPLS	1000	1000	~	MPLS		MPLS
	Loopback0	Branch1-LA	8000000	10.0.1.1							
	Null0	Branch1-LA	1000000								

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 incumbent upon YOU to confirm, or select, the interfaces you wish to monitor. LiveNX may monitor up to 1000 interfaces on a single device.

NAME \$	DEVICE \$	LINE RATE (KB 💲	IP ADDRESS	LABEL 🗘	INPUT CAPACI \$	OUTPUT CAPA \$	WAN (Kbps)	SERVI 🗘	TAGS 🗘	DESCRIPTION \$
name	All ~	line rate	ip address			Output Capa	All 🗸	All V		
GigabitEthernet0/0	Branch1-LA	100000	198.19.1.1	Branch1 LAN	100000	100000	~	Branch		Branch1 LAN
GigabitEthernet0/1	Branch1-LA	2000	100.64.1.2	Internet	2000	2000	✓	Internet		Internet
GigabitEthernet0/2	Branch1-LA	1000	10.255.1.2	MPLS	1000	1000	~	MPLS		MPLS
Loopback0	Branch1-LA	8000000	10.0.1.1							
NullO	Branch1-LA	1000000								

- 12. Select ONLY GigabitEthernet1 & GigabitEthernet3.
- 13. Click Add Selected.

	My Device	is (3)		My	Interfaces (6)			Discovered Device	s (2)			Autoo	discovery	y (2)	
				0.5											
Edit	Refresh L	Ist Redisc	over Interfaces	Configure	Delete					Q S					
DI	EVICE \$	IP ADDRESS	VENDOR \$	MODEL \$	NODE \$	SITE 🗘	INTERFACES \$	POLL \$	QOS	٥	FLOW \$	IP SLA	\$ R	OUTING	۵ ۵
	Device		All ~	Model	Node	Site		All 🗸	All	~	All 🗸	All	~	All	~ /
G	Branch1 🔀	198.19.1.1	Cisco	cisco3945	Local/Server		2	~	-		~	~			
н	IQ-SJ	198.18.129.25	Cisco	cisco3945	Local/Server	San_Jose_DC	2	×	~		×				
В	Branch2-NY	198.19.2.1	Cisco	cisco3945	Local/Server	New_York	2	~	1		✓	~		<	

You now see we've added Branch1-LA 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.

Note: Since the creation of this lab guide, Cisco has changed the labeling on the interfaces. Some of the screenshots may still reflect the older naming convention, i.e. Ethernet 0/0, Ethernet 0/2, while what is shown on your screen may be different – GigabitEthernet1, GigabitEthernet3. Please adjust accordingly and note that items may not appear exactly as they do in the screenshots

Lab 5.2: Manage & Configure Devices

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

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

Lab Steps:

- 1. Login to the LiveNX Client.
- 2. Right-click on Home and Expand All.



Notice that the Topology Pane contains all the devices listed in the Home Tree view. Also note that the Branch1-LA device needs to be configured.

3. Click Manage (Above the Home Tree).

Filter	by:							Clear						
lect	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	cisco 3945	Local								10 seco 🗸	
	Branch2-NY	198.19.2.1	Cisco	cisco3945	Local		\checkmark	\checkmark	\checkmark				10 seco 🗸	
	HQ-SJ	198.18.129.25	Cisco	cisco3945	Local			\checkmark	\checkmark				10 seco 🗸	Configure
iN pol	ling occurs every 15 mi	nutes											Nun	nber of Devia
	Ing occurs every 15 mi	nutes				Global Devi	ce Settin;	gs					Nun	nber of Devic
	-	nutes Configure QoS, FI Sect devices in the to	ow, and I	P SLA the configure buttor	h.	Global Devi Edit			MP Settin	ps			Nun	nber of Devia
	Configurations	Configure QoS, Fl	able and did	P SLA the configure buttor	h.		D	efault SN			s - Not Set		Nun	nber of Devia
	Configurations Configure	Configure QoS, Fl Select devices in the ta	able and did	P SLA the configure buttor	h.	Edit	D	efault SN efault CLI	I Monitori				Nut	
evice (Configurations Configure Remove	Configure QoS, FI Select devices in the ta Remove selected devi	able and did	the configure buttor		Edit	D	efault SN efault CLI	I Monitori	ng Setting			Nun	Clear

- 4. **Un-tick** all but the Poll, QoS, and Flow features.
- 5. Change the Interval on all devices to **10 seconds**.
- 6. Click **Apply**.
- 7. Tick the box next to Branch1-LA device.
- 8. Click Configure.

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

- 9. Use the Default SNMP... Click Next
- 10. Use my default Configuration CLI... Click Next

				Configure Cisco Features for -	Branch1-LA.dcloud.cisco.com (198.19.1.1)
Steps	Device Connection Infor	mation		Steps	CLI Settings (Configuring)
1. Device Connection Information	Enter the SNMP connect	ion information.		1. Device Connection Information	Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).
 CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select WANs Select Peatures Enable Poling Review Configuration Device Updated 	Node P Address Address UneSensor UneSensor SNPP Connec SNPP Version Community String	· · ·	t TargetPort 161	Cull Settings (configuring) Configuring) Cull Settings (Monitoring) Settings (Monitoring) Setter UNAls Setter Interfaces Setter UNAls Setter Interfaces Setter Interfaces Review Comparison Review Comparison Device Updated	Configuration CLI Connection Settings Enter Command Line Interface (CLI) connection settings used to configure these devices. >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
	< Back Next >	Einish	Cancel Help		<back next=""> Finish Cancel Help</back>

11. Check Use the previous page connection settings... Click Next. Ensure Interfaces GigabitEthernet1 & Gigabit Ethernet3... Click Next

Steps	CLI Settings (Monitoring)	Steps	Select Interfa	ices			
 Device Connection Information CLI Settings (Monitoring) CLI Settings (Monitoring) Select UAMs Select UAMs Select UAMs Select Polling Review Configuration Device Updated 	Specify the CLI connection Information Harred by all users. This information will only be used to monitor this device. Required fields are indicated with an astersis (*). Monitor-only CLI Connection Settings Enter Common Lie Information (ULI) connection settings used to monitor this device. Use the default Monitor only CLI connection settings Enter Connection specifys for this device Enter Connection settings for this device Liber name on Device* Enable Password	Device Connection Information CLI Settings (Configuring) CLI Settings (Configuring) S. CLI Settings (Notroting) S. Select Inflarfaces S. Select WAN S. Select WAN S. Select VAN S. Select Configuration S. Review Configuration S. Device Updated	Note: IP add the user guid	erfaces you want to essees and subnet me for more details. CapabitEfhernet1 CapabitEfhernet1 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfhernet2 CapabitEfherne		1000 Interfaces). Jevices that do not pro- Subnet Mask 255, 255, 255, 0 255, 255, 255, 0 255, 255, 255, 0 255, 255, 255, 0 255, 255, 255, 255, 255, 255, 255, 255,	Vide them. See Description Branch LAN Internet MPLS

- 12. **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.
- 13. 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. Match the settings for GigabitEthernet3. Click Next.

teps	Select Features		
 Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces 	Select the features you want to enable section. Features on device Associate Probe at IP Address:	on each interface. Learn i	more about each feature in the Help
5. Select VLANs	Interface	NBAR	NetFlow
6. Select Features 7. Enable Polling B. Review Configuration 9. Device Updated	GgabiEthernet1 GgabiEthernet3		
	<back next=""> Finish</back>		Cancel Help

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 LiveAction created.

14. Enable Polling. Next. Click Continue

		Validation Deta	ils			×
		Validation resul	ts for the current device:			
		Test		Status	Description	
		SNMP connection	1	•	Succeeded	~
		SNMP access		•	Succeeded	
		CLI configure co	nnection	0	Skipped	
nfigure Cisco Features for - E	Branch1-LA.dcloud.cisco.com (198.19.1.1)	CLI configure log	in	\odot	Skipped	
teps	Enable Polling	CLI configure en	able password	\odot	Skipped	
1. Device Connection	Select the features you want to actively monitor and the poling rate for all the features on this device.	CLI monitor conr	lection	\odot	Skipped	
Information	Learn more about polling in the Help section.	CLI monitor login		\odot	Skipped	
2. CLI Settings (Configuring)		CLI monitor enab	le password	\odot	Skipped	
 CLI Settings (Monitoring) Select Interfaces 		Serial number va	lidation	0	Skipped	
 Select Interfaces Select VLANs 	Polling Rate 10 seconds	Model supported		•	Succeeded	
5. Select Features		IOS supported		•	Succeeded	
7. Enable Polling	Poll the following features	NBAR capable		•	Succeeded	
3. Review Configuration	I Flows	NBAR2 capable			Succeeded	
 Device Updated 	∠ QoS	NetFlow collecto	r configure supported		Succeeded	
	□ IP SLA	Flexible NetFlow			Succeeded	
	Routing		(AVC/Medianet) Supported		Succeeded	
	_		mance Monitoring supported		Succeeded	
	LAN*	MACE AVC Supp	- · · ·	0	Not supported	
	* LAN polling occurs every 15 minutes		ifigure supported	Ő	Not supported	
	* For SNMP v3, please see the User Guide on configuring LAN polling.	Mediatrace confi		ě	Succeeded	
		IP SLA Supporte			Succeeded	
		HQF Supported	-		Succeeded	
		MAC Table Supp			Not supported	\checkmark
figure Cisco Features for - Br	(Back <u>Bext</u>) Enish Cancel Hep mnch1-LA.doloud.cisco.com (198.19.1.1)	Configure Cisco Features for	Branch1-LA.dcloud.cisco.com (198.19.1.1		Continu	
	Review Configuration)		
ps	Review Configuration The following commands will be sent to the device. Or you can choose to manually configure the device	Steps	Review Configuration The following commands will be sent to th	- devier ()		
Information	yourself.	Information	yourself.	e device. Or you a	an choose to manually configure	e une ue
CLI Settings (Configuring) CLI Settings (Monitoring)	No configuration command(s) will be sent to the device.	2. CLI Settings (Configuring)				
CLI Settings (Monitoring) Select Interfaces	No configuration command(s) will be sent to the device.	3. CLI Settings (Monitoring) 4. Select Interfaces	collect conting destination			
Select VI ANs		5. Select VLANs	collect couting source as			
Select Features		6. Select Features	collect thestamp sys-uptie			
Enable Poling		7. Enable Polling	collect transport top flags			
Review Configuration		8. Review Configuration	exit			
Device Updated		9. Device Updated	description TO SOT MODIFY			
			exporter: LIVERCTION-FLOWERP			
			cache timeout inactive 10 cache timeout active 60			
			report LIVEACTION-FLORRECOR			
			exis			
			interface GigabitEthernet3			
			ip flew mining LIVEACTION-			
	v					
	 Send the configuration commands to device. 	-	 Send the configuration commands to 			
	I will manually configure the device myself.		I will manually configure the device it I will manually configure the device it	nyself.		
	<back next=""> Finish Cancel Help</back>		<back next=""> Finish</back>		Cancel	
	< Back Next > Einish Cancel Help		< Back Next > Finish		Cancel	

- 15. Select "I will manually configure..." radio button, if available.
- 16. Click Next.
- 17. Click Finish.

The device will be added to the Topology Pane in LiveNX.

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

Lab 5.3: Configure Flow on Devices

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

Lab Steps:

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



2. Select all three devices, click Configure Selected.

Flow Co	onfiguration								_		(
Instructions Select dev	; vices to configure flow										
	uration Table										
Q											
Select	Device	Туре	IP Address	Description	Tags	Traffic Stati	Application	Voice/Video Pe	Traditional	Custom	
	Branch 1-LA	Standard \checkmark	198.19.1.1	Cisco IOS Softwa	WAN, 100	۲		•			
	🛞 Branch2-NY	Standard \checkmark	198.19.2.1	Cisco IOS Softwa	WAN, New	۲	۵	•	0	0	
	🛞 HQ-SJ	Standard 🗸 🗸	198.18.129.25	Cisco IOS Softwa	WAN, San	•	•	•	•	•	
He	þ							Configure Sele	cted	Close	

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.

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

- 3. Select Traffic Statistics (FNF), Application Performance (AVC), and Voice/Video (Medianet) on:
 - a. GigabitEthernet3 on both Branch1-LA and Branch-NY
 - b. GigablitEthernet1 and GigabitEthernet2 on HQ-SJ.

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

Flow Configuration									- 0	
tructions										
onfigure the type of flow you wis	h to receive from the inte	erfaces								
w Configuration Table										
Y										
evice	Туре	IP Address	Description	Tags	Traffic Statist	Application R	Voice/Video Perf	Traditional	Custom	
🛞 Branch1-LA	Standard	√ 198.19.1.1	Cisco IOS Softwar	WAN, 1000,	۲	•	۲		0)
GigabitEthernet0/0		198.19.1.1	Branch 1 LAN	100000, 100						
GigabitEthernet0/2		10.255.1.2	MPLS	MPLS, 1000,						
Branch2-NY	Standard	v 198.19.2.1	Cisco IOS Softwar		•	•	•	•		
GigabitEthernet0/0	-	198.19.2.1	Branch2 LAN	-						
GigabitEthernet0/2		10.255.2.2	MPLS	1544, MPLS,						
- (R) HQ-SJ	Standard	198.18.129.25	Cisco IOS Softwar			•	•	•	0	
GigabitEthernet0/0		198.18.129.25								
GigabitEthernet0/1		10.255.0.2		100000, MPL		v ✓				
Gigabiteti en eto/1	-	10.233.0.2		100000, MPL	2					
Help 4. Click	Preview Cl	_1.	Sa	ave to Devices	Preview CL	Re	evert	Back	Clos	e
4. Click https://www. x type bitid Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed Standed	extended LIVEACTION-ACL-AVC	×							Clos	e
4. Click Mulge CLI Verser	estandes LIVEATION-ACL-AVC any performance-denitor LIVEAT b-any LIVEATION-CLASS-AVC h-any LIVEATION-CLASS-AVC harding LIVEATION-ACL-AVC INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTO-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON	× 108-POLICY-INIFIED	Selec	ct devic		w indivi	dual CLI		Clos	e
4. Click I uligie CLI Viewer to Type to A Boarded Carl Boarded Carl Boarded Carl Boarded Carl Boarded Class-amp AIDC Class-amp AIDC	estandes LIVEATION-ACL-AVC any performance-denitor LIVEAT b-any LIVEATION-CLASS-AVC h-any LIVEATION-CLASS-AVC harding LIVEATION-ACL-AVC INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTO-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON-CLASS-AVCLASS-AVCLANCE INTON-CLASS-AVCLANCE INTON	× 108-POLICY-INIFIED	Select Instructions	ct devic	e to vie	w indivi			Clos	e
4. Click I Mulpie CLI Viewer: 8 Type 124 Standed 124	estendes LIVEACTION-ACL-NUC ANY a performance-monitor lIVEACT b-may lIVEACTION-CLASS-ANY b-may lIVEACTION-CLASS-ANY TOP ANAMA LIVEACTION-ACL-NUC TOP ANAMA LIVEACTION-ACL-NUC TOP ANAMA LIVEACTION-ACL-NUC TOP ANAMA LIVEACTION-ACL-NUC CONTRACT-ANAMA ANAMA ANAMA ANAMA TOP ANAMA ANAMA ANAMA ANAMA ANAMA DESTINGTION-ACLASSICAL LIVEACTION ACLASSICAL ANAMA ANAMA ANAMA ANAMA ANAMA DESTINGTION-ACLASSICAL LIVEACTION ACLASSICAL ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANAMA ANA ANAMA ANAMA ANA	X 108-POLICY-SRIFIED ET	Select Instructions Configure th Flow Configure th	ct devic	eto vie	w indivi	dual CLI			
4. Click f	estended LIVEACTION-ACL-NUC ANY e performance-monitor LIVEACT b-may LIVEACTION-CLASS-AUT 0-may LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOO TOOP name LIVEACTION-ACL-NUC TOO DECEMBER OF A STATE OF A STATE NUCLEAR ACL NUCLEAR ACL NUCLEAR ON-CLASS-MEDILART	X 108-POLICY-SRIFIED ET	Flow Conf Instructions Configure th Flow Configure to Row Configure	ct devic	the to receive from the	w indivi nterfaces	dual CLI	file.		
4. Click I Multiple CLI Viewer * Type Standard Note: Standard Note: Standard Note: Standard Note: Standard Note: Standard Note: Standard Claims and Standard Claims an	estended LIVEACTION-ACL-NUC ANY e performance-monitor LIVEACT b-may LIVEACTION-CLASS-AUT 0-may LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOOP name LIVEACTION-ACL-NUC TOO TOOP name LIVEACTION-ACL-NUC TOO DECEMBER 2014	X 108-POLICY-SRIFIED ET	Elevent Flow Configure Flow Configure Flow Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure Configur	ct devic iguration e type of flow you wi ation Table	the to vie the to receive from the Type Standard	W indivi	dual CLI escription Tags Tr too IOS So	file.	Voice/Vide	Traditio.
4. Click I utget CLIVever	estendes LIVEATION-ACL-BUT any a performance-ensitor LIVEAT h-may LIVEATION-CLASS-MUTION h-may LIVEATION-CLASS-MUTION for the state of the state of the state for the state of the state of the state of the state of the state of the state of class-MUTION-CLASS-MUTION CHASS-MUTION-CLASS-MUTION CHASS-MUTION-CLASS-MUTION CHASS-MUTION-CLASS-MUTION CHASS-MUTION-CLASS-MUTION-CLASS-MUTION CHASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION-CLASS-MUTION	X 108-POLICY-SRIFIED ET	Flow Configure th Flow Configur	ct devic iguration e type of flow you wi ation Table	the to receive from the Type Standard	w indivi nterfaces D 199.19.1.1 Ce 199.19.1.1 Ce 199.19.1.1 Ce	dual CLI escription Tags Tr roo IOS 50 arch 1 LAN -	file.	Voice/Vide	Traditio
4. Click I while CLY lever a yet a yet a yet banded a yet a y	estendes LIVEACTION-ACL-NUC 407 a performance-monitor lIVEACT b-may lIVEACTION-CLASS-NUC b-may lIVEACTION-CLASS-NUC trop name lIVEACTION-ACL-NUC trop name lIVEACTION-ACL-NUC performance-monitor on-CLASS-NUC class-settimet on-CLASS-NUC meth/2 settimet class-settimet on-CLASS-NUC meth/2 settimet on-CLASS-NUC meth/2 settimet on-CLASS-NUC meth/2 settimet on-CLASS-NUC meth/2 settimet on-CLASS-NUC meth/2 settimet on-CLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC meth/2 settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet on-cLASS-NUC settimet	X 108-P0LICY-INIFIED ET 108-P0LICY-INIFIED pot LIVELATION-POLI	Select	ct device iguration e type of flow you wi ston Table	eto vie sh to receive from the Type Standard v	w indivi	dual CLI escription Tags Tr roo IOS 50 arch 1 LAN -	file.	Voice/Vide	Traditio.
4. Click I Magie CLI Viewer ************************************	estended LIVEACTION-ACL-NUC ANY + performance-monitor LIVEACT any LIVEACTION-ACL-NUC any LIVEACTION-ACL-NUC any LIVEACTION-ACL-NUC ACTION-CLASS-WE performance-monitor LIVEACT SN-CLASS-WEDLART ON-CLASS-WEDLART DN-CLASS-WEDLART LIVEACTION-ACLINE LIVEACT SN-CLASS-MEDLART DN-CLASS-MEDLART LIVEACTIONACC-MONITOR LIVEACT NUMP PERformance-monitor LIVEACT NUMP PERfo	X IOB-POLICY-SWIFIED ET IOB-POLICY-SWIFIED put LIVELATION-POLIC	Select Instructions Configure th Flow Configure Q- Device @ Branch @ Ethy @ Ethy @ Ethy	ct device iguration to Table 114A emet0/0 emet0/1 emet0/2 pback0	the to vie the to receive from the Standard v	W indivi IP Address D 198.19.1.1 Gr 198.19.1.1 Gr 100.51.2 MF 100.255.1.2 MF	dual CLI escription Tags Tr roo IOS 50 arch 1 LAN -	file.	Voice/Vide	Traditio
4. Click I Autor Cli	estended LIVEACTION-ACL-NC ANY e performance-monitor LIVEACT b-any LIVEACTION-CLASS-NC b-any LIVEACTION-CLASS-NC MCION-CLASS-NC NCION-CLASS-NC NCION-CLASS-NC TOP telepresent-media e performance-monitor LIVEACT ON-CLASS-NCNUT Intel()2 Upp Performance-monitor LIVEACT performance-monitor LIVEACT performance-monitor LIVEACT DN CONCET, USE NO LIVEACT	X ION-POLICY-ONIFIED ET ION-POLICY-ONIFIED POLICY-ONIFIED POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POL	Select Flow Configure th Flow Configure th Flow Configure th Flow Configure th Configure th Co	ct device iguration to Table 114A emet0/0 emet0/1 emet0/2 pback0	ee to vie sh to receive from the Type Standard ~	w indivi IP Address D 199.19.1.1 Gr 190.75.1.2 MF 10.0.55.1.2 MF 10.0.1 Gr	dual CLI escription Tags Tr too IOS So ternet - %S -	file.	Voice/Vide	Tradito.
4. Click I Autope CLI Verser: X Tree Note: Standard Note: Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Standard Stan	estended LIVEACTION-ACL-DUC May # performance-monitor LIVEACT b-acy LIVEACTION-CLASS-AUC b-acy LIVEACTION-CLASS-AUC b-acy LIVEACTION-CLASS-AUC monitor LIVEACTION-ACL-DUC ACTION-CLASS-AUCLIDIC TO TO DOCLASS-AUCLIDIC LIVEACT ON-CLASS-AUCLIDIC LIVEACT ON-CLASS-AUCLIDIC LIVEACT Symp performance-monitor LIVEACT ON-CLASS-AUCLIDIC LIVEACT ON PODERT. CORS & LIVEACTI ION ADDR AUCLIDIC LIVEACTION ON CLASS - AUCLIDIC LIVEACTION DISTANCE AUCLIDICAL DISTANCE AUCLIDICAL DISTANCE AUCLIDICAL DISTANCE AUCLIDICAL D	X ION-POLICY-ONIFIED ET ION-POLICY-ONIFIED POLICY-ONIFIED POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POL	Select Instructions Configure th Flow Configure th Flow Configure Q- Device @ Branch @ Eth @ Eth @ Eth @ Eth @ Eth @ Eth @ Eth	ct device iguration type of flow you wi ation Table the renet0/1 ernet0/1 ernet0/2 pback0 2-4W ernet0/0 ernet0/0 ernet0/0	the to receive from the Type Standard ~ Standard ~	W indivi IP Address D 198.19.1.1 Gr 193.19.1.1 Gr 100.64.1.2 In 198.19.2.1 Gr 198.19.2.1 Gr	dual CLI escription Tags Th too IOS 50 ternet - 15 - 15 - 15 - 15 - 15 - 15 - 15 - 16 - 16 - 16 - 16 - 16 - 16 - 16 - 16	file.	Voice/Vide	Traditio.
4. Click P Autign CLI Viewer Autign CLI Viewer A	estended LIVEACTION-ACL-NUC 407 e performance-monitor LIVEACT b-may LIVEACTION-CLASS-NUC b-may LIVEACTION-CLASS-NUC TOP name LIVEACTION-ACL-NUC TOP name LIVEACTION-ACL-NUC TOP name LIVEACTION-ACL-NUC performance-monitor LIVEACT on-CLASS-NUC Home Performance-monitor LIVEACT Sep Performan	X ION-POLICY-ONIFIED ET ION-POLICY-ONIFIED POLICY-ONIFIED POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POL	Select Flow Configure th Flow	ct devic iguration e type of flow you wi ston Table 114A emetb/0 emetb/1 emetb/2 pback0 emetb/1 emetb/0 emetb/0 emetb/0 emetb/1 emetb/0	Ce to vie	W indivi IP Address D 199.19.1.1 CK 190.19.1.1 CK 190.255.1.2 MF 10.0.1.1 199.19.2.1 GR 199.19.2.1 GR 199.19.2.1 GR	dual CLI escription Tags Th too IOS 50 ternet - 15 - 15 - 15 - 15 - 15 - 15 - 15 - 16 - 16 - 16 - 16 - 16 - 16 - 16 - 16	file.	Vaice/Vide	Tradito.
4. Click P Autign CLI Viewer Autign CLI Viewer A	estended LIVEACTION-ACL-NC By performance-enclose LIVEACT h-may LIVEACTION-ACL-NC h-may LIVEACTION-ACL-NC N-may LIVEACTION-ACL-NC NC NOT ACL-NC NC NOT ACL-NC NC NOT ACL-NC DEFORMANCE-MONITOR LIVEACT ON-CLASS-NC INFO DEFORMANCE-MONITOR LIVEACT NC NOT ACL-NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC	X ION-POLICY-ONIFIED ET ION-POLICY-ONIFIED POLICY-ONIFIED POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POL	Select Instructions Configure th Flow Configure th Flow Configure th Flow Configure th Gev Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Bevice Be	ct device iguration e type of flow you wi ation Table 144A emetb/0 emetb/1 emetb/1 emetb/1 emetb/1 emetb/1 emetb/1 emetb/1 emetb/2 pback0	the to receive from the Type Standard ~ Standard ~ Standard ~	W indivi IP Address D 198.19.1.1 Cre 198.19.1.1 Cre 100.64.1.2 Int 100.55.1.2 Int 100.52.1 Cre 198.19.2.1 Gre 100.64.2.2 Int 100.64.2.2 Int 100.52.1 Gre 100.52.1 Gre 100.55.1 Gre 100.55	dual CLI escription Tags T too IOS So too IOS So tsos IOS So	file.	Voice/Vide	Tradito.
4. Click I Autor Cli	estended LIVEACTION-ACL-NC By performance-enclose LIVEACT h-may LIVEACTION-ACL-NC h-may LIVEACTION-ACL-NC N-may LIVEACTION-ACL-NC NC NOT ACL-NC NC NOT ACL-NC NC NOT ACL-NC DEFORMANCE-MONITOR LIVEACT ON-CLASS-NC INFO DEFORMANCE-MONITOR LIVEACT NC NOT ACL-NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC	× 108-POLICY-SWIFIED ET 108-POLICY-SWIFIED put lIVEACTION-POLIC 109-POLICY-SWIFIED put lIVEACTION-POLIC 109-POLICY-SWIFIED 0	Select Flow Configure Configure th Flow Configure th Flow Configure Configure th Flow Configure Flow Configure Flow Configure Flow Configure Flow Configure Flow Configure Flow Configure th Flow Configure Flow Configure Fl	ct devic iguration e type of flow you wi ation Table intel0/0 emet0/1 emet0/1 emet0/2 pback0 244Y emet0/2 pback0	the to vie the to receive from the Type Standard ~ Standard ~	W indivi IP Address D 199.19.11 100.54.1.2 In 100.54.1.2 In 100.54.1.2 In 198.19.2.1 Gr 198.19.2.1 Gr 198.19.2.1 Gr 198.19.2.1 Gr 198.19.2.1 Gr 198.19.2.1 Gr 198.19.3.1 Gr 198.19.1 Gr 199.1 Gr 109.1	escription Tags Th co IOS So ts - ts - ts - ts - ts - ts - ts - ts	file.	Voice/Vide	Traditio
4. Click I Autor Cli	estended LIVEACTION-ACL-NC By performance-enclose LIVEACT h-may LIVEACTION-ACL-NC h-may LIVEACTION-ACL-NC N-may LIVEACTION-ACL-NC NC NOT ACL-NC NC NOT ACL-NC NC NOT ACL-NC DEFORMANCE-MONITOR LIVEACT ON-CLASS-NC INFO DEFORMANCE-MONITOR LIVEACT NC NOT ACL-NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC NC	X ION-POLICY-ONIFIED ET ION-POLICY-ONIFIED POLICY-ONIFIED POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POLICY-ONIFIED ION-POL	Select Instructions Configure th Flow Configure th Flow Configure th Flow Configure th Device Perice Perice S Branch S Eth S E	ct device iguration e type of flow you wi ston Table 114.A emet0/0 emet0/1 emet0/2 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 eme	eto vie sh to receive from the Type Standard v Standard v Standard v Standard v	W indivi IP Address D 198.19.1.1 Gr 198.19.1.1 Gr 198.19.1.1 Gr 198.19.2.1 Fr 198.19.2.1 Fr 198.19.2.1 Fr 100.64.2.2 M 100.255.1.2 M 100.255.2.2 M 100.255.2.2 M 100.255.2.3 M 198.18.1 Sending for	dual CLI escription Tags T too IOS So too IOS So tsos IOS So	file.	Voice/vide	Tradito.
4. Click I Mage CLI Vever: Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type Type T	estended LIVEACTION-ACL-NC ary = performance-ensitor IUVEACT h-may IUVEACTION-CLASS-MEDIAN -may IUVEACTION-CLASS-MEDIAN TOTO-CLASS-MEDIAN CONTINUE-CLASS-MEDIAN CONTINUE-CLASS-MEDIAN CONTINUE-CLASS-MEDIANET CONTINUE-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CON-CLASS-MEDIANET CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTINUE-CONTI	× 108-POLICY-SWIFIED ET 108-POLICY-SWIFIED put lIVEACTION-POLIC 109-POLICY-SWIFIED put lIVEACTION-POLIC 109-POLICY-SWIFIED 0	Select Instructions Configure th Flow Configure th Flow Configure th Flow Configure th Device Perice Perice S Branch S Eth S E	ct device iguration e type of flow you wi ation Table 1-LA emet0/0 emet0/1 emet0/2 pbok0 2-AW emet0/0 emet0/1 emet0/0 emet0/1 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0 emet0/0	to receive from the Type Standard ~ Standard ~ Standard ~	W indivi IP Address D 198.19.1.1 Cr 198.19.1.1 Cr 198.19.2.1 Cr 198.19.2.1 Cr 198.19.2.1 Cr 198.19.2.1 Cr 198.19.2.1 Cr 100.64.2.2 In 100.52.2 MF 100.64.2.2 In 100.52.1 Sending for 198.18.; Sori	escription Tags Th co IOS So ts - ts - ts - ts - ts - ts - ts - ts	file.	Voice/Vide	Traditio.

- 6. Click Save to Devices.
- 7. Click Close.

Note: If you get an error while saving to devices... simply click-thru. This is expected on certain versions of LiveNX Client.

Help

Save to Devices Preview CLI Revert Back Close

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



8. Click **Refresh** in the Filter Bar.

Lab 5.4: Delete Unused Interfaces

Remove any interfaces we don't need to collect data from.

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

Lab Steps:

1. Right-click on the HQ-SJ device and **select** Add or Remove Interfaces.



2. Deselect Loopback0.

dd/Edit Interfaces for Cisco Steps	- HQ-SJ.dcloud.cisco.com (198.1) Select Interfaces	8.129.25)		
Select Interfaces Select VLANs	Select the interfaces you want to r	monitor on this de	evice (maximum 100	00 interfaces).
 Select Features Enable Polling Review Configuration Device Updated 	Selected Interface	Trunk	IP Address 198.18.129.25 10.255.0.2 10.0.0.102	Description
	Selected interface(s): 2			F.
	< Back Next > Fi	nish		Cancel Help

3. Select Next until the Device Updated window is displayed.

4. Select Finish to update the device.

Notice that the device now has 2 active interfaces, represented by Gi1 and Gi2



5. Repeat from Lab Step 1 above to perform the same interface removal on Branch1-LA and Branch2-NY (as needed).

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

Lab 5.5: Merge Clouds in Topology

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



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

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

Lab Steps:

1. Right-click on the HQ-SJ Device's Gi2 10.255.0.0/24 network cloud, and select Merge Clouds.



2. On the Create Network Object dialog enter a Name of **WAN**.

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

3. Select "Find" to add more networks.

Name * WAN	
Type * Merged clouds	
	clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge ame flows traversing those clouds are connected via the merged cloud network object.
Clouds *	Click on clouds in the topology
10.255.0.0/24	
	Find
Click on clouds in the topology, or u: 192.168.0.0/24).	se the "Find" button, or type in space separated subnets using CIDR notation (e.g.,
192.168.0.0/24).	se the "Find" button, or type in space separated subnets using CIDR notation (e.g.,
192.168.0.0/24).	
192.168.0.0/24).	
192.168.0.0/24). ext/Shape Network Cloud (blue) Size	
192.168.0.0/24).	

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

	ouds to be me	
	_	10.0.0.102/32
		10.0.1.1/32
	~	10.255.0.0/24
-	▼ ▼	10.255.1.0/24
	- -	10.255.2.0/24
		100.64.1.0/24
Í		100.64.2.0/24
j		198.18.128.0/18
ĺ		198.19.1.0/24
		198.19.2.0/24

- 5. Click OK.
- 6. Enter a Name of WAN.

7. Click OK to finish.

Type * Merged clouds A merged clouds A merged clouds where the same flows traversing those clouds are connected via the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud serves as a bridge locuds * Click on clouds in the topology Clouds * Click on clouds in the topology Find Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24). Clouds * Cloud * Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).	Name *	WAN		
A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud network object. Clouds * Clouds * Clouds * Click on clouds in the topology Find Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.158.0.0/24). Clouds * Clouds * Clouds * Clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.158.0.0/24). Clouds * Cloud				
		A merged cloud replaces the member clouds in the	topology with a single object. When used with flows, the merged cloud serves as a bridg sversing those clouds are connected via the merged cloud network object.	e
Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).		Clouds *	Click on clouds in the topology	
192.168.0.0/24). std std				1
size		192.168.0.0/24).	button, or type in space separated subnets using CIDR notation (e.g.,	
	Size			

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.

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



Lab 6

Lab 6: Making the Topology Work

Lab 6.1: Setting Device Semantics

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

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

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

Lab Steps:

1. Select Expand to set semantics for devices.



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

198.18.133.34 - Remote Des	top Connection							_
LiveAction - localhost								_
File View Users QoS Flow	Routing IP SLA LAN	Tools Report	s Window Dev	Help				
Dashboard Manage 🔣 Collapse								Details
Q.								CPU and Memory Usage
Name	IP Address	Node	Label	Capacity	WAN Service Provi	Site	Site IP	CPU
∃ 💩 Home	100.10.1.1	h and						
Branch1-LA Branch1-LA Sthernet0/0	198.19.1.1 198.19.1.1	Local						Memory
Ethernet0/2	10.255.1.2		LA	1.5 Mbps	v			123MB of
- Branch2-NY	198.19.2.1	Local		101000				Device Details
🗧 🤤 Ethernet0/0	198.19.2.1							Device name
- 🤪 Ethernet0/2	10.255.2.2		NY	1.5 Mbps	▼			Branch1-LA.dcloud.cisco.com
🖻 🌐 HQ-SJ	198.18.129.25	Local						Branch1-EA.0clood.csco.com
\ominus 😌 Ethernet0/0	198.18.129.25							Serial number
- 😌 Ethernet0/1	10.255.0.2		53	1.5 Mbps	V			101
								IP address
								198.19.1.1
								Description
								Cisco IOS Software, Linux Software
								(I86BI_LINUX-ADVENTERPRISEK9-M),
								Experimental Version
								15.4(20140912:223819)
								[jesswan2-liveaction 103]
								Model
								ciscoGatewayServer
								IOS version
								15.40
								Location
								1
								Site
								Site
								IP I
								Enter IP address ranges in CIDR
								Remove unused sites
								Tags
								Enter tag here then press ENTER to
								√ Tag

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.

To tag an interface

- Branch1-LA Interface GigabitEthernet3 Label Interface as LA, give Capacity of 1500 Kbps and select WAN
- Branch2-NY Interface GigabitEthernet3 Label Interface as NY, give Capacity of 1500 Kbps and select WAN
- HQ-SJ Interface GigabitEthernet1 Label Interface as SJ, give Capacity of 1500 Kbps and select WAN

🗛 LiveAction - localhost					
File View Users QoS Flow	Routing IP SLA LAN	Tools Report	s Window Dev Help		
Dashboard Manage 🔣 Collapse					
Q					
Name	IP Address	Node	Label	Capacity	WAN Service Pro
∃~💸 Home					
🗖 💮 Branch1-LA	198.19.1.1	Local			
- 😌 Ethernet0/0	198.19.1.1				
🎯 Ethernet0/2	10.255.1.2		LA	1.5 Mbps	\checkmark
🚊 🛞 Branch2-NY	198.19.2.1	Local			
- 😌 Ethernet0/0	198.19.2.1				
😌 Ethernet0/2	10.255.2.2		NY	1.5 Mbps	\checkmark
🗄 🛞 HQ-SJ	198.18.129.25	Local			
- 😔 Ethernet0/0	198.18.129.25				
😌 Ethernet0/1	10.255.0.2		SJ	1.5 Mbps	

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.

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

Name IP Address Node Label Capacity WAN Service Prov Site Site IP CPU ● BranchIAA 198.19.1.1 Local IA 1.5 Mbps IA Memory Memory <th>-</th>	-
Hone Image: Product IA 198,191.1 Image: Product IA Image: Produc	
Branch14A 198.19.1.1 Local ● Ethernet00 198.19.1.1 Local ● Ethernet010 198.19.2.1 Local ● Ethernet010 198.19.2.1 Local ● Ethernet010 198.19.2.1 Local ● Ethernet010 198.19.2.2 NY ● Ethernet010 198.18.122.55 Local ● Ethernet010 198.18.122.55 Local ● Ethernet010 198.18.122.55 Sarial number ● Ethernet011 10.255.0.2 53 ● Ethernet011 10.255.0.2 53 ● Ethernet011 10.255.0.2 53 ● Ethernet011 10.255.0.2 53	
● Ethernet0/0 198.19.1.1 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	
■ Ethernet0/2 10.255.1.2 LA 1.5 Mbps ✓ ■ Ethernet0/2 10.255.1.2 Local Image: Construction of the state of t	
Bendrot2vW 198.19.2.1 Local Device Details Device Details Device name Device name Bethernet0/2 10.255.2.2 NV 1.5 Mbps Image: Standard Sta	
● Ethernet0(0 196.19.2.1 NY 1.5 Mpps Image: Construction of the second of the	
Chemetol/2 10.255.2 NV 1.5 Mbps S NV 1.5 Mbps S NV 1.5 Mbps S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S	
B (C-3) 199.18.129.25 Local I Construction of the second seco	
Ethernet0/0 198.18.129.25 Ethernet0/1 10.255.0.2 50 1.5 Mpps Select each device individually and	isco.com
Ethernet0/1 10.255.0.2 5J 1.5 Mbps V Select each device individually and	
Select each device individually and	
Select each device individually and	
Select each device individually and	
Select each device Cisco to 5 strues / Cisco t	
individually and	
individually and	Linux Software
give them each a	
IOS version	
15.4()	
Location	
	N N
NA STATES AND A STATE AND A STATES AND A STA	6
St.	6
State	-13
	1 3

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

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



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

Site	WAN In	ter	face Utilizatio	n								
s	Site	extstyle 1	Label	Capacity (Kbps)	Inj	out Avg	In	put Peak	Outp	ut Avg	Output	t Peak
LA			LA	1,500		57 %		65 %		72 %		76 %
NY			NY	1,500		22 %		24 %		17 %		19 9
SJ			SJ	1,500		89 %		93 %		79 %		88 9

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

Notice the Flow Source is set as "wan". 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.

000				LiveAction Training S	essions		10
A Dashboard	_						
System Application Q		IOW IP SLA	WAN-PfR				
Main	*						
	^	Flow Ale	rts - 24 Hou	rs			
Alerts							
Reports		1					
		÷					
Setup	*	E I					
Discover Devices		Alert Count		There is no data	to display for the given time p	eriod	<u>।</u> । । । । । । । ।
Manage Devices		lert					
Define Sites		⊲.					
Configure Alerts							
-		0					
Configure Flow	_ L		_				- -
		Flow source wan		k			
				~			
Application	*						
Application Performance		Basic Flo	w				12/02/
Manage Application Groups							
		Top 10 Sou	urce Addresse	s Bytes 💌		Top 10 Destination Addre	sses Bytes 💌
		Sr	c IP Addr	Bytes V1	Flows	Dst IP Addr	Bytes
		198.19.1.10		65 MB	214	198.18.133.36	
		198.18.133.		47 MB	586	198.19.1.101	
		198.19.2.10		19 MB	618	198.19.1.81	
		H 198, 19, 1.80		18 MB	111	198.19.1.80	
		198.18.128.		18 MB	111	198.19.2.82	
		198.18.128.		18 MB	112	198.18.128.81	
		198.18.128.		18 MB	112	198.18.128.80	
		198.19.1.81		18 MB	110	198.19.2.102	
		198.18.128.	.88	6 MB	15	198.19.2.88	
	L	198.19.1.84	ł	6 MB	15	198.19.1.84	
		1				1	

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

Lab 6.2: Adding Devices to Groups

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

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

Lab Steps:

1. Open the Device Management window by selecting Manage.

0	0				
A Live	Actio	on - loca	alhost		
File V	iew	Users	QoS	Flow	Ro
Dashboa	ard	Manage	Ex	pand	
Q-	_				
		Na	ame	73	
🗉 🚫 H	lome				

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.

- A Device Management Filter by: Filter Clear Select Device Name IP Address Vendor Model Node Group Poll QoS Flow IP SLA Routing LAN* Interval Status 1 minute Configured Branch1-LA 198.19.1.1 Cisco ciscoGatewaySe... Local 5 ~ 198.19.1.1 Cisco ciscoGatewaySe... Local 198.19.2.1 Cisco ciscoGatewaySe... Local **V** Branch2-NY \checkmark \checkmark \checkmark \checkmark 198.18.129.25 Cisco ~ • • • ☑ 1 minute 💌 Configured HO-SJ ciscoGatewaySe... Local * LAN polling occurs every 15 minutes Number of Devices: 3 Device Configurations Global Device Settings Configure QoS, Flow, and IP SLA Select devices in the table and click the configure button. Edit Default SNMP Settings Clear Remove Remove selected device(s). Edit Clear <New Group> Default CLI Monitoring Settings - Not Set Removes selected devices from their groups Edit Default CLI Configuration Settings Clear Edit Groups Edit the groups Apply Close
- 2. Select "Edit Groups"

х

3. Click Add

A Edit Groups			×
Groups			
Name		Size	Add
			Edit
			Remove
	1		
New and modified group entries have a (*).			
		ОК	Cancel

- 4. Enter SJ in the Name field.
- 5. Select HQ-SJ from the All Other Devices list and click the right arrow.
- 6. Click Add, repeat the steps above to create Groups for LA and NY.

Add Group				×
Name (*)				
Description				
All Other Devices	_		up of Devices —	
Q,	Θ	Q-		
(LA) Branch1-LA (NY) Branch2-NY	Ð	HQ-SJ		
		Add	Done	Cancel

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

Once completed your groups should look like the one below.

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

٨	Edit Groups			×
Gro	oups			
	Name	Δ	Size	Add
*	LA	1		Edit
*	NY SJ	1		
	21	1		Remove
			N	
			2	
Net	w and modified group entries have a (*).		
			ок	Cancel
		_		

9. Double-click on the group to expand.



Lab 6.3: Creating Network Objects

Network objects can be used to better visualize and understand how traffic traverses the topology. LiveNX allows you to assign various icons to flow end-points, 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 a number of specific flows and assign appropriate end-point objects.

Lab Steps:

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



- 6. Select an Object/Shape as either"PC" or "Laptop".
- 7. Click OK.

Name *	MediaServer(SEC)
Type *	IP address end point
	Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merged cloud order for flows to be drawn to the network object.
	IP Address *
	192.168.12.3
	Type in an IP address, or select a device interface or IP address end point in the topology.
ject/Shape	Laptop v
ect/Shape Size	File Server
	File Server

8. Click Refresh.

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



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

- 9. Enter the search string: flow.srcip=198.19.2.102
- 10. Select the flow (it will be near the NY device), right click on the IP Address endpoint.
- 11. Select Create Network Object
- 12. Select an Object/Shape as "File Server".
- 13. Click OK.
| A Edit Netw | ork Object X |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name * | 198. 19.2. 102 |
| Type * | IP address end point v |
| | Represents an IP end point in the topology. The IP end point must be connected to/associated with an interface, subnet, or merged doud in order for flows to be drawn to the network object. |
| | IP Address * |
| | 198.19.2.102 |
| | Type in an IP address, or select a device interface or IP address end point in the topology. |
| Object/Shape | File Server 🗸 |
| Size | - |
| Tooltip | |
| * Required Fie | Id OK Cancel |

- 14. Enter the search string: flow.srcip=198.18.133.36
- 15. Select the flow (it will be near the SJ HQ device), right click on the IP Address endpoint.
- 16. Select Create Network Object.
- 17. Select an Object/Shape as "Laptop".
- 18. Click OK.
- 19. Click Refresh.

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



Note: It is always good practice to save your 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**.

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 Interfaces

Lab 7

Lab 7: Console Dashboard & Reports

Lab 7.1: The Client Dashboard

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

Note: Since the System Dashboard's default time interval is 24 hours, you may not see a lot of detail. Zoom-in to see more granular data.

Lab Steps:

	+	A Dashboard	2000		le vere	in the second second	1	1				- 0
	Sea	System Application QoS	Flow ID CI A	WAN-DED								
	10	Main (\$)										
h1-LA h2-NY		Alerts	System /	Alerts - 24 Hou	rs					-		
3			7									Count
		Reports	6							Int Int	terface Up/Down	1,065
			5 s							Flo	N	9
		Setup (R)	84	_						Ro	uting	0
		Discover Devices	1 3				11.111	11111111			6 9 A	0
		Manage Devices	Ale							De De	vice Config Change a	0
		Define Sites								De	vice Up/Down	0
		Configure Alerts								⊠ let	vice CPU/Memory terface Rate	0
		Congue Mers	May 13, 12:00 I	PM May 13.04	100 PM May 13.0	8:00 PM May 14, 12:00 AM	May 1-	14. D4:00 AM	May 14, 08:00 AM			
		Site									10.00	
		Site WAN Interface Utilization									150	n 30m 1hr 4hr
		and most and not outstand	System S	status						05/14/16	, 11:30:00 AM to 05/	14/16, 11:45:00 AM
								52.7 88586				
		Open at startup	Top 10 CP				_	Top 10 Memor	ry Usage			
			Device	A	vo	∽ ¹ Peak		Device	Avg		~1 Peak	
			Branch1-LA HQ-5J			0 %		HQ-63			37 %	38 %
			Branch2-NY			0.96		Branch1-LA Branch2-NY			36 % 35 %	36 % 35 %
			Branch2-NY					Branch2+Hf				
			Branch2-Nr Top 10 Int	erface Bandwidth		0 %	0 %	Branch24ff Top 10 Interfa	ace Drops Output Dro		35 %	35 %
			Branch2+W Top 10 Int	Device	Output BW (Kops) 🤟 Description	0 %	0%	Branch244f Top 10 Interfa	Device	Description		35 %
			Branch2+W Top 10 Int Interface Ethernet0,0	Device HQ-63		0 %	0 %	Branch244f Top 10 Interfa Interface Ethernet0j0	Device Branch1-LA	Description Branch1 LAN	35 %	35 %
			Branch2497 Top 10 Int Interface Ethernet0/0 Ethernet0/2	Device HQ-6J HQ-5J Branch14LA	Description	0 %	0 % ~ 1 1,400 1,250 1,293	Branch24ff Top 10 Interfa Interface Ethernet0/0 Ethernet0/1 Ethernet0/2	Device Branch14A Branch14A Branch14A	Description	35 %	35 %
			Top 10 Int Interface Ethernet0/0 Ethernet0/2 Ethernet0/2	Device HQ-SJ HQ-SJ Branch14A Branch14A	Description MPLS Branch1 LAN	0 %	0 % ~1 1,400 1,250 1,093 849	Branch24H Top 10 Interfa Interface Ethernet()0 Ethernet()1 Ethernet()2	Device Branch1-LA Branch1-LA Branch1-LA HQ-53	Description Branch1 LAN Internet	35 %	35 % Output Drop ~1 0 0 0 0 0 0
r			Branch2497 Top 10 Int Interface Ethernet0/0 Ethernet0/2	Device HQ-6J HQ-5J Branch14LA	Description MPLS Branch1 LAN Branch2 LAN	0 %	0 % 0 %	Branch24ff Top 10 Interfa Interface Ethernet0/0 Ethernet0/1 Ethernet0/2	Device Branch14A Branch14A Branch14A	Description Branch1 LAN Internet MPLS	35 %	35 %
ſ	Col		Branch2-W Top 10 Int Interface Ethernet0,0 Ethernet0,2 Ethernet0,2 Ethernet0,2 Ethernet0,1	Device HQ-5J Branch 14A Branch 14A Branch 2407 Branch 2407 Branch 2407 Branch 14A	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet	0 % Input BW (10pp) 1,000 1,000 650 1,003 100 100 100 100 100 100 100	0 % 1,400 1,250 1,093 849 352 270 <1	Branch24H Top 10 Interfac Interface Ethernet()1 Ethernet()2 Ethernet()2 Ethernet()2 Ethernet()2 Ethernet()3 Ethernet()3	Device Branch1-LA Branch1-LA Branch1-LA HQ-53 HQ-53 Branch2-NY Branch2-NY	Description Branch1 LAN Internet MPLS Branch2 LAN Internet	35 %	35 % Output Drop ~1 0 0 0 0 0 0 0 0 0 0 0
[Co		Branch2-W Top 10 Int Interface Ethernet0/1 Ethernet0/0 Ethernet0/0 Ethernet0/2	Device HQ-53 HQ-53 Branch14A Branch14A Branch12407 Branch2407	Description MPLS Branch1 LAN Branch2 LAN MPLS	0 %	0 % 1,400 1,250 1,093 849 352 270 <1	Branch24W Top 10 Interfa Interface Ethernet0/1 Ethernet0/2 Ethernet0/2 Ethernet0/2 Ethernet0/1 Ethernet0/1	Device Branch14A Branch14A HQ-53 HQ-53 Branch24Y	Description Branch1 LAN Internet MPLS Branch2 LAN	35 %	35 % Output Drop V1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Co		Branch2-W Top 10 Int Interface Ethernet0,0 Ethernet0,2 Ethernet0,2 Ethernet0,2 Ethernet0,1	Device HQ-5J Branch 14A Branch 14A Branch 2407 Branch 2407 Branch 2407 Branch 14A	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet	0 % Input BW (10pp) 1,000 1,000 650 1,003 100 100 100 100 100 100 100	0 % 1,400 1,250 1,093 849 352 270 <1	Branch24H Top 10 Interfac Interface Ethernet()1 Ethernet()2 Ethernet()2 Ethernet()2 Ethernet()2 Ethernet()3 Ethernet()3	Device Branch1-LA Branch1-LA Branch1-LA HQ-53 HQ-53 Branch2-NY Branch2-NY	Description Branch1 LAN Internet MPLS Branch2 LAN Internet	35 %	35 % Output Drop V1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Co		Branch2-NY Top 10 Int Interface Effermet0/0 Effermet0/2 Effermet0/2 Effermet0/1 Effermet0/1 Effermet0/1	Device HQ-5J HQ-5J Branch14A Branch14A Branch14A Branch2407 Branch2407	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet Internet	0 % Input BW (10pp) 1,000 1,000 650 1,003 100 100 100 100 100 100 100	0 % 1,400 1,250 1,093 849 352 270 <1	Branch24H Top 10 Interfa Interface Ethernet()1 Ethernet()2 Ethernet()2 Ethernet()2 Ethernet()3 Ethernet()4 Ethernet()4	Device Branch1-LA Branch1-LA Branch1-LA HQ-53 HQ-53 Branch2-NY Branch2-NY	Description Branch1 LAN Internet MPLS Branch2 LAN Internet	35 %	35 % Output Drop V1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
ſ	Col		branch24V Top 10 Int Interface Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I	Device HQ-6J HQ-6J Branch14A Branch14A Branch240 Branch240 Branch240 Branch240	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet Internet	0 %	0 % 1,400 1,250 399 220 <1 <1	Bandi-24/f Top 10 Interface Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit()	Device Branch14A Branch14A Branch14A HQS3 Branch24Y Branch24Y Branch24Y	Description Branch1 LAN Internet MPLS Branch2 LAN Internet MPLS	J5 %	35 % Output Drop
	Col		Branch2-NY Top 10 Int Interface Effermet0/0 Effermet0/2 Effermet0/2 Effermet0/1 Effermet0/1 Effermet0/1	Device HQ-5J HQ-5J Branch14A Branch14A Branch14A Branch2407 Branch2407	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet Internet	0 %	0 % 1,400 1,250 1,093 849 352 270 <1	Bandi-24/f Top 10 Interface Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit()	Device Branch14A Branch14A Branch14A HQS3 Branch24Y Branch24Y Branch24Y	Description Branch1 LAN Internet MPLS Branch2 LAN Internet	35 %	35 % Output Drop V1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		New Polleg Dasklef Icon	branch24V Top 10 Int Interface Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I Ethernell/I	Device HQ-6J HQ-6J Branch14A Branch14A Branch240 Branch240 Branch240 Branch240	Description MPLS Branch1 LAN Branch2 LAN MPLS Internet Internet	0 %	0 % 1,400 1,250 399 220 <1 <1	Bandi-24/f Top 10 Interface Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit() Eterretit()	Device Branch14A Branch14A Branch14A HQS3 Branch24Y Branch24Y Branch24Y	Description Branch1 LAN Internet MPLS Branch2 LAN Internet MPLS	J5 %	35 % Output Drop

1. Click the Dashboard tab (above the Home Tree-view).

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 Interface Up/Down.
- 3. Left-click-Drag to Zoom into a flow of interest.



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

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



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



5. Click the Alert Type column header to re-sort.

16/05/13 01:35:31 PM 16/05/13 05:49:30 PM 16/05/13 08:44:30 PM 16/05/13 09:04:02 PM	Warning		Group	Alert Type	^1 Details
16/05/13 08:44:30 PM		HQ-SJ	Flow	High media packet loss (percent High media packet loss percent
1.1	Warning	HQ-SJ	Flc Open Report	packet loss p	percent High media packet loss percent
16/05/13 00:04:02 PM	Warning	HQ-SJ	Flo Drill Down on	Specific Flow > Ton	Analysis Report
10/05/15 05:04:02 144	Warning	HQ-SJ	Flo	Тор	Analysis Report
16/05/13 11:01:01 PM	Warning	HQ-SJ	Flc Export Data		Conversations Report
16/05/13 01:35:02 PM	Warning	Branch 1-LA	Flow	High media (Bidir	ectional Source/Destination Pair Report
16/05/13 05:49:30 PM	Warning	Branch1-LA	Flow	High media (· · · · ·
16/05/13 09:04:02 PM	Warning	Branch 1-LA	Flow	right include	ce or Destination Address Report
16/05/13 11:01:01 PM	Warning	Branch 1-LA	Flow		ress Pair Report
16/05/13 01:00:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface er Dest	ination Address Report
16/05/13 01:01:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface er	•
16/05/13 01:06:06 PM	Warning	HQ-SJ	Interface Up/Down	To be from a	ce Address Report
16/05/13 01:07:06 PM	Warning	HQ-SJ	Interface Up/Down Interface Up/Down	Interface er Dest Interface er	ination Address Popularity Report
16/05/13 01:11:36 PM 16/05/13 01:12:06 PM	Warning Warning	HQ-SJ HQ-SJ	Interface Up/Down		ce Address Popularity Report
16/05/13 01:12:06 PM	Warning	HQ-SJ HQ-SJ	Interface Up/Down	THE ACE E	Traffic Report
16/05/13 01:17:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface or	· · · · · · · · · · · · · · · · · · ·
16/05/13 01:22:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface er Dest	ination Site Traffic Report
	-				ce Site Traffic Report
		•		Interface error	Interface name - Ethernet0/0;
16/05/13 01:27:35 PM	Warning	HO-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1;
16/05/13 01:33:06 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0;
16/05/13 01:33:35 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1;
16/05/13 01:38:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/0;
16/05/13 01:38:36 PM	Warning	HQ-SJ	Interface Up/Down	Interface error	Interface name - Ethernet0/1;
16/05/13 01:22:06 PM 16/05/13 01:27:35 PM 16/05/13 01:27:35 PM 16/05/13 01:33:06 PM 16/05/13 01:33:35 PM 16/05/13 01:38:36 PM	Warning Warning Warning Warning Warning Warning	HQ-SJ HQ-SJ HQ-SJ HQ-SJ HQ-SJ HQ-SJ	Interface Up/Down Interface Up/Down Interface Up/Down Interface Up/Down Interface Up/Down Interface Up/Down	Interface er Sour Interface error Interface error Interface error Interface error Interface error	Interface name - Ethernet0/0 Interface name - Ethernet0/1 Interface name - Ethernet0/0 Interface name - Ethernet0/1 Interface name - Ethernet0/0

6. Right-click a Flow alert and select Drill Down... and Top Analysis Report.

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.

be here to filter reports.	Top Analysis											
orts Interface Bandwidth Top Analysis IPs and Ports	Тор А	nalysi	is	£					:	15m 1h 6h	1d 1w 30d 🕻	Custom
Address Applications	05/3	13/16, 01:05	5:31 PM to 05/	13/16, 02:05:3	31 PM			Exec	ute Report			
QoS	Source HQ-	SJ		~	All Interface	es	~	Numbe	er of flows	: 1	CSV F	ile Resul
Network Medianet	Filter *De	faultFilterGroup) v 🤜	Inbound	~			Median	et ·	Time Sorted	- Unique Flows 🗸	
Applications (AVC)	Sauth 4100 B	flow most era - 200	0.4.8 flow port dat-7	10004 & Rew dam - PE	. Rew direction -Thic	DECC & flow mode	mat avant-0.5 flave	redianet.eventStop=0 & flor		nilerEurolError - 67	242745000227222	?
NSEL PfR	Search COP &	now.port.src=200	or a now.port.ost=2	0004 a now.uscp=be	a now.urectorr=146	RESS & NOW THEUR	anet.event=0 & now.n	regianet.eventstop=0 & no	wimedianecimo		20427409993272320	
Wireless AnyConnect										Q,-		
Miscellaneous	Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co Sr	rc Country	Dst Country	RTP SSRC	Dire
tom Reports	May 13, 2016 1:3.	UDP	198.19.1.81	20,004	198.18.128.81	20,004	rф	1 -		-	2432754705	INGR
rt Actions												
rt Actions												
As												
As												
As												
As te												
As te												

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

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

Lab 7.2: Viewing Console Reports

We'll run 3 of the most commonly 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. Select Reports > Flow from the top Menu Bar.
- 2. Select the Inbound and Outbound Combined filter.
- 3. Click Execute Report.



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 time span of the report, the number of flows, or discrete data points, the report displays, and the time-series chart above the Classes Table.

- 4. Click the 6h time setting at the top-right. (we do this in the lab to get more flows)
- 5. Click Execute Report.

Did you notice the report took longer to run this time? Depending on the amount of flows across YOUR production network... report execution will get longer in direct proportion to the time setting. In some cases it may take up to 10 minutes to run the report!

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. On the report menu, open the Address category and right-click Top Conversations, and click **New Report**.
- 2. Click the 6h time setting at the top-right.
- 3. Click Execute Report.

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



This report shows the top conversations in the selected time period including; Source address, Destination address, total flows, etc... a good way to see who is using the bandwidth, and what for... All that Bittorrent may not be good for business! Right-clicking to open a New Report leaves the prior reports open, in a tabbed manner, for comparison purposes.

Flow Identification

- 1. On the report menu, open the QoS category, right-click **DSCP**, and click New Report.
- 2. Click the 6h time setting at the top-right.
- 3. Click Execute Report.

Q. Type here to filter reports.	Application x Top Conversations x DSCP x	
-Reports Interface Bandwidth Top Analysis IPs and Ports	DSCP	15m 1h 6h 1d 1w 30d Custom
-Top Conversations	05/15/16, 03:52:59 PM to 05/15/16, 04:07:59 PM Data bin: 1 minute	Execute Report
-Bidirectional Source/E	Source All Devices V All Interfaces	✓ Number of flows: 44,299 Utilize Long Term Cache
	Filter *DefaultFilterGroup 🗸 🐺 Outbound 🗸	Graph Basic Flow V Time Series V Bit Rate V
	Search Example: (site = Honolulu site = Chicago) & wan & flow.app = webex-meeting	× • ?

LiveAction Lab Workbook Pt. 1

ort Actions	Nur	mber of datasets: 8						Q	
e		DSCP	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
e As		0 (BE)	40,832		16,556,237	49 Mbps	18396 pps	49.8 Mbps	
AS			366	250 MB	1,604,622	2 Mbps	1783 pps	2.3 Mbps	1833 p
te		26 (AF31)	131		460,629	291 Kbps	512 pps	344.9 Kbps	607 p
		34 (AF41)	230	27 MB	40,823	240 Kbps	45 pps	301.4 Kbps	56 ;
		8 (CS1)	197	17 MB	118,117	147 Kbps	131 pps	163.5 Kbps	144 (
		48 (CS6)	125	6 MB	28,982	51 Kbps	32 pps	53.2 Kbps	33 (
		16 (CS2)	2,368	979 KB	2,368	9 Kbps	3 pps	9.6 Kbps	2 (
ule		40 (CS5)	50	24 KB	265	217 bps	0 pps	272 bps	0 p
rt to CSV									

See that the majority of the discovered traffic is marked as 0 (BE). This means that this traffic has not been recognized as a certain type by the router and it will use its BEST EFFORT to rout it. This may be a candidate for marking so that QoS may use priority routing.

Bandwidth by Flow Type

- 1. On the report menu, open the Network category, click **Interface Bandwidth Summary**.
- 2. Enter a Search String: wan & flow.dscp=EF (note upper-case).
- 3. Click the 6h time setting at the top-right.
- 4. Select SJ HQ device.
- 5. Click Execute Report.



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

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

Lab 7.3: Create a Custom Report

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

Lab Steps:

- 1. On the report menu, in the bottom-left Report Actions pane, click Create.
- 2. Enter a Report Name.
- 3. Select the Fields as indicated in the diagram, below.

Rep	ort: M	y IPs & Port	ts Report										
Aggregat	ed: By	rte/Packet	Statisti	cs									
Ту	be: Bi	asic Flow	~										
Directio	on: Ir	nbound and	Outbour	d Combine	d ~								
eys													
Q-													
Selected	N	ame	Field	Name	Search S	trina	Fie	ld ID (v9)	IPF		PE	N	
	Pre	otocol	proto	colIdenti			4		4	- 1	0		_
		C DSCP		sOfServ	and the second sec		5		5		0		
	Sre	c Port	1.0	eTransp			7		7		0		
	Sre	c IP Addr		eIPv4Ad	the state of the s		8		8		0		
	Sre	Prefix Len	sourc	eIPv4Pr	flow.mask	.src	9		9		0		
	In	IF	ingres	sInterface	flow.ifidx.	in	10		10		0		
	Ds	t Port	destin	ationTr	flow.port.	dst	11		11		0		
	Ds	t IP Addr	destin	ationIP	flow.ip.ds	t	12		12		0		
	Ds	t Prefix Len	destin	ationIP	flow.mask	.dst	13		13		0		
	OL	ut IF	egres	sInterface	flow.ifidx.	out	14		14		0		
	Ne	ext Hop IP .	ipNex	tHopIPv	flow.ip.ne	xtHop	15		15		0		
	Sre	c AS	bgpSo	ourceAs	flow.as.sr	c	16		16		0		
		t AS		estinatio			17		17		0		
	BG	P Next Hop	bgpN	extHopI	flow.bgpN	lext	18		18		0		
review													
Rearrange b	y dragg	ing the hea	dings bel	ow.									
Protocol S	irc D	Src Port	Src I	In IF	Appli	Src C		Src Site	Tot	Tot	Tot	Av	Av

- 4. Click Create.
- 5. Select SJ HQ device.
- 6. Click the 6h time setting at the top-right.
- 7. Click Execute Report.

You now have a report which, at-a-glance, shows all the flows that are using Best Effort. Now you go mark these flow for priority processing as part of your production QoS Policy!

Lab 8

Lab 8: QoS

Lab 8.1: QoS Marking Policy

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

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

Lab Steps:

- 1. Right click on the "Branch1-LA" device.
- 2. Highlight QoS, and select Manage QoS Settings.



3. Click the Add Policy Icon.



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

	Add Policy	×
Policy nar	ne: DSCPMARK	
	ОК	Cancel

5. Right Click on your new "DSCPMARK" policy and select "Add Class to Policy"

Δ	Manage QoS Settings - Bra
 Policies Classes Interfaces 	
Policies	Mapped Classes
Copy Po WhyIsThis Delete P	plicy
Add Class Image: Apply P	Add Class to Policy Policy from Interface

- 6. Select "Create a new class" and give the class a name RTP.
- 7. Click OK

	Add Class t	o Policy		×				
Select one of the following options:								
O Use existing	dass: 4C_BL_Critic	alData_App-Mat	ch_Mark	¥				
Oreate new	class: RTP							
	ption will create an er Class tab* to add class							
		OK	Cancel					

8. Select "Add Class to Policy"



- 9. Click Create new class, Label it SIP.
- 10. Click OK.

	Add Class to Policy	×
Select one of the follow	ing options:	
O Use existing class:	4C_BL_CriticalData_App-Match_Mark	¥
Oreate new class:	SIP	
	ill create an empty class. You will need to b" to add classification parameters.	
	OK Cance	1

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

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

	anage QoS Sett	ings - E	Branch1	-LA.dclou	d.ci
2 2 2 2 2 2 3 6 5	•				
Policies Classes Interfaces					
Policies	Mapped Classes	;			
📑 🖷 🖀 🛼 🐂 🐃	🖳 🛐 📑	}			
DSCPMARK	Class Name	Classify	Marking	Queueing	Pol
	RTP	•			
default	SIP				
WhyIsThisHere	class-default	•			
					_
	Mapped Class D				
	Drop all traff	fic for clas	SS		
	Classify Mark	ing Que	ueing Pol	icing Shapir	ng (
	Match on: Any				

Select and match the SIP class...

- 1. Select the SIP Class.
- 2. Select ACL Name as Match Type.
- 3. Select the SIPQoSMark ACL you created.
- 4. Select Add Match Statement.

Manag	ge QoS Settings - Branch1-LA.dcloud.cisco.cor	m (198.19.1.1)	×
4 4 2 2 2 4 5			
Policies Classes Interfaces			
Classes Create and	tch Statements		
A taken type:	ACL Name	Match any 🗸 🗱	
4C_BL_CriticalDat			
4C_BL_Realtime_A Value: 4C_BL_Scavenger	CRITICAL A DENY_GLOBAL_LEARN_LIST	Man Materian Value	
4C-MN_CONTROL	RDP	Ma ACL Name SIPQoSMark	
4C-MN_CRITICAL	RTPACL		
4C-MN_REA	RTPQoSMark SIPQoS		
	SIPQoSMark		
SIP	VOICE_VIDEO V		
Match/match not:	Match 🗸		
	Add Match Statement Replace Match Statement]	

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

- 1. Select the RTP Class.
- 2. Select ACL Name as Match Type.
- 3. Select the RTPQoSMark ACL you created.
- 4. Select Add Match Statement.

A Manag	e QoS Settings - Branch1-LA.dcloud.cisco.cor	n (198.19.1.1)	×
4 4 2 2 2 2			
Policies Classes Interfaces			
Classes Create and E	ch Statements		
Match type:	ACL Name 🗸	Match any 🗸 🐹	
4C_BL_CriticalDat 4C_BL_Realtime_A Value:	CRITICAL	M Match T Value	
4C_BL_Scavenger	DENY_GLOBAL_LEARN_LIST	Ma ACL Name RTPQoSMark	
4C-MN_CONTROL	RDP		
4C-MN_CRITICAL	RTPACL		
	RTPQoSMark SIPQoS		
	SIPQoSMark		
SIP	VOICE_VIDEO V		
Match/match.pot:	Matal		
Match/match.	Match V		
4	Add Match Statement Replace Match Statement		

- 1. Select the Policies Tab.
- 2. Select the RTP Class.
- 3. Select the Marking Tab
- 4. Choose to mark the RTP Traffic with DSCP 46 (EF).

M	anage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)
Policie usses Interfaces	
Policies	Mapped Classes
DSCPMAP SIP dass-default WhyIsThisHere dass-default	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown RTP Image: DSCP: EF Image: DSCP: DSCP: EF Image: DSCP: DSCP: EF
	Mapped Class Detail Drop all traft 3 iss Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported Mark with: Mark with: PoscP 46 (EF) IPv4 Only ATM Cell Loss Priority Frame Relay Discard Eligible Frame Relay Discard Eligible Precedence: sets the precedence: sets the precede
Help	Save to Device Preview CLI Cancel

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

- 1. Select SIP
- 2. Select the Marking tab.
- 3. Mark with DSCP as below.

🔺 Ma	nage QoS Settings -	Branch1-LA.dc	oud.cisco.	com (19	8.19.1.1)			×
🔄 된 💐 🖏 🖓 🍪 🎭 Policies Classes Interfaces								
Policies	Mapped Classes							
🛃 🕸 📚 🛼 💺 🗞 🗠	Pe 🔒 📑							
DSCPMARK	Class Name Classify	Marking Queuei	ng Policing	Shaping	Compression	WRED	DBL	Unknown
	RTP 🔷	DSCP: EF						
dass-default	SIP 👳	DSCP:						
WhyIsThisHere	dass-default 👳							
dass-default								
	Mapped Class Detail							
		ISS						
		-						
	Classify Marking Que	eueing Policing Sr	aping Comp	ression wi	RED DBL Uns	upported		
	Mark with:					ference		
	3 🗹 DSCP	24 (222)				fferentiate		
			~			longing to used on ma		ISS
	IPv4 Only	/					annang.	
	ATM Cell Loss	Priority			M	ark On		
	Frame Relay D	in and Finible				SCP: mark		
	Frame Relay D	iscard Eligible				tting the d		
						rvices co SCP) valu		
						service (
						ecedenc		
						ecedence		b.d.
					<			>
]
Help			Save t	o Device	Preview C	11	C	Cancel

- 4. Click Preview CLI to see the policy you have created.
- 5. Click Save to Device if satisfied.



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

- 1. Select the "DSCPMARK" policy.
- 2. Click the "three arrow" icon to copy policy to devices.
- 3. Select the DSCPMARK Policy.
- 4. Select the other two devices in the topology.
- 5. Click OK

	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (19	8.19.1.1) ×
Image: A state of the state	Apped Classes	
DSCPMARK SIP dass-default WhyISThisHere dass-default	Copy Policy to Devices × Select a policy: DSCPMARK Select the devices to which you want to save this policy: Paranch2-NY.dcloud.cisco.com (198.19.2.1) PHQ-SJ.dcloud.cisco.com (198.18.129.25) OK Cancel ATM Cell Loss Priority Frame Relay Discard Eligible	Compression WRED DBL Unknown ED DBL Unsupported Image: Comparison of the second secon
Help	Save to Device	Preview CLI Close

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

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

Copy Policy to De	evices	×
Saving to devices Branch2-NY.dcloud.cisco.com (198.19.2.1) HQ-SJ.dcloud.cisco.com (198.18.129.25)		
	Cancel	

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.

- 1. Right-Click on the appropriate device.
- 2. Select QoS, Apply Policy to Interface.

		LiveAction - 198.18.133.34	- 🗆 🗙
<u>File View U</u> sers <u>Q</u> oS F <u>l</u> ow	outing IPSLA LAN Tools Reports Window Dev Help		
Dashboard Manage 💽 Expand	QoS Flow Routing IP SLA LAN		
Q	🕂 💠 🔀 🖍 📖 🗸 🔍 🔍 🔍 Audit		
Name			
E A Home			
Branch 1-LA G Branch 2-NY HQ-63	HANKEY		
	3 Branch24IY 198-19-21	Brancht La 1 1 2 2 4 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Polling
			y from Template
			Configuration
		Adjust Input	
		(Adjust Outp	ut QoS
		Manage Qo	5 Settings
		Manage NB/	AR
			to Interface
			icy from Interface
		Interface: HQ-SJ - Ethernet0/0 Copy Policy	to Devices
		QoS Reports	
	QoS Policy Applied	Edit Device Settings	
	8 Normal Orops (See Alerts)	Add or Remove Interfaces	
	@ Warning	HQ-SJ 198.18.129.25 Refresh Device Remove Device	
	Down Main Disabled	Zoom to Device	
	A QoS Poling Disabled Icon	Device Tools	
	ACL Applied	Statistics +	
< >	VLAN VLAN	View	
CPU Memory Flow Buffer	Alerts Advisories Nodes	Group Management	admin: Admin user 04:16:35 PM PST

- 3. Select the "DSCPMARK" policy.
- 4. Click the Input of the LAN Interface



Do this for each device! (loop to #1 above for each device)

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



Lab 8.2: QoS Queueing Policy

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

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

Lab Steps:

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

Qv	🕂 🔶 🖊 📮 -	Q Q /	Audit
Name			
🖶 🐨 🐨 Branch4	Device: Branch1-LA.dcloud.cisco.com		
🗄 🛞 HQ-SJ 📒	Flow	•	Enable QoS Polling Manage QoS Settings
	Routing	•	Revert QoS Configuration
	IP SLA	•	Manage NBAR
	LAN	•	Apply Policy to Interfaces
	Edit Device Settings Add or Remove Interfaces		Remove Policy from Interfaces Copy Policy to Devices
	Refresh Device		Reports
	Remove Device		Nites 1 St
	Zoom to Device		
	Device Tools	•	
	Statistics	•	
	View	•	
	Group Management	•	
			HQ-

- 2. Select the Policies Tab.
- 3. Click Add Policy to create a queuing policy.



4. Name the new policy QUEUEING.



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



- 6. Create a new class labeled VOIP.
- 7. Click OK.



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



- 9. Create a new class and label it SIGNALING.
- 10. Click OK

Add Class to Policy						
Select one of the following options:						
O Use existing clas	ss: 4C_BL_CriticalData_App-Match_Mark	~				
Oreate new class	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

	Manag	e QoS Settings - Branch1-LA.dcloud.cisco.con	m (1	198.19.1.1)		×
4 4 1 2 2	😤 🖏					
Policies Classes	rfaces					
Classes	Create and Edit Mat					
🔁 🖻 🕱 🦳	Match Long	3	1	Match any 🗸 🐹		
4C_BL_CriticalDate	Match type:					
4C_BL_Realtime_A	Value:		1	M Match T Value		
4C_BL_Scavenger		45	M	1a DSCP 46 (EF)		
4C-MN_CONTROL	4	46 (EF) 47				
4C-MN_CRITICAL 4C-MN_REALTIME		48 (CS6)				
RDP		49				
RTP		50				
SIGNALING		51 🗸				
SIP		(Select up to 8 values)	.			
	Match/match not:	Match 🗸				
		IPv4 Only				
	5	Add Match Statement Replace Match Statement				
		Add Match Statement Replace Match Statement				
< >						
Help		Save to Dev	vice	Preview CLI	Cancel	
nep		Save to be	.vice	Freview CLI	Cancel	

Configure SIGNALING Class:

- 1. Select SIGNALING.
- 2. Use DSCP as Match Type.
- 3. Select 24 (CS3).
- 4. Click Add Match Statement.

A Manag	e QoS Settings - Branch1-LA.dcloud.cisco.com	(198.19.1.1)	×
Policies Classes Interfaces			
Classes Create and Edit Mat	ch Statem		
Atch type:		Match any 🗸 👯	_
4C_BL_Realtime_A Value:		M Match T Value	
4C_BL_Scavenger 4C-MN_CONTROL	18 (AF21) 19	Ma DSCP 24 (CS3)	
	20 (AF22)		
4C-MN_REALTIME	21		
	22 (AF23) 23		
I RTP 3	24 (CS3) 🗸		
	(Select up to 8 values)		
VOIP Match/match not:	Match 🗸		
	IPv4 Only		
4	Add Match Statement Replace Match Statement		

Setup VoIP Priorities:

- 1. Select the Policies Tab.
- 2. Select the VOIP Class.
- 3. Select the Queuing Tab.
- 4. Select Priority Queuing, enter a rate of 33%.



Setup Signaling Priorities:

- 1. Select the Signaling Class.
- 2. Select The Queueing Tab.
- 3. Select Class-Based with a rate of 7%.

	Ianage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
 Policies Classes Interfaces 		
Policies	Mapped Classes	
🔁 🕸 📚 🛼 🖡 🖄 🛼		
DSCPMARK	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown	1
	VOIP Priority: 3	
	SIGNALING 🔶 Class-bas	
dass-default	class-default	
whyIsThisHere		
	Mapped Class Detail	
	Drop all traffic for class 2	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Queueing type: Class-based V	
	3 Rate: 7 Percent V Distribute the available A	
	Queue depth: 1 Bytes V Classes by specifying a minimum bandwidth	
	Enable Fair Queueing guarantee to each class.	
	Unknown elements:	
	Class-based: utilizes Class-based weighted fair	
	queueing (CBWFQ) using	
	derived weight for packets	
	from the bandwidth	
	silocated to the class	
Help	Save to Device Preview CLI Cancel	

Create a Shaping Policy:

4. Click Add Policy.

친 원 원 원 원 생 %
Policies Classes Interfaces
Policies
🛃 🖲 🔡 🔝 🐜 🖷 🖏 🍕
Add Policy RK
class-default
. WhyIsThisHere
_

5. Give the Policy a name of Shaper.



- 1. Select the **class-default** class under Shaper.
- 2. Select the Shaping tab.
- 3. Select Average, enter 1500 Kbps.

A 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 Unknown class-default • 1,500 K • • • • •	1
Signaling dass-default		
₩ WhyIsThisHere		
	Mapped Class Detail	
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Shape using: Average V Reference Control the flow of traffic ^	1
	Rate: 1500 Kbps K	
	Committed burst: 256 bits by delaying packets and conforming to a specified bit rate. Excess burst: 0 bits bit rate.	
	Unknown elements: Rate	
	Peak: allows the transmission rate to burst higher than the shaping rate.	
	Average: sets the maximum transmission Y	
Help	Save to Device Preview CLI Cancel	

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

A Mar	nage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
 Policies Classes Interfaces 		
Policies	Mapped Classes	
DSCPMARK	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unkn VOIP Priority: 3 SIGNALING Class-bas class-default Image: Signal and Signal	nwc
	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Shape using: None Reference Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.	^
	Rate Peak: allows the transmission rate to burst higher than the shaping rate. Average: sets the	
Help	Save to Device Preview CLI Cancel	~

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

A Mai	nage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
Image: Second system Image: Second system Policies Classes Policies Image: Second system Image: Second system <t< th=""><th>Mapped Classes</th><th></th></t<>	Mapped Classes	
DSCPMARK OUEUING VOIP SIGNALING dass-default dass-default dass-default WhyIsThisHere	Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknow VOIP • Priority: 3 SIGNALING • Class-bas SIGNALING • Class-bas class-default • • • Mapped Class Detail • • • • • • • Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	vn
	Shape using: None V Reference	

Copy the shaping policy to the other devices:

- 1. Select the Shaper Policy.
- 2. Click the three arrow icon to copy the policy.
- 3. Ensure the Shaper Policy is selected.
- 4. Select the other two devices.
- 5. Click OK to push the policy.

A	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	×
 Image: Second state of the second	2 Mapped Classes	Nown
Help	Save to Device Preview CLI Close	

- 6. Click Close.
- 7. Click OK.



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

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



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

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

10. Click OK.

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



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

Lab 8.3: QoS Verification

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

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

Lab Steps:

Select a device and select QoS and Manage QoS Settings.



- 1. Select the VOIP Class.
- 2. Click the Queueing Tab.
- 3. Select Burst Size of 128000.



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

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

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

- 4. Right-click on the QUEUEING Policy.
- 5. Select Add Class to Policy.



6. Give the new class a label of SCAVENGER.



- 1. Select the Classes Tab.
- 2. Select the Scavenger Class.
- 3. For Match Type select Protocol Using NBAR.
- 4. Select both "bittorrent" and "bittorrent-networking".
- 5. Click Add Match Statement for both Applications.

	Mana	ge QoS Settings - HQ-S	J.dcloud.cisco.com (19	98.18.129.25)	
4 4 4 7	6 5				
Policies Classes	aces				_
Classes	Create and Edit Mat	ch Statements			
👍 🖻 🕱	Match type:	Protocol - using NBAR	~	Match any 🧹 🞇	
RTP SCAVENGER	2 Value:	bhmds	^	M Match T Value	1
SIGNALING		binary-over-http bittorrent		Ma Protocol bittorrent	11
	4	bittorrent-networking		Ma Protocol bittorrent-networking	
VOIP	-	bl-idm			
		blizwow			
		blogger			
		bmpp	×		
	Match/match not:	Match	¥		
	5	Add Match Statement	Replace Match Statement		

- 1. Now let's go back to the Policies Tab
- 2. Select the Scavenger Class
- 3. Then select the Queueing Tab
- 4. Next select Class-based and give the class a rate of 1 percent
- 5. Finally select Save to Device

Ma	anage QoS Settin	gs - HQ-SJ.	dcloud.cis	co.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								
📑 🖷 🖹 🔓 🐜 🖷 🖏 🖷	Pe 👔 📕 🚔								
DSCPMark	Class Name Clas	sify Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	VOIP	•	Priority: 3						
VOIP	SIGNALING		Class-bas						
SIGNALING			Class-bas						
SCAVENGER 2	class-default (•							
class-default									
Shaper									
	Mapped Class Detai								
	Drop all traffic f								
	Classify Marking	Queueing	nicing Shapin	g Compr	ession Wi	RED DBL Uns	upported		
	Queueing type:	lass-based 🗸]			Ref	ference		
	A Rate: 1	Perce					stribute th		
				*			ndwidth t asses by		
	Queue de	pth: 1	Bytes	\sim			nimum bai		-
	Enable Fa	r Queueing				gu	arantee to	each o	slass.
							om the bai		b.d.
						ali <	ncated to	the clas	>
Help			5	Save to	Device	Preview C	LI	C	ancel
			_						

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

Ma	nage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)	×
 Policies Classes Interfaces 		
Policies	Mapped Classes	
DSCPMark	Class Name Classify Marking Queueing Policing Shaping Compre WRED DBL VOIP Priority: 33% STGNALTING Class-based: 7%	U
VOIP SIGNALING SCAVENGER dass-default	CAVENGER Class-based: 1% class-default	
⊖-⊡. dass-default 	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported	
	Queueing type: Class-based v Reference Rate: 1 Percent v Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. Enable Fair Queueing guarantee to each class.	^
	Unknown elements:	-
	Class-based: utilizes Class-based weighted fai queueing (CBWFQ) using derived weight for packet from the bandwidth allocated to the class <	s V
Help	Save to Device Preview CLI Cancel	

Copy the updated policy to other devices in the topology.

- 6. Select the Shaper Policy
- 7. Copy the Policy to Devices.

Policies Classes Interfaces	
Policies	Mapped Classes
📑 🗓 🖹 🔝 🐜 🖷 🖓 📑	
DSCPMark	Dify Ma
DSCPMARK CC	ppy Policy to Devices ify Ma class-default
VOIP	
SIGNALING	
SCAVENGER	
dass-default	
😑 🦢 Shaper	
Class-default	
	Mapped Class Detail
	Drop all traffic for class

8. 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:	↓
Pranch 1-LA.dcloud.cisco.com (198.19.1.1) Pranch 2-NY.dcloud.cisco.com (198.19.2.1)	
OK Cancel	

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

- 9. Select perform this action for all devices which have conflicts.
- 10. Click Overwrite.

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

Ensure the copy is successful.

11. Click Close.

Copy Policy to De	vices ×
Saving to devices Branch 1-LA.dcloud.cisco.com (198.19.1.1) Branch 2-NY.dcloud.cisco.com (198.19.2.1)	
[Cancel Close

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



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

Lab A: Appendix

Lab A.1: Add Device

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

Lab Steps:

12. Select File, Add Device

堤 198.18.133.34 - Remote Desktop							
LiveAction - localhost							
File	View	Users	QoS	Flow	Rou		
Add Device							
	Discover	^r Device	s		-		
	Import D)evices			F		
Export Devices							
Manage Devices							
	Refresh	Devices	5				
	Remove	Networ	k Obje	ts			
	Exit						
					_		

13. Enter 198.19.1.1 in the IP Address field.

14. Select "Use the Default SNMP connection settings".

Add	Device				×
Ste	ps	Device Connection Inform	nation		
1.	Device Connection Information	Enter the SNMP connecti	on information.		
2.	CLI Settings (Configuring)	Node	Local	\sim	
	CLI Settings (Monitoring) Select Interfaces	IP Address	198. 19. 1. 1		
5.	Select VLANs	O Non SNMP device su	ch as NetFlow probes		
6.	Select Features	◯ LiveSensor			
7.	Enable Polling	Use the Default SNM	IP connection settings	Edit	
8.	Review Configuration	O Enter SNMP connect	ion settings for this device		
9.	Device Updated	SNMP Version	Version 2c	✓ Target Port 161	
		Community String			
		< Back Next >	Finish	Cancel Help	

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

Steps CLI Settings (Configuring) 1. Device Connection Information Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*). 2. CLI Settings (Configuring) Configuration CLI connection Settings 3. CLI Settings (Monitoring) Enter Command Line Interface (CLI) connection settings used to configure these devices. 4. Select Interfaces C Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp) 5. Select YLANs Enter connection settings for this device 6. Select Features Enter connection settings for this device 7. Enable Polling Connection Type SSH Y Port* 22 9. Device Updated User name on Device Password on Device*
Enable Password Also use these credentials for monitor mode,
,

Add Device - HQ-SJ.dcloud.cis	co.com (198.18.129.25) 🛛 🗙
Steps	CLI Settings (Monitoring)
 Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select VLANs Select 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. Clise the default Monitor-only CLI connection settings Enter connection settings for this device Connection settings for this device Connection Type SSH y Port* 22 User name on Device* Enable Password
	<back next=""> Finish Cancel Help</back>

- 18. Select "Use the previous page connection settings".
- 19. Click Next.

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

20. Click Continue.

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

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

teps	Se	lect Interface	es			
 Device Connection Information 	Se	lect the inter	faces you want to	monitor on this de	vice (maximum 100	00 interfaces).
2. CLI Settings (Configuring)		Selected	Interface	Trunk	IP Address	Description
3. CLI Settings (Monitoring)		N	Ethernet0/0		198.18.129.25	
4. Select Interfaces		হ	Ethernet0/1 Loopback0		10.255.0.2 10.0.0.102	
5. Select VLANs			NullO		10.0.0.102	
. Select Features			Tunnel0			PFR auto-tunnel for VRF default
. Enable Polling			VoIP-NullO			
Review Configuration						
). Device Updated						
		Selected inter	rtace(s): 3			
	<					Cancel Help

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

Add Device - HQ-5J.dcloud.cisc	:o.com (198.18.129.25) X
Steps	Select VLANs
 Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Polling Review Configuration Device Updated 	Select the VLANs you want to monitor on this device (maximum 25 VLANs). No VLANs were found on the device. No VLANs will be managed.
	< Back Next > Finish Cancel Help

22. 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**.

d Device - HQ-SJ.dcloud.cisc			
Steps	Select Features		
1. Device Connection Information	Select the features you want to enable section.	e on each interface. Learn more -	about each feature in the Help
 CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs 	Features on device Enable Mediatrace Associate Probe at IP Address:		
6. Select Features	Interface	NBAR	NetFlow
7. Enable Polling	Ethernet0/1 Ethernet0/0	ব	<u>ব</u> ব
 Review Configuration Device Updated 	Loopback0	2	
			Ŗ
[< Back Next > Finish		Cancel Help

24. Change the polling rate to 30 seconds.

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

Steps	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 	
5. Select VLANs	Polling Rate 30 seconds
5. Select Features	
7. Enable Polling	Poll the following features
3. Review Configuration	✓ Hows
9. 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.
	K
	· · · · · · · · · · · · · · · · · · ·
	< Back Next > Finish Cancel Help

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

Add Device - HQ-SJ.dcloud.cis	co.com (198.18.129.25)	X
Steps	Review Configuration	
1. Device Connection Information	The following commands will be sent to the device. Or you can choose to manually configure the device yourself.	
2. CLI Settings (Configuring)		_
 CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Polling Review Configuration Device Updated 	<pre>description D0 NOT MODIFY. USED BY LIVEACTION. exporter LIVEACTION-FLOWEXPORTER cache timeout inactive 10 cache timeout active 60 record LIVEACTION-FLOWRECORD exit interface EthernetO/1 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output exit interface EthernetO/0 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output exit interface Loopback0 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output</pre>	
	 Send the configuration commands to device. I will manually configure the device myself. 	
	< Back Next > Finish Cancel Help	

- 26. Select "Send the configuration..." radio button, if available.
- 27. Click Next.

28. Click Finish.

iteps	Device Updated		
1. Device Connection Information	You have configured this device successfull configuration to the device's startup config,		
2. CLI Settings (Configuring)	Device Settings		
3. CLI Settings (Monitoring)	-		Description
4. Select Interfaces	Setting Polling Rate		Description 30 seconds
5. Select VLANs	NetFlow Monitoring		NetFlow collector
6. Select Features	NetFlow Polling		Enabled
7. Enable Polling	Mediatrace		Disabled
2	Adjacency Polling		Enabled
8. Review Configuration	Qos Polling IP SLA Polling		Enabled Enabled
9. Device Updated	CEF		Enabled
	Interface Settings		
	Interface	NBAR	NetFlow
	Ethernet0/1	٠	•
	Ethernet0/0	•	•
	Loopback0	•	•
	1		
		\sim	

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

Lab A.2: Client Device Discovery

As we discovered in a prior Lab, the LiveNX Server in your topology has had device(s) preinstalled. In the following Lab you may add additional devices to your Topology, configure those devices to send flow and SNMP data to the LiveNX Server, and discover what data your LiveNX solution is gathering.

Lab Steps:

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

1. Select File and Discover Devices.

5	98.18.1	33.34 -	Remo	te Desl	kto
🔺 Li	veActio	on - loca	alhost		
File	View	Users	QoS	Flow	Ro
	Add De	vice			
	Discove	er Device	s		
Import Devices					
Export Devices					
Manage Devices					
Refresh Devices					
	Remove	e Networ	rk Obje	cts	
	Exit				

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

Device Discovery	×
Step 1: Specify what to scan	
Specify IP ranges (ex: 192.168.1.1-200) or one IP per line:	
198.19.1.1 198.19.2.1	
O Specify seed device to scan	
IP Address Hops 1	-
Step 2: Specify SNMP settings Image: Step 2: Specify SNMP settings Image: Step 2: Specify SNMP connection settings Image: Step 2:]

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

Step 3: Specify node		
Local		v
	ОК	Cancel

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

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



A Device Discover	y on Local				X
Filter by:		Filter	Clear		
Select	Device Name	IP Address	Hops	Vendor	Model
	Branch2-NY.dcloud.cisco.com	198.19.2.1	0	Cisco	ciscoGatewayServer
	Branch1-LA.dcloud.cisco.com	198.19.1.1	0	Cisco	ciscoGatewayServer
Selected: 2	Discovered: 2 Device Limit: 10,0	00,000 (1 active devices) Add Devices Advan	ced Add	Pause	Stop.

6. Select Yes on the configure devices dialog.



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

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

nfigure Cisco Devices		
iteps	SNMP Settings	
 SNMP Settings CLI Settings (Configuring) 	Enter the SNMP connection information used for monitoring	
 CLI Settings (Monitoring) Validating Devices 	 Use the Default SNMP connection settings C Enter SNMP connection settings for this device 	Edit
5. Select Features	SNMP Version 2c	Target Port 161
6. Enable Polling 7. Update Device	Community String	
8. Devices Configured		
	< Back Next > Finish	Cancel Help

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

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

10. Select Use the previous page connection settings.

Configure Cisco Devices	×
Steps	CLI Settings (Monitoring)
 SNMP Settings CLI Settings (Configuring) 	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 (*).
 CLI Settings (Monitoring) Validating Devices Select Features Enable Polling Update Device Devices Configured 	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 C Use the previous page connection settings C Enter connection settings for this device Connection Type SSH P Port* 22 User name on Device Password on Device* Enable Password
	< Back Next > Finish Cancel Help

11. Click Next

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

CLI Settings (Monitoring) Device Status Description • Validating Devices Branch1-LA.dcloud.cisco.com Succeeded: click for details . Select Features Branch2-NY.dcloud.cisco.com Succeeded: click for details . Enable Polling . . Update Device .	
2. CLI Settings (Configuring) 3. CLI Settings (Monitoring) 4. Validating Devices 5. Select Features 6. Enable Polling 7. Update Device 8. Devices Configured	ow. If a
4. Validating Devices Branch1-LA.dcloud.cisco.com Succeeded: click for details 5. Select Features Branch1-LA.dcloud.cisco.com Succeeded: click for details 6. Enable Polling Jupdate Device Succeeded: click for details 8. Devices Configured Succeeded: click for details	
4. Validating Devices Branch1-LA.dcloud.cisco.com Succeeded: click for details 5. Select Features Branch1-LA.dcloud.cisco.com Succeeded: click for details 6. Enable Polling Jupdate Device Succeeded: click for details 8. Devices Configured Succeeded: click for details	
5. Select Features Branch2-NY.dcloud.cisco.com Succeeded: click for details 6. Enable Polling	
6. Enable Polling 7. Update Device 8. Devices Configured	
3. Devices Configured	
Export Validation Details	
<back cancel<="" finish="" td=""><td>Help</td></back>	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 t	ne devices. Learn more	e about each feature i	n the Help section.
2. CLI Settings (Configuring)	Device	NBAR	NetFlow	Mediatrace
3. CLI Settings (Monitoring)	Branch1-LA.dcloud.cisco.com			Mediatrace
 Validating Devices 	Branch2-NY.dcloud.cisco.com			
5. Select Features				
5. Enable Polling				
7. Update Device				
3. Devices Configured				
	1			
	< Back Next > Finish		Ca	ncel Help

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

Configure Cisco Devices								>
Steps	Enable Polling							
1. SNMP Settings	Select the features you want to act	ively monitor,	and the p	olling rate I	for the dev	ices. Lea	arn more about	
2. CLI Settings (Configuring)	each feature in the Help section.							
3. CLI Settings (Monitoring)							,	
4. Validating Devices	Device	Poll Qos		IP SLA	Routing	LAN*	Interval	Ļ
5. Select Features	Branch1-LA.dcloud.cisco.com Branch2-NY.dcloud.cisco.com	V V V					30 seconds 🔄 30 seconds 🔄	
6. Enable Polling							Too seconds E	1
7. Update Device								
8. Devices Configured								
							\mathbf{k}	
							~	
	,							
	warman III and a							
	* LAN polling occurs every 15 min * For SNMP v3, please see the Us		onfiguring	LAN polling	j.			
	< Back Next > Fin	ish				Cancel	Help	
					_			

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

16. Select Send Updates to Devices and click Send.

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

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

eps	Update Device			
. SNMP Settings . CLI Settings (Configuring) . CLI Settings (Monitoring) . Validating Devices	The selected devices will be updated based You may choose to manually configure the Warning: once update processes have bee more about each feature in the Help section	e devices. en started you will n		ns. Lean
. 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 Se	nd		
	C Manually Configure Devices			
	Export Update Commands			

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

Configure Cisco Devices		×
Steps	Devices Configured	
 SNMP Settings CLI Settings (Configuring) 	The following devices have been configured. Lear	
 CLI Settings (Monitoring) Validating Devices Select Features Enable Polling Update Device Devices Configured 	Device Branch1-LA.dcloud.cisco.com Branch2-NY.dcloud.cisco.com	Summary CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30
	< Back Next > Finish	Cancel Help

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

Lab A.3: Export/Import Device Configuration

Lab Steps:

1. From the File Menu select Export Devices.



2. Deselect Ethernet0/1 and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

dd/Upd	Name	Туре	Device Serial	IP Address	Service	Tags	Capacity (Kb	Label	Poll	Poll QoS	Poll Flow	Poll IP SLA	Poll Rout	Poll LAN	Poll Interval
v	-Branch1-LA.dcloud.cisco	Router	101	198.19.1.1					v	v	V	v	•		30 seconds 💌
V	Ethernet0/0	Interface		198.19.1.1											
	-Ethernet0/1	Interface		100.64.1.2											
•	-Ethernet0/2	Interface		10.255.1.2											
	-Loopback0	Interface		10.0.1.1											
	Null0	Interface													
	Tunnel0	Interface													
	VoIP-NullO	Interface													
•	Branch2-NY.dcloud.cisco	Router	201	198.19.2.1					▼	•	7	▼	•		30 seconds 💌
•	-Ethernet0/0	Interface		198.19.2.1											
	-Ethernet0/1	Interface		100.64.2.2											
•	-Ethernet0/2	Interface		10.255.2.2											
	Loopback0	Interface		10.0.2.1											
	NullO	Interface													
	Tunnel0	Interface													
	VoIP-Null0	Interface													
~	HQ-SJ.dcloud.cisco.com	Router	3	198.18.129.25					~	~	~	V	~		30 seconds 💽
~	Ethernet0/0	Interface		198.18.129.25											
~	-Ethernet0/1	Interface		10.255.0.2											
	Loopback0	Interface		10.0.0.102											
	Null0	Interface													
	Tunnel0	Interface													
	VoIP-Null0	Interface													
					•										

3. Select Export to csv.

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

A Export the co	ontent to a CSV file	×
Look in	n: 📃 Desktop 🍸 🎲 📁 📰 -	
Recent Items Desktop My Documents	 Libraries Administrator Computer Network LiveAction Upgrade updateinterface.csv 	
	File name: updateinterface.csv	port
Network		ancel

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



8. Select the file you previously exported.

	\Lambda Import from a	CSV file						×
	Look in:	🧮 Desktop			 •	1 📂 🎞	•	
2	Recent Items Desktop My Documents Computer	Cibraries Administra Computer Network LiveAction updateinte	Upgrade					
		File name:	updateinterfa	ace.csv			Import	7
	Network	Files of type:	CSV files (*.o	:sv)		-	Cancel	7

9. Click Add/Update Devices.

d/Upd	s selected for Add/Update will Name	Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K	Node	Group	Site	Site CIDR
ajopa			101	198.19.1.1	Cisco	ciscoGatewa		Cisco IOS Software, Linux S		Local	Group	Jire	JILE CIDK
V		Interface		198.19.1.1				Branch1 LAN	10,000				
		Interface		100.64.1.2				Internet	2,000				
		Interface		10.255.1.2				MPLS	10,000				
		Interface		10.0.1.1					4,294,967				
П		Interface							4,294,967				
Π	Tunnel0	Interface						PFR auto-tunnel for VRF de	10,000				
—		Interface							4,294,967				
	-Branch2-NY.dcloud.cisco		201	198.19.2.1	Cisco	ciscoGatewa	15.4()	Cisco IOS Software, Linux S		Local			
- -	Ethernet0/0	Interface	201	198.19.2.1	0.000	cisco dacorram	10110	Branch2 LAN	10,000	Local			
		Interface		100.64.2.2				Internet	2,000				
V		Interface		10.255.2.2				MPLS	10,000				
		Interface		10.0.2.1				hir Co	4,294,967				
		Interface		10.0.2.1					4,294,967				
	-Tunnel0	Interface						PFR auto-tunnel for VRF de	10,000				
	VoIP-Null0	Interface						FIR duto-turinerror wir us	4,294,967				
V		Router	3	198.18.129.25	Cisco	ciscoGatewa	15.40	Cisco IOS Software, Linux S		Local			
<u>م</u>		Interface	3	198.18.129.25	CISCO	USLUGALEWA	15.40	Cisco 105 Sortware, Linux 5	10,000	LULAI			
V		Interface		196.16.129.25					10,000				
		Interface		10.255.0.2									
	Loopback0 Null0	Interface		10.0.0.102					4,294,967				
								and the life stands	4,294,967				
	Tunnel0	Interface						PFR auto-tunnel for VRF de	10,000				
	VoIP-Null0	Interface							4,294,967				
													R
													. 0
					4								

10. Click OK to use the Default SNMP settings.

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

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

Lab A.4: Saving Server Configurations

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

Lab Steps:

1. Open the LiveNX WebUI, select Settings > System Management..

LiveNX Dashboard × +									-		×
🖍 🚖 🗈 🗲 🛈 🖴 https://sedemo1.liveacti	on.com								C	÷	≡
Most Visited											
■ LiveAction [™] WX UX			▲ 174	2	• 2 🌲 307					8 (
Dashboard ^②				Aug	19, 2018 16:30:00	→ Aug 19, 2	018 16:45:00	Add V			
Status		WAN	System				Cisco SD-W	VAN Perfor			
:: Top Sites by WAN Utilization Peak Inbound WAN Interf	ace Utilization 🛛 🗙	:: Top WAN Applications by Bandy	vidth Inbound/Outbound Bandwidth	×	: Top Interfa	ces % Change	d - Interface B	urstable Ra			
Madison/MPLS	65.0	voice-and-video Vo	2.1 Average Input		Inbound RTF	_Birmi		_			
Birmingham MPLS	44.0	desktop-virtualizati			Outbound R	rr_Ma					1.3
Austin MPLS	41.0	transactional-data	0.5		Outbound	rr_Bir					1.1
San_Jose MPLS	37.0	voice-and-video Vi	0.2		Outbound	rr_au I					0.0
London MPLS	11.0	signaling]rtcp	0.1		Outbound	FR_Sa I					0.0
Laurentile HADLO	0.0	contraction destructions and the second second	0.1		In Second DTD	Advert A					<u> </u>

2. Select the Configuration Tab.

System Management									
Licensing Reports	Updates	Properties	Mounted Data	Nodes	Troubleshooting	SNMP Trap	Email Configuration	Configure Proxy	Configurati
Export Import									
PORT CONFIGURATION									
Encrypt									
Add password		۲							
PEAT PASSWORD									
		۲							
Export									
ESTART SERVICE									
Restart									

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



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

Lab A.5: Connect via Remote Desktop Connection

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

To connect useing 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: The instructor may provide you with a Username and Password to connect via RDC. Please make sure you write these on YOUR Class Worksheet. Use information from the Class Worksheet to connect to your assigned Pod.

Lab Steps:

Connect to the virtual Windows 7 Workstation using the IP Address, username, and password pre-printed on the Class Worksheet, unless otherwise instructed.

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

DIAGRAM

퉣 Remote	e Desktop Con	nection		—		×
	Remote Conne					
	Display Local F	Resources	Experience	Advanced		
Logon set	-	e of the re	note computer			
						,
	Computer:	198.18.1	33.34		~	
	User name:	DESKTO	P-69VEDIF\ad	dministrator		
			used to conne ese credentials		mputer.	
	Always ask	for crede	ntials			
Connectio	on settings					
	Save the curre saved connec		tion settings to	an RDP file	or open a	а
	Save		Save As	(Open	
Alide Or	otions			Connect	He	lp

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

Note: Since you are connected to your Student Pod via a VPN, you may need to CHANGE the domain in the RDC User name field to LOCAL.

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

DIAGRAM

퉣 Remo	🌄 Remote Desktop Connection — 🗆 🗙									
N		mote Desk Innectio								
General	Display	Local Resources	Experience	Advanced						
Display	configura	tion								
		e the size of your re the right to use the		. Drag the sl	ider all th	e				
Small Large										
	🗌 Us	e all my monitors for	the remote se	ession						
Colors		e the color depth of est Quality (32 bit)	f the remote se	ession.						
🗹 Displa	y the con	nection bar when I	use the full scr	reen						
A Hide (Options			Connect	He	elp				

- 4. Select Connect.
- 5. Enter the workstation password: C1sco12345 (or otherwise defined by instructor).

DIAGRAM

Windows Security Enter your These credenti	Constant Toolah
	DESKTOP-69VEDIF\administrator
	Use another account
Reme	mber my credentials
	OK Ci

6. Click OK.

Once successfully connected to your Pod you will see the Windows7 Desktop, and be able to access the LiveNX Server, Client, and other pod resources.

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