

LiveAction Training Lab Workbook Pt.2

NXOF-2.LWA.2.0.0

© Copyright 2022, LiveAction, Inc.

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

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

Trademarks:

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

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

July 2022

LiveNX Foundations Workbook 2

Table of Contents

Lab 1: QoS Configuration	5
Lab 1.0: Introduction to QoS	
Lab 1.1: Run Baseline Reports	8
Lab 1.2: Building Filters	13
Lab 1.3: Validating Filters	19
Lab 2: Classification & Marking	23
Lab 2.1: QoS Class Models	24
Lab 2.2: Validate DSCP Markings	
Lab 2.3: Rogue DSCP Markings	31
Lab 2.4: Configure Classification & Marking Policies	32
Lab 2.5: Apply Marking Policies to Interface(s)	40
Lab 2.6: Validate DSCP Settings	
Lab 3: QoS Prioritization & Queueing	
Lab 3.0: Intro to Prioritization	
Lab 3.1: Run the Reports!	51
Lab 3.2: Building Queueing Policies	54
Lab 4: Shaping / Scaling	
Lab 4.0: Intro - Shaping (Scaling)	
Lab 4.1: Shaping (Scaling)	62
Lab 5: Throttling Traffic	
Lab 5.0: Intro - Throttling / Policing	
Lab 5.1: Throttling / Policing	
Lab 5.2: Confirm policing Settings	
Lab 6: Buffer Tuning	
Lab 6.0: Intro – Buffer Tuning	
Lab 6.1: Implementing Tuning	
Lab 7: QoS Alerts 1	00
Lab 7.1: Configure QoS Alerts 1	
Appendices	
Appendix 1: Add Device 1	
Appendix 2: Client Device Discovery1	
Appendix 3: Export/Import Device Configuration1	
Appendix 4: Saving Server Configurations1	
Appendix 5: Connect via Remote Desktop Connection 1	29

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 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 1

Lab 1: QoS Configuration

In this lab we are going to walk through the story of implementing QoS for a small WAN network using LiveNX. When complete we will have used LiveNX to:

- Identify and validate critical traffic is marked with a DSCP tag
- Build Shaping Policies
- Prioritize Voice & Video
- Protect high priority data
- Police scavenger/low priority traffic
- Validated QoS is working end-to-end

Below is a diagram of sample network. There are two branch locations with connections back to HQ via two MPLS Networks. The connectivity is designed as follows:

- HQ-B1 no provider CIR
- HQ-B2 no provider CIR
- NY 1.544Mb provider CIR
- LA 1.544MB provider CIR

For the sake of this lab assume there is no other QoS on the service provider's backbone.



Figure 1

Remember from the presentation that QoS is done in 4 steps:

- Step 1 Recognizing Application traffic (Classification and Marking)
- Step 2 Prioritization (Queueing and Shaping)
- Step 3 Throttling Traffic (Policing and WRED)
- Step 4 Buffer Tuning

We will use LiveNX to walk through this story.

Remember from the slide presentation there are several components to this step.



Figure 2

Day 0 Tasks

The first item that must be understood to successfully implement QoS is to understand a business's critical applications. In our sample network the following applications have been defined as the highest priority:

- Voice (rtp)
- Video (Lync)
- SIP
- Citrix
- NetFlow
- SNMP
- SSH
- Telnet
- Salesforce

We will next use several LiveNX Flow reports to understand the application landscape

Lab 1.1: Run Baseline Reports

This Lab uses the WebUI.

- From the LiveNX Client, Run the Reports > Flow > Applications > Application
 - Keep all filters and report at their default settings (All Devices, Outbound)
 - Implement a Search of "wan" by entering **wan** in the flex search bar.
 - Then click Execute Report

						View Options $\ \cdot \ $	Share Print	Schedule Copy	Clos
plication (F	low)					15 Minute Perio	d (default)	_	ø
rice: All WAN I	Devices Interface: All WAN Interface	faces Display Filter: No Display Filter	ring Direction: Outbound Flow 1	Type: Basic Flow Execution Type: Time	Series Sort By: Bit Rate Bin Duration: Aut	Start Time: Jun 30, 2022 13:39:36 EDT (GMT-04:00	D) End Time: Jun 30, 2022 13:54:36 ED	DT (GMT-04:00) Bin Interval: 1	minute
500								rtp trp-audio 10.21.1.154 snmp ica ipfix statistical-p2p sp ctrix ftp	
0 13:40:00	0 13:41:00 13:	:42:00 13:43:00 1	3:44:00 13:45:00	13:46:00 13:47:00	13:48:00 13:49:00 13:50:	00 13:51:00 13:52:00 1	13:53:00 13:54:00 13:54:36	Total	
Page 1		Total Flows 〇	Total Bytes 🗘	Total Packets O	Average Bit Rate 🗘		Q Search Peak Bit Rate ≎	Peak Packet Rate 🗘	
	Application 🗘		Total Bytes \Diamond 56.41 MB		Average Bit Rate \Diamond 501.40 Kbps	Average Packet Rate \Diamond	Peak Bit Rate 🗘		85
		Total Flows 🗘 58		Total Packets 69,834 147,584	Average Bit Rate 501.40 Kbps 218.34 Kbps				8
	Application 🗘	58	56.41 MB	69,834	501.40 Kbps	Average Packet Rate \Diamond 77.59 pps	Peak Bit Rate \Diamond 564.92 Kbps		8
	Application \Diamond rtp rtp-audio	58	56.41 MB 24.56 MB	69,834 147,584	501.40 Kbps 218.34 Kbps	Average Packet Rate \Diamond 77.59 pps 163.98 pps	Peak Bit Rate \Diamond 564.92 Kbps 270.04 Kbps		8 19 2
	Application \Diamond rtp rtp-audio 10.21.1.154	58 100 77	56.41 MB 24.56 MB 3.71 MB	69,834 147,584 7,912	501.40 Kbps 218.34 Kbps 32.97 Kbps	Average Packet Rate \Diamond 77.59 pps 163.98 pps 8.79 pps	Peak Bit Rate 564.92 Kbps 270.04 Kbps 83.46 Kbps		8 19 2
	Application \Diamond rtp rtp-audio 10.21.1.154 snmp	58 100 77 262	56.41 MB 24.56 MB 3.71 MB 2.61 MB	69,834 147,584 7,912 13,257	501.40 Kbps 218.34 Kbps 32.97 Kbps 23.23 Kbps	Average Packet Rate \Diamond 77.59 pps 163.98 pps 8.79 pps 14.73 pps 14.73 pps	Peak Bit Rate 564.92 Kbps 270.04 Kbps 83.46 Kbps 26.66 Kbps		8 19 2 1 3
	Application \Diamond rtp rtp-audio 10.21.1.154 snmp ica	58 100 77 262 68	56.41 MB 24.56 MB 3.71 MB 2.61 MB 1.44 MB	69,834 147,584 7,912 13,257 23,459	501.40 Kbps 218.34 Kbps 32.97 Kbps 23.23 Kbps 12.77 Kbps	Average Packet Rate 77.59 pps 163.98 pps 8.79 pps 14.73 pps 26.07 pps	Pesk Bit Rate 564.92 Kbps 270.04 Kbps 83.46 Kbps 26.66 Kbps 14.62 Kbps		8 19 2 1 3
	Application \Diamond rtp rtp-sudio 10.21.1.154 ssmpp lca lpftx	58 100 77 262 68 33	56.41 MB 24.56 MB 3.71 MB 2.61 MB 1.44 MB 1.41 MB	69,834 147,584 7,912 13,257 23,459 1,872	501.40 Kbps 218.34 Kbps 32.97 Kbps 23.23 Kbps 12.77 Kbps 12.50 Kbps	Average Packet Rate C 77.59 pps 163.99 pps 8.79 pps 14.73 pps 2.607 pps 2.08 pps 2.08 pps	Peak Bit Rate		8 19 2 1 3
	Application \Diamond rtp rtp-audio 10.21.1.154 ssmpp ica ipfix statistical-p2p	58 100 77 262 68 33 109	56.41 MB 24.56 MB 3.71 MB 2.61 MB 1.44 MB 1.41 MB 1.14 MB	69,834 147,584 7,912 13,257 23,459 1,872 2,071	501.40 Kbps 218.34 Kbps 32.97 Kbps 23.23 Kbps 12.77 Kbps 12.50 Kbps 10.12 Kbps	Average Packet Rate C 77.59 pps 163.98 pps 8.79 pps 14.73 pps 2.08 pps 2.08 pps 2.30 pps 2.30 pps	Peak Bit Rate 564.92 Kbps 270.04 Kbps 83.46 Kbps 2.666 Kbps 14.62 Kbps 7.271 Kbps 13.74 Kbps		

Figure 3

Notice that this report is looking at All Devices and all outbound Interfaces tagged with WAN.

Review the applications on the network – examples of business-critical applications are represented. Notice the ratios of these examples may not be representative of real networks.

This provides a good general breakdown of the overall usage of the business critical on the WAN network as a whole

Run the Reports > Flow > Network > Interface Bandwidth Summary Report

- a. Keep all filters and report at their default settings
- b. Execute Report



This will provide an understanding of each sites' overall WAN utilization.

Re-run this report, but update the Search to: "flow.app=rtp"

This provides an understanding of the utilization of just Voice (rtp) on each WAN circuit.

Re-run this report but update the Search to: "flow.app=10.21.1.154"

This provides an understanding of the utilization of an as yet unidentified application on each WAN circuit.

NXOF-2.LWA.2.0.0



Figure 5

Re-run this report but update the Search to view other key applications as desired.

Run the Report Site Traffic

- a. Keep all filters and report at their default settings
- b. In the report settings select WAN Devices, and All WAN Interfaces.
- c. Execute Report

GENERAL SETT	INGS			REPORT LIST		REPORT DETAILS	
Name				: Interface Bandwidth Summary (Flow)	Fast 🗇 🗃	Report Name	Flow Type
Interface Ban	dwidth Summa	ary		Add New Report	+	Interface Bandwidth Summary	Basic Flow 🗸
Presentation M	lode					Report Description	Execution Type
Standard						Enter report description	Time Series ~
ootnote						Devices	Sort By
Enter report g	roup description	on				All WAN Devices	V Bit Rate V
ime Zone			DST			Interfaces	Business Hours
(GMT-05:00)	America/New Y	York	~			All WAN Interfaces	All Hours
ime Range						Flex Search 🕜	Cannot be used with All Device
Custom						flow.app=rtp	× Auto ~
							1 minut
Start Date	Start Time	End Date	End Time			Display Filter	Raw Flow Data
06/30/2022	13:43	06/30/2022	13:58			No Display Filtering	Due to the options selected, this report will utilize the Raw Flow datastore (slower).
Flex Search 🔞							annee the rail field addatate (alerter).
Ex.: site=Hon	olulu & wan & f	low.app=http	×				
Display Filter							
Select Display	/ Filter						
Sharing Setti	ngs						

Figure 6

Observe the breakdown of bandwidth between site pairs.

Re-run this report, but update the Search to: "flow.app=rtp"

This provides an understanding of just Voice (rtp) on for the site pairs.

Re-run this report but update the Search to view other key applications as desired.

Run the Reports > Flow > Address > **Destination Site Traffic**

- a. Keep all filters and report at their default settings
- b. In the report settings select WAN Devices, and All WAN Interfaces.
- c. Execute Report

								View Sched	lule C	reate Repoi
te Traffic,	, Last Fifteen Minu	ites				View Op	tions ~ Share P	Print Schedule	Сору	Clos
e Traffic (F	Flow)									e de la companya de la
ice: All WAN	N Devices Interface: All	WAN Interfaces Display Filte		Irection: Outbound Flo	w Type: Basic Flow Execu	tion Type: Time Series Sort By	r: Bit Rate Bin Duration: Auto Sta	Irt Time: Jun 30, 2022 13:55:1	16 EDT (GMT-04:0	10)
0		8:00 13:59:00 14:00	:00 14:01:00	14:02:00 14:03:00	14:04:00 14:05:0	0 14:06:00 14:07:00	14:08:00 14:09:00	Hq/LA NY/Hq Hq/NY Unknown Internet/ 14:10:16		:
13:56:00	13:57:00 13:58						Q Search			
13:56:00	13:57:00 13:56						-			
	Source Site 🛇	Destination Site \Diamond	Total Flows 🗘	Total Bytes 🛇	Total Packets 🛇	Average Bit Rate \Diamond	Average Packet Rate 🛇	Peak Bit Rate 🛇	Peak Packe	
		Destination Site \Diamond HQ	Total Flows 🗘 289	Total Bytes 🗘 42.54 MB	Total Packets 🗘 118,785	Average Bit Rate 🗘 378.17 Kbps		Peak Bit Rate 🗘 452.98 Kbps	Peak Packe	t Rate 🗘
	Source Site 🗘						Average Packet Rate 🗘		Peak Packe	t Rate 🗘 141 g
	Source Site 🗘	HQ	289	42.54 MB	118,785	378.17 Kbps	Average Packet Rate 🗘 131.98 pps	452.98 Kbps	Peak Packe	t Rate 🗘 141 (134 (
egend 🗘	Source Site 🗘 LA HQ	HQ LA	289 283	42.54 MB 39.21 MB	118,785 107,557	378.17 Kbps 348.51 Kbps	Average Packet Rate \Diamond 131.98 pps 119.51 pps	452.98 Kbps 401.34 Kbps	Peak Packe	t Rate 🗘 141 134 93 j
Legend 🗘	Source Site 🗘 LA HQ NY	HQ LA HQ	289 283 475	42.54 MB 39.21 MB 11.08 MB	118,785 107,557 59,625	378.17 Kbps 348.51 Kbps 98.48 Kbps	Average Packet Rate 131.98 pps 119.51 pps 66.25 pps	452.98 Kbps 401.34 Kbps 188.74 Kbps	Peak Packe	t Rate 141 p 134 p 93 p 39 p 0 p

Figure 7

Observe which sites are being sent the most data.

Re-run this report, but update the Search to: "flow.app=rtp"

This provides an understanding of which sites are receiving the most Voice (rtp).



Figure 8

Re-run this report but update the Search to view other key applications as desired.

Run the Reports > Flow > Address > **Source Site Traffic Report**

- a. Keep all filters and report at their default settings
 - b. In the report settings select WAN Devices, and All WAN Interfaces.
 - c. Execute Report

						New Features! 🔺 17 🔲 0	• 0 🌲 210 {-} *	Ø - ⇔ - View Schedule	admin
ource Site	Traffic, Last Fiftee	en Minutes				View Options	 Share Print 	Schedule Copy	Close
urce Site T	raffic (Flow)								ø
	Devices Interface: All V	VAN Interfaces Display Filter: No Displ	ay Filtering Direction: Inbound	Flow Type: Basic Flow Execution Type:	Time Series Sort By: Bit Rate Bin Duration:	Auto Start Time: Jun 30, 2022 14:02:48 EDT (GMT-04:	00) End Time: Jun 30, 2022 14:17:48 ED	T (GMT-04:00) Bin Interval: 1	minute
2								HQ LA NY Unknown	=
								Internet	
								Total	
								Total	
0 14:03:00	14:04:00	14:05:00 14:06:00	14:07:00 14:08:00	14:09:00 14:10:00	14:11:00 14:12:00 14:12	1400 141400 141500 1	4:16:00 14:17:48		
0 14:03:00	14:04:00	14:05:00 14:06:00	14:07:00 14:08:00	14:09:00 14:10:00	14:11:00 14:12:00 14:13	14:14:00 14:15:00 1	4:16:00 14:17:00 14:17:48 Q Search		
0 14:03:00	14:04:00 Site ≎	14:05:00 14:06:00 Total Flows ©	1407:00 1498:00 Total Bytes ≎	1439:00 1410:00 Total Packets 🗘	14:11:00 14:12:00 14:13 Average Bit Rate ≎	100 141400 141500 1 Average Packet Rate ≎			
							Q Search Peak Bit Rate 🗘	8	
	Site 🗘	Total Flows 🗘	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate \Diamond	Average Packet Rate 🛇	Q Search Peak Bit Rate \Diamond 448.86 Kbps	8	215 pt 135 pt
	Site 🗘 HQ LA NY	Total Flows 2.279 216 398	Total Bytes 0 44.08 MB 40.52 MB 10.99 MB	Total Packets 147,887 108,506 54,359	Average Bit Rate 🗘 391.80 Kbps 360.21 Kbps 97.65 Kbps	Average Packet Rate 164.32 pps 120.56 pps 60.40 pps	Q. Search Peak Bit Rate 0 448.86 Kbps 434.26 Kbps 155.79 Kbps	8	215 p 135 p 81 p
	Site 🗘 HQ LA	Total Flows 2,279 216	Total Bytes 44.08 MB 40.52 MB	Total Packets 147,887 108,506	Average Bit Rate 🗘 391.80 Kbps 360.21 Kbps	Average Packet Rate \Diamond 164.32 pps 120.56 pps	Q. Search Peak Bit Rate 448.86 Kbps 434.26 Kbps 155.79 Kbps 424 bps	8	215 p 135 p

Figure 9

Observe which sites are sending the most data.

Re-run this report, but update the Search to: "flow.app=rtp"

This provides an understanding of which sites are sending most Voice (rtp).

Re-run this report but update the Search to view other key applications as desired.

After running these reports, we now have a good understanding of how the network is being utilized. We also know per application the breakdown of bandwidth utilization per site.

We will want to keep this understanding in mind as we continue through the lifecycle of the QoS project and beyond.

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 Lab 1.2: Building Filters

This Lab uses the Engineering Console.

The reports we have used so far were using **NBAR** for recognizing specific types of traffic such as Voice (rtp). This can be an excellent way to see specific applications that are known by **NBAR**. In real networks though, **NBAR** is a great, but not a perfect solution for recognizing traffic. Often, one may see multiple different **NBAR** definitions for the same type of application (**cisco-phone-audio and cisco-jabber-audio**) if no NBAR Protocol Pack standardization has occurred or NBAR will return **unknown results** if Protocol Packs are old.

To overcome these challenges with recognizing specific applications of interest, Custom Applications and Application Groups provide an excellent way to administratively define application definitions. As an example, we are now going to build custom applications and an Application Group in LiveNX that could be used for recognizing a **Cisco CallManager IP Phone system**. This is just one example. In a real network the concepts presented should be repeated for other applications of interest on the network.

Lab Steps:

• From the LiveAction map, select the Flow Tab

Dashboard Manage »	Qua How touting IF SEA EAN
Q,-	🕂 🗣 🖏 🗸 📮 🖣 🔍 Tab
Name	Search Example: (site = Honolulu
→ A Home HQ LA NY	

Figure 10

• To Edit or Create a filter, click the 🖾 icon from the options at the top of the map:

All Flow Types	Current Time	٢	Current Polling Interval	٢	Ģ	*DefaultFilterGroup	(Top 50	0	DSCP	 ٢
Figure 11											

• The Display Filters Setup Dialog appears

) 🔘 🔴 🛛 👘	ow Display Filters Setup
Create Filter The Copy The Delter The Remove Reference To EfaultFilterCroup The Remove Reference The Remove Reference The Remove Reference Add Dthr Filter The Remove Reference The Remove Reference The Remove Reference The Remove Reference * "DefaultFilterCroup The Remove Reference The Remove Reference The Remove Reference The Remove Reference * Under Referenced Filter: The Remove Reference The Remove Reference The Remove Reference * Under Referenced Filter: The Remove Reference The Remove Reference The Remove Reference * Videa Referenced Filter: Notes The Remove Reference The Remove Reference * Undea Referenced Filter: Notes The Remove Reference The Remove Reference * Undea Referenced Filter: Notes The Remove Reference The Remove Reference * [Intervoris Referenced Filter: Notes The Remove Reference The Remove Reference * [Intervoris Referenced Filter: Notes The Remove Reference The Remove Reference * [Intervoris Referenced Filter: Notes Remove Reference The Remove Reference * [Routing] Referenced Filter: No	Filter Entry Action: Show or Hide the following IP Type: IP v4 Only IP v6 Only Both IP v4 & IP v6 Color Mapping Label & Color: Web Color Mapping Label & Color: Veb Basic Advanced Select from a pre-defined list of protocols/applications or create new definitions Color Mapping Label & Color: Veb
	Match IP, Range, Subnet
	Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)
	Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g.,
nse füher filter sided a entire an en sideble han ha tan he slited by si	Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1) Match DSCP Match Device Interface Match flows traversing through a particular device's interface inhound and Outbound Combined Outbound Note: Items marked with a (*) are non-historical
ote: Other filters added as entries are not editable here, but can be edited by selv e Filter drop-down box.	Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1) Match DSCP Match Device Interface Match flows traversing through a particular device's interface inhound and Outbound Combined Outbound Note: Items marked with a (*) are non-historical

Figure 12

• In the Filter selection pull-down, select the Voice Filter

Create Filter Popy Cleate Rename	Filter Entry Details Filter Entry Action: O Show or Hide the following
Teredo by IP	IP Type: O IPv4 Only IPv6 Only Both IPv4 & IPv6
Martine Could State Stat	Color Mapping Label & Color: Skinny
	Basic Advanced
Video	Match Protocol/Ports
Voice Web	Select from a pre-defined list of protocols/applications or create new definitions

Figure 13

In its default form, the Voice filter is not built for any specific Vendor's solution. We will modify this filter to make it useful in a Cisco CallManager environment. We will Delete, Add, and edit the Entries of the Filter.

NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook 2
	Flow Display Filters Setup
Create Filter Point Filter Filter Voice Filter Entries Point Filter Add Entry Point Point Voice Point Point Voice Point Point Plying Show IPv4 Only (Prot/App=voip) Point	Filter Entry Details Filter Entry Action: Show or Hide the following IP Type: IPv4 Only IPv6 Only Both IPv4 & IPv6 Color Mapping Label & Color: VoIP Basic Advanced
Skinnyl Show IPv4 Only (Prot/App=skinny) Ventrilo TCP] Show IPv4 Only (Prot/App=ventrilo tcp) Ventrilo UDP] Show IPv4 Only (Prot/App=ventrilo udp) H323] Show IPv4 Only (Prot/App=h323) RTP] Show IPv4 Only (Prot/App=sip) (SIP] Show IPv4 Only (Prot/App=sip)	Select from a pre-defined list of protocols/applications or create new definitions voip Voip U (L4 Protocol=UDP) AND (Src OR Dst=13958 OR 16384)
	Match IP, Range, Subnet Match IP Addresses Regardless of Source or Destination
	Source: Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)
	O (BE)
	Match Device Interface Match flows traversing through a particular device's interface Branch1-LA.dcloud.cisco.com GigabitEthernet1 Ginbound and Outbound Combined Inbound Note: Intergenergied with a (f) are area. Notestrained
Note: Other filters added as entries are not editable here, but of the Filter drop-down box. Help	can be edited by selecting them in Note: Items marked with a (*) are non-historical OK Cancel Apply

Figure 14

- Delete unused Entries
 - VolP
 - Ventrilo TCP
 - Ventrilo UDP
- Add Entry

Note: The following filters may already be present in the Training Pod. Name YOUR new filters with YOUR name or initials.

- Name it MGCP
- Tick "Match Protocols/Ports"
- In the dropdown, select MGCP
- Also select Match DSCP = 31

LiveNX Foundations Workbook 2

😵 Create Filter 🛛 🤯 Copy 📡 Delete 😿 Rename	Filter Entry Details Filter Entry Action: Show or Hide the following IP Type: IPv4 Only IPv6 Only Both IPv4 & IPv6
ilter Entries	Color Mapping Label & Color: MGCP
💫 Add Entry 🕞 Add Other Filter 🕃 Delete Entry 🔯 🐘	Basic Advanced
Voice	
 [Skinny] Show IPv4 Only (Prot/App=skinny) [H323] Show IPv4 Only (Prot/App=h323) [RTP] Show IPv4 Only (Prot/App=rtp) 	Select from a pre-defined list of protocols/applications or create new definitions
 [SIP] Show IPv4 Only (Prot/App=sip) [MGCP] Show IPv4 Only (Prot/App=mgcp) AND (DSCP=0 (BE)) 	mgcp 😌 🔶 Create 🥖 Edit 🗅 Copy
	Match IP, Range, Subnet Match IP Addresses Regardless of Source or Destination
	Source:
	Source: Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1–10.100.0.1)
	Source: Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1) Match DSCP 0 (BE) 29 30 (Wr55)
	Source: Destination: Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)



Edit Entries the following entries with these updates:

H323 - TCP/UDP = Src or Dst = 1718 1719 1720 and DSCP = 46 SIP - TCP/UDP = Src or Dst = 5060 5061 5062 and DSCP = 46 Skinny - TCP = Src OR Dst = 2000 2001 2002 and DSCP = 46 RTP - UDP = Src AND Dst = 16384-32767 and DSCP = 34

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

	Flow Display Filters Setup
🌾 Create Filter 😽 Copy 📡 Delete 😿 Rename	Filter Entry Details
Filter: Voice	Filter Entry Action: O Show or O Hide the following
Filter Entries	IP Type: O IPv4 Only IPv6 Only Both IPv4 & IPv6
Add Entry C Add Other Filter Delete Entry	Color Mapping Label & Color: RTP
Voice	Basic Advanced
 [Skinny] Show IPv4 Only (Prot/App=skinny) AND (DSCP=46 (EF)) [H323] Show IPv4 Only (Prot/App=h323) AND (DSCP=46 (EF)) [RTP] Show IPv4 Only (Prot/App=rtp) AND (DSCP=24 (AF41)) [SP] Show IPv4 Only (Prot/App=mgcp) AND (DSCP=21 (AF41)) [MGCP] Show IPv4 Only (Prot/App=mgcp) AND (DSCP=31) 	Match Protocol/Ports Select from a new chined inst of protocors/ ap, Nortions or create new definitions rtp Create Edit Impy rtp (14 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767)) (14 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767)) (15 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767)) (Dst=16384-32767) AND (Dst=16384-32767) (Dst=16384-32767) AND (Dst=16384-32767) (Dst=16384-32767) (Dst=16384-32767) AND (Dst=16384-32767) (Dst=16384-32767) (Dst=16384-32767) AND (Dst=16384-32767) (Dst=16384-32767) (Dst=16384-32767) AND (Dst=16384-32767) (Dst=1
	*Branch1-LA.dcloud.cisco.com 🗘 *GigabitEthernet1 🗘
	Inbound and Outbound Combined Inbound Outbound Note: Items marked with a (*) are non-historical
Note: Other filters added as entries are not editable here, but can be edited by s the Filter drop-down box.	
Help	OK Cancel Apply
	UK Cance Appry
Figure 16	
Protocols/Applications Setup	
🕂 Create Definition 🗈 Copy 💥 Delete 💹 Rename	
Defined Protocols/Applications: rtp	
Entries	
🔁 Add Entry 🔽 Add Defined Prot/App 🕃 Delete	
Trp	
	84-32767))
Note: Defined protocols/applications added as entries the not e here, but can be edited by selecting them in the drop-rown box	
Entry Details	
Layer 4 Protocol: UDP (17)	
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)	
Неір ОК	Cancel



• When finished, you should have something that looks like the following:

- MGCP TCP/UDP = Src OR Dst = 2427 2727 & TCP = Src or Dst = 2428 and DSCP=31
- H323 TCP/UDP = Src **OR** Dst = 1718 1719 1720 and DSCP=46
- Skinny TCP = Src OR Dst = 2000 2001 2002 and DSCP=46
- SIP TCP/UDP = Src **OR** Dst = 5060 5061 5062 and DSCP=26
- RTP UDP = Src AND Dst = 16384-32767 and DSCP=34

Note: This updated voice filter will work well for our Lab purposes, but in a real networks, it would probably be best to also include IP addresses and/or subnets to these filters for eliminating any false positives.

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 Lab 1.3: Validating Filters

This Lab uses the WebUI and Engineering Console.

The example Filter we created should show us the Voice traffic in our network. The following reports will allow us to confirm the traffic.

Lab Steps:

• From the LiveNX Client map, select the Flow Tab



Figure 18

From the options at the top of the map, select the following settings

 				-								_
All Flow Types	٢	Current Time	٢	Current Polling Interval	Image: Control of the second secon	Voice	3	Top 50	٢	۲	Display Filter Colors	٢
 0										_		

Figure 19

You should be presented with a Flow visualization similar to the following diagram



Figure 20

Confirm in the legend there is Voice traffic being matched. You should see RTP & SIP being matched.



Figure 21

Run the Miscellaneous > User Filter report

- a. Select the Voice filter, but leave all parameters at their default settings
- b. In the report settings select WAN Devices, and All WAN Interfaces.

ENERAL SETTINGS	REPORT LIST		REPORT DETAILS		
lame	User Filter (Flow)	Fast 🗈 🗃	Report Name		Flow Type
User Filter, Last Fifteen Minutes	Add New Report	+	User Filter		Basic Flow
resentation Mode			Report Description		Execution Type
Standard ~			Enter report description		Time Series
ootnote			Devices		Sort By
Enter report group description			All Devices		Bit Rate
ime Zone 🕑 DST			Interfaces		Business Hours
(GMT-05:00) America/New York			All Interfaces		All Hours
					Cannot be used with All De
ïme Range			Flex Search 🕢		Bin Duration
Custom			Ex.: site=Honolulu & wan & flow.app=http	×	Auto
tart Date Start Time End Date End Time			Display Filter		
06/30/2022 15:00 06/30/2022 15:15			Voice	\sim	Raw Flow Data
		L			Due to the options selected, this report will utilize th Raw Flow datastore (slower).
lex Search 😡			Direction		
Ex.: site=Honolulu & wan & flow.app=http ×			Inbound and Outbound Combined		
EX. site-Honolulu & wall & now.app-http					
isplay Filter					
Select Display Filter 🗸					
sharing Settings					
- H \Z.					

Figure 22

c. Execute Report



NXOF-2.LWA.2.0.0

Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically "WAN" interfaces. This will show the volume of bandwidth of the matched applications in the Voice filter

Run the Reports > Flow > Applications > **Application** report

- a. Select the Voice filter, but leave all parameters at their default settings
- b. In the report settings select WAN Devices, and All WAN Interfaces.
- c. Execute Report

								View Schedule	
lication						View Options ~	Share Print	Schedule Copy	Ck
ation (F	low)								
All WAN I	Devices Interface: All WAN interfaces Displ	lay Filter: Voice Direction: Outbour	nd Flow Type: Basic Flow Exe	cution Type: Time Series Sort By: Bit	Rate Bin Duration: Auto Start Time: Ju	n 30, 2022 15:11:45 EDT (GMT-04:00) End Time: J	un 30, 2022 15:26:45 EDT (GMT-04:00)	Bin interval: 1 minute	
500								Ianrevagent TRG Identified Traffic	
0	0 15:13:00 15:14:00	15:15:00 15:16:00	15:17:00 15:18:00	15:19:00 15:20:00	15:21:00 15:22:00	152300 152400 1525		statistical-conf-video	
15:12:00	a 15:13:00 18:14:00	15:15:00 15:16:00 Total Flows ≎	15:17:00 15:18:00 Total Bytes 수	15:19:00 15:20:00 Total Packets ≎	15:21:00 15:22:00 Average Bit Rate ≎		0 15:26:00 15:26:45	statistical-conf-video	
15:12:00						Q	0 15:26:00 15:26:45 Search	Peak Packet Rate 🗘	
15:12:00	Application \Diamond	Total Flows 🗘	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🗘	Q Average Packet Rate \Diamond	00 1526:00 1526:45 Search Peak Bit Rate 🛇	Peak Packet Rate 0	8
15:12:00	Application \Diamond rtp	Total Flows 🗘 57	Total Bytes 🗘 55.70 MB	Total Packets 🗘 68,897	Average Bit Rate \bigcirc 495.14 Kbps	Q Average Packet Rate \Diamond 76.55 pps	0 152600 152645 Search Peak Bit Rate 0 573.15 Kbps	Peak Packet Rate 0	8
15:12:00	Application © rtp rtp-audio	Total Flows \Diamond 57 102	Total Bytes 55.70 MB 25.09 MB	Total Packets 68,897 150,675	Average Bit Rate \Diamond 495.14 Kbps 223.05 Kbps	Average Packet Rate \Diamond 76.55 pps 167.42 pps	0 1526:00 1526:45 Search Peak Bit Rate ≎ 573.15 Kbps 273.38 Kbps	Peak Packet Rate 🛇	8
15:12:00	Application © rtp rtp-audio statistical-p2p	Total Flows 57 102 112	Total Bytes 0 55.70 MB 25.09 MB 1.13 MB	Total Packets 68,897 150,675 2,043	Average Bit Rate 495.14 Kbps 223.05 Kbps 10.06 Kbps	Average Packet Rate \Diamond 76.55 pps 167.42 pps 2.27 pps	0 152600 152645 Search Peak Bit Rate ○ 573.15 Kbps 273.38 Kbps 13.18 Kbps	Peak Packet Rate 🗘	8
15:12:00	Application © rtp rtp-audio statistical-p2p slp	Total Flows 57 102 112 59	Total Bytes 55.70 MB 25.09 MB 1.13 MB 1.10 MB	Total Packets 68,897 150,675 2,043 10,828	Average Bit Rate 495.14 Kbps 223.05 Kbps 10.06 Kbps 9.81 Kbps	Average Packet Rate \Diamond 76.55 pps 167.42 pps 227 pps 12.03 pps	0 152650 152645 Search Peak Bit Rate 0 573.15 Kbps 273.38 Kbps 13.18 Kbps 12.66 Kbps	Peak Packet Rate 🗘	80 200 3 18
	Application 0 rtp rtp-audio atatistical-p2p sip openwebnet	Total Flows 🗘 57 102 112 59 49	Total Bytes 55.70 MB 25.09 MB 1.13 MB 1.10 MB 746.36 KB	Total Packets 68,897 150,675 2,043 10,828 1,003	Average Bit Rate 495.14 Kbps 223.05 Kbps 10.06 Kbps 9.81 Kbps 6.63 Kbps	Q Average Packet Rate © 76.55 pps 167.42 pps 2.27 pps 12.27 pps 12.29 pps 1.11 pps 1.11 pps	0 152600 152645 Starch Peak Bit Rate ○ 573 15 Kbps 273 38 Kbps 133 18 Kbps 133 18 Kbps 12 66 Kbps 9,74 Kbps	Peak Packet Rate 0	86 200 3 115 1 7 7

Figure 24

Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically "WAN" interfaces.

Review the applications matching the Voice Filter. Notice how NBAR sees voice (rtp), sip and video.

Is this right? Shouldn't we just see Voice (rtp and sip) in this report?

Run the Reports > Flow > Analysis > IPs and Ports report

- a. Select the Voice filter, but leave all parameters at their default settings
- b. In the report settings select WAN Devices, and All WAN Interfaces.
- c. Execute Report

															View Schedul	le Create Rep
s and Por	ts, Last Fifteen M	inutes										View 0	Options ~	Share Prir	Schedule	Copy
and Ports	(Flow)															
e: All WAN	Devices Interface: All	WAN Interfaces Display	Filter: Voice Direc	tion: Outbound	Flow Type: Bas)	c Flow Execution Ty	pe: Time Series	Sort By: Bit Rat	e Bin Duration	Auto Should	Walt For Dns Resolut	ion: false Start Tim	e: Jun 30, 2022 16:0	3:00 EDT (GMT-04:00)	End Time: Jun 30, 2022 16	5:18:00 EDT (GMT-04:00)
terval: 1 n	inute															
00																/198.18.128.81/UDP/ .81/198.19.1.81/UDP/
															— 198.18.128	.80/198.19.1.80/UDP/
500															198.18.128	.84/198.19.1.84/UDP/
500															198.19.2.88	4/198.18.128.84/UDP/ 3/198.18.128.88/UDP/
															— 198.19.1.81	0/198.18.128.80/UDP/ 1/198.18.128.81/UDP/
,															Total	.81/198.19.1.81/UDP/
16:04	16:05	16:06	16:07	16:08	16:09	16:10	16:11	16	:12	16:13	16:14	16:15	16:16	16:17	16:18	
	/3 >>>												Q Se	arch		
Page I																
	Src User Name 🗘	Dst User Name 🗘	Src IP Addr 🗘	Src Site 🗘	Src Port 🗘	Dst IP Addr 🗘	Dst Site 🗘	Dst Port 🗘	Protocol 🗘	DSCP 🗘	Application 🗘	Total Flows 🗘	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🗘	
		Dst User Name 🗘	Src IP Addr 🗘 198.19.1.81	Src Site 🗘	Src Port 🗘 20100	Dst IP Addr 🗘 198.18.128.81	Dst Site 🗘 HQ	Dst Port 🗘 20100	Protocol 🗘	DSCP 🗘 34 (AF41)	Application \bigcirc	Total Flows 🗘	Total Bytes ≎ 14.42 MB	Total Packets 🗘 17,864	Average Bit Rate 🗘	Average Packet Ra
																Average Packet R 19.8
gend 🗘	Src User Name 🗘		198.19.1.81	LA	20100	198.18.128.81	HQ	20100	UDP	34 (AF41)	rtp	15	14.42 MB	17,864	128.18 Kbps	Average Packet Ra 19.8
gend 🗘	Src User Name 🗘 -		198.19.1.81 198.18.128.81	LA HQ	20100 20100	198.18.128.81 198.19.1.81	HQ	20100 20100	UDP UDP	34 (AF41) 34 (AF41)	rtp rtp	15 14	14.42 MB 13.77 MB	17,864	128.18 Kbps 122.37 Kbps	Average Packet Ra 19.81 18.93 18.85
gend 🗘	Src User Name 🗘 - -	•	198.19.1.81 198.18.128.81 198.18.128.80	LA HQ HQ	20100 20100 20100	198.18.128.81 198.19.1.81 198.19.1.80	HQ LA LA	20100 20100 20100	UDP UDP UDP	34 (AF41) 34 (AF41) 34 (AF41)	rtp rtp rtp	15 14 14	14.42 MB 13.77 MB 13.74 MB	17,864 17,037 16,999	128.18 Kbps 122.37 Kbps 122.09 Kbps	Average Packet Re 19.8 18.9 18.8 18.8 18.4
	Src User Name 🗘 - - -	•	198.19.1.81 198.18.128.81 198.18.128.80 198.19.1.80	LA HQ HQ LA	20100 20100 20100 20100	198.18.128.81 198.19.1.81 198.19.1.80 198.18.128.80	HQ LA LA HQ	20100 20100 20100 20100	UDP UDP UDP UDP	34 (AF41) 34 (AF41) 34 (AF41) 34 (AF41)	rtp rtp rtp rtp	15 14 14 14	14.42 MB 13.77 MB 13.74 MB 13.44 MB	17,864 17,037 16,999 16,643	128.18 Kbps 122.37 Kbps 122.09 Kbps 119.49 Kbps	Average Packet Ra 19.8 18.9 18.8 18.4 33.0
gend 🗢	Src User Name	•	198.19.1.81 198.18.128.81 198.18.128.80 198.19.1.80 198.18.128.84	LA HQ HQ LA HQ	20100 20100 20100 20100 31196	198.18.128.81 198.19.1.81 198.19.1.80 198.18.128.80 198.19.1.84	HQ LA LA HQ LA	20100 20100 20100 20100 19420	UDP UDP UDP UDP UDP	34 (AF41) 34 (AF41) 34 (AF41) 34 (AF41) 46 (EF)	rtp rtp rtp rtp rtp-audio	15 14 14 14 14 15	14.42 MB 13.77 MB 13.74 MB 13.44 MB 5.94 MB	17,864 17,037 16,999 16,643 29,723	128.18 Kbps 122.37 Kbps 122.09 Kbps 119.49 Kbps 52.84 Kbps	Average Packet Ra 19.8 18.9 18.8 18.4 33.0 32.1
egend 🗢	Src User Name 	• • • •	198.19.1.81 198.18.128.81 198.18.128.80 198.19.1.80 198.19.1.80 198.19.1.84 198.19.1.84	LA HQ HQ LA HQ LA LA	20100 20100 20100 20100 31196 31196	198.18.128.81 198.19.1.81 198.19.1.80 198.19.1.80 198.19.1.84 198.18.128.84	HQ LA LA HQ LA HQ	20100 20100 20100 20100 19420 19420	UDP UDP UDP UDP UDP UDP	34 (AF41) 34 (AF41) 34 (AF41) 34 (AF41) 34 (AF41) 46 (EF) 46 (EF)	rtp rtp rtp rtp rtp-audio rtp-audio	15 14 14 14 14 15 15	14.42 MB 13.77 MB 13.74 MB 13.44 MB 5.94 MB 5.78 MB	17,864 17,037 16,999 16,643 29,723 28,921	128.18 Kbps 122.37 Kbps 122.09 Kbps 119.49 Kbps 52.84 Kbps 51.42 Kbps	
egend 🗢	Src User Name 🗘 - - - - - - - - -	•	198.19.1.81 198.18.128.81 198.18.128.80 198.19.1.80 198.19.1.80 198.19.1.84 198.19.2.88	LA HQ LA HQ LA HQ LA NY	20100 20100 20100 20100 31196 31196 31196	198.18.128.81 198.19.1.81 198.19.1.80 198.19.1.80 198.18.128.80 198.19.1.84 198.18.128.84 198.18.128.88	HQ LA LA HQ LA HQ HQ HQ	20100 20100 20100 20100 19420 19420 19420	UDP UDP UDP UDP UDP UDP UDP UDP	34 (AF41) 34 (AF41) 34 (AF41) 34 (AF41) 46 (EF) 46 (EF) 46 (EF)	rtp rtp rtp rtp-audio rtp-audio rtp-audio	15 14 14 14 15 15 15	14.42 MB 13.77 MB 13.74 MB 13.44 MB 5.94 MB 5.78 MB 5.56 MB	17,864 17,037 16,999 16,643 29,723 28,921 27,788	128.18 Kbps 122.37 Kbps 122.09 Kbps 119.49 Kbps 52.84 Kbps 51.42 Kbps 49.40 Kbps	Average Packet Ra 19.89 18.99 18.89 18.49 33.00 32.11 30.84

Figure 25

Note: In a real network, we would want to work with the various system owners and assign unique port ranges if possible. But in this example, we can use LiveNX's Filter and Search to help identify both types of traffic.

Re-run this report but update the Search to: "wan & (flow.app=rtp | flow.app=sip)".



Figure 26

Notice LiveNX provides the ability to focus on just the traffic of interest!

Note: In a real-world scenario we would repeat these steps for each of the business-critical applications to ensure LiveNX has Filters to accurately identify the traffic.

Lab 2

Lab 2: Classification & Marking

Lab 2.1: QoS Class Models

This Lab uses the Engineering Console.

Now that we have used LiveNX's Filter and Search capabilities to accurately identify and understand the business-critical traffic, we need to assign DSCP markings (QoS tags) on the traffic. In this lab, we are going to use the following 5 class QoS model:

Class Type/Name	5 Class Model	Business Critical Traffic
Voice	EF (46)	rtp
Video	AF41 (34)	openwebnet
High Priority Data	AF31	SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce
Scavenger	CS1 (8)	Unknown yet
Best Effort	BE (0)	n/a

Figure 27

We need to now update the legends in LiveNX to understand these selected DSCP values of interest.

Lab Steps:

• From the LiveNX Client, select the Flow Tab



Figure 28

From the options at the top of the map, select the	ren:
All Flow Types 💌 Current Time 💌 Current Polling Interval	🔽 🖙 Voice 💽 🔽 Top 50 🔽 🗗 DSCP

Figure 29

Set the Attribute to DSCP

Update the values to match those selected for the lab's 5 class QoS model.

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

Color Mapping	×
Select an attribut each value.	e to remap the flow colors. Click the color swatch to modify the color for
Attribute DSCP	×
Select a DSCP v	alue from the drop-down lists below
DSCP	0 (BE)
DSCP	18 (AF21)
DSCP	26 (AF31)
DSCP	34 (AF41)
DSCP	8 (C51)
DSCP	24 (C53)
DSCP	32 (C54)
DSCP	48 (C56)
DSCP	46 (EF)
📕 (Remaining)	
	OK Cancel

Figure 30

NXOF-2.LWA.2.0.0

Lab 2.2: Validate DSCP Markings

This Lab uses the WebUI and the Engineering Console.

Now that we have selected our QoS model, we should validate if any DSCP values are already being used.

• From the LiveAction map, select the Flow Tab



Figure 31

From the options at the top	o of the map, select the followin	g options		
All Flow Types 🔻 Current Time 💌	Current Polling Interval 🔽 🖙 Voice	Top 50	 DSCP 1	•

You should be presented with a Flow visualization like the following diagram



Figure 32

Confirm in the legend what DSCP values are seen.





Since we have the Voice Filter in place, we would hope to only see EF and/or AF31 per the 5 Class QoS model that was chosen for this network. Because there are more values seen, we will further narrow the scope of the filter.

Update the Search to "flow.direction=Egress"



Figure 34

You will see the DSCP markings that are exiting each router. It looks like LA has only BE traffic. Let's look further into exactly what protocols are using each DSCP.



NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2

Note: In the following labs the traffic shown in these images may not reflect what you see in your lab. The intent of these labs is to demonstrate the settings and *process* for using filters, not necessarily the specific traffic found.

We'll use LiveNX Engineering Client reports to investigate further.

- Run the Reports > Flow > QoS > DSCP report
 - Select the Voice filter, but leave all parameters at their default settings
 - Implement a Search of "wan"
 - Execute Report



Figure 36

Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically "WAN" interfaces. This report is good to show the overall bandwidth of Voice traffic in the network and the percent of Voice bandwidth that is / is not marked as desired.

- Run the Reports > Flow > QoS > User Filter > **DSCP Audit** report.
 - Select the Voice filter, but leave all other parameters at their default settings
 - Implement a Search of "wan"
 - Execute Report

NXOF-2.LWA.2.0.0



Figure 37

Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically "WAN" interfaces. It is showing the Source Site, the Filter match, and the DSCP value of the match.

Make note of the DSCP values, especially where you see 0 (BE). We will need to implement/fix the QoS at these sites.

Remember how the ports for Lync and rtp are in the range of 163840-32767. This means that they will both show as RTP here. We would hope to see both 46(EF) and 34 (AF41) for RTP. It is good we already see some of this, but we need to make this better.

- Run the Reports > Flow > QoS > **Application DSCP Audit** report.
 - Select the Voice filter, but leave all parameters at their default settings
 - Implement a Search of "wan"
 - Execute Report



Figure 38

Notice that this report is looking at **All Devices** and **All Interfaces** in the **outbound** direction, but specifically "**WAN**" interfaces. It is showing the Source Site, the application name as learned from NBAR, and the DSCP value of the match.

Make note of the DSCP values, especially where you see 0 (BE). We will need to implement/fix the QoS at these sites.

Also note where Video (openwebnet) is showing as 46(EF).

Note: After validating the DSCP values using the Voice Filter, you would want to create more filters for the other priority applications of the network and repeat these steps.

We will also want to ensure that any non-priority traffic is not accidently or maliciously given a high priority DSCP value.

Lab Steps:

- Run the Reports > Flow > Analysis > IPs and Application report.
 - Select No Display Filter, but leave all parameters at their default settings
 - Implement a Search of "wan & flow.dscp=EF"



• Execute Report

Figure 39

Notice the applications listed in this report.

We would hope to only see Voice (rtp) listed in this example. Anything else needs to be fixed via an update to the networks QoS policies.

We would want to re-run this same type of report but update the Search with the DSCP values of the other priority applications in the network.

Lab 2.4: Configure Classification & Marking Policies

Now that we understand the traffic of the network and the DSCP values that should be marked on each type of traffic, we can use LiveNX to implement the correct QoS policies to the traffic on the routers.

We will create a template QoS policy and apply this to the LAN interface of each of the routers to classify and mark the priority traffic properly.

Lab Steps:

• From the LiveAction map, select the QoS Tab

Dashboard Manage »	QoS	low Ro	uting	IP SL/	A LA	N
Q	⊕	₿⁄	4.	€,	Q,	A

Figure 40

Right-click on the HQ-B2 router, select QoS > Manage QoS Settings



Figure 41

NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook 2	
	Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)	
Policies	Policies Classes Interfaces Mapped Classes Class Name Classify Marking Queueing Policing Shaping Compression N	WRED DBL Unknown
	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED	DBL Unsupported
	Match on: Any	Reference Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class. Match-all: packet must meet all criteria to be a member of the class.
Help Save to Device	Preview CLI Close	

riguit 42

Select the Add Policy icon.

In the Add Policy dialog,	enter the name "SET_	DSCP_LAN
---------------------------	----------------------	----------

• • •	Add Policy	
Policy name:	SET_DSCP_LAN	
	Cancel	ОК

Figure 43

You can now see the new policy with its class-default appearing in the Policies list.



Figure 44

Right-Click on the SET_DSCP_LAN policy and select Add Class to Policy



Figure 45

Select the Create new class option and name the new class SET_DSCP_VOICE

● ○ ● Ac	dd Class to Policy			
Select one of the following	ng options:			
O Use existing class:	LIVEACTION-CLAS	S-AVC 📀		
O Create new class:	SET_DSCP_VOICE			
Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.				
	Cancel	ОК		

Figure 46

You will see the new class SET_DSCP_VOICE appear under the SET_DSCP_LAN policy

$\circ \circ \circ$	Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)
	Policies Classes Interfaces
Policies	Mapped Classes
SET DSCP_VOICE class=default	Class Name Classify Marking Queueing Policing Shaping Compression Class - Clas
	Mapped Class Detail Drop all traffic for class
	Classify Marking Queueing Policing Shaping Compression WRED
	Match on: Any
Help Save to Device	Preview CLI Cancel
Figure 47	

On the Classify Tab, select the Edit button

LiveNX Foundations Workbook 2

		Manage QoS Settings - HQ-	B2.dcloud.cis	co.com (198.18.129.26)		
	5 🔍					
		Policies	Classes In	terfaces		
Classes	Create and Edit Match	Statements				
👍 🛍 🗱	Match type:	COS	0	Match any 😒 🗮		
LIVEACTION-CLASS-A' LIVEACTION-CLASS-M	Value: 0			Match/Match not Match Typ	pe Value	
SET_DSCP_VOICE	1					
	2					
	4					
	5					
	7					
		lect up to 4 values)				
	Match/match not:	Match	()			
	Add Match Stat	tement Replace Match	Statement			
				L		
Help	Save to Device	Preview CLI Cance	el			

Figure 48

Select the Match Type dropdown and select Protocol – using NBAR

Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)		
	b 👒	
		Policies Classes Interfaces
Classes	Create and Edit Mat	ch Statements
LIVEACTION-CLASS-A'	Match type:	Protocol – using NBAR 💿 Match any 📀 🗮
LIVEACTION-CLASS-M		3com-amp3 Match/Match not Match Type Value
SET_DSCP_VOICE		3com-tsmux 3pc
		4chan
		58-city
		914c/g 9pfs
		abc-news
	Matab (matab mat	Match
	Match/match not:	Match
	Add Match S	Statement Replace Match Statement
Help	Save to Device	Preview CLI Cancel
incip	care to benee	

Figure 49

Select the value of **rtp** and click **Add Match Statement**. The protocol rtp will appear in the window at the far right of the window.

NXOF-2.LWA.2.0	.0 LiveNX Foundations Workbook 2
	Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)
Classes Classes UVEACTION-CLASS-A UVEACTION-CLASS-A UVEACTION-CLASS-A M M M M M M M M M M M M M	
Help Save to D	Device Preview CLI Cancel

Figure 50

Select the **Policies** tab at the top left of the screen. Notice the **NBAR protocol match** on the classify tab

	Policies Classes Interfaces	
SICICIES	Policies Classes Interfaces Mapped Classes Class Name Classify Marking Queueing Policing Shaping Compression V SET_DSCP_VOICE Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED Match on: Any Match : Protocol - using NBAR : rtp	WRED DBL Unknown DBL Unsupported Reference Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class. Match-all: packet must meet all criteria to be a member of the class.
	Edit	

Figure 51

• Select the Marking tab.

Select the Mark With check box and select the DSCP value of 46 (EF)
NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook 2	
	Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)	
	Policies Classes Interfaces	
Policies	Mapped Classes	WRED DBL Unknown
	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED Mark with: Solution DSCP © 46 (EF) ©	DBL Unsupported Reference Differentiate packets belonging to this class based on marking.
	 Tunnel IP ATM Cell Loss Priority Frame Relay Discard Eligible 	Mark On DSCP: marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte. Precedence: sets the precedence value in the packet header.
Help Save to Device	Preview CLI Cancel	



Repeat these same steps for adding more classes to the **SET_DSCP_LAN** policy for the other traffic types. Please use the following table for reference:

Class Name	DSCP	NBAR Protocol(s)
SET_DSCP_VOICE	EF (46)	rtp
SET_DSCP_VIDEO	AF41 (34)	MS-Lync
SET_DSCP_HIGH_PRIORITY DATA	AF31 (26)	SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce
SET_DSCP_SCAVENGER	CS1 (8)	Leave blank for now
Best Effort	BE (0)	n/a
Figure 53		

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 When finished, the **SET_DSCP_LAN** policy should look like this:

	Manage QoS Settings - HQ-B2.dcloud.cisco.com (198.18.129.26)	
2 2 2 2 2 2		
	Policies Classes Interfaces	
Policies	Mapped Classes	
	Clace Name Clace (is Marking Ouwering Policing Shaping Compression WF SET_DSCP_VOICE DSCP: EF DSCP: AF41 DSCP-VIDEO DSCP: AF41 DSCP-VIDEO DSCP: AF41 DSCP_HLPRIO DSCP: AF31 DSCP-SE BST_EFFORT DSCP: RE EsT_EFFORT DSCP: BE Class-default Class-default Class-default	RED DBL Unknown
BEST_EFFORT	Mapped Class Detail Drop all traffic for class	
	Classify Marking Queueing Policing Shaping Compression WRED I	DBL Unsupported
	Mark with: DSCP	Reference Differentiate packets belonging to this class based on marking. Mark On
	 IP ATM Cell Loss Priority Frame Relay Discard Eligible 	DSCP: marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte. Precedence: sets the precedence value in the packet header.
Help Save to Device	Preview CLI Cancel	

Select Save to Device.

Select **SET_DSCP_LAN** policy and select **Copy Policies to Devices** icon. This will allow you to push the policy you just created to the other routers in the network.

2 1 1 1 1 1 1
Policies
> 😓 LIVEACTION-POLICY-UNIFIED
V SET_DSCP_LAN
SET_DSCP_VOICE
SET_DSCP_VIDEO
DSCP_HI_PRIORITY_DATA
SET_DSCP_SCAVENGER
BEST_EFFORT
class-default



The Copy Policy to Devices dialog window appears.

NXOF-2.LWA.2.0.0

Select the policy **SET_DSCP_LAN**, check HQ-B2 and the two branch routers, and select **OK**.



Figure 56

The **SET_DSCP_LAN** policy will be copied to the other routers.

Validate the changes saved successfully.

00	Copy Policy to De	vices	
Saving to devices			
	cisco.com (198.19.1.1) cisco.com (198.19.2.1)		
HQ-B1.dcloud.cisco	.com (198.18.129.24)	Succeeded	
	Export CSV	Cancel	Close

Figure 57

Close the Copy Policy to Devices dialog window

Close the Manage QoS dialog window.

You will be prompted to save these changes to the startup configuration, click Yes.

You can click Yes three times, or select the Do not show again option.

Lab 2.5: Apply Marking Policies to Interface(s)

Lab Steps:

Dashboard Manage »	QoS Iow Routing IP SLA LAN
Q,-	🕂 🗣 🖑 🖍 📮 🔹 🔍 🛛 Audit
Name	
🗸 😓 Home	
 HQ LA NY 	

Figure 58

• Select the QoS Tab

Right-click on the LAN interface on one of the routers and select **QoS > Apply Policy to Interface**.

VI1 VI2 CI2 HQ-B2 198.18.129.21 Met.822.121 M	Device: HQ-B2	
$\langle $	QoS	✓ Enable QoS Polling
Log Or	Edit Device Settings Add or Remove Interfaces Refresh Device Remove Device Zoom to Device Device Tools	Create Policy from Template Revert QoS Configuration by user 'admin' Adjust Input QoS Adjust Output QoS Manage QoS Settings Manage NBAR
	Statistics	Apply Policy to Interface
	View	Copy Policy to Devices
	Group Management	. Reports

Note: The LAN interface will be GigabitEthernet2 on each of the routers in this lab.

Figure 59

Select the **SET_DSCP_LAN** policy and tick to apply it in the **input** direction.

Click OK.

NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook 2
Apply Policy to Interfaces	
Select a policy: SET_DSCP_LAN	0
Select the interfaces to which you want to this policy:	apply
Cancel	ок

Figure 60

Follow these same steps to apply the **SET_DSCP_LAN** policy to **the other router's LAN interface.**

Notice how when you do this for **LA router**, you will see **a little box** already around the input side of its LAN interface.



Figure 61 Right-click on the LA router and select QoS > Manage QoS Settings.

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

Notice how it has a policy on it called "**WhyIsThisHere**". Notice how the class-default of this policy is marking traffic as 0 (BE). No wonder we were seeing Voice (rtp) leaving this site as BE!

	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)	
	Policies Classes Interfaces	
Policies	Mapped Classes	ED DBL Unknown
	Mapped Class Detail Drop all traffic for class Classify Marking Queueing Policing Shaping Compression WRED D Match on: Any	DBL Unsupported
		Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class.
	Edit	Match-all: packet must meet all criteria to be a member of the class.
Help Save to Device	Preview CLI Close	

Figure 62

Select the Interface tab

	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)
2 2 2 2 2 2	
	Policies Classes Interfaces
Interfaces	
GigabitEthernet2 GigabitEthernet2 GigabitEthernet3 GigabitEthernet3 GigabitEthernet4 GigabitEthernet4 Output : <none> Output : <none> Output : <none></none></none></none>	Interface name: IP address: IP address mask: Interface description: Pre-classify Link Fragmentation: Maximum delay: ms Interleave
Help Save to Device	Preview CLI Close

Figure 63

Right-click on the **WhyIsThisHere** policy that is highlighted on the input side of the **GigabitEthernet2** interface.

NXOF-2.LWA.2.0.0



Figure 64

Select Remove Policy from Interface

Right-click on the input side of the GigabitEthernet2 interface and select Apply Policy to Interface.



Figure 65

Select the SET_DSCP_LAN policy and select OK.

•	Apply Policy to	Interface	
S	Select the policy to apply to the Input	t of interface Giga	abitEthernet2:
1	SET_DSCP_LAN		0
	•	Cancel	ОК

Figure 66

Select **Save to Device** and close the Manage QoS Settings dialog window. When prompted, save from current running configuration to startup configuration.



Figure 67

Ensure all routers have the **SET_DSCP_LAN** policy applied to their **LAN** interface.

Lab 2.6: Validate DSCP Settings

We now need to validate the QoS policies we have implemented are working correctly.

• From the LiveAction map, select the Flow Tab

Dashboard Manage	» QoS Flow touting IP SLA LAN
Q,	🕂 🗣 🖑 🖊 📮 🔹 🔍 Tab
Name	Search Example: (site = Honolulu
🗸 🕎 Home	
> HQ	
FI (0	

Figure 68

Update the filters to the following parameters

				-					
All Flow Types	Current Time	Current Polling Interval	0	🐺 Voice	0	Top 50	0	dSCP	0
E' (0			_						

Figure 69

Notice how, when the **Voice filter** is in place, we now see only DSCP values 46 (EF), 34 (AF41), and 26(AF31).



Figure 70

LiveNX Foundations Workbook 2





Figure 71

Remember how the ports for Voice (rtp) and Video (Lync) are in the range of 163840-32767. This means that they will both show as RTP here. Therefore, we are seeing 46(EF) and 34 (AF41) for RTP.

This is what we want to see - all high priority DSCP values and no 0 (BE).

Run the Reports > Flow > QOS > DSCP report

- Select the Voice filter, but leave all parameters at their default settings
- Implement a Search of "wan"
- Execute Report



Figure 72

Notice how the DSCP value of 0 (BE) disappears from the graph around the same time as we implemented our QoS Polices.

Note: For the sake of time in this lab, we are only going to focus on this one report. Remember that in a real network, you would repeat these steps for all important applications. We would use

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 the same visualization and reports as we have used previously to validate QoS polices

effectiveness for all priority traffic.

Now that we have used LiveNX to review, implement and validate our QoS Matching and Marking polices, we can now move on to step 2 of the QoS project – Prioritization.

Lab 3

Lab 3: QoS Prioritization & Queueing

Lab 3.0: Intro to Prioritization

LiveAction





In this lab we are going to use LiveNX for creating and validating Queuing and Shaping policies in our network. There are two primary questions that need to be answered before creating any configurations. These are:

- What is the bandwidth allocations needed for each queue?
- What, if any, CIRs are enforced by the service provider?

Lab 3.1: Run the Reports

We will tackle the bandwidth question first. The best way to answer this question is to use LiveNX's reporting to understand the priority application's capacity needs.

Since we have successfully created and validated Matching and Marking polices, we can now just reference the respective DSCP value's bandwidth usage to quantify our applications requirements.

Lab Steps:

- Run the Reports > Flow > Network > Interface Bandwidth Summary report
 - Leave all Filter parameters at their default settings.
 - Implement a Search of "wan & flow.dscp=EF & flow.direction=Egress"



• Execute Report

Notice how this shows a bandwidth graph of the data being transmitted out of each WAN interface. In this example, we are focused on Voice (rtp)/ EF traffic. This is the capacity planning data we need for Voice.

Run the Flow > Network > Interface Bandwidth Summary report

- Leave all Filter parameters at their default settings
- Implement a Search of "wan & flow.dscp=AF41 & flow.direction=Egress"





Notice how this shows a bandwidth graph of the data being transmitted out of each WAN interface. In this example, we are focused on Video (MS-Lync)/AF41 traffic. This is the capacity planning data we need for Video.

Run the Flow > Network > Interface Bandwidth Summary Report

- Leave all Filter parameters at their default settings
- Implement a Search of "wan & flow.dscp=AF31 & flow.direction=Egress"

A How Reports	
Q - Type here to filter reports.	Interface Bandwidth Summary
Reports Interface Bandwidth Top Analysis Ups and Ports Address Address	Interface Bandwidth Summary 15m 1h 6h 1d 1w 30d Custom
IT QoS	Source All Devices V All Interfaces V Est. non-filtered flows: 616 Utilize Long Term Cach
Network Interface Bandwidth Sur	Filter "DefaultFilterGroup V 🔄 Graph Basic Flow V Time Series V Bit Rate V
Bandwidth Summary Traffic Volume Pair	
-Outbound Bandwidth Util	Search van & flow.dscp-AF31 & flow.dscp-
Source or Destination Ne Network Pair	HQ-53.ddoud.disco.com - Ethernet0/1
Source Network	
Destination Network Bidirectional AS Pair	20 Kbps
Source or Destination At	
-AS Pair -Source AS	are the second s
-Destination AS	≝ 10 Kbos
Medianet Applications (AVC)	
B-NSEL	
● PfR ● Wireless	
Wireless AnyConnect	Oct 24, 12:20 AM Oct 24, 12:30 AM Oct 24, 12:40 AM Oct 24, 12:50 AM Oct 24, 01:00 AM Oct 24, 01:10 AM Oct 24, 01:20 AM
⊞ Miscellaneous	Date
Custom Reports	
	Number of datasets: 1
4 D	Device Interface Name Direction Total Bres Total Bres Total Bres Verage bit Rate Average bit Rate Pask bit Rate Pask Pask tet Rate ✓ H->53 Ethernet0/1 EGRESS 552 9 MB 76,316 20 Hops 21 pps/ 21 stops 21 stops 22 stops
	M H2-SJ Etherneou] Exercises 532 9/H8 76,318 20 Kdps 21 pps 21.6 Kdps 23 pps
Report Actions	
Save	
Save As	
Create	
Edit	Branch1-LA.ddoud.cisco.com - Ethernet0/2
Delete	11 kbps
Schedule	10 Kbps
PDF	9 Kbps
Export to CSV	₹ 8 Kbps
Help	2 7 Kbps
	T 6 Kbps
	4 khoe
	1 4 K DRC 1

Notice how this shows a bandwidth graph of the data being transmitted out each WAN interface. In this example, we are focused on High Priority Data/ AF31 traffic. This is the capacity planning data we need for the High Priority Data.

Note: In a real network, it would be best to have at least two weeks of data to formulate the appropriate bandwidth allocations for the priority applications. Also remember that since Priority/LLQ queues have a built-in policer, one would want to over provision the settings based on these queues.

Lab 3.2: Building Queueing Policies

• From the LiveAction map, select the QoS Tab



Right-click the HQ-B1 router, select QoS > Manage QoS Settings



The Manage QoS Dialog Window will open

Manage QoS Settings - HQ-B1.dcloud.cisco.com (198.18.129.24) ×										
5 E I I I I I I I I										
Policies Classes Interfaces										
Policies	Mapped Classe	s								
	🖳 🗈 🕞									
B- ↓ LIVEACTION-POLICY-UNIFIED B- ↓ SET_DSCP_LAN	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
		ffic for class	ng Policing	Shaping Com	pression WR	ED DBL U	nsupported	Deferee		
	Match on: An	<u>ч</u>		Edit				Criteria Match meet ai criteria the clas Match meet ai	s defined show at -any: pao t least on to be a n	left. cket must e of the nember of tet must to be a
Help						Save to I	Device Pr	review CLI		Close

Add a new Policy and name it **QUEUEING**.

Add Policy ×					
Policy name: QUEUEING					
ОК	Cancel				

Create a **new class** for the QUEUEING policy and name it **VOICE**.

Add Class to Policy ×					
Select one of the following options:					
🕕 Use existing class:	LIVEACTION-CLASS-AVC \sim				
Create new dass: VOICE					
Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.					
	OK Cancel				

You should see the VOICE class inside the policy named QUEUEING

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

Policies Classes Interfaces	
Policies	Mapped Classes
🔁 🐮 🔝 🛼 🖏 🦈	
🕀 😼 LIVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Policing Shaping Comp
	VOICE 😐
	class-default 👳
class-default	
E SET_DSCP_LAN	
	Mapped Class Detail
	Drop all traffic for class
	Classify Marking Queueing Policing Shaping Compression WREE
	Match on: Any
	E-da
	Edit

Update the Classes tab of the VOICE class to match DSCP 46 (EF) traffic

NXOF-2.LW	/A.2.0.0	LiveNX Foundations	Workbook 2	2
🛕 Manage QoS Settir	ngs - HQ-SJ.dcloud.	isco.com (198.18.129.25)		×
4 🕹 🎝	al 🗞 🔍			
Policies Classes Inter	faces			
Classes	Create and Edit Mal	ch Statements		
🔒 🗈 😹	Match type:	DSCP	Match any 💌 😻	
LIVEACTION-CLASS	Value:	40 (C55)	M Match T	Value
LIVEACTION-CLASS SET_DSCP_HIGH_P		41	Ma DSCP 46 (EF)	1.0100
SET_DSCP_SCAVEN		42 43		
SET_DSCP_VIDEO		44		
VOICE		45		
		46 (EF) 47		
		(Select up to 8 values)		
	Match/match not:	Match		
		🔲 IPv4 Only		
		Add Match Statement Replace Match Statement		
	_			
I				
Help		Save to Device	Preview CLI	Cancel

Return to the Policies tab

Ensure the **VOICE class** of **QUEUEING** policy is highlighted and select the **Queueing** tab.

Set the **Queueing type** to **Priority** and the bandwidth to **160 Kbps**.

🛕 Manage QoS Settings - HQ-SJ.dcloud.cisc	o.com (198.18.129.25)	×
Image: Second		
Policies	Mapped Classes	
E	Class Name Classify Marking Queueing Policing Shaping Com	npres WRED DBL Unkn
QUEUEING VOICE class-default E-C SET_DSCP_LAN	VOICE OPriority: 160 Kbps dass-default	
	Rate: 160 Kbps Burst size: 32 bytes Unknown elements:	BL Unsupported teference Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. Queueing Type Class-based: utilizes Class-based: utilizes Cl
Help	Save to Device Preview	CLI Cancel

NXOF-2.LWA.2.0.0 LiveNX Foundations Workbook 2 Create the following classes in the QUEUEING policy based on the following table:

Class Name	Match DSCP	Queueing
VOICE	EF (46)	Priority – 160K
VIDEO	AF41 (34)	Priority – 800K
HIGH_PRIORITY DATA	AF31 (26)	Class Based – 64K
SCAVENGER	CS1 (8)	Class Based – 8K
Best Effort	BE (0)	n/a

When finished, the QUEUEING policy should look like this:

Manage QoS Settings - HQ-SJ.dcloud.cisc	o.com (198.18.129.25)
2 2 2 2 2 2 2	
Policies Classes Interfaces	
Policies	Mapped Classes
UVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Pol Sh Com W DBL U
	VOICE Priority: 160 Kbps
VOICE	VIDEO Priority: 800 Kbps
VIDEO	HIGH_PRIORITY_DATA
HIGH_PRIORITY_DATA	SCAVENGER • Class-based: 8 Kbps
SCAVENGER class-default	class-default 🔹
E SET_DSCP_LAN	
	Mapped Class Detail
	Drop all traffic for class
	Classify Marking Queueing Policing Shaping Compression WRED DBL Unsupported
	Queueing type: Class-based Reference Reference
	Distribute the available
	Rate: 8 kbps 💌 bandwidth between
	Queue depth:
	Enable Fair Queueing guarantee to each class.
	E croper de Goodenin
	Unknown elements: Queueing Type
	Class-based: utilizes
	Class-based weighted fair
	queueing (CBMFQ) using
	derived weight for packets
	from the bandwidth allocated to the class.
Help	Save to Device Preview CLI Cancel

Click Save to Device.

Click and highlight the QUEUEING policy and select the **Copy Policies to Devices** icon.

This will allow you to push the policy you just created to the other routers in the network.Lab 3.2: Building Queueing Policies© Copyright LiveAction 2022

LiveNX Foundations Workbook 2

A Manage QoS Settings - HQ-SJ.dcloud.	isco.com (198.18.129.25)	×
Policies Classes Interfaces		
Policies	Mapped Classes	
📑 🖸 🕱 🛍 🔚 🕼 🖏 🛛	9 <u>9</u> m m m	
E- LIVEACTION-POLICY-UNIFIED	Class Name Classify Marking Queueing Po	N Sh Com W DBL U
	VOICE	
- VOICE	VIDEO	
- VIDEO	HTCH PRIORITY DATA A Class-based: 64 Khps	
	Copy Policy to Devices 🛛 🔀 s	
- SCAVENGER	Select a policy:	
class-default		
E- SET_DSCP_LAN	QUEUEING	
	Select the devices to which you want to save this policy:	
	Branch2-NY.dcloud.cisco.com (198.19.2.1)	D DBL Unsupported
	OK Cancel	Reference Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class. Queueing Type
		Class-based: utilizes Class-based weighted fair queueing (CBMFQ) using derived weight for packet from the bandwidth allocated to the class.
Help	Save to Device Pre	sview CLI Close

Push the QUEUEING policy to the other routers

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

Note: We are not applying these policies to interfaces at this step.

If you encounter a conflict - select Overwrite.



Lab 4

Lab 4: Shaping / Scaling

Lab 4.0: Intro - Shaping (Scaling)

Remember, we had stated previously that one of the key questions that needs to be answered before implementing QoS Prioritization is to understand any CIR that may be enforced by the service provider.

Below is a diagram of the lab network. The MPLS network in our lab does have CIRs in place with the following design:

HQ - no provider CIR

NY - 1.5Mb provider CIR

LA - 1.5MB provider CIR

For the sake of this lab assume there is no other QoS on the service provider's backbone.



To accommodate this design, we will need to build the following shaping policies:

- HQ Multi-class hierarchical shaping policy*
- NY basic hierarchical shaping policy
- LA basic hierarchical shaping policy

*Note - that if the service provider did have additional QoS on their backbone, then the multiclass hierarchical policy would not be a requirement.

NXOF-2.LWA.2.0.0LiveNX Foundations Workbook 2Lab 4.1: Shaping (Scaling)

Lab Steps:

- Right Click on HQ-B1 and select **Manage ACL's**. We will create some ACL's first. We will create two ACL's
 - HQ_TO_NY_ACL
 - HQ_TO_LA_ACL

	Local VII Device: HQ-B1		1
GI2 19	QoS	>	
1924	Edit Device Settings		
	Add or Remove Interfaces		/
	Refresh Device		
	Remove Device		SP2 MPL S
	Zoom to Device		
1	Device Tools	>	Save to Startup Config
	Statistics	>	Open Device Web Page
	View	>	Manage ACLs
	Group Management	>	42

- Click on **Create ACL**.
- Select Extended as the ACL Type. Let's do the HQ_TO_NY_ACL first.
- Create a rule allowing 198.18.129.0/24 to 198.19.2.0/24

Add Extended Rule Entry for HQ_TO_NY_ACL		×
permit o deny		
● IP ○ TCP ○ UDP ○ Object-Group < No Object Groups > ∨ ○ Other by Na	ame 🗸 ahp 🗸	
Source	Destination	
◯ any ④ by Network or IP 198.18.129.0/24 ◯ by Object-Group	>> () any () by Network or IP 198.19.2.0/24	🔵 by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >	e.g 192.168.1.0/24 or 192.168.1.19	< No Object Groups >
by Port Equal to V Manage Port(s)	Equal to Manage Port(s)	
Match by DSCP V		
Log Rule Log 🗸		
		OK Cancel

- Click **OK**. If you want to Preview the commands that will be sent to CLI click **Preview CLI**. Then click **Save To Device**.
- Next, create another ACL called **HQ_TO_LA_ACL**.

NXOF	-2.LWA.2.0	.0	LiveNX Fou	undati	ons V	Vorkbook	٢2
	Create ACL		2			\times	
	Type Name / Number	Extended V HQ_TO_LA_ACL			He	lp	
	Access Rules and F	Remarks					
					Create	e Rule	
					Сору	Rule	
					Create F	Remark	
					Edit Rule,	/Remark	
					Delete Rul	le/Remark	
					Move	e Up	
					Move I	Down	
			Preview CLI	Save to [Device	Cancel	

• Create Rule entry with source IP 198.19.129.0/24 and destination IP 198.19.1.0/24

Add Extended Rule Entry for HQ_TO_LA_ACL		×
permit deny		
● IP ○ TCP ○ UDP ○ Object-Group < No Object Groups > \ ○ Other by Name	e v ahp v	
Source O any O by Network or IP 198.19.129.0/24 D by Object-Group	Oestination O any O by Network or IP 198.19.1.0/24	by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 < No Object Groups >	e.g 192.168.1.0/24 or 192.168.1.19	< No Object Groups >
by Port Equal to V Manage Port(s)	<	
Match by DSCP V		
Log Rule Log V		
		OK Cancel

- Click **OK**, then **Save to Device**. (Preview the CLI commands if you want to)
- You should see the two ACLs now created.

NXOF-2.LWA.2.0.0

for HQ-B1		×
Ls)		
∧ Tvpe	Applied Interfaces	Create ACL
Extended (Named)		Edit ACL
Extended (Named)		Delete ACL
		Copy ACL
		Apply / Remove ACL
0.255 198.19.1.0 0.0.0.255		Save ACL File
		Load ACL File
	Extended (Named) Extended (Named)	Ls) Type Applied Interfaces Extended (Named) Extended (Named) Extended (Named) Extended (Named)

- Click Close.
- From the LiveAction map, make sure you are still in the QoS Tab



Right-click on the HQ-B1 router, select QoS > Manage QoS Settings



The Manage QoS Dialog Window will open

🔼 Add Policy 🛛 🗙							
Policy name: MULTI_CLASS_SHAPING							
OK Cancel							

Create two classes within this Policy:

- HQ_TO_NY
- HQ_TO_LA

Manage QoS Settings - H	IQ-B1.dclou	ıd.cisco.	com (19	8.18.129.	24)					×
친 🗐 💭 🎝 🖨 🗞										
Policies Classes Interfaces										
Policies	Mapped Classe	S								
	🕑 🔓 📗	<u>-</u>								
IVEACTION-POLICY-UNIFIED MULTI_CLASS_SHAPING	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	HQ_TO_NY	۲								
HQ_TO_LA	HQ_TO_LA class-default	•								
dass-default	class-default	•								
🗄 🐻 SET_DSCP_LAN										
	Mapped Class [etail								
	Drop all trat	ffic for class								
	Classify Marl	king Queuei	ng Policing	Shaping Com	pression W	RED DBL U	Insupported			
	Match on: An	,						Refere	nce	
	Fild Cir On. An	1							is defined	t by the
									a show at	
									h-any: pa at least or	cket must
										member of
								the cla	ISS.	
								Matel	h-all: pac	ket must
									all criteria	
								memb	er of the o	class.
				Edit						
Help						Save to	Device P	review CLI		Cancel

Edit these classes, but chose the match type of "ACL Name"

🚺 Manage QoS	5 Settings - H	Q-B1.dcloud.cisco.com (198.18.129.24	L)			\times
ella alla alla alla alla alla alla alla						
Classes	Create and Edit Mat	ch Statements		_		
Eest_Effort DATA_HIGH_PRIORITY	Match type: Value	ACL Name Any ACL Name	Match any ~ Match/Mat		Value	
HQ_TO_NY LIVEACTION-CLASS-AN LIVEACTION-CLASS-ME SCAVENGER SET_DSCP_HIGH_PRIC SET_DSCP_VIDEO SET_DSCP_VIDEO SET_DSCP_VOICE VIDEO VOICE	Match/match not:	ACL Number Class COS DSCP Frame relay DE bit Frame relay DE Dit Trame relay DLCI RTP Protocol - using NBAR HTTP Protocol - using NBAR Input interface IP Precedence MAC Destination Address MAC Source Address MPLS experimental topmost Packet length Protocol - using NBAR Protocol - using NBAR Protocol - using NBAR goS group				
Help			Sav	ve to Device	Preview CLI	Close

Match the HQ_TO_NY class to the HQ_TO_NY_ACL Match the HQ_TO_LA class to the HQ_TO_LA_ACL

Manage QoS	Settings - H	Q-B1.dcloud.cisco.	.com (198.18.129.24)				
II 4 💐 🖏 💐 🗞	5						
Policies Classes Interface Classes	create and Edit Mat	the Charles and					
	Create and Edit Mat	tch Statements					
🔒 🗈 🕱	Match type:	ACL Name		Match any	~ 🐹		
Best_Effort DATA_HIGH_PRIORITY	Value:	HQ_TO_LA_ACL		Match/Mat	Match Type	Value	
HQ_TO_LA		HQ_TO_NY_ACL		Match	ACL Name	HQ_TO_NY_ACL	
HQ_TO_NY		LIVEACTION-ACL-AVC		- Hereen	ACC Home	1021010120C	
LIVEACTION-CLASS-AV							
LIVEACTION-CLASS-ME							
SCAVENGER							
SET_DSCP_SCAVENGE							
SET_DSCP_VIDEO	Match/match not:	Match	~				
SET_DSCP_VOICE	Matchinatch hot	Match					
VIDEO		Add Match Statement	Replace Match Statement				
VOICE							
/							
< >							
Help					ave to Device	Preview CLI	Close

When finished, return to the **Policy** tab



Select the **HQ_TO_NY** class and select the **shaping** tab. Set its parameters to:

- Shape using = Average
- Rate = 1,000 Kbps
- Committed burst = 10,000
- Excess burst = 0

Select the **HQ_TO_LA** class and select the **shaping** tab. Set its parameters to:

- Shape using = Average
- Rate = 1,000 Kbps
- Committed burst = 10,000
- Excess burst = 0

Manage QoS Settings - F	HQ-B1.dclou	ud.cisco.	com (19	8.18.129.	24)					\times
2 2 2 2 2 2 2										
Policies Classes Interfaces										
Policies	Mapped Classe									
MULTI_CLASS_SHAPING HQ_TO_LA HQ_TO_NY dass-default QUEUEING VOICE VOICE	Class Name HQ_TO_LA HQ_TO_NY class-default	Classify	Marking	Queueing	Policing	Shaping 1,544 Kbps 1,544 Kbps	Compression	WRED	DBL	Unknown
DATA_HIGH_PRIORITY SCAVENGER Gas-default B & SET_DSCP_LAN	Shape using: Rate: 1,	ffic for class king Queue Average N	Kbps	Shaping Com bits bits	pression Wi	RED DBL U	Insupported	traffic bottle packe	nce of the flow and elimin necks by d ts and cor pecified bil	aate Jelaying nforming
	Overhead Accounting Offset:								allows th mission rat higher thai ng rate. age: sets t num transm o the shapi	e to n the the nission
Help						Save to	Device P	Preview CLI		Cancel

Click-Drag-and-Drop the **QUEUEING** policy to the HQ_TO_NY policy under **MULTI_CLASS_SHAPING**.

Click-Drag-and-Drop the **QUEUEING** policy to the HQ_TO_LA policy under **MULTI_CLASS_SHAPING.**

When finished your view should look like this:

Manage QoS Settings - H	Q-B1.dcloud.cisc	o.com	(198.18	129.24)						\times
친 원 위 위 위 생 책										
Policies Classes Interfaces										
Policies	Mapped Classes									
🛃 🐂 📚 🔝 🔜 🐂 🛼 🗠										
HIVEACTION-POLICY-UNIFIED	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
HQ_TO_LA	VOICE			160 Kbps 800 Kbps						
	DATA_HIGH_PRIORITY	•		Class-base						
	SCAVENGER class-default			Class-base						
Class-default										
B SET_DSCP_LAN										
	Mapped Class Detail									
	Classify Marking Que		ing Shapin	Compression	WRED	DBI Linsur	aported			
			ang	Compression	WILLD	DDL Olisa,	porcea	D-6		
	Shape using: None	\sim						Reference Control t	-	of A
								traffic ar	nd elimina	ite
								bottlener packets		
								to a spe		
								Rate		
								Peak: a	lows the	
								transmis burst hig	sion rate	
								shaping		ine
								Average	e: sets th	le la
								maximun	n transmi	ssion
								rate to th	ne shapin	g rate. ♥
Help						Save to Devi	ice Prev	ew CLI		Cancel

NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook 2
Manage QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5J.dcloud.cisc Policies Image QoS Settings - HQ-5J.dcloud.cisc Policies Image QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5J.dcloud.cisc Image QoS Settings - HQ-5D.lc?-UNIFIED Image QUELETING Image QUELETING	Mapped Classes Class Name Classify Marking Queueing Policing Shaping Compression WRED DBL Unknown VOICE Priority: VIDEO Priority: HIGH_PRIORITY_D Class-b SCAVENGER Class-b Class-default
VIDEO SCAVENGER Class-default E	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

Select the **interfaces** tab and apply the MULTI_CLASS_SHAPING policy to the **output** of the **GigabitEthernet3** interface.

Manage QoS Settings - HQ-B1.dcloud.ci	sco.com (198.18.129.24)		×
Manage QoS Settings - HQ-B1.dcloud.cd Manage QoS Settings - HQ-B1.dcloud.cd Glasses Interfaces Interfaces GlasbitEthernet1 GlasbitEthernet2 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet3 GlasbitEthernet5 GlasbitEth	cisco.com (198.18.129.24) Interface name: GigabitEthernet3 IP address: 100.64.0.2 IP address mask: 255.255.0 Interface description: WAN_SP2_MPLS1 Pre-dassify Link Fragmentation: Maximum delay:ms Interleave		×
Input : <none> Output : <none> Help</none></none>		Save to Device Preview CLI	Cancel

Make sure you select the **MULTI_CLASS_SHAPING** policy

	HQ-B1.dcloud.cisco.com (198.18.129.24)	\times
Image: Second state of the second s	Interface name: GigabitEthernet3 IP address: 100.64.0.2 IP address mask: 255.255.0 Interface description: WAN_SP2_MPLS1 Apply Policy to Interface Select the policy to apply to the Output of interface GigabitEthernet3: LIVEACTION-POLICY-UNIFIED MULTI_CLASS_SHAPING QUEUEING SET_DSCP_LAN MULTI_CLASS_SHAPING QUEUEING SET_DSCP_LAN	
Help	Save to Device Preview CLI	Cancel

Click Save to Device.

Manage QoS Settings - HQ-B1.	dcloud.cisco.com (198.18.129.24)	×
Manage QoS Settings - HQ-B1.0	dcloud.cisco.com (198.18.129.24) Interface name: IP address: 100.64.0.2 IP address: 100.64.0.2 IP address mask: 255.255.0 Interface description: WAN_SP2_MPLS1 Pre-dassify Link Fragmentation: Maximum delay: Interleave ms	
Help	Save to Device	.I Cancel

G	Interface description: WAN_SP2_MPLS1
	Pre-classify Saving to device
	Maximum delay: ms

Then Click **Close**. The **Would you like to save the current running configuration to the startup configuration, i.e., "copy run start**" dialogue box appear. Click **Yes**.



Go back into HQ-B1 Manage QoS Settings. Then click the Copy Policy to Devices box and select the MULTI_CLASS_SHAPING policy, and check HQ-B2 as the destination device.
OF-2.LWA.2.0.0	LiveNX Foundations Workbook 2	
🚺 Manage QoS Settings - H	Q-B1.dcloud.cisco.com (198.18.129.24)	>
Image: Second system Image: Second system Policies Image: Second system Image: Second system Image: Second system Image: Second system	Mapped Classes	WRED DBL Unknown
HQ_TO_INY dass-default QUEUEING E SET_DSCP_LAN	HQ_TO_NY 1,544 Kbps class-de Copy Policy to Devices × Select a policy: MULTI_CLASS_SHAPING ✓ Select the devices to which you want to save this policy: Mapped Proc Branch 1-LA.dcloud.cisco.com (198. 19. 1. 1) Branch 1-LA.dcloud.cisco.com (198. 19. 2. 1) Branch 2-NY.dcloud.cisco.com (198. 19. 2. 1) Match HQ-B2.dcloud.cisco.com (198. 18. 129. 25) Edit	Reference Class is defined by the criteria show at left. Match-any: packet must meet at least one of the criteria to be a member of the class. Match-all: packet must meet all criteria to be a member of the class.

When you hit **OK**, you will see the **Copy Status** box appear. If you get a **Copy QoS Policy to Device Conflict**, select **Overwrite**.

In LiveNX and select the QoS Tab

Right-click on right click on Branch1-LA, select QoS > Manage QoS Settings

Create a new policy and name it "SHAPING_1.544Mb"

Add Policy	×				
Policy name: SHAPING_1.544Mb					
OK Ca	ncel				

Select its class-default and select the Shaping tab.

Implement a shaping policy with the following parameters:

- Shape using = Average
- Rate = 1544 Kbps
- Committed burst = 15,440
- Excess burst = 0

Manage QoS Settings - Bi	Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)									×
 Image: A state of the state of										
Policies 📴 🗮 🔡 🛍 騙 📲 🖏 時	Mapped Classes	•								
CLIVEACTION-POLICY-UNIFIED SET_DSCP_LAN Gass-default WhyIsThisHere	Drop all traf						WRED	DBL	Unknown	
		i44 itted burst: s burst: nead Accounti	Kbps ~ 15,440 0 ing Offset:	bits bits				traffic a bottlene packets to a sp Rate Peak: transm burst h shaping Average maximu	the flow and elimin ecks by d s and con ecified bit allows the ission rate igher than	ate elaying forming rate. e e to t the hission
Help						Save to [Device Pr	eview CLI		Cancel

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

Click-Drag-and-Drop the QUEUEING policy onto the **class-default** of the SHAPING_1.544Mb policy.



NXOF-2.LWA.2.0.0LiveNX Foundations Workbook 2Copy the SHAPING_1.544Mb policy to the other remote router

Manage QoS Settings - Br	anch1-LA.dcloud.cisco.com (198.19.1.1)	×
Manage QoS Settings - B Manage QoS Settings - B Casses Interfaces Policies Casses Interfaces Policies CutreACTION-POLICY-UNIFIED QUEUEING UIDEO DATA_HIGH_PRIORITY SCAVENGER dass-default SET_DSCP_LAN SET_DSCP_LAN SET_DSCP_LAN SET_DSCP_LAN SET_DSCP_LAN SHAPING_LS44Mb Cass-default SHAPING_LS44Mb Cass-default SHAPING_LS44Mb CutreEndefault SHAPING_LS44Mb SHAPIN	Mapped Classes Class Name Classify Marking Queueing Policing Shaping Compression WF class default Copy Policy to Devices Select a policy: SHAPING_1.544Mb Select the devices to which you want to save this policy: Mapped Branch2-NY Disco.com (198.19.2.1) HQ-81.doud, circo, com (198.18.129.2) Unsupported Unsupported	RED DBL Unknown
Help	Cancel	Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate. Rate Peak: allows the transmission rate to burst higher than the shaping rate. Average: sets the maximum transmission rate to the shaping rate. (CLI Cancel

You may be warned there is a conflict. This is because a policy named QUEUEING already exist on the other remote router.

Select Overwrite.

Copy QoS Policy to Device Conflict	\times
Conflicts were encountered when saving the policy on device Branch2-NY.dcloud.cisco.com (198.19.2.1). The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?	
SHAPING_1.544Mb	^
Gass-oerault → Shaping: 1,544,000 bps	
QUEUEING - Overwritten (A policy with the same name exists)	
→ Queueing: Priority 160 Kbps ■ Match DSCP "46 (EF)"	
→ Queueing: Priority 800 Kbps	
Match DSCP "34 (AF41)"	
Queueing: Class-based 64 Kbps	¥
View all conflicts	
Overwrite Skip	

Validate the changes saved successfully.

Copy Policy to Devices	\times
Saving to devices Branch2-NY.dcloud.cisco.com (198.19.2.1) • Succeeded	
Export CSV Cancel	Close

Save to Device and Copy to Startup Config. Then close the Manage QoS Settings dialog window.

In LiveNX console, select the **QoS** Tab

NXOF-2.LWA.2.0.0

Right-click on the WAN interface (GigabitEthernet4) on the NY router, select **QoS > Apply Policy to Interface**



Apply the SHAPING_1.544Mb policy to the **output** of GigabitEthernet4.

Apply Policy to Interfaces \times
Select a policy: SHAPING 1.544Mb A Select the interfaces to which you want to apply this policy: GigabitEthernet4 Output B
OK Cancel

Repeat this process and apply the **SHAPING_1.544Mb** policy to the other WAN interface (**GigiabitEthernet3**).

Once you are complete with **Branch1-LA**, do the same with **Branch2-NY** and apply the policy **to both WAN Interfaces** (GigabitEthernet 3 and GigabitEthernet4)

You can verify that the configuration is complete and correct by reviewing the **Interfaces** tab of each router.

Manage QoS Settings - Branch1-LA.dclo	oud.cisco.com (198.19.1.1)	\times
2 4 9 9 8 6 %		
Policies Classes Interfaces		
Interfaces		
GigabitEthernet1 GigabitEthernet2 GigabitEthernet2 GigabitEthernet3 Output: <none> GigabitEthernet4 GigabitEthernet4 GigabitEthernet5 Output: <shaping_1.544mb GigabitEthernet5 GigabitEthernet5 Output: <none> GigabitEthernet5 Output: <none> Output: <none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></shaping_1.544mb </none>	Interface name: IP address: IP address mask: Interface description: Interface description: Interface name: Interface name:	
Help	Save to Device Preview CLI Close	

Lab 5

Lab 5: Throttling Traffic

LiveAction

Step 3 -- Throttle Traffic (Policing and WRED)



· WRED - Selectively drop specific data before congestion occurs

Investigate the current traffic flows.

From the LiveNX Client, select the QoS Tab •



Select GigabitEthernet3 from the HQ-B2 router





Notice the applications listed in the NBAR view at the top right of the page:



Why do we see bittorrent, bittorrent-networking, on our business network?



Run a Flow > Application report to see the same type of data.

Lab 5.1: Throttling / Policing

We'll implement a basic policing polity to throttle any scavenger (less than default) traffic. Lab Steps:

• From the LiveAction map, select the QoS Tab



Right-click on the HQ-B2 router and select QoS > Manage QoS Settings

	Local Device: HQ-B2			
	QoS	> 🗸	Enable QoS Polling	
<u>1996</u> 1997	Edit Device Settings		Create Policy from Template	
	Add or Remove Interfaces		Revert QoS Configuration by user 'admin'	
Other	Refresh Device		Adjust Input QoS	
	Remove Device		Adjust Output QoS	
	Zoom to Device		Manage QoS Settings	
	Device Tools	>	Manage NB	
	Statistics	>	Apply Policy to Interface	
	View	>	Remove Policy from Interface	
	Group Management	>	Copy Policy to Devices	
'			Reports	

Remember how we created a SET_DSCP_SCAVENGER class as part of the SET_DSCP_LAN policy? But also remember how we did not assign any classification to this class.

Class Name	DSCP	NBAR Protocol(s)
SET_DSCP_VOICE	EF (46)	rtp
SET_DSCP_VIDEO	AF41 (34)	Lync
SET_DSCP_HIGH_PRIORITY	AF31	SIP, SNMP, NetFlow, SSH, Telnet, Citrix,
DATA		Salesione
SET_DSCP_SCAVENGER	CS1 (8)	Leave blank for now
Best Effort	DE (0)	n/a

Manage QoS Settings - HQ-SJ.dcloud.cisc	o.com (198.18.129.25)				×
2 2 2 2 2 2 2					
Policies Classes Interfaces					
Policies	Mapped Classes				
🔁 🖲 🗟 🔝 🐜 🐴 🖏 🤫					
E LIVEACTION-POLICY-UNIFIED	Class Name	Classify	Marking	Q Po Sh	Co W
	SET_DSCP_VOICE	٠	DSCP: EF		
SET_DSCP_VOICE	SET_DSCP_VIDEO	۲	DSCP: AF41		
SET_DSCP_VIDEO			DSCP: CS1		
SET_DSCP_SCAVENGER	DET_DSCP_SCAVENGER		DSCP; CSI		
class-default					
	1				
	Mapped Class Detail				
	🔲 Drop all traffic for class				
	Classify Marking Queueing Polici	na Í Shanin			
		ng phoping	g compression		
	Match on: Any			Reference	
					defined by the
				criteria si	how at left.
				Match-a	ny:packet must
					east one of the
					be a member of
				the class	
				Match-a	II: packet must
					riteria to be a
	1		_	member (of the class.
		Edit	:		
I				,	
Help		Save	to Device	Preview CLI	Cancel

Update the **SET_DSCP_SCAVENGER** class with the following traffic:

- Bittorrent
- Bittorrent-networking

🔼 Manage QoS	5 Settings - H	Q-B2.dcloud.cisco.	.com (198.18.129.2	25)	5)	\times
	S					
Policies Classes Interface	es					
Classes	Create and Edit Ma	tch Statements				
Best_Effort	MB	Protocol - using NBAR bitbucket		~		_
DATA_HIGH_PRIORITY	value:	bitcoin		^		_
HQ_TO_LA HQ_TO_NY		bitly			Match Protocol - using N bittorrent Match Protocol - using N bittorrent-networking	_
LIVEACTION-CLASS-AV		bittorrent				
LIVEACTION-CLASS-ME		bittorrent-networking			E	
SCAVENGER		blackboard-com			-	- 11
SET_DSCP_HIGH_PRIC		blaze-news				- 11
SET_DSCP_SCAVEN		bleacher-report		~		
SET_DSCP_VIDEO	Match/ma	Match		\sim		
VIDEO		Add Match Statement	Replace Match Statement			
▼ VOICE					F	
Help					Save to Device Preview CLI Cancel	

When finished, the SET_DSCP_LAN policy should look like this:

Manage QoS Settings - H	IQ-B2.dcloud.cisco.com	(198.1	8.129.2	25)						\times
J f l l l l l l l l										
Policies Classes Interfaces										
Policies	Mapped Classes									
🛃 🖩 📚 🚵 🐜 📲 🖏 🗠	Pe 😭 🛃 🚔									
LIVEACTION-POLICY-UNIFIED MULTI CLASS SHAPING	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	SET_DSCP_VOICE SET_DSCP_VIDEO		DSCP: EF DSCP:							
SET_DSCP_LAN	SET_DSCP_HIGH_PRIORITY_DATA	•	DSCP:							
SET_DSCP_VIDEO	SET_DSCP_SCAVENGER Best Effort	•	DSCP: DSCP: BE							
SET_DSCP_HIGH_PRIORITY_DATA	dass-default		DSCP; DE							
Best_Effort										
lass-default	Mapped Class Detail									
	Drop all traffic for class									
	Classify Marking Queueing Po	lising Cha	-in- Com	and MD						
		iung ana	ping Comp	ression with	ED DDL	Unsupport				
	Match on: Any							ference lass is de		
	Match : Protocol - using NBAR : bi Match : Protocol - using NBAR : bi		etworkir					riteria sho		
							M	latch-any	r: packe	t must
							m	eet at lea	st one o	fthe
								riteria to b le class.	e a men	nber of
								latch-all:	nacket	must
								eet all crit		
	<		>				m	ember of	the clas	S.
			Edit							
Help					Save t	o Device	Preview (CLI	(Cancel

Select the **Policing** tab and **update** the following settings:

LiveNX Foundations Workbook 2

- Policing Enabled
- Committed Information Rate = 8Kbps
- Conform Action = Transmit
- Exceed Action = Drop

Manage QoS Settings - H	Q-B2.dcloud.cisco.com	(198.1	8.129.2	.5)						\times
친 🗐 💭 🖏 🖓 🍪 🦠										
Policies Classes Interfaces										
Policies	Mapped Classes									
	🖳 🔂 🕞 📄				_					
LIVEACTION-POLICY-UNIFIED MULTI_CLASS_SHAPING	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
	SET_DSCP_VOICE	٠	DSCP: EF							
	SET_DSCP_VIDEO		DSCP:							
SET_DSCP_VOICE	SET_DSCP_HIGH_PRIORITY_DATA SET_DSCP_SCAVENGER		DSCP:		8 Kbps					
SET_DSCP_VIDEO	Best_Effort	•	DSCP: BE		01000					
SET_DSCP_HIGH_PRIORITY_DATA	class-default	•								
Best_Effort										
class-default										
	Mapped Class Detail									
	Drop all traffic for class									
	Classify Marking Queueing Pol	icing Sha	ping Comp	ression WR	ED DBL	Unsupporte	ed			
	Enable policing						Re	ference		
		-					Li	mits the b	andwidth	^
	Committed Information Rate:	8	kbps					ilized by a		
	Peak Information Rate:							affic by sp and width		
	Committed burst: 1,000		oytes					id the res		
								resholds	have bee	n
	Excess burst: 1,000		oytes				e	ceeded.		
	Conform action: Transmit		~~				R	ate		
	Exceed action: Drop		\sim				b	os: avera	ge rate in	bits
	Malata a Marca (Da Guill)		~				pe	er second		
	Violate action: (Default)							ercent: a	verage rs	ata
								percent		110
							ba	ndwidth.		~
Help					Save t	o Device	Preview		Ca	ancel

Select Save to Device.

Copy the SET_DSCP_LAN policy to the other available routers.



Note: You will get a conflict waning... simply select Overwrite.



Validate the changes saved successfully., Click Close,



Close the Manage QoS Settings Dialog Window

Lab 5.2: Confirm policing Settings

Lab Steps:

• Select the QoS Tab.



From the device list, select the HQ-B2 router's **LAN interface** – **GigabitEthernet2** Update the real-time view's options to just include the **input**.



Note: If any of the policies are exceeded, they will show as AMBER. The amber confirms that drops are occurring inside the queue.



Lab 6

Lab 6: Buffer Tuning

Lab 6.0: Intro – Buffer Tuning

Buffer Tuning

LiveAction



Buffer tuning is an advanced QoS topic that LiveNX can greatly assist with simplifying the implementation and validation. It should be noted that buffer tuning should usually only be implemented for important, bursty traffic classes like video, desktop replacement applications (VDI), or transactional data.

This lab is based on an issue that happens about every 20-30 minutes. You may have to wait to see this issue or review historic data to find the issue. This is a very good re-world scenario.

- 1. The first place to look for the issue is to review the in-application alerts.
 - a. At the bottom left of the LiveNX window, note the Alert button. Yours may or may not be red.



- b. Double click the alert button
- c. The In-Application Alert view appears

Time	 Severity 	Device	Group	Alert Type	Details				
UZZ/US/ZI U4:U7:II PM	warning	Di driuriz-INT	Device Config Change and Access	Device configuration changed	Username - aumin; Commanus				
022/03/21 04:07:36 PM	Warning	Branch2-NY	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; interface Gi	gabitEthernet3;
022/03/21 04:08:03 PM	Warning	Branch1-LA	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; interface Gi	gabitEthernet3;
022/03/21 04:08:18 PM	Warning	Branch 1-LA	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- exit; interface Gigabi	tEthernet4; service-polic	y output SHAPING_1.544	чb
22/03/21 04:23:34 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthern				
22/03/21 04:23:45 PM	Warning	Branch1-LA	QoS	Class dropped rate	CLEARED: Interface name - Gig	abitEthernet4; Interfa	ace direction - OUTPUT;	Policy name - QUEUEING;	Class name - V
22/03/21 04:33:33 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthern	et4; Interface directio	n - OUTPUT; Policy nam	e - QUEUEING; Class nar	me - VOICE; Thr.
22/03/21 04:33:43 PM	Warning	Branch1-LA	QoS	Class dropped rate	CLEARED: Interface name - Gig	abitEthernet4; Interfa	ace direction - OUTPUT;	Policy name - QUEUEING;	Class name - V.
022/03/21 04:37:05 PM	Warning	HQ-B2	Device Config Change and Access		Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; interface Gi	gabitEthernet3; .
2022/03/21 04:37:23 PM	Warning	HQ-B2	Device Config Change and Access		Username - admin; Commands				
2022/03/21 04:43:32 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthern	et4; Interface directio	n - OUTPUT; Policy nam	e - QUEUEING; Class nar	me - VOICE; Thr.
022/03/21 04:43:42 PM	Warning	Branch1-LA	QoS	Class dropped rate	CLEARED: Interface name - Gig	abitEthernet4; Interfa	ace direction - OUTPUT;	Policy name - QUEUEING;	Class name - V.
022/03/21 04:47:31 PM	Warning	HQ-B2	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; class-map S	ET_DSCP_SCAVE
022/03/21 04:49:07 PM	Warning	HQ-B1	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; class-map S	ET_DSCP_SCAVE
022/03/21 04:49:08 PM	Warning	Branch1-LA	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; class-map S	ET_DSCP_SCAVE
022/03/21 04:49:09 PM	Warning	Branch2-NY	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; class-map S	ET_DSCP_SCAVE
022/03/21 04:49:38 PM	Warning	HQ-B2	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; policy-map	SET_DSCP_LAN;
022/03/21 04:49:59 PM	Warning	HQ-B1	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; policy-map	SET_DSCP_LAN;
2022/03/21 04:50:00 PM	Warning	Branch1-LA	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; policy-map	SET_DSCP_LAN; .
2022/03/21 04:50:00 PM	Warning	Branch2-NY	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; policy-map	SET_DSCP_LAN; .
022/03/21 04:50:18 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthern	et4; Interface directio	n - OUTPUT; Policy nam	e - QUEUEING; Class nar	ne - VOICE; Thr.
022/03/21 04:50:28 PM	Warning	Branch1-LA	QoS	Class dropped rate	CLEARED: Interface name - Gig	abitEthernet4; Interfa	ace direction - OUTPUT;	Policy name - QUEUEING;	Class name - V.
2022/03/21 04:50:28 PM	Warning	HQ-B2	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; config t; policy-map	SET_DSCP_LAN; .
022/03/21 04:51:19 PM	Warning	HQ-B2	Device Config Change and Access	Device configuration changed	Username - admin; Commands	- show privilege; termi	nal length 0; terminal wid	th 0; copy running-config	startup-config
2022/03/21 04:53:30 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthern	et4; Interface directio	n - OUTPUT; Policy nam	e - QUEUEING; Class nar	me - VOICE; Thr.
022/03/21 04:53:41 PM	Warning	Branch1-LA	QoS	Class dropped rate	CLEARED: Interface name - Gig	abitEthernet4; Interfa	ace direction - OUTPUT;	Policy name - QUEUEING;	Class name - V.
nly the last 100 alerts are :	shown.								
·		and all the second second							
Bring this window to the	front when a n	iew alert is received							
Beep when a new alert i	s received								
beep when a new aler ch	areceiveu								
						Clear list	Export list	Historical search	Configure al
						Ciear list	Export list	mistorical search	Configure ale

- d. Are there any alerts class drop alerts from the VOICE class?
- e. If not, we will want to wait or do a Historic Search for class-dropped rate (see Appendix A.)
- f. If there are any alerts for VOICE, note the device and interface where the drop occurred. In this example, the device is **Branch1-LA**, and the interface is **GigabitEthernet4**, and the direction is **egress (output)**.
- g. Select this interface from the device list.



h. From the real-time interface view, if necessary, update the view to Class/Class Drops, and Output.



i. The bottom section of the window is a **QoS drops** report. Note if there have been any QoS drops in the VIDEO class.



- j. There have been minimal drops in the VOICE Class.
- k. Click and drag your mouse on the bottom graph to make an outline of a box. When you let go the map should zoom in.



I. The zoomed-in graph shows the minimal drops happening in the VOICE (purple) class and the class-default (grey). In this example there have been 7 drops at peak in the VOICE class.





- m. To investigate the same type of drops from a historical report select the icon.
- n. The Pre-Policy and Post-Policy Drops report will open.
- Click and drag your mouse on the bottom graph to make an outline of a box. When you let go the map should zoom in. Note that there are minimal VIDEO (purple) drops in this example too.



- p. Remember we configured the **VOICE** queue for each site to 800Kbps each.
- q. The Pre-Policy graph above shows 742 Kbps peak VOICE traffic on the SHAPING_1.544Mb policy.

r. This is above the provisioned 160K. We need to implement some buffer tuning.

Lab 6.1: Implementing Tuning

Lab Steps:

• Select the QoS Tab



Right-click the HQ-B2 router and select QoS > Manage QoS Settings



Expand the QUEUEING Policy

Select the VOICE class.

Select the Queueing tab

Tick the **Burst option** and set it to **128000**.

Manage QoS Settings - H	Q-B2.dcloud.cise	co.com	(198.1	8.129.25)						\times
친 원 원 원 원 생 %										
Policies Classes Interfaces										
Policies	Mapped Classes									
📴 🐂 🔡 🏡 🐜 🐂 🛼 😜	Pe 🕒 🛃 📄									
	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
		۲		160 Kbps						
	VIDEO DATA_HIGH_PRIORITY			800 Kbps Class-based: 64 Kbps						
VIDEO DATA_HIGH_PRIORITY	SCAVENGER			Class-based: 8 Kbps						
SCAVENGER	class-default	•								
dass-default										
B SET_DSCP_LAN										
	Mapped Class Detail									
	Drop all traffic for cla	ass								
	Classify Marking Que	eueiny Pol	licing Shar	oing Compression W	RED DBL	Unsupport	ed			
		_		5				eference		
	Queueing type: Priorit	ty v~					-	istribute th	ne availa	ble ^
	Rate: 160	Kbps	200				b	andwidth	betwee	n
	Priority Level Non	e 🖂						lasses by ninimum ba		-
	Burst size: 12	28000	bytes					uarantee t		
	Unknown elements	:	_				G)ueueing	Туре	
							C	lass-bas	ed: utili:	zes
								lass-base ueueing ((-	
								erived we		
								om the ba		
							a	llocated to	the clas	ss. 🗸
							<	1		>
Help					Save	to Device	Preview	CLI	0	Cancel

Select the **Save to Device** button.

Copy the QUEUEING policy to the **other devices via Copy Policy to Devices** icon.



When the conflict warning appears, select overwrite.

Copy QoS Policy to Device Conflict	\times
Conflicts were encountered when saving the policy on device HQ-B1.dcloud.cisco.com (198.18.129.24). The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?	
QUEUEING - Overwritten (A policy with the same name exists) VOICE VOICE Match DSCP "46 (EF)" VIDEO VIDEO Auth DSCP "34 (AF41)" DATA_HIGH_PRIORITY Queueing: Class-based 64 Kbps Match DSCP "26 (AF31)" SCAVENGER View all conflicts	~
Perform this action for all devices which have conflicts	
Overwrite Skip	

Validate the changes saved successfully.



Close the Manage QoS Settings Dialog window.

Accept the suggestion to copy the current running configuration to the startup config.

Lab 7

Lab 7: QoS Alerts

QoS Alerting is an integral LiveNX component for managing and troubleshooting the system.

Alerting is a balancing act of noise vs actionable data. LiveNX default settings work well in many organizations for providing a balanced approach. Often, it is best to tune the alerting mechanism further to get the most from the solution.

Whenever LiveNX detects a QoS performance issue, the tool will show the respective device, interface, and class, as well as change color to amber. An alert will also be generated. Below is an example of the LiveNX **In-Application Alerts** view:

ime	 Severity 	Device	Group	Alert Type	Details
22/03/21 07:33:31 PM	Warning	Branch 1-LA	QoS	Class dropped rate	Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 15.655514
22/03/21 07:33:42 PM	Warning	Branch 1-LA		Class dropped rate	CLEARED interface name + OICE; Threshold - greater than 0.0; Class Corp rate - OLEUEING; Class name + VOICE; Threshold - greater than 0.0; Class Corp rate
22/03/21 07:43:28 PM	Warning	Branch1-LA		Class dropped rate	Therface name - Gigabilitäthemet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.; Class drop rate - 6.\$81333
22/03/21 07:43:39 PM	Warning	Branch 1-LA		Class dropped rate	CLEARED: Interface name - GloabitEthernet4: Interface direction - OUTPUT: Policy name - OUEUEING: Class name - VOICE: Threshold - greater than 0.0; Class drop rate
22/03/21 07:53:26 PM	Warning	Branch 1-LA		Class dropped rate	Interface name - GloabitEthernet+: Interface direction - OUTPUT: Policy name - OUEUEING: Class name - VOICE: Threshold - greater than 0.0: Class drop rate - 12,672659
22/03/21 07:53:37 PM	Warning	Branch 1-LA		Class dropped rate	CLEARED: Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - OUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate
22/03/21 08:03:28 PM	Warning	Branch1-LA	QoS	Class dropped rate	Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 11.014643
22/03/21 08:03:38 PM	Warning	Branch 1-LA	QoS	Class dropped rate	CLEARED: Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate
2/03/21 08:06:12 PM	Warning	HQ-B2	Device Con	Device configuration c	Username - admin; Commands - show privilege; terminal length 0; terminal width 0; config t; policy-map QUEUEING; class VOICE; no priority 160; priority 160 128000
22/03/21 08:08:18 PM	Warning	HQ-B1	Device Con	Device configuration c	Username - admin; Commands - show privilege; terminal length 0; terminal width 0; config t; policy-map QUEUEING; class VOICE; no priority 160; priority 160 128000
22/03/21 08:08:19 PM	Warning	Branch 1-LA	Device Con	Device configuration c	Username - admin; Commands - show privilege; terminal length 0; terminal width 0; config t; policy-map QUEUEING; class VOICE; no priority 160; priority 160 128000
2/03/21 08:08:20 PM	Warning	Branch2-NY	Device Con	Device configuration c	Username - admin; Commands - show privilege; terminal length 0; terminal width 0; config t; policy-map QUEUEING; class VOICE; no priority 160; priority 160 128000
2/03/21 08:09:38 PM	Warning	HQ-B2	Device Con	Device configuration c	. Username - admin; Commands - show privilege; terminal length 0; terminal width 0; copy running-config startup-config

The following Lab directs you to create an Alert when QoS problems are detected.

Lab Steps:

• Tools > Configure Alerts

🔼 LiveNX - 34.136.141.179



Ignore the message regarding reporting in the WebUI. This is normal – and reporting as we need it will still work here.

The default QoS alerts are highlighted below. These settings work well in many environments.

Configure Alerts ×
Routing Triggers LAN Triggers Notification Syslog
Device/QoS Triggers Flow Triggers IP SLA Triggers
Generate an alert when
Warning V A device becomes unavailable
CPU and Memory
✓ Warning ∨ A device's CPU usage reaches or exceeds (>=) 80 %
✓ Warning ✓ A device's memory usage reaches or exceeds (>=) 90 %
Device Config Change and Access
Warning V The running config changed time is later than the startup config changed time
Warning Commands are sent to a device using the monitor-only CLI credentials
Warning V The device configuration has been changed by LiveNX
Interface Errors
Warning V An interface becomes unavailable
☑ Warning ✓ An interface has errors (CRC, Frame, Overrun, Ignore, Abort)
QoS Drops
Configuring the following alert triggers will affect the drop status for devices and interfaces.
Warning V Interface drop rate exceeds (>) 2,500.000 pps
Generate events only for selected interfaces
☑ Warning ✓ Class drop rate exceeds (>) 0.000 Kbps
Warning V Class-default drop rate exceeds (>) 1,500.000 Kbps
Help OK Cancel

Note: If a network uses policers, it is often best to tune the global Class drop rate exceeds setting.

NXOF-2.LWA.2.0.0

LiveNX Foundations Workbook 2

In the example below it has been changed from 0 to 1500. This means that all classes that drop data, including high priority classes like VOICE and VIDEO, **will not alert** *unless* they drop at a rate greater than 1500Kbps.

Configure Alerts	×				
Routing Triggers LAN Triggers Notification	Syslog				
Device/QoS Triggers Flow Triggers IP SLA Trig	gers				
Generate an alert when Device Down					
Warning V A device becomes unavailable					
CPU and Memory					
Warning V A device's CPU usage reaches or exceeds (>=) 80 %					
Warning V A device's memory usage reaches or exceeds (>=) 90 %					
Device Config Change and Access					
Warning V The running config changed time is later than the startup config change	d time				
$\hfill Warning \hfill \bigvee$ Commands are sent to a device using the monitor-only CLI credentials					
Warning V The device configuration has been changed by LiveNX					
Interface Errors					
Warning V An interface becomes unavailable					
Warning V An interface has errors (CRC, Frame, Overrun, Ignore, Abort)					
QoS Drops					
Configuring the following alert triggers will affect the drop status for devices and interfaces.					
Warning V Interface drop rate exceeds (>) 2,500.000 pps					
Generate events only for selected interfaces					
Warning V Class drop rate exceeds (>) 1,500.000 Kbps					
Warning Class-default drop rate exceeds (>) 1,500.000 Kbps					
Help	Cancel				

To modify this condition and ensure VIOCE and VIDEO classes still alert if there are any drops:

Select the **Custom Triggers** tab.

Click Add.

🔼 Configure A	lerts			\times
Routina Triagers	LAN Trioders	Custom Triggers	Notification	Syslog
Device/QoS Trig	gers	How Iriggers 📈	IP SLA Trigg	jers
Generate an alert when				
Warning A	device becomes unav	ailable		

Create a custom trigger type Class and set it with the following parameters:

- Filter = *leave blank*
- Class name = VOICE
- Direction = Output
- Traffic type = Drop
- Operator = greater than
- Value = 0

🛕 Configure A	lerts			\times
Device/QoS Tr		Flow Triagers Custom Triggers	IP SLA Tri	
Routing Triggers	LAN Trigge		Notification	Syslog
	Add (Type Class	Custom Trigger	Edit	Delete
	Class name	VOICE		
	Direction	Output	×.	
	Traffic type	Drop	×.	
	Operator	greater than		
	Value	0	kbps	
	Syslog Severity	Warning	**	
		OK Cance	e	
Help			OK	Cancel

Device/QoS Triggers Flow Triagers IP SLA Triggers Routing Triggers LAN Triggers Custom Triggers Notification Syslog Add Edit Delete Class: Class dropped packets for output direction of VOICE is greater than 0.0 kbps Voice is greater than 0.0 kbps	🔼 Configure A	lerts				\times	
Add Edit Delete	Device/QoS Tri	ggers	Flow Trie	oders	IP SLA Triggers		
	Routing Triggers	LAN Triggers	Custor	n Triggers	Notification	Syslog	
Class: Class dropped packets for output direction of VOICE is greater than 0.0 kbps				Add	Edit	Delete	
	Class: Class dropped packe	ts for output direction	of VOICE is g	reater than 0.0	0 kbps		

Repeat these steps and create a Custom trigger for the VIDEO and HIGH_PRIORITY_DATA classes.

This will ensure these classes always alert when drops occur.

Configure A	lerts				\times	
Device/QoS Tri	Flow Tric	oders	IP SLA Triggers			
Routing Triggers	LAN Triggers	rs Custom Triggers Notification		Notification	Syslog	
			Add	Edit	Delete	
Class: Class dropped packets for output direction of VOICE is greater than 0.0 kbps Class: Class dropped packets for output direction of VIDEO is greater than 0.0 kbps Class: Class dropped packets for output direction of HIGH_PRIORITY_DATA is greater than 0.0 kbps						

After the alert thresholds have been updated, open the **In Applications Alert** view. At the bottom left of the LiveNX window, Double click the alert button. In this example the Alert button is red, indicating that a new alert has been received.

	Device	Group	Alert Type	Details
 Severity 				
				Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 15.655514 CLEARED: Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - OUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 15.655514
				Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 6.581333
				CLEARED: Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - OUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 12.672659
				CLEARED: Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICCE; Threshold - greater than 0.0; Class drop rate -
				Interface name - GigabitEthernet4; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate - 11.014643 CLEARED: Interface name - GigabitEthernet4: Interface direction - OUTPUT; Policy name - OUEUEING; Class name - VOICE; Threshold - greater than 0.0; Class drop rate -
				CLEAKED; interface name - signoticitmements; interface direction - OUIPU; Policy name - Quebulink; Class and - Volice; internoid - greater than 0.0; class drop rate - Username - admin; Commands - show privilege: terminal length 0; terminal width 0; config ti policy-map OURLEINK; class VOICE: no priority 160;
				Username - admin; Commarks - show privlege; terminal length 0; terminal width 0; config 1; policy-map QUEUEINS; cass VOLE; no priorty 100; priorty 100 128000 Username - admin; Commarks - show privlege; terminal length 0; terminal width 0; config 1; policy-map QUEUEINS; cass VOLE; no priorty 160; priorty 160 128000
				Username - admin; Commarks - show privlege; terminal length o; terminal width o; config t; poky-map QUEUENS; Gass VOICE; no priorty 160; priorty 160 128000 Username - admin; Commarks - show privlege; terminal length o; terminal width o; config t; poky-map QUEUENS; Gass VOICE; no priorty 160 128000
				Username - admin: Commanda - show privilege; temmai ergori o; temmai widir o; comig ti poicy-map Quebeerve; class voice; no privilegi toto; teodo username - admin: Commanda - show privilege; temmai ergori o; terminal widir o; comig ti poicy-map QUEBERVE; class voice; no privile; 160; zisovi 16
				Username - admin: Commanda - show privlege; terminal length 0; terminal widdr 0; comg tip policymag ogcoccard; cass voice; no priority 160 priority
	new alert is received			
	Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning Warning	Warning Brandh1.A Warning HQ-82 Warning HQ-82	Warning Branch11.A QoS Warning HoreA1.A Device Con. Warning Branch11.A Device Con. Warning Branch11.A Device Con.	Warring Warring Warring Branchild. QoS Example QoS Marking Branchild. Gase dropped rate dropped rate Marring Branchild. QoS Marking QoS Marking Mark

Click the **Clear List** Button

🔺 Ir	n-Application	Alerts										-		×
Time		 Severity 	Device	Group	Alert Type	Details								
														~
	ne last 100 alerts are sh													
	ng this window to the f		w alert is received					N						
Be	ep when a new alert is	received						2		_				
									Clear list	Export list	Historical	search	Configure a	lerts

Monitor the system for any **new** QoS Alerts.

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

Lab Steps:

• Select File, Add Device



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

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

• Click Next.

LiveNX Foundations Workbook 2

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

Add Device - HQ-SJ.dcloud.ci	sco.com (198.18.129.25) >			
Steps	CLI Settings (Configuring) Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).			
1. Device Connection Information				
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 VLANs 6. Select Features	Use my default Configuration CLI connection settings Edit			
7. Enable Polling	C Enter connection settings for this device			
8. Review Configuration	Connection Type SSH 🕝 Port* 22			
9. Device Updated	User name on Device			
	Password on Device*			
	Enable Password			
	Also use these credentials for monitor mode.			
	<back next=""> Finish Cancel Help</back>			

• Click Next.

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

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

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

• Click Continue.

Test	Status	Description
5NMP connection		Succeeded
5NMP access		Succeeded
CLI configure connection	\odot	Skipped
CLI configure login	\odot	Skipped
CLI configure enable password	\odot	Skipped
CLI monitor connection	\odot	Skipped
CLI monitor login	\odot	Skipped
CLI monitor enable password	\odot	Skipped
Serial number validation		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	\odot	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.

Add Device - HQ-SJ.dcloud.cise	:0.CC	om (198.18.	129.25)				×
Steps	Se	lect Interface	es				
1. Device Connection Select the interfaces you want to Information				to monitor on this device (maximum 1000 interfaces).			
2. CLI Settings (Configuring)		Selected	Interface	Trunk	IP Address	Description	
3. CLI Settings (Monitoring) 4. Select Interfaces		াব	Ethernet0/0		198.18.129.25		_
		হ	Ethernet0/1 Loopback0		10.255.0.2 10.0.0.102		
5. Select VLANs			NullO		10.0.0.102		
6. Select Features			TunnelO			PFR auto-tunnel for VRF default	t
7. Enable Polling			VoIP-NullO				
8. Review Configuration							
9. Device Updated							
		5elected inter	rface(s): 3				
	<	Back	Next >	Finish		Cancel Help	

• Click Next.

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

Steps	Select VLANs
1. Device Connection Information	Select the VLANs you want to monitor on this device (maximum 25 VLANs).
2. CLI Settings (Configuring)	No VLANs were found on the device. No VLANs will be managed. \mathcal{K}
3. CLI Settings (Monitoring)	<u>▲</u> [∧]
4. Select Interfaces	
5. Select VLANs	
6. Select Features	
7. Enable Polling	
8. Review Configuration	
9. Device Updated	
	< Back Rent > Finish Cancel Help

• 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**.

eps	Select Features		
. Device Connection Information	Select the features you want to enab section.	le on each interface. Learn more a	about each feature in the Help
 CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs 	Features on device		
5. Select Features	Interface	NBAR	NetFlow
 Enable Polling Review Configuration Device Updated 	Ethernet0/1 Ethernet0/0 Loopback0	র র র	<u>र</u> र
			l≩

- Click Next.
- Change the polling rate to 30 seconds.

Appendix 1: Add Device © Copyright LiveAction 2022

LiveNX Foundations Workbook 2

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

Steps Enable Polling			
1. Device Connection Select the features you want to actively monitor and the polling rate for all the features on this devi Information Learn more about polling in the Help section.	ice.		
2. CLI Settings (Configuring)			
3. CLI Settings (Monitoring)			
4. Select Interfaces			
5. Select VLANs Polling Rate 30 seconds			
6. Select Features Poll the following features			
7. Enable Polling			
Review Configuration 🔽 Flows			
9. Device Updated 🔽 Qo5			
IP SLA			
✓ Routing			
LAN*			
* LAN polling occurs every 15 minutes			
* For SNMP v3, please see the User Guide on configuring LAN polling.			
Ν			
h3			
<back next=""> Finish Cancel H</back>	Help		

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

eps	Review Configuration	
. Device Connection Information	The following commands will be sent to the device. Or you can choose to manually configure the device yourself.	
. CLI Settings (Configuring)		
. CLI Settings (Monitoring) . Select Interfaces	description DO NOT MODIFY. USED BY LIVEACTION.	^
. Select VLANs	cache timeout inactive 10 cache timeout active 60	
. Select Features . Enable Polling	record LIVEACTION-FLOWRECORD	
Review Configuration Device Updated	interface Ethernet0/1 ip flow monitor LIVEACTION-FLOWMONITOR input ip flow monitor LIVEACTION-FLOWMONITOR output exit interface Ethernet0/0 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 output	
	 Send the configuration commands to device. I will manually configure the device myself. 	

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

XOF-2.LWA.2.0.	D LiveNX For	undations Workb	book 2	
dd Device - HQ-SJ.dcloud.cis	co.com (198.18.129.25)		Ē	
Steps	Device Updated			
1. Device Connection Information	You have configured this device successfu configuration to the device's startup confi			
2. CLI Settings (Configuring)	Device Settings			
3. CLI Settings (Monitoring)	-			
 Select Interfaces 	Setting Polling Rate		Description 30 seconds	
. Select VLANs	NetFlow Monitoring		NetFlow collector	
. Select Features	NetFlow Polling		Enabled	
. Enable Polling	Mediatrace		Disabled	
Review Configuration	Adjacency Polling Qos Polling		Enabled Enabled	
). Device Updated	IP SLA Polling		Enabled	
s. Device opuateu	CEF		Enabled	
	Interface Settings			
	Interface	NBAR	NetFlow	
	Ethernet0/1	٠	٠	
	Ethernet0/0 Loopback0		•	
		•		
	< Back Next > Finish	🗟	Cancel Help	

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

Appendix 2: Client Device Discovery

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

• Select File and Discover Devices.



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

Device Discovery		×					
Step 1: Specify wh	at to scan						
Specify IP ranges (⊙ Specify IP ranges (ex: 192.168.1.1-200) or one IP per line:						
198.19.1.1 198.19.2.1							
C Specify seed device	e to scan						
IP Address		Hops 1 💌					
	MP connection settings tion settings for this device	Edit Target Port 161					
Community String							

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

Step 3: Specify node		
Local		-
	ОК	Cancel

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

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



LiveNX Foundations Workbook 2

a		Filte	r Clear		
Select	Device Name	IP Address	Hops	Vendor	Model
V	Branch2-NY.dcloud.cisco.com	198.19.2.1	0	Cisco	ciscoGatewayServer
	Branch1-LA.dcloud.cisco.com	198.19.1.1	0	Cisco	ciscoGatewayServer
ted: 2	Discovered: 2 Device	Limit: 10,000,000 (1 active devices)			

• Select Yes on the configure devices dialog.



• Use the default SNMP connection settings and then select Next

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

Configure Cisco Devices		×
Steps	SNMP Settings	
 SNMP Settings CLI Settings (Configuring) CLI Settings (Monitoring) Validating Devices Select Features Enable Polling Update Device Devices Configured 	Enter the SNMP connection information used for monitoring the selected devices.	
	< Back Next > Finish Cancel Help	

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

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

LiveNX Foundations Workbook 2

• 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. Ise the default Monitor-only CLI connection settings Edit Ise the previous page connection settings Enter connection settings for this device Connection Type SSH Port* User name on Device Password						
	< Back Next > Finish Cancel Help						

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

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

LiveNX Foundations Workbook 2

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

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

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

onfigure Cisco Devices								
Steps	Enable Polling							
 SNMP Settings CLI Settings (Configuring) 	Select the features you want to actively monitor, and the polling rate for the devices. Learn more about each feature in the Help section.							
3. CLI Settings (Monitoring)								
 Validating Devices 	Device Branch1-LA.dcloud.cisco.com	Poll	QoS V	Flow	IP SLA	Routing	LAN*	Interval
5. Select Features	Branch1-LA.dcloud.cisco.com Branch2-NY.dcloud.cisco.com				V			30 seconds 💌
5. Enable Polling								,
7. Update Device								
3. Devices Configured								
								L _e
	, * LAN polling occurs every 15 mir * For SNMP v3, please see the U		on con	figuring L	.AN polling	I.		
	< Back Next > Fir	rish					Cancel	Help

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

• Select Send Updates to Devices and click Send.

Update Device						
The selected devices will be updated based on the configuration changes if necessary. You may choose to manually configure the devices. Warning: once update processes have been started you will not be able to return to earlier screens. Learn						
		ot be able to retain to earlier screens, Lea				
Douiso	Status	Description				
		Update Required; click to view				
ud.cisco.com		Update Required: click to view				
s to Devices Sen	<u>.</u>					
figure Devices 🛛 🕞						
e Commands						
	o manually configure the orate processes have been eature in the Help section Device Jod.cisco.com d.cisco.com s to Devices figure Devices	a manually configure the devices. ate processes have been started you will n eature in the Help section. Device Status ud.cisco.com O ud.cisco.com O s to Devices Send				

• 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 on You may choose to manually configure the de Warning: once update processes have been si more about each feature in the Help section.	vices.					
. 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 Send	1					
	C Manually Configure Devices	_					
	Export Update Commands						

LiveNX Foundations Workbook 2

• Click finish to add the devices into the topology.



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

Appendix 3: Export/Import Device Configuration

Lab Steps:

• From the File Menu select Export Devices.

👼 198.18.133.34 - Remote Desktop							
LiveAction - localhost							
File View Users QoS Flow Ro							
Add Device							
Discover Devices							
Import Devices							
Export De zes							
Manage Devices							
Refresh Devices							
Remove Network Objects							
Exit							

• Deselect **GigabitEthernet3** and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

dd/Up	Name	Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (Kb	Marda	Site	Site CIDR	Data Cen
	Branch1-LA.dcloud.cisco.c		101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	LA	10.0.1.1, 198.19.1	
	GigabitEthernet1	Interface	101	198.19.1.1	Cisco	CISCOUSK1000V	10.3.2	Branch1 LAN	1,000,000	LOCAI	LA	10.0.1.1, 190.19.1	
	GigabitEthernet2	Interface		100.64.1.2				Internet	2,000				
	GigabitEthernet3	Interface		10.255.1.2				MPLS	1,000				
	Loopback0	Interface		10.255.1.2				MPLS	8,000,000				
	- Nullo	Interface		10.0.1.1					10,000,000				
		Interface							10,000,000				
	HQ-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	но		
		Interface	2	198.18.129.24	Cisco	CISCOUSKIUUUV	10.3.2			LOCAI	nų		
	- GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000				
	GigabitEthernet2 Loopback0	Interface		100.64.0.2				Internet	1,000,000				
	··· Loopbacku ··· Null0												
	··· VoIP-Null0	Interface Interface							10,000,000				
			_		-				10,000,000				_
	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
	GigabitEthernet1	Interface Interface		198.18.129.25					1,000,000				
	GigabitEthernet2			10.255.0.2					1,000,000				
	- Loopback0	Interface		10.0.0.102					8,000,000				
	NullO	Interface							10,000,000				
	··· VoIP-Null0	Interface							10,000,000				_
~	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		
~	GigabitEthernet1	Interface		198.18.129.23					1,000,000				
	- Loopback0	Interface		10.0.0.103					8,000,000				
	··· NullO	Interface							10,000,000				
	··· VoIP-Null0	Interface							10,000,000				

• Select Export to csv.

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



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



• Select the file you previously exported.

NXOF-2.LWA.2.0.0	LiveNX Foundations Workbook
Import from a CS¥ file	×
Look in: 📃 Desktop	💌 🦸 📂 🎞 -
Recent Items Desktop My Documents	
a Computer	
Network	einterface.csv Import es (*,csv) Cancel

• Click Add/Update Devices.

	pdate Devices s selected for Add/Update will b	e added or u	pdated								Q-			×
id/Upd		Туре	Device Serial	IP Address	Vendor	Model	IOS Version	Description	Line Rate (K	Node	Site	Site CIDR	Data Ce	
	Branch1-LA.dcloud.cisco	Router	101	198.19.1.1	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	LA	10.0.1.1, 198.1	Г	
1	- GigabitEthernet1	Interface		198.19.1.1				Branch1 LAN	1,000,000				_	
	- GigabitEthernet2	Interface		100.64.1.2				Internet	2,000					
2	GigabitEthernet3	Interface		10.255.1.2				MPLS	1,000					
	Loopback0	Interface		10.0.1.1					8,000,000					
	- NullO	Interface							10,000,000)				
	VoIP-Null0	Interface							10,000,000)				
	HO-B1.dcloud.cisco.com	Router	2	198.18.129.24	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		Г	
Image: A start and a start	- GigabitEthernet1	Interface		198.18.129.24				HQ-LAN	1,000,000				_	
2	- GigabitEthernet2	Interface		100.64.0.2				Internet	1,000,000					
	- Loopback0	Interface							8,000,000					
	NullO	Interface							10,000,000)				
	VoIP-Null0	Interface							10,000,000					
	HQ-B2.dcloud.cisco.com	Router	3	198.18.129.25	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		Г	
	GigabitEthernet1	Interface		198.18.129.25					1,000,000				_	
	- GigabitEthernet2	Interface		10.255.0.2					1,000,000					
Π	Loopback0	Interface		10.0.0.102					8,000,000					
Π	NullO	Interface							10,000,000)				
Π	VoIP-Null0	Interface							10,000,000					
	HQ-MC.dcloud.cisco.com	Router	1	198.18.129.23	Cisco	ciscoCSR1000v	16.3.2	Cisco IOS Software [Denali],		Local	HQ		Г	
~	- GigabitEthernet1	Interface		198.18.129.23					1,000,000				_	
	Loopback0	Interface		10.0.0.103					8,000,000					
	- NullO	Interface							10,000,000					
	VoIP-Null0	Interface							10,000,000)				
		_			<									ł
								Add/Update Devices	Import from CSV		Export to CS	V	Close	

2

• Click OK to use the Default SNMP settings.

LiveNX Foundations Workbook 2

A		×
Node	Local	_
Ouse the Default SNM	1P connection settings	Edit
C Enter SNMP connect	ion 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.

NXOF-2.LWA.2.0.0LiveNX Foundations Workbook 2Appendix 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:

• Open the LiveNX WebUI, select Settings.

E LiveAction №												۰.	
Overview Enter Filter Request Here	•										φ	Settings	
Sites, Devices, Interfaces by Statuses						Active Alerts							Setti Diagnosti
SITES: 2		DEVICES: 4		INTERFACES: 8		ALERTS					_		
sires (3) • HQ • LA	0	DEVICES E ² • Roath1-LA • HQ-B1 • HQ-B2 • HQ-MC	0	INTERFACE CF OpablEment1Drach1LA OpablEment1HO 81 OpablEment1HO 82 OpablEment2HO 82 OpablEment2Ho 82 OpablEment2Ho 81 OpablEment2HO 81 OpablEment2HO 82 OpablEment3Drach1LA	0		No	Active Aler	5		-		

• Select Configuration.

≡ LiveAction [.]	NX
Settings	
Q Search	
Configuration	
Data Source Management	
Data Store Device Entity Page Reports	
Email Configuration	
Integrations	×
License Configuration	^
License Expiration Notification	
LiveNA Configuration	
Mounted Data Nodes	
Properties	~
Ргоху	
Reports	~
Security Single Sign On	~
SNMP Trap	
Syslog	
Troubleshooting	~
Updates Web UI Data Store	

- Click Export.
- Enter encryption password if preferred.



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

Appendix 5: Connect via Remote Desktop Connection

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

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

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

Lab Steps:

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

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

DIAGRAM

Nemote Desktop Connection – 🗆 🗙											
Remote Desktop Connection											
General	Display	Local Re	sources	Experience	Advanced						
Logon s	ettings —										
	Enter	the name	of the ren	note computer							
	Comp	uter:	198.18.133.34 🗸								
	dministrator										
				used to conne ese credentials		mputer.					
	Alv	vays ask f	or creden	tials							
Connec	tion settin	gs									
Save the current connection settings to an RDP file or open a saved connection.											
	0)pen									
Hide Options											

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

№ Remote Desktop Connection											
Remote Desktop Connection											
General Display	Local Resources	Experience	Advanced								
Display configur	ation										
	Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.										
Small Large Full Screen											
Colors Choose the color depth of the remote session. Highest Quality (32 bit) Display the connection bar when I use the full screen											
Display the connection bar when I use the full screen Hide Options Connect Help											

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

DIAGRAM



• Click OK.

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

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