LiveAction®

LiveNX Engineering Console

User Guide

LiveAction, Inc. 960 San Antonio Road, Ste. 200 Palo Alto, CA 94303, USA +1 (888) 881-1116 https://www.liveaction.com

Copyright © 2021 LiveAction, Inc. All rights reserved

20210326-LNXEC_211a

Contents

Chapter 1	Introduction	1
	About LiveNX	2
	Technology Modules	3
	QoS Module	4
	Flow Module	
	Routing Module	
	IP SLA Module	
	LAN Module	
	Contacting LiveAction Support	
Chapter 2	LiveNX Engineering Console User Interface	8
	About the Engineering Console User Interface	
	Topology View Interface Controls	
	View Menu	
	Exporting and Importing a LiveNX Configuration	
	LiveNX Technology Tabs	
	Usage and Deployment Guidelines	
	LiveNX Interface Color Codes	
	Logical Topology (Preview)	
	LiveNX Best Practices	
	Groups	
	Sites and Site IPs	
	WAN and Service Provider	
	Label	
	Capacity	
	Device and Interface Tags	19
	Reporting	19
Chapter 3	Dashboard	21
-	About the Dashboard	22
	Technology Dashboards	
	System Dashboard	
	System Alerts	
	, Top CPU Usage	
	Top 10 Memory Usage	
	Top 10 Interface Bandwidth (Input or Output)	
	Top 10 Interface Drops (Input Drops or Output Drops)	
	Site WAN Interface	
	Application Dashboard	
	QoS Dashboard	
	QoS Alerts – 24 Hours	
	Top 10 Class Input Bandwidth Pre- or Post-Policy	
	Top 10 Class Output Bandwidth Pre- or Post-Policy	
	Top 10 Class Output Bandwidth Pre- or Post-Policy	
	Top 10 Class Input Drops by Bitrate	
	Top 10 Class Output Drops by Bitrate	
	Flow Dashboard.	
	Flow Alerts – 24 Hours	
	Flow Source	
	Top 10 Source Addresses [Bytes or Flows]	

	Top 10 Destination Addresses (Bytes or Flows)	
	Top 10 Source Countries [Bytes or Flows]	
	Top 10 Destination Countries [Bytes or Flows]	
	Top 10 DSCP (Bytes or Flows)	
	Top 10 Interfaces (Outbound) [Bytes or Flows]	
	Top 10 Application [Bytes or Flows]	
	Top 10 Application Performance	
	Top 10 Voice/Video Performance	
	Top 10 HTTP Host	
	IP SLA Dashboard	
	Last 100 Alerts	
	Trending	
	Test Types	
	System Tests	
	WAN Dashboard	
	Configure App Groups	
	Top 10 Alerts by Site	
	Site Utilization by Application Group	
	Site Utilization by Service Provider	
	Top 10 Alerts by Application Group	
	Application Group Bandwidth by Site	
	Application Group Bandwidth by Service Provider	
	Top 10 Alerts by Service Provider	
	Service Provider Utilization by Application Group	
	Service Provider Utilization by Site	
	Learn PfRv3 Settings	
	The Note Column Identifies the Following	
	Details Displayed Are	
Chapter 4	Alerts and Notifications	69
Chapter 4	Alerts and Notifications	
Chapter 4	About Alerts and Notifications	
Chapter 4	About Alerts and Notifications View Alerts	
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts	
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts	
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts Device/QoS Triggers	
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts Device/QoS Triggers Flow Triggers	70 70 71 71 72 73
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts Device/QoS Triggers Flow Triggers IP SLA Triggers	70 70 71 71 72 72 73 74
Chapter 4	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts Device/QoS Triggers Flow Triggers IP SLA Triggers Routing Triggers	70 70 71 71 71 72 73 73 74 75
Chapter 4	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers .	70 70 71 71 72 73 73 74 75 76
Chapter 4	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers .	70 70 71 71 72 73 73 74 75 76 76 76
Chapter 4	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . LAN Triggers . Alert Notification Configuration .	70 70 71 71 72 73 73 74 75 76 76 78
Chapter 4	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications.	70 70 71 71 72 73 73 74 75 75 76 76 76 78 80
Chapter 4	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . LAN Triggers . Alert Notification Configuration .	70 70 71 71 72 73 73 74 75 75 76 76 76 78 80
Chapter 4 Chapter 5	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications.	70 70 71 71 72 73 73 74 75 76 76 76 78 80 80
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . LAN Triggers . Alert Notification Configuration . Syslog Notifications . Status Bar Alerts .	70 70 71 71 72 73 74 74 75 76 76 76 78 80 80 80 80 80
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications . Status Bar Alerts . Reporting .	70 70 71 71 72 73 74 75 76 76 76 78 80 80 80 80 80 82 83
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications. Status Bar Alerts . Reporting . About Reporting . Reporting Best Practice.	70 70 71 71 72 73 74 75 76 76 76 78 80 80 80 80 80 80 83 83 83
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications. Status Bar Alerts . About Reporting .	70 70 71 71 72 73 73 74 74 75 76 76 76 78 80 80 80 80 80 80 80 80 80 83 83 83 83
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications . Status Bar Alerts . Reporting . About Reporting . Reporting Best Practice . Engineering Console Reporting .	70 70 71 71 72 73 73 74 74 75 76 76 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . LAN Triggers . Alert Notification Configuration . Syslog Notifications . Status Bar Alerts . Reporting . About Reporting . Reporting Best Practice . Engineering Console Reporting . QoS Report .	70 70 71 71 72 73 74 74 75 76 76 76 76 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications . Status Bar Alerts . Reporting . About Reporting . Reporting Best Practice . Engineering Console Reporting . QoS Report . Device Search .	70 70 71 71 72 73 74 74 75 76 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications . View Alerts . Historical Alerts . Configure Alerts . Device/QoS Triggers . Flow Triggers . IP SLA Triggers . Routing Triggers . LAN Triggers . Custom Triggers . Alert Notification Configuration . Syslog Notifications . Syslog Notifications . Status Bar Alerts . Reporting . About Reporting . Reporting Best Practice . Engineering Console Reporting . QoS Report . Device Search . Chart Zoom . Report Legend .	70 70 71 71 72 73 74 75 76 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications	70 70 71 71 72 73 74 75 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications	70 70 71 71 72 73 74 75 76 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications	70 70 71 71 72 73 74 75 76 76 76 76 78 80 80 80 80 80 80 80 80 80 80 80 80 80
	About Alerts and Notifications View Alerts Historical Alerts Configure Alerts Device/QoS Triggers Flow Triggers IP SLA Triggers Routing Triggers LAN Triggers Custom Triggers Alert Notification Configuration Syslog Notifications Status Bar Alerts Reporting About Reporting. About Reporting QoS Report Device Search Chart Zoom Report Legend Report Legend Report Actions Interface Utilization Report	70 70 71 71 72 73 74 74 75 76 76 76 76 80 80 80 80 80 80 80 80 80 80 80 80 80

Application	
11	
QoS	
Network	
Medianet	
Application (AVC)	
Wireless	
Miscellaneous	
Report Features	
Report Search	
Drill Down/Change Report	
Report Actions	
Roles	
Routing Reports	
IP SLA Reports	
Time Ranges	
Warning Thresholds	
Available Reports	
Device Pick List	
Device Pick List Drilling-down to Reports	
e 1	
Saving Reports	
Printing and Exporting Reports	
Lan Reports	
Report Scheduler	
Report Schedule Options	
Long-Term Reports	
Scheduled Reports	
Custom Dashboard	
QoS	115
About OoS	
	116
QoS Configuration	
QoS Configuration Manage QoS Settings Screen	
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ	
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab	116
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab	116 116 116 2F)119 120 122
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog	116 116 116 PF)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy	116 116 (F)
QoS ConfigurationManage QoS Settings ScreenHierarchical Queuing Framework (HQManage QoS Settings—Classes TabManage QoS Settings—Interfaces TabMaximum Reserved Bandwidth DialogAdjust Input QoS PolicyAdjust Output QoS Policy	116 116 9F)
QoS ConfigurationManage QoS Settings ScreenHierarchical Queuing Framework (HQManage QoS Settings—Classes TabManage QoS Settings—Interfaces TabMaximum Reserved Bandwidth DialogAdjust Input QoS PolicyAdjust Output QoS PolicyManaging DMVPN QoS Policies	116 116 116 PF)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies	116 116 116 119 120 122 Box 123 123 124 125 127
QoS ConfigurationManage QoS Settings ScreenHierarchical Queuing Framework (HQManage QoS Settings—Classes TabManage QoS Settings—Interfaces TabMaximum Reserved Bandwidth DialogAdjust Input QoS PolicyAdjust Output QoS PolicyManaging DMVPN QoS Policies	116 116 116 119 120 122 Box 123 123 124 125 127
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies	116 116 116 117 119 120 122 3 Box 123 123 124 125 127 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring	116 116 116 (F)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options	116 116 116 (F)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options	116 116 116 9F)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options Graphing Display	116 116 116 9F)
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options QoS Monitoring to Flow Reports	116 116 116 119 120 122 Box 123 123 124 124 125 127 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options QoS Monitoring to Flow Reports Historical Views	116 116 116 116 119 120 122 3 Box 123 123 123 124 124 125 127 129 129 129 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options QoS Monitoring to Flow Reports Historical Views Policy Management	116 116 116 117 119 120 122 3 Box 123 123 124 125 127 129 129 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options Graphing Display QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies	116 116 116 116 119 120 122 123 123 123 123 124 125 127 129 129 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies	116 116 116 117 119 120 122 123 123 123 124 125 127 129 129 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options Graphing Display QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies Saving, Loading, and Copying QoS Pol Creating Policies from Templates	116 116 116 117 119 120 122 120 122 123 123 124 125 127 129 129 129 129 129 129 129 129
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Graphing Options Graphing Display QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies Saving, Loading, and Copying QoS Pol Creating Policies Ising NBAR	116 116 116 117 118 119 120 121 122 30 121 122 123 124 125 127 129 129 129 129 130 131 131 131 132 icies 132 133 134 135
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies Saving, Loading, and Copying QoS Pol Creating Policies Using NBAR Customizing NBAR Protocols	116 116 116 116 119 120 122 3 Box 123 123 124 124 125 127 129 129 129 129 129 129 129 129
QoS Configuration	116 116 116 116 117 120 121 122 3Box 123 123 123 123 124 125 127 129 129 129 129 129 129 129 129 129 129 129 129 129 130 131 131 131 131 131 132 icies 132 133 135 136 5 137
QoS Configuration Manage QoS Settings Screen Hierarchical Queuing Framework (HQ Manage QoS Settings—Classes Tab Manage QoS Settings—Interfaces Tab Maximum Reserved Bandwidth Dialog Adjust Input QoS Policy Adjust Output QoS Policy Managing DMVPN QoS Policies VLAN Service Policies QoS Monitoring Interface Selection Display Options QoS Monitoring to Flow Reports Historical Views Policy Management Applying and Removing Policies Saving, Loading, and Copying QoS Pol Creating Policies Using NBAR Customizing NBAR Protocols	116 116 116 116 117 120 121 122 3Box 123 124 125 127 129 129 129 129 129 129 129 129 129 129 129 129 129 130 131 131 131 131 132 133 134 135 136 137 138

Chapter 6

	WAN Link Shaping140
	VoIP QoS Policy Creation
Chapter 7	Flow
	Flow Overview
	Supported Flow Technologies
	Benefits
	Key Features
	LiveNX Flow Visualizations
	System View
	System View Drill Down to Flow Report
	Search
	System Flow Table
	LiveNX Tips
	Device View
	Interface View162
Chapter 8	Searching and Filtering 163
	About Searching and Filtering
	Key Features
	Flow Technology Type Grouping164
	Flexible Templates
	Flow Filters
	Custom End Point Filter 001:
	Filter Entries
	Filter Entry Details
	Filter Entry Action
	IP Type
	Color Mapping Label & Color167
	Match Protocol/Ports
	Match IP, Range, Subnet168
	Match DSCP168
	Match Device Interface168
	Match Flow Size168
	Match TCP Flags169
	Match Autonomous System Number (ASN)169
	Match Next Hop, IP, Range, Subnet169
	Match IPv6 Flow Label
	Match MAC Address
	Match VLAN
	Protocols/Applications Setup170
	Flow Color Mapping
	Flow Path Analysis
	Historical Playback. 177
	Create ACLs Based on Flows
	Flow Buffers
	Flow Data Status
	Database File Size
	IP Mapping
	IP Blacklist
	Alerting
	NetFlow Collection
	Cisco Device and NetFlow Version Support
	LiveNX NetFlow Process Overview
	Databases
	Databases
	Derice and Display I needs

	Real-Time and Historical Displays	
	Cisco NetFlow Collector Commands	
	Flexible NetFlow (FNF)	
	Advantages	
	Features for Tracking	
	Platforms	
	Configure Flow	
	6	
	Enabling NetFlow.	
	Disabling NetFlow	
	Advanced NetFlow Collector Commands	
	Precautions When Using NetFlow Collector Mode	
	Deployment Considerations	
	LiveNX Flow Configuration	
	Cisco NetFlow	
	Default Flow Settings	190
	Device Configuration Notes	190
	IPv4 Configuration	
	IPv6 Configuration	
	Medianet Configuration	
	Cisco Adaptive Security Appliance (ASA) Configuration	
	Minimum Required Template Fields	
	Non-Cisco Device Flow	
	sFlow Collection.	
	sFlow Export Format	
Chapter 9	Routing	195
Unapter 5	Routing Overview	
	-	
	Applications and Benefits	
	Network Architecture Analysis	
	Security	
	Troubleshooting	
	How LiveNX Routing Works	
	LiveNX Tip—The "Other" Interface	
	LiveNX Routing Views	
	Refresh Timeout Limit	
	Routing Adjacency	199
	Next-Hop Routing	
	Routing Device-Level View	
	Routing Table	
	Adjacency Table	
	LiveNX Policy-Based Routing (PBR)	
	What is Policy-Based Routing?	
	Policy-Based Routing Monitoring Configuration	
	PBR Monitoring	
	PBR Configuration	
	Creating a Route Map	
	Match Commands	
	Set Commands	
	Preview CLI.	
	Policy-Based Routing Workflow	
	Applying Policy-Based Routing	
	Monitoring Policy-Based Routing	
	LiveNX Virtual Routing and Forwarding (VRF)	
A		
Chapter 10	IP SLA	
	IP SLA Overview.	
	About Cisco IOS IP SLA.	

	Key Features and Benefits	
	Getting Started with LiveNX IP SLA	211
	Cisco IOS and Catalyst Operating System Version IP SLA Support	212
	Network Device Considerations	212
	CPU Usage	212
	Configuring LiveNX IP SLA	212
	Setup Quick Test Wizard	213
	Managing Tests	217
	Advanced Test Scheduling	219
	Advanced Test Scheduling	219
	Test Groups	220
	IP SLA System Tests	220
	Managing IP SLA System Tests	221
Chapter 11	LAN	225
	LAN Overview	
	Key Features and Benefits	
	Real-Time Monitoring	
	Getting Started With LiveNX LAN	
	Network Visualization	
	VLAN List in the System Hierarchy View.	
	VLANs in the Add Device Process	
	Spanning Tree Highlighting Through a Network	
	Real-time Monitoring	
	Find IP and MAC addresses	
	T - 1-	0.40
Chapter 12	Tools	
	Tools Overview	
	System Advisories	
	IP Mapping	
	IP Blacklist.	
	MSI Endpoints	
	Use/Edit VSOM (Video Surveillance Operation Manager) Mappings.	
	Manage Performance Groups and Application Groups	
	Manage Performance Groups	
	Manage Application Groups	
	Manage/Define Custom Applications	
	DNS Name Resolution	
	Device Tools	
	Saving Changes to the Device's Startup Configuration	
	Accessing the Device Web Page from LiveNX	
	Managing ACLs	
	Statistics	
	Miscellaneous OID Polling and Charting	
	Group Management	
	Options	
	Database	
	Email	
	SMTP Server	
	Email Settings	
	Send a Test Email	
	Security	
	Export Server/Client /Nodes Logs	
	Export Device Data	274

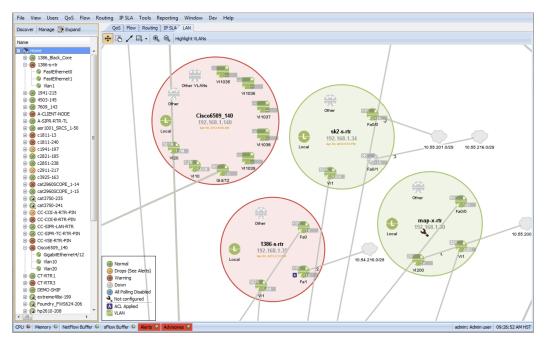
CHAPTER 1

Introduction

In this chapter:

About LiveNX	2
Contacting LiveAction Support.	7

About LiveNX



LiveNX is an intelligent, action-oriented software that provides real-time visualizations, deep monitoring, configuration, and troubleshooting of multi-vendor network devices, with an easy-to-use graphical user interface. The system consists of a lightweight, but highly scalable framework and multiple technology modules, each providing specialized software functions and feature sets. Technology modules currently available are LiveNX QoS, Flow, Routing, IP SLA and LAN.

LiveNX delivers its network and application monitoring capabilities via two User Interfaces. The Operations Dashboard delivered via Web technologies is the primary interface and is built for Day 2 network operations. The Engineering Console is delivered via a thick-client and is built for configurations (for e.g., QoS policies) and caters to Network Engineers and Architects who want to perform deeper troubleshooting tasks. This User Guide is built for users of the Engineering Console. For the User Guide built for users of the Operations Dashboard, please refer to our complete documentation at <u>https://</u> <u>docs.liveaction.com/LiveNX</u>.

LiveNX provides a different approach to network management that combines extensive device knowledge with rich network visualizations. The software captures the actual router and switch configurations to build a highly interactive "mental model" of the network, enabling users to literally "see" flows, routes, and QoS policies operating in real time—across the network topology and deep inside each device. The result is an incredibly true and relevant understanding of the network for fast and accurate troubleshooting and highly informed decision making.

LiveNX is available as virtual, physical or cloud appliances. We support flexible deployment options based on our Customers' requirements. LiveNX appliances are self-contained with operating system, system libraries, applications, and utilities. As mentioned earlier, LiveNX supports two user interfaces—a web driven Operations Dashboard and a thick-client driven Engineering Console. The features available and the number of network devices that can be managed concurrently depend on the license purchased. The software includes a comprehensive collection of pre-configured device settings and templates based on industry and manufacturer best practices that enable network engineers at any experience level to perform advanced router functions with ease and confidence.

For monitoring, the software polls the remote network devices at a user-settable polling rate using SNMPv2 or SNMPv3. The polling engine has been optimized to poll at a speed of up to 10-second intervals for fast updating of information and values that show actual rather than averaged rates for the instant, accurate feedback. The data is also stored in its own database for report generation and historical views.

For configuration, the software includes an intelligent, knowledge-driven engine with self-contained rules for each of the various technologies supported. Network engineers can connect to the routers using Telnet or SSH for advanced, on-the-fly router configuration without the need to use the Cisco command line interface (CLI).

Technology Modules

LiveNX is a modular software framework that enables live viewing and control of multiple device technologies using a single tool and a common user interface. Technology modules are currently available for the following, with new modules added in the future as they become available:

- QoS
- Flow
- Routing
- IP SLA
- LAN

Configuration features

- Full Modular QoS CLI (MQC) and Hierarchical Queuing Framework (HQF) configuration support
- Powerful editor engine for safely constructing a complex set of configuration changes offline, validating the correctness and utility of those changes, and then applying them to the remote device all at once
- Easy-to-use, full QoS editor
 - Custom inbound and outbound QoS policy editor
- Graphical pie charts depicting bandwidth allocation among classes
 - "Snapshot" capability for capturing current configurations
- Manual rollback feature to load previous snapshots into the device at any time
- Application and removal of QoS policies for multiple interfaces
- Ability to push QoS configurations to multiple devices easily
- Hierarchical policy creation for advanced configurations and WAN shaping
- Custom NBAR protocol definitions
- Unknown port identification and NBAR protocol match creation
- CLI command preview
 - GRE tunnel QoS and visualization
- Pre-defined QoS policy templates based on Cisco and industry best practices
- Instant QoS policy creation using NBAR capabilities

Monitoring features

- Rate-based NBAR graphs
- Pre- and post-QoS graphs
- QoS packet drop graph
- Interface-level packet drop graph
- Extreme low-level graphs of CBQoS statistics

- Built in CBQoS MIB viewer
- Ability to graph hierarchical policies
- Multi-day interactive baseline graphs
- Reporting capabilities
- Export data and screen capture capabilities

Troubleshooting features

- QoS Audit capability across the network
- Unknown port discovery
- View QoS graphs across routers
- Topology-based QoS state indicator

QoS Module

The LiveNX QoS technology module monitors and configures Quality of service (QoS) on Cisco routers and Catalyst switches that support Modular QoS CLI. For more details, refer to Chapter 6, *QoS*.

Flow Module

The LiveNX Flow technology module provides advanced system-level flow visualization, as well as internal router and interface flow visualizations and graphs. For more details, refer to Chapter 7, *Flow*.

Features

- Topology-based flow view across multiple devices
- Supports Cisco NetFlow v5, v9 and flexible NetFlow, IPFIX, Juniper J-Flow, sFlow from various vendors including Hewlett-Packard, Alcatel-Lucent, and 3Com
- NetFlow views inside the router for tracing flows from ingress to egress
- Full reporting capabilities
- Flow based dashboards
- Flow filtering based on DSCP, port, source address, or destination address
- Flow tables with the ability to sort and select flows
- Detailed information on individual flows
- Works in NetFlow MIB and Collector modes
- Ability to start and stop NetFlow data on a per-device basis
- Flow graph per interface based on destination or source address, DSCP, or port
- Ability to resolve IP addresses to hostname

Benefits

- Faster troubleshooting of the network
- Ability to view flows across the network
- Ability to pinpoint entry and exit of flows
- Improved visibility and understanding of the flows
- Observe the effects of routing and PBR, such as route updates and asymmetric routing

Routing Module

The LiveNX Routing technology module provides real-time routing-layer visualizations for Cisco networks. In addition, the module's policy-based routing feature provides a high degree of control, allowing users to route traffic easily and predictably over user-specified paths. For more details, refer to Chapter 9, *Routing*.

Features

- System-level topology view of active routes
 - Displays by protocol, directionality, and destination
 - Mouse-over displays individual route statistics
 - Next-Hop Routing visualization
 - OSPF and EIGRP neighbor adjacency
- Device route-table views in graphical and tabular form
 - Shows destinations for interface
 - Displays all entries or filtered entries only
- Route display filtering by protocol
 - Filters by direct and static routes
 - Filters EIGRP, OSPF, BGP, and RIP protocols
 - Filters per user and periodic downloaded static routes
 - Other filters: IS-IS, mobile, on demand, IGRP, EGP
- Route display filtering by destination
 - Shows default route
 - Shows routes to destination IP address
 - Shows routes to destination network
- Export function
 - Exports route and route table information for further analysis
 - Exports forwarding tables to CSV file (by device)
- Refresh real-time updates of routing layer—refreshes all routes or specified routes only
- Troubleshooting capabilities
 - Displays routing loops and asymmetric routes
 - Alerts to routing instabilities
 - Detects black holes
 - Provides error summarization
- Policy-based routing (PBR)
 - Configuration and editing of PBR and Set statements
 - Editing of existing route map configurations
 - Validates user entries to ensure PBR compliance
 - Displays indicate where PBR is applied
 - Exports route map statistics

- Displays static routes and PBR issues
- Virtual Routing and Forwarding (VRF) visualization
 - Displays virtual routing and forwarding tables
 - Exports VRF tables to CSV file

IP SLA Module

The LiveNX IP SLA technology module makes Cisco IOS IP service level agreement (SLA) operations easily accessible for generating synthetic network traffic to monitor latency, loss, jitter, and mean opinion score (MOS) for VoIP. For more details, refer to Chapter 10, *IP SLA*.

Features

- Latency, loss, jitter, and MOS performance measurements
- System wide IPSLA hub and spoke and mesh configurations
- Test types: DHCP, DNS, FTP, HTTP, ICMP Echo, Jitter, Path Echo, Path Jitter, UDP Echo
 - Traffic type configuration
- Protocol type: more than 10 protocol types
 - DHCP: destination, source, circuit ID, remote ID, subnet mask
- Test frequency setting
- Jitter test parameters—VoIP codec simulation (G.711 ulaw, G.711 alaw, G.729a)
 - Mode: active or passive
 - Packet priority: normal or high
 - Precision: in microseconds or milliseconds
- IP SLA topology view (real time)
 - Multiple colors for visualization
 - Loss indicators
 - Normal and above-threshold indicators
 - Lists of running tests (indicating source, type, status)
- Quick and full test options
- Set up responder at destination
- Start/Stop traffic tests
- Edit, save, or delete test configurations
- Export results to CSV file
- Historical reporting (live update averages over timeline)
 - Variable sampling rates: from 10 seconds to 5 minutes
 - Latency: milliseconds over time, microseconds for jitter
 - Loss: number of dropped packets
 - VoIP MOS range: 1-5

LAN Module

The LiveNX LAN technology module provides real-time Layer 2 visualizations for networks, including trunk interfaces, port channels, VLAN associations and bandwidth percentages. For more details, refer to Chapter 11, *LAN*.

Features

- Network Visualization
 - Automatic device discovery
 - VLAN trunk, port channel names
 - VLAN associations within a device
 - VLAN highlighting through a network
 - Input/Output bandwidth of each VLAN and port interface
- Real-Time Monitoring
 - Trunk and access bandwidth information through network polling
 - Layer 2 QoS statistics including CoS, DSCP and IP precedence
 - Dropped packets, interface warnings through network polling at the VLAN level

Contacting LiveAction Support

Please contact LiveAction support at *https://www.liveaction.com/support/technical-support/* if you have any questions about the installation and use of LiveNX.

An RMA (Return Material Authorization) number must be obtained from LiveAction before returning hardware. Please contact LiveAction technical support at *https://www.liveaction.com/support/technical-support/* for instructions.

CHAPTER 2

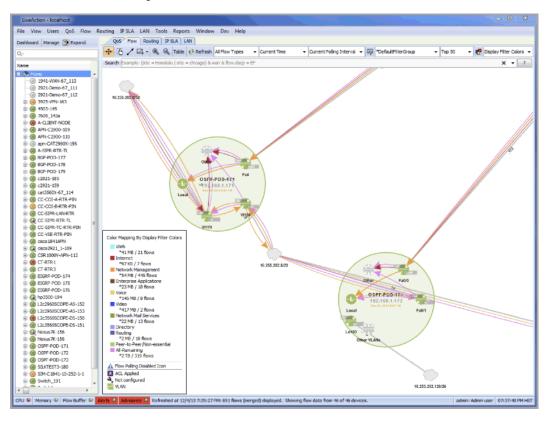
LiveNX Engineering Console User Interface

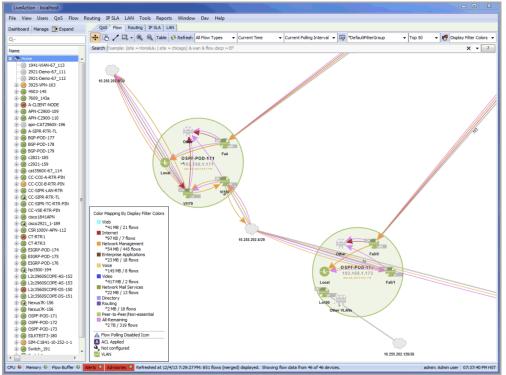
In this chapter:

About the Engineering Console User Interface	9
LiveNX Best Practices	13

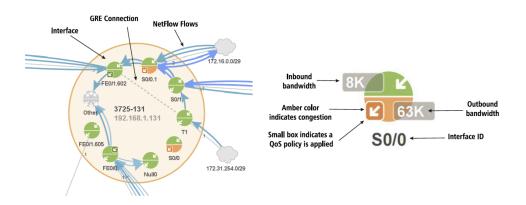
About the Engineering Console User Interface

In the topology view, the objects in the main window represent network devices, subnets, and other user-definable objects. The larger circles represent network devices. Individual interfaces are shown as smaller circles inside the network device. Devices may be organized into groups that will appear as annotated, colored rectangles.

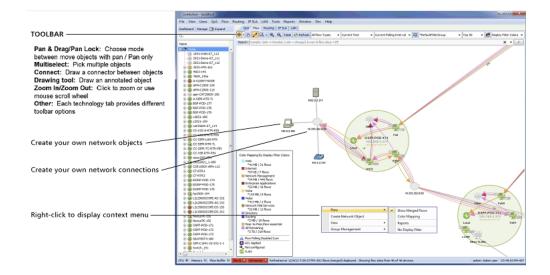


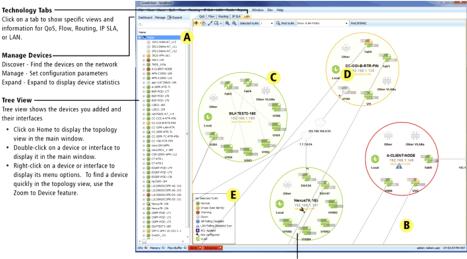


The top half of each interface represents inbound traffic and the bottom half represents outbound traffic. The color of each half indicates its status—green indicates normal, orange indicates congestion, and gray indicates the interface is disabled. Inbound and outbound bandwidth values for each interface can be displayed by right-clicking on the device.



Topology View Interface Controls





Basic Navigation

- To zoom, use mouse scroll wheel or press [Ctrl] [+] and [Ctrl] [-] · To pan the network, click and drag the background area

Main Window - (Topology View shown)

- A To display the Topology (Home) view, click Home in the Tree view B - Connected ports appear as solid lines - wider lines depict greater bandwidth
- · To move objects, click and drag the object
- Devices appear as large circles. Double-click for device level view.
- D Interfaces appear as smaller circles. Double-click for interface level view
- E Information legend identifies interface items and color coding

View Menu

The View menu contains menu options related to the topology views. These options include:

- Save Image saves a PNG image of the current topology view
- Fit to View resizes the topology view to fit all the objects on the topology
- **Reset View** resets the pan and zoom of the topology to the default view
- **Reset Layout** resets the layout of the topology.
- **Note** Any changes you made to the layout (moving devices) will be reset to the default layout.
 - Sync to Master Layout synchronizes your current topology layout with the saved master layout
 - Save as Master Layout saves the current topology layout as the "master layout."

Note Only users with the admin role can save a master layout.

- **Show Bandwidths** toggles the display of bandwidth statistics on the topology (shown on the interface icons)
- Show ACLs toggles the display of icons indicating that an ACL is applied to the interface
- Show Legends toggles the display of the legend in the lower-left corner of the topology
- Scale Names toggles a control to maintain a viewable font size for the device name and IP address while zooming in and out in the system view. Default: Scale Names is enabled.
- Force Subnet Display for All Interfaces toggles a control to override cases where interfaces don't show its associated subnet cloud. Cases, where this occurs, are with SVI interfaces for which there are no access ports associated with the VLAN and sub-interface parent interfaces with assigned IP addresses. This is available for the admin user only.
- **Export Topology to Visio** allows exporting the topology view into a Visio file format. Click on Export Main Topology to export the main topology. Collapsed groups will appear as collapsed groups during the export. To show all devices, click on a group, select Expand All and then export. Click on Export Group Topologies to export each group as a separate tab within Visio. Click to

highlight the desired groups to export. Click on Browse to determine the file location for the exported .vdx file and then click on Export. This feature is supported using Visio 2013.

A Export	t Visio Diagram	×
Visio File	sers\LiveAction Demo\Documents\4.2\export_2_visio.vdx	Browse
	rt Main Topology ort Group Topologies	
QA-L2-C Kapiolani	ampus Campus	
	Export	Cancel

Exporting and Importing a LiveNX Configuration

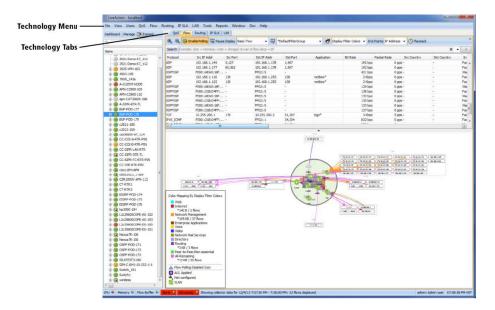
Configurations can be exchanged between different installed LiveNX clients in order to simplify environment setup. To export a LiveNX configuration, first launch the Management Console from the LiveNX server. Then go to the Manage menu and select Export Configurations. The configuration will be saved to a configuration file.

To import a saved LiveNX configuration file, go to the Manage menu and select Import Configurations. LiveNX must be restarted to load the imported layout.

Note Configuration exporting and importing functions are only available to the Administrator.

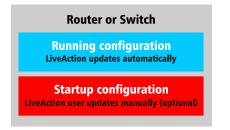
LiveNX Technology Tabs

The LiveNX software currently supports QoS, Flow, Routing, IP SLA and LAN. Settings and information for each of these technologies can be accessed by clicking on the technology tabs or by selecting the technology menus.



Usage and Deployment Guidelines

LiveNX runs as an appliance (virtual, physical or cloud) and enables full control of network devices from the appliance's location. The Engineering Console runs on a Windows or Mac computer as a client through which a User can make configuration changes. The software updates the running configuration of the device. For the changes to be permanent, you can manually invoke the device's command to save the settings to the device's startup configuration.

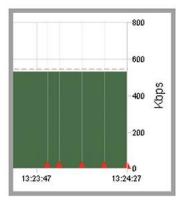


LiveNX Interface Color Codes

The various colors used in the software indicate a specific status as shown in the table below.

Green	Normal
Dark Green	Normal and QoS policy exist on interface
Orange	Congestion or drops occurring
Red	High CPU or memory usage on device
Gray	Device or interface down
Blue	Polling to device turned off

If any error occurs on the graph, a red triangular indicator will appear. Causes of the errors may include missed polling due to dropped packets, a non-responsive device, or other connectivity issues.



Logical Topology (Preview)

The logical topology view allows LiveNX users to focus on a specific section of their topology.

LiveNX Best Practices

Web search, a daily ritual in our connected lives is highly effective due to tagging of information. Wouldn't it be great if you had a similar capability to search and ask questions related to the network? LiveNX network semantics help you understand and troubleshoot their network better and faster. Using LiveNX's big data analytics platform you can tag network devices and interfaces to enable search, reporting and dashboard capabilities. LiveNX provides a rich and flexible way to leverage network semantics. You have the capability to assign multiple tags to a device or interface to gain improved understanding of the network and extract relevant data faster via search, reports or dashboard. Network semantics can be leveraged to identify and create:

- Groups
- Sites and Site IPs
- WAN Links
- Service Providers
- Labels
- Capacity
- Device and Interface Tags
- Data Centers

Groups

A group represents a collection of network devices and are created to easily view the relevant information. When managing multiple network devices in LiveNX, it is recommended that you create groups. Groups help visually and logically organize devices and enable easy access to critical information related to the group. All network devices in a group are visualized on the topology as part of the group. In our case, we have created multiple groups based on location e.g. LA, London, Santa Clara etc., as shown below.

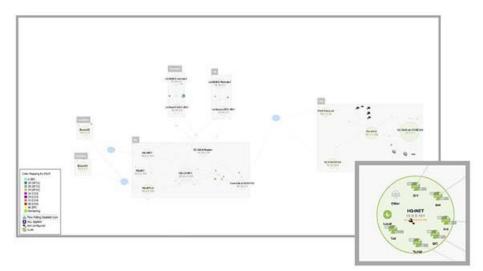


Each group contains network devices managed by LiveNX and can be seen by expanding the group as shown below. You can expand the group to see the network devices. Each network device can be further expanded to see the managed interfaces. For each managed entity, LiveNX provides detailed information about the device and interface.

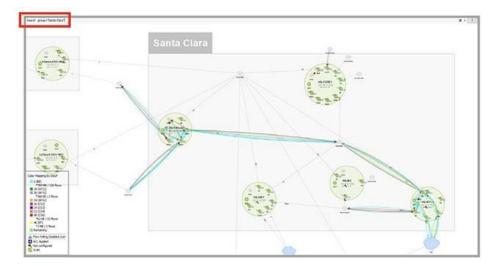
**	P AMPRO	note	Leve	Capitity	-	mark Pri-	540	the P	Tap	Destro-	Arries .	04	Hampy	part.	Case dragt	Date (hanged
() Hang		_	-										_	_		
(i) (it Contine MANAIN	10.00.21	10.0	-				Sate they	M-0-0 M-0, M-0-0 M-1, M		Cause Md.	Langelog	~		~	~	
in (i) OC-math-Ander	10.00.2.00	Land						HAR BUT HAR HE H.		Carp 30		2	- 2	12		And in case of the lot of
IS OF INCOMES	15.35.2.254	1000					Same Care	BAAMS, BAAMS, BA.		Carta XD		20				Arr \$1, 2010 7:00 are
IN CONCINCT	16.8.6.101	Local					Sette Des	\$5.0.0. MIL \$5.0.0. MIL 10.		Carin 32			- 22			Arr 10, 2010 1-12,000
10 HOHO	10.0.0.000	Local					Same Class	\$1.0.0 W1 \$1.0.0 W1 \$1.0		Case 83		100	142			Test 191, 2014 2 110 44
1 8 HO HILL	10.0.0 102	Local					Sarta, Data	100.00.00.00.00.00.		Gaug 32						34-08-2216-33-04
												- 21		-		
10.00 76.0272	10.3.3.254	Liverst Aude								Case Mr.	Long. Inc.					THE R. POST AND P.
Contraction of	10.5.2.10	Line of Andre					140			Painets						NA
1 (a) 10 (85) -6 CONDIN	10.1.1.1	Linet in Assiste					9.9			Caux 32-						
C 1C AGADEIDA	10.00.00.0	Lines Aude					HQ			Calls M	Lock/w					N/R
D ⁴							C74									
IS IS LOTTE - 2023 AUS	10.00.2.5	Local Division								Carto 32	Sint-	4	- 44			3445,208,34798
IE IE LADOR America	10.30.5.1	Line .					Las Argeles			Cere 32		14	14		6	
ander .																
In the brand 2	100.21	Lince					Landan	106-103-024, 10:03:13		Gau 32	Looking					Sam 10. 2010 0 2110
and Indiana																
A B Banchi	10.0.1.1	Local					Loder	196.16.1.074.10.0.1		Cera 35	Long-Jac					Aug. 10. 10. 10. 10. 10.
Texts																
141 (2) LADent-3121422	10.36.3.6	Local								Owo 33	time.		- 64	5	6	34-17,25117,4194
In III LADINO-remain2	10.30.8.1	Local					Taianta			Geo 33	Lines.m		- W	6	6	Apr 22, 30 of 10 C2 AM

LiveNX provides an intuitive and interactive topology as shown below. Groups enable visualization and quick problem resolution on the topology map. Each square box on the topology corresponds to a group with network devices and third-party flow elements contained within each group.

You can zoom in or out of a group for visualizing network devices and interfaces. Grouping capability makes the topology scalable. Zooming in and out can automatically expand and collapse the groups which make it easier to view all flow info to and from groups. You can double-click on a group to expand a group. Zooming into a group shows network devices and third-party flow generating devices. Each bigger circle in a group represents a network device while interfaces with ingress and egress are denoted by arrows. Any issue on the device or interface is highlighted in red or yellow. Simply click on the element to get additional details.

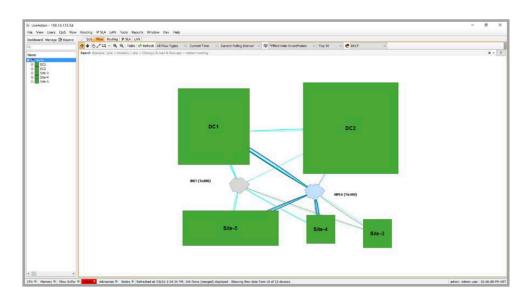


Additionally, a search filter applied to a particular group shows flow data related to all the devices in the specified group only. This helps narrow traffic flow visualization and makes for easier troubleshooting. The figure below shows the flows related to group Santa Clara when a filter for group=Santa_Clara is applied.



Grouping devices are also important to help visualize the flows ingressing and egressing a collapsed group. The ingress and egress flow from a group can be to another device or another group as shown below.

Collapsed groups also increase the performance of LiveNX by efficiently rendering the devices on the topology. You can simply zoom into a group to see the details.



Sites and Site IPs

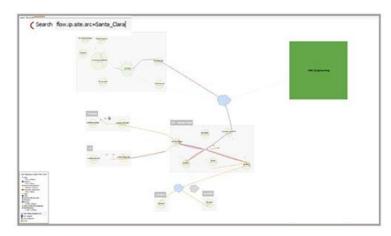
The site is another label that can be assigned to a network device. Sites are not visually displayed on the topology. However, sites are a logical grouping of devices and used for searching, running reports and observing data on the dashboard. LiveNX recommends that you should assign network devices to a site and make the site name correspond to the group name (e.g. if you have created a group LA and assigned network devices to the group, assign site LA to those same network devices). Typically, a site corresponds to the geographic location of the branch/data center. Once sites are assigned to devices, site info can be used to run flow queries, reports and dashboard. Sites created in the figure below are the same as the groups created in LiveNX.

ne	IP Address	Node	Label	Capacity	WAN	Service Pro	Site	Site IP	Tags	Descrip	Poling	OPU .	Memory	Interf	Class drop	Date Changed
Home DC HQ HQ PA-9372	10.1.1.254	Livef0(-Node)	1							Cisco NO-	Impute	•	•			May 26, 2014 1 16 PM
TH C PAN Frend	10.1.2.10	LivelO: Node1					10			Perinde						NA
. SC-3850-48-CORESW	10.1.1.1	UveNX-Node1					HQ			Cisco 10			0	•	0	Hey 19, 2016 2:50 PH
CASASSISX	10.10.20.9	LiveNX Node1					HQ			Osco Ad	1 minute	•	•	•	•	N/A
1 CADemo-2921-R01	10.30.3.1	Local								Cisco 10	10 sec	0	0	•	0	Jun 07, 2015 7:47 PM
ADEMO-Remote1	10.30.5.1	Local					Los_Angeles			Cisco (O,					-	
London																
Branch2	10.0.2.1	Local					London	198.19.2.0/24, 10.0.2.1		Cisco IO	1 minute		0		•	Jun 68, 2016 9:24 PF
Sydney																
Toronto	10.0.1.1	Local					Syndey	198.19.1.0/24, 10.0.1.1		Cece (0	1 minute		•	•	•	Jun 108, 2016 9:00 PM
1 (a) LADem0-2921-R02	10.30.3.6	Local								Cisco 10	10 sec	0		0	0	Jun 07, 2016 7:48 PM
E G LADEMO remote2	10.30.6.1	Local					Toronto			Cisco 10		0	0	0	6	Apr 22, 2015 11:02 AM

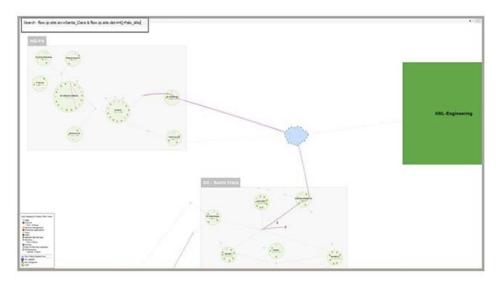
In addition to assigning a site to device(s), site also has a Site IP field as shown below. Site IP field can contain multiple entries and can be either an IP range or IP addresses. Providing Site IP information enables LiveNX to display relevant flows to and from sites, helping identify site-to-site traffic.

Site	۲
Site	London
IP	198.19.2.0/24 10.0.2.1
DC	Enter IP address ranges in CIDR format

When troubleshooting an issue between two sites, you can use site search queries to filter flows between applicable sites and relevant application(s) for quick visibility and faster troubleshooting. For example, if an admin wants to view all the flows originating from a site (Santa Clara), they can simply enter a query flow.ip.site.src=Santa_Clara with the result being shown below.

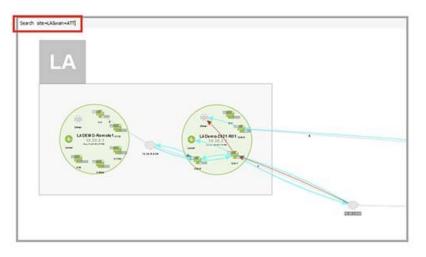


In addition, the admin can further narrow down the query to show flow data only between two specific sites. In our case, we are interested in the source as Santa Clara and destination being Palo Alto. The query will be flow.ip.site.src=Santa_Clara & flow.ip.site.dst=HQ-Palo_Alto with the result shown below.



WAN and Service Provider

LiveNX recommends tagging all WAN links in the network. When filtering flows, you can use the WAN filter to see traffic related to WAN flows only. Filtering traffic for WAN shows the usage of WAN links and the major consumers of bandwidth. A WAN link can be identified by simply checking the WAN check box. In addition to the WAN check box, another label called Service Provider is available for further identification of the WAN link. You can use this field to either identify the name of the Service Provider or the type of link e.g. MPLS, Internet etc. Links depicted as WAN with the Service Provider label is displayed on the LiveNX topology and helps visualize WAN related info. In our example, the network admin has filtered the flows based on the site and WAN provider.



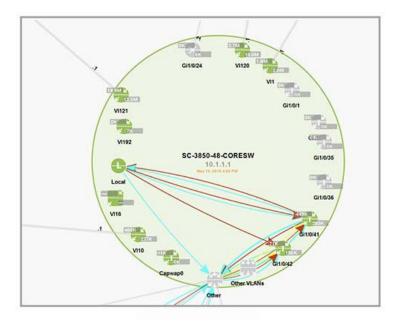
Label

You can also assign a label to interface(s). Labels are an additional identifier that can be used to search and filter the information available. Simply assign a label to the interface by selecting a previous label or adding a new one.

Details	
Interface Details	*
Interface name	
Ethernet1/12	
IP address	
12.33.223.132	
Description	
outside	
Interface type	
ethernet_csmacd	
Interface speed	
0	
Define	۲
Label outside	
Capacity	100000 Kbps
Service Provider	
V WAN	
Name ATT	~
Remove unused servi	ice providers
Tags	
Enter tag here then pres	is ENTER to add
✓ Tag	Used
√ frewall	

Capacity

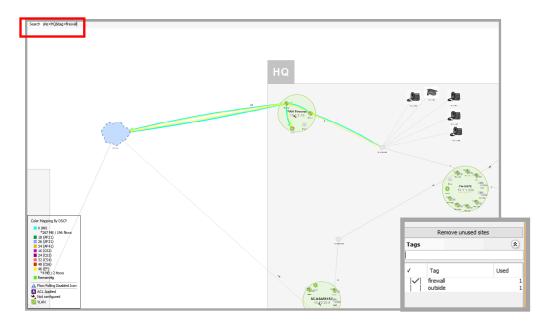
Capacity field denotes the capacity of an interface. Often, the configured capacity/bandwidth of an interface can be different from the maximum bandwidth of the physical interface. Once you have configured the capacity, the capacity information is leveraged for capacity planning reports. It is important to configure the capacity of interfaces for accurate 99th and 95th utilization. Leveraging the percentile utilization helps in accurate capacity planning.



You can see interface details by simply zooming in on a network device on the topology. The topology shows the device with the bigger circle with all its interfaces within that circle. Each interface has an ingress and egress and the capacity shown is the bandwidth of that interface.

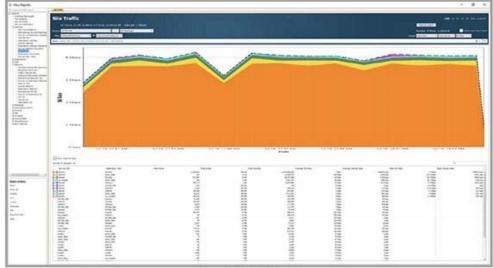
Device and Interface Tags

Tags can be assigned to network devices or interfaces. You can use tags to filter flows in their search queries. Tags assigned to network devices or interfaces do not show up visually on the topology, however, they are helpful in filtering flows. The figure below shows the ability to visualize and filter flows based on tags. In this case, we have applied a filter site=HQ&tag=firewall which shows only the flows related to the device(s) tagged as firewall.



Reporting

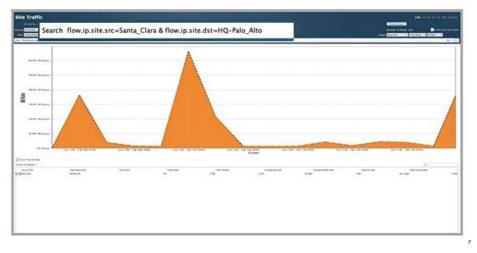
LiveNX also provides the capability to leverage its extensive reporting capabilities with network semantics. Network instrumentation and flows generate a lot of data which has to be processed in a meaning-



ful way for accurate decision making (e.g. a user can run site to site reports by simply running a Site report). If the sites are properly identified, the report represents the flow data between sites.

Figure 14. Site Report

You can further filter the data in the report by using search queries similar to the ones identified in the Sites section. In our case, we run a site-to-site report between Santa Clara and Palo Alto with Santa Clara as the source and Palo Alto as the destination. The report in the image below shows the traffic between those two sites only with the query flow.ip.site.src=Santa_Clara & flow.ip.site.dst=HQ-Palo_Alto.



LiveNX provides a rich variety of network semantics to filter relevant flow information and enable faster troubleshooting. Adding semantics is an evolutionary exercise as you get increasingly familiar with LiveNX and the power of semantics. As a starting point, we recommend that you:

- Create groups to organize and visualize network devices on the topology
- Assign sites to devices that correspond to the groups
- Identify and check the WAN links and identify the Service Provider or the type of link
- · Assign capacity to the WAN interfaces and critical network interfaces
- Labels and Tags can be part of an ongoing effort to effectively help in troubleshooting

CHAPTER 3

Dashboard

In this chapter:

About the Dashboard	22
QoS Dashboard	29
WAN Dashboard	<u>60</u>

About the Dashboard

Technology Dashboards

The LiveNX Dashboard provides real-time system-level alert and device status information. The Dashboard section is segmented into the flowing actionable areas, on the left Search, and subject tree, and on the right five subject tabs QoS, Flow, Routing, IP SLA, and WAN. Due to the system level, the dashboard can also be configured to open upon start-up of the LiveNX client.

Dashboards are segmented into two areas, the Menu tree on the left-hand side and the Display area. To enable automatic startup, go to the Dashboard, click on the drop-down in the top left-hand corner of the device tree view and enable Open at startup. Each Dashboard consists of a set of predefined widgets. Below is an example of the System Dashboard in the Java client.

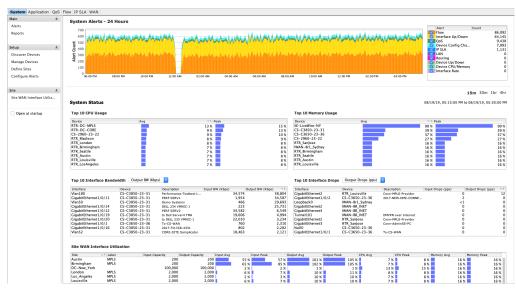


The Action bar of the Dashboard (on the left) displays a set of actions that can be taken, each of these actions is covered in the corresponding topic Chapters:

- Alerts Chapter 4, Alerts and Notifications
- Reports Chapter 5, *Reporting*

System Dashboard

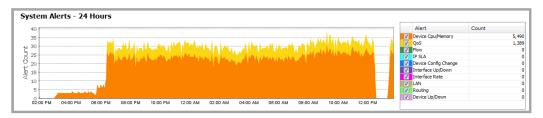
The System Dashboard presents a snapshot of the resources in the network, it lists the Alert count, and a set of widgets that display the status of Top devices in each category, CPU, Memory, Interface Bandwidth and Drops, and WAN Utilization. Within each widget the order can be displayed from Highest to Lowest, or vice-a-versa by clicking on the title bar within each widget.



Site WAN Interface in the action column will display The Site – WAN Interface report. This report provides a historical summary of the QoS properties of all the interfaces that are defined as WAN interfaces, grouped by Site tag.

System Alerts

The System Alerts – 24 Hours charts the total number of generated alerts within the last 24 hours. The chart uses a rolling window format. The most recent count of alerts is generated at the right edge of the chart and older data is moved to the left until any data beyond 24 hours is deleted from the chart.



The legend to the right of the System Alerts chart is a tabular summary of the total generated alerts for the chart duration. Use the check box alongside each alert type to enable or disable viewing the alert category from the chart.

The charts and tables below the System Alerts graph provide real-time average data for the dashboard time duration selected. Four-time durations are available: last 15 minutes, last 30 minutes, last 1 hour and last 4 hours. Default is last 15 minutes.

Top CPU Usage

The Top 10 CPU usage chart is a bar chart summarizing the top 10 devices with the highest average and peak % CPU usage. Click on the Device header to list the ten devices in alphanumeric order. Click on the Avg header to toggle the chart to sort from the lowest to the highest average % CPU usage. Click on the Peak header to toggle the chart to sort from the lowest to the highest peak % CPU usage. Default is top 10 devices with the highest average CPU usage.

Device Av	∕g ▼ 1	Peak
LA2921-R01	48 %	48 %
TO2921-R01	43 %	43 %
DC-ASA5515x	39 %	39 %
PA-3850	36 %	36 %
HNL-ASA Device CPU/Memor	v Usage Report 34 %	34 %
DC-Core1 Joso	33 %	33 %
cat2960SCOPE_1-15	33 %	33 %
cat2960SCOPE_1-14	33 %	33 %
APN-AS-17	29 %	29 %
APN-DS-16	28 %	28 %

Right-click on an entry in the table and then select View Graph to bring up a historical Device CPU and Memory Usage time-series report. The report will automatically use the selected device.

•••				QoS Report	s				
Q- Type here to filter repoi			1000						
Interface Bandwidth 11 Interface Utilization 11 Interface Bandwidth Con 11	/14/1	1d 1w 30d 90d	11/14/16, 03:30:	.00 PM Data bin:	te Report				
Pre-Policy and Post-Polic				CPU	and Memory	Usage			
Pre-Policy and Post-Polic Pre-Policy and Post-Polic Top CPU Usage Top Interface Bandwidth Top Interface Bandwidth Top Class Brops Site Bandwidth Interface Burstable Rate Site WAN Interface Utiliz Site Alert Cetail Site Alert Cetail Custom Reports Cap CPU vear/v	100								
Report Actions	0								
Save		Nov 14, 03:16 PM	Nov 14, 03:18 PM	Nov 14, 03:20 PM	Nov 14, 03:22 PM	Nov 14, 03:24 PM	Nov 14, 03:26 PM	Nov 14, 03:28 PM	
Save As	Nam	e U Usage		Average		99%	Peak		99%
Delete		mory Usage				27%			27%
Schedule									
PDF									
Export to CSV									
Help									
101-1267									

Top 10 Memory Usage

The Top 10 Memory usage chart is a bar chart summarizing the top 10 devices with the highest average and peak % memory usage. Click on the Device header to list the ten devices in alphanumeric order. Click on the Avg header to toggle the chart to sort from the lowest to the highest average % memory usage. Click on the Peak header to toggle the chart to sort from the lowest to the highest peak % memory usage. Default is top 10 devices with the highest average memory usage.

Device A	vg = 1	Peak
LA2921-R01	48 %	48 %
TO2921-R01	43 %	43 %
DC-ASA5515x	39 %	39 %
PA-3850	36 %	36 %
HNL-ASA Device CPU/Memo	ry Usage Report 34 %	34 %
DC-Core1	33 %	33 %
cat2960SCOPE_1-15	33 %	33 %
cat2960SCOPE_1-14	33 %	33 %
APN-AS-17	29 %	29 %
APN-DS-16	28 %	28 %

Right-click on a device name in the table and then select View Graph to bring up a historical Device CPU and Memory Usage time-series report. The report will automatically use the selected device.

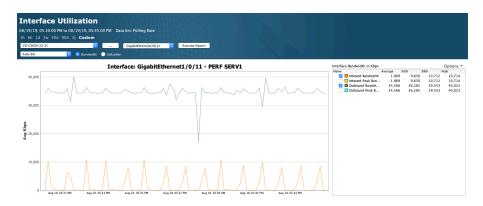
				QoS Repor	ts				
Q- Type here to filter repoi	1	11.00							
▼ Reports	Dev	ice CPU/	Memory	Usage					
Device CPU/Memory Usage Interface Bandwidth	A set of the								
Interface Utilization				:00 PM Data bin	: none				
Interface Bandwidth Compa	1h 6h	1d 1w 30d 90	d ly Custom						
Interface/Interface Drops NBAR Comparison	PA-38	i0	\$	Execu	ite Report				
NBAR and Post-Policy									
Pre-Policy and Post-Policy				CPU	and Memory	Usage			
Pre-Policy and Post-Policy (2
Pre-Policy and Post-Policy [Top CPU Usage	60								
Top Memory Usage									
Top Interface Bandwidths	50 -								
Top Interface Drops Top Class Bandwidths	e								
Top Class Drops	Percent Usage								
Site Bandwidth	ut n	-							-
Interface Burstable Rate	2 30 -								
Site WAN Interface Utilizatie Site Alert	Pe								
Site Alert Detail	20 -								
Custom Reports									
	10						****		
Report Actions	0 1	Nov 14, 02:46 PM	Nov 14, 02:48 PM	Nov 14, 02:50 PM	Nov 14, 02:52 PM	Nov 14, 02:54 PM	Nov 14, 02:56 PM	Nov 14, 02:58 PM	
Save	Nar			Average	0		Peak		
Save As		PU Usage Iemory Usage				65% 36%			66% 36%
Delete		lemory usage				30%			30%
Schedule	I								
PDF	I								
Export to CSV	I								
Help	1								

Top 10 Interface Bandwidth (Input or Output)

The Top 10 interface bandwidth table lists the top 10 interfaces with the highest bandwidth. Use the drop-down to select between Input Bandwidth and Output Bandwidth. Default is Output Bandwidth. Click on any column header to re-sort the top interfaces alphanumerically by interface, device or description or numerically by either input or output bandwidth.

Top 10 Interfac	e Bandwidth	0	utput BW (Kbps)	0	
Interface	Device		Description	Input BW (Kbps)	Output BW (1
Vlan180	CS-C3850-23-	31	Performance-Test	37,273	41,803
GigabitEthernet	CS-C3850-23-	31	PEI		34,566
Vlan50	CS-C3850-23-	31	De Interface Ut	ilization Report	30,730
GigabitEthernet	CS-C3850-23-	31	DELL 234 VMNIC-1	227	24,393
GigabitEthernet	CS-C3850-23-	31	PERF SERV2	34,579	6,406
GigabitEthernet	CS-C3850-23-	31	to Dell Server4 TMA	19,007	4,861
GigabitEthernet	CS-C3850-23-	31	to DELL 233 VMNI	20,721	3,113
GigabitEthernet	CS-C3650-23-	36	To-CS-WAN	798	2,278
GigabitEthernet	CS-C3850-23-	31	2017-TO-ISR-4331	832	2,256
Vlan52	CS-C3850-23-	31	CORE-SITE Samp	19,481	2,244

Right-click on an entry in the table and select View Bandwidth Chart to generate an Interface Utilization Report.

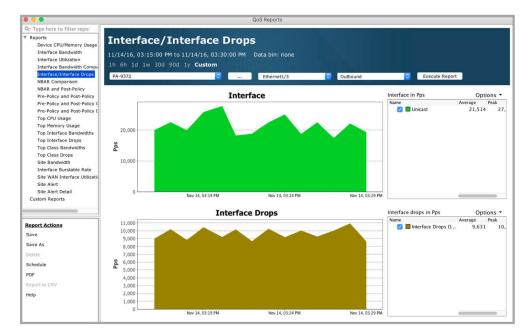


Top 10 Interface Drops (Input Drops or Output Drops)

The Top 10 interface drops table lists the top 10 interfaces with the highest number of drops. Use the drop-down to select between Input Drops and Output Drops. Default is Output Drops. Click on any column header to re-sort the top interfaces alphanumerically by interface, device or description or numerically by either input or output drops.

Top 10 Interface	Diops Output	Drops (pps) ᅌ		
Interface	Device	Description	Input Drops (pps)	Output Drop 🔻 1
Ethernet1/3	PA-9372		0	9,631
FastEthernet Inte	rface/Interface D	Props Report	1,129	1,278
GigabitEthernetu/1	LAZ9ZI-KUI		0	35
GigabitEthernet0/0/	1 DC-WAN-Route	0	<	
GigabitEthernet4	DC-MPLS		0	<
/Common/input	PA-F5LBM		72	(
lo	LiveSensor-PA		0	(
eth0	LiveSensor-PA		0	(
eth1	LiveSensor-PA		0	(
eth2	LiveSensor–PA		0	(

Right click on a table entry and select Interface/Interface Drops Report to generate a comparison interface/interface drops report using the selected device and interface.



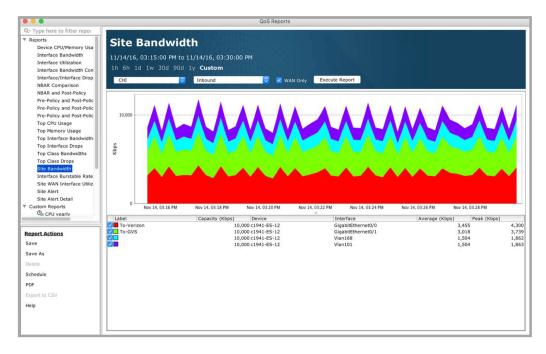
Site WAN Interface

The Site WAN Interface Utilization table lists all sites defined as WAN sites in the System Device View and site details including labels, capacity, input and output average and peak %. The Input Average and Input Peak % is computed by taking the percentage of input or output measured bandwidth relative to the user-defined capacity value in the system table. If the user-defined capacity field is blank, then the In and Out Capacity fields will be blank.

Site	▲ 1 Label	Capacity	Input Avg		Input Peak		Output Avg		Out	put Peak	CPU Avg		CPU Peak	M	lemory Avg	Memor	y Peak
BOS	To-AT&T	10,000		30 %		38%		34 %	6	38 %		99 %		99 %	25	%	25 %
CHI	To-Verizon	10,000		35 %		43 %		30 %	6	40 %		99 %		99 %	27	%	27 %
CHI	To-GVS	10,000		30 %		37%		34 9	6	43 %		99 %		99 %	27	%	27 %
CHI		10,000		15 %		19%		0 9	6	0 %		99 %		99 %	27	%	27%
CHI		10,000		15 %		19%		0 9	6	0 %		99 %		99 %	27	%	27 %
Chicago		100,000		0 %		0 %		0 9	6	0 %		4 %		5 %	11	%	11%
Chicago		100,000		0 %		0 %		0 9	6	0 %	1	4 %	i	5 %	11	%	11 %
Chicago		1,000,000		0 %		0 %		0 9	6	0 %	1	4 %	i	5 %	11	%	11 %
Chicago		1,000,000		0 %		0 %		0 9	6	0 %	1	4 %	i	5 %	11	%	11 %
DataCent	erCA	1,000		0 %		0 %		0 9		0 %				- / -	38		38 %
DataCent	erCA	1 000		0.%		0.%		0.9	<i>.</i>	0.94					2.0	92	22 0/

Right click on a field in the Site WAN Interface Utilization table and choose among three reports: Site Bandwidth, Interface Utilization, or Device CPU/Memory Usage. For each report, LiveNX automatically uses the selected device and interface; inbound is also selected as the default direction.

Site Bandwidth report



Interface Utilization report

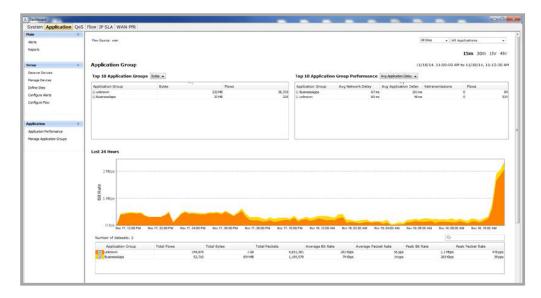
	QoS Reports		
Q- Type here to filter report Peports Device CPU/Memory Usa Interface Bandwidth Interface Bandwidth Con Interface Office 2000 NBAR Comparison NBAR Comparison NBAR Comparison NBAR and Post-Policy Pre-Policy and Post-Policy	Interface Utilization 11/14/16, 03:15:00 PM to 11/14/16, 03:30:00 PM Data bin: Polling Rate 1h 6h 1d 1w 30d 90d 1y Custom C1941:E5-12 C C C C C C C C C C C C C C C C C C C		
Pre-Policy and Post-Polic Pre-Policy and Post-Polic Top CPU Usage Top Nemory Usage Top Interface Bandwidth Top Interface Drops Top Class Bandwidth Top Class Bandwidth Site Alert Detail Top Class Bandwidth Site Alert Detail Top Class Bandwidth Top	Interface: GigabitEthernet0/0 - 1.0.0 Mbps	Interface Bandwidth in Kbps Fame Inbound Bandwidth Dubound Pask Ban. C Dubound Pask B	Options * 930 93h 3,455 4,156 3,455 4,156 3,035 3,649 3,035 3,649 4,156 4,156 3,035 3,649 4,156 4

Device CPU/Memory Usage report

•••				QoS Report	S				
Q+ Type here to filter repoi		12 12 12 12 12 12	1000 - 1000						
 Preports Prevoca cir/Ut/demary Usin Interface Bandwidth Interface Bandwidth Interface Bandwidth Interface Bandwidth Pre-Policy and Post-Polic Pro-Police Bandwidth Top Interface Bandwidth Top Interface Bandwidth Top Interface Bandwidth 	11/14/16 1h 6h c1941-ES	5, 03:15:00 PM to 1d 1w 30d 90d		00 PM Data bin:	none « Report and Memory	Usage			
Top Class Drops Site Bandwidth Interface Burstable Rate Site WAN Interface Utiliz Site Alert Detail ♥ Custom Reports @ CPU veariv Report Actions	60	Nov 14, 03:16 PM	Nov 14, 03:18 PM	Nov 14, 03:20 PM	Nov 14, 03:22 PM	Nov 14, 03.24 PM	Nov 14, 03 26 PM	Nov 14, 03:28 PM	
Save	Name			Average	0	terre transferre and	Peak		
Save AS Delete Schedule PDF Export to CSV Help	CPL	Usage mory Usage		Average		99% 27%	reak		99% 27%

Application Dashboard

The Application Dashboard presents a snapshot of the Applications transiting the network, it lists the Application groups Bit Rate, and a set of widgets that display the status of Top Application by, Bytes/ Flows, Performance, Voice/Video Performance, and HTTP Host. Within each Widget, the order can be displayed from Highest to Lowest, or vice-a-versa by clicking on the title bar within each widget.



In the top right, there is two drop-down selections that provide more granularity for the dashboard. The first is used to display the results per site or all sites. The Second is used to display the results per application, or all applications.

The Application Performance in the Action menu will open the Flow reports section which is covered later in this chapter.

The Manage Application Groups will open the Manage Application Dialog which allows the user to manage the Application groups by adding, deleting or editing the groups already defined.

QoS Dashboard

The QoS Dashboard presents a snapshot of the Quality of Service Policies active within the network, it lists the QoS Alert Rate, and a set of widgets that display the status of Top QoS Status by, Input Bandwidth, Output Bandwidth, Input Drops by Bitrate, Output Drops by Bitrate, and Application Bandwidth. Within each widget the order can be displayed from Highest to Lowest, or vice-a-versa by clicking on the title bar within each widget.

OoS Alerts - 24 Hour	-								
Que Alertes Et Hou								Alert Count	
40 35	. Audadu AA		Www.	h.				Class dropped rate Class-default dro Interface dropped	9,4
\$ tu 30 25								Class pre-policy d Class post-policy	
20 IS								Class dropped pac NBAR protocol dat	
₹ ¹⁵							•	NBAK protocol dat	
5									
0 08:00 PM	10:00 PM	12:00 AM 02:00 AM	04:00 AM 06:00 AM	08.00 AM	10:00 AM 12:00 PI	M 02:00 PM	04:00 PM 05:00 Pf		
\$								15m 30m	n 1hr 4
OoS Status									
Qos Status							08/19	/19, 05:45:00 PM to 08/19/19, 0	06:00:0
Top 10 Class Input Ban	width Pre-Policy	🗧 🗌 Exclude class-default			Top 10 Class Output Band	width Post-Policy ᅌ	Exclude class-default		
Class	Interface	Device	Input BW (Kbps)		Class	Interface	Device	Output BW (Kbps)	
SET_DSCP/SET_DSCP_VOICI SET_DSCP/class-default	GigabitEthernet2 GigabitEthernet3	RTR-DC-MPLS RTR Madison		793 471	SHAPING/class-default/QUE SHAPING/class-default/QUE		RTR_LosAngeles RTR_Birmingham		
MonitorUsingNbar GI3 In I	GigabitEthernet3	RTR_Louisville		305	SHAPING/class-default/QUE	GigabitEthernet2	RTR Louisville		
MonitorUsingNbar GI3 In/	GigabitEthernet3	RTR_London		287	SHAPING/class-default/QUE	GigabitEthernet2	RTR_SanJose		
SET_DSCP/class-default SET_DSCP/class-default	GigabitEthernet3 GigabitEthernet3	RTR_SanJose RTR_Seattle		217 217	SHAPING/class-default/QUE SHAPING/class-default/QUE	GigabitEthernet2	RTR_Austin RTR_London		
SET_DSCP/class-default SET_DSCP/SET_DSCP_VOIC	GigabitEthernet3	RTR_Seattle		110	SHAPING/class-default/QUE SHAPING/class-default/QUE	GigabitEthernet2 GigabitEthernet2	RTR_London RTR_Madison		
SET_DSCP/SET_DSCP_VOICI	GigabitEthernet3	RTR_Madison		83	SHAPING/class-default/QUE	GigabitEthernet2	RTR_Seattle		
SET_DSCP/SET_DSCP_VOICI	GigabitEthernet3	RTR_SanJose		83	SHAPING/class-default/QUE	GigabitEthernet2	RTR_Madison		
SET_DSCP/SET_DSCP_VIDEO	GigabitEthernet3	RTR_Seattle		81	SHAPING/class-default/QUE	GigabitEthernet2	RTR_London		
Top 10 Class Input Drop	s By Bitrate 🗌 Exc	lude class-default			Top 10 Class Output Drop	s By Bitrate 🗌 Exclud	e class-default		
Class SET DSCP/SET DSCP VOIC	Interface	Device RTR SanJose	Input BW (Kbps)		Class SHAPING/class-default/QUE	Interface	Device RTR Madison	Output BW (Kbps)	
Ingress_Policer_VoIP/VoIP-	GigabitEthernet2	RTR_Sanjose RTR_LosAngeles		<1	SHAPING/class-default/QUE SHAPING/class-default/QUE	GigabitEthernet2 GigabitEthernet2	RTR_Madison		
SET_DSCP/class-default	GigabitEthernet3	RTR_SanJose		0	SHAPING/class-default/QUE	GigabitEthernet2	RTR_London		
SET_DSCP/class-default	GigabitEthernet3	RTR_Seattle		0	SHAPING/class-default/QUE	GigabitEthernet2	RTR_Austin		
SET_DSCP/class-default SET_DSCP/class-default	GigabitEthernet3 GigabitEthernet2	RTR_Madison RTR-DC-MPLS		0	SHAPING/class-default/QUE SHAPING/class-default/QUE	GigabitEthernet2 CigabitEthernet2	RTR_Birmingham RTR_Seattle		
SET DSCP/SET DSCP VOIC		RTR Sanlose		ŏ	SHAPING/class-default/QUE	GigabitEthernet2	RTR Louisville		
SET_DSCP/SET_DSCP_VOICI		RTR_Seattle		0	SHAPING/class-default/QUE		RTR_LosAngeles		
SET_DSCP/SET_DSCP_VOICI SET_DSCP/SET_DSCP_VOICI	GigabitEthernet3	RTR_Madison RTR-DC-MPLS		0	SHAPING/class-default/QUE SHAPING/class-default/QUE		RTR_Louisville RTR_Birmingham		
SET_DSCP/SET_DSCP_VOIC	Gigabitethemetz	RTR-DC-MPLS		U	SHAPING/class-default/QUL	GigabitEthernet2	KTK_birmingham		
Top 10 Application Band	width								
Application(NBAR)	Interface	Device	Output BW (Kbps)	$= \pm 1$					
statistical-conf-audio	GigabitEthernet3	RTR-DC-MPLS		531					
unknown	GigabitEthernet3	RTR-DC-MPLS		262					
	GigabitEthernet3 GigabitEthernet2 GigabitEthernet2	RTR-DC-MPLS RTR-DC-MPLS RTR Madison		230					

Detterrit	A DESCRIPTION OF THE OWNER OWNER OF THE OWNER	Contraction of the	a sugar succession of	- 1. 3		-		- 0
tere Oct Per IPEL	a)							
tain .	0o5 Alerts	24 Hours						
***	Que Merte	21100015						
	** y						Alen	Churt
Anara la	401						The face or sport panets	6.56
	The sky	ditude makers	2.0.00.00	a said to be a		the second se	2 Case & suged and	LH
	2 March	MIMMAN MA	of Party is Mandalan	المعادر العاري العاريك	Wall (Mar) (Mar) (MANA AND I	Considerant in second pro-	8.10
Setup	· 8 =			Contraction of the second	and the second second		Can be side data - se	1
Order Steel	1 10	A SHARE SHARE	A STATE OF THE OWNER.	the last of south definition of	is a weath of the life	and a family of	Case prof grik y data rate	1
							Cos #updpates	1
Configure Alertic	灌林						Partial protocol tata rate	
	2.0							
Quinter	877 · · · · · · · · · · · · · · · · · ·	state the second second	and state and state as	a series and the set of	tion and international states	A REAL PRIME THE		
Out town auds	and the second sec	sails and on				the state		
Are closed with								
	QuS Status Top 18 Class I	npat Kandwidth 👳		as drive.	Top 10 Class O		NALES COLOR OF PARTIES	
	Case	Ditaria:	Owine	Separated (Hugs)	Case	presentation in the local division of the lo	Deves	Curput the (rises)
	Particul POLICIDES		10470572-047	(5.94)		instante with the		1.14
	des triat	0004741404	1041012-047	2.14	A STATE OF THE	Sph@renet.55		10
	hand_networkshap		ST 47K1	44	NAM ANY APPRICA	Partitive for the factor	C7 #741	
	then shrin A	Patternetul	00000478496	11	Cart.	Part Party (1)	000038476498	
	Telak, tetustational		004034478498		ine-whee	Partnerstyll.	LC COMPANY AND	
	des drin.t	Petteret()	00403419709	10	pentel	Generatio	2525-079-383	
	540.000	Pailtenet()	CTACRES	1	ches-infaut	naithenet/3	004039438498	
	Partition -	Failtfarte(U)	CC-IGH HTR.III,	4		Soldferend St.	aw bit takch ist	1
	YEAR Jern Larisian	Failtherats/3	004008478499	6		Spectrework.	eracand-sc	
	des arts a	faitheret/s	02-020-419-939	4	the offset	Pertheries()	CT-#791	
	Top 10 Class 1	input Crops By Bits	ata Estada das des		Top 10 Class O	utput Drops By	Bilirate Cladulation	~
	One	Distan	Device	Drivel Ref (March)	Cest	Distantiacia	Device	Over the (stan)
	Serving	Faitherst()	00-000-010-000	and the second se	Service	Faitheret/I	10.003-0479-029	Contract Contract
	internet of	Continents	1525-09-163		parent of	Sectorial.0	3025-dRe W1	
	permitting data to		00-094149-474	6	parameterization default de	faddened.d	024044444	
	perenticises defaultion		00-094146-474		parent/desi-defaulty.		004994-04479	
	peretities defailed		ACCIDIMUM ATM		peretting delasts.		00.694149478	
	perent/two default)		00-009 LAN-819	¢	peret/des-default).		00.6341.45478	
		Factorierot.8	05-6299-Lah-879	e .	permittion default.	NextRenet(8	CC 4296 LAN #78	
	perint tax default)				the strappy manifest	Generation,0	42925-085	
	data spig-mentor	Operative rest/d	40823-385				00404416-0	
	tions upon mentor time circle.4	PaddanettA	004894.459.05		siles of aut	Pailtereich		
	data spig-mentor					failteret/8 failteret/8	00.0004439.494	
	dan kupa namba Anarak Kut Anarak Kut	Performent/A	004894.459.05	1.0.0	siles of aut			
	den opprætte Jese defaut Tep 18 Applie	Failtereitit Failtereitit	00-004-474-494 00-000-4-474-494	Charles and	siles of aut			
	Top 10 Application (VLM)	Faitheratist Faitheratist etion Randwidth	CC-4294-4294-76, CC-CCL-4-874-4994 Device	Codevel Bind (Classi)	siles of aut			
	te + grap nentra fine officit fine think Top 10 Applicit Application (NSM) encourt D D	Patternel() Patternel() Patternel() Patternel() Patternel() Patternel()	OC-OP-LATER PL OC-COLLATER PL Obvios an UNIDPOINT	4,600	siles of aut			
	In a gap canno time dirk at time dirk at Top 18 Apple: Application (NSA), where 0 0 where 0 0	Patteret) Patteret) Patteret) Patteret) Patteret Patteret Spatteret Pattere	CC-QM-475-A, CC-CC-4475-Pp. Device er IRI (PC)-10 er IRI (PC)-10	4,600 4,602	siles of aut			
	te a que canto des defait faise defait faise defait Aquitador (1934), efector (1934), efector (1934), efector (1934), efector (1934),	Pattervitit faithervitit stor Randwidth besithervitit besithervitit besithervitit besithervitit	Orient Orient ar 10 (PC-10) ar 10 (PC-10) ar 10 (PC-10) ar 10 (PC-10)	4,1400 4,1472 1,1121	siles of aut			
	Application (NSA) Application (NSA) Application (NSA) artered D 0 artered D 0 brog D 4 broken D 0	Patteret) Patteret) Patteret) Patteret) Patteret Patteret Spatteret Pattere	CC-QM-475-A, CC-CC-4475-Pp. Device er IRI (PC)-10 er IRI (PC)-10	4,600 4,602	siles of aut			
	te a que canto des defait faise defait faise defait Aquitador (1934), efector (1934), efector (1934), efector (1934), efector (1934),	Patteretiit faitteretiit batteretiit bakteretiit bakteretiit dakteretiit dakteretiit	Octoperation A, OCCOLLARY APA Device or UR (DAC)-10 or UR (DAC)-10 or UR (DAC)-10 or UR (DAC)-10 or UR (DAC)-10 or UR (DAC)-10	4,500 4,502 1,525 1,591	siles of aut			

The QoS System Audit in the Action menu will open the Policy and Performance Audit Report which is covered later in this chapter. Right-clicking on any of the widgets will give the user the option to view the Pre- and Post-Policy graphs for the policy selected.

QoS Alerts – 24 Hours

The QoS Alerts – 24 Hours charts the total number of generated QoS related alerts within the last 24 hours. The chart uses a rolling window format. The most recent count of QoS alerts is generated at the right edge of the chart and older data is moved to the left until any data beyond 24 hours is deleted from the chart.



The legend to the right of the QoS Alerts chart is a tabular summary of the total generated QoS alerts for the chart duration. Use the check box alongside each alert type to enable or disable viewing the QoS alert category from the chart.

The tables below the QoS Alerts graph provide real-time average data for the dashboard time duration selected. Four-time durations are available: last 15 minutes, last 30 minutes, last 1 hour and last 4 hours. The default is last 15 minutes.

Top 10 Class Input Bandwidth Pre- or Post-Policy

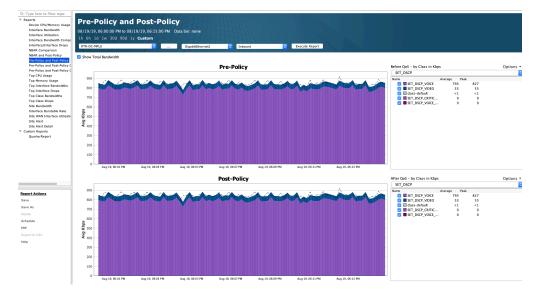
Right-click on an entry in the table and then select View Graph to bring up a Pre-Policy and Post-Policy comparison graph for the selected device, interface and Inbound direction.

Top 10 Class Output Bandwidth Pre- or Post-Policy

The Top 10 Class Output Bandwidth table summarizes the top 10 interfaces with the highest input bandwidth, class, interface and device name. Click on the Pre-Policy or Post-Policy to choose between the two options. Click on the Exclude class-default check box to remove any class-default from the top 10 list. The default is off.

Top 10 Class Input Bandwidth Pre-	Policy ᅌ 🗌 Exc	lude class-default
Class Interface	Device	Input BW (Kbps)
VLAN1_SET_DSCP Vlan1	c2921-ES-13	6,378
CameraShape Pre-Policy and Post-Poli	cy Report 2	3,459
MonitorUsinginua Gigauitettiettiettietti/ 1	C1941-C3-12	2,209
MonitorUsingNba GigabitEthernet0/1	c1941-ES-12	544
VLAN1_SET_DSCP Vlan1	c2921-ES-13	237
MonitorUsingNba GigabitEthernet0/1	c1941-ES-12	173
VLAN1_SET_DSCP Vlan1	c2921-ES-13	81
MonitorUsingNba GigabitEthernet0/1	c1941-ES-12	77
MonitorUsingNba GigabitEthernet0/1	c1941-ES-12	18
MonitorUsingNba GigabitEthernet0/1	c1941-ES-12	3

Right-click on an entry in the table and then select Pre-Policy and Post-Policy Report to bring up a Pre-Policy and Post-Policy report for the selected device, interface and Inbound direction.



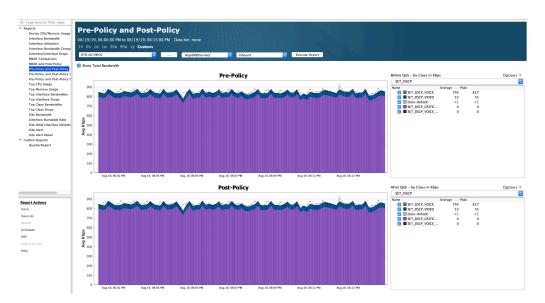


Top 10 Class Output Bandwidth Pre- or Post-Policy

The Top 10 Class Output Bandwidth table summarizes the top 10 interfaces with the highest input bandwidth, class, interface and device name. Click on the Pre-Policy or Post-Policy to choose between the two options. Click on the Exclude class-default check box to remove any class-default from the top 10 list. The default is off.

Class	Interface		Device		Output BW (Kbps)
WAN-Shaping/clas	GigabitEthernet0/	1	c2921-ES-13		5,49
MonitorUsingNbar	GigabitEthernet0/	0	c1941-ES-12		2,20
CZ_SHAPING&QUE	FastEthernet()/1/	1	c7971_FS_13		2,18
TRAFFIC_SHAPING	Gig Pre-Policy	and	d Post-Policy I	Report	2,16
TRAFFIC_SHAPING	GigabitEthernet0/	2	c2921-ES-13		69
CZ_SHAPING&QUE	FastEthernet0/1/	1	c2921-ES-13		69
MonitorUsingNbar	GigabitEthernet0/	0	c1941-ES-12		54
WAN-Shaping/clas	GigabitEthernet0/	1	c2921-ES-13		23
WAN-Shaping/clas	GigabitEthernet0/	1	c2921-ES-13		22
WAN-Shaping/clas	GigabitEthernet0/	1	c2921-ES-13		20

Right-click on an entry in the table and then select Pre-Policy and Post-Policy Report to bring up a Pre-Policy and Post-Policy report for the selected device, interface and Outbound direction.



Top 10 Class Input Drops by Bitrate

The Top 10 Class Input Drops by Bitrate table summarizes the top 10 interfaces with the highest input drop rates in Kbps, its class, interface and device name. Click on the Exclude class-default check box to remove any class-default from the top 10 list. The default is off.

Top 10 Class Input Drops By Bitrate 🗌 Exclude class-default

Class Interface	Device	Input BW (Kbps)	± 1
SET_DSCP/SET_DS GigabitEthernet3	RTR_SanJose		83
Ingress_Policer_V GigabitEthernet2	RTR_LosAngeles		<1
SET_DSCP/class-d GigabitEthernet3	RTR_SanJose		0
SET_DSCP/class-d GigabitEthernet3	RTR_Birmingham		0
SET_DSCP/class-d GigabitEthernet3	RTR_Seattle		0
SET_DSCP/class-d GigabitEthernet3	RTR_Madison		0
SET_DSCP/class-d GigabitEthernet2	RTR-DC-MPLS		0
SET_DSCP/SET_DS GigabitEthernet3	RTR_SanJose		0
SET_DSCP/SET_DS GigabitEthernet3	RTR_Birmingham		0
SET_DSCP/SET_DS GigabitEthernet3	RTR_Seattle		0

Top 10 Class Output Drops by Bitrate

The Top 10 Class Output Drops by Bitrate table summarizes the top 10 interfaces with the highest output drop rates in Kbps, its class, interface and device name. Click on the Exclude class-default check box to remove any class-default from the top 10 list. The default is off.

Top 10 Class Output Drops By Bitrate Exclude class-default

Class	Interface	Device	Output BW (Kb	$-\pm 1$
SHAPING/class-de	GigabitEthernet2	RTR_Madison		362
SHAPING/class-de	GigabitEthernet2	RTR_Seattle		98
SHAPING/class-de	GigabitEthernet2	RTR_Birmingham		92
SHAPING/class-de	GigabitEthernet2	RTR_London		88
SHAPING/class-de	GigabitEthernet2	RTR_Austin		88
SHAPING/class-de	GigabitEthernet2	RTR_Seattle		70
SHAPING/class-de	GigabitEthernet2	RTR_Louisville		66
SHAPING/class-de	GigabitEthernet2	RTR_Seattle		32
SHAPING/class-de	GigabitEthernet2	RTR_Louisville		27
SHAPING/class-de	GigabitEthernet2	RTR LosAngeles		26

Flow Dashboard

The Flow Dashboard presents a snapshot of the individual flows transiting the network, it lists the Flow Alert Rate, and a set of widgets that display the status of Top Flow Status by Source Address, Destina-

tion Address, Source Countries, Destination Countries, DSCP, Interface (outbound), Applications, Application Performance, Voice/Video Performance, and HTTP Host. Within each widget, the order can be displayed from Highest to Lowest, or vice-a-versa by clicking on the title bar within each widget.

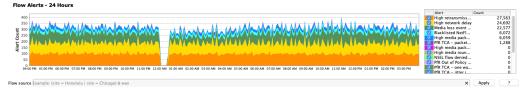
$\frac{1}{1000} \frac{1}{1000} \frac{1}{1000} \frac{1}{1000} \frac{1}{1000} \frac{1}{10000} \frac{1}{100000} \frac{1}{1000000} \frac{1}{1000000} \frac{1}{10000000000000000000000000000000000$													24 Hours	Flow Alerts - 2	\$
sort e e e e e e e e e e		Alext Count													ts
a a b	27,56 24,68 22,57	High retransmiss	M. M. M.		MIM						laval.		be Ma	350	orts
word Docks in Sits inge Alcha inge Alch	6,07	Blacklisted NetFl		MANA ANA	A A A A A A A	AMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		HAMAN MAN	Anna		mn	Anna anna		250	2
<i>μ</i> devices sols sols	6,05		And Administration	1. Ale March	LALAN		AL. 14			N	In Make	All have been	AMAN	2 200	wer Devices
Since per Adris per Ad					12.1.1.1	10.00 400.00								B 150	
Normer			i hat hill na hat d												
pin for the form of the														0	
Image: Control of the second		PfR TCA - one wa	02:00 PM	12:00 PM	10:00 AM	00:00 AM	06:00 AM	04:00 AM	02.00 AM	12:00 AM	10:00 PM	OB:00 PM	06:00 PM	04:00 PM	
Image: constraint of the second se	v -	× Apply									1.8	du Laita - Chinan		Character Francisco	
Image: Second) or warn	and I site = criticage	. (site = Honolo	Flow source example.	
Instrument For Descret defenses Descret defenses <thdescret defenses<="" th=""> Descret defenses <thdesc< td=""><td>Um Ihr</td><td>15m 30</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>ion A</td></thdesc<></thdescret>	Um Ihr	15m 30													ion A
Application Column Top 10 Source Addresses Top 10 Source Addresses Top 10 Destination Addresses Top 10 Top 10 Top 10 Source Addresses Top 10 Source Addresses <th< td=""><td>9,03:50:00</td><td>08/23/19, 03:35:00 PM to 08/23/19</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Basic Flow</td><td></td></th<>	9,03:50:00	08/23/19, 03:35:00 PM to 08/23/19												Basic Flow	
P = 10 db Para				Thurs. 10								flaura 🖸			
Image: Section of the section of t				is Flows	n Addresses	Top 10 Destination						riows 💟	Addresses	Top 10 Source A	
Image: constraint of the second se	75,26			Bytes					ows.			Bytes			
Image: Construction 6 in image: 100 million 100 million 400 million Image: Construction 6 in image: 100 million 100 million 100 million Image: Construction 6 in image: 100 million 100 million 100 million Image: Construction	75,22	74 MB	874		31		13,326			65 MB				RTR_Seattle	
If the D-C CORE 6 j / l / l / l / l / l / l / l / l / l /	1														
Image: construction of the second	1				ney -36	IWAN-Br1_Sydne									
St. Control Trans	48,340	1 G8	, j		50	▼ -	17,676			3 MB					
RTI-DC-ONG 573 kB 3.562 RTI-DC-ONG 173 kB RTI-DC-ONG 573 kB 3.562 RTI-DC-ONG 173 kB Top 10 Source Countries Internet 173 kB 173 kB Second 100 second 173 kB 173 kB Top 10 Source Countries Internet Internet Internet Second 10 second 10 second 10 second Second 10 second 20 second 10 second Second 10 second 10 second 20 second Second 10 second 10 second 20 second Second 10 second 10 second 20 second Second 10 second 10 second 10 second <td>12,344</td> <td></td> <td>RTR_Seattle</td> <td></td>	12,344													RTR_Seattle	
Number Coole Set Number Set Number Coole	12,00	/3 MB	373		Y		3,362			573 KB					
Top 10 Source Countries Top 10 Destination Countries Pres > Control Pres > 1 form Pres > 1 form > Universe 3 G 1 20041 Pres > 1 form > Universe 3 G 1 20041 > 1 0 (UNITED STATE 3 G > UNIVERSE 3 G 1 20041 > 1 0 (UNITED STATE 3 G > UNIVERSE 3 G 1 20041 > 1 0 (UNITED STATE 3 G > UNIVERSE 3 G 1 20041 > 1 0 (UNITED STATE 3 G > UNIVERSE 3 G 1 20041 > 1 0 (UNITED STATE 3 G > UNIVERSE 7 MB 4 7 + 0 (UNITED STATE 3 G > UNIVERSE 3 0 H 1 0 H 1 0 H 1 0 H > UNIVERSE 3 0 H 1 0 H 1 0 H 1 0 H > UNIVERSE 3 0 H 1 0 H 1 0 H 1 0 H > UNIVERSE 3 0 H 1 0 H 1 0 H 1 0 H > UNIVERSE 3 0 H 1 0 H 1 0 H 1 0 H > UNIVERSE	11,98	73 MB	373				3,355			569 KB			RE	RTR-DC-COF	
				s Bytes 😋	n Countries	Top 10 Destination						ytes 😳	Countries By	Top 10 Source C	
- Unknown 15 Cd 223,212 - Unknown 29 Cd - Unknown 15 Cd 223,212 - Unknown 29 Cd - Unknown 15 Cd 223,212 - Unknown 29 Cd - Unknown 15 Cd 223,212 - Unknown 29 Cd - Unknown 15 Cd 223,212 - Unknown 50 Cd - Unknown 15 Cd 223,212 - Unknown 50 Cd - Unknown 15 Cd 223,212 - Unknown 50 Cd - Unknown 15 Cd 223,212 - Unknown 50 Cd - Unknown 15 Cd 230 Cd 15 Cd 230 Cd - Unknown 50 Cd 16 Cd 24 Cd 24 Cd 24 Cd - I Cd (CANADA 51 B4 460 + - I Cd (CANADA 24 Fd 24 Fd - I Cd (CANADA 51 B4 460 + - I Cd (CANADA 24 Fd 24 Fd - I Cd (CANADA 51 B4 460 + - I Cd (CANADA 24 Fd 24 Fd - Unknown 51 B4		v1 flows		Bytes		Det Country			flows	v1		Bytes		Src Country	
Image: Construction State Construction 93 Mail 47,156 Image: Construction State Construction 55 Mail Image: Construction State Construction 39 Mail 61,31 Image: Construction State Construction 94 Mail Image: Construction State Construction 39 Mail 61,31 Image: Construction State Construction 94 Mail Image: Construction State Construction 24 Mail 44 Mail 44 Mail 44 Mail Image: Construction State Construction 24 Mail 11,31 44 Mail 11,31 Mail Image: Construction State Construction 34 Mail 11,31 11,31 Mail 11,31 Mail Image: Construction State Construction 34 Mail 11,31 Mail 11,31 Mail 11,31 Mail Image: Construction State Construction 34 Mail 11,31 Mail 11,31 Mail 11,31 Mail Image: Construction State Construction 34 Mail 34 Mail 11,31 Mail 11,31 Mail Image: Construction State Construction 34 Mail 11,31 Mail 11,31 Mail 11,31 Mail Image: Construction State Construction 34 Mail 34,32 Mail 11,31 Mail 11,31 Mail	335,1	29 GB				► Unknown	228,212			15 G8		10100		▷ Unknown	
• III CUMUTE DIRACDOM 39 Mai 6130 110 FIGURATOR 91 Mai • III CUMUTE DIRACDOM 24 4 941 • 110 FIGURATOR 91 Mai • III CUMUTE DIRACDOM 24 4 941 • 110 FIGURATOR 91 Mai • III CUMUTE DIRACDOM 24 Mai 941 • 110 FIGURATOR 91 Mai • III CUMUTE DIRACDOM 21 Mai 441 91 Mai 91 Mai • III CUMUTE DIRACDOM 21 Mai 110 FIGURATOR 204 Mai • III CUMURANE 24 Mai 113 Mai 110 FIGURATOR • III CUMURANE 201 Mai 21 • 100 FIGURATOR 117 Mai • III DIRACDOM 201 Mai 21 • 100 FIGURATOR 110 FIGURATOR • III DIRACDOM 110 FIGURATOR 110 FIGURATOR 117 Mai • IIII DIRACDOM 110 FIGURATOR 117 Mai 110 FIGURATOR • IIII DIRACDOM 110 FIGURATOR 117 Mai 117 Mai • IIII DIRACDOM 110 FIGURATOR 110 FIGURATOR 117 Mai • IIII DIRACDOM 110 FIGURATOR 010 FIGURATOR 010 FIGURA	219,1 46,4				ATES	US/UNITED STATE							STATES	US/UNITED 5	
+ iii di All'AlSTAULA 7 bis 9 7 iii di All'ALSTAULA 5 15 80 + iii di All'ALSTAULA 7 bis 9 7 iii di All'ALSTAULA 5 15 80 + iii di All'ALSTAULA 2 12 4 40 1 12 6 1 12 6 + iii di All'ALSTAULA 2 12 4 40 1 12 6 1 12 6 + iii di All'ALSTAULA 2 12 4 40 1 12 7 1 12 6 + iii di All'ALSTAULA 2 12 4 1 12 7 1 12 6 1 12 7 + iii di All'ALSTAULA 2 12 4 1 12 7 1 12 7 1 12 7 + iii di All'ALSTAULA 2 12 8 1 12 7 1 12 7 1 12 7 + iii di All'ALSTAULA 2 12 8 2 1 8 2 1 1 12 7 1 12 7 + iii di All'ALSTAULA 2 12 8 2 1 10 15 7 1 12 7 1 12 7 1 12 7 + iii di All'ALSTAULA 2 12 8 2 12 10 11 11 12 7 1 12 7 1 12 7 1 12 7 + iii di All'ALSTAULA 2 12 8 2 12 10 11 11 12 7 2 12 10 11 11 12 7 1 12 7 1 12 7 + 0 00 10 10 10 10 10 10 10 10 10	40,4														
• id (CVANDA 221 88 469 • 201 48 204 48 • id (CVANDA 221 88 469 • 101 (VINTRIBLADDS) 204 48 • id (CVANDA 54 88 1.13 • 001 (VINTRIBLADDS) 204 48 • id (CVANDA 54 88 1.13 • 001 (VINTRIBLADDS) 1.13 • id (CVANDA 201 48 1.13 • 001 (VINTRIBLADDS) 1.14 • id (CVANDA 201 48 1.13 • 001 (VINTRIBLADDS) 1.14 • id (CVANDA 201 48 1.14 • 001 (VINTRIBLADDS) 1.14 • id (DVANDA 201 48 1.14 • 001 (VINTRIBLADDS) 1.14 • id (DVANDA 201 48 1.14 1.14 1.14 • id (DVANDA 201 48 1.14 1.14 1.14 • id (DVANDA 201 48 1.14 1.14 1.14 1.14 • id (DVANDA 201 48 1.14 1.14 1.14 1.14 1.14 • id (DVANDA 201 48 1.14 1.14 1.14 1.14 1.14 1.14 <td>1,1</td> <td>535 KB</td> <td>5</td> <td></td> <td>NGDOM</td> <td>► 38 GB/UNITED KINC</td> <td>87</td> <td></td> <td></td> <td>7 ME</td> <td></td> <td></td> <td></td> <td>B AU/AUSTRAL</td> <td></td>	1,1	535 KB	5		NGDOM	► 38 GB/UNITED KINC	87			7 ME				B AU/AUSTRAL	
• B (V)(C)(IN)A 404 K8 1,185 • B (A)(A)(XTMUA)A 127 K8 • B (V)(C)(IN)A • B (V)(C)(IN)A 131 G8 131 G8 • B (V)(C)(IN)A • D (V)(C)(IN)A 131 G8 134 G8 • B (V)(C)(IN)A • D (V)(C)(IN)A 131 G8 134 G8 • B (V)(C)(IN)A • D (V)(C)(IN)A 134 G8 134 G8 • D (D) (D)COP (Initial) • D (V)(D) 104 G8 104 G8 • D (D) (D)COP (Initial) • D (V) (Initial) 104 G8 104 G8 • D (D) (D)COP (Initial) • D (V) (Initial) 0 (Initial) 0 (Initial) 0 (Initial) • D (D) (D)COP (Initial) • D (V) (Initial) 0 (Initial) 0 (Initial) 0 (Initial) 0 (Initial) 0 (Initial) • D (D) (D)COP (Initial) • D (Initial) 0 (Initia) 0 (Initia) 0 (In															
Image: Second	3	204 KB	2							521 KE			`		
bit of CCECK HERVILIC 201 K8 20 = SS/SINGADORE 147 K8 Top 10 DSCP Price Distribution (Top 10 DSCP Price Pr					•	UA/UKRAINE	932						E	► UA/UKRAINE	
DGCP Pytes - 1 Ress. Dot // Device - 1 Ress. - 1 Ress. 1 - 100 - 1 (GL 340,327 - 1 (GL 540,327 - 1 (GL 540,327 - + 0 (69/21) - 1 (GL 340,327 - 1 (GL 540,327 - 6 (GL 540,327 + 4 (69) - 43,946 17,728 Cgabitthermatl/0/11 GL 540,327	3	147 KB	1			SG/SINGAPORE	52			201 KE			REPUBLIC	CZ/CZECH R	
⇒ 0.00 21.03 369.326 19 FortiGate Freewall 9 GB ⇒ 18.04721) 1.08 49.070 1.5.2522-311 8.6B > 46.097 45.358 17.728 GrapabitThermet1/0/11 C5.4580-22-311 4.6B				i) Bytes ᅌ	(Outbound)	Top 10 Interfaces (Bytes ᅌ	Top 10 DSCP	
> 18 (M/21) 1 GB 49 (57) -1 C5-C3850-23-31 8 GB > 8 d6 (F) 483 MB 17,728 Gapabitthment10/11 C5-C3850-23-31 4 GB			Bytes						Flows			Bytes			
▶ 46 (EF) 483 MB 17,728 GigabitEthernet1/0/11 CS=C3850-23-31 4 GB	15,7														
	81,4														
	3.0	3 GB		S-C3850-23-31		GigabitEthernet1/0/1	11.173			156 ME				№ 46 (EF) № 48 (CS6)	

The Application Performance in the Action menu will open the Application Report which is covered later in this chapter.

Right-clicking on any of the widgets will give you the option to view the specific report for the item selected.

Flow Alerts – 24 Hours

The Flow Alerts – 24 Hours charts the total number of generated Flow related alerts within the last 24 hours. The chart uses a rolling window format. The most recent count of Flow alerts is generated at the right edge of the chart and older data is moved to the left until any data beyond 24 hours is deleted from the chart.



The tables below the Flow Alerts – 24 Hours graph provide real-time average data for the dashboard time duration selected. Four-time durations are available: last 15 minutes, last 30 minutes, last 1 hour and last 4 hours. The default is last 15 minutes. The first six tables (Source Addresses, Destination Addresses, Source Countries, Destination Countries, DSCP and Outbound Interfaces) use basic flow. The other three tables (Applications, Video Performance, and Application Performance) use flex flow. Both tables use flow sources as defined in the Dashboard Sources.

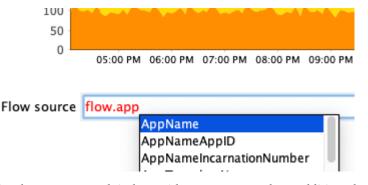
Flow Source



The LiveNX Flow source is an alphanumeric field to filter the flow dashboard based on the system and flow entities. Searchable system entities include device, interface, site, tag and WAN parameters. Searchable flow entities include IP address, DSCP, port, protocol and application.

- Click on the Flow source field to begin typing in the desired search parameters.
- The general syntax of the search field is shown in the example below. (site = Honolulu | site = Chicago) & wan
- Click on Apply to apply the search. Click on the 'X' to clear the search field.
- Boolean expressions OR = 'l' and AND = '&'; grouping uses '()')

The Search editor provides tooltips to assist in creating the search expressions. Click on the desired entity to add it to the expression.



The Flow source search is done with a one pass search. In addition, the system level entities need to be in a single clause. For example, (site = Honolulu | site = Chicago) & flow.ip=1.1.1.1 is allowed, but (site = Honolulu & flow.ip=1.1.1.1) | (site = Chicago & flow.ip=1.1.1.1) is not allowed.

LiveNX supports a large number of system and flow searchable entities. Click on the ? to display the list of searchable entries as well as some example search expressions.

' Example	
site=Honolulu & wan	Flows from specific site with WAN-tagged interfaces
flow.dscp=EF	Flows with DSCP EF markings
flow.ip.src=1.1.1.1	Flows with specific source IP
flow.ip.dst=1.1.1.1 & flow.ip.src=2.2.2.2	Flows with specific source and destination IP
flow.ip.site=Honolulu	Flows from specific source or destination site
flow.ip.site.src=Sacramento	Flows from specific source site
flow.ip.site.dst="New York"	Flows from specific destination site
flow.ip=1.1.1.0/24	Flows with source or destination ip that match /24
flow.ip=192.168.0.55/0.0.255.0	Use of wild cards to match flows with ip address where 3rd octect is an
flow.srclp=172.16.1.0 & flow.srcMask=24	Flows with source ip that match /24
flow.device=Cisco1811 & flow.interface=FastEthernet0	Flows from specific device and interface
flow.device=Cisco1811 & flow.interface.in=FastEthernet0	Flows from specific device and in bound on interface
flow.app=ms-lync	Flows identified as ms-lync
flow.protocol=TCP	Flows that are TCP traffic
(site=A site=B) & tag=Primary	Flows from site A or B over interfaces tagged as Primary

Top 10 Source Addresses [Bytes or Flows]

The Top 10 Source Addresses table lists the top 10 devices generating the largest number of bytes or flows from a source address. Click on the + sign to the left of the IP address to show the devices associated with the source IP address.

Fop 10 Source Ad	ldresses Bytes ᅌ		
Src IP Addr	Bytes	▼1 Flov	vs
▼ 192.168.15.200		729 MB	15,643
c2921-ES-1	Source Address Repo	ort	7,829
c1941-ES-1	Source Address Rept		7,814
10.254.20.88	Add 192.168.15.200	558	
192.168.12.2			12,300
10.0.0.2	Add 192.168.15.200		314
10.0.12.2	Copy 192.168.15.20	0 to clipboard	301
10.254.100.2		59 MB	748
192.168.10.2		2 MB	192
10.254.254.214		429 KB	28
1 - 1 1 1 1 1 1 7 7 7		410 KB	17

Right-click on Top 10 Source Addresses to generate a Source Address inbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the table.



Right-click on an IP address in the Source Address table to select from Graph View, Add to IP Blacklist, Add to IP mapping or Copy to clipboard.

Top 10 Source Ad	Idresses Bytes ᅌ	
Src IP Addr	Bytes 🔍 1 Flows	
▼ 192.168.15.200	729 MB	15,643
c2921-ES-1 c1941-ES-1	Source Address Report	7,829 7,814
10.254.20.88192.168.12.2	Add 192.168.15.200 to IP Blacklist Add 192.168.15.200 to IP Mapping	558 12,300
10.0.0.2 10.0.12.2	Copy 192.168.15.200 to clipboard	314 301
10.254.100.2	59 MB	748
▶ 192.168.10.2	2 MB	192
10.254.254.214	429 KB	28

Graph View – generates a Source Address inbound flow report for the selected source IP address for all devices.

	Flow Reports
Q. Type here to filter repoi	Source Address
▼ Reports	
Interface Bandwidth	
Top Analysis	Source Address 15m 1h 6h 1d 1w 30d Custom
IPs and Ports	
IPs and Application	11/14/16, 03:35:00 PM to 11/14/16, 03:50:00 PM Data bin: 1 minute Execute Report
All Unique Flows	
	Source All Devices 🖓 All Interfaces 🖓 Number of flows: 15,710 🗌 Utilize Long Term Cache
Top Conversations	Filter *DefaultFilterGroup 🕞 👼 Inbound 😒 Graph Basic Flow 😒 Time Series 🕴 Bytes 😒
Bidirectional Source/I	Filler Deladarite of top and another of the series of offers of the series of offers
Source or Destination Address Pair	Search wan & flow.ip.src=192.168.15.200 × * ?
Destination Address	
Source Address	
Destination Address F	S0 MB
Source Address Popu	
Site Traffic	40 MB
Destination Site Traff	dei ori
Source Site Traffic	
▶ Applications	¥3 30 MB
▶ QoS	230 MB
Network	20 MB-
▶ Medianet	
Applications (AVC)	
▶ Firewall	10 MB -
▶ PfR	
 Wireless AnyConnect 	0 B Nov 14, 03:37 PM Nov 14, 03:39 PM Nov 14, 03:41 PM Nov 14, 03:43 PM Nov 14, 03:43 PM Nov 14, 03:45 PM Nov 14, 03:47 PM Nov 14, 03:49 PM
P Anyconnect	וועט בא, ט בא דייש אוויין אין אין אין אין אין אין אין אין אין
Report Actions	Show Total Bytes
Save	Number of datasets: 1 Q-
Sile of	
Save As	Src IP Addr Total Plows Total Packets Average Bracket R Peak BIt Rate Peak Packet Rate [Src Country]
Create	▼ 192.168.15.200 15,710 721 MB 3,402,394 6.41 Mbps 3780.44 pps 6.63 Mbps 3831 pps -
Edit	
Delete	
Schedule	
PDF	
Export to CSV	
Control Contro	
Help	

Add to IP Blacklist – adds the IP address to the LiveNX blacklist. The blacklist feature is covered in Chapter 12, *Tools*.

Add to IP Mapping – allows you to create an alphanumeric name to the selected IP address. The IP mapping feature is covered in Chapter 12, *Tools*.

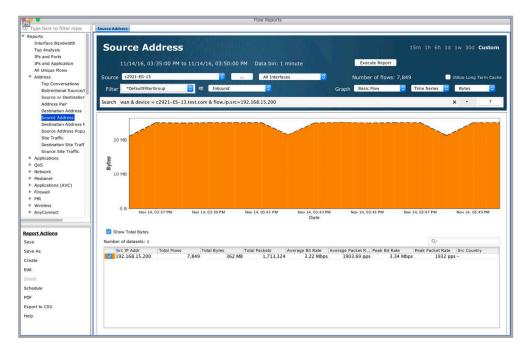
Copy to Clipboard – copies the selected IP address to the clipboard.

Src IP Addr		Bytes	₩1	Flows	
▼ 192.168.15.200		_ /	729 MB		15,643
<pre>c2921-ES-1 c1941-ES-1 > 10.254.20.88 > 192.168.12.2 > 10.0.0.2 > 10.0.12.2</pre>	Add 19 Add 19	92.168.15.2	eport 200 to IP Blackli 200 to IP Mappi .200 to clipboa	ng	7,829 7,814 558 12,300 314 301
 10.0.12.2 10.254.100.2 192.168.10.2 	.,		59 MB 2 MB		748 192
▶ 10.254.254.214 ▶ 151 101 40 72			429 KB		28

Expand an IP address to show devices and right click on a device to select between Graph View and Top Analysis View.

Top 10 Source Ad	dresses Bytes 🗘		
Src IP Addr	Bytes	▼ ¹ Flows	
▼ 192.168.15.200		721 MB	15,710
c2921- <u>FS-13</u>		362 MB	7,849
c1941- Sou	rce Address Report	359 MB	7,861
▶ 10.254.20 Tor	Analysis View	666 MB	549
▶ 192.168.1 <u>∠.∠</u>	, marysis tren	648 MB	12,263
▶ 10.0.12.2		168 MB	301
▶ 10.0.0.2		167 MB	310
▶ 10.254.100.2		58 MB	736
▶ 192.168.10.2		2 MB	197
▶ 10.254.254.214		490 KB	29
1 - 1 - 1 - 1 - 1		410 KD	10

Graph View – generates a Source Address inbound flow report for the selected source IP address for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.



Top Analysis View – generates a Top Analysis inbound flow report for the selected device.

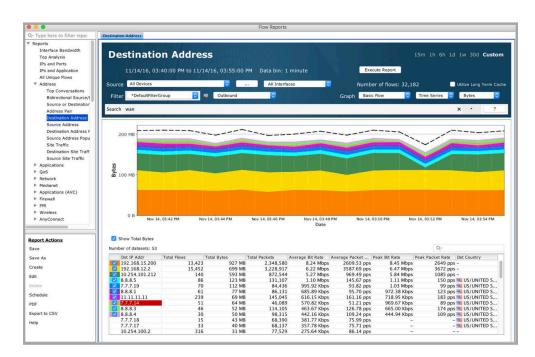
					Flow Rep	ports						
Type here to filter repoi	Top Analysis											
Reports												
Interface Bandwidth	Ton	Analys									1d 1w 30d	C
Top Analysis	TOP	Analys	15							iem tu ou	10 IW 200	Custo
IPs and Ports												
IPs and Application	1	/14/16 03:3	5:00 PM to 11/14	/16.03:5	0.00 PM				xecute Report			
All Unique Flows		1,14,10,05.5	5.00 111 10 11/14	,10, 05.5								
		c2921-ES-13										
Address	Source	C2921-ES-13		~	All I	nterfaces		Nur	nber of flows:	5,000+	cs	V File Re
Applications		*DefaultFilterGro	oup 🜔 🖷	Inboun					asic Flow		Sorted - Unique	El a una
▶ QoS	Filter	*DefaultFilterGro	oup 🔽 🔤	Inboun	J V			В	asic Flow	- Time	Sorted - Unique	FIOWS
Network						121.20100						-
Medianet	Search wa	an & device = c	2921-ES-13.test.co	om & flow.ip	o.src=192.168.15.20	00					× ·	?
Applications (AVC)												
Firewall										0	*	
▶ PfR	Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co		Packet Rate	Src Country	Dst C
Wireless	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	11.18 Kbps			-
AnyConnect	Nov 14, 201		192.168.15.2		192.168.12.2	443	secure-http*	1	7.29 Kbps			-
▶ Ziften	Nov 14, 201		192.168.15.2		192.168.12.2	80	Maxis_Server**		1.89 Kbps			-
Miscellaneous	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	9.90 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	28.21 Kbps			-
ustom Reports	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	7.65 Kbps			-
AppDscp	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	130.58 Kbps			-
asdf	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	1.88 Kbps			-
avc-asr-test	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	12.48 Kbps			-
banwidth	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	1.97 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	53	dns	1	512.00 bps			-
benstest	Nov 14, 201		192.168.15.2		192.168.12.2		dns	1	488.00 bps			-
Construction BKPPort	Nov 14, 201		192.168.15.2		192.168.12.2		dns	1	568.00 bps			-
boss45	Nov 14, 201		192.168.15.2		192.168.12.2	80	ms-office-365		320.00 bps			-
Boston	Nov 14, 201		192.168.15.2		192.168.12.2	53	dns	1	464.00 bps			-
~	Nov 14, 201		192.168.15.2		192.168.12.2		skype	1	3.08 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	13.87 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	13.78 Kbps			-
port Actions	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	12.35 Kbps			-
ve	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	12.47 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	12.38 Kbps			-
ve As	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	12.52 Kbps			-
eate	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	5.45 Kbps			-
cove	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	7.12 Kbps			-
it	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	16.08 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http*	1	2.02 Kbps			-
lete	Nov 14, 201		192.168.15.2		192.168.12.2	53	dns	1	472.00 bps			-
hedule	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	7.44 Kbps			-
	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	6.55 Kbps			-
F	Nov 14, 201		192.168.15.2		192.168.12.2	80	http	1	20.54 Kbps			-
port to CSV	Nov 14, 201		192.168.15.2		192.168.12.2	53	dns	1	448.00 bps			-
port to CSV	Nov 14, 201		192.168.15.2		192.168.12.2	53	dns	1	448.00 bps			-
1p	Nov 14, 201	6 UDP	192.168.15.2	. 60,131	192.168.12.2	53	dns	1	448.00 bps	0.00 p	ps –	-
										Previous	Flows 1 - 5.00	

Top 10 Destination Addresses (Bytes or Flows)

The Top 10 Destinations Addresses table lists the top 10 devices generating the largest number of bytes or flows to a particular destination address. Click on the + sign to the left of the IP address to show the devices associated with the Destination IP address.

	Flows		
Dst IP Addr	Bytes	▼ ¹ Flows	
▶ 192.168.15.200		927 MB	13,423
▶ 192.168.12.2		699 MB	15,452
10.254.101.212		593 MB	140
▶ 8.8.8.5		123 MB	86
7.7.7.19		112 MB	70
▶ 8.8.8.1		77 MB	61
▶ 11.11.11.11		69 MB	239
▶ 7.7.7.14		64 MB	51
▶ 8.8.8.3		52 MB	46
▶ 8.8.8.4		50 MB	30

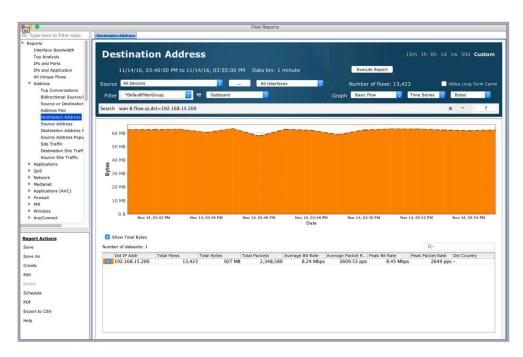
Click on the Top 10 Destination Addresses header to generate a Destination Address outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



Right-click on a device in the Destination Address table to select from Graph View, Add to IP Blacklist, Add to IP mapping or Copy to clipboard.

Dst IP Addr	Bytes				
192.168.15.20	0	927 MB			
192.168.12.2	Destination Address Rep	port	15,452		
10.254.101.2	140				
8.8.8.5	86				
7.7.7.19	Add 192.168.15.200 to	IP Mapping	70		
8.8.8.1	Copy 192.168.15.200 to	11 5	61		
11.11.11.11	Copy 192.108.13.200 to	5 chpbbard	239		
7.7.7.14		64 MB	51		
8.8.8.3		52 MB	46		
▶ 8.8.8.4		50 MB	30		

Graph View – generates a Destination Address outbound flow report for the selected source IP address for all devices.



Add to IP Blacklist – adds the IP address to the LiveNX blacklist. The blacklist feature is covered in Chapter 12, *Tools*.

Add to IP Mapping – allows you to create an alphanumeric name to the selected IP address. The IP mapping feature is covered in Chapter 12, *Tools*.

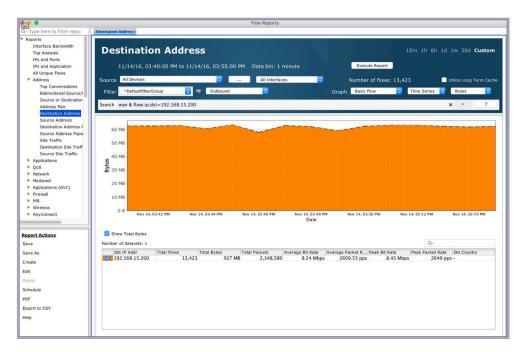
Copy to clipboard - copies the selected IP address to the clipboard.

Top 10 Destinat		dresses Flows 👻		v 1		
Dst IP Addr		Bytes		Flows		
30.20.20.1			396 MB		1,136	
192.168.1.185	Graph \	liew	MB		693	
± 192.168.1.136	· · ·	Add 30.20.20.1 to IP Blacklist			681	
192.168.1.142	Add 30.				668	Ξ
± 192.168.1.33	Add 30.	20.20.1 to IP Mapping	MB		621	
192.168.1.138			MB		589	
192.168.1.149	Copy 30	0.20.20.1 to clipboard	MB		566	
192.168.1.135			8 MB		528	
± 10.255.203.6			602 MB		478	
255.255.255.255			202 KB		450	
CC CTOD LANL DT			20.140		76	

Expand an IP address to show devices and right click on a device to select between Graph View and Top Analysis View.

Dst IP Addr	Bytes	▼ ¹ Flows				
▶ 192.168.15.20	0	927 MB	13,423			
192.168.12.2 10.254.101.2	Destination Address Rep	port	15,452 140			
8.8.8.5	Add 192.168.15.200 to	2.168.15.200 to IP Blacklist				
7.7.7.19	Add 192.168.15.200 to	2.168.15.200 to IP Mapping				
▶ 8.8.8.1 ▶ 11.11.11.11	Copy 192.168.15.200 to	2.168.15.200 to clipboard				
7.7.7.14		64 MB	51			
8.8.8.3		52 MB				
▶ 8.8.8.4		50 MB	30			

Graph View – generates a Destination Address outbound flow report for the selected destination IP address for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.



Top Analysis View – generates a Top Analysis outbound flow report for the selected device.

B	Top Analysi											
Reports												
Interface Bandwidth	Ton	Analys	ic							5m 1h 6h	1d 1w 30d	Custo
Top Analysis		Analys										Cubto
IPs and Ports												
IPs and Application		11/14/16, 03:3	5:00 PM to 11/14	/16, 03:50	:00 PM			Exec	ute Report			
All Unique Flows												
Address	Source	c2921-ES-13			All I	nterfaces		Numbe	er of flows:	5 000+		V File Re:
Applications	Jource					Rendees		Numbe	i or nows.	5,000+		
	Filter	*DefaultFilterGro	up 🚺 🦷	Inbound	0			Basic	Flow	C Time	Sorted - Unique	Flows
▶ QoS	riter										oorico oriiqui	
Network	Count	and the desidence of	2921-ES-13.test.co		102 100 15 2	0					× ·	7
Medianet	Search	wan & device = c.	2921-ES-13.test.co	m & flow.ip	src=192.168.15.20	00					× ·	
Applications (AVC)												-
▶ Firewall										Q		
▶ PfR	Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co Bit F	1310	Packet Rate	Src Country	Dst (
► Wireless	Nov 14, 20		192.168.15.2.		192.168.12.2	80	http*		11.18 Kbps	10.08 p		Dst C
	Nov 14, 20 Nov 14, 20		192.168.15.2.		192.168.12.2	443	secure-http*	1	7.29 Kbps	10.08 p		-
AnyConnect						443 80	Maxis_Server**	1				-
▶ Ziften	Nov 14, 20		192.168.15.2		192.168.12.2	80		1	1.89 Kbps	1.22 p		-
Miscellaneous	Nov 14, 20		192.168.15.2		192.168.12.2		http	1	9.90 Kbps	5.60 p		-
Custom Reports	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*		28.21 Kbps	21.55 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*	1	7.65 Kbps	21.74 p		-
AppDscp	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1 1	30.58 Kbps	40.32 p		-
asdf	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	1.88 Kbps	3.12 p		-
avc-asr-test	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	12.48 Kbps	8.36 p		-
banwidth	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*	1	1.97 Kbps	2.15 p		-
benstest	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns		512.00 bps	0.00 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns	1	488.00 bps	0.00 p		-
4 BKPPort	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns	1	568.00 bps	0.00 p		-
boss45	Nov 14, 20		192.168.15.2		192.168.12.2	80	ms-office-365		320.00 bps	0.00 p		-
Boston	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns		464.00 bps	0.00 p		-
~	Nov 14, 20		192.168.15.2		192.168.12.2	61,677	skype	1	3.08 Kbps	3.08 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	13.87 Kbps	8.01 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http		13.78 Kbps	7.71 p		-
port Actions	Nov 14, 20		192.168.15.2		192.168.12.2	80	http		12.35 Kbps	7.40 p		-
ve	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	12.47 Kbps	8.01 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	12.38 Kbps	7.39 p		-
ve As	Nov 14, 20		192.168.15.2		192.168.12.2	80	http		12.52 Kbps	8.03 p		-
ate	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*	1	5.45 Kbps	5.60 p		-
rate	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*	1	7.12 Kbps	7.32 p		-
t	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	16.08 Kbps	9.07 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http*	1	2.02 Kbps	5.75 p		-
lete	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns	1	472.00 bps	0.00 p		-
hedule	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	7.44 Kbps	7.89 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	80	http	1	6.55 Kbps	6.31 p		-
F	Nov 14, 20		192.168.15.2		192.168.12.2	80	http		20.54 Kbps	32.99 p		-
	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns	1	448.00 bps	0.00 p		-
port to CSV	Nov 14, 20		192.168.15.2		192.168.12.2	53	dns	1	448.00 bps	0.00 p		-
1p	Nov 14, 20	016 UDP	192.168.15.2	60,131	192.168.12.2	53	dns	1	448.00 bps	0.00 p	ps –	-
-												

Top 10 Source Countries [Bytes or Flows]

The Top 10 Source Countries table lists the top 10 countries generating the largest number of bytes or flows. Click on the + sign to the left of the source country to show the devices associated with the source country.

	Flows		
Src Country	Bytes	▼ ¹ Flows	
Unknown		2 GB	31,08
US/UNITED STATES		4 MB	34
c1811-ES-11		4 MB	34
IE/IRELAND		350 KB	1
ZA/SOUTH AFRICA		5 KB	

Click on the Top 10 Source Country header to generate a Source Country inbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

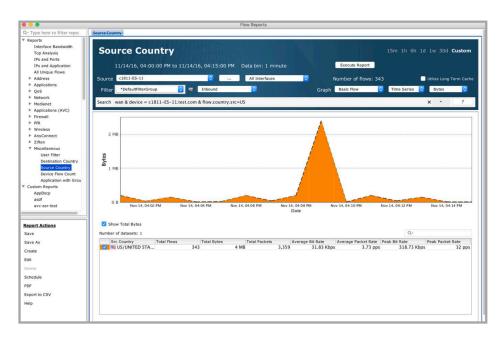
			Flow Reports					
Type here to filter report	Source Country							
Reports								
Interface Bandwidth	0							
Top Analysis	Source C	ountry					15m 1h 6h 1d	d 1w 30d Custo
IPs and Ports								
IPs and Application	11/14/16, 0	03:55:00 PM to 11/14/16, 04:10:	00 PM Data bin: 1 m	inute	Exe	cute Report		
All Unique Flows								
Address	Source All Devices	O	All Interfaces		Numb	er of flows: 31	.437	Utilize Long Term Ca
Applications	and the second sec	And in the other states in the state of the	Longer of Longer Lands					
QoS	Filter *DefaultFilt	erGroup 😮 🤯 Inbound			Graph Basi	c Flow	Time Series 🗘	Bytes 🗘
Network	A CONTRACTOR OF THE OWNER							
Medianet	Search wan							× • ?
Applications (AVC)	and the second s							
Firewall								
PfR								
Wireless								
AnyConnect								
Ziften								
Miscellaneous								
User Filter	Bytes Bytes							
Destination Country	yte							
Source Country	-							
Device Flow Count								
Application with Grou								
Application with Grou								
Application with Grou								
Application with Grou ustom Reports								
Application with Grou ustom Reports AppDscp	0 B Nov	14, 03:57 PM Nov 14, 03:59 PM	Nov 14, 04:01 PM	Nov 14, 04:03 PM	1 Nov 14,	04:05 PM	Nov 14, 04:07 PM	Nov 14, 04:09 PM
Application with Grou ustom Reports AppDscp asdf	0.B-Nov	14, 03:57 PM Nov 14, 03:59 PM	Nov 14, 04:01 PM	Nov 14, 04:03 PM Date	1 Nov 14,	04:05 PM	Nov 14, 04:07 PM	Nov 14, 04:09 PM
Application with Grou ustom Reports AppDscp asdf	0.B Nov	14, 03:57 PM Nov 14, 03:59 PM	Nov 14, 04:01 PM		Nov 14,	04:05 PM	Nov 14, 04:07 PM	Nov 14, 04:09 PM
Application with Grou ustom Reports AppDscp asdf avc-asr-test	0 B		Nov 14, 04:01 PM		1 Nov 14,	04:05 PM	Nov 14, 04:07 PM	Nov 14, 04:09 PM
Application with Grou stom Reports AppDscp asdf avc-asr-test ort Actions	Nov		Nov 14, 04:01 PM		1 Nov 14,	04:05 PM		Nov 14, 04:09 PM
Application with Grou ustom Reports AppDscp asdf avc-asr-test ort Actions e	Nov			Date			Q-	
Application with Grou stom Reports AppDscp asdf avc-asr-test ort Actions e	Nov	Total Flows Total Byte	rs Total Packets	Date Average Bil	t Rate Aver	sge Packet Rate	Q- Peak Bit Rate	Peak Packet Rate
Application with Grou ustom Reports AppDacp asdf avc-asr-test cont Actions re re As	Nov	Total Flows Total Byte 31,082	rs Total Packets	Date Average Bil 210,824 2	t Rate Aver 1.49 Mbps	ige Packet Rate 7456.47 pps	Q- Peak Bit Rate 22.10 Mbps	Peak Packet Rate
Application with Grou ustom Reports AppDacp asdf avc-asr-test cott Actions re re re As ate	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou stom Reports Applotop asdr avc-asr-test ort Actions e e As ate	Show Total Bytes Number of datasets: 4 Src Country V. Unknown	Total Flows Total Byte 31,082 342 12 12	zs Total Packets 2 GB 6,7 4 MB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 81.95 Kbps	nge Packet Rate 7456.47 pps 3.73 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou stam Reports Applocp asidf avc-asr-test ort Actions e e As ate	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou usom Reports AppDrop avc-asr-test ere re as aster test test test test test test test	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou users AppDrop asdf access-test wort Actions ref e As ate celse cedule	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou usom Reports AppDrop asdf avc-asr-test cre re re st t t t t	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou Custom Reports AppDscp asdf	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou ustom Reports AppDeop asdf avc-asr-test ve ve As test ate t t	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp
Application with Grou usom Reports Apports asdr avc-asr-test ascr re re as as re as t st st st st st st st st st st st st	Show Total Bytes Number of datasets: 4 Src Country Olivery Oli	Total Flows Total Byte 31,082 342 12 12	25 Total Packets 2 GB 6,7 4 MB 350 KB	Date Average Bil 710,824 2 3,360 3 296	t Rate Aver 1.49 Mbps 1.95 Kbps 3.11 Kbps	age Packet Rate 7456.47 pps 3.73 pps 0.33 pps	Q- Peak Bit Rate 22.10 Mbps 318.73 Kbps 16.05 Kbps	Peak Packet Rate 5 7685 pp 5 32 pp 5 1 pp

Right-click on a source country to display a Source Country inbound flow report specific to the selected country.



Expand a source country to show devices and right click on a device to select between Graph View and Top Analysis View.

Graph View – generates a Source Country inbound flow report for the selected source country for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.



Top Analysis View - generates a Top Analysis inbound flow report for the selected device.

Type here to filter repo	Top Analysis									
	TOP Analysis									
Reports										
Interface Bandwidth	Top Analy	cic						5m 1h 6h 1		Custom
Top Analysis	TOP Analy	515						200 10 00 1	u 1W 200	custom
IPs and Ports										
IPs and Application	11/14/16.04	00:00 PM to 11/14/16.	04:15:00 PM				Execute Report			
All Unique Flows										
Address	Source c1811-ES-11		O	All Interfaces					-	File Resu
	Source clair-es-II		✓ …	All Interfaces	~	Nu	mber of flows:	343	csv	File Resu
Applications	Filter *DefaultFilter	iroup	Inbound				Basic Flow	Time Co	rted - Unique F	
► QoS	Filter *DefaultFilter	roup 🔽 🔻	Inbound				basic Flow	Time Sc	rted - Unique r	riows
Network				INTERNET COMPANY					_	
Medianet	Search wan & device =	c1811-ES-11.test.com &	flow.country.src=l	JS					×・	?
Applications (AVC)										
Firewall								Q		
	(m)									
PfR	Time Protocol	Src IP Addr Src			Application	Flow Record Co			Src Country	Dst Co
Wireless	Nov 14, 2016 TCP	52.8.208.186 443		3.202.1 39,134	secure-http*	1			US/United	
AnyConnect	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 44,866	dns*	1	632.00 bps		US/United	
Ziften	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 40,310	dns*	1	968.00 bps		US/United	
Miscellaneous	Nov 14, 2016 TCP	172.217.4.174 443		3.202.1 52,189	secure-http*	1			US/United	
ustom Reports	Nov 14, 2016 TCP	52.8.208.186 443		3.202.1 39,136	secure-http*	1	55.15 Kbps		US/United	
	Nov 14, 2016 TCP	52.8.208.186 443		3.202.1 39,137	secure-http*	1	57.75 Kbps		US/United	
AppDscp	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 33,357	dns*	1	888.00 bps		US/United	
asdf	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 51,550	dns*	1	1.87 Kbps		US/United	
avc-asr-test	Nov 14, 2016 ICMP	72.234.37.62 0		3.202.1 2,816	unknown	1	1.34 Kbps		US/United	
banwidth	Nov 14, 2016 ICMP	64.233.174.2 0		3.202.1 2,816	unknown	1	1.41 Kbps		US/United	
benstest	Nov 14, 2016 ICMP	108.170.234 0		3.202.1 2,816	unknown	1	6.77 Kbps		US/United	
SKPPort BKPPort	Nov 14, 2016 ICMP	216.239.59.2 0		3.202.1 2,816	unknown	1	704.00 bps		US/United	
	Nov 14, 2016 UDP Nov 14, 2016 TCP	72.235.80.12 53		3.202.1 49,930	dns* http*	1	1.10 Kbps 480.00 bps		US/United	
boss45				3.202.1 59,037		1			US/United	
Boston	Nov 14, 2016 TCP Nov 14, 2016 TCP	172.217.4.174 80		3.202.1 37,592 3.202.1 40.501	http*	1	480.00 bps 480.00 bps		US/United	
<u>^</u>	Nov 14, 2016 TCP	172.217.4.174 80 172.217.4.174 80		3.202.1 40,501 3.202.1 43,370	http*	1	480.00 bps 480.00 bps		US/United US/United	
						1				
port Actions	Nov 14, 2016 TCP	172.217.4.174 80		3.202.1 55,418	http*	1	480.00 bps		US/United	
port Actions	Nov 14, 2016 TCP Nov 14, 2016 TCP	172.217.4.174 80 172.217.4.174 80		3.202.1 40,962 3.202.1 49,654	http*	1	480.00 bps 480.00 bps		US/United US/United	
/e	Nov 14, 2016 TCP	172.217.4.174 80		3.202.1 37.964	http*	1	480.00 bps		US/United	
ve As	Nov 14, 2016 TCP	172.217.4.174 80		3.202.1 56.353	http*	1	480.00 bps 480.00 bps		US/United	
/e As	Nov 14, 2016 TCP	172.217.4.174 80		3.202.1 57,928	http*	1	480.00 bps 480.00 bps		US/United	
ate	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 51,669	dns*	1	1.87 Kbps		US/United	
	Nov 14, 2016 ICMP	172.217.4.174 0		3.202.1 0	unknown	1	1.01 Kbps		US/United	
t	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 36,000	dns*	1			US/United	
ete	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 44.993	dns*	1	1.10 Kbps		US/United	
	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 46,516	dns*	1	1.09 Kbps		US/United	
nedule	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 57,895	dns*	1			US/United	
	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 35,105	dns*	1	960.00 bps		US/United	
r	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 57,445	dns*	1			US/United	
port to CSV	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 41.326	dns*	1	1.06 Kbps		US/United	
	Nov 14, 2016 UDP	72.235.80.12 53		3.202.1 42,317	dns*	1			US/United	
lp		7 L.L. 5 5.00.1 L 33	10.100		0113		332.00 Ups	0.00 pps		

Top 10 Destination Countries [Bytes or Flows]

The Top 10 Destination Countries table lists the top 10 countries receiving the largest number of bytes or flows. Click on the + sign to the left of the destination country to show the devices associated with the destination country.

	Flows		
Dst Country	Bytes	▼ ¹ Flows	
Unknown		2 GB	30,693
V 🧮 US/UNITED STAT	ES	719 MB	1,361
c2921-ES-13		695 MB	770
c1941-ES-12		24 MB	161
c1811-ES-11		249 KB	430
CN/CHINA		2 MB	29
MX/MEXICO		1 MB	15
FR/FRANCE		1 MB	14
IQ/IRAQ		711 KB	15
IE/IRELAND		20 KB	54
	~ ^	2 1/ 0	1

Click on the Top 10 Destination Country header to generate a Destination Country outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



Right-click on a destination country to display a Destination Country outbound flow report specific to the selected country.



Expand a destination country to show devices and right click on a device to select between Graph View and Top Analysis View.



Graph View – generates a Destination Country outbound flow report for the selected destination country for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.

2- Type here to filter report	Top Analysis									
	Top Analysis									
Reports				antitueste su	STATISTICS.					
Interface Bandwidth	Ton Anoly							15m 1h 6h		
Top Analysis	Top Analy	SIS						15m 1n 6n	1d 1w 30d	Custon
IPs and Ports										
IPs and Application	11/14/16.04	05:00 PM to 11/1	4/16.04:20	:00 PM			Execute Report			
All Unique Flows	11/14/10, 04									
	Source c2921-ES-13				Interfaces					
Address	Source cz921-ES-13		~	All 1	Interraces	<u> </u>	Number of flows	5: 770	cs	V File Res
Applications	Filter *DefaultFilterG	roup	Outbour				Basic Flow		Sorted - Unique	Channe .
▶ QoS	Filter *DefaultFilterG	roup 🔽	Uutbour	id 🗸			Basic Flow	Time	Sorted - Unique	FIOWS
▶ Network	A A A MARCEL CONTRACTOR				111.11.11.1111					
Medianet	Search wan & device =	c2921-ES-13.test.c	om & flow.co	ountry.dst=US					× ·	?
Applications (AVC)			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		IN A DURING THE					
► Firewall								0	-	
▶ PfR	Time Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co Bit Rate	Packet Rate	Src Country	Dst C
▶ Wireless	Nov 14, 2016 UDP	10.0.0.2	20	7.7.7.19	1,028	ftp-data	1 926.71 Kbp			📑 U
AnyConnect	Nov 14, 2016 UDP	10.0.0.2	20	7.7.7.19	1,027	ftp-data	1 16.66 Kbp			💻 U
▶ Ziften	Nov 14, 2016 UDP	10.0.0.2	7,777	7.7.7.17	7,777	unclassified	1 269.20 Kbp			💷 U
Miscellaneous	Nov 14, 2016 UDP	10.0.12.2	1,027	8.8.8.2	1,604	citrix-static	1 20.53 Kbp			🎫 U
	Nov 14, 2016 UDP	10.0.0.2	1,028	7.7.7.15	1,604	citrix-static	1 38.89 Kbp			💷 U
Custom Reports	Nov 14, 2016 UDP	192.168.12.2		11.11.11.12	13,958	VoIP13958	1 72.99 Kbp			💷 U
AppDscp	Nov 14, 2016 UDP	192.168.12.2	13,958	11.11.11.13	13,958	VoIP13958	1 72.99 Kbp			💷 U
asdf	Nov 14, 2016 UDP	192.168.12.2		11.11.11.14	13,958	VoIP13958	1 72.99 Kbp			🎫 U
avc-asr-test	Nov 14, 2016 UDP	10.0.12.2	16,384	8.8.8.2	16,384	ServerMirrorP				💻 U
banwidth	Nov 14, 2016 UDP	192.168.12.2		11.11.11.11	69	tftp*	1 82.36 Kbp			🔜 U
	Nov 14, 2016 UDP	192.168.12.2	179	11.11.11.11	179	bgp	1 18.27 Kbp	os 10.02 p	ps –	💷 U
benstest	Nov 14, 2016 UDP	192.168.12.2	520	11.11.11.11	520	rip	1 18.27 Kbp	os 10.02 p	ps –	💻 U
SKPPort BKPPort	Nov 14, 2016 UDP	192.168.12.2	7,648	11.11.11.11	7,648	cuseeme	1 36.54 Kbp	os 20.03 p	ps –	💻 U
boss45	Nov 14, 2016 UDP	10.0.12.2	16,388	8.8.8.5	16,384	Google_Stats**				🔜 U
Boston	Nov 14, 2016 UDP	192.168.12.2	64,442	11.11.11.11	5,004	CiscoRTP-Vi	1 205.54 Kbp	os 38.29 p	ps –	🛄 U
A	Nov 14, 2016 UDP	10.0.12.2	20	8.8.8.5	1,027	ftp-data	1 65.84 Kbr	os 5.57 p	ps –	💻 U
	Nov 14, 2016 UDP	10.0.12.2	1.026	8.8.8.2	1.604	citrix-static	1 53.07 Kbr	os 44.82 p	ps -	💷 U
	Nov 14, 2016 UDP	10.0.0.2	1,027	7.7.7.15	1,604	citrix-static	1 40.65 Kbp	os 34.33 p	ps –	🔜 U
port Actions	Nov 14, 2016 UDP	10.0.0.2	1,026	7.7.7.14	69	tftp*	1 508.77 Kb	os 43.03 p	ps –	📑 U
	Nov 14, 2016 UDP	10.0.0.2	1.028	7.7.7.15	1,604	citrix-static	1 60.72 Kbr	os 51.28 p	ps –	💻 U
ive	Nov 14, 2016 UDP	10.0.12.2	1,027	8.8.8.1	69	tftp*	1 248.31 Kbp	os 24.87 p	ps –	💷 U
ave As	Nov 14, 2016 UDP	192.168.12.2		11.11.11.11	5,005	rtcp	1 159.45 br			💷 U
	Nov 14, 2016 UDP	10.0.12.2	7,777	8.8.8.3	5,555	unclassified	1 39.07 Kb	os 9.25 p	ps –	💷 U
reate	Nov 14, 2016 UDP	10.0.0.2	7,777	7.7.7.17	5,555	unclassified	1 27.14 Kb	os 6.43 p	ps –	💷 U
lit	Nov 14, 2016 UDP	10.0.12.2	16,386	8.8.8.4	16,384	unclassified	1 60.22 Kbr			🔜 U
	Nov 14, 2016 UDP	10.0.12.2	16,390	8.8.8.1	16,384	unclassified	1 72.99 Kbp		ps –	💷 U
elete	Nov 14, 2016 UDP	10.0.12.2	7,777	8.8.8.3	7,777	unclassified	1 387.17 Kb			🔜 U
hedule	Nov 14, 2016 UDP	10.0.0.2	1,027	7.7.7.14	69	tftp*	1 430.51 Kbr			🔜 U
nequie	Nov 14, 2016 UDP	10.0.0.2	1,026	7.7.7.15	1,604	citrix-static	1 41.37 Kbp			💷 U
F	Nov 14, 2016 UDP	10.0.0.2	20	7.7.7.19	1,025	HSA-Testing**				📑 U
	Nov 14, 2016 UDP	10.0.0.2	1,028	7.7.7.14	69	tftp*	1 258.92 Kbr			🔜 U
port to CSV	Nov 14, 2016 UDP	10.0.12.2	1,026	8.8.8.1	69	tftp*	1 550.98 Kbp	os 46.60 p	ps –	🔜 U
elp	Nov 14, 2016 UDP	10.0.0.2	20	7.7.7.19	1,026	ftp-data	1 28.86 Kbr	os 8.43 p	ps –	🔜 U
aip (

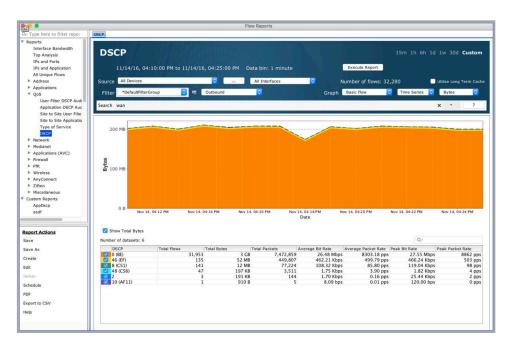
Top Analysis View - generates a Top Analysis outbound flow report for the selected device.

Top 10 DSCP (Bytes or Flows)

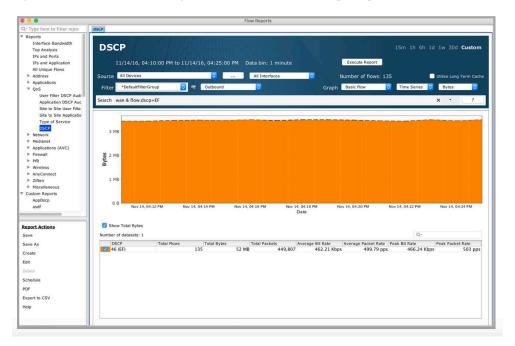
The Top 10 DSCP table lists the top 10 DSCP values associated with the largest number of outbound bytes or flows. Click on the + sign to the left of the DSCP value to show the devices associated with the DSCP value.

DSCP Flows	Bytes		
▶ 0 (BE)		3 GB	31,953
▶ 46 (EF)		52 MB	135
▶ 8 (CS1)		12 MB	141
▶ 48 (CS6)		197 KB	47
▶ 2		191 KB	3
▶ 10 (AF11)		910 B	1

Click on the Top 10 DSCP header to generate a DSCP outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

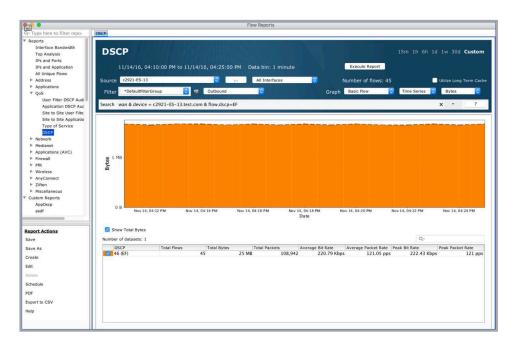


Right-click on a DSCP value to generate an outbound flow report specific to the selected DSCP value.



Expand a DSCP value to show devices and right click on a device to select between Graph View and Top Analysis View.

Graph View – generates a DSCP outbound flow report for the selected DSCP value for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.



Top Analysis View - generates a Top Analysis outbound flow report for the selected device.

					Flow Reports	5						
Type here to filter repoi	Top Analysis											
eports												
Interface Bandwidth												
Top Analysis	Top Analys	is									6h 1d 1w 30d	Custo
	rop runaryo											
IPs and Ports										_		
IPs and Application	11/14/16, 04:1	0:00 PM to 11/14	/16, 04:25	:00 PM					Execute Repor	t		
All Unique Flows												
Address	Source c2921-ES-13		0	All I	nterfaces			N	umber of flow	/s: 45	C C C	SV File Re
Applications		THE REAL PROPERTY OF	1 1 1 1 1	THE R. P. LEWIS CO., LANSING MICH.							_	
▶ QoS	Filter *DefaultFilterGro	up 😒 🖷	Outboun	d 🗘					Basic Flow	۲ 😂	Time Sorted - Unique	e Flows
Network	1 I I manufacture	COLUMN TWO IS NOT			NINKLY							
 Medianet 	Search wan & device = ca	2921-ES-13.test.co	m & flow.ds	cp=EF							×	?
												_
Applications (AVC)											Q	
▶ Firewall											Q.,	
▶ PfR	Time Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co	Bit Rate	Packet Rate	Src Country	Dst Country	In IF
▶ Wireless	Nov 14, 2016 UDP	192.168.12.2	13,958	11.11.11.14	13,958	VoIP13958	1	72.99 Kbps	40.01 pp	-	US/United	Vlan1
AnyConnect	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.99 Kbps	40.01 pp		US/United	
≥ Ziften	Nov 14, 2016 UDP	192.168.12.2		11.11.11.12	13,958	VoIP13958	1	72.99 Kbps	40.01 pp		US/United	
Miscellaneous	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VoIP13958	1	72.98 Kbps	40.01 pps		US/United	
	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.98 Kbps	40.01 pps		US/United	
Custom Reports	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	72.98 Kbps	40.01 pps		🔜 US/United	
AppDscp	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	73.01 Kbps	40.03 pps		US/United	
asdf	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	73.01 Kbps	40.03 pp		🔜 US/United	
avc-asr-test	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VoIP13958	1	73.01 Kbps	40.03 pp		US/United	
banwidth	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
benstest	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
BKPPort	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	-	72.98 Kbps	40.01 pp		US/United	
boss45	Nov 14, 2016 UDP Nov 14, 2016 UDP		13,958 13,958	11.11.11.13 11.11.11.12	13,958 13,958	VoIP13958 VoIP13958		72.98 Kbps 72.98 Kbps	40.01 pp: 40.01 pp:		US/United	
Boston	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VolP13958		72.98 Kbps	40.01 pp		US/United	
ClarkBEIPs	Nov 14, 2016 UDP	192.168.12.2		11.11.11.14	13,958	VolP13958		72.99 Kbps	40.02 pp		US/United	
	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VolP13958	-	72.99 Kbps	40.02 pp		US/United	
	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VolP13958		72.99 Kbps	40.02 pp		US/United	
port Actions	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VolP13958	1	72.99 Kbps	40.01 pp		US/United	
ive	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VolP13958	1	72.99 Kbps	40.01 pp		US/United	
	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VolP13958	1	72.99 Kbps	40.01 pp		US/United	
ve As	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.99 Kbps	40.01 pp		US/United	
eate	Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VoIP13958	1	72.99 Kbps	40.01 pp		US/United	
	Nov 14, 2016 UDP	192.168.12.2	13,958	11.11.11.12	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	Vlan1
it	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
lete	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
10.00	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
nedule	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
	Nov 14, 2016 UDP	192.168.12.2		11.11.11.12	13,958	VoIP13958	1	72.99 Kbps	40.02 pp		US/United	
F	Nov 14, 2016 UDP		13,958	11.11.11.14	13,958	VoIP13958	1	72.98 Kbps	40.01 pp		US/United	
port to CSV	Nov 14, 2016 UDP		13,958	11.11.11.13	13,958	VoIP13958	1	72.98 Kbps	40.01 pp		US/United	
	Nov 14, 2016 UDP Nov 14, 2016 UDP		13,958	11.11.11.12	13,958	VoIP13958	1	72.98 Kbps	40.01 pps		US/United	
10		192.168.12.2		11.11.11.12	13,958	VoIP13958		72.98 Kbps	40.01 pps		US/United	

Top 10 Interfaces (Outbound) [Bytes or Flows]

The Top 10 Interfaces (Outbound) table summarizes the top 10 interfaces with the highest number of outbound bytes or flows.

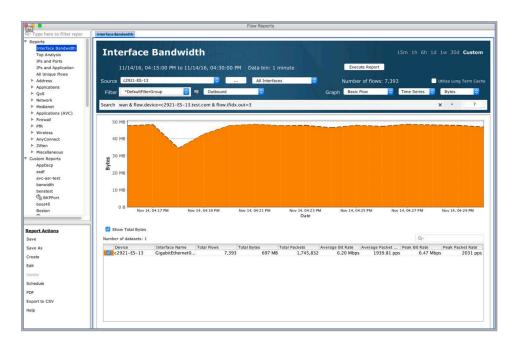
	Flow	s		
Out IF	Device	Bytes	▼ ¹ Flows	
GigabitEthernet0/1	c2921-ES-13		697 MB	7,408
GigabitEthernet0/0	c1941APN-212		653 MB	538
FastEthernet0	c1811-ES-11		359 MB	8,246
GigabitEthernet0/1	c1941-ES-12		339 MB	7,877
GigabitEthernet0/0	c1941-ES-12		332 MB	6,783
GigabitEthernet0/2	c2921-ES-13		304 MB	299
FastEthernet0/1/1	c2921-ES-13		299 MB	297
Vlan100	c1941APN-212		60 MB	738
Vlan101	c1941-ES-12		260 KB	36
Vlan168	c1941-ES-12		137 KB	58

Click on the Top 10 Interfaces (Outbound) to generate a Traffic Volume Pair outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



Right-click on an entry to choose between Graph View and Top Analysis View.

Graph View – generates a Traffic Volume Pair outbound flow report for the selected output interface.



Top Analysis View - generates a Top Analysis outbound flow report for the selected device.

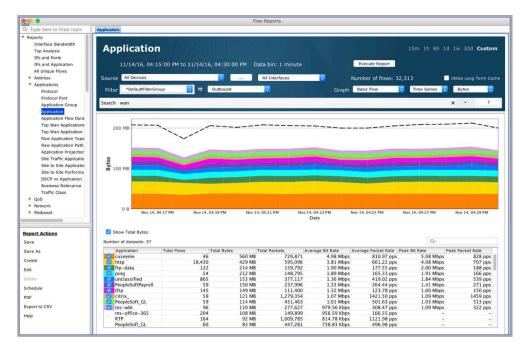
Type here to filter repo	Top Analysis							
Reports								
Interface Bandwidth								
	Top Analys	ic					5m 1h 6h 1d 1w 30	d Custom
Top Analysis	TOP Analys							
IPs and Ports								
IPs and Application	11/14/16, 04:1	5:00 PM to 11/1-	4/16, 04:30	0:00 PM		Execute Report		
All Unique Flows								
▶ Address	Source c2921-ES-13			All Interfaces		Number of flows:	5 000+	SV File Resu
Applications	Jource					Number of nows.	5,000+	SV The Read
P Applications ► OoS	Filter *DefaultFilterGr	oup 🔂 🛛	Outbour	d 🖸		Basic Flow	Time Sorted - Uniqu	ue Flows
	The second second							
Network	Search wan & flow.devic	2021 FC 12 +-		- Kalu and D				2
Medianet	Search wan & flow.devic	e=c2921-E5-13.te	st.com & flov	w.ifidx.out=3			× •	
Applications (AVC)	The second second second second second	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 J					
▶ Firewall							Q,-	
▶ PfR	Time Protocol	Src IP Addr	Src Port	Dst IP Addr Dst Port	Application	Flow Record Co Bit Rate	Packet Rate Src Country	Dst C
► FIR Wireless	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.315	http*	1 41.96 Kbps	5.03 pps -	Dst Ci
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,315	http	1 41.96 Kbps 1 265.30 Kbps	26.52 pps -	
AnyConnect	Nov 14, 2016 TCP	192.168.12.2	3,389	192.168.15.2 4,287	PeopleSoft U		187.50 pps -	-
Ziften	Nov 14, 2016 UDP	192.168.12.2	5,060	11.11.11.11 5.060	sip*	1 22.20 Kbps	14.02 pps -	= US
Miscellaneous	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,305	http	1 22.20 Kbps 1 24.39 Kbps	2.63 pps -	- 03
Custom Reports	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,303	secure-http*	1 2,39 Kbps	0.76 pps -	-
AppDscp	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.286	http	1 22.47 Kbps	2.38 pps -	-
asdf	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,280	http	1 22.80 Kbps	2.36 pps -	-
	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4.298	http	1 45.51 Kbps	4.71 pps -	-
avc-asr-test	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.293	http	1 92.29 Kbps	8.93 pps -	-
banwidth	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,296	http	1 21.40 Kbps	2.26 pps -	-
benstest	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,281	http	1 31.80 Kbps	3.32 pps -	-
BKPPort	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.289	http	1 31.85 Kbps	3.31 pps -	-
boss45	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4.306	http	1 39.82 Kbps	4.17 pps -	-
Boston	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,308	http	1 40.44 Kbps	4.19 pps -	-
Boston	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2.282	http	1 3.54 Kbps	1.53 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,291	http	1 24.71 Kbps	3.19 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.311	http	1 23.57 Kbps	2.67 pps -	-
port Actions	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,303	http	1 2.51 Kbps	1.52 pps -	-
ve	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,308	http	1 2.84 Kbps	1.74 pps -	-
ive	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,312	http*	1 969.04 bps	0.77 pps -	-
ive As	Nov 14, 2016 UDP	192.168.12.2		192.168.15.2 64,232	dns	1 4.26 Kbps	0.00 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,317	http	1 5.14 Kbps	6.07 pps -	-
eate	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,278	http	1 1.04 Mbps	105.77 pps -	-
lit	Nov 14, 2016 UDP	192.168.12.2		192.168.15.2 60,143	dns	1 3.70 Kbps	0.00 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,294	http	1 25.89 Kbps	2.63 pps -	-
lete	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,300	http	1 29.79 Kbps	3.09 pps -	-
hedule	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4,291	http	1 13.76 Kbps	1.39 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,299	Maxis_Server**		4.68 pps -	-
0F	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 2,318	http	1 24.14 Kbps	8.40 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,319	http	1 12.55 Kbps	7.25 pps -	-
port to CSV	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,310	http	1 29.31 Kbps	3.15 pps -	-
elp	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4,312	http	1 32.30 Kbps	3.39 pps -	-
						,	Previous Flows 1 - 5.	000 Next

Top 10 Application [Bytes or Flows]

The Top 10 Application table lists the top 10 applications generating the largest number of bytes or flows. Click on the + sign to the left of the Application name to show the devices associated with the application.

	Flows			
Application name	Bytes	₩1	Flows	
cuseeme		560 MB		46
c1941APN-212		516 MB		15
c2921-ES-13		44 MB		29
c1941-ES-12		456 B		2
http		429 MB		18,430
▶ ftp-data		214 MB		122
▶ ping		212 MB		54
unclassified		153 MB		865
PeopleSoftPayroll		150 MB		59
▶ tftp		149 MB		145
		101 140		F0

Click on the Top 10 Applications header to generate an Application outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

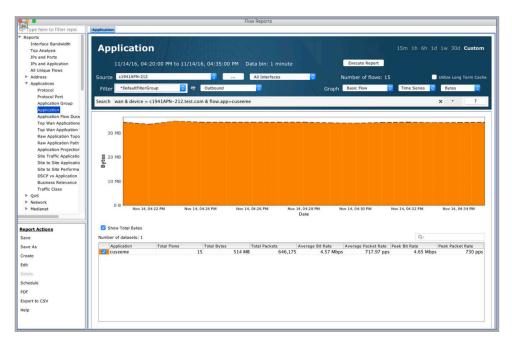


Right click on an application in the table to graph all applications across all devices.

			Flow Reports					
Type here to filter report	Application							
Reports								
Interface Bandwidth	A DESCRIPTION OF THE OWNER							
	Application						15m 1h 6h 1d	1w 30d Custon
Top Analysis	Application							211 300 003001
IPs and Ports								
IPs and Application	11/14/16, 04:15	:00 PM to 11/14/16, 04:30:00	PM Data bin: 1	minute		Execute Report		
All Unique Flows								
Address	Source All Devices		All Interfa	ces	N	lumber of flows: 75	· · · · ·	Utilize Long Term Cad
Applications	and the second s	States of the local division of the local di	and the second se					
Protocol	Filter *DefaultFilterGrou	ip 🗘 😓 Outbound			Graph	Basic Flow	Time Series	Bytes ᅌ
Protocol Port		and the second se	and the second	10.XV				
	Search wan & flow.app=cu	iseeme						× • ?
Application Group	and a now app -co							17 Landa
Application								
Application Flow Dura								
Top Wan Applications	40 MB							
Top Wan Appilcation	40 MB							
Raw Application Topo								
Raw Application Path								
Application Projection	30 MB							
Site Traffic Applicatio								
Site Traffic Applicatio	5							
Site to Site Applicatio	20 MB							
Site to Site Applicatio Site to Site Performa	Bytes B 20 MB							
	20 мв							
Site to Site Performa								
Site to Site Performa DSCP vs Application	20 MB							
Site to Site Performa DSCP vs Application Business Relevance Traffic Class								
Site to Site Performa DSCP vs Application Business Relevance Traffic Class	10 MB -							
Site to Site Performa DSCP vs Application Business Relevance Traffic Class QoS Network	10 MB -	7.94 Nor. 14.04.10.84	Nov.14 (4-21 RM	Neu Id	0.132.04	m14 0625 BM	Nex 14 (M-27 BH	New 14 OI-20 PM
Site to Site Performa DSCP vs Application Business Relevance Traffic Class QoS Network	10 MB -	7 PM Nov 14, 04:19 PM	Nov 14, 04:21 PM			w 14, 04:25 PM	Nov 14, 04:27 PM	Nov 14, 04:29 PM
Site to Site Performa DSCP vs Application Business Relevance Traffic Class QoS Network	10 MB -	7 PM Nov 14, 04:19 PM	Nov 14, 04:21 PM	Nov 14, (Da		v 14, 04:25 PM	Nov 14, 04:27 PM	Nov 14, 04:29 PM
Site to Site Performa DSCP vs Application Business Relevance Traffic Class • QoS • Network • Medianet	10 MB - 0 B - Nov 14, 04:1	7 PM Nov 14, 04:19 PM	Nov 14, 04:21 PM			w 14,04.25 PM	Nov 14, 04:27 PM	Nov 14, 04:29 PM
Site to Site Performa DSCP vs Application Business Relevance Traffic Class • QoS • Network • Medianet	10 MB -	7 PM Nov 14, Ö4 19 PM	Nov 14, 04:21 PM			w 14, 04.25 PM	Nov 14, 04:27 PM	Nov 14, 04:29 PM
Site to Site Performa DSCP vs Application Business Relevance Traffic Class 2 QoS Network • Network • Medianet	10 MB 0 B Nov 14, 04:1	7 PM Nov 14, 04 19 PM	Nov 14, 04:21 PM			w 14, Ó4 25 PM		Nov 14, 04:29 PM
Site to Site Parforma DSCP vs Application Business Relevance Traffic Class QoS • Network • Medianet	10 MB · 0 B Nov 14, 04:1 Show Total Bytes Number of datasets: 11	La Paren - Japan Kondria Alberta Jak		Da	ate		Q.	
Site to Site Parforma DSCP vs Application Business Relevance Traffic Class Qo5 • Network • Medianet	10 MB 0 B Nov 14, 04 1	Total Flows Total Bytes	Total Packe	Da ts Ave	ate erage Bit Rate	Average Packet Rate	Q- Peak Bit Rate	Peak Packet Rate
Sile to Sile Performa DSCP vs Application Business Relevance Traffic Class Qo5 Network Medianet	10 MB 0 B New 14, 04:1 Show Total Bytes Number of datasets: 11 Application	Total Flows Total Bytes 46	Total Packe 560 MB	Da ts Avi 729,871	ate erage Bit Rate 4.98 Mbps	Average Packet Rate 810.97 pps	Q- Peak Bit Rate 5.08 Mbps	Peak Packet Rate 828 pp
Site to Site Performa DSCP vs Application Business Relevance Traffic Class Qo5 Network Nedianet Per As er & As ate	10 MB 0 B Nov 14, 04.1	Total Flows Total Bytes 46	Total Packe 560 MB 3 MB	Da ts Av. 729,871 6,256	ate erage Bit Rate 4.98 Mbps 23.80 Kbps	Average Packet Rate 810.97 pps 6.95 pps	Q Peak Bit Rate 5.08 Mbps 357.01 Kbps	Peak Packet Rate 828 pp 104 pp
Sile to Site Ferforma DSCP vs Application Business Relevance Traffic Class QoS Network Medianet Per Associations re e As ate	10 MB 0 B Nov 14, 04 1 Show Total Bytes Number of datasets: 11 Application C citrix-static Pop3	Total Flows Total Bytes 46 1 1	Total Packe 560 MB 3 MB 966 KB	Da ts Avv 729,871 6,256 1,830	erage Bit Rate 4.98 Mbps 23.80 Kbps 8.59 Kbps	Average Packet Rate 810.97 pps 6.95 pps 2.03 pps	Q- Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps	Peak Packet Rate 828 pp 104 pp 30 pp
Site to Site Ferforma DSCP vs Application Business Relevance Traffic Class Q QS Q QS Network Medianet Protocological Protocolo	10 MB 0 B Nev 14, 64 1 Show Total Bytes Number of datasets: 11 Application Application Concernent Concernent Pappia	Total Flows Total Bytes 46 1 1 15	Total Packe 560 MB 3 MB 966 KB 620 KB	Da ts Av. 729,871 6,256 1,830 570	erage Bit Rate 4.98 Mbps 23.80 Kbps 8.59 Kbps 5.51 Kbps	Average Packet Rate 810.97 pps 6.95 pps 2.03 pps 0.63 pps	Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 82.70 Kbps	Peak Packet Rate 828 pp: 104 pp: 30 pp: 30 pp: 9 pp:
Site to Site Ferforma DSCP vs Application Business Relevance Traffic Class Q QS Q QS Network Medianet Protocological Protocolo	10 MB 0 B Nov 14, 64 1 C Show Total Bytes Number of attacks: 11 Applexian C curseme C cursem	Total Flows Total Bytes 46 1 1	Total Packe 560 MB 3 MB 966 KB 620 KB 582 KB	Da ts Avr 729,871 6,256 1,830 570 523	erage Bit Rate 4.98 Mbps 23.80 Kbps 8.59 Kbps 5.51 Kbps 5.18 Kbps	Average Packet Rate 810.97 pps 6.95 pps 2.03 pps 0.63 pps 0.58 pps	Q- Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 82.70 Kbps 77.62 Kbps	Peak Packet Rate 828 pp 104 pp 30 pp 9 pp 8 pp
Site to Site Ferforma DSCP vs Apoletaon Business Relevance Traffic Class 4 QAS • Medianet • Network • Network • Network • K • K • K • K • K • K • K • K	10 MB 0 B Nev 14, 64 1 Nev	Total Flows Total Bytes 466 1 15 2 2	Total Packe 560 MB 3 MB 966 KB 620 KB 582 KB 109 KB	Da ts Avi 729,871 6,256 1,830 570 523 946	erage Bit Rate 4.98 Mbps 23.80 Kbps 8.59 Kbps 5.18 Kbps 5.18 Kbps 968.42 bps	Average Packet Rate 810.97 pps 6.95 pps 2.03 pps 0.63 pps 0.63 pps 1.05 pps	Q- Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 82.70 Kbps 77.62 Kbps 14.52 Kbps	Peak Packet Rate 828 pp: 104 pp: 30 pp: 9 pp: 8 pp: 15 pp:
Site to Site Ferforma DSCP vs Application Business Relevance Traffic Class Q QS ve Relanet Medianet Pretkankt Relanet	10 MB 0 B Nov 14, 641 C Show Total Bytes Number of datasets: 11 Application C critic-static C useene C critic-static C http: C htt	Total Flows Total Bytes 466 1 15 2 2	Total Packe 560 MB 3 MB 966 KB 620 KB 582 KB 109 KB 103 KB	Da ts Avi 729,871 6,256 1,830 570 523 946 958	erage Bit Rate 4.98 Mbps 23.80 Kbps 8.59 Kbps 5.18 Kbps 5.18 Kbps 968.42 bps 916.04 bps	Average Packet Rate 810.97 pps 6.95 pps 0.63 pps 0.63 pps 1.05 pps 1.06 pps 1.06 pps	Q- Peak Bit Rate 5.08 Mbps 557.01 Kbps 128.83 Kbps 82.70 Kbps 77.62 Kbps 13.74 Kbps 13.74 Kbps	Peak Packet Rate 828 pp 104 pp 30 pp 9 pp 8 pp 15 pp 15 pp
Site to Site Performa DSCP vs Application Business Relevance Traffic Class © QSS • Relevance • Network • Network • Network ve ve ve ve As sate • te medule	10 MB 0 B Nev 14, 041 P Shew Total types Number of datasets 11 Application C criteries 20 June 20 20 June	Total Flows Total Bytes 46 1 15 2 2 2 2 2 2	Total Packe 560 M8 3 M8 966 K8 620 K8 582 K8 109 K8 103 K8 103 K8 100 K8	Da ts Avi 729,871 6,256 1,830 570 523 946 958 1,078	erage Bit Rate 4.98 Mbps 2.3.80 Kbps 5.51 Kbps 5.18 Kbps 968.42 bps 916.04 bps 884.45 bps	Average Packet Rate 810.97 pps 6.95 pps 0.63 pps 0.58 pps 1.05 pps 1.05 pps 1.20 pps 1.20 pps	Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 77.62 Kbps 13.74 Kbps 13.76 Kbps	Peak Packet Rate 828 pp: 104 pp: 30 pp: 9 pp 9 pp 8 pp: 15 pp: 15 pp: 15 pp: 17 pp:
Site to Site Ferforma DSCP vs Application Business Relevance Traffic Class © QSS v Relavance reduced reduce	10 MB 0 B Nev K, 64 1 C Show Total Bytes Number of datasets: 11 Application C critrix-static C pop3 C unclassified C unclassified C critrix-static C RTC-AMPS-VDEOD C critrix-static C RTC-AMPS-VDEOD C Critrix-Static C Critrix-Static C RTC-AMPS-VDEOD C Critrix-Static C C Critrix-Static C C C C C C C C C C C C C C C C C C C	Total Flows Total Bytes 466 1 15 2 2	Total Packe 560 MB 3 MB 966 KB 620 KB 582 KB 109 KB 103 KB 100 KB 81 K8	Da 729,871 6,256 1,830 570 523 946 958 1,078 535	erage Bit Rate 4.98 Mbps 23.80 Kbps 5.51 Kbps 5.18 Kbps 968.42 bps 916.04 bps 884.45 bps 722.51 bps	Average Packet Rate 810.97 pps 6.95 pps 0.63 pps 0.63 pps 1.05 pps 1.06 pps 1.20 pps 0.59 pps	Q- Peak Bit Rate 5.08 Mbps 55.701 Kbps 128.83 Kbps 77.62 Kbps 14.52 Kbps 13.74 Kbps 13.74 Kbps 13.26 Kbps 10.83 Kbps	Peak Packet Rate 828 pp 30 pp 9 pp 8 pp 15 pp 15 pp 17 pp 8 pp
Site to Site Performs DSCP vs Application Business Relevance Traffic Class In Network In Network Network Sect Actions Ve eate eate eate hetdule In Performance Per	10 MB 0 B Nov 14, 04.1 C Show Total Bytes Number of datasets: 11 Appletation C curseme C cur	Total Flows Total Bytes 46 1 15 2 2 2 2 2 2	Total Packe 3 M8 3 M8 966 K8 620 K8 582 K8 103 K8 103 K8 100 K8 81 K8 67 K8	Da 729,871 6,256 1,830 570 523 946 958 1,078 535 361	ate 4.98 Mbps 23.80 Kbps 5.18 Kbps 5.18 Kbps 916.04 bps 916.04 bps 884.45 bps 722.51 bps 595.31 bps	Average Packet Rate 810.97 pps 6.95 pps 0.63 pps 0.58 pps 1.05 pps 1.05 pps 1.20 pps 0.59 pps 0.40 pps	Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 77.62 Kbps 13.74 Kbps 13.26 Kbps 13.26 Kbps 13.83 Kbps 8.93 Kbps	
Site to Site Performa DSCP vs Application Business Relevance Traffic Class > QoS Network > Relavance ve As cost R R Hedue Hedue R R	10 MB 0 B Nev K, 64 1 C Show Total Bytes Number of datasets: 11 Application C critrix-static C pop3 C unclassified C unclassified C critrix-static C RTC-AMPS-VDEOD C critrix-static C RTC-AMPS-VDEOD C Critrix-Static C Critrix-Static C RTC-AMPS-VDEOD C Critrix-Static C C Critrix-Static C C C C C C C C C C C C C C C C C C C	Total Rows Total Bytes 46 1 15 2 2 2 2 2 1	Total Packe 560 MB 3 MB 966 KB 620 KB 582 KB 109 KB 103 KB 100 KB 81 K8	Da 729,871 6,256 1,830 570 523 946 958 1,078 535	erage Bit Rate 4.98 Mbps 23.80 Kbps 5.51 Kbps 5.18 Kbps 968.42 bps 916.04 bps 884.45 bps 722.51 bps	Average Packet Rate 810.97 pps 6.95 pps 0.63 pps 0.58 pps 1.05 pps 1.05 pps 1.20 pps 0.59 pps 0.40 pps	Peak Bit Rate 5.08 Mbps 357.01 Kbps 128.83 Kbps 77.62 Kbps 13.74 Kbps 13.26 Kbps 13.26 Kbps 13.83 Kbps 8.93 Kbps	Peak Packet Rate 828 pp: 30 pp: 9 pp: 8 pp: 15 pp: 17 pp: 17 pp: 8 pp:

Expand an application in the table to show devices and right click on a device to select between Graph View and Top Analysis View.

Graph View – generates an Application outbound flow report for all applications and all devices within the system.



Top Analysis View - generates a Top Analysis outbound flow report for the selected device.

					Flow Re	ports						
Q- Type here to filter report	Top Analysis											
Reports	Toprenditysis											
Interface Bandwidth												
	Ton A	Analysis								5m 1h 6h	1d 1w 30d	Custom
Top Analysis	100	, indiana york										
IPs and Ports									te Report			
IPs and Application	11/1	4/16, 04:20:	00 PM to 11/14	/16, 04:35:	00 PM			Exec	ite keport			
All Unique Flows					LAT THE WAY	WHITE PARTY	MARK 1					
▶ Address	Source c19	941APN-212		2	All 1	nterfaces	Q	Numbe	r of flows:	15	cs	V File Result
Applications		DefaultFilterGroup		Outbound	<u>^</u>			Basic	ri		Sorted - Unique	
▶ QoS	Filter *C	JeraultriiterGroup		Outbound	×			Basic	Plow	Time :	sorted - Unique	Plows V
Network												2
Medianet	Search wan	& device = c194	\$1APN-212.test	com & flow.ap	p=cuseeme						×・	<u> </u>
Applications (AVC)	the second se											
▶ Firewall										0,-		
▶ PfR	Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Flow Record Co Bit R	ate	Packet Rate	Src Country	Dst Cou
▶ Wireless	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.59 Mbps	720.08 pp		-
AnyConnect	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.47 Mbps	701.90 pp		-
▶ Ziften	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.58 Mbps	718.99 pp		-
Miscellaneous	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.59 Mbps	720.01 pp		-
Custom Reports	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.59 Mbps	720.05 pp		-
	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2		cuseeme	1	4.58 Mbps	719.92 pp		-
AppDscp	Nov 14, 2016 Nov 14, 2016		10.254.20.88 10.254.20.88	7,648 7,648	10.254.101.2. 10.254.101.2.		cuseeme	1	4.59 Mbps 4.59 Mbps	720.03 pp 720.03 pp		-
asdf	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.59 Mbps 4.55 Mbps	720.03 pp 714.31 pp		-
avc-asr-test	Nov 14, 2016.		10.254.20.88	7,648	10.254.101.2		cuseeme	1	4.54 Mbps	712.16 pp		
banwidth	Nov 14, 2016		10.254.20.88	7.648	10.254.101.2		cuseeme	1	4.56 Mbps	716.40 pp		-
benstest	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.58 Mbps	719.28 pp		-
SKPPort BKPPort	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.58 Mbps	718.86 pp		-
boss45	Nov 14, 2016		10.254.20.88	7,648	10.254.101.2.		cuseeme	1	4.56 Mbps	716.26 pp		-
Boston	Nov 14, 2016	UDP	10.254.20.88	7,648	10.254.101.2.	7,648	cuseeme	1	4.59 Mbps	720.06 pp	5 -	-
^												
Report Actions												
Save												
Save As												
Create												
Create												
Edit												
Delete												
Schedule												
PDF												
Export to CSV												
Export to CSV Help												

Top 10 Application Performance

Top 10 Application Performance Avg Application Delay Image: Control of the second										
Application name	Avg Network Del	Avg Applica 💌 1	Retransmissions	Flows						
rtmpe	0 ms	513 ms	0	14						
unknown	0 ms	504 ms	0	129						
PeopleSoftPa	0 ms	108 ms	262	15						
citrix	86 ms	76 ms	0	15						
▶ ms-wbt	75 ms	75 ms	0	30						
secure-http	6 ms	10 ms	14	3						
▶ ssl	6 ms	10 ms	30	7						
▶ http	2 s	2 ms	865	39						
▶ citrix_	2 ms	2 ms	0	15						
▶ cuseeme	0 ms	0 ms	0	3						

Top 10 Voice/Video Performance

Top 10 Voice/Vid	eo Performance	Jitter ᅌ	
Application name	RTP SSRC	Jitter 🔽 1 Loss E	vents
▶ RTP	1921471849	153.30 s	15,161
PeopleSofl_GL	4080166714	10.10 s	15
▶ RTP-CAMPUS	1347903890	1.00 s	(
PeopleSofl_GL	1347903890	1.00 s	(
▶ RTP-CAMPUS	4080166714	507.78 ms	869
▶ RTP-CAMPUS	1929191128	502.05 ms	(
▶ RTP	1929191128	379.67 ms	24,239
▶ RTP	1699594607	366.16 ms	(
▶ RTP-CAMPUS	1699594607	350.49 ms	(
▶ RTP-CAMPUS	1929191128	256.17 ms	(

Top 10 HTTP Host

HTTP Host	HTTP Hit Count			
cdn.content.prod.cms.msn.com		47	110 KE	
wpad.apn.com		42	106 KE	
wpad.APN.COM		36	59 KE	
fonts.googleapis.com	n 32			
www.pandora.com		29	8 ME	
mail.office365.com		29 14		
www.ebay.com		29	5 ME	
www.cisco.com		29	2 ME	
www.gotomeeting.com		28	26 KB	
www.salesforce.com		25	22 KE	

IP SLA Dashboard

The IP SLA Dashboard presents a snapshot of the IP Service Levels that are active within the network, it lists the Thresholds in the past Hour, 6 Hours, or 1 day. It displays the Overall Health, the last 100 Alerts, Trending of the Alerts and type of Alerts. Within each widget the order can be displayed from Highest to Lowest, or vice-a-versa by clicking on the title bar within each widget.



Right-clicking in any of the widgets will give you the option to view the Pre- and Post-Policy graphs for the policy selected.

Click on the + sign next to Warning Thresholds to customize the dashboard parameters. This is a Warning message specific to the IP SLA technology and does not generate alerts in the LiveNX system.

Warning	[hre	sholds				U	pdate Dashboard
Report a	Wa	rning W	hen:				
Video				Voice		Data Ap	plications
Latency	>	1,000	ms	MOS	< 3.5	Latency	> 1,000 ms
Loss	>	1	packets				
Jitter	>	100	ms				

- Video test types include telepresence, IP TV, and VSC. Latency, loss, and jitter values are configurable, allowing you to fine-tune the test to your needs.
- The MOS score is used to determine health.

 Data applications are a collection of IP SLA test types, including, DNS, DHCP, HTTP, FTP, PATH_ECHO, UDP_ECHO, and ICMP_ECHO tests. Latency is the most important value for these tests.

The overall health chart displays a running count of the health values of each test attempt across all devices in the application. Any records that exceed the thresholds defined in the Warning Thresholds section of the IP SLA dashboard will appear as a warning.



Right click on the bar chart to select most Successful/Warnings/Errors Report and save an image.

IP SLA Overall Health report: depending on the bar chart selected, LiveNX generates an IP SLA Overall Health report sorted by Normal in highest to lowest order if you right clicked on the Normal bar, Warning in highest to lowest order if you right clicked on the Warnings bar, and Errors in highest to lowest order if you right clicked on the Errors bar.

ports	TD SI A	Overa	ll Health								
Overall Health	IT SEA		in meantin								
Overall System Health	11/14/16	02.40.04 BM	to 11/14/16, 04:40:04 P								
Single Test Time Series											
Single Type Health	1h 6h 1d										
Video Operation Threshold				ALL REAL OF							
	Warning Th	resholds		Execute Report							
Video Operation Time Serie											
stom Reports											
health	ld Type	Tag	Device Destination	Avg Latency (Avg Jitter (Avg	Loss (pack A	vg M N	⇒1 Warn	ng Errors	Record	ls
💁 Test - Test	1 Jitter		cat3850APN 10.254.254.212	0.00	1.13	0.00	4.06	30	0	0	3
Test-Test	2 Jitter		c1811-ES-1 192.0.1.2	71.66	225.21	0.00	4.06	14	0	0	1
-	76 DNS	DNS Server 2	Cisco6509_1 mail.google.com	1.00				1	0	0	
	9 ICMP Echo	Layer 2 Test	Cisco6509_1 30.30.10.5	721.00				1	0	0	
	10 ICMP Echo	Layer 2 Test	Cisco6509_1 30.30.10.5	811.00				1	0	0	
	77 DNS	DNS Server 2	Cisco6509_1 mail.google.com	506.00				1	0	0	
	69 DNS	DNS Server 1	Cisco6509_1 mail.google.com	282.00				1	0	0	
	1 ICMP Echo	Layer 2 Test	Cisco6509_1 30.30.10.5	6,826.00				0	1	0	
	4 Jitter		c1811-ES-1 10.0.0.1	106.08	242.86	0.00	2.85	0	14	1	1
		Layer 2 Test	Cisco6509_1 30.30.10.5	1,676.00				0	1	0	
		DNS Server 2	Cisco6509_1 mail.google.com	1,161.00				0	1	0	
		DNS Server 2	Cisco6509_1 mail.google.com	6,267.00				0	1	0	
		Layer 2 Test	Cisco6509_1 30.30.10.5	1,429.00				0	1	0	
		Layer 2 Test	Cisco6509_1 30.30.10.5	8,002.00				0	1	0	
	5 Jitter		c1811-ES-1 10.0.12.1	99.65	220.86	0.00	2.85	0	14	2	1
		DNS Server 2	Cisco6509_1 mail.google.com	6,507.00				0	1	0	
		Layer 2 Test	Cisco6509_1 30.30.10.5	1,558.00				0	1	0	
1	71 DNS	DNS Server 1	Cisco6509_1 mail.google.com	5,564.00				0	1	0	
rt Actions		Layer 2 Test	Cisco6509_1 30.30.10.5	2,400.00				0	1	0	
	1 Jitter		c1811-ES-1 192.168.11.2	94.49	223.31	0.00	2.85	0	13	4	1
		DNS Server 1	Cisco6509_1 mail.google.com	2,233.00				0	1	0	
As		Layer 2 Test	Cisco6509_1 30.30.10.5	11,891.00				0	1	0	
		DNS Server 1	Cisco6509_1 mail.google.com	6,087.00				0	1	0	
	3 Jitter		c1811-ES-1 192.0.1.1	96.76	237.07	0.00	2.85	0	14	0	1
lule		Layer 2 Test DNS Server 1	Cisco6509_1 30.30.10.5 Cisco6509_1 mail.google.com	5,149.00 12,573.00				0	1	0	
	73 DNS	DNS Server 1	CISC06509_1 mail.google.com	12,575.00				0	1	0	
rt to CSV											

Save image: create a .png file of the bar chart for saving.

Last 100 Alerts

This table displays the last 100 IP SLA alerts that have appeared in LiveNX. The alerts are configured in the IP SLA triggers section in the Configure Alerts dialog box.

Time	Severity	Device	Туре	Details
2013/06/06 02:	Warning	OSPF-POD-172	IP SLA error	Test ID - 43; E
2013/06/06 02:	Warning	OSPF-POD-172	IP SLA error	Test ID - 29; E
2013/06/06 02:	Warning	OSPF-POD-172	IP SLA error	Test ID - 21; E
2013/06/06 02:	Warning	c2821-185	IP SLA error	Test ID - 8; Er
2013/06/06 02:	Warning	c2821-185	IP SLA error	Test ID - 7; Er
2013/06/06 02:	Warning	c2821-185	IP SLA error	Test ID - 6; Er
2013/06/06 02:	Warning	OSPF-POD-173	IP SLA error	Test ID - 4; Er
2013/06/06 02:	Warning	CT-RTR1	IP SLA error	Test ID - 12; E
2013/06/06 02:	Warning	CT-RTR1	IP SLA error	Test ID - 10; E
2013/06/06 02:	Warning	CT-RTR1	IP SLA error	Test ID - 8; Er
2013/06/06 02:	Warning	CT-RTR1	IP SLA error	Test ID - 6; Er
		:		

Trending

The trending section displays a time-series chart depicting the aggregated health values for all tests. Right click on the chart to select among Reset Zoom, Most Successful/Warnings/Errors report, Save Image.



Reset Zoom – left click and drag to zoom the trending chart to the area selected. Use the Reset Zoom to return to the default view.

Most Successful, Warnings or Errors Report— depending on the color selected (green, yellow or red), LiveNX generates an IP SLA Overall Health report sorted by Normal in highest to lowest order if you right clicked in the green area, Warning in highest to lowest order if you right clicked in the yellow area, and Errors in highest to lowest order if you right clicked in the red area.

Test Types

The Test Types table displays the health values for all user-configured systems.

Normal	Warning	Errors
3,749	0	22,559
070		15,70
Mo	ost Successful Report	180
60	0	120
0	0	30
0	0	6
0	0	6
	60 0	Most Successful Report 60 0 0 0 0 0

Highlight a row and then right-click on an entry in the Normal, Warning or Errors cell to generate an IP SLA Single Type Health report sorted by the most Normal, the most Warnings or the most Errors, respectively.

pe here to filter repor		_		IP SLA Repor		_	_					
orts		Single	Туре Не	alth								
Sverali Healui		Unigic	i ype ne									
Overall System Health	1/14/16, 0	3:41:16 PM	to 11/14/16, 0	4:41:16 PM								
Single Test Time Series	1b 6 b 1d	Lw 30d Custo										
single Type nearth	Li on iu .											
/ideo Operation Threshold	All Devices		0		ICMP Echo							
/ideo Operation Time Serie	, an betteeb				TCHI ECHO							
tom Reports												
	Warning Thr	resholds			Execute Report							
Test - Test												
Test-Test					Latency (ms)							-
	ld Type	Tag	Device	Destination		Avg	Max	Normal #1	Warning	Errors	Records	f.
	9 ICMP Echo	Layer 2 Test	Cisco6509_14	30.30.10.5	721.00	721.00	721.00	1		0	0	
	10 ICMP Echo	Layer 2 Test	Cisco6509_14	30.30.10.5	811.00	811.00	811.00	1		0	0	
	1 ICMP Echo	Layer 2 Test	Cisco6509_14		6,826.00	6,826.00	6,826.00			1	0	
	2 ICMP Echo		Cisco6509_14		1,558.00	1,558.00	1,558.00			1	0	
	3 ICMP Echo		Cisco6509_14		11,891.00	11,891.00				1	0	
		Layer 2 Test	Cisco6509_14		5,149.00	5,149.00	5,149.00			1	0	
		Layer 2 Test Layer 2 Test	Cisco6509_14 Cisco6509_14		1,429.00 1,676.00	1,429.00	1,429.00			1	0	
		Layer 2 Test	Cisco6509_14		8,002.00	8,002.00	8,002.00			1	0	
		Layer 2 Test	Cisco6509_14		2,400.00	2,400.00				1	0	
	o temp ceno	Layer 2 Test	CISC00309_14	50.30.10.5	2,400.00	2,400.00	2,400.00	0		1	U	
rt Actions												
As												
2												
lule												
t to CSV												
t to CSV												

System Tests

The System Tests table displays the health values for all user-configured system tests.

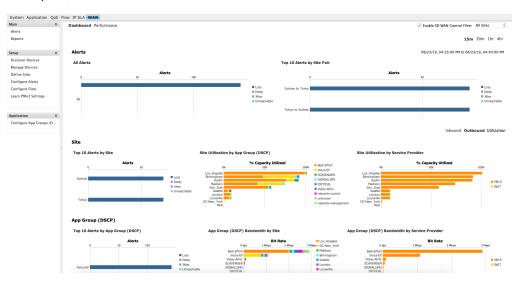
System Test	is		
System Test	Normal T	Warning	Errors
daily test		0	Aost Warnings Report

Highlight a row and then right-click on an entry in the Normal, Warning or Errors cell to generate an IP SLA System Test Health report for the selected system test sorted by the most Normal, the most Warnings or the most Errors, respectively.

1	_		_	_		IP SLA R	eports	_		_	_	_		_	_		
Q- Type here to filter repoi						CARLES IN COLUMN											
	10/15 1h 6h	/16, 1d ystem	05:4: 1w 3 Tests	2:43 P 80d Cu	M to 11/14	tem Hea /16, 04:42:43		eport									
C Test-Test	Name	ID	Туре	Tag	Device	Destination	Latency (ms) Min Avg	Max	Jitter (ms) Min Avg	Max	Loss (Min	packets) Avg	Max		Warn I	Errors	Reco
Report Actions Save																	
Save As Delete Schedule																	
PDF Export to CSV																	
Help																	

WAN Dashboard

The WAN Dashboard presents a snapshot of the state of Per Flow Routing that is active within the Wide Area Network (WAN). It displays Alerts group by all alerts and by Site pairs, by Site, Application Group, Site Utilization, by App group (Bandwidth by Site, by Service Provider), by Service Provider (Utilization, by site).



Configure App Groups

Click on a chart title within the dashboard to automatically generate a LiveNX PfR flow report. Mouse over the bar of interest to get tool tips, including the value of each segment in a stacked bar.

The PfR dashboard charts alerts, site, application group and service provider statistics in either the Inbound or Outbound direction. Click on either Inbound or Outbound to select the direction; default is Outbound. The charts compute statistics for the last 15 minutes, 30 minutes, 1 hour or 4 hours. Click on 15m, 30m, 1h or 4h to select the duration. The date and time values below the duration selection indicate the start and end times of the charted data.

There are two charts in the Alerts section of the PfR Dashboard: All Alerts and Top 10 Alerts by Site Pair. PfRv3 supports four alerts: Loss, Delay, Jitter and Unreachable.

All Alerts charts the total number of alerts for the system in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts.





Top 10 Alerts by Site Pair charts the top 10 site pairs that generate the largest number of alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. The sites are device level attributes that are user-defined in the Device/Interface tree view. Defining sites is described – BasicSetup.

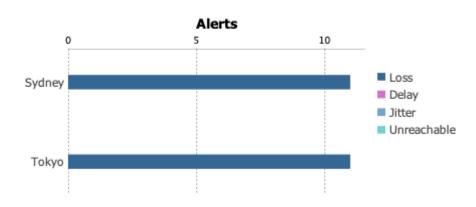
Top 10 Alerts by Site Pair



There are three charts in the Site section of the PfRv3 Dashboard: Top 10 Alerts by Site, Site Utilization by Application Group, and Site Utilization by Service Provider.

Top 10 Alerts by Site

Top 10 Alerts by Site charts the top 10 sites generating the most alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. The sites are device level attributes that are user-defined in the Device/Interface tree view.

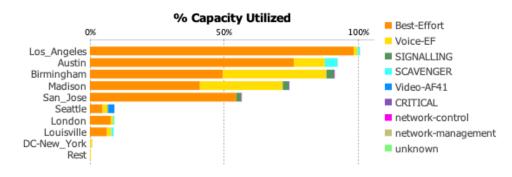


Top 10 Alerts by Site

Site Utilization by Application Group

Site Utilization by Application Group charts the capacity of each site, based on the application groups. The capacity is charted in a stacked bar chart format, color-coded to indicate the applications used by

that site. Sites are device level attributes and capacities are interface level attributes that are user-defined in the device/interface tree view. Application groups are attributes that are user-defined in the Configure Application Groups section of the PfRv3 Dashboard.

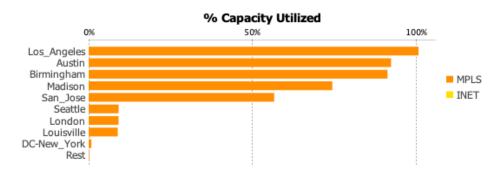


Site Utilization by App Group (DSCP)

Site Utilization by Service Provider

Site Utilization by Service Provider charts the capacity of each site, based on the service provider. The capacity is charted in a stacked bar chart format, color-coded to indicate the service providers associated to that site's interfaces. Sites are device level attributes, while capacities and service providers are interface level attributes that are user-defined in the device/interface tree view.

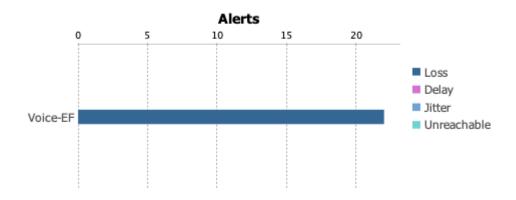
Site Utilization by Service Provider



There are three charts in the Application Group section of the PfRv3 Dashboard: Top 10 Alerts by Application Group, Application Group Bandwidth by Site and Application Group Bandwidth by Service Provider.

Top 10 Alerts by Application Group

Top 10 Alerts by App Group (DSCP)

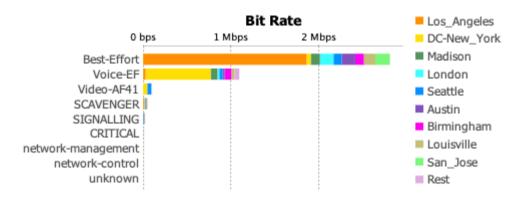


Top 10 Alerts by Application Group charts the top 10 application groups generating the most alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. The application groups are attributes that are user-defined in the Configure Application Groups section of the PfRv3 Dashboard.

Application Group Bandwidth by Site

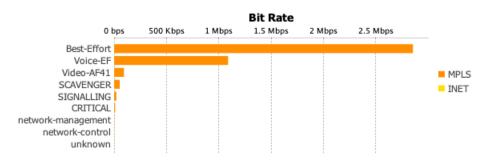
Application Group Bandwidth by Site charts the highest bandwidth application groups. The application groups are charted in a stacked bar chart format, color-coded to indicate the various sites associated with the application groups. The sites are device attributes that are user-defined in the Device/ Interface tree view and application groups are attributes that are user-defined in the Configure Application Groups section of the PfRv3 Dashboard.

App Group (DSCP) Bandwidth by Site



Application Group Bandwidth by Service Provider

Application Group Bandwidth by Service Provider charts the highest bandwidth applications by application group. The application groups are charted in a stacked bar chart format, color-coded to indicate the various service providers associated with the application groups. The service providers are interface attributes that are user-defined in the Device/Interface tree view and application groups are attributes that are user-defined in the Configure Application Groups section of the PfRv3 Dashboard.



App Group (DSCP) Bandwidth by Service Provider

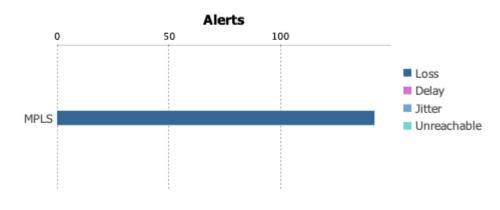
There are three charts in the Service Provider section of the PfRv3 Dashboard: Top 10 Alerts by Service Provider, Service Provider Utilization by Application Group and Service Provider Utilization by Site.

Top 10 Alerts by Service Provider

Top 10 Alerts by Service Provider charts the top 10 service providers generating the most alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. Service providers are interface level attributes that are user-defined in the Device/Interface tree view.

Service Provider

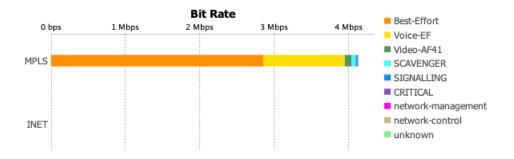
Top 10 Alerts by Service Provider



Service Provider Utilization by Application Group

Service Provider Utilization by Application Group charts the percent of capacity utilized by service provider. The utilized capacity is charted in a stacked bar chart format, color-coded to indicate the application groups associated with that service provider. Capacities and service providers are interface level attributes that are user-defined in the Device/Interface tree view and application groups are attributes that are user-defined in the Configure Application Groups section of the PfRv3 Dashboard.

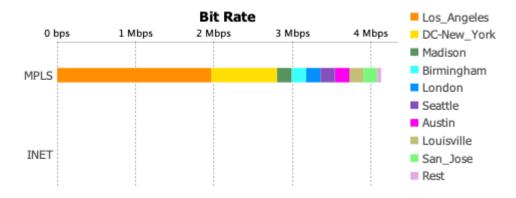
Service Provider Bandwidth by App Group (DSCP)



Service Provider Utilization by Site

Service Provider Utilization by Site charts the percent of capacity utilized by service provider. The utilized capacity is charted in a stacked bar chart format, color-coded to indicate the sites associated with that service provider. Sites are device attributes while capacities and service providers are interface attributes that are user-defined in the Device/Interface tree view.

Service Provider Bandwidth by Site



Learn PfRv3 Settings

The Learn PfRv3 Settings feature allows users to easily setup the PfR/IWAN semantics to monitor Performance. These Settings will allow LiveNX to populate the WAN/PfR dashboard. The settings learned are as follows:

- PfRv3 devices including master controller and border router loopback IP address at each site
- Sites
- WAN Tunnels
- Capacities of the WAN Tunnels
- Service Providers
- Site IP Addresses

System Application	QoS	Flow IP SLA	WAN	
Main	*			
Alerts				
Reports		Site		
Setup	*	Top 10	Alerts by Site	
Discover Devices				
Manage Devices			0 10	
Define Sites				
Configure Alerts		Sydney	/	_
Configure Flow				
Learn PfRv3 Settings				
		Tokyo		

Once selected, the dialog window will appear. Select the appropriate time range for LiveNX to learn the settings for all the sites in your system.

• •	Learn PfRv3 Settings								
PfR Learn Sit	e Details								
LiveNX will attempt to learn your existing PfR site details by analyzing flow data being sent. All PfR devices of an existing site must be monitored by and exporting PfR flows to LiveNX in order to learn the details of that site.									
1Hour 1Day 1V	Veek Custom								
	Learn Cancel								

The Learning process will analyze flow data being sent by the PfR enabled devices in the network. Options include 1 hour, 1 day, 1 week and a Custom time range. Once the process completes you will see the sites that were learned (including the Loopback IP addresses of the Master Controller (MC) associated with each site).

			Site Name:	
lote	Site Name	Loopback IP	Tokyo	
	Tokyo Sydney	10.0.0.103 10.0.0.104	Site IPs:	
	-,,		10.0.0.101	
			10.0.0102	
			10.0.0.103	
			20.1.1.0/24 21.1.1.0/24	
			21.1.1.0/24	
			Devices:	
			Master Controller:	
			Hostname Loopback IP	
			WAN-DC-MC 10.0.0103	
			Border Routers:	
			Hostname Loopback IP WAN Interfa Service Pro Input Capac Output	t Cap.
			WAN-BR_I 10.0.0.101 Tunnel101 INET 10000 10000	
				<i>.</i>
			Apply	/ Site

The Note Column Identifies the Following

- NEW: New site Learned during this process
- UPDATES: New site IP address prefixes were learned
- LO_IP_ONLY: Only the Loopback IP address of the sire was learned
- GRP_SITE: If this appears please remove the grouping (refer to *Manage Performance Groups and Application Groups* on page 248)

Details Displayed Are

- Site Name (editable): The site name is automatically populated by LiveNX, and will be the DNS name associated with the MC's Loopback IP address or the hostname.
- Site IP's (editable): The loopback IP addresses of the PfRv3 MC and BR9 per site will be populated here, along with the learned IP prefixes for user traffic per site.
- Master Controller: Details of the MC including the hostname and IP address of the MC
- Border Routers: Hostname, Loopback IP, WAN interfaces, service providers and capacities per WAN link
- To apply the settings for a site click Apply Site and to apply for ALL sites click Apply
- The learned site settings can now be confirmed in the expanded device view

IP Address	Node	Label	Input Capac	Output Cap	WAN	Service Pr	Site	Site IP
							Birmingham DC-New_York	10.100.51.0/24,192.158.102.0/24 192.166.10.0/24,192.168.15.0/24
							Los_Angeles	192.168.107.0/24
10.100.51.35 22.1.1.254 10.0.0.104 172.16.1.1 172.16.2.1	Local		5.0 Mbps 10.0 Mbps	5.0 Mbps 10.0 Mbps		MPLS INET	Sydney	10.0.0.104,22.1.1.0/24
11.11.11.3 21.1.1.254	Local		10.0 Mbps	10.0 Mbps		INET	Токуо	10.0.0.101,10.0.0.102,10.0.0.103,20.1.1.0/24,21.1.1.0/24
10.100.51.31 11.11.11.2 20.1.1.254	Local				8		Токуо	10.0.0.101,10.0.0.102,10.0.0.103,20.1.1.0/24,21.1.1.0/24
10.100.51.30 10.100.51.20	Local		510 Mpp3	2.0 Mbp3	Ĩ		Токуо	10.0.0.101,10.0.0.102,10.0.0.103,20.1.1.0/24,21.1.1.0/24
	10.100.51.35 22.1.1.254 10.0.0.104 172.16.1.1 172.16.2.1 11.11.1.3 21.1.1.254 11.11.1.3 21.1.1.254 11.11.1.2 20.1.1.254 11.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.1.1.2 20.1.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2 20.1.254 11.1.2	10.100.51.35 Local 22.1.1.254 100.0.104 172.16.1.1 172.16.2.1 10.100.51.32 Local 11.11.11.3 21.1.1254 10.100.51.31 Local 11.11.11.2 20.1.1254 10.100.51.30 Local 10.100.51.30 Local 10.100.51.25 Local	10.100.51.35 Local 22.1.254 10.00.104 172.16.1. 172.16.1. 172.16.2.1 10.100.51.32 Local 11.11.1.3 21.1.254 10.100.51.31 Local 11.11.1.2 20.1.254 10.100.51.30 Local 10.100.51.20 Local	10.100.51.35 Local 22.1.1254 100.0.0104 172.16.11 5.0 Mbps 172.16.21 10.0 Mbps 10.100.51.32 Local 11.11.11.3 21.1.1254 10.0 Mbps 10.100.51.31 Local 11.1.11.12 20.1.1254 5.0 Mbps 10.100.51.30 Local 10.100.51.20 Local	10.100.51.35 Local 22.1.254 10.0.0.104 172.16.1.1 5.0 Mbps 5.0 Mbps 172.16.2.1 10.0 Mbps 10.0 Mbps 10.100.51.32 Local 11.11.1.3 21.1.254 10.100.51.31 Local 10.100.51.30 Local 10.100.51.30 Local 10.100.51.20 Local	10.100.51.35 Local 22.1.1.254 10.0.0.104 172.16.1.1 172.16.2.1 10.100.51.32 Local 11.11.11.3 21.11.254 10.25.13 Local 10.100.51.31 Local 11.11.11.2 20.11.254 10.100.51.30 Local 10.100.51.20 Local 10.100.51.21 Local	10.100.51.35 Local 22.1.254 10.0.0.104 172.16.1.1 172.16.1.1 10.100.51.32 Local 11.11.11.3 21.11.254 10.25.45 10.0 Mbps 10.0 Mbps 2 INET 10.100.51.31 Local 11.11.11.2 20.1.254 10.100.51.30 Local 10.100.51.30 Local 10.100.51.20 Local	Birmingham DC-New_York 10.100.51.35 Local 22.1.254 Sydney 10.00.51.35 Loca 172.16.1 5.0 Mbps 5.0 Mbps 172.16.1 10.0 Mbps 10.0 Mbps 11.11.11 11.11 Tokyo 11.11.12 10.0 Mbps 10.0 Mbps 11.11.12 Tokyo INET 10.100.51.30 Local Tokyo 11.11.12 S.0 Mbps MPLS 10.100.51.30 Local Tokyo 10.100.51.30 Local Tokyo 10.100.51.21 Local Tokyo

• The WAN-PfR dashboard will now also populate statistics.

Note When changes are made to the dashboard the update will finish in approximately 10 minutes.

CHAPTER 4

Alerts and Notifications

In this chapter:

About Alerts and Notifications

LiveNX supports real-time monitoring of the network and generates alerts to the user when anomalous network conditions occur. LiveNX creates visual changes in the system view that affect the status icons for devices and interfaces, and keeps a running log of all alerts generated by the system. To prevent false warnings from occurring, LiveNX provides the user with the flexibility to define the thresholds that define the anomalous network condition.

View Alerts

LiveNX displays all alerts in a real-time fashion. Go to Tools > View Alerts.

Time 🔺	Severity	Device	Group	Alert Type	Details
019/08/30 04:15:3	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - http; Source IP add
019/08/30 04:15:3	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - DemoServer; Sourc
019/08/30 04:15:4	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - secure-pop3; Sour
019/08/30 04:15:4	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - unknown; Source IP
2019/08/30 04:15:4	Alert	SE-LiveWire-NY	Flow	High network delay	Application name - http; Source IP add
2019/08/30 04:15:4	Alert	RTR-DC-CORE	Flow	High network delay	Application name - http; Source IP add
2019/08/30 04:15:4	Alert	SE-LiveWire-NY	Flow	High network delay	Application name - DemoServer; Sourc
2019/08/30 04:15:4	Alert	RTR-DC-CORE	Flow	High network delay	Application name - DemoServer; Sourc
019/08/30 04:15:4	Alert	RTR-DC-CORE	Flow	High network delay	Application name - secure-pop3; Sour
2019/08/30 04:15:4	Alert	SE-LiveWire-NY	Flow	High network delay	Application name - secure-pop3; Sour
2019/08/30 04:15:4	Alert	RTR-DC-CORE	Flow	High network delay	Application name - unknown; Source IP
2019/08/30 04:15:4		SE-LiveWire-NY	Flow	High network delay	Application name - unknown; Source IP
2019/08/30 04:15:4	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - ms-office-web-app
2019/08/30 04:15:4		RTR-DC-MPLS	Flow	High network delay	Application name – google-services; S
2019/08/30 04:15:4	Alert	RTR-DC-MPLS	Flow	High network delay	Application name - outlook-web-servic
2019/08/30 04:15:4		RTR-DC-CORE	Flow	High network delay	Application name - ms-office-web-app
2019/08/30 04:15:4		RTR-DC-CORE	Flow	High network delay	Application name – google-services; S
2019/08/30 04:15:4		SE-LiveWire-NY	Flow	High network delay	Application name - Office WebApp; So
2019/08/30 04:15:4		SE-LiveWire-NY	Flow	High network delay	Application name – google-services; S
2019/08/30 04:15:4		SE-LiveWire-NY	Flow	High network delay	Application name - outlook-web-servic
2019/08/30 04:15:4		RTR-DC-CORE	Flow	High network delay	Application name - outlook-web-servic
2019/08/30 04:15:4		SE-LiveWire-NY	Flow	Blacklisted NetFlow address	Blacklisted address - 192.168.107.11
2019/08/30 04:15:4		RTR_Austin	Routing	Routing Adjacency State Change	Protocol type - EIGRP; Neighbor addre
2019/08/30 04:15:4		RTR_Louisville	QoS	Class dropped rate	Interface name – GigabitEthernet2; Int
2019/08/30 04:15:4		SE-LiveWire-LA	Flow	Blacklisted NetFlow address	Blacklisted address - 192.168.107.11
2019/08/30 04:15:4		RTR_Seattle	QoS	Class dropped rate	Interface name – GigabitEthernet2; Int
2019/08/30 04:15:4		RTR_Seattle	QoS	Class dropped rate	Interface name – GigabitEthernet2; Int
2019/08/30 04:15:4		RTR_LosAngeles	IP SLA	Low MOS score	Test ID - 1; Threshold - less than or e
2019/08/30 04:15:4		CS-C3850-23-31	Interface Up/Down		Interface name – GigabitEthernet1/0/1
2019/08/30 04:15:4		CS-C3850-23-31	Interface Up/Down		Interface name – GigabitEthernet1/0/2
2019/08/30 04:15:4	Warning	CS-C3850-23-31	Interface Un/Down	Interface down	Interface name – GigabitEthernet1/0/3
only the last 100 alerts	are shown				
Bring this window t	o the front	when a new alert is received			
• • • • • • • • • • • • • • • • • • •					
Beep when a new al	ert is recei	vea			
			Clear list	Export list	Historical search Configure alerts

The In-Application Alerts window retains the most recent 100 alerts and displays them with the most recent at the top of the window. Alerts no longer pertinent can be removed by selecting the alerts and either pressing the Delete key or right clicking and choosing Remove Selected Alerts. Fields are:

- Time time of the alarm
- Severity choices are Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug. Default is Warning (severity choices are covered in the following Configure Alerts section)
- Device device name
- Alert Type alert type definitions and thresholds are covered in the following Configure Alerts section
- Details provides additional details about the alert including cleared status, interface name, and threshold violations.

Enable the check box to bring the window to the front when a new alert is received or to beep when a new alert is received. The default for both is disabled.

- Clear List clicking on this button immediately clears the In-Application Alert window
- Export List allows the user to store the alert information in a .csv format
- · Historical Search provides the user with historical and sorting capability for the alerts
- · Configure Alerts allows user-defined thresholds and alert severity definitions

Both the View Alerts and Historical Alerts (see next section) can drill down to a time series report specific to that individual alert. In order to access the report, right-click on the alert in question and select Open Report. A time series report encompassing the previous and next thirty minutes from the time of the alert will be generated.

Historical Alerts

LiveNX supports user-defined alert filtering on the In-Application Alerts. Click on Tools > View Alerts and click on Historical search.

2019/08/30 04:17:2	Alert	AppleFastLane-4331	Flow	High network delay
2019/08/30 04:17:2	Alert	•••	Flow	High retransmission count
2019/08/30 04:17:2	Warning	WAN-MPLS-CORE	Device Config Chan	Running config may have changed
2019/08/30 04:17:2	Alert		Flow	High retransmission count
2019/08/30 04:17:3	Alert	RTR-DC-MPLS	Flow	Blacklisted NetFlow address
2019/08/30 04:17:3	Warning	RTR Austin	Device Config Chan	Running config may have changed
2019/08/30 04:17:3	Warning			Class dropped rate
2019/08/30 04:17:3	Alert	RT Open Report		High retransmission count
2019/08/30 04:17:3	Warning	RT Drill Down on Specific Flow	/ 🕨 e Config Chan	Running config may have changed
2019/08/30 04:17:3	Warning	RT		Class dropped rate
2019/08/30 04:17:3	Alert	RT × Remove Selected Alerts		High retransmission count
2019/08/30 04:17:3	Warning	WAN-DC-MC	Device Config Chan	Running config may have changed
2019/08/30 04:17:3	Alert	RTR-DC-CORE	Flow	Blacklisted NetFlow address
2019/08/30 04:17:3	Alert	SE-LiveWire-LA	Flow	High retransmission count
2019/08/30 04:17:4	Alert	RTR LosAngeles	Flow	Blacklisted NetFlow address
2019/08/30 04:17:4	Warning		QoS	Class dropped rate
2019/08/30 04:17:4	Warning	-		Interface down
2010/08/30 04-17-4	Warning		Interface IIn /Down	Interface down

LiveNX supports five filter types; each is independently enabled or disabled. Default is disabled for all types except time, which is defaulted to the last hour since the dialog was opened. If no filters are selected, all results are returned.

- Filter by Time create a time range to filter the alerts using the Start Time/ End Time dialog boxes
- Filter by Device filter the alerts by using the drop-down menu to list only the desired device
- Filter by Alert Type filter the alerts by selecting only an alert type using the drop-down menu
- Filter by Severity filter the alerts by selecting one of the eight available severity labels. There is an additional option. Include Higher Priorities that will include all priorities above the selected severity level (i.e. If WARNING is selected, alerts of WARNING, ERROR, CRITICAL, ALERT and EMERGENCY severity will also be returned).
- Maximum Number of Results limit the number of alerts viewed by selecting the drop-down for 100, 200, 500, 1000, 10,000 or 100,000 alerts. Default is 100.

Select Execute to return the desired historical search.

Helpful Tip: If the maximum number of results is reached for any query, narrow the scope and re-execute the query. The alerts returned from a query are not ordered and thus the list may be missing key alert values.

Use the magnifying glass and the adjacent text box to further filter the alerts via alphanumeric searches. This search bar has a range of options ranging from searching case sensitive to only searching for specific columns. Click on the magnifying glass to see all possible filters.

Note This search only filters the list of alerts gathered, because of the desired filtering.

The current list of alerts can be exported in .csv format by right-clicking on any cell and selecting Export Data.

Configure Alerts

Alert thresholds and severity levels are user-configured with the Configure Alerts dialog box. Go to Tools > Configure Alerts or Tools > View Alerts and click on the Configure alerts button at the bottom of the page.

LiveNX supports eight types of alerts and notifications: Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug. Default is Warning.

Each alert can be enabled by clicking on the check box and using the dropdown to select the desired Alert type.

Device/QoS Triggers

			Configure Alerts			
Device	/QoS Triggers	Flow Triggers	IP SLA Triggers	Routing Triggers	LAN Triggers	►
Generat	e an alert when					
Device	Down					
	Warning ᅌ	A device becomes	unavailable			
CPU ar	nd Memory					
	Warning \$	A device's CPU usa	ge reaches or exceed	s (>=) 80 %		
	Warning \$	A device's memory	usage reaches or ex	ceeds (>=) 90 %		
Device	e Config Change a	nd Access				
	Warning ᅌ	The running config	g changed time is late	er than the startup conf	ig changed time	
	Warning ᅌ	Commands are ser	nt to a device using th	ne monitor-only CLI cre	edentials	
	Warning ᅌ	The device configu	ration has been chan	ged by LiveNX		
Interfa	ce Errors					
	Warning ᅌ	An interface becor	nes unavailable			
	Warning \$	An interface has e	rrors (CRC, Frame, Ov	errun, Ignore, Abort)		
QoS D	rops					
Confi	guring the followi	ing alert triggers wil	l affect the drop statu	us for devices and inter	faces.	
	Warning \$	Interface drop rate	exceeds (>) 2,500.	000 pps		
	Generate eve	ents only for selecte	d interfaces			
	Warning ᅌ	Class drop rate ex	ceeds (>) 1.000	Kbps		
	Warning ᅌ	Class-default drop	o rate exceeds (>) 1	500.000 Kbps		
L						
Help				C	ancel Of	K

Device Down

- The device alert is logged in the In-Application Alerts window and increments the Device Up/ Down Alert count in the System Dashboard when the device SNMP polling status changes between responsive and unresponsive.
- Default for the Device Down alert trigger is disabled.

CPU and Memory

- The values in the CPU and memory thresholds are editable only if that alert is enabled (check box is checked).
- These alerts are logged in the In-Application Alerts window and increment the Device CPU/ Memory Alert count in the System Dashboard when the Device CPU or memory usage state exceeds the defined threshold. The count is also incremented when the CPU or memory usage state falls within the defined threshold.

- The device alerts (turns red) in the System Tree View and the Topology View if either the device's CPU or memory alert threshold is exceeded and the alert is enabled.
- Default for the CPU and Memory Device alert triggers are enabled and thresholds set at 80%.

Config Change and Access

- The config change alert is logged in the In-Application Alerts window and increments the Device Config Change Alert count in the System Dashboard when the device's running config changed time is more recent than the startup-config changed time.
- The commands sent by monitor only credentials alert is triggered whenever the system uses the monitor only credentials if that was specified for a device and these credentials are used to send commands to the device.
- The device configuration alert is logged in the In-Applications Alerts window and increments the Device Config Change Alert count in the System Dashboard when any device's configuration is changed by LiveNX. The alert contains the device name, the username and the commands sent to the device.
- Default for the Config Change alert triggers is disabled.

Interface

- The interface unavailable alert is logged in the In-Application Alerts window and increments the Interface Up/Down Alert count in the System Dashboard when the interface SNMP polling status changes between responsive and unresponsive.
- The interface errors alert is logged in the In-Application Alerts window when the interface generates CRC, frame, overrun, ignore or abort errors.
- Default for the interface error triggers is disabled.

QoS Drops

- The values in the Interface drop, Class drop and Class-default drop thresholds are editable only if that threshold is selected. Note that the Interface drop rate is in packets per second, while the Class drop and Class-default drop rates are in Kilobits per second (Kbps).
- Click on the Generate events only for selected interfaces check box to trigger the interface drop alerts only on the interfaces selected during the Add or Discover Device process. Default for the selected interfaces check box is disabled.
- The status icons for devices and interfaces will change only if the threshold desired is enabled (check box is checked).
- The QoS alert is logged in the In-Application Alerts window and increments either the Interface drop, Class drop rate or Class-default drop rate count when those respective rates exceed the user-defined rates.
- Default for all QoS alert triggers is enabled. Default for Interface drop rates; Class drop rates and Class-default drop rates is 0.

Flow Triggers

To configure alerts in the Flow technology, go to Tools > Configure Alerts > Flow Triggers tab.

Device	e/QoS Trigg	ers	Flow Triggers	IP SLA Triggers	Routing Triggers	LAN Triggers
	e an alert w	hen				
Flow						
	Alert	\$	The endpoint of ar	observed flow is a bla	acklisted address	
Media	net					
	Alert	\$	Media loss event o	ccurred		
	Alert	٢	Media packet drop	ped by router		
	Alert	٢	Media min jitter re	aches or exceeds (>=)	150	ms
	Alert	٢	Media max jitter re	aches or exceeds (>=)	150	ms
	Alert	٢	Media mean jitter i	reaches or exceeds (>=	=) 500	ms
	Alert	٢	Media bit rate reac	hes or exceeds (>=)	15,000	kbps
	Alert	٢	Media packet rate	reaches or exceeds (>=	=) 3	pps
	Alert	\$	Media packet loss	percentage reaches or	exceeds (>=) 1.0	01 %
	Alert	٢	Media round-trip t	ime reaches or exceed	s (>=) 3	ms
Applic	ations (AVC	າ				
	Alert	Ŷ		e per connection reach		200 ms
	Alert	\$	Retransmission co	unt reaches or exceed	s (>=) 45	
PfR						
	Alert	\$	Performance Based	Routing (PfRv2) Out o	f Policy event occur	rred
	Alert	\$	Performance Based	Routing (PfRv3) thres	hold crossing alert l	has occured
NSEL						
	Alert		Network Security F	vent Logging (NSEL) fl	ow denied event or	curred
-			Retwork Security E	went zogging (NSEL) II	on active event oc	curred

Each alert can be enabled by clicking on the check box and using the drop-down to select the desired Alert type. The values in the Medianet thresholds (min jitter, max jitter, mean jitter, bit rate, packet rate, packet loss and round-trip time) and in the Applications (AVC) thresholds (network delay and retransmission count) are editable only if the alert is enabled (check box is checked). The Flow, Medianet, AVC, PfR and Medianet alerts are viewed in the Tools > View Alerts and in the Reporting > Flows > Dashboard. The threshold crossing alerts for PfRv3 are for delay, jitter, drop and unreachable.

IP SLA Triggers

To configure alerts in the IP SLA technology, go to Tools > Configure Alerts > IP SLA Triggers tab.

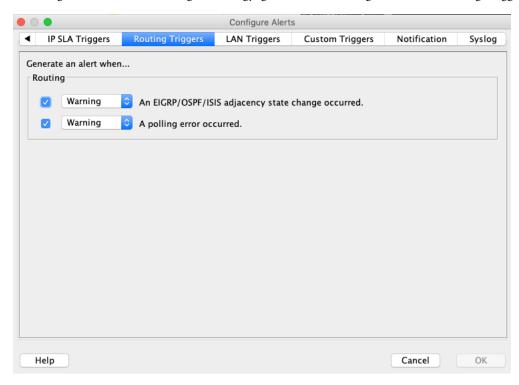
_	LA Triggers	Routing Triggers	LAN Triggers	Custom Triggers	Notification	Syslo
	an alert whe	:n				
IP SLA-						
0	Warning	Catency (round-t	rip time) for a test	reaches or exceeds (>:	=) 200	ms
	Warning	A test exceeds (>	>) 3 erro	rs		
litter (V	oice)					
	Warning	OMOS score for a j	jitter test reaches o	r falls below (<=) 3.0	00	
	Warning	Jitter test packet	loss reaches or exc	eeds (>=) 3.000	pps	
	Warning	A test exceeds (>	>) 3 erro	rs		
Video						
	Warning	◇ Video latency rea	ches or exceeds (>	=) 200	ms	
	Warning	Video jitter reach	es or exceeds (>=)	3.00 ms		
0.0	Warning	Video packet los	s reaches or exceed	s (>=) 3.000	pps	

Each alert can be enabled by clicking on the check box and using the dropdown to select the desired Alert type. The values in the IP SLA thresholds are editable only if the alert is enabled (check box is checked). The IP SLA alerts are viewed in the Tools > View Alerts and in the Reporting > IP SLA > Dashboard.

Default for all IP SLA Triggers is disabled.

Routing Triggers

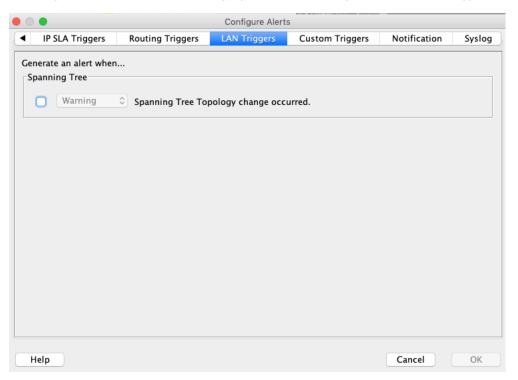
To configure alerts in the Routing technology, go to Tools > Configure Alerts > Routing Triggers tab.



Each routing alert can be enabled by clicking on the check box and using the drop-down menu to select the desired Alert type. The EIGRP/OSPF/IS-IS (Enhanced Interior Gateway Routing Protocol/Open Shortest Path First/Intermediate System-Intermediate System) and the polling error alerts can be enabled or disabled independently. If a routing alert is generated, the alert displays whether it is a state change or polling error and describes the routing protocol, the IP address and the applicable state change. Please see the alert details in the Alert Notification Configuration section occurring later in this chapter. Default for both routing alerts is disabled.

LAN Triggers

To configure alerts in the LAN technology, go to Tools > Configure Alerts > LAN Triggers tab.



The spanning tree topology alert is enabled by clicking on the check box and using the drop-down to select the desired Alert type. This generates an alert for any spanning tree change across all VLANs in the system. The LAN alerts are viewed in Tools > View Alerts. The LAN alert details include the VLAN index and a description of the state change that generated the alert.

Note Since many alerts can be generated, listening and learning Spanning Tree state changes are intentionally not reflected in the alerts. Spanning tree ports in those states will be in a blocked state.

Custom Triggers

Four classes of custom triggers can be configured:

- QoS Class
- NBAR
- Interface
- Flow

Custom triggers can be set to trigger notifications based on threshold exceptions such as QoS drops. A list of created triggers appears in the list box.

IP SLA Triggers	Routing Trigge	rs LAN Triggers	Custom Triggers	Notification	Syslog
Add Edit	Delete				
ow: CriticalVoiceOutsid		ion of CigobitEthernot?	on device RTR_Louisville i	c lace than 2000 (hhne
terrace: interrace dat	a rate for input direct	ion of Gigabitethernetz	on device KTK_Louisville I	s less than 5000.0) KDPS
		Add Custom Trigg	er		
	Type Interfac	e	•		
	Device	ASA Firewall	•		
	Interface	eth1			
	Direction	Input			
			_		
	Operator	less than			
	Value		kbps		
	Syslog Severity	Warning	\$		
			ncel OK		
		Cu			

Tagged alerts can be created using the custom alert triggers. A QoS class, NBAR or Flow tagged alert is created by using a custom alert trigger and then filtering the alert trigger based on the user-defined attributes in the system device tree. These custom alert triggers can then be named or tagged to describe the specific alert based on the filter attributes chosen.

			Add Custom Trigger
pe F	Flow		
lame	FlowAlert		
			restant 0 suga
	*Filter is req		router1 & wan
	Filter is req	uneu	
enera Flow	ate an alert w	hen	
riow			
	Alert	\$	The endpoint of an observed flow is a blacklisted address
Medi	anet		
	Alert	٢	Media loss event occurred
	Alert	0	Media packet dropped by router
	Alert	0	
	Alert		
		0	Media max jitter reaches or exceeds (>=) 150 ms
	Alert	0	Media mean jitter reaches or exceeds (>=) 500 ms
	Alert	\$	Media bit rate reaches or exceeds (>=) 15,000 kbps
	Alert	\$	Media packet rate reaches or exceeds (>=) 3 pps
	Alert	\$	Media packet loss percentage reaches or exceeds (>=) 1.001 %
	Alert	\$	Media round-trip time reaches or exceeds (>=) 3 ms
Appli	ications (AVC	.)	
	Alert	\$	Network delay time per connection reaches or exceeds (>=) 200 ms
	Alert	0	
	ritere	~	
PfR			
	Alert	٢	Performance Based Routing (PfRv2) Out of Policy event occurred
	Alert	\$	Performance Based Routing (PfRv3) threshold crossing alert has occured
NSEL			
	Alert	^	Network Security Event Legging (NISEL) flow don't down a count of
	Alert	0	Network Security Event Logging (NSEL) flow denied event occurred

Alert Notification Configuration

Notification that an alert condition has been triggered can be conveyed in the following methods:

- Notification within LiveNX (in-application alert)
- Notification via e-mail
- Notification within LiveNX and via e-mail

		Configure Alert	S							
◄ IP SLA Triggers	Routing Triggers	LAN Triggers	Custom Triggers	Notification	Syslog					
General ✓ Ignore repeated alerts within the following interval: 1 minute ✓ Send message when alert cleared Generate a Test Alert Now										
In-Application Notifications ✓ Send In-Application Notifications □ Send Email Notifications										
SMTP server	smtp.office365.com	n		Configure						
	Recipient addresses: pgayam@liveaction.com, jmathew@liveaction.com (comma-separated)									
To reduce the number of email messages sent, alerts will be queued and sent in batches. Maximum send delay: 5 minutes										
Help				Cancel	OK					

To suppress multiple alerts of the same condition that occur within a given timeframe, select the Ignore repeated alerts within the following interval check box. For example, when CPU usage spikes beyond the set threshold, the alarm could repeat itself six times within a minute, depending on the polling cycle set for the device (e.g., 10-second polling). In this situation, a single alarm per minute would likely suffice.

Note An exception is made for the NSEL flow denied event occurred alert. The NSEL flow denied event alert will trigger no matter what ignore interval is selected. This exception was made to continue to record alerts for the instance where the security device alerts on multiple flows denied event occurrences for different flows within the same ignore interval.

E-mail alert notifications are sent when the first of the following conditions have been met:

- Total number of alerts reaches 200
- Maximum send delay timer time since last alert reached maximum delay (default is 5 minutes)

	Severity	Device	Group	Alert Type	Details
014/07/08 11:40:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:40:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 11:44:05 AM	Warning	2921-Demo-67_111	Device CPU/	High memory use	Percent memory utilization - 92%
014/07/08 11:46:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:46:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 11:53:05 AM	Warning	2921-Demo-67_111	Device CPU/	High memory use	Percent memory utilization - 92%
014/07/08 11:53:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:53:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 11:53:57 AM	Warning	2921-Demo-67_112	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:53:57 AM	Warning	2921-Demo-67_112	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 11:58:05 AM	Warning	2921-Demo-67_111	Device CPU/	High memory use	Percent memory utilization - 92%
014/07/08 11:58:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:58:05 AM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 11:58:57 AM	Warning	2921-Demo-67_112	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 11:58:57 AM	Warning	2921-Demo-67_112	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 12:03:05 PM	Warning	2921-Demo-67_111	Device CPU/	High memory use	Percent memory utilization - 93%
014/07/08 12:03:05 PM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
014/07/08 12:03:05 PM	Warning	2921-Demo-67_111	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Out
014/07/08 12:03:57 PM	Warning	2921-Demo-67_112	QoS	Interface dropped packets	Interface name - GigabitEthernet0/0; Interface direction - Inp
nly the last 100 alerts are sh	nown.				
Bring this window to the f	rront when a n	ew alert is received			
Beep when a new alert is	received				
				Clear list	Export list Historical search Configure alerts

Sub	ject:	LiveAction Alert Message	e - 13 Alerts		
l	_i\	veAction A		lessages	2
	#	Time	Severity	Alert Type	Details
	1.	2014-07-08 13:27:18	Warning	Test alert	
	2.	2014-07-08 13:29:01	Warning	Test alert	
	3.	2014-07-08 13:30:23	Warning	Class dropped rate	1941-WAN-67_113; 192.1(
	4.	2014-07-08 13:30:23	Warning	Class dropped rate	1941-WAN-67_113; 192.1(
	5.	2014-07-08 13:30:20	Warning	Test alert	
	6.	2014-07-08 13:32:02	Warning	Test alert	
	7.	2014-07-08 13:30:23	Warning	Test alert	

Syslog Notifications

Alerts generated by LiveNX can be sent to a Syslog server. Set up the Syslog server location and message format using the Syslog tab.

STATUS & TIME

Status:	I	\sim
Time opened:	Acknowledged	
Active for:	Active	
SOURCE INFO	Ignored	
Device:	Resolved	

Message priority/level is set in the Trigger windows for each of the alert types.

Status Bar Alerts

The status bar at the bottom of the LiveNX screen includes an alert status icon

Green icon	Alerts have been configured.
Gray icon	Alerts not configured.
Red background	New alerts (unviewed alerts in dialog).
Normal background	No new (unviewed) alerts.
Red background	Clears when user opens alerts dialog.

CHAPTER 5

Reporting

In this chapter:

About Reporting	83
Report Search	99
Lan Reports	08

About Reporting

LiveNX provides a reporting system that allows you to analyze events and statistics captured by the system. The Reporting function can be accessed through the Java Client or through the Web interface. We recommend that you start using the web interface based reporting functionality.

Reporting Best Practice

Web interface reporting provides two capabilities that help you to leverage the power of reporting. You can start with a report and drill down as well as pivot. Let's consider an example where you would want to know the applications being detected on the network. An application report shows the list of applications across the network along with the bandwidth being consumed by those applications.

Application,	Last Fifteen Minutes	5					View Options ${\scriptstyle\checkmark}$	Share Print	Schedule Copy	Close
Application (F	low)									ø G
Device: All WAN I	Devices Interface: All WAS	Interfaces Displa	ay Filter: No Display Filtering Dire	ection: Outbound Flow Type: Bas	ic Flow Execution Type: Time Series	Sort By: Bit Rate Bin Duration: Auto	Start Time: Sep 09, 2019 16:38:22 PDT (GMT-07:00)	End Time: Sep 09, 2019 16:53:22 PD	T (GMT-07:00) Bin Interval: 1 r	minute
7.5 5 BIt Broo (Mpbo)	F								Ttp-video ortita-static VoiP outook-web-service trp-suido-smartprobe vosuble Tip Video netfix ssi ssi	≡
16:39:00 << Page 1	16:40:00 / 12 >>>	16:41:00	16:42:00 16:43:00	16:44:00 16:45:	00 16:46:00 16:4	7.00 16:48:00 16:49:00	16:50:00 16:51:00 1	6:52:00 16:53:22 Q Search		0 ±
Legend O	Application O		Total Flows 🗘	Total Bytes 🔾	Total Packets 🛇	Average Bit Rate 🗘	Average Packet Rate 🛇	Peak Bit Rate 🗘	Peak Packet Rate 🗘	
-	rtp-video		28	369.15 MB	272,232	3.28 Mbps	302.48 pps	3.81 Mbps		351 pps
-	citrix-static		135	68.87 MB	339,255	612.17 Kbps	376.95 pps	660.74 Kbps		406 pps
-	VoIP		144	67.75 MB	338,765	602.25 Kbps	376.41 pps	1.11 Mbps		694 pps
-	outlook-web-service	Apply VoIP to S	Search Filter	15.32 MB	114,654	136.14 Kbps	127.39 pps	297.41 Kbps		280 pps
-	rtp-audio-smartprobe	Apply Specific	Flow to Search Filter	11.69 MB	146,170	103.94 Kbps	162.41 pps	104.65 Kbps		163 pps
-	youtube		/oIP as Application	11.63 MB	205,230	103.37 Kbps	228.03 pps	200.42 Kbps		450 pps
-	rtp		/oIP as Top Conversations	8.17 MB	61,492	72.66 Kbps	68.32 pps	91.74 Kbps		85 pps
-	Video		/oIP as Interface Bandwidth	6.92 MB	34,608	61.53 Kbps	38.45 pps	94.93 Kbps		59 pps
-	netflix	Drill down on V		6.76 MB	147,216	60.10 Kbps	163.57 pps	95.74 Kbps		265 pps
_	ssl	Drill down on V	/oIP as IPs and Ports	6.22 MB	82,637	55.27 Kbps	91.82 pps	117.56 Kbps		213 pps

The next logical step would be to further drill down and examine the various clients that might be using those applications. Simply select the application of interest and right click on it to get the ability to drill down into the details.

ill down o	NoIP as Top Co	nversations from	n Application							View Options $$	Share Pr	int Schedule	Copy Clo
p Conversat	ions (Flow)												1
	evices Interface: Al 2019 16:53:22 PDT (G			Itering Direction: Ou	sbound Flow Type: I	Basic Flow Executio	n Type: Time Series Se	ort By: Bit Rate Flex Search	h: flow.app="VolP" Bin Duration:	Auto Should Walt For	Dns Resolution: faise Star	t Time: Sep 09, 2019 16:38:22	PDT (GMT-07:00)
1.5												= 192.168.102 = 22.1.1.10/20 = 192.168.100	11/192.168.10.16 11/192.168.10.13 1.1.10 11/192.168.10.11 5/192.168.104.11 1/192.168.100.11 6/192.168.105.11 3/192.168.105.11 3/192.168.102.11
0 16:39.00 Page 1	16:40:00 /2>≫	16:41:00	16:42:00	16:43:00 1	6:44:00 16:4	15:00 16:46:	00 16:47:00	16:48:00	16:49:00 16:50:00	16:51:00	16:52:00 Q S	16.53:22 sarch	
gend O	Src IP Addr O	Site 🗘	Dst IP Addr 🗘	Dst Site 🗘	Total Flows O	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🗘	Average Packet Rate 🗘	Peak Bit Rate 🗘	Peak Packet Rate 🛇	Src Country O	Dst Country O
	192.168.104.11	Madison	192.168.10.15	DC-New_York	15	8.68 MB	43,424	77.20 Kbps	48.25 pps	77.22 Kbps	48 pps		
	192.168.105.11	London	192.168.10.16	DC-New_York	15	8.68 MB	43,423	77.20 Kbps	48.25 pps	77.22 Kbps	48 pps		-
	192.168.102.11	Birmingham	192.168.10.13	DC-New_York	15	8.68 MB	43,421	77.19 Kbps	48.25 pps	77.22 Kbps	48 pps		
	22.1.1.10	Sydney	20.1.1.10	Tokyo	15	5.79 MB	28,940	51.45 Kbps	32.16 pps	51.46 Kbps	32 pps	US/UNITED STATES	US/UNITED STAT
	192.168.100.11	Seattle	192.168.10.11	DC-New_York	15	4.21 MB	21,051	37.42 Kbps	23.39 pps	37.44 Kbps	23 pps		
-	192.168.10.15	DC-New_York	192.168.104.11	Madison	5	3.74 MB	18,700	33.24 Kbps	20.78 pps	100.08 Kbps	62 pps		
	192.168.10.11	DC-New_York	192.168.100.11	Seattle	5	3.74 MB	18,700	33.24 Kbps	20.78 pps	100.10 Kbps	62 pps		
	192.168.10.16	DC-New_York	192.168.105.11	London	5	3.74 MB	18,699	33.24 Kbps	20.78 pps	100.08 Kbps	62 pps		
	192.168.10.13	DC-New_York	192.168.102.11	Birmingham	5	3.74 MB	18,699	33.24 Kbps	20.78 pps	100.08 Kbps	62 pps		

Drilling down into the applications shows the top conversations that are happening for that particular application. This provides users the ability to track which applications are consuming the bandwidth and the users responsible for it.

Engineering Console Reporting

The Engineering Console Reporting is accessible from the main toolbar and is accessed by topic: QoS, Flow, Routing, IP SLA, LAN, and Schedule or build a Custom Dashboard.

LAN Tools	Reports	Help
	QoS	
	Flow	
Types ᅌ	Routing IP SLA	l
flow.app = web		
	Schedu	le
	Custom	Dashboard

QoS Report

LiveNX supports several QoS reports for analyzing historical information. The reporting feature allows you to generate reports in PDF format. Most reports allow you to select the specific interfaces and devices. From the main menu bar, go to Reports > QoS.

• • •	QoS Reports
Q- Type here to filter repo	
Reports Device CPU/Memory Usa Interface Bandwidth Interface Utilization Interface Bandwidth Com	Device CPU/Memory Usage 1h 6h 1d 1w 30d 90d 1y Custom AppleFastLane-3560
Interface/Interface Drop NBAR Comparison NBAR and Post-Policy Pre-Policy and Post-Polic Pre-Policy and Post-Polic Pre-Policy and Post-Polic Top CPU Usage Top Memory Usage Top Interface Bandwidth Top Interface Bandwidths Top Class Bandwidths Top Class Drops Site Bandwidth Interface Burstable Rate Site WAN Interface Utiliz Site Alert Site Alert	AppleFastLane-3560
Custom Reports	

LiveNX generates several QoS reports listed in the left-hand column. Click on the desired report, choose the parameters for the chart, and then click on Execute Report. Please refer to the table below for details about each QoS report.

Report Name	Report Description	Chart Parameters
Device CPU/Memory Usage	Displays % utilization of the device CPU and memory as a function of time.	Device
Interface Bandwidth	Compare inbound and outbound bandwidth for a given device and interface over the same time period in Kbps.	Device, Interface
Interface Utilization	Used to view inbound and outbound bandwidth with 95th, 99th and peak values. Where the peak that this graph shows is the highest peak that was monitored at the native polling rate regardless of the bin size used.	Device, Interface, Inbound/ Outbound
Interface Bandwidth Comparison	Compare 2 interfaces: Displays an overlay chart of two devices' interfaces' bandwidths in Kbps. Compare 2 time periods: Displays two stacked charts of a device interface's bandwidth over different start times covering the same time span.	Compare 2 interfaces: Device, Interface, Inbound/Outbound Compare 2 time periods: Set Time 1, Set Time 2, Device, Interface, Inbound/Outbound
Interface/Interface Drops	Compare interface and interface drop rates for a given device and interface over the same time period in packets/second.	Device, Interface, Inbound/Outbound
NBAR Comparison	Compare 2 interfaces: Displays two devices' interfaces' traffic by NBAR type in Kbps for the same time span. Compare 2 time periods: Displays a single device interface's traffic by NBAR type in Kbps over different start times covering the same time span.	Compare 2 interfaces: Device, Interface, Inbound/Outbound Compare 2 time periods: Set Time 1, Set Time 2, Device, Interface, Inbound/Outbound
NBAR and Post-Policy	Displays a device interface's traffic by NBAR type and the Post-Policy traffic in Kbps for the same time span.	Device, Interface, Inbound/ Outbound
Pre-Policy and Post-Policy	Displays a device interface's traffic by Class type and the Pre- or Post-Policy traffic in Kbps for the same time span.	Device, Interface, Inbound/ Outbound
Pre-Policy and Post-Policy Comparison	Compare 2 interfaces: Displays two devices' interfaces' traffic by Class type and the Pre- or Post-Policy traffic in Kbps for the same time span. Compare 2 time periods: Displays a single device interface's traffic by Class type and the Pre- or Post-Policy traffic in Kbps over different start times covering the same time span.	Compare 2 interfaces: Device, Interface, Inbound/Outbound, Pre- Policy/Post-Policy Compare 2 time periods: Set Time 1, Set Time 2, Device, Interface, Inbound/Outbound, Pre-Policy/ Post- Policy

Pre-Policy and Post-Policy Drops	Displays a device interface's traffic by Class type and the Post-Policy Drops in Kbps for the same time span.	Device, Interface, Inbound/ Outbound
Top CPU Usage	Displays a bar graph of the device's average and peak % CPU usage over the desired time period.	All Devices/Individual Device
Top Memory Usage	Displays a bar graph of the device's average and peak % memory usage over the desired time period.	All Devices/Individual Device
Top Interface Bandwidths	Displays a table of the interface bandwidths in kilobits per second, averaged over the desired time period for all devices, or for a given device.	All Devices/Individual Device, Inbound/Outbound
Top Interface Drops	Displays a table of the highest interface's drop bandwidth in packets per second, averaged over the desired time period for all devices, or for a given device.	All Devices/Individual Device, Inbound/Outbound
Top Class Bandwidths	Displays a table of the highest class bandwidths in kilobits per second, averaged over the desired time period for all devices, or for a given device.	All Devices/Individual Device, Inbound/Outbound, Pre-policy/ Post- policy, Exclude Class-default checkbox
Top Class Drops	Displays a table of the highest class drop bandwidths in kilobits per second, averaged over the desired time period for all devices, or for a given device.	All Devices/Individual Device, Inbound/Outbound, Pre-policy/ Post- policy, Exclude Class-default checkbox
Site Bandwidth	Displays a time-series chart showing current, average and peak bandwidth in kilobits per second from the selected site to all other sites or from all other sites to the selected site.	Site, Inbound/Outbound, WAN checkbox
Interface Burstable Rate	Displays a bar chart of interfaces for all devices, summarizing 99th % bandwidth and 95th% bandwidth.	Inbound/Outbound
Site – WAN Interface Utilization	Displays a table of all interfaces with the WAN checkbox enabled, showing bar graphs of interface input and output bandwidth % capacity, CPU and memory % utilization.	
Site Alert	Aggregates a count of alerts by site tag with individual counts for QoS categories: Device Up/Down, Device CPU/Memory, Device Config Change, Interface Up/Down and Interface Rate as well as overall Flow IP SLA, LAN and Routing alert counts.	
Site Alert Detail	Aggregates a count of alerts by site tag with individual counts for the various Alert Names.	

Device Search

Click on the button labeled as ... between the device drop-down button and the Execute Report button to display the device pick list.

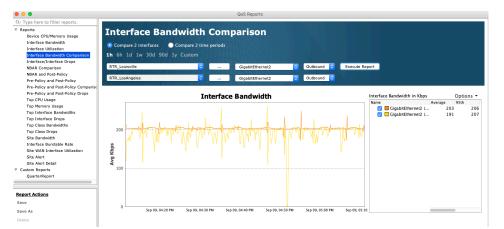
		Q03 r	leports				_
l- Type here to filter repo			10/02				
Reports	evice CPU/Mem	ory lleage					
Device CPU/Memory Usa	evice cro/men	iory usage					
Interface Bandwidth							
Interface Utilization 1h	6h 1d 1w 30d 90d 1y Cu	stom					
Interface Bandwidth Con			STRUCTURE S				
Interface/Interface Drop	ppleFastLane-3560	···· 0	Execute Repor	t de la constante			
NBAR Comparison		Select [Device				
NBAR and Post-Policy	Q-						
Pre-Policy and Post-Polic	0.						
Pre-Policy and Post-Polic							_
Pre-Policy and Post-Polic	Device Name	Device Add Vendor 10.100.5 Non-SNMP	Model	Group	Node	Site	٦
Top CPU Usage	AppleFastLane-3560 AppleFastLane-4331	10.100.5 Non-SNMP 10.100.5 Non-SNMP	Non-SNMP Non-SNMP		Local		
Top Memory Usage	AppleFastLane=4331 ASA Firewall	10.100.5 Non-SNMP	Non-SNMP	Internet	Local	Internet	
Top Interface Bandwidth	CS-2960-23-22	10.100.5 Cisco	catalvst29		Local	Internet	
Top Interface Drops	CS-AnyConnectSamplicator	10.100.5 Non-SNMP		Internet	Local	Internet	
	CS-C3650-23-36	10.100.1 Cisco	ciscoC365		Local	Internet	
Top Class Bandwidths	CS-C3850-23-31	10.100.5 Cisco	cat38xxst		Local	Internet	
Top Class Drops	FortiGate Firewall	10.100.5 Non-SNMP		Internet	Local	Internet	
Site Bandwidth	IPv6FlowDevice	10.100.5 Non-SNMP	Non-SNMP	et	Local	internet	
Interface Burstable Rate	IWAN-Br1 Sydney	10.100.5 Cisco	ciscoCSR1	Sydney	Local	Sydney	
Site WAN Interface Utiliz	IWAN-BR INET	10.100.5 Cisco	ciscoCSR1	Tokyo	Local	Tokyo	
Site Alert	IWAN-BR_MPLS	10.100.5 Cisco	ciscoCSR1	Tokyo	Local	Tokyo	
Site Alert Detail	IWAN-DC-MC	10.100.5 Cisco	ciscoCSR1	Tokyo	Local	Tokyo	
	IWAN-MPLS-CORE	10.100.5 Cisco	ciscoCSR1	Impairment	Local	Impairment	
Custom Reports	LiveAgent360Concentrator	10.100.5 Non-SNMP	Non-SNMP	Florida	Local	Florida	
	LiveAgentConcentrator	10.100.5 Non-SNMP	Non-SNMP	Florida	Local	Florida	
	MerakiNetflow	10.100.5 Non-SNMP		Internet	Local	Internet	
leport Actions	PaloAltoNetwork Firewall	10.100.5 Non-SNMP		Internet	Local	Internet	
Save	RTR-DC-CORE	10.100.5 Cisco	ciscoCSR1			DC-New	
	RTR-DC-MPLS	10.100.5 Cisco	ciscoCSR1			DC-New	
Save As	RTR_Austin	10.100.5 Cisco	ciscoCSR1	Austin	Local	Austin	
Delete							
Schedule					Cance	el Sele	

Use the scroll bars to locate the desired device, or type in the search bar adjacent to the magnifying glass to filter the list of devices. Click on a category to choose the desired match field. Default is All, Case insensitive and Match anywhere. Once the device is located, double click on the row or click once to highlight the row and then click on Select to choose the desired device.

Select Device						
Q- ASA						0
Device Name	Device Add Ven	dor Model	Group	Node	Site	Tags
ASA Firewall	10.100.5 Nor	-SNMP Non-SNMP	Internet	Local	Internet	

Following are two examples of LiveNX QoS reports.

The following images depict Interface Bandwidth Comparison report. By choosing "Compare 2 interfaces" and then selecting the desired device, interface, inbound or outbound, and then clicking Execute Report, LiveNX creates a line chart overlaying the selected device interface bandwidth over the same time span.



The following image is an NBAR Comparison report. By choosing "Compare 2 time periods" and then clicking Execute Report, LiveNX creates two stacked charts to compare NBAR traffic bandwidth at two different times for the desired device, interface, and input or output traffic.

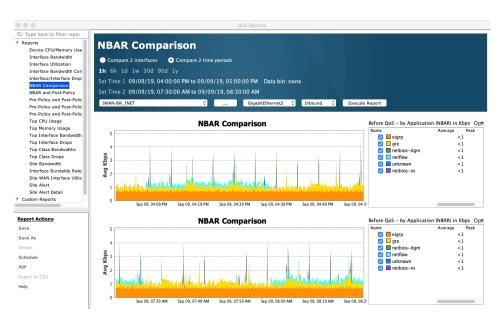


Chart Zoom

To expand a portion of the chart, hold the left mouse button down and drag to the right. A box will appear showing the area to zoom in. To return to the default view, right click on the chart and select "Reset zoom."

Report Legend

The Report Legend can be sorted by columns. Click on the desired column header to sort the legend in either ascending or descending order. Please see the image below for an example of a legend with visible Options. To add or remove items from the chart, check or uncheck items in the legend.

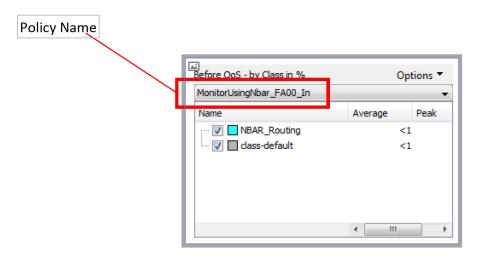
Click Options > Select all to select all items for viewing in the chart.

Click Options > Select none to unselect all items for viewing in the chart.

Click Options > Export legend data to create a CSV file containing the data in the legend. For reports with two legends, both legends will be exported. The default location where the CSV file will be saved to is your LiveNX Client desktop.

Name		*	Select	all		
🔽 🔲 VI	an 1 (1386_Bl		Select	none		
🔽 📕 Fa	astEthernet0,	-	Export	leger	nd data	

Specific to QoS Pre-Policy and Post-Policy reports, the input or output interface policy is shown as part of the header in the legend. If there was a policy change for that interface during the specified time span, the combo box will allow the user to select the desired policy for viewing within the chart. Please see the image below for a Pre-Class legend with the policy name displayed in the header.



Report Historical Time Span Selection

The time span of historical data is selectable at the top of the report.

- 1h time span of historical data is selectable at the top of the report
- 6h time span of historical data is selectable at to the present
- 1d time span of historical data is selectable at to the present
- 1w time span of historical data is selectable at to the present
- 30d time span of historical data is selectable at to the present

- 90d time span of history from ninety days in the past to the present 1y time span of history from ninety days in the past to the present
- Custom span of history from an end time



Report Actions

There are seven report actions: Save, Save As, Delete, Schedule, PDF, Export to CSV, and Help.

- Save LiveNX brings up a dialog box. Enter a report name in the dialog box. The report will be saved under Custom Reports.
- Save As after selecting a saved report for viewing, if you change any report attribute (e.g., time span, device, interface), you can create a new custom report by clicking on Save As and naming the report with a different report name.

Note LiveNX will not allow you to save another custom report with the same report name.

	🛑 🔘 🌑 Save Report As				
Enter Report Name:					
	ОК	Cancel			

- Delete deletes a report. Select a report name under Custom Reports and click on Delete.
- Schedule allows automatic generation and delivery of custom reports. Additional details can be found in the Report Scheduler section of this chapter.
- PDF allows creating and saving a PDF version of the report.

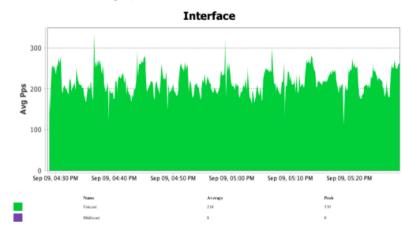
Interface/Interface Drops

09/09/19 04:28:34 PM PDT (UTC-0700) - 09/09/19 05:28:34 PM PDT (UTC-0700)

Options

- Device: RTR_Austin.liveaction.com
- Interface: GigabitEthemet3
 Direction: INPUT

Interface/Interface Drops by Name



- Export to CSV saves the report legend to a comma-separate value (CSV) file. The default file location where the CSV file will be saved to is the LiveNX Client desktop.
- Help launches the LiveNX User Guide.

Interface Utilization Report

This report shows the inbound and outbound bandwidth based on the user selected bin size or auto bin size. When using the auto bin size, the system will determine the optimal bin size to use for the particular report duration time period. The report shows both inbound and outbound bandwidth along with the peak. The peak value is enabled by clicking on the legend for inbound and outbound peak separately. The peak value used in the report is the highest peak rate seen in that bin at the polling rate. For example, if the device is being polled at 10-second interval and the report is generated for a month using a 15-minute bin size, the peak will show the highest rate found in that bin at the 10-second data over the entire month.



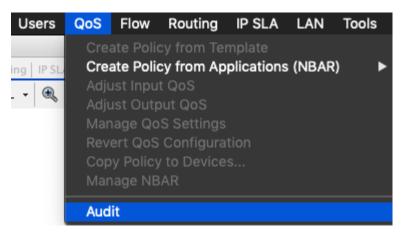
The legend will show the 95th, 99th and peak value individual for the 4-time series information for inbound based on bin, outbound based on bin, inbound peak rate and outbound peak rate. Those val-

ues can be exported using the Options menu on the legend. Exporting to the CSV option in the Report Action panel will export the 4 -time series data set as shown below.

RTR_Louisville - OUTPUT - Interface Bandwidth in Kbps				
Name	Average	95th	99th	Peak
Inbound Bandwidth	11.80811405	29.32239914	31.79039955	32.81760025
Inbound Peak Bandwidth	11.80811405	29.32239914	31.79039955	32.81760025
Outbound Bandwidth	203.3231354	206.1573639	220.2638092	247.526825
Outbound Peak Bandwidth	203.3231354	206.1573639	220.2638092	247.526825

QoS Audit

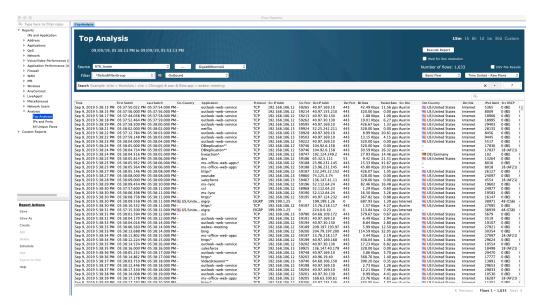
A QoS Policy and Performance Audit report is also available to analyze and summarize the policies enabled, identify any policy issues, and report on performance anomalies. This report is accessed via the Reporting menu or the QoS toolbar.



	Main Perfo	ormance	lssues	Polici	es			
QoS Policy an Aonday, September 9, 2019 5:37 Pl		form	anc	e A	udi	t Rep	ort	
Summary								
Devices								
Number of devices analyzed:		17						
Number of devices with QoS enable	d:	16						
Number of devices showing drops:		8						
Interfaces								
Number of interfaces with policies ap	oplied (in/out):	93/30						
Number of interfaces showing drops	:	10						
Policies								
Number of policies found on all device	ces:	57						
Number of distinct named policies:		12						
Number of distinct class names foun	d on all devices	s: 37						
Number of distinct applied class nam	nes:	23						
ssues								
Number of system issues:		2	Details					
Number of device issues:		11						
Device	Configured Device	Acquired Running Config	Drops	Issues	QoS Or	1		
CS-2960-23-22.liveaction.com	х	x				Details		
CS-C3650-23-36.Liveaction	x	x		x	x	Details		
CS-C3850-23-31.liveaction.com	x	x		x	x	Details		

Flow Reports

LiveNX allows you to access and analyze historical Flow data through Flow Reports. The reports can be accessed by clicking Reports > Flow in the menu bar or "Reports" in the toolbar of any of the Flow views.



Available Reports

There are several reports available in the left-hand tree view in the Flow Reports dialog. They are grouped by type. Clicking the "+" icon next to a report type will expand it and show the available reports.

- Interface Bandwidth report showing interface bandwidth information in either time-series or aggregation format. Default is Time-series and Outbound.
- Top Analysis lists all flow data for a given device and flow technology type sorted by time.
- Address Reports
- Top Conversations counts total flows, input bytes, input bit rate, output bytes and output bit rate for a given source and destination IP address pair. Use the drop-down to select between Time Series or Aggregation.
- Bidirectional Source/Destination Pair counts flow data between an IP address pair by sorting the address. Use the Filter drop-down to choose among Inbound, Outbound or Inbound and Outbound. o Default direction: Outbound
- Source or Destination Address aggregates flow data regardless if the IP address is a source address or destination address. This report is useful for to determine which endpoints are sending/ receiving the most data.
- **Note** In the time series report, flows will be double-counted-the amount of traffic coming and going will always be counted.
 - Default direction: Inbound and Outbound
 - Address Pair counts flow data across a directed IP address pair: source (the first IP address) to a
 destination (the second IP address). o Default direction: Outbound Destination Address shows
 flows based on destination IP address.
 - Default direction: Outbound
 - Source Address shows flows based on source IP address.
 - Default direction: Inbound
 - Destination Address Popularity shows flow counts and number of unique IP connections for each destination IP address.

- Default direction: Outbound
- Source Address Popularity shows flow counts and number of unique IP connections for each source IP address.
 - Default direction: Inbound
- Site Traffic shows bit rates and flow counts for each user-defined site and site IP range. Sites without a site IP range will show up as an Unknown site.
 - Default direction: Inbound and Outbound
- Destination Site Traffic shows bit rates and flow counts for each user-defined destination site and site IP range. Sites without a site IP range will show up as an Unknown site.
 - Default direction: Outbound
- Source Site Traffic shows bit rates and flow counts for each user-defined source site and site IP range. Sites without a site IP range will show up as an Unknown site.
 - Default direction: Inbound

Application

- Protocol shows flow data associated with protocols, e.g. TCP.
- Application shows flow data associated with applications and NBAR applications.
- DSCP vs Application shows DSCP (differentiated services code point) and IPv6 traffic class counts in a stacked chart with the application type.

QoS

- Type of Service shows flow counts of the Type of Service values in the inbound, Outbound or Inbound and Outbound direction of the desired device. Default is Outbound.
- DSCP shows flow counts of the DSCP values in the Inbound, Outbound or Inbound and Outbound direction of the desired device. Default is Outbound.

Network

- Interface Bandwidth Summary this report must be used with a tagged item when selecting an All
 Devices report, as described in the Defining Sites and Tags section of Chapter 4 Basic Setup. For
 All Devices, this creates a separate report for each device counting the total flows, total bytes, total
 packets, average bit rate, average packet rate, peak bit rate and peak packet rate of every tagged
 interface.
- Bandwidth Summary creates a separate Inbound, Outbound and Inbound and Outbound report, listing the device and interface names, the total flows, total bytes, total packets, average bit rate, average packet rate, peak bit rate and peak packet rate.
- Traffic Volume Pair shows flow data associated with the interfaces on the device selected. It should be noted that some interfaces that are shown in the chart and table may not exist on the device. For those interfaces, it is not possible to drill down to a Top Analysis report.
- Outbound Bandwidth Utilization shows flow data from interfaces on the device selected. Default is outbound.
- Bidirectional Network Pair shows flow data between source and destination subnet pairs. Default is outbound.
- Source or Destination Network shows flow data from all subnets, regardless if it is a source or destination network. Default is Inbound and Outbound.

- Network Pair shows flow data across a directed network pair: source (the first subnet) to a
 destination (the second subnet). Default is Outbound. Source Network shows flow data by
 source subnet. Default is Inbound.
- Destination Network shows flow data by destination subnet. Default is Outbound.
- Bidirectional AS Pair shows flow data between source and destination autonomous system pairs. Default is Outbound.
- Source or Destination AS shows flow data from all autonomous system numbers, regardless if it is a source or destination. Default is Inbound and Outbound.
- AS Pair shows flow data across a directed autonomous system pair: source (first AS) to a destination (second AS). Default is Outbound.
- Source AS shows flow data by source autonomous system number. Default is Inbound.
- Destination AS shows flow data by destination autonomous system number. Default is Outbound.

Medianet

- Jitter/Loss shows Medianet information for each pair of IP addresses (source and destination), including min, max mean, and max jitter, and loss event counts.
- Round Trip Time shows Medianet information

Application (AVC)

- AVC Application shows flow data by AVC type.
- Top Applications Performance shows Application Visibility and Control (AVC) performance data for a given device by application including average performance rate, average and maximum application delay (AD), client network delay (CND), server network delay (SND), and network delay (ND); total application response time (ART), total volume (client bytes + server bytes), responses, transaction time (TT) sum, total retransmissions, and new connections.
- Application Performance charts AVC performance data over time for a given device and application.
- Policy Classification charts the total flow counts per AVC Policy and QoS Classification Hierarchies for the specified time range. Note that the Policy QoS Classification Hierarchy field lists the parent policy only and the QoS Classification Hierarchy field lists the parent and child class policy.
- Top Policy Performance charts performance data (Total Volume, Total Application Response Time, New Connections or Retransmissions) of the AVC Policy and QoS Classification Hierarchies for the specified time range.
- **Note** The Policy QoS Classification Hierarchy field lists the parent policy only and the QoS Classification Hierarchy field lists the parent and child class policy.
 - Top Policy Applications Performance charts performance data (Total Volume, Total Application Response Time, New Connections or Retransmission) of the AVC Policy, QoS Classification Hierarchies and Application (NBAR) for the specified time range.
 - HTTP Host charts total flow counts by HTTP Host for the specified time range.

NSEL

• Denied Security Events – shows denied event count information for a given source and destination IP address.

• ACL Pair – shows the denied event count information for a given ingress and egress ACL ID.

PfR

- Alerts All charts the count of PfRv3 alerts for a given device or all devices.
- Alerts by Site charts the count of PfRv3 alerts for each site.
- Alerts by Application Group charts the count of PfRv3 alerts for every defined application group.
- Alerts by Service Provider -charts the count of PfRv3 alerts for every service provider.
- Alerts by Site Pair charts the count of PfRv3 alerts between the source and the destination site.
- Corrected vs. Uncorrected charts the count of PfRv3 alerts that had a completed mitigation result.
- Application Group Bandwidth charts the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices.
- Application Group Bandwidth by Site charts the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each application group, aggregated by site.
- Application Group Bandwidth by Service Provider charts the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each application group, aggregated by the service provider.
- Site Capacity Utilization charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices.
- Site Capacity Utilization by Application Group charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each site, aggregated by application group.
- Site Capacity Utilization by Service Provider charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each site, aggregated by service provider.
- Service Provider Capacity Utilization charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for a given device or all devices.
- Service Provider Capacity Utilization by Application Group charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each service provider, aggregated by application group.
- Service Provider Capacity Utilization by Site charts the utilized capacity %, the number of flows, bytes, packets, bit rate or packet rate for a given device or all devices for each service provider, aggregated by site.
- Out of Policy Events shows out of policy counts for a given Border Router IP Address, PfR reason and Application tag. Report also displays traffic class information.

Wireless

- Wireless SSID charts the Top 10 Service Set Identifiers (SSID) with the highest traffic rates. Default is Outbound.
- Wireless SSID DSCP charts the Top 10 differentiated service code points (DSCP) and SSID with the highest traffic rate. Default is Outbound.
- Wireless SSID Application charts the Top 10 Application type (NBAR) and SSID with the highest traffic rate. Default is Outbound.
- Wireless SSID Unique Clients charts the Top 10 unique IP connections (source IP addresses) and SSID with the highest traffic rate. Default is Outbound.

- Wireless Access Point charts the Top 10 Wireless Access Point (AP) MAC addresses with the highest traffic rate. Default is Outbound.
- Wireless Access Point Application charts the Top 10 WAP MAC addresses and application type (NBAR) with the highest traffic rate. Default is Outbound.

• Wireless Access Point Unique Clients – shows flow data and the number of unique IP connections by Wireless access point MAC address. Default is Outbound.

Miscellaneous

- User Filter shows flow data using the selected display filter.
- Destination Country shows flow data going to a specific country.
- Source Country shows flow data coming from a specific country.
- Device Flow Count displays devices and counts the total flows exported.

Caveats

Directionality is available in some reports. "Inbound" is essentially Ingress, and "Outbound" is essentially Egress. Direction is only applicable to NetFlow collector version 9 (NetFlow version 5 does not include direction). If version 5 is used, the data will be double-counted; ingress and egress collection is enabled by default on interfaces, and NetFlow version 5 cannot distinguish the direction. As of LiveNX version 2.3, NetFlow version 9 is enabled when configuring flow exports using LiveNX's "Add Device Wizard."

Report Features

The report highlights any data that exceeds an alert value for the given flow technology. Alerting must be enabled for the given technology for the highlighting to be visible. Scroll horizontally to find a dark red highlighted cell, which indicates the specific attribute causing the alert condition. The reports list can be filtered using the filter box above the tree view. Reports will be filtered by the report name. After a report is selected, the report's configuration options appear in the header of the report. There are several configuration options common to all reports (Device, Interfaces, time range, etc.), but some reports will have additional options.

- Source: There are two drop-down lists to select the desired device and interface. The first dropdown can go from All Devices to an Individual Device. In between the two dropdown lists is a ... labeled button. Click to display a device pick list with an alphanumeric entry for searching the list. For more details on the device pick list, please see the Device Pick List section in the QoS reports. If an individual device is selected, then the interface dropdown will select either All Interfaces, or list the interfaces specific to that device. If All Devices is chosen, then the interface dropdown choice is All Interfaces. All devices, past and current, will appear in the device drop-down.
- Tags and Filters: Filter your flow report by typing in your defined Labels, Site, Tags or WAN designation. These reports will use all devices; a dialog box will alert you that these designations require the Source field to be All Devices.
- Filter: Dropdown list of common filters and any user-defined filters.
- Filter Icon: Brings up the Flow Display Filters Setup to create user-defined filters. Direction: Choose among Inbound, Outbound or Inbound and Outbound. • Graph: Choose between Aggregation and Time-Series. Choose from Bytes, Bit Rate, Bytes, Packets or Packet Rate. For Top Analysis chart, choose among Basic Flow, Medianet, Application (AVC), NSEL, PfR, Wireless and Unknown flow types.
- Utilize Long-Term Cache: This forces the graph to use the long-term 15-minute data store for generating a report. Typically, the software will determine which store to use, the raw or long-term depending on the number of days, but in some cases with devices with large number of flow. In

some cases, where there are a lot of flows from a device, it is more efficient to force the reporting to leverage the long-term store and this option allows the user to override the default behavior.

- Display Options: There are three options for displaying the top analysis data in time.
 - Time Sorted: Unique Flows: Displays unique flows in time from the oldest to the most recent. Uniqueness is determined by the following fields: Protocol, Source IP Address, Source Port, Destination IP
 - – Address, Destination Port, Type of Service, Input Interface, Output Interface, First Switched, RTP SSRC, direction. Unique Flows is the default selection.
- Time Sorted: Raw Flows: Displays all flows in time from the oldest to the most recent.
- Byte Sorted: merge active flows and sort by highest byte count to lowest byte count for up to 5,000 flows. The Sorted paging option is available for Flow Types: Basic Flow and Medianet.
- Historical time period: Choose among 15m (15 minutes), 1h (one hour), 6h (six hours), 1d (one day), 1w (one week), 30d (thirty days) or Custom. When choosing custom, select the desired Start and End Date and Time.
- Est. non-filtered flows: Shows an estimate of the number of flows for the selected time range, device, interface and direction. Estimates give an approximate idea of the amount of data to expect.
- Execute Report: Click on the Execute Report button to create the Flow Report.
- CSV File Results: Click on the check box and click on Execute Report to send the full set of flow data in the table to the LiveNX server using a CSV format. A confirmation dialog box will appear to load the LiveNX server web page. Click on the OK button to proceed. On the LiveNX Server web page, right-click on the Right click to save CSV file link and then select Save target as... to save the report to a CSV file.

Report Search

The LiveNX Flow reports have a Search field to filter the flow report results based on the system and flow entities. The Search alphanumeric field is located in the report header. Searchable system entities include device, interface, site, tag and WAN parameters. Searchable flow entities include IP address, DSCP, port, protocol and application.

- Click on the Search field to begin typing in the desired search parameters.
- The general syntax of the search field is shown in the example displayed as a default entry.
- (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
- Use the Enter key to apply the search. Click on the 'X' to clear the search field. Click on the down carat symbol to display a history of previous searches. The searches are kept on a per client basis; the history is removed with the LiveNX Client is closed.
- Boolean expressions OR = 'l' and AND = '&'; grouping uses '()')

The Search editor provides tool tips to assist in creating the search expressions. Click on the desired entity to add it to the expression. NBAR uses dynamic lists based on the capability of the device.

Top Analysis 09/09/19, 05:38:13 PM to 09/09/19, 05:53:13 PM					
Source RTR_Austin	Source RTR_Austin				
Filter *DefaultFilterGroup ᅌ 😽 Outbour					
Search flow.app.nbar=	3com-amp3				
Time Sep 9, 2019 5:38:13 PM Sep 9, 2019 5:38:15 PM Sep 9, 2019 5:38:17 PM Sep 9, 2019 5:38:18 PM Sep 9, 2019 5:38:18 PM Sep 9, 2019 5:38:21 PM	3com-tsmux 3pc 4chan 58-city 914c/g 9pfs CAllic 05:38:02.000 PM 05:38:	Src Country .000 PM - .000 PM - .000 PM - .000 PM - .000 PM - .000 PM -			

Filtering can also be done through the Filter combo box; filtering is done first with the combo box and then the Search alphanumeric field. The Search is done with a one pass search. In addition, the system level entities need to be in a single clause. For example, (site = Honolulu | site = Chicago) & flow.ip=1.1.1.1 is allowed, but (site = Honolulu & flow.ip=1.1.1.1) | (site = Chicago & flow.ip=1.1.1.1) is not allowed.

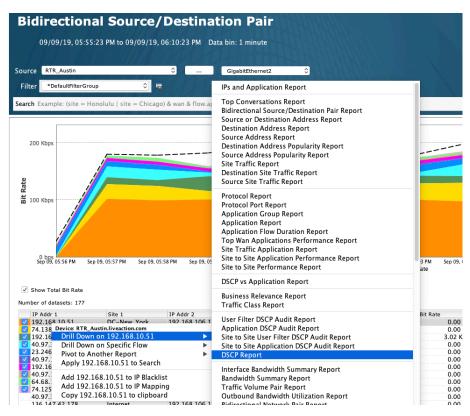
LiveNX supports a large number of system and flow searchable entities. Click on the ? to display the list of searchable entries as well as some example search expressions.

● ● ● Flex	Text Search
Q	
▼ Example	
site=Honolulu & wan	Flows from specific site with WAN-tagged interfaces
flow.dscp=EF	Flows with DSCP EF markings
flow.ip.src=1.1.1.1	Flows with specific source IP
flow.ip.dst=1.1.1.1 & flow.ip.src=2.2.2.2	Flows with specific source and destination IP
flow.ip.site=Honolulu	Flows from specific source or destination site
flow.ip.site.src=Sacramento	Flows from specific source site
flow.ip.site.dst="New York"	Flows from specific destination site
flow.ip=1.1.1.0/24	Flows with source or destination ip that match /24
flow.ip=192.168.0.55/0.0.255.0	Use of wild cards to match flows with ip address where 3rd octe
flow.srclp=172.16.1.0 & flow.srcMask=24	Flows with source ip that match /24
flow.device=Cisco1811 & flow.interface=FastEthernet0	Flows from specific device and interface
flow.device=Cisco1811 & flow.interface.in=FastEthernet0	Flows from specific device and in bound on interface
flow.app=ms-lync	Flows identified as ms-lync
flow.protocol=TCP	Flows that are TCP traffic
(site=A site=B) & tag=Primary	Flows from site A or B over interfaces tagged as Primary
▼ System	
group	group=Engineering
device	device=Cisco1811
interface	interface=FastEthernet0
(Name)	

(Description)

Drill Down/Change Report

When viewing a time-series or aggregation flow report, you can drill-down to provide in-depth analysis of a particular flow in the report or change the flow report without changing the report configuration options. If you would like to drill down to see details on a particular entry, click on the desired flow, right-click and choose a drill down option.



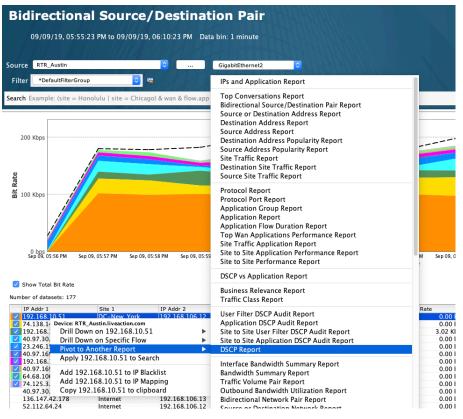
In this example, selecting Drill Down on 192.168.10.51 and then selecting DSCP report creates a DSCP flow report as a tabbed selection next to the Bidirectional Network Pair report. The drilled down DSCP report shows the DSCP values filtered on the IP address chosen from the previous chart. The Filter: IP designation is automatically added to the Tags and Filters configuration header of the flow report.

ource	RTR_Austin	:23 PM to 09/09/19, 06	o	GigabitEthernet2	
Filter	*DefaultFilterGro	up 🚺 📼	Outbound		
	flow.ip=192.168.1			Report	_
Bit Rate	100 Kbps 90 Kbps 80 Kbps 70 Kbps 50 Kbps 40 Kbps 30 Kbps 20 Kbps 10 Kbps		Bandu Traffi Outbo Bidire Source Netwo Source AS Pa Source Destii Interf	ace Bandwidth Summary Report vidth Summary Report c Volume Pair Report ctional Network Pair Report e or Destination Network Report ork Pair Report e Network Report ation Network Report ctional AS Pair Report e or Destination AS Report ir Report e AS Report ation AS Report ace Bandwidth Report ter Site Bandwidth Report	
Number DS	Device: RTR_Austin Drill Down on (Drill Down on S	D (BE) Specific Flow	App C App C Site C Site C Servic Servic VPN F VRF R	Group (DSCP) Bandwidth Report Group (DSCP) Bandwidth by Site Report Group (DSCP) Bandwidth by Service Provider Report apacity Utilization Report apacity Utilization by App Group (DSCP) Report apacity Utilization by Service Provider Report e Provider Bandwidth Report te Provider Bandwidth by App Group (DSCP) Report te provider Bandwidth by Site Report teport eport	Se p 09 : Bit Rate
	Pivot to Anothe Apply 0 (BE) to		Destin Source Device	Filter Report Iation Country Report e Country Report e Flow Count Report cation with Group Report	

To drill down further, select the desired DSCP value and select another report. In this case, selecting the Drill Down on 0 and then selecting Source Country report will create a Source Country flow report as

another tab, filtered by IP address and DSCP value. The resultant flow report will indicate both the Filter. IP and the Filter: DSCP in the Tags and Filters section of the flow report.

You can change report from a given flow report using the same report configuration parameters by right-clicking on a flow in the table and be selecting one of the other reports in the drop-down menu. Instead of using the Drill Down feature, which automatically filters the list, selecting a report will create a new unfiltered flow report as another tab. In this example, highlighting a flow and clicking on DSCP report will create another DSCP report as a second tab, this time with no filters.



Since it is not a Drill Down on type report, LiveNX creates another DSCP tab containing a DSCP flow report that does not have an IP filter in the Tags and Filters section.

IP Addr 1	Site 1	IP Addr 2
192.168.10.	DC New Yest	103 100 100 13
74.138.149.	Device: RTR_Austin.liveaction	
192.168.10.	Drill Down on 192.168	
40.97.30.13	Drill Down on Specific	Flow 🕨
23.246.15.1	Pivot to Another Repor	t 🕨
40.97.169.1	Apply 192.168.10.51 t	o Search
192.168.10.		o o cui chi
40.97.169.1	Add 192.168.10.51 to	IP Blacklist
64.68.106.1	Add 192.168.10.51 to	IP Manning
74.125.3.74	Copy 192.168.10.51 to	
40.97.30.13	Copy 192.168.10.51 to	o clipboard

Right-clicking on an Address flow report allows three other features: Add to IP Blacklist, Add to IP Mapping, Copy to Clipboard.

- Add to IP Blacklist right click on the desired IP address in an Address flow report and select Add to IP Blacklist to move this IP address to the blacklist stored in LiveNX. Details on the IP Blacklist can be found in Chapter 11 Tools.
- Add to IP Mapping right click on the desired IP address in an Address flow report and select Add to IP Mapping to bring up the Add IP Mapping dialog box. Details on the IP Mapping feature can be found in Chapter 11 – Tools.

• Copy IP Address to Clipboard – right click on the desired IP address in an Address flow report and select Copy IP Address to clipboard to copy the IP address to the client clipboard. In this example, using View by Application creates a Combined Application flow report using the selected flow.

Report Actions

There are seven report actions: Save, Save As, Delete, Schedule, PDF, Export to CSV and Help. The flow report has an additional report action: Create.

- Save LiveNX brings up a dialog box. Enter a report name in the dialog box. The report will be saved under Custom Reports.
- Save As after selecting a saved report for viewing, if you change any report attribute (e.g., time span, device, interface), you can create a new custom report by clicking on Save As and naming the report with a different report name.

Note LiveNX will not allow you to save another custom report with the same report name.

Save Report A	۹s
t Name:	
OK	Cancel
	t Name:

• Create – create a custom flow report choosing a user-defined title and report fields. By clicking and dragging on the headers shown in the Preview window, you can further customize your flow report by reordering the data fields within your report. Clicking on Create will add the new custom report to the Custom Reports section. The Create feature is available for Admin users only.

		by cc,	Facket	Statist	ics.							
eys												
Q												
Selected	Na	ame	Field I	Name	Search S	tring	Field ID (v9)	IPFIX	ID	PE	N	
V	Pro	otocol	protoc	olIdenti	flow.prot	ocol	4	4		0		-
	Sro	DSCP	ipClass	sOfServ	flow.tos.s	src	5	5		0		1
V	Sro	Port	source	Transp	flow.port	.src	7	7		0		
V	Sro	: IP Addr	source	IPv4Ad	flow.ip.sr	c	8	8		0		
	Src	Prefix Len	source	IPv4Pr	flow.mask	c.src	9	9		0		
	In	IF	ingres	sInterface	flow.ifidx	.in	10	10		0		
1	Dst	t Port	destin	ationTr	flow.port	.dst	11	11		0		
1	Ds	t IP Addr	destin	ationIP	flow.ip.ds	st	12	12		0		
	Dst	t Prefix Len	destin	ationIP	flow.mask	c.dst	13	13		0		
	Ou	t IF	egress	Interface	flow.ifidx	.out	14	14		0		
	Ne	xt Hop IP .	ipNext	HopIPv	flow.ip.ne	extHop	15	15		0		
	Src	: AS	bgpSo	urceAs	flow.as.sr	rc	16	16		0		
	Ds	t AS	bgpDe	stinatio	flow.as.d	st	17	17		0		
	BG	P Next Hop	bgpNe	xtHopI	flow.bgpN	Vext	18	18		0		-
		ing the hea	-									
Protocol	Src IP	Src Port	Dst I	Dst Port	Appli	Src C.	Dst C	Tot	Tot	Tot	Av	Av

- Delete deletes a report. Select a report name under Custom Reports and click on Delete.
- Schedule allows automatic generation and delivery of custom reports. Additional details can be found in the Report Scheduler section of this chapter.
- PDF allows creating and saving a pdf version of the report. For flow reports with multiple tabs, clicking on PDF provides a user-selectable choice between creating a PDF of only the current tabbed report or a PDF of all the tabbed reports in one collated report.
- Export to CSV allows you to save all the data shown in the table, which is useful for external analysis.
- Help launches the LiveNX User Guide.

Roles

Only Admin and Full Config users can add, edit, and delete reports. All other users can generate reports, including viewing saved reports.

Routing Reports

Routing reports give you information on routing adjacency history and events. You can access the reports by selecting Reporting > Routing > Reports in the main menu or clicking on the Reports button in the toolbar in the Routing tab.



LiveNX provides two types of routing reports as shown in the list in the top left-hand window. The Routing Adjacency History report displays any and all OSPF or EIGRP adjacencies established during the specified time period for a specified device or all devices. In between the two dropdown lists is a ... labeled button. Click to display a device pick list with an alphanumeric entry for searching the list. For more details on the device pick list, please see the Device Pick List section in the QoS reports. The Adjacency Events report shows the time-stamped history of adjacency status changes (from up to down, or down to up).

Note The neighbor up/down events in the Adjacency Events report is determined differently for OSPF, IS-IS, and EIGRP. For OSPF, a neighbor's up or down status indicates that the neighbor state changed from any of the non-full states to full, or from full to any non-full states, respectively. For IS-IS, up indicates that the adjacency state is up and down indicates that the adjacency state is down, init or failed. For EIGRP, a neighbor's up or down status is determined by whether the neighbor exists in the SNMP table.

			Routing Reports		
Type here to filter repo					
eports	Deutine Adie				
Routing Adjacency Events	Routing Adja	cency Even	[S		
Routing Neighbor History					
	11/14/16, 04:24:46 PM to	11/14/16, 05:24:46 PM			
ustom Reports	1h 6h 1d 1w Custom				
	In on Id In Cascom				
	All Devices	S	Execute Report		
			a Surana mana ang ang ang ang ang ang ang ang ang		
		1 Device	Protocol	Neighbor	Event
	Mon Nov 14 16:24:46 PST 2016	cat3850APN-214	OSPF	10.254.252.213	🔁 Full
	Mon Nov 14 16:24:46 PST 2016	cat3850APN-214	OSPF	10.254.254.212	E Full
	Mon Nov 14 16:24:46 PST 2016	cat3850APN-214	OSPF	10.254.249.215	🔁 Full
	Mon Nov 14 16:24:47 PST 2016	c1811-ES-11	EIGRP	192.168.15.10	
	Mon Nov 14 16:24:47 PST 2016	c1811-ES-11	EIGRP	192.168.10.1	
	Mon Nov 14 16:24:58 PST 2016	c1941-ES-12	EIGRP	192.168.11.2	D Up D Up
	Mon Nov 14 16:24:58 PST 2016	c1941-ES-12	EIGRP	192.168.10.2	Up
	Mon Nov 14 16:25:09 PST 2016	c2921-ES-13	EIGRP	192.168.11.1	D Up
	Mon Nov 14 16:25:09 PST 2016	c2921-ES-13	EIGRP	192.168.12.14	Z Full
	Mon Nov 14 16:25:35 PST 2016 Mon Nov 14 16:25:35 PST 2016	c1941APN-212 c1941APN-212	OSPF	10.254.253.213 10.254.255.216	S Full
	Mon Nov 14 16:25:35 PST 2016 Mon Nov 14 16:25:35 PST 2016	c1941APN-212 c1941APN-212	OSPF	10.254.255.216	Z Full
	Mon Nov 14 16:25:35 PST 2016 Mon Nov 14 16:25:38 PST 2016	c1941APN-212 cisco2921APN-216	OSPF	10.254.254.214	Full
	Mon Nov 14 16:25:38 PST 2016 Mon Nov 14 16:25:38 PST 2016	cisco3850APN-215	OSPF	10.254.249.214	Full Full
	Mon Nov 14 16:25:38 PST 2016 Mon Nov 14 16:25:38 PST 2016	cisco3850APN-215	OSPF	10.254.250.213	E Full
	MOIT NOV 14 10.23.38 F31 2010	CISC03830AFI4-213	OSFF	10.234.230.215	Ca Full
	1				
oort Actions					
/e					
re As					
ete					
edule					
ort to CSV					
p					

The Routing Neighbor History report displays all OSPF, IS-IS or EIGRP adjacencies established during the specified time period for a specified device or all devices.

-		Routing Reports		
. Type here to filter rep	01			
Reports	Routing Neighl	or History		
Routing Adjacency Ev	ents Kouting Neight	JOI HISLOLY		
Routing Neighbor Hist	ory 11/14/16, 04:25:15 PM to 11/	14/16 05:35:15 04		
Custom Reports	11/14/16, 04.25.15 PM to 11/	14/16, 05:25:15 PM		
	1h 6h 1d 1w Custom			
	the second se	Execute Report		
	All Devices	C Execute Report		
	Device		Neighbor	
	c1941-ES-12	Protocol EIGRP	192.168.11.2	
	c1941-ES-12 c1941-ES-12	EIGRP	192.168.10.2	
	c1941-ES-11	EIGRP	192.168.15.10	
	c1811-ES-11	EIGRP	192.168.10.1	
	c2921-ES-13	EIGRP	192.168.11.1	
	c2921-ES-13	EIGRP	192.168.12.14	
	cat3850APN-214	OSPF	10.254.252.213	
	cat3850APN-214	OSPF	10.254.249.215	
	cat3850APN-214	OSPF	10.254.254.212	
	cisco2921APN-216	OSPF	10.254.255.212	
	cisco3850APN-215	OSPF	10.254.250.213	
	cisco3850APN-215	OSPF	10.254.249.214	
	c1941APN-212	OSPF	10.254.253.213	
	c1941APN-212	OSPF	10.254.255.216	
	c1941APN-212	OSPF	10.254.254.214	
port Actions				
ve				
ve As				
lete				
nedule				
F				
port to CSV				
lp				

The length of historical data is selectable at the top of the chart, and there are five to choose from 1h (one hour), 6h (six hours), 1d (one day), 1w (one week) and Custom. When selecting Custom, select the desired Start Time and End Time for the report. Select the desired device or All Devices in the combo box.

			Routing Reports		
Q+ Type here to filter repor			Constraint and a second se		
Reports Routing Adjacency Events	Routing Adjac	ency Event	S		
Routing Neighbor History	11/14/16, 04:25:55 PM to 1	1/14/10 05:25:55 04			
Custom Reports		.1/14/16, 05:25:55 PM			
10000000000000000000000000000000000000	1h 6h 1d 1w Custom				
	All Devices		Execute Report		
	All Devices	••••••••••••••••••••••••••••••••••••••	Execute Report		
	Ti 7609_143	U			
	MAPN-AS-17		Protocol	Neighbor	Event
	MAPN-AS-17 MAPN-AS-18		EIGRP	192.168.15.10 192.168.10.1	🗾 Up 🗾 Up
	MAPN-A5-10 MAPN-CAT_3560_10		EIGRP	192.168.10.1	
	MAPN-CAT_3560_10 MAPN-CAT_3560_14		EIGRP	192.168.12.14	
	MAPN-CA1_3560_14 MAPN-DS-15		EIGRP	192.168.11.2	
	MAPN-DS-15 MAPN-DS-16		EIGRP	192.168.10.2	
	Mon Nov 14 16:26:37 PST 2016	cisco3850APN-215	OSPE	10.254.249.214	A op A Full
	Mon Nov 14 16:26:37 PST 2016	cisco3850APN-215	OSPF	10.254.250.213	A Full
	Mon Nov 14 16:26:38 PST 2016	cisco2921APN-216	OSPE	10.254.255.212	D Full
	Mon Nov 14 16:26:47 PST 2016	cat3850APN-214	OSPF	10.254.252.213	Full
	Mon Nov 14 16:26:47 PST 2016	cat3850APN-214	OSPF	10.254.254.212	🖸 Full
	Mon Nov 14 16:26:47 PST 2016	cat3850APN-214	OSPF	10.254.249.215	🖸 Full
	Mon Nov 14 16:30:35 PST 2016	c1941APN-212	OSPF	10.254.253.213	🖸 Full
	Mon Nov 14 16:30:35 PST 2016	c1941APN-212	OSPF	10.254.255.216	🔽 Full
	Mon Nov 14 16:30:35 PST 2016	c1941APN-212	OSPF	10.254.254.214	🔁 Full
	Mon Nov 14 16:30:35 PST 2016	c1941APN-212	OSPF	10.254.253.213	🔁 Full
		c1941APN-212	OSPF	10.254.255.216	🔼 Full
	Mon Nov 14 16:30:35 PST 2016	c1941APN-212	OSPF	10.254.254.214	Full
	_				
Report Actions					
Save					
Save As					
Delete					
Schedule					
PDF					
Export to CSV					
Help					

Click Execute Report to generate a report. Any report configuration can be saved as a custom report for easy retrieval at a later time.

IP SLA Reports

IP SLA reports give you in-depth information on the tests running in LiveNX. You can access the reports by selecting the Reporting > IP SLA > Reports menu item in the main menu or clicking on the Reports button in the toolbar in the IP SLA tab.

∏ ● ●				IP SLA Rep	orts							
Type here to filter repo												_
Reports			11 11 14	1063963030								
Overall Health	IP SLA	Overa	II Healt	th is a second								
Overall System Health	11/14/16,	04:23:12 PM	to 11/14/16	5, 05:23:12 P	М							
Single Test Time Series	1b 6b 1d	1w 30d Cus	tom									
Single Type Health	In on Iu											
Video Operation Threshold	► Warning Th	rocholde			Execute Report							
Video Operation Time Serie	- wanning m	resiloius		TT DESTRUCTION	Execute Report							
Custom Reports												<u> </u>
Ch health	I.I. There	T	Dec. inc.	Description of the second s	Laura Laura and L		a Lana (a a de		-1.00			
Test - Test	ld Type	Tag	Device	Destination	Avg Latency (Avg Jitter (Av 1.00				rning Errors	Reco	
Test-Test	1 Jitter 2 Jitter		c1811-ES-1	10.254.254.212	0.00	228.15	0.00	4.06	31 13	0	0	3
lest-lest	2 Jitter 76 DNS	DNS Server 2			75.21	228.15	0.00	4.06	13	0	0	-
		Layer 2 Test	Cisco6509_1	mail.google.com	721.00				1	0	0	
	10 ICMP Echo		Cisco6509_1		811.00				1	0	0	
	77 DNS	DNS Server 2		mail.google.com	506.00				1	0	0	
	69 DNS	DNS Server 2 DNS Server 1		mail.google.com	282.00				1	0	0	
	4 Jitter	Divo Server 1	c1811-ES-1		99,94	247.77	0.00	2.85	0	13	0	1
		Layer 2 Test	Cisco6509_1		6,826.00	247.77	0.00	2.05	0	13	0	
		Layer 2 Test	Cisco6509_1		1,676.00				0	1	0	
	78 DNS	DNS Server 2		mail.google.com	1,161.00				0	1	0	
	74 DNS	DNS Server 2		mail.google.com	6,267.00				0	1	0	
		Laver 2 Test	Cisco6509_1		1,429.00				0	1	0	
		Laver 2 Test	Cisco6509_1		8.002.00				0	1	0	
	5 Jitter		c1811-ES-1		98.15	222.92	0.00	2.85	0	13	4	1
	75 DNS	DNS Server 2		mail.google.com	6,507,00	and the		2100	0	1	0	
	2 ICMP Echo	Laver 2 Test	Cisco6509_1		1,558.00				0	1	0	
	71 DNS	DNS Server 1		mail.google.com	5,564.00				0	1	0	
port Actions		Layer 2 Test	Cisco6509_1		2,400.00				0	1	0	
	1 Jitter		c1811-ES-1		91.39	246.69	0.00	2.85	0	13	1	1
ave	70 DNS	DNS Server 1	Cisco6509_1	mail.google.com	2,233.00				0	1	0	
ave As	3 ICMP Echo	Layer 2 Test	Cisco6509_1	30.30.10.5	11,891.00				0	1	0	
	72 DNS	DNS Server 1	Cisco6509_1	mail.google.com	6,087.00				0	1	0	
elete	3 Jitter		c1811-ES-1		97.78	232.25	0.00	2.85	0	12	5	1
chedule		Layer 2 Test	Cisco6509_1		5,149.00				0	1	0	
chequie	73 DNS	DNS Server 1	Cisco6509_1	mail.google.com	12,573.00				0	1	0	
DF												
kport to CSV												
lelp												

Time Ranges

You can view report data for the following time ranges:

- 1h one hour
- 6h –six hours
- 1d one day
- 1w one week
- 30d thirty days
- Custom (specify a custom date and time range for the report)
- Click on a time range in the report header to select it.

Warning Thresholds

Warning thresholds allow you to customize the dashboard parameters. Click the "+" icon next to the "Warning Thresholds" label to expose the following options:

- Video video test types include telepresence, IP TV, and VSC. Latency, loss, and jitter values are configurable, allowing you to fine-tune the test to your needs.
- Voice the MOS score is used to determine health.
- Data Applications data applications are a collection of IP SLA test types, including, DNS, DHCP, HTTP, FTP, PATH_ECHO, UDP_ECHO, and ICMP_ECHO tests. Latency is the most important value for these tests.

Available Reports

Several default report types are shown in the left-hand tree view:

- Overall Health displays a table with the average IP SLA test results and health values for all tests.
- Overall System Health displays the same values as the Overall Health report, but results are aggregated by system test instead of individual tests.

- Single Test Time Series displays a time series report for an individual IP SLA test.
- Single Type Health displays the min/max/average and health values for a single test type (DHCP, DNS, FTP, etc.). You can run the report for all devices or a single device that you specify. The columns in the report change depending on the test type. For example, a data application test type will only show latency, whereas a video test will show latency, loss, and jitter.
- Video Operation Threshold displays the health attempts of all video tests. You can run the report for all devices or a specified device. Video Operation Time Series displays the loss, jitter, and latency values of all videos tests on all devices or a specified device in a time-series report.

Device Pick List

The Single Test Time Series, Single Type Health, Video Operation Threshold and Video Operation Time Series reports provide a device drop-down menu and a ... labeled Device Pick List button. Click to display a device pick list with an alphanumeric entry for searching the list. For more details on the device pick list, please see the Device Pick List section in the QoS reports.

Drilling-down to Reports

You can drill-down from a report to see a different view of the data. For example, you can right-click on a row in the Overall Health report to display a time-series report of the selected test.

Saving Reports

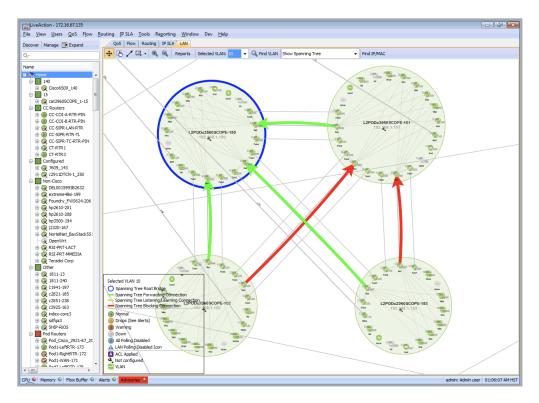
You can configure a report and save the selected parameters, making it easy for you or other users to run the report at a later time. Configure the parameters of the report and then click the Save or Save As button in the lower-right section of the IP SLA Reports dialog.

Printing and Exporting Reports

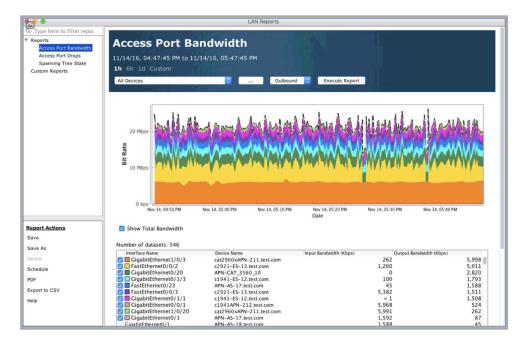
Click the "View HTML" button to create an HTML file of the report, making it easy to print and share the report. Click the Export to CSV button to export the data shown in the report to a comma-separated value file. Additional Ways to Create Reports Reports can be created from the system topology view. Find a test that you want to run a report on, right-click the test's edge and select Show Time Series Report. Reports can also be created from the IP SLA device view. Right-click on an item in the test legend (right-hand panel), and select Show Time Series Report.

Lan Reports

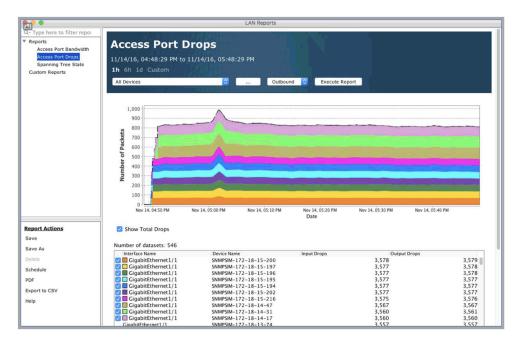
LAN reports provide detailed results on the bandwidth, drops and spanning tree state for both the entire system and for individual devices. The LAN reports can be accessed by clicking on either the Reporting > LAN > LAN Reports. LAN Reports can be accessed by the Reports button in the toolbar in the LAN tab. The image below shows where the Reports button is located in the LAN tab.



LiveNX provides three reports as shown in the list at the top left-hand side in the window below: Access Port Bandwidth, Access Port Drops and Spanning Tree State. For the access port reports, the length of historical data is selectable at the top of the chart: 1h (last hour), 6h (last six hours), 1d (last day) and Custom. When selecting Custom, the select the desired Start Time and End Time for the LAN Report. The image below shows a Device Bandwidth chart with a time span of one hour. When choosing the Access Port Bandwidth report, select the desired device and Inbound or Outbound using the two respective combo boxes. Click on the Execute Report button to display the desired data. The table accompanying the chart describes the access ports and their input and output bandwidths in Kbps. Specific access ports can be viewed in the chart by enabling or disabling them via the check boxes next to their names in the table.



When choosing the Access Port Drops report, select the desired device and Inbound or Outbound using the two respective combo boxes. Click on the Execute Report button to display the desired data. The table accompanying the chart describes the access ports and the number of packets dropped in both directions in the desired timeframe.



When choosing the Spanning Tree State Report, select the desired time, VLAN and either All Devices or a specific device using the dropdown menu. Click on Execute Report to display the desired data.

Note The Spanning Tree State Report tabulates information at a specific point in time and not over a time period. The Spanning Tree State Report is not available as a Scheduled Report.

					LAN Reports				
२ . Type here to filter repo		Mart II	W.M.A.A.K.A	114	Hansen and the second second				
Reports	Snanni	ina	Tree St	tate	Report				
Access Port Bandwidth				luce	Report				
Access Port Drops	11/14/16, 05	:49:00	PM						
Spanning Tree State		e ᅌ							
Custom Reports	Current Time	e 🗢	VLAN: 1		All Devices	\$	Ex	ecute Report	
	Device Na ^{A 3}	Prior	Is Root Br 72	Root Br	idae 🔺 1	Port T	Interface N	Connected To Device	Connected To Inte A
	c2921-ES-13	32768	Y	c2921-E		Designated		APN-CAT_3560_14	GigabitEthernet0/3
	c2921-ES-13	32768	Y	c2921-E	S-13	Designated	FastEthernet0/0/2		
	c2921-ES-13	32768	Y	c2921-E		Designated	FastEthernet0/0/3		
	APN-CAT_3560		N	c2921-E		Root	GigabitEthernet0/3		FastEthernet0/0/1
	APN-CAT_3560		N	c2921-E		Designated	GigabitEthernet0/2		
	APN-CAT_3560 c1941APN-212	32768	N	c2921-E		Designated	Port-channel1	 Bridge ID 24626.00-1e-49-16	
	C1941APN-212	32768	N	Bridge I	ID 24626.00-1e-49-16	ROOT	GigabitEthernetu	. Bridge ID 24626.00-1e-49-16	STP Port #16
eport Actions									
ive									
ave As									
elete									
chedule									
DF									
xport to CSV									
lelp									
	11.1								

The Access Port Bandwidth and the Access Port Drops reports include a ... labeled button. Click to display a device pick list with an alphanumeric entry for searching the list. For more details on the device pick list, please see the Device Pick List section in the QoS reports. Custom reports can be created using the Save or Save As button. Once a desired report is saved, the report name appears in the Custom Report list. After a custom report is created, it can be scheduled using the report scheduling feature. There are six buttons for the LAN reports: Save, Save As, Delete, View HTML, Export to CSV, and Help. These buttons work the same way as the ones for the QoS and routing reports.

Report Scheduler

In the Reporting tab, click Reports > Schedule.

Report Scheduling	1000					(c
Report will e Weekly report will b Report will e Monthly report will b	e created on the created from 12 xecute the next d e created from (xecute on Saturd be created from 1	11 And to 11 And the second se	:59 PM hh:mm	- hh:mm		
Send Email Notific	cations					
SMTP server	: smtp.gmail.cor	m			Configure	
Recipient addresses (comma-seperated)		tion.com				^
Max rows per report	for the hyperlin httpserver.ho	ks for the custom i	he LiveAction Server' reports in the email t LiveAction Manager	to work. To set the nent Console.	hostname, set the	n order
Max rows per report Attach Reports	for the hyperlin httpserver.ht : 200	ks for the custom i	reports in the email f	to work. To set the	hostname, set the	•]
Attach Reports	for the hyperlin httpserver.ho : 200 - : Technology	ks for the custom i	reports in the email f	to work. To set the nent Console.	All Reports	•]
Attach Reports	for the hyperlin httpserver.ht 200 - : Technology FLOW FLOW FLOW FLOW FLOW FLOW	ks for the custom i ost property in the	reports in the email 1 LiveAction Manager	to work. To set the nent Console. Collate:	hostname, set the	•]
Attach Reports Sustom Reports Report AppDscp BKPPort CPU yearly Clarkstest2 IPs and Ports IPsAndPorts	for the hyperlin httpserver.ht 200 - : 200 - :	Hourly	Daily	weekly	hostname, set the	upings
Attach Reports Custom Report Report AppDscp BKPPort Clarkstest2 IPs and Ports IPsAndPorts KTN Qtrly Test R	for the hyperlin httpserver.ht 200 - : 200 - :	Hourly	Daily	weekly	hostname, set the	upings

Report Schedule Options

Each scheduled report can be run on a daily, a weekly and/or a monthly schedule. The Report Schedule Options allows the LiveNX administrator to schedule the specifics of the daily, weekly and monthly reports.

The hourly report creates a report at the top of each hour and will begin when you define the hourly report. The start times are fixed to be at the start of each hour and the reports are stored with a unique name indicating the time range per day. The daily report creates a report with data collected within the user-defined start and end times. The start time default is 12:00 AM and the stop time default is 11:59 PM.

The daily report begins at the user-defined execute time; the default is 12:30 AM. Times are based on the LiveNX Server's local time. To minimize CPU impact, create the reports during low traffic time periods.

The weekly report will create a report with data collected within the user-defined start and end dates. Seven 7-day options are available in the drop-down, one for starting the weekly report on each day of

the week. The default is a 5-day Monday to Friday report. In all weekly reports, the report collects data from 12:00 midnight on the first day and ends at 11:59 PM on the last day. The weekly report will be generated on the day after the report end date; default time is 2:00 AM. To minimize CPU impact, create the weekly reports during low traffic time periods.

Note When upgrading from a LiveNX version earlier than 3.15, any existing weekly reports may have incomplete data during the first week after the upgrade. LiveNX version 3.15 and higher creates the weekly reports from the long-term database, and this requires several days of data to create the initial report.

The monthly report will create a report with data collected from the first to the last day of the month. To minimize CPU impact, create the monthly reports during low traffic time periods.

Long-Term Reports

LiveNX can generate long-term reports by using aggregated flows for faster results when dealing with reports that span greater than multiple days. Details of the aggregated flows can be found in Chapter 7 – LiveNX Flow, under LiveNX NetFlow Process Overview. The long-term reports using aggregated flows can be generated by:

- Creating custom reports and scheduling it for one week or one month
- Creating ad hoc reports that match the flow dashboards source that is greater than four days

Schedule long-term reports by selecting the Weekly or Monthly check box in the Report Scheduling dialog box or right click on a saved custom report name in the Flow Report Tree and right click on Add to schedule.

Flow Reports	
Q- Type here to filter reports.	Destination Country
Reports Interface Bandwidth Top Analysis Address Applications	Destination Country
Protocol Application Pos Network	Source All Devices All Interfaces Filter *DefaultFilterGroup Gutbound G
Applications (AVC) Avecage NSEL PfR Wireless	Search Example: (site = Honolulu site = Chicago) & wan & flow.app = webex-meeting
Miscellaneous Custom Reports Destination Country New Report Add to schedule	

Choose Weekly or Monthly to add it to the Report Schedule.

Schedule Destination Country
Schedule this report:
Daily Veekly V Monthly
See Report Scheduling dialog for details on the scheduled time.
*Flow search filters are not applied for long term reports
OK Cancel

Send Email Notifications

Clicking on the Send Email Notifications check box enables the e-mail service.

When the check box is enabled, the Configure... button becomes active.

Recipient Address: enter the desired recipients' e-mail addresses separated by commas.

Go to the LiveAction Management Console and enter the LiveNX Server's IP address or hostname in the HTTP server. host field in the Properties tab. This allows the hyperlinks for the custom reports in the e-mail to work. Click on Apply and then Stop and Start the LiveNX Server for the configuration change to take effect.

Max Rows Per Report: Use the up or down arrows to increase or decrease the size of the individual report. The minimum size is 50 rows; the default is 200 rows.

Click on Attach Reports to include the scheduled reports as PDF attachments.

Click on the Collate and choose among All Report, By Technology or Custom. Choose All Reports to group the reports in alphabetical order. Choose By Technology to group the scheduled reports so all the QoS reports are together, all the Flow reports are together, etc. Choose Custom to collate scheduled reports in a user-configurable manner. Click on Edit Custom Groupings, use the Add button to define a custom report group, select from the other reports column and add that to the current group of reports. Your reports will now get collated based on the group definitions.

Add Group		×
Name (*)		
All Other Reports		Current Group of Reports
QT	•	Q
AG Bandwidth by Site	Ð	
AP Bandwidth by SP		
Access Port Bandwidth		
Access Port Drops		
Alerts All		
Alerts by Application Gro		
Alerte by SP		

For details on Configure, please see Options below.

Scheduled Reports

LiveNX automatically populates the Scheduled Reports with a compilation of all the Custom QoS, Flow, Routing, IP SLA, and LAN report.

- Select the desired custom reports for automatic generation by clicking on the Daily or Weekly check box in the list.
- Uncheck the check box to remove the particular report from the automatic Daily or Weekly schedule.

Custom Dashboard

The Custom Dashboard allows users to create a user-defined dashboard that displays data for different technologies. Go to Reporting > Custom Dashboard.

Any number and any combination of chart types can be added to the Custom Dashboard: Flow, NBAR, Class, Interface, and Destination. Drag and drop a chart icon into the custom dashboard window in the desired order.



By dragging charts into the custom dashboard window, any combination of the five chart types can be displayed in the Custom Dashboard. The nine horizontal and vertical dots next to each chart are used as separators between adjacent charts and function as size controls. When you put the cursor over a size control, the cursor changes to a double-sided arrow, and you can shrink or expand the chart in the horizontal or vertical direction by using the horizontal or vertical size controls, respectively. Putting the cursor over a chart's title bar changes the timestamp on the right-hand side to two icons: a close icon in the right-hand corner and a collapse or expand chart icon to the left of the close icon.

A new Custom Dashboard is created by clicking on the New button at the top left-hand corner of the custom dashboard window. Each Custom Dashboard can be renamed by double-clicking on the tab. The Hide Palette/Show Palette button allows the user to hide or to show the five chart icons at the bottom of the Custom Dashboard. The default setting is Show Palette. Once created, each Custom Dashboard is automatically saved when the user closes the custom dashboard window. Details of each chart are shown on the following pages.

CHAPTER 6

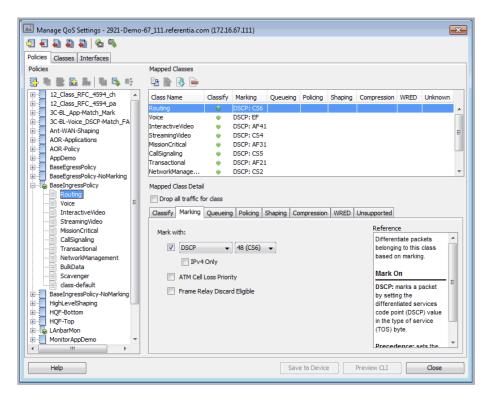
QoS

In this chapter:

About QoS	116
VLAN Service Policies	. 127
QoS Monitoring	. 129
QoS Usage and Applications	. 138

About QoS

The LiveNX QoS user interface provides easy navigation and management of QoS policies at the system, device, and interface levels. This section describes the major screens, operations, and functionality of LiveNX QoS. The tree view on the left side of the screen displays the various devices and interfaces and allows quick navigation. The color indicator on the devices and interfaces changes to orange when congestion or drops are occurring, and to green if the device or interface is operational. A similar set of QoS features is available from the QoS menu.



QoS Configuration

LiveNX QoS configuration capabilities give you the power to read, edit, save, and share QoS policies across your Cisco devices. The QoS settings for your routers allow you to classify traffic into different categories, and provide different levels of service for these traffic types in order to meet the specific network utilization objectives of your organization.

LiveNX reads the QoS settings in your device and displays them on the Manage QoS Settings screen, where you can perform any number of configuration changes. These include creating or removing policies and classes, adding match statements to classes, mapping classes to policies, configuring specific feature actions (such as marking, queuing, policing, and shaping) within a given mapped class, and managing hierarchical policy relationships.

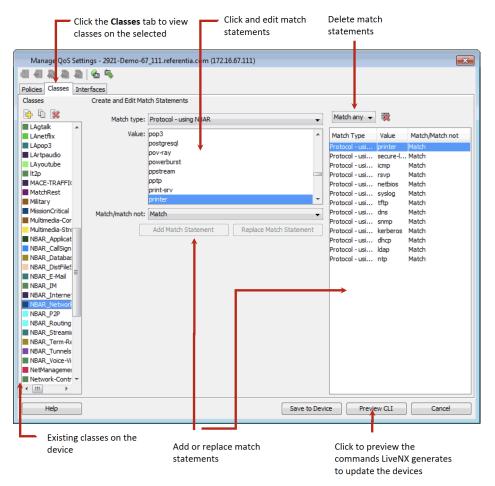
The QoS capabilities of LiveNX allow you to create policies from scratch, or from templates and wizards. Combined with its in-depth QoS monitoring capabilities, the software provides real-time feedback on how well the configuration is working. A built-in ACL editor is provided to create rules for use with QoS, if needed. Policies can be saved as individual files to be shared with other users. Snapshots save all the QoS settings in a particular router to a single file, which can be used for backup and to restore the router to previous states.

Manage QoS Settings Screen

You can create and edit the device configuration elements in any order. Click Preview CLI at any time to see the commands that will be used to send the changes to the device. If you enter invalid or conflicting

values, an error will appear in the affected area, and you will not be able to save or preview your changes until the error has been corrected.

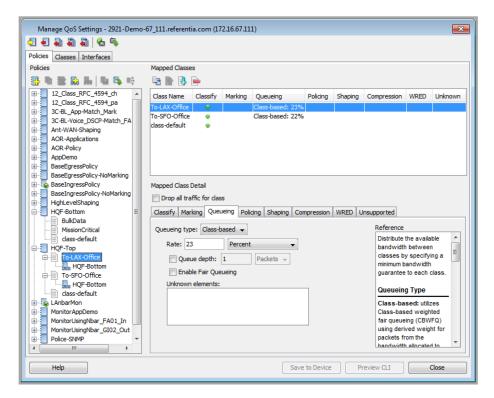
The main Manage QoS Settings screen provides all the QoS capabilities of the router within a single dialog box. This dialog box can be accessed by right-clicking on any of the devices or their interfaces, or from the QoS menu. The tree view at left shows existing policies for the device and the Mapped Classes list shows the classes that make up the policy. The tabs below indicate the various QoS features available for the selected class.



Manage QoS Settings - 2921-Demo-	67_111.referentia.co	m (172.16	5.67.111)						— ×
🔁 🗐 🗿 🦣 🚳 🦠									
Policies Classes Interfaces									
Policies	Mapped Classes								
📑 🐂 📚 🔝 🐜 🐃 🛸 👳	🖳 🛃 📲								
	Class Name	Classify	Marking	Queueing	g Policing	Shaping	Compression	WRED	Unknown
IZ_Class_R+C_+39+_ba IZ_Class_R+C_+39+_ba IZ_Class_R+C_+39+_ba	Routing	۲	DSCP: CS6						A
3C-BL-Voice_DSCP-Match_FA	Voice	•	DSCP: EF						
Ant-WAN-Shaping	InteractiveVideo	•	DSCP: AF41						=
AOR-Applications	StreamingVideo	•	DSCP: CS4						-
AOR-Policy	MissionCritical	•	DSCP: AF31						
AppDemo	CallSignaling	•	DSCP: CS5						
BaseEgressPolicy	Transactional	•	DSCP: AF21						
BaseEgressPolicy-NoMarking	NetworkManage	•	DSCP: CS2						-
BaseIngressPolicy	Mapped Class Detail								
Routing	Drop all traffic fo	ar daga							
Voice E		or class							
InteractiveVideo	Classify Marking	Queuein	g Policing	Shaping (Compression	WRED	Unsupported		
StreamingVideo							Referen		
MissionCritical	Mark with:								kate 🔺
CallSignaling	DSCP		48 (CS6)					ntiate pac no to this	NG13
Transactional	USCP	•	48 (CS6)	•				ng to this on markin	
NetworkManagement	IPv4	Only					baseu (n markin	y.
BulkData							Mark ()n	
Scavenger	ATM Cell	Loss Prior	ity						
BaseIngressPolicy-NoMarking	Frame Re	elay Discar	d Eligible					marks a p	acket
HighLevelShaping			-				by setti	ng the itiated se	nuicee
HQF-Bottom								int (DSCI	
HOF-Top								pe of sei	
the LAnbarMon							(TOS) t		
MonitorAppDemo 🔻									-
							Precer	lence's	ets the
									-1
Help				Sa	ive to Devic	e	Preview CLI		Close

The marking tab allows device configuration control for DSCP or IP Precedence, ATM Cell Loss Priority and Frame Relay Discard Eligible. Enable the check box next to the DSCP drop-down and then select either DSCP or IP Precedence. After choosing DSCP or IP Precedence, use the adjacent dropdown box to define the DSCP or IP Precedence value. Enable the IPv4 check box to mark only IPv4 packets and disable the check box to mark IPv4 and IPv6 packets.

- Enable the ATM Cell Loss Priority check box to mark the ATM CLP bit.
- Enable the Frame Relay Discard Eligible check box to mark the FR DE bit.
- Default for all three check boxes is disabled.



Enable queueing capability by selecting either Class-based, Priority or Fair in the Queueing type: dropdown. The fourth option is None. Default is None. The Priority option is available when selecting a new class within a policy.

If Class-based is selected, then type in the desired Rate in either Percent (amount of guaranteed bandwidth as an absolute percent of available bandwidth), Percent of remaining (amount of guaranteed bandwidth as a relative percent of available bandwidth) or Kbps. Enable Queue depth to define the maximum number of packets a queue can hold for a class policy configured in a policy map. Enable Fair Queueing to extend standard fair queueing functionality to provide support for user-defined traffic classes.

If Fair is selected, enable Queue depth to define the maximum number of packets a queue can hold for a class policy configured in a policy map.

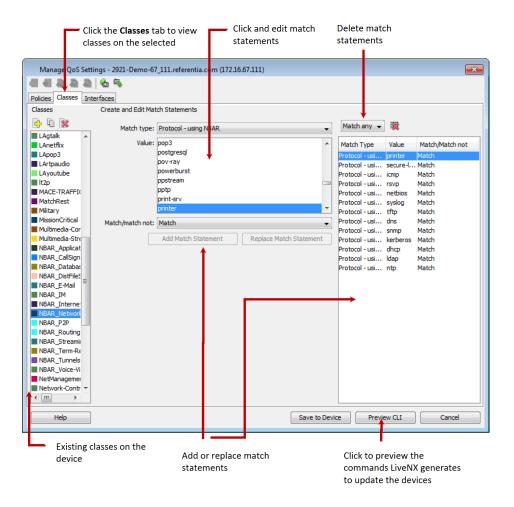
Hierarchical Queuing Framework (HQF)

LiveNX can monitor two-level QoS policies and limited three-level policies.

Manage QoS Settings - 2921-Demo	-67_111.referentia.com (172.16.67.111)	
5 🗐 🔊 🎝 🗿 🏀 🖏		
Policies Classes Interfaces		
Policies	Mapped Classes	
🚰 🐂 📚 🏡 🐜 👒 👒	🕒 🖿 🛃 🚔	
12 Class, RFC-4594, ch 12 Class, RFC-4594, pa 12 Class, RFC-4594, pa 3C-BL-App-Match_Mark 3C-BL-App-Match_Mark 3C-BL-App-Match_Mark 3C-BL-App-Match_Mark ACR-Applications ACR-Applications ACR-Applications ACR-Applications ASB-Applemo BaseEgressPolicy-NoMarking High-Bottom MosionCritical dass-default HQF-Bottom To-SFO-Office LoftbarMon LanbarMon LanbarMon	Class Name Classify Marking Queueing Policing Shap ToLAX-Office Class-based: 23% To-SPO-Office Class-based: 22% class-based: 22% class	
MonitorUsingNbar_FA01_In MonitorUsingNbar_GI02_Out Police-SNMP		fair queueing (CBWFQ) using derived weight for packets from the
Help	Save to Device	Preview CLI Close

Manage QoS Settings—Classes Tab

The Classes tab on the Manage QoS Settings screen allows the creation of classes by defining the various match criteria for classifying packets. The match types can be AND'ed or OR'ed together to create very specific class definitions. Select the IPv4 Only check box when setting up the class-map for matching on IP Precedence = 1.



See the following Image for an example of matching using NBAR2

- Choose Protocol using NBAR groups in the Match type drop-down.
- Choose the desired NBAR2 category using the Group drop-down: Application Group, Category, Sub Category, P2P Technology, Encrypted or Tunnel.
- Choose the desired NBAR2 value for the selected category in the Sub Group drop-down.

		11.referentia.com (172.	16.67.111)		-		
Policies Classes Interf							
T ORCES	Create and Edit Mat	-h Chatananata					
Classes	Create and Edit Mat	ion Statements					
📑 🗓 🕱	Match type:	Protocol - using NBAR gro	2010	-	Match any 👻 💥		
11C_BL_CallSignal			•	- 4			
11C_BL_CriticalDa		Select group and sub grou listed. Selecting individual	up to create match on all protocols	s	Match Type	Value	Match/Match not
11C_BL_Interactiv		isten, selecung inulvidual	protocoris optional.		Protocol - using NBAR	cuseeme	Match
11C_BL_IPRouting	Group:	category		-	RTP Protocol - using	al	Match
11C_BL_Network					Protocol - using NBAR	netshow	Match
11C_BL_Scavenge	Sub Group:	voice-and-video		-			
11C_BL_Streaming	Protocol:	Protocol	Description				
11C_BL_Transacti	(Optional)						
11C_BL_Voice_Col	(Optional)	airplay	Apple AirPlay wireless me	*			
12C-MN_BROADC		aol-messenger-audio	AOL Instant Messenger A				
12C-MN_BULK-DA		aol-messenger-video	AOL Instant Messenger Vi				
12C-MN_MULTIME		appleqtc	apple quick time				
12C-MN_MULTIME		appleqtcsrvr	appleqtcsrvr				
12C-MN_NETWOR		audio-over-http	Audio traffic over HTTP				
12C-MN_NETWOR		babelgum	Internet TV web platform				
12C-MN_REALTIM		cisco-ip-camera	Cisco video surveillance c	Ŧ			
12C-MN_SCAVENC	Match/match not:	Match		-			
12C-MN_SIGNALIN							
12C-MN_TRANSAC		Add Match Statement	Replace Match Statement	t			
12c-MN_VOICE 12C-MN_VOICE							
3C BL CallSignalin							
3C BL CriticalDatz							
3C BL Realtime A							
3C BL Voice DSC							
4EYES-Enclave							
Best-Effort							
Bittorrent							
۰ ۲							
Help					Save to Device	Previe	ew CLI Close
				_			

- Saved Access Control Lists (ACLs) can be used to create QoS classes.
- Go to the device tree view, click on the device with saved ACLs, right click on QoS and then choose Manage QoS Policies.

Manage QoS Setting	gs - 3925-VPN-163.re	ferentia.com (192.168.1.163)				23
	è 🖏					
Policies Classes Interf	aces					
Classes	Create and Edit Mat	ch Statements				
🔁 🗓 🕱	Match type:	ACI Name	Match all 👻 🗱			
AdTest						_
DMVPN-spoke1-bgp		adObject	Match Type	Value	Match/Match not	
DMVPN-spoke1-cusee		DMVPN-bgp-179 DMVPN-cuseeme-7648	ACL Name	DMVPN-bgp-179	Match	
DMVPN-spoke1-other		DMVPN-cuseeme-7648 DMVPN-other-13958				
DMVPN-spoke 1-sip		DMVPN-other-13958 DMVPN-sip-5060				
DMVPN-spoke1-tftp		DMVPN-tftp-69				
DMVPN-spoke2-bgp DMVPN-spoke2-cusee		permit-all				
DMVPN-spoke2-cusee						
DMVPN-spoke2-sip						
DMVPN-spoke2-tftp	Match/match not:	Match				
MATCH-ALL		Add Match Statement Replace Match Statement				
permit-all						
III ►						
Help			Save to Device	Preview C	LI Close	
nep			Save to Device	Preview C	Close	

In the Manage QoS Settings window, click on the Classes tab. Use the Match type drop-down to select ACL Name. The Values correspond to the saved ACL names. Highlight the desired ACL and choose Match or Match not. Click on Preview CLI to review the match command and Save to Device to add this to the QoS settings of that device.

For additional details about managing Access Control Lists, please see Chapter 12, Tools.

Manage QoS Settings—Interfaces Tab

The Interfaces tab on the Manage QoS Settings screen shows where the QoS policies are applied to the device, and the various interface-level settings. The right side of the screen displays interface informa-

tion, including Maximum reserved bandwidth, Link Fragmentation, and Pre-classify for identifying traffic prior to encryption.

Vanage QoS Settings - 2921-Demo-67_111	referentia	ia.com (172.16.67.1.1)
5 E B B B B & %		
Policies Classes Interfaces		
Interfaces		
Embedded-Service-Engine0/0	*	
Input : <none></none>		Interface name: GigabitEthernet0/1
Output : <none></none>		
E S FastEthernet0/0/0		IP address: 10.0 4.2
Input : <none></none>		
Output : <none></none>		IP address mask: 255.255.255.0
FastEthernet0/0/1		Interface description:
Input : <none></none>		
Output : <none> FastEthernet0/0/2</none>		
Input : <none></none>		
Output : <none></none>		
- Input : <none></none>		Maximum reserved bandwidth: 75 🐳 %
Output : <none></none>	=	* This device supports HQF, therefore reserved bandwidth settings are ignored
□ · · · · · · · · · · · · · · · · · · ·		
Input : <none></none>		Pre-classify
Output : <none></none>		Link Fragmentation:
⊡ 🚭 GigabitEthernet0/1		Maximum delay: ms
Input : BaseIngressPolicy		Maximum delay: ms
Output : LAnbarMon		
⊖		
		Interleave
🗄 😌 NullO		Turcucave
🖶 🚭 Vlan1		
Input : <none></none>		
Output : <none></none>	-	
🖮 🤮 Vlan 10		
Help		Save to Device Preview CLI Close
i icip		

Maximum Reserved Bandwidth Dialog Box

The Set Max Reserved Bandwidth dialog box provides control over each of the interface's bandwidth settings. This setting is used to define the maximum allowable bandwidth that can be reserved by individual classes for any QoS policy applied to that particular interface.

Adjust Input QoS Policy

The Adjust Input Policy dialog box provides a quick way to make changes to QoS policies already applied in the inbound direction. It is specifically designed for applying drops and policing on inbound classes. This dialog box is accessible from the QoS menu.

Adjust Input Policy 'BaseIr	ngressPolicy' on 2921-Dem	o-67_111.referentia.c	om (172.16.67.111)	
Policing by Class				
Class Name	Drop	Police	Police Settings	Other Settings
Routing				•
Voice				٠
InteractiveVideo				٠
StreamingVideo				٠
MissionCritical				٠
CallSignaling				٠
Transactional				٠
NetworkManagement				•
BulkData		\checkmark	8 Kbps	5 👻
Scavenger				
dass-default				•
			ſ	
Help				Save to Device Cancel

Adjust Output QoS Policy

The Adjust Output Policy dialog box provides a quick way to visualize and make changes to QoS policies already applied in the outbound direction. It is specifically designed for changing queue types and bandwidth allocations, applying drops, and WAN shaping for hierarchical policies. This dialog box is accessible from the QoS menu.

Class Name Queue Setting Reserved Bandwidth Other Settings Routing Class-based Queueing 8 % • Voice Priority Queueing 512 Kbps • InteractiveVideo Class-based Queueing 30 % • StreamingVideo Class-based Queueing 5 % • CallSignaling Class-based Queueing 3 % • CallSignaling Class-based Queueing 3 % • Bandwidth Summary by Interface Show units as: Percent • Bandwidth Summary by Interface Show units as: Percent • InteractiveVideo 6,000 \$hoes \$hoe units as: Percent GashtEthernet0/2 / Output 100,000 \$,000 \$1.53% \$hoe Guaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output \$% \$% \$% \$% StreamingVideo \$% \$% \$% \$% \$% \$% \$% Guaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output \$% \$% \$% \$%					
Voice Priority Queueing 512 (kbps) InteractiveVideo Class-based Queueing 30 % StreamingVideo Class-based Queueing 5 % % MissionCritical Class-based Queueing 8 % % CalSignaling Class-based Queueing 3 % % Transactional Class-based Queueing 5 % % Bandwidth Summary by Interface Shape link to: 6,000 kbps using Average Show units as: Percent * *This device supports HQF, therefore Max Reserved andwidth is fixed at 100% (minimum 1% for class-default) Interface Bandwidth (kbps) Shaped (kbps) Reserved (Percent) GigabitEthernet0/2 / Output 100,000 6,000 91.53% Guaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo 5% StreamingVideo 5% StreamingVideo 6% StreamingVideo 7% StreamingVideo 7% StreamingVideo 7% StreamingVideo 7% StreamingVideo 7% StreamingVideo 7% StreamingVideo 18%	Class Name	Queue Setting	Reserved Bandwidth		Other Settings
InteractiveVideo Class-based Queueing StreamingVideo StreamingV	Routing	Class-based Queueing -	8	%	•
StreamingVideo Class-based Queueing Class-based Queueing Show units as: Percent Class-based Queueing Show units as: Percent This device supports HQF, therefore Max Reserved andwidth is fixed at 100% (minimum 1% for class-default) Interface Bandwidth (Kops) Shaped (Kops) Reserved (Percent) SigabitEthernet0/2 / Output Class-based Queueing StreamingVideo StreamingVideo StreamingVideo StreamingVideo StreamingVideo Califismating ClassionCritical StreamingVideo Califismating ClassionCritical StreamingVideo Califismating ClassionCritical StreamingVideo Califismating StreamingVideo Streaming	/oice	Priority Queueing 🗸	512	Kbps	
AlssionCritical Class-based Queueing 8 96 0 CallSignaling Class-based Queueing 3 96 0 transactional Class-based Queueing 5 % 0 Bandwidth Summary by Interface Shape link to: 6,000 Kbps using Average Shape link to: 6,000 Kbps Verage Shape link to: 6,000 Shape (kbps) Reserved (Percent) andwidth is fixed at 100% (minimum 1% for class-default) Interface Bandwidth Allocation for Interface GigabitEthernet0/2 / Output Suaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo Voice Shape (kbps) Reserved (Percent) StreamingVideo Shape (kbps) Reserved (Percent) 18%	InteractiveVideo	Class-based Queueing -	30	%	•
alsignaling Class-based Queueing 3 9% Class-based Queueing 5 % Class-ba	StreamingVideo	Class-based Queueing -	5	%	-
ransactional Class-based Queueing 5 % andwidth Summary by Interface Shape link to: 6,000 kbps using Average Shape link to: 6,000 kbps Using Average Shape link to: 6,000 kbps Reserved andwidth is fixed at 100% (minimum 1% for class-default) Interface Bandwidth (kbps) Shaped (kbps) Reserved (Percent) igabitEthernet0/2 / Output 100,000 6,000 \$11.53% Suaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo Voice % StreamingVideo 5% Reserved 8% MissionCritical 8% Available 18%	fissionCritical	Class-based Queueing -	8	%	•
andwidth Summary by Interface Shape link to: 6,000 Kbps using Average Shape link to: 6,000 Kbps using Average Shape link to: 6,000 Kbps Show units as: Percent And Shape link to: 6,000 Shaped (kbps) Reserved (Percent) Interface Bandwidth (kbps) Shaped (kbps) Reserved (Percent) Interface Bandwidth Allocation for Interface GigabitEthernet0/2 / Output Suaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo StreamingVideo StreamingVideo StreamingVideo StreamingVideo Interface InteractiveVideo Interface InteractiveVideo Interac	allSignaling	Class-based Queueing -	3	%	•
Shape link to: 5,000 Kbps using Average Shape link to: 5,000 Kbps using Average Shape link to: 5,000 Kbps Shape link to: 5,000 Kbps Shape link to: 5,000 Kbps Reserved andwidth is fixed at 100% (minimum 1% for class-default) Interface Bandwidth (kbps) Shaped (kbps) Reserved (Percent) IsgabitEthernet0/2 / Output 100,000 5,000 S1.53%	ransactional	Class-based Queueing -	5	%	-
uaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo StreamingVideo 5% MissionCritical 8% CallSignaling	the second of the filles of the second filles with the second of the sec				
Suaranteed Bandwidth Allocation for Interface GigabitEthernet0/2 / Output InteractiveVideo StreamingVideo 5% MissionCritical 8% CallSignaling					1
InteractiveVideo StreamingVideo 5% MissionCritical 8% CallSignaling 18%	interface	Bandwidth (Kbps)			
3% / Scavenger	Interface iigabitEthernet0/2 / Output	Bandwidth (Kbps) 100,000			

The revert QoS configuration is available to undo the last QoS change made via the Manage QoS Settings dialog or the adjust input QoS or the adjust Output QoS settings. When selected, LiveNX sends a dialog box to confirm the revert command.

C	onfirm Revert QoS Configuration	×
	You are about to replace the current QoS configuration with the last saved configuration. Would you like to continue?	
	Do not show again OK Cancel	

Managing DMVPN QoS Policies

LiveNX can create and manage QoS policies on Dynamic Multipoint Virtual Private Network (DMVPN) tunnel endpoints and then apply them to tunnel interfaces.

In this example, a DMVPN-spoke1 policy is created consisting of six classes, each with a unique DSCP marking. A similar policy is created called DMVPN-spoke2.

Manage QoS Settings - 3925-VPN-163.re	ferentia.com (192.168.1.)	163)								23
2 9 9 9 9 9 4 %										
Policies Classes Interfaces										
Policies	Mapped Classes									
🛃 🖏 📚 💫 🌆 🖏 👒 👳	🖳 📄 🛃 🚔									
DMVPN-spoke 1	Class Name	Classify	Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
DMVPN-spoke1-tftp DMVPN-spoke1-bgp	DMVPN-spoke 1-tftp		DSCP: AF11							
DMVPN-spoke1-other	DMVPN-spoke 1-bgp	•	DSCP: EF							
DMVPN-spoke 1-sip	DMVPN-spoke1-other DMVPN-spoke1-sip	:	DSCP: AF41 DSCP: AF21							
DMVPN-spoke1-cuseeme dass-default	DMVPN-spoke1-cuseeme	•	DSCP: AF31							
Cass-default DMVPN-spoke1-shaper	class-default	•								
DMVPN-spoke2										
DMVPN-spoke2-shaper	Mapped Class Detail									
ernit-ai	Drop all traffic for class	s								
	Classify Marking Que	ueing Pol	icing Shaping	Compressio	w WRED	DBL Unsu	pported			
1	Match on: All						Re	eference		
	Match : ACL Name : DM	VDN_tftp_6	0	_				lass is de	fined by	the
	Plater rate rate rome	in the day of	-				c	riteria sho	w at lef	t. 🔰
								latch-any	r: nacke	tmust
								neet at leas		
							-	riteria to b	e a men	nber of
							tr	he class.		
										must meet
							-	Il criteria t he class.	o be a m	nember of
			Edit					10 01033.		
1										
					_					
Help					Save	to Device	Preview	CLI		Close

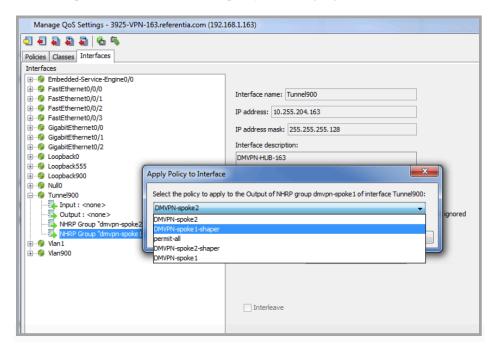
A hierarchical policy may be created to shape the specific spoke for a particular average bandwidth.

Manage QoS Settings - 3925-VPN-163.r	eferentia.com (192.16	8.1.163)							23
2 2 2 2 2 2 2									
Policies Classes Interfaces									
Policies	Mapped Classes								
DMVPN-spoke1	Class Name Class	sify Marking	Queueing	Policing	Shaping	Compression	WRED	DBL	Unknown
DMVPN-spoke1-bgp	dass-default	<u>ې</u>			50 Kbps				
DMVPN-spoke1-other									
DMVPN-spoke1-sip DMVPN-spoke1-cuseeme									
dass-default									
DMVPN-spoke 1-shaper dass-default									
DMVPN-spoke 1	Mapped Class Detail								
DMVPN-spoke2 DMVPN-spoke2-shaper	Drop all traffic for	dass							
permit-all	Classify Marking (Queueing Policing	Shaping Co	mpression	WRED DBL	Unsupported			
	Shape using: Avera	-					Referen	e	
			1				Control	the flow	of traffic 🔺
	Rate: 50	Kbps -	-					ninate bot ving pack	
	Committed	burst: 256	bits					ning to a s	specified
	Excess burs	st: 0	bits				bit rate.		E
	Unknown elemen	nts:		_			Rate		
							Peak: a	llows the	,
								ssion rate oher than	
							shaping		ule
							Augras	e: sets t	
								m transm	
	L								
Help					Save to De	evice Pre	view CLI		Close

Each shaped policy can then be assigned to the desired next hop routing protocol (NHRP) tunnel interface by right-clicking on the NHRP group.

Manage QoS Settings - 3925-VPN-163.referentia.com (192.168.1.163)					
2 🗐 🎝 🎝 🎝 🖗 🦠					
Policies Classes Interfaces					
Interfaces					
😥 😌 Embedded-Service-Engine0/0					
🗄 😌 FastEthernet0/0/0	Interface name: Tunnel900				
🗄 😌 FastEthernet0/0/1	Interface name: Tunnel900				
🗄 🖓 FastEthernet0/0/2	IP address: 10.255.204.163				
🗄 😌 🚱 FastEthernet0/0/3					
🗄 🖷 🤪 GigabitEthernet0/0	IP address mask: 255.255.255.128				
🗄 🖷 🤪 GigabitEthernet0/1					
🗄 🖷 🤪 GigabitEthernet0/2	Interface description:				
😟 😌 Loopback0	DMVPN-HUB-163				
🗄 🐨 🤪 Loopback555					
Eoopback900					
I I ···· · · · · · · · · · · · · · · ·					
Tunnel900	Maximum reserved bandwidth: 75 🐳 %				
Input : <none></none>	* This double supervised by the second by the second				
Output : <none></none>	* This device supports HQF, therefore reserved bandwidth settings are ignored				
NHRP Group "dmvpn-spoke2" : <none></none>	Pre-classify				
Vlan1					
	entation:				

Use the drop-down to select the desired policy for the highlighted interface.



VLAN Service Policies

LiveNX can manage QoS policies for switches that have configurable QoS service policies on a per VLAN basis.

Note Only devices with pre-defined VLAN ranges can be added through LiveNX.

In this example, the FastEthernet2/3 interface has 2 VLAN ranges defined. Once defined, LiveNX can apply and remove policies for the defined VLAN ranges.

To apply a policy to a given VLAN range, right click on the device and select QoS > Manage QoS Settings. Then select the Interfaces tab and then find the desired interface & VLAN range and select Apply Policy to Interface.

Manage QoS Settings - 4503-145.referentia.com (192.168.1	145)					
 Image: A state of the state of						
Interfaces						
	Interface name: FastEthernet2/3					
Output : <none> VLANs "21-22" Input : tcpmatch</none>	IP address:					
VLANs '21-22' Output : <none> VLANs '25-26' Input : abc</none>						
VLANs "25-26" Output : <none> Remove Policy from Interface FastEthernet2/30</none>						
Input : <none> Output : <none> FastEthernet2/31</none></none>						
Tastethernet2/31 Input : <none> Output : <none></none></none>	Maximum reserved bandwidth: 75 🕪 %					
	Pre-dassify					
Gutput : <none></none>	Link Fragmentation:					
Input : <none></none>	Maximum delay: ms					
E-S FastEthernet2/34						

LiveNX will then provide a list of pre-defined policies. Use the dropdown menu to select the desired policy. Click on OK to continue or Cancel to return to the Manage QoS Settings window.

Apply Policy to Interface	×
Select the policy to apply to theOutputof VLANs 2	1-22:
QA-TEST-PM	-
4C-BL_Empty_DSCP-Mark_VL1_Out_pa_0 4C-BL_DSCP-Match_VL1_Out_ch_0 Dave-EF	
Le tcpmatch	
4C-BL_DSCP-Match_VL1_Out_pa_0 4C-BL_Empty_DSCP-Mark_VL1_Out_ch_0 udp-netflow	
PM_MATCH_ALL	Ŧ

LiveNX will then add the given policy to the defined VLAN range.

Manage QoS Settings - 4503-145.referentia.com (192.168.1.145)					
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2					
Interfaces					
Output: cnone> FastEthernet2/3 VLANs "21-22" Input: tcpmatch VLANs "21-22" Output: tcpmatch VLANs "25-26" Input: abc VLANs "25-26" Output: cnone> FastEthernet2/30 FastEthernet2/30 GastEthernet2/30 GastEthernet3/30 Ga	Interface name: FastEthernet2/3 IP address: IP address mask: Interface description:				
FastEthernet2/31 Input: <none> FastEthernet2/32 FastEthernet2/32 FastEthernet2/32 FastEthernet2/33 FastEthernet2/33 FastEthernet2/34</none>	Maximum reserved bandwidth: 75 🖗 % Pre-dassify Link Fragmentation: Maximum delay: Interleave				

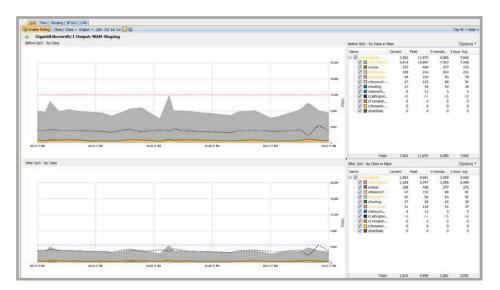
At the bottom of the Manage QoS Settings window, click on Preview CLI to review the CLI commands prior to saving to the device. Click on Save to Device to apply the policies to the desired VLAN range.

To remove a QoS policy from a given VLAN range, highlight a given VLAN range, right click and select Remove Policy from Interface.

Manage QoS Settings - 4503-145.referentia.com (192.168.1.	145)						
2 I I I I I I I I I I I I I I I I I I I							
Policies Classes Interfaces							
Interfaces							
Output : <none></none>							
Input : <none></none>	Interface name: FastEthernet2/3						
	IP address:						
VLANs "21-22" Input : tcpmatch	IF dual CSS.						
VLANs "21-22" Output : tcpmat							
VLANs "25-26" Input : abc 🖉 Apply Policy	to Interface						
VLANs "25-26" Output : <none> 4 Remove Poli</none>	cy from Interface						
🖶 🤤 FastEthernet2/30							
🛶 Input : <none></none>							
🖃 🤣 FastEthernet2/31							
- Jinput : <none></none>	Maximum reserved bandwidth: 75 🔷 %						
😑 😌 FastEthernet2/32	Pre-classify						
Input : <none></none>							
	Link Fragmentation:						
🗐 😌 FastEthernet2/33	Maximum delay: ms						
Input : <none></none>							
Output : <none></none>	Interleave						
🗇 🙆 EastEthernet2/24							

QoS Monitoring

QoS can be monitored for individual interfaces on a device. The monitoring window is separated by the inbound direction on top and the outbound direction on the bottom. For both directions, the top graph shows what the traffic looks like before QoS is applied, and the bottom graph shows what traffic looks like after QoS is applied.



Interface Selection

Select an interface to monitor by clicking on it from the device list or by double-clicking the interface in the topology view. The interface graphs will appear in the main window.

Display Options

Depending on your selection, LiveNX will display Before-QoS and After-QoS graphics and statistics, or the input, output, or both.

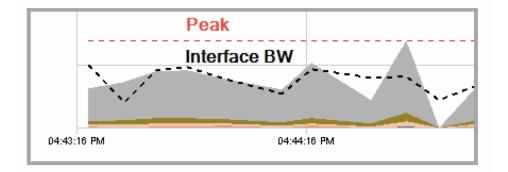
QoS Graphing Options

Various combinations of graphs can be selected from the drop-down list:

- Application—Uses Cisco NBAR capability to identify applications
- Class—QoS policy-based statistics. If there is no policy, then only the traffic outline is displayed.

- Class Drops—Packet drops that are occurring inside the QoS policy
- Interface Drops—Raw packet drops at the interface level
- Interface—Aggregate bandwidth of the interface

Graphing Display

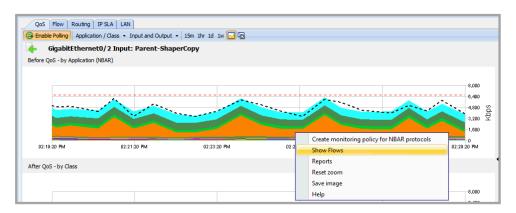


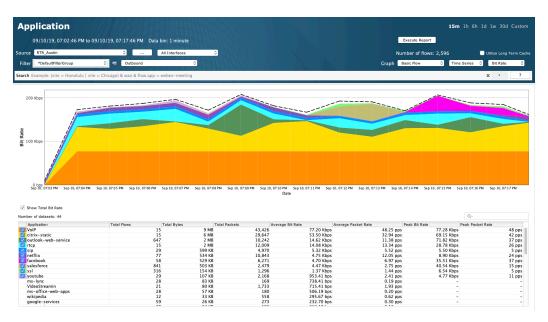
- Stacked area chart displays the data shown in the legend. If the policy is hierarchical, the child
 policy class information is charted in the class and class drop views.
- Black dotted line represents the interface bandwidth from the IF mib and is shown to help for correlation purposes. Since the IF mib operates separately from the CBQoS mib, the lines may not align especially at 10 second polling rates due to when the mib may be updated by the device. To turn off the line using the toolbar button.
- The red dotted line represents the peak bandwidth.



QoS Monitoring to Flow Reports

LiveNX can create application flow reports from the QoS real-time interface graphs for further QoS Class or Policy analysis. Right-click on the QoS real-time interface graphs and select Show Flows.





LiveNX creates an Application Flow Report automatically filling in the device, interface and input direction parameters from the QoS real-time interface graph.

Historical Views

Historical views allow you to view past data interactively. See the Reporting > QoS Reports section for more information.

Policy Management

LiveNX provides many capabilities for managing QoS policies. It utilizes a rule-based engine that performs policy management based on the current state and configuration of the device, and intelligently applies commands to resolve any conflicts or to warn of any conflicts.

Some of the management tasks that the software provides are:

- Applying and removing policies to interfaces
- Removing all policies from all interfaces
- Creating policies from best-practice templates
- Creating policies based on application graphs using NBAR Saving and loading policies from files
- Saving and loading ACL policies using QoS from files Pushing policies out to multiple devices at once
- Saving and loading snapshots of all QoS settings on a device

Apply Policy to Interface]		Snapsho	options	;	—	Class opti	ons		
Remove polic	y									
Manage QoS Settings - 2921-Demo-	57_111.referentia.cor	n (172.16	6.67.111)							x
👌 e a a a a 🖉 🛶 🛶										
Policies Classes Interfaces										
Policies	Mapped Classes									
5 H 2 A H H 5 H	De 🗈 😣 🚘	<u> </u>								
	Class Name	Classify	Marking	Queueing	Policina	Shaping	Compression	WRED	Unknown	
12_Class_RFC_4594_D 12_Class_RFC_4594_D 12_Class_RFC_4594_D 3C-BL_App-Match_Mart 3C-BL_Voice_DSCP-Match_FA Ant-WAN-Shaping AOR-Applications AOR-Applexo BaseEgressPolicy BaseEgressPolicy BaseEgressPolicy BaseEgressPolicy	Routing	•	DSCP: CS6							
3C-BL_App-Match_Mark 3C-BL-Voice_DSCP-Match_FA	Voice	٠	DSCP: EF							
ant WAN Shaping	InteractiveVideo	•	DSCP: AF41							
	StreamingVideo	•	DSCP: CS4							=
AOR-Policy	MissionCritical	•	DSCP: AF31							
AppDemo	CallSignaling	•	DSCP: CS5							
BaseEgressPolicy	Transactional NetworkManage		DSCP: AF21 DSCP: CS2							
BaseEgressPolicy-NoMarking	NetworkManage	•	DSCP: CS2							+
BaseIngressPolicy	Mapped Class Detail									
Rouding	🔲 Drop all traffic fo	r dass								
Voice	Classify Marking	Oueuein	Policina	haning Co	moression	WRED	Unsupported			
StreamingVideo		Queueing	a l'r olicing l'		mpression	WINED				
MissionCritical	Match on: Any						Referen	ce		_
CallSignaling	Match : Protocol -	using NBA	R : bgp					defined		
Transactional	Match : Protocol -	using NBA	R : eigrp				criteria	show at	left.	
NetworkManagement	Match : Protocol -						Match		ket must	
BulkData	Match : Protocol -	using NBA	R : ospf					least on		
Scavenger									nember of	
							the class	S.		
HighLevelShaping										
HOF-Bottom									et must mee	
BaseIngressPolicy-NoMarking HighLevelShaping HQF-Bottom HQF-Top				Edit			all criter the clas		a member of	
E							ule clas	ia.		
🖶 🗐 MonitorAppDemo 🔻										
4 III >										
Help				Save	e to Devic		Preview CLI		Close	
- Andrew - A				Loan					Ciose	
Policy options										

Applying and Removing Policies

Context-sensitive menus on the interfaces and devices provide shortcuts for applying and removing policies from the main interface. As shown in the Manage QoS Settings screen, the toolbar provides the following methods for applying policy changes to your interfaces:

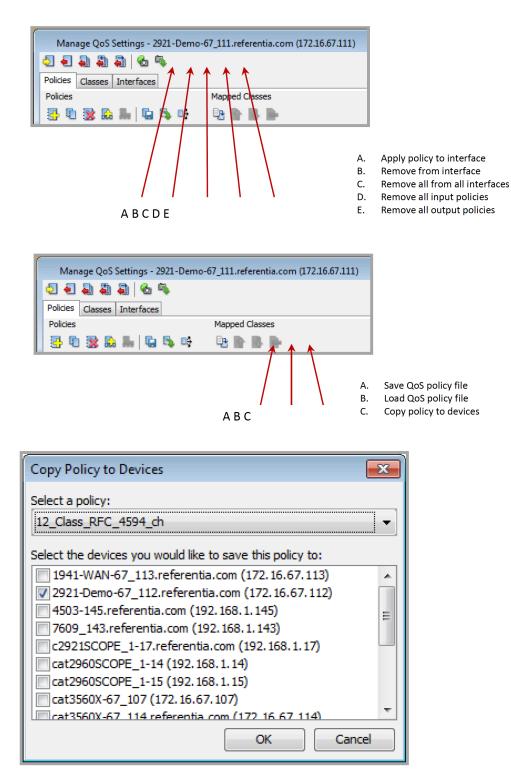
Note When a policy is applied to multiple interfaces, changing the policy will affect every interface to which the policy is applied.

Also note that there are some QoS actions that can be applied to the outbound portion of the interface, but not to the inbound portion. Policies that have this conflict will not be applied to the interface.

Saving, Loading, and Copying QoS Policies

All the operations for loading and saving QoS policies are located on the Manage QoS Settings screen:

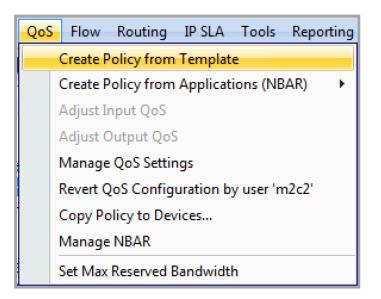
- To save a policy to disk—From the Manage QoS Settings screen, click the "Save QoS Policy File" icon. This will save the NBAR and ACLs that are required for the policy to operate. The file will have a .qos-policy extension.
- To load a policy from disk—From the Manage QoS Settings screen, click the "Load QoS Policy File" icon to load previously saved files or files that are provided by other users.
- To copy a QoS policy to other devices on the network—From the Manage QoS Settings screen, click the "Copy Policy to Devices" icon to open a dialog box for specifying which devices to which the policy will be saved. This command will also copy the ACL and/or custom NBAR used in any class match to the devices you select. If there are any configuration conflicts, a warning will appear with an option to overwrite conflicting changes.



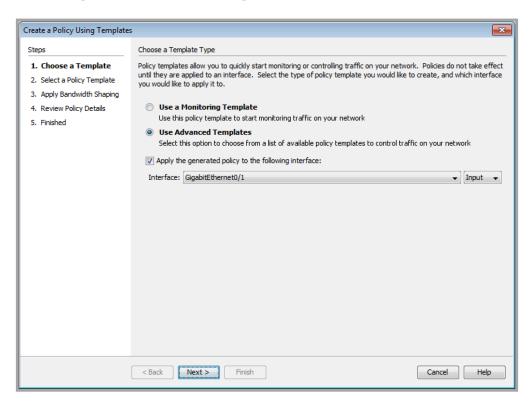
Creating Policies from Templates

Creating a policy from templates allows you to quickly apply a policy based on Cisco best practices and recommendations. A policy with up to 11 classes can be created for monitoring or controlling traffic using various classification methods.

1. Select Create policy from Template from the QoS menu.



- 2. A wizard will guide you through various templates that can be applied, or simply stored on the device for editing and applying to various interfaces. Indicate if you want to apply a monitor-only template or if you want to use an advanced template for controlling traffic. Also, indicate if you want to apply the policy you select to a specific interface.
- **3.** Follow the wizard instructions and select the policy templates you want to apply to your device. In the example below, Use Advanced Templates has been selected.



Create a Policy Using Templates	1	
Steps 1. Choose a Template Type 2. Select a Policy		nown in gray cannot be applied because they contain settings which are d direction, or other settings on the router.
 Select a Policy Apply Bandwidth Shaping Review Policy Details Finished 	Incompatible with the selected interface an Policy Templates I1C-8L_App-Match Ark I1C-8L_Complete I1C-8L_Complete I1C-8L_SCP-Match I1C-8L_Empty_DSCP-Mark I2 Class RFC 4594 I2 C	d direction, or other settings on the router. Description 11 Class Cisco Baseline NBAR Matching, DSCP Marking, and Queuing Policy Details Policy Details 11C-BL_Complete_GI01_In + Marking: DSCP "EF" + Queueing: Priority 10%
	4C-BL_Empty 4C-B_Empty_DSCP-Mark <	A Marking: DSCP "CS3" Queueing: Class-based 2% Cancel Help

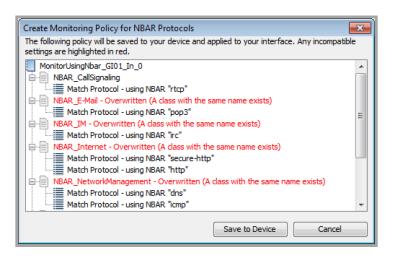
Creating Policies Using NBAR

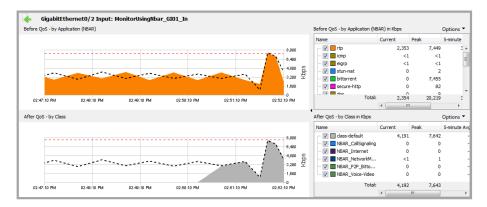
LiveNX makes it easy to create a monitoring policy based on the NBAR protocols that the device has recognized, and provides a skeleton policy for further editing.

1. Right-click the interface to create the policy on and choose QoS on the context menu and select Create Policy from Applications (NBAR) and choose the interface direction.

QoS Flow Routing IP SLA Tools Reporting	Help			
Create Policy from Template	LAN			
Create Policy from Applications (NBAR)	Using Input			
Adjust Input QoS	Using Output			
Adjust Output QoS				
Manage QoS Settings				
Revert QoS Configuration by user 'm2c2'				
Copy Policy to Devices				
Manage NBAR				
Set Max Reserved Bandwidth				

2. The software will list all the protocols and categories. Any incompatible settings will be highlighted in red. Click Save to Device, and a policy will automatically be applied to the interface that will monitor the traffic. The bottom graph shows the applied monitoring policy.





Customizing NBAR Protocols

NBAR protocol settings can be customized in the Manage Application Recognition (NBAR) editor. Select Manage Application Recognition (NBAR) from the QoS interface right-click context menu.

File View Users QoS	Flow Routing IP SLA Tools Reporting Help	
Discover Manage Expa	nd QoS Flow Routing IP SLA LAN	
	Enable Polling	
Name	Name	Policy
Arme Standalone Standalone Standalone GigabitEthernet() GigabitEthernet() GigabitEthernet()	I/1 → Output D/0 → GigabitEthernet0/2	BaseIngressPolicy LAnbarMon
😑 🛞 2921-Demo-67 11	vice: 2921-Demo-67 111.referentia.com	WAN-Shaping
GigabitEthe	OoS	
GigabitEthe		Chable QoS Polling
- 🛞 2921-Demo-67	Flow	Manage QoS Settings
GigabitEthe	Routing •	Revert QoS Configuration by user 'm2c2'
GigabitEthe	IP SLA	Manage NBAR
😌 NullO	LAN	Apply Policy to Interfaces
🖻 🛞 4503-145		Remove Policy from Interfaces
😌 FastEthern	Edit Device Settings	
- 😌 FastEthern	Add or Remove Interfaces	Copy Policy to Devices
GigabitEthe	Refresh Device	Reports
Port-chann	Remove Device	
Port-chann	Device Tools	
😔 Port-chann		
ian 🛞 7609_143	Statistics •	
😌 Port-chann	View •	
Port-chann	Group Management	
Port-criann		1

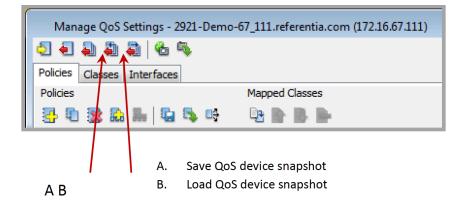
Existing protocols can be customized by adding, removing or changing TCP and UDP port numbers. Unknown protocols can be identified and assigned a new name.

Manage Ports - 2921-Demo-67_111	Manage Ports - 2921-Demo-67_111
Manage Application Recognition (NBAR) Show Unknown Application Ports	Manage Application Recognition (NBAR) Show Unknown Application Ports
Built In Protocols	Unknown Protocols Refresh
Protocol Layer 4 Pr Port	Debug Running, last refresh at 03:06:47 PM
active-directory TCP 443 445 139 389 135	Calculations made over 0.05 second interval
active-directory UDP 389	Calculations made over 0.03 second interval
activesync TCP 80	Port Layer 4 Protocol Protocol Number of Packets Rate (pps) Delta (packets)
adobe-connect TCP 443.80	
aol-messenger TCP 80 1080 443 5190 aol-messenger TCP 3478	
* Port mapping has been changed from the default Restore Defaults Remap Port value(s)	
Custom Protocols	
Protocol Layer 4 Protocol Port	
Delete Create Custom Protocol	
Refresh	Export Data Create Custom Protocol
Close	Close

Saving and Loading QoS Snapshot Files

A snapshot is a file that saves all the QoS settings, including any custom NBAR and ACLs that are used in QoS policies, for later use. The snapshot remembers all the policies that are currently applied on the interfaces that will be restored when the snapshot is later reloaded. Snapshots are a good way to create rollback points or to archive current configurations that can be used for specific situations.

You can save or load snapshots by clicking on the Save QoS Device Snapshot (A) or Load QoS Device Snapshot (B) icons on the Manage QoS Settings screen:



QoS Usage and Applications

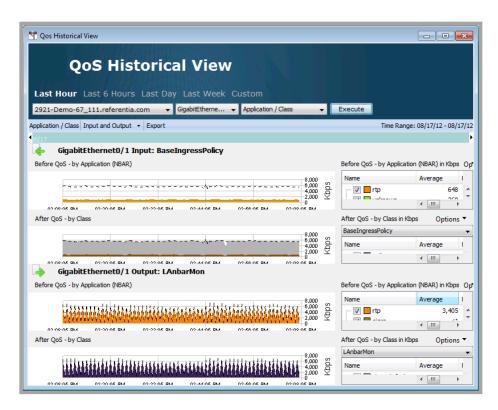
Planning and Implementing Quality of Service Policies

The process of creating Quality of Service (QoS) policies can be broken down into three steps:

- 1. Identify network traffic, baseline behavior, and service-level requirements
- 2. Divide traffic into application classes
- 3. Define QoS policies for the application class to meet service-level requirements

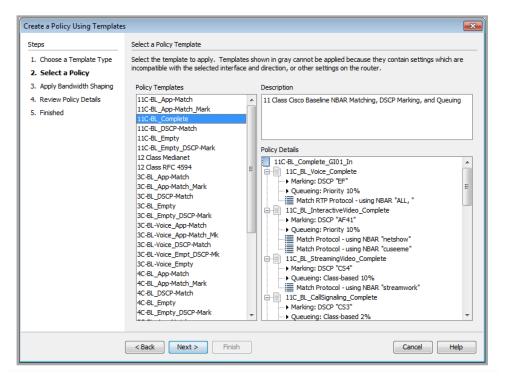
Identify network traffic, baseline behavior, and service-level requirements

Perform a network audit using the QoS historical views to identify traffic types and volumes. LiveNX provides this functionality through the monitoring graphs. Then, perform a business review on the priorities and specific requirements for the discovered traffic.



Divide traffic into application classes

Traffic can be divided into classes based on the identified traffic and the business requirements. The Cisco baseline model, which consists of 11 classes, is designed to provide granularity for various class types with different service requirements. Each type of class may have unique QoS requirements that must be configured and monitored. For initial QoS deployment, a smaller 4- or 5-class model can be used to simplify the process. The model can easily be expanded over time as additional applications and requirements arise.



Define QoS policies for the application class to meet service-level requirements

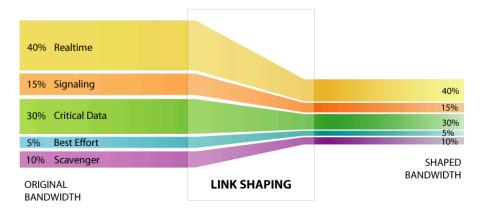
QoS policies should be designed from high-level requirements to meet specific objectives. Once the requirements are understood, they can be translated to QoS best practices for the various application types.

- Some best practices include using DSCP markings and marking the packets as close to the source of the traffic as possible.
- Recreational or Scavenger traffic should be policed as close to the source as possible to prevent unnecessary bandwidth usage ifit exceeds a certain threshold.
- Critical applications should be ensured through class definitions to meet service level agreements.
- A majority of the traffic will be classified as default, so enough bandwidth should be provided to support this type of traffic.
- Real-time traffic should use priority queues and be assigned adequate bandwidth. However, you should limit the overall priority queue to 33% of the available bandwidth to prevent starving other application traffic.
- The total bandwidth allocation for classes other than default should not exceed 75% of a link's capacity, to account for Layer 20verhead and Best Effort traffic.

Manage QoS Settings - 2921-Demo-I	67_111.referentia.com (172.1)	5.67.111)								x
5 I I I I I I I I I I I I I I I I I I I										
Policies Classes Interfaces										
Policies	Mapped Classes									
📴 🛍 📚 🦍 🐘 🐴 🖏 🔫										
11C-BL_Complete 11C_BL_Voice_Complete 11C_BL_InteractiveVideo 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_ContractoreVideo 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_CallSignaling_Cor 11C_BL_Scavenger_Compt 11C_BL_Scavenger_Compt 12_Class_RFC_4594_ch 2_CBL_App-Match_Mark 3C-BL_ApeMatch_Mark 3C-BL_ApeMatch_Mark 3C-BL_ApeMatch_Mark 3C-BL_ApoPemo BaseEgressPolicy BaseEgressPolicy BaseEgressPolicy-NoMarking Hight_evelShaping HQF-Top Hight_Andmon 4	Class Name 11C_BL_callSignaling_Com 11C_BL_TPRouting_Complete 11C_BL_VetWorfManagem 11C_BL_TransactionalData 11C_BL_StransactionalData 11C_BL_Stransa	De De De De De De De De De De	SCP: SCP: SCP: SCP: SCP: SCP: SCP: BE		n WRE	Sha	compre poported Reference Class is de criteria sho Match-all; all criteria to the class. Match-all; all criteria to the class.	fined by w at left st one o e a mem packet r	: must fthe berof nust meet	
Help				Save to Devi	ce [Previe	ew CLI		Close	

WAN Link Shaping

QoS polices for WAN aggregators typically configure various queuing, marking, shaping, policing, and link fragmentation settings. In most cases, there is a link-speed mismatch between the internal network speed and the external WAN link speed. In such cases, the best method is to use a hierarchical policy where the QoS policy is shaped to the link capacity of the WAN.



Creating a hierarchical WAN link-shaping policy involves creating a high-level (parent) shaping policy and then associating it with a lower-level (child) policy that actually defines the classes. In the following image, the high-level parent shaping policy basically consists of a class default that has an average shaping value set to the link capacity. A standard 11-class base child policy is then associated using the hierarchical policy dialog box, or by simply dragging the child policy onto the class default of the parent.

When applied to an interface, this policy forces the interface to shape all outgoing traffic to the class default shaping. Once shaped, the lower level QoS policy enforces the bandwidth requirements based on the shaped value and not the raw interface speed itself.

The easiest way to set up a hierarchical policy is to use the template-creation wizard built into the LiveNX software to guide you through the process of automatically creating a hierarchical policy.

Manage QoS Settings - 2921-Demo	o-67_111.referentia.com (172.16.67.111)	83
친 원 🎝 🎝 🖨 🌜 🖏		
Policies Classes Interfaces		
Policies	Mapped Classes	
11C-BL_Complete	Class Name Classify Marking Queueing Policing Shaping Compression WRED Unknow	wn
12_class_RFC_4599_ch 12_class_RFC_4594_pa 3C-BL_App-Match_Mark 3C-BL_Voice_DSCP-Match_FA0n Ant-WAN_Shaping_	SNMP-Traffic dass-default	
SNMP-Traffic	Create Hierarchical Policy	
AOR-Applications	Select the parent policy, containing class and child policy to	
AOR-Policy	create a hierarchical policy:	
AppDemo BaseEgressPolicy BaseEgressPolicy-NoMarking	Parent policy: Ant-WAN-Shaping	
BaseIngressPolicy	Class: class-default	
BaseIngressPolicy-NoMarking	Child policy BaseEgressPolicy-NoMarking	
HighLevelShaping HQF-Bottom HQF-Top LAnbarMon	OK Cancel Class is defined by the criteria show at left.	
MonitorAppDemo MonitorUsingNbar_FA01_In MonitorUsingNbar_GI02_Out Police-SNMP	Match-any; packet must meet at least one of the criteria to be a member of the class.	
WAN-Shaping	Edit Match-all: packet must me all criteria to be a member of the class.	
Help	Save to Device Preview CLI Cancel	

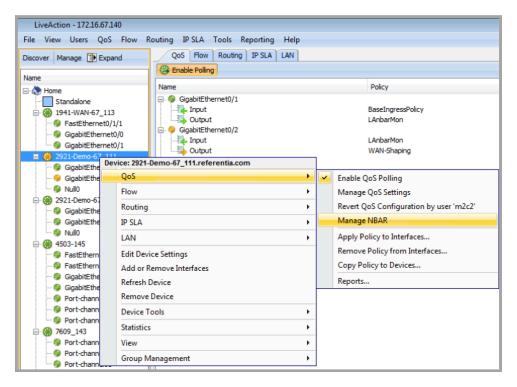
Class Name	Queue Setting	Reserved Bandwidth			Other Settings	
Routing	Class-based Queueing	- 8	%	•		
/oice	Priority Queueing	▼ 512	Kbps	-	•	ſ
nteractiveVideo	Class-based Queueing	→ 30	%	-		
treamingVideo	Class-based Queueing	▼ 5	%	-		
lissionCritical	Class-based Queueing	▼ 8	%	-		
CallSignaling	Class-based Queueing	▼ 3	%	-		
Transactional	Class-based Queueing	▼ 5	%	-		
This device supports HQF, the andwidth is fixed at 100% (mir	imum 1% for class-default)				Show units as:	Percent
This device supports HQF, the bandwidth is fixed at 100% (min	refore Max Reserved imum 1% for class-default)	Shaped (Khoc)		Pa	L.	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface	refore Max Reserved	Shaped (Kbps) 6,000			Show units as: [served (Percent) 53%	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps)				served (Percent)	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps)	6,000			served (Percent)	Percent -
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000	6,000			served (Percent)	Percent -
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	erfore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu	6,000 t			served (Percent)	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo 30%	6,000 t Voice 9% Routing			served (Percent)	Percent -
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo	6,000 t Voice 9%			served (Percent)	Percent -
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo 30% StreamingVideo	6,000 t Voice 9% Routing			served (Percent)	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo 30% StreamingVideo 5% MissionCritical	6,000 t Voice 9% Routing 8%			served (Percent)	Percent
This device supports HQF, the andwidth is fixed at 100% (mir Interface SigabitEthernet0/2 / Output	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo 30% StreamingVideo 5% MissionCritical 8%	6,000 t Voice 9% Routing			served (Percent)	Percent
Shape link to: 6,000 This device supports HQF, the bandwidth is fixed at 100% (mir Interface GigabitEthernet0/2 / Output Guaranteed Bandwidth Allocatio	refore Max Reserved imum 1% for class-default) Bandwidth (Kbps) 100,000 on for Interface GigabitEthernet0/2 / Outpu InteractiveVideo 30% StreamingVideo 5% MissionCritical	6,000 t Voice 9% Routing 8% Available			served (Percent)	Percent

VoIP QoS Policy Creation

A voice call tends to be classified as RTP protocol; unfortunately, there are many other applications that also use RTP. One of the ways to classify voice traffic managed by Cisco Call Manager, Cisco Call Manager Express, and Asterisk Call Manager, is to use a custom NBAR classification.

Select Manage NBAR from the QoS device right-click context menu.

1. Select Manage NBAR from the QoS device right-click context menu.



2. Manage Ports dialog will popup. On the Manage Application Recognition (NBAR) tab, click Create Custom Protocol.

Manage Ports - 292	1-Demo-67_11	1		- • •
Manage Application Reco	gnition (NBAR)	Show Unknown	Application Ports	
Built In Protocols				
Protocol	Layer 4 Pr	Port		
active-directory	тср	443 445 139 389	135	*
active-directory		389		
activesync	TCP	80		
adobe-connect		443 80		
aol-messenger	TCP	80 1080 443 519	0	
aol-messenger		3478		*
* Port mapping has been	changed from	the default	Restore Defaults	Remap Port
value(s)				
Custom Protocols				
Protocol Lay	er 4 Protocol		Port	
VoIP UDP			13960 16304	
		Del		Custom Protocol
		De	Create	Custom Protocol
				Refresh
				d
				Close

3. This will bring up a dialog box in which the name, protocol type, and port information can be entered.

Create Custom Protocol	×
How do you want to name the custom NBAR protocol? Specify a custom name (IOS version 12.3(4)T or later) Select predefined custom name (older IOS versions)	
Protocol Name VOIP Layer 4 Protocol UDP Port Map	
Range To (up to 1000 ports)	
Port(s) 13960 16304	
Save to Device Can	cel

When completed, the command ip nbar custom voip udp 13960 16304 will be issued to the device. Once the custom protocol is created, it is available for use by the NBAR engine and will show up in the monitoring graphs.

Manage Ports - 2	921-Demo-67_1	11	- • •
Manage Application R	ecognition (NBAR)	Show Unknown Application Ports	
Built In Protocols			
Protocol	Layer 4 Pr	Port	
active-directo	ry TCP	443 445 139 389 135	
active-directo	ry UDP	389	
activesync	TCP	80	
adobe-connec		443 80	
aol-messenge		80 1080 443 5190	
aol-messenge		3478	*
* Port mapping has b value(s)	een changed from	Restore Defaults	Remap Port
Custom Protocols			
Protocol I	ayer 4 Protocol.	Port	
VoIP U	DP	13960 16304	
		Delete Create	e Custom Protocol
			Refresh
			Kerresn
			Close

On the Manage QoS Settings screen, create a class for the VoIP traffic using the newly-created NBAR VoIP protocol.

Manage QoS Settin	ngs - 2921-Demo-67	_111.referentia.com (172.16.67.111)		— ×
a a 🎝 🎝 🞝	🐁 🖏			
Policies Classes Inter	rfaces			
Classes	Create and Edit Mat	ch Statements		
🔁 🖻 🕱				
	Match type:	Protocol - using NBAR	Match any 👻	×
NBAR_Internet NBAR_Network	Value:	vnc-http	Match Type	Value Match/Matc
NBAR_Network		VoIP	Haterrype	
NBAR Routing		vpp	Protocol - using NB	AR VOIP Match
NBAR_Streamin		vpps-qua		
NBAR_Term-Re		vpps-via		
NBAR_Tunnels		vrrp		
NBAR_Voice-Vi		vsinet		
NetManagemer		vslmp		
Network-Contr	Match/match not:	Match		
NetworkManag			2	
NIPR-Enclave		Add Match Statement Replace Match Statement		
OAM				
Realtime-Intera				
Routing Scavenger				
Scavenger				
Signaling				
SIPR-Enclave				
SNMP-Traffic				
StreamingVideo				
To-LAX-Office				
To-SFO-Office				
Transactional				
Transactional-L				
UN-Endave				
Voice				
VoIP-Telephon 👻				
4 III +				
Help		Save to De	vice Preview	CLI Cancel
пер		Save to be	Preview	Cancer

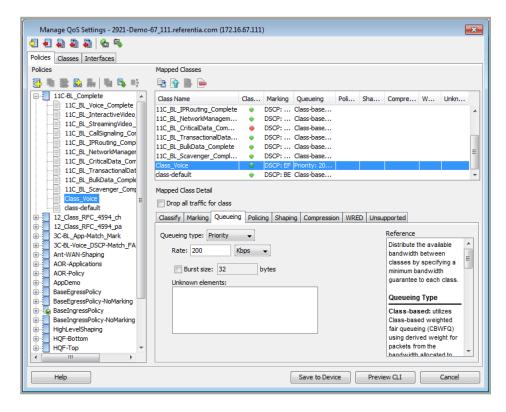
4. Create a policy based on the Cisco 11-class model using the template wizard. The class can use the VoIP class created in the previous step, and the various QoS settings can be configured.

Manage QoS Settings - 2921-Demo	.67_111.referentia.com (172.16.	.67.111)				(×
친 🗐 🜲 🗸 🖓 🖓							
Policies Classes Interfaces							
Policies	Mapped Classes						
📑 🐂 📚 🔝 🐜 🐃 🎭 👳	92 🛐 📕 🚔						
11C-BL_Complete	Class Name	Clas Marking	Queueing	Poli Sha	Compre	W Unkn	
11C_BL_Voice_Complete	11C_BL_IPRouting_Complete	 DSCP: 	Class-base				
11C_BL_InteractiveVideo 11C_BL_StreamingVideo	11C_BL_NetworkManagem		Class-base				
11C BL CallSignaling Cor	11C_BL_CriticalData_Com		Class-base				
11C_BL_IPRouting_Comp	11C_BL_TransactionalData		Class-base				
11C_BL_NetworkManager	11C_BL_BulkData_Complete	•	Class-base				Ξ
11C_BL_CriticalData_Com	11C_BL_Scavenger_Compl	•	Class-base				
11C_BL_TransactionalDat	Class_Voice class-default	• •	Class-base				
11C_BL_BulkData_Comple	class-default	DSCP: BE	Class-base				-
11C_BL_Scavenger_Com	Mapped Class Detail						
Class_Voice	Drop all traffic for class						
class-default							
12_Class_RFC_4594_ch	Classify Marking Queueing	Policing Shapi	ng Compressio	on WRED U	nsupported		
12_Class_RFC_4594_pa 3C-BL_App-Match_Mark	Match on: Any				Reference		
3C-BL_App-Match_Mark						fined by the	
Ant-WAN-Shaping	Match : Protocol - using NBAF	R : VoIP			criteria sho		
AR-Applications					on torna on to		
AOR-Applications					Match-any	: packet must	
AppDemo						st one of the	
BaseEgressPolicy						e a member of	
BaseEgressPolicy-NoMarking					the class.		
BaseIngressPolicy					Martak alla	packet must mee	
BaseIngressPolicy-NoMarking						o be a member of	
HighLevelShaping		E	dit		the class.	o be a member of	' I I I
HQF-Bottom							
HQF-Top 🔻							
۰ III ۲					L		
							_
Help			Save to Devi	ce Pr	eview CLI	Cancel	

5. On the Marking tab for the Voice class, set the DSCP marking to 46 (EF) to differentiate the traffic.

Image: Second
Policies Mapped Classes Policies Class Name Class Marking Queueing Pol Sha Compre W Unkn Class Name Class DSCP: Class-base IIC.BL_StreamingVideo_
Policies Mapped Classes Image: Complete Image: Complete Image: Complete: Image: Complete
IIC-BL_Complete Class Name Class Marking Queueing Poli Sha Compre W Unkn IIC-BL_Voice_Complete IIC-BL_Plotting_Complete DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_Plotting_Complete DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_CriticalData_com DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_TransactionalData DSCP: Class-base IIC-BL_Voitorg_Complete DSCP: Class-base DSCP: Class-base IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsingVoice DSCP: Class-base E IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsingVoice DSCP: Class-base E IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsetionalDat OSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: Class-base E IIC-BL_StarsetionalDat DSCP: Class-base T IIC-BL_StarsetionalDat DSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: BE Cla
IIC-BL_Complete Class Name Class Marking Queueing Poli Sha Compre W Unkn IIC-BL_Voice_Complete IIC-BL_Plotting_Complete DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_Plotting_Complete DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_CriticalData_com DSCP: Class-base IIC-BL_StreamingVideo_ IIC-BL_TransactionalData DSCP: Class-base IIC-BL_Voitorg_Complete DSCP: Class-base DSCP: Class-base IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsingVoice DSCP: Class-base E IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsingVoice DSCP: Class-base E IIC-BL_TransactionalDat DSCP: Class-base E IIC-BL_StarsetionalDat OSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: Class-base E IIC-BL_StarsetionalDat DSCP: Class-base T IIC-BL_StarsetionalDat DSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: BE Class-base T IIC-BL_StarsetionalDat DSCP: BE Cla
11C_BL_Voice_Complete 11C_BL_PRouting_Complete 0.5CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_PRouting_Complete 0.5CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 0.5CP: Class-base 11C_BL_StreamingVideo_ 0.5CP: Class-base 0.5CP: Class-base 11C_BL_StreamingVideo_ 0.5CP: BE Class-base 0.5CP: BE Class-base 11C_BL_StreamingVideo_ 0.5CP: BE Class-base 0.5CP: BE Class-base
11C_BL_InteractiveVideo 11C_BL_PKouting_Complete 05CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_Pkouting_Complete 05CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_ChetworkManagem 05CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_ChetworkManagem 05CP: Class-base 11C_BL_PRouting_Comp 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 05CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: Class-base 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: Class-base 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: Class-base 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: BE Class-base *
11C_BL_StreamingVideo_ 11C_BL_VetworrManagem 05CP: Class-base 11C_BL_CallSignaling_Comp 11C_BL_CriticalData_Com 05CP: Class-base 11C_BL_PRouting_Comp 11C_BL_PretworrManager 05CP: Class-base 11C_BL_PretworrManager 11C_BL_StreamingVideo_ 05CP: Class-base 11C_BL_PretworrManager 11C_BL_StreamingVideo_ 05CP: Class-base 11C_BL_StreamingVideo_ 11C_BL_StreamingVideo_ 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: Class-base 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: Class-base 05CP: Class-base 11C_BL_StreamingVideo_ 05CP: CP: Class-base 05CP: CP: Class-base 11C_BL_StreamingVideo_ 05CP: EF 05CP: EF dass-deFault 05CP: BE Class-base v Mapped Class Detail 05CP: BE Class-base v
11C_BL_calSignaling_Cor 11C_BL_criticalData_com 05CP: Class-base 11C_BL_TRAviting_Comp 11C_BL_TransactionalData 05CP: Class-base 11C_BL_TransactionalData 05CP: Class-base 11C_BL_Scavenger_Complete 11C_BL_TransactionalData 05CP: Class-base 05CP: Class-base 11C_BL_TransactionalData 05CP: Class-base 05CP: Class-base 11C_BL_TransactionalData 05CP: BE Class-base 11C_BL_Scavenger_Comple 05CP: BE Class-base
11C_BL_IPRouting_Comp 11C_BL_URdsata_Complete DSCP: Class-base 11C_BL_Victorata_Complete DSCP: EF 11C_BL_Scavenger_Complete DSCP: BE Class-base 11C_BL_Scavenger_Complete DSCP: BE Class-base 11C_BL_Scavenger_Complete DSCP: BE Class-base 11C_BL_Scavenger_Complete DSCP: BE Class-base
11C_BL_NetworkManager 11C_BL_Stavbata_complete USCP:: Class-base 11C_BL_CriticalData_com 11C_BL_Scavenger_compl DSCP:: Class-base 11C_BL_TransactionalDat Class_Voice DSCP: BE Class-base 11C_BL_Scavenger_compl. DSCP: BE Class-base 11C_BL_Scavenger_complete DSCP: BE Class-base
11C_BL_CriticalData_Com 11C_BL_Scavenger_comp 05CP: EF 11C_BL_Stavenger_comp 05CP: EF 11C_BL_Scavenger_comp 05CP: BE Class-base
11C_BL_TransactionalDat Class_voice USCP: EF Class_voice 11C_BL_SulkOata_Comple DSCP: BE Class_voice Image: Class_voice 11C_BL_Scavenger_Comple Mapped Class Detail Image: Class_voice Image: Class_voice Class_Voice Image: Class_voice Image: Class_voice Image: Class_voice
IIC_BL_BukData_Comple IIC_BL_Scavenger_Comp IIC_BL_Scavenger_Comp Gass_Voice Dron all traffic for class
11C_BL_Scavenger_Com; Mapped Class Detail Cass_Voice Dron all traffic for class
12_Class_RFC_4594_ch Classify Marking Queueing Policing Shaping Compression WRED Unsupported
12_Class_RFC_4594_pa
C-BL_App-Match_Mark Mark with: C-BL-Voice_DSCP-Match_FA Differentiate packets
Ant-WAN-Shaping V DSCP - 46 (EF) - belonging to this class
AOR-Applications Dased on marking.
AR-Policy
ATM Cell Loss Priority
BaseEgressPolicy DSCP: marks a packet
baseLgressPolicyPromaining by setting the
BaseIngressPolicy differentiated services
BaseIngressPolicy-NoMarking code point (DSCP) value
HighLevelShaping in the type of service
HQF-Bottom (TOS) byte.
HQF-Top Treedence sets the T
Help Save to Device Preview CLI Cancel
nep Save to Device Preview CLI Cancel

6. Set up the voice class as a priority queue and reserve bandwidth based on the requirements for voice traffic. Policing and header compression for RTP traffic can also be enabled if desired.



7. Create a separate class for the voice signaling protocols. The image below shows a voice signaling class with NBAR-based matches for SIP, Skinny, and H.323 protocols. The queue type can be set up as class-based queuing, and bandwidth allocation can be determined from the system baseline. When marking voice signaling, the DSCP value should be set to CS3.

CHAPTER 7

Flow

In this chapter:

Flow Overview	148
System View Drill Down to Flow Report.	150
Device View	158

Flow Overview

The LiveNX Flow technology module for the LiveNX software provides an innovative network topology view with end-to-end NetFlow, sFlow, and J-Flow visualizations of live traffic across the network. This enables you to quickly drill down to individual devices or interfaces for more detail on flow characteristics such as IP addresses, DSCP values, byte rates and count. In addition, the LiveNX Flow technology provides historical and real-time reporting, filtering, flexible support for different templates and many other features, which makes it easy identify trouble spots on the network and gain a better understanding of traffic patterns.

Supported Flow Technologies

The LiveNX Flow technology module supports the flow technologies from the following vendors:

- Cisco NetFlow (version 5 and version 9)
- Cisco AVC (Application Visibility and Control)
- Cisco Medianet Performance Monitor
- Cisco NSEL (NetFlow Secure Event Logging)
- Cisco PfR (Performance Routing)
- Cisco Sampled NetFlows
- Cisco AnyConnect
- IPFIX
- Juniper J-Flow
- Hewlett-Packard sFlow
- Alcatel-Lucent sFlow
- 3Com sFlow

Benefits

- Provide faster troubleshooting of the network.
- View flows across the network from source to destination.
- Pinpoint entry and exit of flows.
- Acquire a deeper understanding of flow paths.
- Observe the effects of routing and PBR settings, such as route updates and asymmetric rout
- Effortlessly enable the flow capabilities of your device without using the command line.

Key Features

- A dashboard aggregation of the flows in your network.
- A system level view of the flows in your network that provides end-to-end graphical topology visualizations and tabular aggregations of flows across the system.
- A device level view of the flows from a specific device that provides a topology visualization and table representation.
- An interface view of input and output flows from a particular interface.
- Various reports that allow that provide forensic capabilities to find specific historical flows; playback, time series charts, aggregation charts, drill down to raw flows, etc.

- Filter traffic based on specific parameters such as DSCP, port, source address, and destination address for more focused viewing.
- A search field in the system view, flow dashboard and flow reports to provide user-defined filtered results for system and flow entities.
- Support most of the major flow technologies (NetFlow, sFlow, J-Flow, IPFIX) from a variety of vendors.
- View Cisco Medianet Performance Monitor, AVC, NSEL, PfR.
- Store all flow information for historical analysis and forensics.
- Provide the ability to start and stop flow data gathering on a per-device basis.
- Resolve addresses to hostnames.
- Allow data to be stored as CSV files and image captures

LiveNX Flow Visualizations

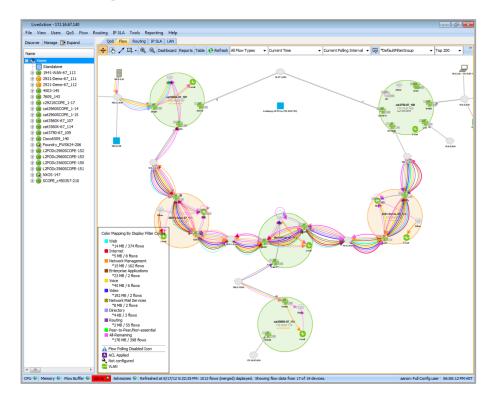
The LiveNX Flow technology module for the LiveNX software provides five different levels of visualizations of flow information. They are the Dashboard, System View, Device View, Interface View, and Reports. This section describes each of them in detail.

System View

The system view provides the ability to visualize flows from each device on the system topology. LiveNX connects flows with the same 5 Tuple (Protocol, Source IP Address, Source Port, Destination IP Address, Destination Port, and DSCP) from different devices to represent the device flows as a single flow across the system network. This provides an end-to-end visualization of the traffic path. The controls of the system flow visualization are located on the tool bar of the Flow Tab.

- Dashboard (button): launches the flow dashboard which contains quick summary of flow related statistics. Reports (button): launches the flow reporting window which provides top analysis, time series and aggregation reports of different types.
- Table (button): launches the System Flow Table window which contains an aggregation of the flows from each device.
- Refresh (button): refreshes the flows currently drawn on the system topology and in the system flow table. The following options dictate what flows that are retrieved from the LiveNX Server:
 - Flow Technology Type Selector: this provides a mechanism to restrict the types of flows that are retrieved. All Flow Types will retrieve all types. Selecting any of the following will restrict the retrieval to just the
 - selected type: Application (AVC), Basic Flow, Medianet, NSEL, PfR and Unknown.
 - Current Time Selector: provides a mechanism to retrieve historical flows or the current traffic flowing throw the system.
 - Polling Interval Selector: provides a mechanism to specify the duration to query for the flows. For example, setting the selector to Last 30 Minutes will provide the top 200 flows for the last 30 minutes per device.
 - Filter Selector: provides the ability to filter the flows retrieved during the refresh.
 - Top/Bottom Flows Selector: provides the ability to set the number of flows per device to retrieve during the refresh process.
 - Color Mapping Selector: provides the ability to color match the flows retrieved during the refresh by a certain algorithm.

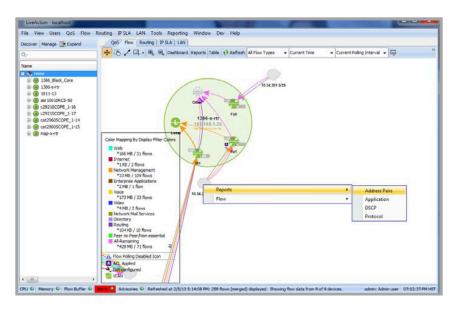
- A Color Mapping legend is overlaid on the topology to indicate flow coloring and the number of bytes and flows that match each of the color mapping. The legend can be toggled on and off by opening the View menu and selecting Show Legends.
- Flows can be drawn on the system topology as merged or unmerged. This can be changed by going to the Flow menu and selecting Show Merged Flows.
- Mousing over a flow provides bit rate, total bytes, and source and destination information.
- Clicking on a flow, highlights each segment, so you can quickly trace the path of the flow across the network topology.
- Double clicking on a device in the system topology navigates to the device view for that device.
- Double clicking on a flow in the system topology opens the system flow table; highlighted rows in the table correspond to the flow of interest.



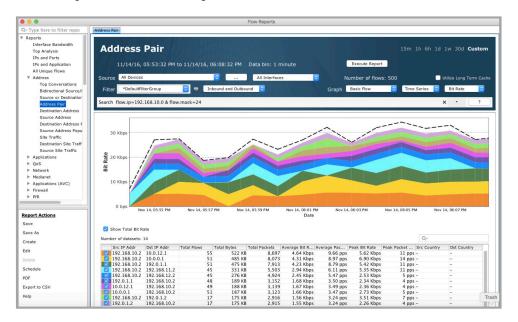
System View Drill Down to Flow Report

The system view flow visualization can be used to generate a flow report specific to a subnet cloud, a device, an interface on that device or a specific flow by right-clicking on the subnet cloud, the device, the interface, or the flow endpoint.

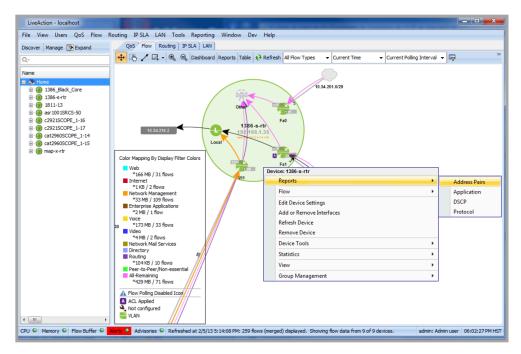
Subnet cloud drill down: Right click on the subnet cloud of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



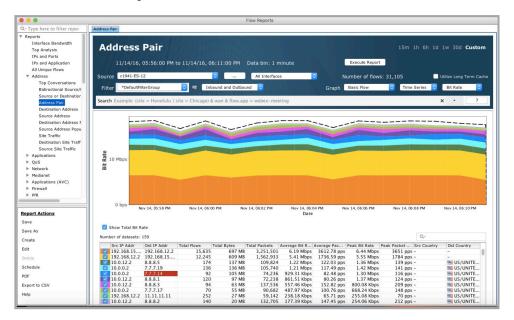
In this example, the desired Address Pair report lists the flows through the subnet cloud by Source IP and Destination IP address. A two-tier filter for IP source/destination address AND interface type is automatically selected to create this report. The flow data is aggregated from the nearest connected interface to prevent double counting of flows.



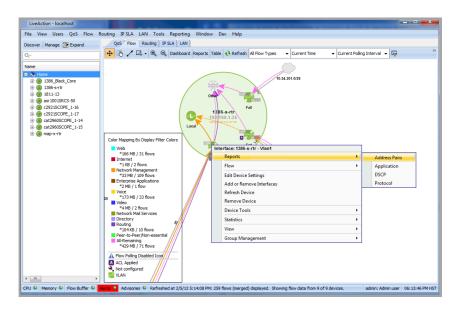
Device drill down: Right click on the device of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



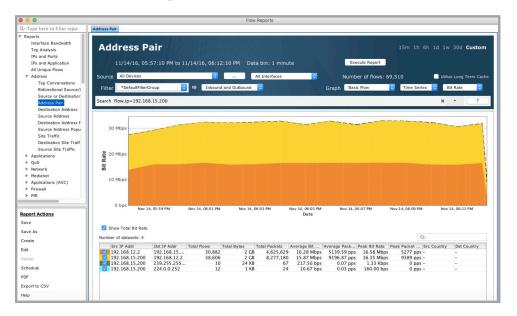
In this example, the desired Address Pair report lists the flows through all the interfaces of the selected device by source and destination address pairs. The desired device and all interfaces are automatically selected to create this report.



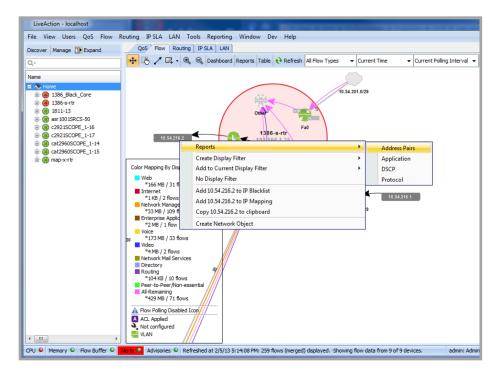
Interface drill down: Right click on the interface of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



In this example, the desired Address Pair report lists the flows through the selected device and the selected interface by source and destination address pairs. The desired device and interface are automatically selected to create this report.



Flow endpoint drill down: Right click on a flow endpoint and select one of the four reports: Address Pairs, Application, DSCP or Protocol



In this example, the desired Address Pair report lists the flows through the selected Source and Destination IP address. A two-tier filter for IP source/destination address AND interface type is automatically selected to create this report. The flow data is aggregated from the nearest connected interface to prevent double counting of flows. Additional details on using Filters in Flow Reports can be found in – Reporting.



Search

Linektion - koalwat	
File View Users QoS Flow Routing IPSLA LAN Tools Reports Window Dev Help	
Datiboard Manage (Filogand QoS flow Routing (Fila LM)	
Q. Topologi Facility - R. R. Table & Refer & Million Types - Durrent Time - Current Palling Interval - Rig Topfour/Riter Cators - Top 50 - R Contact Face Current Palling Interval - Rig Topfour/Riter Cators -	
Neme Search Example: (alte = Horodule site = dhougo) & wan B Row.dug = B ²	x • 2
B A Hore	

The LiveNX flow system view has a Search field to filter the system view based on the system and flow entities. The Search field is located under the Flow tab's main toolbar and is available in the system topology, the flow dashboard and the flow reports.

Searchable system entities include device, interface, site, tag and WAN parameters. Searchable flow entities include the IP address, DSCP, port, protocol, and application. CIDR notation can be used on the IP address, for example, "flow.ip=10.0.0/8." Wildcards can be used on the IP address, for example, "flow.ip=10.0.0.2/0.255.255.0" would match the IP address where the first and last octet are 10 and 2 respectively. More granular matches can be done such as "flow.ip=72.128.0.22/0.127.255.0."

Click on the Search field to begin typing in the desired search parameters.

The general syntax of the search field is shown as shaded text to represent an example entry.

(site = Honolulu | site = Chicago) & wan & flow.app = WebEx-meeting

Use the Enter key to apply the search. Click on the 'X' to clear the search field. Click on the down carat symbol to display a history of previous searches. The searches are kept on a per client basis; the history is removed with the LiveNX Client is closed.



Boolean expressions OR = '|' and AND = '&'; grouping uses '()'.

The Search editor provides tooltips to assist in creating the search expressions. Click on the desired entity to add it to the expression. NBAR uses dynamic lists based on the capability of the device.



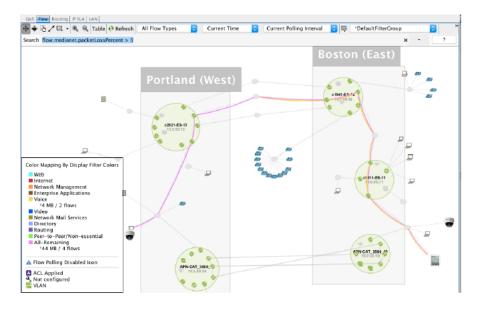
Filtering can be done through the main toolbar dropdowns as well as the Flow Display Filter combo box. Filtering is first done via the main toolbar dropdowns, the Flow Display Filter combo-box and lastly, the Search field.

The Search is done with a one pass search. In addition, the system level entities need to be in a single clause. For example, (site = Honolulu | site = Chicago) & flow.ip=1.1.1.1 is allowed, but (site = Honolulu & flow.ip=1.1.1.1) | (site = Chicago & flow.ip=1.1.1.1) is not allowed.

LiveNX supports a large number of system and flow searchable entities. Click on the ? to display the list of searchable entries as well as some example search expressions.

ξ τ	
Example	
site=Honolulu & wan	Flows from specific site with WAN-tagged interfaces
flow.dscp=EF	Flows with DSCP EF markings
flow.ip.src=1.1.1.1	Flows with specific source IP
flow.ip.dst=1.1.1.1 & flow.ip.src=2.2.2.2	Flows with specific source and destination IP
flow.ip.site=Honolulu	Flows from specific source or destination site
flow.ip.site.src=Sacramento	Flows from specific source site
flow.ip.site.dst="New York"	Flows from specific destination site
flow.ip=1.1.1.0/24	Flows with source or destination ip that match /24
flow.ip=192.168.0.55/0.0.255.0	Use of wild cards to match flows with ip address where 3rd octe.
flow.srcIp=172.16.1.0 & flow.srcMask=24	Flows with source ip that match /24
flow.device=Cisco1811 & flow.interface=FastEthernet0	Flows from specific device and interface
flow.device=Cisco1811 & flow.interface.in=FastEthernet0	Flows from specific device and in bound on interface
flow.app=ms-lync	Flows identified as ms-lync
flow.protocol=TCP	Flows that are TCP traffic
(site=A site=B) & tag=Primary	Flows from site A or B over interfaces tagged as Primary
System	
group	group=Engineering
device	device=Cisco1811
interface	interface=FastEthernet0

Relational operators > and < can be used for flow.medianet.packetLossCount and flow.medianet.packetLossPercent, and only in topology view. For example, show flows with packet loss > 3% in topology view.



System Flow Table

The System Flow Table displays the flows from an entire network aggregated by flow technology. To open the table, click on the Table button the toolbar on the Flow tab. If you select a specific flow technology type during a System Refresh, then only the corresponding technology type tab will be populated.

For Basic Flow, the flow records are merged based off Source IP, Destination IP, Source Port, Destination Port, and DSCP and sorted by byte count and then the top 200 flows per device are displayed for the given time range. A non-zero value in the Sampler ID column denotes flows that are sampled.

For Medianet, the flows are merged based off Source IP, Destination IP, Source Port, Destination Port, DSCP, and RTP SSRC and sorted by byte count and then the top 200 per device are displayed for the

given time range per device. Packet Loss %, Interarrival Jitter Mean, and Lost Event Count values are the max of all the records that were merged based off the tuples.

For AVC and NSEL, the last 200 records per device are shown for the given time frame.

The Unknown flow technology type is a flow type that doesn't match any of the other flow types: Application (AVC), Basic Flow, Medianet, NSEL or PfR.

Flows generating an alert are highlighted in light red; the specific attribute exceeding an alert limit is highlighted in dark red. The alerts must be enabled for the particular flow technology for this to be visible.

Note If a given flow with the same source and destination IP addresses are exported from the device using a different technology type, then the same flow would be represented in each flow technology type tab. The corresponding flow in the system topology view will only be shown once. The App Name field in the System Flow Table combines Application and NBAR Application data. When both are present, NBAR Application takes precedence. App Names followed by a (number:number) designate NBAR applications.

Basic	Flow Medianet	Application (AV	C) NSEL							
Color	Protocol	Src IP	Src Port	Src Country	Dst IP	Dst Port	Dst Country	App Name	DSCP	Total Bytes
	UDP	192.0.3.25	5,003	-	192.0.2.25	5,003	-	rtp	40 (CS5)	93 M
	UDP	192.0.3.25	6,111	-	192.0.2.25	5,111	-	rtp	40 (CS5)	91 M
	UDP	192.0.3.25	E 004	1	100 0 0 05	5 ,001	-	unclassified	0 (BE)	720 KI
	UDP	192.0.2.25	Show Flow	Path Analysi	s	,001	-	unclassified	0 (BE)	720 Ki
	EIGRP	10.0.4.1	Define Cur	tom Applicat	ion Based on Fl	-	-	eigrp	48 (CS6)	5 KI
	EIGRP	192.0.1.3	Denne cu	Applicat	ion based on th		-	unclassified	48 (CS6)	5 KI
	UDP	192.0.3.25	Add 192.0.	3.25 to IP Blac	:klist	.,967	-	unclassified	0 (BE)	5 KI
	UDP	192.0.3.25	Add 192.0.	3.25 to IP May	ning	,967	-	unclassified	0 (BE)	5 KI
	UDP	192.0.2.25				,003	-	unclassified	0 (BE)	4 KI
	UDP	192.0.2.25	Copy 192.0).3.25 to clipb	oard	,111	-	unclassified	0 (BE)	4 Ki
	UDP	192.0.3.25	Export Flov	v Data		,967	-	unclassified	0 (BE)	960
	ICMP	192.0.3.25		-	192.0.2.25	2,048	-	ping	0 (BE)	768
	ICMP	192.0.2.25	-	-	192.0.3.25	-	-	ping	0 (BE)	768
	UDP	192.0.2.25	1,967	-	192.0.3.25	5,001	-	unclassified	0 (BE)	6248

Right click on either the source or destination IP address in the System Flow Table and LiveNX provides additional options:

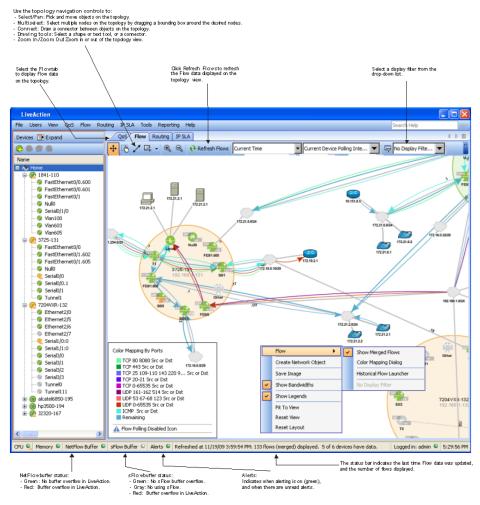
- Show Flow or Medianet Flow Path Analysis displays an end-to-end analysis of the flow on a perhop basis in the Basic Flow tab. Displays and end-to-end analysis of the Medianet flow on a perhop basis in the Medianet flow tab.
- Define Custom Application Based on Flow allows you to label a flow with a custom name and description.
- Add to IP Blacklist highlights identification of IP addresses by turning it red in the topology device, flow table, and historical views. Please see Chapter 12, *Tools* for Additional Information On the IP Blacklist Feature.
- Add to IP Mapping allows mapping of IP addresses to a user-defined label. Please see Chapter 12, *Tools* for Additional Information On the IP Mapping Feature.
- Copy to Clipboard creates a one-click method to copy the IP address. Export Flow Data creates a .csv file of the system flow table.

Right click on any item in the System Flow Tab other than an item in either the Src IP, or the Dst IP to show flow path analysis, to define custom application based on flow, or to export the System Flow Table to a .csv file.

LiveNX Tips

• Make sure polling is enabled in LiveNX. Click Enable Polling in the device's toolbar, or go to the Tools menu and select Options, and then select Polling to enable polling for all of your devices.

- To view detailed information on individual flows, separate the flows if they are merged: Right click and select Show Merged Flows to toggle that option on and off. Mouse over each flow to see its information.
- Use the wheel button to zoom in and out.
- Network devices will be grayed out if they do not support flows.



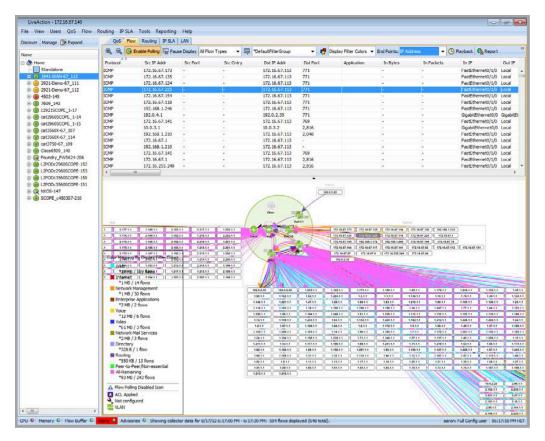
Device View

The device flow view provides a topology and table view of the traffic flowing through the device. The device view automatically refreshes the flows displayed in the table and topology based on the configured polling rate. The controls of the device flow visualization are located on the tool bar of the Flow Tab.

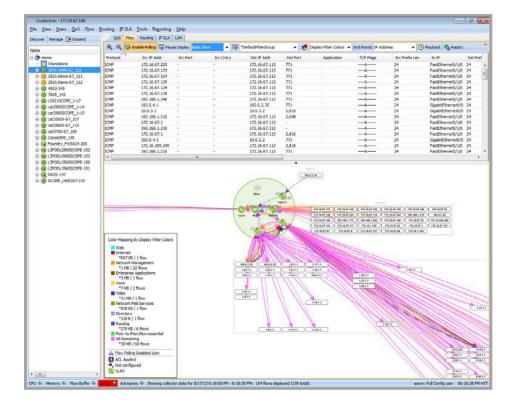
- Enable Polling (button): enables and disable the collection of flow data from the device.
- Pause Display (button): pauses the automated refresh on the current interval. While the device view is paused you may change the various selectors to change what is visualized for the current interval.
- Selectors that change the flows retrieved and how they are visualized:
- Flow Technology Type Selector: this provides a mechanism to restrict the types of flows that are retrieved. All Flow Types will retrieve all types. Selecting any of the following will restrict the retrieval to just the selected type: Application (AVC), Basic Flow, Medianet, NSEL, PfR, and Unknown. For Basic Flow and Medianet, the flows are the top 200 by byte count for the given time period. For AVC, PfR, and NSEL, the flows are the last 200 flows in that given time period.

- Filter Selector: provides the ability to filter the flows retrieved during the refresh.
- Color Mapping Selector: provides the ability to color match the flows retrieved during the refresh by a certain algorithm.
- End Point Selector provides the ability to change how the flows are drawn on the topology.
- A Color Mapping legend is overlaid on the topology to indicate flow coloring and the number of bytes and flows that match each of the color mappings. The legend can be toggled on and off by opening the View menu and selecting Show Legends.
- Flows can be drawn on the topology as merged or unmerged. This can be changed by going to the Flow menu and selecting Show Merged Flows. Mousing over a flow provides bit rate, total bytes, and source and destination information.
- The highlighting of the flows is linked to the table and the topology.

Interfaces labeled Local in this graph indicate flows to and from the router itself. Interfaces labeled Null indicate flows that are dropped or are multicast or broadcast in the nature that the router received them. The App Name field in the Table View combines Application and NBAR Application data. When both are present, NBAR Application takes precedence. App Names followed by a (number: number) designate NBAR applications.

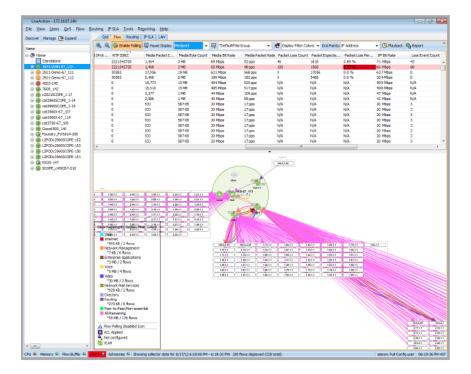


cover Manage DExpand	Out Field	Routing IP SLA											
		Enable Poling		(AVIS) - 500	"DefaultFilterGroup		Display Filter Col	ors + End Points: 1	Address	- 00	Nayback	Report	
me										1. Carlo	-		
Home	Protocol	Src IP Addr	Src Cntry	Det IP Addr	Dst Port	Application		In Packet			Out IF		Out By
Standalone	TCP	1.64.1.1	MK/Hong Kong		8,797		08	0		abitEthernet0/1			
1941-WAN 67_113	TCP	1.65.1.1	HK/Hong Kong		8,797		0.8	0		abitEthernet0/1			
2921-Demo-67_111	TCP	1.70.1.1	Childhina 🔤	2.70.1.1	8,797	*	0.8	0		abitEthernet0/1			
@ 2921-Demo-67_112	TCP	1.73.1.1	 JP/Japan 	2.73.1.1	8,797		0 B	0		abitEthernet0/1			
4503-145	TCP	1.75.1.1	 3P/Japan 	2.75.1.1	8,797		0.8	0		abitEthernet0/1			
2609_143	UDP	192.0.2.35		10.0.2.1	10,222		2 MB	5,524		abitEthernet0/1			0 B
0 c2921SCOPE_1-17	LOP	10.0.2.25		192.0.2.25	1,967	-	360 B	2		abitEthernet0/0		ernet0/1	3048
at29605COPE_1-14	LOP	10.0.2.25	1.1	192.0.2.25	6,002	a.,	24 MB	22,026	Gig	abitEthernet0/0	NURO N		08
Cat2960SCOPE_1-15	LOP	192.0.2.35		10.0.2.1	13,958		983 KB	4,724	Gg	abitEthernet0/1	Null0		80
at3560X-67_107	LOP	192.0.2.35	1.0.0	10.0.2.1	179	bgp	12488	595	Gig	abitEthernet0/1	NURO .		08
	LCP	192.0.2.35	a	10.0.2.1	69	tftp	589 108	584	Gig	abitEthernet0/1	NullO	-	80
at3560x-67_114	LOP	192.0.2.35	(a)	10.0.2.1	110	pop3	894 KB	1,759	Gg	abitEthernet0/1	Null0	-	08
cat3750-67_109	LOP	192.0.2.35		10.0.2.25	5,004		5.148	3,605		abitEthernet0/1			80
Cisco6509_140	UDP	192.0.2.35	241	10.0.2.25	5,005		816 B	12		abitEthernet0/1		-	0 B
Foundry_FWS624-206	LOP	192.0.2.35		10.0.2.1	520	rip	124 88	596		abitEthernet0/1			08
L2PODc29605COPE-152	LOP	192.0.2.35		10.0.2.1	7,648	cuseeme	30 MB	31,188		abitEthernet0/1			0 B
L2PODc2960SCOPE-153	* L.												
				-(
				(0-10-10-10	Martin Martin Martin Ato							
	2			(0-10-10-10								
				X	C		10811				124611	10511	
			_	X			120411 1		11401	11611	17811	1.28.1.1	1.
	Color Mappin	g By Daplay Filter Color	•	X	1000 WINAS7, 113		129411 1 12811 1	11.1 11.11 1.11 140.1.1	1210.1.1	118.11	17811	12811	
	Color Mappin	g By Display Fiter Color	•	X	ан 		120x11 1 120x11 1 120x11 1 120x11 1	11.1 11.11 1.1.1 1.40.1.1 1.1.1 1.101.1.1	1296.11	13811 13811 1397.11	17811 1.9611 1.7713	13811 13811 14611	
	Web	g By Display Fiter Calor 5 / 199 Hows	8	X			120411 1 13813 1 10013 1 124613 1	111 1111 141 4811 141 14811 141 13811	13811 129311 13611 13611	1.00.1.0 1.00.1.1 1.001.1.1 1.102.1.1	17811 1.96513 1.97713 1.98213	138.11 1.196.1.1 1.40.1.1 1.196.1.1	1
	Web *17 ME	3 / 189 flows	8	X			12611 1 12613 1 13613 1 12613 1 12613 1 10 1603 1 10	111 111 141 4014 141 111 141 111 141 111 14014	1.0811 1.293.11 1.3611 1.902.13 1.902.13	19811 18811 19811 19811 19811	12811 13611 12711 138212 12812	12811 12611 12611 12611 12611 126211	
	Web *17 ME Internet *304 B	3 / 189 flows	5	X	200 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		120411 1 13813 1 19913 1 120613 1 120613 1 1 120613 1 1 10013 1 1	11.1 1.1.1 8.5.1 6.83,1.5 8.5.1 1.186,1.7 11.1 1.226,1.7 8.5.1 1.226,1.7 8.5.1 1.226,1.7 8.5.1 1.226,1.7	10811 12831 13811 01233 01233 1855	19811 19811 19811 19811 19811	12833 04840 12740 04840 12840 12840 14853	128.1.1 1.00.1.1 1.00.1.1 1.00.1.1 1.00.1.1 1.00.1.1	
	Web *17 NE Internet *3048 Network	/ 189 flows / 11 flows Management	•	X	0		1204.1.1 1 1.38.1.1 1 1.99.1.3 1 1.298.1.3 1 1.288.1.3 1 1.288.1.3 1 1.286.1.1 1 1.286.1.2 1	11.1 11.11 11.1 1	10811 12831 13611 13611 01233 01233 1855 1855	19811 13811 13811 13811 13811 18811 19811	12011 04600 12700 04800 12800 12800 12800	12011 12011 14011 14011 14011 14011 12011 12011	
	Web *17 NE Internet *304 B Network Enterpre	3 / 189 flows	5	X	Alexandre (1) Alexand	20051 407 407 407 407 407 407 407 407 407 407	1204.1.1 1 1.06.1.2 1 1.06.1.3 1.5 1.266.1.1 1.5 1.266.1.1 1.5 1.265.1 1.5 1.266.1 1.5 1.266.1 1.5 1.566.1 1.5 1.567.1 1.5 1.577.1 1.5	11.1 11.1 8.1 6.20.1.5 8.5.1 5.106.5.1 8.5.1 5.206.5.1 8.5.1 5.206.5.1 8.5.1 5.206.5.1 8.5.1 5.106.5.1 8.5.1 5.106.5.1 8.5.1 5.106.5.1 8.5.2 5.106.5.1 8.5.3 5.106.5.1 5.5 5.106.5.1	10841 12841 13611 13611 10823 1853 1853 1853	19811 (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811)	12811 14813 12713 12813 12813 14853 14853 14853	12811 12811 14611 14611 12811 12811 12811 12811 12811	
	Web *17 ME Distances *304 B Network Enterprise Voice	/ 189 flows / 11 flows Management		X		- 22011 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211	120411 1 13811 1 138513 1 138513 1 128513 1 1 128513 1 1 138513 1 1 138513 1 1 138513 1 1	11.1 11.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.102.1 1.1 1.102.1 1.1 1.000.1 1.1 1.000.1 1.1 1.000.1 1.1 1.000.1	108411 128041 13611 08241 1851 1851 1851 18711 18711	19811 (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811)	12011 13611 12711 12811 12811 12811 12851	1.28.1.1 1.196.1.1 1.46.1.1 1.202.1.1 1.202.1.1 1.202.1.1 1.205.1.1 1.206.1.1 1.206.1.1	
	Web *17 ME Internet *3048 Network Enterpris Vaice	5 / 189 flows / 11 flows Management se Applications	5	X			128110 1 12813 4 12813 4 12813 1 12813 1 12811	111 1111 8.1 6.83.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 8.1 0.96.1 9.1 0.86.1	0.0811 12000 13001 0.0201 1455 1455 1455 1455 1455 1455 1455 14	11811 148111 148111 148111 148111 148111 1481111 148111 148111 1481111 14811111111	12011 12860 12700 12800 12800 14800 14800 14800 14800 14800 14800	1.28.1.1 1.46.1.7 1.46.1.7 1.202.1.1 1.202.1.1 1.202.1.1 1.205.1.1 1.206.1.1 1.206.1.1 1.206.1.1 1.206.1.1	
	Web *17 ME Internet *3048 Network Enterpris Vaice	8 / 199 flows / 11 flows Management se Applications Mail Services	5	X		- 22011 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211 10211	120411 1 1 13513 1 1 100513 1 1 100511 1 1 100513 1 100515 1 100515 1 100515 1 100515 1 10051	11.1 11.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.201.1 1.1 1.102.1 1.1 1.102.1 1.1 1.000.1 1.1 1.000.1 1.1 1.000.1 1.1 1.000.1	108411 128041 13611 08241 1851 1851 1851 18711 18711	19811 (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811) (2811)	12011 1284.0 1271.0 1280.0 128	1.28.1.1 1.28.1.1 1.44.1.1 1.282.1.1 1.282.1.1 1.282.1.1 1.282.1.1 1.281.1.1 1.281.1.1 1.271.1 1.271.1	
	Veb *17 ME Internet *30+8 Network Enterpris Voice Voice Voice Voice Voice Voice Voice Voice	9 / 189 Hows / 11 Hows Management se Applications Mail Services /	8	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	1.28.1.1 1.46.1.7 1.46.1.7 1.202.1.1 1.202.1.1 1.202.1.1 1.205.1.1 1.206.1.1 1.206.1.1 1.206.1.1 1.206.1.1	
	Vieb *17 MB Internet *30+8 Network Enterpris Valce Video Network Directory Routing Peer-toi	9 / 189 flows / 11 flows Management se Applications Mail Services y Peer/Non-essential		X			120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1233 1233 1233 1233 1233 1233 1233	13811 13813 13613 13613 13813 13817 13817 13817 13817 13811 13918 10911 109213 109713	12011 1284.0 1271.0 1280.0 128	1.28.1.1 1.28.1.1 1.44.1.1 1.282.1.1 1.282.1.1 1.282.1.1 1.282.1.1 1.281.1.1 1.281.1.1 1.271.1 1.271.1	
	Veb *17 ME Internet *30+8 Network Enterpris Voice Voice Voice Voice Voice Voice Voice Voice	9 / 189 flows / 11 flows Management se Applications Mail Services y Peer/Non-essential	•	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	128.11 128.11 144.11 144.11 1288.11 1288.11 1288.11 1288.11 1281.11 1281.11 128.11	
	Veb "17 ME "14thened "20+10 Network Sinterpris Voice Video Network Directory Routing Peter-to-i All-Rema	9 / 189 flows / 11 flows Management se Applications Mail Services y Peer/Non-essential	4	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	128.11 1298.11 144.13 1298.21 1282.11 1282.11 1284.11 1284.11 1284.11 1284.11 1284.11 1284.11 1284.11	
	Vieb *37 NB *37 NB *304 B Network Enterprit Vide Network Director Routing Peer to All-Rema	9 / 189 flows / 118 flows Management Avail Services v Peer/Non-essential aring mg Disobled Icon	8	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	128.11 5.296.11 146.13 5.296.11 1.202.11 1.202.11 1.202.11 1.202.11 1.202.11 1.203.11 1.203.11 1.203.11 1.203.11 1.203.11	1.4
	Web *37 Me Internet *30+B Network Enterprin Voice Voice Voice Voice Netmork Directory Routing Peer 40- Al-Rem Al-Rem	5 / 199 flows / 11 flows Management se Applications Mail Services / Peer/Non-essential aring mp Disabled Icon led	5	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	128.11 128.11 144.13 144.13 1282.13 1282.13 1282.13 1281.13 1281.13 1281.13 1281.13 1281.11 1281.11	
	Vieb *37 NB *37 NB *304 B Network Enterprit Vide Network Director Routing Peer to All-Rema	5 / 199 flows / 11 flows Management se Applications Mail Services / Peer/Non-essential aring mp Disabled Icon led	4	X		- 2294.1 - 2094.1 - 2	120110 1 128.17 0 128.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.17 0 1286.18 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0 1286.19 0	111 1111 641 648.1 643 6.98.1 643 6.98.1 643 6.98.1 644 6.98.1 645 6.98.1 645 6.98.1 644 6.98.1 644 6.98.1 644 6.98.1 645 6.98.1 644 6.98.1	0.0811 120.01 13611 0.0233 0.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233 1.0233	19211 18811 19211 192211 192211 192211 192211 192911 192911 192911 192911	12011 12010 12711 12813 12813 14813 14813 14813 14811 14811 14811 14811	128.11 5.296.11 146.13 5.296.11 1.202.11 1.202.11 1.202.11 1.202.11 1.202.11 1.203.11 1.203.11 1.203.11 1.203.11 1.203.11	



LiveAction - ncc-1701												x
File View Users QoS Flow Routing	IP SI	LA Tools	Reporting Wind	ow Dev Help								
		Oos	Flow Routing I									
Discover Manage Discover									1			>>
Name	De	Q Q	Enable Polling	🙀 Pause Display 🔀	1 - 🛱	*DefaultFilterGroup	👻 🛃 Dis	play Filter Colors	End Points: IP Address	• • (S Playback	
- A Home		Protocol	1 Src IP Add	r Src Port	Src Cntry	Dst IP Addr	Dst Port	Application	In IF	Out IF	ICMP IP	Pv4
1386_Black_Core.referentia.com		ICMP	172.16.67.	33 -		192, 168, 1, 242			0	Local	3	
B @ 1386-s-rtr.referentia.com		ICMP	172.16.67.	118 -	-	192.168.1.242	-		0	Local	3	
B 1811-13.referentia.com		ICMP	172.16.67.	124 -	-	192.168.1.242	-		0	Local	3	
🕀 🛞 1841-Demo-67_111.referentia.com		ICMP	172.16.67.			192.168.1.242	-		0	Local	3	
B @ 1841-WAN-67_119.referentia.com		ICMP	172.16.67.			192.168.1.242	-		0	Local	3	
B @ 1941-Demo-67_113.referentia.com		TCMP	192, 168, 1,	246 -	-	192, 168, 1, 242			0	Local	3	
B 2811-Demo-67_112.referentia.com												
⊕ ⊕ 4503-145.referentia.com												_
A-CLIENT-NODE.referentia.com												
A-SIPR-RTR-TL.referentia.com												
B Q asr1001_SRCS_1-50.referentia.com							\frown					
e 🛞 c1941-197.referentia.com												
e 🛞 c2821-185.referentia.com	=						Offer III					
						/	Other 📖	a francisco de la constante de				
B @ c2921SCOPE_1-16.referentia.com							ir	aice	Nut			
B @ c2921SCOPE_1-17.referentia.com		1	12.168.1.242	2.16.67.116 172.16.67.24	172.16.47.154 192.168.1	249	rete 😱 🕯		10.0.0.254			
⊞- 🛞 c3560-44					192.168.1.246 172.16.67		0 4 Nut	- / -				
@ cat2960SCOPE_1-14					172.16.67.33 172.16.67	11	1 9					
B @ cat2960SCOPE_1-15				2.16.67.130				and a				
Gat3560X-67_114.referentia.com							June /					
III 🛞 CC-COI-A-RTR-PIN.referentia.com		Color Mar	oping By Display Filter	Colors			agrand .					
🗄 🛞 CC-COI-B-RTR-PIN.referentia.com		Web										
B @ CC-SIPR-LAN-RTR.referentia.com		Inter										
B Q CC-SIPR-RTR-TL			rork Management			urity.	and .					
B B CC-SIPR-TC-RTR-PIN.referentia.com		*0	B / 49 flows			10.255	254.1					
CC-VSE-RTR-PIN.referentia.com			rprise Applications									
B @ Cisco6509_140.referentia.com		Voice Video										
discoasa.referentia.com			ork Mail Services									
- 🧐 inside		Direc										
- 🧐 outside		Rout										
- 🧐 untrusted			-to-Peer/Non-essenti	al								
CT-RTR1.referentia.com			emaining B / 151 flows									
H 🛞 CT-RTR3.referentia.com												
🗄 🎯 extreme48si-199			Polling Disabled Icon									
⊞- 🚳 hp3500-194		\Lambda ACL /										
B (2) 12320-167	-		onfigured									
A man.v.str m3r3 i amr mil	F.	VLAN										
CPU Memory Flow Buffer Alerts	Adv	isories 🍳 Sh	nowing flow data for	5/13/12 1:02:30 PM -	1:03:00 PM: 200 flows of	lisplayed (6,370 total)			a	idmin: Admin usi	er 01:03:23 PM	MHST

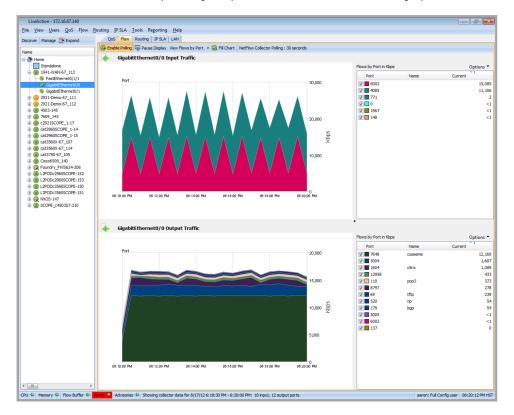
The Image Below shows a device-level view with Medianet flows highlighted in light red. This indicates that the particular Medianet flow is under alert. Scroll horizontally along the table until there is a dark red cell, indicating the particular attribute that exceeded the alert threshold. For details on the Medianet threshold values, or any threshold alert, please see Chapter 12, *Tools*.



The Image Below shows a device-level view with Medianet flows highlighted in light red. This indicates that the Medianet flow is under alert. Scroll horizontally along the table until there is a dark red cell, indicating the attribute that exceeded the alert threshold. For details on the Medianet threshold values, or any threshold alert, please see Chapter 12, *Tools*.

Interface View

At the interface level, the main window shows live graphics of inbound and outbound traffic. In this view, you can display flows by Port DSCP, Source IP, and Destination IP. The device hierarchy on the left side of the screen allows you to quickly select different interfaces to display in this view.



CHAPTER 8

Searching and Filtering

In this chapter:

About Searching and Filtering	164
Historical Playback	177
Enabling NetFlow	187

About Searching and Filtering

Key Features

This section explains some of the advanced features in the LiveNX Flow technology module. Most of these features are used on various views described in the section above.

Flow Technology Type Grouping

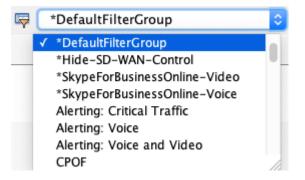
LiveNX categorizes and groups Flows into different Flow Technology Types when processing the data. This grouping separates Basic Flow, Medianet, AVC, NSEL, PfR and Unknown from each other, so that the appropriate data can be aggregated together. When appropriate, a selector is provided to allow the specification of a single or all flow technology types.

Flexible Templates

LiveNX flexibly supports various Flow templates and is able to provide aggregated data and visualization of nearly all fields that can be exported by todays flow collectors.

Flow Filters

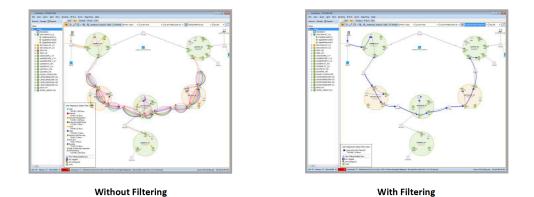
Filtering capabilities are provided at both the system- and router-level views, and provide similar functionality. When there are many flows traversing the network, the Flow graphs can become overwhelming. The filtering capabilities allow the user to show only specific flows that match particular criteria.



By default, LiveNX includes several pre-defined Flow filters. The Flow filter option also allows the creation and editing of user-defined filters. In the example below, the Custom End Point Filter will filter the display of Flow data, limiting the display to a specific device, interface, interface direction (ingress), and bit rate. The image below shows the application of the user-defined

Custom End Point Filter 001:

Flow Display Filters Setup	×
Image: Cost of Filter Image: Cost of F	Filter Entry Details Filter Entry Action: Show or Hde the following IP Type: Pr4 Only Pr4 6 Drly Both Pr4 8 IPv6 Color Happing Label & Color: Custom End Point Filter001 Basic Advanced Match Protocol/Ports Select from a pre-defined ist of protocols/appications or oreate new definitions Comparison of the state
	Match IP, Range, Subnet Match Source: IP Addresses, Any Destination IP Addresses Source: I92.0.2.35
	Destination:
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.	Hatch Device Interface Match flows traversing through a particular device's interface 1941-WAN-67_113.referentia.com Phound and Outbound Inbound @ Inbound Mate: Theme macked with a (*) are non-histopical



Flow filters can be set up at both the system- and device-level views, and are independent of each other. Filtering can minimize the number of flows displayed in system- and device-level views; extraneous flows can make it difficult to find relevant data within the view. Each piece of flow data is comprised of a particular set of attributes; flow filtering is provided on the following:

Layer 4 protocol.

- Source and destination TCP and UDP ports.
- Source and destination IP addresses.
- DSCP values.
- Flow size, either byte count or bit rate.
- Flows traversing into or out of a particular device interface.

Additionally, each flow filter can be assigned a unique color to enhance visual identification in the various views. To access the Flow Filter, click on the Flow topology tab, and then click the Filter icon in the toolbar.

Clicking the Filter icon displays the Flow Display Filters Setup dialog box. Pre-defined filters can be selected, or custom filters can be created.

• •	Flow Display Filters Setup
Create Filter Vr Copy Colete Rename Filter: [ad hoc filter] Filter Entries Add Entry Pr Add Other Filter Relate Entry Filter Entry Filter Fil	Flow Display Filters Setup Filter Entry Action: • Show or Hide the following IP Type: • IPv4 Only IPv6 Only Both IPv4 & IPv6 Color Mapping Label & Color: • Show or Advanced Basic Advanced Match Protocol/Ports Select from a pre-defined list of protocols/applications or create new definitions Image: Select from a pre-defined list of protocols/applications or create new definitions
	Match 1P, Range, Subnet
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter	
drop-down box. Help	OK Cancel Apply

Use the following commands to apply the filters listed in the Filter combo box. At start-up, LiveNX provides pre-defined filters.

Button	Description
Create Filter	Creates a new filter
Сору	Copies the selected filter
Delete	Deletes the selected filter
Rename	Renames the selected filter

Filter Entries

The Filter Entries tree view represents filter settings of the currently selected filter. Each filter is composed of sub-filter entries which are listed in the tree view. All sub-filter entries are AND'ed together to form the filter. For example, the following will filter all flows that have DSCP value 5 AND a source or destination IP address of 192.168.1.1 Use the following commands to add and delete sub-filter entries:

Button	Description
Add Entry	Adds a new filter entry.
Add Other Filter	Adds an existing filter as an entry to the current filter. This feature permits the reuse of existing filters to build up more complex filters.
Delete Entry	Deletes the highlighted filter entry. This command applies to the current filter entry selected in the tree view.

Filter Entry Details

Use the Filter Entry Details section to modify existing sub-filter entries. Select a sub-filter entry in the Filter Entries tree view and modify the filter options.

Filter Entry Action

Determines whether the selected filter entry is applied to show or hide flows that match the filter entry's criteria.

IP Type

Show	Indicates a positive filter entry. If a flow <i>matches</i> the filter entry's criteria, it will return a value "true," and if all other filter entries are "true," it will display the flow.
Hide	Indicates a negative filter entry. If a flow <i>does not</i> match the filter entry's criteria, it will return a value "true," and if all other filter entries are "true," it will hide the flow.

Select an IP type (IPv4 Only, IPv6 Only, or Both IPv4 & IPv6) to use for a filter entry. If Both IPv4 & IPv6 is selected, only fields common to both IPv4 and IPv6 will be filtered on. Any type of IP filtering options will be disabled; IP-type filters only support one IP type at a time.

Color Mapping Label & Color

Filter Entry Details Filter Entry Action: (a) Show or (b) Hide the following IP Type: (a) IPv4 Only (b) IPv6 Only (c) Both IPv4 & IPv6 Color Mapping Label & Color: Web Ŧ Web Basic Advanced Internet A Network Management Match IPv6 Flow Label Enterprise Applications Voice All-Remaining Enter IPv6 flow label values or range Network Mail Services Directory Match MAC Address 9 Peer-to-Peer/Non-essential All-Remaining Source: Video Routing Destination: 14 Enter individual MAC addresses or r 15 01-23-45-67-89-ab a001.2500.000 16 17 Match VLAN 18 19 (Remaining) Source:

Designate a color to identify this filtered flow type by.

Assigned colors will be displayed when the Flow Color Mapping setting is set to Display Filter Colors.

Match Protocol/Ports

Accessed by clicking the Basic tab. If this check box is enabled, the filter entry will match on IP protocol/ port numbers. A set of pre-defined protocol/port entries can be selected from the combo box. Use the following commands to extend pre-defined entries with custom entries. All of these commands will bring up the Protocols/Applications Setup dialog box.

Button	Description
Create	Creates a new match entry
Edit	Edits the selected match entry
Сору	Copies the selected match entry

Match IP, Range, Subnet

Accessed by clicking the Basic tab. If this check box is enabled, the filter entry will match on a specific IP, an IP range, or an IP subnet. Use the combo box to select match options. Disabled if Both IPv4 & IPv6 is selected.

Match IP Address Regardless of Source or Destination	Enables the Source and Destination fields. Matches all flows with either specified source or destination IP(s).
Match Source IP Addresses, Any Destination IP Addresses	Enables the Source field. Matches all flows with the specified source IP(s).
Match Destination IP Addresses, Any Source IP Addresses	Enables the Destination field. Matches all flows with the specified destination IP(s).
Match Source and Destination IP Addresses	Enables both the Source and Destination fields. Matches all flows with the specified source $IP(s)$ and destination $IP(s)$.
Match Source and Destination IP Address Bi-Directionally	Enables both Source and Destination fields. The filter matches all traffic from the Source address to the Destination address OR from the Destination address to the Source address.

In the Source and Destination fields, enter IP addresses, ranges, and/or subnets, separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-100.0.1).

Match DSCP

Accessed by clicking the Basic tab. If this check box is enabled, the filter entry will match on a specific DSCP. Select the DSCP value from the combo box. To match on multiple DSCP values, add more filter entries since only one DSCP value can be specified per filter entry.

Match Device Interface

Accessed by clicking the Basic tab. If this check box is enabled, the filter entry will match flows based on a specified device interface. Select a device and an interface from the combo boxes. Select a filter option:

Button	Description						
Input or Output	Filters on traffic in both directions						
Input	Filters on incoming traffic						
Output	Filters on outgoing traffic						

Match Flow Size

Accessed by clicking the Advanced tab. If this check box is enabled, the filter entry will match flows based on a specific range of packet sizes (kb), a specific range of flow rates (Kbps), or numbers of pack-

ets in the flow. Select Rate, Bytes, or Packets from the combo box and enter upper and lower limits in the fields provided. Click Max to automatically reset the value to the default: 4,924,967.

Note If a flow has no packet information (i.e., null), the filter will not attempt to match against it. Flows with zero values will be matched if that value is included in the specified range.

Match TCP Flags

Accessed by clicking the Advanced tab. If this check box is enabled, any combination of TCP flags can be specified for filtering. Select AND (default) or OR Boolean matching from the combo box. When using AND matching, the flags set in the flow must match the filter's flag setting exactly to register a match. With OR matching, a match will be registered if any of the flags specified in the filter is present in a flow; no match will be registered if no flags are set in a flow.

Note If a flow has no TCP flag information (i.e., null), the filter will not attempt to match against it. LiveNX will not specifically check for TCP protocol flows when matching TCP flag information.

Match Autonomous System Number (ASN)

Accessed by clicking the Advanced tab. Select an option from the combo box and enter the Source and Destination ASNs in the text boxes (maximum of 200 characters each). Each text box can accommodate space-delimited ASNs, and an ASN range denoted with a dash (-) between the lower and upper bounds of the range, with no spaces. Values within an entry field will be OR matched.

Option	Description					
Match ASN Regardless of Source or Destination	Enables the Source and Destination fields. Matches all flows with either specified source or destination values.					
Match Source ASN, Any Destination ASN	Enables the Source field. Matches all flows with the specified source values.					
Match Destination ASN, Any Source ASN	Enables the Destination field. Matches all flows with the specified destination values.					
Match Source and Destination ASN	Enables both the Source and Destination fields. Matches all flows with both the specified source and destination values.					

Note Currently, only 2-byte ASNs (range 0–65535) are supported (refer to RFC 5396, Textual Representation of Autonomous System (AS) Numbers).

Match Next Hop, IP, Range, Subnet

Accessed by clicking the Advanced tab. If this check box is enabled, the Next Hop IP filter will filter on single IPs, space-delimited IPs, IP ranges, or subnets (using CIDR notation). This filter matches against the Next Hop IP address rather than the source and destination IP information for a flow. Disabled if Both IPv4 & IPv6 is selected.

Enter a maximum of 200 characters. Denote a range with a dash (–) between the lower and upper bounds of the range, with no spaces. A valid range cannot have equal lower- and upper-bound values.

Note If a flow has no Next Hop IP information (i.e., null), the filter will not attempt to match against it. If the filter is enabled, but no value is entered in the text box, the filter will behave as if it is not enabled. A zero Next Hop IP value (e.g., 0.0.0.0) will only be matched if a zero IP address is entered in the text box.

Match IPv6 Flow Label

Accessed by clicking the Advanced tab. If this check box is enabled, the flow label filter will filter on single IPv6 flow label values or ranges of space-delimited values. Acceptable flow label values must fall within the 1–1048575 range. Disabled if IPv4 Only is selected.

Match MAC Address

Accessed by clicking the Advanced tab. If this check box is enabled, the filter will match on space-delimited values or ranges. Supports dashes (-) and colons (:) as delimiters, as well as the Cisco standard dotted notation for MAC addresses (e.g., xxxx.xxxx).

Option	Description
Match Mac Addresses Regardless of Source or Destination	Enables the Source and Destination fields. Matches all flows with either specified source or destination values.
Match Source Mac Addresses, Any Destination Mac Addresses	Enables the Source field. Matches all flows with the specified source values.
Match Destination Mac Addresses, Any Source Mac Addresses	Enables the Destination field. Matches all flows with the specified destination values.
Match Source and Destination Mac Addresses	Enables both the Source and Destination fields. Matches all flows with both the specified source and destination values.

Match VLAN

Accessed by clicking the Advanced tab. If this check box is enabled, the filter will match on individual values or ranges. Acceptable VLAN values must fall within the range of 1–4095.

Option	Description						
Match VLAN Regardless of Source or Destination	Enables the Source and Destination fields. Matches all flows with either specified source or destination values.						
Match Source VLAN, Any Destination VLAN	Enables the Source field. Matches all flows with the specified source values.						
Match Destination VLAN, Any Source VLAN	Enables the Destination field. Matches all flows with the specified destination values.						
Match Source and Destination VLAN	Enables both the Source and Destination fields. Matches all flows with both the specified source and destination values.						

Protocols/Applications Setup

The Protocols/Applications Setup dialog box allows the creation of custom match filters based on protocols/port numbers.

Protocols/Applications Setup						
🕂 Create Definition 🗅 Copy 💥 Delete 🛒 Rename						
Defined Protocols/Applications: test						
Entries						
🕒 Add Entry 🛛 🕞 Add Defined Prot/App 🕞 Delete						
test						
Note: Defined protocols/applications added as entries are not editable here,						
but can be edited by selecting them in the drop-down box above.						
Entry Details Layer 4 Protocol: UDP (17)						
Ports						
Match Ports Regardless of Source or Destination 👻						
Source: 161						
Destination:						
Enter port numbers or ranges separated by spaces (e.g., 80 88-443)						
Help OK Cancel						

The commands at the top of the dialog box apply to the container definitions in the Defined Protocols/ Applications combo box:

Button	Description							
Create Definition	Creates a custom match definition container							
Сору	Copies the select match definition container							
Delete	Deletes the selected match definition container							
Rename	Renames the selected match definition container							

Once a match definition container is selected from the Defined Protocols/Applications combo box, match entries can be added to it. Match entries are listed in the Entries tree view. Each matching entry identifies a specific protocol (e.g., application)/port number or range. A set of button commands allow the addition of match entries.

Button	Description
Add Entry	Adds a new defined protocol/application entry
Add Defined Prot/App	Adds an existing defined protocol/application entry
Delete	Deletes a defined protocol/application entry

To edit a matching entry, select it in the Entries tree view by highlighting it. Once a matching entry is selected, the Entry Details options are enabled.

Flow Color Mapping

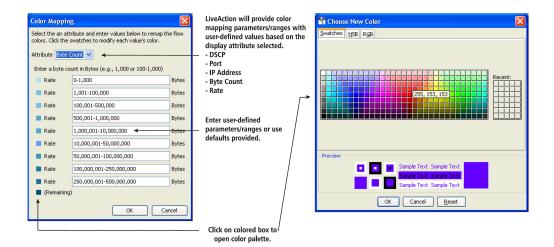
The Flow Color Mapping feature allows the assignment of colors to Flow connectors to easily view traffic characteristics at a glance. The Flow Color Mapping options are:

- DSCP—color flow by DSCP marking
- Port—color flow connector by port and by source/destination/both
- IP Address—color flow connector by IP address (ingress/egress/both)
- Byte Count (default)—color flow connector by byte count
- Rate—color flow connector by rate Display Filter Colors—color flow connector by the assigned filter

To modify Color Mapping options, click the Color Mapping Configuration icon xxx and select one of the attributes listed in the menu. See the Flow Filters section for information on assigning colors to flow filters.

Note IPv6 is not fully supported

	. ToorsEound				_						
QoS Flo	w Routing IP SLA	LAN									
۹ ۹ 🚱	Enable Polling	use Display Medianet	- 🖙	*DefaultFilterGroup	•	e	Byte Count 🗾 👻	End Points:	IP Address 👻	Neport	
Protocol	Src IP Addr	Src Port	Src Cntry	Dst IP Addr	Dst Port		Port	In Bytes	In Packets	In IF	Out IF
UDP	192.0.2.35	3,446	-	10.0.2.25	5,004		DSCP IP Address	2 MB	1,596	GigabitEthernet0/1	GigabitE
UDP	192.0.2.35	3,446	-	10.0.2.25	5,004		Byte Count	2 MB	1,532	GigabitEthernet0/1	GigabitE
UDP	10.0.2.25	6,002	-	192.0.2.25	6,002		Rate	19 MB	16,655	GigabitEthernet0/0	GigabitE
UDP	10.0.2.25	6,002	-	192.0.2.25	6,002		Display Filter Colors	6 MB	5,488	GigabitEthernet0/0	GigabitE
UDP	192.0.2.35	7,648	-	10.0.2.1	7,648		cuscenie	15 MB	15,584	GigabitEthernet0/1	GigabitE
LIDP	192.0.2.35	7.648		10.0.2.1	7.6.48		cuseeme	15 MB	15.502	GinabitEthernet0/1	GinabitE



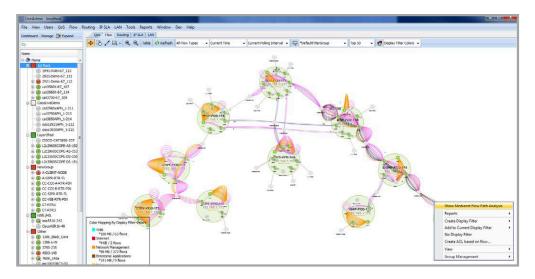
Flow Path Analysis

LiveNX provides detailed end-to-end traffic performance using standard Flexible NetFlow packets, general MIB information and the LiveNX alerts. The Flow Path Analysis, Medianet Flow Path Analysis

and Application Visibility and Control (AVC) Flow Path Analysis features combine this information into a single table that can be used to troubleshoot problems on the network using a specific flow. This feature is accessible from the tables and topologies in the flow system, device, and historical playback views, as well as the Top Analysis report. Flow alerts and performance measurements statistics are provided on a per hop basis. The following steps show how to access the Flow Path Analysis through the flow system topology view.

- Step 1: Go to the Flow tab in the System Topology View
- Step 2: Filter for either Basic Flows, Medianet flows or AVC flows
- Step 3: Right click on the flow of interest and select Show Flow Path Analysis, Show Medianet Flow Path Analysis or Show AVC Flow Path Analysis

The first two examples show access to the Flow and the Medianet Flow Path Analysis through the system topology. The third example shows access to the AVC Flow Path Analysis through the AVC tab within the System Flow Table.



	lasic Flow	Medianet	Application (AVC) NSEL								
Color	Protocol	Src IP	Src Country	Dst IP	Dst Port	Dst Country	App Name	DSCP	Total Bytes	ND Sum	Retransm
	TCP	1.181.1.1	CN/China	2.181.1.1		🔤 IR/Iran, Islamic Republic of		0 (BE)	619 KB	24 ms	
	TCP	1.180.1.1	💯 CN/China	2.180, 1.1	00	TO Area. Televic Domublic of	abava aaint	0 (BE)	3 KB	24 ms	
	TCP	10.0.6.100	-	10.0.7	Show App	lication (AVC) Flow Path Anal	ysis	0 (BE)	0 B	0 ms	
	TCP	1.232.1.1	: KR/Korea, Republic of	2.232.	Define Cu	stom Application Based on Flo	100	0 (BE)	0 B	0 ms	
	TCP	1.239.1.1	: KR/Korea, Republic of	2.239.	Denne ou	storn Application based on the	:	0 (BE)	0 B	0 ms	
	TCP	1.240.1.1	😻 KR/Korea, Republic of	2.240.	Add 2.180	.1.1 to IP Blacklist	-	0 (BE)	0 B	0 ms	
	TCP	1.241.1.1	: KR/Korea, Republic of	2.241.	Add 2,180	.1.1 to IP Mapping	:	0 (BE)	0 B	0 ms	
	TCP	1.242.1.1	😻 KR/Korea, Republic of	2.242.		11 5	-	0 (BE)	0 B	0 ms	
	TCP	1.243.1.1	😻 KR/Korea, Republic of	2.243.	Copy 2.18	0.1.1 to clipboard	:	0 (BE)	0 B	0 ms	
	TCP	1.244.1.1	😻 KR/Korea, Republic of	2.244.	Export Flo	w Data		0 (BE)	0 B	0 ms	
	TCP	1.245.1.1	😻 KR/Korea, Republic of	2.245		Depoendary	anare point	0 (BE)	0 B	0 ms	
	TCP	1.246.1.1	😻 KR/Korea, Republic of	2.246.1.1	80	DE/Germany	share-point	0 (BE)	0 B	0 ms	
	TCP	1.247.1.1	: KR/Korea, Republic of	2.247.1.1	80	DE/Germany	share-point	0 (BE)	0 B	0 ms	
	TCP	1.248.1.1	😻 KR/Korea, Republic of	2.248.1.1	80	SE/Sweden	share-point	0 (BE)	0 B	0 ms	
	TCP	1.249.1.1	: KR/Korea, Republic of	2.249.1.1	80	E SE/Sweden	share-point	0 (BE)	0 B	0 ms	
	TCP	1.250.1.1	: KR/Korea, Republic of	2.250.1.1	80	SE/Sweden	share-point	0 (BE)	0 B	0 ms	

Evaluate table results

LiveNX identifies the Flow, Medianet or AVC flow across the system based on the 5-tuple (source IP address, destination IP address, protocol, source port and destination port) and the RTP SSRC value.

The header information above the table entries describes the flow under analysis listed in order: protocol, source IP address, source port, destination IP address, destination port and SSRC value. The date and time range corresponds to the range of the query period (currently fixed at 5 minutes). Click on Refresh to update the table with the most recent data. Devices are displayed as column headers from left to right corresponding to the order that the flow traverses through the devices. The ordering of the columns is user-selectable; to reorder the columns, click on the device name in the column header, then click-drag the columns to reorder.

The row headers represent device, interface or performance attributes. Entries within a given row indicate the attribute value at the device shown in the column header. Medianet attributes include Jitter Mean, Packet Loss Count, Packet Expected Count and Packet Loss %; these statistics are not available in the Flow Path Analysis. AVC attributes include Application Delay Average, Network Delay Average and Retransmissions. Red or yellow table entries indicate performance exceeding alert or drop thresholds as defined in Tools > Configure Alerts.

Flow Path Ana	lysis				
Flow: UDP 192.0.2	2.35:4805 -> 10.0.2.25:5	004		1/27/14 11:26:00 AM - 11:31:00 AM	Refresh Show Path
	2921-Demo-67_111	1941-WAN-67_113	2921-Demo-67_112		
evice Name	2921-Demo-67_111	1941-WAN-67_113	2921-Demo-67_112		
PU Usage	72 - 77 %	98 - 99 %	55 - 58 %		
n IF +	GigabitEthernet0/1	GigabitEthernet0/1	GigabitEthernet0/1		
ut IF +	GigabitEthernet0/2	GigabitEthernet0/0	GigabitEthernet0/2		
n QoS Policy +	BaseIngressPolicy	Policy_NBAR	No Policy		
ut QoS Policy +	WAN-Shaping	WAN-Shaping	Parent-Shaper		
it Rate	222 Kbps - 4 Mbps	5 Mbps - 5 Mbps	394 Kbps - 405 Kbps		

Flow: UDP 192.0.3.25:5003 -	> 192.0.2.25:5003 SSRC: 30583	9/30/13 10:06:2	21 PM - 10:11:21 PM	Refresh Sho	w Path
	1941-WAN-67_113.referentia.com	2921-Demo-67_111.referentia.com	cat3560X-67_107		
Device Name	1941-WAN-67_113.referentia.com	2921-Demo-67_111.referentia.com	cat3560X-67_107		
CPU Usage +	56 - 64 %	99 %	95 - 96 %		
In IF +	FastEthernet0/1/1	GigabitEthernet0/2	Vlan1001		
Out IF +	GigabitEthernet0/0	GigabitEthernet0/1	Local		
In QoS Policy +	No Policy	No Policy	No Policy		
Out QoS Policy +	WAN-Shaping	No Policy			
Jitter Mean	2.60 - 3.70 ms	0.93 ms	122.74 ms		
Packet Loss Count	0	0	46		
Packet Expected Count	435 - 6,176	3,634	0 - 110		
Packet Loss % *	0.00 %	0.00 %	41.81 %		
Loss Event Count *	0	0	0 - 24		
Forwarding Status	Forwarded	Forwarded	Unknown		
Media Bit Rate	19 Kbps - 274 Kbps	161 Kbps	0 bps - 3 Kbps		
IP Bit Rate	0 bps - 280 Kbps	0 bps - 164 Kbps	0 bps - 3 Kbps		
DSCP and IPv6 Traffic Class	CS5 (40)	CS5 (40)	CS5 (40)		

In cases where devices within a given Medianet or AVC flow do not support Medianet or AVC, then the Medianet or AVC related attributes will be blank, as shown in the 2921-Demo-67_112 device column shown below.

Flow: TCP 1.4.1.1	->2.4.1.1:80		10/27	/14 11:53:00 AM - 11:58:00 AM	Refresh	Show Path
	LANIKAI_2921_1-105	LANIKAI_1941_1-106	LANIKAI_2921_1-107			
Device Name	LANIKAI_2921_1-105	LANIKAI_1941_1-106	LANIKAI_2921_1-107			
Application	share-point	share-point	share-point			
CPU Usage +	74 %	82 - 84 %	75 - 77 %			
In IF +	GigabitEthernet0/1	GigabitEthernet0/1	GigabitEthernet0/1			
Out IF +	GigabitEthernet0/2	GigabitEthernet0/0	GigabitEthernet0/2			
In QoS Policy +	SET_DSCP	No Policy	11C-BL_App-Match_GI01_In			
Out QoS Policy +	SHAPING	No Policy	MonitorUsingNbar_GI02_Out			
DSCP	BE (0)	BE (0)	BE (0)			
App Delay Avg	0 ms		16 ms			
Network Delay	12 ms		20 ms			
Retransmissions *	0		0			
Bit Rate	11 Kbps	154 Kbps	11 Kbps			

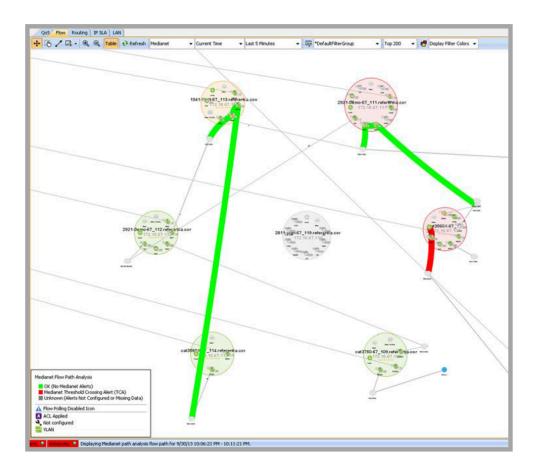
Flow: UDP 192.0.2.35:1083 -	> 10.0.2.25:5004 SSRC: 2221342720	1/3/14	2:18:40 PM - 2:23:40 PM Refresh	Show Path
	2921-Demo-67_111.referentia.com	1941-WAN-67_113.referentia.com	2921-Demo-67_112.referentia.com	cat3560X-67_107
Device Name	2921-Demo-67_111.referentia.com	1941-WAN-67_113.referentia.com	2921-Demo-67_112.referentia.com	cat3560X-67_107
CPU Usage +	66 - 77 %	72 - 85 %	75 - 83 %	51 - 62 %
In IF +	GigabitEthernet0/1	GigabitEthernet0/1	GigabitEthernet0/1	Null
Out IF +	GigabitEthernet0/2	GigabitEthernet0/0	GigabitEthernet0/2	Null
In QoS Policy +	BaseIngressPolicy	Policy_NBAR	No Policy	No Polic
Out QoS Policy +	WAN-Shaping	WAN-Shaping	Parent-Shaper	No Polic
Jitter Mean *	0.20 - 2.75 ms	0.47 - 2.10 ms		0.33 - 1.34 m
Packet Loss Count	0	11 - 10,494		0 - 4,20
Packet Expected Count	14,802 - 35,666	174 - 29,434		15,697 - 33,48
Packet Loss % *	0.00 %	6.32 - 35.65 %		0.00 - 19.14 %
Loss Event Count *	0	9 - 4,519		0 - 2,05
Forwarding Status	Forwarded	Forwarded		Unknow
Media Bit Rate *	655 Kbps - 2 Mbps	216 Kbps - 838 Kbps		699 Kbps - 1 Mbp
IP Bit Rate	669 Kbps - 2 Mbps	221 Kbps - 856 Kbps		710 Kbps - 1 Mbp
DSCP and IPv6 Traffic Class	AF41 (34)	AF41 (34)		BE (0
Last Media Event	Normal	Normal		Norma
Bit Rate			386 Kbps	-

Attribute	Value	Color
Device Name	Device Name	Note: Only Medianet alerts and thresholds are used to determine the device color. Green: Medianet alerts enabled, none exceeded alert thresholds. Red: At least one Medianet alert exceeded threshold. Gray: No Medianet alerts enabled or missing data.
CPU Usage	Min & max % values for the defined query period	Red: CPU usage exceeded alert threshold.
In IF	Input interface name	Amber: Ingress interface drops exceeded enabled drop alert threshold.
Out IF	Output interface name	Amber: Egress interface drops exceeded enabled drop alert threshold.
In QoS Policy	Input QoS policy name. The policy name reflects the current policy applied even if the query time is in the past.	Amber: Class drops detected in the input policy.
Out QoS Policy	Output QoS policy name. The policy name reflects the current policy applied even if the query time is in the past.	Amber: Class drops detected in the input policy.
Jitter Mean	Min and max mean values for the defined query period.	Red: Jitter mean value exceeded enabled mean jitter alert threshold.
Packet Loss Count	Min and max packet loss values for the defined query period.	
Packet Expected Count	Min and max packet expected count values for the defined query period.	
Packet Loss %	Min and max packet loss % values for the defined query period.	Red: Packet loss % exceeded enabled packet loss % threshold.
Loss Event Count	Min and max loss event count values for the defined query period.	Red: Loss event count > 0 and media loss event alert enabled.
Forwarding Status	Medianet forwarding status.	
Media Bit Rate	Min and max Medianet bit rates over the defined query period.	Red: Media bit rate count exceeded enabled media bit rate threshold.
IP Bit Rate	Min and max Medianet IP bit rates over the defined query period.	
DSCP and IPv6 Traffic Class	The DSCP value.	
Last Media Event	The last Medianet media event within the query period.	
Application Delay Average	Average application delay in milliseconds.	
Network Delay Average	Network delay in milliseconds.	Red: AVC network delay time per connection exceeded enabled AVC network delay time threshold.
Retransmission Count	Retransmission count.	Red: Retransmission count exceeded enabled retransmission threshold

- A "*" is appended to the end of the attribute name if the corresponding Medianet or AVC alert is enabled within LiveNX.
- A "+" is appended to the end of the attribute name if the corresponding Device/QoS alert is enabled within LiveNX.

Step 5: Click on Show Path in the Path Analysis Table to visualize and isolate the Flow, Medianet or AVC flow through the system topology

The flow colors correspond to the device colors in the Basic, Medianet or AVC Flow Path Analysis table. After clicking on Show Path, if you click on Refresh, only the Path Analysis table will update; you will need to click Show Path again to reflect the updated path results. **Note** Other operations in the flow system view such as changing the filter, refreshing, or merging/unmerging flows will remove the path analysis flow and redraw the system view normally. Click Show Path to redraw the path analysis flow.



Historical Playback

The Historical Playback feature in the Flow device-level view replays the historical Flow data collected over the previous 24-hour period. This feature has access to all the Flow data collected by LiveNX, and all the filtering options are available. Device-level flow playback can be shown in 10-second, 30-second, 1-minute, 5-minute, 30-minute, or 1-hour frames.

To open the flow historical playback feature, click Flow > Historical Playback.

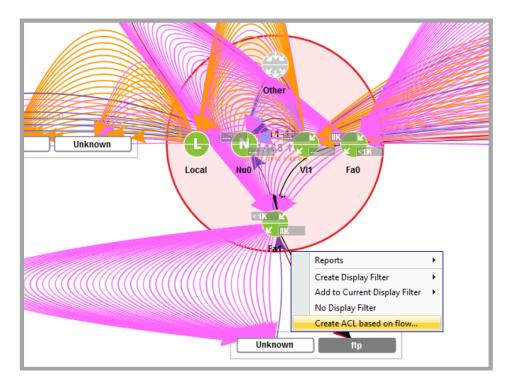
Note Historical Playback may cause flows to be dropped.

Below is an example of the Historical Playback display:

🗞 🔍 Basic	Flow 👻 🖙	*DefaultFilterGroup	p 👻	📑 Display Filter Colors 👻	End Points: IP Ad	dress 👻	Show 30 second	s 👻 per frame		1
• II ∢ D	Playback Fastest	- Date: Aug 17	7, 2012 👻 1	12:01:00 AM				09:17:30 AM	12:01:00 AN	1
^ 1 me	Protocol	Src IP Addr	Src Port	Src Cntry	Dst IP Addr	Dst Port	Application	TCP Flags	Src Pre	fi
:00:19 AM	UDP	172.16.67.145	61,473	-	172.16.67.113	161	snmp	—_A	24	
:00:30 AM	TCP	2.244.1.16	80	DE/Germany	1.244.1.1	4,266	http	APS	8	
:00:30 AM	TCP	2.244.1.4	443	DE/Germany	1.244.1.1	4,244	secure-http	-AP-S-	8	
:00:30 AM	TCP	2.23.1.1	110	EU/Europe	1.23.1.1	2,873	pop3	-AP-SF	8	
:00:30 AM	TCP	2.31.1.1	110	GB/United Kin	. 1.31.1.1	2,873	pop3	-AP-SF	8	
:00:31 AM	TCP	2.43.1.1	110	IT/Italy	1.43.1.1	2,873	pop3	-AP-SF	8	
:00:31 AM	UDP	2.4.1.1	55,542	FR/France	1.4.1.1	23,030		——A——	8	
:00:31 AM	UDP	1.4.1.1	23,030	CN/China	2.4.1.1	55,542		——A——	8	
		III			1.122.1.1 1.129	1 1 1 - 11 - 4	1.143.1.1 1.156.1		1.78.1.1	ſ
Web *7 MB / 12 Internet Network Ma	anagement		Local 172.16.87.1		1.122.1.1 1.128 1.206.1.1 1.216 1.906.1.1 1.100 1.906.1.1 1.1000 1.906.1.1000 1.906.1.100 1.906.1.10000 1.906.1.1000 1.906.1.10000000000000000000000000000000	1.1 1.226.1.1	1103.1.1 H 1.106. 1225.1.1 H 1.245. 1103.1.1 H 1.245.	1.1 1.7.1.1	1.78.1.1 1.87.1.1 1.161.1.1	
Color Mapping B Web *7 MB / 1: Internet Network MB / 1: Enterprise / Voice Video Network Ma	24 flows anagement 2 flows Applications 772:1687.32 172:168 172:1687.32 1772:168 172:1687.32		172.16.67.1 192.168.1.246 172.16.87.140		1.206.1.1 1.215 1.96.1.1 1.02	1.1 1.226.1.1	1.235.1.1 1.245.1	1.1 1.7.1.1	1.87.1.1	
Color Mapping B "Web "7 MB / 1: Internet Network Mr "2 MB / 1: Enterprise , Voice Video Video Network Mr "3 MB / 4 Directory Routing Peer-to-Peer- All-Remainin	24 flows anagement 2 flows Applications <u>1722-1667-352</u> <u>1722-167</u> 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 1722-167 172 1722-167 1722 1722 1722 172 172 172	Fa0150 77.455 172.16.67.116 77.255 172.16.47.135	172.16.67.1 192.168.1.246 172.16.87.140		1206.1.1 1216 141.1.1 1102	1.1 1.226.1.1	1.235.1.1 1.245.1	1.1 1.7.1.1	1.87.1.1	
Color Mapping B Web *7 MB / 1: Internet Network Mr *2 MB / 1: Enterprise / Voice Video Network Mr *3 MB / 4! Directory Routing Peer-to-Per	24 flows anagement 2 flows Applications 172:66:7:554 472:66:7:554 472:66:7:554 472:66:7:554 472:67:72:67 8 flows	Fa0150 77.455 172.16.67.116 77.255 172.16.47.135	172.16.67.1 192.168.1.246 172.16.67.224		1206.1.1 (1215 196.1.1 (102) 196.1.1 (102) 196.1.1 (102) 196.1.1 (102) 196.1.1 (102) 196.1	1.1 1.226.1.1	1.235.1.1 1.245.1	13 0 17.43 0 13 0 1682.13 0	1.87.1.1	

Create ACLs Based on Flows

Access Control Lists can be created directly from the system flow view. Right click on a flow (not merged) in the topology view and select Create ACL based on flow.



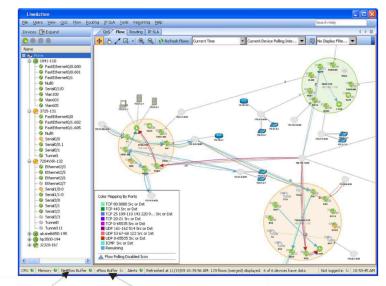
The resultant ACL Extended rule menu will appear with the relevant source IP, destination IP and port information already filled in.

Create a New ACL from Flow for 1811-13	×
Ereate a new ad with name Append rule to Insert rule at beginning of	
🖲 permit 🔘 deny 🔘 remark	
⑦ IP ⑧ TCP ◎ UDP ◎ Object-Group < No Object Groups >	
Source	
any by Network or IP 16.16.16 by Object-Group any by Network or IP 10.16.16.16 by Object-Group >> c = 100 160 1 0/04 = 100 160 1 0/04	
e.g 192.168.1.0/24 or 192.168.1.19 <no groups="" object=""> + e.g 192.168.1.0/24 or 192.168.1.19 <no groups="" object=""> +</no></no>	oups > -
⊘ by Port Equal to ✓ Manage Port(s)	
36105	
Match by DSCP v	
Log Rule Log 👻	
Save to Devio	e Cancel

For additional details about managing Access Control Lists, please see Chapter 12, Tools.

Flow Buffers

The Flow buffer status indicators will display the states of the Flow buffers.



NetFlow buffer status indicator sFlow buffer status indicator

- Green = normal
- Red = buffer overflow

The buffers will, under normal operating circumstances, remain green. If the indicator turns red, this indicates that the flow buffer has been exceeded. For Cisco devices, decreasing the number of devices utilizing NetFlow Collector mode will help remedy the situation.

The limitation of the flow buffer is determined by the performance of the Server or Node on which LiveNX is installed.

Flow Data Status

LiveNX also provides a report showing the status of flow data collection. To open the Flow Data Status dialog, select Flow > Data Status Report

Click Execute Overflow Status to view overflow, packet rate, and drops.

Click Execute Flow Counts to view current statistics for flow collection. Use the combo box to select 1, 6, 12, or 24 hours of data. The total flows and flows per second statistics are for the chosen duration. The flow count is the aggregate of flows overall flow technology types.

Verflow Status Execute Overflow Counts Node 2 Total Drops Current Overflowed: Current Packet rate: Total Drop: Total Drop: Current Drop: low Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Totals Overall: 99,465 flows. 1,657.75 flows per second.	Execute Overflow Counts Node 2 Total Drops Current Overflowed: Current Packet rate: Total Drop: Total Drop: Current Drop: low Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Totals			Flow Data Status		
Execute Overflow Counts Current Overflowed: Current Packet rate: Total Drop: Current Drop: Ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	Execute Overflow Counts Current Overflowed: Current Packet rate: Total Drop: Current Drop: Current Drop: Current Drop: Current Plow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Overall: 99,465 flows. 1,657.75 flows per second. Node 42 Device Count Flow Count Flow Count	verflow Status				
Ias Ever Overflowed: Current Packet rate: Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	las Ever Overflowed: Current Packet rate: Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Totals Overall: 99,465 flows. 1,657.75 flows per second. Node 42 Device Count Flow Count Flow Rate (fps) 1	Execute Overflow Counts	Node		≜ ² Total Drops	
Ias Ever Overflowed: Current Packet rate: Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	las Ever Overflowed: Current Packet rate: Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Totals Overall: 99,465 flows. 1,657.75 flows per second. Node 42 Device Count Flow Count Flow Rate (fps) 1	Current Quarflows				
Current Packet rate: Total Drop: Current Drop: w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	Current Packet rate: Total Drop: Current Drop: w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute \$ Totals Overall: 99,465 flows. 1,657.75 flows per second. Node ^2 Device Count Flow Count Flow Rate (fps) *1					
Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	Total Drop: Current Drop: ow Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Overall: 99,465 flows. 1,657.75 flows per second. Node 1 Flow Rate (fps)					
Current Drop: w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals	Current Drop: w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute © Totals Overall: 99,465 flows. 1,657.75 flows per second. Node ^2 Device Count Flow Count Flow Rate (fps) ~1	Current Packet rate:				
w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute \$ Totals	w Counts Execute Flow Counts Perform a full query for the count Data for last 1 minute Iminute Overall: 99,465 flows. 1,657.75 flows per second. Node Iminute 1 Flow Rate (fps)	Total Drop:				
Execute Flow Counts Perform a full query for the count Data for last 1 minute 0	Execute Flow Counts Perform a full query for the count Data for last 1 minute Totals Overall: 99,465 flows. 1,657.75 flows per second. Node 2 Device Count Flow Count Flow Rate (fps) 1	Current Drop:				
		Execute Flow Counts				
Device A 3 Node 2 IP Address Flow Count Flow Rate (fps) 1		Totals Overall: 99,465 flows. 1,657. Node 2 Device of Local	75 flows per	r second. Flow Count 41	Flow Rate (99,465	1,657.75
	SA Firewall Local 10.100.51.19 21,302 355.03	Totals Overall: 99,465 flows. 1,657. Node 2 Device 0 Local	75 flows per Count	Flow Count 41	Flow Rate (99,465 Flow Count	1,657.75
ISA Firewall Local 10.100.51.19 21,302 355.03		Totals Overall: 99,465 flows. 1,657. Node 2 Device (Local Device SA Firewall	75 flows per Count	Flow Count 41 A1 A2 IP Address 10.100.51.19	Flow Rate (99,465 Flow Count 21,302	1,657.75 1,657.75 Flow Rate (fps) 1
ASA Firewall Local 10.100.51.19 21,302 355.03 CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58	CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58	Totals Overall: 99,465 flows. 1,657. Node Local Device SA Firewall SS-C3850-23-31.liveaction.com	75 flows per Count ³ Node Local Local	Flow Count 41 41 41 41 41 41 41 41 41 41 41 41 41	Flow Rate (99,465	1,657.75 1,657.75 Flow Rate (fps) 71 355.03 346.58
ASA Firewall Local 10.100.51.19 21,302 355.03 CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9	CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9	Totals Overall: 99,465 flows. 1,657. Node Local Device SA Firewall SC-C3850-23-31.liveaction.com uppleFastLane-4331	75 flows per Count	r second. Flow Count 41 ▲2 IP Address 10.100.51.19 10.100.51.21	Flow Rate (99,465 Flow Count 21,302 20,795 12,054	Flow Rate (fps) 1,657.75 355.03 346.58 200.9
ASA Firewall Local 10.100.51.19 21,302 355.03 CSA-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9 ortiGate Firewall Local 10.100.51.29 8,977 149.62 SE-LiveWire-NY Local 10.100.50.80 6,207 103.45	CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9 FortiGate Firewall Local 10.100.51.29 8,977 149.62 E-LiveWire-NY Local 10.100.50.80 6,207 103.45	Totals Overall: 99,465 flows. 1,657. Node Local Device SA Firewall SS-C3850-23-31.liveaction.com ppleFastLane-4331 ortiGate Firewall E-LiveWire-NY	75 flows per Count ^A ³ Node Local Local Local Local	▲ 2 IP Address 10.100.51.19 10.100.51.21 10.100.51.21	Flow Rate (99,465 Flow Count 21,302 20,795 12,054 8,977	Flow Rate (fps) 1,657.75 55.03 346.58 200.9 149.62
ASA Firewall Local 10.100.51.19 21,302 355.03 CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9 FortiGate Firewall Local 10.100.51.29 8,977 149.62	CS-C3850-23-31.liveaction.com Local 10.100.51.1 20,795 346.58 AppleFastLane-4331 Local 10.100.51.21 12,054 200.9 FortiGate Firewall Local 10.100.51.29 8,977 149.62 SE-LiveWire-NY Local 10.100.50.80 6,207 103.45 RTR-DC-MPLS Local 10.100.51.4 6,184 103.07	Totals Overall: 99,465 flows. 1,657. Node Local Device SA Firewall SS-C3850-23-31.liveaction.com ppleFastLane-4331 ortiGate Firewall E-LiveWire-NY TR-DC-MPLS	75 flows per Count ³ Node Local Local Local Local Local Local Local	Flow Count 41 41 41 41 41 41 41 41 41 41 41 41 41	Flow Rate (99,465 Flow Count 21,302 20,795 12,054 8,977 6,207 6,184	Flow Rate (fps) 1,657.75 5.03 346.58 200.9 149.62 103.45 103.07

Database File Size

Over time, collecting Flow and QoS historical data can consume a considerable amount of disk space. To view and modify the database storage settings, select Options from the Tools menu, and then click Database.

0 0	Options	
	Database	
-©	All nodes Local	
Preferences Database	✓ Use 'All nodes' config QoS Database location: /data/livenx-server/data/nodes/Local/data/snmpstore	Back
	Database size: 28.418 GB (28.102 GB available for deletion)	Rese
Email	Automatically purge data older than: 180 C days (1 to 999 days)	Purg
9	Before purging, archive to: Local	
f Security	Flow	De als
	Database location: /data/livenx-server/data/nodes/Local/data/flowstore	Back
	Database size: 78.187 GB (74.086 GB available for deletion)	Res
	Automatically purge data older than: 30 C days (1 to 365 days)	Purg
	Before purging, archive to: Local	
	Alert	
	Database location: /data/livenx-server/data/nodes/Local/data/alertstore2	Back
	Database size: 144.279 MB (136.275 MB available for deletion)	Res
	Automatically purge data older than: 60 C days (1 to 365 days)	Pur
	Before purging, archive to: Local	
	Clong-Term	
		Pack

IP Mapping

The IP Mapping feature allows the mapping of an IP address or hostname to a user-defined label. This feature only affects the labeling within LiveNX and does not affect any actual DNS or hostname configurations.

IP Blacklist

The IP Blacklist feature allows the identification of IP addresses or hostnames that will appear in red in the topology, device, flow table, and historical views. This is a method of identifying quickly and visually any known anomalies. Alerts can be configured to notify the users when blacklisted IP addresses occur in the flow data.

Alerting

See Chapter 12, *Tools* for information about configuring Alerts.

NetFlow Collection

LiveNX is able to receive NetFlow from an array of different network devices. These devices mainly consist of Cisco, but LiveNX can also receive flow data from several different vendors. The following will describe mostly Cisco routers and switches.

Cisco Device and NetFlow Version Support

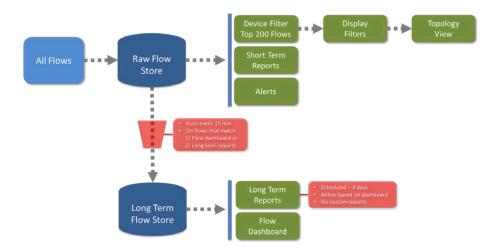
LiveNX NetFlow currently works with most Cisco routers and some Cisco switches.

Devices Supported	Cisco NetFlow Version	Cisco IOS Version
Cisco ASA 5500 security devices	Version 9	ASA 8.3
Cisco ASR 1000 series routers	Versions 5, 9	2.6.0 (12.2.(33)XNF)
Cisco 800 series routers	Versions 5, 9	12.3, 12.4, 15.0, 15.1
Cisco 1800 series routers	Versions 5, 9	12.3, 12.4, 15.0, 15.1
Cisco 1900 series routers	Versions 5, 9	15.0, 15.1
Cisco 2600 XM series routers	Versions 5, 9	12.3, 12.4
Cisco 2800 series routers	Versions 5, 9	12.3, 12.4, 15.0, 15.1
Cisco 2900 series routers	Versions 5, 9	15.0, 15.1
Cisco 3600 series routers	Versions 5, 9	12.3, 12.4, 15.0, 15.1
Cisco 3700 series routers	Versions 5, 9	12.3, 12.4
Cisco 3800 series routers	Versions 5, 9	12.3, 12.4, 15.0, 15.1
Cisco 3900 series routers	Versions 5, 9	15.0, 15.1
Cisco 7200 series routers	Versions 5, 9	12.3, 12.4
Cisco 7600 series routers*	Versions 5, 9	12.2
Cisco Catalyst 4500*	Versions 5, 9	12.2
Cisco Catalyst 6500*	Versions 5, 9	12.2

Note See http://www.cisco.com/go/fn for more information on required hardware for these platforms

LiveNX NetFlow Process Overview

The diagram below shows the LiveNX NetFlow components and how they fit into the process.



Collector Polling Modes

Cisco devices can provide NetFlow data in one or two different modes. LiveNX supports only Collector mode polling.

Databases

LiveNX stores raw flow data in the flow store database to generate flow topology views, short-term reports and flow related alerts. The raw flow data gets aggregated every 15 minutes and stored in the

long-term store database to generate the flow dashboard and the long-term reports. Long-term reports include scheduled reports with durations of greater than 4 days and ad hoc reports based on the flow dashboard. Custom flow reports (i.e., flow reports created using user-defined fields) regardless of duration length are generated using the raw flow store database.

Device and Display Filters

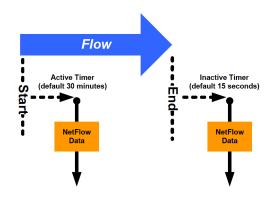
To make it easier to isolate and view specific flow information, LiveNX provides extensive filtering options that can be applied to both real-time and historical displays. Device filtering allows you to collect specific flow data from the devices and to reduce the amount of NetFlow information LiveNX processes.

Real-Time and Historical Displays

The real-time display gives you current NetFlow data, plus live visualizations at the topology-, device-, and interface-level views. The historical display review allows you to recall and visually examine detailed device-level information from the database.

Cisco NetFlow Collector Commands

The software will set up the NetFlow commands automatically on the device. Users can also manually change or add settings to adjust the behavior and performance of the device. The following table shows some of the NetFlow commands that are available. The Image below also shows the relationship between a flow in the network device and when NetFlow Collector data is sent back to LiveNX NetFlow. Additional information on NetFlow is available on the Cisco website.



Note Various timers and their effects as a new traffic flow starts and ends, traversing the network device. Based on a timer, the network device will forward a notification to the software, which will then display data on the screen.

NetFlow Command	Description
ip flow-cache timeout active 1	This command specifies when NetFlow Collector information is sent after a flow becomes active. By default, the last value in the argument is 30, which means long- lasting flows over 30 minutes will not show up until they hit this timeout value. For more interactive debugging, a value of 1 minute is suggested, which will have the effect of more information being sent to the software.
ip flow-cache timeout inactive 15	This command specifies when NetFlow Collector information is sent after a flow becomes inactive. By default, the timeout value is set to 15 seconds.
ip flow-export destination [ip address] 2055	This command is automatically set up by the software to tell the device where to send NetFlow Collector information (IP address of the PC where the software is installed). The last value is the port number typically used.
ip flow-export version [Version Number]	The software currently supports NetFlow versions 5 and 9. If NetFlow is not configured on the device, the software will enable version 5. If NetFlow is already configured on the device, then the software will operate with that NetFlow version.
ip flow-export source [interface]	This command can be used to tell the device which interface to use for sending NetFlow information to the software.
ip flow ingress ip flow egress	These commands are issued on a per-interface basis for collecting NetFlow information on flows in either direction. By default, LiveNX will configure egress and ingress NetFlow export for a Cisco routing device interface. This can be changed manually at the command line.

Note Some Cisco devices may not support egress export, and LiveNX will indicate the egress commands that failed. Unless the ingress commands also show up in the failed list, they will have been applied successfully. See *http://www.cisco.com/go/fn* for more information on supported platforms.

Flexible NetFlow (FNF)

Flexible NetFlow allows user-configurable NetFlow record formats, selecting from a collection of fields:

- Key, non-key, counter, timestamp
- User-defined NetFlow key fields

Advantages

- Tailor a cache for specific applications not covered by the existing 21 NetFlow features in traditional NetFlow
- Different NetFlow caches (e.g., per subinterface, per direction [ingress, egress], per sampler)
- Better scalability, since flow record customization for a particular application, reduces the number of flows to monitor

Features for Tracking

- Layer 2 for switching environments
- Layer 3 and Layer 4 for IP info (more so than with traditional NetFlow)
- Up to Layer 7 with deep packet inspection (NBAR integration in IOS 15.0.)
- Medianet Performance Monitoring

Platforms

See *http://www.cisco.com/go/fn* for more information on supported platforms. Beginning with Cisco IOS Release 12.4(20)T, traditional NetFlow for IPv6 is being replaced by Flexible NetFlow for IPv6. Cisco Express Forwarding (CEF) or distributed CEF (dCEF) is required.

Configure Flow

The Configure Flow feature allows each device to get configured for either standard or Flexible Net-Flow. Click Flow > Configure Flow or by right-clicking on a device in the device view and then selecting Flow > Configure Flow. This capability is available to Admin and Full-Config user roles.

After clicking on Flow > Configure Flow, LiveNX displays a Flow Configuration summary table listing all the devices discovered by LiveNX as well as its properties including Type, IP Address, Description, Tags, and several Flow Configuration Options.

	t devices to configure flow onfiguration Table										
Q	oninguration rable										_
Sel	Device	Туре	IP Address	Description	Tags	Traffic	Applic	Voice/Vid	Traditi	Custom	
	1386_Black_Core	Standard		33 Cisco IOS S	bridg	•	\odot	0	6	•	
	1811-13	Standard	+ 192.168.1.	13 Cisco IOS S	-		\odot	•	6		Ξ
	1811-240	Standard		240 Cisco IOS S	-	•	\odot	•	۲	•	
	1941-WAN-67_113	Standard		113 Cisco IOS S	-	۲	۲	۲			
	2921-Demo-67_111	Standard		111 Cisco IOS S	-	0	0	0	\odot	\odot	
	2921-Demo-67_112	Standard		112 Cisco IOS S	-	•	•	۵	•	•	
	3750-235	Standard	+ 192.168.1.	235 Cisco IOS S	-	0		(7.11)	0	0	
	3925-VPN-163	Standard	+ 192.168.1.	163 Cisco IOS S	-		21-Demo eAction Fl	•67_112 NF configurat	ion found		
	4503-145	Standard		145 Cisco IOS S	-			I-FLOWMON		0	
-	A	- · · ·	1				GigabitEt	nernet0/1		0	

The Type drop-down field is used to determine the device series. Default is standard. Other options are the Catalyst 3850 (two flow monitors for monitoring an interface: ingress and egress), Catalyst 4500 (only allows monitoring in the ingress direction) and Catalyst 6500. LiveNX takes a best guess at the device type; the drop-down selection allows you to change the Type as needed.

The IP Address is the IP Address of the device.

The Description is the description field retrieved from the device. It should match the Description field that is shown in the LiveNX system device expanded view.

The Tags are the compilation of the labels, capacities, WAN, Sites, and Tags that you defined for that device. Creating labels, capacities, WAN, Sites & Tags are covered in Chapter 12- Reports.

The Traffic Statistics (FNF), Application Response Time (AVC), Voice/Video Performance (Medianet), Traditional NetFlow and Custom (Flexible NetFlow settings not set by LiveNX) flow configuration options summarize the device's capability to support the various flow configuration options, as well as to show the flow configuration currently configured on that device.

- A green LED indicates the flow technology that is configured on that device.
- A white LED indicates the flow technology that is supported on the device, but is not currently configured.
- The LED with the strikeout marking indicates a flow technology that is not supported on that device.

In the example shown above, the 2921-Demo-67_112 device has Traffic Statistics (FNF), Application Response Time (AVC) and Voice/Video Performance flow technologies configured, while Traditional NetFlow and Custom NetFlow are supported, but not configured.

over over an entry in the flow configuration columns to get additional details about the flow configuration by the interface.

Type in an alphanumeric string next to the magnifying glass to filter the flow configuration table.

Configure or modify your device's flow configuration by clicking on the leftmost check box and clicking on Configure Selected. After loading in the device configurations, LiveNX will expand the device entries in the Flow Configuration table to include the managed interfaces.

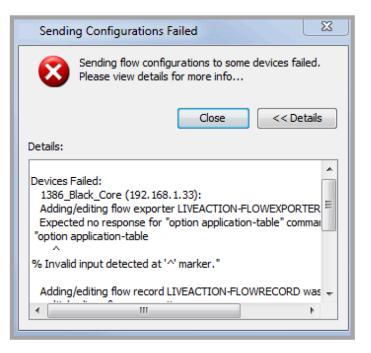
_	tructions onfigure the type of flow you	wish to receive fr	om the	interfaces								
	w Configuration Table											
Q	v.											
De	vice	Туре		IP Address	Description	Tags	Traffic	Applica	Voice/Vide	Traditio	Custom	
.	1386_Black_Core	Standard	•	192.168.1.33	Cisco IOS So	bridge		0	0	۲		
	- 🚱 FastEthernet4	-		10.54.201.1	LINK_TO_SI	engine		-	-	V		
	🍪 Tunnel0	-				sick bay		-				
	🎯 Tunnel 1	-				transp		-	-			
	🔮 Tunnel 2	-				bridge		-	-	V		
	🚱 Vlan201	-		10.54.200.1	SatCOMM m	bridge		-		V		
	🚱 Vlan216	-		10.54.216.1	Tunnel 216 V	ten for		-		V		
	😔 Vlan54	-		10.54.200.9	WiMax VLAN	weapons		-		V		
÷	3 2921-Demo-67_112	Standard	-	172.16.67.112	Cisco IOS So	-	۲	۲	۲			
	😔 GigabitEthernet0/1	-		10.0.3.1	1941-Demo	-	v		V			
	😌 GigabitEthernet0/2	-		192.0.4.2	cat3750-67	-	V	V	V			
	😌 Loopback0	-		112.112.112.112		-	V					L
	😌 Tunnel0	-		100.100.100.112			7					

Click on a check box to toggle the various flow configuration options. A hyphen mark in a flow technology entry indicates a flow technology which is unsupported by that device. Once a new selection is made, the Save to Devices, Preview CLI and Revert buttons will be enabled.

• Preview CLI – click on Preview CLI to review the commands that LiveNX will send to the device to re-configure flows on the selected interfaces. Use the device table on the left to select a device in the list.

Multiple CLI V	iewer		X
Device	Туре	2921-Demo-67_112	
1386_Black_Core		config t	
2921-Demo-67	Standard	class-map LIVEACTION-CLASS-MEDIANET	
		no match access-group name match5004	
		exit	
		interface Loopback0	=
		mace enable	
		exit	
		flow monitor type mace LIVEACTION-FLOWMONITOR-AVC	
		no record LIVEACTION-FLOWRECORD-AVC	
		exit	
		no flow record type mace LIVEACTION-FLOWRECORD-AVC	
		no flow exporter LIVEACTION-FLOWEXPORTER	
		flow exporter LIVEACTION-FLOWEXPORTER	
		description DO NOT MODIFY. USED BY LIVEACTION.	
		destination 172.16.131.121	
		source GigabitEthernet0/0	
		transport udp 2055	
		template data timeout 600	
		option application-table	
			Close

- Revert click on the Revert button to return your flow configuration settings back to the initial state prior to any "Save to Devices" command.
- Back click on the Back button to return to the device the only view of the flow configuration table.
- Close close the flow configuration table.
- Save to Devices LiveNX will ask you to confirm that you would like to configure the devices. If confirmed, LiveNX will modify the flow configuration for the selected interfaces on the device. A message will be generated to indicate successful re-configuration of that device or to indicate details on the errors encountered during the flow configuration.



Enabling NetFlow

According to Cisco best practices, enabling NetFlow export consists of two steps:

- Enabling NetFlow on the relevant physical and logical interfaces on the network device
- Enabling the device to export the flow information from the device over the network

Item	Description			
Working With Existing NetFlow Tools	Because more than one NetFlow tool may be talking to a particular device, users should be cautious when setting up the software with respect to these other tools, since some of the settings may be incompatible. Also note that the IOS has limits on the number of NetFlow Collector export targets.			
NetFlow Polling	LiveNX only supports Collector mode. Collector mode depends on the expiration of active and inactive flows, and therefore may result in delays when depicting the flow characteristics within the device.			
Device and Software CPU Utilization	Because NetFlow adds additional processing requirements on the device, users should monitor CPU utilization from time to time. Also, if the Collector sends a lot of NetFlow data, this can substantially increase CPU usage on the device and client PC. CPU usage can be reduced by lowering polling rates or turning polling off for the devices. Merged flows can also be displayed in place of individual flows to further reduce CPU usage on the PC. For NetFlow Collector mode, settings can be changed on the device to reduce CPU usage, such as adding filters and reducing the refresh rate of templates being sent. For more information, refer to the Cisco NetFlow Configuration Guide.			
NetFlow Bandwidth Usage	In collector mode, a large amount of NetFlow packets may be sent from the device to the software. For this reason, caution should be taken to understand the impact on the network and the device. The settings can be changed from the Tools menu by selecting Options and then clicking Polling . From the Interval column, select the polling rate from the drop-down list. The indicator will turn red if too much NetFlow data comes in from devices.			
Starting NetFlow Collector Mode	NetFlow must be enabled on the router or switch, which the software can do for you when the device is added. When the flow is sent to the software and NetFlow polling is enabled, the software will display NetFlow information.			
Specifying NetFlow Data Using the CLI	Although LiveNX NetFlow does not require the use of the command line interface (CLI), the CLI can be used, if desired, to set up the device for specific NetFlow data.			
NAT in Collector Mode	In Collector mode, the device will be sending the data back to the software. If the device is behind a NAT boundary, it may not be able to send the packet back to the PC on which the software is running.			
Accuracy and Flows From Interfaces Without NetFlow	If NetFlow is not enabled on all interfaces, the flow view may have gaps and will not provide a true representation of the top flows in the device. For this reason, ingress and egress NetFlow should be enabled on the major interfaces on the device.			
Removing Software as Collector	When you properly exit LiveNX NetFlow while it is running in Collector mode, the software will automatically remove itself as a Collector export target. However, if the software is abnormally terminated, the export target may not have been removed in the device. You can check this by looking for ip flow-export destination in the running configuration, or by looking at the device's export status. To remove the Collector manually, issue the no ip flow-export destination command directly on the device.			
Item	Description			

Item	Description
Software IP Address and Using DHCP in Collector Mode	When using the software in NetFlow Collector mode, care must be taken to ensure that the IP address given to the device for the PC with the LiveNX software installed does not change. If the PC with the installed software received its IP address by DHCP, it should either be configured to always receive the same IP address or set up as a static IP address.
Firewall Issues	When using the software in NetFlow Collector mode, the user must ensure that the NetFlow packets from the device can traverse the firewalls in the network, as well as on the PC that is running the software. NetFlow data is typically a UDP packet running on port 2055. This port may need to be configured on the firewall to allow data to pass through.
Scalability	The software can scale to include many devices, but the ability to scale is dependent on the type of PC, its capabilities, the polling rate, and type of graphs being displayed.
NetFlow Collector Expiration Behavior	The expiration timers can be adjusted to change how quickly the device exports NetFlow records and how quickly flows will appear in LiveNX. The shorter the active and inactive times, the more responsive the NetFlow display will appear. However, this may increase the amount of processing required.

LiveNX is able to configure traditional NetFlow on most NetFlow capable devices. If you configure Net-Flow using the Command Line Interface (CLI), you must decide whether to enable ingress NetFlow, egress NetFlow, or both for each device. This decision depends on the intended use, topology, and whether or not the device supports either or both directions.

Note Egress NetFlow is dependent on the version of Cisco IOS you are running. For more information, go to: *http://www.cisco.com/go/fn*.

Disabling NetFlow

The following example shows how to disable ingress NetFlow for an interface labeled "GigabitEther-net0/0."

myrouter#configure terminal

myrouter(config)#interface GigabitEthernet0/0

myrouter(config-if)#no ip flow ingress To disable egress NetFlow, use the ip flow egress interface subcommand as follows: myrouter(config)#interface GigabitEthernet0/0

myrouter(config-if)#no ip flow egress

Note Ingress NetFlow is the most commonly used method. Egress NetFlow is more commonly used with MPLS VPN. The MPLS Egress NetFlow Accounting feature allows you to capture IP flow information for packets undergoing MPLS label disposition (i.e. it captures packets that arrive on a router as MPLS packets and are transmitted as IP packets). Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computations that occur in the traffic-forwarding path of the router.

Advanced NetFlow Collector Commands

Cisco devices are able to support advanced capabilities, including the ability to filter or sample particular flows. This helps narrow down the NetFlow data that is sent to the software and also reduces the CPU consumption of the device. NetFlow input filtering and random-sampled NetFlow features can set up the device to collect data from specific subsets of traffic.

The NetFlow input filters provide NetFlow data for a specific subset of traffic by creating filters for selected flows. By creating a class map for input filtering, this helps focus the NetFlow data on the desired types of traffic. The random-sampled NetFlow feature randomly selects a packet from a sequence of packets or provides the random sampling from the device's NetFlow cache. The sampling period can be adjusted depending on the amount of granularity desired. Additional information on configuring these options can be found on the Cisco website.

Precautions When Using NetFlow Collector Mode

- The amount of bandwidth used to send NetFlow data and its effect on device performance should be verified.
- NetFlow Collector in the software has to be manually started by clicking Enable Polling, or going to the Tools menu and selecting Options, and then clicking Polling for each device when it is initially brought in.
- The software enables ingress and egress NetFlow and will collect all NetFlow data from the device, but will only show the top 200 flows based on size. Adjust the device NetFlow settings such as filtering, sampling, template refresh, and various timers to ensure the device is within operational limits.

Deployment Considerations

For optimal performance, the following are additional items that should be considered prior to deploying the LiveNX NetFlow technology module:

LiveNX Flow Configuration

Cisco NetFlow

LiveNX NetFlow will automatically set up the device for proper NetFlow operations. Typically, the user will not have to send any other commands to the device, except for specialized behavior or for flexible NetFlow setups. The wizard for adding devices into the software will guide the user through the procedure and send down the proper settings to the device.

Note Changes that are made to the device's running configuration only. To make them permanent, these new settings can be saved manually to the device's startup configuration.

Default Flow Settings

By default, LiveNX listens for NetFlow Collector traffic on port 2055 and sFlow traffic on 6343. If you need to modify these settings from their defaults, they can be modified in the "application.proper-ties.example" file. Start by renaming the file to "application.properties" and edit it in a text editor.

Note Because it can generate a large volume of packets, polling for NetFlow Collector mode is turned off by default. Polling can be enabled by clicking Polling on the Options dialog box, accessed from the Tools menu by selecting Options, or by clicking Enable Polling in the device-level view.

If an interface sending NetFlow Version 9 IPv4 data, disable Version 5 data export on that interface; otherwise, data may be double counted. If Version 9 is used for IPv6 data, Version 5 doesn't need to be disabled).

To edit the flow export port and data directory, go to: .. Program FilesLiveAction Server2.2configapplication.properties

Device Configuration Notes

IPv4 Configuration

- There must not be duplicated configurations between standard collection and Flexible NetFlow (i.e. if all interfaces are set up for standard collection and one of those interfaces will be used for Flexible NetFlow, standard NetFlow must be disabled on that particular interface).
- When using Flexible NetFlow for IPv4, the minimum required fields must be met for LiveNX to collect data. (Refer to the Minimum Required Template Fields table for a list of minimum required fields. LiveNX does not collect data from all fields).

IPv6 Configuration

- Ensure that multiple IPv6 Flexible NetFlow configurations that meet the minimum required template fields are not created; otherwise, duplicated flows will be received.
- When using Flexible NetFlow for IPv6, the minimum required fields must be met for LiveNX to collect data. (Refer to the Minimum Required Template Fields table for a list of minimum required fields. LiveNX does not collect data from all fields).

Medianet Configuration

LiveNX supports both the RTP and TCP performance monitor flow record types.

Note If using Performance Monitoring Flexible NetFlow on the same interface with standard NetFlow exports you may see the same flow show up twice (once for Medianet Performance Monitoring and once for the standard NetFlow export).

Cisco Adaptive Security Appliance (ASA) Configuration

- LiveNX collects modified standard template fields exported by an ASA. Configuration of ASAs is not supported; you must set up access lists and flow export manually. Select the Monitor Only check box on the Add Device dialog box when adding an ASA to the topology (i.e. no support for QoS, IP SLA, Routing, or access control list management).
- Refer to the Minimum Required Template Fields table for a list of minimum template fields required for LiveNX to collect ASA data.

Minimum Required Template Fields

- A = Field required in order for LiveNX to identify and store ASA flows
- R = Field required in order for LiveNX to identify and store flows
- S = Stored by LiveNX in its NetFlow database
- T = Part of standard IOS NetFlow template
- N/A = Not applicable

Field Type	IPv4 Field Usage	IPv6 Field Usage	LiveNX GUI Field Name	Description
IN_BYTES	R, S, T	R, S, T	Bytes	Incoming counter for the number of bytes associated with an IP flow.
IN_PKTS	S, T	S, T	Packets	Incoming counter for the number of packets associated with an IP flow.
PROTOCOL	A, R, S, T	A, R, S, T	Protocol	IP protocol identifier (e.g., TCP, UDP, ICMP, etc.)
SRC_TOS	R, S, T	R, S, T	DSCP	Type of Service byte setting when entering incoming interface.
TCP_FLAGS	S, T	S, T	TCP Flags	Cumulative of all TCP flags seen for this flow.
L4_SRC_PORT	A, R, S, T	A, R, S, T	Src Port	TCP/UDP source port number (i.e., FTP, Telnet, or equivalent).
IPV4_SRC_ADDR	A, R, S, T		Src IP Addr	IPv4 source address.
SRC_MASK	S, T		Src Prefix Len	Source address subnet mask length.
INPUT_SNMP	A, R, S, T	A, R, S, T	In IF	Input identifying interface index.
L4_DST_PORT	A, R, S, T	A, R, S, T	Dst Port	TCP/UDP destination port number (i.e., FTP, Telnet, or equivalent).
IPV4_DST_ADDR	A, R, S, T		Dst IP Addr	IPv4 destination address.
DST_MASK	S, T		Dst Prefix Len	Destination address subnet mask length.

Field Type	IPv4 Field Usage	IPv6 Field Usage	LiveNX GUI Field Name	Description
OUTPUT_SNMP	A, R, S, T	A, R, S, T	Out IF	Output identifying interface index.
IPV4_NEXT_HOP	S, T		Next Hop IP Addr	IPv4 address of next-hop router.
SRC_AS	S, T	S, T	Src AS	Source BGP autonomous system number.
DST_AS	S, T	S, T	Dst AS	Destination BGP autonomous system number.
LAST_SWITCHED	R, S, T	R, S, T	Last Switch	System uptime at which the last packet of this flow was switched.
FIRST_SWITCHED	R, S, T	R, S, T	First Switch	System uptime at which the first packet of this flow was switched.
IPV6_SRC_ADDR		R, S, T	Src IP Addr	IPv6 source address.
IPV6_DST_ADDR		R, S, T	Dst IP Addr	IPv6 destination address.
IPV6_SRC_MASK		S, T	Src Prefix Len	Length of IPv6 source mask.
IPV6_DST_MASK		S, T	Dst Prefix Len	Length of IPv6 destination mask.
IPV6_FLOW_LABEL		R, S, T	IPv6 Flow Label	IPv6 flow label per RFC 2460 definition.
ICMP_TYPE	S	s	ICMP Type	Internet Control Message Protocol (ICMP) packet type.
FLOW_SAMPLER_ID		S, T	N/A	ldentifier shown in "show flow-sampler."
IN_SRC_MAC	s	s	In Src MAC	Incoming source MAC address.
SRC_VLAN	S	S	Src VLAN	Virtual LAN identifier associated with ingress interface.
DST_VLAN	S	S	Dst VLAN	Virtual LAN identifier associated with egress interface.
DIRECTION		S, T	N/A	Flow direction: 0 = ingress flow, 1 = egress flow
IPV6_NEXT_HOP		S, T	Next Hop IP Addr	IPv6 address of next-hop router.
IPV6_OPTION_HEADERS		S, T	N/A	IPv6 option headers found in the flow.

Field Type	IPv4 Field Usage	IPv6 Field Usage	LiveNX GUI Field Name	Description
IN_DST_MAC	s	s	In Dst MAC	Incoming destination MAC address.
IN_PERMANENT_BYTES	А	А	Bytes	Running byte counter for a permanent flow.
FORWARDING STATUS	s	s	N/A	Forwarding status of flow (Refer to the Cisco Technology White Paper, NetFlow Version 9 Flow-Record Format.).
app_id	S	s	NBAR App	NBAR application identifier.

Non-Cisco Device Flow

LiveNX Flow monitoring of devices other than Cisco devices is enabled by default.

Note However, it is necessary to manually configure a non-Cisco device to export its Flow information.

Click File > Edit Device Settings to change non-Cisco device settings.

Edit Non-Cisco - J2320-16	ı 🛛	Edit Non-Cisco - J2320-167	
Steps	Device Connection Information	Steps	Enable Poling
1. Device Connection Information	Enter the SNMP connection information	1. Device Connection Information	Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section
2. Select Interfaces	IP Address 192,168.1.167	2. Select Interfaces	
3. Enable Polling	IP Address 192.166.1.167	3. Enable Polling	
4. Device Updated	Ube the Default SMPE connection settings Exter SMPE connection settings for this device SMPE Version V2C Y Target Port Est Community String	4. Device Updated	Poling Rate 🛛 seconds 💌 Polithe following features 💟 Flows
	<back next=""> Finish Cancel Help</back>		<back cancel="" hep="" hep<="" th=""></back>

sFlow Collection

The sFlow standard describes a mechanism for capturing traffic data in switched or routed networks. It uses a sampling technology to collect statistics from the device and is applicable to high-speed networks. A sFlow agent is the implementation of the sampling mechanism on the hardware. The sFlow Collector is a central server which collects sFlow datagrams from agents and stores them for analysis. The sFlow agent uses two forms of operation: a statistical packet-based sampling of switched or routed packets, and time-based sampling of interface counters. The basis for the LiveNX implementation of a sFlow Collector is similar to the collection and parsing of NetFlow and J-Flow packets. The LiveNX sFlow Collector collects and parses sFlow export packets sent by a remote network device, and passes along the flow information to the LiveNX flow database.

sFlow Export Format

The sFlow Collector supports parsing of the three main sFlow export versions: 2, 4, and 5. Flow information will be gathered from either the flow packet header provided in the export packet or the IP Flow information data format. Only IPv4 flows are currently supported.

Because sFlow does not provide switch time information, the start time for the flow will be reported as the uptime of the device when the export packet was received, as reported in the export packet header. The last switch time will be the same as the first switch time since this information is unknown and cannot be estimated. This restriction means the flow data rate cannot be calculated.

sFlow Collector

The sFlow Collector parses received export packets using the published export format to collect the following fields from either the packet header or the IP Flow information format.

- IPv4 source address
- IPv4 destination address
- Input interface
- Output interface
- Flow byte count
- First switched time
- Layer 4 source port
- Layer 4 destination port
- IP protocol number
- ToS

Because sFlow does not provide timely information, the start time for the flow will be reported as the uptime of the device when the export packet was received, as reported in the export packet header. The last switch time will be the same as the first switch time since this information is unknown and cannot be estimated. This restriction means the flow data rate cannot be calculated.

The flow byte count will be calculated using the following formula:

UDP traffic	Byte Count = Mean Skip Count * UDP Datagram Length
Non-UDP traffic	Byte Count = Mean Skip Count * (Sampled Packet Size – Stripped Count – Frame Offset to IP Header)

J-Flow Collection

The J-Flow Collector will collect the following fields from either the packet header or the IP flow information format:

- IPv4 source address
- IPv4 destination address
- Input interface
- Output interface
- Flow byte count
- First switched time
- Last switched time
- Layer 4 source port
- Layer 4 destination port
- IP protocol number
- ToS

CHAPTER 9

Routing

In this chapter:

Routing Overview.	196
LiveNX Policy-Based Routing (PBR)	203

Routing Overview

LiveNX Routing is a technology module that provides real-time routing-layer visualizations for Cisco networks, including Virtual Routing and Forwarding (VRF) tables. In addition, the module's policy-based routing feature provides a high degree of control, allowing users to route traffic easily and predictably over user-specified paths.

Applications and Benefits

Network Architecture Analysis

- Identify routing protocols in use
- Establish baseline nominal routing behavior
- Perform Virtual Routing and Forwarding
- Rich routing topology visualizations

Security

- Identify hijacked routes
- Track routes for suspicious flows to source-specific hostnames or IPs
- Zero in on specific traffic by filtering routes by destination or type

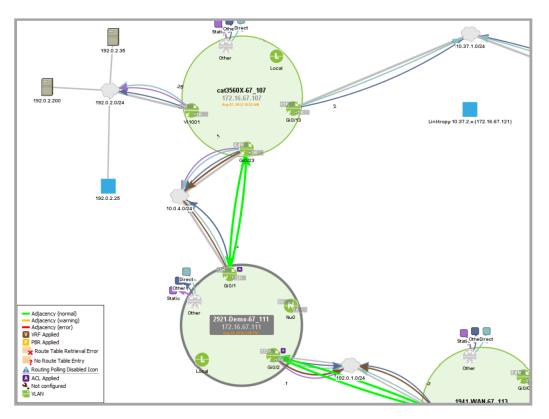
Troubleshooting

The LiveNX routing feature can be used to detect the following information and conditions:

- Static routes
- Black holes
- PBR applied, but forgotten
- Summarization errors
- Route loops
- Asymmetric routing
- EIGRP, IS-IS and OSPF Adjacency conditions

How LiveNX Routing Works

LiveNX shows routes in both tabular and graphical formats. The graphical topology view is given in the context of the physical interfaces on each network device. Each subnet is represented as a "cloud," and route arrows originate at router interfaces and terminate at the subnet "cloud" to which they route. In this way, LiveNX gives a bird's-eye view of routing across multiple devices.



LiveNX Routing Topology View—the Routing module retrieves routing information by opening a CLI connection (either Telnet or SSH) to the device and issuing a "show" command (show IP route for the route table and show route-map for the PBR statistics). This data is kept in a database on the LiveNX server.

LiveNX Tip—The "Other" Interface

The interface labeled Other in each network device shown in the topology view is a catchall for any routing points in the network device that are not otherwise shown. In the case where Null traffic is not displayed separately, routes attached to Null would be shown using the Other interface.

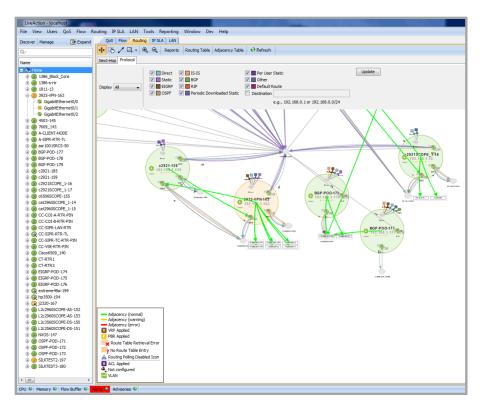
LiveNX Routing Views

System-Level View

The Routing system-level view makes it easy to visualize routing across your network. The system-level routing visualization shows the routes of all devices in a graphical format. The route paths and the interfaces that are routing them are indicated by arrows. The directional arrows are also color coded to indicate whether the route is a static route or derived from a particular routing protocol. You can apply a filter to display routes based on specific protocols and/or destinations.

Filtering Routes

The Protocol option filters by protocol or destination IP. LiveNX parses the routing information collected to determine the route for a particular protocol or destination network (in CIDR format). Click on the Protocol tab to display route filter options.

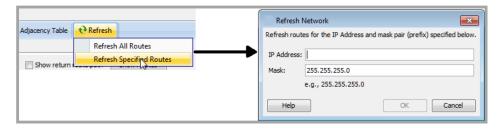


Refresh Routes

Route displays are refreshed manually. To refresh the routing tables and the information in the system topology view, click Refresh Routes in the Routing toolbar and select an option. If Refresh Specified Routes is selected, indicate the route IP address and mask pair, as shown below.

Note The following describes the Cisco IP address and mask pair prefix according to Cisco's command reference, "When the longer-prefixes keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed."

For more information, go to: http://www.cisco.com/en/US/docs/ios/12_2/iproute/command/reference/ 1rfindp2.html#wp1022511.



Refresh Timeout Limit

Some refresh operations may take a long time due to one or more of the following factors:

- The device has a very large routing table.
- There is a very high load on the CPU running LiveNX.
- The device is connected to LiveNX over a high-latency path.

If the route display refresh is not completed within 30 seconds, LiveNX will time out and show an error message. If this happens, reduce the load by limiting the refresh operation to specific routes that match the specified IP address and mask pair prefix, rather than refreshing all routes.

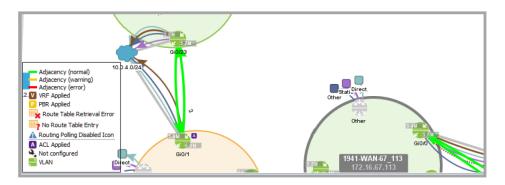
Note The refresh operation applies only to the display, and does not affect the device's configuration or any of the routes themselves.

Routing Adjacency

The Protocol tab displays neighbor adjacencies for the EIGRP and OSPF routing protocols. This information is displayed visually on the system level topology within the Protocol sub tab and in table form within the Adjacency Table. Adjacency information can be displayed with protocol filter information or each type of data shown exclusively by using the Display drop down in the Protocol tab.



The adjacencies will show up as edges from router interface to adjacent router interface. In cases where the interface of the adjacency cannot be determined the edge will show from the router itself and not from any particular interface. The adjacency will be colored either green, orange or red. For the case of OSPF, green indicates a FULL state, DOWN state is red and all other states such as INIT, ATTEMPT, 2WAY, LOADING, EXSTART, LOADING, EXCHANGE are in orange.



Next-Hop Routing

Next-Hop Routing provides a graphical representation of next-hop entries in route tables. This provides you with an easier means of understanding system-level routing across their networks.

A path in the Next-Hop visualization is a set of edges that describes the route from the source point to the destination. Endpoints in the topology can be one of three types: interface, network, or node. A network interface on a device loaded into the system can be the source or destination point of the routing algorithm. An IP network connected to an interface loaded into the system can also be the source or destination point of the routing algorithm. The third endpoint type, node, must be an IP address of a node that is contained in a network loaded into the system. If the node address does not exist in a network in the system, the node cannot be used as a source address; no routing will be performed in this case. If the node is a destination, routing will progress to the last device in the system that can route the packet, and the node will be represented by a "missing node" object.

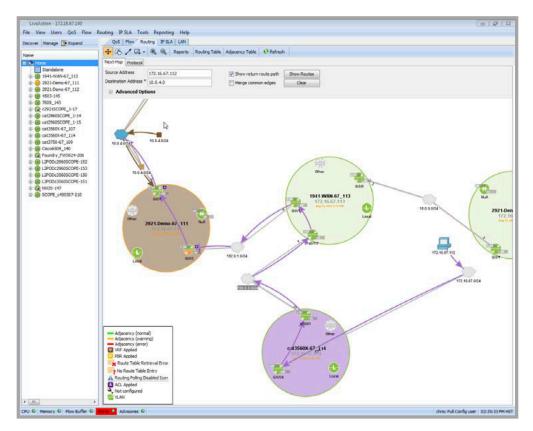
To access Next-Hop Routing visualization, click on the Routing tab. Below the system topology toolbar, select Next-Hop.

QoS Flow Routing IP SLA LAN	
🕂 🔀 🖍 🖫 🔹 🔍 Reports Routing Table	Adjacency Table 🕂 Refresh
Next-Hop Protocol	
Source Address 192.168.1.0	Show return route path Show Routes
Destination Address * 192, 168, 1, 33	Merge common edges
Advanced Options	
Merge threshold 1	
Show loops	
☑ Enable colors	

Use the parameters below to set up Next-Hop Routing. Click Show Routes to execute Next-Hop Routing visualization, or click Clear to reset the view.

Parameter	Description
Source address	Originating (starting-point) router's IP address.
Destination address	Target (ending-point) device or host IP address.
Show return route path	Select the check box to draw the return route as another line.
Merge common edges	Select the check box to combine common edges when Next-Hop routes are drawn. Unmerged edges are only displayed if the check box is cleared; merged edges are only displayed if the check box is selected.
Clear	Removes drawn Next-Hop routes.
Show routes	Draws the specified route.
Merge threshold	Limits the number of drawn routes to merge.
Show loops	Select the check box to draws routes.
Enable colors	Select the check box to display drawn routes in colors, rather than in black.

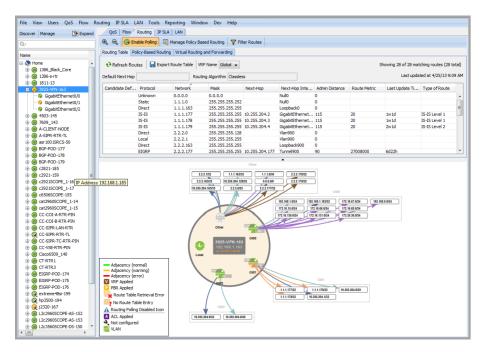
Next-Hop Routing visualization in the system topology view is displayed as a bold, light purple-colored line. If the destination address is not represented in the current set of network devices, as in the example below, a new icon representing the destination device is created.



Routing Device-Level View

The device-level view provides a graphical visualization of routes associated with a specific device. The route paths and the interfaces, which route them are indicated by arrows. The directional arrows are also color coded to indicate whether the route is a static route or derived from a particular routing protocol.

The upper portion of the screen shows the device's route table in tabular format. You can also apply a filter to display routes based on specific protocols and/or destinations.



Note There is no interface-level view on the Routing tab. Clicking on an interface will bring up the device-level view for the router associated with that interface.

Routing Table

In the routing topology home view, click on an individual device and then click on Routing Table in the menu bar within the Routing tab to view the Routing Table specific to that device.

3925-VPN-	163.referen	tia.com ×								
🔁 Refresh Ro Nefault Next Hop		xport Route Table Routing	g Algorithm Class	less			Show	ing 28 of 28 matcl Last update	ning routes (28 to d at 4/25/13 9:0	
Candidate D	Protocol	Network	Mask	Next-Hop	Next-Hop In	Admin Distance	Route Metric	Last Update	Type of Route	
	Unknown	0.0.0.0	0.0.0.0		NullO	0				۰.
	Static	1.1.1.0	255.255.255		NullO	0				Π.
	Direct	1.1.1.163	255.255.255		Loopback0	0				
	IS-IS	1.1.1.177	255.255.255	10.255.204.2	GigabitEthern	115	20	1w1d	IS-IS Level 1	
	IS-IS	1.1.1.178	255.255.255	10.255.204.3	GigabitEthern	115	20	1w1d	IS-IS Level 1	
	IS-IS	1.1.1.179	255.255.255	10.255.204.4	GigabitEthern	115	20	2w1d	IS-IS Level 2	
	Direct	2.2.2.0	255.255.255		Vlan900	0				
	Local	2.2.2.1	255.255.255		Vlan900	0				
	Direct	2.2.2.163	255.255.255		Loopback900	0				
	EIGRP	2.2.2.177	255.255.255	10.255.204.177	Tunnel900	90	27008000	6d22h		
	EIGRP	2.2.2.178	255.255.255	10.255.204.178	Tunnel900	90	27008000	6d22h		
	EIGRP	2.2.2.179	255.255.255	10.255.204.179	Tunnel900	90	27008000	6d22h		
	Direct	10.255.204.0	255.255.255		GigabitEthern	0				
	Local	10.255.204.1	255.255.255		GigabitEthern	0				Ξ
	Direct	10.255.204.8	255.255.255		GigabitEthern	0				
	Local	10.255.204.9	255.255.255		GigabitEthern	0				
	Direct	10.255.204.128	255.255.255		Tunnel900	0				
	Local	10.255.204.163	255.255.255		Tunnel900	0				
	Static	172.16.15.0	255.255.255.0	192.168.1.1		1	0			
	Static	172.16.66.0	255.255.255.0	192.168.1.1		1	0			

Adjacency Table

In the routing topology home view, click on the Adjacency Table in the menu bar within the Routing tab to view all neighbor adjacencies. Tabs are available to see all neighbors or neighbor devices filtered by routing protocol.

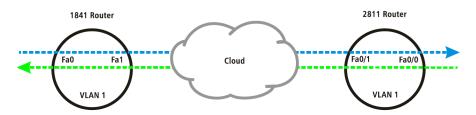
Adjacency Neighbors: All Protocols						
Export						
·		~				
All Neighbors	EIGRP OSP	F IS-	IS			
Device			Interface	Neighbor IP	Protocol	
1386_Black_Core			FastEthernet4	254.128.0.0	EIGRP	
1386_Black_Core				10.54.201.2	OSPF	
CT-RTR3				172.16.13.10	OSPF	
CC-SIPR-RTR-TL				192.168.100.2	OSPF	
CT-RTR1				172.16.13.30	OSPF	
EIGRP-POD-174				10.255.201.10	EIGRP	
EIGRP-POD-174				10.255.201.1	EIGRP	
EIGRP-POD-174				10.255.201.6	EIGRP	
OSPF-POD-171				10.255.202.10	OSPF	
OSPF-POD-171				10.255.202.11	OSPF	
OSPF-POD-171				10.255.202.1	OSPF	
L2c3560SCOPE-DS-1	51			10.0.200.1	EIGRP	
L2c3560SCOPE-DS-1	51			10.0.10.3	EIGRP	
L2c3560SCOPE-DS-1	51			10.0.20.2	EIGRP	
L2c3560SCOPE-DS-1	51			10.0.40.2	EIGRP	
L2c3560SCOPE-DS-1	51			10.0.30.3	EIGRP	
L2c3560SCOPE-DS-1	.50			10.0.20.3	EIGRP	
L2c3560SCOPE-DS-1	.50			10.0.40.3	EIGRP	
L2c3560SCOPE-DS-1	.50			10.0.30.2	EIGRP	
L2c3560SCOPE-DS-1	.50			10.0.100.1	EIGRP	
L2c3560SCOPE-DS-1	.50			10.0.10.2	EIGRP	
1811-13				192.168.1.240	EIGRP	
1811-13				192.168.1.235	EIGRP	
1811-13			EastEthernet1	30.13.17.2	FIGRP	

LiveNX Policy-Based Routing (PBR)

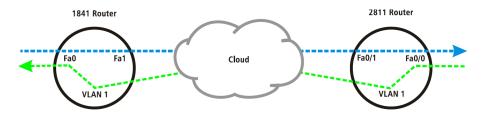
For greater route control, LiveNX Routing allows you to create Policy-Based Routing (PBR) rules and apply these rules to your devices.

What is Policy-Based Routing?

Policy-based routing is used to change the path that a flow with a specific destination address takes out of the router. In the example below, the normal flow of VoIP traffic between the 2811 router and the 1841 router is shown:



In the following example, PBR will be applied to the 2811 router on the Fas0/0 interface, so that traffic flows through the VLAN 1 interface rather than Fa0/1. The flow will also enter the 1841 router from the VLAN 1 interface instead of Fa1. This can be visualized using NetFlow displays for the 2811 and 1841 routers.



Note The policy is applied at the ingress interface of the receiving router.

Policy-Based Routing Monitoring Configuration

LiveNX allows easy monitoring and configuration of routes using visual route mapping. From the Routing menu, select Manage Policy-Based Routing to configure PBR.

PBR Monitoring

For monitoring, the software reads the PBR policies directly from the devices and provides statistics for these policies. You can then use the LiveNX NetFlow module to troubleshoot PBR visually, using a flowbased view of the effects of PBR on application flows coupled with statistics on the PBR policies and underlying ACLs.

PBR Configuration

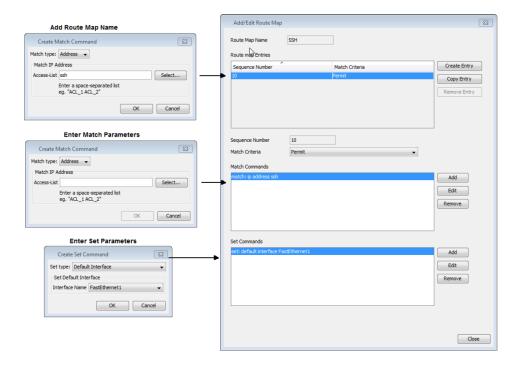
LiveNX also provides a complete PBR configuration solution in conjunction with its built-in ACL editor. Configuring PBR involves creating a route map consisting of a match to identify the incoming packets on a particular interface, and the set actions to perform on these packets.

Click Manage Policy Based Routing to create, edit, and apply PBR on a device.

Manage Policy Based Routir	ng - 4503-145.referentia.com (192.168.1.145)	X
Route Map 💌	Route Map Entries	
SSH	10:Permit match: ip address ssh	Add Route Map
	- set: default interface FastEthernet1	Edit Route Map
		Copy Route Map
		Delete Route Map
		Apply Route Map to Interface
		Remove Route Map from Interface
]
Help	Save to Device	Preview CLI Cancel
	Save to Device	

Creating a Route Map

Click Add Route Map on the Manage Policy Based Routing dialog box to access the route map editor (Add/Edit Route Map). The top portion of the editor shows the series of entries, each entry consisting of match commands and set commands.



Match Commands

The match commands determine how to match the packets, and the set commands determine the actions to be performed. Match commands are typically created using a pre-defined ACL, which can be constructed using the LiveNX ACL editor.

Set Commands

Set commands determine how the packet will be treated once it is identified. PBR provides a rich set of actions to be performed, including altering the default routing behavior and changing ToS values. Multiple set commands can be added to perform multiple actions on the packets.

Preview CLI

Click Preview CLI on the Manage Policy-Based Routing dialog box to view the commands before they are sent to the device.

Manage Policy Base	d Routing - 4503-145.referentia.com (192.168.1.145)	12	Preview CLI	127
Route Map +	Route Map Entries		config t	-
	B 10 Permit	Add Route Map	route map 55H permit 10 match ip address sch set default interface PastEthernet 1	
	- set: default interface FastEthemet1	Edit Route Map	set default interface PastEthernet1	
		Copy Route Map		
		Delete Route Map		
		Apply Route Map to Interface		
		Remove Route Map from Interface		
			,	Core
Help	Save	a Device Preview CL1 Cancel		

Policy-Based Routing Workflow

The following is an example workflow for configuring, monitoring, and adjusting PBR-based actions:

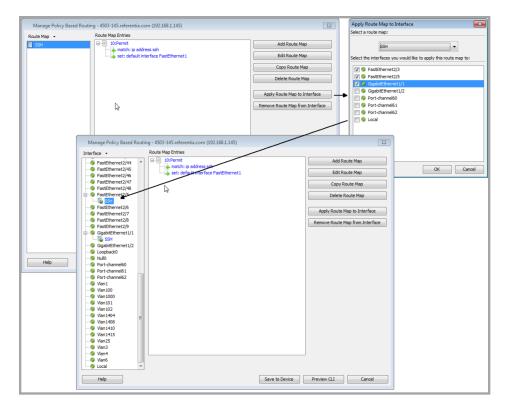
- Create ACL for use with PBR.
- Create PBR to be used.
- Apply PBR to inbound interface.
- Observe PBR and ACL statistics for proper matches.
- Use Flow views to observe flow changes.
- Adjust PBR for proper operation.

	Routing IPSLA Tools Reporting Help	
cover Manage 🕐 Expand	QoS Plaw Routing IP SLA LAN	
ne	R, R, G thable Poling R Manage Policy Based Routing Titler Routes	
Home	Routing Table Policy-Based Routing Virtual Routing and Porwarding	
- 5tandalone 8- 39 1941-WAN-67_113	🔁 Refresh 🛛 🔒 Export Route Map Statistics	
B 3 2921-Deno-67_111	Appled Route Maps	Please Refresh Statut
1 3 2771 0emo-47_112 2: 3 4503-145	Name Packets Evtes Acoled Interfaces	
8 7609_143	Gabitithemeti/2	
C c29215COPE_1-17	Gij Dpemit (refresh) (refresh)	
CM129605COPE_1-14	a match: p address RefrectFlow a set: p next-hop 172.16.1.11	
Cat3560x-67_107		
eat3560x-67_114		
Cacce509_140		
Q Foundry_FW5624-206		
B L3PODc29605C0PE-152		
 E2PODc29605C0PE-153 E2PODc35605C0PE-150 		0.0.2
LIPODe35605COPE-151		(and the second s
R NK05-147		2.0.0.0/8 10.0.0/24 192.0.4.2/32
6 SCOPE_c450357-210		10.0.2.0/24 172.16.255.0/24 192.0.4.0/24
	002	
	Nu0	
	Nuo	
	001 2921-Demo-67 112	172.30.30.0.24 192.168.0
	001 2921-Demo-67_112 172.16.67.112	172.30.30.0.24 192.168.0
	001 2921-Demo-67_112 122.16.67.112 172.16.67.112 172.16.67.112	172.30.30.0.24 192.168.0
	GID1 2921-Demo-67_112 100.4.024 192.0.3.024 192.0.3.024 100.3.102 24 100.5.57.112 Ag 11.005.5574	2
	001 2921-Demo-67_112 122.16.67.112 172.16.67.112 172.16.67.112	172.30.30.0.24 192.168.0
	00-1 100.4.024 1120.3.024 1	2
	00-1 2921-Demo-67_112 10.0.4.024 192.0.3.024 24 192.0.2.024 192.0.2.024 10.0.3.102 24 192.0.2.024 Appendy formal Appendy formal 100.3.102	2
	GD1 2921-Demo-67_112 1 100.4.024 192.0.3.024 1 192.0.2.024 100.3.102 1 192.0.9.024 100.3.102 1 100.4.024 100.3.102 1 100.4.024 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1 0.0.3.102 100.3.102 1	2 Other
	00:1 2921-Demo-67_112 1 100.4.024 192.0.3.024 24 192.0.3.024 10.0.3.102 24 192.0.3.024 10.0.3.102 24 192.0.4.024 10.0.3.102 24 192.0.4.024 10.0.3.102 26 10.0.3.102 10.0.3.102 29 10.0.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.4.024 10.0.3.102 20 10.0.3.102 10.0.010 20 10.0.010 10.0.010 20 10.0.010 10.0.010 20 10.0.010 10.0.010 <	2 Other
	GD-1 2921-Demo-67_112 10.0.4.024 192.0.3.024 24 192.0.2.024 10.0.3.192 10.0.3.192 24 192.0.2.024 10.0.3.192 10.0.3.192 24 192.0.2.024 10.0.3.192 10.0.3.192 26 10.0.3.192 27 10.0.3.192 28 10.0.3.192 29 10.0.3.192 29 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192	2 Other
	00-1 2921-Demo-67_112 172.16.67.112 172.16.75.112 172.15.112 172.112 172.15.112 172	2 Other
	GD-1 2921-Demo-67_112 10.0.4.024 192.0.3.024 24 192.0.2.024 10.0.3.192 10.0.3.192 24 192.0.2.024 10.0.3.192 10.0.3.192 24 192.0.2.024 10.0.3.192 10.0.3.192 26 10.0.3.192 27 10.0.3.192 28 10.0.3.192 29 10.0.3.192 29 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192 20 10.0.3.192	2 Other
	60-1 2921-Demo-67_112 10.0.4.0/24 192.0.3.0/24 24 192.0.2.0/24 10.0.3.1/32 10.0.3.1/32 24 192.0.2.0/24 10.0.3.1/32 10.0.3.1/32 24 192.0.2.0/24 10.0.3.1/32 10.0.3.1/32 26 10.0.3.1/32 27 10.0.3.1/32 28 10.0.3.1/32 29 10.0.3.1/32 29 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 10.0.3.1/32 20 </td <td>2 Other</td>	2 Other

Applying Policy-Based Routing

From the Manage Policy-Based Routing dialog box, click Apply Route Map to Interface to apply policies to multiple interfaces.

To see how the PBR policies are applied to interfaces, change Route Map to Interface in the upper left drop-down list on the Manage Policy-Based Routing dialog box.



Monitoring Policy-Based Routing

The route map statistics shown below will provide the number of packets and bytes that are hitting that particular policy map. These statistics can also be exported to a CSV file for further analysis.

- 1. Select the device or interface to be monitored.
- 2. On the Routing tab, click the Policy-Based Routing tab.
- 3. Click Refresh to update the statistics.
- 4. To save the statistics to a CSV file, click Export Route Map Statistics.

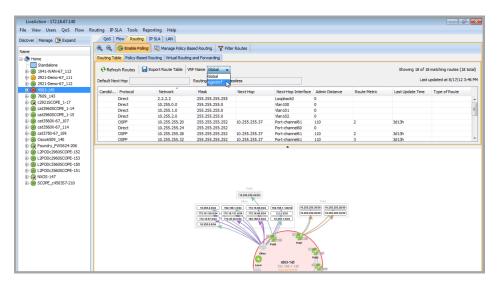
LiveNX Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) refers to a router's capability to store more than one routing table, which separates traffic in each VRF from all other traffic and the Global routing table traffic. Thus, one physical router can serve as multiple routers, with all virtual routers' traffic securely isolated in virtual realms. This feature is only available for Cisco devices. LiveNX allows you to visualize and list VRF routes by network device. Currently, LiveNX does not support PBR with VRF. View VRF data that LiveNX parses in the routing tables by selecting the VRF Name from the drop-down list in the Route Table toolbar. LiveNX automatically detects VRF tables.

Routing Table Policy-Based Routing Virtual Routing and Forwarding						
🔁 Refresh Routes 🛛 🔚 Export Ro						
Default Next Hop Routing mgmtVrf assless						
Candid Protocol Net	twork Mas	sk Next-	Нор			

Note Select Global to display the non-VRF, "normal" routing table; and the visualization of the device, its interfaces, and their associated routes.

Select a VRF route table from the drop-down list on the Routing > Route Table tab in the device view. In this example, there is one mgmtVrf (VRF) tables and one Global (normal) table. LiveNX will display the selected routing table in the top pane, and a graphical route map in the bottom pane.



CHAPTER 10

IP SLA

In this chapter:

IP SLA Overview	210
Advanced Test Scheduling	219

IP SLA Overview

LiveNX IP SLA is a technology module that makes Cisco IOS IP Service Level Agreement (SLA) operations easily accessible for generating synthetic network traffic to monitor latency, loss, jitter, and MOS (for VoIP).

LiveNX SLA is part of the LiveNX software framework that enables network engineers at all experience levels to perform advanced Cisco device operations quickly and easily on live networks. Its highly interactive graphical interface delivers the full functionality and flexibility of the device features without the need to learn and use Cisco device command lines.

About Cisco IOS IP SLA

Cisco IOS IP SLA is a capability embedded in most devices that run Cisco IOS software. Its service-level assurance metrics and methodology allows you to increase network reliability by verifying service guarantees with precise service-level assurance measurements. IP SLA can validate network performance, proactively identify network issues, and simplify the deployment of new IP services.

Cisco IOS IP SLAs generate synthetic test traffic in a continuous, reliable, and predictable manner to enable accurate measurement of network performance. This traffic can be sent across the network to measure performance among multiple network locations or across multiple network paths. IP SLA uses timestamp information to facilitate the calculation of performance metrics such as jitter, latency, network and server response times, packet loss, and Mean Opinion Score (MOS).

Key Features and Benefits

Ease of Use

LiveNX makes Cisco IP SLA easy to use. An intuitive graphical interface replaces complicated command lines, making on-the-fly test configuration and execution easy and understandable.

Improved Efficiency

Reduces time required for network deployment, maintenance, and training, while improving network availability.

Built-In IP SLA Expertise

LiveNX IP SLA is based on Cisco best practices and an extensive knowledge base of Cisco IP SLA features and functions.

Rich Visualizations

LiveNX provides graphical views of latency, loss, jitter, and MOS over IP SLA. It also displays real-time topological views and test status, as well as test results plotted historically on a timeline.

Test Traffic Generation

Generates and sends synthetic test traffic from the router for measuring network performance. Enables detailed editing of test configurations to simulate complex traffic patterns.

Interactive

Start, stop, and edit traffic tests in real time.

Non-Disruptive

LiveNX IP SLA is a software-based solution that requires no physical topology changes or service interruptions to install.

Exceptional ROI

LiveNX QoS takes full advantage of existing Cisco device features, significantly reducing the need to purchase separate test networks and hardware-based test equipment, including traffic generators, far end-point probes, and analyzers.

Getting Started with LiveNX IP SLA

IP SLA Compatible Devices

The LiveNX IP SLA feature is capable of supporting Cisco devices that are IP SLA-enabled. The following is a list of Cisco devices that support IP SLA. A voice image is required for some platforms.

- Cisco 12000 Series Internet Routers
- Cisco 7500 Series Routers
- Cisco 7200 Series Routers
- Cisco 7000 Series Routers
- Cisco 6400 Series Broadband Aggregators
- Cisco 3900 Series Integrated Services Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3600 Series Multiservice Platforms
- Cisco 3200 Series Mobile Access Routers
- Cisco 2900 Series Integrated Services Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 2600 Series Multiservice Platforms
- Cisco 2500 Series Routers
- Cisco 2000 Series Routers
- Cisco MWR 1900 Series Mobile Access Routers
- Cisco 1900 Series Integrated Services Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 1700 Series Access Routers
- Cisco 1600 Series Routers
- Cisco 1400 Series Routers
- Cisco 1000 Series Routers
- Cisco 800 Series Routers
- Cisco Catalyst 6500 Series Switches
- Cisco Catalyst 6000 Series Switches Module Switch Feature Card (MSFC)
- Cisco Catalyst 6000 Series Switches (running IOS)
- Cisco Catalyst 5000 Series Switches Router Switch Module (RSM)
- Cisco Catalyst 5000 Series Switches Router Switch Feature Card (RSFC)
- Cisco Catalyst 4200 Series Switches
- Cisco Catalyst 4000 Series Switches (running IOS)

- Cisco Catalyst 3750 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3500 Series Switches
- Cisco Catalyst 2900 Series Switches

Cisco IOS and Catalyst Operating System Version IP SLA Support

IOS Routers

• IP SLA is available on all routing platforms, from the 800 series up to the 12000 series.

Catalyst Switches

- IP SLA is available for 2900, 3500, 3700, 4000 (SUP4), and 6000 (MSFC or MWAM) series Catalyst switches.
- IP SLA is included in the IP feature set from 11.3 up to 12.2 and above.
- The IP voice or upper feature set is required, starting with IOS release 12.3T and all of 12.4 and above.

Network Device Considerations

For accurate time measurements, network devices must be synchronized with a common reference clock. This can be accomplished by using Network Time Protocol (NTP) synchronization with an NTP server, or by assigning one network device to function as a time master server.

The accuracy of one key latency metric that is directly linked to NTP is the LiveNX UDP, jitter, one-way delay test operation. This IP SLA operation can test and report the one-way delay for both the outbound and return paths between two points on the network. Here, the data returned by IP SLAs will depend directly on the engineering design, deployment, and accuracy of NTP in your networks.

CPU Usage

Normal scheduling of IP SLA allows for one operation at a time. If no start time is specified, the operation starts immediately. This is not a problem if a single operation is defined and activated manually by an operator using the CLI. The situation changes with LiveNX if multiple operations are defined without specific start times and the network device reboots.

For example, if 1,000 operations were defined for one device without staggered start times and a reboot occurs, all of these operations would start instantly and simultaneously. This would result in a CPU spike at the device and potentially a sudden burst of IP SLA test traffic in the network. Either of these effects can have a negative impact on network efficiency and measurement accuracy.

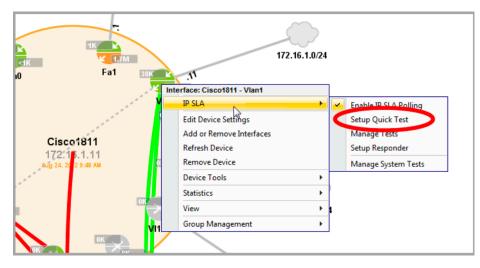
Configuring LiveNX IP SLA

Below are examples of some generalized performance metrics recommended by Cisco for various types of traffic:

Application or Traffic Type	Maximum Packet Loss	Maximum One-Way Latency	Maximum Jitter
Voice over IP	1%	120 ms	30 ms
Videoconferencing (two-way)	1%	200 ms	50 ms
Streaming (one-way) Video	2%	5 seconds	N/A

Setup Quick Test Wizard

Network verification and testing can be set up quickly using the LiveNX IP SLA Setup Quick Test wizard. The quick test can be invoked by clicking the Quick Test or right clicking on the particular interface you want to generate the IPSLA test stream from.



The following example goes through setting up a test to measure jitter, latency, and loss between two routers.

1. In the IP SLA tab toolbar, click Setup Quick Test to display the Setup Quick Test dialog box. If the Log In Required window appears, you must log in with Admin or Full Config credentials.

Setup Quick Test	×
Device 1941-WAN-67_113	•
Entry ID	1
Test type	Path Echo 👻
Tag (Optional)	Path Echo Test 123
Source address	FastEthernet0/1/0 (172.16.67.113)
Destination address*	10.0.2.1
(IP or host name)	Click on an interface to select its IP address.
Frequency 60	seconds
	Save to Device Cancel

2. Select the source router or switch from the Device drop-down list of available devices.

The Entry ID number is filled in automatically. This is a unique number that identifies the test in the Cisco router.

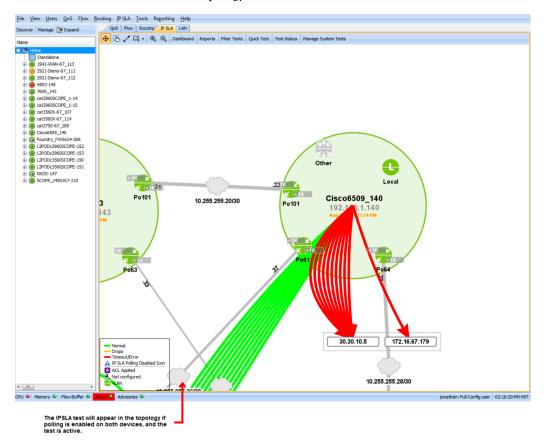
3. Select Test type. Options are DHCP, DNS, ICMP Echo, FTP, HTTP, Jitter, Video, UDP Echo, Path Jitter, and Path Echo.

"Echo" refers to the receiving router sending back the data unchanged to the sending router, and "jitter" indicates variations in delay times between multiple UDP Echo packets. "Path" refers to the display of the path the test traffic will take through the network.

Path Echo and Path Jitter tests measure the time between sending and receiving acknowledgment of user Datagram Protocol (UDP) Echo (port 7) packets. This is useful in determining round-trip delay for programs using UDP to communicate over the network.

Video is a new test function also known as Medianet IPSLA Video Operation. This test type is capable of generating synthetic Telepresence, IPTV and IP video surveillance traffic.

- 4. Enter the optional Tag value to use as the name, label, or description of the test.
- **5.** Select the Source address from the dropdown list of interfaces. All existing interfaces for the device should be listed.
- 6. Select the Destination address (IP address or hostname) by clicking on the desired destination device interface in the IP SLA topology view.



 Enable IP SLA polling for both devices by going to File > Mange Devices. Select the appropriate check boxes in the Poll and IPSLA column. Polling must be enabled before IP SLA test results will appear.

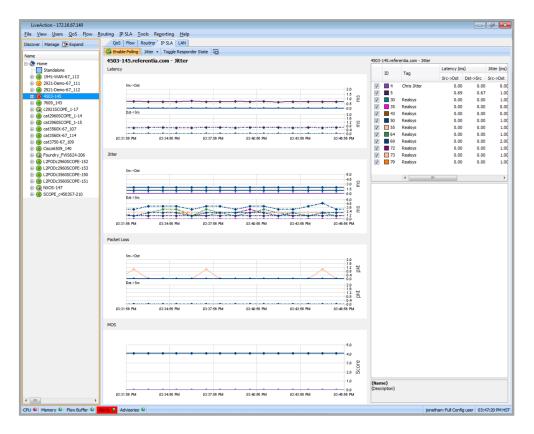
d Device cover Devices	Filte	r by:					Filter		Clear]				
nage Devices	Select	Device Name	IP Address	Vendor	Model	Group	Pol	Q05	Flow	JP SLA	Routing	LAN*	Interval	Status
resh Devices	13	1941-WAN-67_113.referen	172.16.67.113	Cisco	cisco 1941		[9]		1	1		23	30 seco	Configured
nove Network Objects	12	2921-Demo-67_111.referen	172.16.67.111	Cisco	cisco2921			1	1	1	1	83	30 seco	Configured
and a superior	10	2921-Demo-67_112.referen	172.16.67.112	Cisco	cisco2921		(9)	1		4	1	V	10 seco •	Configured
	10	4503-145.referentia.com	192.168.1.145	Cisco	cat4503		197	120	197	192	12	121	30 seco 👻	Configured
	10	7609_143.referentia.com	192.168.1.143	Cisco	asco7606		1		1	N/A			30 seco	Configured
	10	c2921SCOPE_1-17.referent	192.168.1.17	Cisco	disco2921		1	V	1	1		1	30 seco •	Configured
	10	cat29605COPE_1-14	192.168.1.14	Cisco	catalyst296024TT				23	1		23	30 seco	Configured
	10	cat2960SCOPE_1-15	192.168.1.15	Cisco	catalyst296024TT		(9)		10			23	30 seco	Configured
	10	cat3560X-67_107	172.16.67.107	Cisco	cat3560x24		(12)		(1)				30 seco	Configured
	13	cat3560X-67_114.referenti	172.16.67.114	Cisco	cat3560x24		17	1		1		1	30 seco	Configured
	10	cat3750-67_109.referentia	172.16.67.109	Cisco	catalyst37kxStack		12	4		19		12	30 seco	Configured
	10	Cisco6509_140.referentia.c	192.168.1.140	Cisco	cat6506		1	1	12	12			30 seco	Configured
	10	Foundry FWS624-206	192.168.1.206	Unknown	Unknown		1	121	1	1	13	171	30 seco 👻	Not Config
	10	L2PODc2960SCOPE-152.ref	192.168.1.152	Cisco	catalyst29608TCS		N.	1		N/A			30 seco 👻	Configured
	10	L2PODc2960SCOPE-153.ref	192.168.1.153	Cisco	catalyst29608TCS			1	5	N/A			30 seco	Configured
	10	L2PODc3560SCOPE-150.ref	192.168.1.150	Cisco	Unknown		(V)		1	1			30 seco	Configured
	10	L2PODc35605COPE-151.ref	192.168.1.151	Cisco	Unknown		(2)	12		1			30 seco	
	10	NXOS-147	192.168.1.147	Cisco	Unknown		1		1			12	30 seco	Not Config
	15	SCOPE_c450357-210.refer	192.168.1.210	Cisco	catalyst4503e		193	19				[7]	30 seco +	
	*LAN pr	olling occurs every 15 minutes												
	Device	Configurations					Global Device S	ettings						
			re QoS, Flow,				Edit	Defa	uit SNMP S	ettings				Clear
		Remove S	Select devices in the table and click the configure button. Remove Selected Device(s).				Edit Default CLI Monitoring Settings - Not Set					Set		Clear
	Nut	Number of Devices: 19					Edit Default CLI Configuration Settings							Clear

- 8. To monitor this test, click Show Test Status in the IP SLA tab toolbar. This will bring up the Test Status window that will show you statistics for latency, jitter, and loss.
 - The test will run continuously by default until ended.
 - Statistics will take one polling interval (default is 60 seconds) to refresh.

QoS Flow Routing	IP SLA LAN				
🕂 🚯 🖊 📭 • 🔍	R Dashboard	Reports Filter Tests	Quick Test	Test Status	Manage System Tests

Curre	nt 🔘 /	Averages	Run Tests 🔹	 Stop 	p Tests	 Mar 	nage To	ests Expo	t		Q. Type here to fi	lter tests
All te	ests D	HCP DNS	ICMP Echo	FTP H	ПТР	Jitter	Video	UDP Echo	Path Jitter	Path Echo	2	
			-	Prope	erties							
tatus	us ID Group ID Type		Tag	Tag Device Destination/URL							Attempts	
	1	3	2 DNS	Refer	entia Di	NS Serve	er 2	cat3560	(-67_107	mai	il.google.com	60
	14	1	2 DNS	Refer	entia Di	NS Serve	er 2	cat3560	(-67_107	mai	il.google.com	60
	1	5	Video					cat3560	(-67_107	10.	37.2.1	0
	16	5	Video	ChrisS	SysTest	Vid		cat3560	(-67_107	172	2.16.67.114	0
		1	Video	Chris\	/idTest			cat3750	67_109	172	2.16.67.114	0
	36	5	2 DNS	Refer	entia Di	NS Serve	er 1	cat3750	67_109	mai	il.google.com	60
0	3	7	Video	Chris	Video fr	om 109		cat3750	67_109	192	2.0.2.25	56,085
	38	3	2 DNS	Refer	entia Di	NS Serve	er 1	cat3750	67_109	mai	il.google.com	60
	39	9	2 DNS	Refer	entia Di	NS Serve	er 1	cat3750	67_109	mai	il.google.com	60
	4)	2 DNS	Refer	entia Di	NS Serve	er 1	cat3750	67_109	mai	il.google.com	60
	4	1	2 DNS	Refer	entia Di	NS Serve	er 1	cat3750-	67_109	mai	il.google.com	60
	1	1	Jitter					4503-14	5	192	2.168.1.143	0
	:	2	ICMP Echo					4503-14	5	192	2.168.1.143	0
	1	3	DHCP					4503-14	5	10.	102.102.1	0
0		1	Jitter	Chris	Jitter			4503-14	5	10.	10.0.1	35,731
6	1	5	Jitter					4503-14	5	192	2.168.1.145	35,731
6		5	1 DNS	DNS S	erver 1			4503-14	5	mai	il.google.com	2,383
0	1	7	1 DNS	DNS S	erver 1	L		4503-14	5	mai	il.google.com	2,383
0	8	3	1 DNS	DNS S	erver 1			4503-14	5	mai	il.google.com	2,382
6	9	9	1 DNS	DNS S	erver 1			4503-14	5	mai	il.google.com	2,382
0	10)	1 DNS	DNS S	erver 1	L		4503-14	5	mai	il.google.com	2,382
6	1	1	2 DNS	DNS S	erver 2	2		4503-14	5	mai	il.google.com	2,383
0	1	2	2 DNS	DNS S	erver 2	2		4503-14	5	mai	il.google.com	2,383
0	1	3	2 DNS	DNS S	erver 2	2		4503-14	5	mai	il.google.com	2,382
6	14	4	2 DNS	DNS S	erver 2	2		4503-14	5	mai	il.google.com	2,382
6	1	5	2 DNS	DNS S	erver 2	2		4503-14	5	mai	il.google.com	2,382
	16	5	3 Jitter	Reals	ys			4503-14	5	192	2.168.1.33	600
	1	7	3 Jitter	Reals	ys			4503-14	5	192	2.168.1.33	600
	18	3	3 Jitter	Reals	ys			4503-14	5	192	2.168.1.35	600
	19	9	3 Jitter	Reals	vs			4503-14	5	192	2.168.1.35	600

Additional detailed test information can be accessed by clicking on the originating router while in the IP SLA view. This displays a set of graph for Latency, Jitter, Packet Loss and MOS scores as shown below.



9. By selecting the viewing mode, various different sets of graphs can be shown that are appropriate for the test being run.

🚼 LiveAction - 172.16.67.140	StiveAction - 172.16.67.140								
<u>File View Users QoS Flow Routing IP SLA Tools Reporting Help</u>									
Discover Manage Expand QoS Flow Routing IP SLA LAN									
Name	🛞 Enable Polling	Jitter 👻 Toggle Re	esponder State						
- A Home	4503-145.refe	Jitter	ter						
Standalone	Latency	Video							
🗄 🛞 1941-WAN-67_113		Other							
🕀 🛞 2921-Demo-67_111	Src->Dst								
⊕ 🛞 2921-Demo-67_112									
# 4503-145									

10. The IP address in the Destination/URL field can be changed to a user-defined value by the Edit IP Mapping feature.

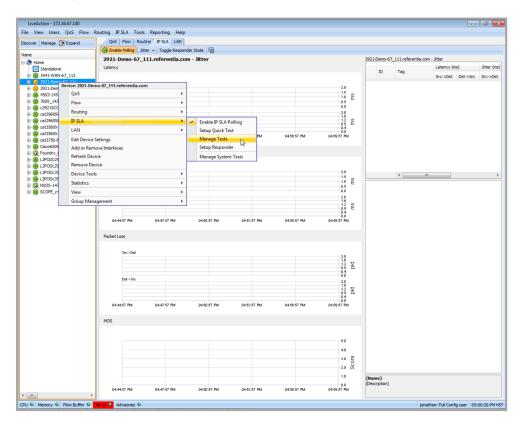
Curre	nt 🔘 A	verages 🕘	Run Tests 👻	Stop Tests • Manage	ge Tests Export	Q+1	ype here to filter tests	
All te	ests Di	HCP DNS	ICMP Echo	FTP HTTP Jitter Vie	deo UDP Echo Path Jitter P	ath Echo		
Status	ID	Group ID	Tune	Properties			Attempts	Error
Status	10	Group ID	Туре	Tag	Device	Destination/URL	Attempts	crior
•	2		Path Echo	2	SCOPE_c4503S7-210	192.168.1.33	365 5	luccess
6	4	-	ICMP Echo		SCOPE_c4503S7-210	192.168.1.179	367 5	Success
6	5		Video	DELETE-ME	SCOPE_c4503S7-210	172.16.67.109	365 5	Success
6	71		Jitter	test 71	SCOPE_c4503S7-210	192.168.1.33	365 5	Success
6	1		ICMP Echo		asr1001_SRCS_1-50		10,1441	imeout
	2		HTTP		asr1001 SRCS 1-50		10.100	ons Ouerv E

11. By selecting Tools > Edit IP Mappings described in *IP Mapping* on page 241, select Add and then type in a user-defined Name and the desired IP Address. The new user-defined value is displayed in the Destination/URL field.

		A	Dur Taala	0.00.7		· · · · · · · · · · · · · · · · · · ·	at English				0	and a filler to	1	
 Curre 		Averages G	Run Tests 🔻	Stop I	ests 🔹 I	Manage Te	sts Expor	t			Q+ Type n	ere to filter te	STS	
All te	ests 🛛	OHCP DNS	ICMP Echo	FTP HTT	P Jitter	Video	UDP Echo	Path Jitter	Path Echo					
Chathar		Course TD	Ture	Propert	es								Error	
Status	ID	Group ID	Туре	Tag			Device	Device		Destination/URL		Attempts	Error	
•		2	Path Echo	2			SCOPE_C	4503\$7-210	Lab			36	7 Success	
9		4	ICMP Echo				SCOPE_C	450357-210	192	168.1.179		36	9 Success	
9		5	Video	DELETE-	ИE		SCOPE_C	4503\$7-210	172	16.67.109		36	7 Success	
6	7	1	Jitter	test 71			SCOPE_c	4503\$7-210	Lab			36	7 Success	
•		1	ICMP Echo				asr 1001_	SRCS_1-50				10,14	6 Timeout	
		2	HTTP				acr 100 1	SRCS 1-50				10.15	1 Dns Ouerv E	

Managing Tests

For extended test coverage and scheduling capability, access configuration options from the IP SLA menu, or right-click on the network device from which the test will be started.



The manage test window allows you to create, delete, copy and group tests. The main window is shown below.

Manage Tests - c18	811-13.referentia.com (192.168.1.1	13)
	ove Test 🛯 📋 Copy Test 👇 Add	i Group 🔲 Remove Group 🕘 Schedule Now 🕘 Remove Schedule
ID A 1	Start Time Type	Entry ID 2 Entry type Jitter
-36	ICMP Echo ICMP Echo ICMP Echo	Owner
38 39 40	ICMP Echo ICMP Echo ICMP Echo	
41	HTTP	Destination address*
42	HTTP HTTP	172.16.17.1
-44	HTTP	Destination port*
-45	HTTP	5000
-46	HTTP	Source address
-47	HTTP	172.16.18.2
-48	HTTP	Codec
49	HTTP HTTP	Codec type G729A 🗸
	now HTTP now HTTP	Advantage factor 0 (0-20) Number of packets 1,000 (1-60,000 packets) Number of bytes 32 (16-1,500 bytes)
⊟- 1 51	now ICMP Echo	
□ - 1 -52 -53	now Jitter Jitter	E Start Time now
⊡- ¶28 54	now HTTP	Life Forever (1-2,147,483,647 seconds)
E Tests	Jitter	Age Out (1-2,073,600 seconds. Blank for indefinite)
2	now Jitter	Recurring (1)
3	now Jitter now Jitter	
-5	now ICMP Echo	Advanced Mode
Help		Save to Device Preview CLI Close

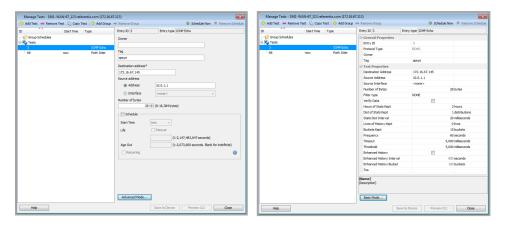
Adding a new test is done by clicking Add Test, which brings up a dialog with basic test parameters.

	Manage Tests - 4503-1	45.referentia.com (192.168.1.145)	
Add new IP SLA test		Test 🗓 Copy Test 🕴 Add Group - Remove Group 🕘 Schedule Now 🔍 Remove Schedule	
	ID A 1	Start Time Tune Fotry ID 6 Fotry tune DNS	
	🖃 🎲 Group Schedules	New IP SLA - 4503-145	Parameter selection will
	□ - 1 6	Entry ID 84 Test type DHCP	 vary depending on type of test selected
	7	Owner	lest selected
	-8	Tag	
	9		
		DHCP	
	🖻 🖅 2	Destination address*	
	-11 -12		
	-13	Source address	
	14	Circuit ID (Hexadecimal)	
		Remote ID (Hexadecimal)	
	🖻 - 🌠 3	Subnet mask 255 . 255 . 0	
	-17		
	19		
	20	rds)	
	21	Blank for indefinite)	
	22	0	
	23		
	24 25		
	26		
	27		
	28		
	29		
	31		
	-33	OK Cancel	
	34		
		Tilos	
	Help	Save to Device Preview CLI Close	

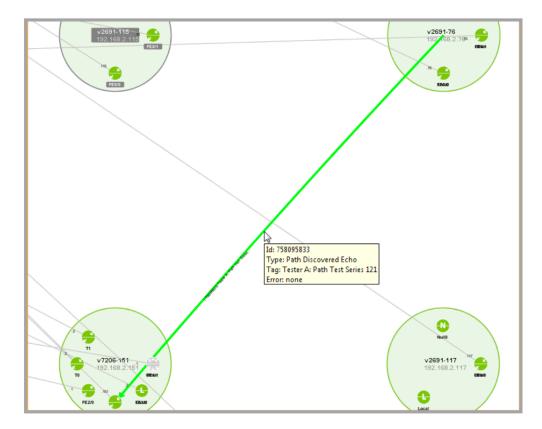
Once a test is created, it can be edited using either the basic or advanced mode. Click Basic Mode or Advanced Mode to toggle between basic and advanced configuration modes. Parameters edited in one mode will persist in the other mode; validation is also enforced in both modes. In Basic Mode, required fields are denoted with an asterisk (*).

Save to Device and Preview CLI are enabled when changes have been made and all changes are valid. View Errors will be enabled if there are any validation errors. Click View Errors to display a list of all errors.

Refer to the Cisco reference manual for descriptions of all Path Echo configuration parameters.



In the system topology view, Path Echo test results are displayed in visual form, delivering rich context for instant understanding. Colored icons indicate operating success or failure status quickly and easily for each test.



Advanced Test Scheduling

Advanced Test Scheduling

Scheduling had been enhanced, allowing you to better control when tests are run:

Manage T	ests - c1811-13.referentia.com (19	2.168.1.13)		
	💻 Remove Test 🛛 📗 Copy Test	🕂 Add Group 🔹	Remove Group	Schedule Now O Remove Schedule
ID	Start Time Typ	e	Entry ID 1	Entry type Group Schedule
🖶 🕼 Group S	chedules		Group Schedule	0
= 🔂 1	now			
6		ICMP Echo	Schedule Period*	60 (1-604,800 seconds)
-7		ICMP Echo	Frequency	Range
□ • 1 1 2 1 1 1 1 1 1 1 1 1 1		нттр		
	now	ппе		60 - (1-604,800 seconds)
	now		Start Time	now 👻
12	1011	HTTP		
🖨 🔂 5	now		Life	Forever
17		HTTP		(1-2,147,483,647 seconds)
6 👘 📄	now			(1-2,147,403,647 seconds)
51		ICMP Echo	Age Out	(1-2,073,600 seconds. Blank for indefinite)
🖹 🖻 🐨 🔂 7	now			
52		Jitter	* Required Field	
53		Jitter		
E Tests		Jitter		
-2	now	Jitter		
-3	now	Jitter		
4	now	Jitter		
5	now	ICMP Echo		
			Advanced Mode	
Help				Save to Device Preview CLI Close

Start time – you can now configure tests to run now, on a specified date, at a specified time, or after a specified period of time elapses.

Frequency - the amount of time after which each IP SLA operation is restarted.

Life – the amount of time the test actively collects information. You can configure tests to run forever, or for a specified duration

Age Out – the amount of time to keep the test in memory when it is not actively collecting information. You can set data to expire after a specified time.

Test Groups

Groups are now available to help you schedule multiple tests quickly and easily. Click the Add Group button to create a new group. The New Group dialog will appear, allowing you to configure the group's schedule. After creating the group, you can edit the configuration by selecting the group in the tree view. The group's schedule configuration will appear in the right-hand section of the dialog. Click the Add Test button to add a new test to the selected group, or drag-and-drop existing tests into the group. Click the Remove Schedule button (or right-click a group and select Remove Schedule) to prevent the group's tests from running. Click the Remove Group button (or right-click a group and select Remove Group) to remove the group. Any tests in the removed group will still be available under the Tests item in the tree view.

IP SLA System Tests

The IP SLA System Test feature allows you to quickly setup multiple IP SLA tests on systems of devices. You can use this feature to test remote office connections, cloud-based service connections, or any other scenario where you want to manage multiple IP SLA tests.

Note IP SLA System Tests are a collection of individual tests defined and managed by LiveNX—the routers running the tests are not aware of the tests running on other devices.

Name	Туре	Description
Application: HTTP	Applications	Hub and Spoke, Hub to Spoke;
realtime: telepresence	Realtime Services	Hub and Spoke, Bi-directional; 3
realtime: jitter	Realtime Services	Hub and Spoke, Bi-directional; 2

Managing IP SLA System Tests

The "IP SLA System Tests" dialog is used to manage the IP SLA system tests—adding, removing, editing and copying tests can be performed in this dialog. The IP SLA System Tests dialog can be accessed from the following places using the "Manage IP SLA System Tests" menu item:

The IP SLA main menu

Device right-click pop-up menu in the IP SLA system topology view

The IP SLA submenu in the device tree right-click pop-up menu

The IP SLA system topology view toolbar

Add Test

The "Add Test" button starts the "IP SLA System Test Creation" wizard.

IP SLA System Test Creation	Wizard	×
Steps	Select System Test Type	
1. Select System Test Type	Select the type of system test to create:	
2. System Test Name	Realtime Services	-
3. Select IP SLA Test Types	Realtime Services Applications	
4. Select Network Topology	Applications	
5. Select Test Source and Destinations		
6. Schedule the System Test		
 Confirm System Test Settings 		
8. Configuration Results		
	< Back Dext > Einish Can	cel

Select System Test Type

Two types of IP SLA system tests can be set up: Real-time Services and Applications. Each type of system test provides different options for the types of IP SLA tests that can be run and the network topologies that can be used.

System Test Name

Step 2 allows you to specify a name for the IP SLA system test. When individual IP SLA tests are configured on the devices, this name will also be used in the IP SLA test tag field.

Select IP SLA Test Types

Different system tests allow for different IP SLA test types. For each test type, a specified number of test instances can be set up. All test instances will use the same settings with the exception of tests that use port numbers. For those tests, an attempt can be made to use unique port numbers for each test instance. LiveNX will attempt to use select ports from the range defined in this step—the default port range is 5000 to 50000. The wizard will attempt to detect already used ports by looking at all of the other IP SLA tests configured on the devices. The wizard is not currently capable of detecting ports used by the devices that are not specified in configured IP SLA tests, such as a device Web server.

Real-time Services Test

- Jitter
- Video

Applications Test

- DHCP
- DNS

- ICMP Echo
- FTP
- HTTP

Select Network Topology

This step allows you to select the network topology used in the tests.

Mesh: All connections are bidirectional between devices

Hub and Spoke: Options to use bidirectional, hub to spoke, and spoke to hub connections

With application system tests, only "Hub and Spoke" with hub to spoke connections is available.

Select Test Source and Destinations

Depending on the system test type and topology, different device selection options will be available:

Real-time Services with Mesh Topology: Selection of all devices to be used in the test

Real-time Services with Hub and Spoke Topology: Selection of a single hub device and one or more spoke devices

Application (only Hub and Spoke are supported): Selection of one or more hub devices. The spokes are determined by the destinations specified when the IP SLA test types are selected.

Note All IP SLA capable devices specified as destinations for the real-time tests will be set up as an IP SLA responder and that setting will not be removed when the IP SLA system test is removed.

Schedule the System Test

This step allows you to schedule when IP SLA system tests will run. The following options can be configured:

Start Time – you can now configure tests to run now, on a specified date, at a specified time, or after a specified period of time elapses.

Frequency - the amount of time after which each IP SLA operation is restarted.

Life – the amount of time the test actively collects information. You can configure tests to run non-stop, or for a specified duration.

Age Out – the amount of time to keep the test in memory when it is not actively collecting information. You can set data to expire after a specified time.

IP SLA System Tests do not support the frequency range setting, because the same settings should be used for all devices participating in the IP SLA system tests and some older devices/IOSs do not support the frequency setting.

Confirm System Test Settings

On this step, the device configs are reloaded so LiveNX can determine how the IP SLA tests should be configured on the devices. A summary of the IP SLA system test settings is shown, including which port numbers will be used.

- Clicking the Preview CLI button displays commands that will be sent to the devices to configure the IP SLA system tests.
- Clicking the View Errors button will show any errors that occurred while loading a device config.
- Real-time services tests, the Fine Tune button allows you to manually override port number values.

Configuration Results

This step shows a list of devices that are part of the IP SLA system test. Successfully configured devices will have a green icon next to them and red icons will appear next to devices where a configuration problem occurred.

The View Errors button is used to view the errors that occurred. After clicking Finish, the IP SLA system test is saved in the application.

Remove Test

Clicking the Remove Test button displays the Remove IP SLA System Test dialog. When the dialog box opens, the config models of all of the devices will be reloaded to confirm which commands need to be sent to the devices. A gray icon indicates a successful read. A red icon indicates an error.

Clicking the Preview CLI button displays the commands that will be used to remove the system tests. When reading the config models, a gray icon indicates a successful read and red indicates an error. Any errors that occur can be viewed using the View Errors button.

Clicking the OK button removes the IP SLA tests from the devices. If any configuration errors occur when removing tests, they will appear in a new dialog box. The Cancel button cancels the removal and closes the dialog box.

Note Multiple tests can be selected for removal.

Edit Test

Clicking the Edit Test button opens the wizard and allows you to edit the system test.

Note When editing a test, the test type cannot be changed.

Copy Test

Clicking Copy Test opens the IP SLA System Test Creation Wizard pre-populated with the settings of the selected test. The name of the test copy is automatically modified to avoid conflicts with the original.

CHAPTER 11

LAN

In this chapter:

LAN Overview	226
Spanning Tree Highlighting Through a Network	233

LAN Overview

LiveNX LAN is a technology module that provides real-time layer 2 visualizations for networks, including trunk interfaces, port channels, VLAN associations, spanning tree connections, and bandwidth percentages.

Key Features and Benefits

Network Visualization

- VLAN trunk, port channel names
- VLAN associations within a device
- VLAN highlighting through a network
- Input/Output bandwidth of each VLAN switch virtual interface and trunk port
- Spanning tree root bridges Spanning tree forwarding, listening/learning, and blocking connections
- Find IP/MAC

Real-Time Monitoring

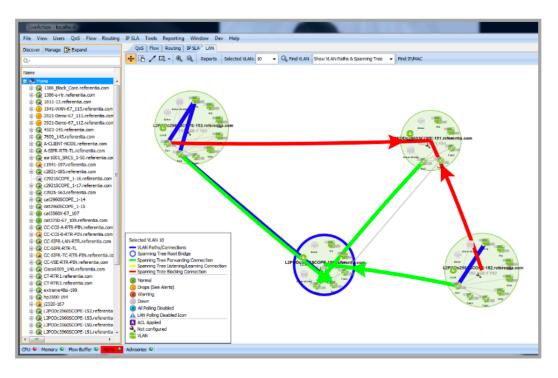
- Trunk and access bandwidth information through network polling
- Layer 2 QoS statistics including CoS, DSCP, and IP precedence
- Dropped packets, interface and spanning tree topology change warnings through network polling at the VLAN level

Getting Started With LiveNX LAN

The setup is the same as the other LiveNX technologies.

Network Visualization

The following image is a representative sample of devices and the additional trunks, port channels, spanning tree bridge, spanning tree connections and VLANs visible with the LAN technology in the System View.



LAN related icons visible in the System View of every technology tab are listed below:

10.3.2 Trunk Port	 The icon with the "T" signifies a Trunk Port on a device. In this example, the name of the interface is Port-channel 4 (Po4). A dashed line indicates which VLANs the port is trunking. Note that these dashed lines are only shown on the LAN tab since there could be many of these lines which adds additional overhead in rendering. A solid line indicates that a port is connected to another port or trunk port. The width of the solid lines indicate the relative bandwidth of the link; the wider the line, the larger the bandwidth of that link. Other interfaces may be labeled as Fa (Fast Ethernet) or Gi (Gigabit Ethernet). As with other LiveNX technologies, real-time input bandwidth is shown in the top half and real-time output bandwidth is shown in the bottom half. Tool tips (rolling over icon) provide additional information: Name, IP address, Type, Descr., Input Policy, Output Policy, Input ACL, Output ACL.
10.3.3 VLAN Switch Virtual Interface	 The round icon with the VI designation signifies a VLAN switch virtual interface (SVI) with an IP address. In this example, the name of the interface is VI201 (VLAN interface 201). Dashed lines (LAN tab only) describe associations between the particular VLAN and its trunk port. As with other LiveNX technologies, real-time input bandwidth is shown in the top half and real-time output bandwidth is shown in the bottom half. Tool tips (rolling over the icon) provide additional information: Name, VLAN Name, IP address, Type, Description, Input Policy, Output Policy, Input ACL, Output ACL, Input BW, Output BW.
10.3.4 VLAN	 The square icon signifies a non-SVI VLAN on a device. In this example, the name of the VLAN is VI101 (VLAN interface 101). Dashed lines (LAN tab only) describe associations between the particular VLAN and its trunk port.Tool tips (rolling over icon) provide additional information: Name, VLAN Name, Type, Description, Input BW and Output BW.
10.3.5 VLAN (no access ports)	The square icon with dashes instead of displayed BW values signifies VLANs with no access ports.
10.3.6 Other VLANs Other VLANs	This gray square icon signifies all remaining (those not selected in the device wizard) non-SVI VLANs over the up to 25 VLANs selected for display in the device wizard.

VLAN List in the System Hierarchy View

Only SVI VLANs are visible individually in the System Hierarchy view. All selected non-SVI VLANs (i.e. VLANs selected in the device wizard) are aggregated into a node named "VLANs." Click on the + sign to the left of the device name to expand the interface and VLAN names. Roll over the VLAN name to display tooltips describing details about the VLAN. Similar to interfaces, VLAN congestion indicators will display in both the topology view and in the system hierarchy view, and represent the congestion state of all the represented VLANs.

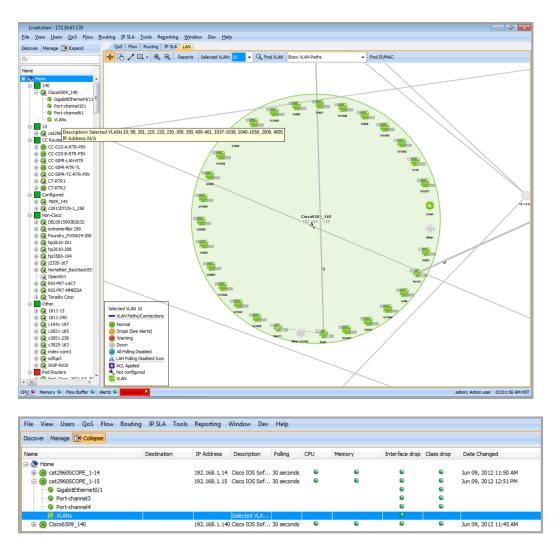


Fig. 10-2: Expanded System Hierarchy View with VLANs

VLANs in the Add Device Process

During the Add Device process, LiveNX allows user-selection of the VLANs to display in the topology view. VLANs listed here are Layer 2 related VLANs and are not Interface VLANs, which are selectable in the Select Interfaces step in the wizard. VLANs not associated with at least one access port will not be included for selection. At most 25 VLANs can be selected for display. The LiveNX default automatically selects the first 5 VLANs during the Add Device process.

Steps	Select VLANs			
1. Device Connection Information	Select the VLA	Ns you want to monitor on this	device (maximum 25 VLANs).	
 CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANS Select VLANS Select Peatures Enable Polling Review Configuration Device Updated 	Selected V V V	VLAN 5 10 20 22 30 40 46 50 60 61 111 999	DescriptionVideo c15VLAN10VLAN0020VLAN0022VLAN0030VLAN0040VoiceVLAN0050VLAN0060VLAN0061VLAN0111VLAN0999	
	< Back	Next > Finish		Cancel Help

VLAN Highlighting Through a Network:

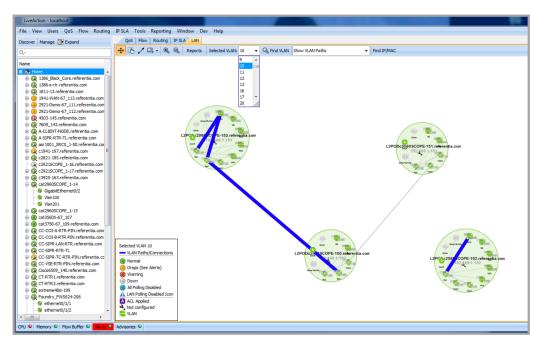
Use the Selected VLAN: drop-down menu to select any available VLAN index in the entire system topology. The VLAN will be highlighted in the system view.

The specific VLAN is highlighted as it traverses through the network.

LiveAction - localhost	
File View Users QoS Flow Routing	IP SLA Tools Reporting Window Dev Help
Discover Manage Discover	QoS Flow Routing IP SLA LAN
Q-	🕂 🔀 🖍 🖫 🔍 🔍 Reports Selected VLAN: 10 🗸 🖓 Find VLAN Show VLAN Paths 🗸 Find IP/MAC
Name	
E 🔊 Home 🔺	
⊕ Q 1386_Black_Core.referentia.com ⊕ Q 1386-s-rtr.referentia.com	

Use the Selected VLAN: drop-down menu to select any available VLAN index in the entire system topology. The VLAN will be highlighted in the system view.

The specific VLAN is highlighted as it traverses through the network.



Use the Find VLAN button to search by either VLAN Index or VLAN name. To find a VLAN, either type in the VLAN index or the VLAN name to highlight the VLAN. Typing in partial names will provide a list of all VLANs containing that string of characters.

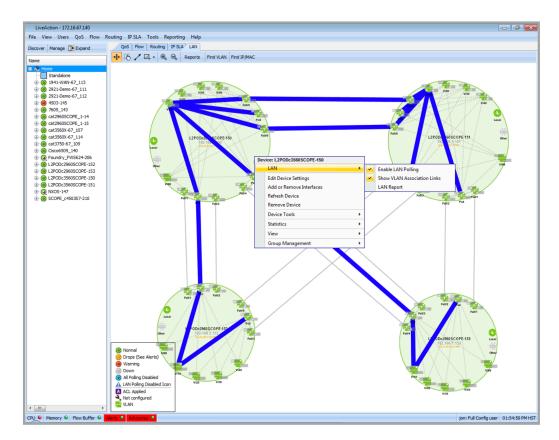
🔍 Find VLAN		
Select a VLAN to display it in the LA	N tab system topology:	
Q- VLAN3		8
VLAN Index	Name(a)	
	Name(s)	
± 30	USER30, Vlan30	
± 31	Vlan31	
± 300	Test, Vlan300	
± 350	Testing, Vlan350	
± 369	Vlan369	

Clicking on the "+" to the left of the VLAN index displays a list of devices that the VLAN is configured on.

Q VLAN3		-
-		
/LAN Index	Name(s)	
30	USER30, Vlan30	
7609_143.referentia.com	Vlan30	
(iii) cat2960SCOPE_1-14	Vlan30	
(6) cat2960SCOPE_1-15	Vlan30	
🛞 Cisco6509_140.referentia.com	Vlan30	
L2PODc2960SCOPE-152.referentia.com	USER 30	
L2PODc2960SCOPE-153.referentia.com	USER 30	
L2PODc3560SCOPE-150.referentia.com	USER.30, Vlan.30	
L2PODc3560SCOPE-151.referentia.com	USER30, Vlan30	
SCOPE_c4503S7-210.referentia.com	Vlan30	
🛞 Switch-180.referentia.com	Vlan30	
8 31	Vlan31	
E 300	Test, Vlan300	
B 350	Testing, Vlan350	
B 369	Vlan369	

- All, VLAN Index or Name(s): Desired values include both of the table columns, only the VLAN Index column or only the Name(s) column. Default is All.
- Case Sensitive or Case Insensitive: Desired values are either Case Sensitive or Case Insensitive. Default is Case Insensitive.
- Use Wild Cards or Use Regular Expression: Selecting Use Wild Cards and then typing *x will filter all entries in the desired column containing an x. Selecting Use Wild Cards and then typing ??x will filter all entries in the desired column where the third character is an x. Selecting Use Regular Expression and then typing x will filter all entries in the desired column containing the string x. Both are defaulted off.
- Match from Start, Match Exactly, Match Anywhere: The filter will display all column entries that match from the start, that match exactly, or that match anywhere within that column's value. Default is Match anywhere.
- Keep Parent Row If Any of the Children Match, Keep the Children If Any of the Ancestors Match: Unselecting Keep Parent Row If Any of the Children Match will filter out the parent row if the parent does not match the contents of the sort criteria. Unselecting Keep the Children If Any of the Ancestors Match will filter out the children if none of the children match the contents of the sort criteria. Default is both options are enabled.

To hide the dashed VLAN association links, right click on a device then click on LAN > Show VLAN Association Links to uncheck the option. The default is Show VLAN Association Links = enabled.

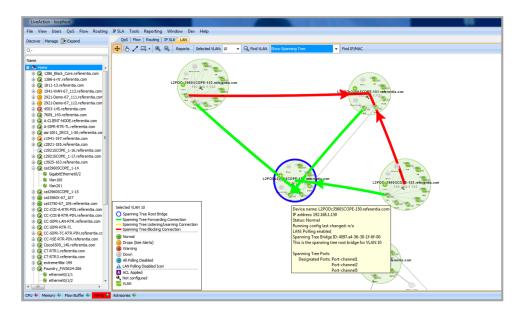


Spanning Tree Highlighting Through a Network

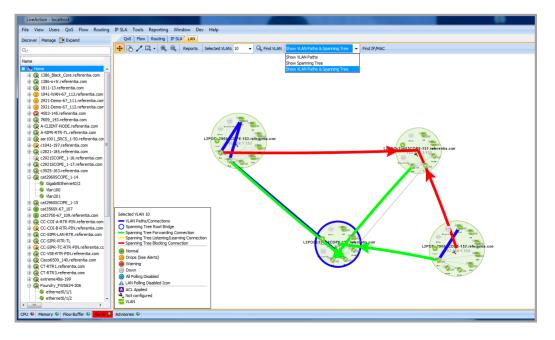
LiveNX provides the ability to highlight spanning tree information in the system view.

In the LAN tool bar, select the desired VLAN and then use the drop-down to select Show Spanning Tree. The topology highlights the spanning tree connections and root bridge per VLAN and shows spanning tree topology changes as they occur (how fast the changes are detected is dependent on the LAN polling settings).

The image below depicts the root bridge, three forwarding connections and two blocking connections. The arrows indicate the path to the root bridge where the base of the connection represents either a blocked or root port and the head of the arrow points to a designated port. The arrows will be drawn to or from the middle of a device if the spanning tree port is not visible in the topology. Spanning tree devices not added into LiveNX will be shown using its bridge ID. Tooltips are available by hovering over the desired device providing additional spanning tree information including spanning tree bridge ID, root bridge, and root, designated, and blocked ports. Tooltips are also available by hovering over the desired spanning tree connection to see connection state information.



Select Show VLAN Paths & Spanning Tree to highlight both in the System View. The Spanning Tree information will be overlaid on the VLAN path.



Real-time Monitoring

LiveNX provides the capability to display real-time trunk and access port statistics for a given VLAN on a device.

Use the VLAN drop-down to list the trunk and access ports associated with the VLAN. Selecting an individual VLAN in the System Hierarchy or clicking on the VLAN in the topology view automatically selects the VLAN in the drop-down. The default selection is All.

The alert indicator in the first column of each row describes the trunk and access port health; the alert colors are the same as the topology view legend.

Click on the desired device in the LAN tab to display the statistics.

1	Enable Poling									
ne internet interne	and the second se									
Home Cat29605COPE_1-14	VLAN: A	• Show	Layer 2 QoS							
	Trunk Parts									
GgabitEthernet0/1	Interface = 1	VLAN(s)	Trust	Input Bandwalth Olber	() Output Bandw	with (Kbos) Input (Dreps	onnected Device	Connected Interface
- B Port-marries				Sibrit Bandwidth (KDDR		(GIP (KODR)	rops Culpu			
	FastEthernet1/1 FastEthernet1/5	10, 20, 30, 40, 45, 50,			152	12		- 9	K2960SCOPE_1-14	FestEthemet0/1
	Fastthemet1/5	1, 20, 20, 30, 40, 46,			1	12				
C606509_140	GosbiEthernet1/6	1, 10, 20, 30, 40, 46,			1	12			750-235.referentia.com	
	GloabiEthernet4/11	1, 10, 20, 30, 40, 46,				15			129605COPE_1-15	GgabiEthernet0/1
	GoabiEthernet4/8	1, 10, 20, 30, 40, 46,			5	19			129609COPE_1-15	GigabitEthernet0/2
	GigabitEthernet4/8	1, 10, 20, 30, 40, 46,			<1	19			KOS-147.referentia.com(TBM	
	GigabitEthernet6/1 Port-channel4	1, 10, 20, 30, 40, 46,			3	17			09_143.referentia.com	GigabitEthernet2/1
	U Port-channel-40	1, 10, 20, 30, 40, 46, 1, 10, 20, 30, 40, 46,							129605COPE_1-13 750-235.referentia.com	
GigabitEthernet4/8	o ronoaneo	1, 10, 20, 30, 40, 40,	50, 60, 4						/so-235./enerentea.com	
GigabitEthernet5/1 Wan20 St VLANs	Access Ports									
	Interface	VLAN(s)	IP Address(es)	Trust	Input Bandwidth (Kbps)	Output Bandwidth (Kbps)	Input Drops	Output Drops	Connected Device	Connected Interface
	© FastEthernet1/2	1		C05		0	0			
	U FastEthernet1/3	201		Precedence		0	0			
	FasiEthernet1/30	1069				0	0			
	C FastEthernet1/39	30				0	0		-	
	D FastEthernet1/40	4094				0	0			
	G FastEthernet1/41	1				0	0			
	C FastEthernet1/42	1				0	0			
	E FastEthernet1/43	1				0	0			
	E FastEthernet1/44	1				0	0			
	G FastEthernet1/45	4				0	0	 • 	×	
	© FastEthernet1/46	1				0	0			
	© FastEthernet1/47	1				0	0			
	FastEthernet1/48	50	30.30.50.254, 30.30.20.200			5	6	÷		
	CigabitEthernet6/2									

The statistics are separated into Trunk Ports and Access Ports. Both tables display Interface, Trust, Input Bandwidth (Kbps), Output Bandwidth (Kbps), Interface Drop, Connected Device and Connected Interface.

- Interface Name: Interface associated with the desired device.
- Trust: Class of Service (CoS), Differentiated Services Code Point (DSCP), IP Precedence (Precedence) or none (untrusted).
- Input Bandwidth: Input bandwidth for that interface. Output Bandwidth: Output bandwidth for that interface.
- Interface Drop: Alert indicator with Green for Normal, Yellow for Drops, Red for Warning, Gray for Down and Blue for All Polling Disabled.
- Connected Device: Device connected to the Interface. Connected Interface: Interface name of the connected device.

Right-clicking on the text in a table entry provides two options: Show Interface Details and Export Data.

- Show Interface Details LiveNX displays two boxes: show interface and show policy-map.
- Show interface port provides packet statistics at the last polling interval. The Refresh button will update the stats based on the most current polling interval.
- Show policy-map provides packet statistics for all classes for the service policies defined at the last polling interval. The Refresh button will update the stats based on the most current polling interval. Export Data brings up a dialog box to allow you to save the contents of the Layer 2 statistics table into a CSV (comma separated value) formatted text file.

View Interface Details for Port-channel2	×
View the interface status and the packet statistics for all classes configured for the service policies on interface Port-char	nnel2
show interface Port-channel2	
show interface Port-channel2	_
<pre>Port-channel2 is up, line protocol is up (connected) Hardware is EtherChannel, address is 2c36.f884.3f84 (bia 2c36.f884.3f84) Description: c3560SCOPE-150 Po2 MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full-duplex, 100Mb/s, link type is auto, media type is unknown input flow-control is off, output flow-control is unsupported Members in this channel: Fa0/3 Fa0/4 ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:01, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Description </pre>	E F
show policy-map interface Port-channel2	_
show policy-map interface Port-channel2	
§ Invalid input detected at '^' marker.	
Refresh Clos	se

Click on the Show Layer 2 QoS button to display Layer 2 QoS statistics in tabular form.

Interface Name	Port Type	Trust	Direction	Queue	Threshold	Total Dropped Packets	Drop Rate (pps)	COS-Map	DSCP Range
GigabitEthernet6/1	Trunk		Outbound	2	2	933	0	000114	over range
FastEthernet 1/1	Trunk	CoS	Outbound	2	2	552	0	467	32, 48, 56
astEthernet1/1	Trunk	CoS	Outbound	1	1	3.6 M	0	01	0,8
SigabitEthernet4/11	Trunk	DSCP	Inbound	1	1	44.8 K	0	01234567	0-63
GigabitEthernet4/16	THATK	USC.	Outbound	1	1	97	0	01204007	0.00
FastEthernet1/1	Trunk	CoS	Outbound	2	1	36	0	5	40
asiculemeti/1			Outbound	1	1	16.9 M	0	5	
astEthernet1/2	Trunk	CoS	Outbound	2	1	141 K	0	5	40
FastEthernet1/2	Trunk	CoS	Outbound	1	1	7.4K	0	01	0,8
SigabitEthernet4/11	Trunk	DSCP	Outbound	1	1	5.7 M	0	01	0-15
SigabitEthernet4/2	TOTAL	000	Outbound	2	2	2.5 G	0	• •	0.15

The Layer 2 QoS Statistics table lists all interfaces and its QoS statistics. The table can be filtered using four fields. Each can be enabled on or off independently from the other. The default filter is Interface with queue drops = Enabled.

- Interface with queue drops Displays all interfaces where the Total Dropped field is > 0.
- Priority queue stats Displays all interfaces with COS-Map = 5.
- Inbound queues Displays all interfaces with the Direction = Inbound.
- Outbound queues Displays all interfaces with the Direction = Outbound.

Export Data brings up a dialog box allowing you to save the contents of Layer 2 QoS Statistics into a .csv (comma separated value) format.

Find IP and MAC addresses

LiveNX can attempt to find IP and MAC addresses within the system using information obtained from polling the MAC address forwarding, and MAC address and ARP tables in the SNMP MIB on the devices. This information is polled every 15 minutes. Click on Find IP/MAC in the toolbar of the topology view or on LAN > Find IP/MAC in the LiveNX Client main menu. For this feature to work, LAN polling must be enabled for all devices of interest.

File View Users QoS Flow F	Routing IP SLA Tools Reporting Window Dev Help
Discover Manage Expand	QoS Flow Routing IP SLA LAN
Name	🕂 🔀 🖍 🗔 👻 🔍 Reports 🛛 Find VLAN 🛛 Find IP/MAC
🗖 🚫 Home	
⊕ @ cat2960SCOPE_1-14	
Cat2960SCOPE_1-15	
GigabitEthernet0/1	
Port-channel3	
⊟ @ Cisco6509_140	
Generation Generatio Generation Generation Generation Generation Generation	
😔 FastEthernet 1/5	
😌 FastEthernet 1/6	
😔 GigabitEthernet4/11	
GigabitEthernet4/12	
GigabitEthernet4/8	
GigabitEthernet6/1	
VLANs	
1	

File View Users QoS Flow F	outing IP SLA LAN Tools Reporting Window Dev Help
Discover Manage 🗈 Expand	Qos Flow Find IP/MAC
Q	🕂 🔁 🖍 🖳 🔹 🔍 Reports Selected VLAN: 1 🔹 🔍 Find VLAN Show VLAN Paths 🔹 Find IP/MAC
Name	
😑 🐼 Home	

The Find IP/MAC command can also be found by right-clicking on a device in the topology view and selecting LAN > Find IP/MAC.

File View Users QoS Flow F	Routing IP SLA LAN Tool	ls Repo	orting Window	Dev Help	
Discover Manage 🗈 Expand	QoS Flow Routing	IP SLA	LAN		
Q	Enable Polling				
Name	VLAN: All 🗸	Show	Layer 2 QoS		
1386 Black Core	Trunk Ports				
Device: 1386_Black_Core.	referentia.com		VLAN(s)	Trust	
QoS		•			
Flow		•			
Routing		+	>		
Routing P SLA P SLA P SLA		>			
		• •	Enable LAN Poll	ing	
Edit Device Settings			Find IP/MAC		
Add or Remove Interf	aces	~	Show VLAN Ass	ociation Links	
Image: Construction Edit Device Settings Image: Construction Add or Remove Interf Image: Construction Refresh Device Image: Construction Remove Device			Reports		
Remove Device					
Device Tools		•			
Device Tools		•			
🗄 🛞 🛛 View		•			
Group Management		•			

Note If SNMP V3 is used for polling, the "context vlan- match prefix" arguments must be added to your SNMP-server group command. An example of the command is shown below:

snmp-server group <group name> v3 priv snmp-server group <group name> v3 priv context vlan-match prefix

Type in the IP or MAC address in the top row of the Resolve IP and MAC Addresses table. Note that the text turns red until a valid IP or MAC address is entered. Click on Resolve to begin the search.

Resolve IP and				
Type in a single IP	Resolve			
Device Name				

Entering an IP address will provide the MAC address and the device and interface closest to the IP or the actual device and interface if it is an IP on a device.

Right click on the found device and click on Zoom to Device to automatically center the device in the system topology view. The Zoom to Device feature will not appear if you are accessing a device or inter-

face view. If the desired device is part of a user-defined group, then the Zoom to Device will zoom to the group that contains the desired device.

Resolve IP and MAC Addresses							
192.168.1.150	Resolve						
Device Name	MAC Address(es)	VLAN Index					
L2PODc3560SCOPE-150	GigabitEthernet0/1	a456.301f.6f41	201				
	Zoom to Device						

Entering a MAC address provides the IP corresponding to the MAC address and the device and interface closest to where the MAC address was discovered.

Resolve IP and MAC A			
a456.301f.6f41	Resolve		
Device Name	Interface Name	IP Address(es)	VLAN Index
L2PODc3560SCOPE-150	GigabitEthernet0/1	192.168.1.150	201

Output of Resolve IP and MAC Addresses Table for a MAC Address Input

Right click on the found device and click on Zoom to Device to automatically center the device in the system topology view. The Zoom to Device feature will not appear if you are accessing a device or interface view. If the desired device is part of a user-defined group, then the Zoom to Device will zoom to the group that contains the desired device.

CHAPTER 12

Tools

In this chapter:

Tools Overview.	241
Manage Performance Groups and Application Groups	248
DNS Name Resolution	258
Device Tools	260
Statistics	266

Tools Overview

System Advisories

Notifications on abnormal server performance can be viewed in the Advisories Viewer. Select the viewer from Tools > View Advisories.

LiveAction - localhost			
File View Users QoS Flow R	Routing IP SLA LAN	Tools Reports Window Dev Help	_
Dashboard Manage Image Expand Q Name Image <	QoS Flow Rou	View Alerts Configure Alerts View Advisories Use IP Mappings Edit IP Mappings Use IP Blacklist Edit IP Blacklist MSI Endpoints Use VSOM Mappings Edit VSOM Mappings Manage Custom Applications Define Custom Application	s Cu webex-meet 192.1

v 1			
Time 1	Severity	Title	Node
014/07/08 10:06:50 AM	😂 ERROR	Error Connecting to Device	Local
014/07/08 10:06:07 AM	🛕 WARNING	HTTP Server Hostname Not Config	u Server
		hostname for the embedded web server has no figured. Please configure the "httpserver.host" (

IP Mapping

The IP Mapping feature allows the mapping of an IP address or hostname to a user-defined label. This feature only affects the labeling within LiveNX and does not affect any actual DNS or hostname configurations.

IP Mappings can be managed by selecting Tools > Edit IP Mappings. IP Mappings can be created, edited, removed, exported and imported from within the Edit IP Mapping Dialog.

To show IP Mappings, select Tools > Use IP Mappings. IP Mappings will now appear on the topology, flow tables and reports.

Too	Is Reporting Help							
	View Alerts		Edit IP	Mapping				×
	Configure Alerts		IP Mappin	g				
	View Advisories		Nam	e		IP Addresses		Add
~	Use IP Mappings			tNode-01		172.16.67.73		Import
_	Edit IP Mappings		Route	er-B erNode-01		192.168.1.135 172.16.67.42		
 Image: A start of the start of	Use IP Blacklist	3	Serve	envoue-o I		1/2.10.07.42		Export
	Edit IP Blacklist							Edit
	Port Assignments							Remove
	Enable DNS Resolution (Global)							
	Show DNS Names							
	Device Tools	•						
	Statistics	•						
	Group Management	•						
	Options							
			New IP Ma	apping entries l	nave a (*).			
								Caral
							ОК	Cancel

IP Mappings can also be created by right-clicking an endpoint on the flow topology or tables, and selecting Add [IP Address] to IP Mapping.

172.16.67.24	9		~ 2
		Create Display Filter	•
		Add to Current Display Filter	►
r		No Display Filter	
		Add 172.16.67.249 to IP Blacklist	
		Add 172.16.67.249 to IP Mapping	
		Copy 172.16.67.249 to clipboard	5
		Create Network Object	

NOTE: IPv6 is not supported.

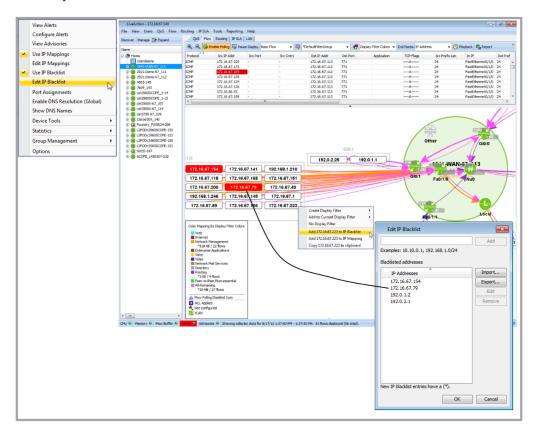
IP Blacklist

The IP Blacklist feature allows the identification of IP addresses or hostnames that will appear in red in the topology, device, Flow table, and historical views. This is a method of identifying quickly and visually any known anomalies.

The IP Blacklist can be managed by selecting Tools > Edit IP Blacklists. IP addresses can be added to the blacklist, edited exported and imported in the Edit IP Blacklist dialog.

IP addresses can also be added to the blacklist by right-clicking an endpoint on the topology or table and selecting Add [IP Address to IP Blacklist.

The example below shows blacklisted entries.



MSI Endpoints

Media Services Interface (MSI) is used to provide better visibility and services to media applications.

To include MSI endpoints in your system topology, go to Tools > MSI endpoints.

Click on Add, specify the IP addresses of your endpoints, select among User/Password, User/Password Proxy or Certificate and then complete the fields. Click on OK.

MSI Endpoints	x
Alias	IP PerfMon
MSI Endpoints Specify IP ranges (ex: 192.168 10.81.74.98 10.81.74.66	X (3.1.1-200) or one IP per line:
 User/Password User/Password Proxy Certificate 	User Name: admin
	OK Cancel
Add Remove Edit	Performance Monitors

Click on the desired IP address and click on Edit to add an Alias.

MSI Endpoints				x
Alias		IP	PerfMo	on
		10.81.74.66	Off	
		10.81.74.98	S Off	:
	Fdit Endpoint Alias: EX IP: 10 User Name: ad Password: cis	60 .81.74.66 min		
Add Remove	ādit		Performance Monitors]

Right click on an individual endpoint to see flows, to show modules or to export data associated with that endpoint.

MSI Endpoints		×
Alias	IP	PerfMon
	10.81.74.66 10.81.74.98 Show Flows Show Modules	C Off
	Export Data	
Add Remove Edit	Performance	Monitors

Return to the MSI Endpoints window, choose an MSI endpoint and then select Performance Monitors. Choose a time interval to monitor the data and then select either flow type Real-time Transport – RTP or Transmission Control Protocol – TCP.

Source IP	Source Port	Destination IP	Destination Port	IP Protocol
).81.74.98	2376	10.81.74.66	2328	UDP
.81.74.66	2328	10.81.74.98	2376	UDP
.81.74.98	2378	10.81.74.66	2330	UDP
.81.74.66	2330	10.81.74.98	2378	UDP
.81.74.98	2380	10.81.74.66	2332	UDP
.81.74.66	2332	10.81.74.98	2380	UDP
.81.74.98	2382	10.81.74.66	2334	UDP
.81.74.66	2334	10.81.74.98	2382	UDP
erval (seconds): 10	Flow Type:			

Select a flow, right click and select Show Reports to view the Performance Monitor Report. In this example, the test was run four times at ten-second intervals.

 Seq Num	 	End Time	SSRC	RTP Bit Rate (Kbps)		RTP Pkts Lost	DSCP	
		2013-01-11T23:18:23Z	-	69	NOT COLLECTED	NOT COLLECTED	NOT COLLECTED	NOT C
		2013-01-11T23:18:13Z		69	NOT COLLECTED	NOT COLLECTED	NOT COLLECTED	NOT (
		2013-01-11T23:18:03Z		69	NOT COLLECTED	NOT COLLECTED	NOT COLLECTED	NOT
	2013-01-11T23:17:43Z	2013-01-11T23:17:53Z	0	69	NOT COLLECTED	NOT COLLECTED	NOT COLLECTED	NOT

To get per hop performance data, go to the System Flow Table, click on the Medianet tab and then select the desired flow.

Applicatio	n (AVC) Ba	asic Flow Medianet NSEL													
Color	Protocol	Src IP	Src Ports	Src Co	Dst IP	Dst Port	Dst Co	App N	DSCP	Total B	V	Pack	Inter	Loss	DSC
	UDP	10.81.74.98	2,378	-	10.81	2,330	-		0 (BE)	55 MB	3923	0.00 %	0.271	0	(q
	UDP	10.81.74.98	2,376	-	10.81	2,328	-		0 (BE)	6 MB	3716	0.00 %	0.207	0	0
	UDP	10.81.74.66	2,328	-	10.81	2,376	-		46 (EF)	3 MB	2287	0.00 %	0.129	0	46
	UDP	10.81.74.66	2,328	-	10.81	2,376	-		0 (BE)	2 MB	2287	0.00 %	0.119	0	0
	UDP	10.81.74.66	2,330	-	10.81	2,378	-		32 (CS4)	24 MB	2087	0.00 %	0.108	0	32
	UDP	10.81.74.66	2,330	-	10.81	2,378	-		0 (BE)	16 MB	2087	0.00 %	0.105	0	(
	LIDP	10.4.51.15	5.002	-	10.4	16,400			0 (BE)	5 MB	1227	0.00 %	41.79	0	1

Right-click on the selected flow, choose Execute Mediatrace and select MSI Endpoint. Click on Execute Mediatrace.

System Flow Table			
Application (AVC) Basic Flow M	Execute Mediatrace (Command X	l.
Color Protocol 5 UDP 10.81.74.5 Dr	Source Ip Address: Source Port: : Destination Ip Address: Destination Port: : Time to live: nitiate Mediatrace from:		7 Pack Inter Loss DSC 123 0.00 % 0.271 0 0
	C Other Device:		

The Mediatrace report tabulates the performance data on a per-hop basis from source to destination.

Use/Edit VSOM (Video Surveillance Operation Manager) Mappings

VSOM is a full-featured video surveillance operations management application that runs on the Cisco Video Surveillance Media Server (VSMS) and Cisco Video Surveillance Virtual Matrix (VSVM) server platforms. LiveNX adds VSOM servers into its application to provide visualization and monitoring of the servers and its associated IP cameras. LiveNX will interrogate the VSOM server, retrieve its IP address and its attached devices and then display the device name in the topology for use in the LiveNX dashboards and reports.

Click on Tools > Edit Vsom Mappings. Then click on Add. Type in the Host, User Name, Password and Domain information in the Add Server window. Click on OK. LiveNX will alert you if you did not add a VSOM server name or if you use incorrect login credentials. Click on Add to append multiple VSOM

Servers to this list. Click on Remove to delete an entry in the table. Highlight a table entry and click on Edit to modify the User Name, Password or Domain.

Mediatrace Flow: 10.81.74.98:237	diatrace Flow: 10.81.74.98:2378 -> 10.81.74.66:2330							
	cdn-ex90	4503E-AA0601	VXR-AA0301	2921-AA0110	2921-AA0109-SW	2811-AA011		
Device	cdn-ex90	4503E-AA0601	VXR-AA0301	2921-AA0110	2921-AA0109-SW	281		
Hop Number	0	1	2	3	4			
Нор Туре	-	-	-	-	N/A			
Ingress Interface	None	Gi2/46	Gi0/2	Gi0/1	Gi0/1			
Egress Interface	eth0	Gi2/3	Gi0/1	Gi0/2	Gi0/2			
RTP Jitter	0.00 ms	0.50 ms	0.24 ms	0.08 ms	0.00 ms			
RTP Packet Lost	0	0	0	0	0			
RTP Packet Expected	909	913	913	910	0			
RTP Packet Loss %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %			
IP Packet Drops	0	0	0	0	0			
IP Packet Drop Reason	0	0	0	64	0			
Media Bit rate	681 Kbps	691 Kbps	691 Kbps	684 Kbps	0 bps			
IP Bit rate	0 bps	706 Kbps	705 Kbps	705 Kbps	0 bps			
DSCP	0 (BE)	0 (BE)	0 (BE)	0 (BE)	0 (BE)			
Trace RTT	- ms	- ms	- ms	- ms	0 ms			

Highlight a VSOM server and click Refresh Selected to retrieve any additional information from the VSOM server. Click on Refresh All to retrieve additional information from all the VSOM servers in the list.

VSOM Server	2				X
Host Name		User	Domair	ı	
	Add Server	11			
	Host: User Name: Password: Domain:				
			ок С	ancel	
Add	Remove Edit		Refresh Se	elected Re	fresh All

Right-click on any VSOM server in the list and select either Show Devices or Export Data.

Show Devices: LiveNX will interrogate the VSOM server to find the IP cameras or other IP devices associated with the VSOM server. The list shows the Device IP address and the Device Name. Click on the red x in the top right corner to close this window. If this Device IP list is incomplete, close the window, refresh the device and right click on Show Devices again.

Device IP	Device Name
92.168.200.18	Amster5 South
92.168.200.11	Amster5 West
92.168.200.12	EU Overview
92.168.200.15	SJ-28 East
92.168.200.13	SJ-28 North
92.168.200.14	SJ-28 South
92.168.200.16	SJ-28 West
92.168.200.11	US Overview

Export Data: LiveNX generates a .csv file listing the VSOM Servers Host Names, User & Domain Names.

Click Tools > Use VSOM Mappings to map the device IP addresses to Device Names for use in the topology views, reports and dashboard. If Use IP Mappings and Show DNS Names are also enabled in the Tools drop-down list, then mappings are done using IP Mappings first, then VSOM Mappings and then Show DNS names.

Manage Performance Groups and Application Groups

Manage Performance Groups

The Performance Group Mapping feature allows you to define and map custom application groups to the desired differentiated services code point (DSCP) values. Click on Tools > Manage Performance Groups or click on Configure Performance Groups in the left-hand column of the WAN-PfR Dashboard. This will open the Edit Performance Group Mapping window. Click on Add to add user-defined performance groups. Use the drop-down menu to select the desired DSCP value. Click on the Fill SLA defaults using to find a typical profile. Choices include Voice Profile, Real-Time Video Profile, Low Latency Data Profile, Best Effort Profile and Scavenger Profile. The SLA values can be edited as well. Click on Add another to continue mapping performance groups to DSCP values, click on Add to return to the Edit Performance Group Mapping window or click on Cancel to return to the Edit Performance Group Mapping window without adding a performance group.

A Edit Perfor	mance Group Mapp	ing	Σ	3		
Performance G	roup Mapping					
DSCP	^	Performance Group	Add			
			Import			
	Add Performa	×				
	Performance Grou					
	DSCP	0 (BE)	•			
	SLA Configuration					
		Fill SLA defaults using	Best Effort Profile 🗸 🗸			
	Enable	Error	Voice Profile			
		Loss 10.0	Real Time Video Profile Low Latency Data Profile			
	V (Delay 500	Bulk Data Profile			
		Jitter 0	Best Effort Profile Scavenger Profile			
New Performar						
		Add Another	Add Cancel			

In the Edit Performance Group Mapping window, click on Import to copy in another LiveNX user's performance groups in .txt format, or Export to transfer your performance group mapping to another LiveNX user. Highlight an existing line in the Performance Group Mapping table and click on Edit to modify the existing mapping or Remove, to remove the item from the list.

Manage Application Groups

The Manage Application Groups feature allows you to define custom application groups as a way to group applications together.

Click Tools > Manage Application Groups or click on Manage Application Groups in the left-hand column of the Application Dashboard. This will open the Manage Application Groups window.

Click on Add Group to add a user-defined group.

Click on Add Definition and use the check box to select one to many applications that will be associated to this group.

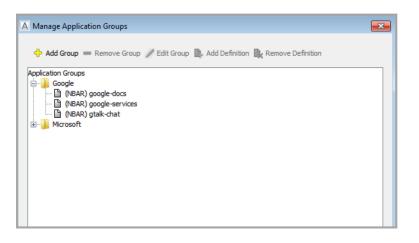
Click on OK when complete.

Click on an Application Group and select Remove Group to remove this group from the list.

Click on an Application Group and select Edit Group to rename the Application Group.

Click on a definition within a group and select Remove Definition to remove the application from the group.

Click on Apply to save changes and Click on OK to close the window.



Application aol-protocol	Vendor NBAR	
apl-protocol	NRAD	
	NDAK	
ms-dynamics-crm-online	NBAR.	
groupwise	NBAR.	
texar	NBAR.	
google-docs	NBAR.	
songsari	NBAR	
hamachi	NBAR	
banyan-vip	NBAR	
wccp	NBAR	
cooltalk	NBAR	
egp	NBAR	
vid	NBAR	
gtalk-chat	NBAR	
ms-lync-video	NBAR	
creativepartnr	NBAR	
masqdialer	NBAR	
netbios-ns	NBAR	
google-services	NBAR	
rap	NBAR	
cdc	NBAR	
xfer	NBAR.	

Manage/Define Custom Applications

The Custom Applications feature allows you to define and edit custom applications based on a specific, list or range of IP addresses, by protocol, by port number or by Layer 4 Protocol (TCP, UDP, DCCP or SCTP). Creation of custom applications is reserved for admin and full-config user roles. Once created, the custom application is visible to all users.

To create a custom application, go to Tools > Define Custom Applications.

Choose a name, a description, and an IP address and/or port number. The IP Address can be entered as one IP per line, a range of IP addresses, or a specific subnet address. Wildcards can also be used with the IP address, for example, "10.0.0.2/0.255.255.0." A valid port number can be entered between 0 and 65535.

Define Cu	ustom Application						
Name:	userguide						
Description:	used as an example for the user guide illustrations						
IP Address:	IP Address: Specifiy IP ranges (ex: 192.168.1.1-200) or one IP per line 10.28.95.3 10.28.95.8-100 10.28.95.101/24						
Port:	6000 Layer 4 Protocol: TCP						

Adding both an IP Address and a Port Number will define your custom application to the defined IP address AND port number. If both IP Address and Port Number are used, define the Source IP Address with the Source port or the Destination IP Address with the Destination port.

If you specify both port and address, the mapping only works for (source IP and source port) or (destination IP and destination port) combinations.

Click on Save to add this to your custom application list.

To review or to edit your list of custom applications, go to Tools > Manage Custom Applications.

Highlight a row and click on the Up or Down button to move the table entry higher or lower in the list. The order defines precedence of that particular custom application. In cases where there are multiple application names for the same IP address, the higher placed item takes precedence.

1	Manage Custom	Applications			X
	Up Dowr	n Q.			Show default
	Name	Description	IP	Port	Layer 4 Pr
		used as an example for t		60	000 TCP
	trainingnetflow uhvtc	video for netflow training conference call	12.13.14.15 192.168.1.1	3	350 TCP
	Nev	w Edit	Remove	Save	Close

The header row with the magnifying glass filters the list based on the defined alphanumeric string.

Manage C	ustom Appli	cations			×
Up	Down	λ∼ tcp		S	how default
Name	Desc	iption	IP	Port	Layer 4 Pr
userguide uhvtc	used a	as an example for t rence call	10.28.95.3, 10 192.168.1.1		TCP TCP
	New	Edit	Remove	Save	Close

Click on Show default to list a table of the common port assignments. The table is shown below. Any port assignment defined in the Custom Application takes precedence over the common port assignment.

Port	Layer 4 Protocol	Name	Description	
	7 TCP	echo	Echo	
	7 UDP	echo	Echo	0
11 TCP		systat	Systat	
11 UDP		systat	Systat	
13 UDP		daytime	Daytime	
13 TCP		daytime	Daytime	
19 UDP		chargen	Chargen	
19 TCP		chargen	Chargen	
21 TCP		ftp	Ftp	
22 UDP		pcanywhere	Pcanywhere	
22 TCP		ssh	Ssh	
23 TCP		telnet	Telnet	
25 TCP		smtp	Smtp	
	37 TCP	time	Time	
	37 UDP	time	Time	
	43 TCP	nicname	Nicname	
	43 LIDP	nicname	Nicname	

Click on New to return to the Define Custom Application dialog box.

Click on a user-defined Custom Application and click on Edit to edit the defined custom application using the Edit Custom Application window. Click in the field that you want to modify, edit as desired and click on OK to continue.

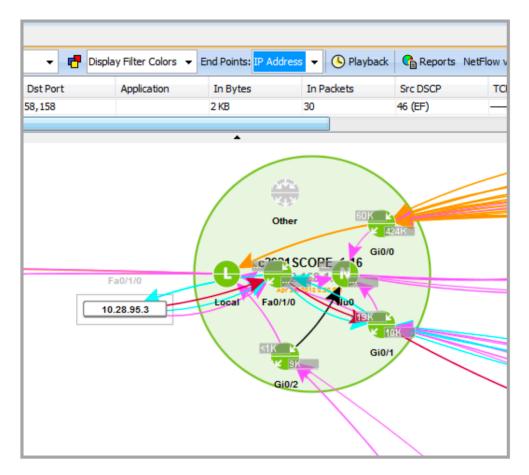
Edit Cust	om Application
Name:	userguide
Description:	used as an example for the user guide illustrations
IP Address:	Specifiy IP ranges (ex: 192.168.1.1-200) or one IP per line 10.28.95.3 10.28.95.10-10.28.95.100 10.28.95.0/24
Port:	5000 Layer 4 Protocol: TCP 👻
	OK Cancel

Click on a user-defined Custom Application and click on Remove to remove the custom application from the list.

Click on Save to save the custom application list. This list is viewable by all the LiveNX user roles.

Click on Close to close the Manage Custom Applications window.

The Custom Applications are viewable in the topology view. Click on the Flow tab and display IP Address in the End Points drop-down. Then select Applications and see that your defined IP Address displays your custom application name. Go to that particular defined IP address in the topology view, click on the Applications in the End Points drop-down in the Flow tab.



Click on the custom application name in the device view to highlight all custom applications of that type in the flow table.

UBP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63/88 679 0 (BE) UDP 172.16.67.135 61,945 - 192.168.1.16 161 smmp 57/88 614 0 (BE) UDP 172.16.67.130 64,463 - 192.168.1.16 161 smmp 83/88 93 0 (BE) UDP 172.16.67.172 57,385 - 192.168.1.16 161 smmp 8/88 88 0 (BE) UDP 172.16.67.140 55,584 - 192.168.1.16 161 smmp 8/88 88 0 (BE) UDP 192.168.0.125 53,466 - 192.168.1.16 161 smmp 8/88 82 0 (BE) UDP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8/88 82 0 (BE) UDP 172.16.725 59,385 - 192.168.1.16 161 smmp 8/88 82 0 (BE) UDP 172.16.725 59,385 - 192.168.1.16 161 smmp 8/88 82 0 (BE) UDP 172.168.1.16 161 smmp 8/88 80 (BE) UDP 172.168.1.16 161 smmp 8/88 80 (BE) UDP 172.168.1.16	CP 10.28.95.3 37,680 80.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 39,791 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 37,680 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13,168 - 10.28.95.2 - userguide 176 4 0 (BE) CP 10.28.95.3 13,	CP 10.28.95.3 17,680 0 0.0.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 39,791 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 13,168 - 102.28.52 - userguide 176 4 0.0E3 DP 172.16.67.131	Protocol	Src IP Addr	Src Port	Src Cntry	Dst IP Addr	Dst Port	Application	In Bytes	In Packets	Src DSCP
CP 10.28.95.3 39,791 90.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 17,680 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 172.16.6.7.101 61,028 - 192.168.1.16 161 smp 57.86 614 0 (BE) DP 172.16.6.7.	CP 10.28.95.3 39,791 0.010.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 17,680 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 13,168 - 10.28.95.2 - userguide 176 B 4 0.0E2 DP 172.16.67.131	CP 10.28.95.3 39,79.1 0.0.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 17,680 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 13,158 - 30.10.10.2 21 userguide 176.8 4 0.0E3 CP 10.28.95.3 13,158 - 10.01.0.2 21 userguide 176.8 4 0.0E3 CP 10.28.95.3 - 10.28.95.7 - userguide 176.8 4 0.0E3 CP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.18 679 0.0E5 DP 172.16.67.131 61,453	ГСР	10.28.95.3	39,791	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
CP 10.28.95.3 17,680 0.010 10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) SPFIGP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) SPFIGP 10.28.95.3 - - 10.28.95.3 - 102.168.1.16 161 smp 57 KB 614 0 (BE) DP 172.16.67.135 61,453 - 192.168.1.16 161 smp 53 KB 567 0 (BE)	CP 10.28.95.3 17,680 • 80.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176.8 4 0.0E2 SPFICP 10.28.95.3 - - 102.895.2 - userguide 64.8 1 48 (CS6) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 53.18 56.7 0.0E3 DP 172.16.67.135 61,44.3 - 192.168.1.16 161 smmp 53.18 56.7 0.0E3 DP	CP 10.28.95.3 17,680 90.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 11,372 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 11,352 - 30.10.10.2 21 userguide 176.8 4 0 (BE) CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176.8 4 0 (BE) SSPFIGP 10.28.95.3 - - userguide 176.8 4 0 (BE) D/P 172.16.67.130 64,463 - 192.168.1.16 161 smmp 53.78 614 0 (BE) D/P 172.16.67.130 64,463 - 192.168.1.16 161 smmp 53.78 614 0 (BE) D/P 172.16.67.122 57.385 <t< td=""><td>ГСР</td><td>10.28.95.3</td><td>17,680</td><td>-</td><td>30.10.10.2</td><td>21</td><td>userguide</td><td>176 B</td><td>4</td><td>0 (BE)</td></t<>	ГСР	10.28.95.3	17,680	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
CP 10.28.95.3 11.372 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 11.372 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) SSPFIGP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) SSPFIGP 10.28.95.3 - 10.28.95.2 - userguide 176 B 4 0 (BE) DP 172.16.67.101 61.028 - 192.168.1.16 161 smp 57 KB 614 0 (BE) DP 172.16.67.131.02 64,83 - 192.168.1.16 161 smp 8 KB 93 0 (BE) DP 172.1	CP 10.28.95.3 11.372 S0.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 11.572 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 8 4 0 (BE) CP 10.28.95.3 - 10.28.95.2 - userguide 176 8 4 0 (BE) SPFIGP 102.895.3 - 102.895.2 - userguide 176 8 4 0 (BE) JDP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 53.18 679 0 (BE) JDP 172.16.67.131 61,453 - 192.168.1.16 161 smmp 818 88 0 (BE) JDP 172.16.67.	CP 10.28.95.3 11.372 80.10.10.2 21 userguide 176.8 4 0 (E) CP 10.28.95.3 11.372 - 30.10.10.2 21 userguide 176.8 4 0 (E) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176.8 4 0 (E) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176.8 4 0 (E) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176.8 4 0 (E) SPFIGP 10.28.95.3 - 10.28.95.2 - userguide 176.8 4 0 (E) DP 172.16.67.135 61.545 - 192.168.1.16 161 smp<	ГСР	10.28.95.3	39,791	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
CP 10.28.95.3 11.372 0.10 10.2 21 userguide 176 B 4 0.0ED CP 10.28.95.3 13.168 - 30.10 10.2 21 userguide 176 B 4 0.0ED CP 10.28.95.3 13.168 - 30.10 10.2 21 userguide 176 B 4 0.0ED SPFETGP 10.28.95.3 13.168 - 30.10 10.2 21 userguide 176 B 4 0.0ED SPFETGP 10.28.95.3 - - 10.28.95.2 - userguide 64 B 1 48 (CS6 DP 172.16.67.113 61.945 - 192.168.1.16 161 smp 57 K8 614 0.0ED DP 172.16.67.130 64.463 - 192.168.1.16 161 smp 57 K8 614 0.0ED DP 172.16.57.132 67.385 - 192.168.1.16 151 smp<	CP 10.28.95.3 11.372 = 80.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176.8 4 0.0E2 CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176.8 4 0.0E2 SPFEGP 10.28.95.3 - - 30.10.10.2 21 userguide 176.8 4 0.0E2 DP 172.16.6.7.10 61,028 - 102.895.2 - userguide 64.8 1 48 (C56) DP 172.16.6.7.13 61,455 - 192.168.1.16 161 smmp 53/48 679 0.0E1 DP 172.16.7.131 61,463 - 192.168.1.16 161 smmp 53/48 567 0.0E1 DP 172.16.7.12 57,385 - 192.168.1.16 161 smmp 81/8 88 0.0E1 DP	CP 10.28.95.3 11.372 80.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 4 0 (BE) CP 10.28.95.3 13.168 - 30.10.10.2 21 userguide 176 4 0 (BE) SPFIGP 10.28.95.3 - - 10.28.95.2 - userguide 64.8 1 48 (CS6) DP 172.16.67.135 61.545 - 192.168.1.16 161 smmp 63.48 679 0 (BE) DP 172.16.67.135 61.545 - 192.168.1.16 161 smmp 53.48 567 0 (BE) DP 172.16.67.121 65.380 - 192.168.1.16 161 smmp 848 93 0 (BE) DP 172.16.67.124 55.584 - 192.168.1.16 161 smmp 848 82 0 (BE) DP 172.16.67.125 </td <td>ГСР</td> <td>10.28.95.3</td> <td>17,680</td> <td>-</td> <td>30.10.10.2</td> <td>21</td> <td>userguide</td> <td>176 B</td> <td>4</td> <td>0 (BE)</td>	ГСР	10.28.95.3	17,680	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
CP 10.28.95.3 13,168 - 20.10.10.2 21 userguide 176 B 4 0 (BE) DSPFIGP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) DSPFIGP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0 (BE) DSPFIGP 10.28.95.3 - - userguide 176 B 4 0 (BE) D/P 172.16.67.130 61,028 - 192.168.1.16 161 smmp 57 K8 614 0 (BE) D/P 172.16.67.130 64,463 - 192.168.1.16 161 smmp 57 K8 677 0 (BE) D/P 172.16.67.121 65,380 - 192.168.1.16 161 smmp 8 K8 93 0 (BE) D/P 172.16.67.140 55,584 - 192.168.1.16 161 smmp 8 K8 82 0 (BE) D/P 172.16.67.235	CP 10.28.95.3 13,168 0 0.010.10.2 21 userguide 176 B 4 0.0E2 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0.0E2 DP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 B 4 0.0E2 DP 10.28.95.3 - 10.28.95.2 - userguide 176 B 4 0.0E2 DP 172.16.67.131 61,028 - 192.168.1.16 161 smp 63/8 679 0.0E2 JDP 172.16.67.130 64,463 - 192.168.1.16 161 smp 53/8 567 0.0E2 JDP 172.16.67.130 64,463 - 192.168.1.16 161 smp 818 88 0.0E2 JDP 172.16.67.120 53,83 - 192.168.1.16 161 smp 818 88 0.0E2 JDP 172.16.67.140	CP 10.28.95.3 13,168 - 00.10.10.2 21 userguide 176 4 0.0E3 CP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0.0E3 DP 10.28.95.3 13,168 - 30.10.10.2 21 userguide 176 4 0.0E3 DP 172.16.67.101 61,028 - 192.168.1.15 161 smp 57/08 614 0.0E3 DP 172.16.67.135 61,4453 - 192.168.1.16 161 smp 57/08 614 0.0E3 DP 172.16.67.130 64,463 - 192.168.1.16 161 smp 51/88 567 0.0E3 DP 172.16.67.127 57,385 - 192.168.1.16 161 smp<	ГСР	10.28.95.3	11,372	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
CP 10.28.95.3 13,168 0.10.10.2 21 userguide 176.8 4 0.0ED DSPFIGP 10.28.95.3 - - 10.28.95.2 - userguide 64.8 1 48 (CS6) D/P 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.48 679 0 (EE) D/P 172.16.67.135 61,545 - 192.168.1.16 161 smmp 53.48 679 0 (EE) D/P 172.16.67.135 61,545 - 192.168.1.16 161 smmp 53.48 679 0 (EE) D/P 172.16.67.132 63,83 - 192.168.1.16 161 smmp 53.48 567 0 (EE) D/P 172.16.67.172 57,385 - 192.168.1.16 161 smmp 8.48 88 0 (EE) D/P 192.168.0.125 53,466 - 192.168.1.16 161 smmp 8.48 82 0 (EE) D/P	CP 10.28.95.3 13.168 0.10.10.2 21 userguide 176.8 4 0.0E3 DSPFIGP 10.28.95.3 - - 10.28.95.2 - userguide 64.8 1 48 (CS6) DP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.48 67.9 0 (EE) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 53.48 614 0 (EE) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 53.48 567 0 (EE) DP 172.16.67.132 65,380 - 192.168.1.16 161 smmp 818 88 0 (EE) DP 172.16.67.140 55,584 - 192.168.1.16 161 smmp 818 82 0 (EE) DP 172.16.67.125 53,486 - 192.168.1.16 161 smmp 818 82 0 (EE) DP 192.16	CP 10.28.95.3 13.168 Image: CP set of the set o	ГСР	10.28.95.3	11,372	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
DSEFIGP 10.28 95.2 - usergude 64.8 1 48 (C56) DP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.K8 679 0 (EE) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 57.K8 614 0 (EE) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 57.K8 614 0 (EE) DP 172.16.67.132 65,360 - 192.168.1.16 161 smmp 57.K8 567 0 (EE) DP 172.16.67.121 65,380 - 192.168.1.16 161 smmp 8.K8 93 0 (EE) DP 172.16.67.124 55,584 - 192.168.1.16 161 smmp 8.K8 88 0 (EE) DP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8.K8 82 0 (EE) DP 172.16.67.235 59,383	SSPFIGP 10.28.95.3 . 10.28.95.2 . userguide 64.8 1 48 (C56) DP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.48 679 0 (EE) DP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 57.48 614 0 (EE) DP 172.16.67.130 64,463 - 192.168.1.16 161 smmp 57.48 614 0 (EE) DP 172.16.67.120 64,463 - 192.168.1.16 161 smmp 57.48 614 0 (EE) DP 172.16.67.172 57.385 - 192.168.1.16 161 smmp 8.48 93 0 (EE) DP 172.16.67.149 55.584 - 192.168.1.16 161 smmp 8.48 82 0 (EE) JDP 192.168.1.16 161 smmp 8.48 82 0 (EE) JDP 192.168.1.16 161 smmp <	SSPFIGP 10.28.95.3 - 10.28.95.2 - userguide 64.8 1 48 (C56) DP 172.16.6.7.101 61,028 - 192.168.1.16 161 smmp 63.48 679 0 (BE) DP 172.16.6.7.135 61,545 - 192.168.1.16 161 smmp 57.48 614 0 (BE) DP 172.16.6.7.130 64,463 - 192.168.1.16 161 smmp 53.48 56.7 0 (BE) DP 172.16.6.7.121 65,380 - 192.168.1.16 161 smmp 848 93 0 (BE) DP 172.16.6.7.172 57,385 - 192.168.1.16 161 smmp 848 88 0 (BE) DP 172.16.6.7.235 59,383 - 192.168.1.16 161 smmp 848 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 848 82 0 (BE) DP <t< td=""><td>TCP</td><td>10.28.95.3</td><td>13,168</td><td>-</td><td>30.10.10.2</td><td>21</td><td>userguide</td><td>176 B</td><td>4</td><td>0 (BE)</td></t<>	TCP	10.28.95.3	13,168	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
DSPEIGP 10.28.95.3 - - IO.28.95.2 - userguide 64.8 1 48 (CS6) JOP 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.K8 679 0 (BE) JOP 172.16.67.135 61,545 - 192.168.1.16 161 smmp 57.K8 614 0 (BE) JOP 172.16.67.135 64,463 - 192.168.1.16 161 smmp 53.K8 567 0 (BE) JOP 172.16.67.121 65,300 - 192.168.1.16 161 smmp 53.K8 567 0 (BE) JOP 172.16.67.121 65,300 - 192.168.1.16 161 smmp 8.K8 88 0 (BE) JOP 172.16.67.124 55,364 - 192.168.1.16 161 smmp 8.K8 82 0 (BE) JOP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8.K8 82 0 (BE)	DSPEIGP 10.28.95.3 - - IO2.38.95.2 - userguide 64.8 I 48 (Cs6) DP 172.16.6.7.101 61,028 - 192.168.1.16 161 smmp 63.48 679 0 (EE) JDP 172.16.6.7.135 61,545 - 192.168.1.16 161 smmp 53.48 567 0 (EE) JDP 172.16.6.7.132 64,463 - 192.168.1.16 161 smmp 53.48 567 0 (EE) JDP 172.16.6.7.121 65,380 - 192.168.1.16 161 smmp 8.48 93 0 (EE) JDP 172.16.6.7.124 55,384 - 192.168.1.16 161 smmp 8.48 88 0 (EE) JDP 172.16.6.7.235 53,486 - 192.168.1.16 161 smmp 8.48 82 0 (EE) JDP 172.16.6.7.235 59,383 - 192.168.1.16 161 smmp 8.48 82 0 (EE) J	SSPEIGP 10.28.95.3 - i 10.28.95.2 - userguide 64B I 48 (Cs6) D/P 172.16.67.101 61,028 - 192.168.1.16 161 smmp 63.K8 679 0 (PE) D/P 172.16.67.135 61,545 - 192.168.1.16 161 smmp 57.K8 614 0 (RE) D/P 172.16.67.135 64,463 - 192.168.1.16 161 smmp 53.K8 567 0 (RE) D/P 172.16.67.121 65,380 - 192.168.1.16 161 smmp 53.K8 567 0 (RE) D/P 172.16.67.142 55,380 - 192.168.1.16 161 smmp 8.K8 88 0 (RE) D/P 172.16.67.149 55,584 - 192.168.1.16 161 smmp 8.K8 82 0 (RE) D/P 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8.K8 82 0 (RE)	TCP	10.28.95.3	13,168	-	30.10.10.2	21	userguide	176 B	4	0 (BE)
DP 172.16.67.135 61,945 - 192.168.1.16 151 srmp 57/68 614 0 (BE) DP 172.16.67.130 64,463 - 192.168.1.16 161 srmp 53/68 567 0 (BE) DP 172.16.31.121 65,380 - 192.168.1.16 161 srmp 8/68 93 0 (BE) DP 172.16.57.172 57,385 - 192.168.1.16 161 srmp 8/68 88 0 (BE) DP 192.168.0.125 53,466 - 192.168.1.16 161 srmp 8/68 88 0 (BE) DP 192.168.0.125 53,466 - 192.168.1.16 161 srmp 8/68 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8/68 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8/68 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8/68 82 0 (BE) DP 172.16.67.235 59,083 - 192.168.1.16 161 srmp 8/68 82 0 (BE) DP 172.166.161 srmp 8/68 82 0 (BE) DP 172.166.161 srmp 8/68 82 0 (BE) DP 172.166.161 srmp 8/68 82 0 (BE) DP 172.166.16	DP 172.16.67.135 61,945 - 192.188.1.16 161 smmp 57/88 614 0 (EE) DP 172.16.67.130 64,463 - 192.188.1.16 161 smmp 53/88 567 0 (EE) DP 172.16.57.131.121 65,380 - 192.188.1.16 161 smmp 8/88 93 0 (EE) DP 172.16.67.172 57,385 - 192.168.1.16 161 smmp 8/88 88 0 (EE) DP 192.168.0.125 53,466 - 192.168.1.16 161 smmp 8/88 88 0 (EE) DP 172.16.67.255 59,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 192.168.0.125 53,466 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 172.16.67.255 59,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 172.16.67.255 59,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 172.16.67.255 59,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) DP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 8/88 82 0 (EE) UNP 172.16.72.255 199,383 - 192.168.1.16 161 smmp 188 188 189 180 190 190 190 190 190 190 190 190 190 19	DP 172.16.67.135 61,945 - 192.168.1.16 151 snmp 57/88 614 0 (BE) DP 172.16.67.130 64,463 - 192.168.1.16 151 snmp 53/88 567 0 (BE) DP 172.16.31.121 65,380 - 192.168.1.15 151 snmp 8/88 93 0 (BE) DP 172.16.57.172 57,385 - 192.168.1.16 151 snmp 8/88 88 0 (BE) DP 172.16.57.172 55,384 - 192.168.1.16 151 snmp 8/88 88 0 (BE) DP 192.168.0.125 33,486 - 192.168.1.16 151 snmp 8/88 88 2 0 (BE) DP 172.16.57.235 59,383 - 192.168.1.15 151 snmp 8/88 82 0 (BE) DP 172.16.57.235 59,383 - 192.168.1.16 151 snmp 8/88 82 0 (BE) DP 172.16.57.235 59,384 - 192.168.1.16 151 snmp 8/88 82 0 (BE) DP 172.16.57.235 59,384 - 192.168.1.16 151 snmp 8/88 82 0 (BE) DP 172.16.57.235 59,384 - 192.168.1.16 151 snmp 8/88 80	OSPFIGP	10.28.95.3	-	-	10.28.95.2	-	userguide	64 B		48 (CS6)
JDP 172.16.67.130 64,463 - 192.168.1.16 161 srmp 53.KB 567 0 (BE) JDP 172.16.7127 57,385 - 192.168.1.16 161 srmp 8.KB 93 0 (BE) JDP 172.16.7127 57,385 - 192.168.1.16 161 srmp 8.KB 88 0 (BE) JDP 172.16.7140 55,584 - 192.168.1.16 161 srmp 8.KB 88 0 (BE) JDP 172.16.725 53,465 - 192.168.1.16 161 srmp 8.KB 88 0 (BE) JDP 172.16.725 59,383 - 192.168.1.16 161 srmp 8.KB 82 0 (BE) 	DDP 172.16.67.130 64,463 - 192.168.1.16 161 srmp 53.168 567 0 (BE) DDP 172.16.7127 57,385 - 192.168.1.16 161 srmp 8.165 88 0 (BE) DDP 172.16.67.170 55,584 - 192.168.1.16 161 srmp 8.165 88 0 (BE) DDP 192.168.0.125 53,486 - 192.168.1.16 161 srmp 8.168 88 0 (BE) DDP 192.168.0.125 53,486 - 192.168.1.16 161 srmp 8.168 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 8.168 82 0 (BE) ADP 172.168.175 167 82 82 82 82 82 82 82 80 (BE) ADP 172.168.175 167 82 82 82 82 82 80 (BE) ADP 172.168.175 167 82 82 82 80 (BE) ADP 172.168.175 167 82 82 82 80 (BE) ADP 172.168.175 167 82 82 80 (BE) ADP 172.168.175 167 82 82 80 (BE) ADP 172.168.175 167 82 82 80 (BE) ADP 172.168.175 172 82 82 80 (BE) ADP 172.168.175 172 82 82 80 (BE) AD	DPP 172.16.67.130 64,463 - 192.168.1.16 161 srmp 53.48 567 0 (BE) DP 172.16.131.121 65,380 - 192.168.1.16 161 srmp 848 93 0 (BE) DP 172.16.67.172 57,385 - 192.168.1.16 161 srmp 848 88 0 (BE) DP 172.16.57.149 55,584 - 192.168.1.16 161 srmp 848 88 0 (BE) DP 172.16.7.235 53,486 - 192.168.1.16 161 srmp 848 82 0 (BE) DP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 848 82 0 (BE) DP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 848 82 0 (BE) DP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 848 82 0 (BE) DP 172.16.7.235 59,383 - 192.168.1.16 161 srmp 848 82 0 (BE) A A A A A A A A A A A A A A A A A A A	JDP	172.16.67.101	61,028	-	192.168.1.16	161	snmp	63 KB	679	0 (BE)
DP 172.16.131.121 65,380 - 192.158.1.16 161 srmp 8 KB 93 0 (BE) DP 172.16.57.172 57,385 - 192.158.1.16 161 srmp 8 KB 88 0 (BE) DP 192.168.0.125 53,465 - 192.158.1.15 161 srmp 8 KB 88 0 (BE) DP 172.16.57.235 59,383 - 192.158.1.16 161 srmp 8 KB 82 0 (BE) DP 172.16.57.235 59,383 - 192.158.1.16 161 srmp 8 KB 82 0 (BE) V T	DP 172.16.67.172 57,385 - 192.168.1.16 151 srmp 8 K8 93 0 (BE) DP 177.16.67.172 57,385 - 192.168.1.16 161 srmp 8 K8 88 0 (BE) DP 192.168.0.125 53,486 - 192.168.1.16 151 srmp 8 K8 88 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 K8 82 0 (BE) ADP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 K8 82 0 (BE) ADP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 K8 82 0 (BE) K Local L	DDP 172.16.131.121 65,380 - 192.168.1.16 161 srmp 8 K8 93 0 (BE) DP 172.16.67.172 57,385 - 192.168.1.16 161 srmp 8 K8 88 0 (BE) DP 192.168.0.125 53,486 - 192.168.1.16 161 srmp 8 K8 88 0 (BE) DP 192.168.0.125 53,486 - 192.168.1.16 161 srmp 8 K8 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 K8 82 0 (BE) V V V T	JDP	172.16.67.135	61,545	-	192.168.1.16	161	snmp	57 KB	614	0 (BE)
DP 172.16.57.172 57,385 - 192.168.1.16 151 srmp 8 KB 93 0 (BE) DP 172.16.57.172 57,385 - 192.168.1.16 151 srmp 8 KB 88 0 (BE) DP 192.168.0.125 53,465 - 192.168.1.16 151 srmp 8 KB 88 0 (BE) DP 192.168.0.125 53,465 - 192.168.1.16 151 srmp 8 KB 82 0 (BE) DP 172.16.57.235 59,383 - 192.168.1.16 161 srmp 8 KB 82 0 (BE) V V V V V V V V V V V V V V V V V V V	DP 172.16.67.172 57,385 - 192.168.1.16 151 smp 8 K8 93 0 (BE) DP 172.16.67.172 57,385 - 192.168.1.16 151 smp 8 K8 88 0 (BE) DP 172.16.67.140 55,584 - 192.168.1.16 151 smp 8 K8 88 0 (BE) DP 192.168.0.125 53,466 - 192.168.1.16 151 smp 8 K8 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smp 8 K8 82 0 (BE) A to the second	DPP 172.16.67.172 57,385 - 192.168.1.16 151 smmp 8 K8 93 0 (BE) DP 172.16.67.172 57,385 - 192.168.1.16 151 smmp 8 K8 88 0 (BE) DP 192.168.0.125 53,465 - 192.168.1.16 151 smmp 8 K8 88 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smmp 8 K8 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smmp 8 K8 82 0 (BE) V V V C V V C V V V V V V V V V V V V V	JDP	172.16.67.130	64,463	-	192.168.1.16	161	snmp	53 KB	567	0 (BE)
DP 172.16.67.172 57,365 - 192.163.1.16 161 srmp 8 KB 88 0 (BE) DD 172.16.67.140 55,584 - 192.163.1.16 161 srmp 8 KB 88 0 (BE) DP 192.163.0.125 53,466 - 192.163.1.16 161 srmp 8 KB 82 0 (BE) DD 172.16.67.235 59,383 - 192.163.1.16 161 srmp 8 KB 82 0 (BE) DD 172.16.67.235 59,383 - 192.163.1.16 161 srmp 8 KB 82 0 (BE) Local Local Local Local Local Local Local	DP 172.16.67.172 57,385 - 192.168.1.16 161 srmp 8 KB 88 0 (BE) DP 172.16.67.149 55,584 - 192.168.1.16 161 srmp 8 KB 88 0 (BE) DP 192.168.0.25 53,486 - 192.168.1.16 161 srmp 8 KB 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 KB 82 0 (BE) A the state of the sta	DP 172.16.67.172 57,385 - 192.168.1.16 151 smp 8 K8 88 0 (BE) DP 172.16.67.140 55,584 - 192.168.1.16 151 smp 8 K8 88 0 (BE) DP 192.168.0.25 53,486 - 192.168.1.16 151 smp 8 K8 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smp 8 K8 82 0 (BE) A total tota	JDP	172.16.131.121		-	192.168.1.16	161		8 KB	93	
JDP 172.16.67.140 55,584 - 192.168.1.16 161 srmp 8 KB 88 0 (BE) JDP 192.168.0.125 53,486 - 192.168.1.16 161 srmp 8 KB 82 0 (BE) JDP 172.16.67.235 59,383 - 192.168.1.16 161 srmp 8 KB 82 0 (BE) ✓	DP 172.16.67.149 55,584 - 192.168.1.16 151 srmp 8 K8 88 0 (EE) DP 192.168.0.125 53,486 - 192.168.1.16 151 srmp 8 K8 82 0 (EE) DP 172.16.67.235 59,383 - 192.168.1.16 151 srmp 8 K8 82 0 (EE) ∢ Local	DP 172.16.67.149 55,584 - 192.168.1.16 151 smmp 8.K8 88 0 (EE) DP 192.168.0.125 53,486 - 192.168.1.16 151 smmp 8.K8 82 0 (EE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smmp 8.K8 82 0 (EE) ∢	JDP			-						
DP 192.168.0.125 53,485 - 192.168.1.16 151 srmp 8 KB 82 0 (BE) DP 172.16.67.235 59,383 - 192.168.1.16 151 srmp 8 KB 82 0 (BE)	DP 192.168.0.125 53,486 - 192.168.1.16 151 smmp 8 K8 82 0 (EE) DP 172.16.67.235 59,383 - 192.168.1.16 151 smmp 8 K8 82 0 (EE) ✓ Local Local Local Local Local Local Local Local	DP 192.168.0.125 53,465 - 192.168.1.16 161 snmp 8 K8 82 0 (EE) DP 172.16.67.235 59,383 - 192.168.1.16 161 snmp 8 K8 82 0 (EE) 	JDP			-						
DP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8 KB 82 0 (BE) ✓ Local Locad Local Local Local Loca	UDP 172.16.67.235 59,383 - 192.168.1.16 161 smmp 8 K8 82 0 (BE)	UDP 172.16.67.235 59,383 - 192.168.1.16 161 smp 8 K8 82 0 (9E)				-						
Local Cocal Cocal Faoining	Local	< International Control C				-						
Local Control	Local Cocal	Local C C C C C C C C C C C C C C C C C C C			,							- ()
		Fa0/1/0					snmp				Local	Apr X
userguide												
userguide	the second s											
userguide												

The custom application can also be configured directly from either the flow table in the device view or in the System Flow Table.

Right click on a flow in the flow table and click on Define custom application based on flow...to bring up the Define Custom Application window.

۹ 🕲	Enable Polling Day	ise Display Basic F	low 👻 🔄	*DefaultFilterGroup	👻 📑 Dis	olay Filter C	olors 👻	End Points: Applic	ation 🔻 🕓 Playback	Reports
col	Src IP Addr	Src Port	Src Cntry	Dst IP Addr	Dst Port	Applicat	v 1 ion	In Bytes	In Packets	Src DSCP
	10.28.95.3	39,508	-	30.10.10.2	21	userguid	e	176 B	4	0 (BE)
	10.28.95.3	49,868	-	30.10.10.2	21	userguid	e	176 B	4	0 (BE)
	10.28.95.3	49,868	-	30.10.10.2	21	userguid	e	176 B	4	0 (BE)
	172.16.67.101	61,028	-	192.168.1.17	161	snmp		58 KB	634	0 (BE)
	172.16.67.135	61,545	-	192, 168, 1, 17	161	snmp		40.100	FOF	le (TE)
	172.16.67.130	64,463	-	192.168.1.17	161	snmp	Report	ts		► E)
	172.16.131.121	65,380	-	192.168.1.17	161	snmp	Gener	ate Web Report		E)
							Export	Flow Data		
							Define	custom applica	tion based on flow	
							Execut	te Mediatrace		
							Create	Display Filter		+
		Fa0/0/1		Local			Add to	Current Display	Filter	+

Right click on a flow in the System Flow Table and click on Define custom application based on flow... to bring up the Define Custom Application window.

Applic	ation (AVC) Ba	sic Flow Medianet	NSEL						
Color	Protocol	Src IP	Src Port	Src Country	Dst IP	Dst Port	Dst Country	App Name	0
	TCP	10.255.203.2	80	-	10.255.203.6	55,481	-	youtube (13	0 (
	TCP	10.255.203.2	80	-	10.255.203.6	55,465	-	youtube (13	0 (
	TCP	10.255.203.2	80	-	10.255.203.6	55,477	-	youtube (13	0 (
	TCP	10.255.203.2	80		10.255.203.6	55,475	-	youtube (13	0 (
	TCP	10.255.203.6	55,481	-	10.255.203.2	80	-	youtube (13	00
	TCP	10.255.203.6	55,465	-	10.255.203.2	80	-	youtube (13	0 (
	TCP	10.255.203.6	55,477		10.255.203.2	80	-	youtube (13	00
	TCP	10.255.203.6	55,475		10.255.203.2	80	-	youtube (13	0 (
	TCP	10.28.95.3	51,490	-	30.10.10.2	21	US/Unite	userguide	0 (
	TCP	10.28.95.3	45,635	-	30.10.10.2	21	US/Unite	userguide	0 (
	TCP	10.28.95.3	27,252		30.10.10.2	21	US/Unite	userguide	00
	TCP	10.28.95.3	19,551	-	30.10.10.2	21	US/Unite	userquide	0 (
	TCP	10.28.95.3	17,860	-	30.10.10.2		US/Unite		0 (
	TCP	10.28.95.3	63,708		30, 10, 10, 2		US/Unite		0 0
	OSPFIGP	10.28.95.3	-	-	224.0.0.5		-	userquide	48
	LIDP	10.255.203.6	2,091	-	10.255 203 2	5 004	-	unknown (13	0.0
	TCP	10.255.203.2	3,389	-	10.255	Define custom	application bas	sed on flow	
	TCP	10.255.203.2	61,680		10.255				
	TCP	10.255.203.6	48,219	-	10.255	Add 10.255.203.	2 to IP Blacklis	t	
	UDP	10.255.203.6	24,404	-	10.255	Add 10.255.203	2 to IP Mappir	g	
	UDP	10.255.203.2	24,576		10.255	Copy 10.255.20	2.7 to cliphoar	-	
	TCP	10.255.203.2	80	-	10.255	Copy 10.200.20	5.2 to cirpooard	-	
	TCP	10.255.203.6	52,255	-	10.255	Export Flow Dat	te		
	UDP	10.255.203.10	1,604		10.0.0.2	10,222	-	unknown (13	9
	TCP	10 255 203 6	55 436		10 255 203 2	80	-	unknown (13	0.0

In both these cases, the Define Custom Application window automatically fills in the IP Address and the Port field based on that particular flow's destination IP address and destination port.

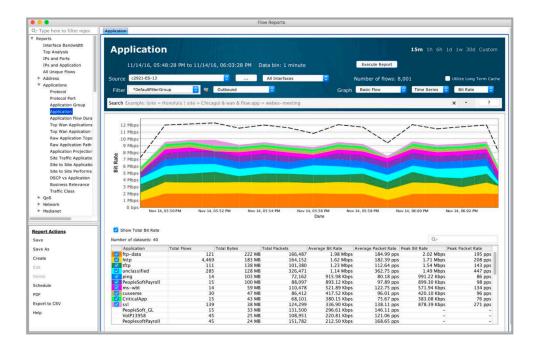
Define Cu	ustom Application					
Name:	userguidenew					
Description:	another example for the user manual					
IP Address:	Specifiy IP ranges (ex: 192.168.1.1-200) or one IP per line 10.255.203.2					
Port:	5004 Layer 4 Protocol: UDP 🗸					
Mana	Manage Custom Applications Save Cancel					

Click on Save and the new application name is visible in the flow table.

Amir	ation (AVC) Ba	sic Flow Mediane							
Color	Protocol	Src IP	Src Port	Src Country	Dst IP	DstPort	Dat Country	App Name	DS
	TCP	10.255.203.2	80	-	10.255.203.6	55,475	-	youtube (13	0.0
	TCP	10.255.203.6	55,481	-	10.255.203.2	80	-	youtube (13	00
	TCP	10.255.203.6	55,465	-	10.255.203.2	80	-	youtube (13	0 (
	TCP	10.255.203.6	55,477	-	10.255.203.2	80	-	youtube (13	0 (
	TCP	10.255.203.6	55,475	-	10.255.203.2	80	-	youtube (13	0 (
	UDP	10.255.203.6	2,091	-	10.255.203.2	5,004	-	userguidenew	0 (
	TCP	10.28.95.3	51,490	-	30.10.10.2	21	🚾 US/Unite	userguide	0 (
	TCP	10.28.95.3	45,635	-	30.10.10.2	21	🚾 US/Unite	userguide	0 (
	TCP	10.28.95.3	27,252	-	30.10.10.2	21	🚾 US/Unite	userguide	0 (
	TCP	10 28 95 3	19 551	-	30 10 10 2	21	🚾 US/Unite	usernuide	0.0

The defined custom application name appears in the Top Analysis and the Applications flow reports under Applications.

••				Flow Reports				
- Type here to filter repoi	Top Analysis							
Reports								
Interface Bandwidth	- EI = I = I = I = I = I = I = I = I = I							
Top Analysis	Top Analys	is					15m 1h 6h 1d 1w 30d	
IPs and Ports							_	
IPs and Application	11/14/16, 05:4	7:23 PM to 11/14	/16, 06:02:2	13 PM		Execute Report		
All Unique Flows				<u> </u>				
Address	Source c2921-ES-13		٠.	All Interfaces	\$	Number of flows	: 5,000+ 🔤 csv	/ File Result
Applications	and the second			THE R. P. LEWIS CO., LANSING MICH.	ALC: NOT			
Protocol	Filter *DefaultFilterGre	sup 😒 🖷	Outbound	0		Basic Flow	Time Sorted - Unique	Flows 🗘
Protocol Port	The second s							
	Search Example: (site = H	onolulu site = Ch	icado) & wan &	flow.app = webex-meeting			× •	?
Application Group	search example. (site = it	onorara i site = cii	cugo, a waite	nomapp - nebex-meeting			~	<u> </u>
Application								
Application Flow Dura							Q	
Top Wan Applications	Time Protocol	Src IP Addr	Src Port	Dst IP Addr Dst Port	Application	Flow Record Co Bit Rate	Packet Rate Src Country	Dst Cor
Top Wan Appilcation	Nov 14, 2016 ICMP	192.168.12.2	0	192.168.15.2 0	ping	1 974.19 Kbr		-
Raw Application Topo	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.274	http	1 18.43 Kbr		-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 4.299	Maxis Server**	1 384.00 br		-
Raw Application Path	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 50.861	ssl	1 308.99 Kbr		-
Application Projection	Nov 14, 2016 UDP	192,168,12,2		192.168.15.2 19.420	rtp	1 74.71 Kbr		-
Site Traffic Applicatio	Nov 14, 2016 UDP	192.168.12.2	53	192.168.15.2 61.148	dns	1 3.90 Kbr		-
Site to Site Applicatio	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4.287	http	1 46.82 Kbr		-
Site to Site Performa	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 4.293	http	1 38.52 Kbr		-
DSCP vs Application	Nov 14, 2016 TCP	192.168.12.2	15.255	192.168.15.2 4.111	unclassified	1 320.00 br		-
	Nov 14, 2016 UDP	10.0.12.2	1.027	8.8.8.1 69	tftp*	1 500.32 Kbr		US/
Business Relevance	Nov 14, 2016 TCP	192.168.12.2	61.623	192.168.15.2 37.555	PeopleSoft P	1 757.47 br		-
Traffic Class	Nov 14, 2016 TCP	192.168.12.2	37,555	192.168.15.2 61,623	PeoplesoftPa	1 2.13 Kbr	os 0.92 pps -	-
▶ QoS	Nov 14, 2016 TCP	192.168.12.2	61,682	192.168.15.2 9,435	Eds_Tablet_D			-
Network	Nov 14, 2016 TCP	192.168.12.2	9,435	192.168.15.2 61,682	PeoplesoftPa	1 458.18 br	os 0.91 pps -	-
Medianet	Nov 14, 2016 UDP	10.0.12.2	16,386	8.8.8.4 16.384	unclassified	1 60.22 Kbr	s 33.02 pps -	US/
Prediamer	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,166	http	1 6.65 Kbr	4.26 pps -	-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,167	http	1 12.28 Kbp	4.31 pps -	-
	Nov 14, 2016 UDP	192.168.12.2	53	192.168.15.2 52,636	dns	1 3.90 Kbp	o.00 pps -	-
port Actions	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,174	http*	1 320.00 br	os 0.00 pps -	-
ve	Nov 14, 2016 UDP	192.168.12.2		192.168.15.2 58,674	dns	1 3.82 Kbr		-
~	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,171	http*	1 320.00 br		-
ve As	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,190	http*	1 320.00 bp		-
	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,172	http*	1 320.00 bp		-
eate	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,208	secure-http*	1 314.00 Kbp		-
t	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,220	secure-http*	1 44.86 Kbp		-
	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,204	secure-http*	1 160.00 Kbp		-
lete	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,175	http*	1 320.00 br		-
hedule	Nov 14, 2016 TCP	192.168.12.2	80	192.168.15.2 2,178	http*	1 320.00 br		-
	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,199	secure-http*	1 104.67 Kbp		-
F	Nov 14, 2016 TCP	192.168.12.2		192.168.15.2 2,197	secure-http*	1 98.50 Kbp		-
port to CSV	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,200	secure-http*	1 98.50 Kbp		-
	Nov 14, 2016 TCP	192.168.12.2	443	192.168.15.2 2,201 192.168.15.2 2,210	secure-http* secure-http*	1 157.00 Kbp 1 143.00 Kbp		-
	Nov 14, 2016 TCP	192.168.12.2						



DNS Name Resolution

The DNS Name Resolution features allows the display of host names associated with the IP addresses in LiveNX. An admin user can enable DNS Name Resolution by selecting Tools > Enable DNS Resolution (Global).

Too	ls	Reporting	Window	Dev	Help
	۷	iew Alerts			
	С	onfigure Aler	ts		
	۷	iew Advisorie	s		
~	U	se IP Mappin	gs		
	E	dit IP Mappin	igs		
~	U	se IP Blacklist	t		
	E	dit IP Blacklis	t		
	Ν	ISI Endpoints			
	Ρ	ort Assignme	ents		
	E	nable DNS Re	solution (G	lobal)	
	S	how DNS Nar	mes		
	D	evice Tools			•
	St	tatistics			•
	G	roup Manage	ement		•
	0	ptions			

Once enabled, a check box will appear next to the Enable DNS Resolution (Global). To disable, select Tools > Enable DNS Resolution (Global). Prior to enabling DNS resolution, an alert appears to warn you that this may increase the amount of NetBIOS traffic from the server.

Enable D	NS Resolution
	Enabling DNS resolution may result in increase NetBIOS traffic from the server. It is recommend that NetBIOS be disabled when using this feature.
	NetBios can be disabled under the advance settings of the Inerface Protocol Version Properties for the appropriate interface.
	OK Cancel

To disable NetBIOS for Windows7 operating systems, open the Network and Sharing Center in the Control Panel. Click on the appropriate Local Area Connection. Click on Properties, then TCP/IPv4, then Properties. Click on Advanced and then go to the WINS tab and select Disable NetBIOS over TCP/IP. Click on OK.

Advanced TCP/IP Settings	? ×
IP Settings DNS WINS	
WINS addresses, in order of use:	
Add Edit	Remove
If LMHOSTS lookup is enabled, it applies to all o TCP/IP is enabled.	connections for which
Enable LMHOSTS lookup	Import LMHOSTS
NetBIOS setting Default: Use NetBIOS setting from the DHCP set is used or the DHCP server does not pr enable NetBIOS over TCP/IP. Enable NetBIOS over TCP/IP Disable NetBIOS over TCP/IP	
[OK Cancel

To disable NetBIOS for Windows Server operating systems, open the Server Manager and select Tools > System Configuration in the Menu Bar. Go to the Services tab and disable TCP/IP NetBIOS Helper. Click on OK.

Seneral	Boot		Startup T	ools				
Servic	e			Manufacturer		Status	Date Disabled	~
🖌 Wo	orkstatio	n		Microsoft Corporation	n	Running		
🖌 Lin	k-Layer	Topology Di	scovery	Microsoft Corporation	n	Stopped		
🗌 ТС	P/IP Net	BIOS Helpe	r	Microsoft Corporation	n	Running		
🖌 Loo	al Sessi	on Manager		Microsoft Corporation	n	Running		
🖌 Mu	ltimedia	Class Sched	luler	Microsoft Corporation	n	Stopped		
🖌 Wi	ndows F	irewall		Microsoft Corporation	n	Running		
🖌 Dis	tributed	Transaction	n Coordin	Microsoft Corporation	n	Running		
🖌 Mic	rosoft is	SCSI Initiato	r Service	Microsoft Corporation	n	Stopped		
🖌 Wi	ndows I	nstaller		Microsoft Corporation	n	Stopped		
🖌 🖌 Wi	ndows I	nternal Data	abase	Microsoft Corporation	n	Running		
🖌 Ne	twork A	ccess Protec	tion Agent	Microsoft Corporation	n	Stopped		
🖌 Ne	twork C	onnectivity	Assistant	Microsoft Corporation	n	Stopped		\sim
		secure Micr		es may not be disabled	l.	Enable	all Disable	all

Once DNS Resolution is enabled, any user role can select Tools > Show DNS Names to show hostnames in the flow views (system and device view topology, flow tables, lists and reports).

Too	Is Reporting Help							
	View Alerts							
	Configure Alerts							
	View Advisories							
 Image: A start of the start of	Use IP Mappings							
	Edit IP Mappings							
 Image: A start of the start of	Use IP Blacklist							
	Edit IP Blacklist							
	Port Assignments							
	Enable DNS Resolution (Global)							
~	Show DNS Names							
	Device Tools	1º						
	Statistics	•						
	Group Management	•						
	Options							

Device Tools

Saving Changes to the Device's Startup Configuration

When a device is added to LiveNX, the software makes changes automatically to the device's running configuration, but not to the startup configuration file. If you want to make these changes permanent, select the device from the list on the left side of the LiveNX screen, and then select Save to Startup Config from the File menu and click Yes to save them to the startup configuration file.

Si	Save Startup Config - c2921SCOPE_1-17.referentia.com (192.168.1.17)						
	Would you like to save the current running configuration to the device's startup config, i.e., "copy run start"?						
	Do not show again (current configuration will not be saved to startup configuration on further use)						
	Yes No						

Accessing the Device Web Page from LiveNX

If your device supports it, LiveNX can open its internal web page. Select Open Device Web Page from the Tools menu.

Note Administrator or Full Configuration privileges are needed to open and use the LiveNX CLI terminal window.

-	Reporting Help View Alerts	1			Sang Hander L About 1 Kalf	- • •
	Configure Alerts	-	DefaultFilterGroup			cisco
	View Advisories Use IP Mappings	Cntry		D	Taska C Oversitere LAN	
	Edit IP Mappings		172.16.67.113	77 77	gP Basic Configuration	
	Use IP Blacklist		172.16.67.113	77	LAV Total Supported LAN: 3 Configured LAN Interface: 3	
	Edit IP Blacklist		172.16.67.113	77	Ø neval	
	Port Assignments Enable DNS Resolution (Global)		172.16.67.113 172.16.67.113	77 77 77	Git curce 協いAT	
	Show DNS Names		172.16.67.113		Windows Security	
	Device Tools		Save to Startup Config		The server 172.16.67.112 at level_15_access requires a username and Total WARConnections: 0	
	Statistics	-	Open Device Web Page	2	password.	
	Group Management	•	Manage ACLs	.he	Warning: This server is requesting that your username and password be	
	Options				sent in an insecure manner (basic authentication without a secure connection).	
					Firewait: Not Configured	
					User name Password	
					Remember my credentials	
					OK Cancel 012259 UTC Sar Au	g 18 2012

Managing ACLs

LiveNX includes an Access Control List (ACL) editor that allows you to edit and create ACL rules for use with QoS match capabilities. The ACL editor also provides an option to save and load ACLs from a file. The ACL Management dialog box can be accessed from Tools > Manage ACLs.

ACL Management for 1811-1	3		<u> </u>
Current Router 1811-13			
Access Control Lists (ACLs)		
Name / Number	Туре	Applied Interfaces	Create ACL
deny_199	Standard (Named)		Edit ACL
			Delete ACL
			Copy ACL
			Apply / Remove ACL
Access Rule Entries			
deny host 192.168.1.199			Save ACL File
			Load ACL File
			Close
			Close

To create an ACL, click on Create ACL.

Create ACL		×
Name (Number	tandard tandard tandard tanded	Help
Remarks		
remark deny 192.168.1.19	99	Create Remark
		Edit Remark
		Remove Remark
Access Rules		
		Create Rule
		Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
	Preview CLI	Save to Device Cancel

Choose between Standard or Extended. Standard uses ACL numbers between 1-99 or 1300-1999. Extended uses ACL numbers between 100-199 or 2000-2699. Alphanumeric characters are allowed in the Name/Number field with no blank spaces.

Click on Create Remark to create a remark for the ACL.

Click on Create Rule to create access rules to allow or to deny a particular IP address. Two windows are available to create or to edit rules, depending on whether a Standard or an Extended ACL was created.

For the standard ACL rule, create a rule by selecting permit or deny, and selecting the desired source IP address for this rule.

Add Standard Rule Entry for deny_199	
💿 permit 🔘 deny	
Source	
any O by Network or IP	
e.g 192.168.1.0/24 or 192.168.1.19	
🔄 Log Rule	
	OK Cancel

For the extended ACL rule, additional selections are available. In addition to permit or deny, other selections include protocol (IP, TCP or UDP), Object-Group or by IP protocol name (ahp, eigrp, esp, gre, icmp, igmp, ip, ipinip, nos, ospf, pcp, pim tcp or upd) or IP protocol number.

Edit Extended Rule Entry for DMVPN-other-13958	
ermit	
⑦ IP ◎ TCP ⑧ UDP ◎ Object-Group serviceObject → ◎ Other by N	y Name v lahp v
Source	Destination
💿 any 💿 by Network or IP 💿 by Object-Group	● any ● by Network or IP ● by Object-Group
e.g 192.168.1.0/24 or 192.168.1.19 destinationNetworkObject 👻	>> e.g 192.168.1.0/24 or 192.168.1.19 destinationNetworkObject +
by Port Equal to Manage Port(s)	Ø by Port Equal to ✓ Manage Port(s)
13959 sourceNetworkObject	<< 13958
networkObject	
Match by DSCP v	
Log Rule Log v	
	OK Cancel

LiveNX reads the Object-Group information already created in the device configuration and displays any available selections through the drop-down.

The by Port selection is available if either TCP or UDP is selected. Options are equal, not equal, greater than, less than or between. The Manage Port(s) button provides a list of commonly used ports. Different rules can be created for Source and Destination. Use the >> if you would like to copy the Source parameters to the Destination side and use the << if you would like to copy the Destination parameters to the Source side.

Click on Match to select traffic based on DSCP or on IP precedence. Default is off.

Click on Log Rule and select either Log to Log matching packets or Log Input to Log the ingress interface and source MAC address, in addition to the packet's source and destination IP address and ports. Default is off. Click on Preview CLI to see the commands in CLI format prior to saving it to the device. Click on Save to Device to transmit the CLI commands to the device. Click on Cancel to close the window without making a change to the ACL rules.

Preview CLI	
<pre>config t ip access-list resequence DMVPN-other-13958 10 10 ip access-list extended DMVPN-other-13958 no 10 permit 17 any eq 13958 any eq 13958 10 permit object-group serviceObjectChild object-group networkObjectChild any </pre>	*
Close	

Once a rule is created for the ACL, highlight the rule to edit, copy or delete the created rule. Repeat the Create Rule to add additional access rules for a given Access Control List. Rules are executed in the order from the top down, so highlight a rule in the list and use the Move Up or Move Down button to reorder the rules in the Access Rules window.

Edit Extended ACL DM	VPN-bgp-179	×
Туре	Extended 👻	
Name / Number	DMVPN-bgp-179	Help
Remarks		
		Create Remark
		Edit Remark
		Remove Remark
Access Rules		
permit udp any eq 179 permit tcp any eq bgp a		Create Rule
permit top any eq ogp t	אוז כק טפָר	Edit Rule
		Copy Rule
		Delete Rule
		Move Up
		Move Down
·	Preview CLI Save	to Device Cancel

Once the Access Control List is saved to the device, click on Apply/Remove ACL.

CL Management for 181	1-13		X
Current Router 1811-1	3		
Access Control Lists (A	CLs)		
Name / Number	Туре	Applied Interfaces	Create ACL
deny_199	Standard (Named)		Edit ACL
			Delete ACL
			Copy ACL
			Apply / Remove ACL
Access Rule Entries			
leny host 192.168.1.199			Save ACL File
			Load ACL File
			·

The Apply Access List to Interface window automatically lists all interfaces on that device. Click on the desired interface to apply the interface to, select Inbound Direction and/or Outbound direction and click on Apply Access List to Selected Interface to designate the desired ACL. The UI will ask if you are sure before modifying the interface configuration.

Apply Access List to Inte	rface		×
Access-List to Apply	deny_199	•	
Async1 FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet5 FastEthernet6 FastEthernet7 FastEthernet8 FastEthernet9 Loopback1	E	 Inbound Direction Access List applied: Dutbound Direction Access List applied: 	Remove none Remove none
	Apply Access	List to Selected Interface	Cancel

For a QoS policy that uses an ACL as part of its class definitions, the ACL will automatically be included when loading and saving QoS policy files; it is not necessary to load and save the ACL file separately.

To load an ACL file from one device to another, save the ACL to a file and then open the editor on the target device. Then, load the ACL file and save it to the device. LiveNX will warn if there are any conflicts.

Current Router	2921-Dem	10-67_112			
Access Contro	l Lists (ACL	_s)			
Name / Number	^	Туре	Applied Interfaces		Create ACL
ACL-IPSLAVO-60		Extended (Named)			
BlockAttack		Extended (Named)	GigabitEthernet0/2	-	Edit ACL
BlockBGP		Extended (Named)	orgabilization conje		Delete ACL
BlockFlow		Extended (Named)			Delete ACL
MACE-ACL		Extended (Named)			Copy ACL
match-13958		Extended (Named)			
Redirect		Extended (Named)		E	Apply / Remove ACL
RedirectFlow		Extended (Named)			
StopVoice		Extended (Named)			
TO-4EYES		Extended (Named)			
TO-AGENCY		Extended (Named)			
TO-COALITION		Extended (Named)			
TO-SIPR-130		Extended (Named)			
video-flow		Extended (Named)		*	
video-flow Access Rule Er	ntries	Extended (Named)			Save ACL File

Statistics

Miscellaneous OID Polling and Charting

Miscellaneous OID polling utilizes a generic polling framework within LiveNX to gather vendor-specific or miscellaneous device information and statistics. From the Tools menu, select Statistics > Manage Custom OID Charts and enter in the OID string. Polled data and charts are accessed by going to the Tools menu and selecting Statistics > Show Custom OID Charts.

View Alerts					10-1
Configure Alerts View Advisories		*DefaultFilterGroup	- 1	Name Units 1.2 Interested interface Used padiets	Ad Ed Rem
I Use ID Manual and	: Cntry	Dst IP Addr	Dst Port		Ken
Use IP Mappings		172.16.67.113	771	T Edit Custom OID	
Edit IP Mappings		172.16.67.113	771	and the second se	
Use IP Blacklist		172.16.67.113	771		
Edit IP Blacklist	_	172.16.67.113	771	Name interested interface Licast	
Edit IP Diacklist	_	172.16.67.113	771	Units packets	
Port Assignments	-	172.16.67.113	771	OK Cancel	
Enable DNS Resolution (Global)	_	172.16.67.113	771		
Show DNS Names		1/2.16.67.113			
Device Tools			•		
Statistics	Show	Interface Details			
Group Management	Show	All Interfaces		OK	Can
Options	Show	ACL Statistics			

Miscellaneous Oll	D Polling				🗖 🕑
olled Device/Field:			(×
			(pkts)		
			(prics)		1,808,025,
					1,808,000,
					1,807,975,
					1,807,950,
					1,807,925,.
					1.807,900,.
					1,807,875,.
10:28:09 AM	10:30:09 AM	10:32:09 AM	10:34:09 AM	10:36:09 AM	10:38:09 AM
olled Device/Field:			())		~
			(packets)		315,540,000
					315,535,000
					315,530,00
					315,525,00
					315,520,00
10:28:09 AM	10:30:09 AM	10:32:09 AM	10:34:09 AM	10:36:09 AM	315,515,00 10:38:09 AM
olled Device/Field:			Miscellaneous Devic		~
				(pkts) (packe	5)
02:00:00 PM	02:00:00 PM	02:00:00 PM	02 00 30 PM	02.00.00 PM	02.00.00 PM
olled Device/Field:					
02:00:00 PM	02:00:00 PM	02:00:00 PM	02:00:00 PM	02:00:00 PM	02:00-00 PM
		12.20.00 110	22.20.00 1 11		22.20.00 T M

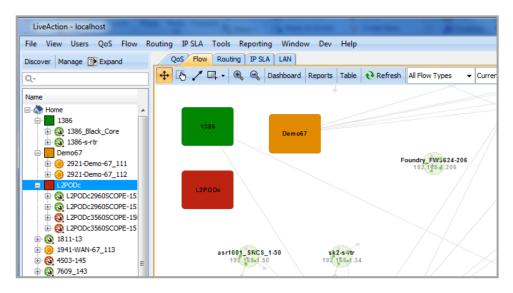
Group Management

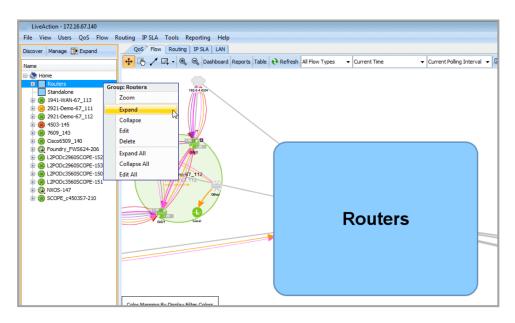
File View Users QoS Flow	Routing IP SLA	_		-								
Niscover Manage 🗈 Expand	QoS Flow		View Alerts									
			Configure Alerts	-	DefaultFilterGroup	- 1	Display Filter Colors 👻	End Points: IP Address	- ()	layback Ca Report		
Name	A1		View Advisories									
- A Home	Protocol		Use IP Mappings	Cntr		Dst Port	Application	TCP Flags	Src Prefix Len	In IF	Dst P	ref
- Standalone	ICMP				192.0.2.35	771		——A——	24	GigabitEthernet0/0		
😐 🛞 1941-WAN-67_113	ICMP		Edit IP Mappings		172.16.67.113	769		——A——	24	FastEthernet0/1/0		0
🗄 🋞 2921-Demo-67_111	ICMP	~	Use IP Blacklist		172.16.67.113	2,048		——A——	24	FastEthernet0/1/0		
B @ 2921-Demo -67_112	ICMP		Edit IP Blacklist		172.16.67.113	-		——A——	24	FastEthernet0/1/0		
H 4503-145	ICMP		Edit IP blacklist		172.16.67.113	-		——A——	24	FastEthernet0/1/0		
Image: Book and the second	ICMP		Port Assignments		172.16.67.113	2,816		A	24	FastEthernet0/1/0		
et2960SCOPE_1-14	ICMP		Enable DNS Resolution (Global)	-	172.16.67.113	2,816		A	24	FastEthernet0/1/0		
General Control Contro	ICMP <			-	172.16.67.113	771		—A—	24	FastEthernet0/1/0	24	
e- 🛞 cat3560X-67_107	•		Show DNS Names	-								,
e Gerat Control Co			Device Tools			-			/		¥.	1
General Control (1998) General Contr			Statistics >	-					52	4.1M		\leq
E- Osco6509_140									KUN.			
Foundry_FWS624-206			Group Management		Edit Groups				Other	A Gon	101	
E 2PODc2960SCOPE-152			Options		63		Gi0/1			0.0		
E2PODc2960SCOPE-153			options	-	Expand All Groups		GIU/1					۱.
L2PODc3560SCOPE-150			n		Collapse All Groups	192.0.2.25	192.0.1.1					۱.
E 00 L2PODc3560SCOPE-151	· · · · ·					192.0.2.25	192.0.1.1	5.4M K	10 1 100	13 37 13		1
• Q NXOS-147	192,168,1,210		172.16.67.157 172.16.67.112		192.0.2.35	192.0.2.35				Land and the second sec		

Create a new group by selecting the Add button, naming your group and adding devices to it. Use the scroll bars to find the devices in the list or type in the start of the device name in the field to the right of the magnifying glass to filter the list. Click on the magnifying glass to enable additional tools (case sensitive, wild cards, partial matches) to assist in filtering the list.

Edit Groups		×	Add Group	x
Groups			Name (*) L2PODc	
Name	Size	Add	Desception L2 testing pod	_
Demo67 1386 L2PODc	2 2 2 4	Edit	All Other Devices Current Group of Devices Q- Image: Contract Contend Contrelation Contract Contend Contract Contrel	
New and modified group entries have a (*)			C2921SCOPE_1-17 C39225-163 cat2960SCOPE_1-14 ~ Asterisks (*) indicate required fields.	
, , , , , , , , , , , , , , , , , , , ,	ОК	Cancel	Add Done Cancel	

Once a group is created, the grouped devices will appear in the topology view as a single entity labeled with the assigned name. Devices can be expanded from and collapsed back into, the group by rightclicking the group and selecting Expand or Collapse. The group color is determined by the device in the group with the most severe alert color indicator. This way, in the system topology, if any one device within a group turns either red or orange from a nominal green color, then the entire group icon will turn to that same alert color. The order of color alert severity is Red (Warning), Orange (Drops), Green (Normal), Blue (All Polling Disabled) and Gray (Down). In the images below, L2PODc group status is red because at least one of the devices within that group is red.





Options

The Options dialog allows LiveNX settings and preferences to be managed. The Options dialog can be accessed by selecting Tools > Options.

Preferences

The Preferences section of the Options dialog allows you to use device names instead of hostnames, reset window sizes and warning dialogs. You can also set directory locations for the different files that LiveNX will save.

The device or hostname changes are visible in the System Hierarchy View and the System Topology.

Options		X
Database	al remote1	
Preferences	nfig	^
QoS Database location:	c: \dev\LiveAction\data\nodes\Local\data\snmpstore	Backup now
Database Database size:	2.339 GB (1.995 GB available for deletion)	Reset now
Automatically p	urge data older than: 30 days 👻	Purge now
Email Before purging,	archive to: c:\dev\BackupTestQoS_Local	
Flow		
Security Database location:	c:\dev\LiveAction\data\nodes\Local\data\flowstore	Backup now
Database size:	637.199 MB (477.932 MB available for deletion)	Reset now
√ Automatically p	urge data older than: 30 days 🔻	Purge now E
✓ Before purging,	archive to: c:\dev\BackupTestFlow_Local	
Alert		
Database location:	c: \dev\LiveAction \data \nodes \Local \data \alertstore 2	Backup now
Database size:	66.508 MB (41.427 MB available for deletion)	Reset now
✓ Automatically p	urge data older than: 30 days 🔹	Purge now
✓ Before purging,	archive to: c:\dev\BackupTestAlert_Local	
Long-Term		
Database location:	c: \dev \LiveAction \data \nodes \Local \data \ongtermstore	Backup now
Database size:	255.861 MB (191.639 MB available for deletion)	Reset now
✓ Automatically p	urge data older than: 30 days 🔻	Purge now
Refore purging	archive to:	•
	A	Close

Database

The Database section of the Options dialog allows you to manage settings related to the databases used by LiveNX. Database management can be completed on all Nodes including the LiveNX Server by using the All Nodes tab. Individual Nodes can be controlled by clicking on the corresponding Node tab.

Options		x
Preferences	Database All nodes Local remote1 QoS	
Database	Image: Solid participation Image: Solid participation Image: Solid participation Reset now Image: Reset now Image: Solid participation Image: Solid participation Image: Reset now Image: Reset now Image: Solid participation Image: Solid participation Image: Reset now Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Reset now Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid participation Image: Solid particitettic partitetticipation Image: Solid p	
Email	Image: Solution of the second sec	
	Alert	
	Long-Term	
	☑ Display a warning when free disk space falls below: IGB ▼	
	Apply	

Preferences	Database	
Preferences		
	All nodes Local remote 1	
Freierences	✓ Use 'All nodes' config	
	QoS	
Database	Database location: c:\dev\LiveAction\data\nodes\Local\data\snmpstore	Backup now
	Database size: 2.339 GB (1.995 GB available for deletion)	Reset now
\geq	✓ Automatically purge data older than: 30 days	Purge now
Email	Before purging, archive to: c:\dev\BackupTestQoS_Local	
	Flow	
Security	Database location: c:\dev\LiveAction\data\nodes\Local\data\flowstore	Backup now
Jecon,	Database size: 637.199 MB (477.932 MB available for deletion)	Reset now
		Purge now
	✓ Automatically purge data older than: 30 days ▼	Furge now
	✓ Before purging, archive to: c:\dev\BackupTestFlow_Local	
	Alert	
	Database location: c: \dev \LiveAction \data \nodes \Local \data \alertstore2	Backup now
	Database size: 66.508 MB (41.427 MB available for deletion)	Reset now
	✓ Automatically purge data older than: 30 days -	Purge now
	Before purging, archive to: c:\dev\BackupTestAlert_Local	
	Database location: c:\dev\LiveAction\data\nodes\Local\data\ongtermstore	Backup now
		Reset now
	Database size: 255.861 MB (191.639 MB available for deletion)	
	✓ Automatically purge data older than: 30 days ▼	Purge now
	7 Refore purging archive to: c:\dev\RackupTectLopgTerm_Local	

All Nodes tab: Changes made in this tab will affect all Nodes in the LiveNX system. LiveNX generates four databases: QoS, Flow, Alert and Long-Term. Each database can be configured across all Nodes to:

- Enable a warning when the database exceeds either 500 MB, 1 GB, 2 GB, 5 GB, 10 GB, 50 GB, 100 GB or 500 GB. Default is warning = ON and size = 500 MB.
- Enable an automatic purge feature for data older than 1, 2, 5, 10, 30 or 60, 90, 120, 180 or 360 days. Default is auto-purge = ON and age = 10 days for the QoS, Flow and Alert databases and 365 days for the Long-Term database.
- To save database data before purging, click on the Before purging, archive to: check box. For example, to store the database data in the same directory as the LiveNX Server data, type C"LiveAction Server Data<LiveAction Version>. Reset a particular database (QoS, Flow, Alert or Long-term) across all Nodes by clicking on the Reset now button. This will erase all data collected in that database.
- Purge a particular database (QoS, Flow, Alert or Long-term) across all Nodes by clicking on the Purge now button. This will erase all data older than the specified duration selected in the drop-down menu.
- Enable a warning when the free disk space on any Node exceeds either 1 GB, 10 GB, 20 GB, 30GB, 50 GB or 100 GB. Default is warning = ON and size = 1 GB.
- **Note** LiveNX supports an automatic purge to ensure that there is sufficient space to store about one minute worth of SNMP, Flow, Alert and Long-term data. This is not user-configurable, but the auto-purging of the four databases are done only as a last resort, to ensure that there is sufficient space to store the most recent data.

Individual NTab: Although the default is to use the All Nodes configuration, each Node's database may be configured separately by unchecking the Use All Nodes Config check box and selecting the individual tab for the desired Node. In addition to displaying the Volume size and Volume size free for the individual Node, each database within that Node can be configured to:

- Backup an individual database by clicking on the Backup now button—This saves a copy of the database to a directory on the Node. After clicking on the Backup now button, LiveNX prompts you to specify the backup directory on the Server. To store the backup data in the same directory as the LiveNX Server data, type C: LiveAction Server Data<LiveAction Version>. The backup QoS, Flow, Alert and Long-term databases will be stored in the location selected with the filenames Snap store, Flowstore, Alert store and longterm store, respectively, each appended with the backup creation time in the
- YYYY.MM.DD.HH.MM.SS format. If disk space is an issue, you are advised to move the backup files off-line and purge the local copy. The backup QoS, Flow and Alert database directories can be added back to LiveNX to analyze historical information by using the Mounted Data feature in the LiveNX Server console. Please see Mounting Data Directories into the LiveNX Server section of Chapter 2 Installation. The Long-term Database cannot be mounted; replacement requires manually swapping the long-term databases out in the Flowstore-dashboard cache directory in the LiveNX Server Data directory.
- Reset a database (QoS, Flow, Alert or Long-term) on the individual Node by clicking on the corresponding Reset now button. This will erase all data collected in that database.
- Purge a particular database (QoS, Flow, Alert or Long-term) on the individual Node by clicking on the corresponding Purge now button. This will purge all data older than the specified duration selected in the drop-down menu in the All Nodes tab.

Email

The Email section of the Options dialog allows you to set SMTP Server and email sender options. These will be used when LiveNX sends out reports, alerts and notifications. The values entered depend on your specific e-mail service. The image below shows how to configure LiveNX to send e-mail to a Gmail account.

Options	
Preferences Database	Email SMTP Server Host name *: smtp.gmail.com Port *: 465 Username: user's e-mail login Password: ••••••• Security: SSL •
Email Security	Email Settings Sender address *: sender's e-mail address Sender name: sender's name Send a test email Clear
	OK Cancel Apply

SMTP Server

 Hostname—Enter your SMTP host name. • Port number—Default for SMTP is 25, TLS is 587, and SSL is 465. • Username—Enter your username to access your e-mail account. • Password—Enter your password to access your e-mail account. • Security—Choices are: NONE, TLS (Transport Layer Security), and SSL (Secure Sockets Layer)

Email Settings

• Sender address—Enter the sender's e-mail address. • Sender's name—Enter the sender's name.

Send a Test Email

This will send a test e-mail back to the sender's e-mail address.

Security

The Security section of the Options dialog allows you to manage security settings for LiveNX. You can set a password policy and login control options.

Options		
Preferences Database Email	Security Title Bar Security Label Select the security level to be displayed in the Application Title. Click on Apply to set the level. None Click on Apply to set the level. None Click on Apply to set the level. Required properties are indicated with an '** Password Policy	
Security	Password expires after Allow password change once in Number of previous passwords to save	60 days 1 day(s) 3 previous
	Password Restriction Minimum characters required Number of uppercase characters required	5 chars.
	Number of lowercase characters required Number of numeric characters required Number of special characters required Constraint down in the set of the	1 dars.
	1	OK Cancel Apply

Export Server/Client /Nodes Logs

The Export Logs feature provides detailed network information to assist LiveNX support in resolving management or monitoring issues.

On the LiveNX Client, go to Help > Export Logs.

On the LiveNX Server, go to Help > Export Logs.

Click on the Device Information check box to export additional device information.

Export Lo	ogs
?	Include additional information?
	Yes No

Clicking on the Device Information check box will allow LiveNX to create a .csv file containing device information including serial number, IP address, vendor, model, IOS, feature capability and interfaces. This file will be added to the .zip file containing the other export logs, either client or server.

Note Please ensure that the LiveNX Server is on and running prior to exporting the logs.

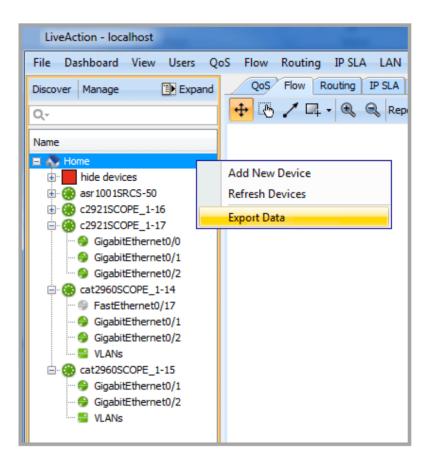
To get information from the LiveNX Nodes, go to the LiveAction Management Console and click on the Nodes tab. Right click on the status column of any Node with status = Connected and select Export Logs.

Export Device Data

LiveNX uses the expand and collapse feature of the device tree in order for a user to hide certain information from exporting to a log file. To prevent certain devices from exporting to a log, create a group and then shrink the group, so no device are visible. To prevent certain interfaces from exporting to a log, shrink the interfaces so only the device is visible. Right-click on the device tree and select Export Data.

Export Device Data

LiveNX uses the expand and collapse feature of the device tree in order for a user to hide certain information from exporting to a log file. To prevent certain devices from exporting to a log, create a group and then shrink the group, so no device are visible. To prevent certain interfaces from exporting to a log, shrink the interfaces so only the device is visible. Right-click on the device tree and select Export Data.



The .csv file will display only those devices and interfaces visible in the device tree.

	А	В	С
1	Device se	Name	IP Addı
2		Home	
3		hide devices	
4	SSI154204	asr1001SRCS-50.referentia.com	192.168
5	FTX1528A	c2921SCOPE_1-16.referentia.com	192.168
6	FTX1542A	c2921SCOPE_1-17.referentia.com	192.168
7		GigabitEthernet0/0	192.168
8		GigabitEthernet0/1	30.240.
9		GigabitEthernet0/2	30.13.1
10	FCQ1531Z	cat2960SCOPE_1-14.referentia.com	192.168
11		FastEthernet0/17	
12		GigabitEthernet0/1	
13		GigabitEthernet0/2	
14		VLANs	
15	FCQ1531Z	cat2960SCOPE_1-15.referentia.com	192.168
16		GigabitEthernet0/1	
17		GigabitEthernet0/2	
18		VLANs	
19			