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

20210326-LNXEC_211a

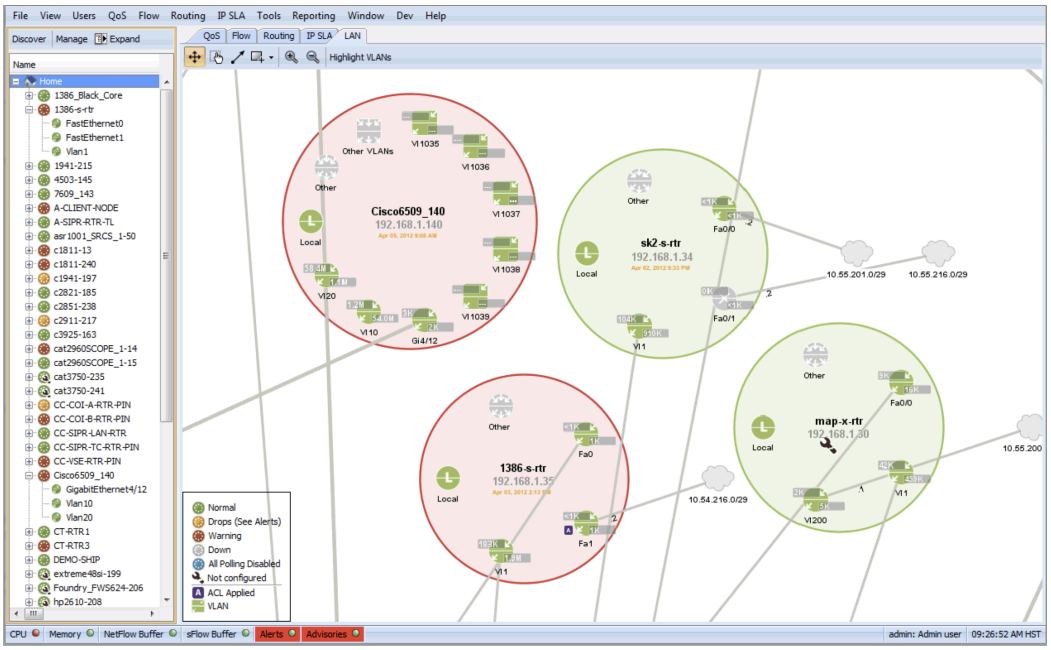
Contents

CHAPTER 1

Introduction

In this chapter:

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 *https://docs.liveaction.com/LiveNX*.

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.

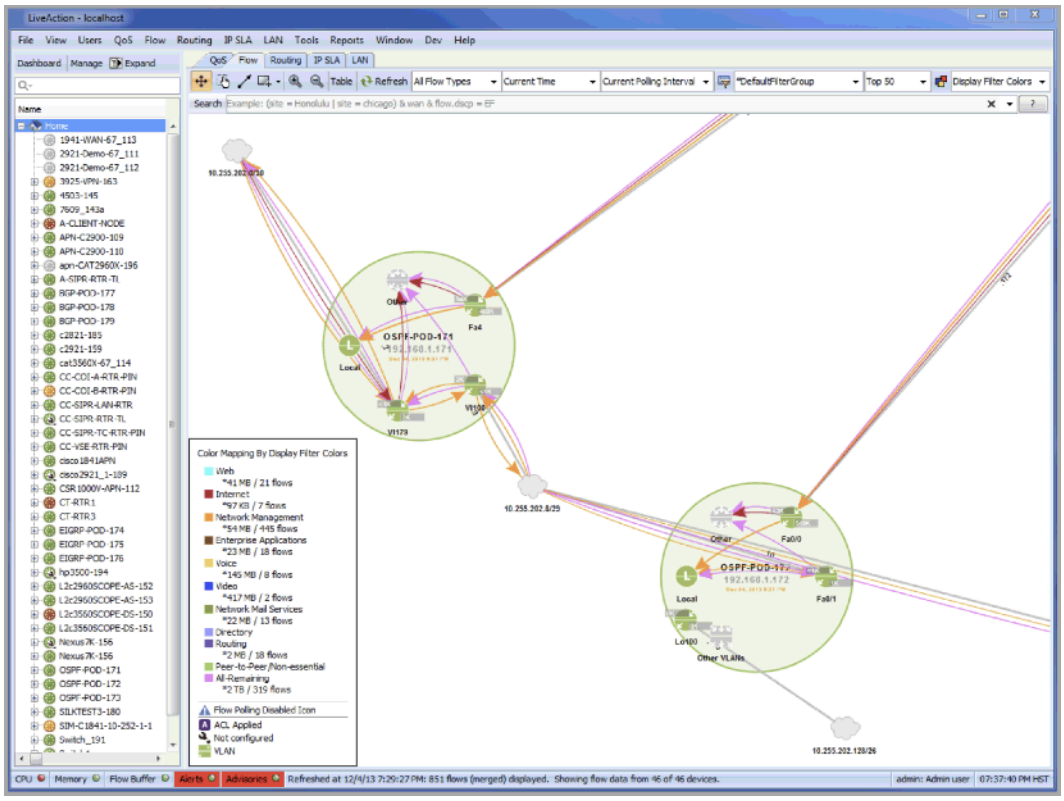
CHAPTER 2

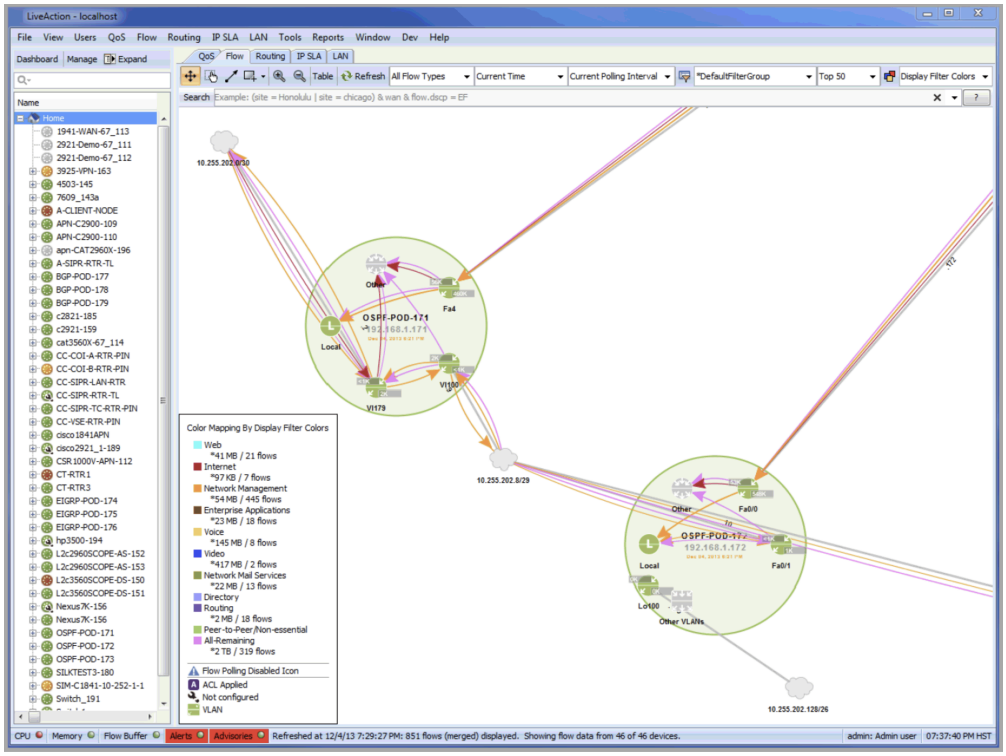
LiveNX Engineering Console User Interface

In this chapter:

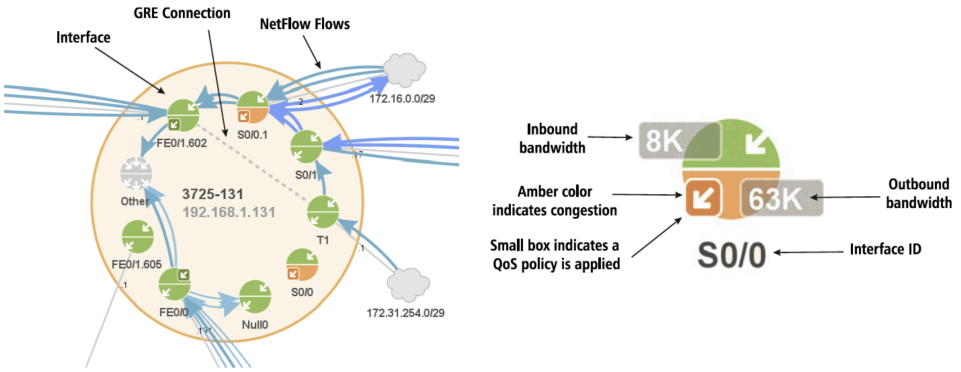
About the Engineering Console User Interface

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.

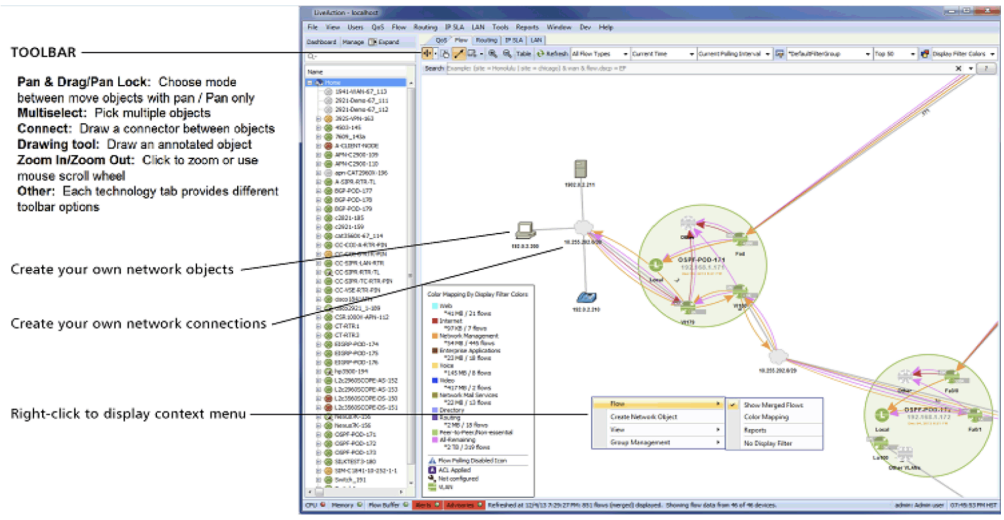


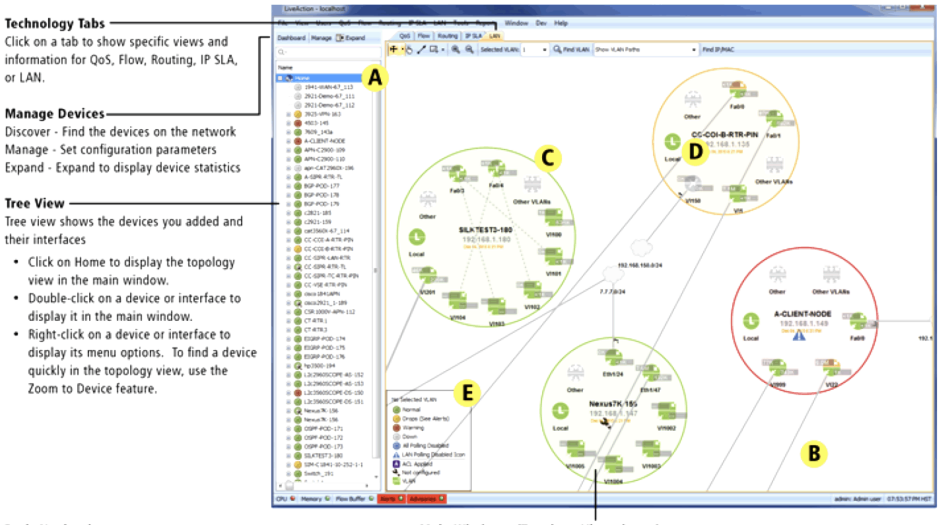


The top half of each interface represents inbound traffic and the bottom half represents outbound traffic. The color of each half indicates its status—green indicates normal, orange indicates congestion, and gray indicates the interface is disabled. Inbound and outbound bandwidth values for each interface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



Topology View Interface Controls





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.

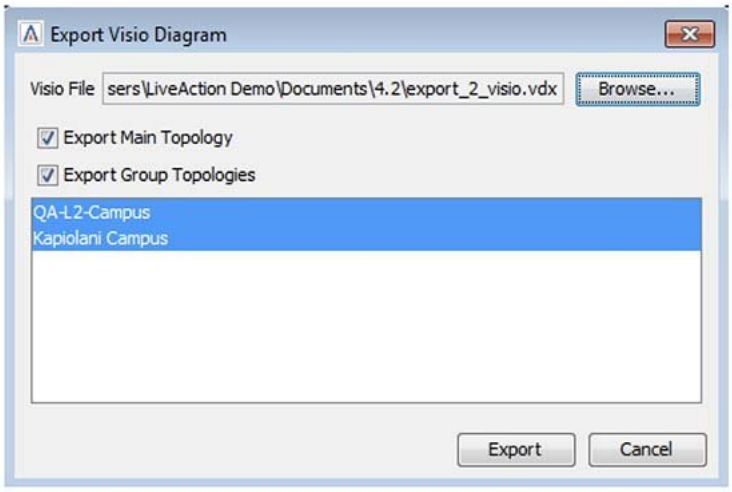
Note Any changes you made to the layout (moving devices) will be reset to the default layout.

- **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.



Exporting and Importing a LiveNX Configuration

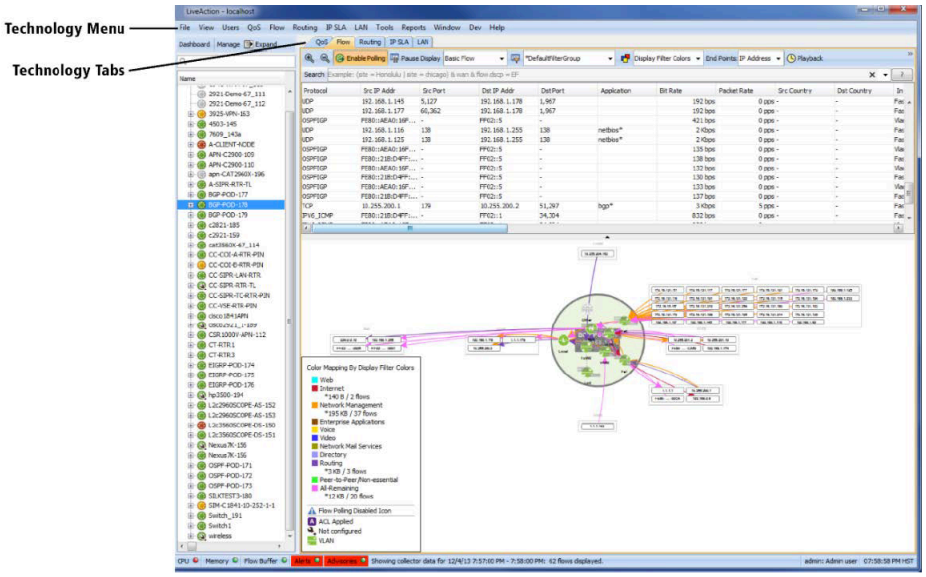
Configurations can be exchanged between different installed LiveNX clients in order to simplify environment setup. To export a LiveNX configuration, first launch the Management Console from the LiveNX server. Then go to the Manage menu and select Export Configurations. The configuration will be saved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

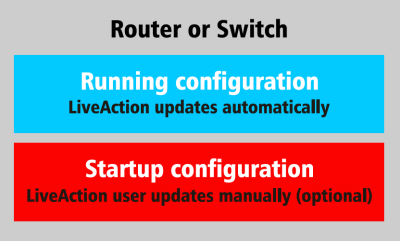
LiveNX Technology Tabs

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.

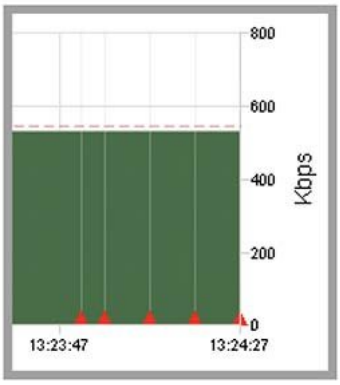


LiveNX Interface Color Codes

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

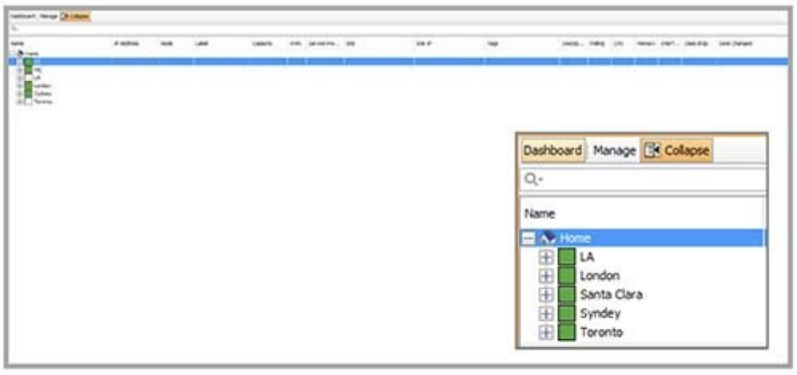
Web search, a daily ritual in our connected lives is highly effective due to tagging of information. Wouldn't it be great if you had a similar capability to search and ask questions related to the network? LiveNX network semantics help you understand and troubleshoot their network better and faster. 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:

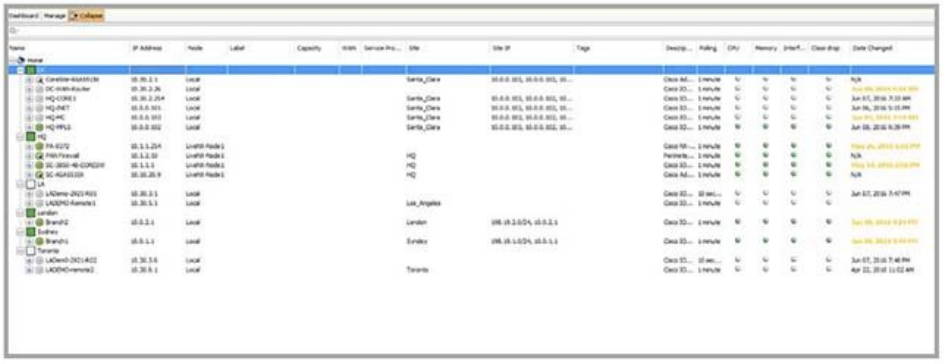
- Groups
- Sites and Site IPs
- WAN Links
- Service Providers
- Labels
- Capacity
- Device and Interface Tags
- Data Centers

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.

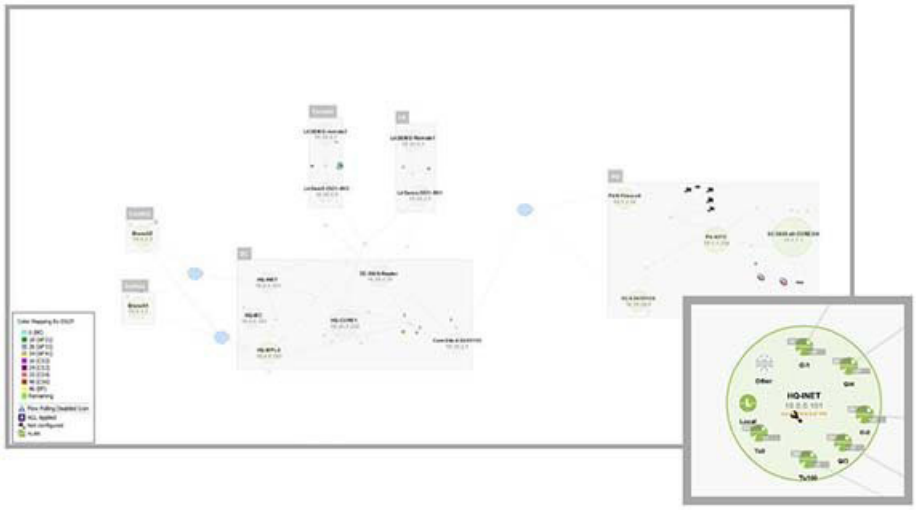


Each group contains network devices managed by LiveNX and can be seen by expanding the group as shown below. You can expand the group to see the network devices. Each network device can be further expanded to see the managed interfaces. For each managed entity, LiveNX provides detailed information about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

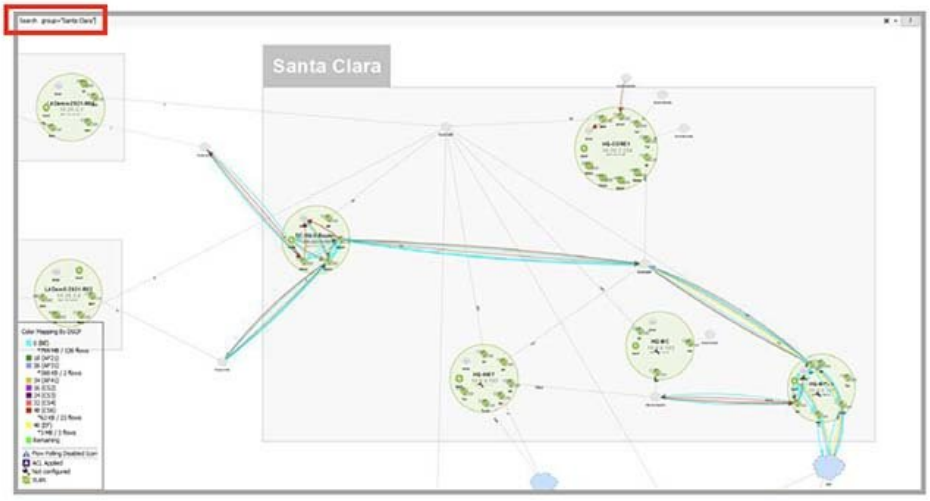


LiveNX provides an intuitive and interactive topology as shown below. Groups enable visualization and quick problem resolution on the topology map. Each square box on the topology corresponds to a group with network devices and third-party flow elements contained within each group.

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.

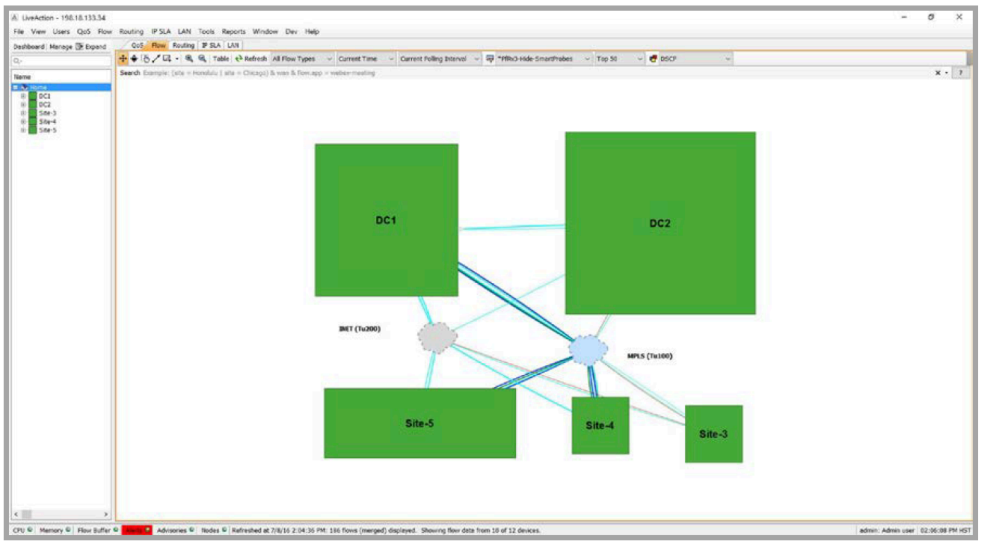


Additionally, a search filter applied to a particular group shows flow data related to all the devices in the specified group only. This helps narrow traffic flow visualization and makes for easier troubleshooting. The figure below shows the flows related to group Santa Clara when a filter for group=Santa_Clara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

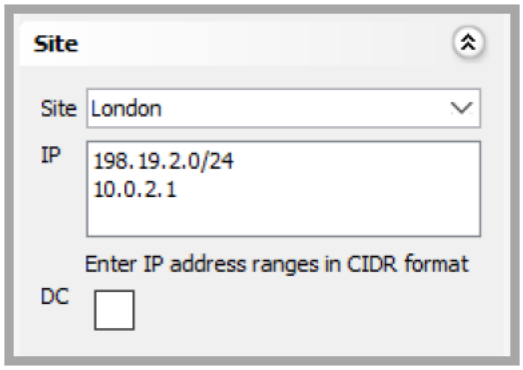
Collapsed groups also increase the performance of LiveNX by efficiently rendering the devices on the topology. You can simply zoom into a group to see the details.



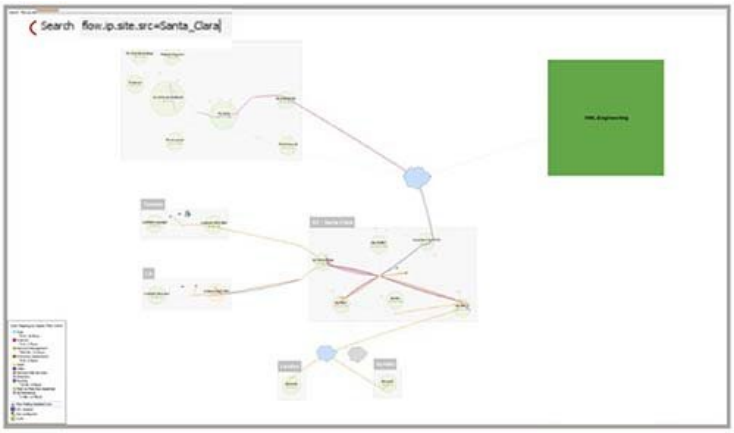
Sites and Site IPs

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.

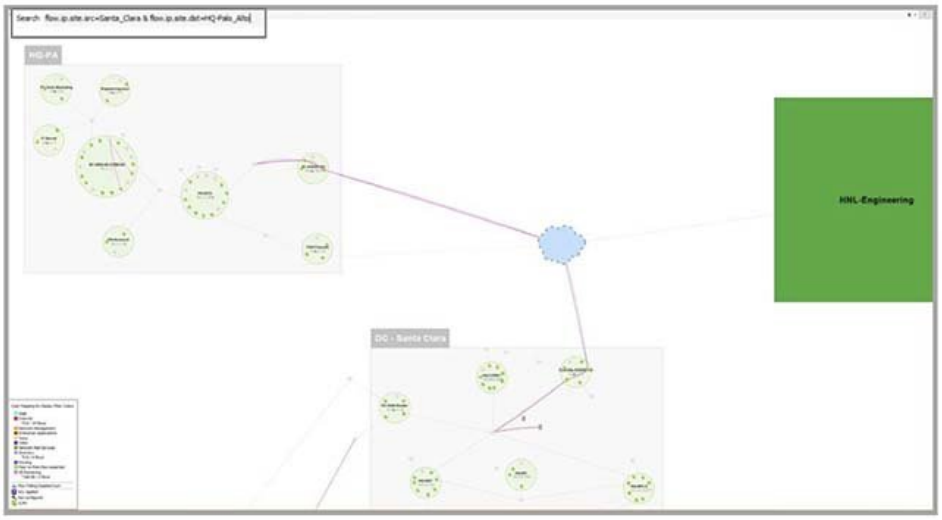
In addition to assigning a site to device(s), site also has a Site IP field as shown below. Site IP field can contain multiple entries and can be either an IP range or IP addresses. Providing Site IP information enables LiveNX to display relevant flows to and from sites, helping identify site-to-site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



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.

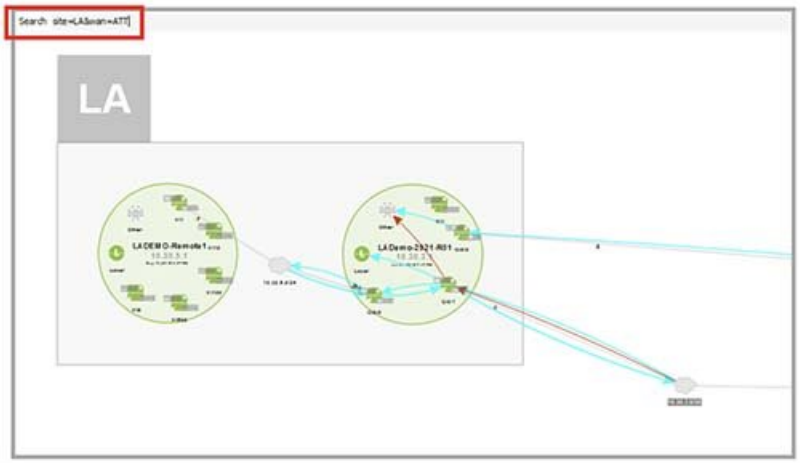


In addition, the admin can further narrow down the query to show flow data only between two specific sites. In our case, we are interested in the source as Santa Clara and destination being Palo Alto. The query will be flow.ip.site.src=Santa_Clara & flow.ip.site.dst=HQ-Palo_Alto with the result shown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

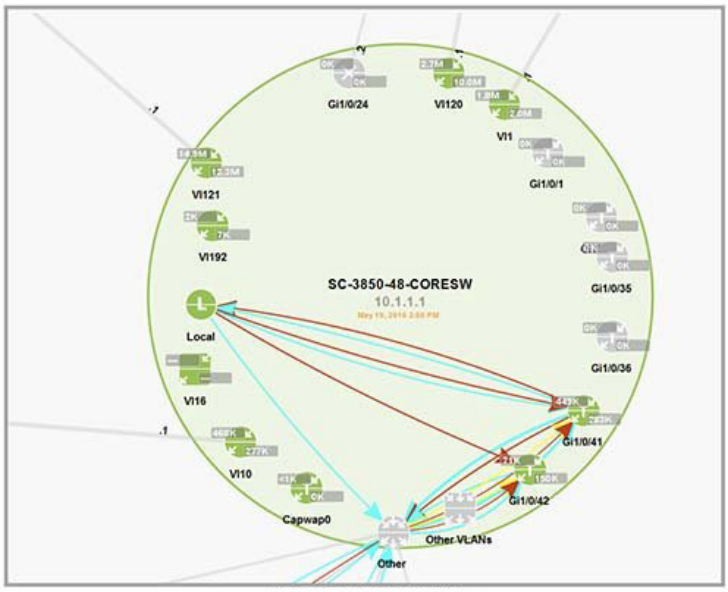


Label

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.

Capacity

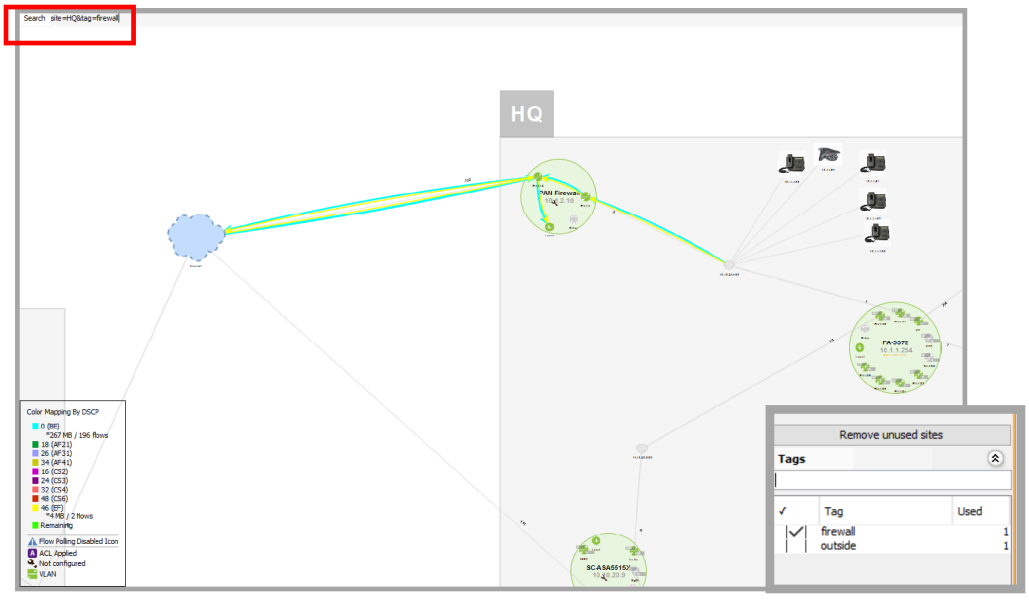
Capacity field denotes the capacity of an interface. Often, the configured capacity/bandwidth of an interface can be different from the maximum bandwidth of the physical interface. Once you have configured the capacity, the capacity information is leveraged for capacity planning reports. It is important 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.

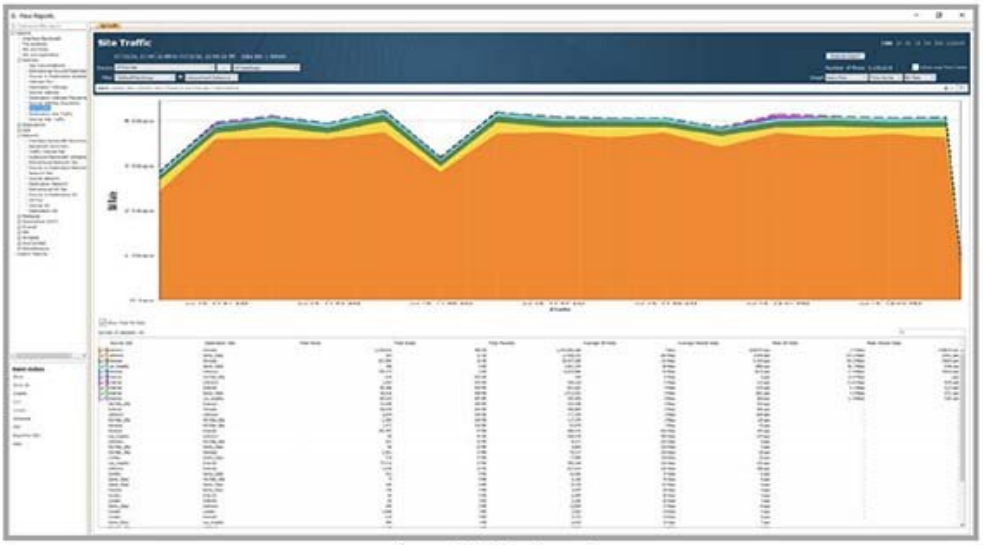
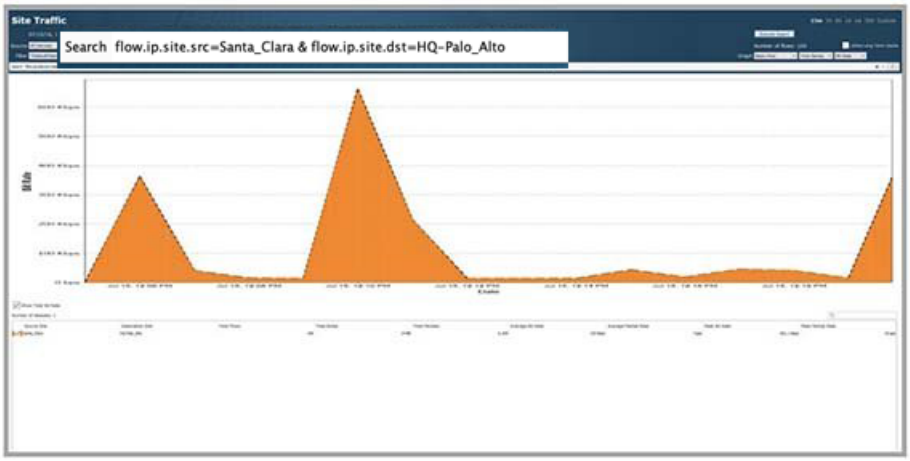


Figure 14: Site Report

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

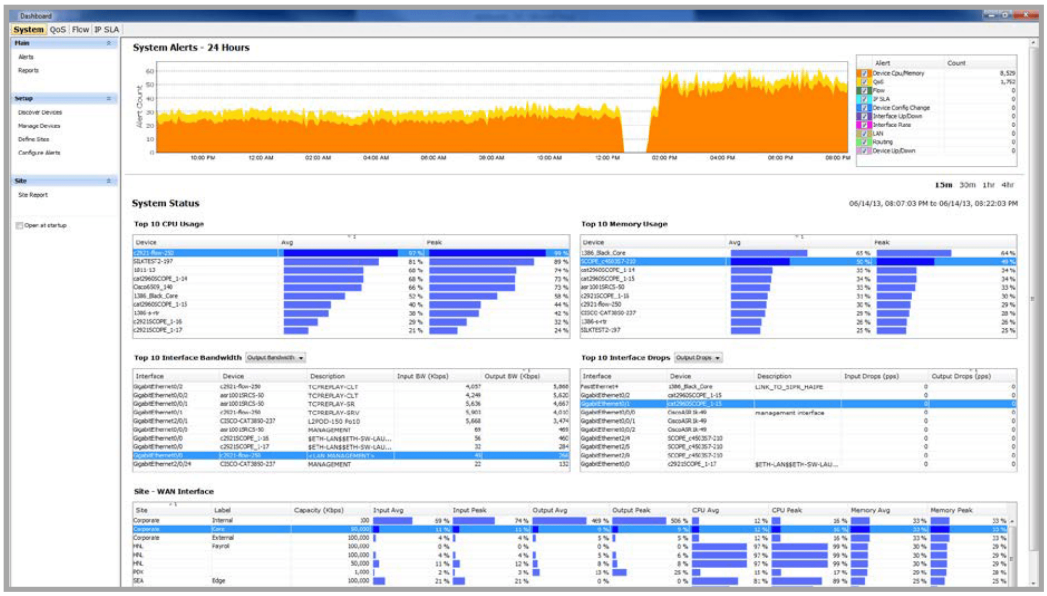
In this chapter:

About the Dashboard

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.

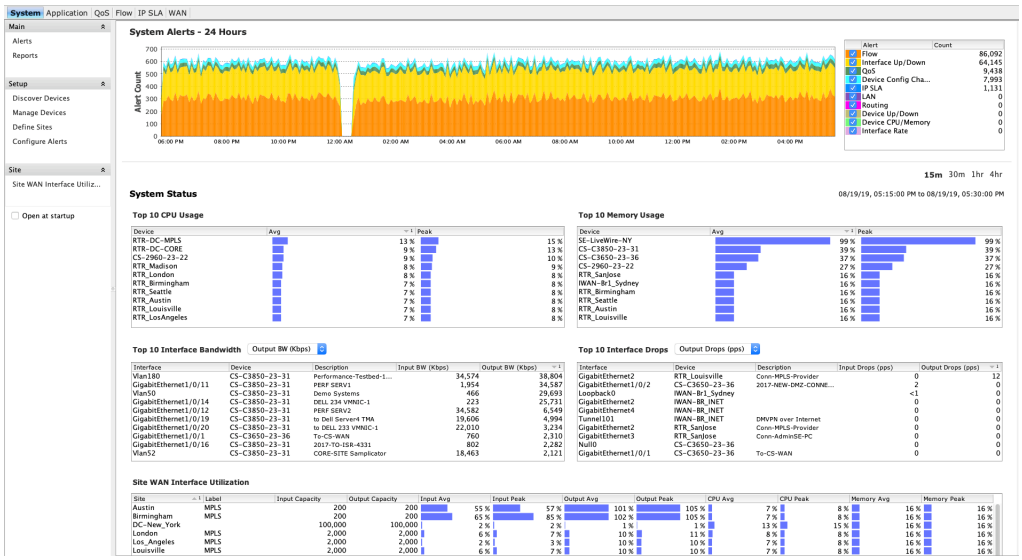


The Action bar of the Dashboard (on the left) displays a set of actions that can be taken, each of these actions is covered in the corresponding topic Chapters:

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

System Dashboard

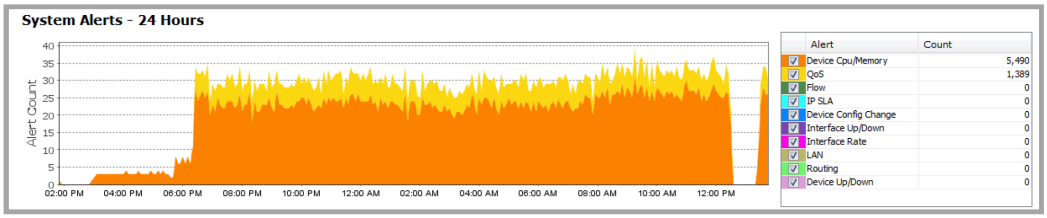
The System Dashboard presents a snapshot of the resources in the network, it lists the Alert count, and a set of widgets that display the status of Top devices in each category, CPU, Memory, Interface Bandwidth and Drops, and WAN Utilization. Within each widget the order can be displayed from Highest 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.

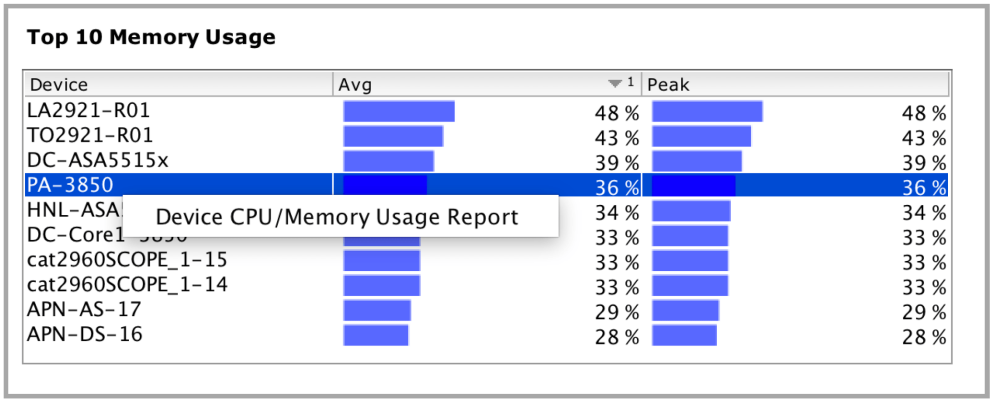


The legend to the right of the System Alerts chart is a tabular summary of the total generated alerts for the chart duration. Use the check box alongside each alert type to enable or disable viewing the alert category from the chart.

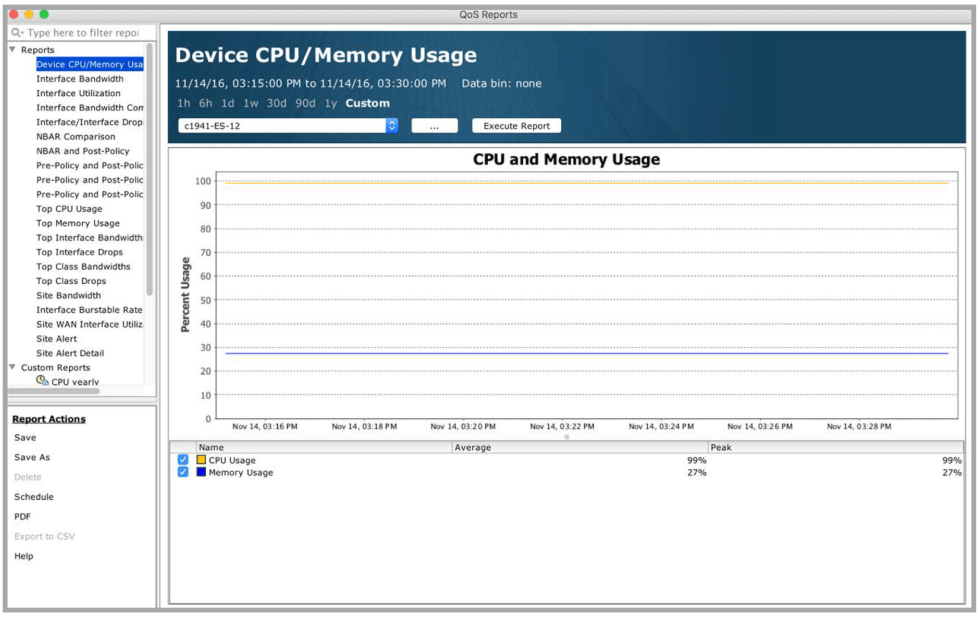
The charts and tables below the System Alerts graph provide real-time average data for the dashboard time duration selected. Four-time durations are available: last 15 minutes, last 30 minutes, last 1 hour and last 4 hours. Default is last 15 minutes.

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.

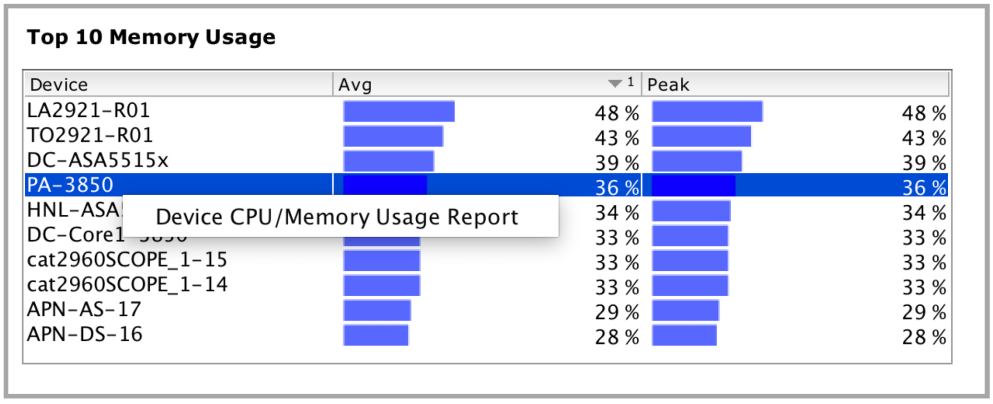


Right-click on an entry in the table and then select View Graph to bring up a historical Device CPU and Memory Usage time-series report. The report will automatically use the selected device.

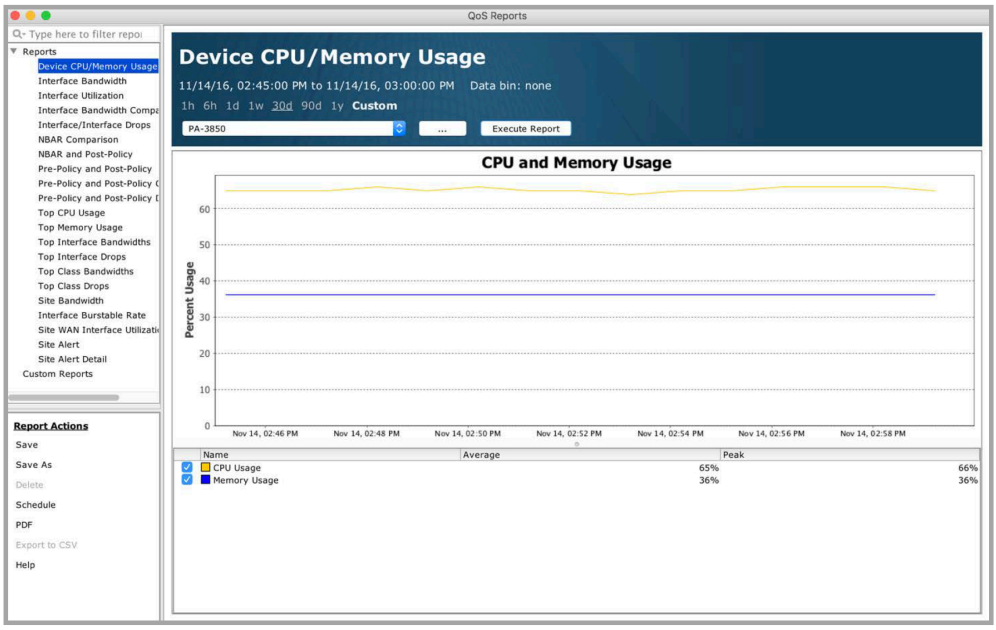


Top 10 Memory Usage

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.

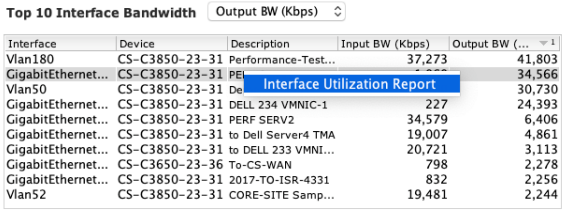


Right-click on a device name in the table and then select View Graph to bring up a historical Device CPU and Memory Usage time-series report. The report will automatically use the selected device.

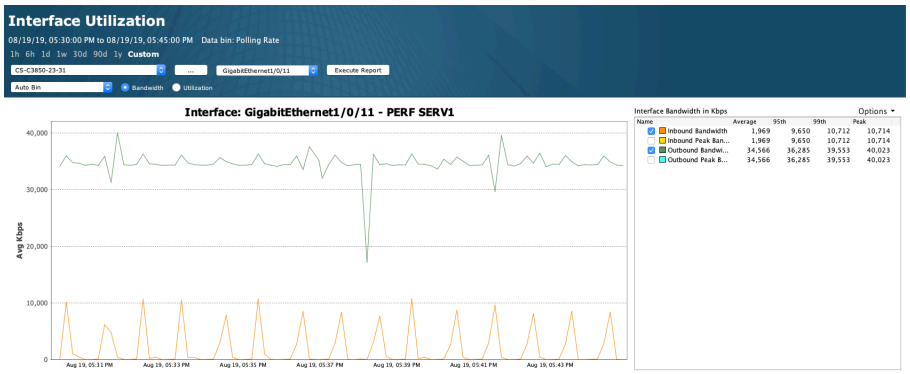


Top 10 Interface Bandwidth (Input or Output)

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.

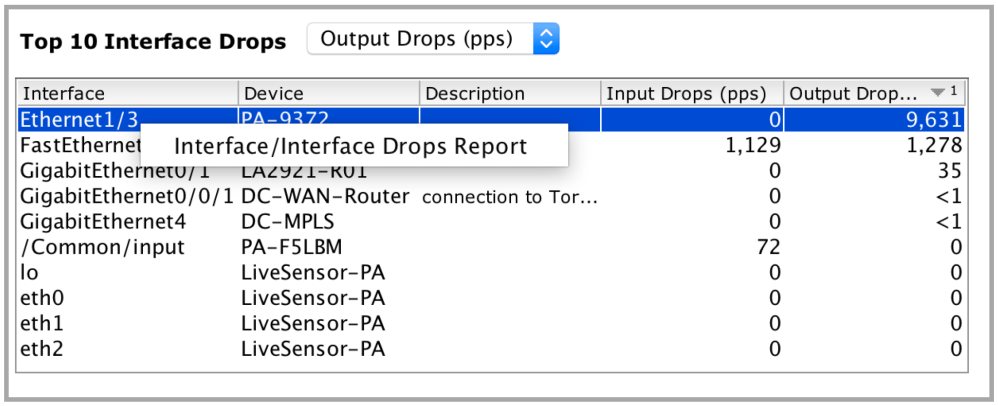


Right-click on an entry in the table and select View Bandwidth Chart to generate an Interface Utilization Report.

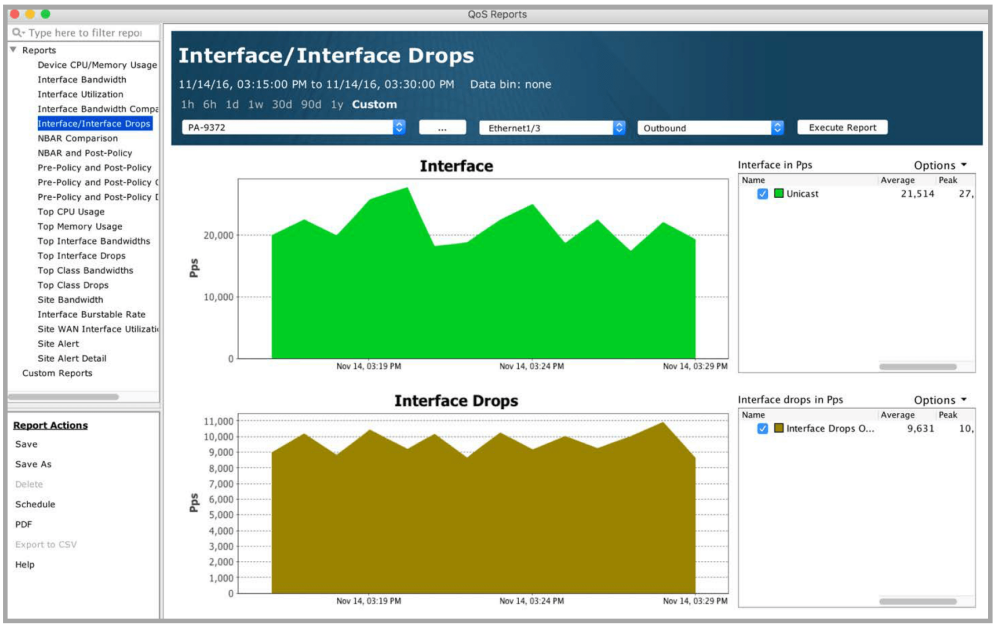


Top 10 Interface Drops (Input Drops or Output Drops)

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.

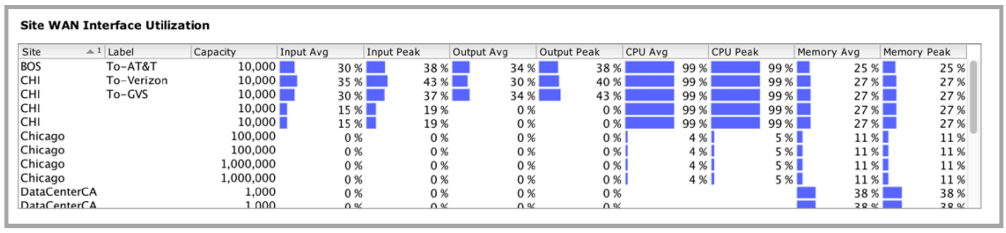


Right click on a table entry and select Interface/Interface Drops Report to generate a comparison interface/interface drops report using the selected device and interface.



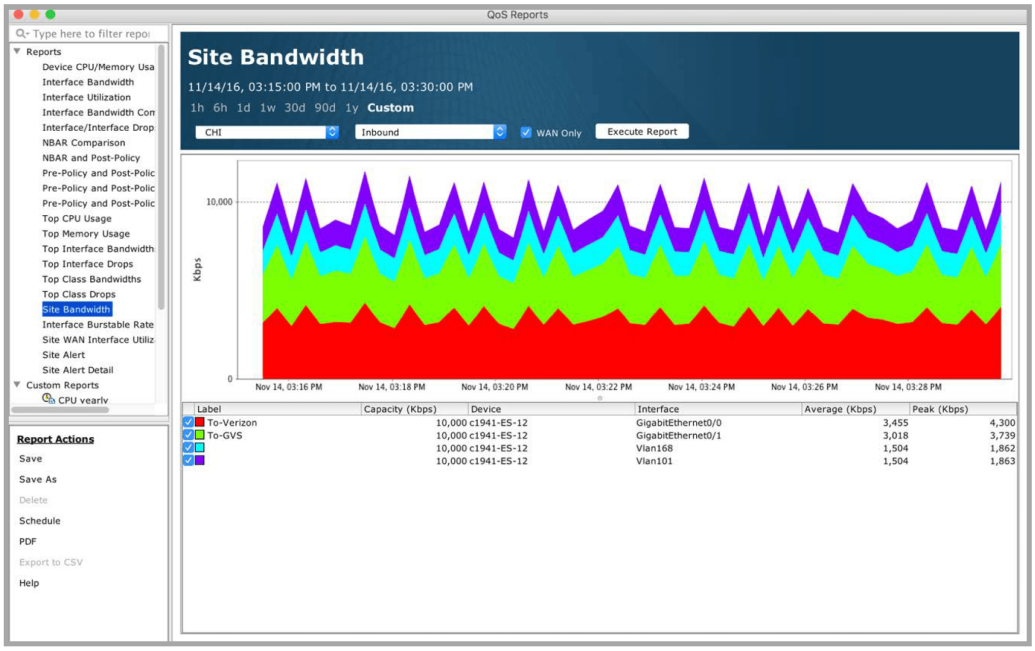
Site WAN Interface

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.

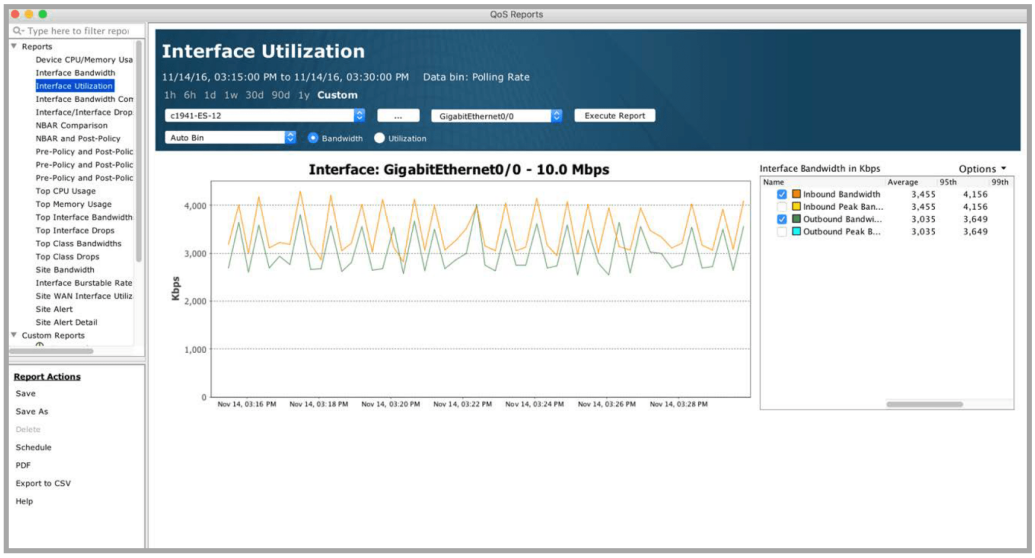


Right click on a field in the Site WAN Interface Utilization table and choose among three reports: Site Bandwidth, Interface Utilization, or Device CPU/Memory Usage. For each report, LiveNX automatically uses the selected device and interface; inbound is also selected as the default direction.

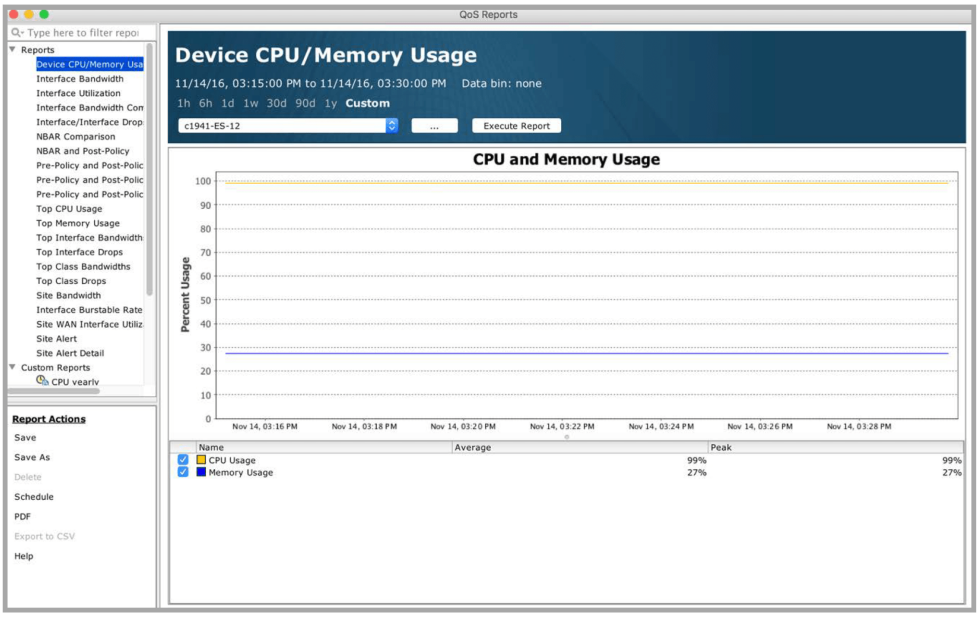
Site Bandwidth report



Interface Utilization report



Device CPU/Memory Usage report



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.

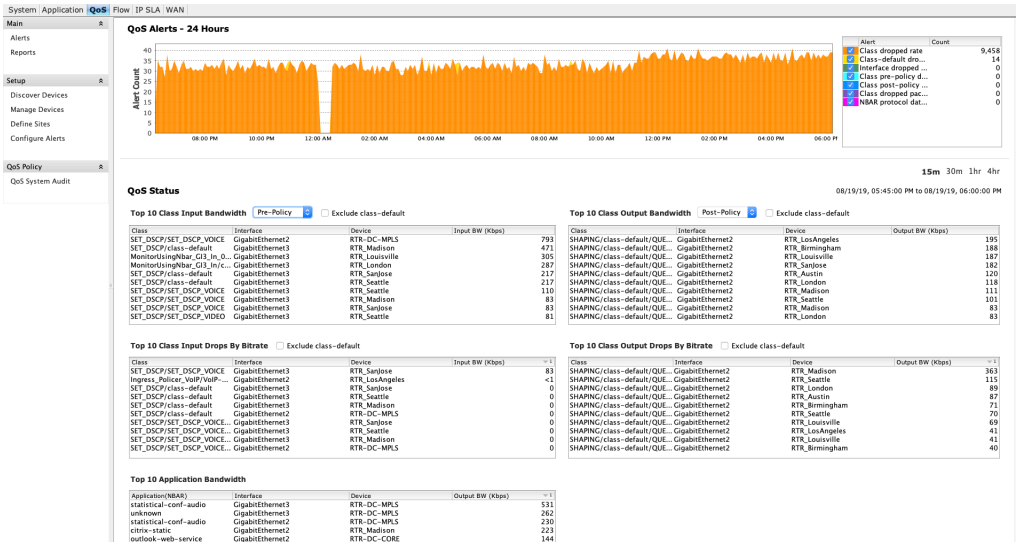
In the top right, there is two drop-down selections that provide more granularity for the dashboard. The first is used to display the results per site or all sites. The Second is used to display the results per application, or all applications.

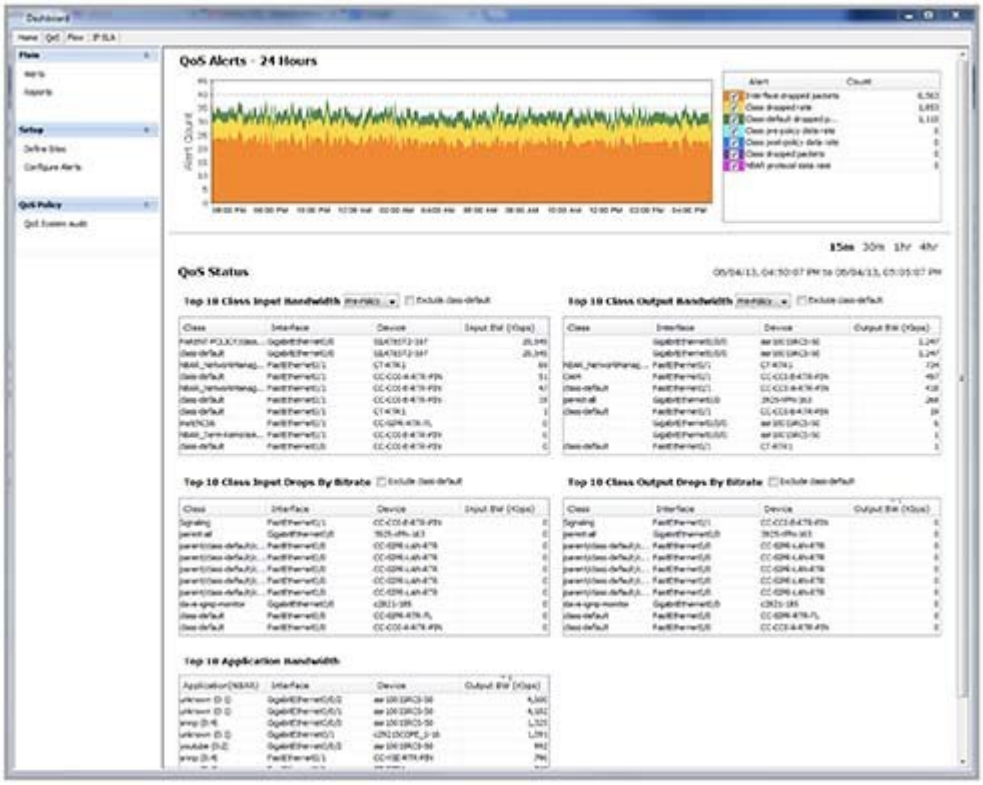
The Application Performance in the Action menu will open the Flow reports section which is covered later in this chapter.

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.

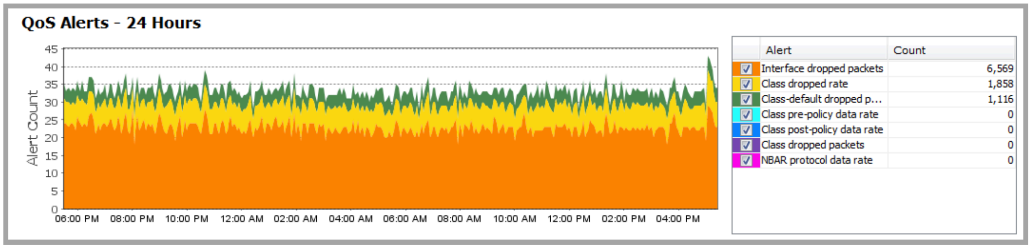




The QoS System Audit in the Action menu will open the Policy and Performance Audit Report which is covered later in this chapter. Right-clicking on any of the widgets will give the user the option to view the Pre- and Post-Policy graphs for the policy selected.

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.

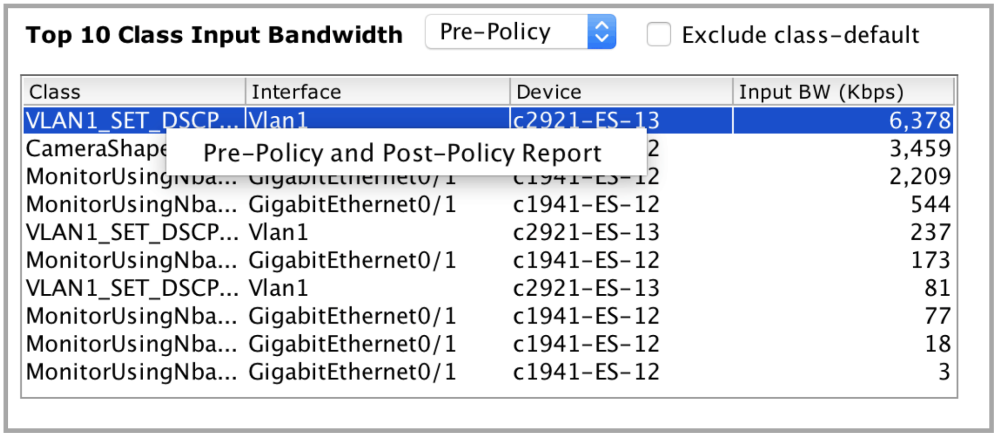
The tables below the QoS Alerts graph provide real-time average data for the dashboard time duration selected. Four-time durations are available: last 15 minutes, last 30 minutes, last 1 hour and last 4 hours. The default is last 15 minutes.

Top 10 Class Input Bandwidth Pre- or Post-Policy

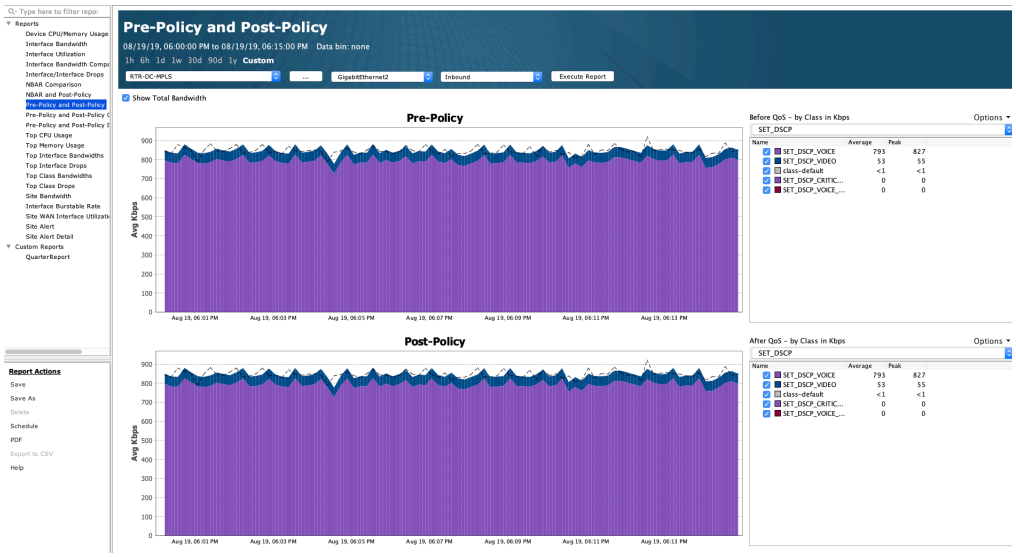
Right-click on an entry in the table and then select View Graph to bring up a Pre-Policy and Post-Policy comparison graph for the selected device, interface and Inbound direction.

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.

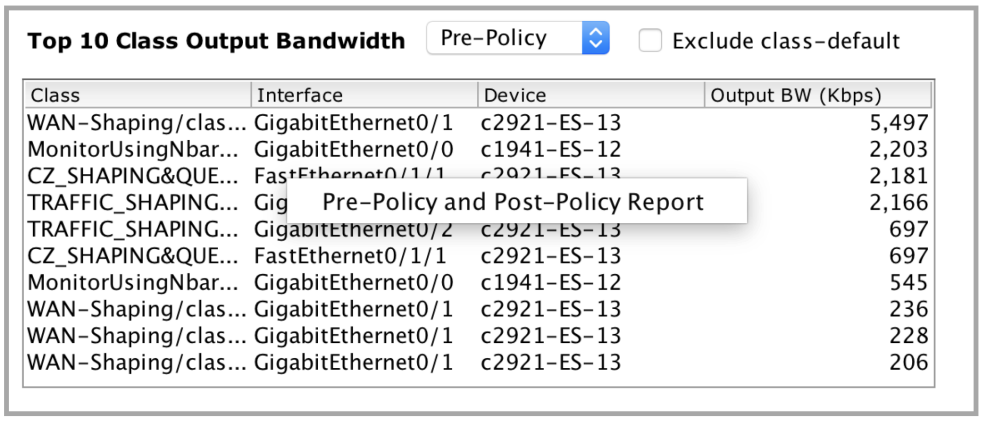


Right-click on an entry in the table and then select Pre-Policy and Post-Policy Report to bring up a Pre-Policy and Post-Policy report for the selected device, interface and Inbound direction.

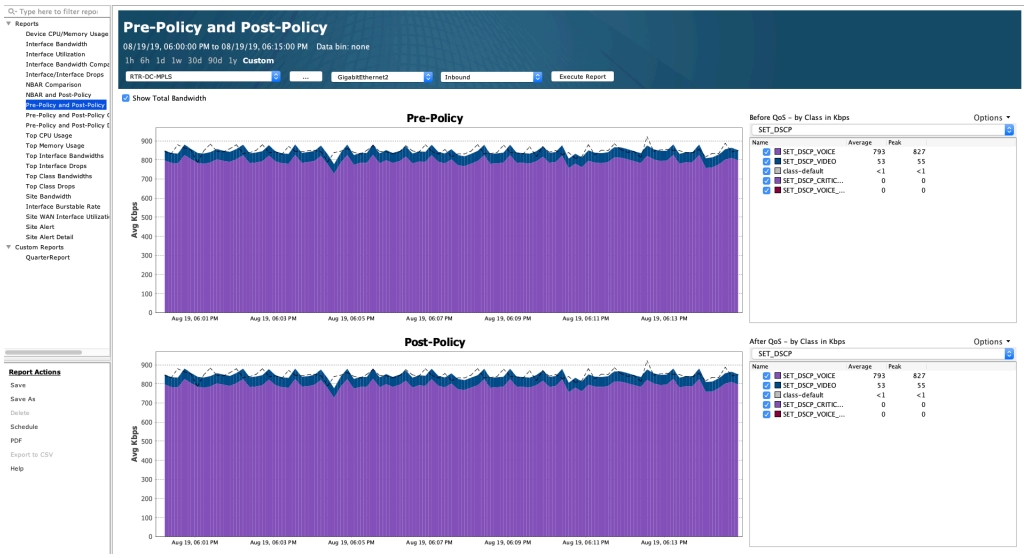


Top 10 Class Output Bandwidth Pre- or Post-Policy

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.



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)
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.

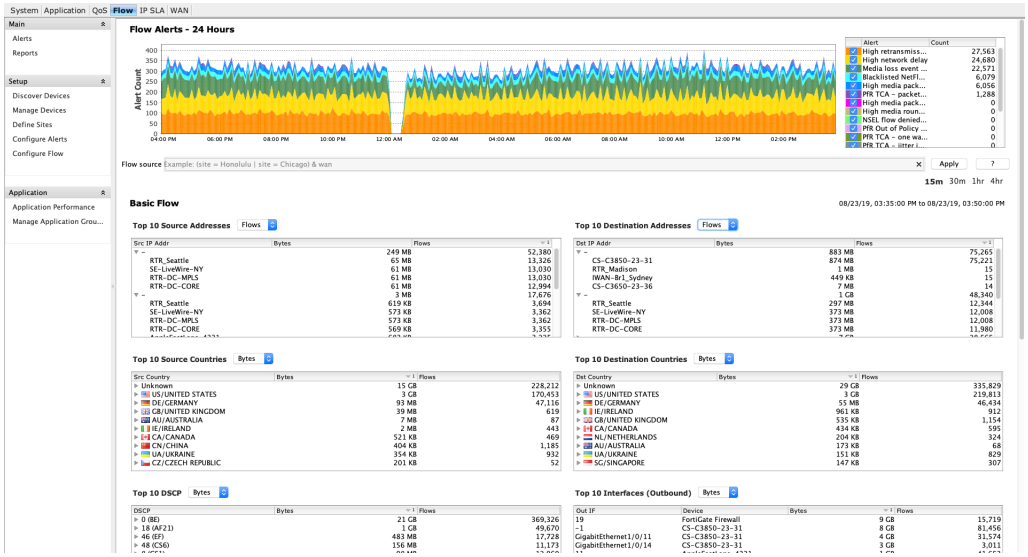
Top 10 Class Output Drops By Bitrate ☐ Exclude class-default

Class	Interface	Device	Output BW (Kb...
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.

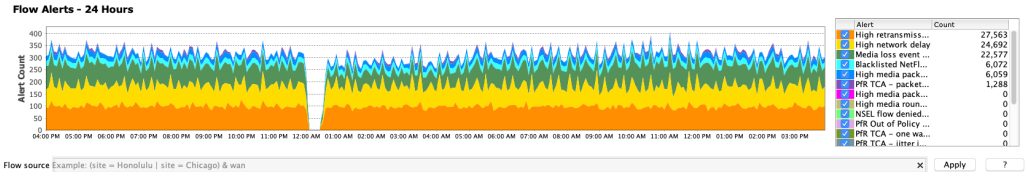


The Application Performance in the Action menu will open the Application Report which is covered later in this chapter.

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

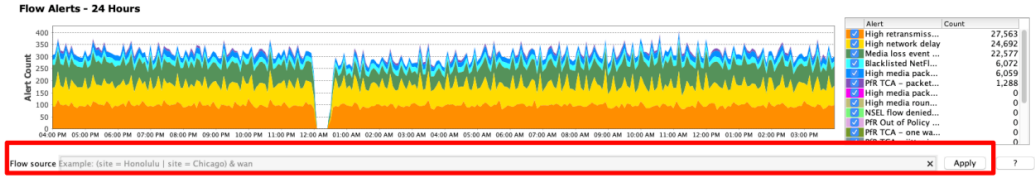
Flow Alerts – 24 Hours

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.

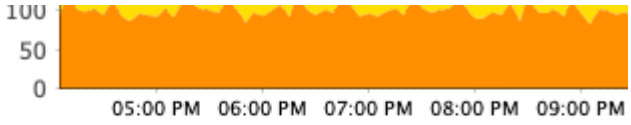
Flow Source

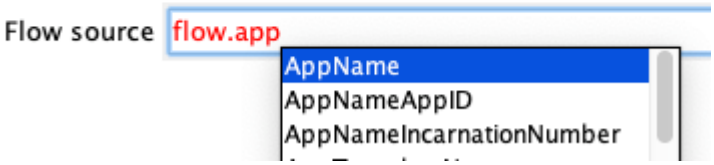


The LiveNX Flow source is an alphanumeric field to filter the flow dashboard based on the system and flow entities. Searchable system entities include device, interface, site, tag and WAN parameters. Searchable flow entities include IP address, DSCP, port, protocol and application.

- 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 = 'I' 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.





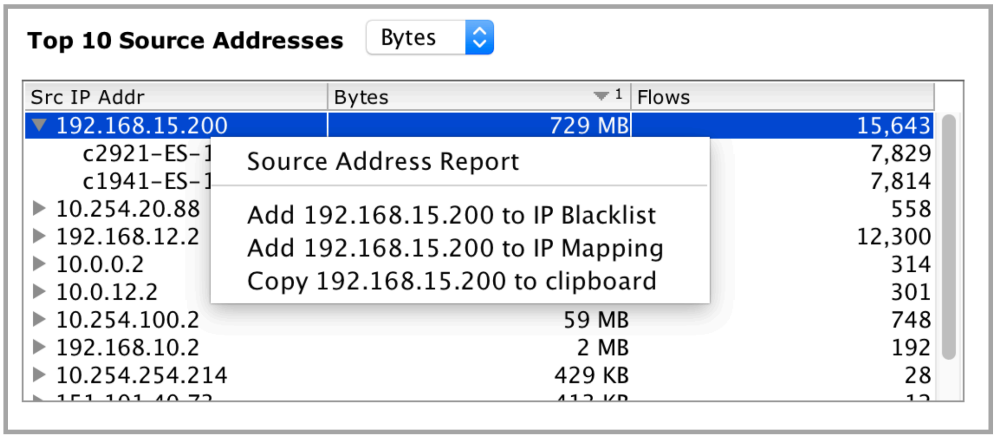
The Flow source search is done with a one pass search. In addition, the system level entities need to be in a single clause. For example, (site = Honolulu | site = Chicago) & flow.ip=1.1.1.1 is allowed, but (site = Honolulu & flow.ip=1.1.1.1) | (site = Chicago & flow.ip=1.1.1.1) is not allowed.

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.

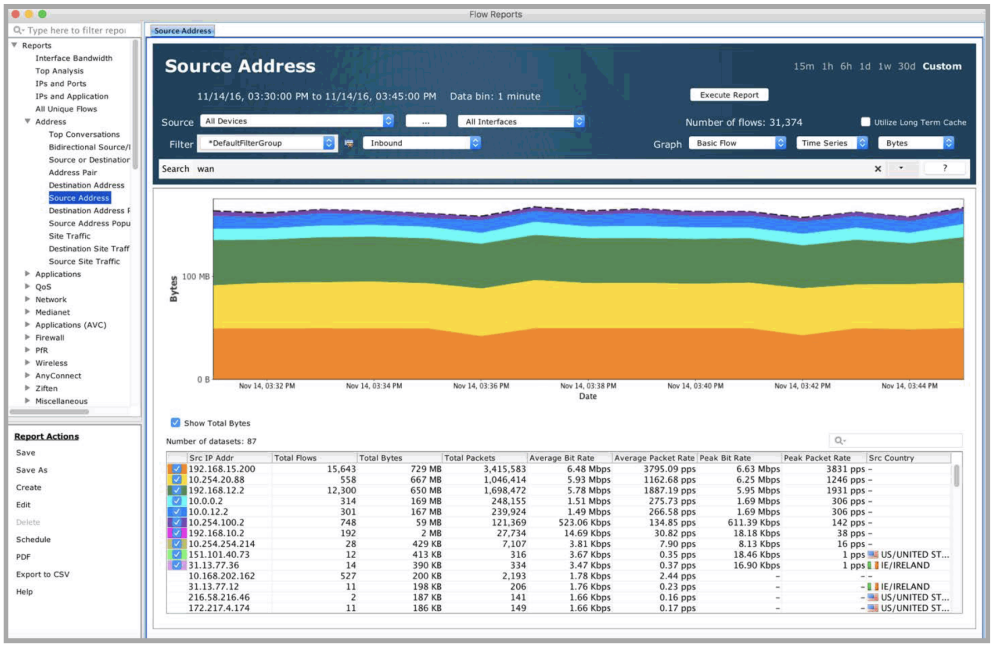
Example	
site=Honolulu & wan	Flows from specific site with WAN-tagged interfaces
flow.dscp=EF	Flows with DSCP EF markings
flow.ip.src=1.1.1.1	Flows with specific source IP
flow.ip.dst=1.1.1.1 & flow.ip.src=2.2.2.2	Flows with specific source and destination IP
flow.ip.site=Honolulu	Flows from specific 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.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

Top 10 Source Addresses [Bytes or Flows]

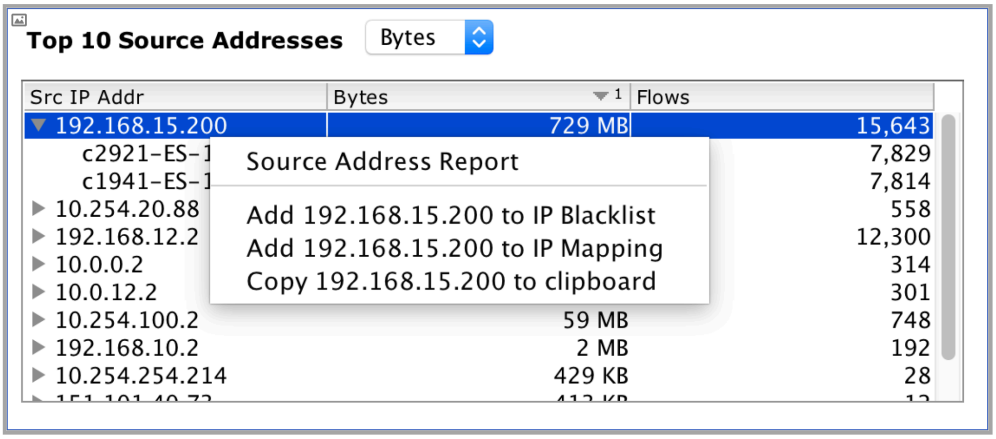
The Top 10 Source Addresses table lists the top 10 devices generating the largest number of bytes or flows from a source address. Click on the + sign to the left of the IP address to show the devices associated with the source IP address.



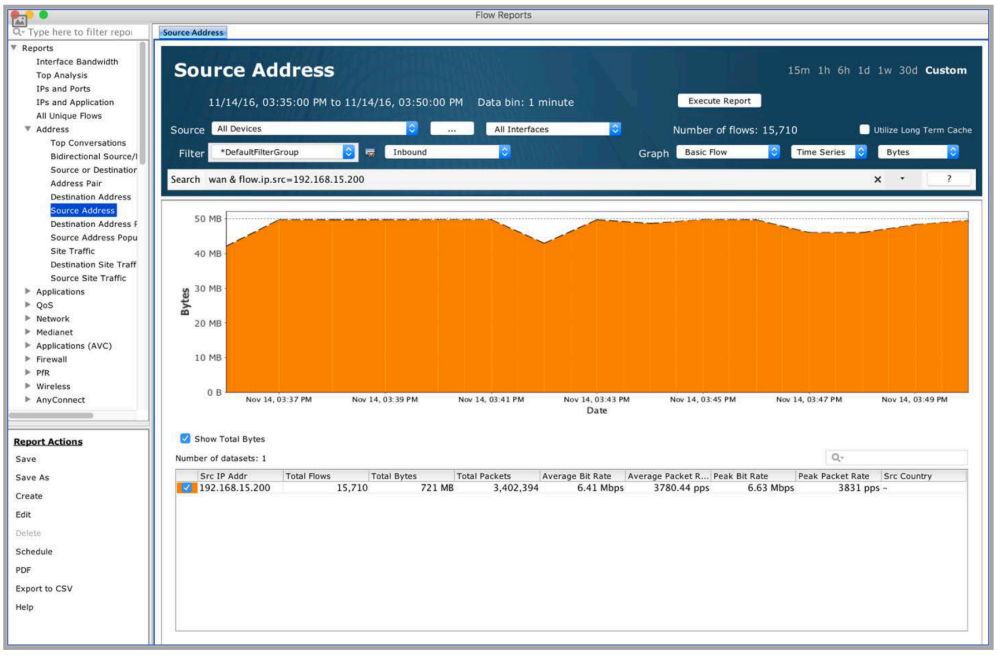
Right-click on Top 10 Source Addresses to generate a Source Address inbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the table.



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.



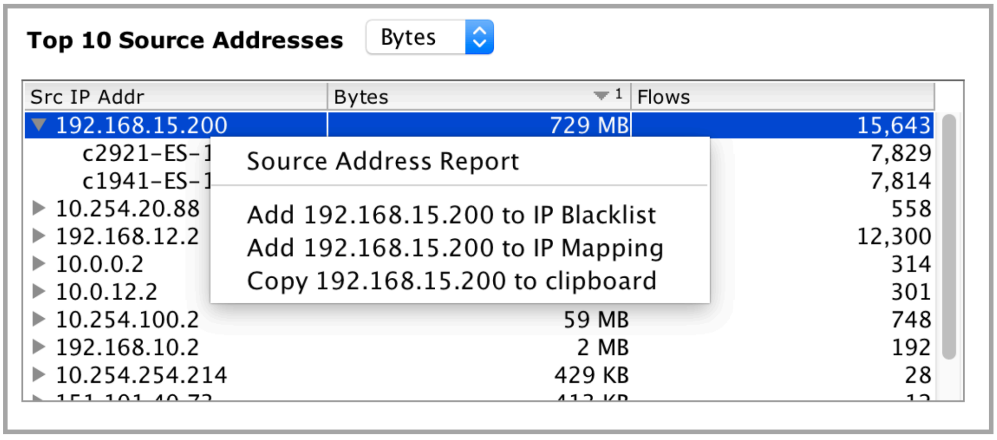
Graph View – generates a Source Address inbound flow report for the selected source IP address for all devices.



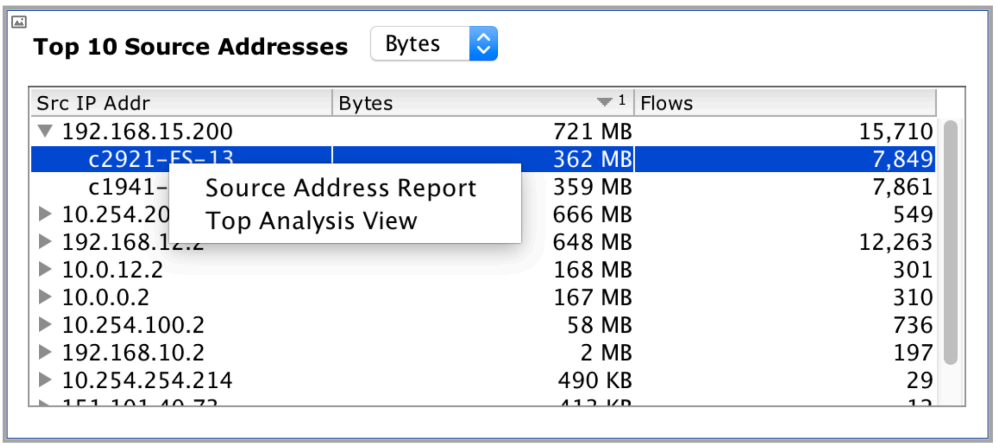
Add to IP Blacklist – adds the IP address to the LiveNX blacklist. The blacklist feature is covered in Chapter 12, *Tools*.

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*.

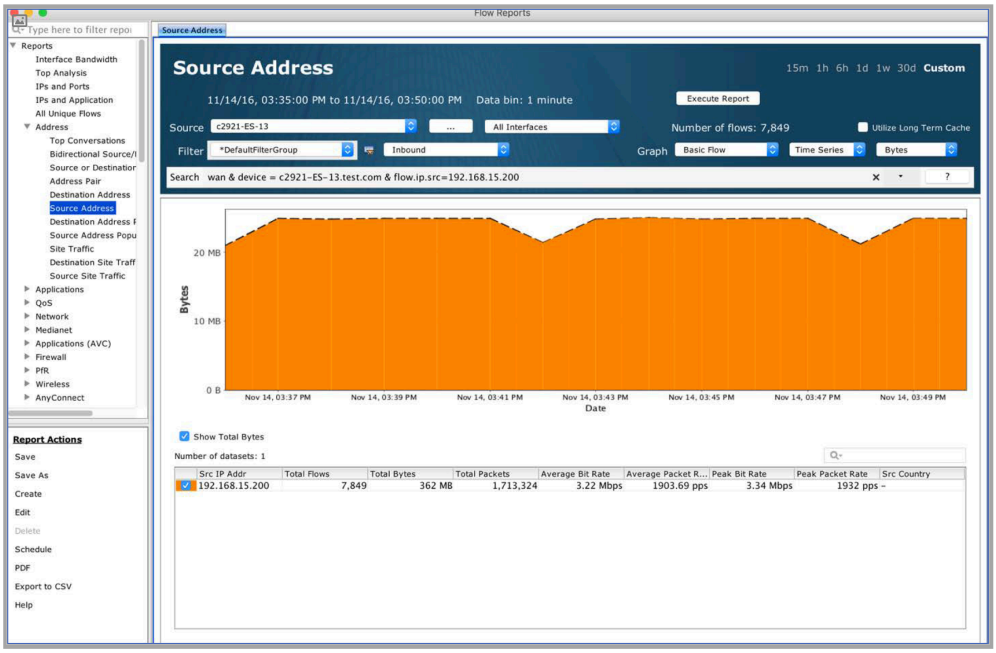
Copy to Clipboard – copies the selected IP address to the clipboard.



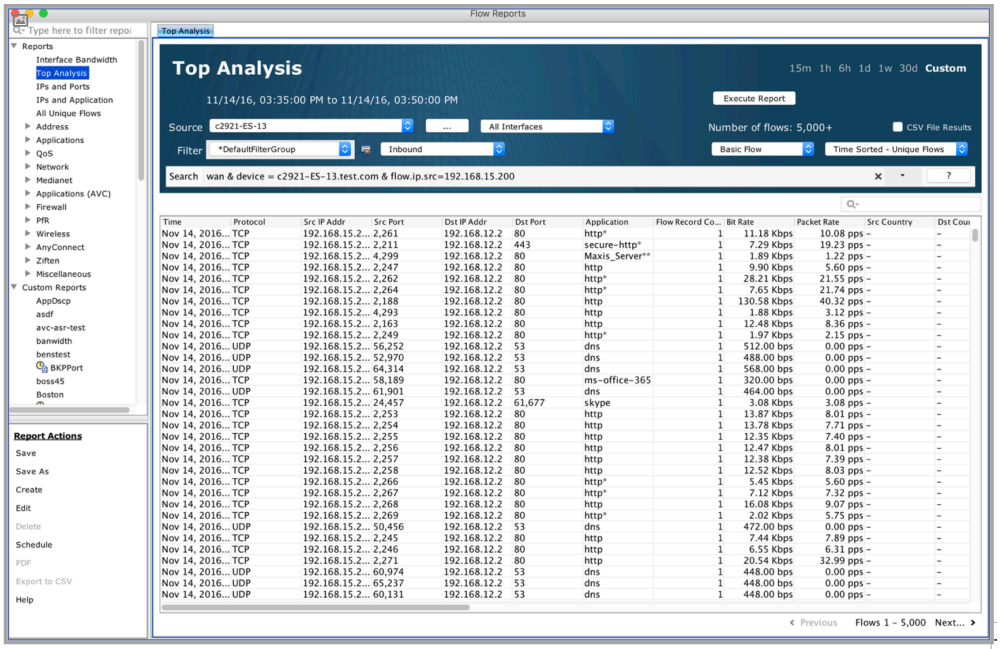
Expand an IP address to show devices and right click on a device to select between Graph View and Top Analysis View.



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.

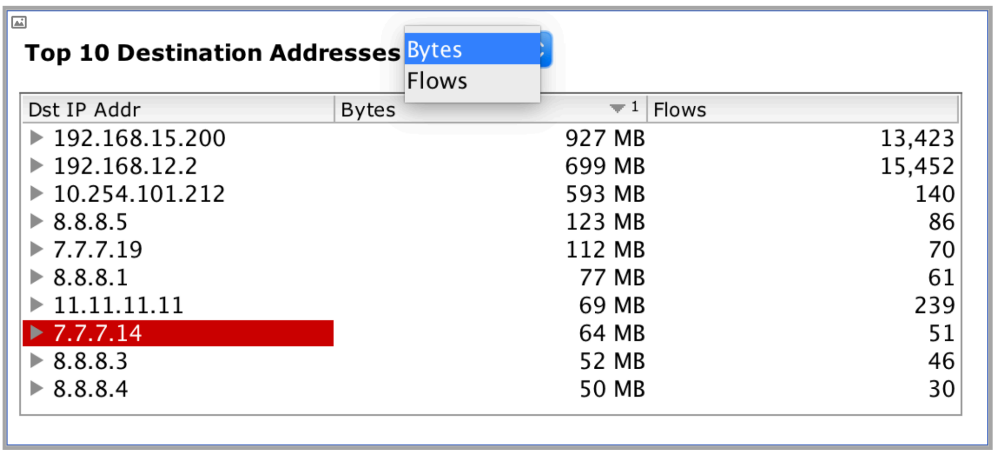


Top Analysis View – generates a Top Analysis inbound flow report for the selected device.

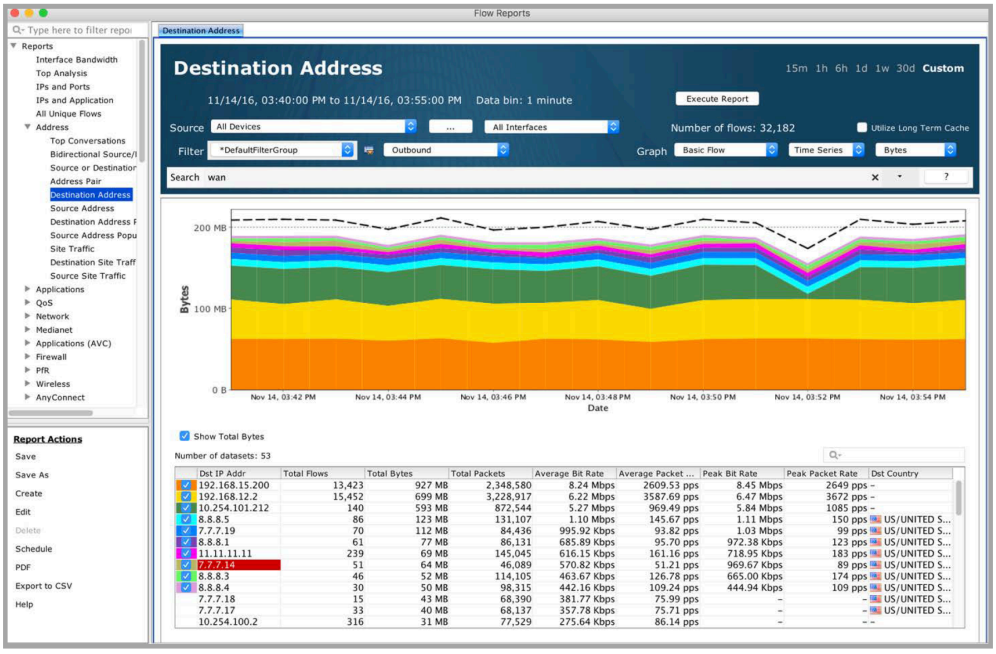


Top 10 Destination Addresses (Bytes or Flows)

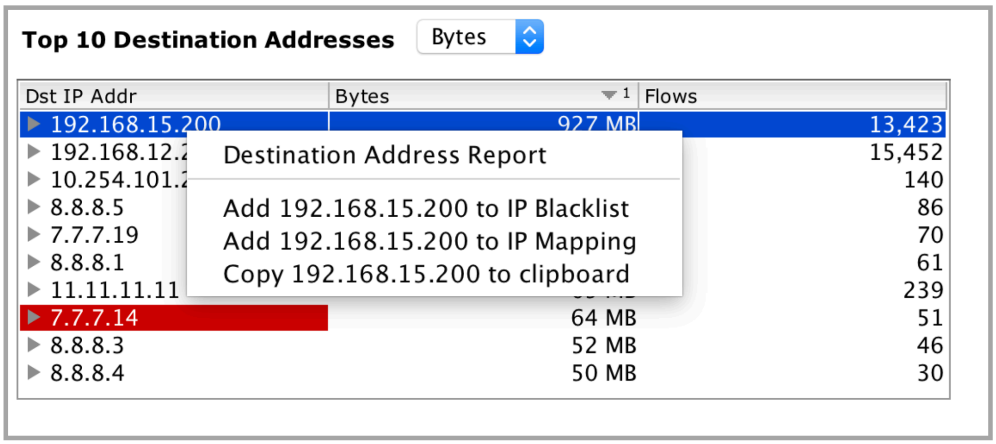
The Top 10 Destinations Addresses table lists the top 10 devices generating the largest number of bytes or flows to a particular destination address. Click on the + sign to the left of the IP address to show the devices associated with the Destination IP address.



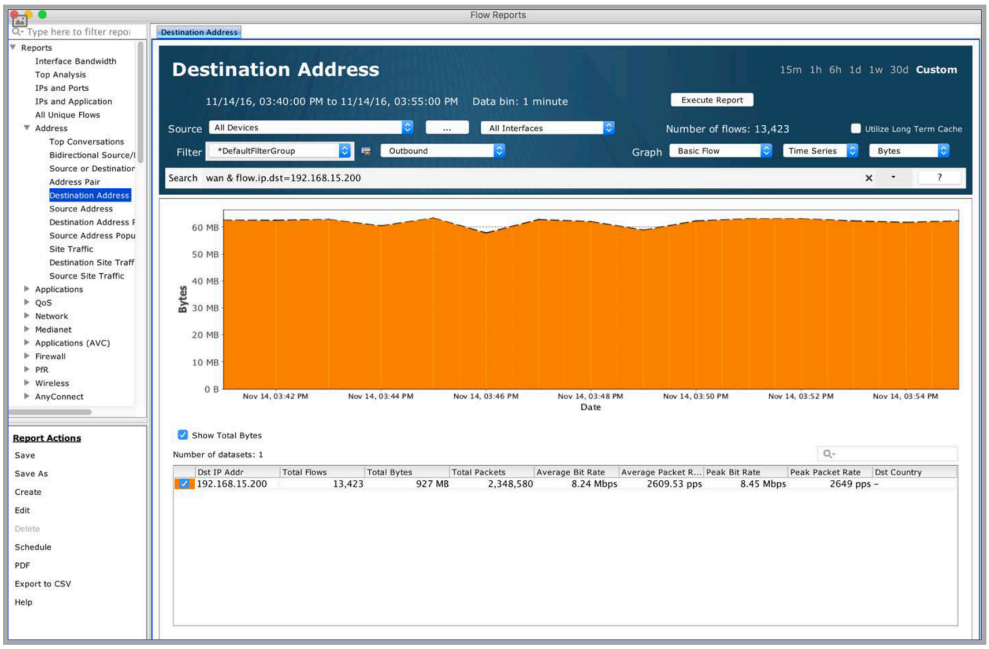
Click on the Top 10 Destination Addresses header to generate a Destination Address outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



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.



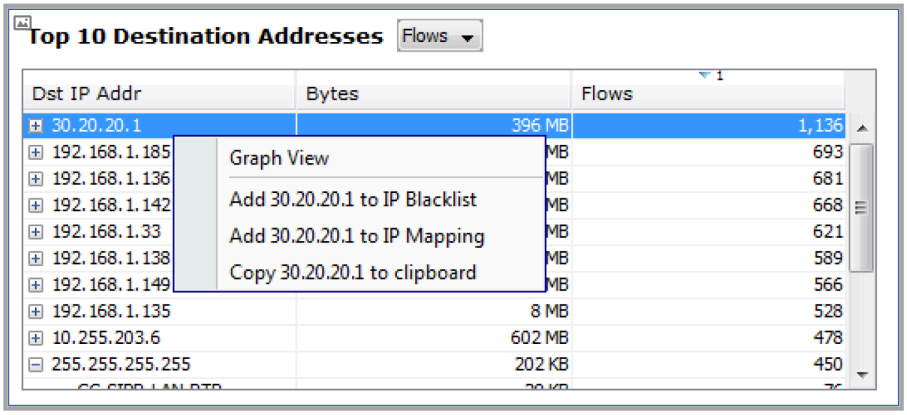
Graph View – generates a Destination Address outbound flow report for the selected source IP address for all devices.



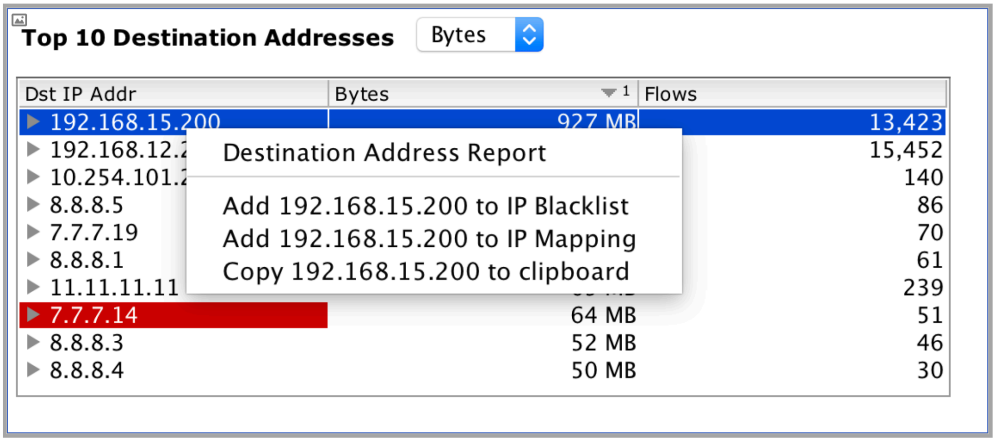
Add to IP Blacklist – adds the IP address to the LiveNX blacklist. The blacklist feature is covered in Chapter 12, *Tools*.

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*.

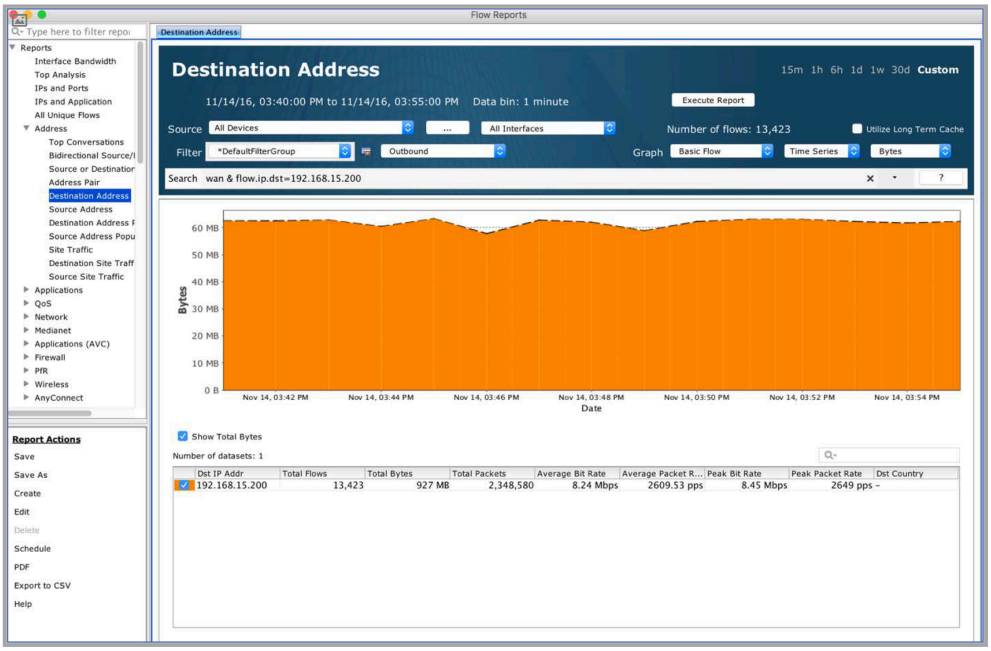
Copy to clipboard – copies the selected IP address to the clipboard.



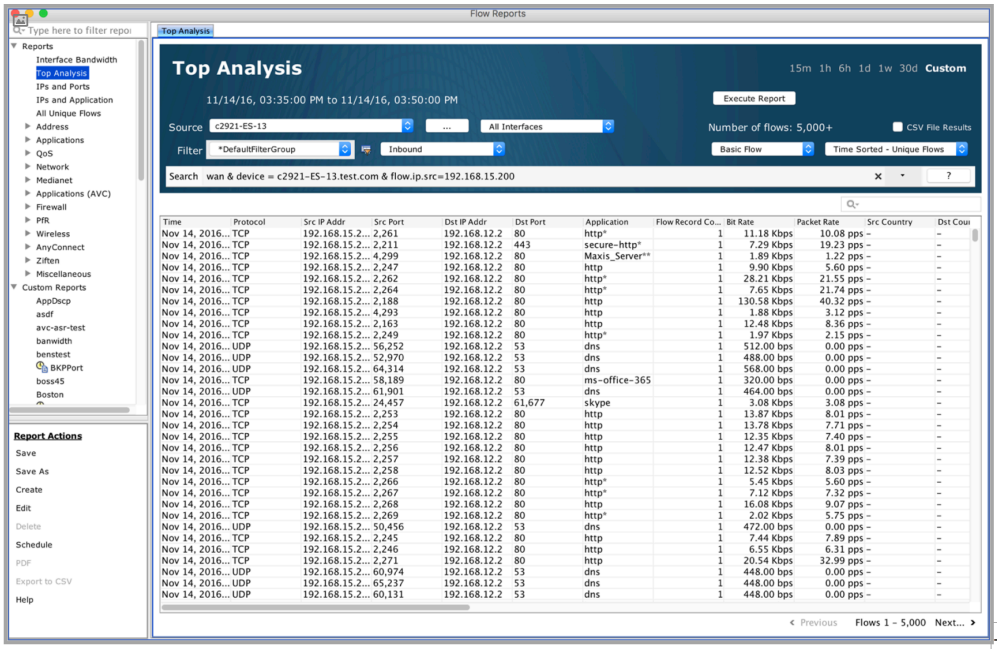
Expand an IP address to show devices and right click on a device to select between Graph View and Top Analysis View.



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.

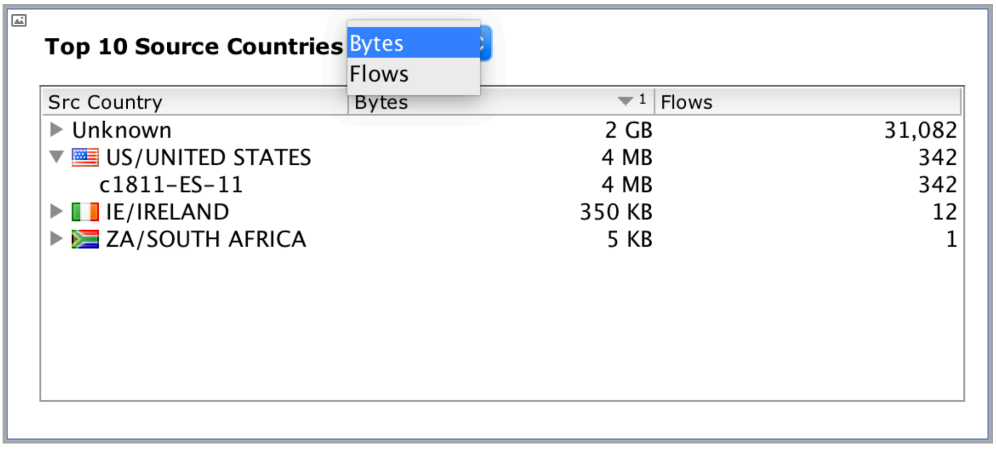


Top Analysis View – generates a Top Analysis outbound flow report for the selected device.



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.

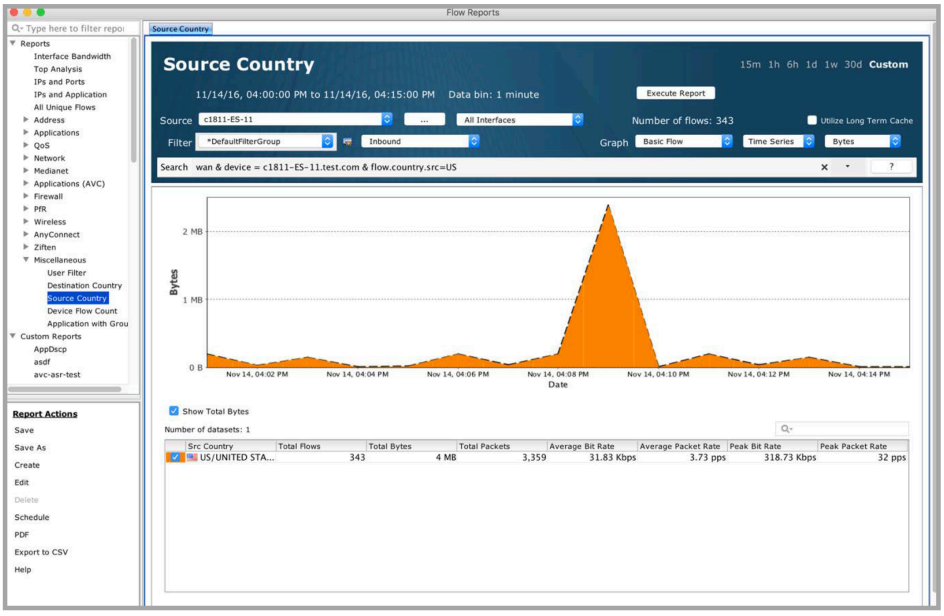


Click on the Top 10 Source Country header to generate a Source Country inbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

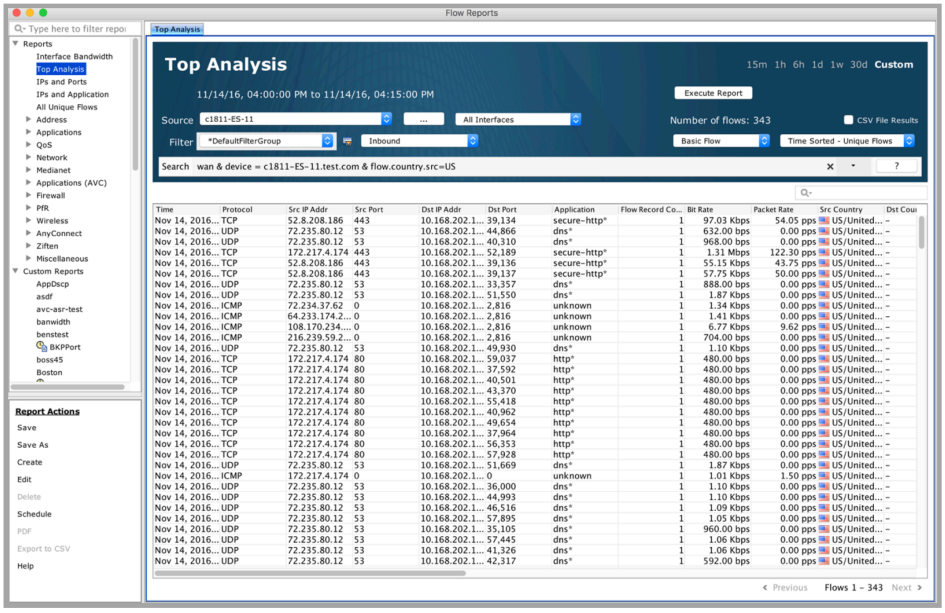
Right-click on a source country to display a Source Country inbound flow report specific to the selected country.

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.

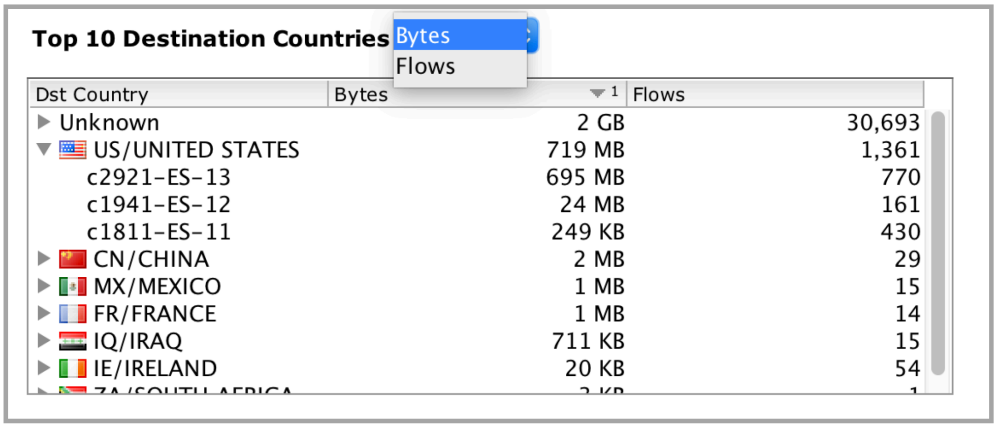


Top Analysis View – generates a Top Analysis inbound flow report for the selected device.

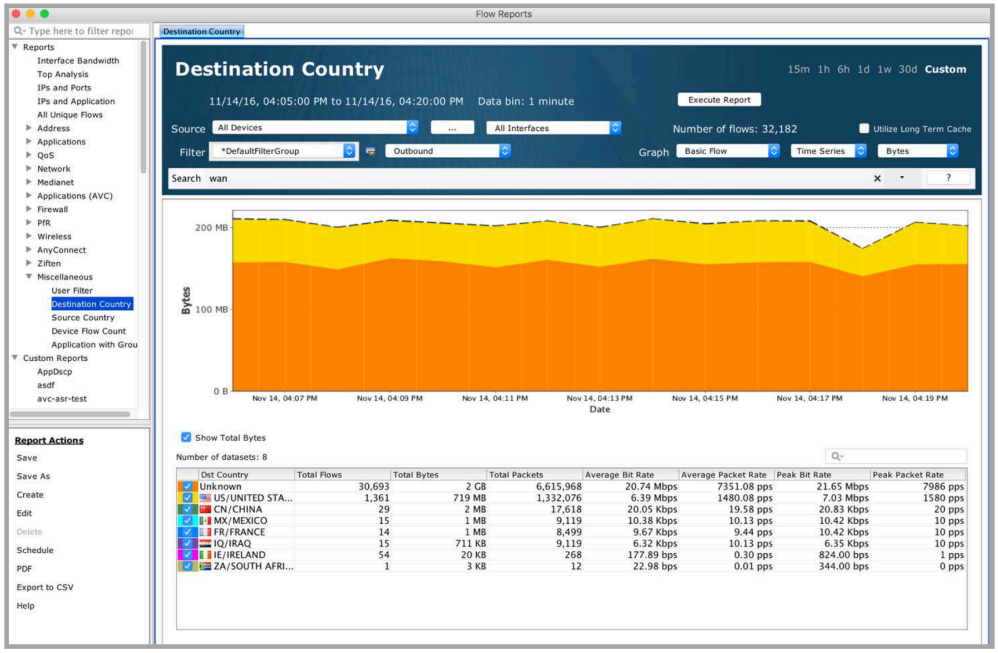


Top 10 Destination Countries [Bytes or Flows]

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.

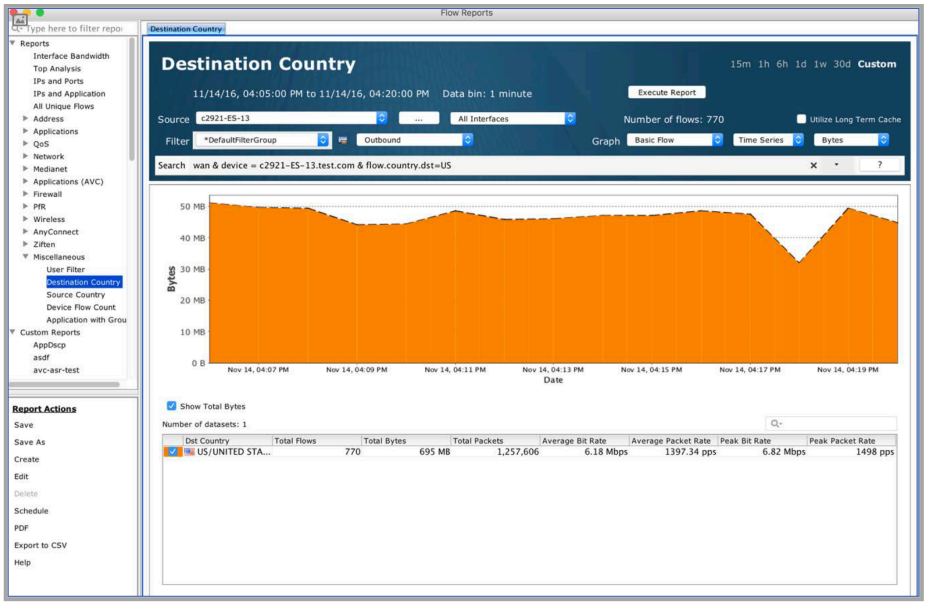


Click on the Top 10 Destination Country header to generate a Destination Country outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

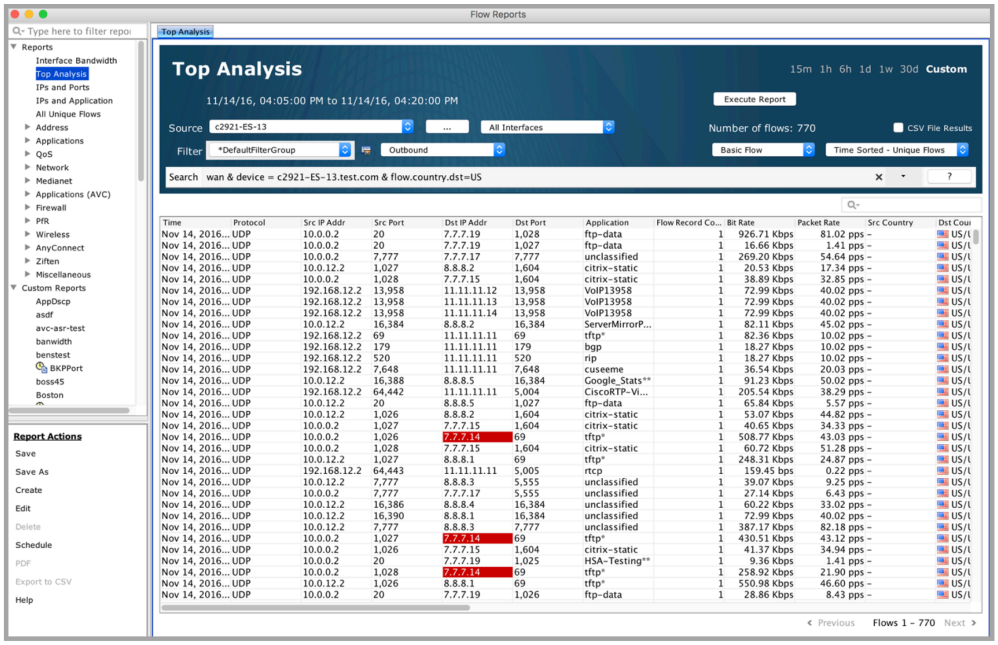


Right-click on a destination country to display a Destination Country outbound flow report specific to the selected country.

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



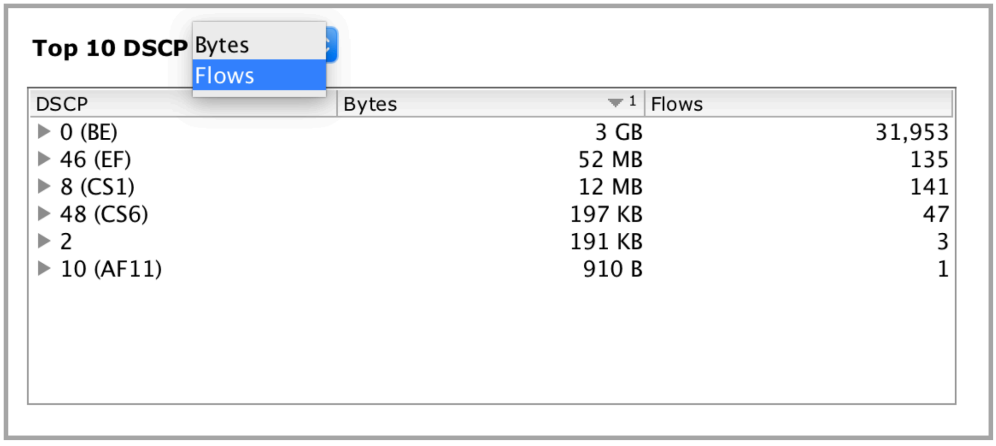
Graph View – generates a Destination Country outbound flow report for the selected destination country for all devices. A Tag Filters alert dialog window may appear to ask if you would like to query for All Devices.



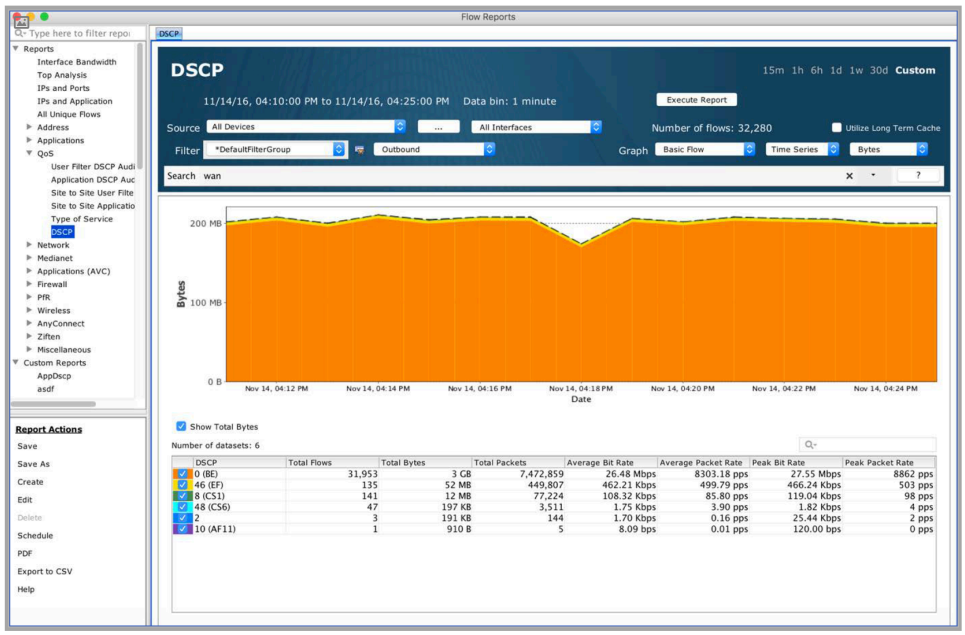
Top Analysis View – generates a Top Analysis outbound flow report for the selected device.

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.



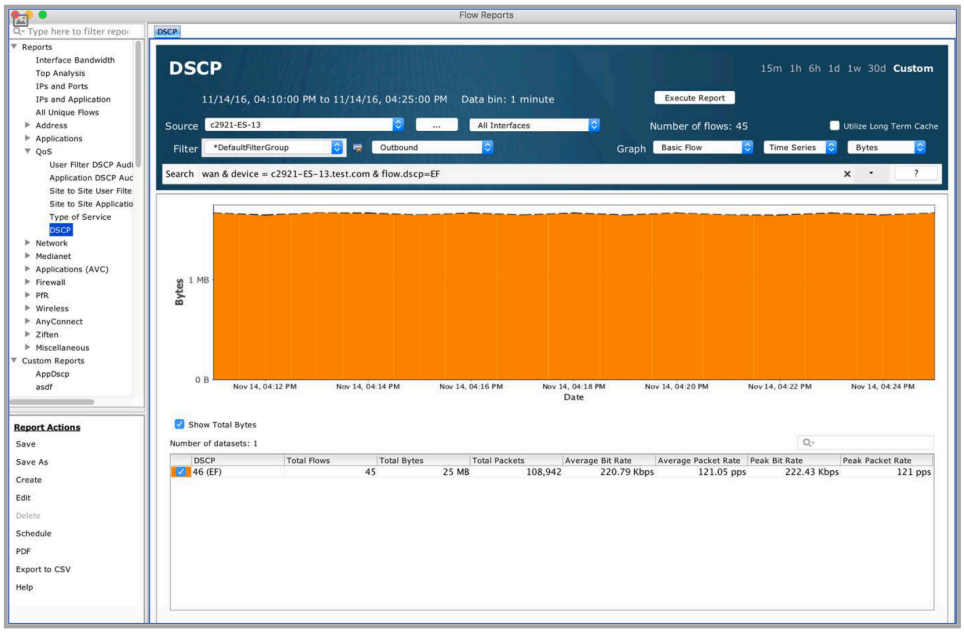
Click on the Top 10 DSCP header to generate a DSCP outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



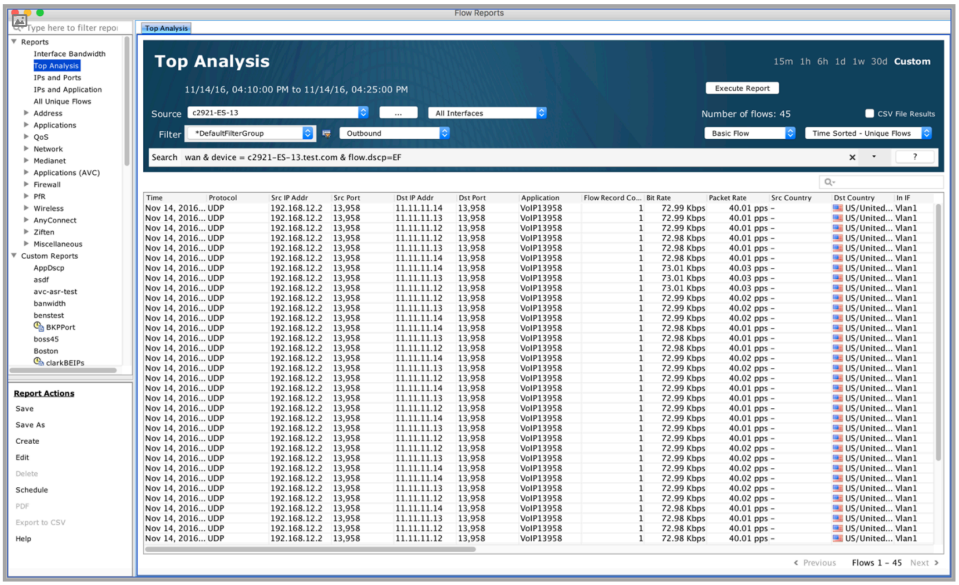
Right-click on a DSCP value to generate an outbound flow report specific to the selected DSCP value.

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.

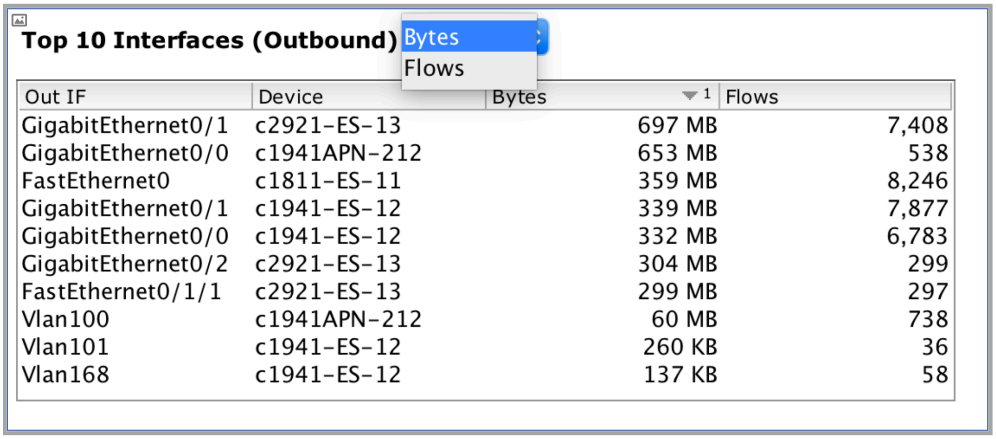


Top Analysis View – generates a Top Analysis outbound flow report for the selected device.



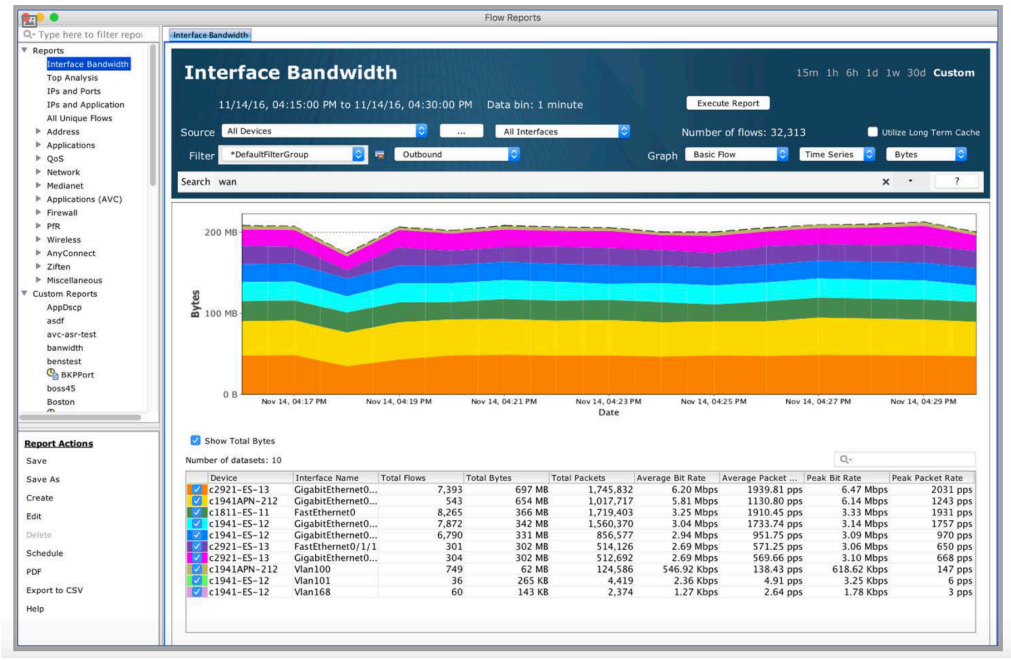
Top 10 Interfaces (Outbound) [Bytes or Flows]

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



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

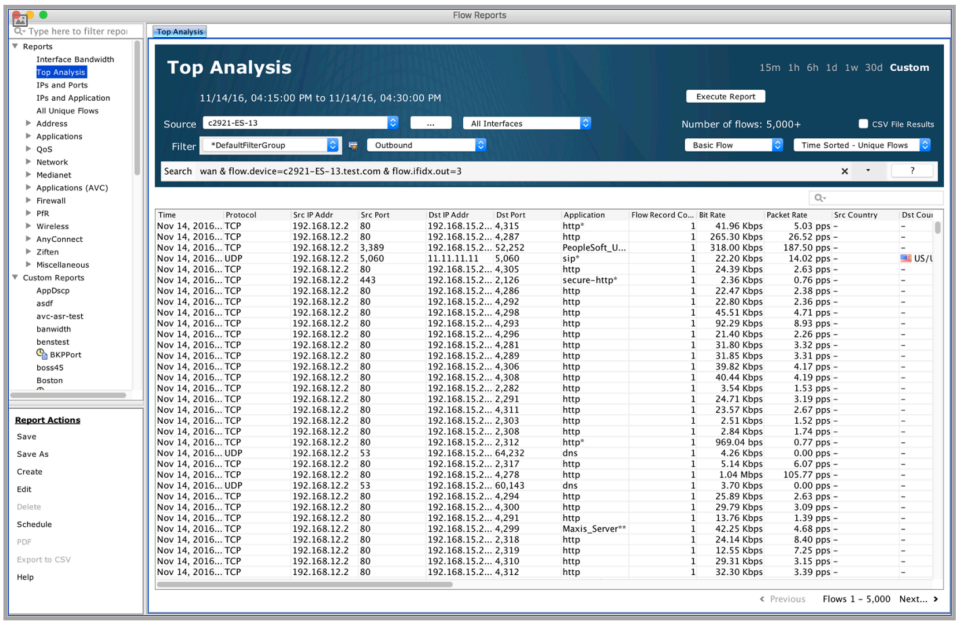
Click on the Top 10 Interfaces (Outbound) to generate a Traffic Volume Pair outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.



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

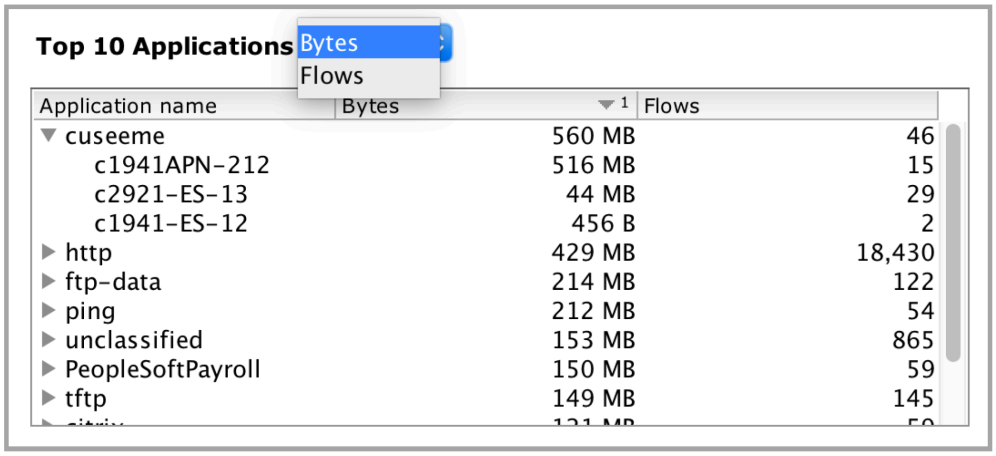
Graph View – generates a Traffic Volume Pair outbound flow report for the selected output interface.

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



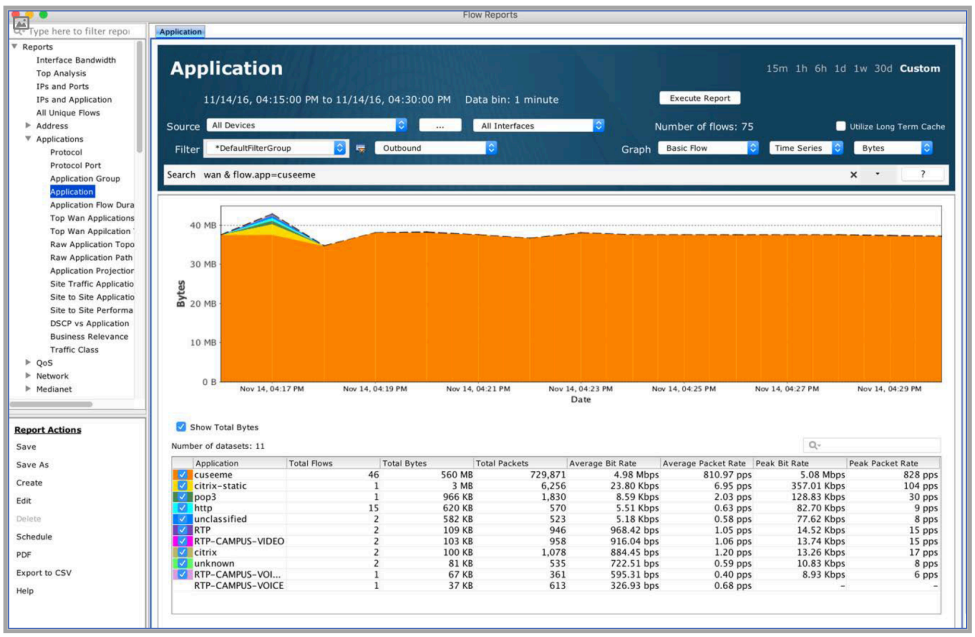
Top 10 Application [Bytes or Flows]

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.



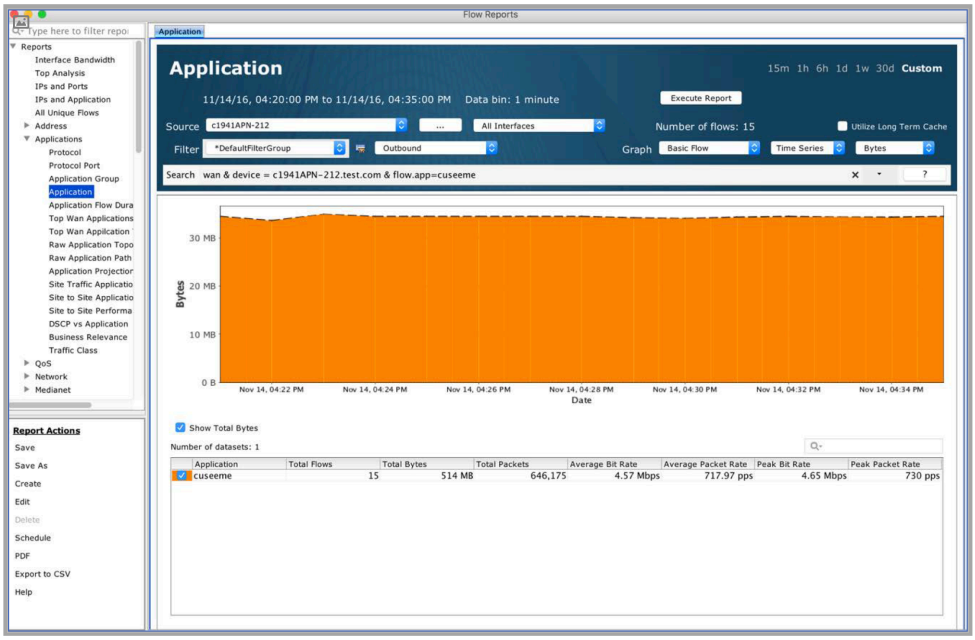
Click on the Top 10 Applications header to generate an Application outbound flow report for all devices and all interfaces sorted in order by Bytes or Flows as selected from the previous table.

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

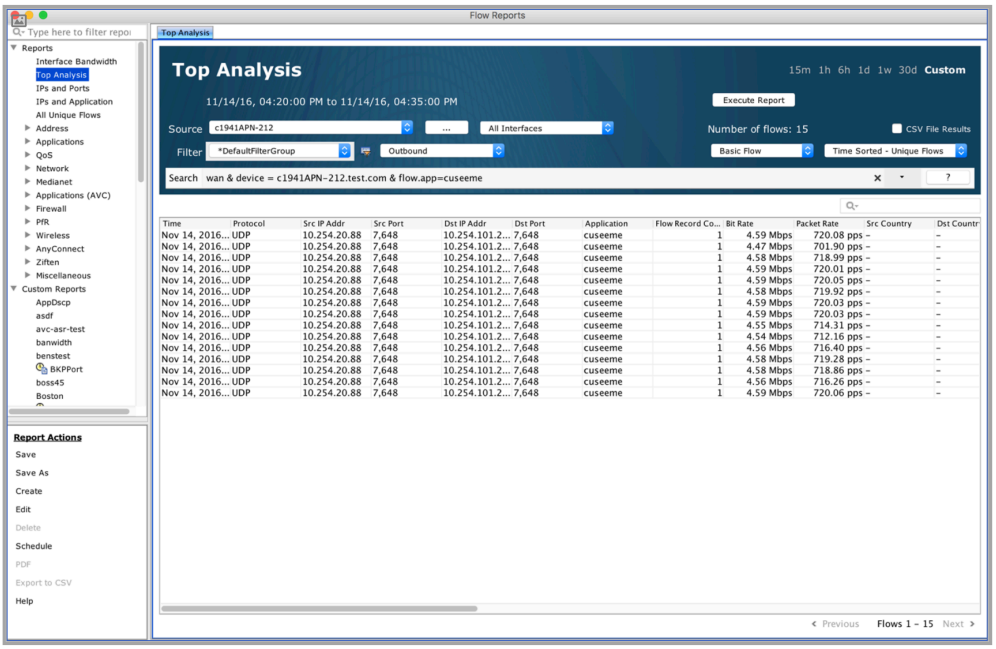


Expand an application in the table to show devices and right click on a device to select between Graph View and Top Analysis View.

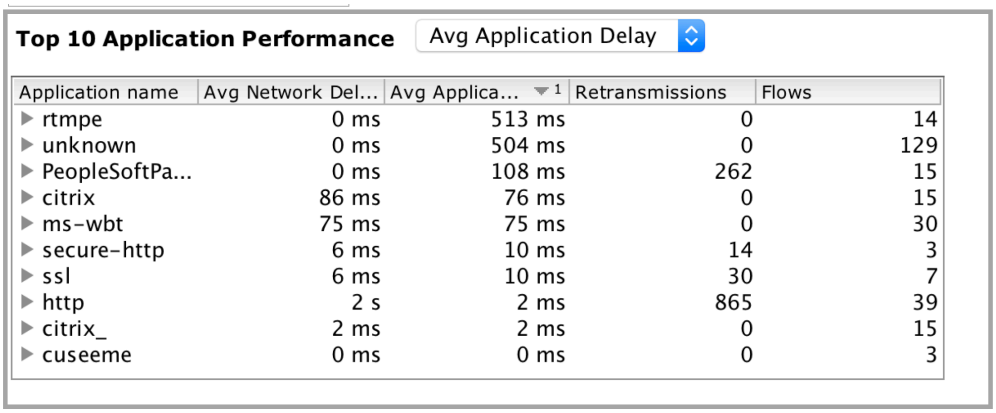
Graph View – generates an Application outbound flow report for all applications and all devices within the system.



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



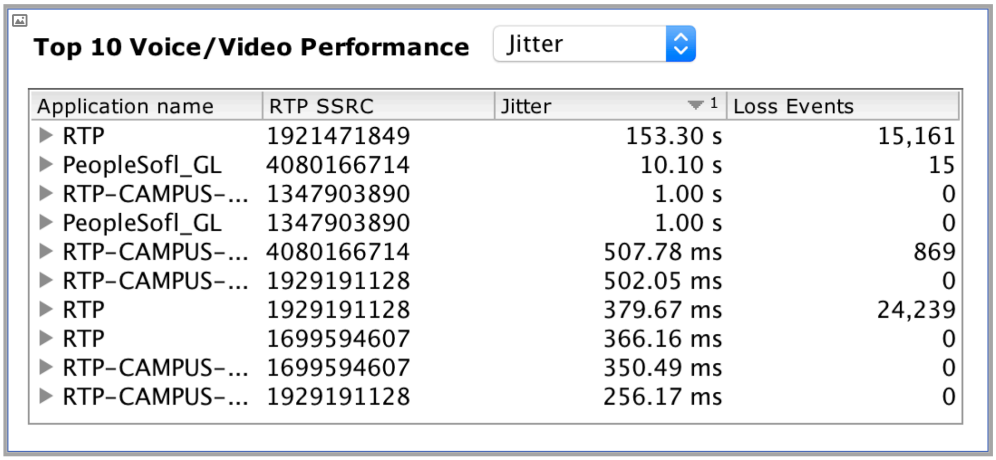
Top 10 Application Performance



Top 10 Application Performance Avg Application Delay

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/Video Performance Jitter

Application name	RTP SSRC	Jitter ▼1	Loss Events
▶ RTP	1921471849	153.30 s	15,161
▶ PeopleSofl_GL	4080166714	10.10 s	15
▶ RTP-CAMPUS-...	1347903890	1.00 s	0
▶ PeopleSofl_GL	1347903890	1.00 s	0
▶ RTP-CAMPUS-...	4080166714	507.78 ms	869
▶ RTP-CAMPUS-...	1929191128	502.05 ms	0
▶ RTP	1929191128	379.67 ms	24,239
▶ RTP	1699594607	366.16 ms	0
▶ RTP-CAMPUS-...	1699594607	350.49 ms	0
▶ RTP-CAMPUS-...	1929191128	256.17 ms	0

Top 10 HTTP Host

Top 10 HTTP Host HTTP Hit Count

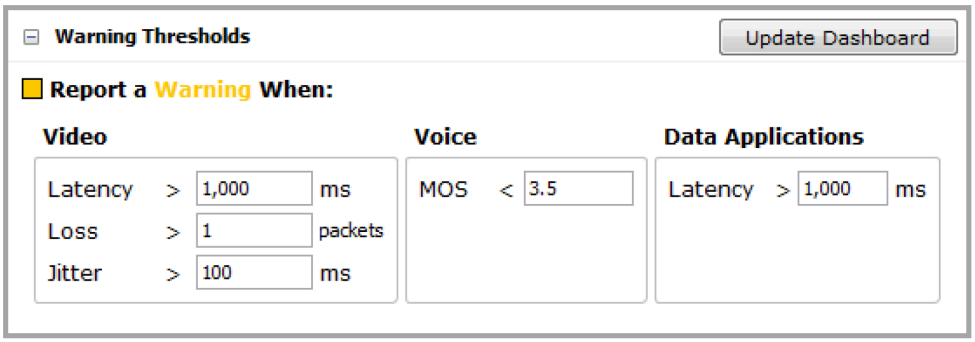
HTTP Host	HTTP Hit Count	Bytes
cdn.content.prod.cms.msn.com	47	110 KB
wpad.apn.com	42	106 KB
wpad.APN.COM	36	59 KB
fonts.googleapis.com	32	13 KB
www.pandora.com	29	8 MB
mail.office365.com	29	14 KB
www.ebay.com	29	5 MB
www.cisco.com	29	2 MB
www.gotomeeting.com	28	26 KB
www.salesforce.com	25	22 KB

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.

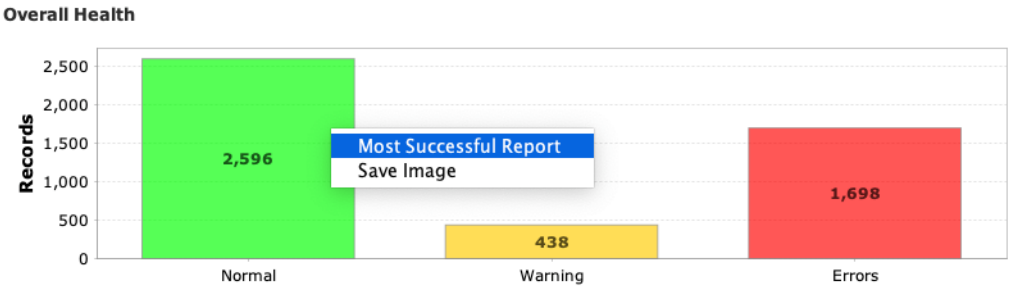
Click on the + sign next to Warning Thresholds to customize the dashboard parameters. This is a Warning message specific to the IP SLA technology and does not generate alerts in the LiveNX system.



- 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.

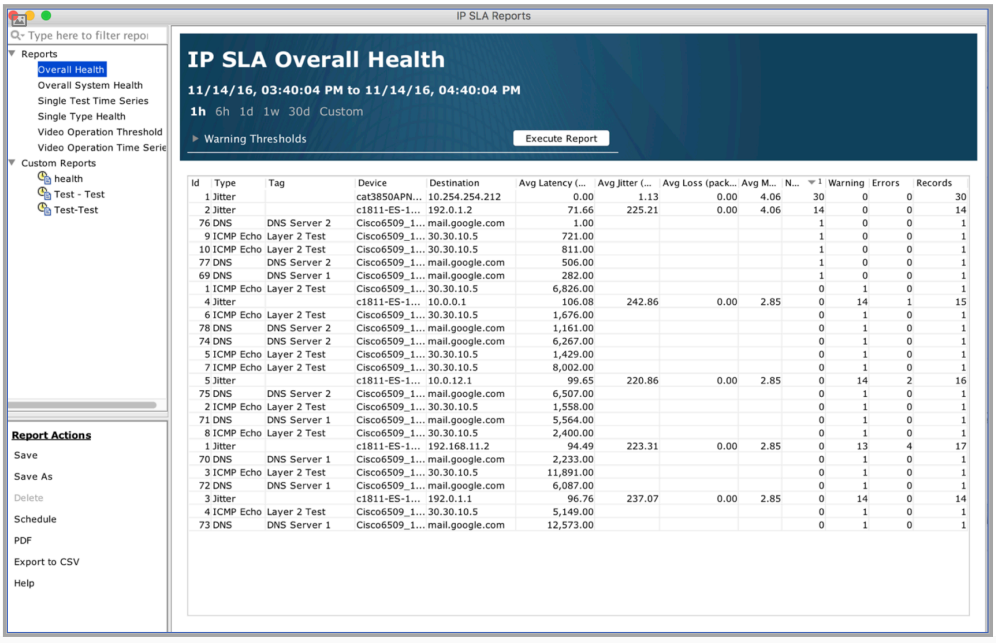
- Data applications are a collection of IP SLA test types, including, DNS, DHCP, HTTP, FTP, PATH_ECHO, UDP_ECHO, and ICMP_ECHO tests. Latency is the most important value for these tests.

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.

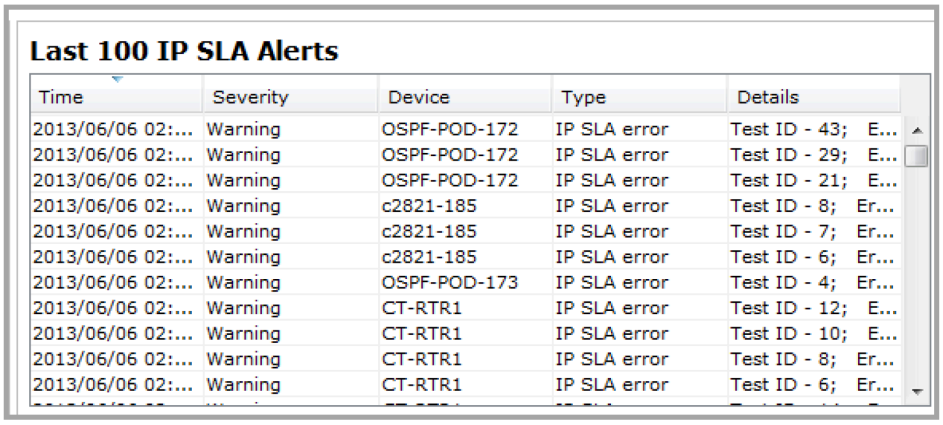
IP SLA Overall Health report: depending on the bar chart selected, LiveNX generates an IP SLA Overall Health report sorted by Normal in highest to lowest order if you right clicked on the Normal bar, Warning in highest to lowest order if you right clicked on the Warnings bar, and Errors in highest to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



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.

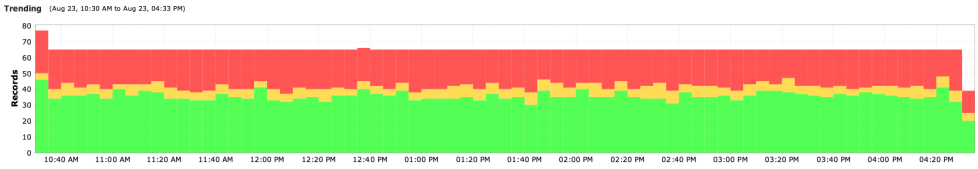


Last 100 IP SLA Alerts

Time	Severity	Device	Type	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.

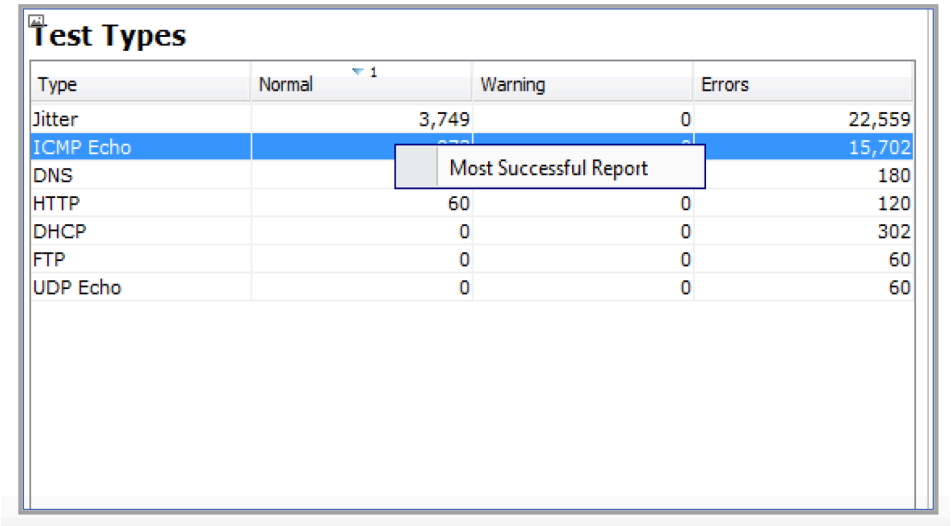


Reset Zoom – left click and drag to zoom the trending chart to the area selected. Use the Reset Zoom to return to the default view.

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.

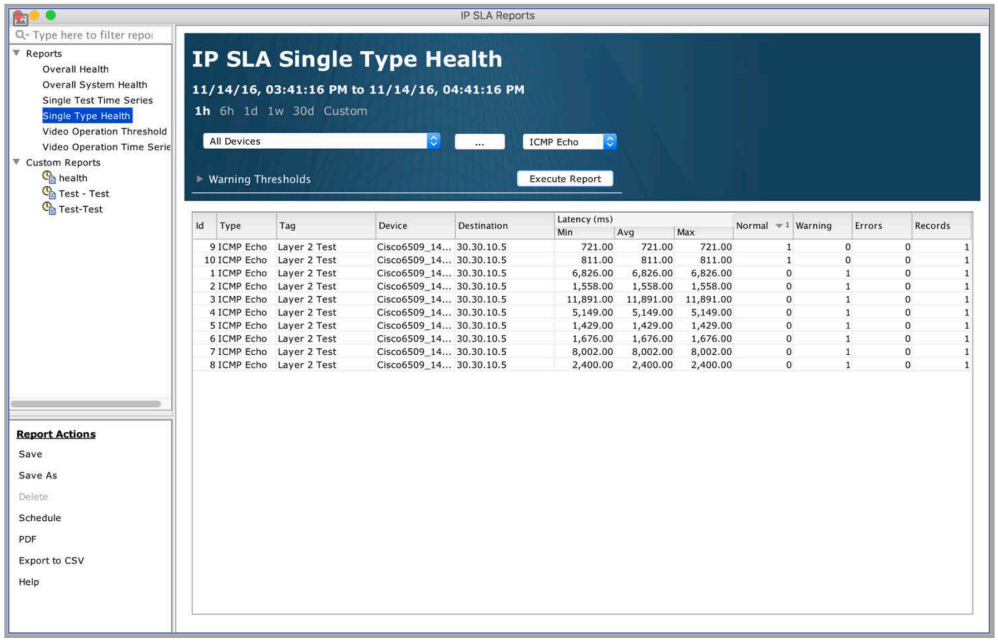


Test Types

Type	Normal	Warning	Errors
Jitter	3,749	0	22,559
ICMP Echo			15,702
DNS			180
HTTP	60	0	120
DHCP	0	0	302
FTP	0	0	60
UDP Echo	0	0	60

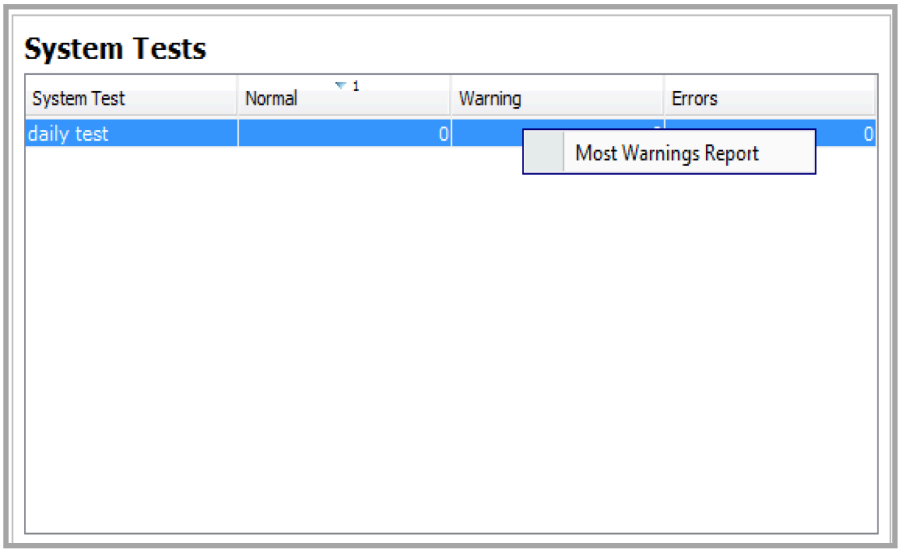
Most Successful Report

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.

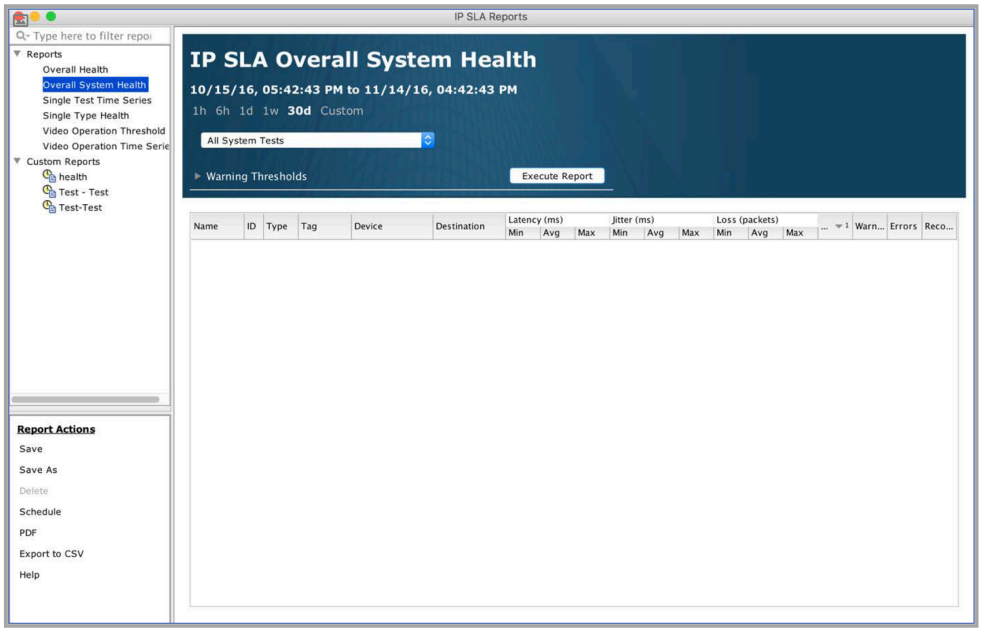


System Tests

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

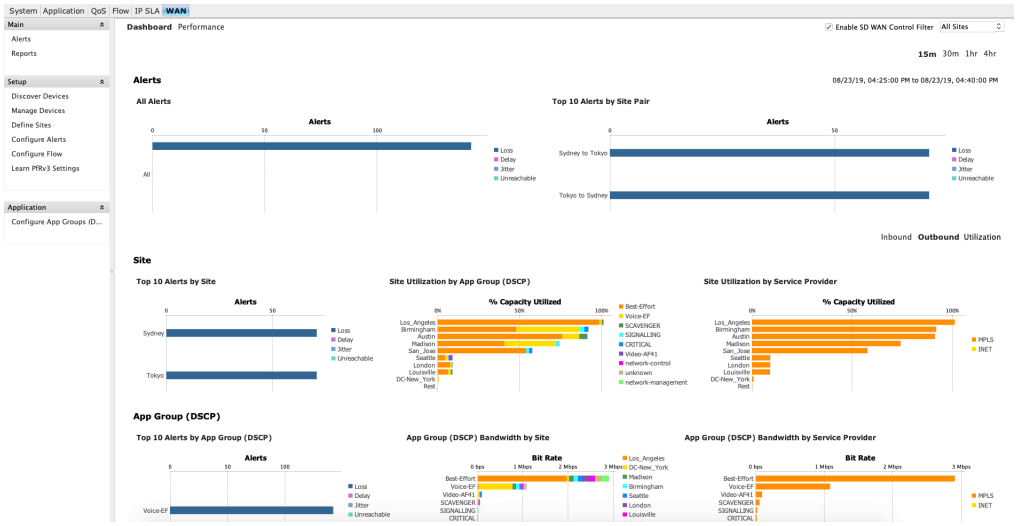


Highlight a row and then right-click on an entry in the Normal, Warning or Errors cell to generate an IP SLA System Test Health report for the selected system test sorted by the most Normal, the most Warnings or the most Errors, respectively.



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).



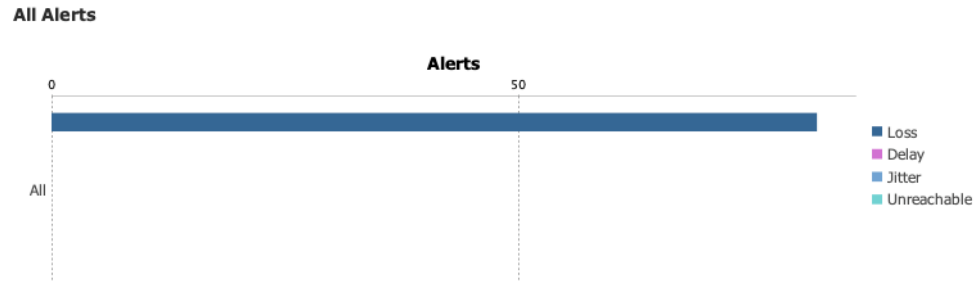
Configure App Groups

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.

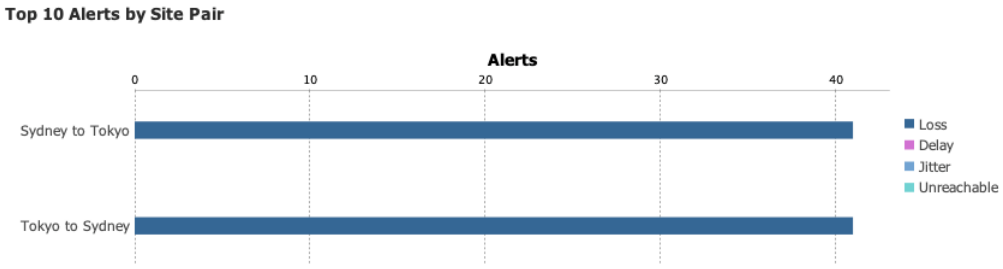
The PfR dashboard charts alerts, site, application group and service provider statistics in either the Inbound or Outbound direction. Click on either Inbound or Outbound to select the direction; default is Outbound. The charts compute statistics for the last 15 minutes, 30 minutes, 1 hour or 4 hours. 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.



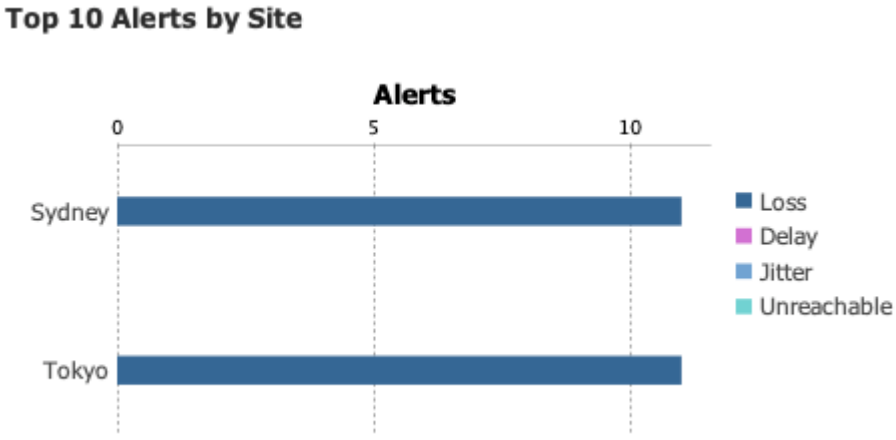
Top 10 Alerts by Site Pair charts the top 10 site pairs that generate the largest number of alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. The sites are device level attributes that are user-defined in the Device/Interface tree view.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



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

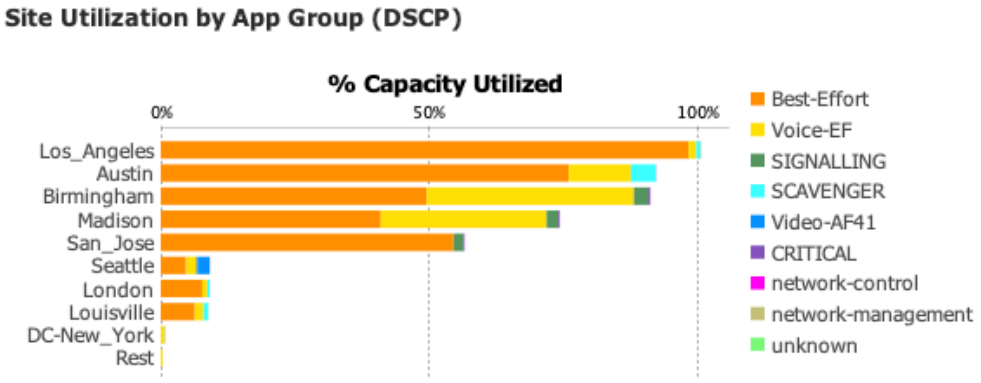
Top 10 Alerts by Site charts the top 10 sites generating the most alerts. The alerts are charted in a stacked bar chart format, color-coded to indicate the four types of PfRv3 alerts. The sites are device level attributes that are user-defined in the Device/Interface tree view.



Site Utilization by Application Group

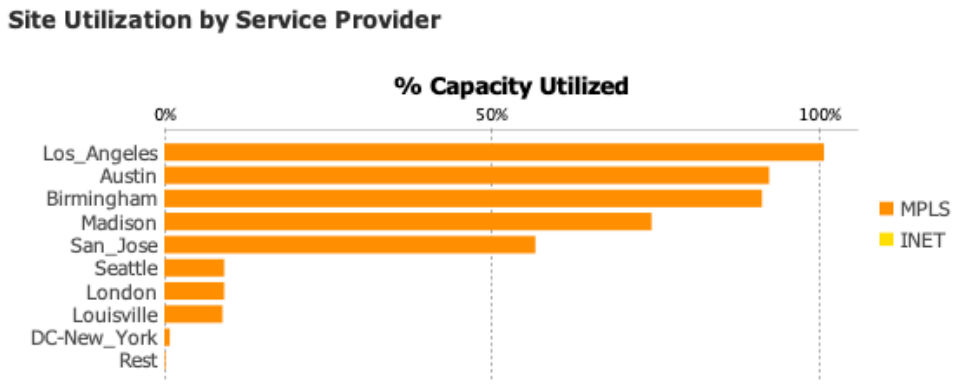
Site Utilization by Application Group charts the capacity of each site, based on the application groups. The capacity is charted in a stacked bar chart format, color-coded to indicate the applications used by

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.



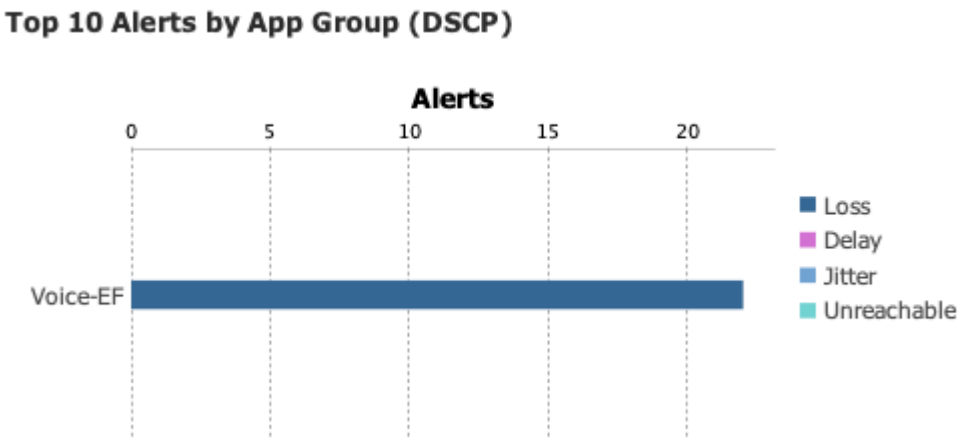
Site Utilization by Service Provider

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.



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.

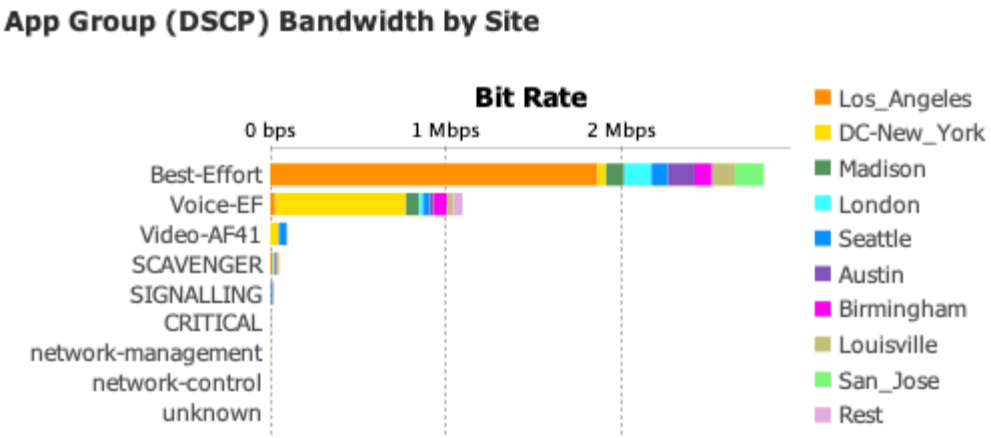
Top 10 Alerts by Application Group



Top 10 Alerts by 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.

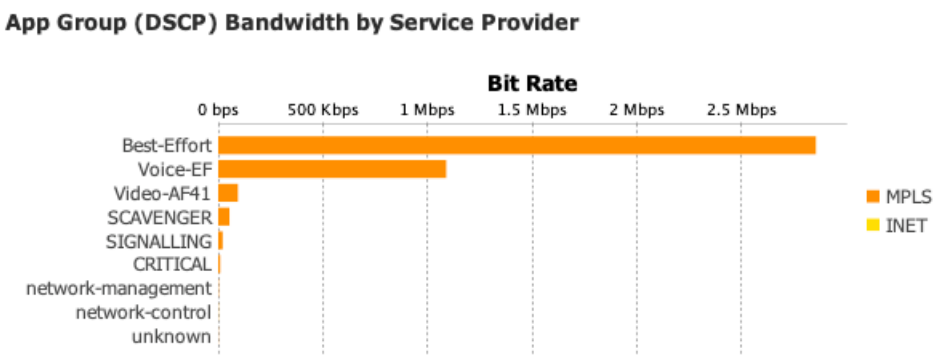
Application Group Bandwidth by Site

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.



Application Group Bandwidth by Service Provider

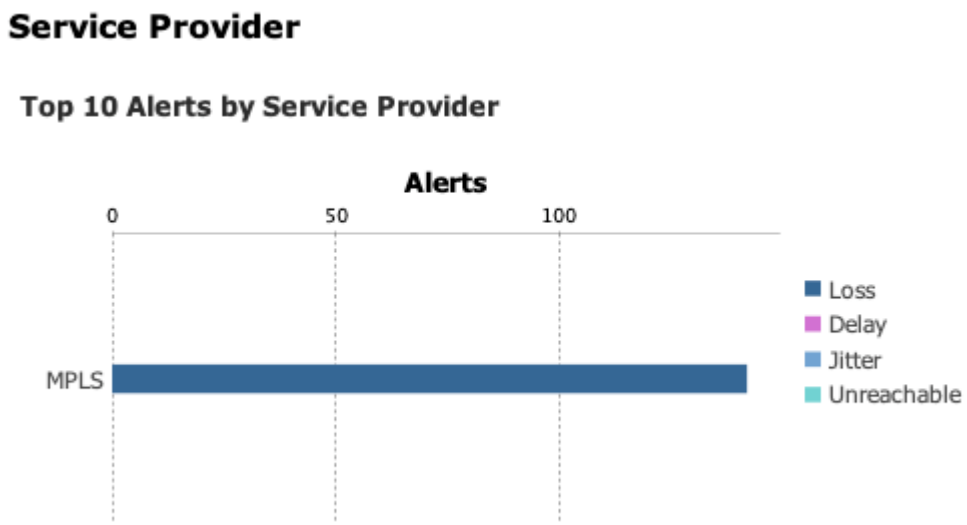
Application Group Bandwidth by Service Provider charts the highest bandwidth applications by application group. The application groups are charted in a stacked bar chart format, color-coded to indicate the various service providers associated with the application groups. The service providers are interface 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.



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.

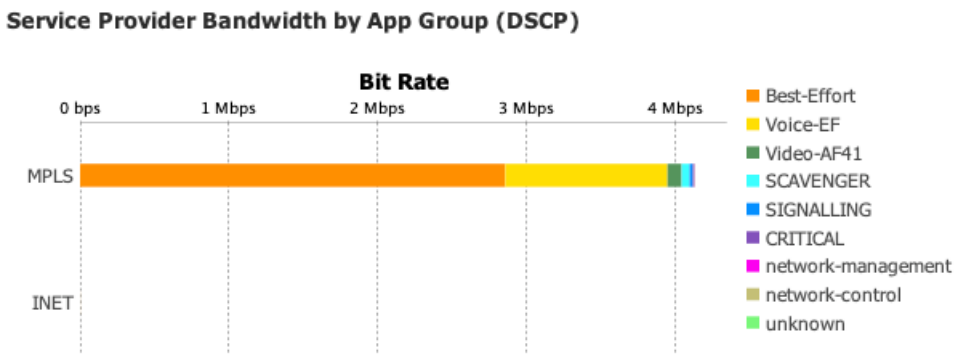
Top 10 Alerts by Service Provider

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.



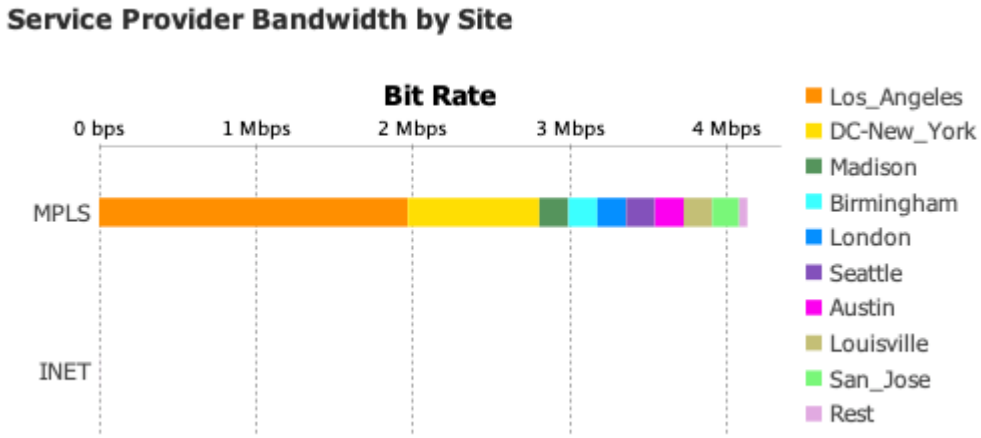
Service Provider Utilization by Application Group

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 Utilization by Site

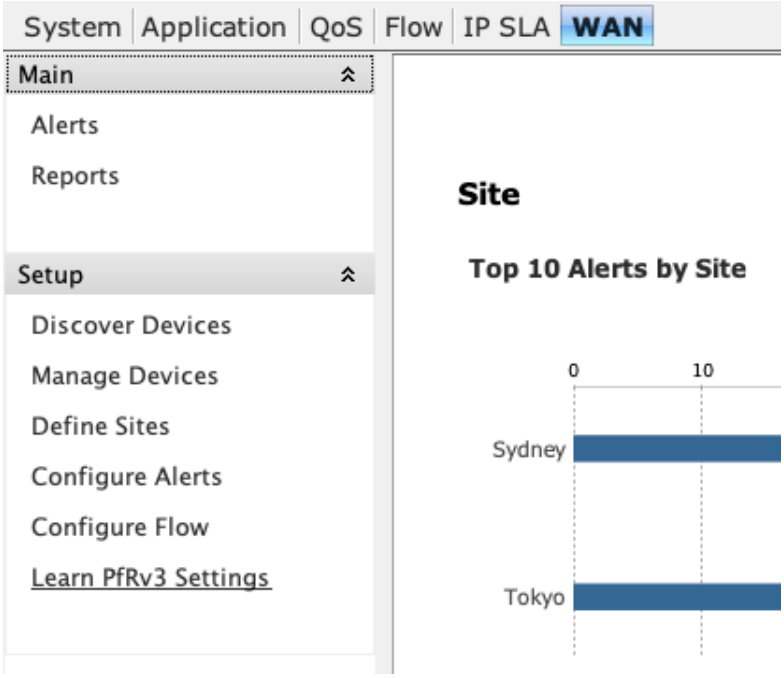
Service Provider Utilization by Site charts the percent of capacity utilized by service provider. The utilized capacity is charted in a stacked bar chart format, color-coded to indicate the sites associated with that service provider. Sites are device attributes while capacities and service providers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



Learn PfRv3 Settings

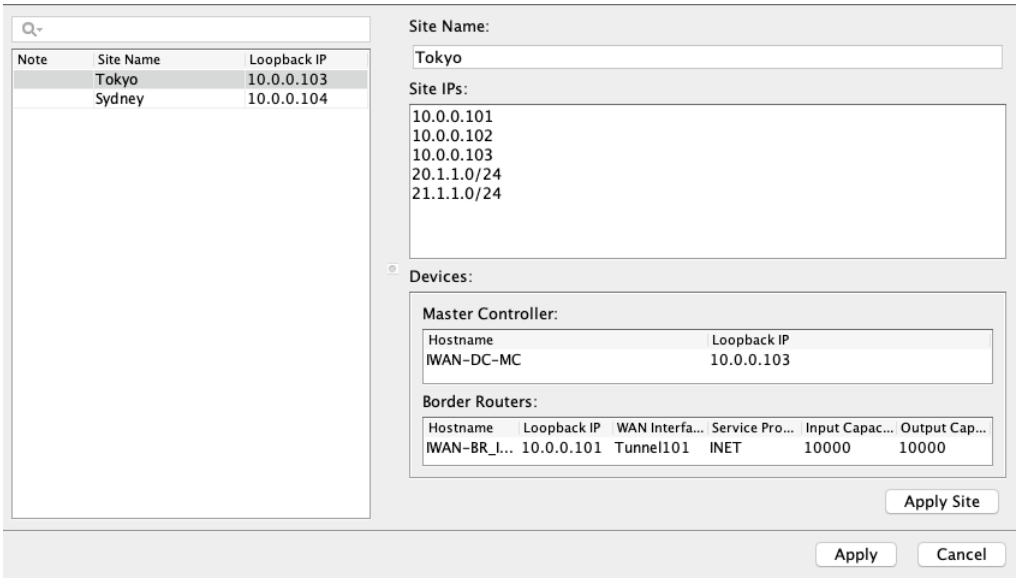
The Learn PfRv3 Settings feature allows users to easily setup the PfR/IWAN semantics to monitor Performance. These Settings will allow LiveNX to populate the WAN/PfR dashboard. The settings learned are as follows:

- 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



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.

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).

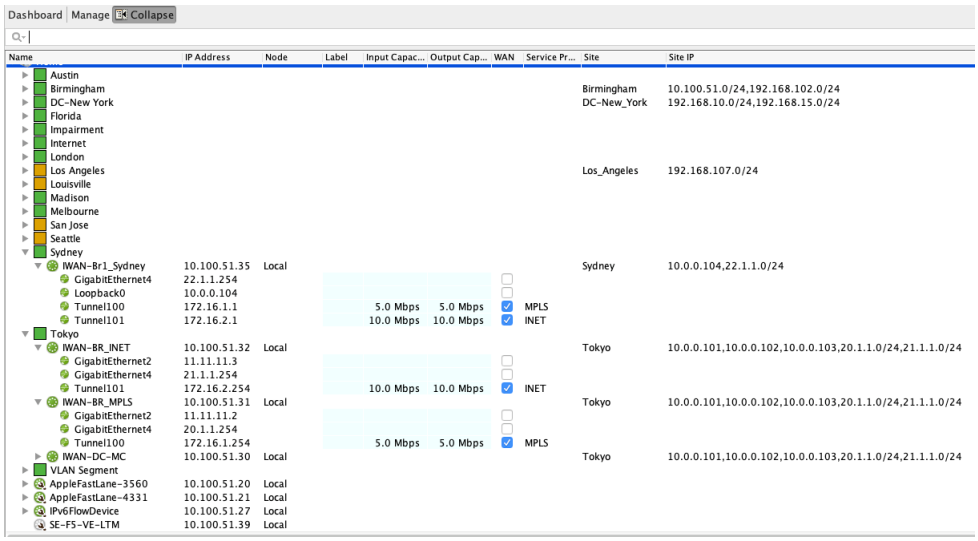


The Note Column Identifies the Following

- 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



- 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

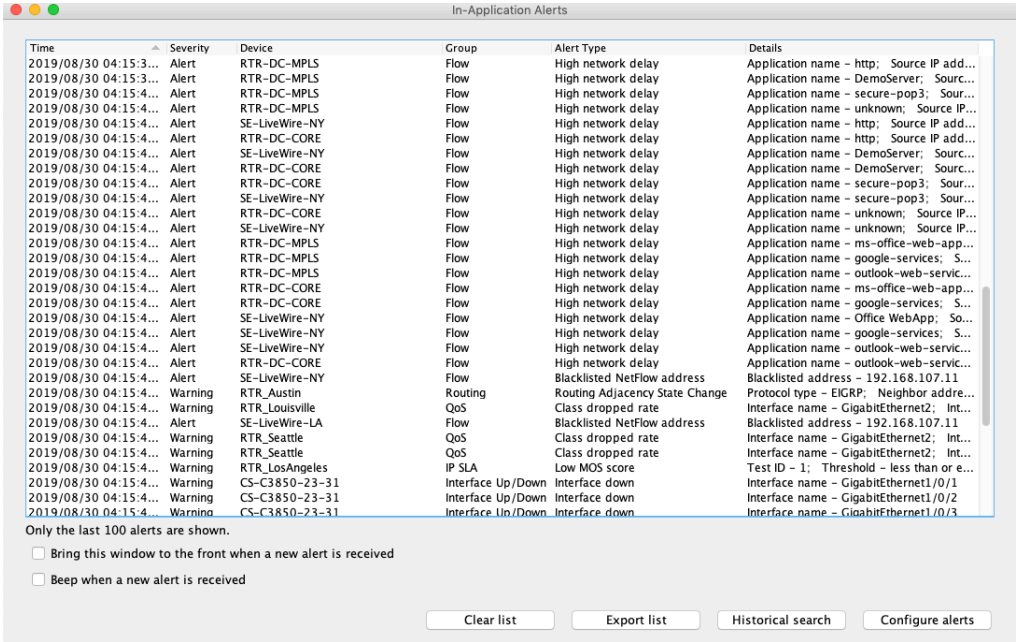
In this chapter:

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.



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.

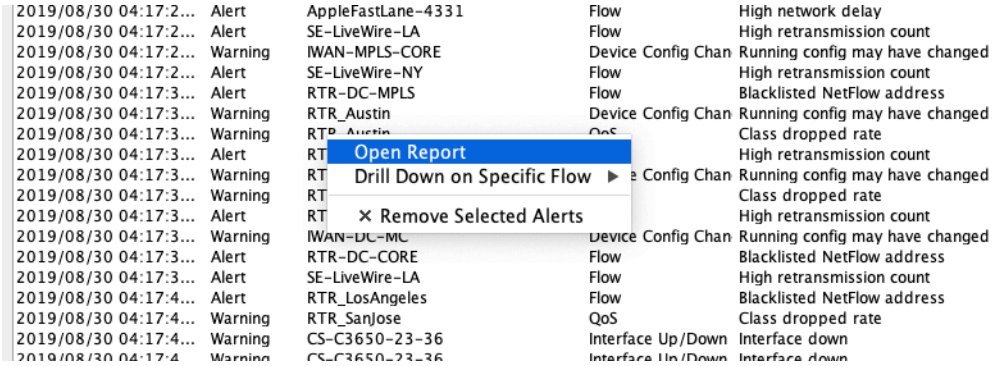
- Clear List – clicking on this button immediately clears the In-Application Alert window
- Export List – allows the user to store the alert information in a .csv format
- Historical Search – provides the user with historical and sorting capability for the alerts
- Configure Alerts – allows user-defined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



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.

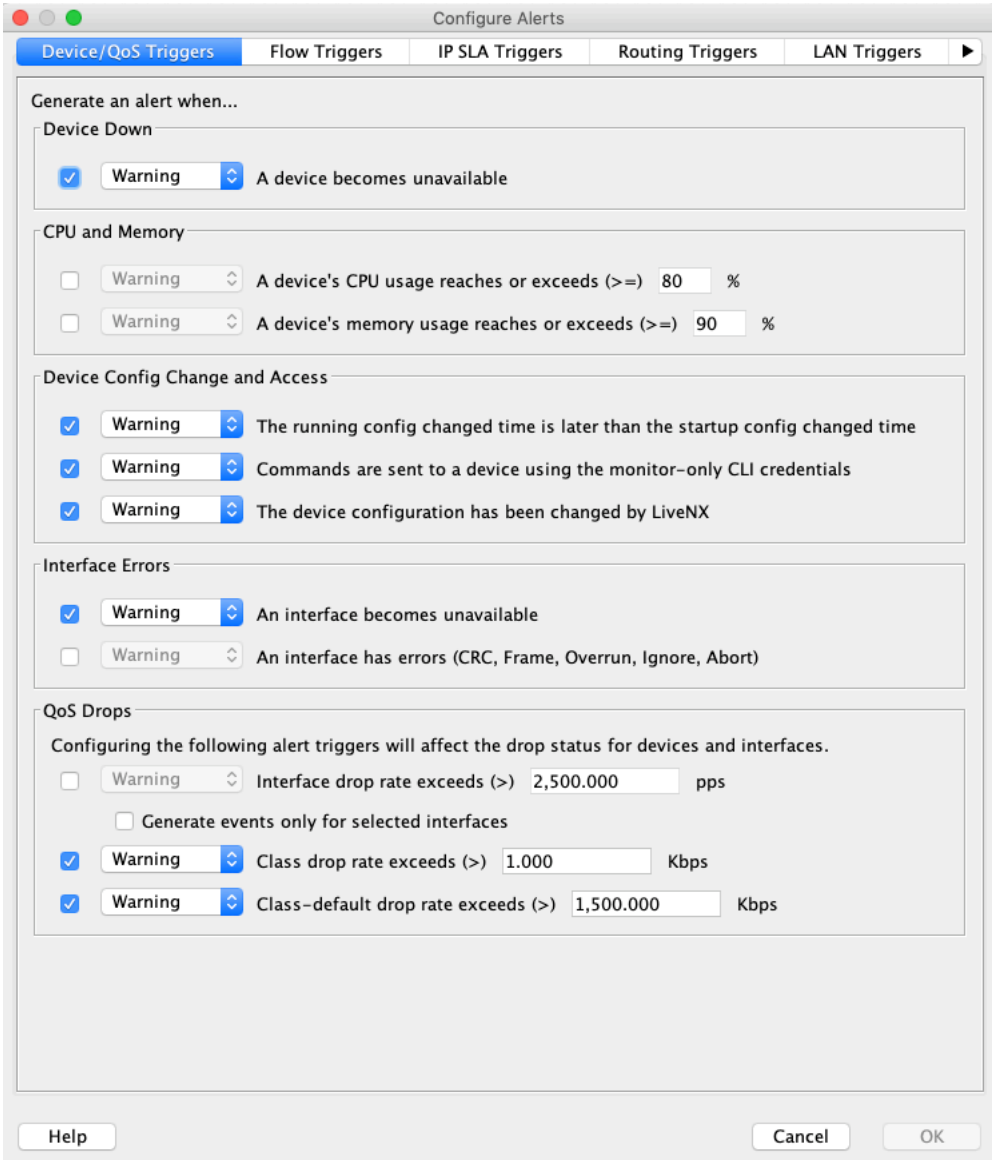
Configure Alerts

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



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

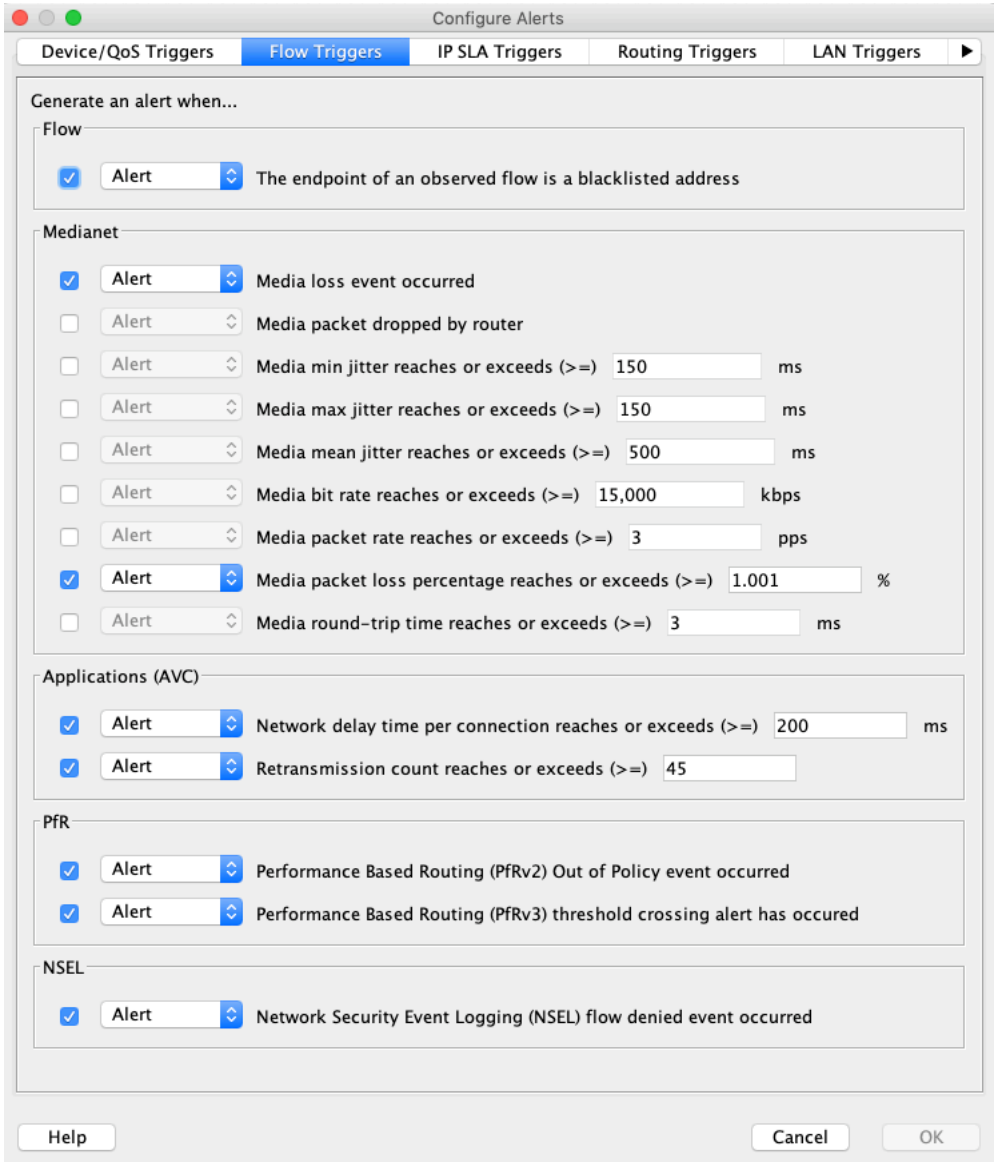
- The interface unavailable alert is logged in the In-Application Alerts window and increments the Interface Up/Down Alert count in the System Dashboard when the interface SNMP polling status changes between responsive and unresponsive.
- The interface errors alert is logged in the In-Application Alerts 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

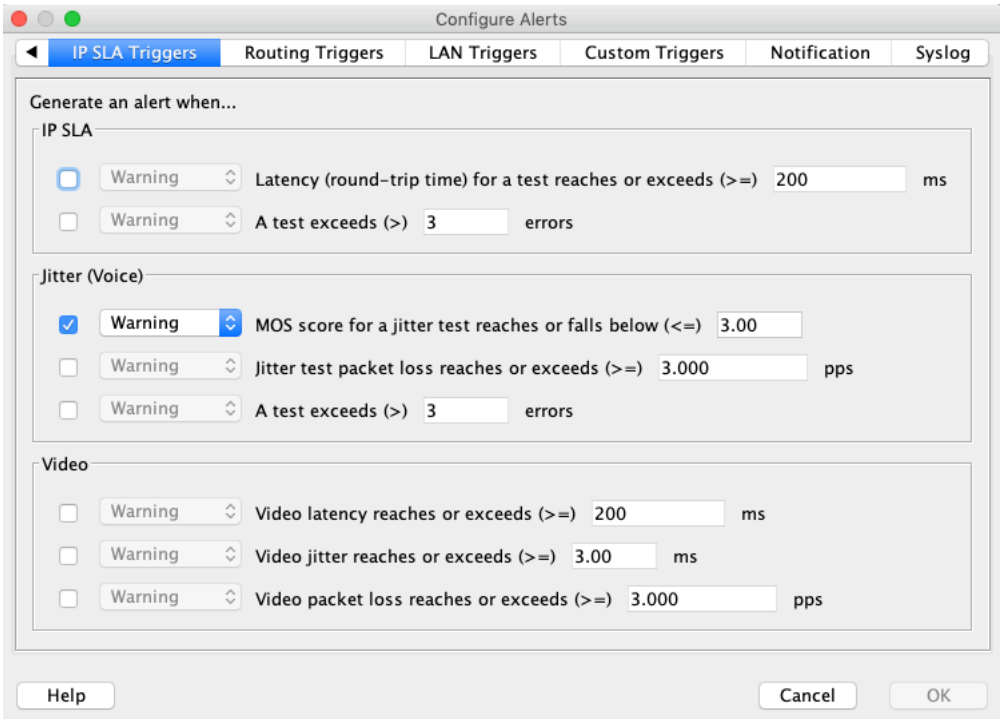
To configure alerts in the Flow technology, go to Tools > Configure Alerts > Flow Triggers tab.



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.

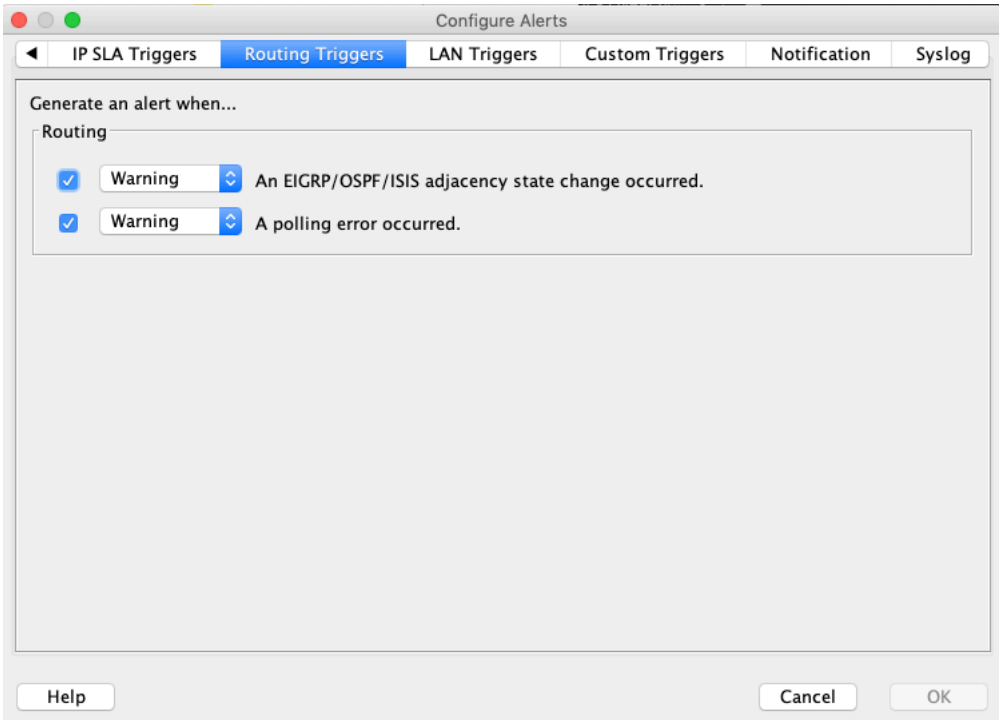


Each alert can be enabled by clicking on the check box and using the dropdown to select the desired Alert type. The values in the IP SLA thresholds are editable only if the alert is enabled (check box is checked). The IP SLA alerts are viewed in the Tools > View Alerts and in the Reporting > IP SLA >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

Default for all IP SLA Triggers is disabled.

Routing Triggers

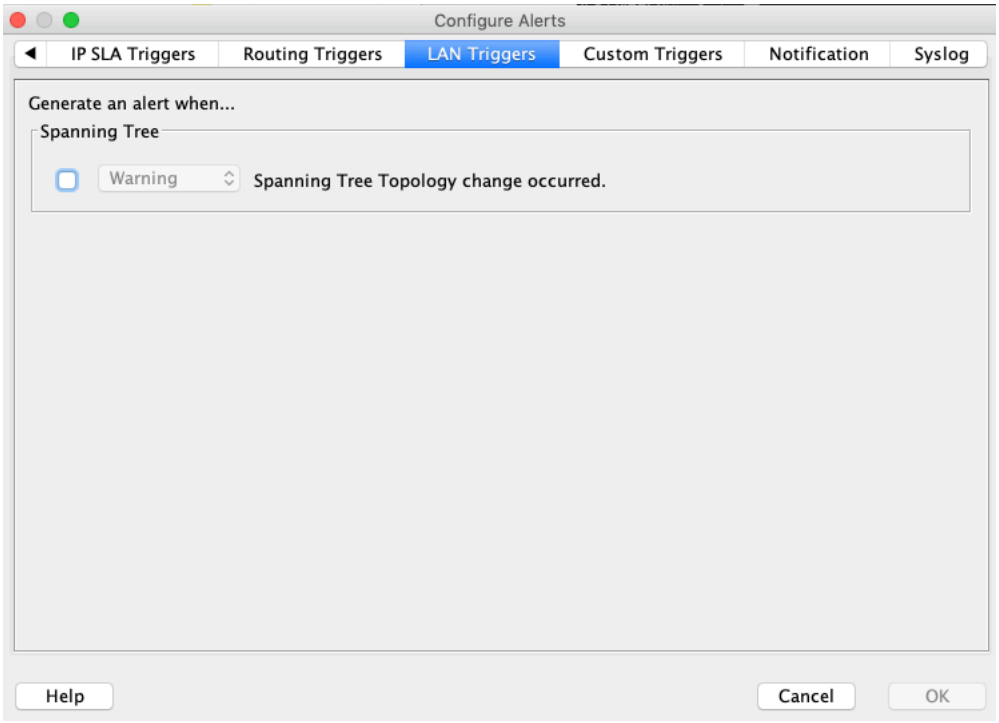
To configure alerts in the Routing technology, go to Tools > Configure Alerts > Routing Triggers tab.



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.

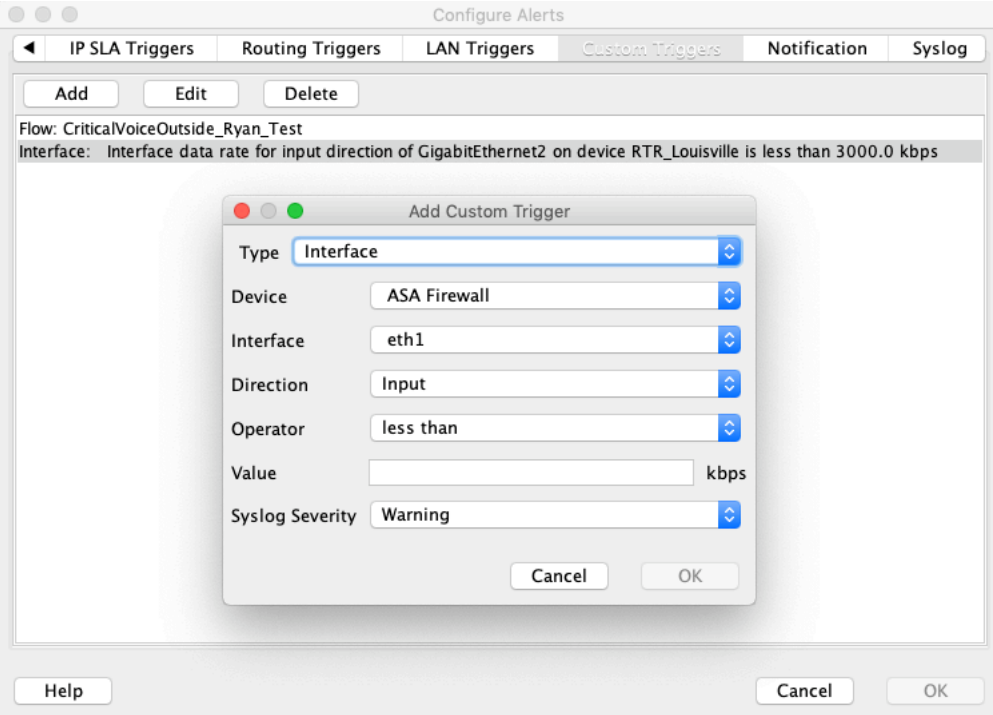
Note Since many alerts can be generated, listening and learning Spanning Tree state changes are intentionally not reflected in the alerts. Spanning tree ports in those states will be in a blocked state.

Custom Triggers

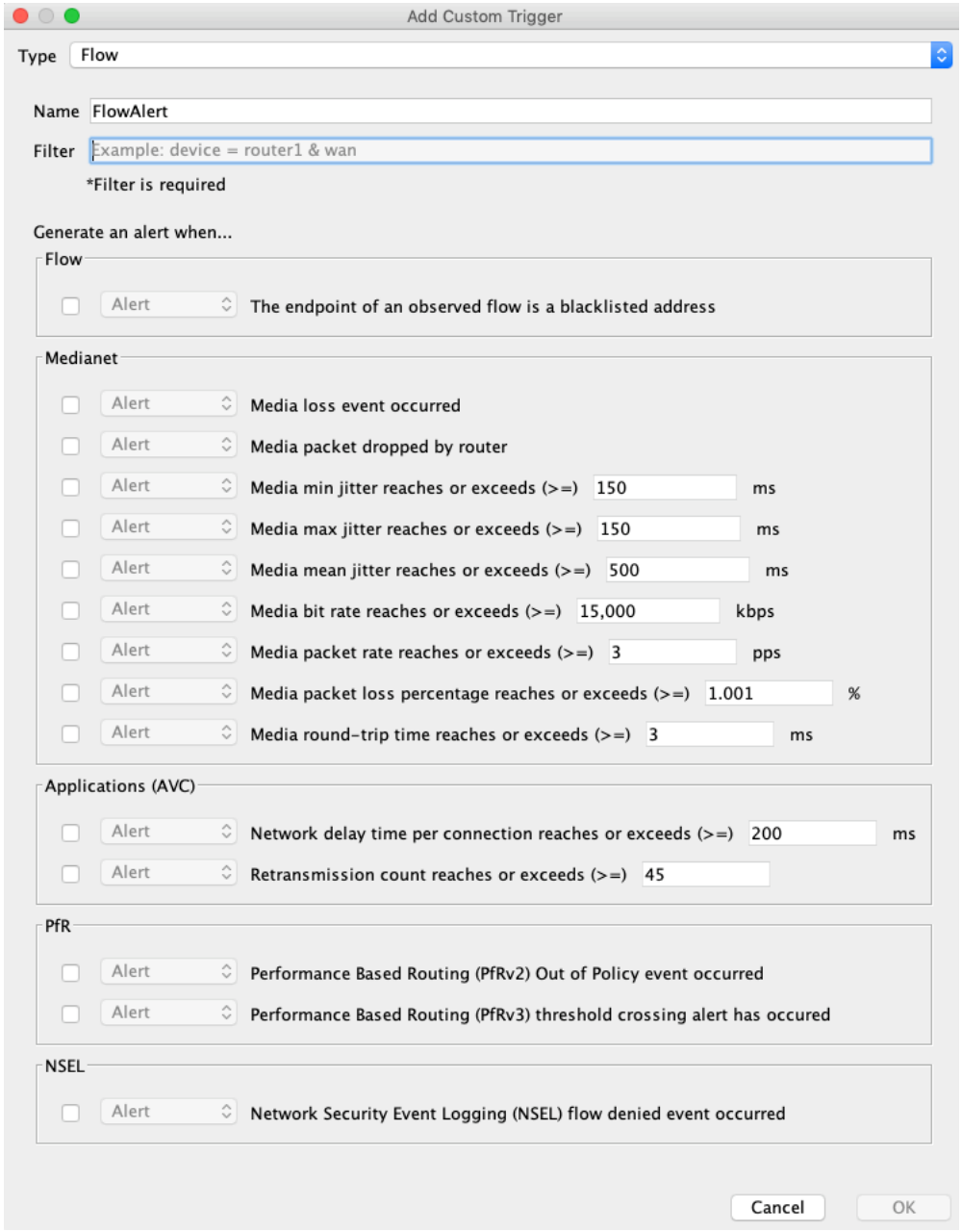
Four classes of custom triggers can be configured:

- 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.



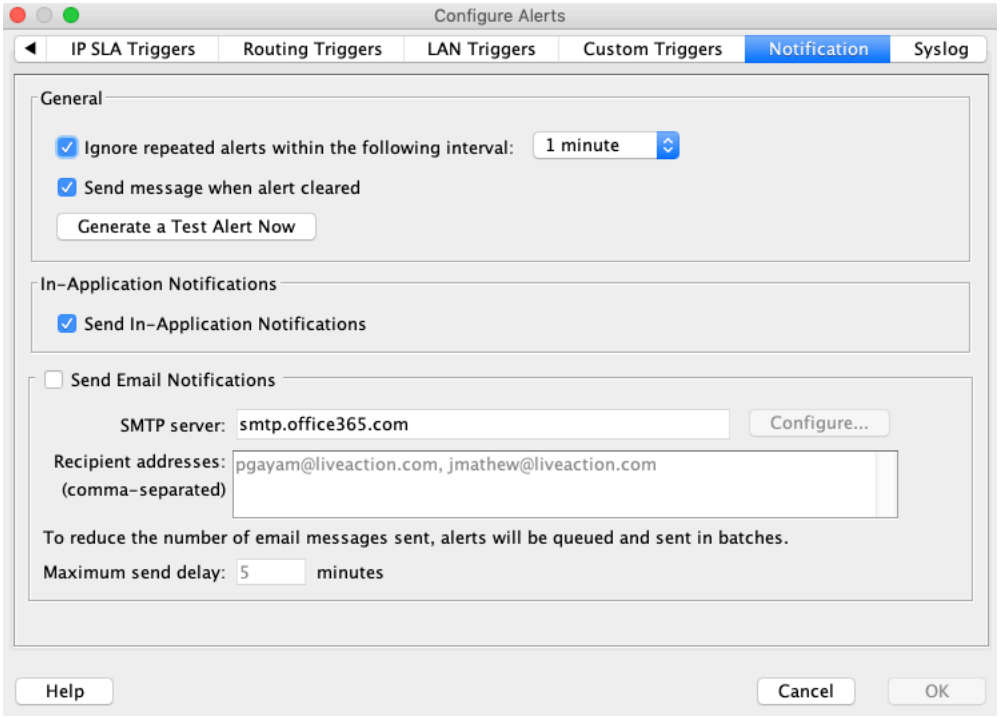
Tagged alerts can be created using the custom alert triggers. A QoS class, NBAR or Flow tagged alert is created by using a custom alert trigger and then filtering the alert trigger based on the user-defined attributes in the system device tree. These custom alert triggers can then be named or tagged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



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

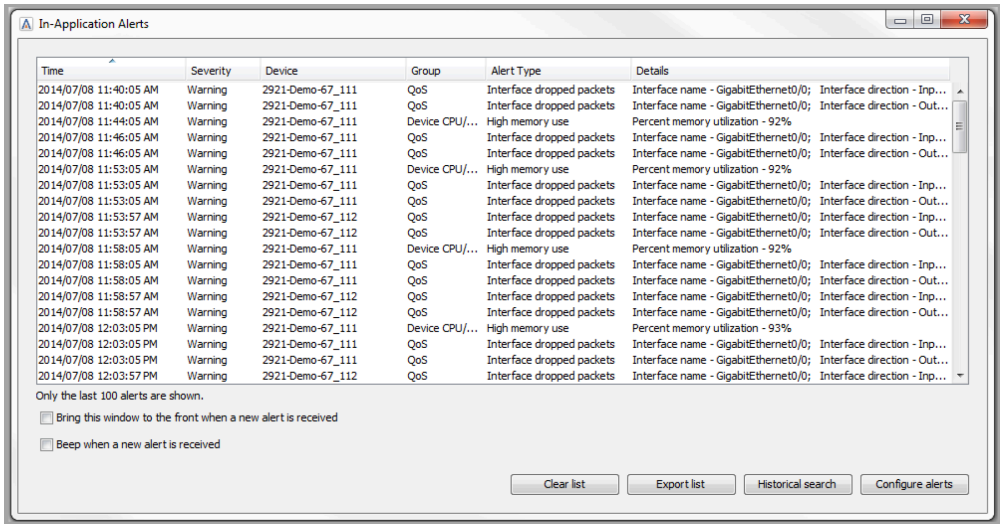


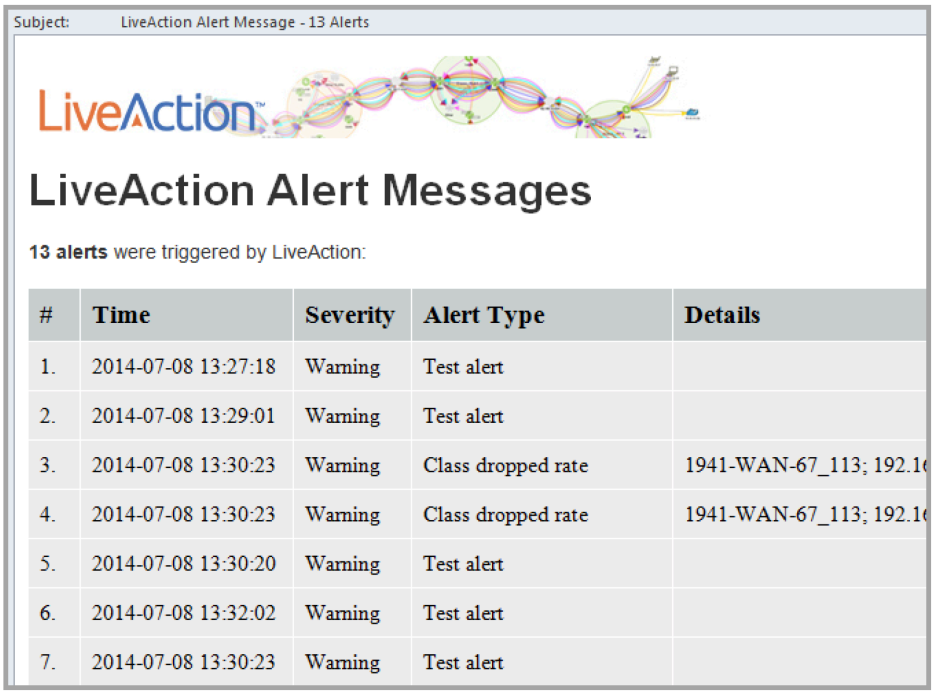
To suppress multiple alerts of the same condition that occur within a given timeframe, select the Ignore repeated alerts within the following interval check box. For example, when CPU usage spikes beyond the set threshold, the alarm could repeat itself six times within a minute, depending on the polling 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)





Subject: LiveAction Alert Message - 13 Alerts

LiveAction

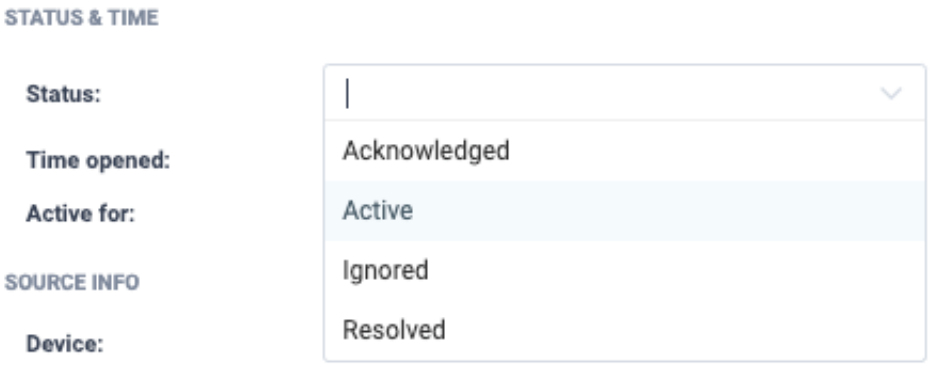
LiveAction Alert Messages

13 alerts were triggered by LiveAction:

#	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.



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

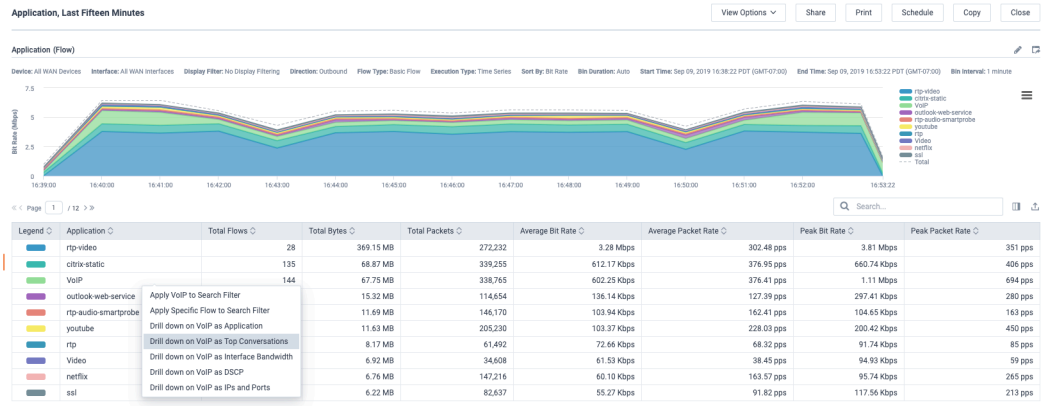
In this chapter:

About Reporting

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.

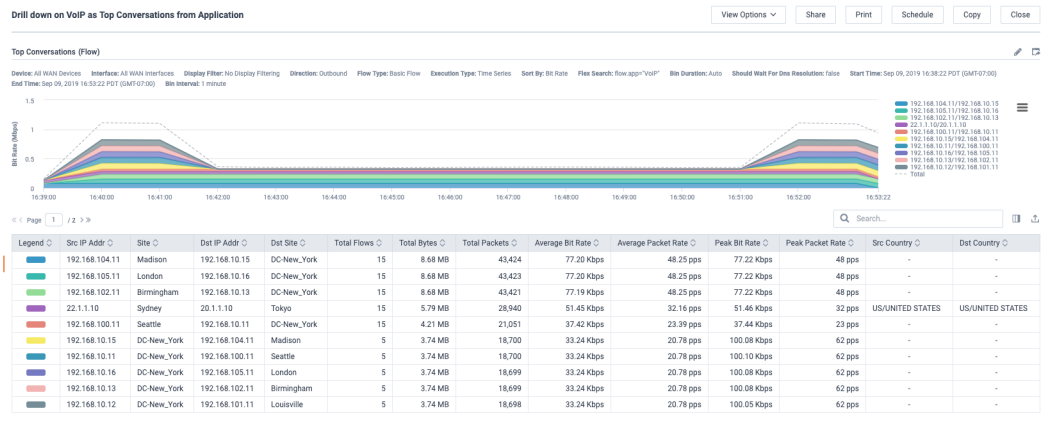
Reporting Best Practice

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.



Legend	Application	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		15.32 MB	114,654	136.14 Kbps	127.39 pps	297.41 Kbps	280 pps
	rtp-audio-smartprobe		11.69 MB	146,170	103.94 Kbps	162.41 pps	104.65 Kbps	163 pps
	youtube		11.63 MB	205,230	103.37 Kbps	228.03 pps	200.42 Kbps	450 pps
	rtp		8.17 MB	61,492	72.66 Kbps	68.32 pps	91.74 Kbps	85 pps
	Video		6.92 MB	34,608	61.53 Kbps	38.45 pps	94.93 Kbps	59 pps
	netflix		6.76 MB	147,216	60.10 Kbps	163.57 pps	95.74 Kbps	265 pps
	ssl		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.

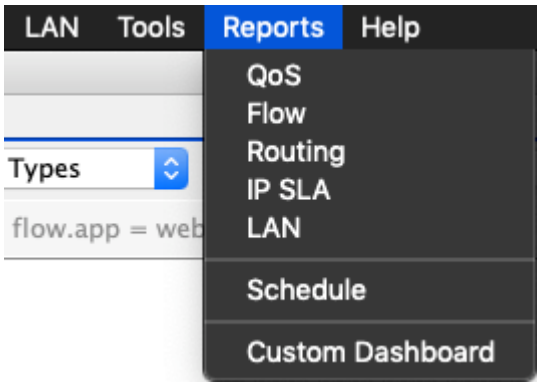


Legend	Src IP Addr	Site	Dst IP Addr	Dst Site	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate	Src Country	Dst Country
	192.168.104.11	Madison	192.168.10.15	DC-New_York	15	8.68 MB	43,424	77.20 Kbps	48.25 pps	77.22 Kbps	48 pps	-	-
	192.168.105.11	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 STATES
	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	-	-
	192.168.10.12	DC-New_York	192.168.101.11	Louisville	5	3.74 MB	18,698	33.24 Kbps	20.78 pps	100.05 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.

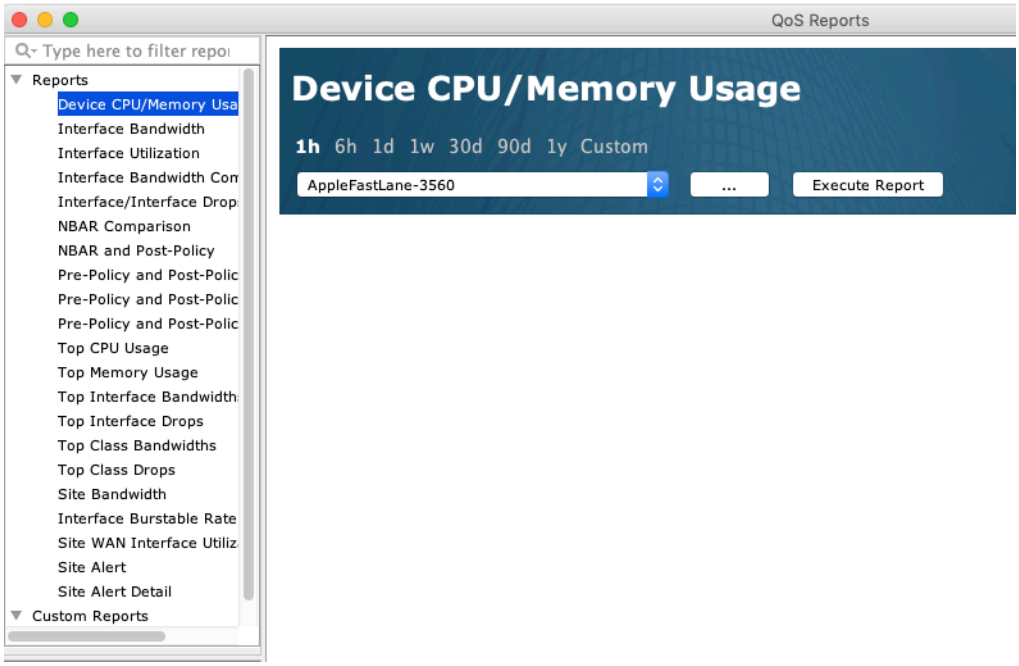
Engineering Console Reporting

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.



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.



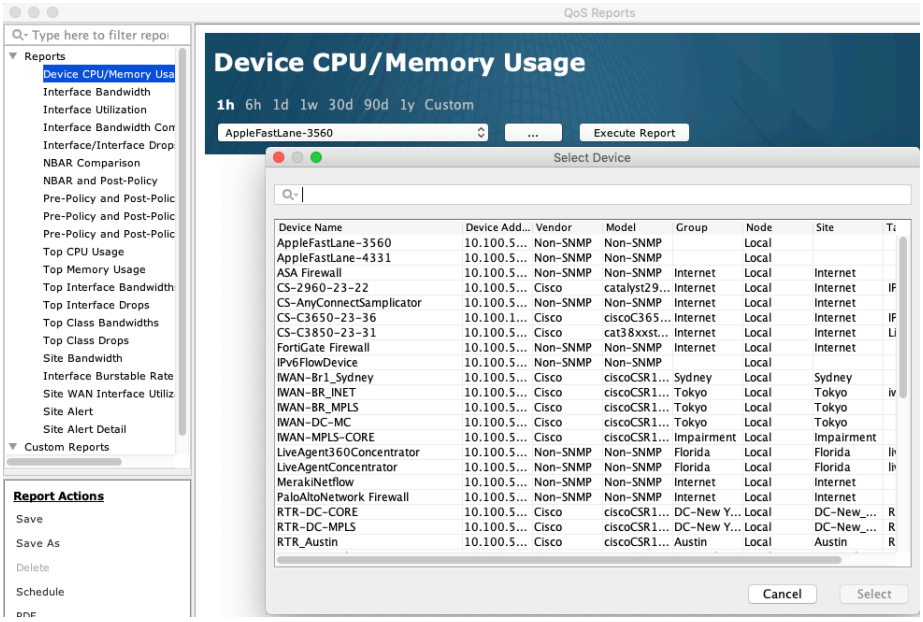
LiveNX generates several QoS reports listed in the left-hand column. Click on the desired report, choose the parameters for the chart, and then click on Execute Report. Please refer to the table below for details about each QoS report.

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

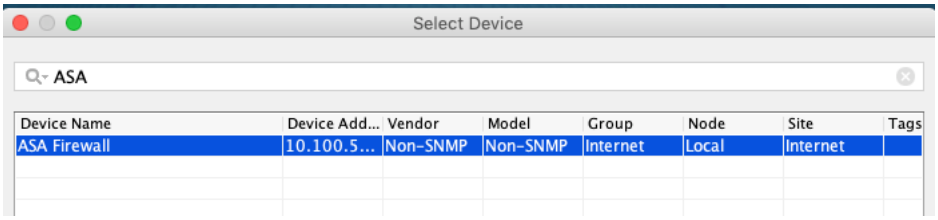
Pre-Policy and Post-Policy Drops	Displays a device interface's traffic by Class type and the Post-Policy Drops in Kbps for the same time span.	Device, Interface, Inbound/ Outbound
Top CPU Usage	Displays a bar graph of the device's average and peak % CPU usage over the desired time period.	All Devices/Individual 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.

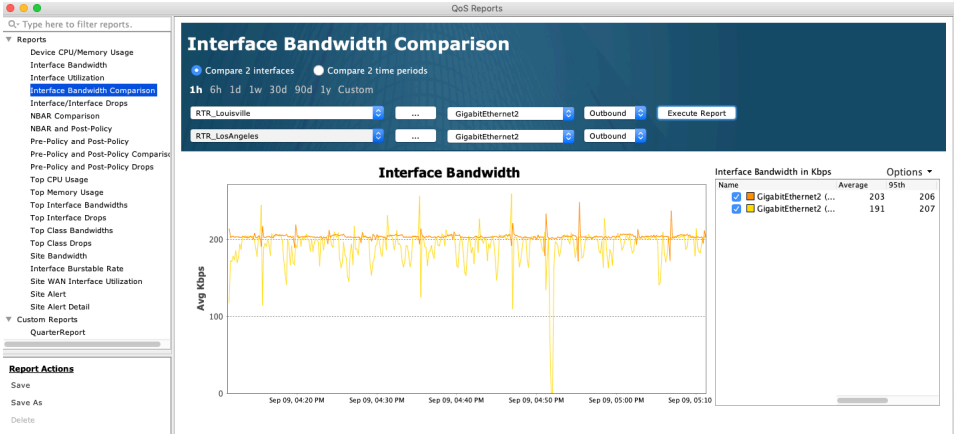


Use the scroll bars to locate the desired device, or type in the search bar adjacent to the magnifying glass to filter the list of devices. Click on a category to choose the desired match field. Default is All, Case insensitive and Match anywhere. Once the device is located, double click on the row or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



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.

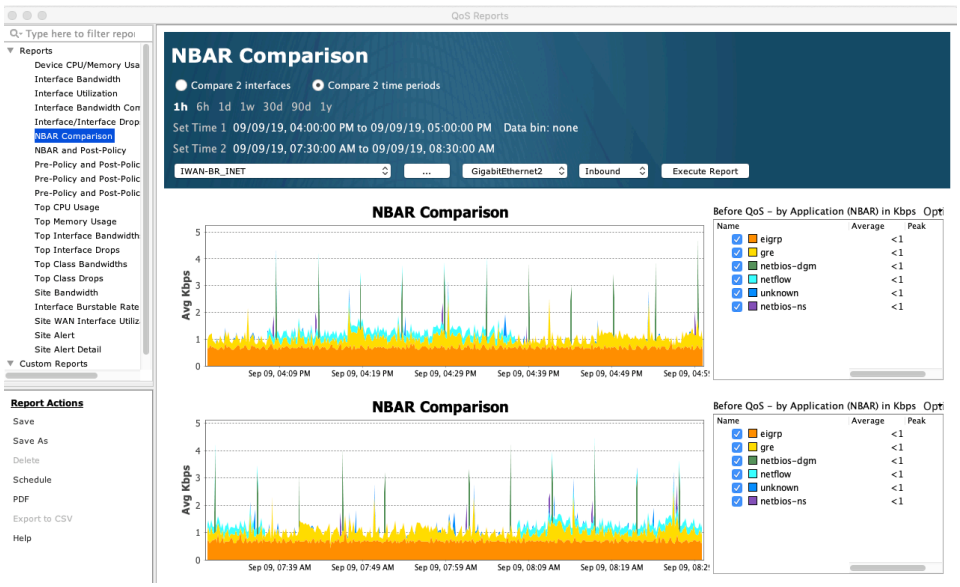


Chart Zoom

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."

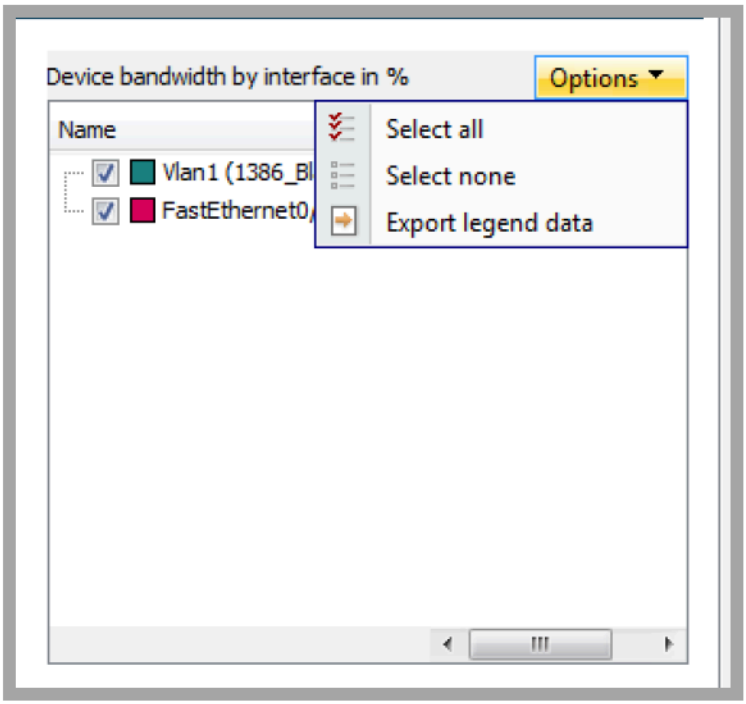
Report Legend

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.

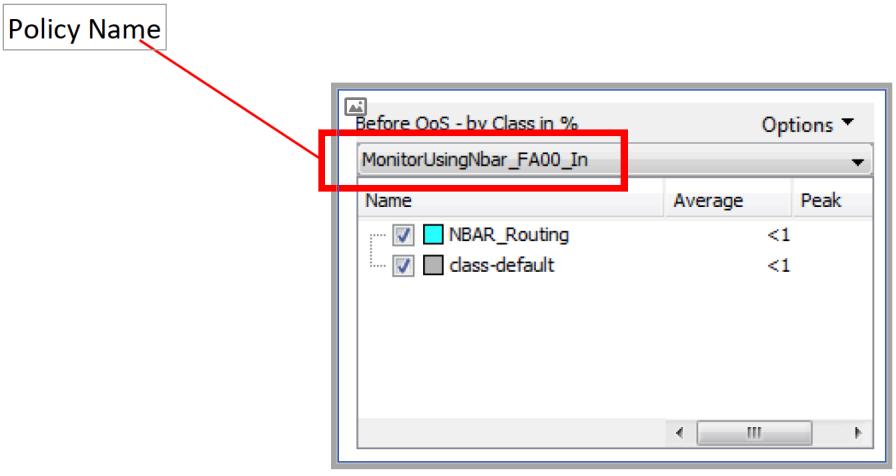
Click Options > Select all to select all items for viewing in the chart.

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.



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

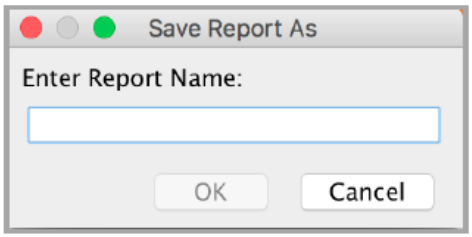
- 90d time span of history from ninety days in the past to the present • 1y time span of history from ninety days in the past to the present
- Custom span of history from an end time

Report Actions

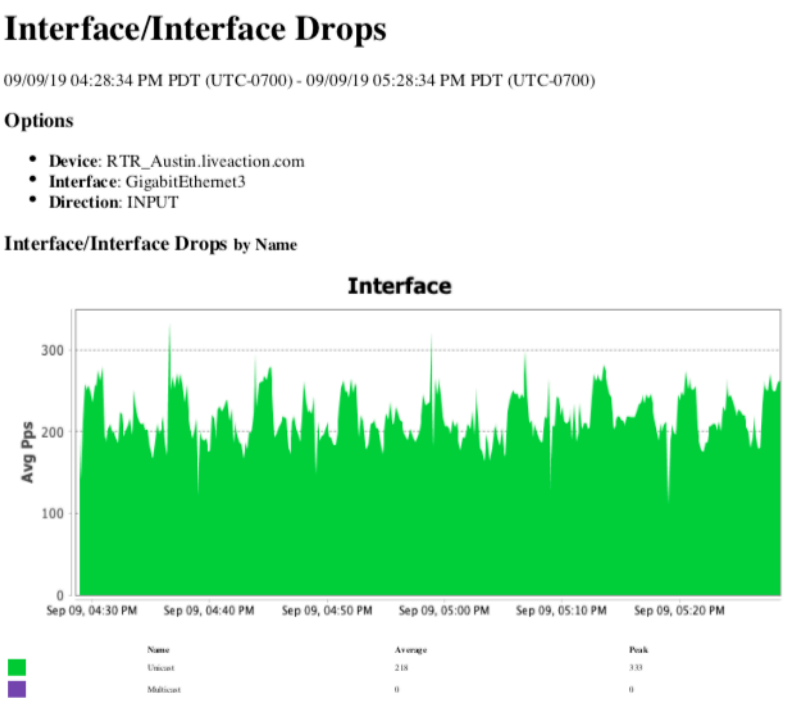
There are seven report actions: Save, Save As, Delete, Schedule, PDF, Export to CSV, and Help.

- 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.



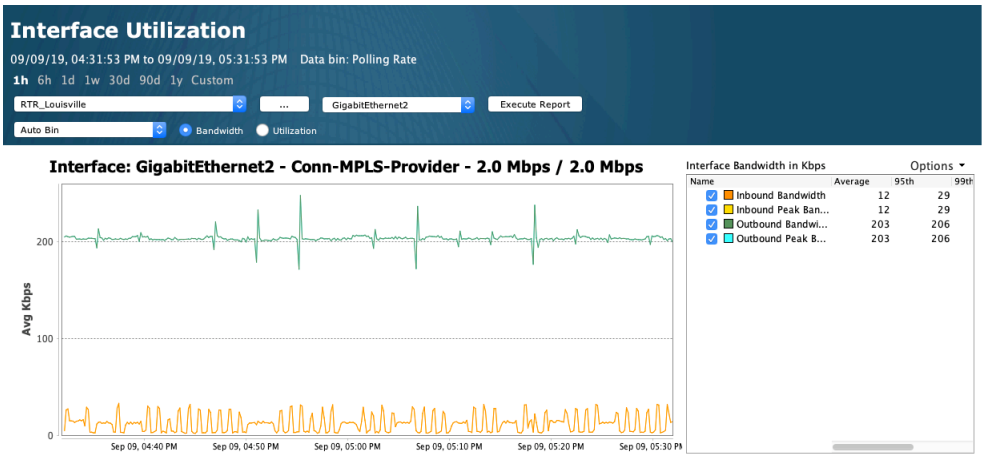
- Delete – deletes a report. Select a report name under Custom Reports and click on Delete.
- Schedule – allows automatic generation and delivery of custom reports. Additional details can be found in the Report Scheduler section of this chapter.
- PDF – allows creating and saving a PDF version of the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



- 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.



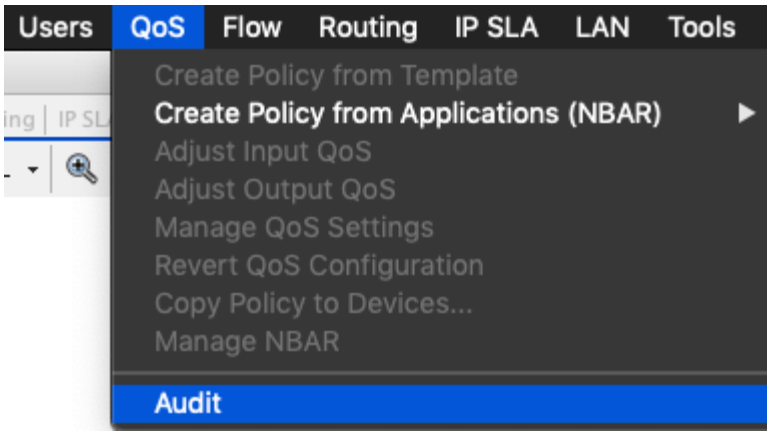
The legend will show the 95th, 99th and peak value individual for the 4-time series information for inbound based on bin, outbound based on bin, inbound peak rate and outbound peak rate. Those val-

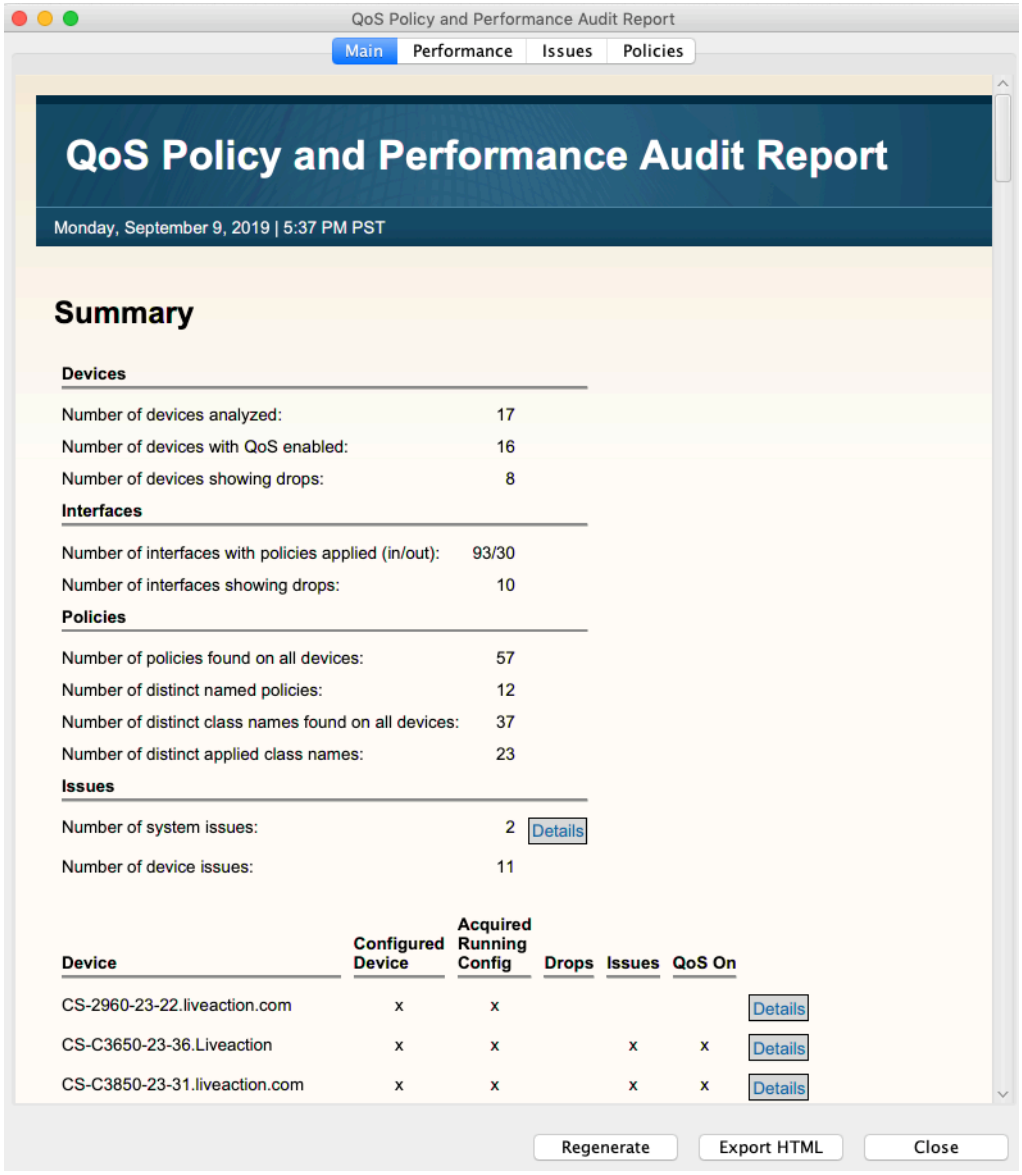
ues can be exported using the Options menu on the legend. Exporting to the CSV option in the Report Action panel will export the 4 -time series data set as shown below.

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

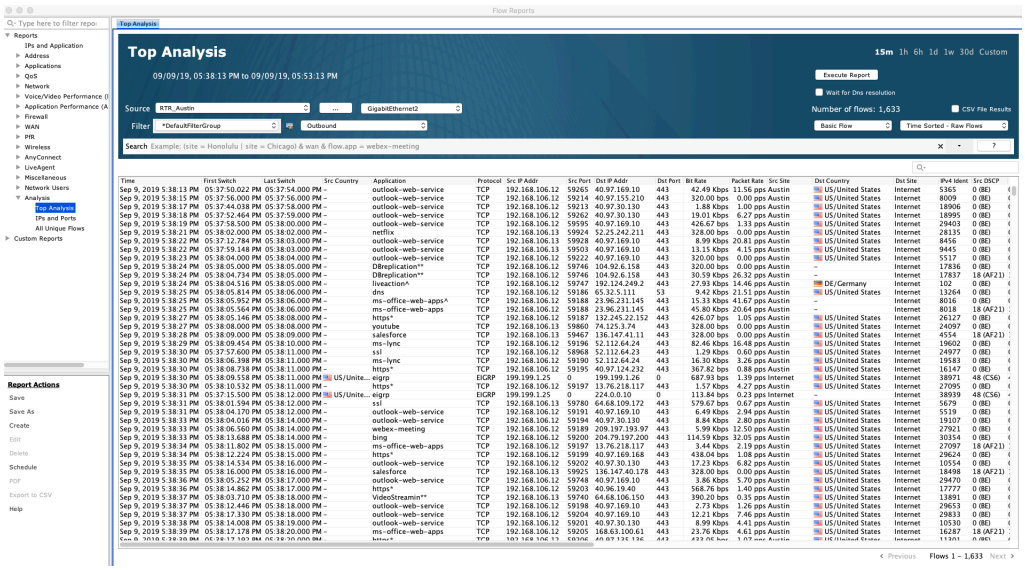
A QoS Policy and Performance Audit report is also available to analyze and summarize the policies enabled, identify any policy issues, and report on performance anomalies. This report is accessed via the Reporting menu or the QoS toolbar.





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 drop-down 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.

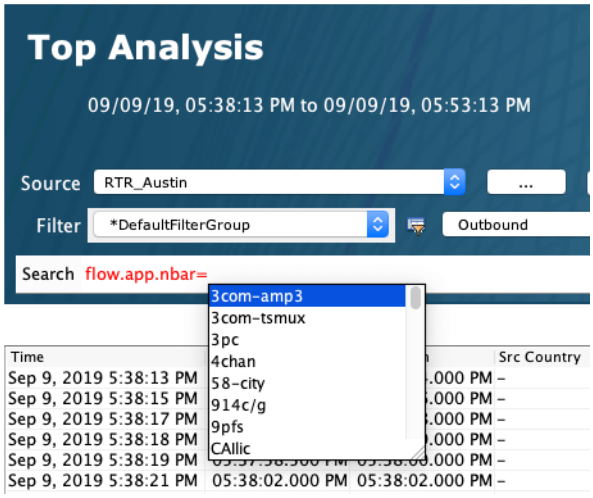
- Display Options: There are three options for displaying the top analysis data in time.
  - – Time Sorted: Unique Flows: Displays unique flows in time from the oldest to the most recent. Uniqueness is determined by the following fields: Protocol, Source IP Address, Source Port, Destination IP
  - – 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.

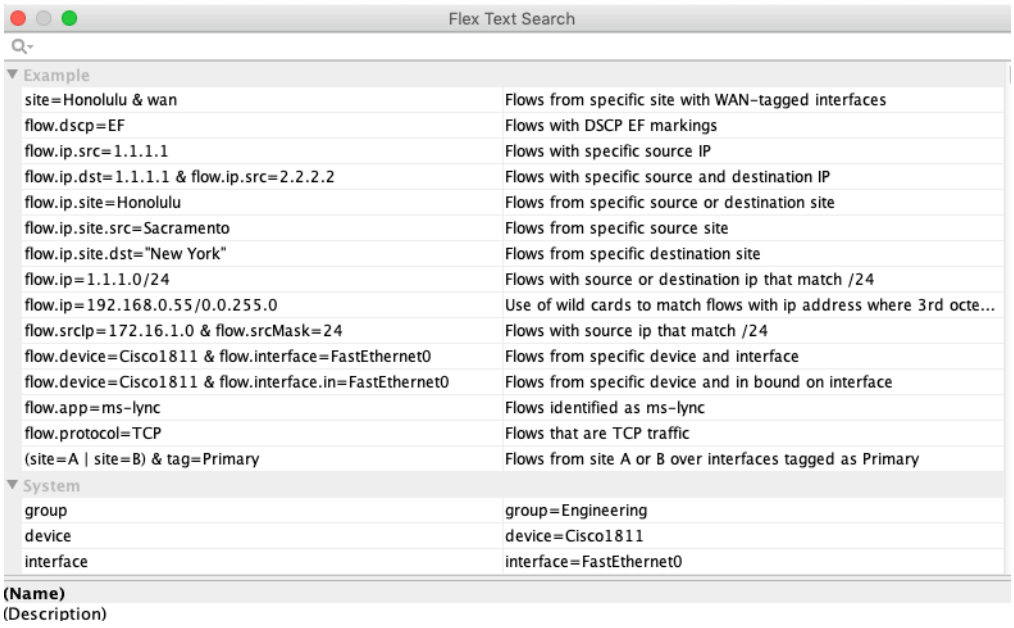
- Click on the Search field to begin typing in the desired search parameters.
- The general syntax of the search field is shown in the example displayed as a default entry.
- (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
- Use the Enter key to apply the search. Click on the ‘X’ 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 = ‘|’ 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.



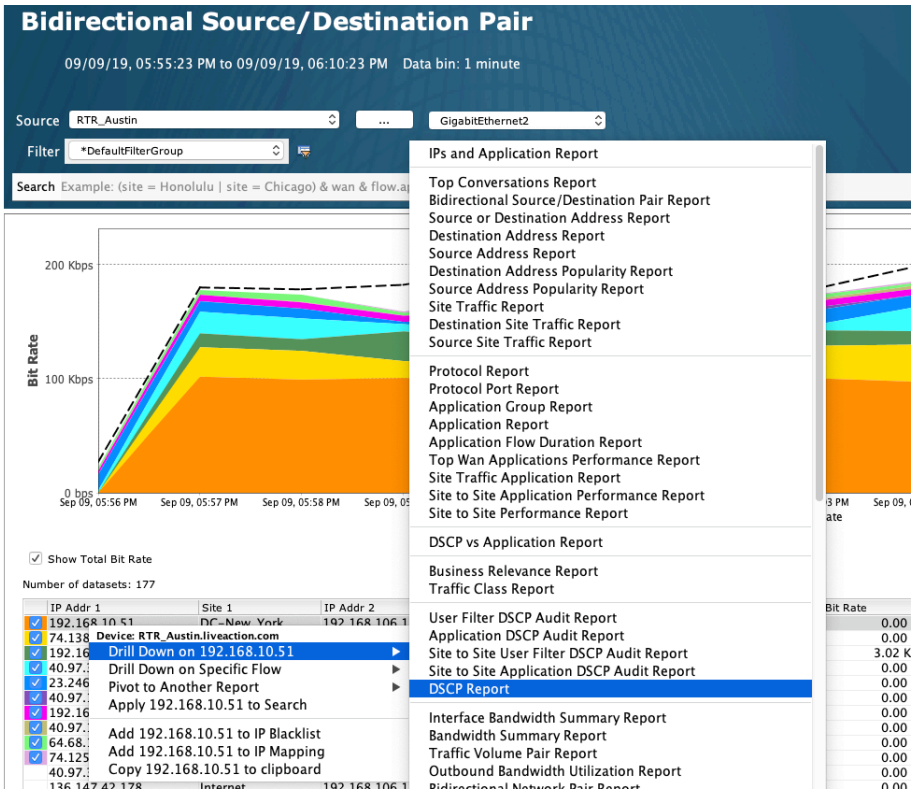
Filtering can also be done through the Filter combo box; filtering is done first with the combo box and then the Search alphanumeric field. The Search is done with a one pass search. In addition, the system level entities need to be in a single clause. For example, (site = Honolulu | site = Chicago) & 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.

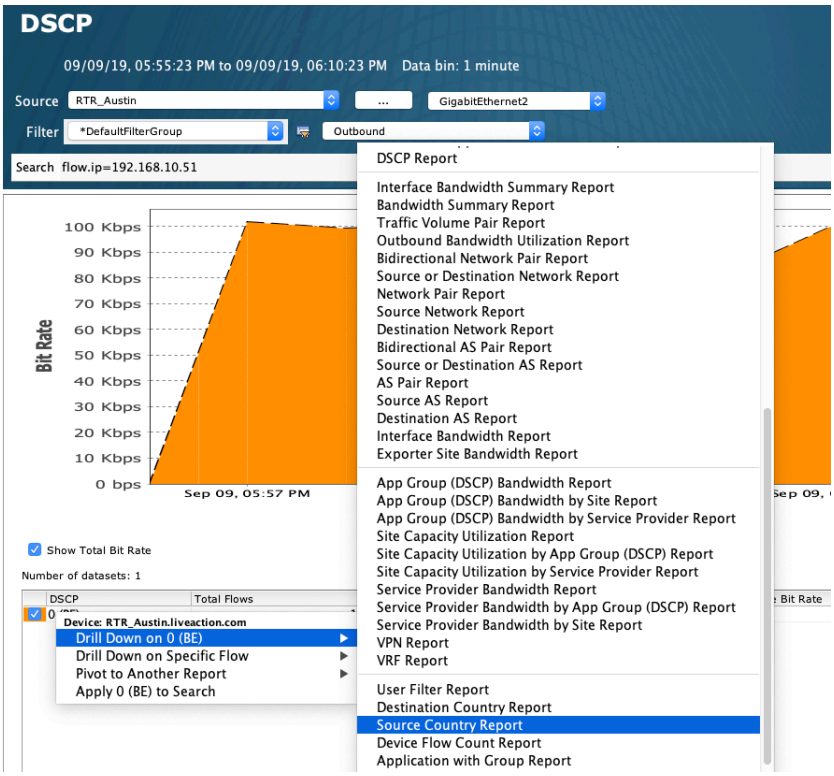


Drill Down/Change Report

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.



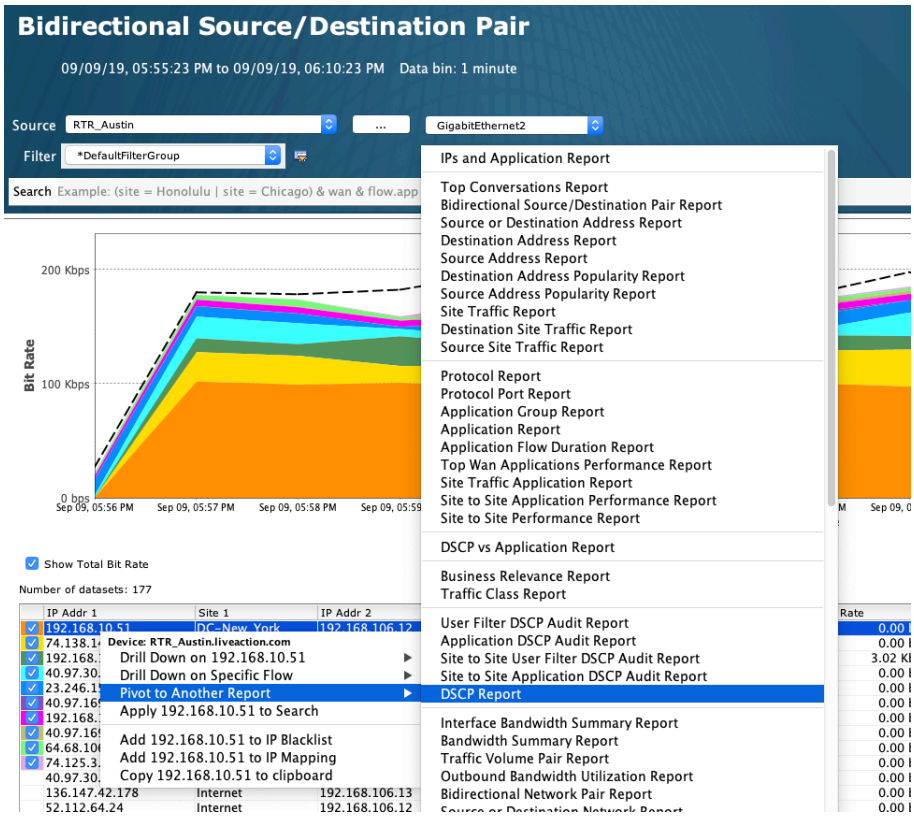
In this example, selecting Drill Down on 192.168.10.51 and then selecting DSCP report creates a DSCP flow report as a tabbed selection next to the Bidirectional Network Pair report. The drilled down DSCP report shows the DSCP values filtered on the IP address chosen from the previous chart. The Filter: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



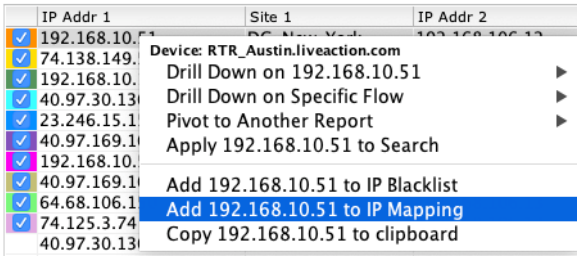
To drill down further, select the desired DSCP value and select another report. In this case, selecting the Drill Down on 0 and then selecting Source Country report will create a Source Country flow report as

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.



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.

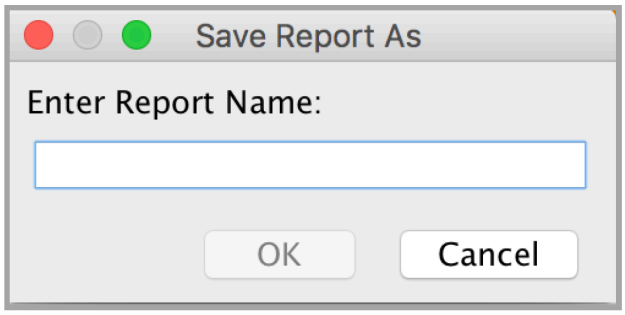
- Copy IP Address to Clipboard – right click on the desired IP address in an Address flow report and select Copy IP Address to clipboard to copy the IP address to the client clipboard. In this example, using View by Application creates a Combined Application flow report using the selected flow.

Report Actions

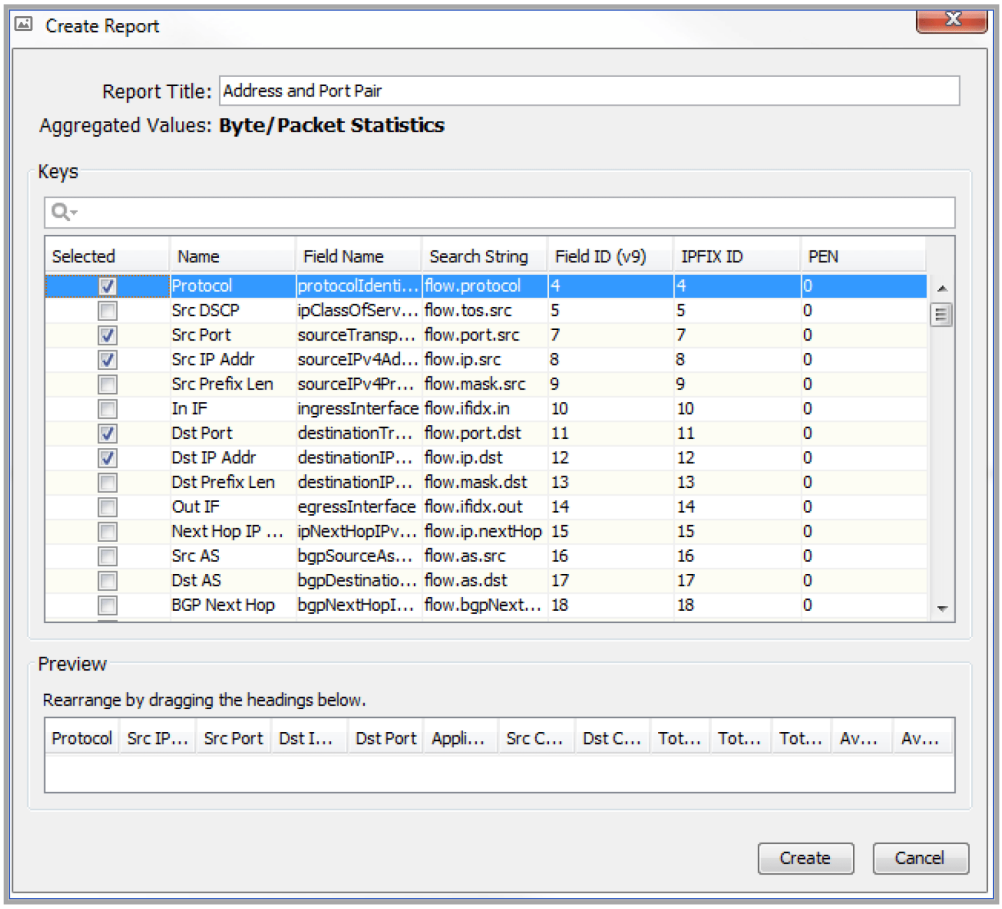
There are seven report actions: Save, Save As, Delete, Schedule, PDF, Export to CSV and Help. The flow report has an additional report action: Create.

- 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.



- 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.



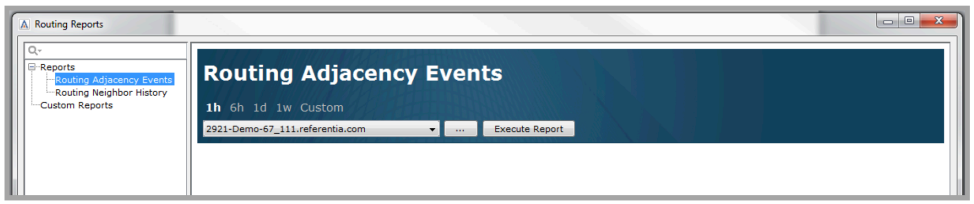
- Delete – deletes a report. Select a report name under Custom Reports and click on Delete.
- Schedule – allows automatic generation and delivery of custom reports. Additional details can be found in the Report Scheduler section of this chapter.
- PDF – allows creating and saving a pdf version of the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

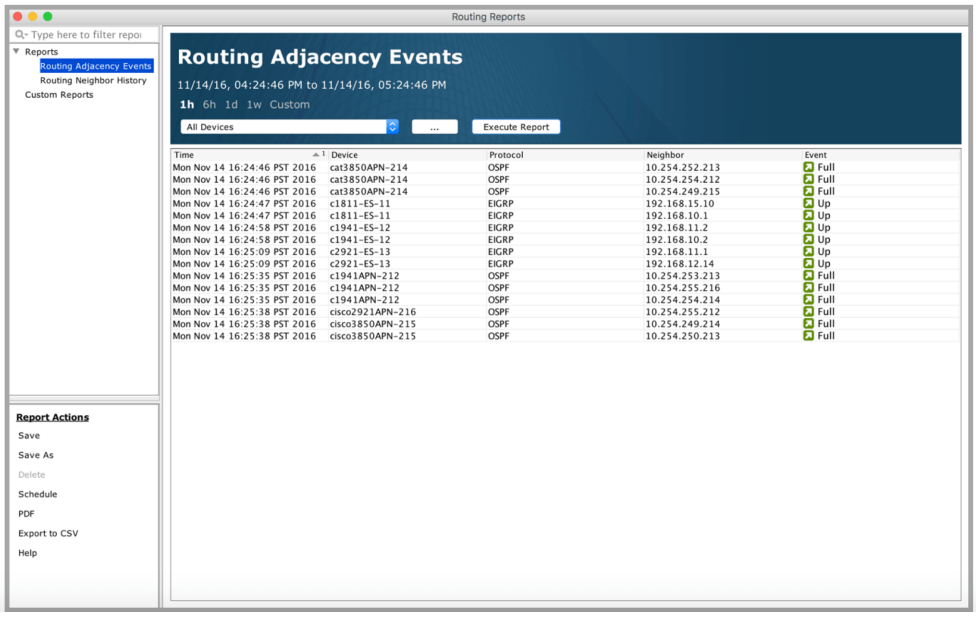
Routing Reports

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.

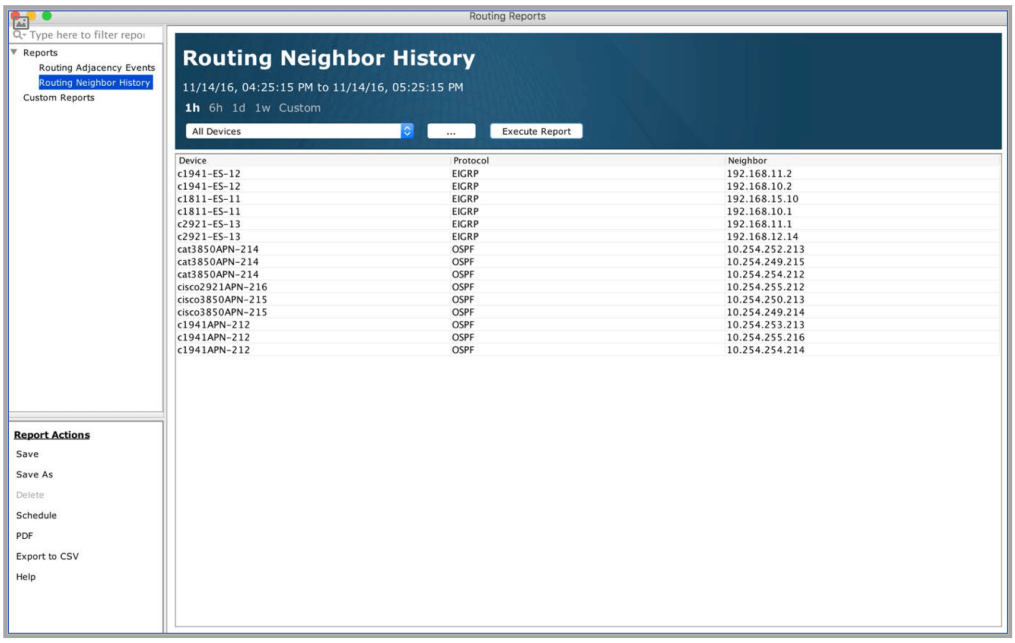


LiveNX provides two types of routing reports as shown in the list in the top left-hand window. The Routing Adjacency History report displays any and all OSPF or EIGRP adjacencies established during the specified time period for a specified device or all devices. In between the two dropdown lists is a … 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).

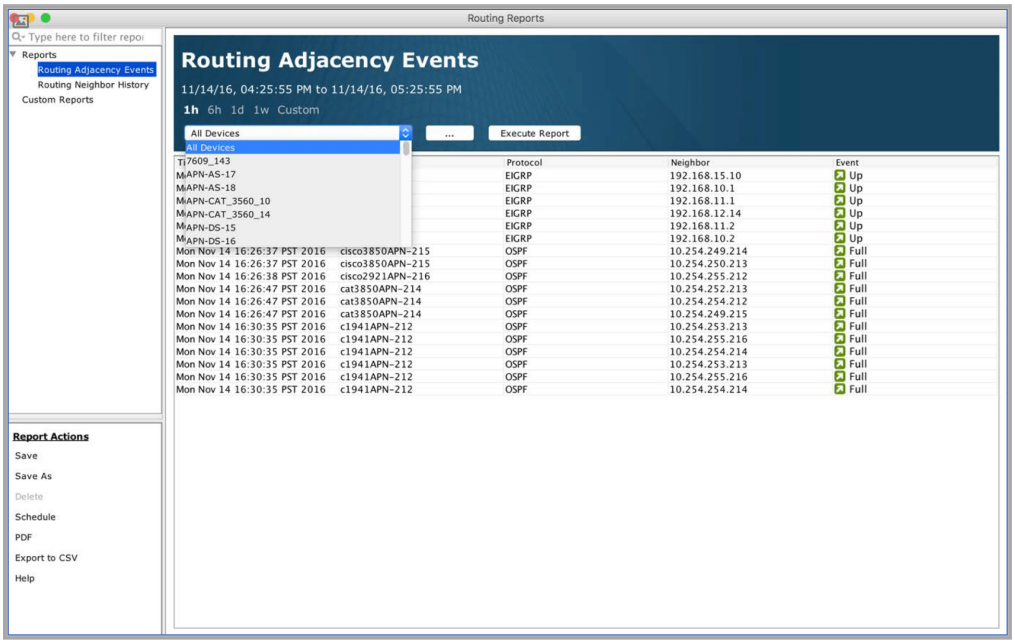
Note The neighbor up/down events in the Adjacency Events report is determined differently for OSPF, IS-IS, and EIGRP. For OSPF, a neighbor's up or down status indicates that the neighbor state changed from any of the non-full states to full, or from full to any non-full states, respectively. For IS-IS,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



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.



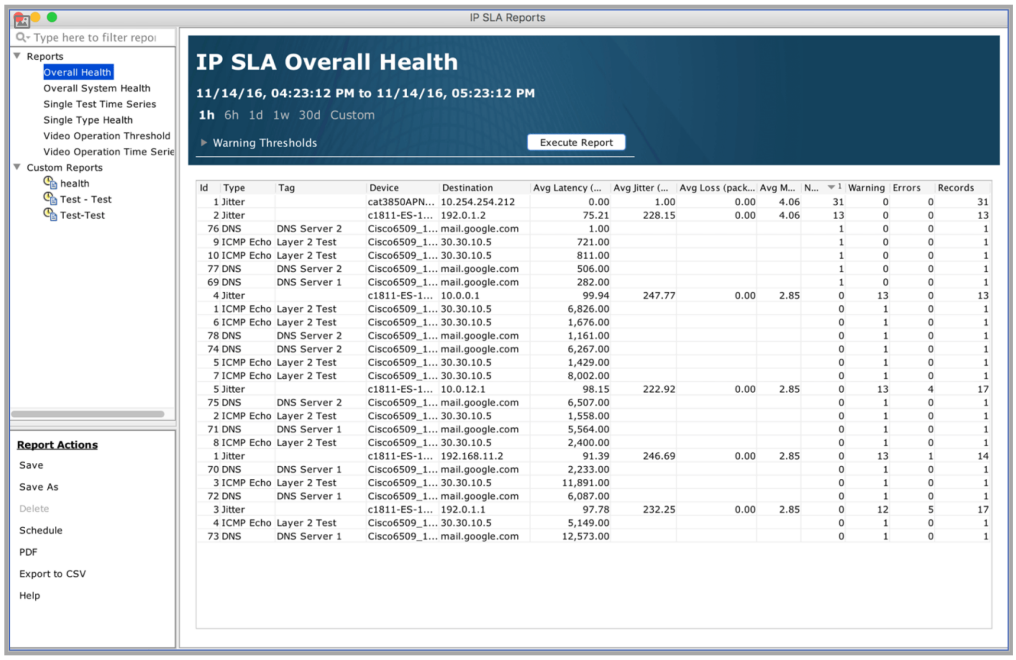
The length of historical data is selectable at the top of the chart, and there are five to choose from 1h (one hour), 6h (six hours), 1d (one day), 1w (one week) and Custom. When selecting Custom, select the desired Start Time and End Time for the report. Select the desired device or All Devices in the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



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.



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

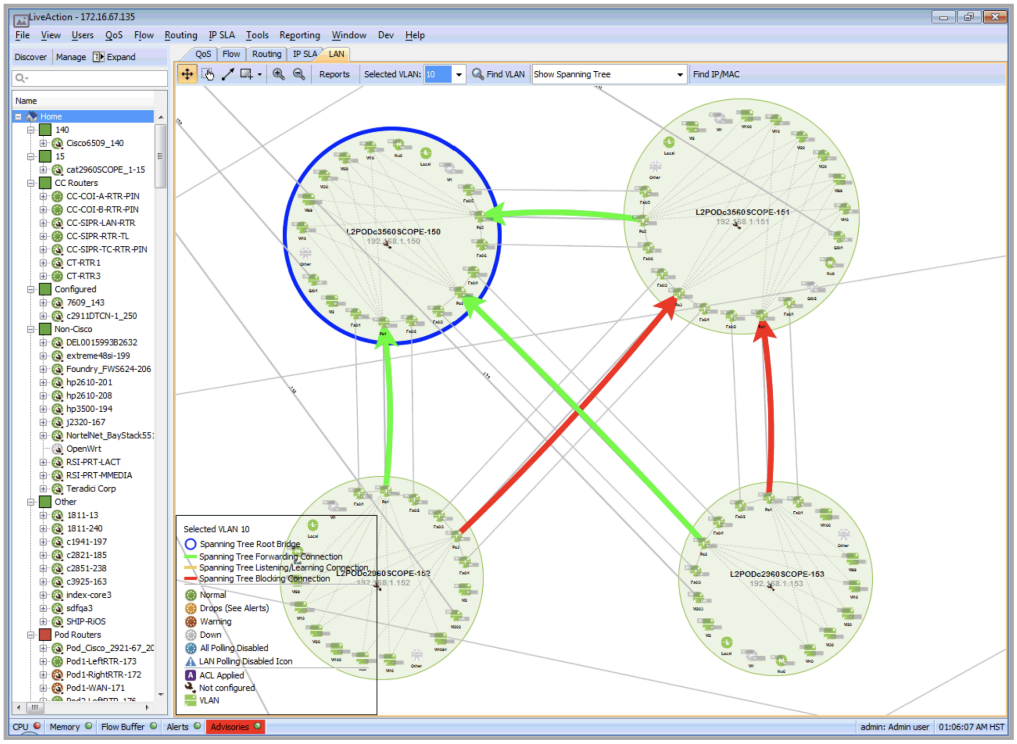
You can configure a report and save the selected parameters, making it easy for you or other users to run the report at a later time. Configure the parameters of the report and then click the Save or Save As button in the lower-right section of the IP SLA Reports dialog.

Printing and Exporting Reports

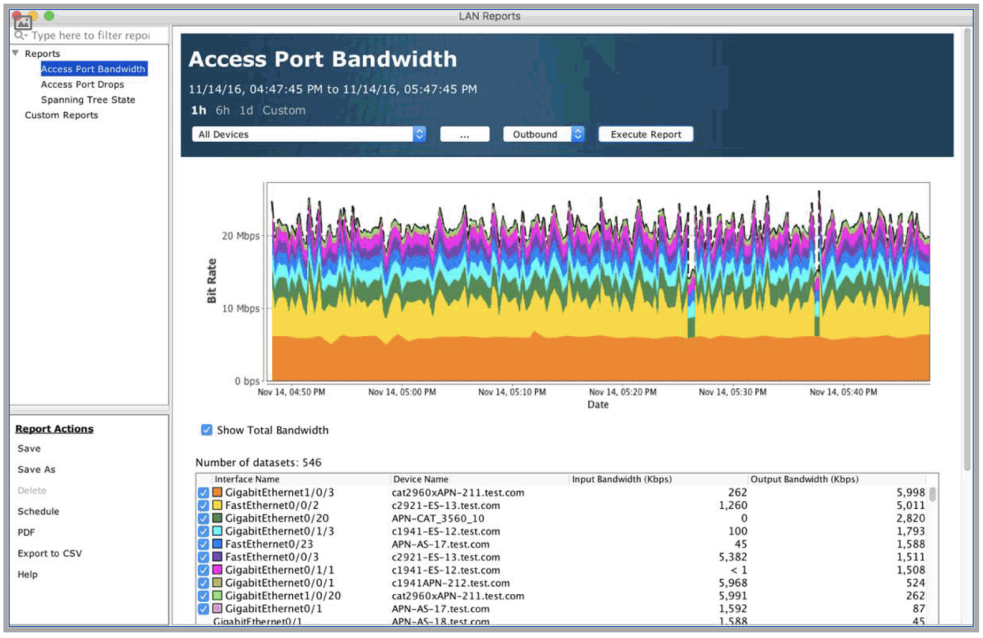
Click the “View HTML” button to create an HTML file of the report, making it easy to print and share the report. Click the Export to CSV button to export the data shown in the report to a comma-separated value file. Additional Ways to Create Reports Reports can be created from the system topology view. 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

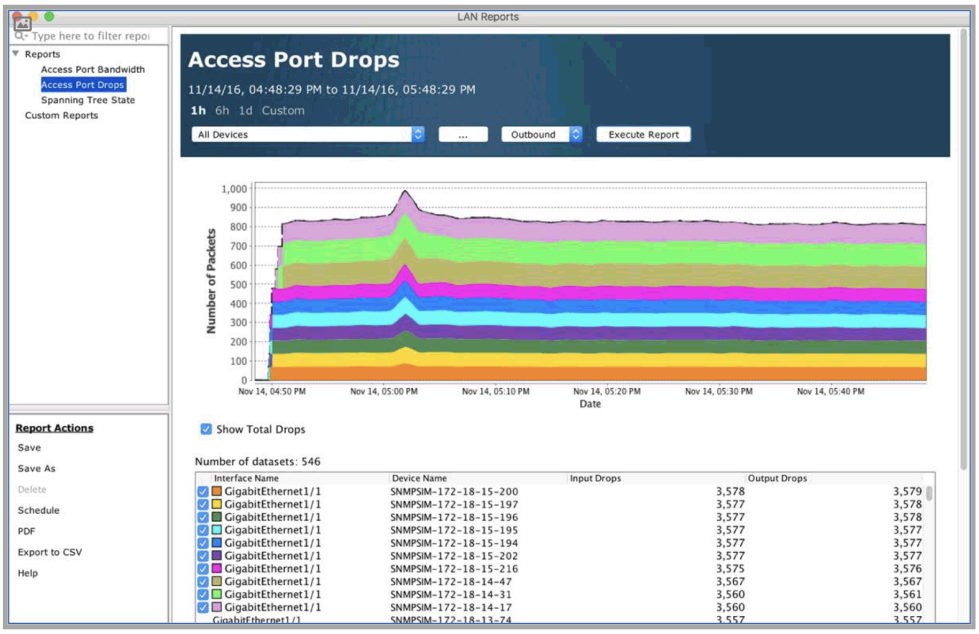
LAN reports provide detailed results on the bandwidth, drops and spanning tree state for both the entire system and for individual devices. The LAN reports can be accessed by clicking on either the Reporting > LAN > LAN Reports. LAN Reports can be accessed by the Reports button in the toolbar in the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

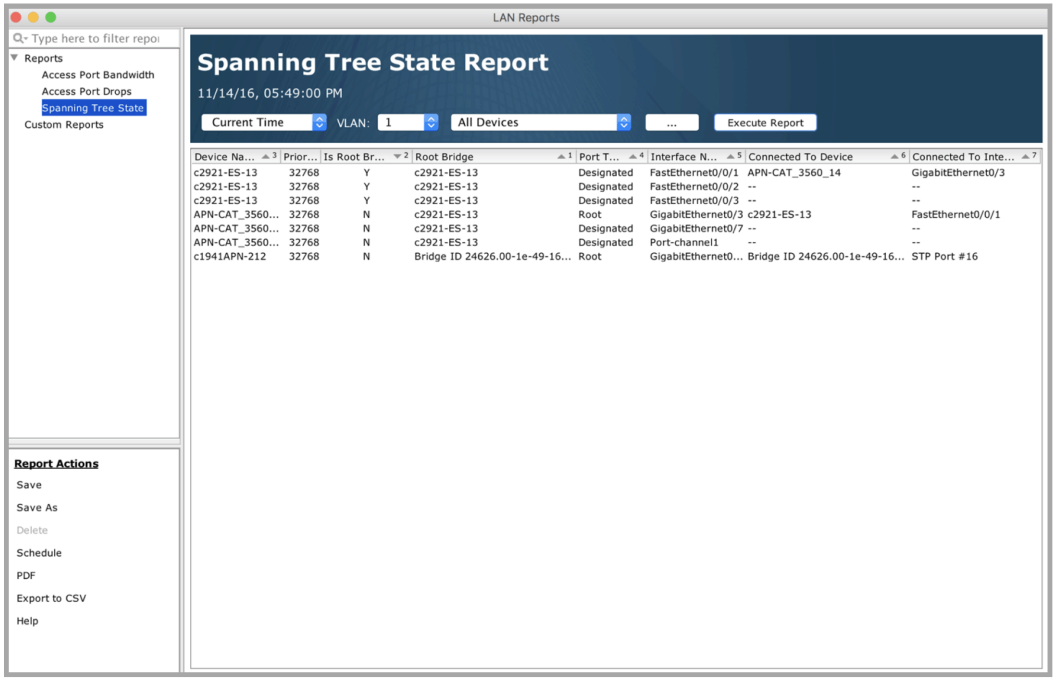


When choosing the Access Port Drops report, select the desired device and Inbound or Outbound using the two respective combo boxes. Click on the Execute Report button to display the desired data. The table accompanying the chart describes the access ports and the number of packets dropped in both directions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

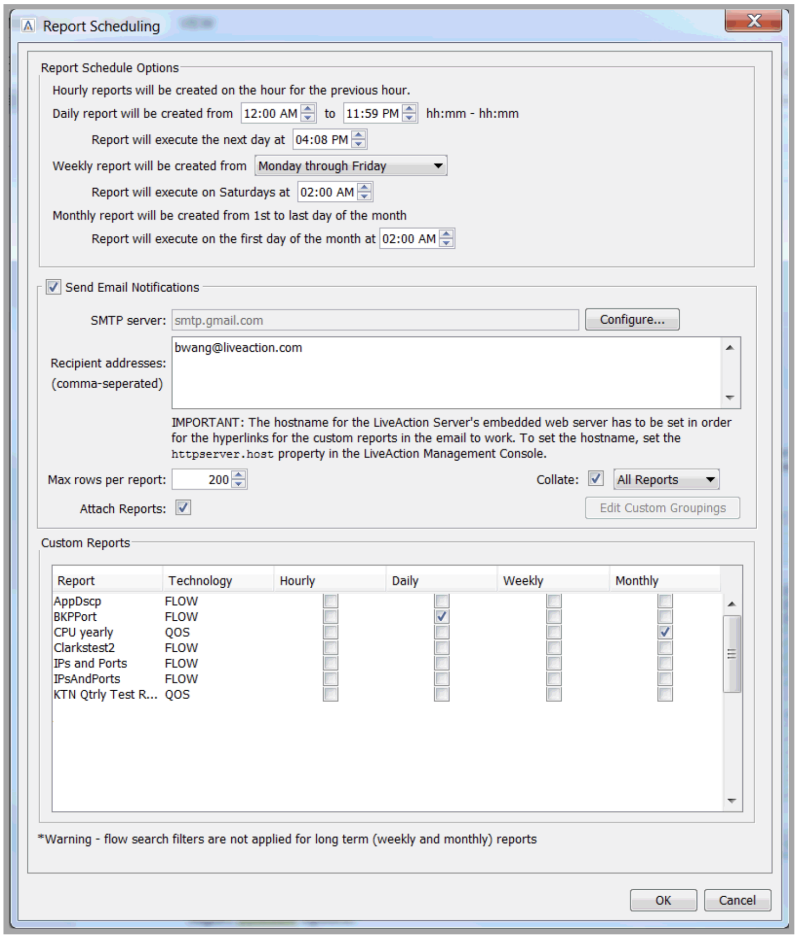


The Access Port Bandwidth and the Access Port Drops reports include a … labeled button. Click to display a device pick list with an alphanumeric entry for searching the list. For more details on the device

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 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.

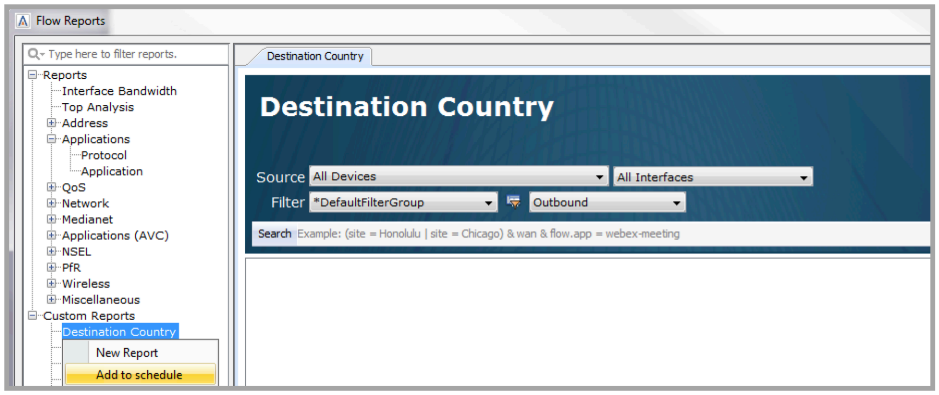
The monthly report will create a report with data collected from the first to the last day of the month. To minimize CPU impact, create the monthly reports during low traffic time periods.

Long-Term Reports

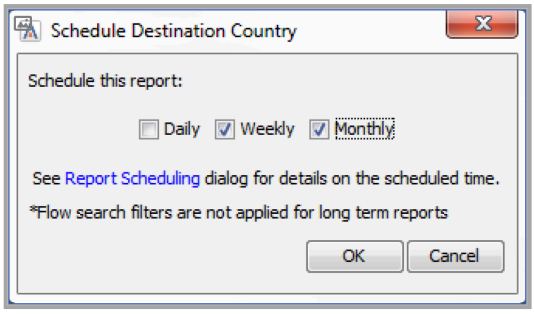
LiveNX can generate long-term reports by using aggregated flows for faster results when dealing with reports that span greater than multiple days. Details of the aggregated flows can be found in Chapter 7 – LiveNX Flow, under LiveNX NetFlow Process Overview. The long-term reports using aggregated flows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



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



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.

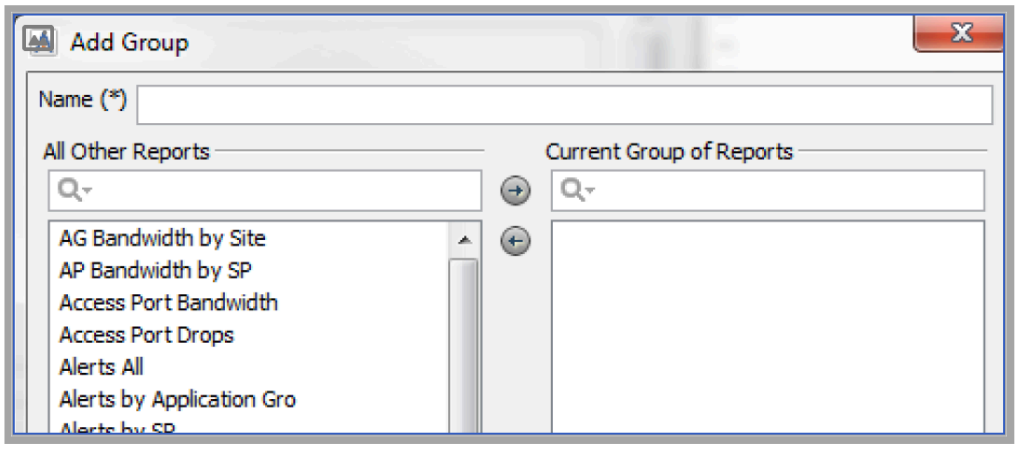
Recipient Address: enter the desired recipients' e-mail addresses separated by commas.

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.



For details on Configure, please see Options below.

Scheduled Reports

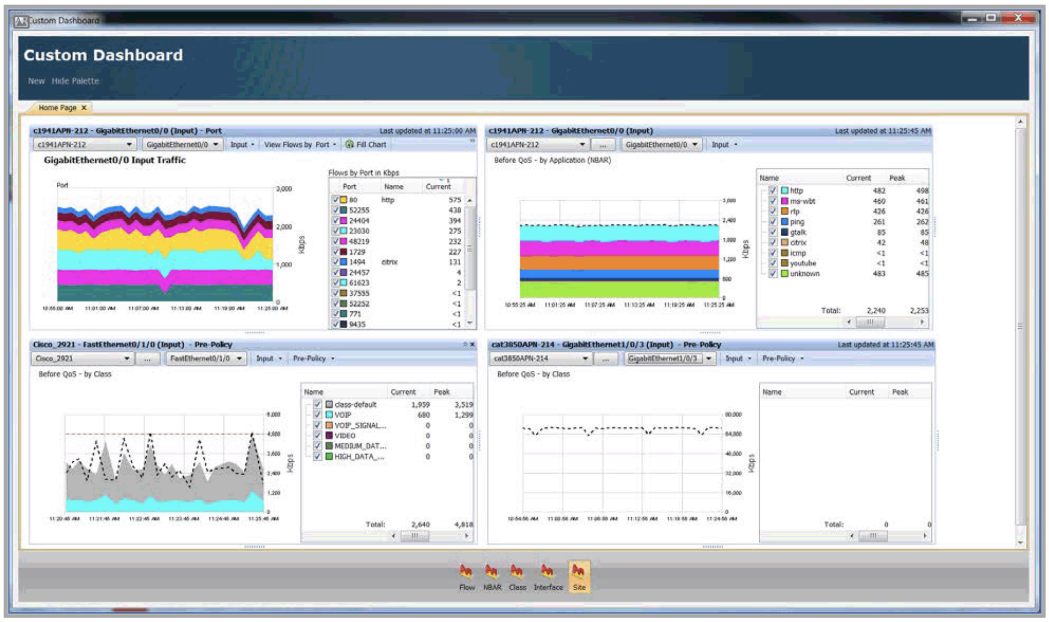
LiveNX automatically populates the Scheduled Reports with a compilation of all the Custom QoS, Flow, Routing, IP SLA, and LAN report.

- 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.

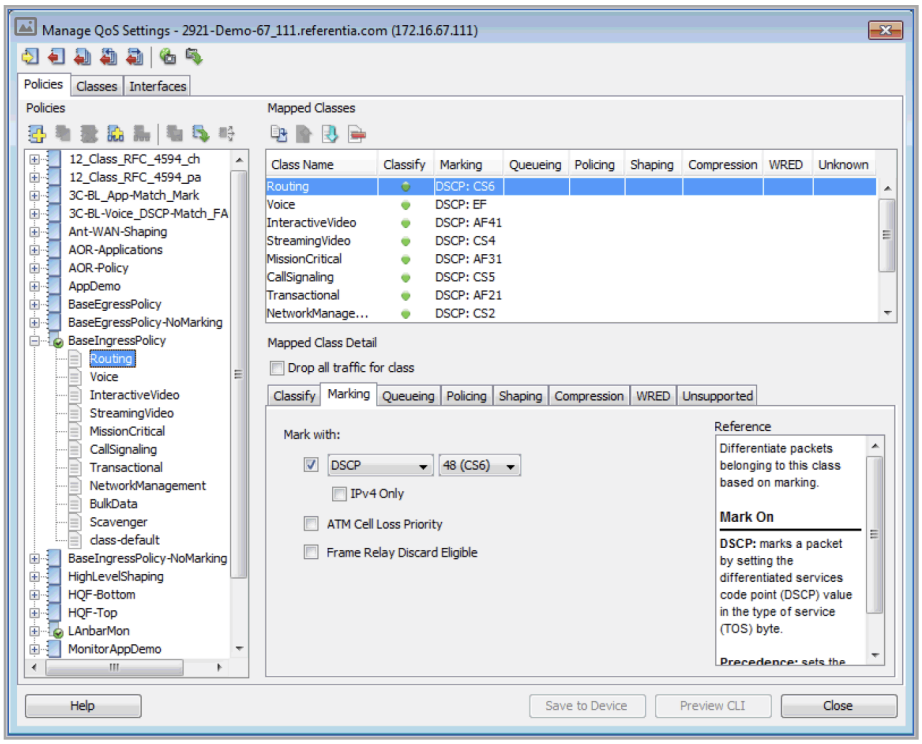
CHAPTER 6

QoS

In this chapter:

About QoS

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.

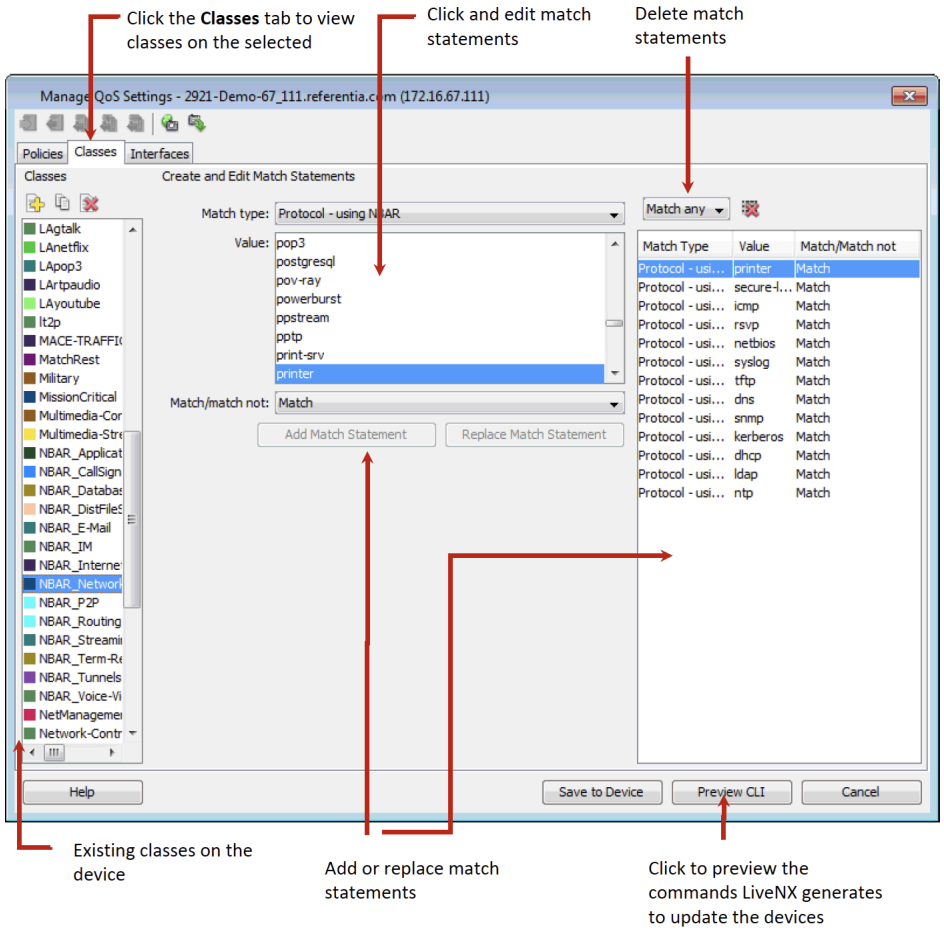
The QoS capabilities of LiveNX allow you to create policies from scratch, or from templates and wizards. Combined with its in-depth QoS monitoring capabilities, the software provides real-time feedback on how well the configuration is working. A built-in ACL editor is provided to create rules for use 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.

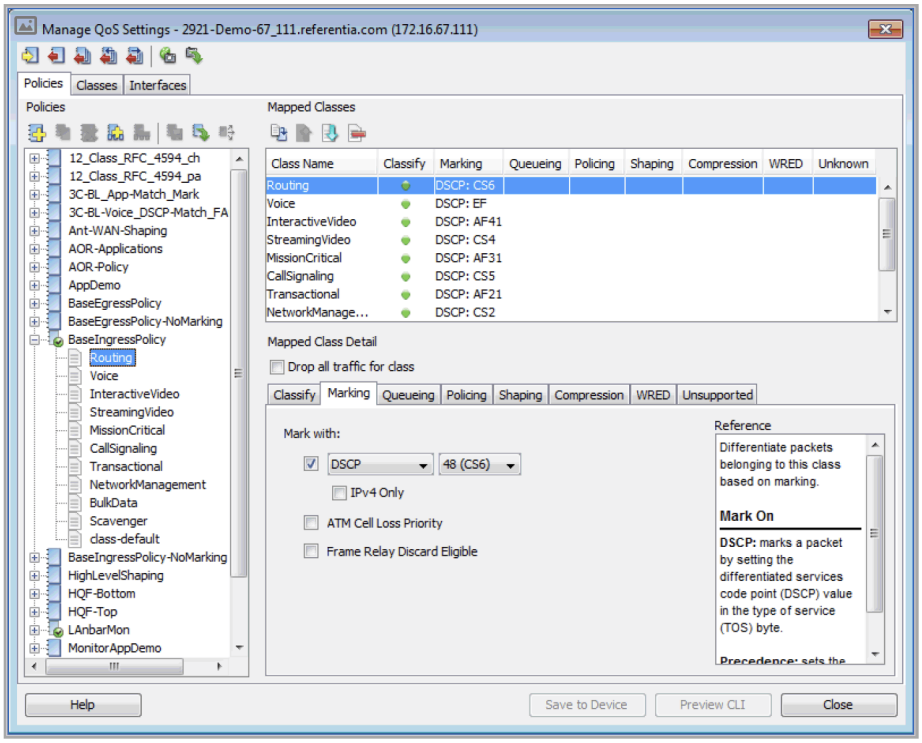
Manage QoS Settings Screen

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.

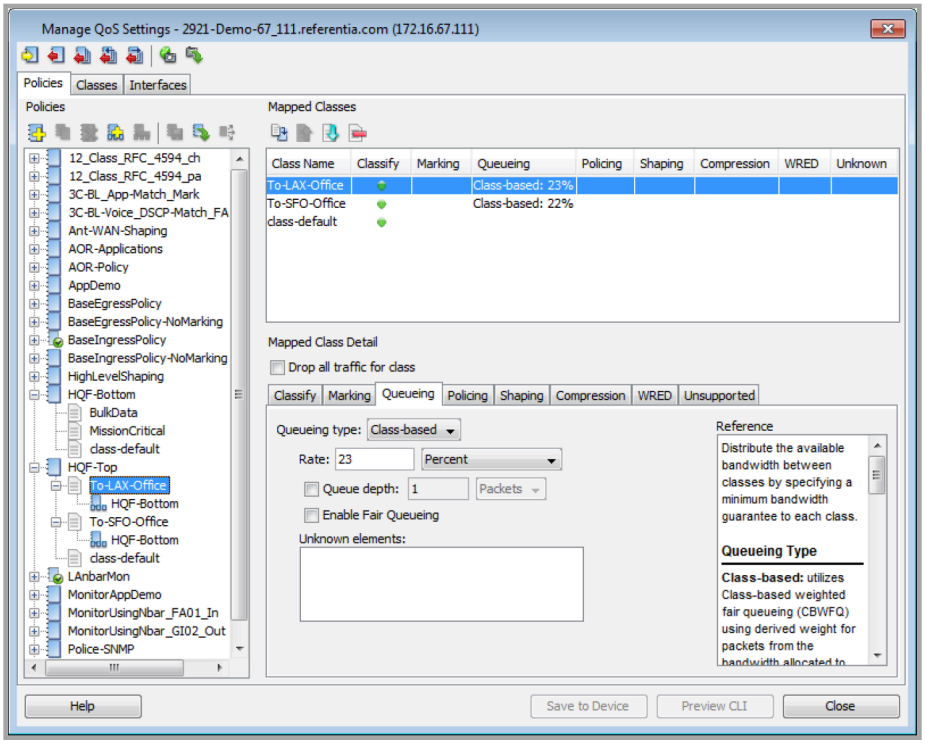
The main Manage QoS Settings screen provides all the QoS capabilities of the router within a single dialog box. This dialog box can be accessed by right-clicking on any of the devices or their interfaces, or from the QoS menu. The tree view at left shows existing policies for the device and the Mapped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





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 drop-down 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.



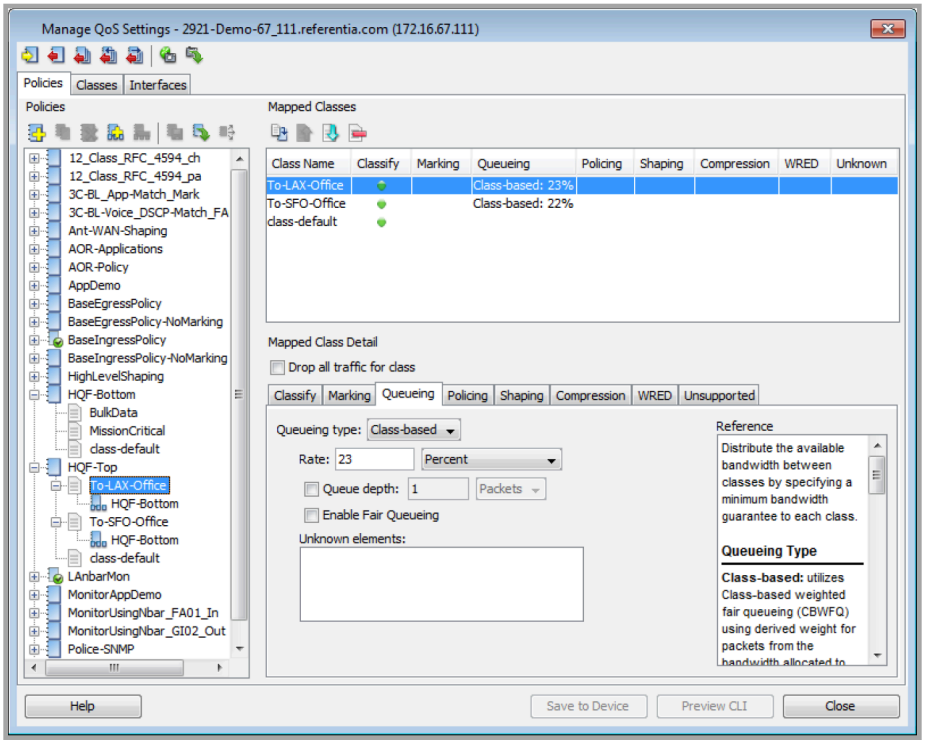
Enable queueing capability by selecting either Class-based, Priority or Fair in the Queueing type: drop-down. The fourth option is None. Default is None. The Priority option is available when selecting a new class within a policy.

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.

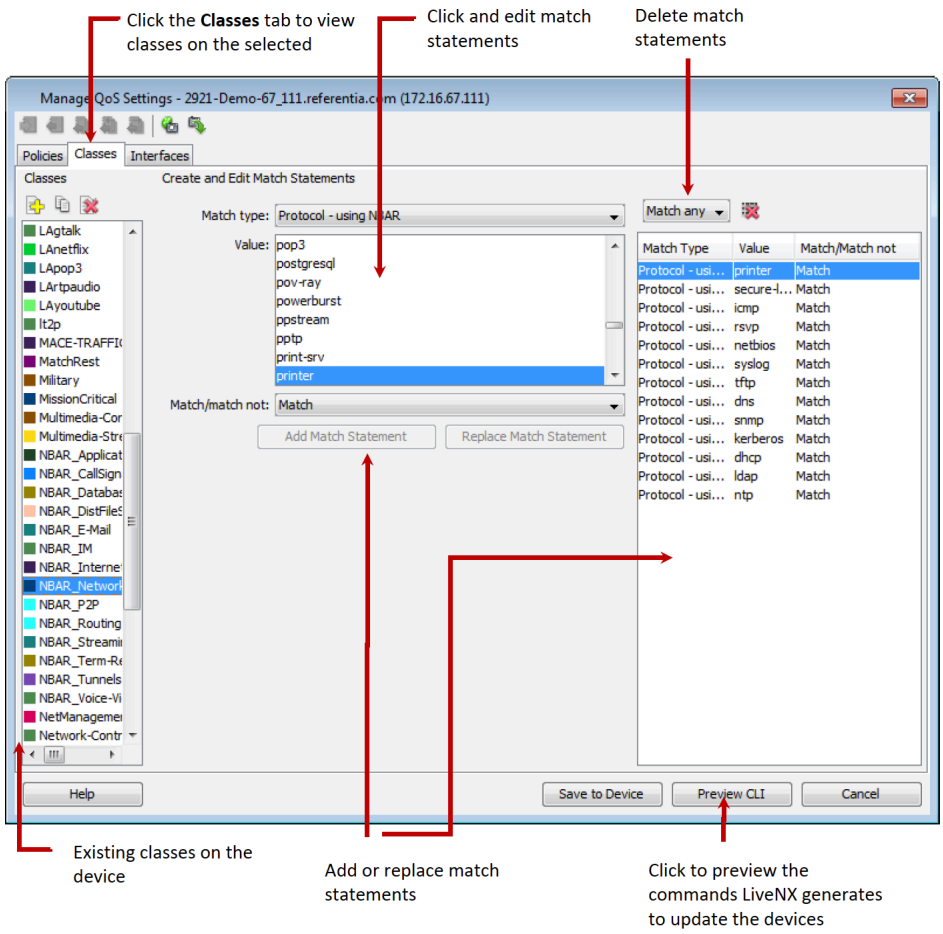
Hierarchical Queuing Framework (HQF)

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



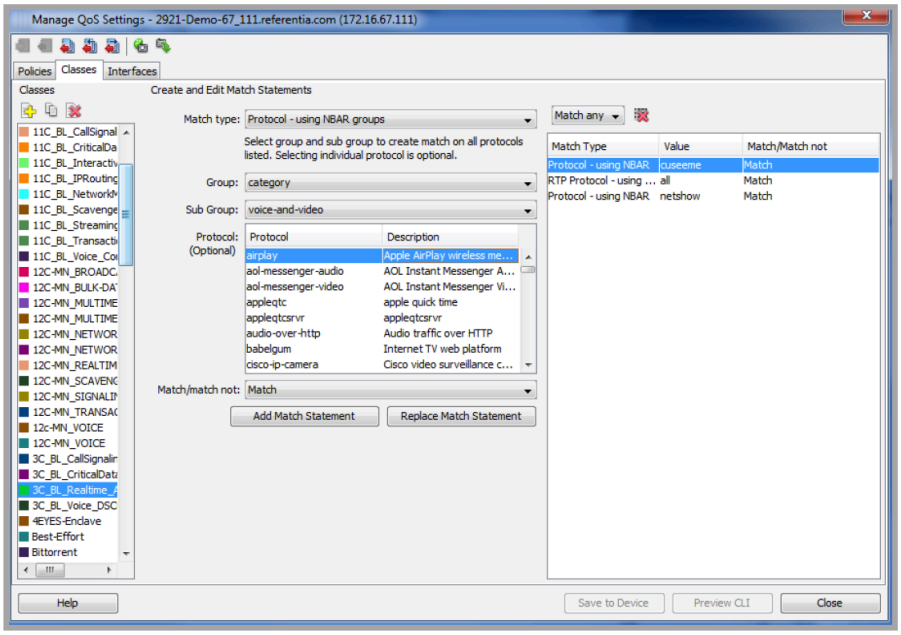
Manage QoS Settings—Classes Tab

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.

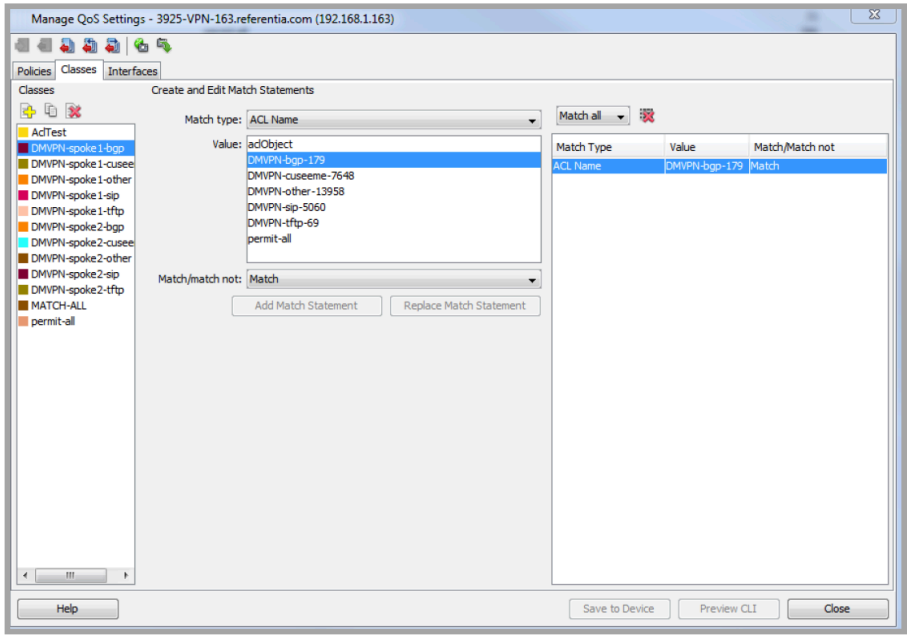


See the following Image for an example of matching using NBAR2

- 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.



- 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.



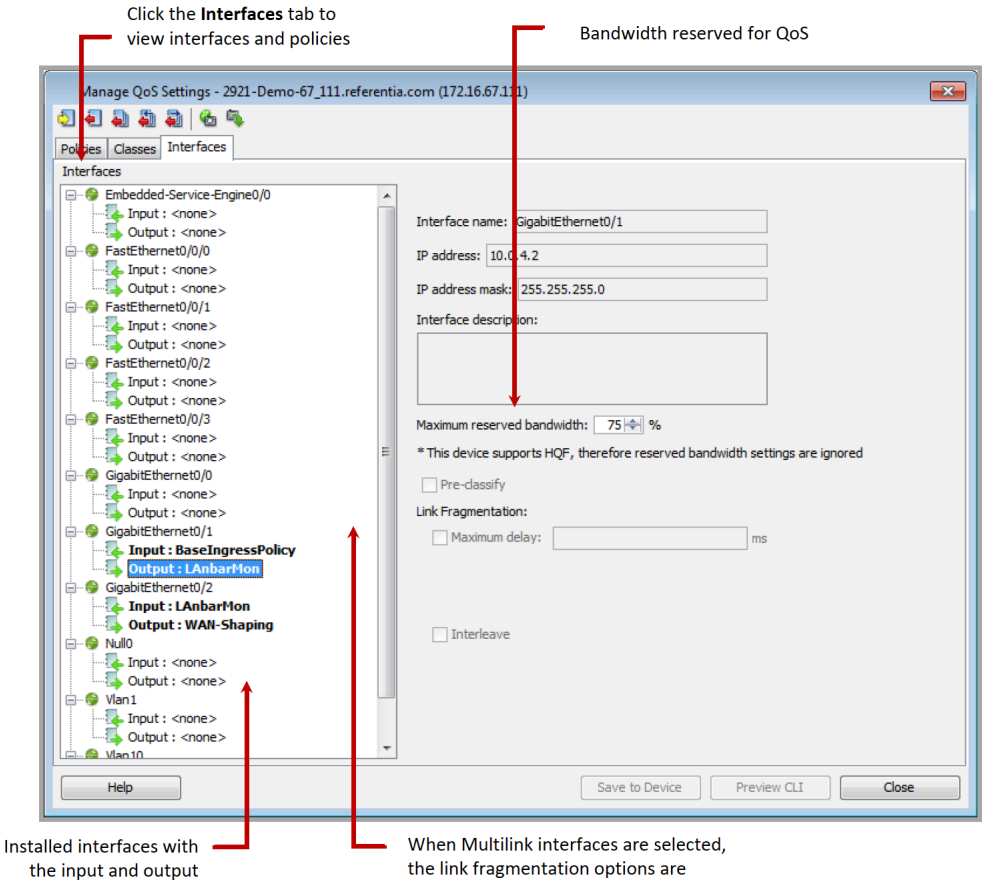
In the Manage QoS Settings window, click on the Classes tab. Use the Match type drop-down to select ACL Name. The Values correspond to the saved ACL names. Highlight the desired ACL and choose Match or Match not. Click on Preview CLI to review the match command and Save to Device to add this to the QoS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

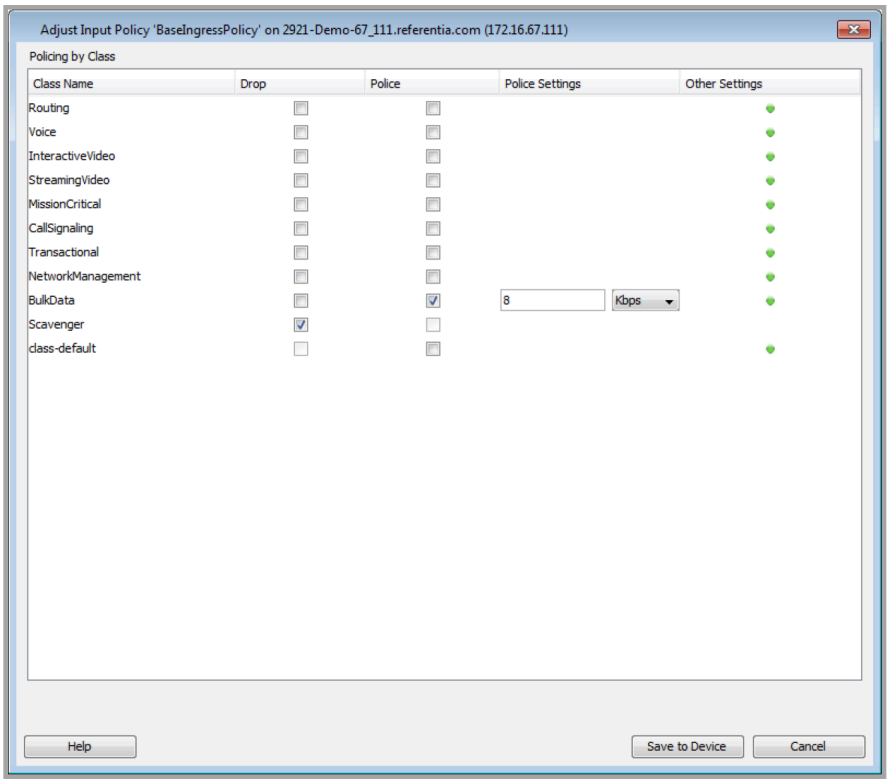


Maximum Reserved Bandwidth Dialog Box

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.

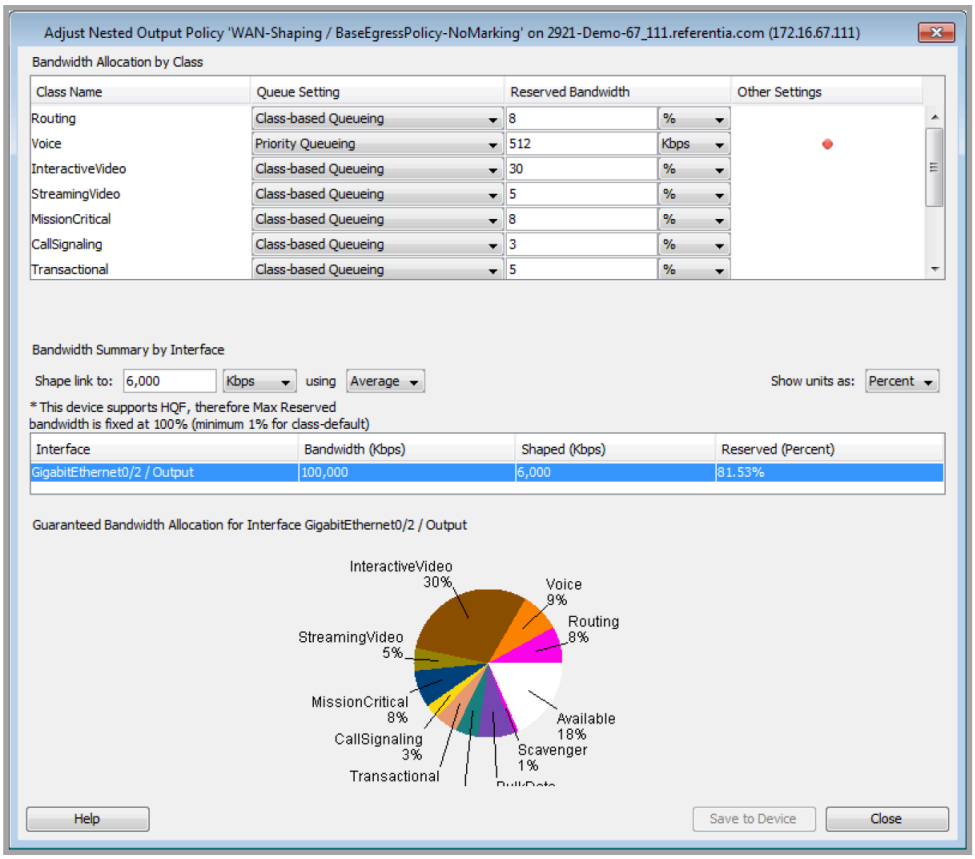
Adjust Input QoS Policy

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.

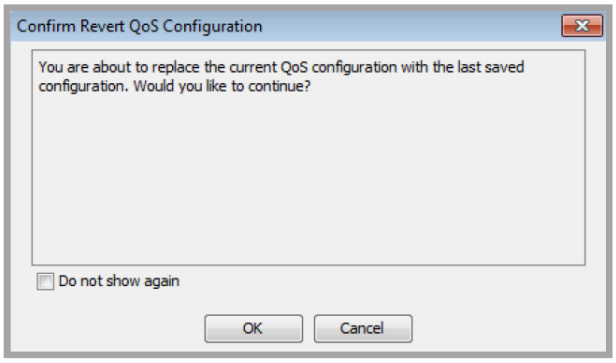


Adjust Output QoS Policy

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.



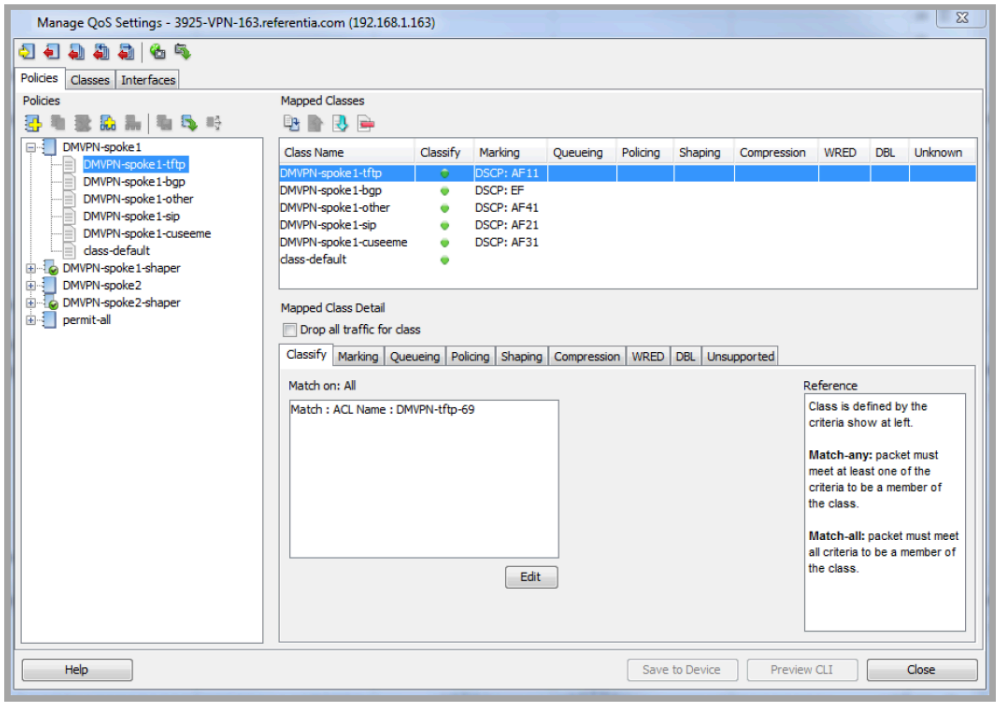
The revert QoS configuration is available to undo the last QoS change made via the Manage QoS Settings dialog or the adjust input QoS or the adjust Output QoS settings. When selected, LiveNX sends a dialog box to confirm the revert command.



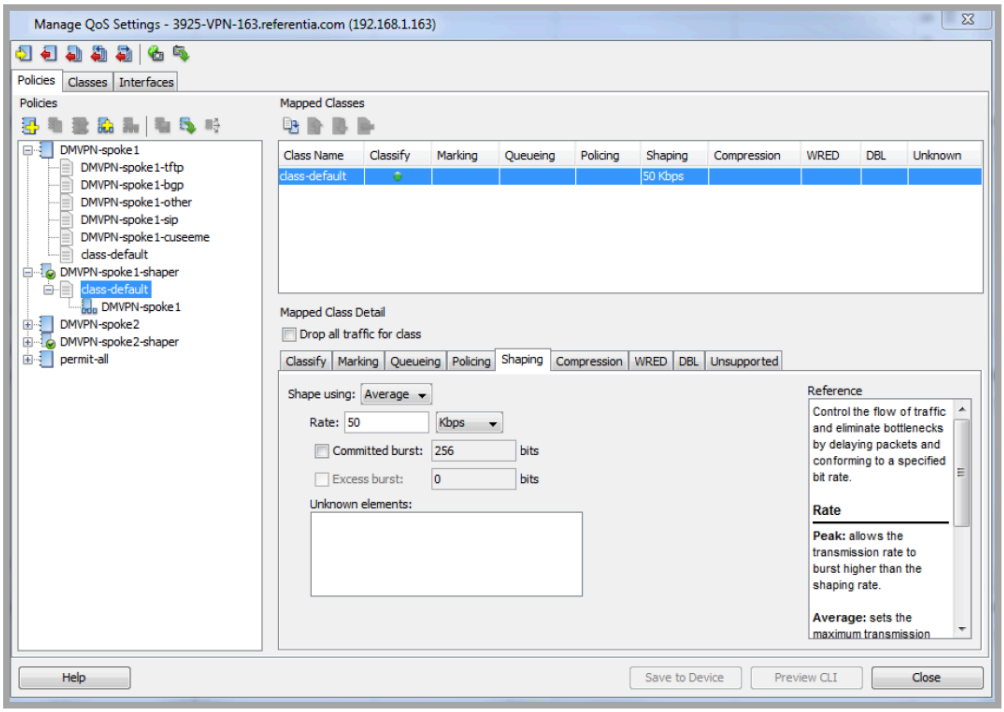
Managing DMVPN QoS Policies

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

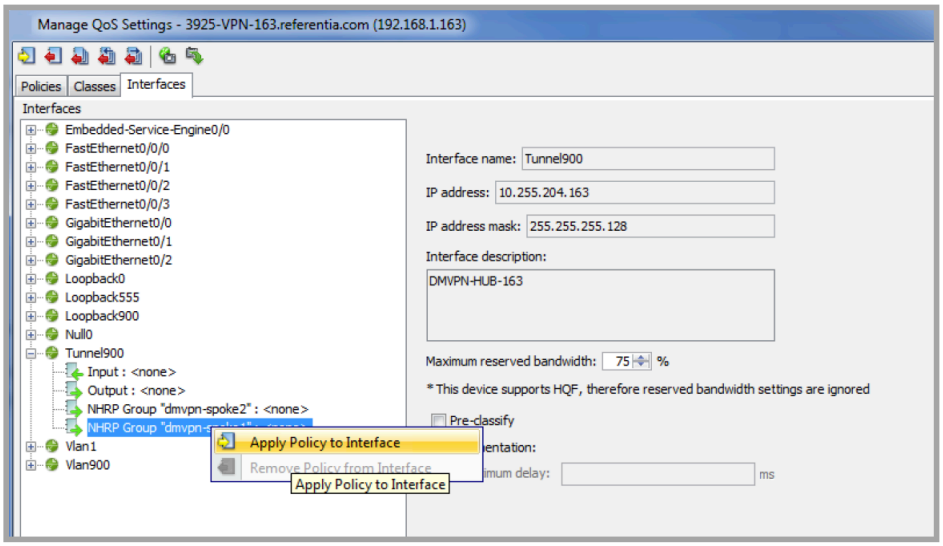
In this example, a DMVPN-spoke1 policy is created consisting of six classes, each with a unique DSCP marking. A similar policy is created called DMVPN-spoke2.



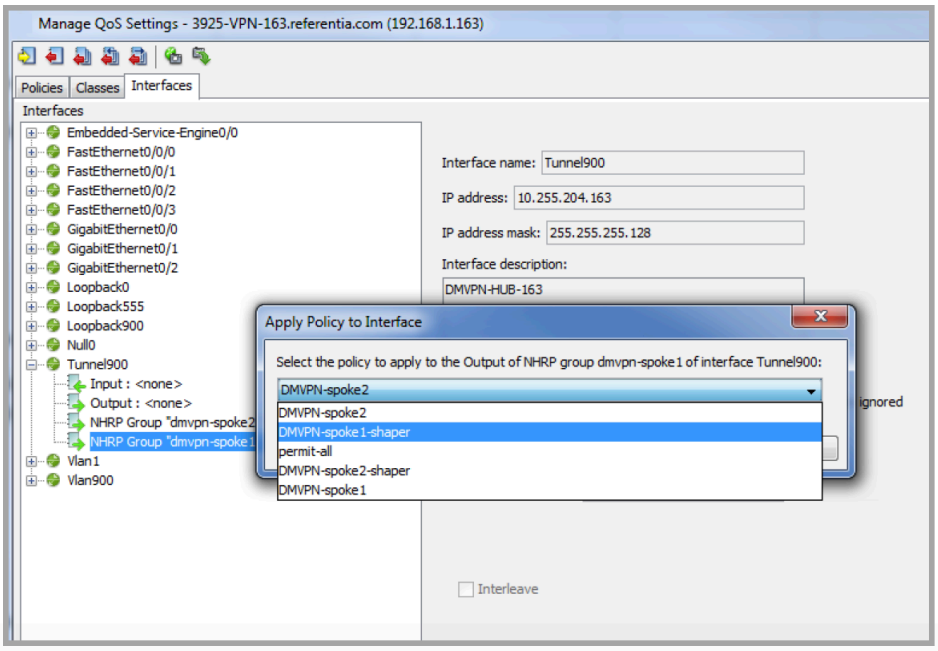
A hierarchical policy may be created to shape the specific spoke for a particular average bandwidth.



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



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



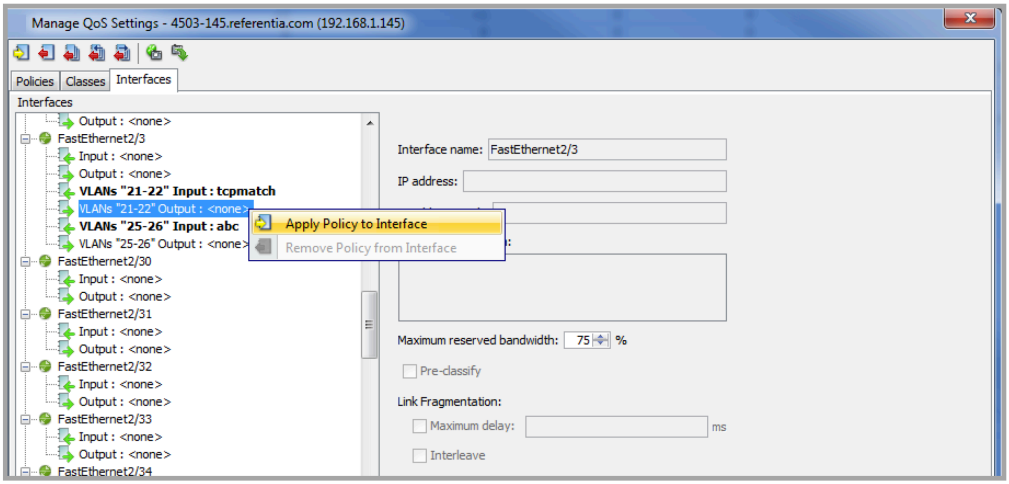
VLAN Service Policies

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

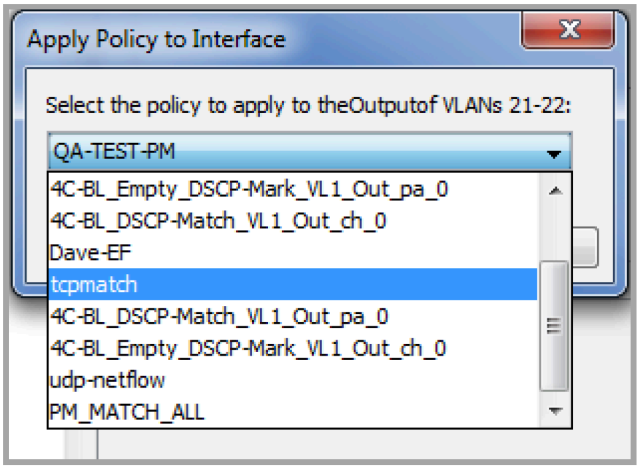
Note Only devices with pre-defined VLAN ranges can be added through LiveNX.

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.

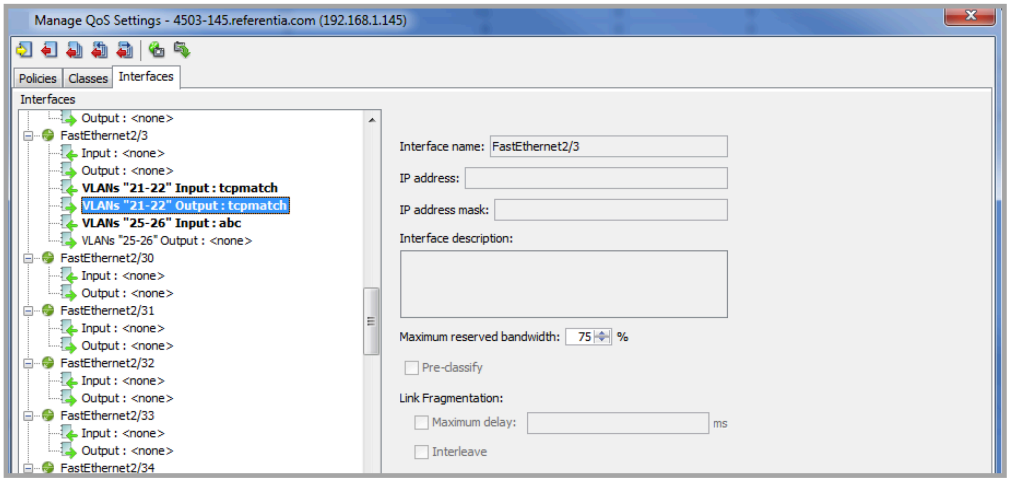
To apply a policy to a given VLAN range, right click on the device and select QoS > Manage QoS Settings. Then select the Interfaces tab and then find the desired interface & VLAN range and select Apply Policy to Interface.



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.

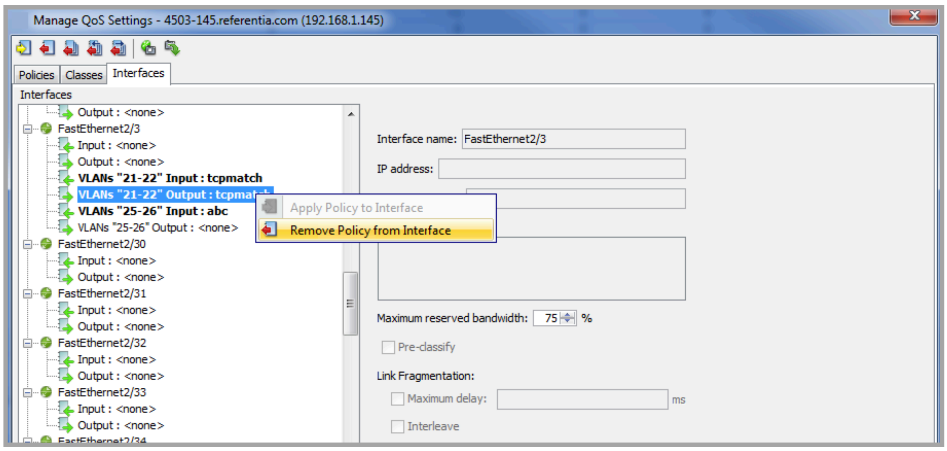


LiveNX will then add the given policy to the defined VLAN range.



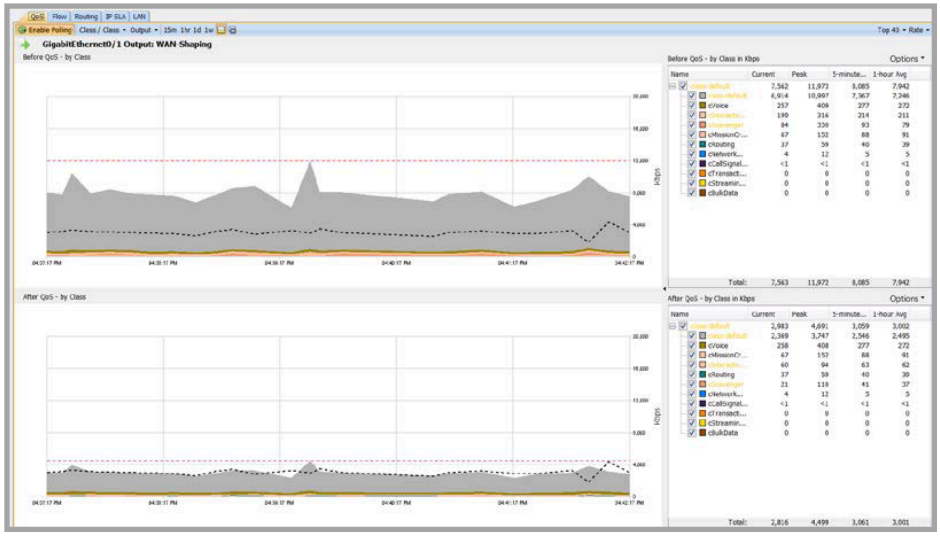
At the bottom of the Manage QoS Settings window, click on Preview CLI to review the CLI commands prior to saving to the device. Click on Save to Device to apply the policies to the desired VLAN range.

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



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.

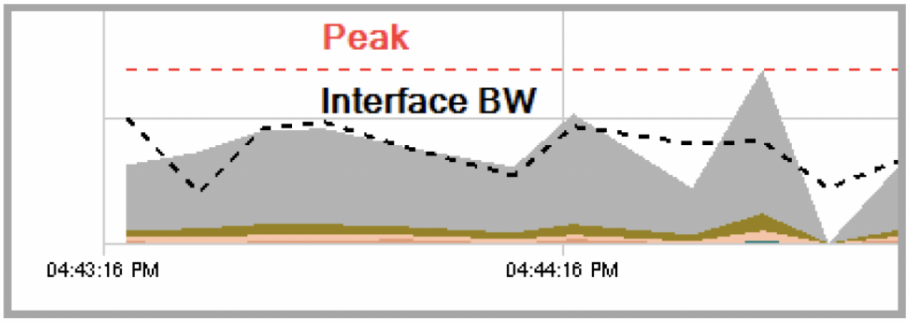
QoS Graphing Options

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

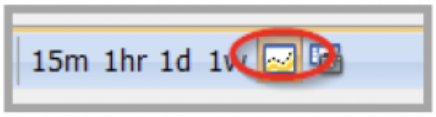
- Application—Uses Cisco NBAR capability to identify applications
- Class—QoS policy-based statistics. If there is no policy, then only the traffic outline is displayed.

- 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

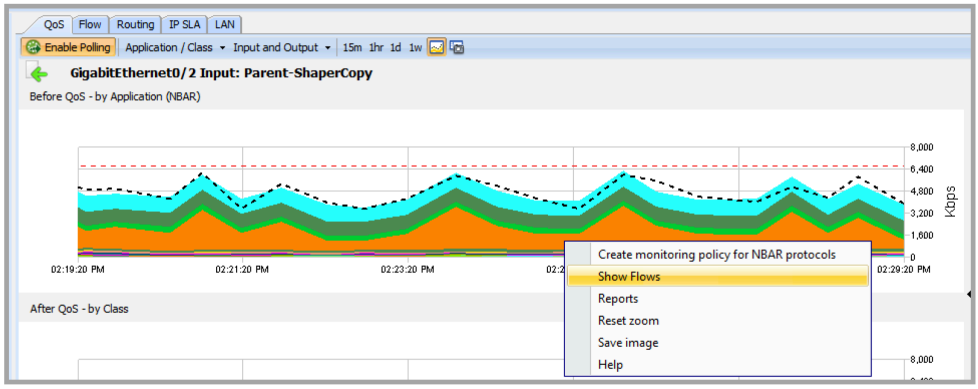


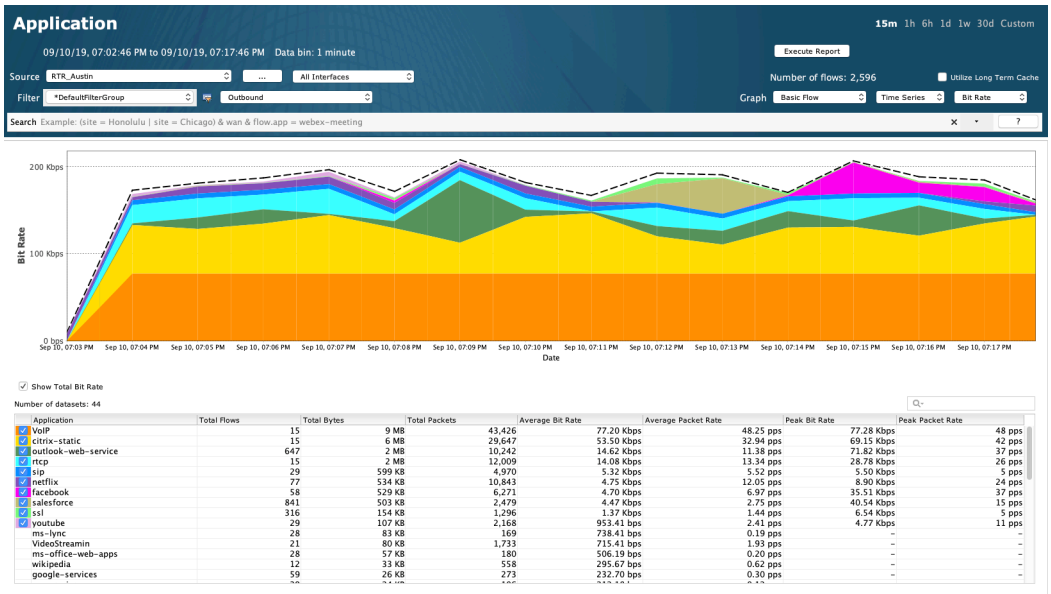
- Stacked area chart displays the data shown in the legend. If the policy is hierarchical, the child policy class information is charted in the class and class drop views.
- Black dotted line represents the interface bandwidth from the IF mib and is shown to help for correlation purposes. Since the IF 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

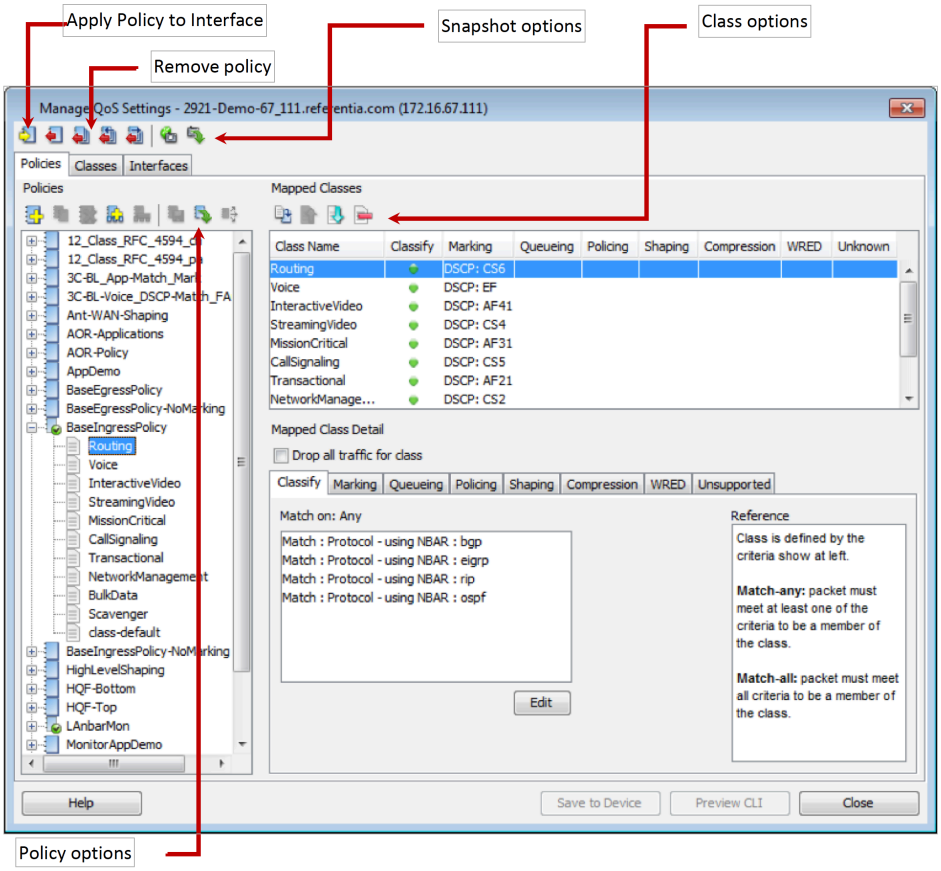
Historical views allow you to view past data interactively. See the Reporting > QoS Reports section for more information.

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



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:

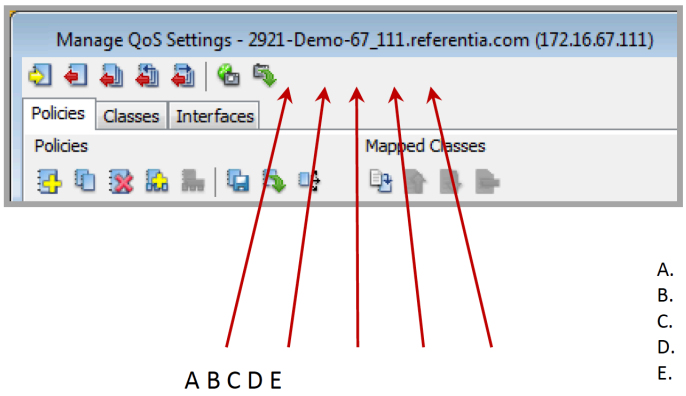
Note When a policy is applied to multiple interfaces, changing the policy will affect every interface to which the policy is applied.

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.

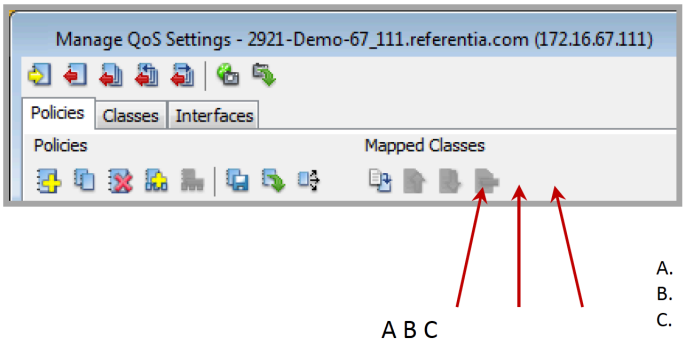
Saving, Loading, and Copying QoS Policies

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

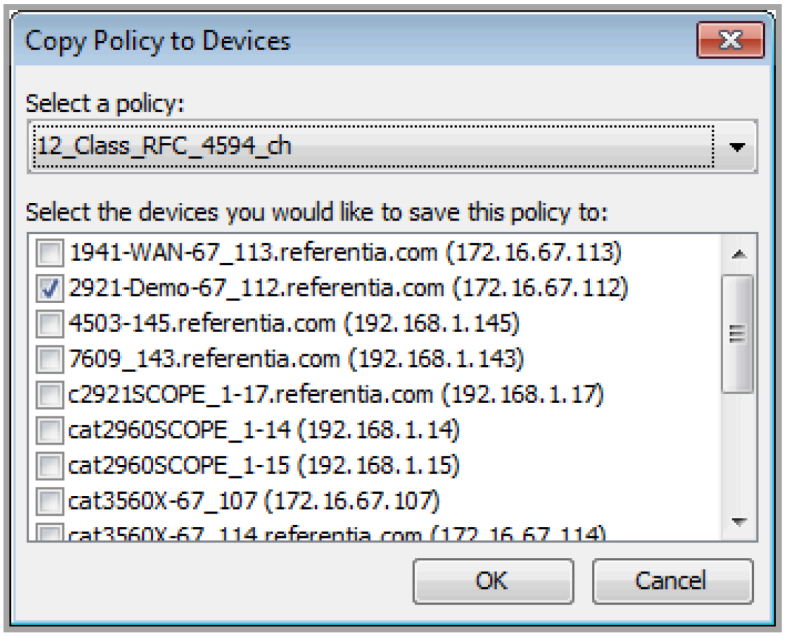
- To save a policy to disk—From the Manage QoS Settings screen, click the “Save QoS Policy File” icon. This will save the NBAR and ACLs that are required for the policy to operate. The file will have a .qos-policy extension.
- To load a policy from disk—From the Manage QoS Settings screen, click the “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.



A. Apply policy to interface
B. Remove from interface
C. Remove all from all interfaces
D. Remove all input policies
E. Remove all output policies



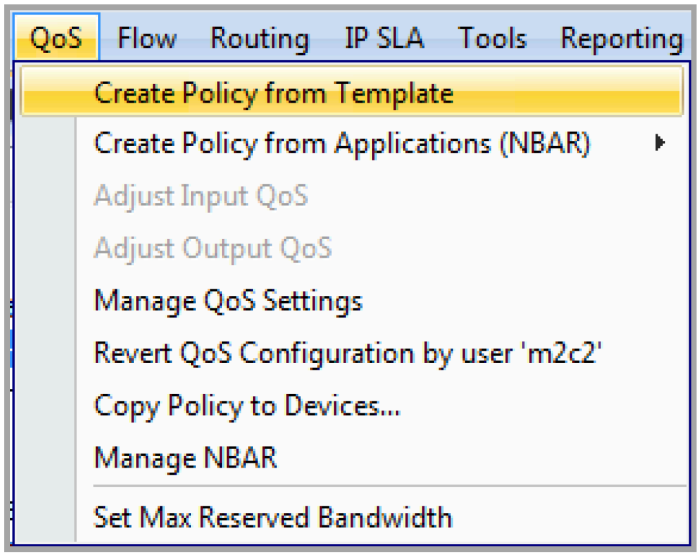
A. Save QoS policy file
B. Load QoS policy file
C. Copy policy to devices



Creating Policies from Templates

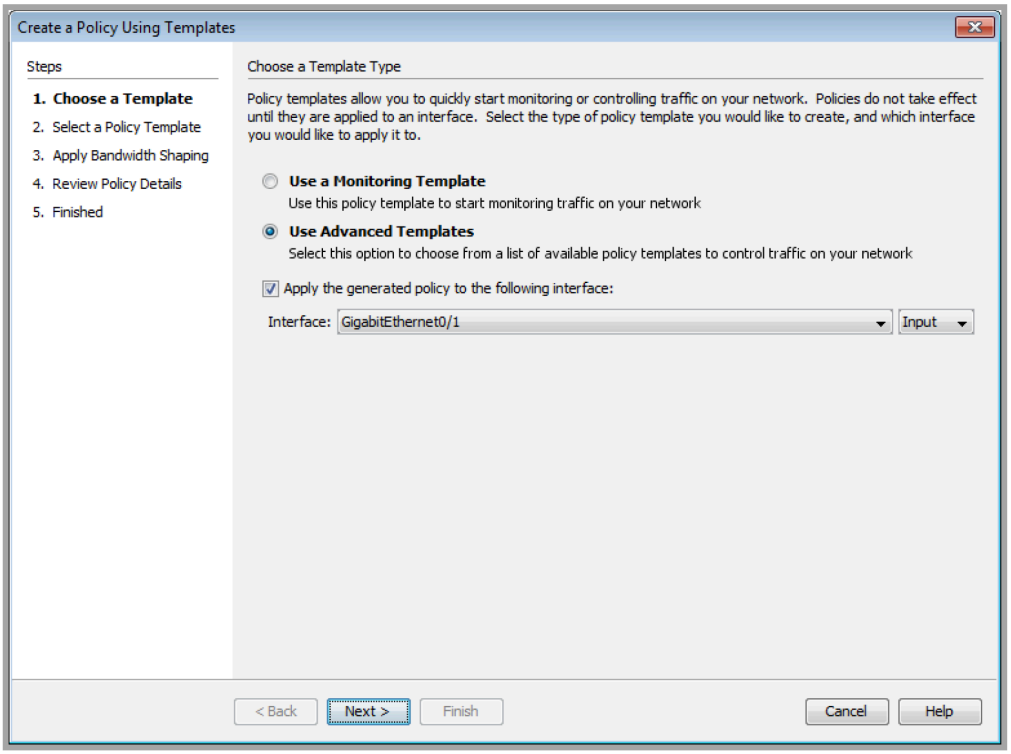
Creating a policy from templates allows you to quickly apply a policy based on Cisco best practices and recommendations. A policy with up to 11 classes can be created for monitoring or controlling traffic using various classification methods.

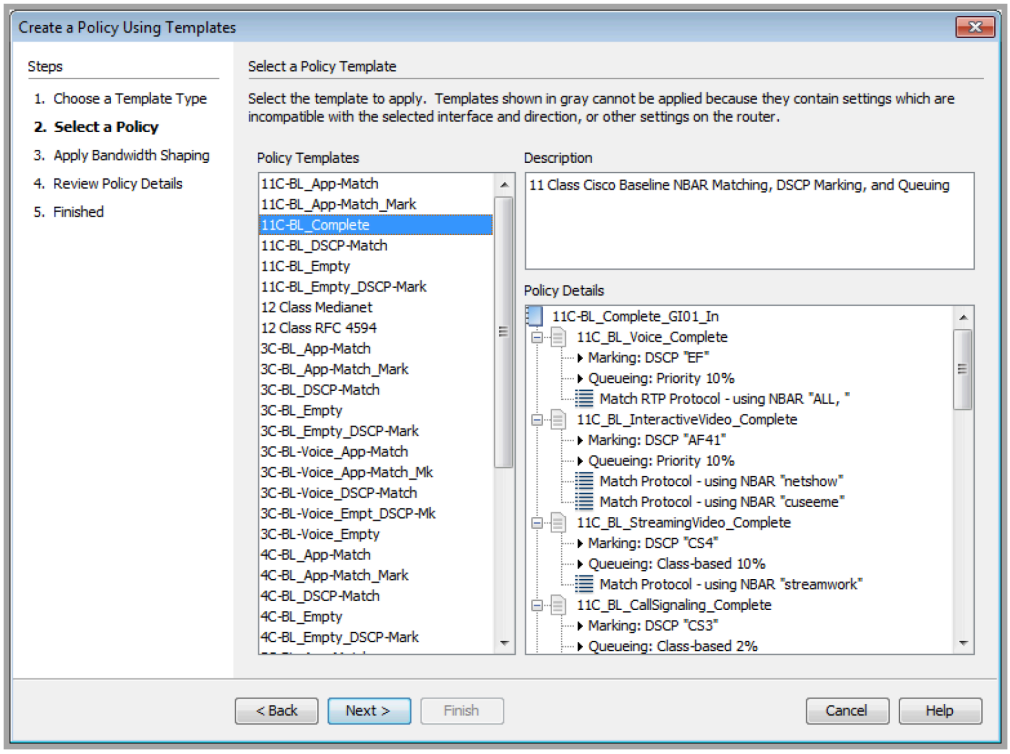
1. Select Create policy from Template from the QoS menu.



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.

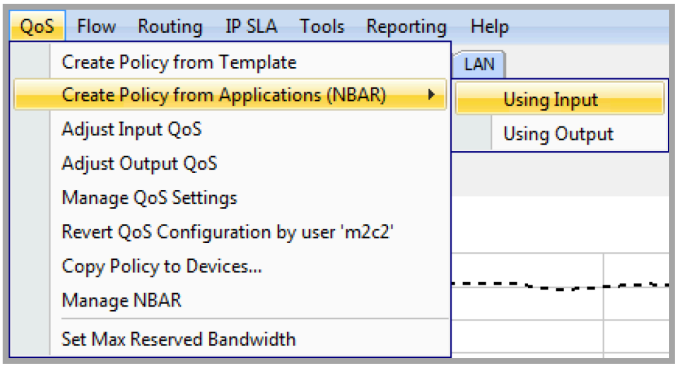




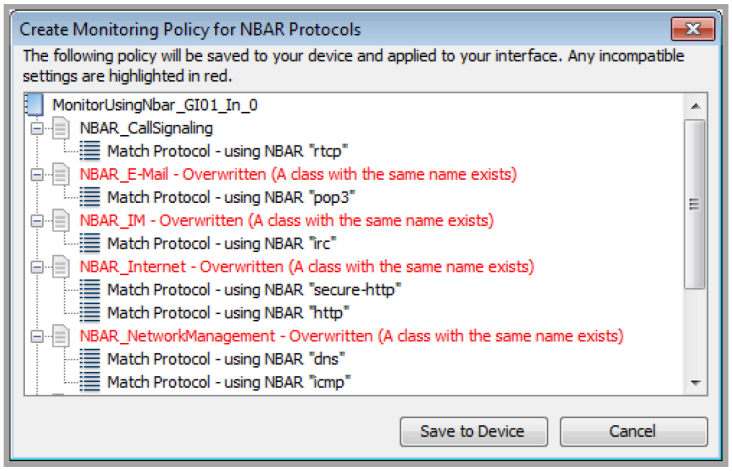
Creating Policies Using NBAR

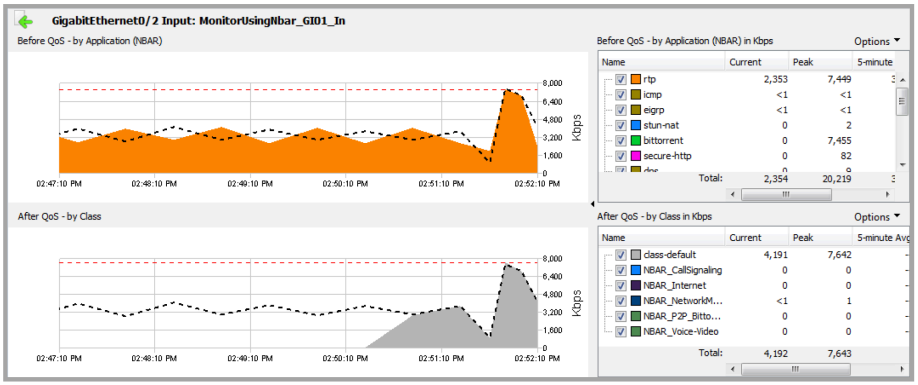
LiveNX makes it easy to create a monitoring policy based on the NBAR protocols that the device has recognized, and provides a skeleton policy for further editing.

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.



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.

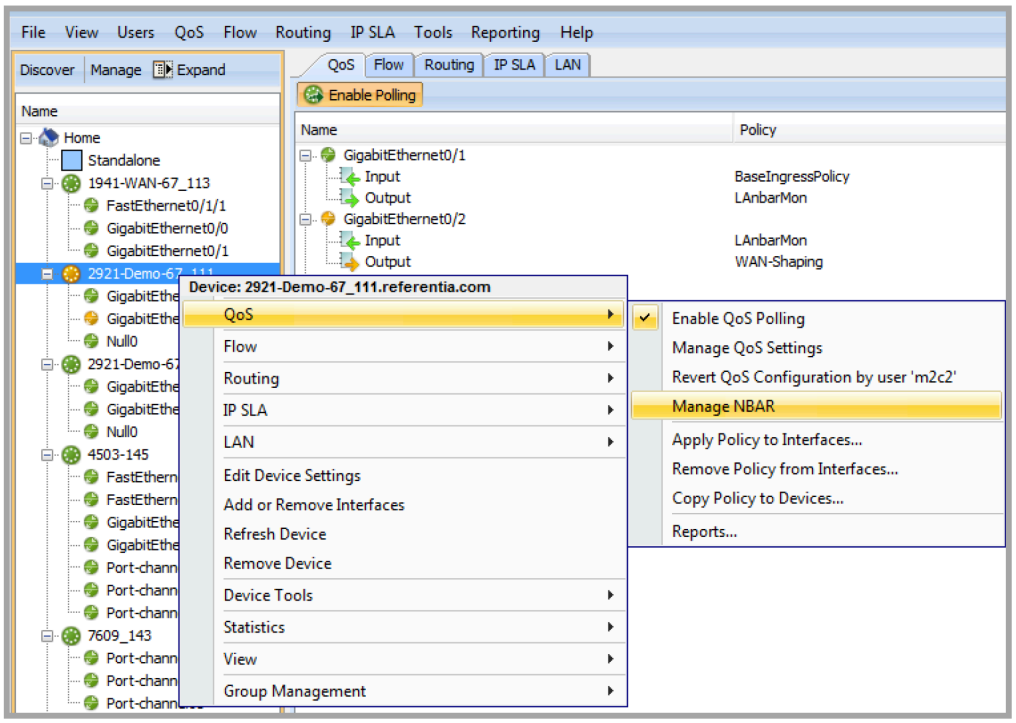




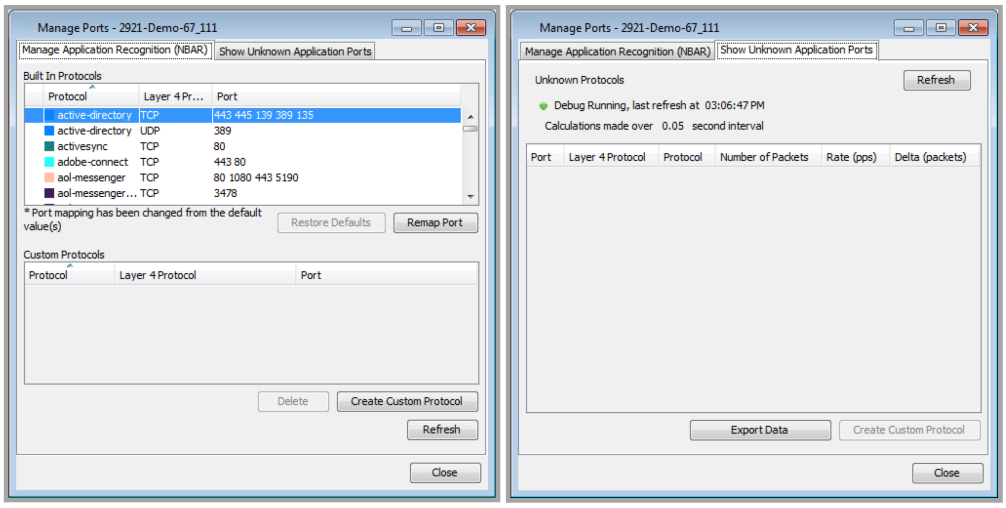
Customizing NBAR Protocols

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.



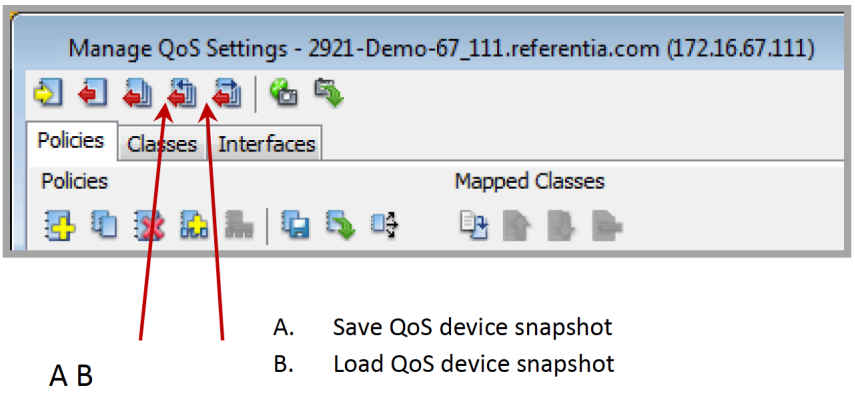
Existing protocols can be customized by adding, removing or changing TCP and UDP port numbers. Unknown protocols can be identified and assigned a new name.



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

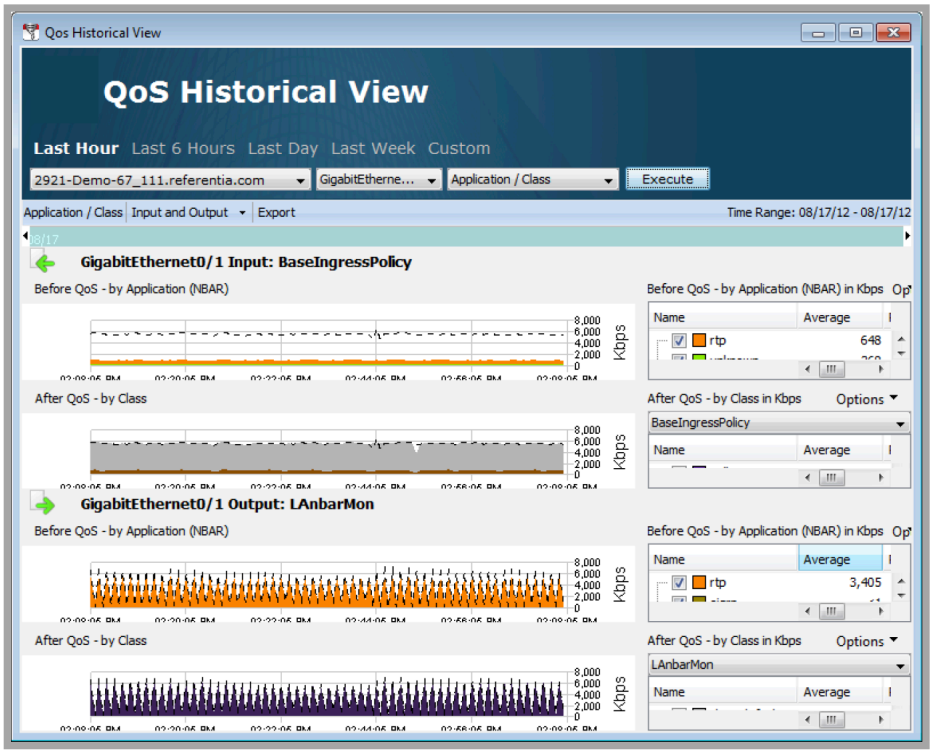
Planning and Implementing Quality of Service Policies

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

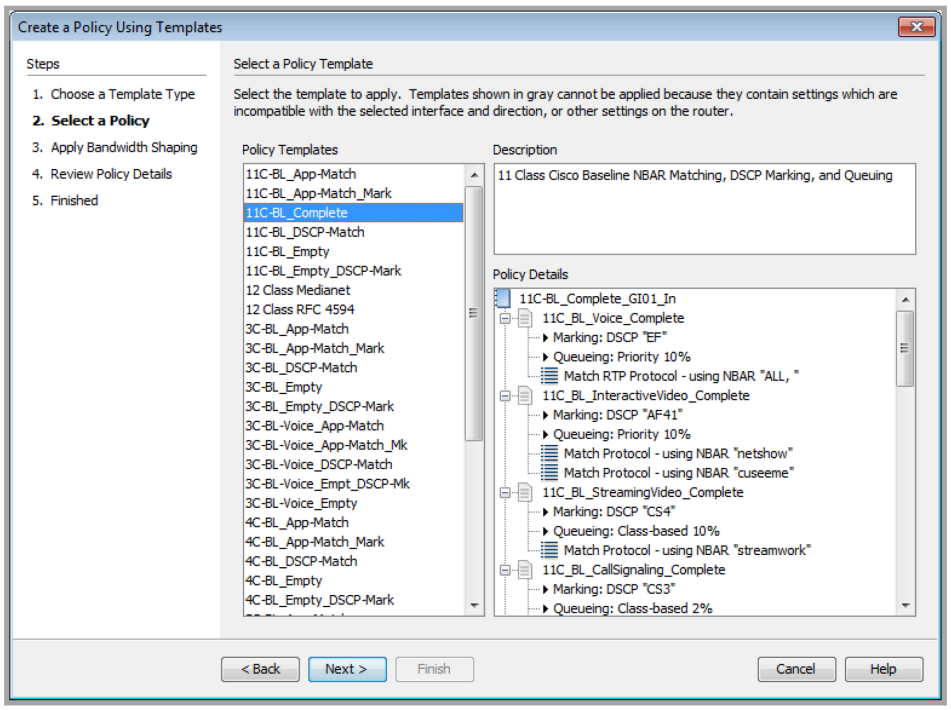
Identify network traffic, baseline behavior, and service-level requirements

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

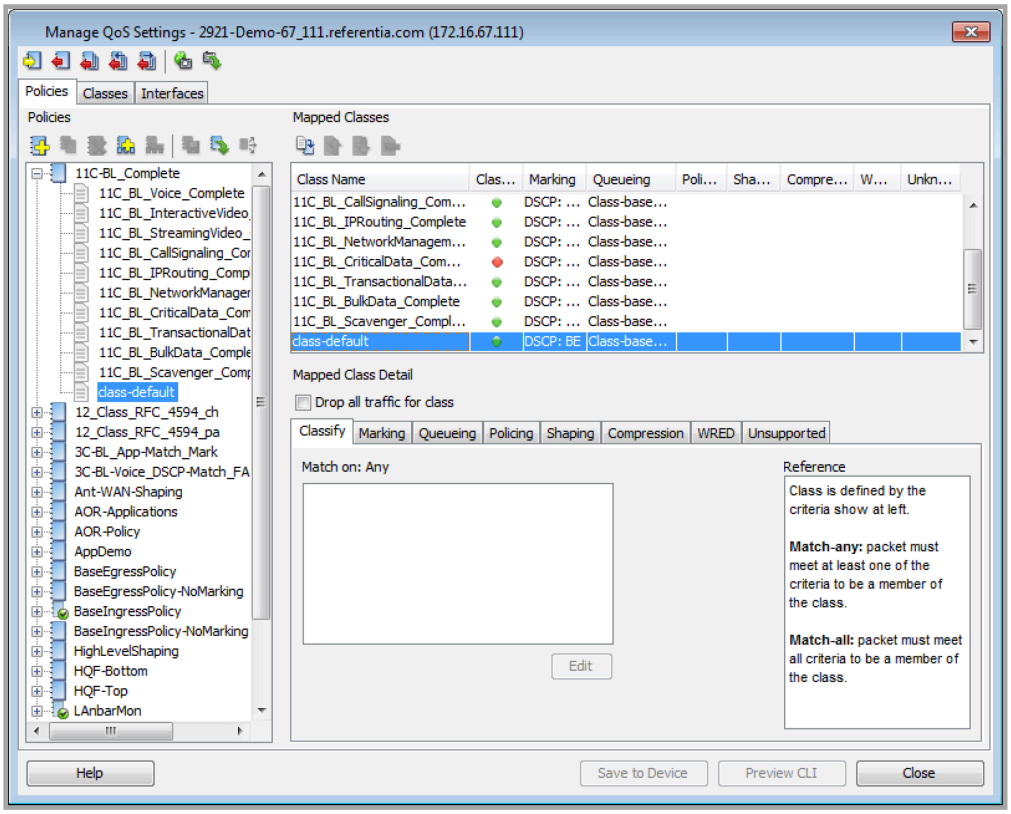
Traffic can be divided into classes based on the identified traffic and the business requirements. The Cisco baseline model, which consists of 11 classes, is designed to provide granularity for various class types with different service requirements. Each type of class may have unique QoS requirements 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

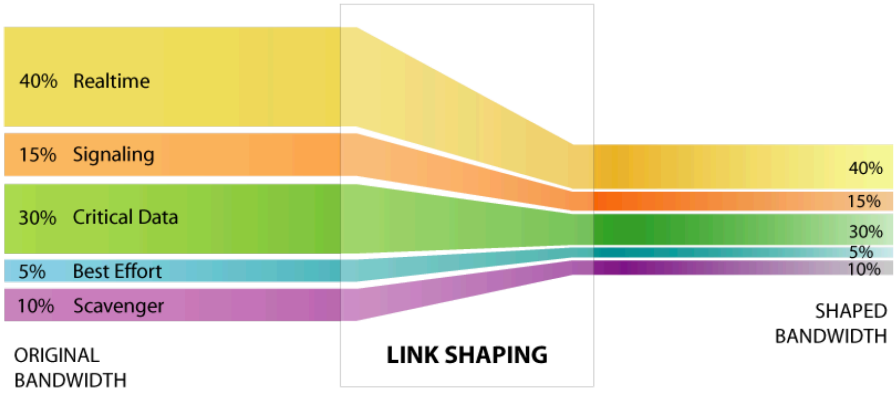
QoS policies should be designed from high-level requirements to meet specific objectives. Once the requirements are understood, they can be translated to QoS best practices for the various application types.

- 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 priorityqueue 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 2overhead and Best Effort traffic.



WAN Link Shaping

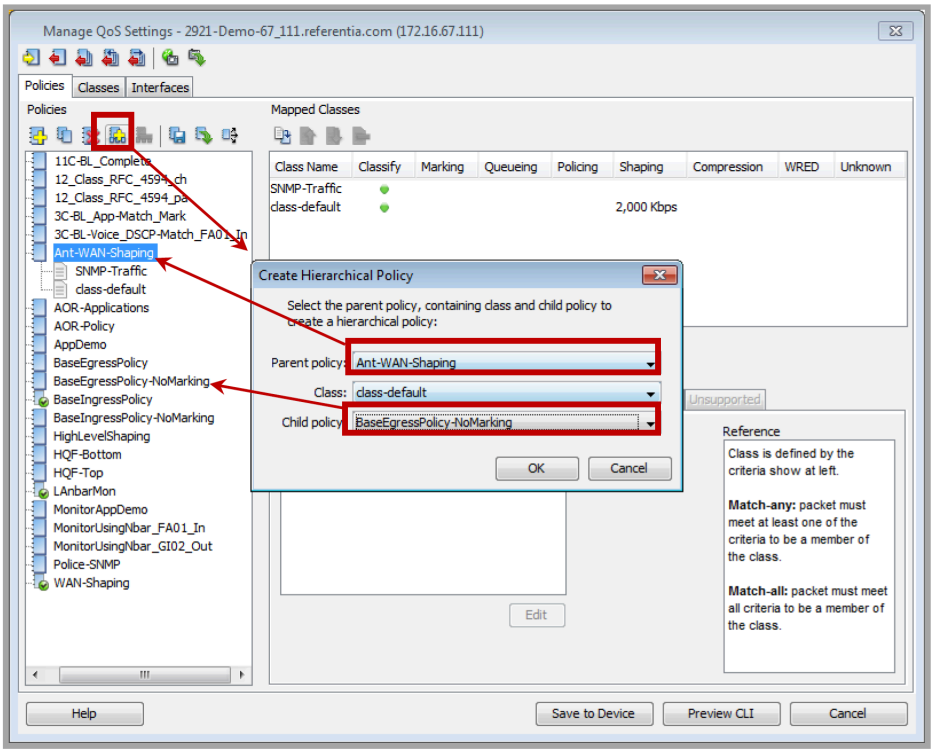
QoS polices for WAN aggregators typically configure various queuing, marking, shaping, policing, and link fragmentation settings. In most cases, there is a link-speed mismatch between the internal network speed and the external WAN link speed. In such cases, the best method is to use a hierarchical policy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

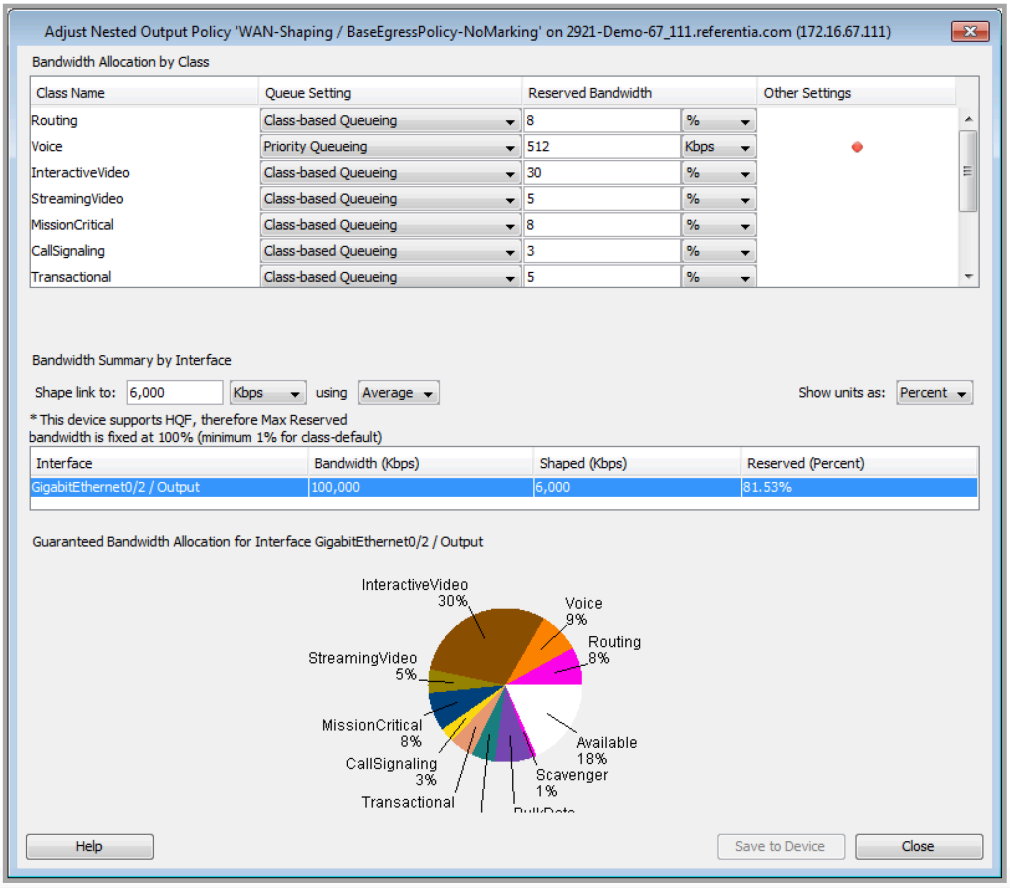


Creating a hierarchical WAN link-shaping policy involves creating a high-level (parent) shaping policy and then associating it with a lower-level (child) policy that actually defines the classes. In the following image, the high-level parent shaping policy basically consists of a class default that has 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.



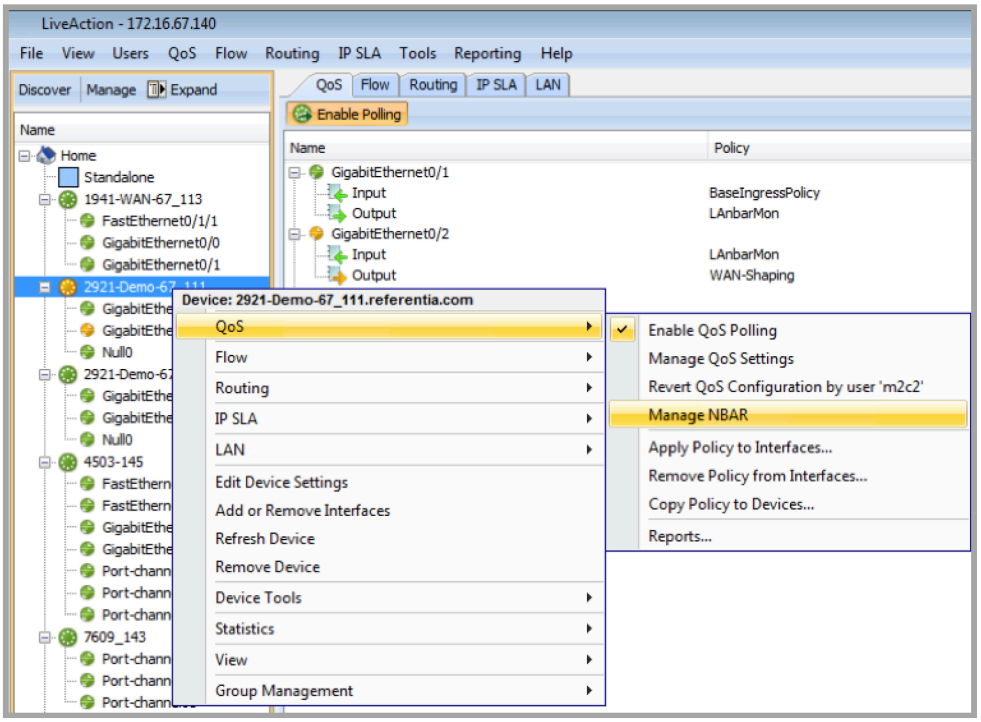


VoIP QoS Policy Creation

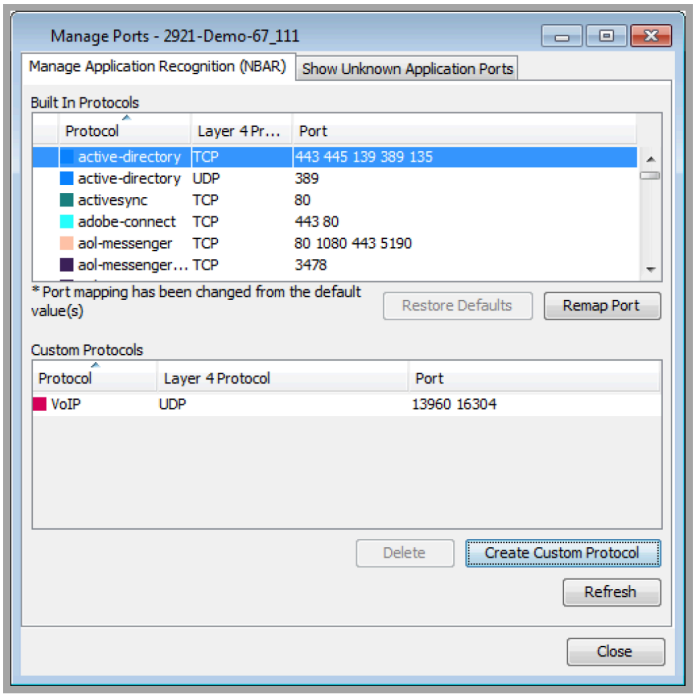
A voice call tends to be classified as RTP protocol; unfortunately, there are many other applications that also use RTP. One of the ways to classify voice traffic managed by Cisco Call Manager, Cisco Call Manger Express, and Asterisk Call Manager, is to use a custom NBAR classification.

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

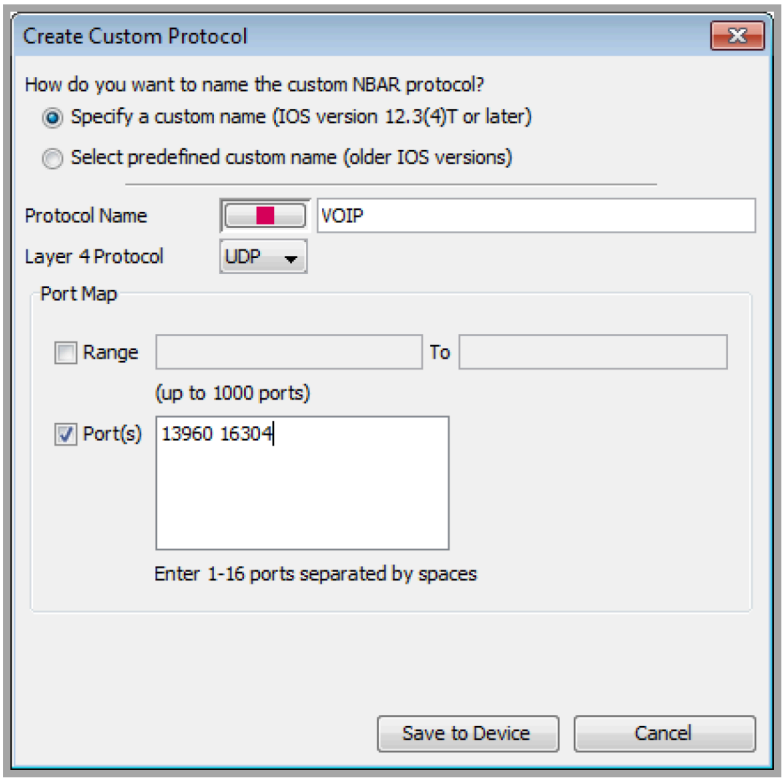
1. Select Manage NBAR from the QoS device right-click context menu.



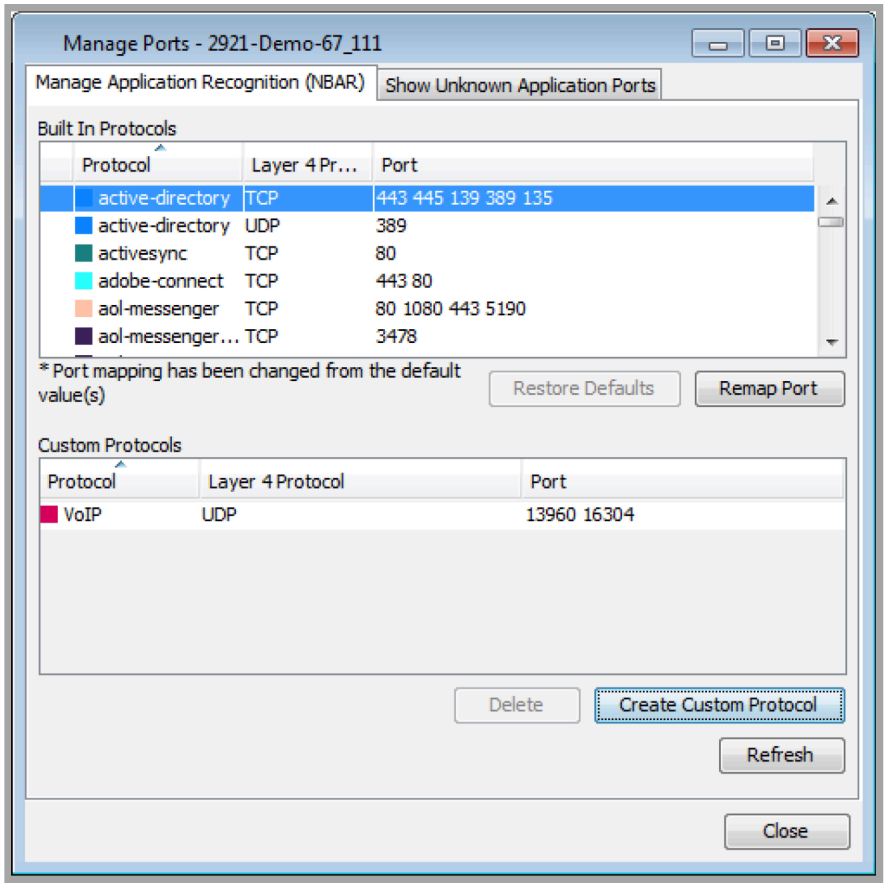
2. Manage Ports dialog will popup. On the Manage Application Recognition (NBAR) tab, click Create Custom Protocol.



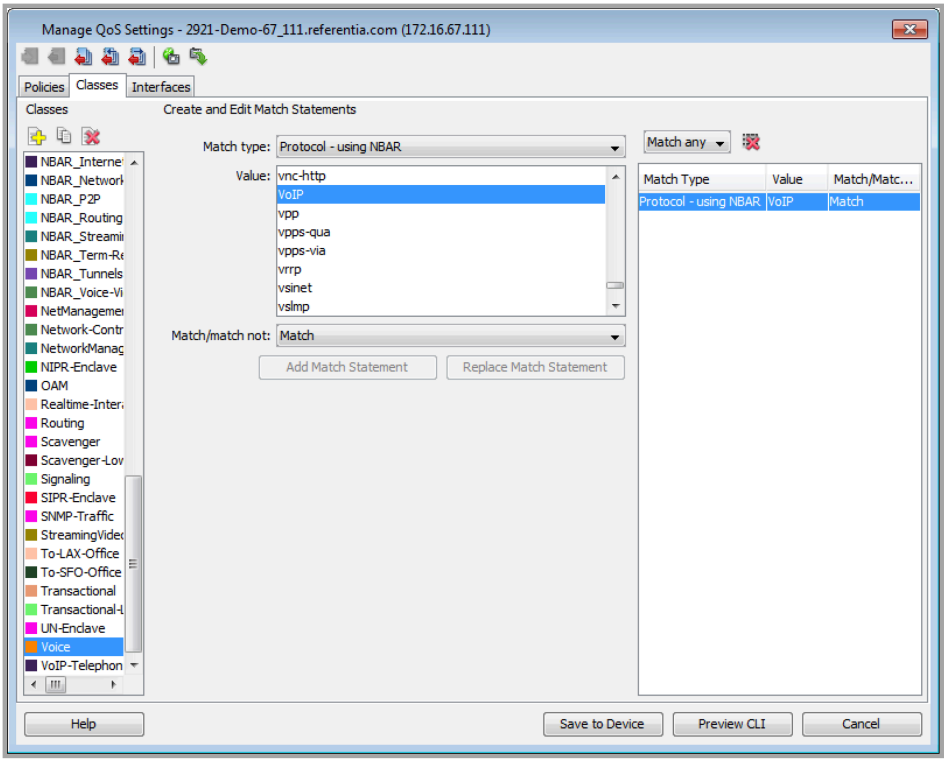
3. This will bring up a dialog box in which the name, protocol type, and port information can be entered.



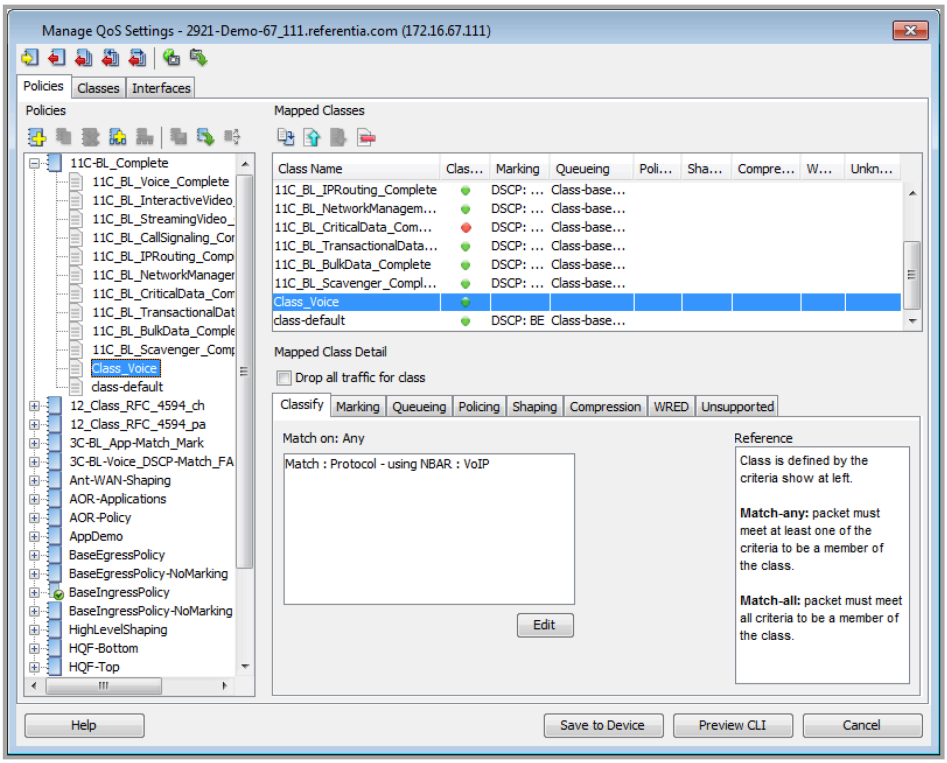
When completed, the command ip nbar custom voip udp 13960 16304 will be issued to the device. Once the custom protocol is created, it is available for use by the NBAR engine and will show up in the monitoring graphs.



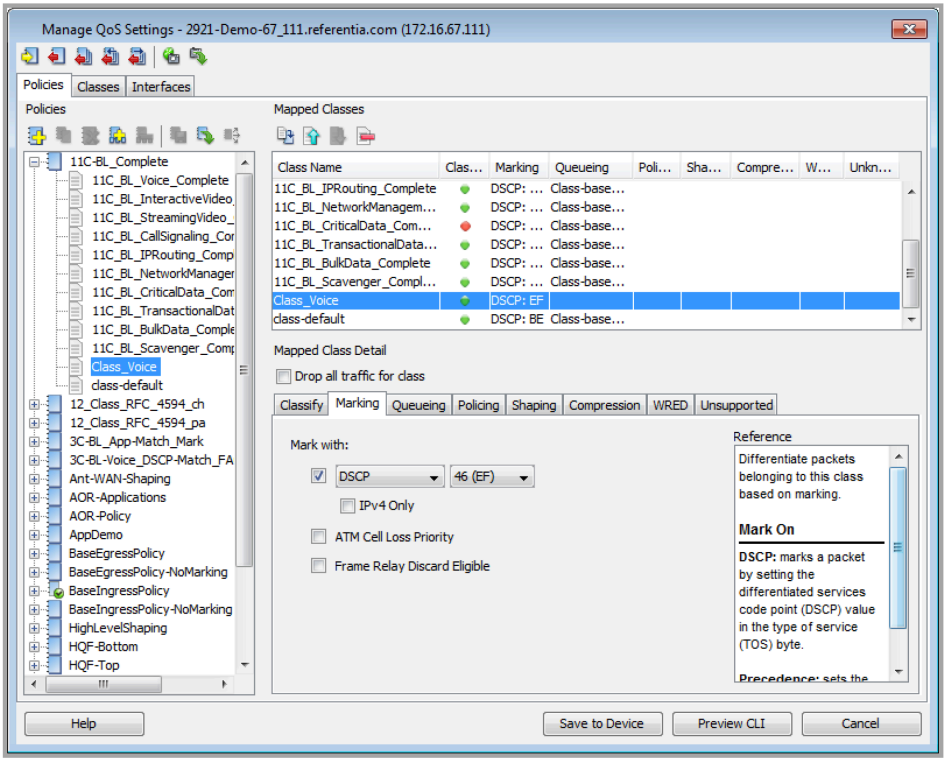
On the Manage QoS Settings screen, create a class for the VoIP traffic using the newly-created NBAR VoIP protocol.



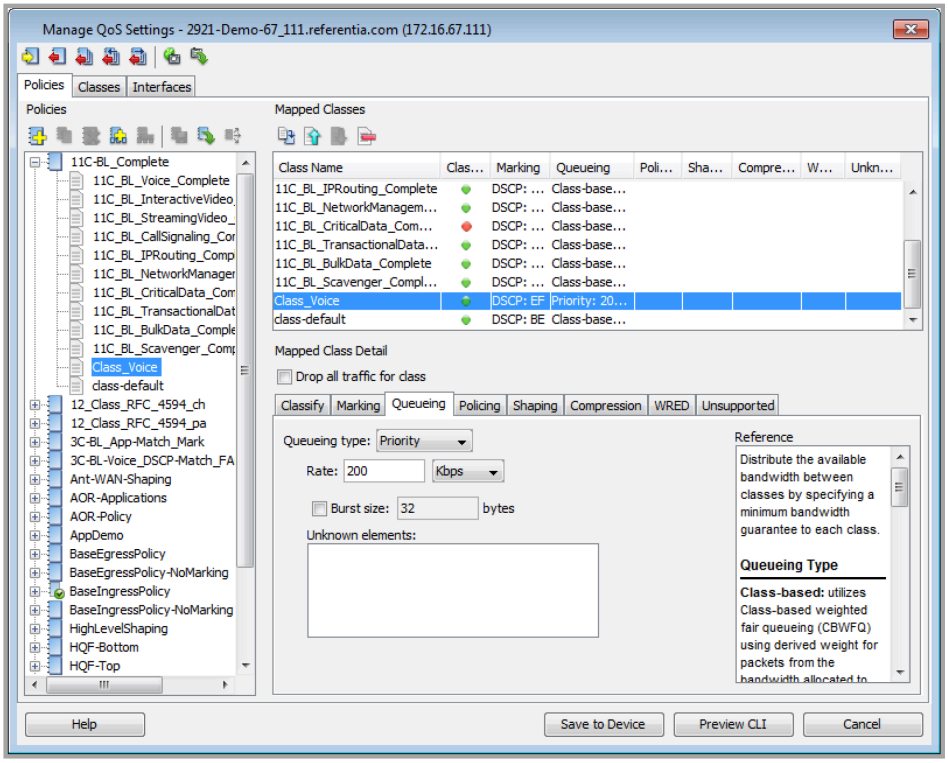
4. Create a policy based on the Cisco 11-class model using the template wizard. The class can use the VoIP class created in the previous step, and the various QoS settings can be configured.



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



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

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

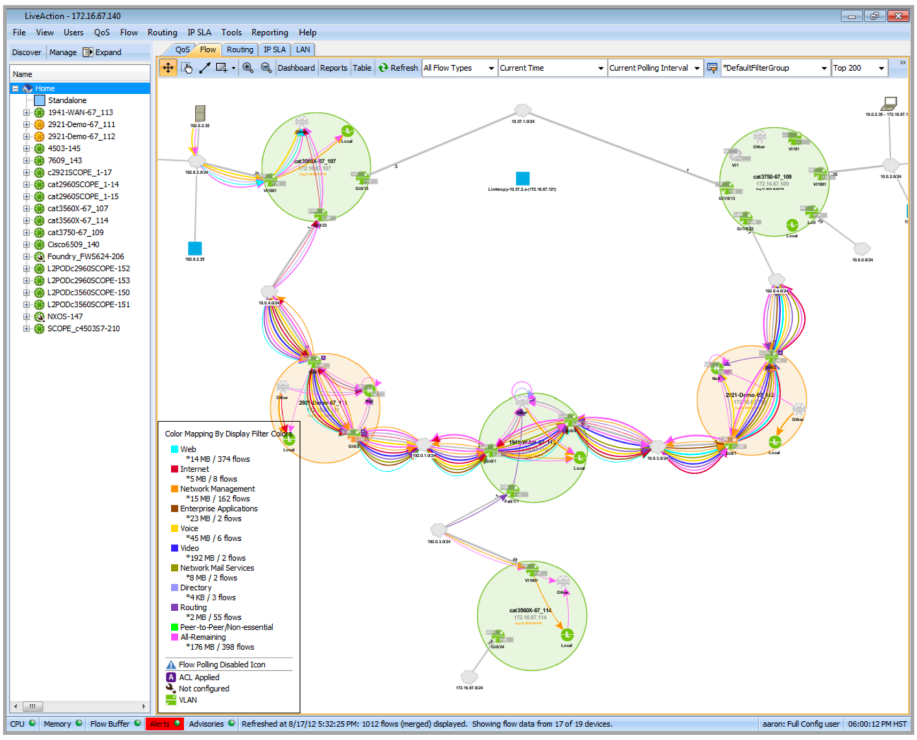
The LiveNX Flow technology module for the LiveNX software provides five different levels of visualizations of flow information. They are the Dashboard, System View, Device View, Interface View, and Reports. This section describes each of them in detail.

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.

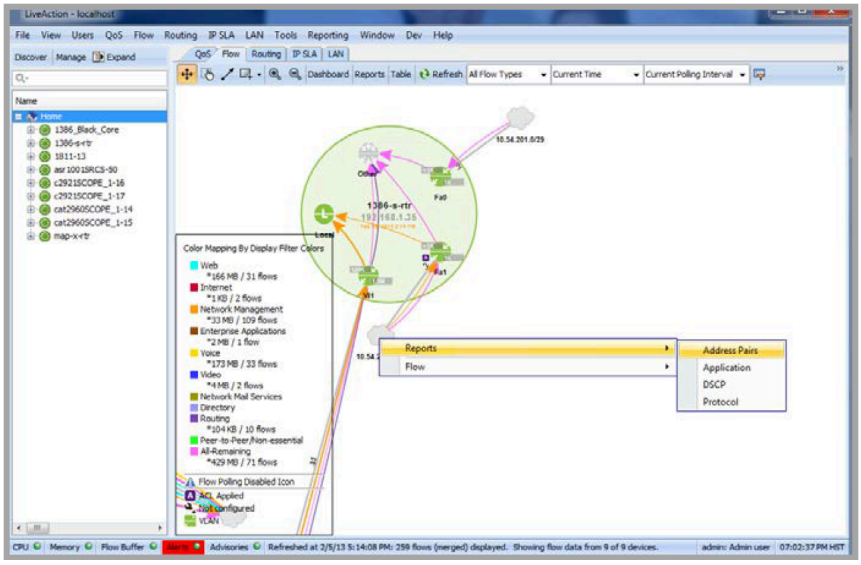
- A Color Mapping legend is overlaid on the topology to indicate flow coloring and the number of bytes and flows that match each of the color mapping. The legend can be toggled on and off by opening the View menu and selecting Show Legends.
- Flows can be drawn on the system topology as merged or unmerged. 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.



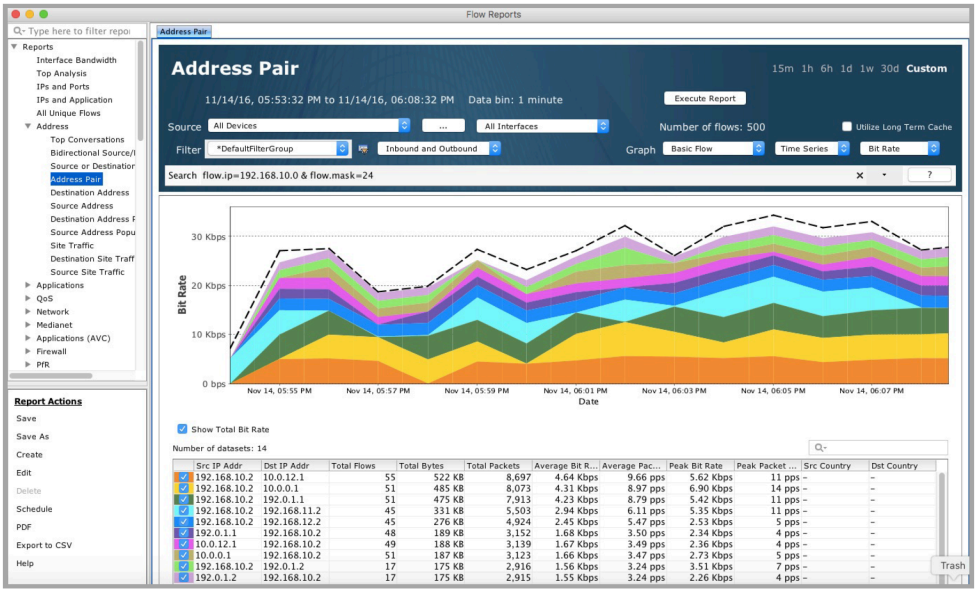
System View Drill Down to Flow Report

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.

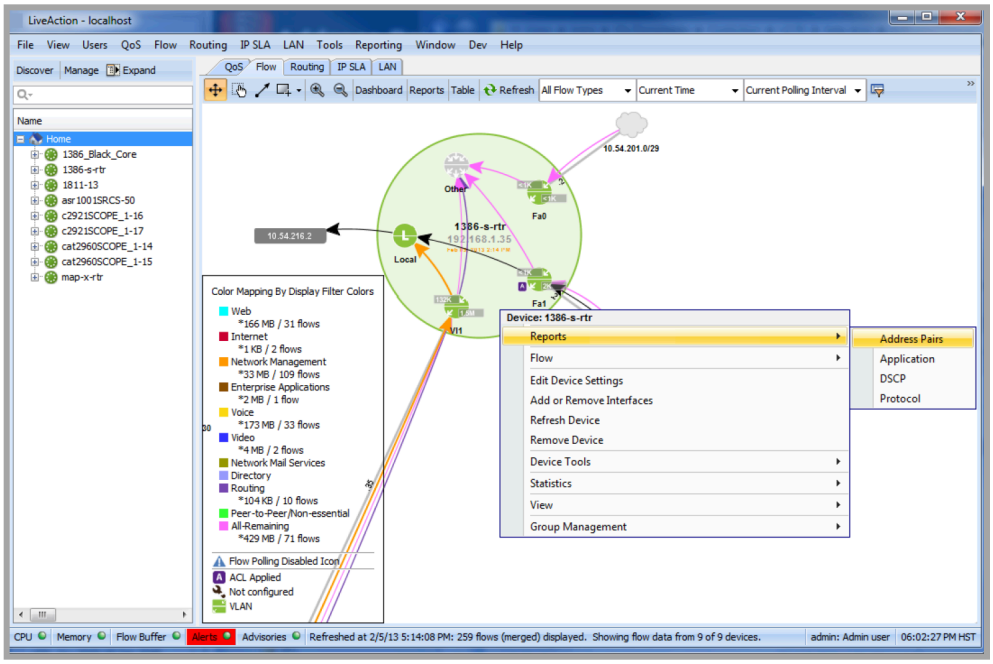
Subnet cloud drill down: Right click on the subnet cloud of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



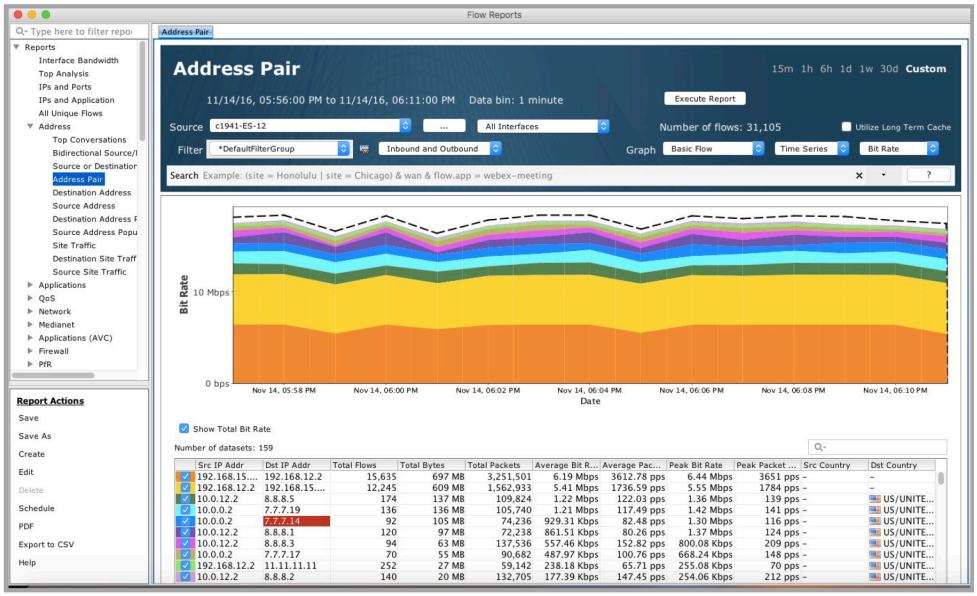
In this example, the desired Address Pair report lists the flows through the subnet cloud by Source IP and Destination IP address. A two-tier filter for IP source/destination address AND interface type is automatically selected to create this report. The flow data is aggregated from the nearest connected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



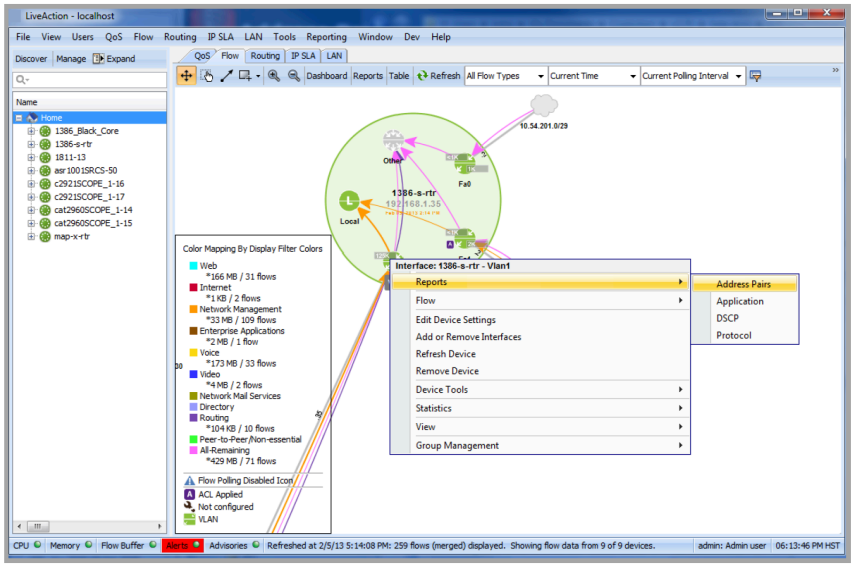
Device drill down: Right click on the device of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



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.

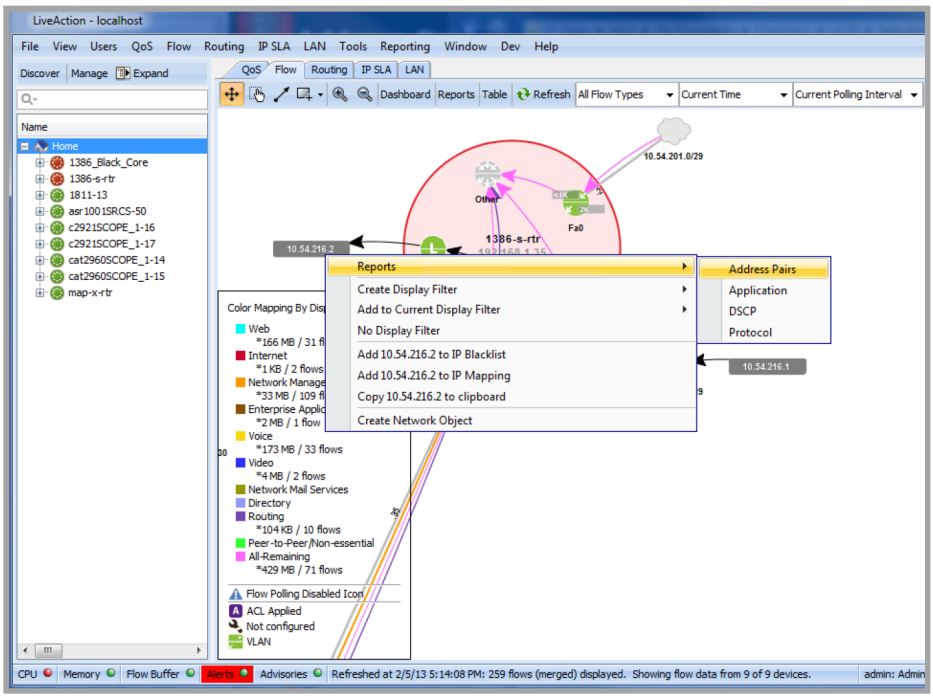


Interface drill down: Right click on the interface of interest and select one of the four reports: Address Pairs, Application, DSCP or Protocol.



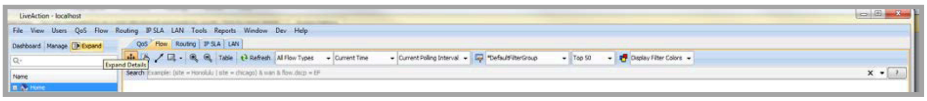
In this example, the desired Address Pair report lists the flows through the selected device and the selected interface by source and destination address pairs. The desired device and interface are automatically selected to create this report.

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



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.

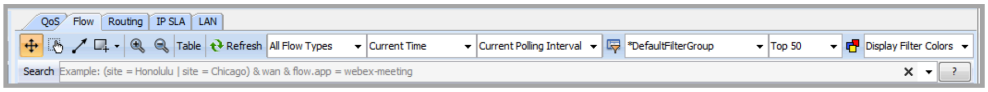
Searchable system entities include device, interface, site, tag and WAN parameters. Searchable flow entities include the IP address, DSCP, port, protocol, and application. CIDR notation can be used on the IPaddress, for example, “flow.ip=10.0.0.0/8.” Wildcards can be used on the IP address, for example, “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.

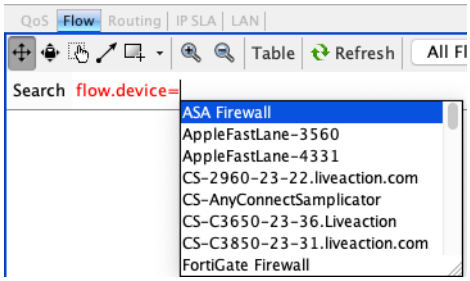
(site = Honolulu | site = Chicago) & wan & flow.app = WebEx-meeting

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 ‘( )’.

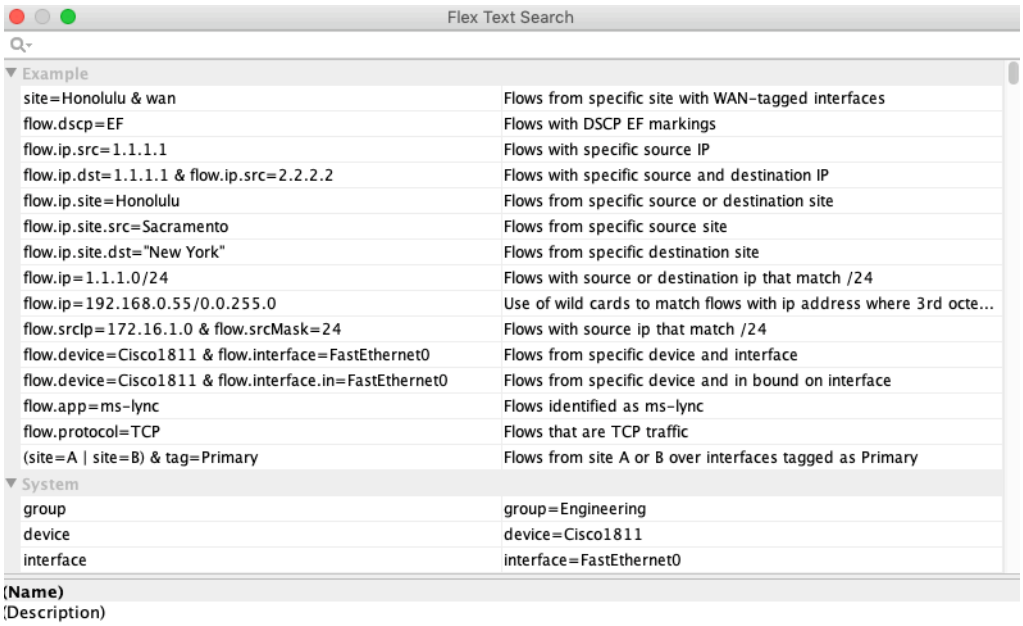
The Search editor provides tooltips to assist in creating the search expressions. Click on the desired entity to add it to the expression. NBAR uses dynamic lists based on the capability of the device.



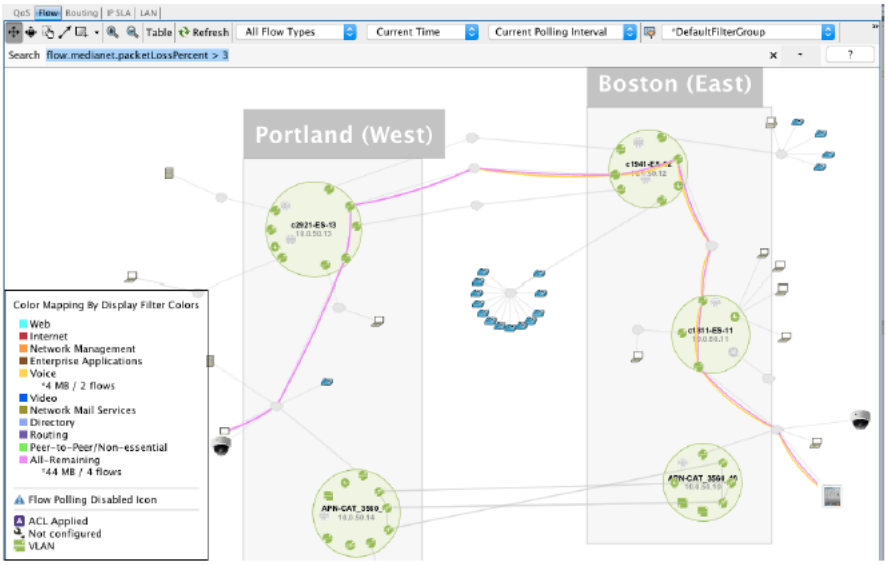
Filtering can be done through the main toolbar dropdowns as well as the Flow Display Filter combo box. Filtering is first done via the main toolbar dropdowns, the Flow Display Filter combo-box and lastly, the Search field.

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.



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

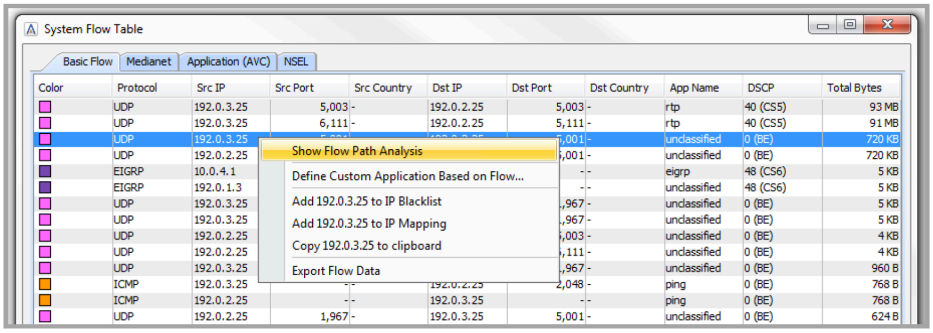
given time range per device. Packet Loss %, Interarrival Jitter Mean, and Lost Event Count values are the max of all the records that were merged based off the tuples.

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.



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

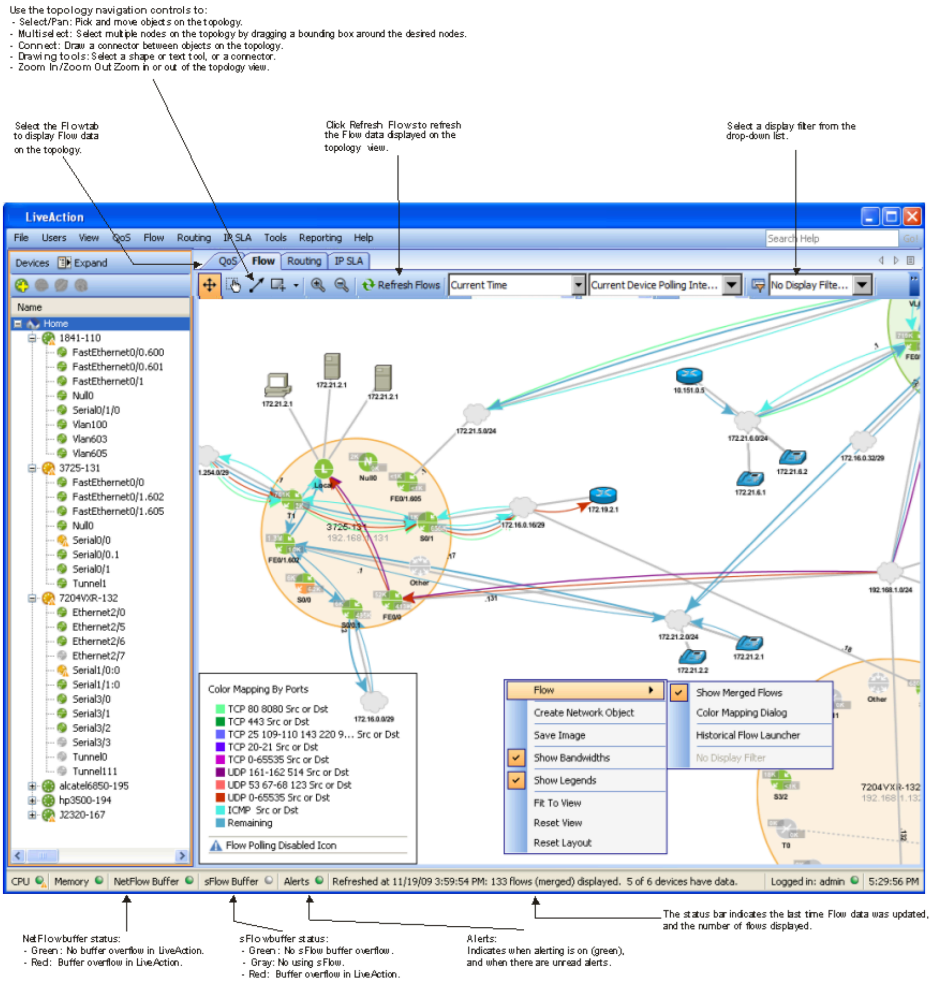
- Show Flow or Medianet Flow Path Analysis – displays an end-to-end analysis of the flow on a per-hop basis in the Basic Flow tab. Displays and end-to-end analysis of the Medianet flow on a per-hop basis in the Medianet flow tab.
- Define Custom Application Based on Flow – allows you to label a flow 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.



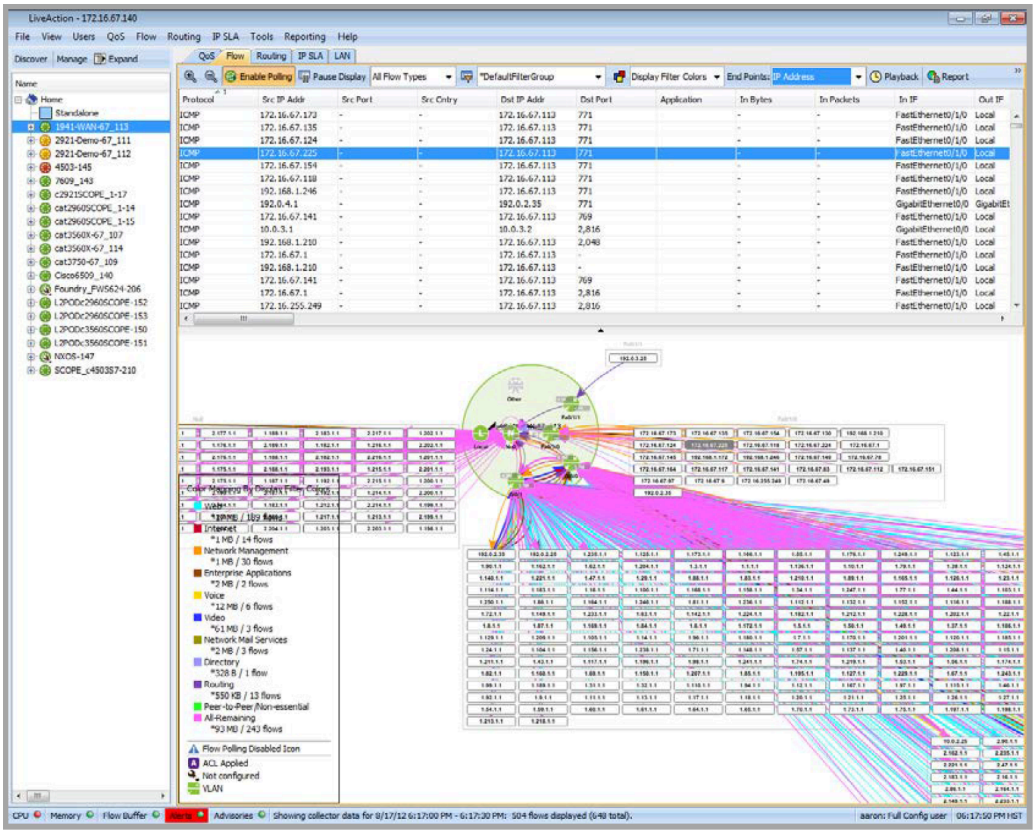
Device View

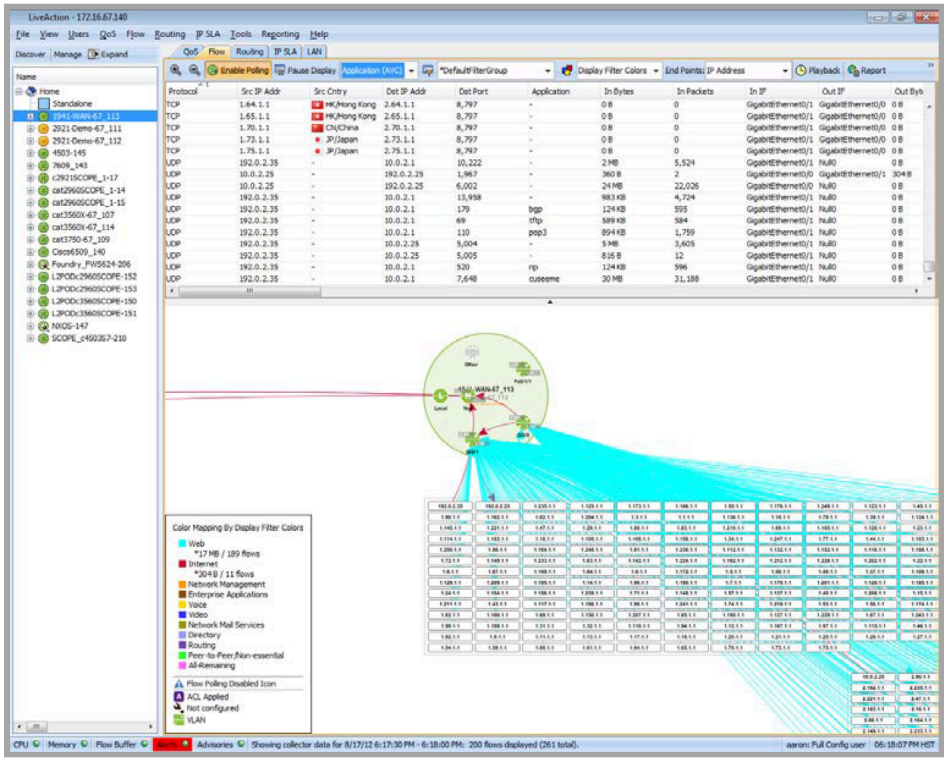
The device flow view provides a topology and table view of the traffic flowing through the device. The device view automatically refreshes the flows displayed in the table and topology based on the configured polling rate. The controls of the device flow visualization are located on the tool bar of the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

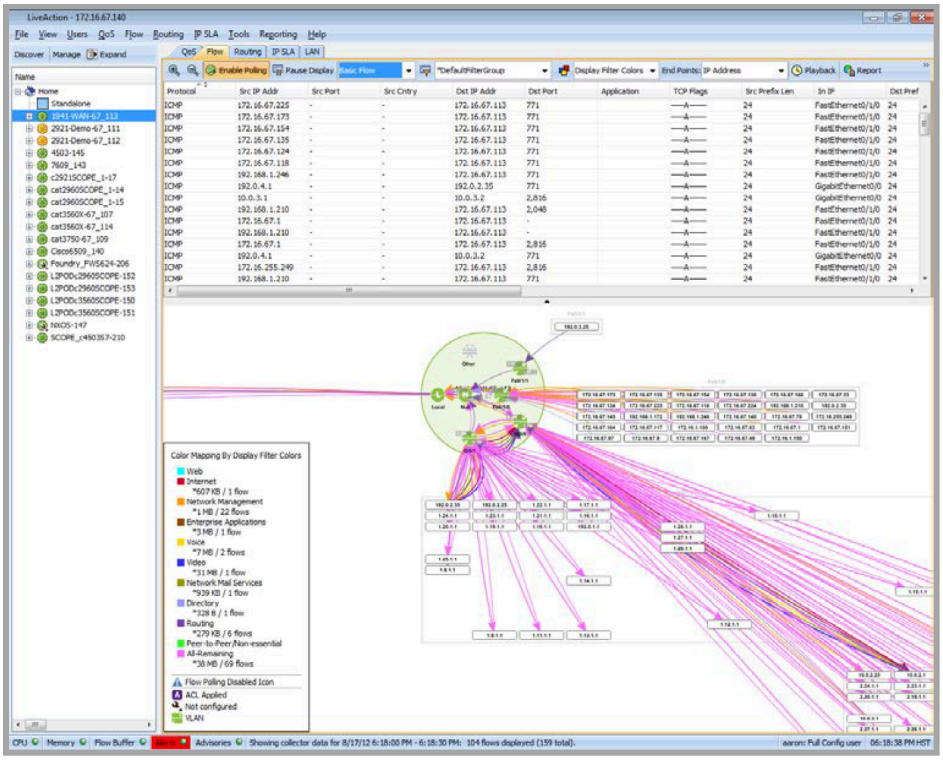
- Enable Polling (button): enables and disable the collection of flow data from the device.
- Pause Display (button): pauses the automated refresh on the current interval. While the device view is paused you may change the various selectors to change what is visualized for the current interval.
- Selectors 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.

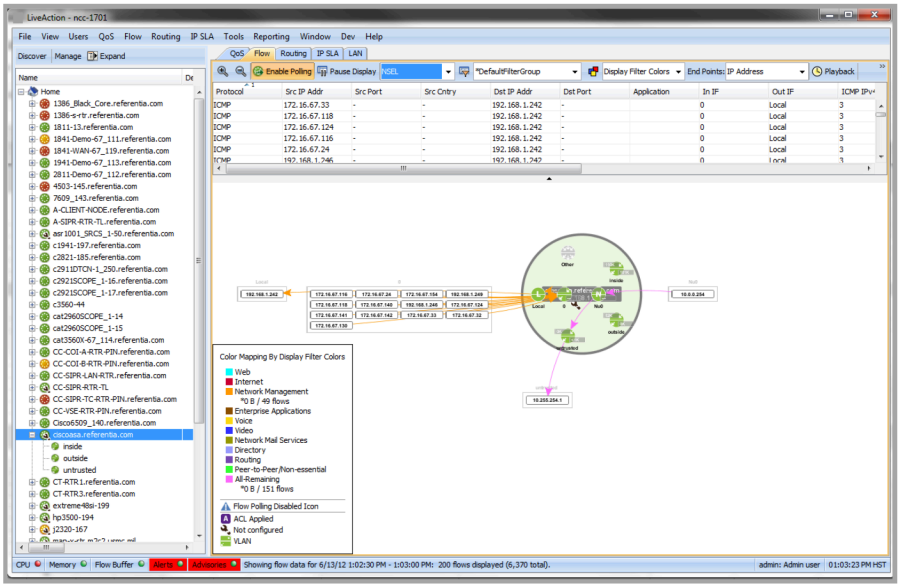
- Filter Selector: provides the ability to filter the flows retrieved during the refresh.
- Color Mapping Selector: provides the ability to color match the flows retrieved during the refresh by a certain algorithm.
- End Point Selector provides the ability to change how the flows are drawn on the topology.
- 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.

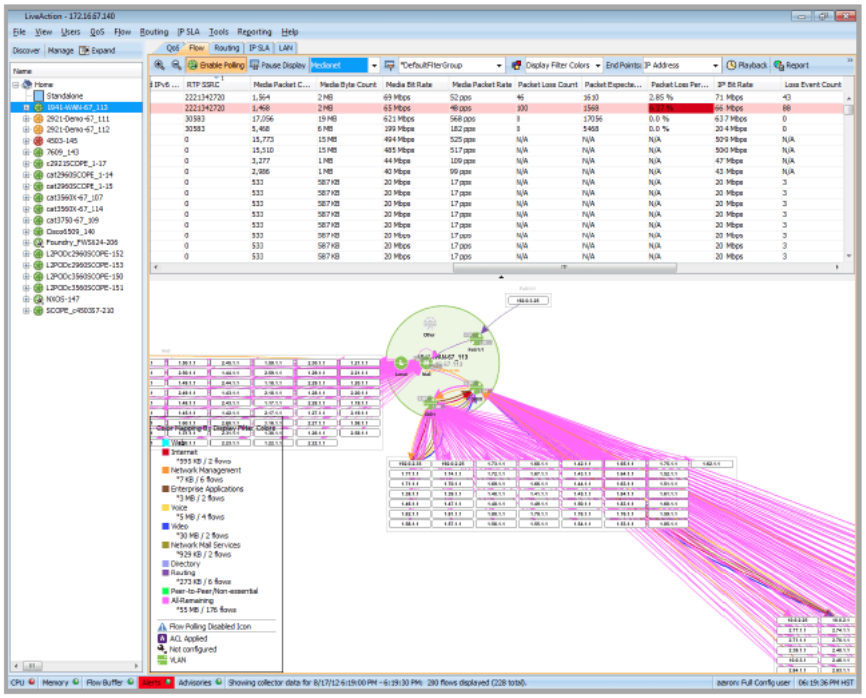








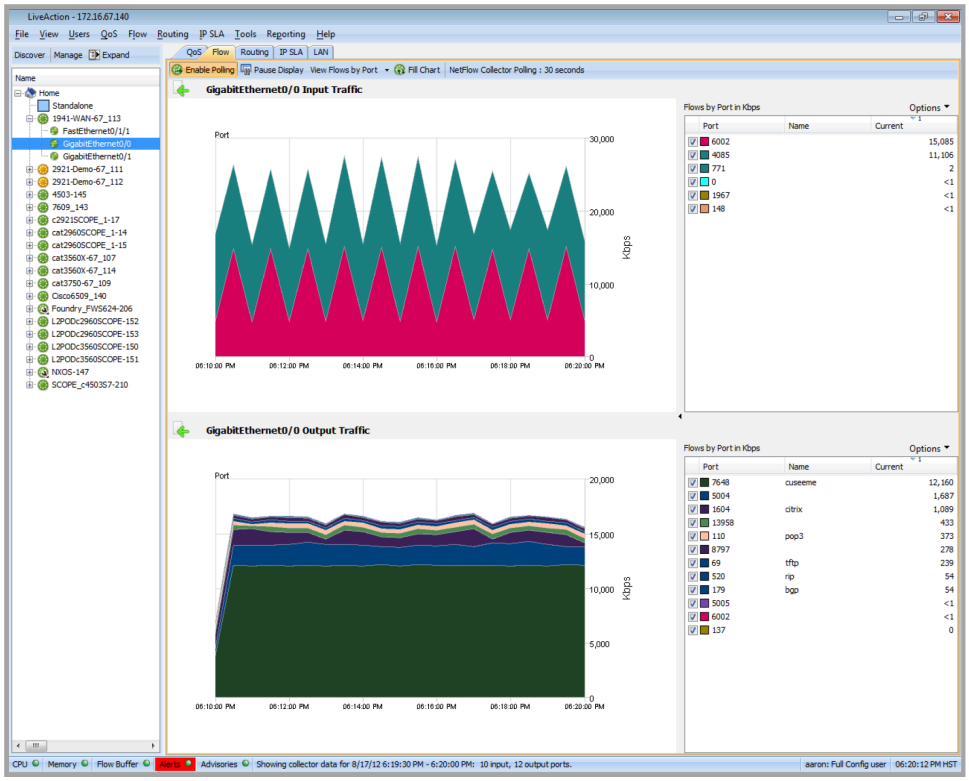
The Image Below shows a device-level view with Medianet flows highlighted in light red. This indicates that the particular Medianet flow is under alert. Scroll horizontally along the table until there is a dark red cell, indicating the particular attribute that exceeded the alert threshold. For details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

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

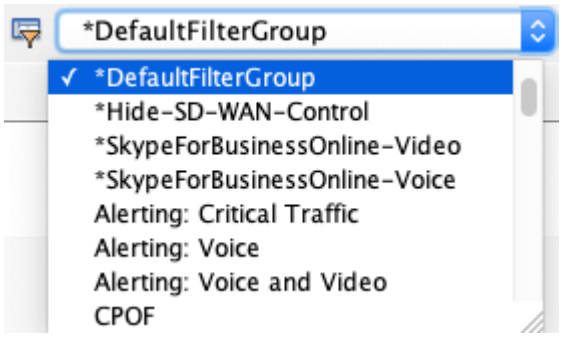
LiveNX categorizes and groups Flows into different Flow Technology Types when processing the data. This grouping separates Basic Flow, Medianet, AVC, NSEL, PfR and Unknown from each other, so that the appropriate data can be aggregated together. When appropriate, a selector is provided to allow the specification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

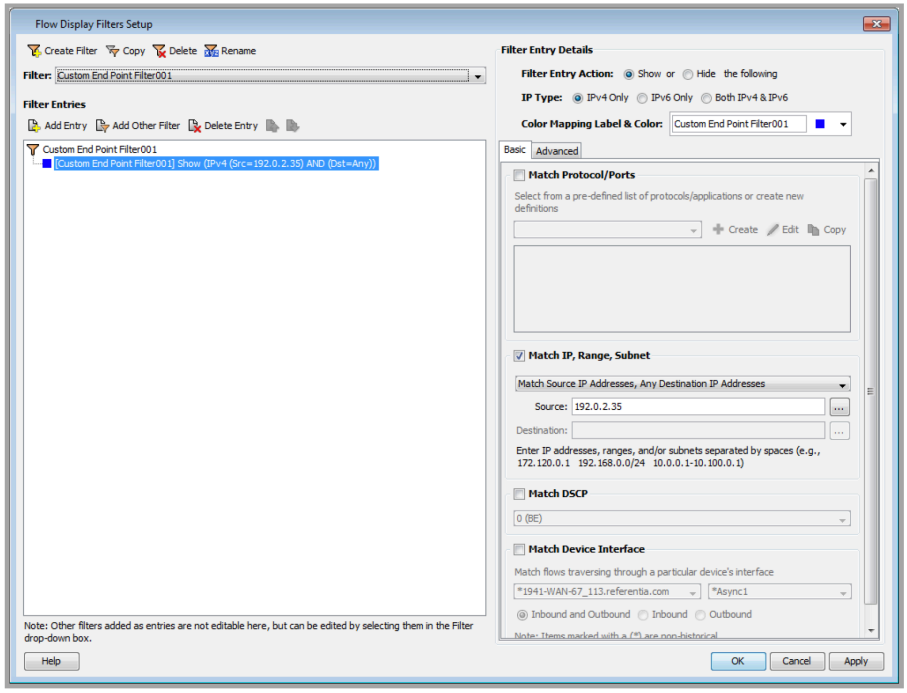
Flow Filters

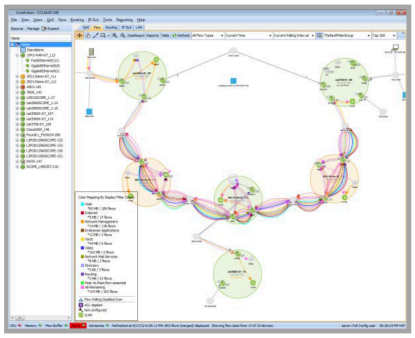
Filtering capabilities are provided at both the system- and router-level views, and provide similar functionality. When there are many flows traversing the network, the Flow graphs can become overwhelming. The filtering capabilities allow the user to show only specific flows that match particular criteria.



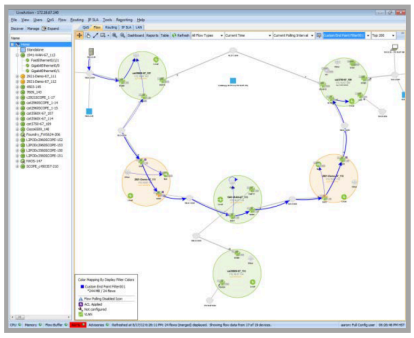
By default, LiveNX includes several pre-defined Flow filters. The Flow filter option also allows the creation and editing of user-defined filters. In the example below, the Custom End Point Filter will filter the display of Flow data, limiting the display to a specific device, interface, interface direction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

Custom End Point Filter 001:





Without Filtering



With Filtering

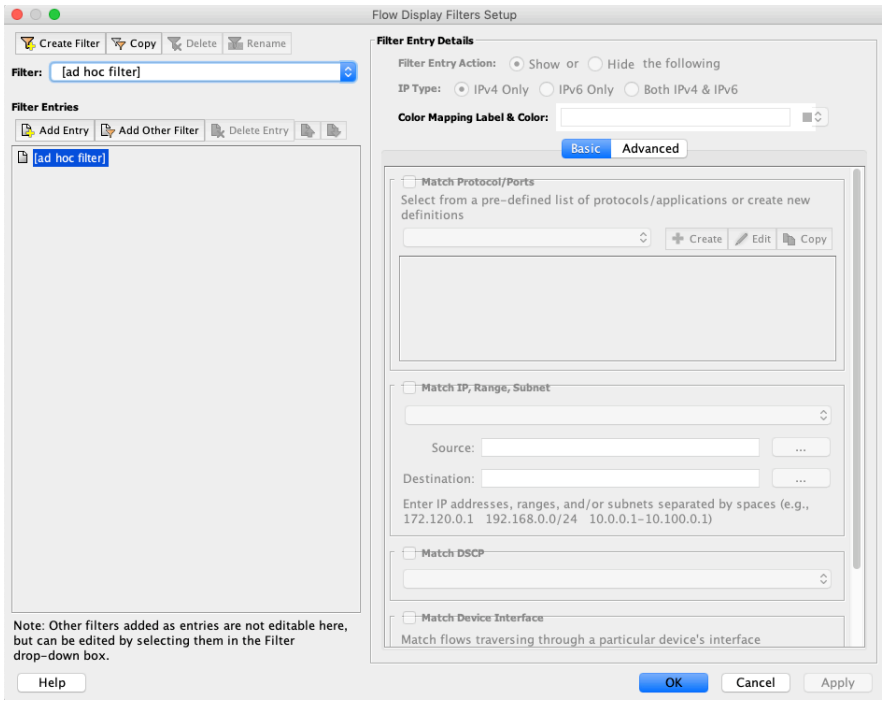
Flow filters can be set up at both the system- and device-level views, and are independent of each other. Filtering can minimize the number of flows displayed in system- and device-level views; extraneous flows can make it difficult to find relevant data within the view. Each piece of flow data is comprised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



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
Copy	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.

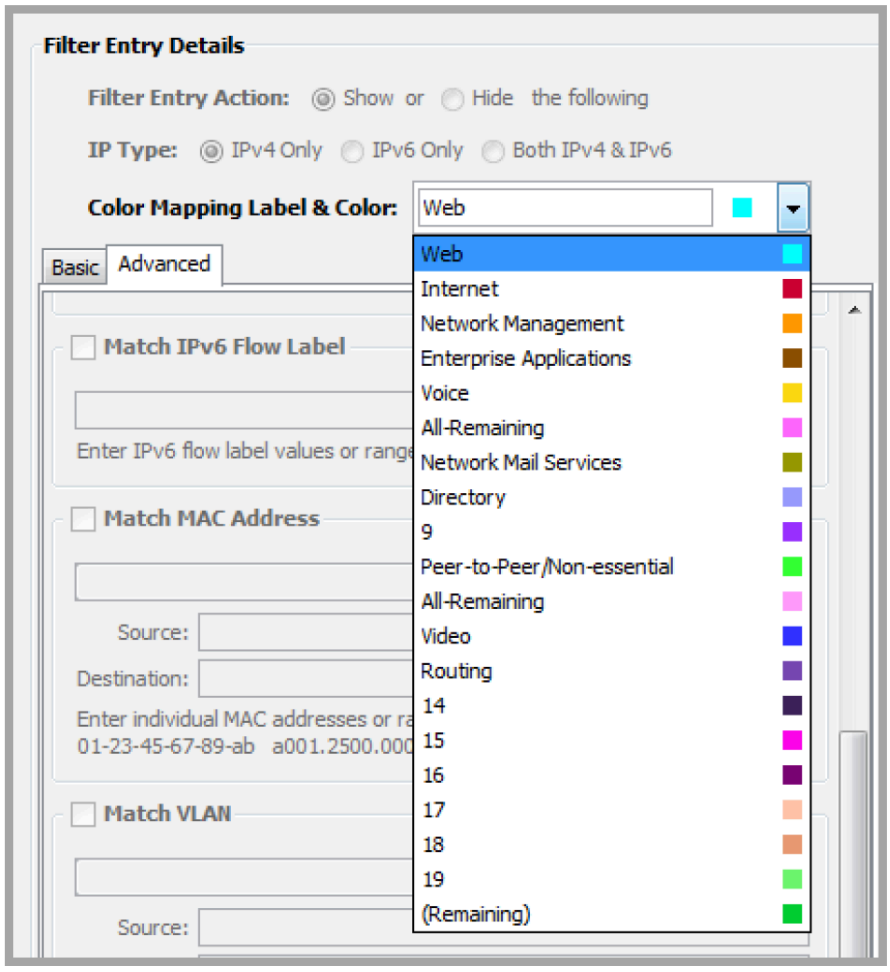
IP Type

Show	Indicates a positive filter entry. If a flow *matches* 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 *does not* 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

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
Copy	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.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.

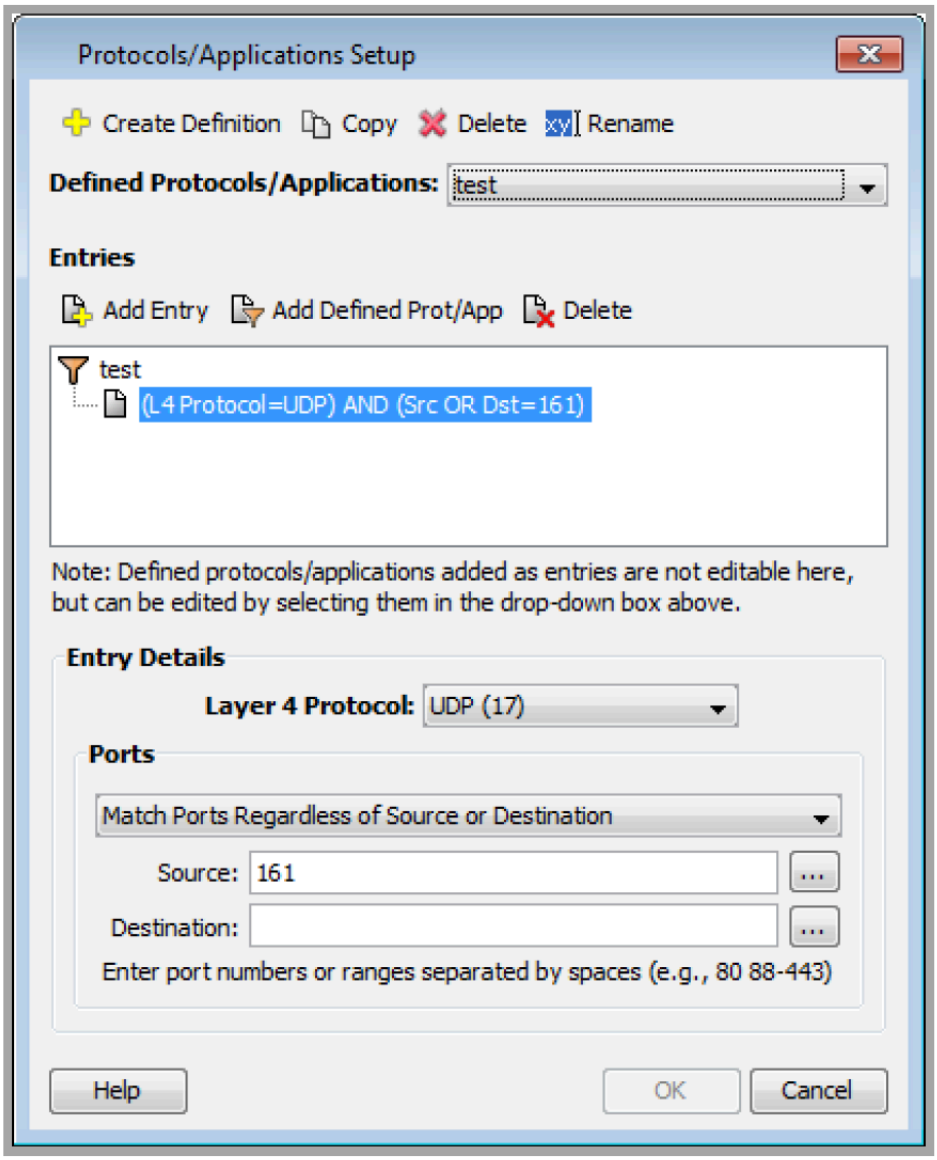
Match VLAN

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.



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
Copy	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.

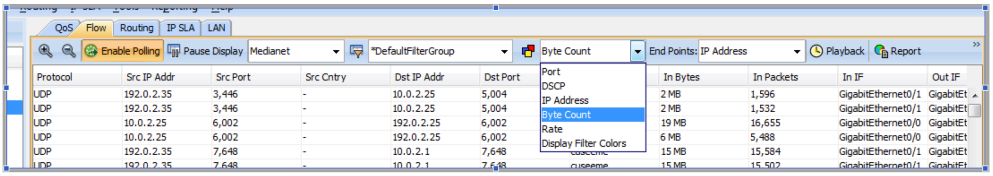
Flow Color Mapping

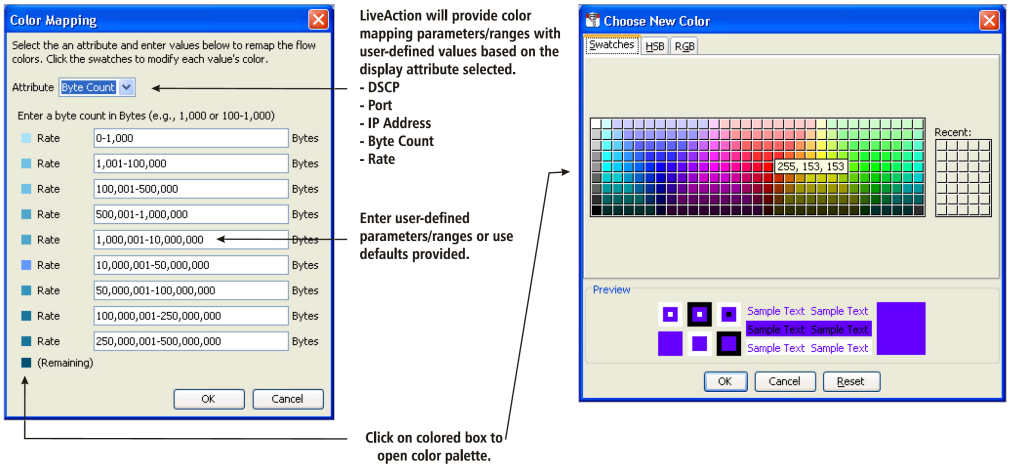
The Flow Color Mapping feature allows the assignment of colors to Flow connectors to easily view traffic characteristics at a glance. The Flow Color Mapping options are:

- 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





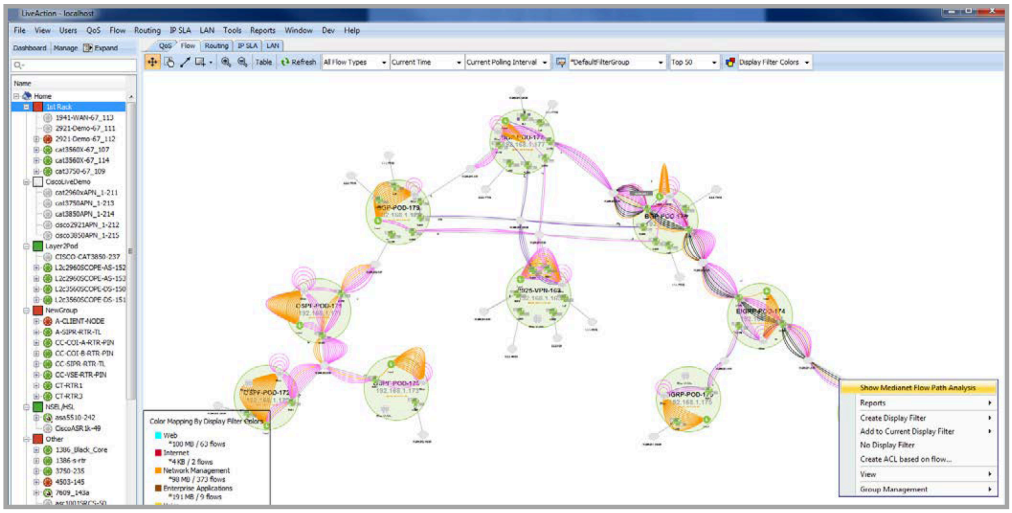
Flow Path Analysis

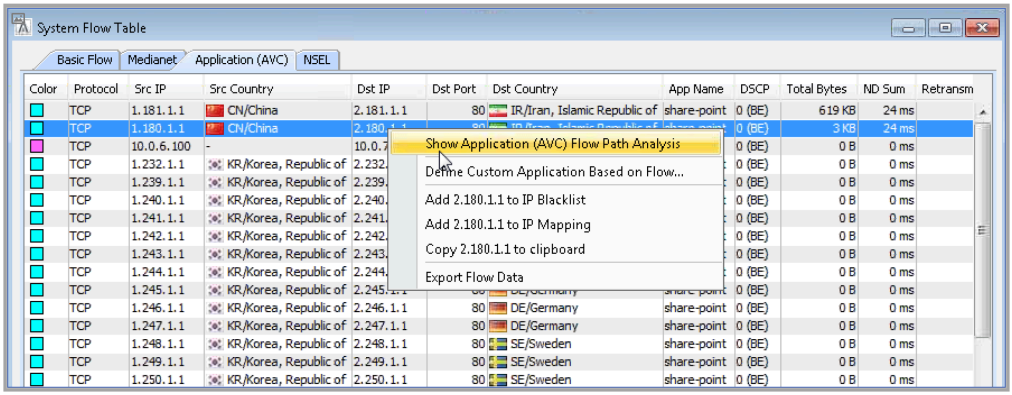
LiveNX provides detailed end-to-end traffic performance using standard Flexible NetFlow packets, general MIB information and the LiveNX alerts. The Flow Path Analysis, Medianet Flow Path Analysis

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.





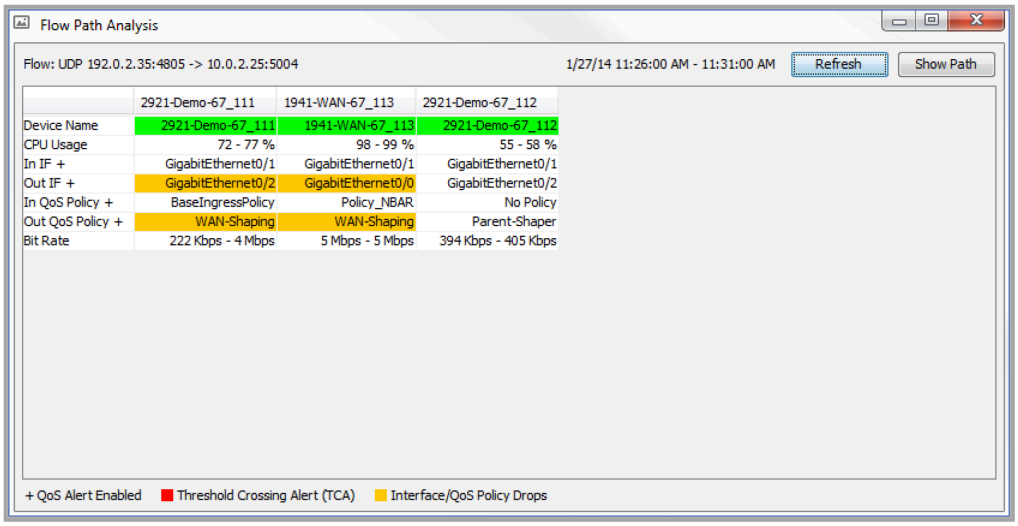
Evaluate table results

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.

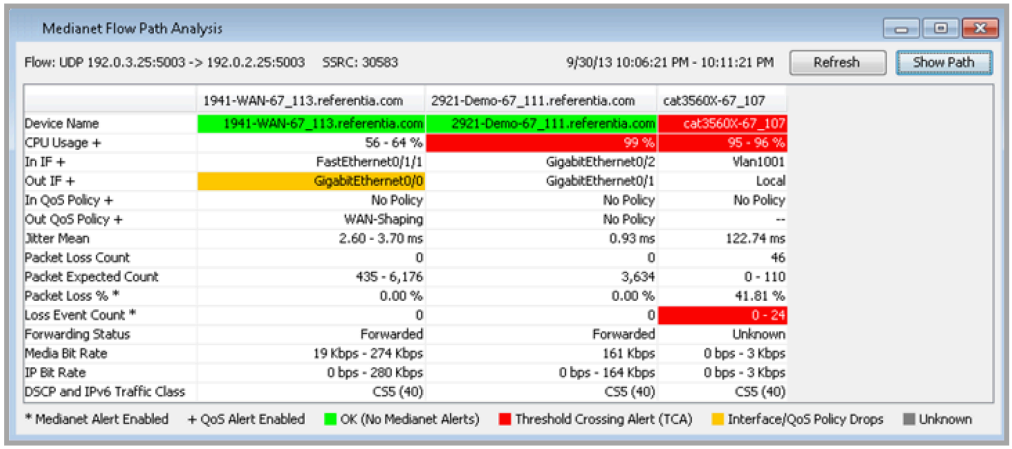
The header information above the table entries describes the flow under analysis listed in order: protocol, source IP address, source port, destination IP address, destination port and SSRC value. The date and time range corresponds to the range of the query period (currently fixed at 5 minutes). Click 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.

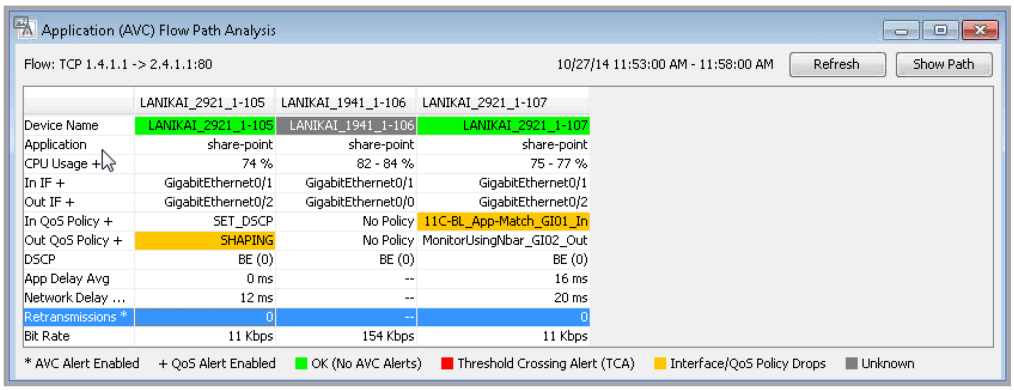


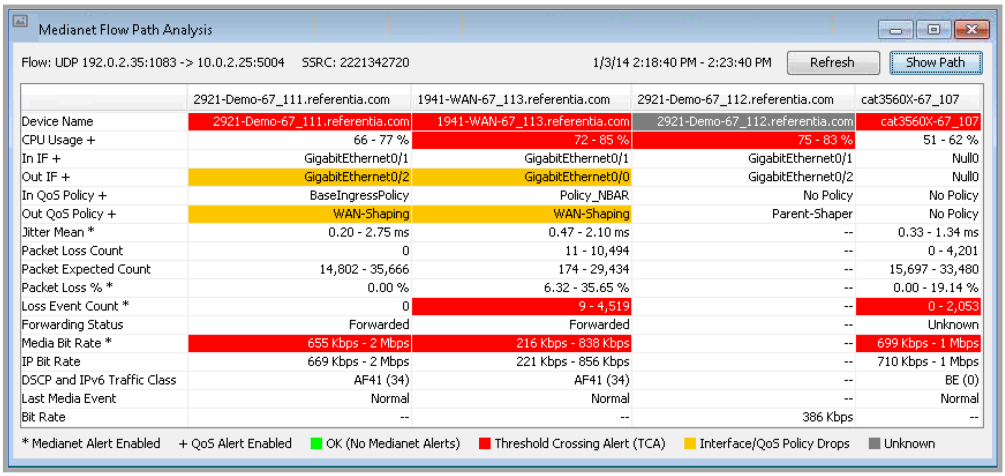
	2921-Demo-67_111	1941-WAN-67_113	2921-Demo-67_112
Device Name	2921-Demo-67_111	1941-WAN-67_113	2921-Demo-67_112
CPU Usage	72 - 77 %	98 - 99 %	55 - 58 %
In IF +	GigabitEthernet0/1	GigabitEthernet0/1	GigabitEthernet0/1
Out IF +	GigabitEthernet0/2	GigabitEthernet0/0	GigabitEthernet0/2
In QoS Policy +	BaseIngressPolicy	Policy_NBAR	No Policy
Out QoS Policy +	WAN-Shaping	WAN-Shaping	Parent-Shaper
Bit Rate	222 Kbps - 4 Mbps	5 Mbps - 5 Mbps	394 Kbps - 405 Kbps



	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.


Application (AVC) Flow Path Analysis
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
Application
CPU Usage +
In IF +
Out IF +
In QoS Policy +
Out QoS Policy +
DSCP
App Delay Avg
Network Delay ...
Retransmissions *
Bit Rate
share-point
74 %
82 - 84 %
75 - 77 %
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/0
SET_DSCP
No Policy
11C-BL_App-Match_GI01_In
SHAPING
MonitorUsingNbar_GI02_Out
BE (0)
0 ms
12 ms
16 ms
20 ms
11 Kbps
154 Kbps
* AVC Alert Enabled
+ QoS Alert Enabled
OK (No AVC Alerts)
Threshold Crossing Alert (TCA)
Interface/QoS Policy Drops
Unknown


Medianet Flow Path Analysis
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
CPU Usage +
In IF +
Out IF +
In QoS Policy +
Out QoS Policy +
Jitter Mean *
Packet Loss Count
Packet Expected Count
Packet Loss % *
Loss Event Count *
Forwarding Status
Media Bit Rate *
IP Bit Rate
DSCP and IPv6 Traffic Class
Last Media Event
Bit Rate
66 - 77 %
72 - 85 %
75 - 83 %
51 - 62 %
GigabitEthernet0/1
GigabitEthernet0/2
GigabitEthernet0/0
Null0
BaseIngressPolicy
Policy_NBAR
No Policy
WAN-Shaping
Parent-Shaper
0.20 - 2.75 ms
0.47 - 2.10 ms
0.33 - 1.34 ms
0
11 - 10,494
0 - 4,201
14,802 - 35,666
174 - 29,434
15,697 - 33,480
0.00 %
6.32 - 35.65 %
0.00 - 19.14 %
9 - 4,519
0 - 2,053
Forwarded
Unknown
655 Kbps - 2 Mbps
216 Kbps - 838 Kbps
699 Kbps - 1 Mbps
669 Kbps - 2 Mbps
221 Kbps - 856 Kbps
710 Kbps - 1 Mbps
AF41 (34)
Normal
386 Kbps
* Medianet Alert Enabled
+ QoS Alert Enabled
OK (No Medianet Alerts)
Threshold Crossing Alert (TCA)
Interface/QoS Policy Drops
Unknown

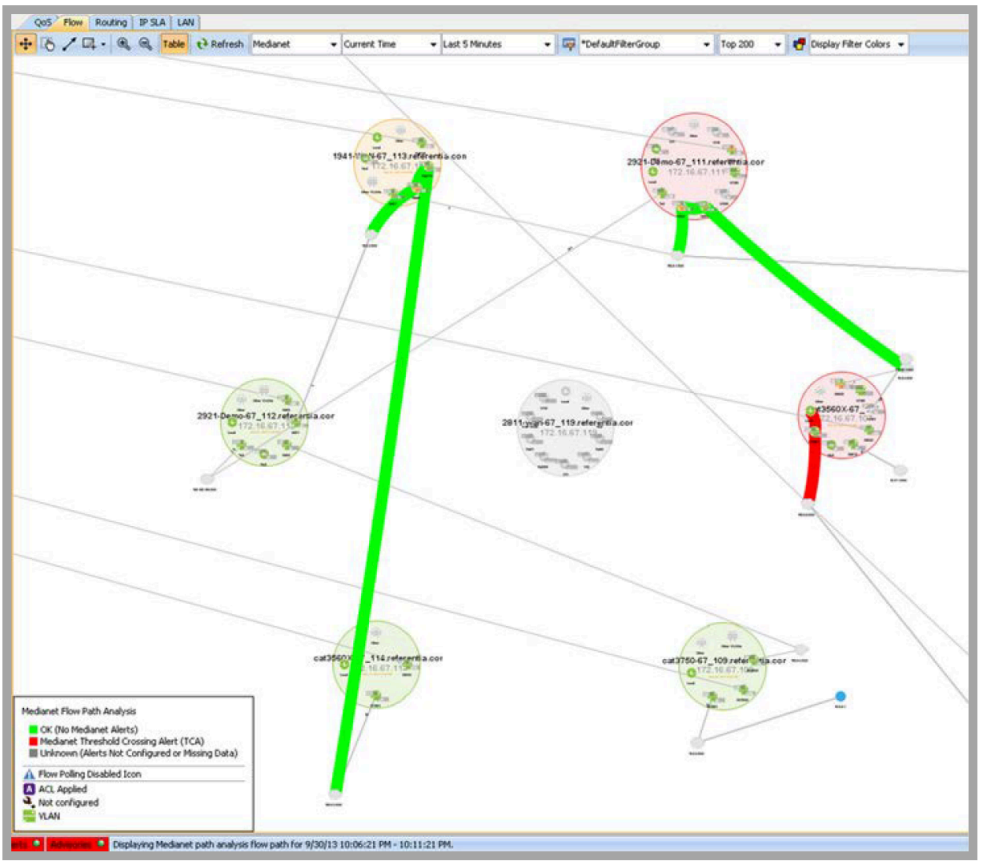
Attribute	Value	Color
Device Name	Device Name	**Note: Only Medianet alerts and thresholds are used to determine the device color.** Green: Medianet alerts enabled, none exceeded alert thresholds. Red: At least one Medianet alert exceeded threshold. Gray: No Medianet alerts enabled or missing data.
CPU 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.



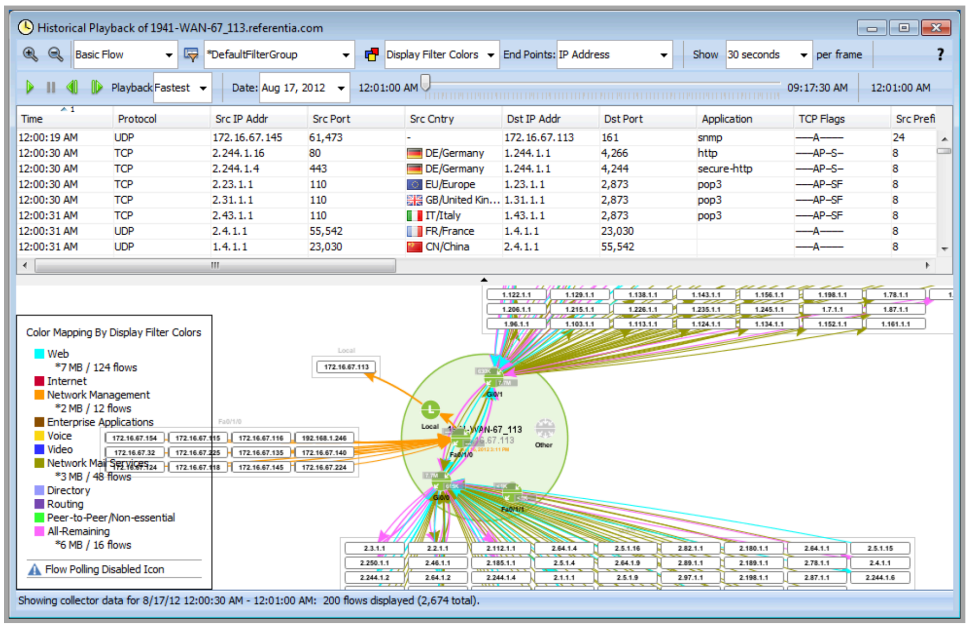
Historical Playback

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.

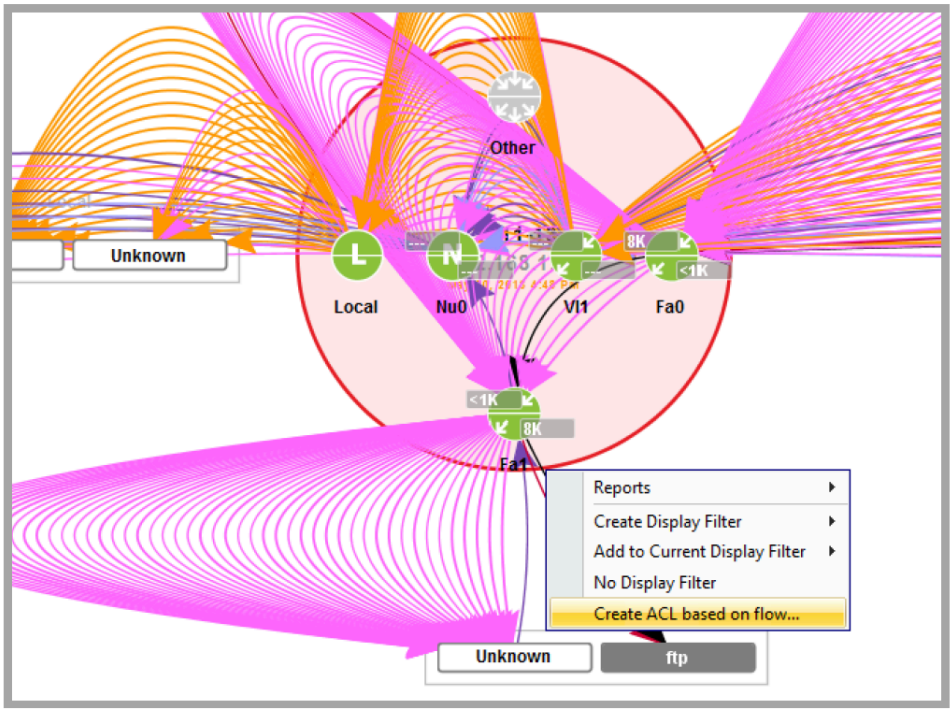
Note Historical Playback may cause flows to be dropped.

Below is an example of the Historical Playback display:

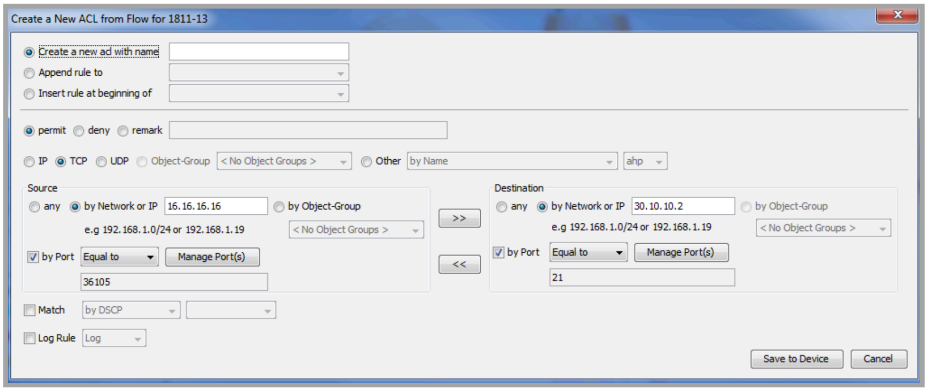


Create ACLs Based on Flows

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.



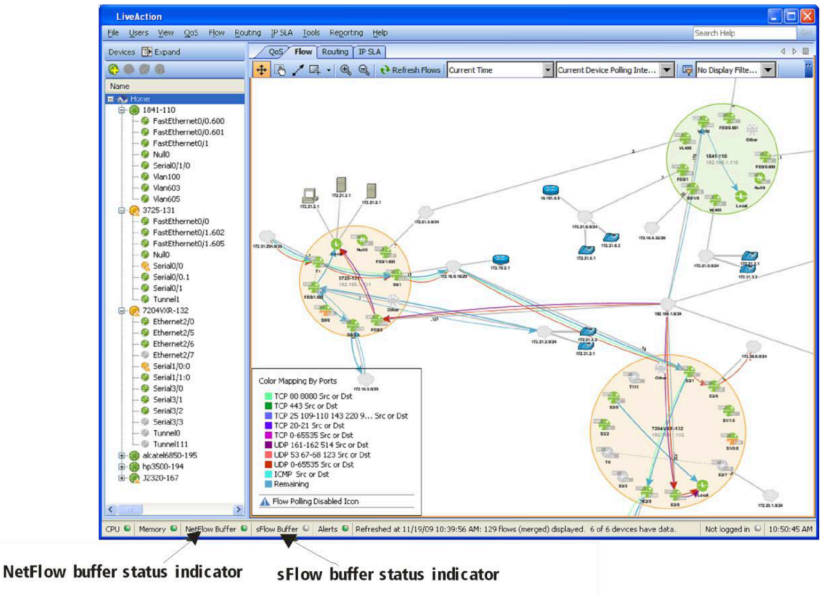
The resultant ACL Extended rule menu will appear with the relevant source IP, destination IP and port information already filled in.



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.



- 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.

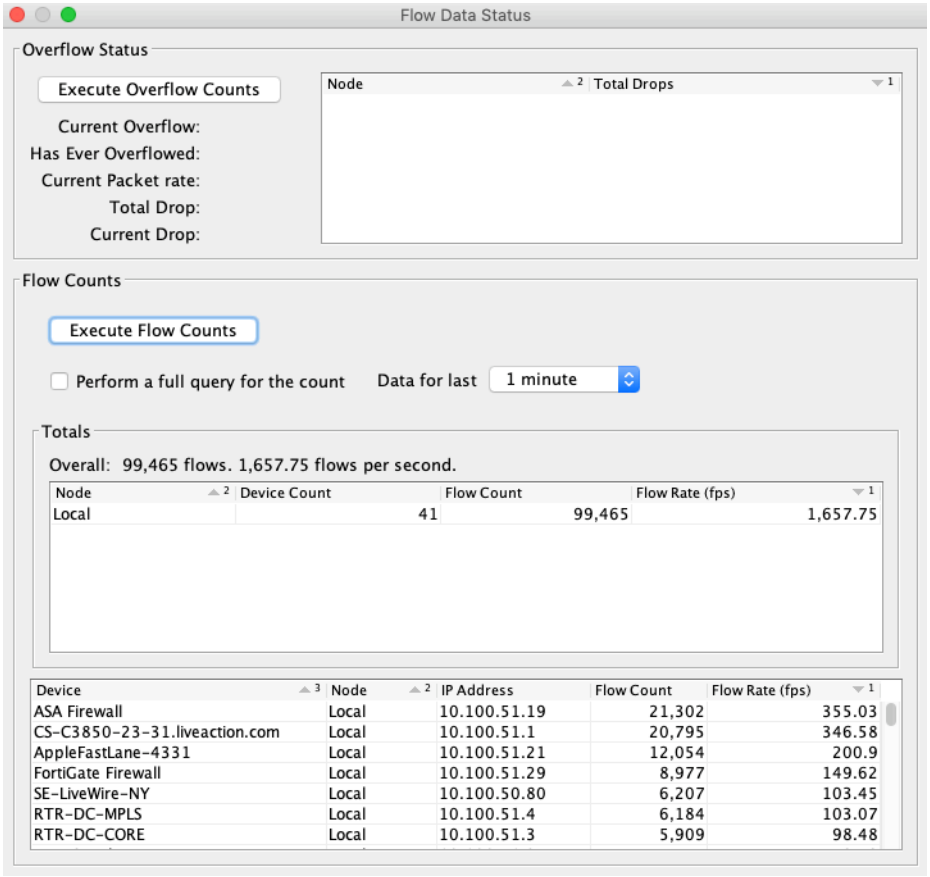
The limitation of the flow buffer is determined by the performance of the Server or Node on which LiveNX is installed.

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

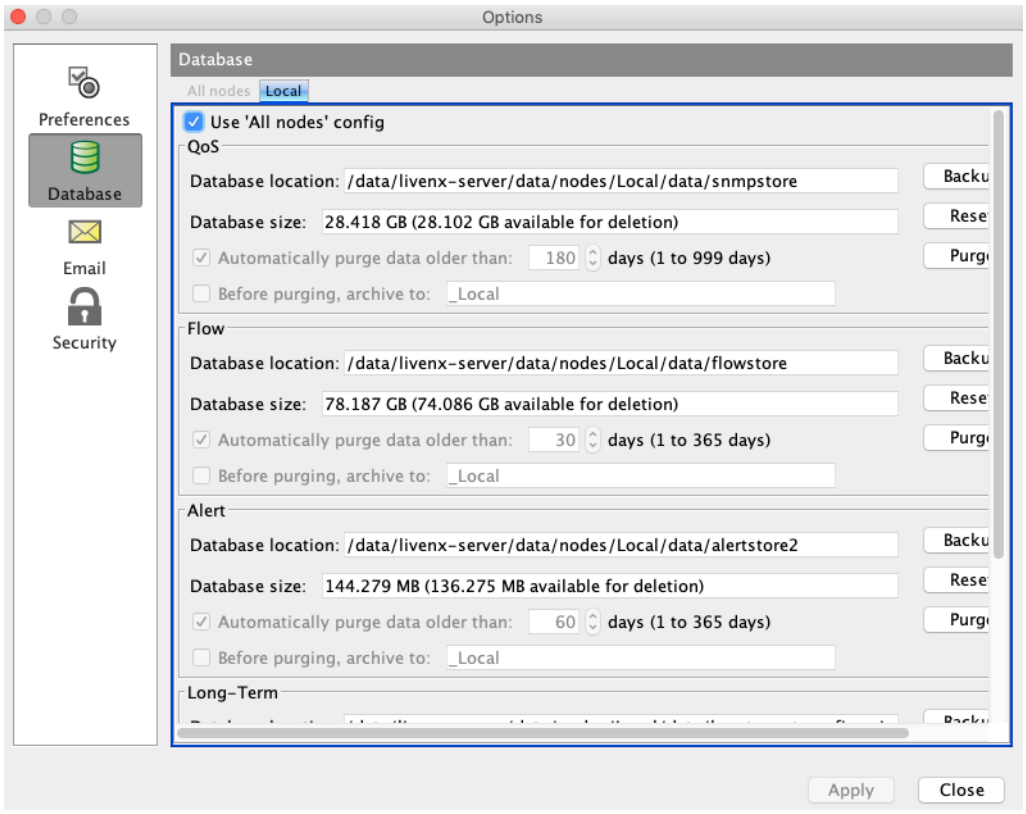
Click Execute Overflow Status to view overflow, packet rate, and drops.

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.



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.



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

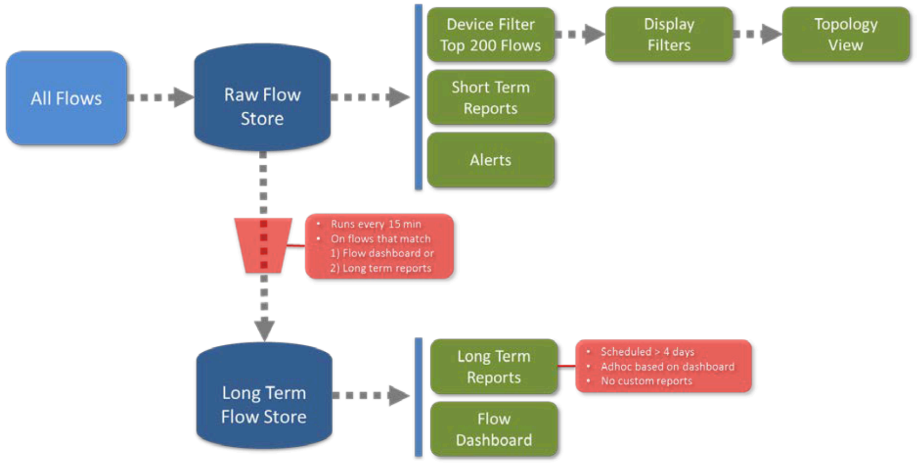
LiveNX NetFlow currently works with most Cisco routers and some Cisco switches.

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

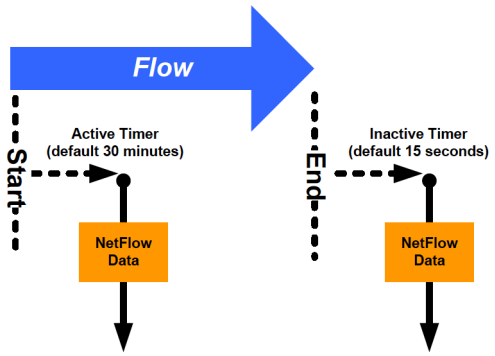
To make it easier to isolate and view specific flow information, LiveNX provides extensive filtering options that can be applied to both real-time and historical displays. Device filtering allows you to collect specific flow data from the devices and to reduce the amount of NetFlow information LiveNX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

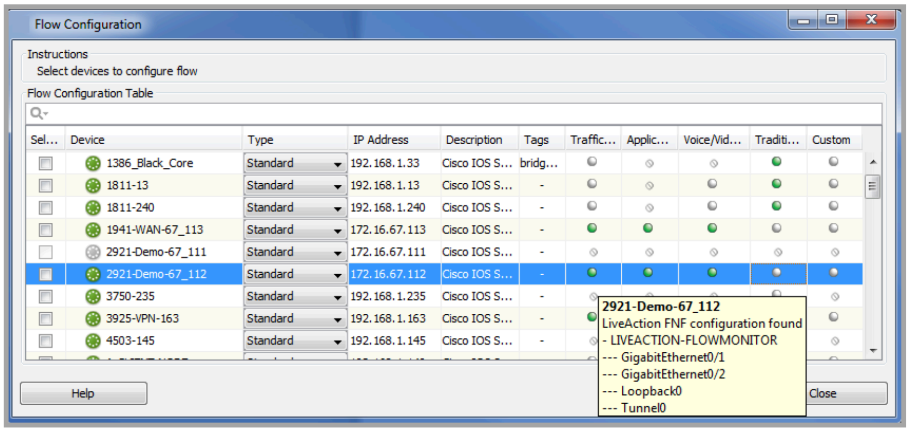
Platforms

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.



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.

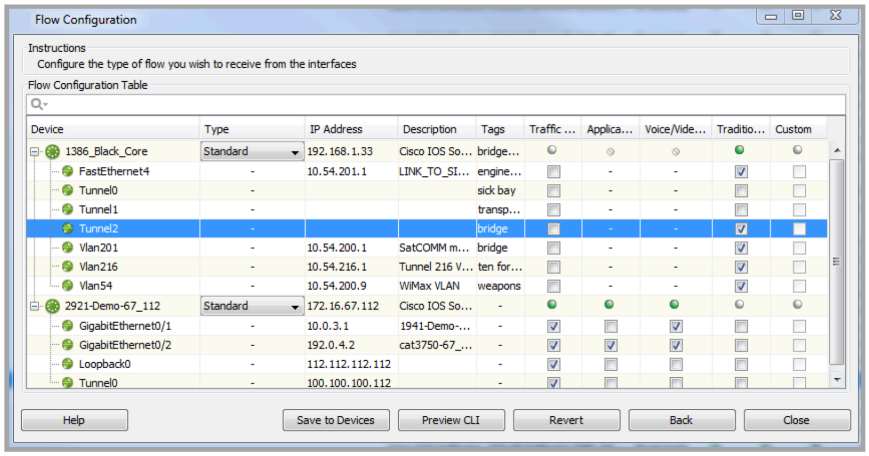
- A green LED indicates the flow technology that is configured on that device.
- A white LED indicates the flow technology that is supported on the device, but is not currently configured.
- The LED with the strikeout marking indicates a flow technology that is not supported on that device.

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.

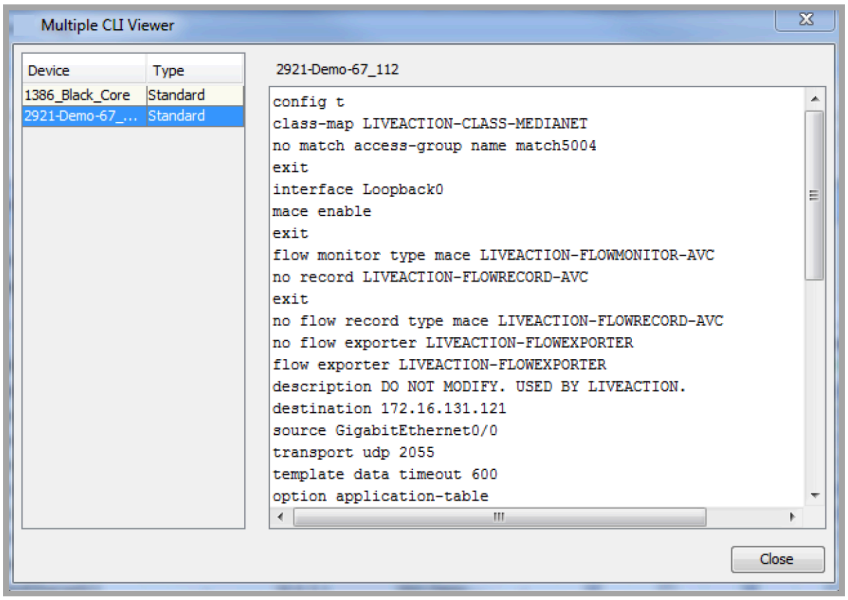
Type in an alphanumeric string next to the magnifying glass to filter the flow configuration table.

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.

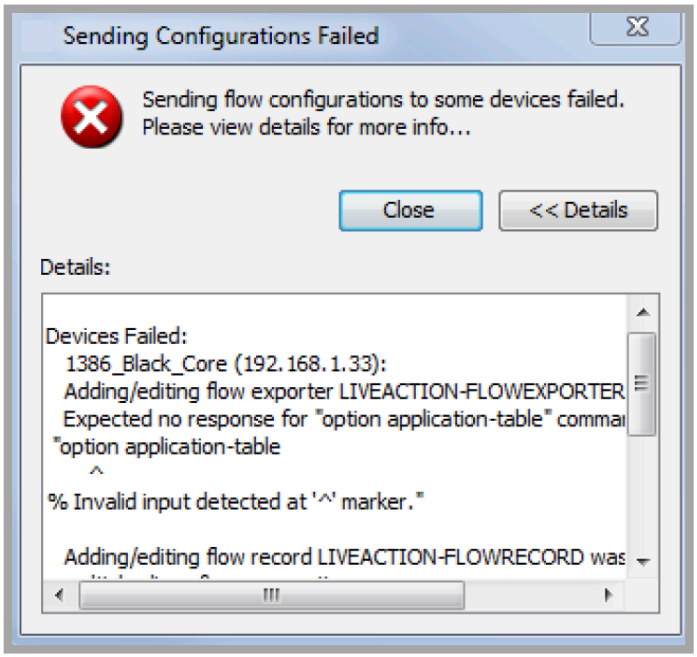


Click on a check box to toggle the various flow configuration options. A hyphen mark in a flow technology entry indicates a flow technology which is unsupported by that device. Once a new selection is made, the Save to Devices, Preview CLI and Revert buttons will be enabled.

- 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.



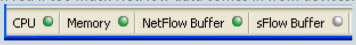
- Revert – click on the Revert button to return your flow configuration settings back to the initial state prior to any “Save to Devices” command.
- Back – click on the Back button to return to the device the only view of the flow configuration table.
- Close – close the flow configuration table.
- Save 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
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 NetFlow 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 "GigabitEthernet0/0."

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.properties.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	Identifier 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.

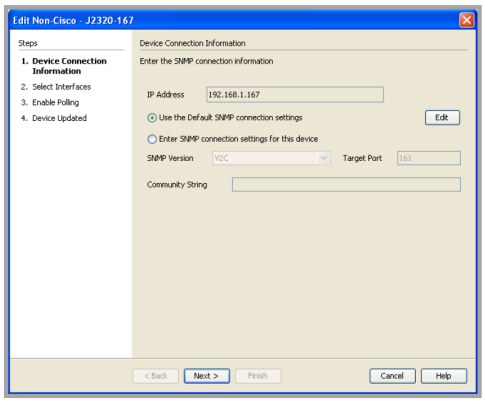
Field Type	IPv4 Field Usage	IPv6 Field Usage	LiveNX GUI Field Name	Description
IN_DST_MAC	S	S	In Dst MAC	Incoming destination MAC address.
IN_PERMANENT_BYTES	A	A	Bytes	Running byte counter for a permanent flow.
FORWARDING STATUS	S	S	N/A	Forwarding status of flow (Refer to the Cisco Technology White Paper, *NetFlow Version 9 Flow-Record Format*.).
app_id	S	S	NBAR App	NBAR application identifier.

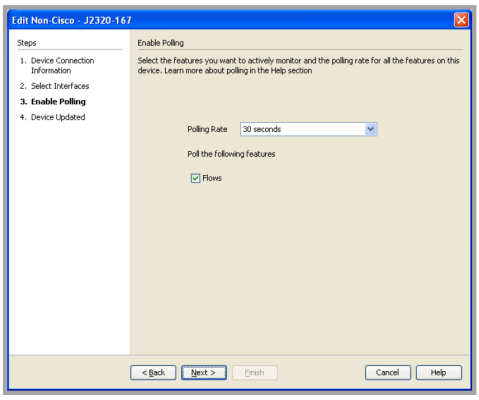
Non-Cisco Device Flow

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.





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

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

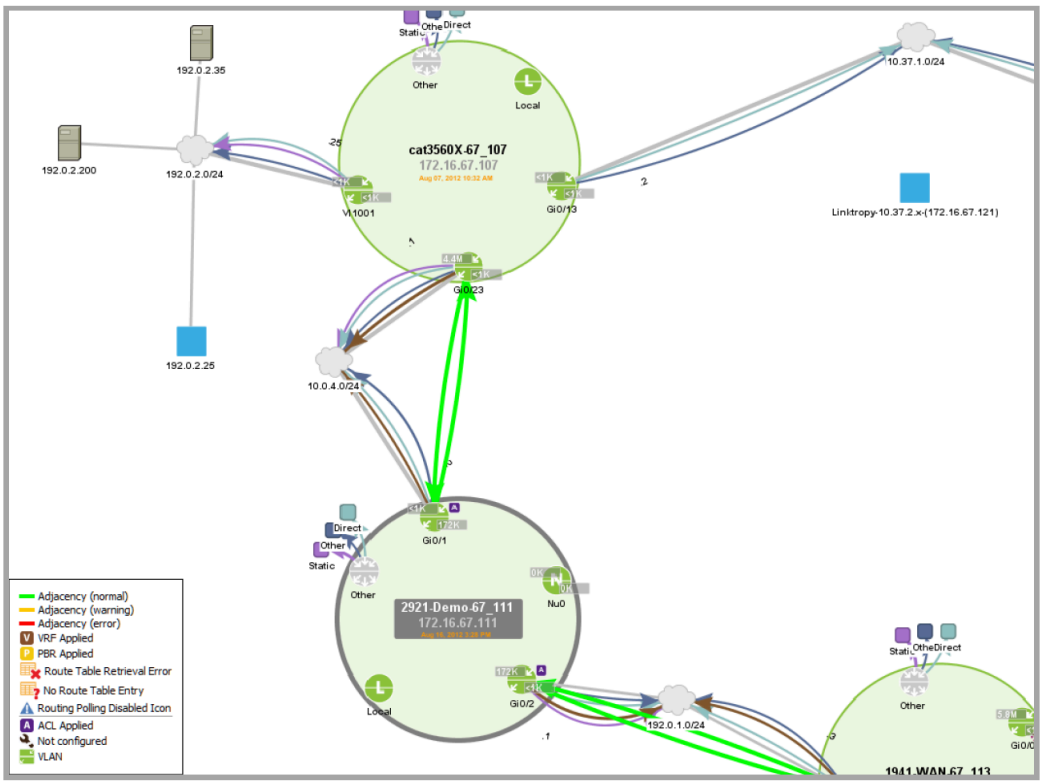
Troubleshooting

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.

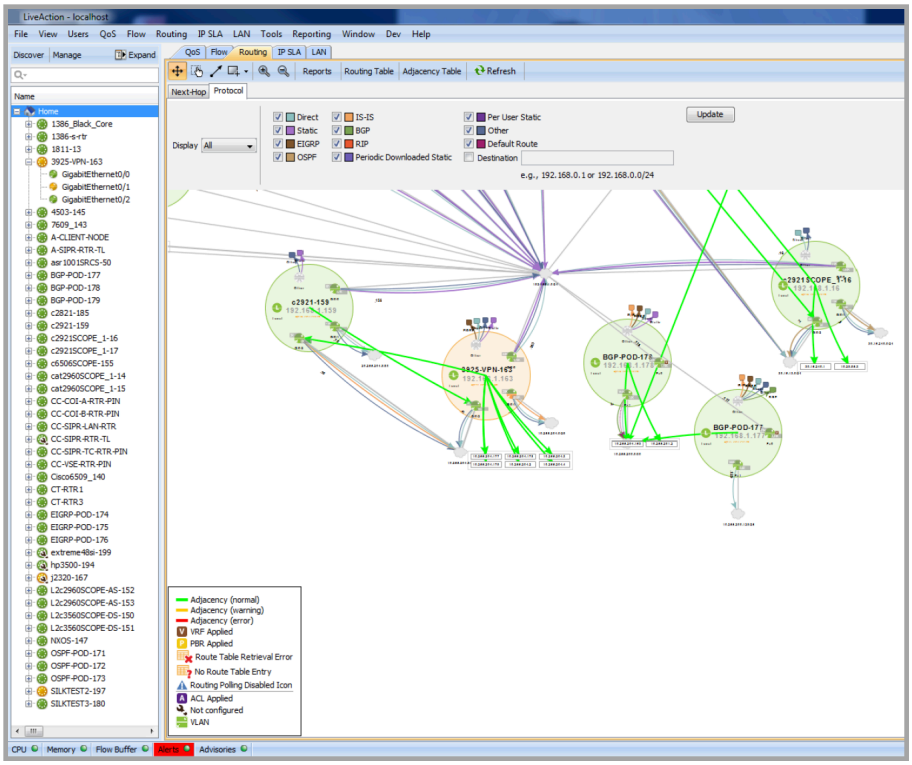
LiveNX Routing Views

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.

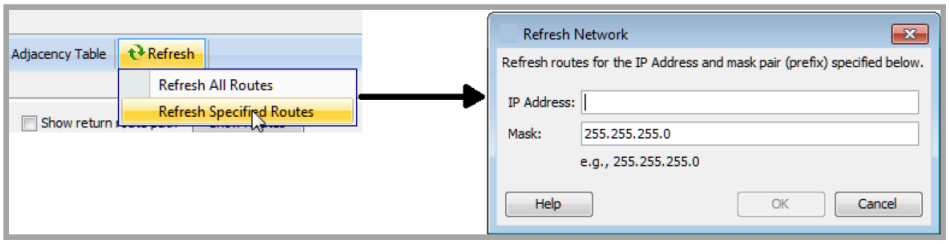


Refresh Routes

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:

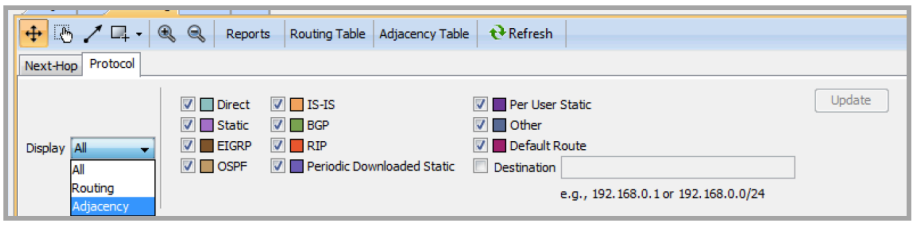
- The device has a very large routing table.
- There is a very high load on the CPU running LiveNX.
- The device is connected to LiveNX over a high-latency path.

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.

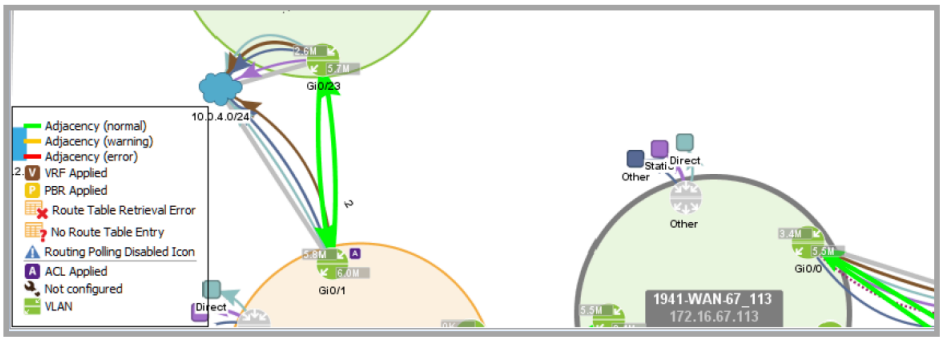
Note The refresh operation applies only to the display, and does not affect the device's configuration or any of the routes themselves.

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.

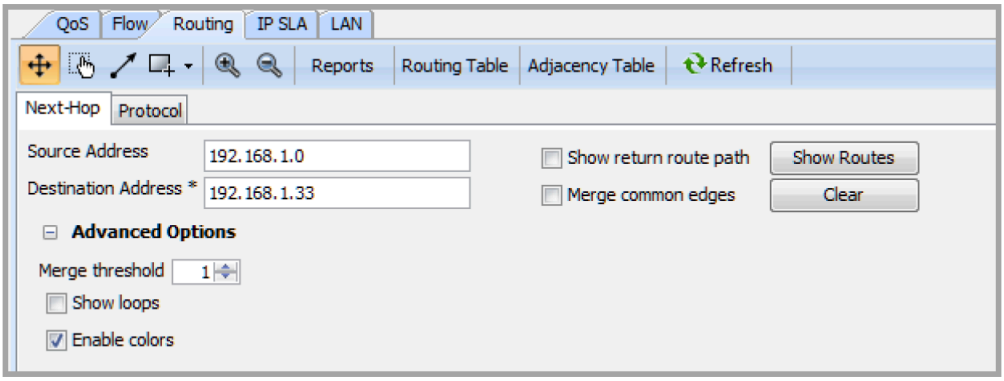


Next-Hop Routing

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.

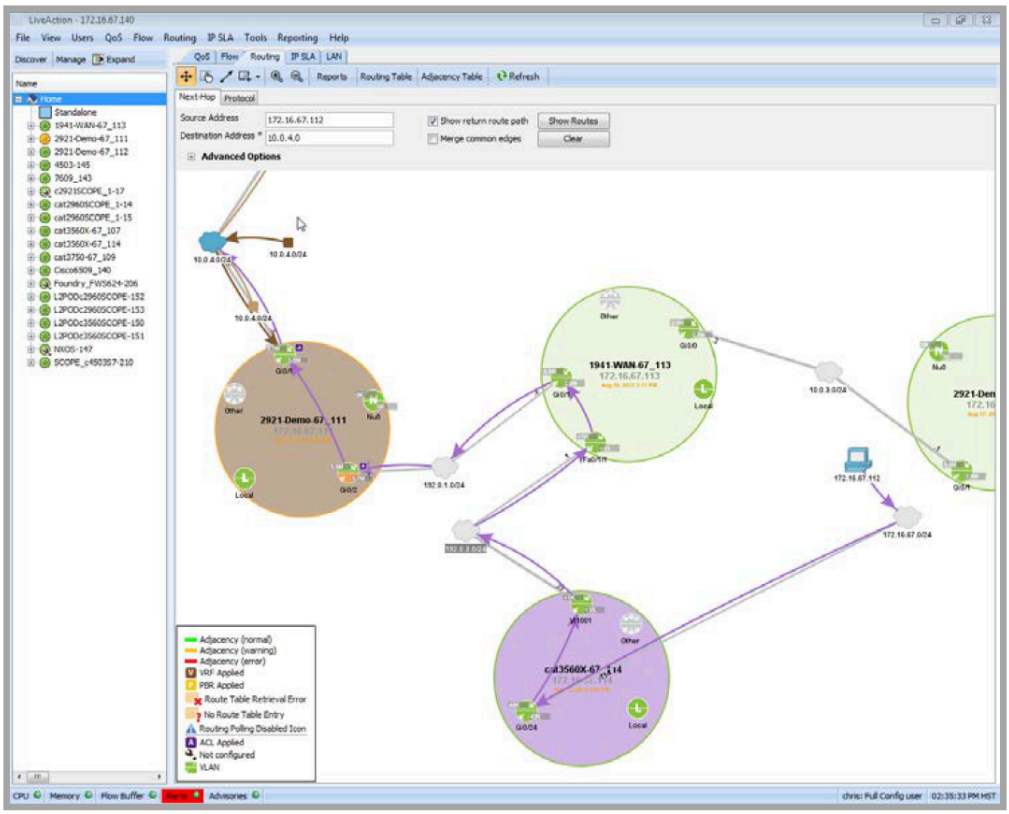
To access Next-Hop Routing visualization, click on the Routing tab. Below the system topology toolbar, select Next-Hop.



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.

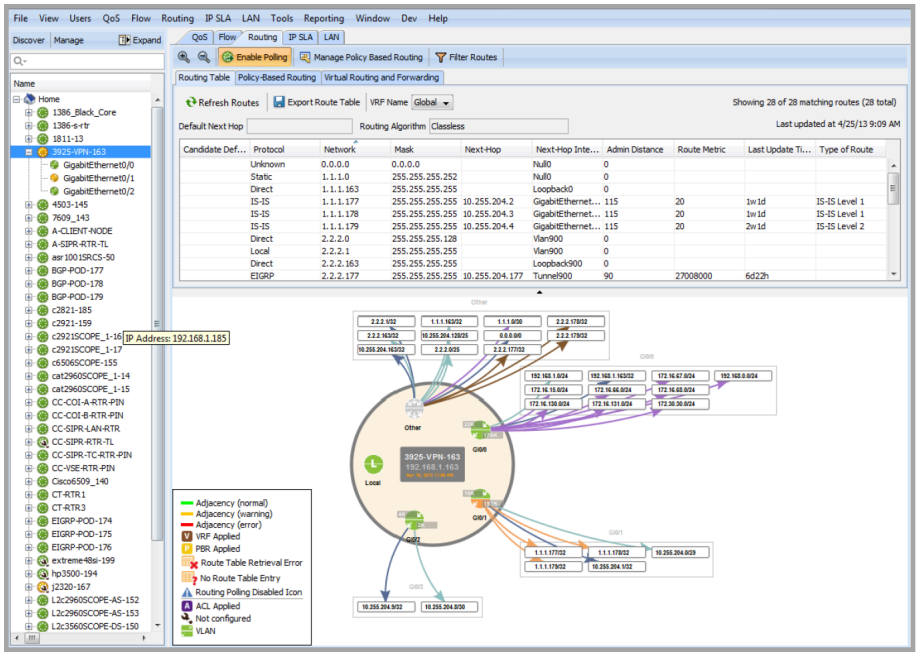
Next-Hop Routing visualization in the system topology view is displayed as a bold, light purple-colored line. If the destination address is not represented in the current set of network devices, as in the example below, a new icon representing the destination device is created.



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.

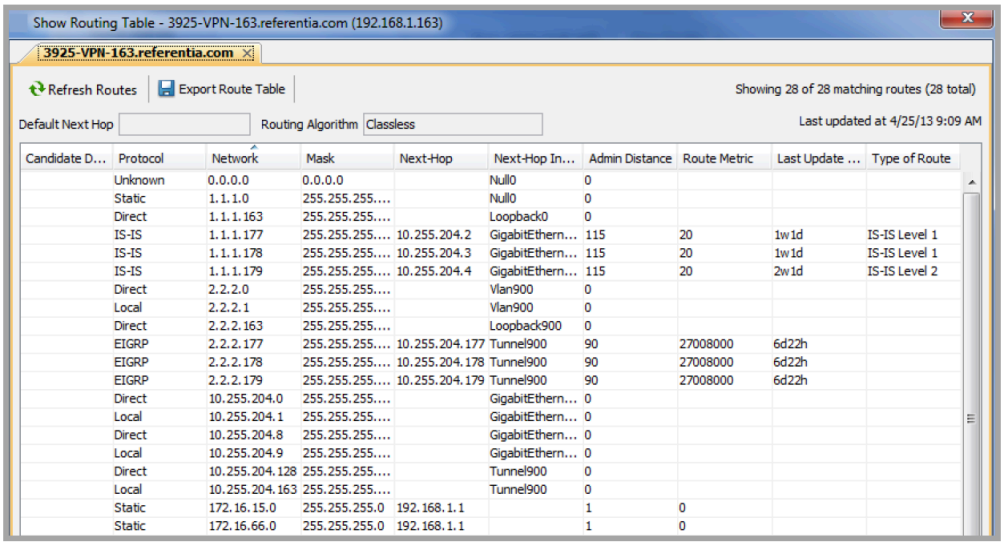
The upper portion of the screen shows the device's route table in tabular format. You can also apply a filter to display routes based on specific protocols and/or destinations.



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

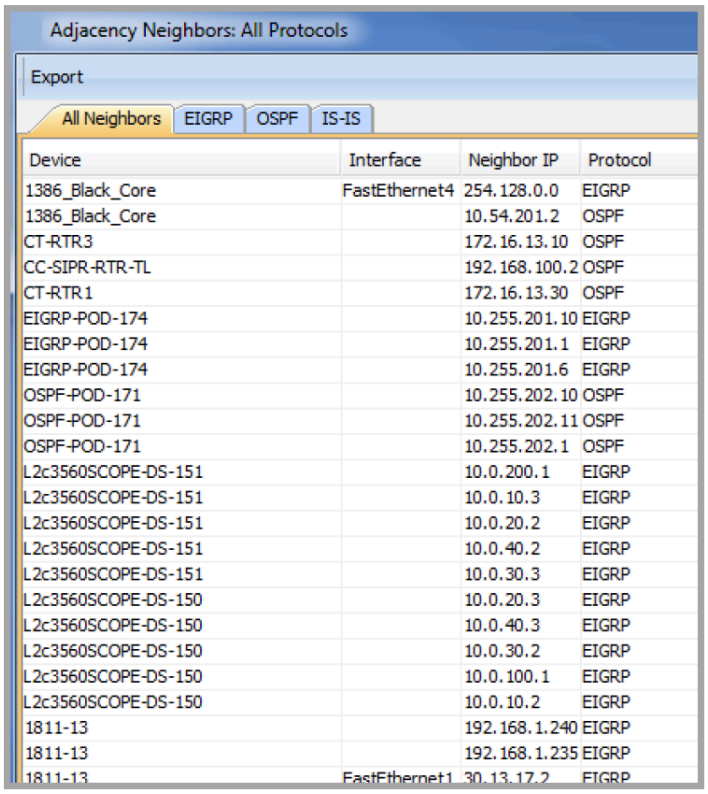
In the routing topology home view, click on an individual device and then click on Routing Table in the menu bar within the Routing tab to view the Routing Table specific to that device.



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		Null0	0			
	Static	1.1.1.0	255.255.255....		Null0	0			
	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			
	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.



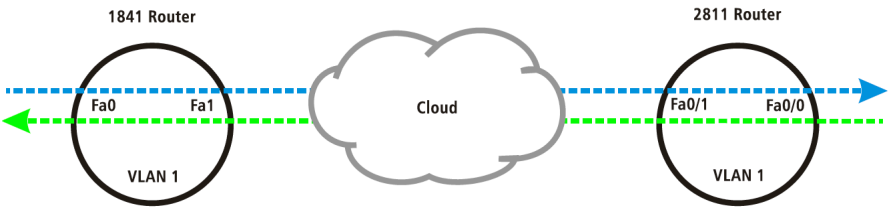
Device	Interface	Neighbor IP	Protocol
1386_Black_Core	FastEthernet4	254.128.0.0	EIGRP
1386_Black_Core		10.54.201.2	OSPF
CT-RTR3		172.16.13.10	OSPF
CC-SIPR-RTR-TL		192.168.100.2	OSPF
CT-RTR1		172.16.13.30	OSPF
EIGRP-POD-174		10.255.201.10	EIGRP
EIGRP-POD-174		10.255.201.1	EIGRP
EIGRP-POD-174		10.255.201.6	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-151		10.0.200.1	EIGRP
L2c3560SCOPE-DS-151		10.0.10.3	EIGRP
L2c3560SCOPE-DS-151		10.0.20.2	EIGRP
L2c3560SCOPE-DS-151		10.0.40.2	EIGRP
L2c3560SCOPE-DS-151		10.0.30.3	EIGRP
L2c3560SCOPE-DS-150		10.0.20.3	EIGRP
L2c3560SCOPE-DS-150		10.0.40.3	EIGRP
L2c3560SCOPE-DS-150		10.0.30.2	EIGRP
L2c3560SCOPE-DS-150		10.0.100.1	EIGRP
L2c3560SCOPE-DS-150		10.0.10.2	EIGRP
1811-13		192.168.1.240	EIGRP
1811-13		192.168.1.235	EIGRP
1811-13	FastEthernet1	30.13.17.2	EIGRP

LiveNX Policy-Based Routing (PBR)

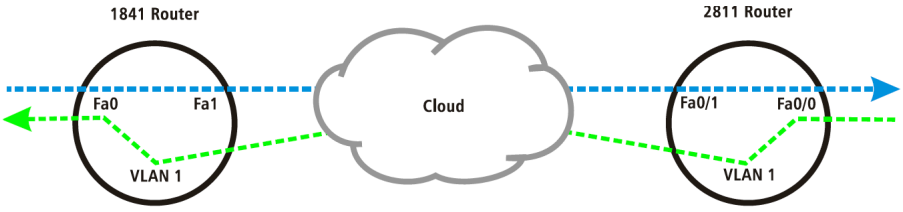
For greater route control, LiveNX Routing allows you to create Policy-Based Routing (PBR) rules and apply these rules to your devices.

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.

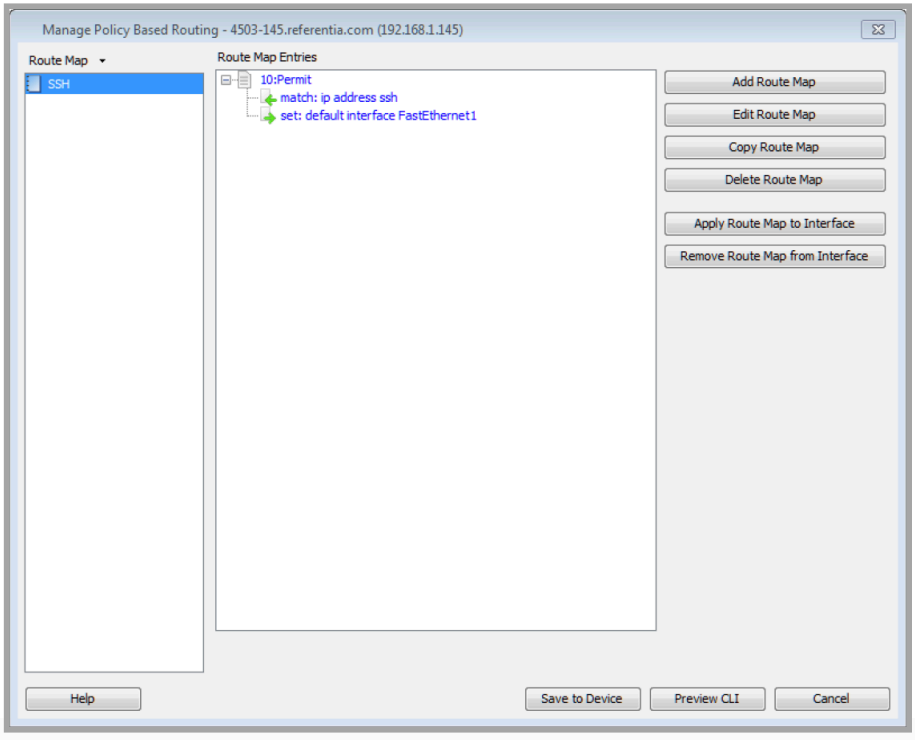
PBR Monitoring

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 flow-based view of the effects of PBR on application flows coupled with statistics on the PBR policies and underlying ACLs.

PBR Configuration

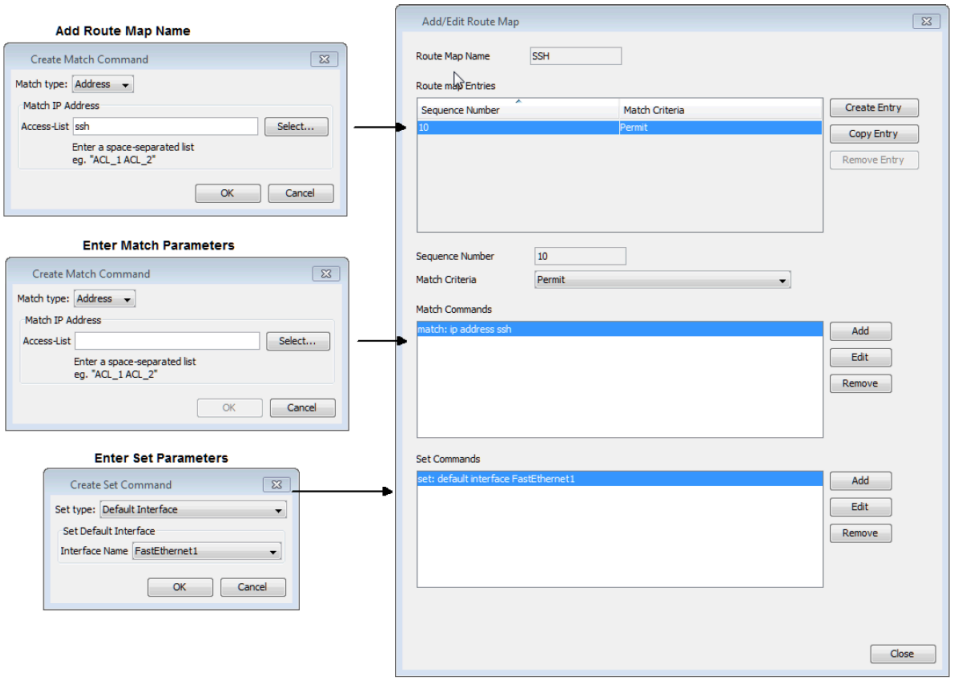
LiveNX also provides a complete PBR configuration solution in conjunction with its built-in ACL editor. Configuring PBR involves creating a route map consisting of a match to identify the incoming packets on a particular interface, and the set actions to perform on these packets.

Click Manage Policy Based Routing to create, edit, and apply PBR on a device.



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

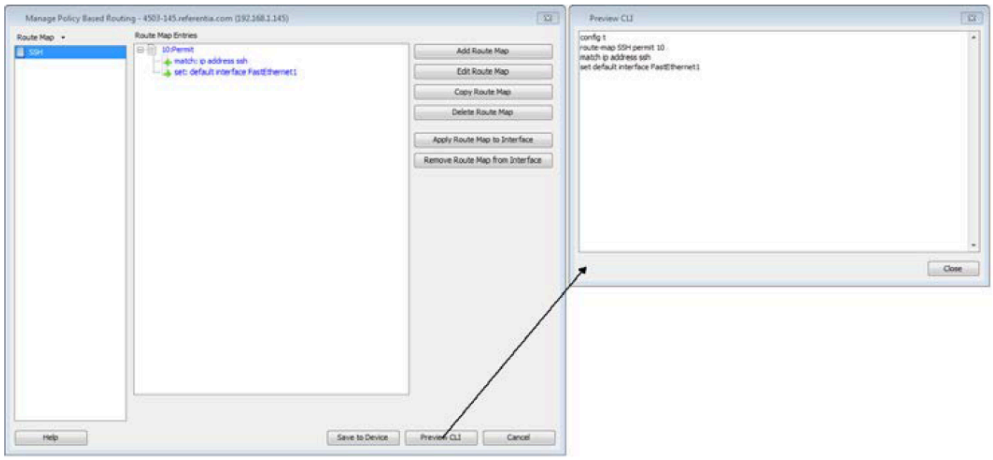
The match commands determine how to match the packets, and the set commands determine the actions to be performed. Match commands are typically created using a pre-defined ACL, which can be constructed using the LiveNX ACL editor.

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

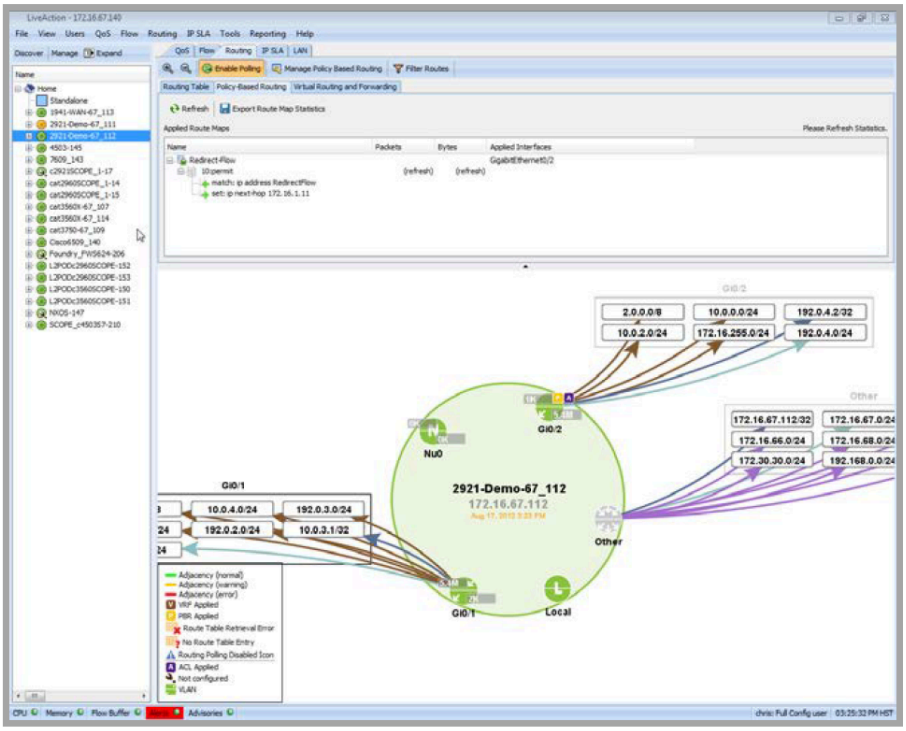
Click Preview CLI on the Manage Policy-Based Routing dialog box to view the commands before they are sent to the device.



Policy-Based Routing Workflow

The following is an example workflow for configuring, monitoring, and adjusting PBR-based actions:

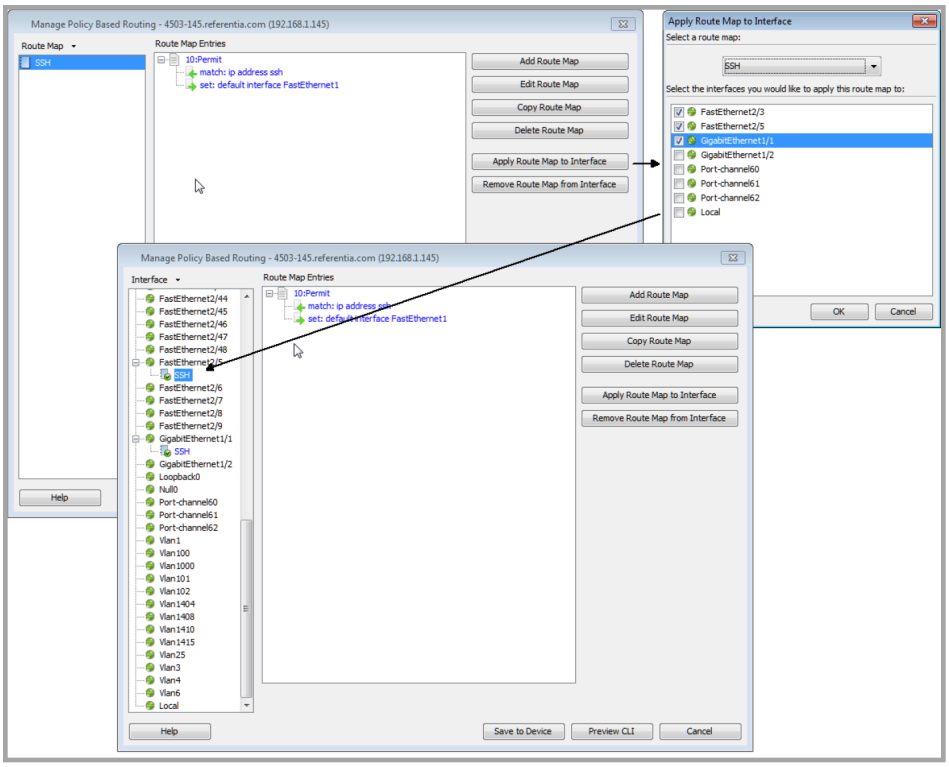
- Create ACL for use with PBR.
- Create PBR to be used.
- Apply PBR to inbound interface.
- Observe PBR and ACL statistics for proper matches.
- Use Flow views to observe flow changes.
- Adjust PBR for proper operation.



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.



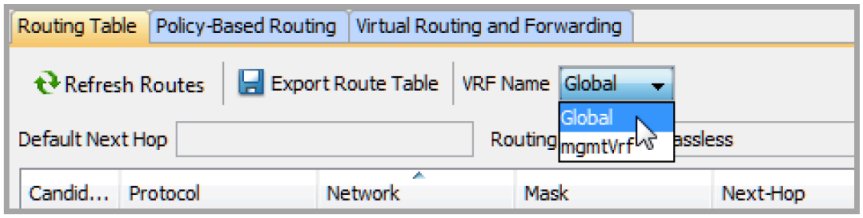
Monitoring Policy-Based Routing

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.

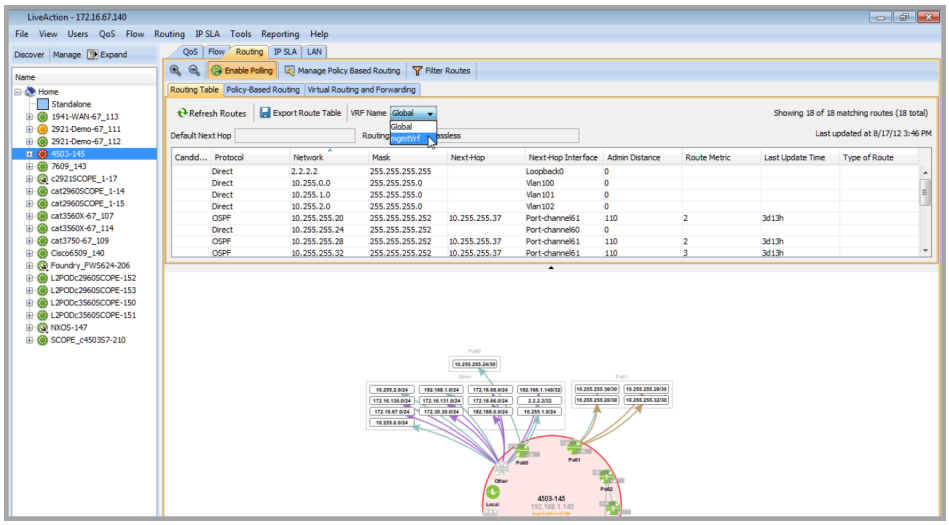
LiveNX Virtual Routing and Forwarding (VRF)

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.



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.



IP SLA

In this chapter:

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.

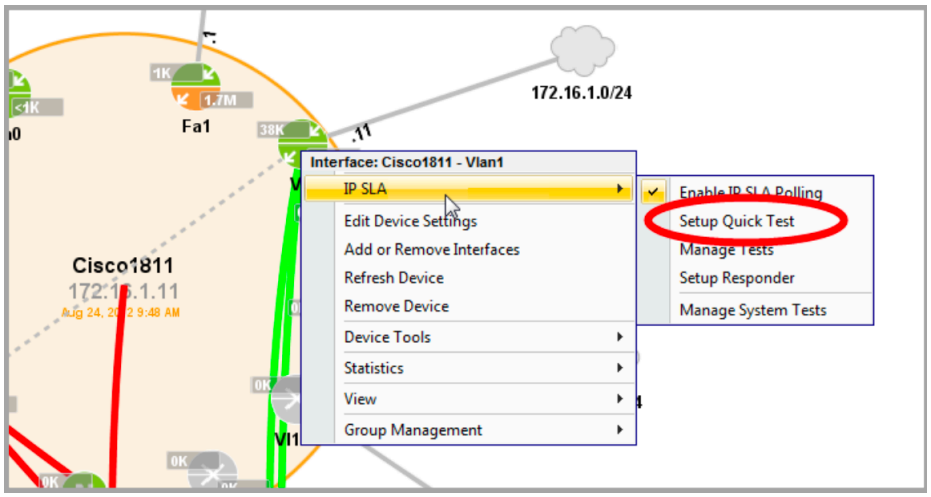
Configuring LiveNX IP SLA

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

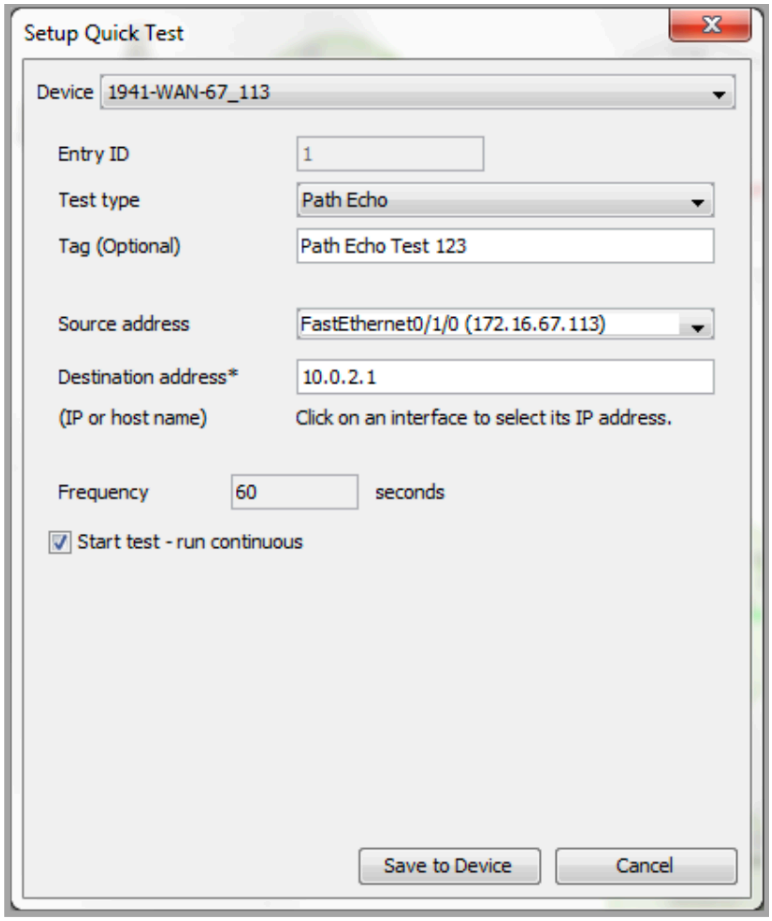
Setup Quick Test Wizard

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.



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.

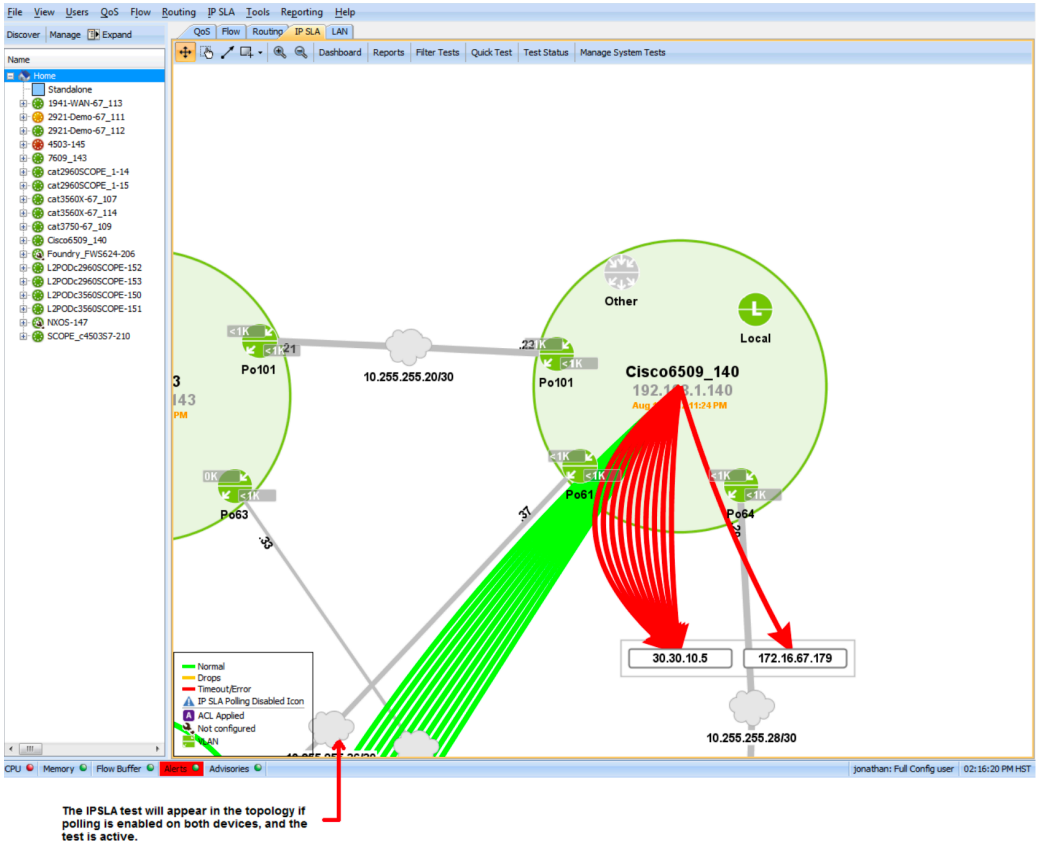
   Path Echo and Path Jitter tests measure the time between sending and receiving acknowledgment of user Datagram Protocol (UDP) Echo (port 7) packets. This is useful in determining round-trip delay for programs using UDP to communicate over the network.

   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.

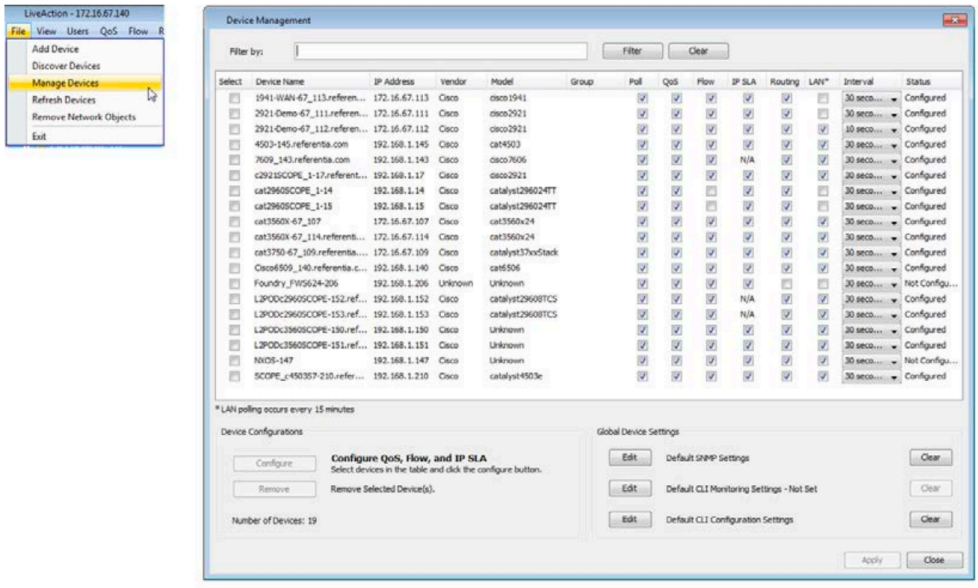
4. Enter the optional Tag value to use as the name, label, or description of the test.

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.

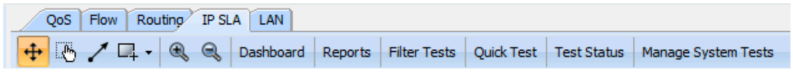


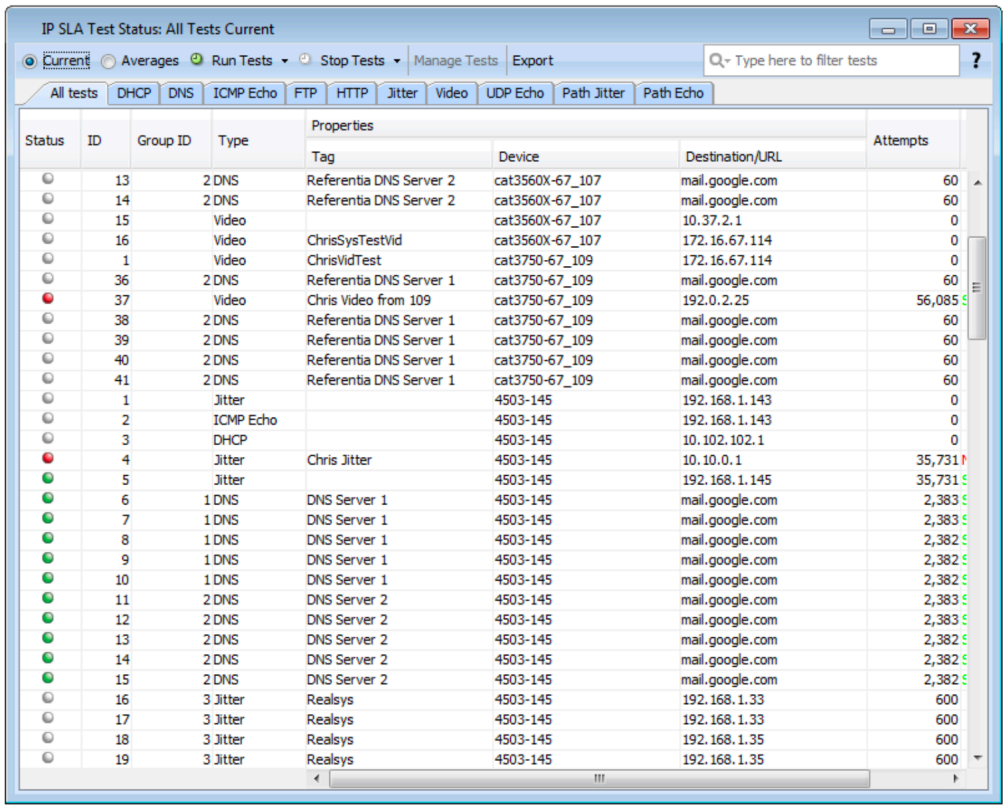
7. Enable IP SLA polling for both devices by going to File > Mange Devices. Select the appropriate check boxes in the Poll and IPSLA column. Polling must be enabled before IP SLA test results will appear.



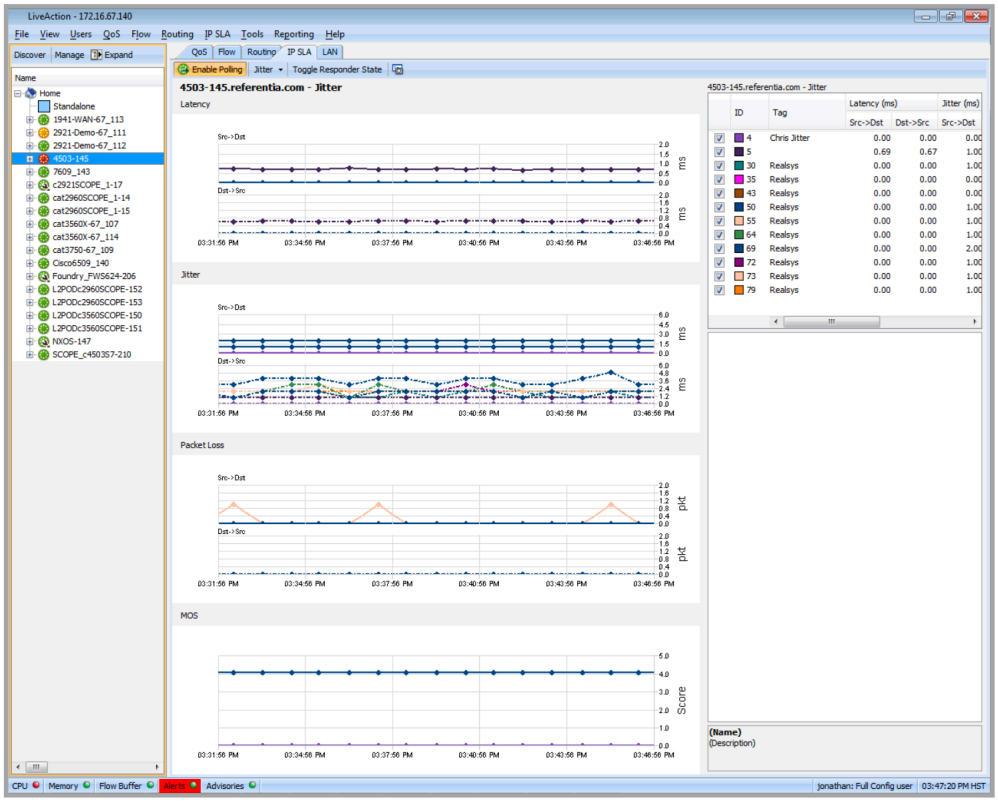
8. To monitor this test, click Show Test Status in the IP SLA tab toolbar. This will bring up the Test Status window that will show you statistics for latency, jitter, and loss.

   - The test will run continuously by default until ended.
   - Statistics will take one polling interval (default is 60 seconds) to refresh.

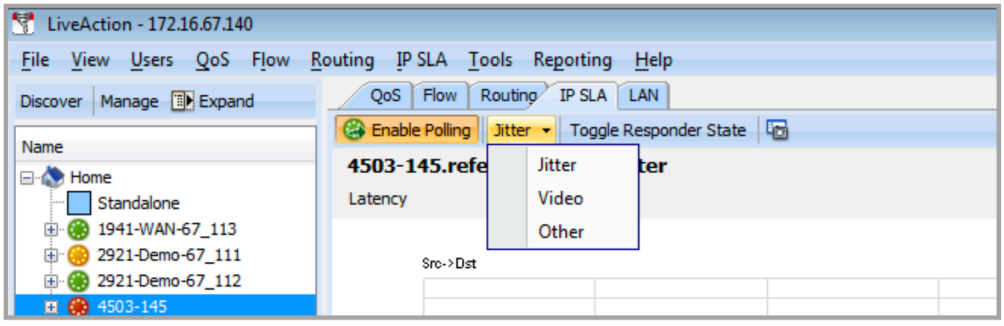




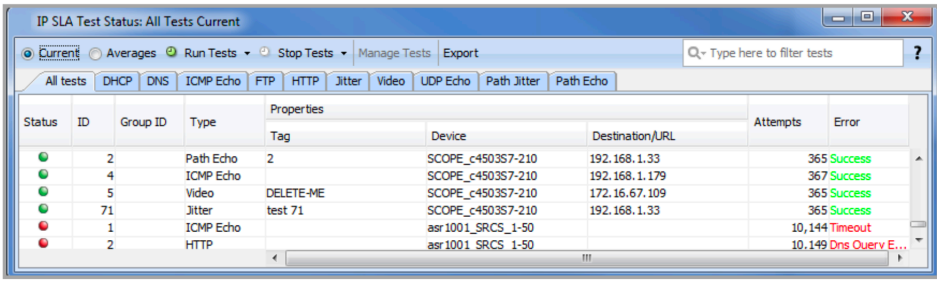
Additional detailed test information can be accessed by clicking on the originating router while in the IP SLA view. This displays a set of graph for Latency, Jitter, Packet Loss and MOS scores as shown below.



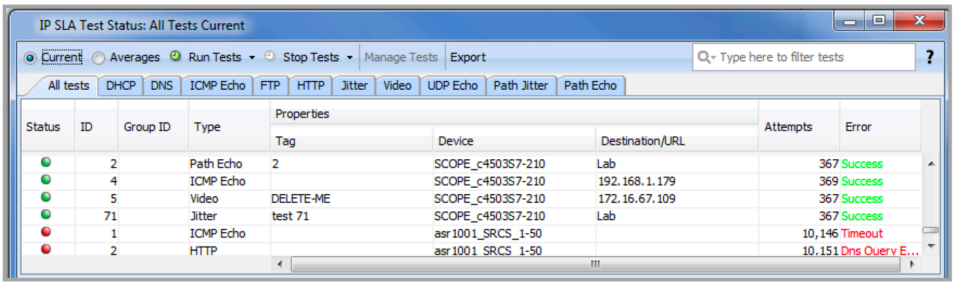
9. By selecting the viewing mode, various different sets of graphs can be shown that are appropriate for the test being run.



10. The IP address in the Destination/URL field can be changed to a user-defined value by the Edit IP Mapping feature.

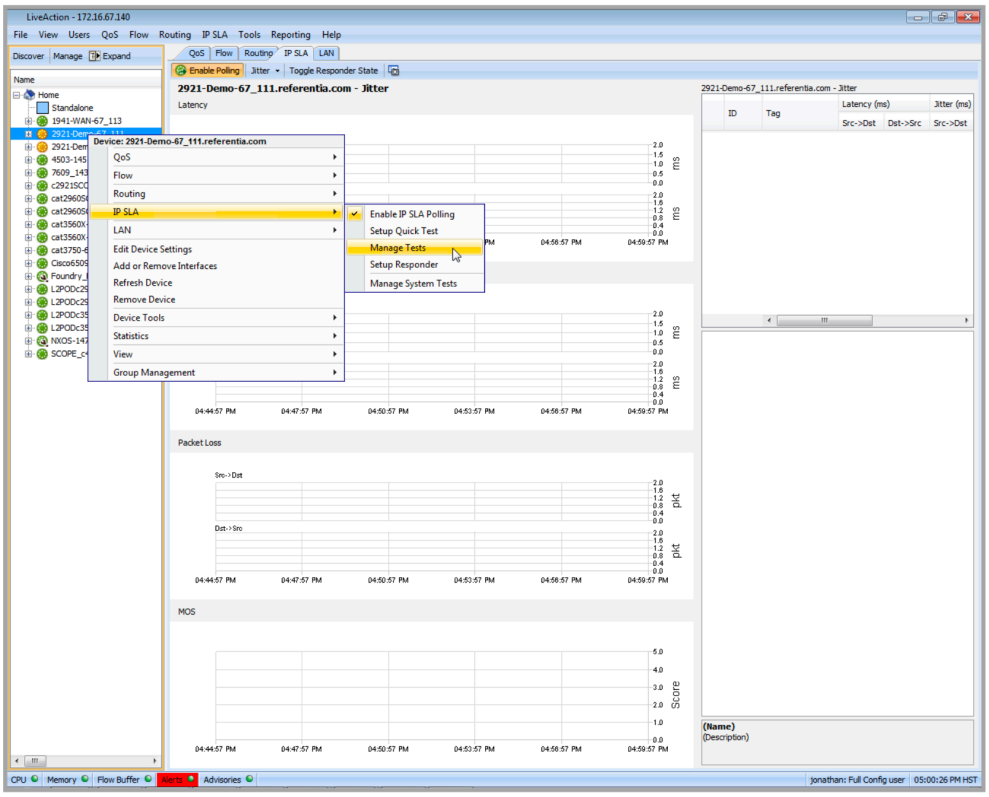


11. By selecting Tools > Edit IP Mappings described in *IP Mapping* on page 241, select Add and then type in a user-defined Name and the desired IP Address. The new user-defined value is displayed in the Destination/URL field.

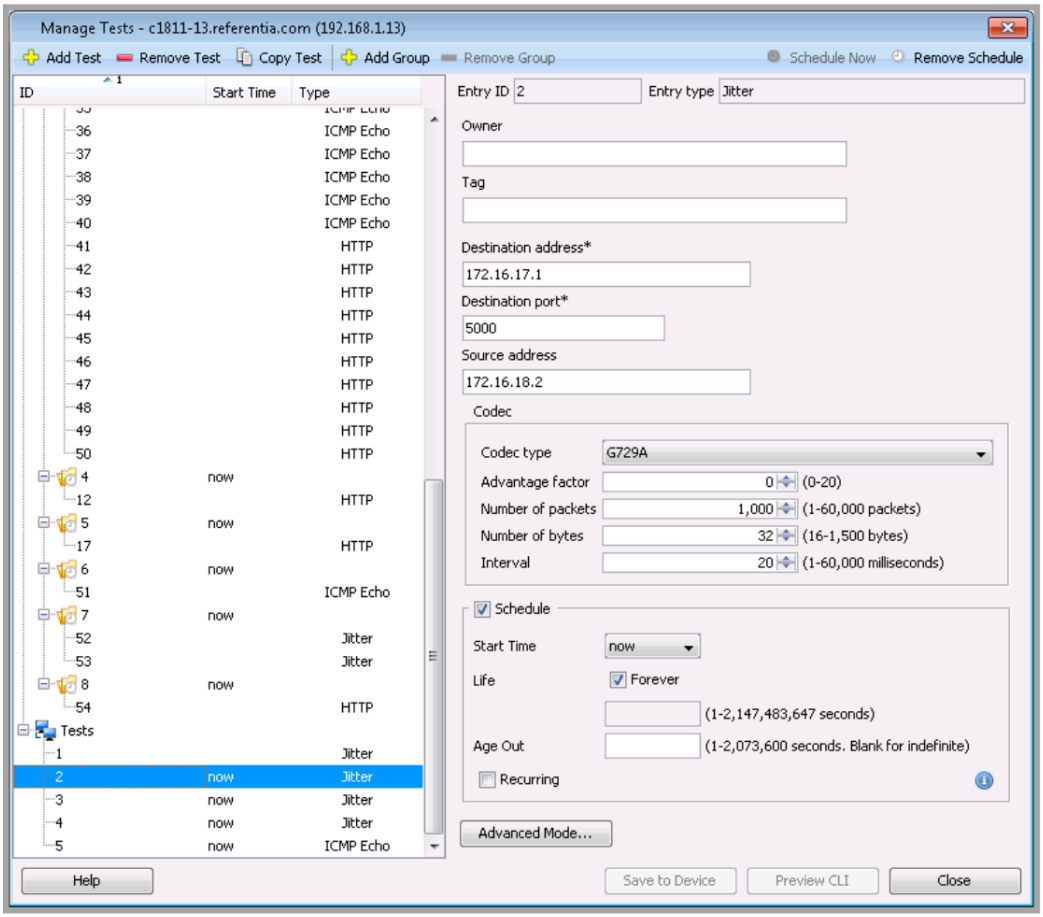


Managing Tests

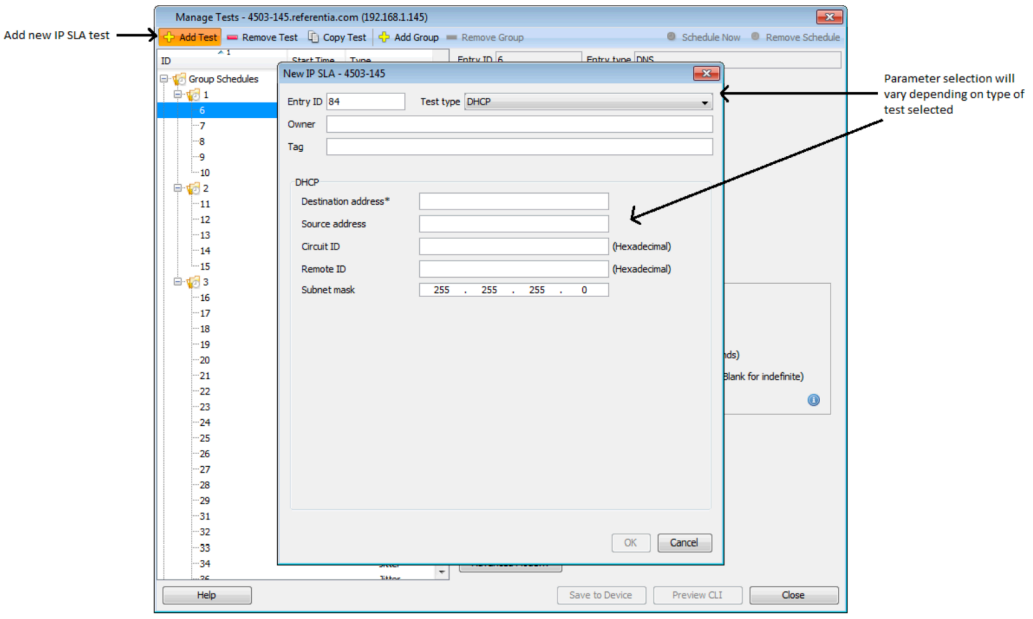
For extended test coverage and scheduling capability, access configuration options from the IP SLA menu, or right-click on the network device from which the test will be started.



The manage test window allows you to create, delete, copy and group tests. The main window is shown below.



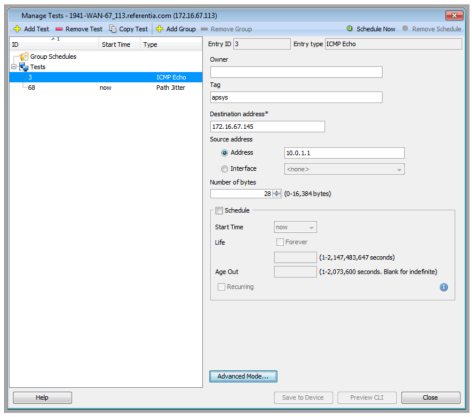
Adding a new test is done by clicking Add Test, which brings up a dialog with basic test parameters.

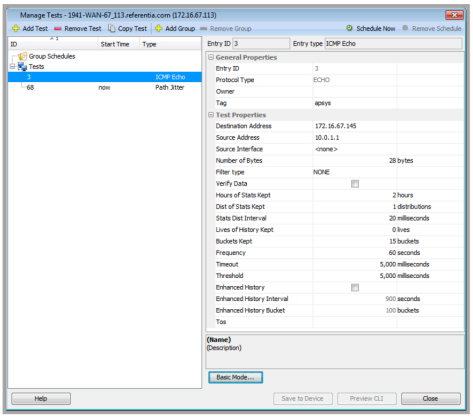


Once a test is created, it can be edited using either the basic or advanced mode. Click Basic Mode or Advanced Mode to toggle between basic and advanced configuration modes. Parameters edited in one mode will persist in the other mode; validation is also enforced in both modes. In Basic Mode, required fields are denoted with an asterisk (*).

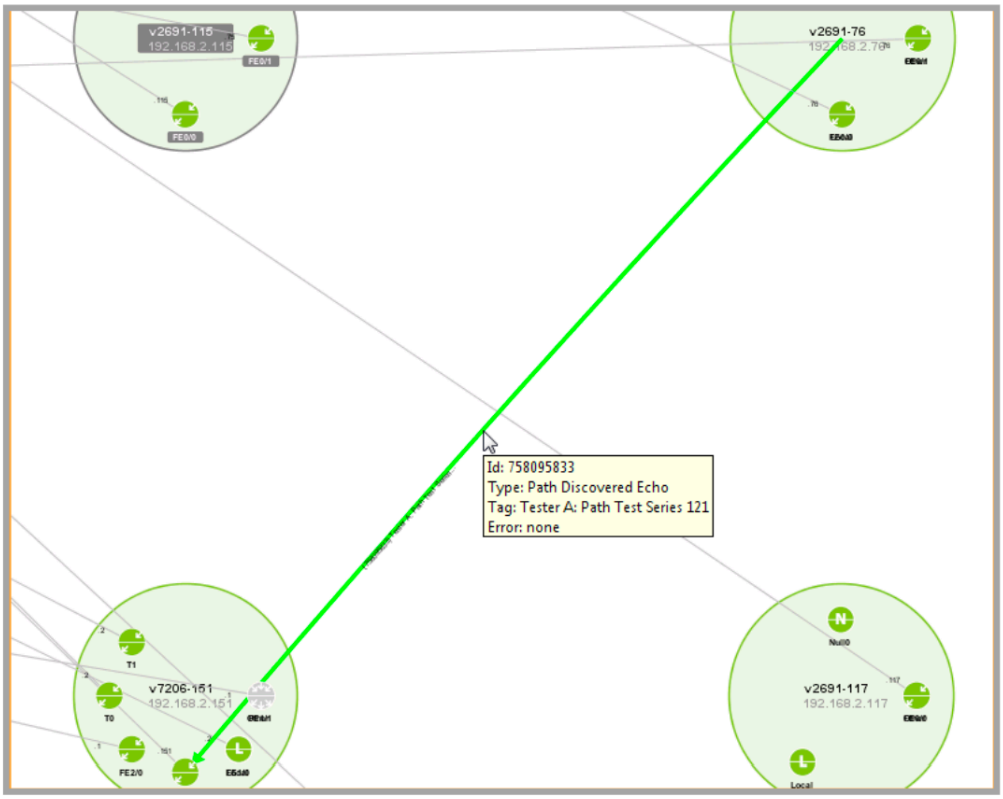
Save to Device and Preview CLI are enabled when changes have been made and all changes are valid. View Errors will be enabled if there are any validation errors. Click View Errors to display a list of all errors.

Refer to the Cisco reference manual for descriptions of all Path Echo configuration parameters.





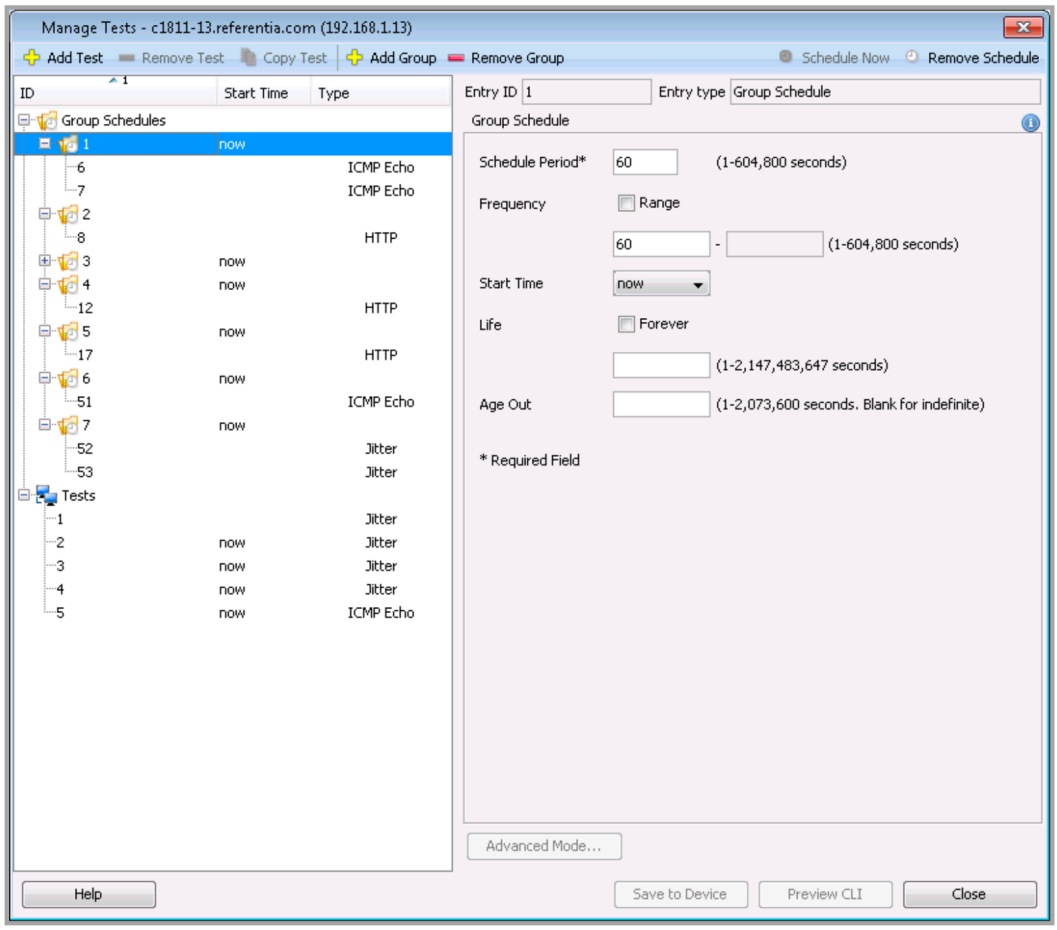
In the system topology view, Path Echo test results are displayed in visual form, delivering rich context for instant understanding. Colored icons indicate operating success or failure status quickly and easily for each test.



Advanced Test Scheduling

Advanced Test Scheduling

Scheduling had been enhanced, allowing you to better control when tests are run:



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.

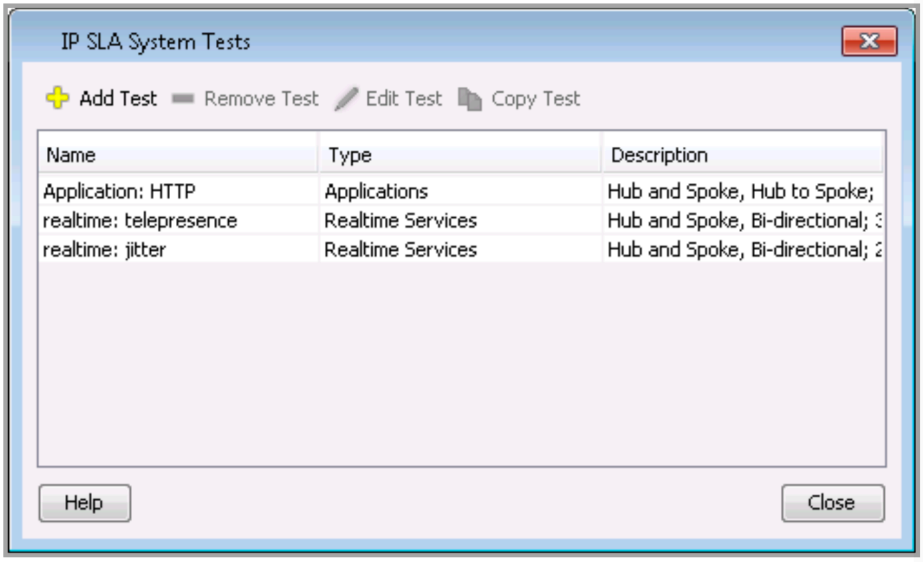
Test Groups

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.



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

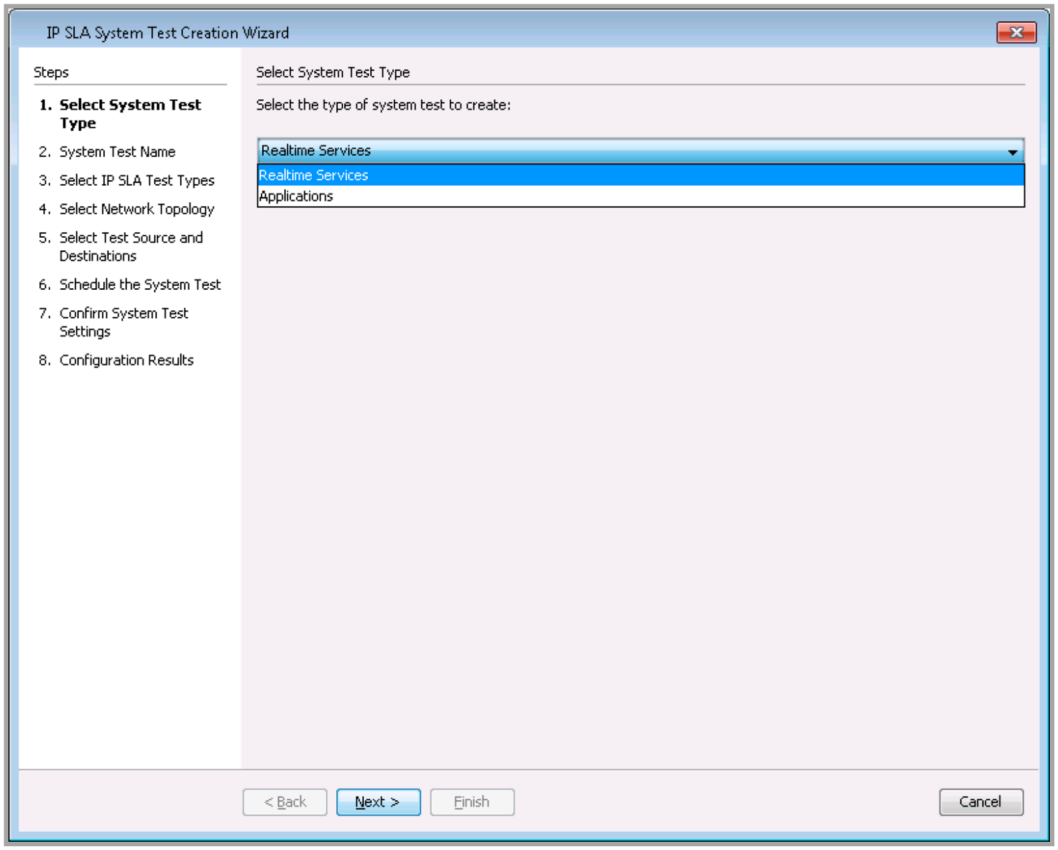
Device right-click pop-up menu in the IP SLA system topology view

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.



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.

LAN

In this chapter:

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

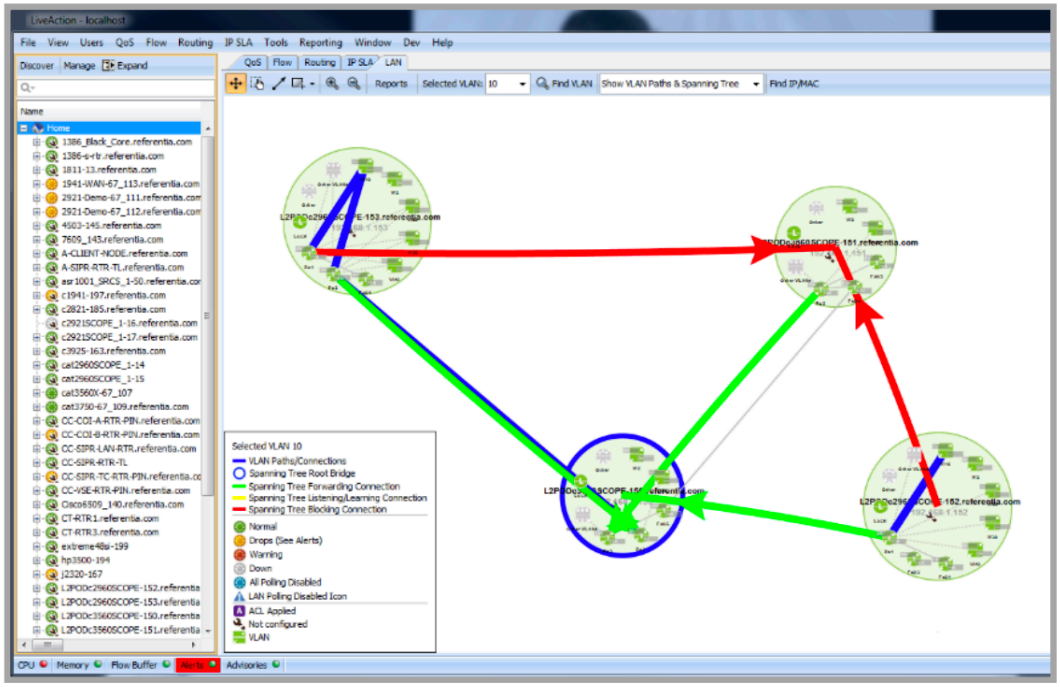
- Trunk and access bandwidth information through network polling
- Layer 2 QoS statistics including CoS, DSCP, and IP precedence
- Dropped packets, interface and spanning tree topology change warnings through network polling at the VLAN level

Getting Started With LiveNX LAN

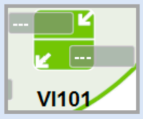
The setup is the same as the other LiveNX technologies.

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 Vl designation signifies a VLAN switch virtual interface (SVI) with an IP address. In this example, the name of the interface is Vl201 (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 Vl101 (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 	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.

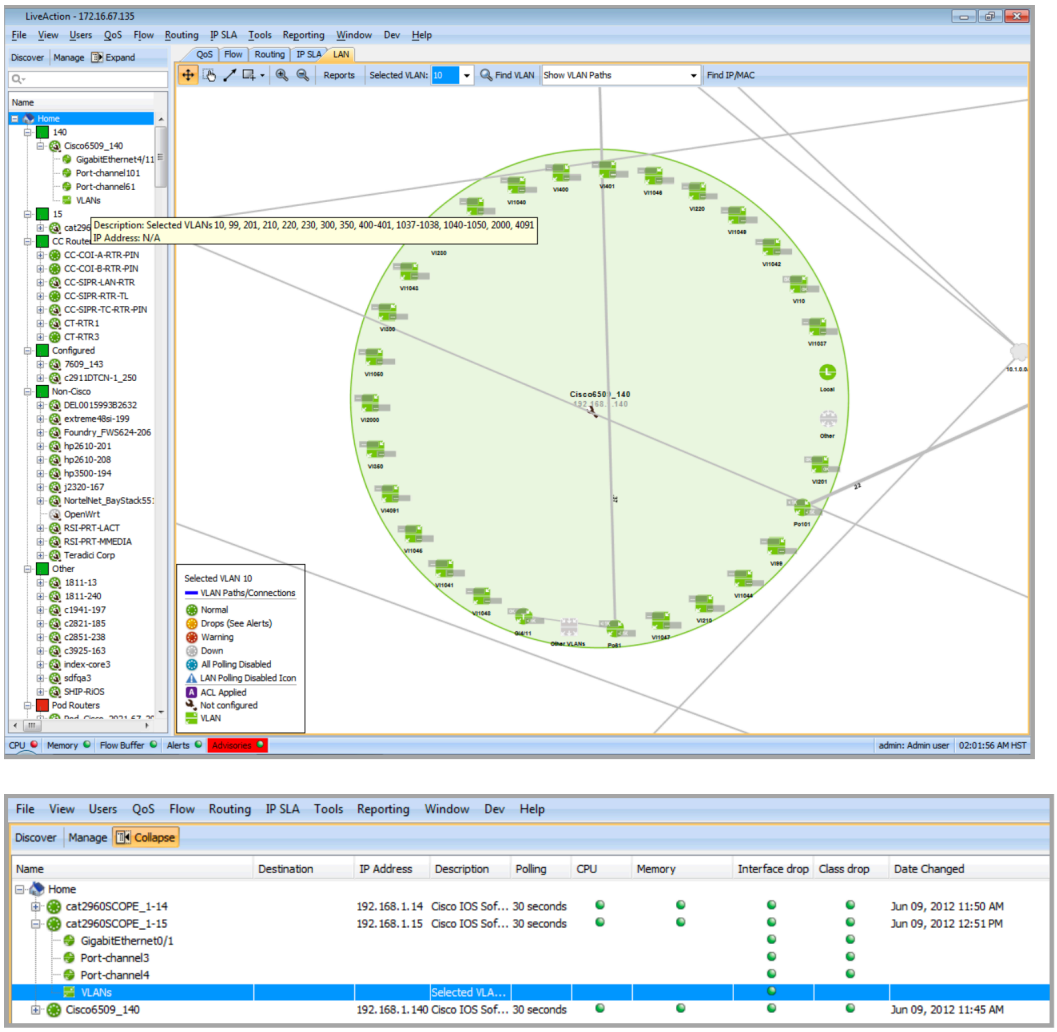
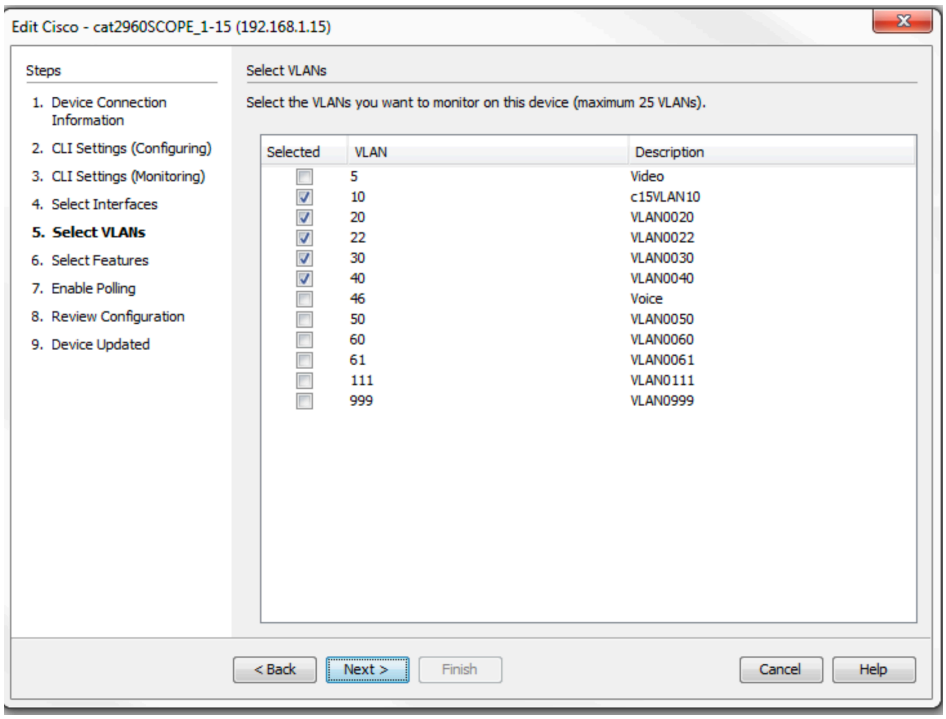


Fig. 10-2: Expanded System Hierarchy View with VLANs

VLANs in the Add Device Process

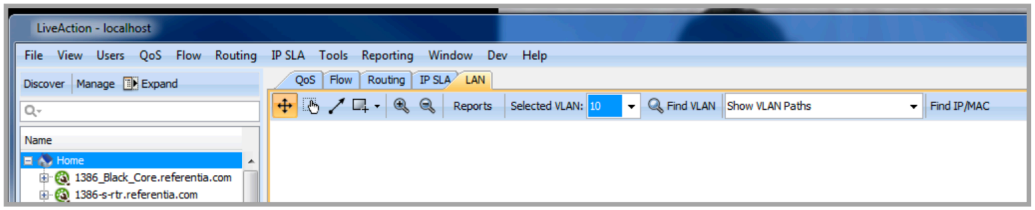
During the Add Device process, LiveNX allows user-selection of the VLANs to display in the topology view. VLANs listed here are Layer 2 related VLANs and are not Interface VLANs, which are selectable in the Select Interfaces step in the wizard. VLANs not associated with at least one access port will 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.



VLAN Highlighting Through a Network:

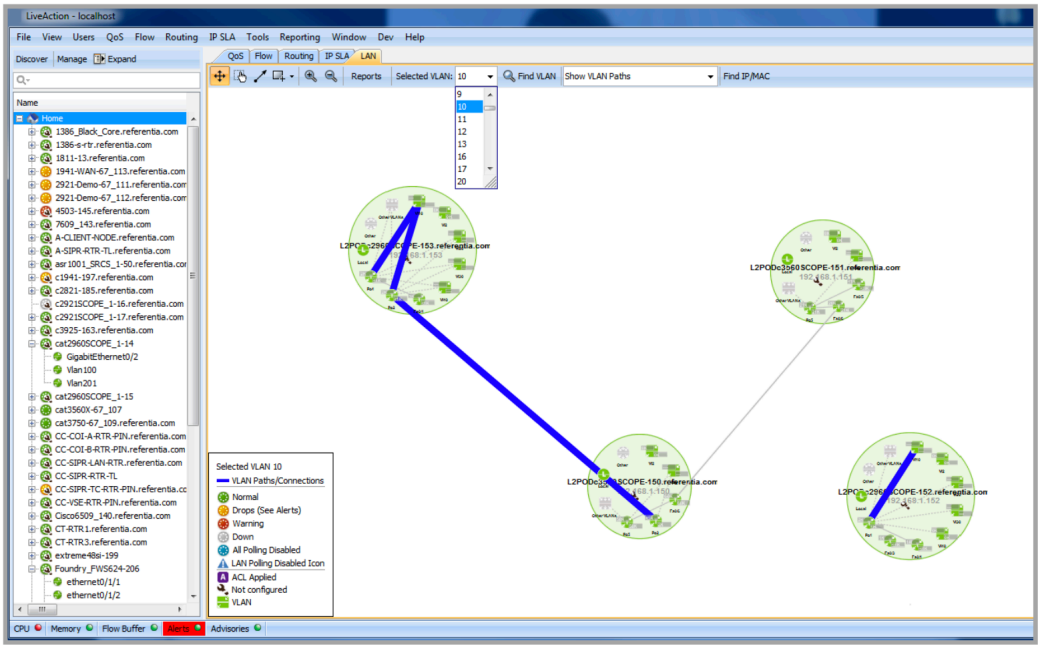
Use the Selected VLAN: drop-down menu to select any available VLAN index in the entire system topology. The VLAN will be highlighted in the system view.

The specific VLAN is highlighted as it traverses through the network.

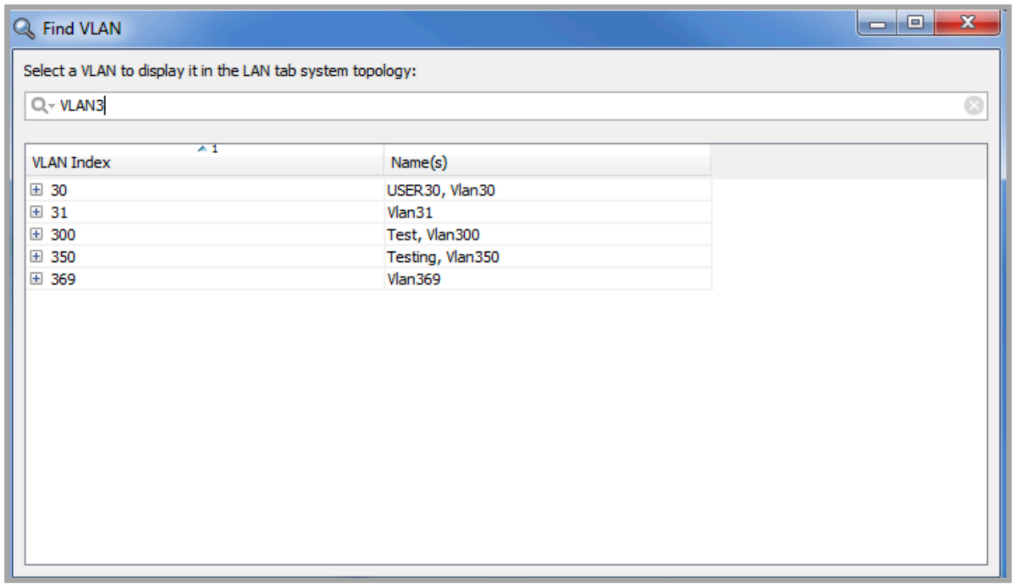


Use the Selected VLAN: drop-down menu to select any available VLAN index in the entire system topology. The VLAN will be highlighted in the system view.

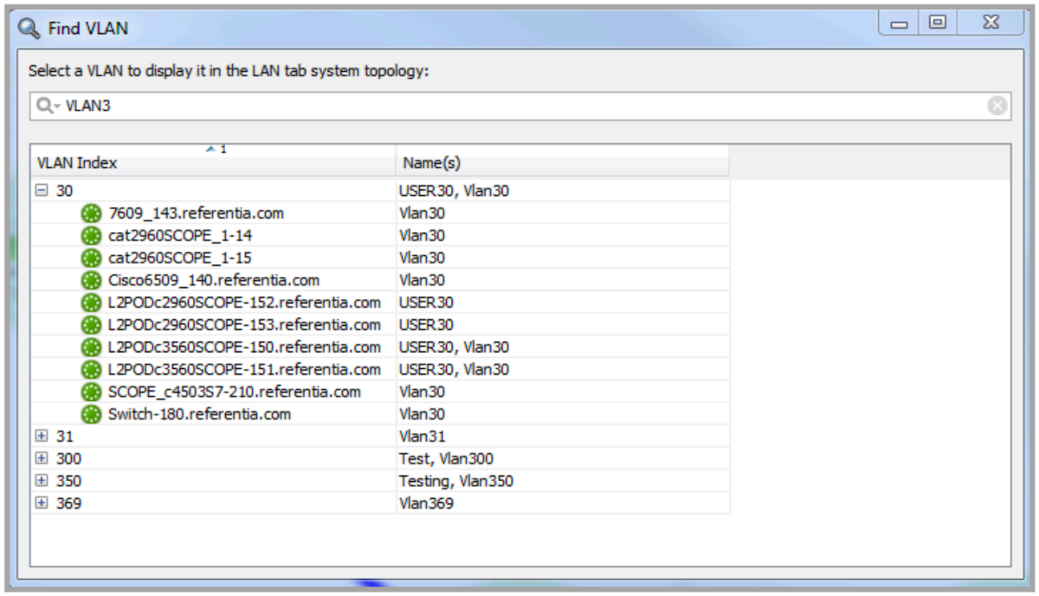
The specific VLAN is highlighted as it traverses through the network.



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.

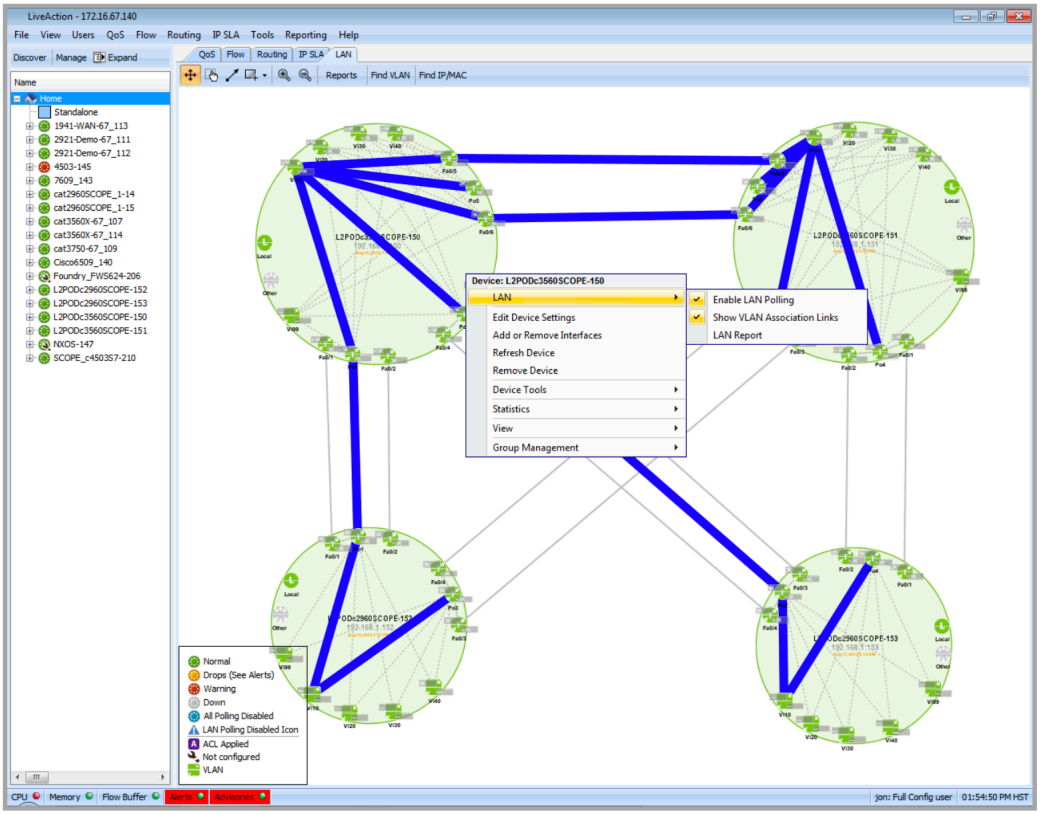


Clicking on the "+" to the left of the VLAN index displays a list of devices that the VLAN is configured on.



- 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.

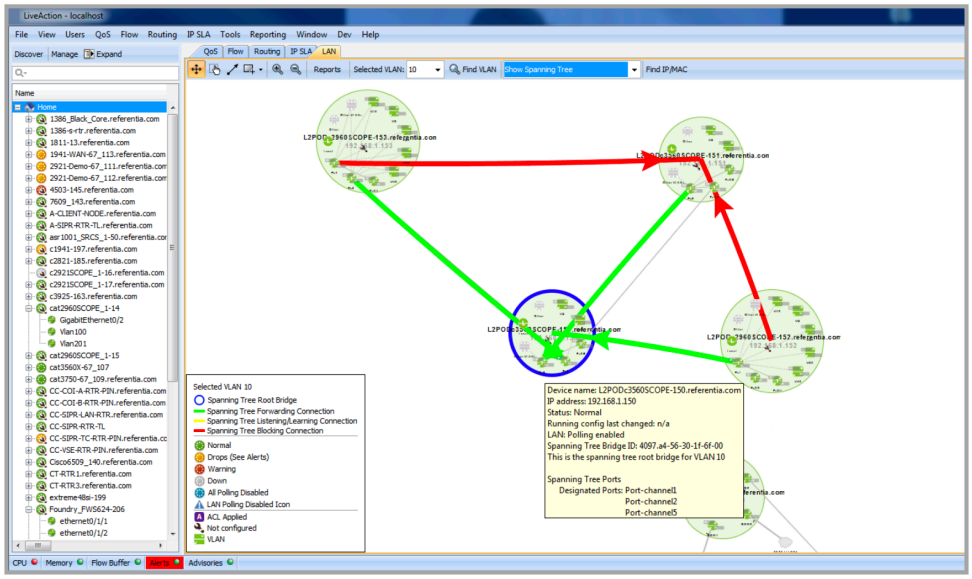


Spanning Tree Highlighting Through a Network

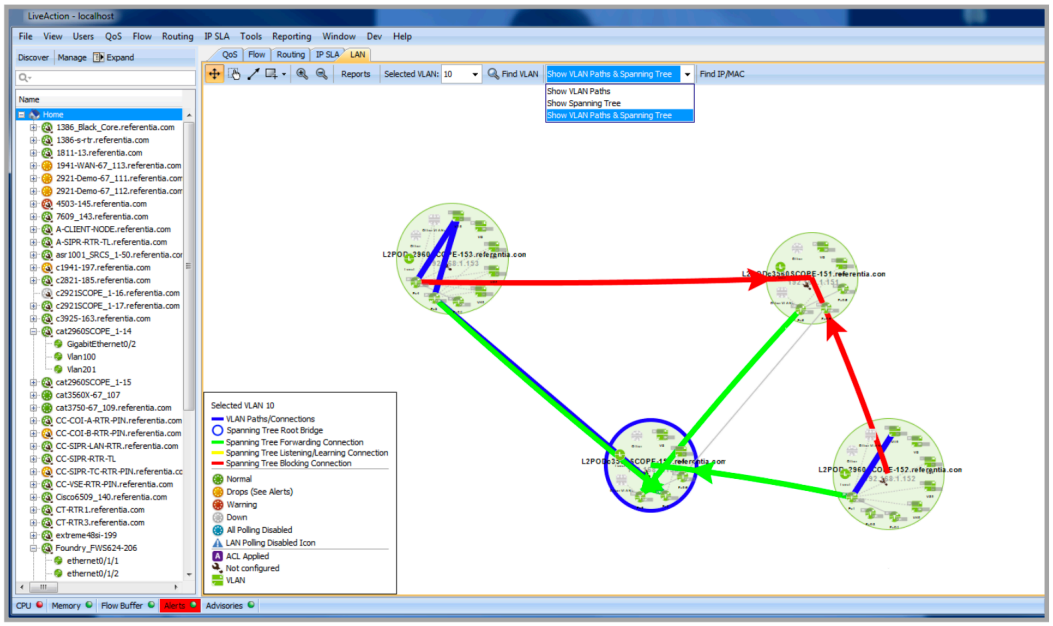
LiveNX provides the ability to highlight spanning tree information in the system view.

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.



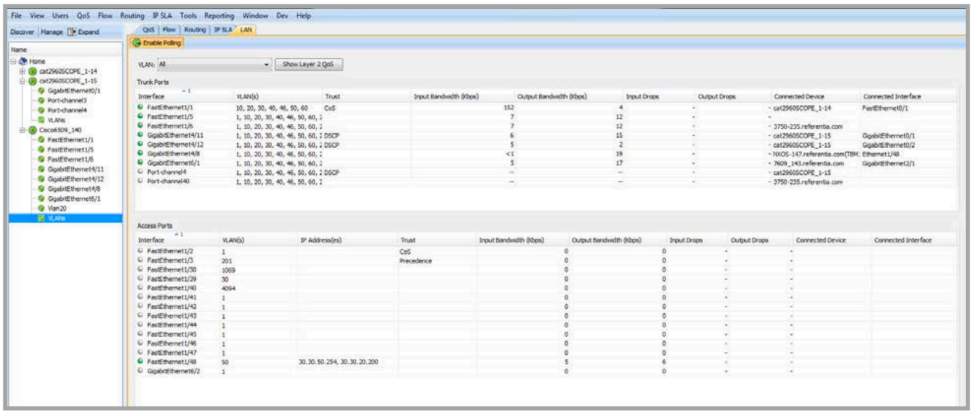
Real-time Monitoring

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.

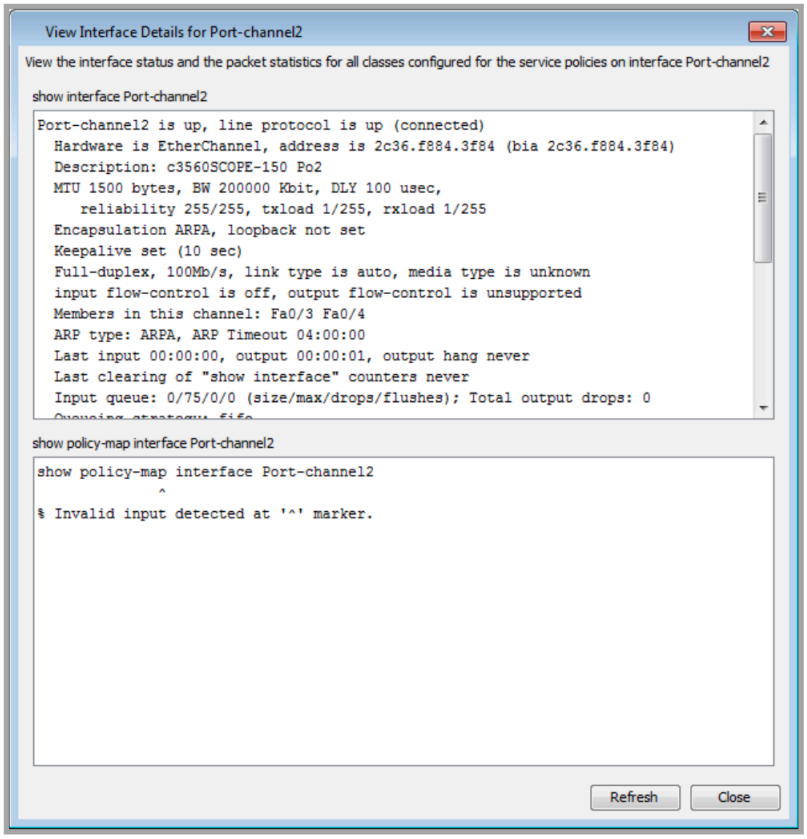


The statistics are separated into Trunk Ports and Access Ports. Both tables display Interface, Trust, Input Bandwidth (Kbps), Output Bandwidth (Kbps), Interface Drop, Connected Device and Connected Interface.

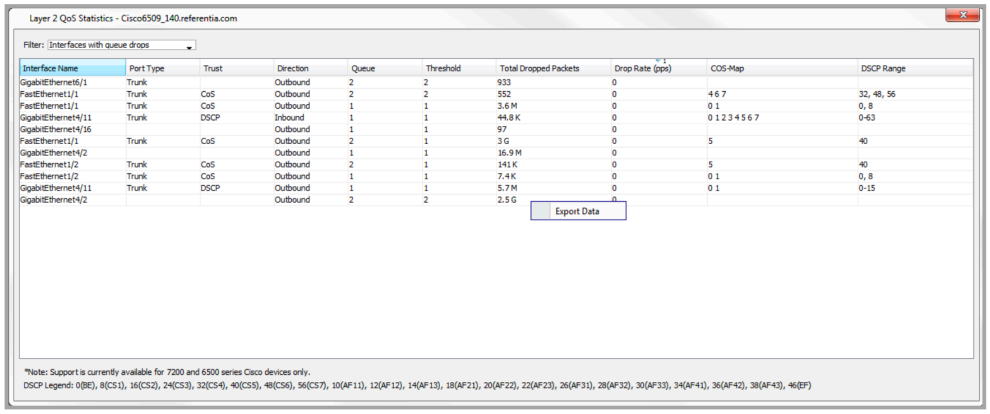
- Interface Name: Interface associated with the desired device.
- Trust: Class of Service (CoS), Differentiated Services Code Point (DSCP), IP Precedence (Precedence) or none (untrusted).
- Input Bandwidth: Input bandwidth for that interface. • Output Bandwidth: Output bandwidth for that interface.
- 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.



Click on the Show Layer 2 QoS button to display Layer 2 QoS statistics in tabular form.



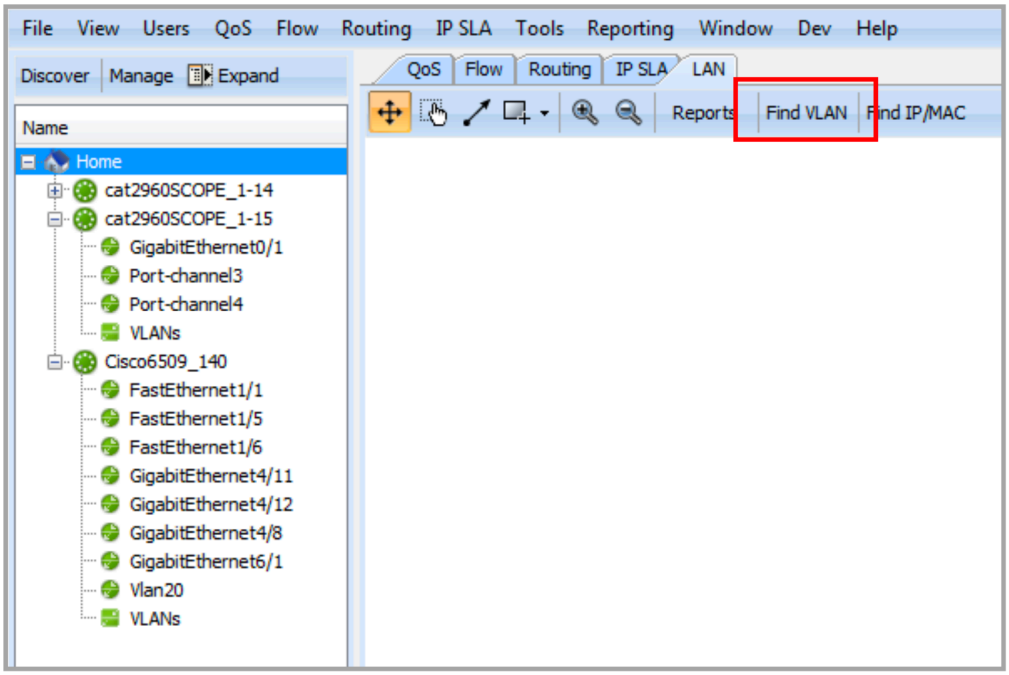
The Layer 2 QoS Statistics table lists all interfaces and its QoS statistics. The table can be filtered using four fields. Each can be enabled on or off independently from the other. The default filter is Interface with queue drops = Enabled.

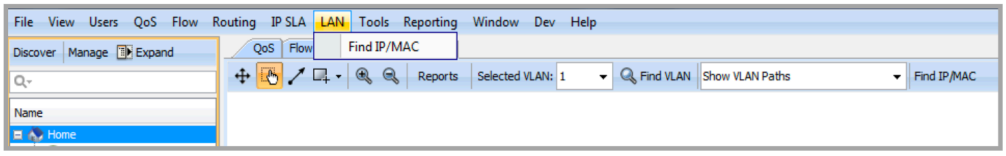
- Interface with queue drops – Displays all interfaces where the Total Dropped field is > 0.
- Priority queue stats – Displays all interfaces with COS-Map = 5.
- Inbound queues – Displays all interfaces with the Direction = Inbound.
- Outbound queues – Displays all interfaces with the Direction = Outbound.

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.

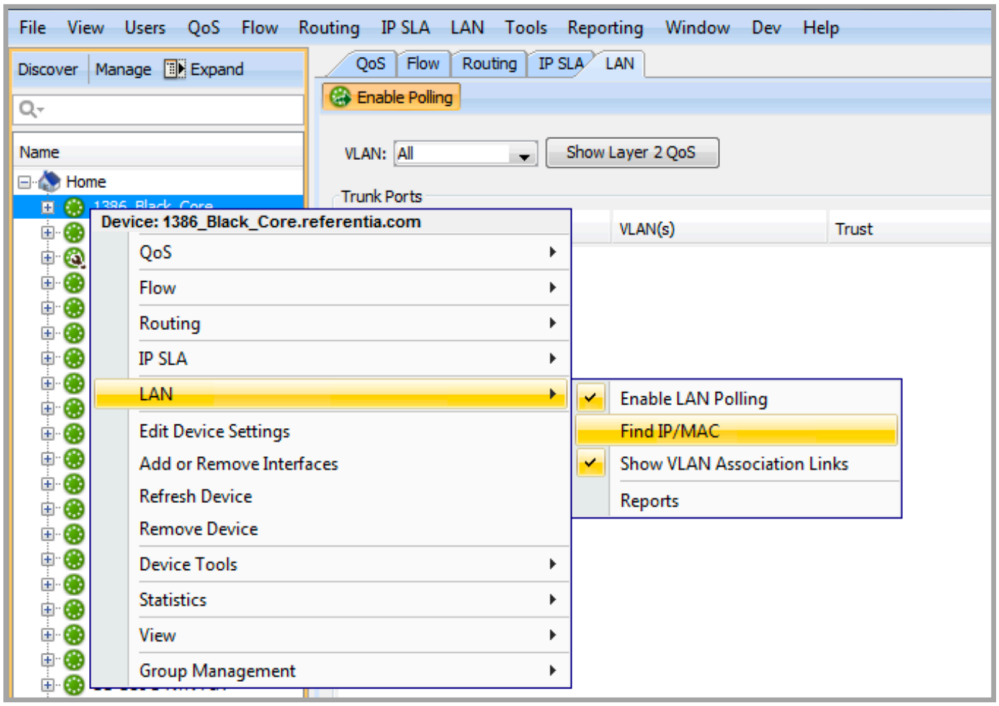
Find IP and MAC addresses

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.





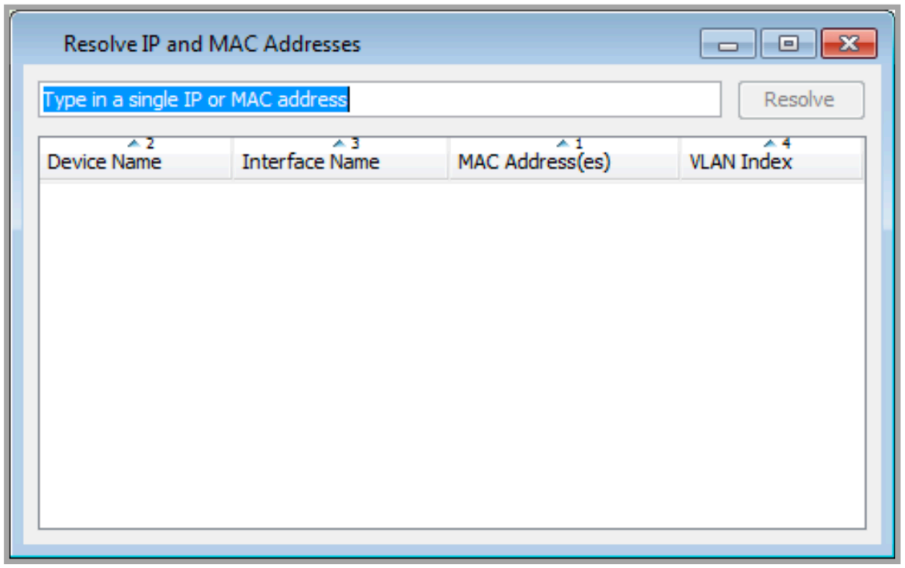
The Find IP/MAC command can also be found by right-clicking on a device in the topology view and selecting LAN > Find IP/MAC.



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

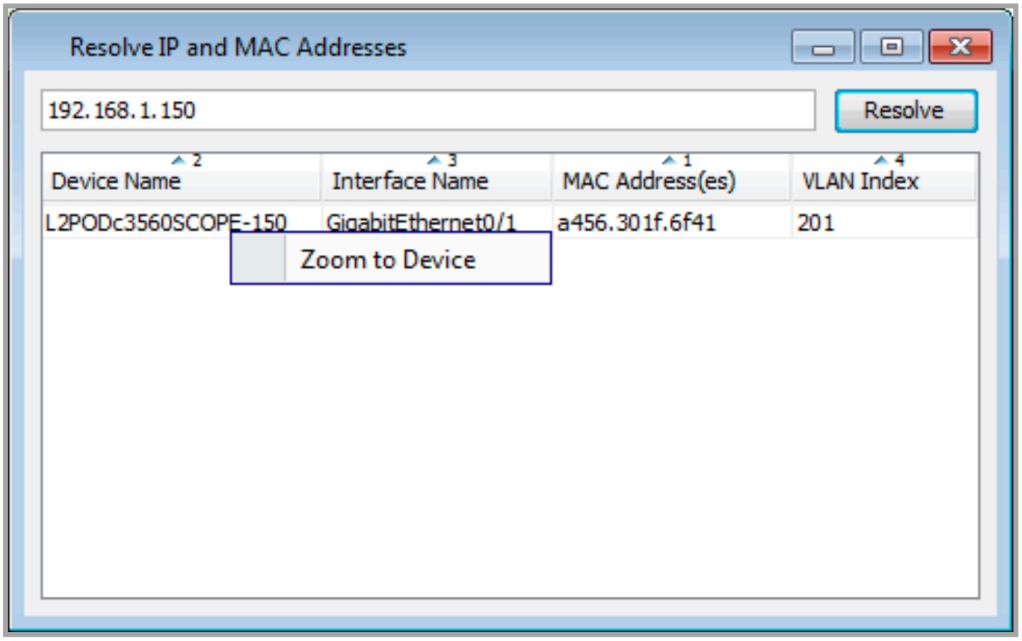
Type in the IP or MAC address in the top row of the Resolve IP and MAC Addresses table. Note that the text turns red until a valid IP or MAC address is entered. Click on Resolve to begin the search.



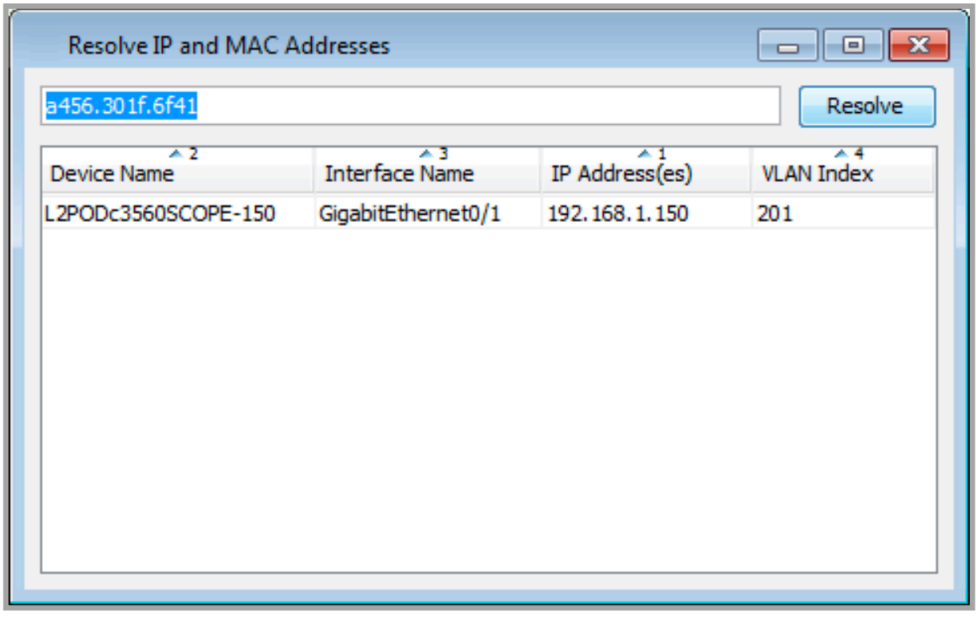
Entering an IP address will provide the MAC address and the device and interface closest to the IP or the actual device and interface if it is an IP on a device.

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.



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.



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

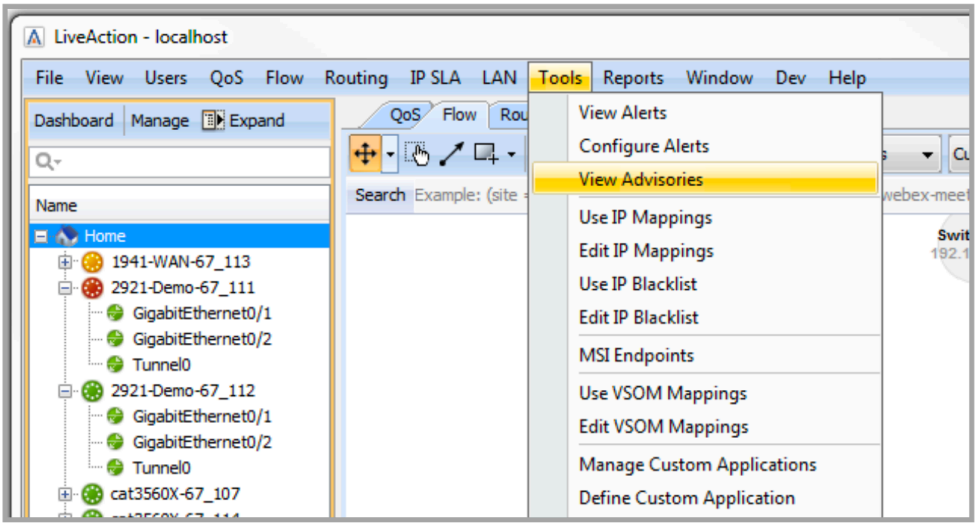
Tools

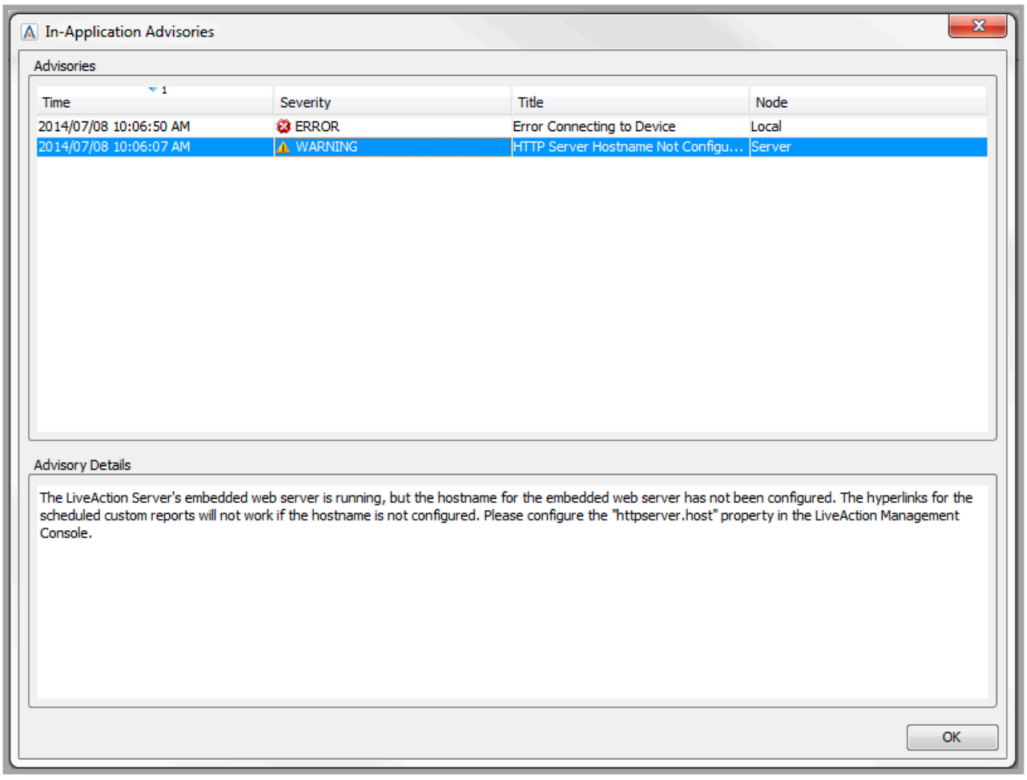
In this chapter:

Tools Overview

System Advisories

Notifications on abnormal server performance can be viewed in the Advisories Viewer. Select the viewer from Tools > View Advisories.



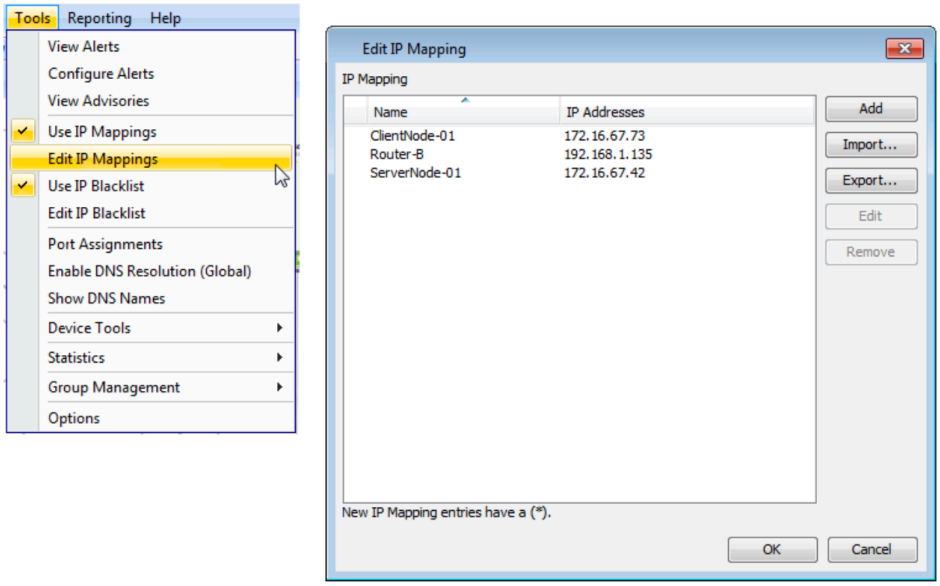


IP Mapping

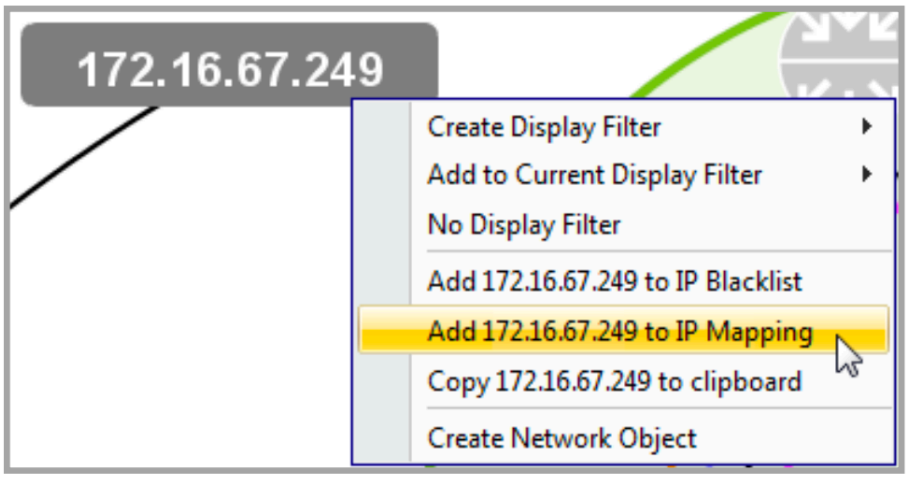
The IP Mapping feature allows the mapping of an IP address or hostname to a user-defined label. This feature only affects the labeling within LiveNX and does not affect any actual DNS or hostname configurations.

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.



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.



NOTE: IPv6 is not supported.

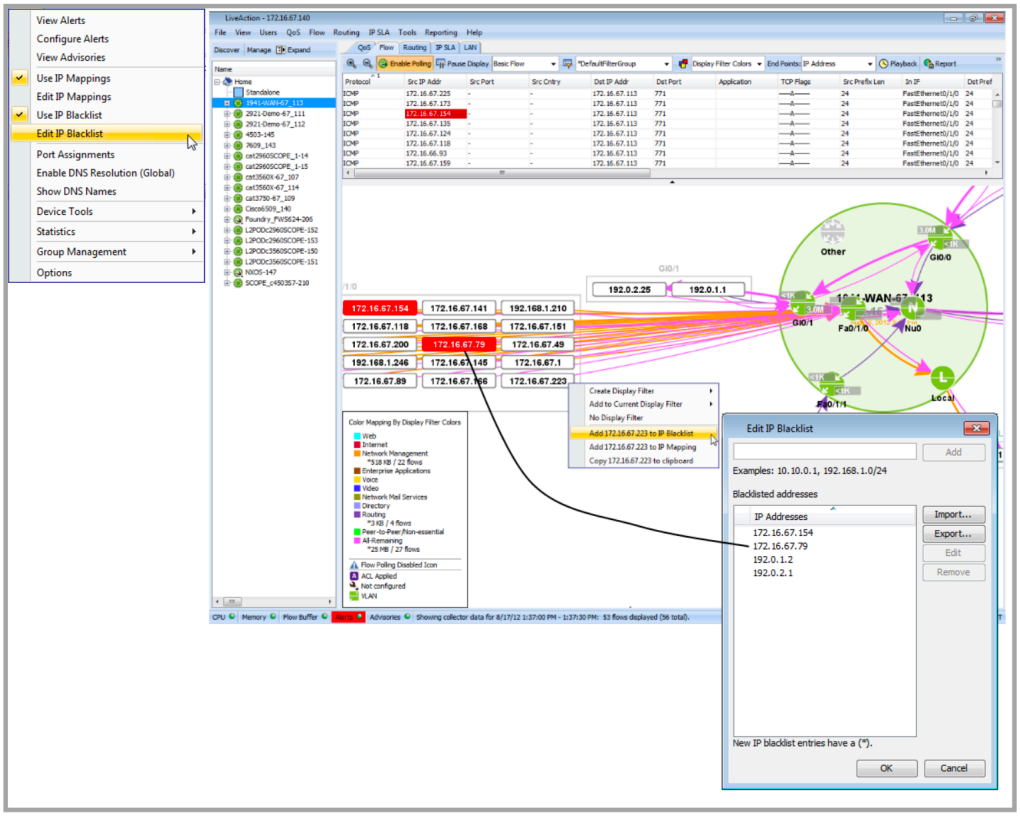
IP Blacklist

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.

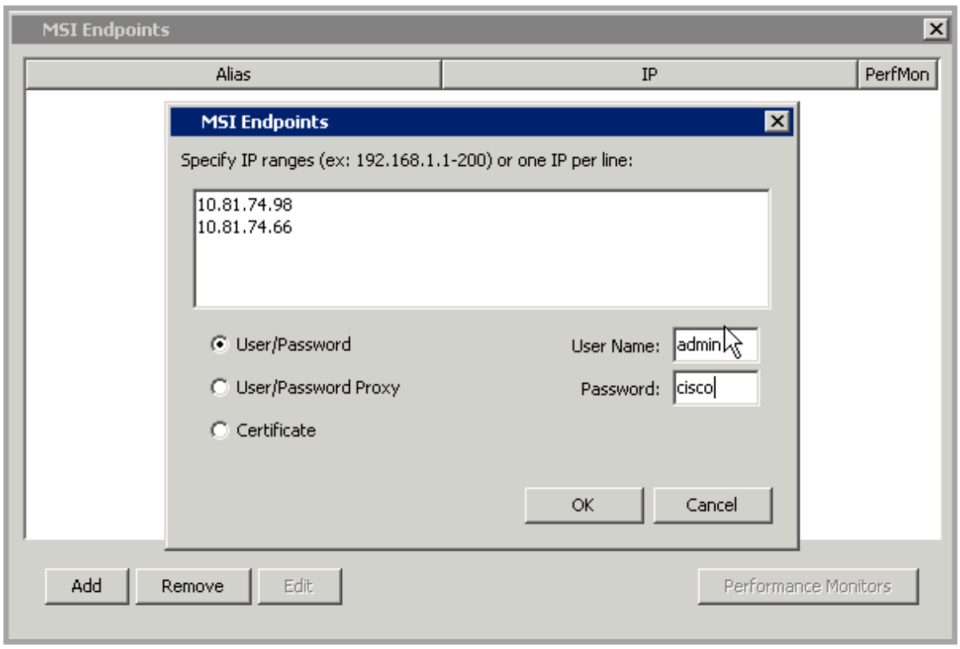


MSI Endpoints

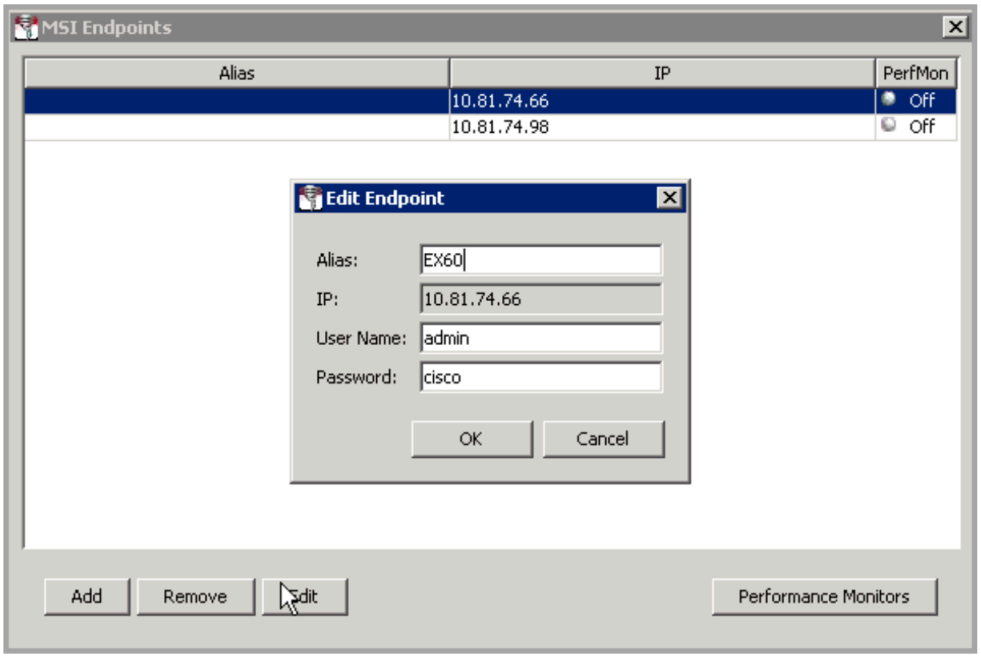
Media Services Interface (MSI) is used to provide better visibility and services to media applications.

To include MSI endpoints in your system topology, go to Tools > MSI endpoints.

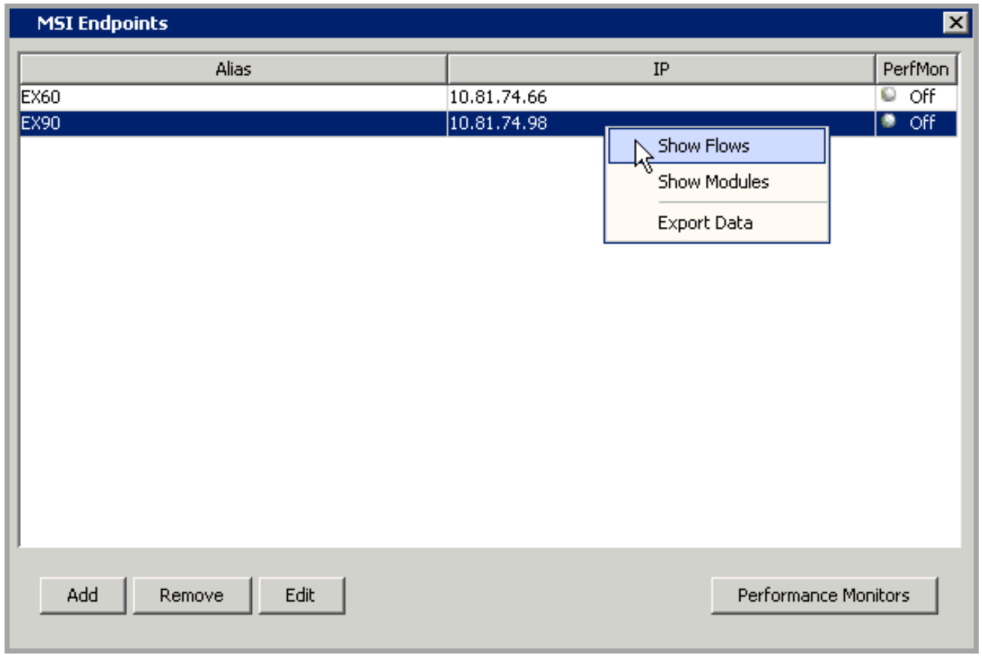
Click on Add, specify the IP addresses of your endpoints, select among User/Password, User/Password Proxy or Certificate and then complete the fields. Click on OK.



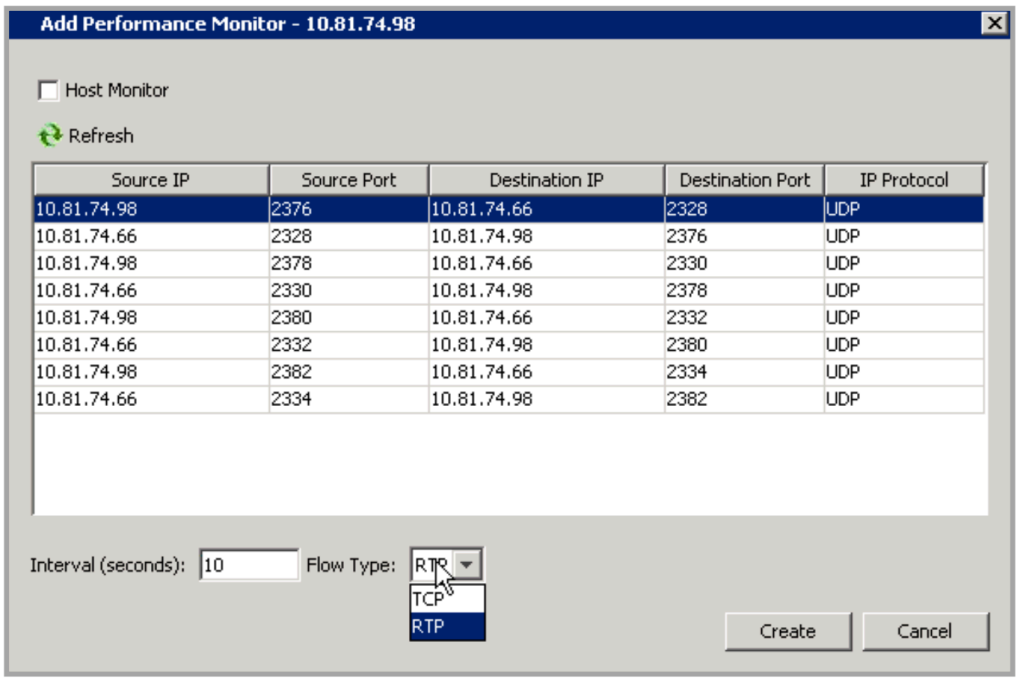
Click on the desired IP address and click on Edit to add an Alias.



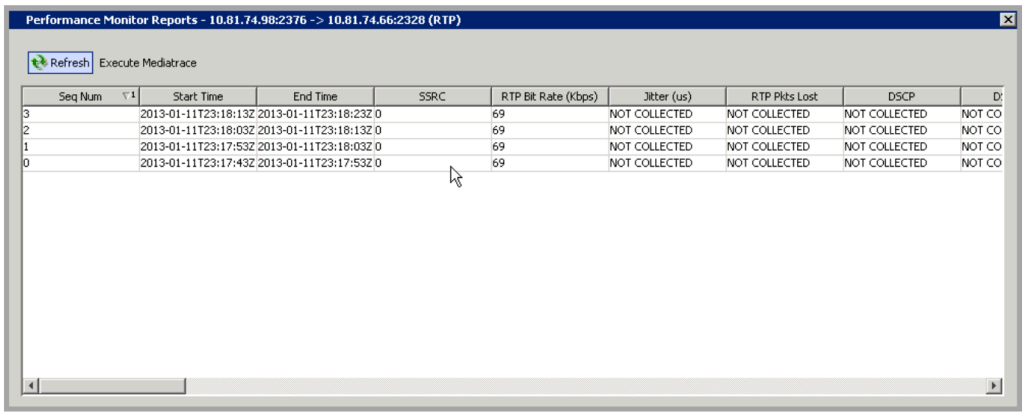
Right click on an individual endpoint to see flows, to show modules or to export data associated with that endpoint.



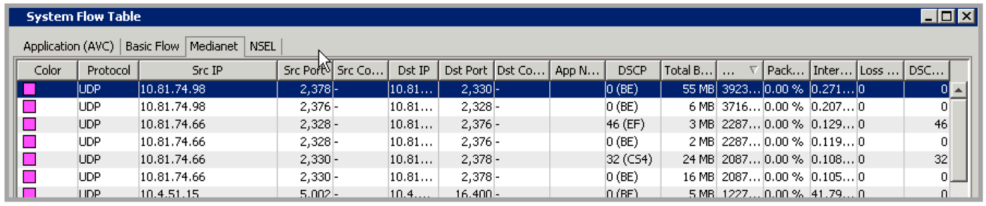
Return to the MSI Endpoints window, choose an MSI endpoint and then select Performance Monitors. Choose a time interval to monitor the data and then select either flow type Real-time Transport – RTP or Transmission Control Protocol – TCP.



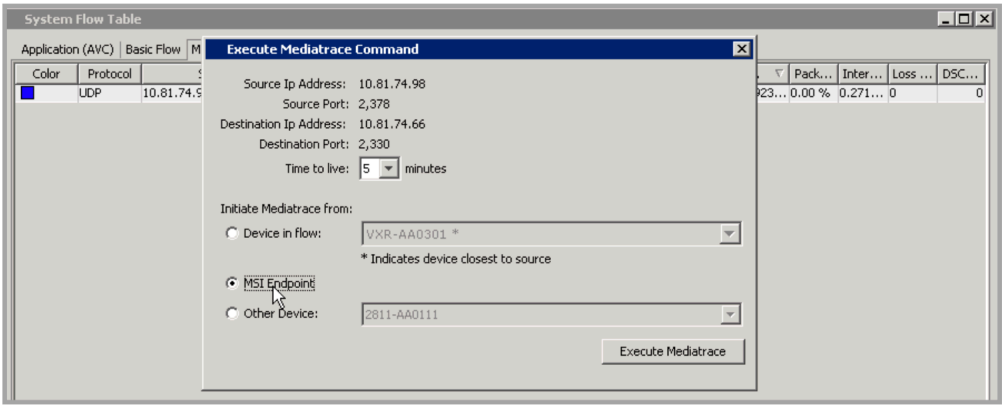
Select a flow, right click and select Show Reports to view the Performance Monitor Report. In this example, the test was run four times at ten-second intervals.



To get per hop performance data, go to the System Flow Table, click on the Medianet tab and then select the desired flow.



Right-click on the selected flow, choose Execute Mediatrace and select MSI Endpoint. Click on Execute Mediatrace.



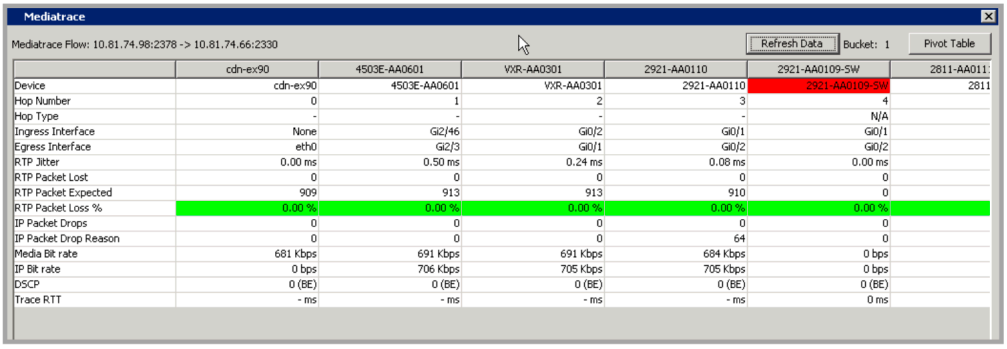
The Mediatrace report tabulates the performance data on a per-hop basis from source to destination.

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.

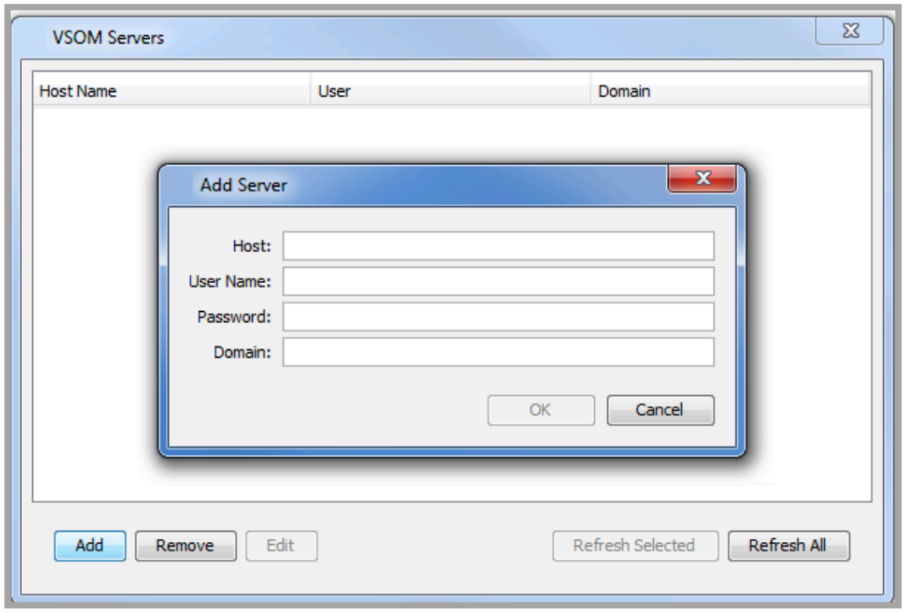
Click on Tools > Edit Vsom Mappings. Then click on Add. Type in the Host, User Name, Password and Domain information in the Add Server window. Click on OK. LiveNX will alert you if you did not add a VSOM server name or if you use incorrect login credentials. Click on Add to append multiple VSOM

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.



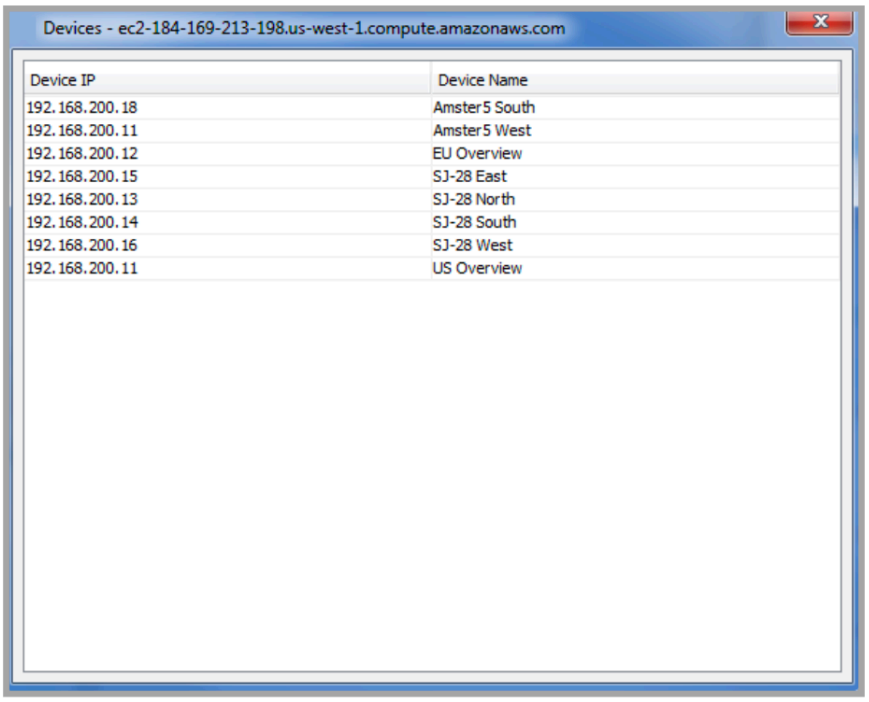
	cdn-ex90	4503E-AA0601	VXR-AA0301	2921-AA0110	2921-AA0109-SW	2811-AA011
Device	cdn-ex90	4503E-AA0601	VXR-AA0301	2921-AA0110	2921-AA0109-SW	2811
Hop Number	0	1	2	3	4	
Hop Type	-	-	-	-	N/A	
Ingress Interface	None	Gi2/46	Gi0/2	Gi0/1	Gi0/1	
Egress Interface	eth0	Gi2/3	Gi0/1	Gi0/2	Gi0/2	
RTP Jitter	0.00 ms	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.



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.



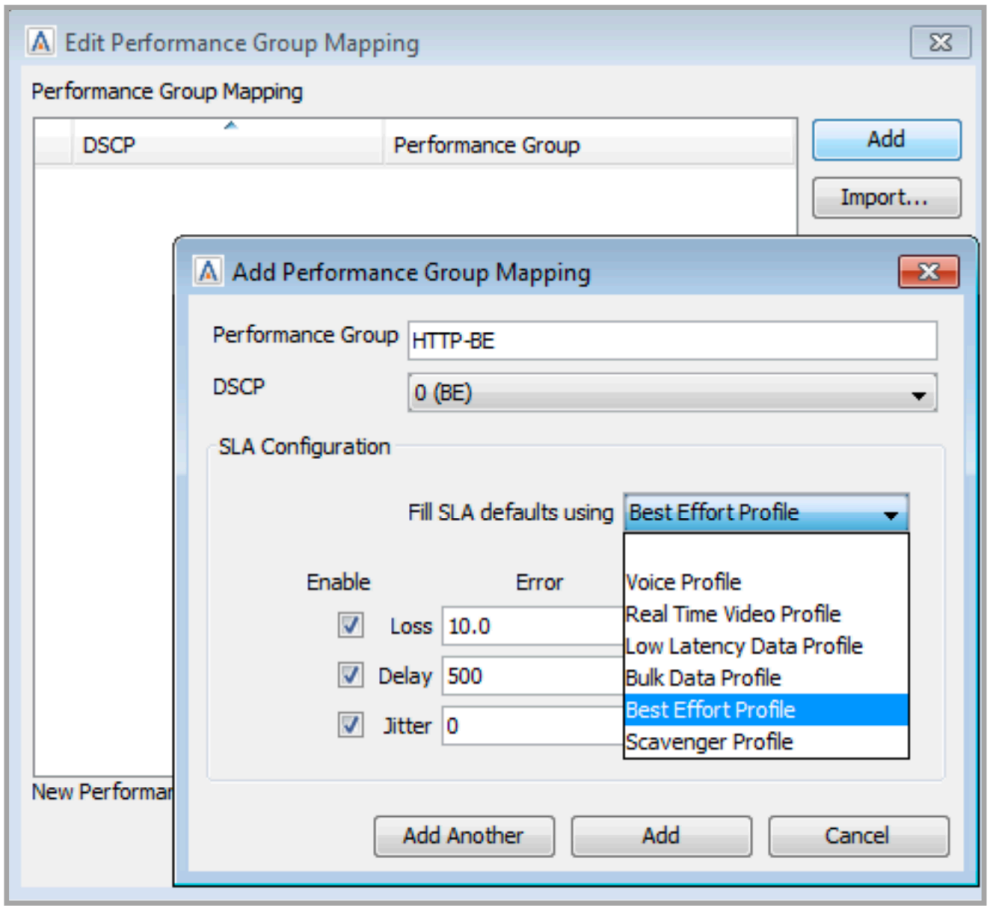
Export Data: LiveNX generates a .csv file listing the VSOM Servers Host Names, User & Domain Names.

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.



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.

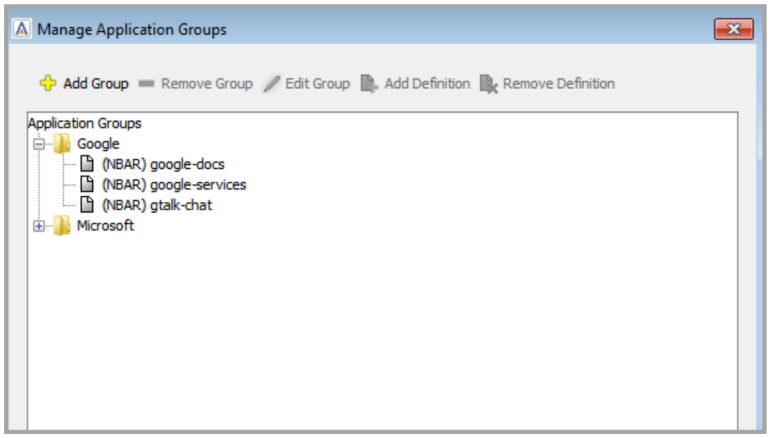
Click on OK when complete.

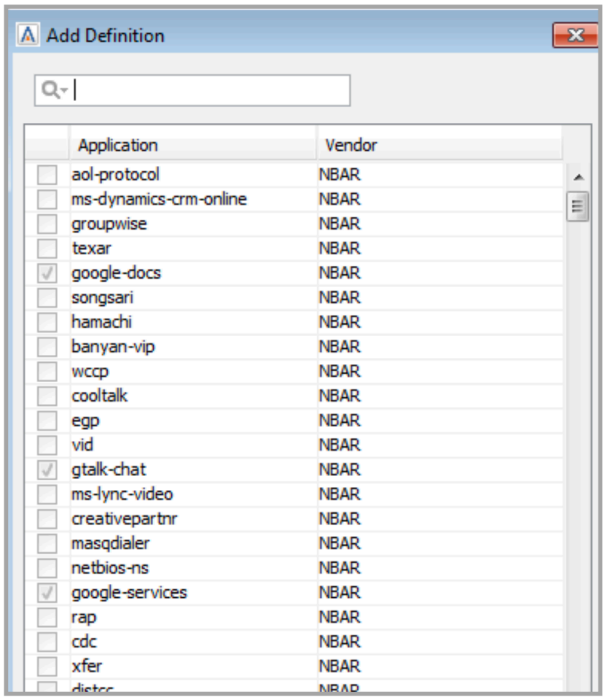
Click on an Application Group and select Remove Group to remove this group from the list.

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.



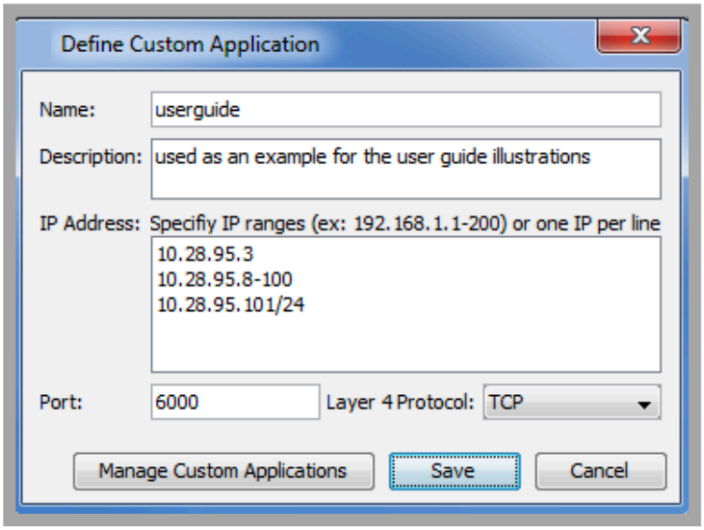


Manage/Define Custom Applications

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.



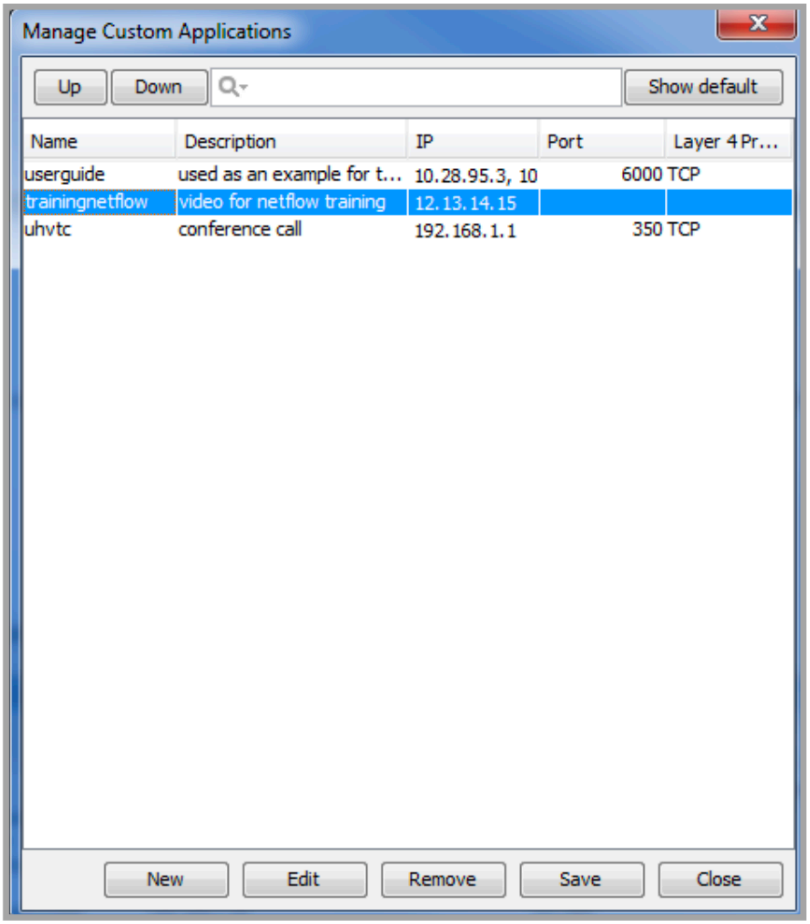
Adding both an IP Address and a Port Number will define your custom application to the defined IP address AND port number. If both IP Address and Port Number are used, define the Source IP Address with the Source port or the Destination IP Address with the Destination port.

If you specify both port and address, the mapping only works for (source IP and source port) or (destination IP and destination port) combinations.

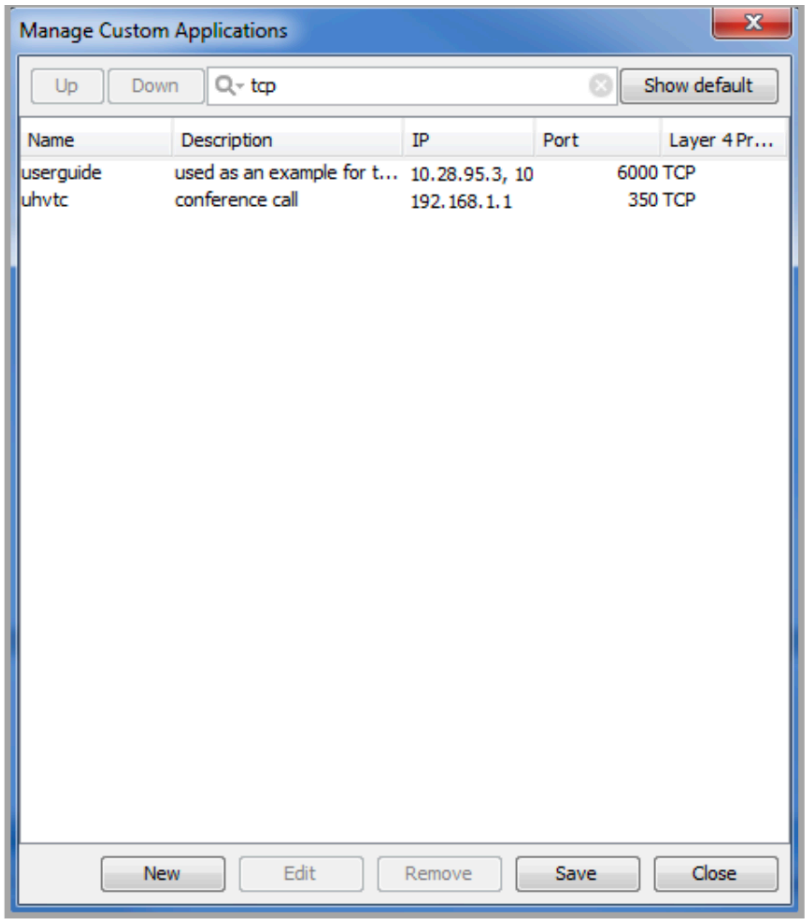
Click on Save to add this to your custom application list.

To review or to edit your list of custom applications, go to Tools > Manage Custom Applications.

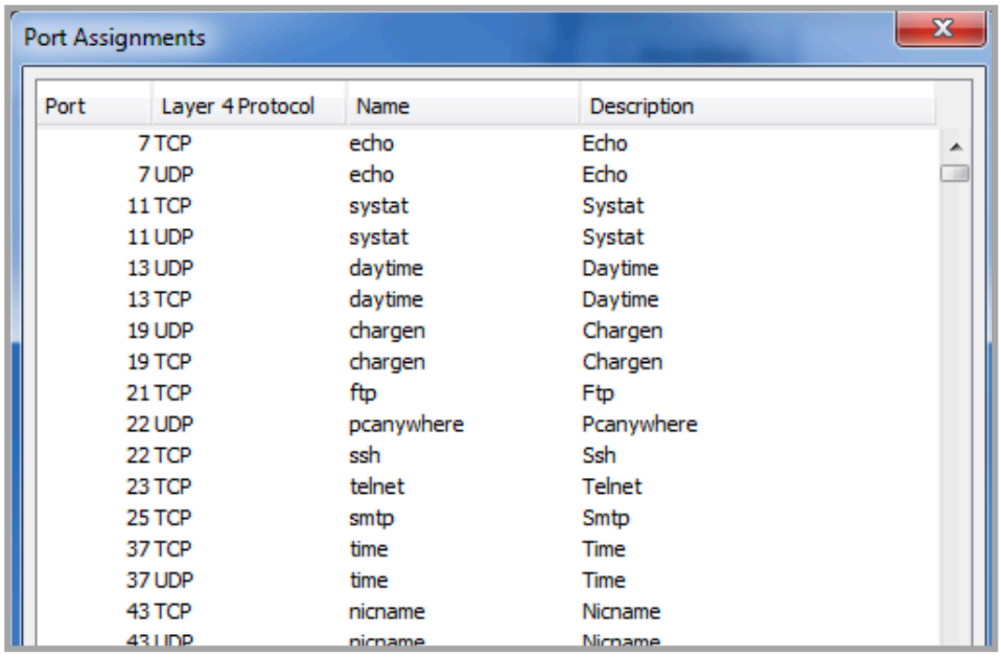
Highlight a row and click on the Up or Down button to move the table entry higher or lower in the list. The order defines precedence of that particular custom application. In cases where there are multiple application names for the same IP address, the higher placed item takes precedence.



The header row with the magnifying glass filters the list based on the defined alphanumeric string.

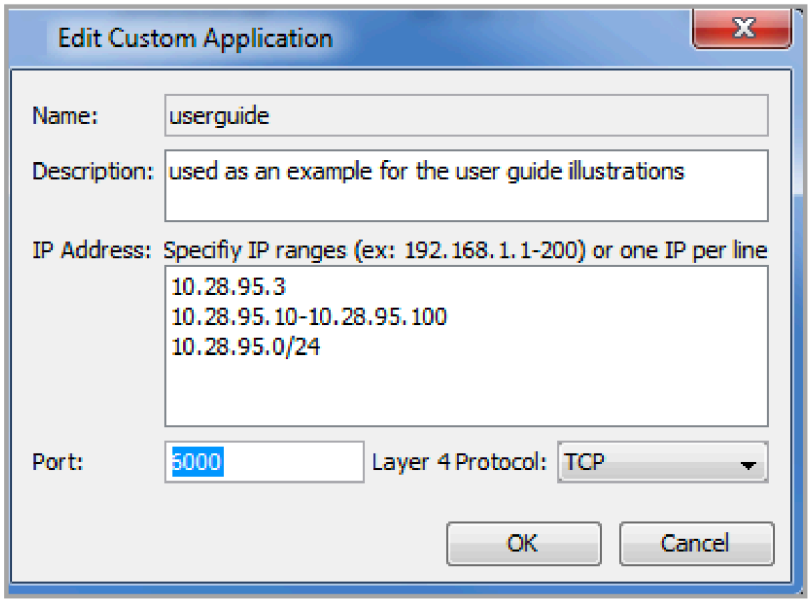


Click on Show default to list a table of the common port assignments. The table is shown below. Any port assignment defined in the Custom Application takes precedence over the common port assignment.



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.

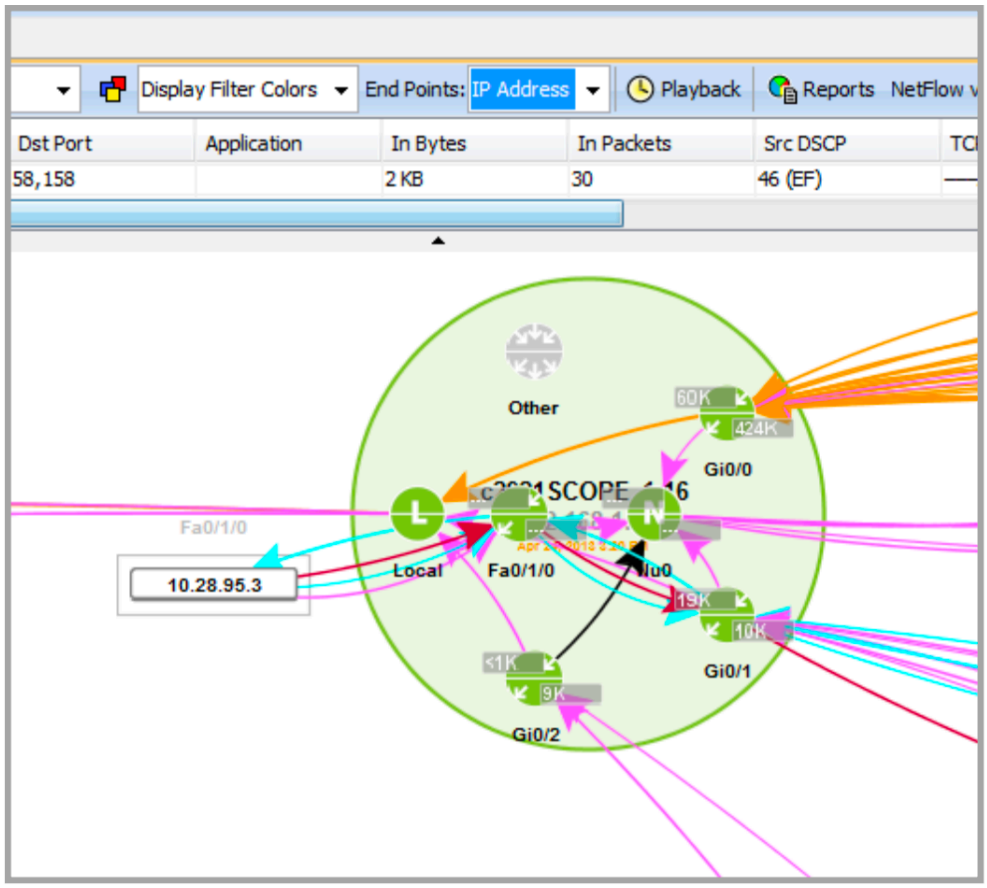


Click on a user-defined Custom Application and click on Remove to remove the custom application from the list.

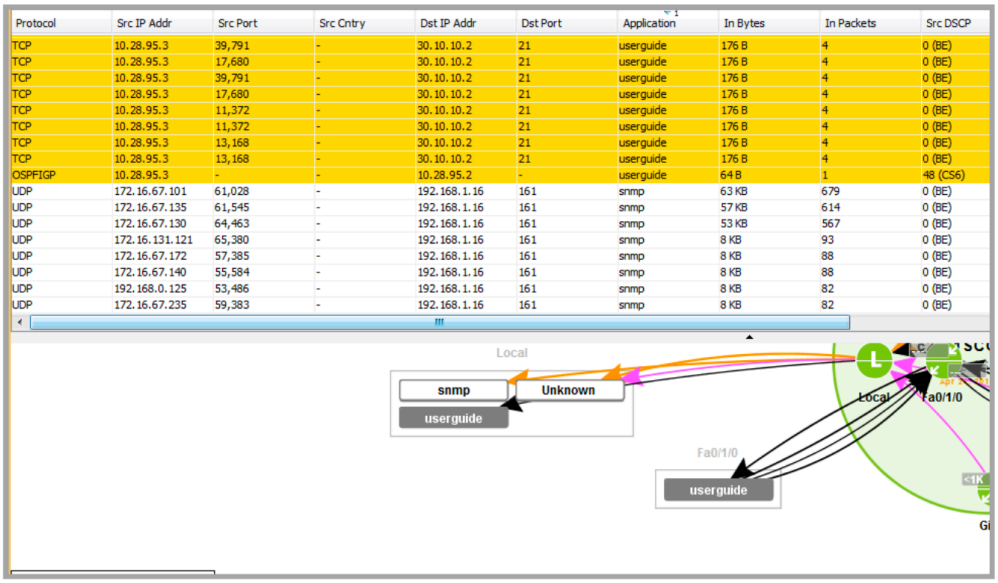
Click on Save to save the custom application list. This list is viewable by all the LiveNX user roles.

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.

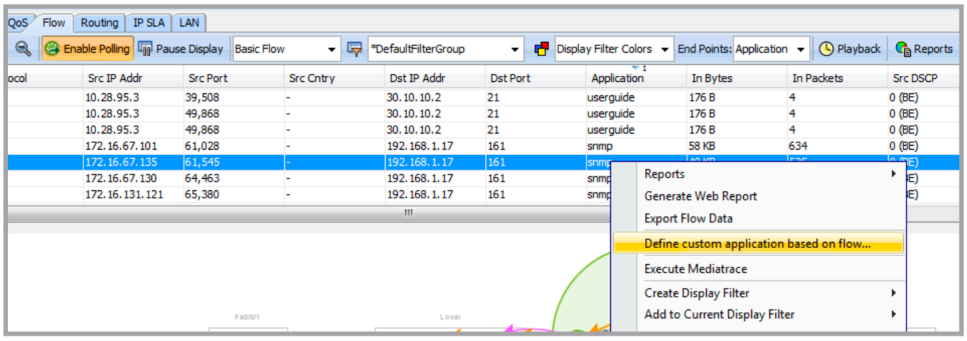


Click on the custom application name in the device view to highlight all custom applications of that type in the flow table.

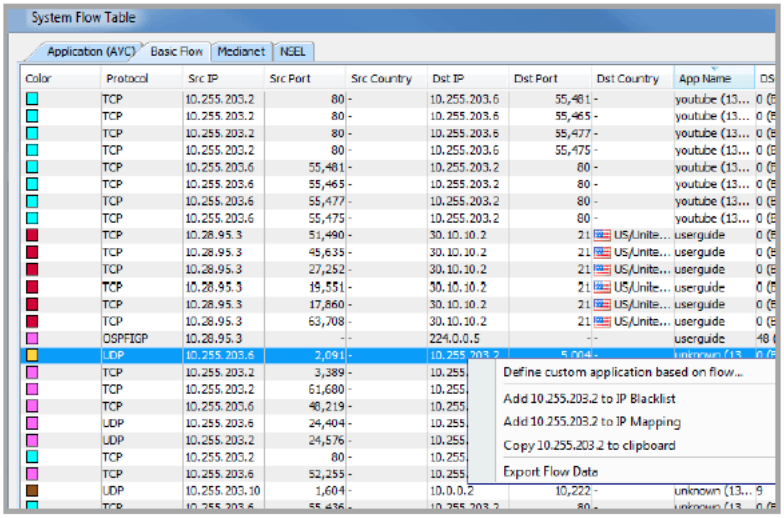


The custom application can also be configured directly from either the flow table in the device view or in the System Flow Table.

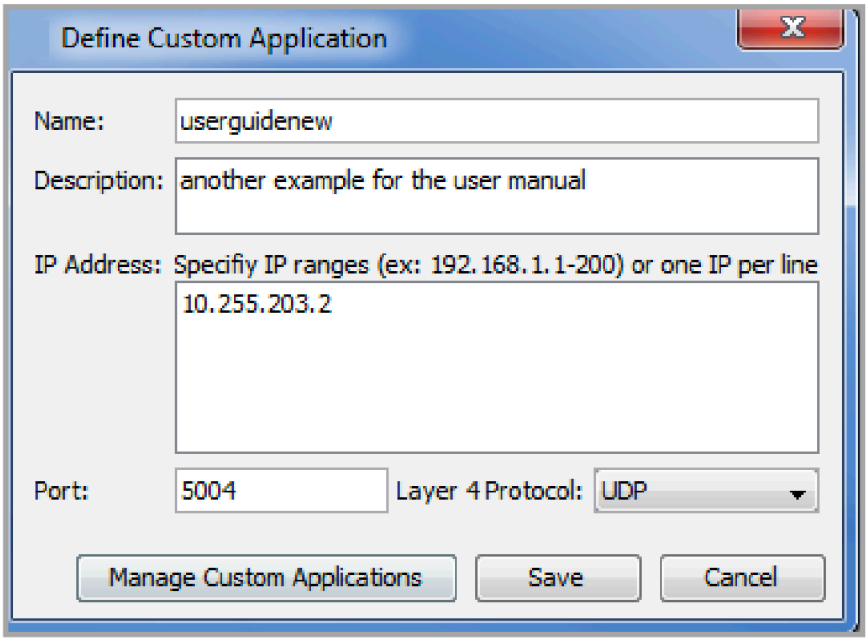
Right click on a flow in the flow table and click on Define custom application based on flow…to bring up the Define Custom Application window.



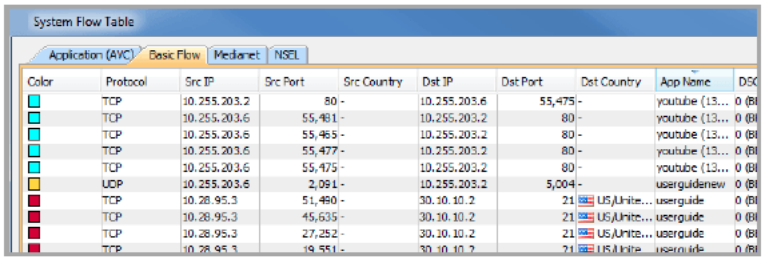
Right click on a flow in the System Flow Table and click on Define custom application based on flow… to bring up the Define Custom Application window.



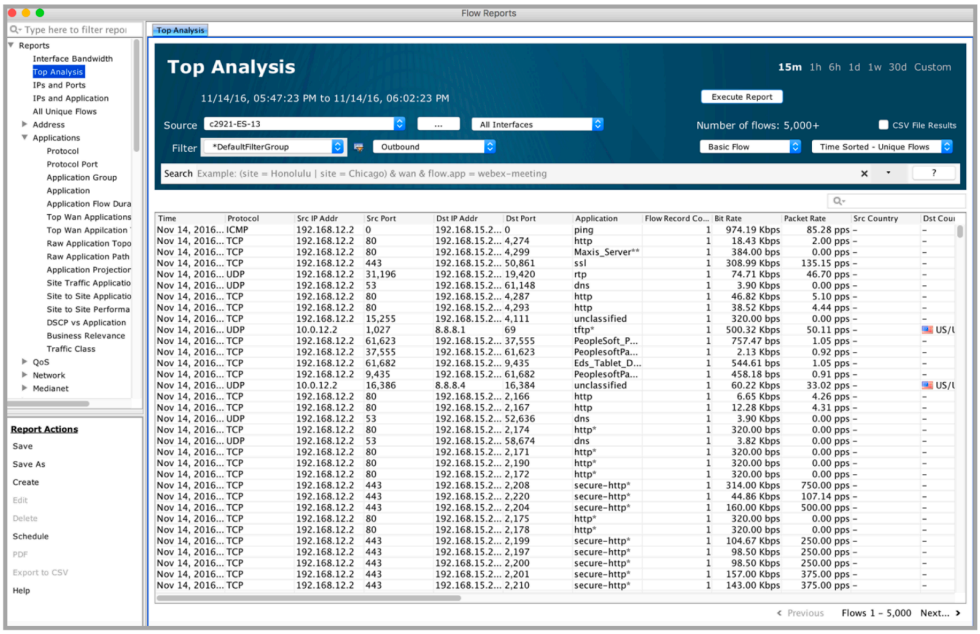
In both these cases, the Define Custom Application window automatically fills in the IP Address and the Port field based on that particular flow's destination IP address and destination port.

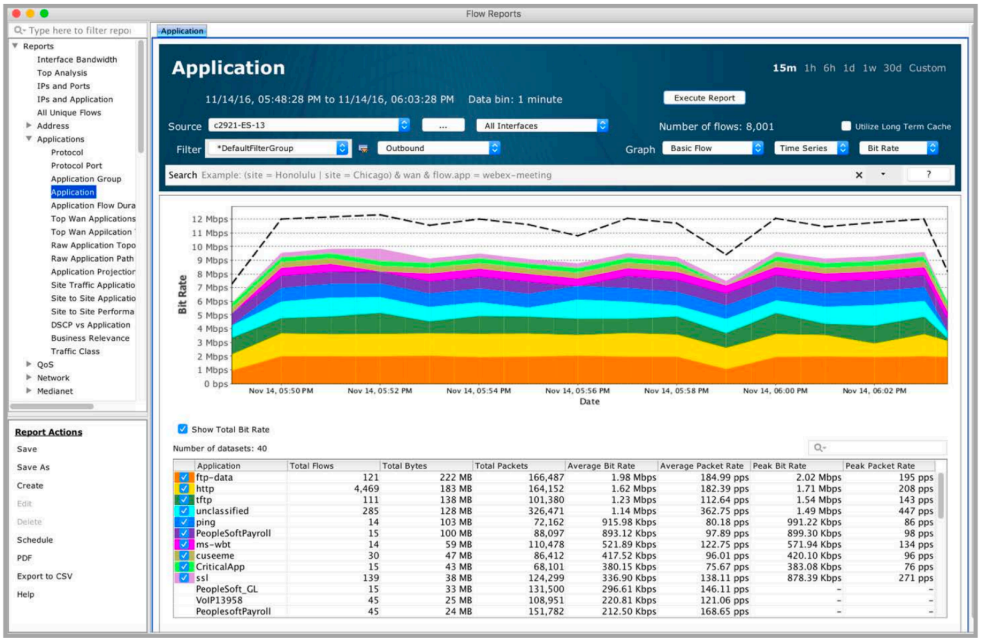


Click on Save and the new application name is visible in the flow table.



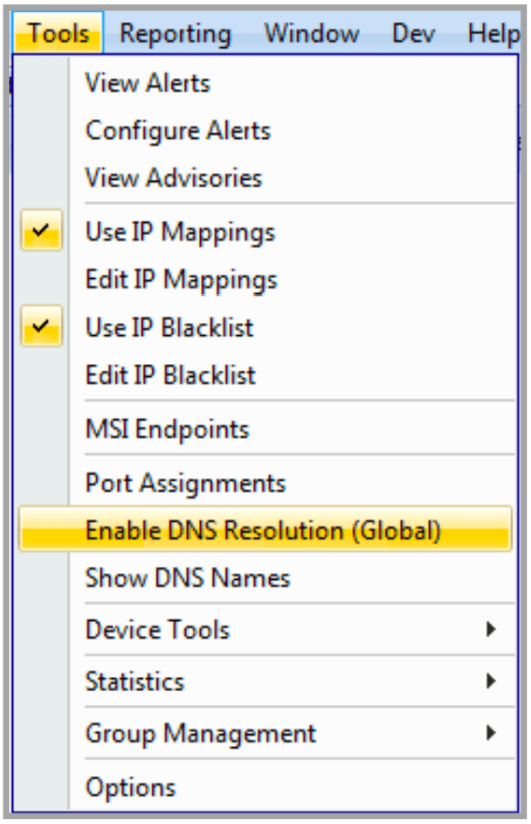
The defined custom application name appears in the Top Analysis and the Applications flow reports under Applications.



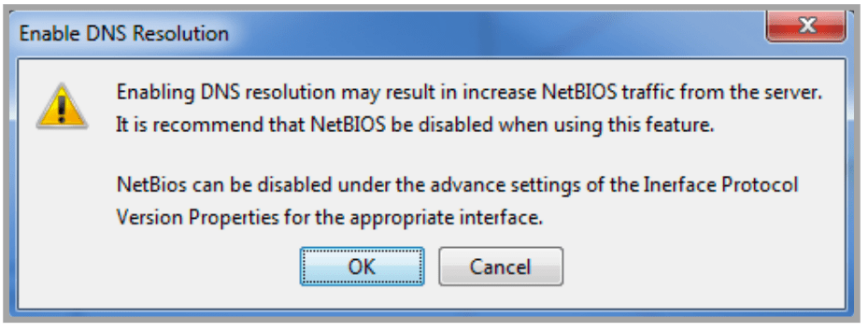


DNS Name Resolution

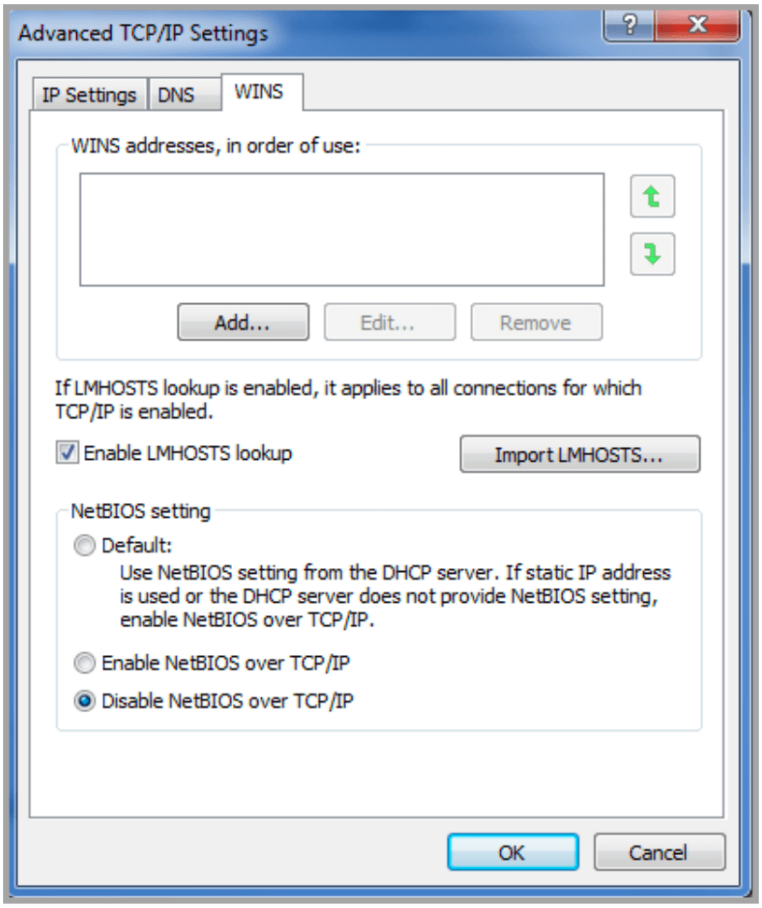
The DNS Name Resolution features allows the display of host names associated with the IP addresses in LiveNX. An admin user can enable DNS Name Resolution by selecting Tools > Enable DNS Resolution (Global).



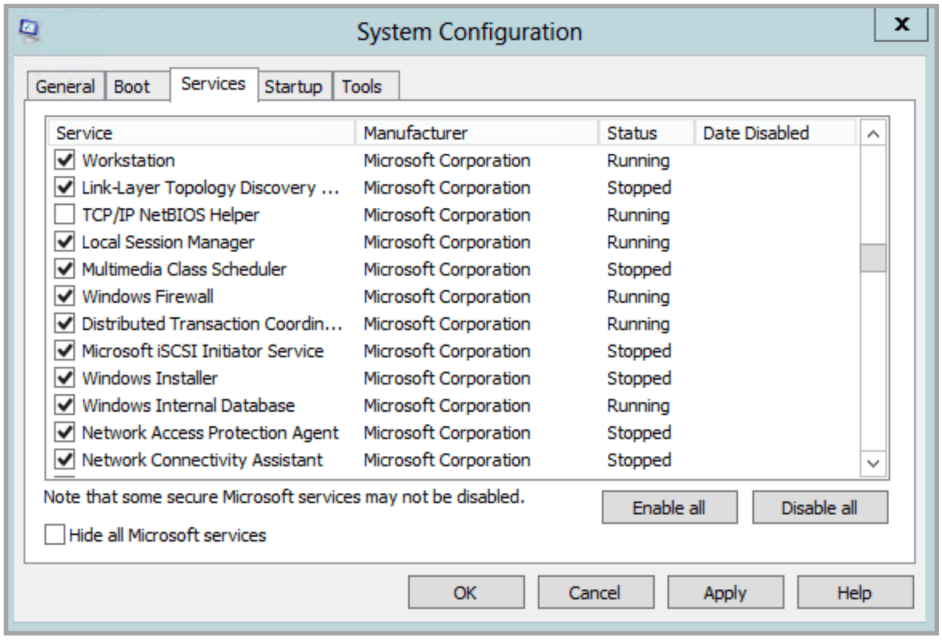
Once enabled, a check box will appear next to the Enable DNS Resolution (Global). To disable, select Tools > Enable DNS Resolution (Global). Prior to enabling DNS resolution, an alert appears to warn you that this may increase the amount of NetBIOS traffic from the server.



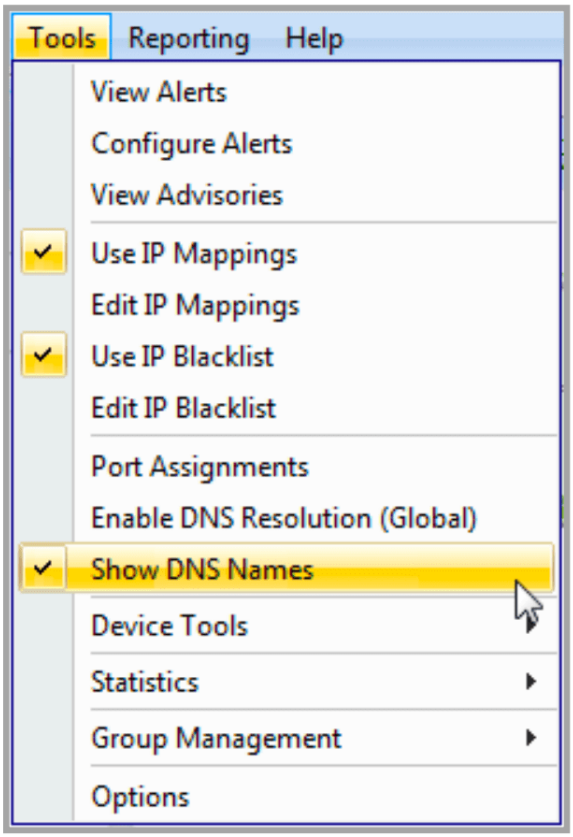
To disable NetBIOS for Windows7 operating systems, open the Network and Sharing Center in the Control Panel. Click on the appropriate Local Area Connection. Click on Properties, then TCP/IPv4, then Properties. Click on Advanced and then go to the WINS tab and select Disable NetBIOS over TCP/IP. Click on OK.



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.



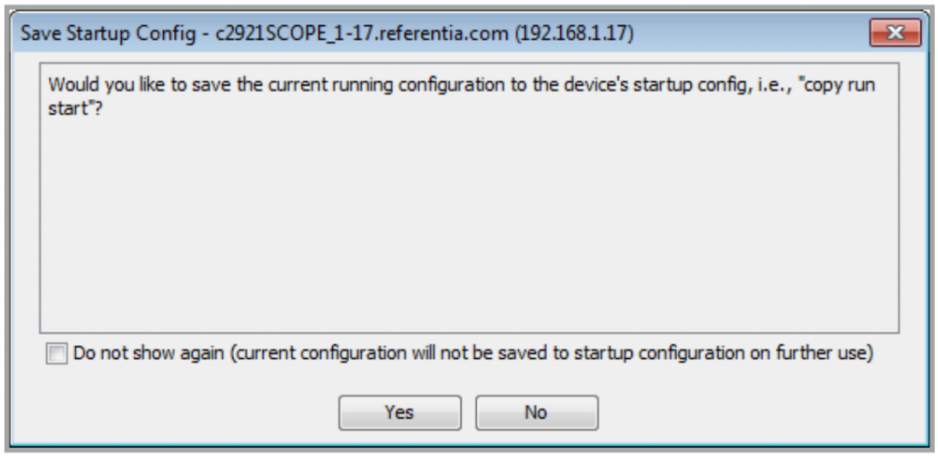
Once DNS Resolution is enabled, any user role can select Tools > Show DNS Names to show hostnames in the flow views (system and device view topology, flow tables, lists and reports).



Device Tools

Saving Changes to the Device's Startup Configuration

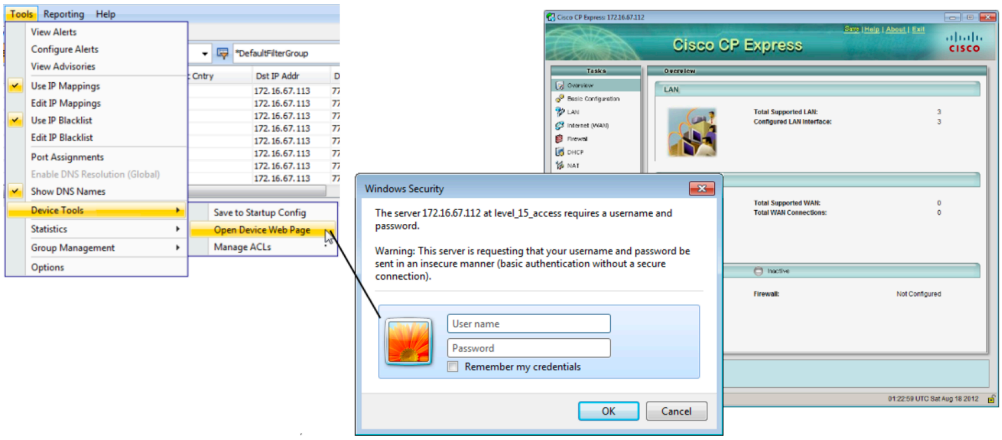
When a device is added to LiveNX, the software makes changes automatically to the device's running configuration, but not to the startup configuration file. If you want to make these changes permanent, select the device from the list on the left side of the LiveNX screen, and then select Save to Startup Config from the File menu and click Yes to save them to the startup configuration file.



Accessing the Device Web Page from LiveNX

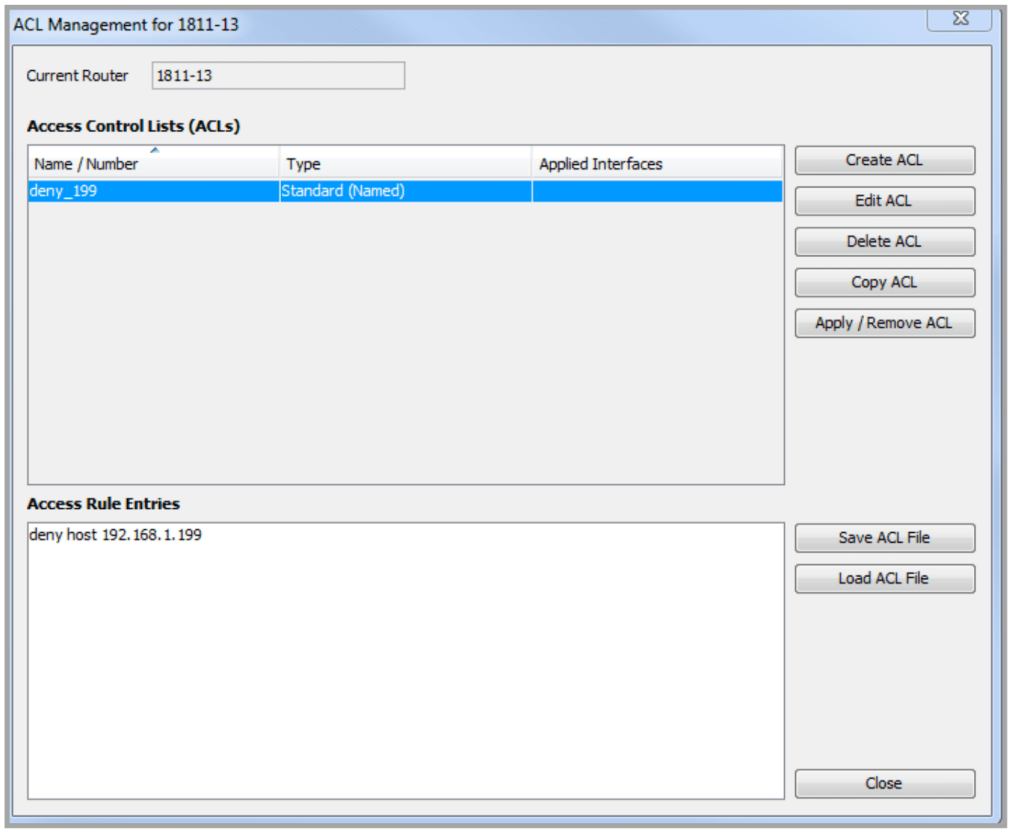
If your device supports it, LiveNX can open its internal web page. Select Open Device Web Page from the Tools menu.

Note Administrator or Full Configuration privileges are needed to open and use the LiveNX CLI terminal window.

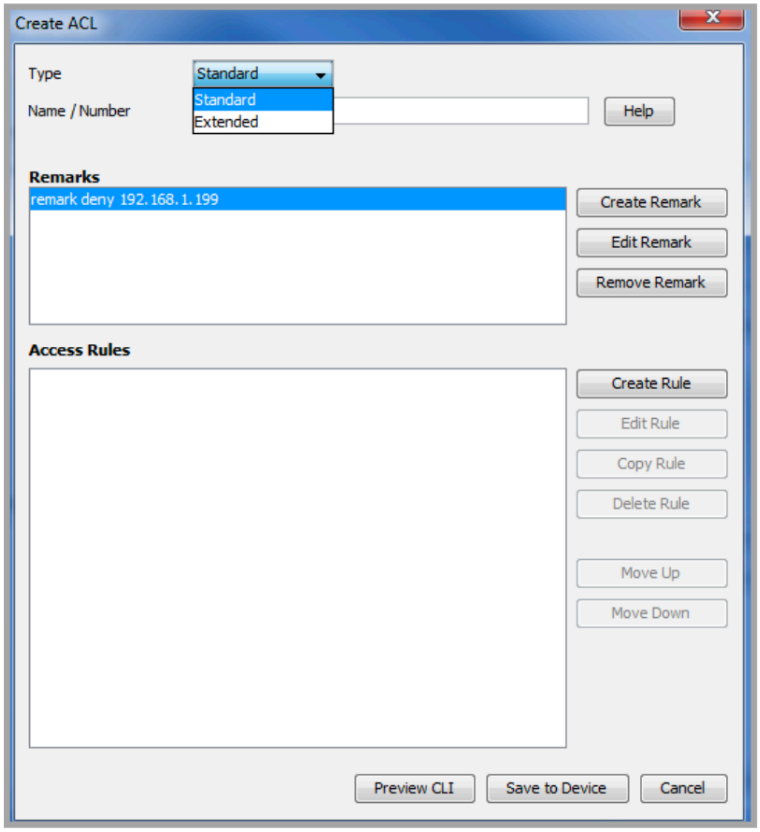


Managing ACLs

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.



To create an ACL, click on Create ACL.

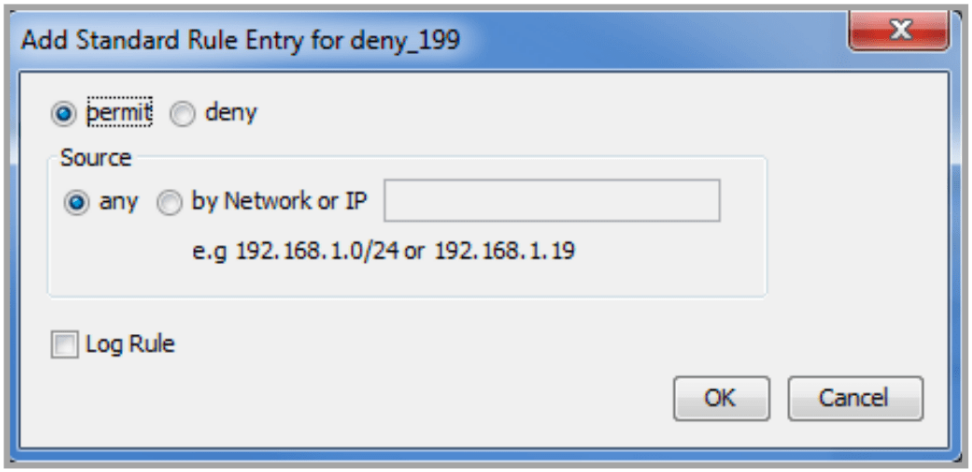


Choose between Standard or Extended. Standard uses ACL numbers between 1-99 or 1300-1999. Extended uses ACL numbers between 100-199 or 2000-2699. Alphanumeric characters are allowed in the Name/Number field with no blank spaces.

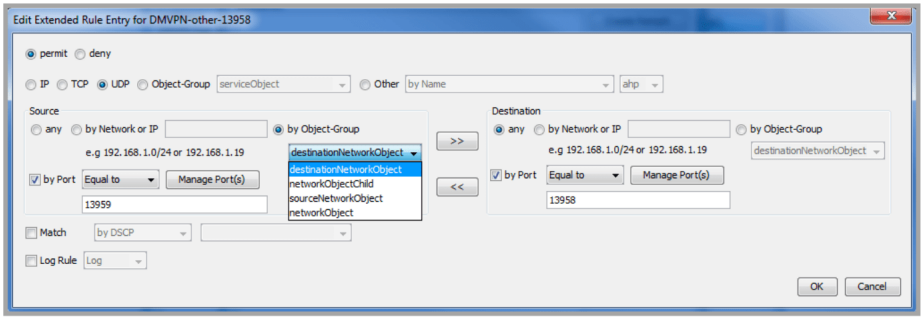
Click on Create Remark to create a remark for the ACL.

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.



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.

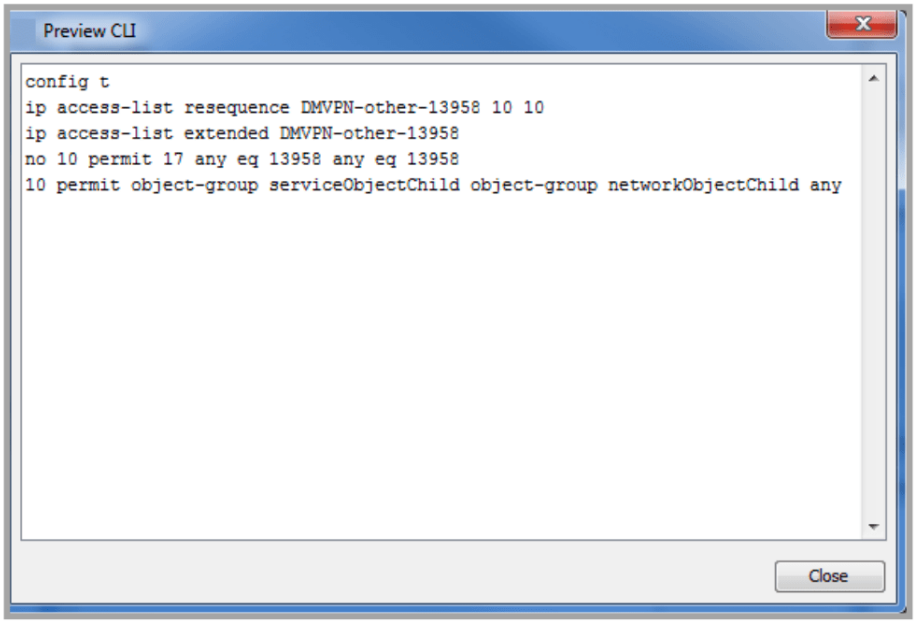


LiveNX reads the Object-Group information already created in the device configuration and displays any available selections through the drop-down.

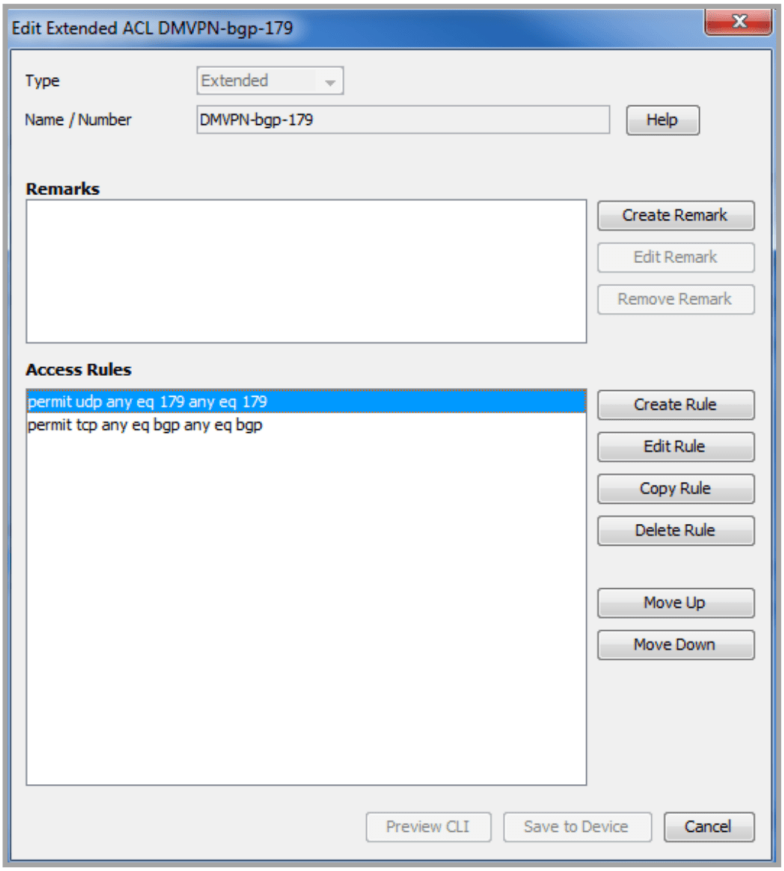
The by Port selection is available if either TCP or UDP is selected. Options are equal, not equal, greater than, less than or between. The Manage Port(s) button provides a list of commonly used ports. Different rules can be created for Source and Destination. Use the >> if you would like to copy the 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.

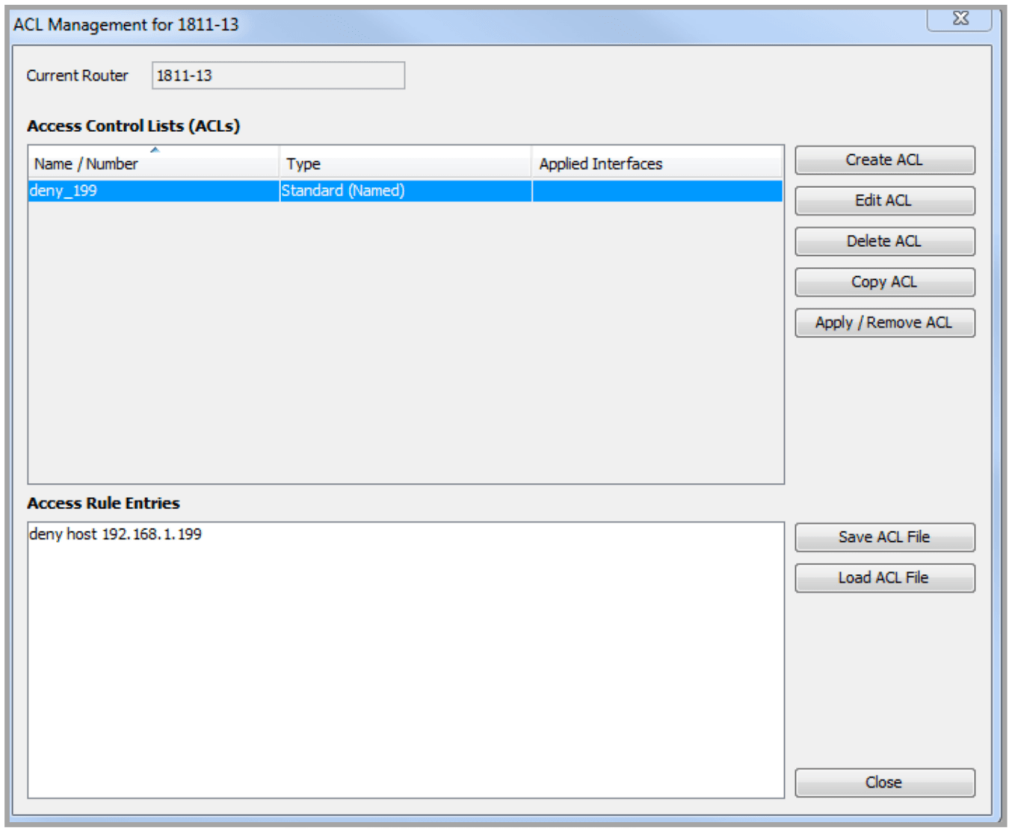
Click on Log Rule and select either Log to Log matching packets or Log Input to Log the ingress interface and source MAC address, in addition to the packet's source and destination IP address and ports. Default is off. Click on Preview CLI to see the commands in CLI format prior to saving it to the device. 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.



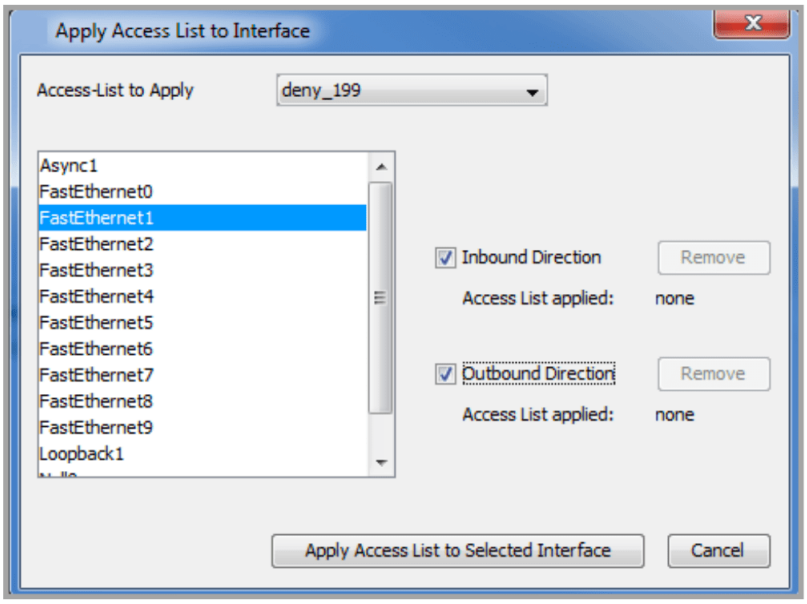
Once a rule is created for the ACL, highlight the rule to edit, copy or delete the created rule. Repeat the Create Rule to add additional access rules for a given Access Control List. Rules are executed in the order from the top down, so highlight a rule in the list and use the Move Up or Move Down button to reorder the rules in the Access Rules window.



Once the Access Control List is saved to the device, click on Apply/Remove ACL.

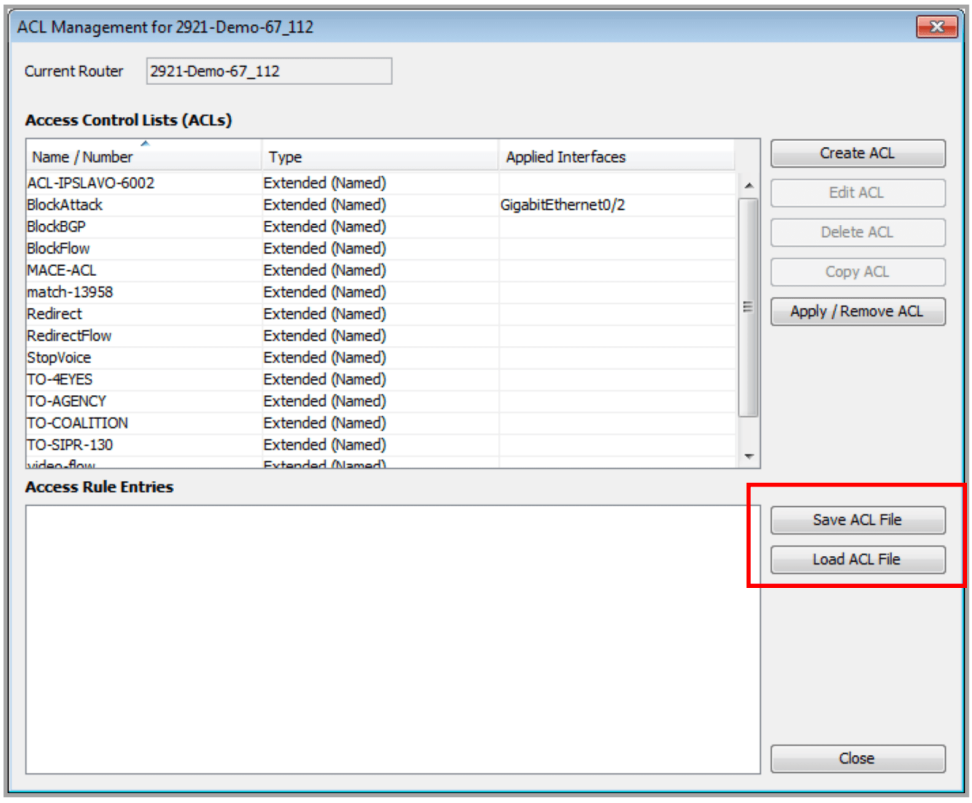


The Apply Access List to Interface window automatically lists all interfaces on that device. Click on the desired interface to apply the interface to, select Inbound Direction and/or Outbound direction and click on Apply Access List to Selected Interface to designate the desired ACL. The UI will ask if you are sure before modifying the interface configuration.



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.

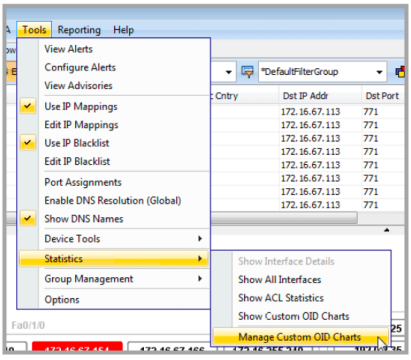
To load an ACL file from one device to another, save the ACL to a file and then open the editor on the target device. Then, load the ACL file and save it to the device. LiveNX will warn if there are any conflicts.

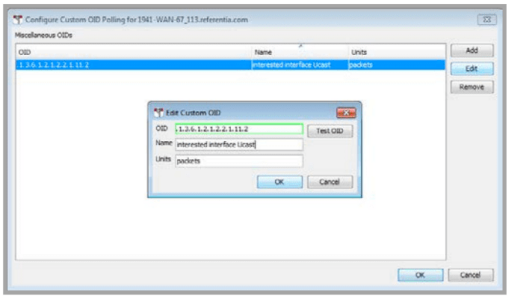


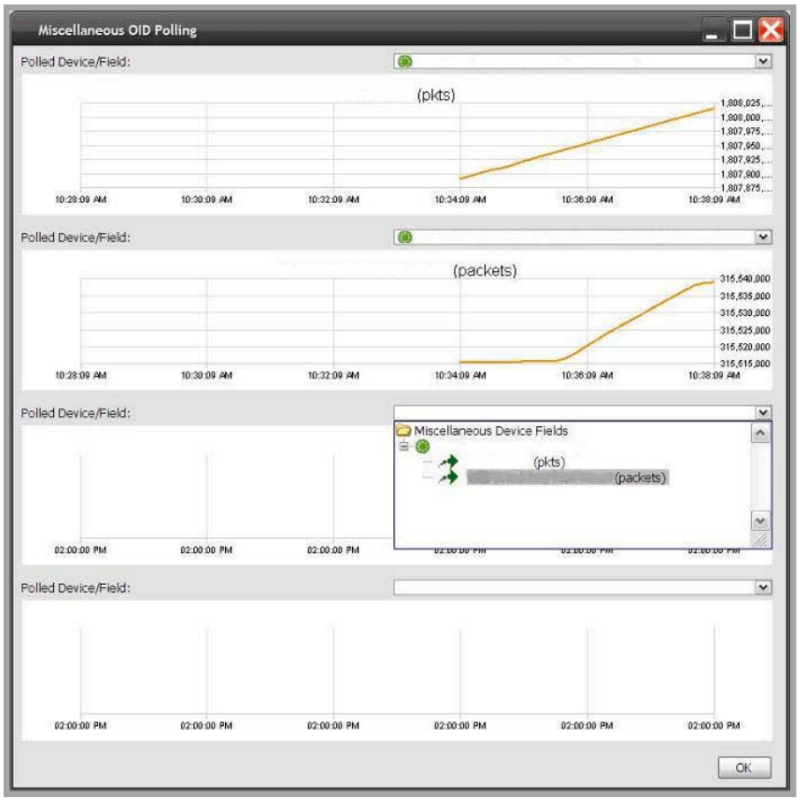
Statistics

Miscellaneous OID Polling and Charting

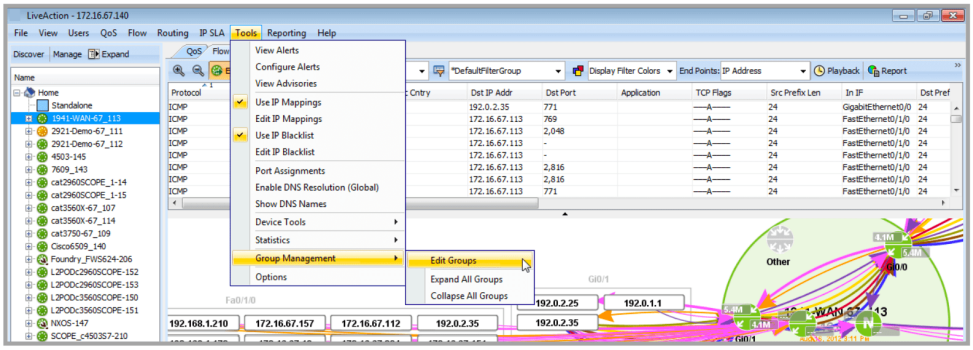
Miscellaneous OID polling utilizes a generic polling framework within LiveNX to gather vendor-specific or miscellaneous device information and statistics. From the Tools menu, select Statistics > Manage Custom OID Charts and enter in the OID string. Polled data and charts are accessed by going to the Tools menu and selecting Statistics > Show Custom OID Charts.



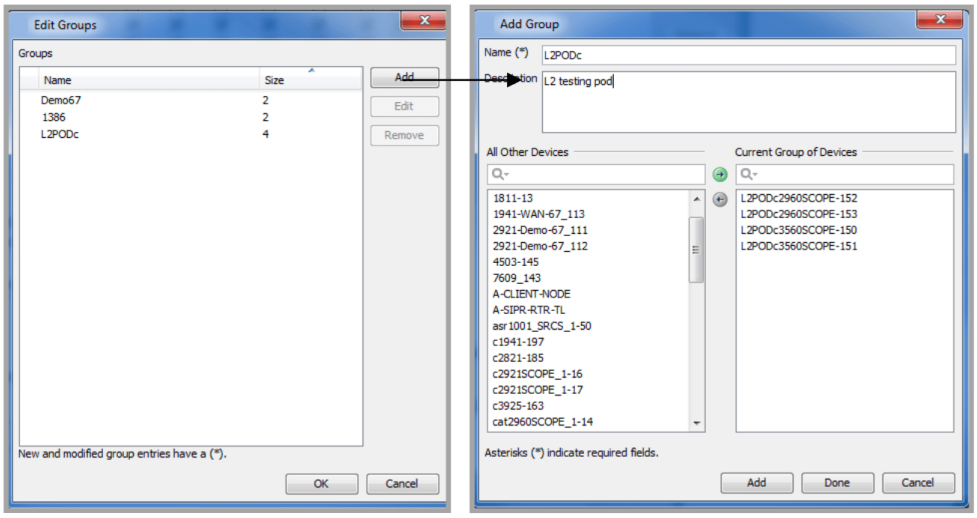




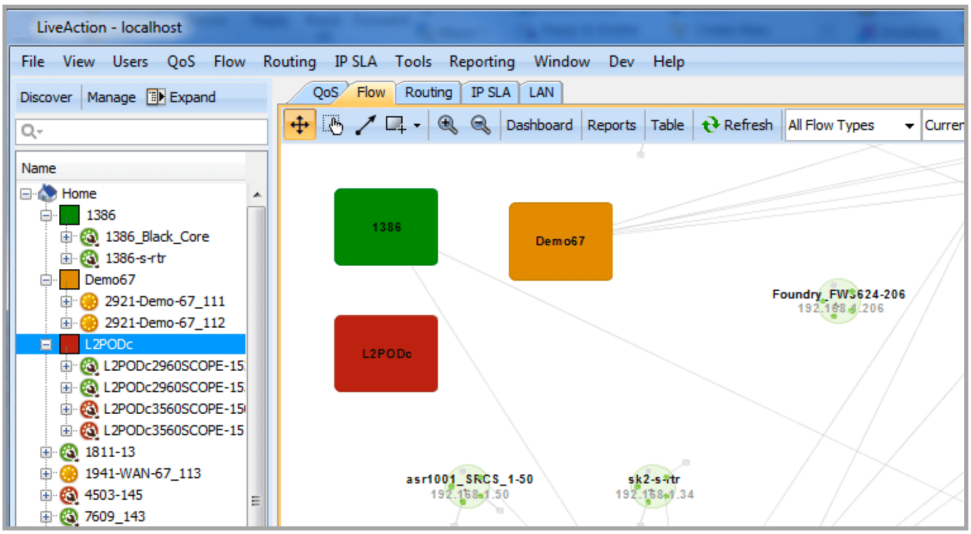
Group Management

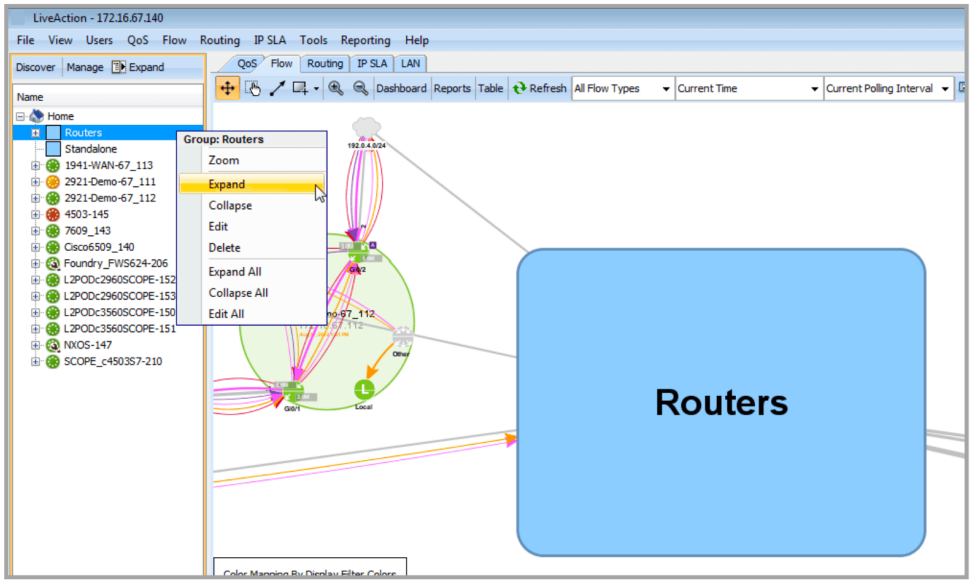


Create a new group by selecting the Add button, naming your group and adding devices to it. Use the scroll bars to find the devices in the list or type in the start of the device name in the field to the right of the magnifying glass to filter the list. Click on the magnifying glass to enable additional tools (case sensitive, wild cards, partial matches) to assist in filtering the list.



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 right-clicking 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.





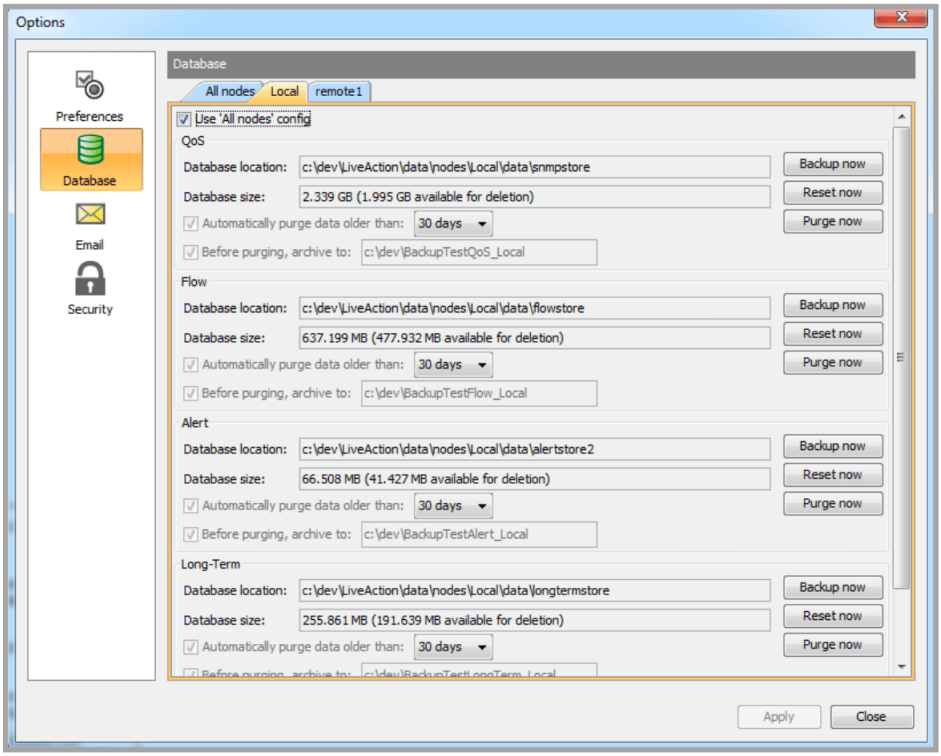
Options

The Options dialog allows LiveNX settings and preferences to be managed. The Options dialog can be accessed by selecting Tools > Options.

Preferences

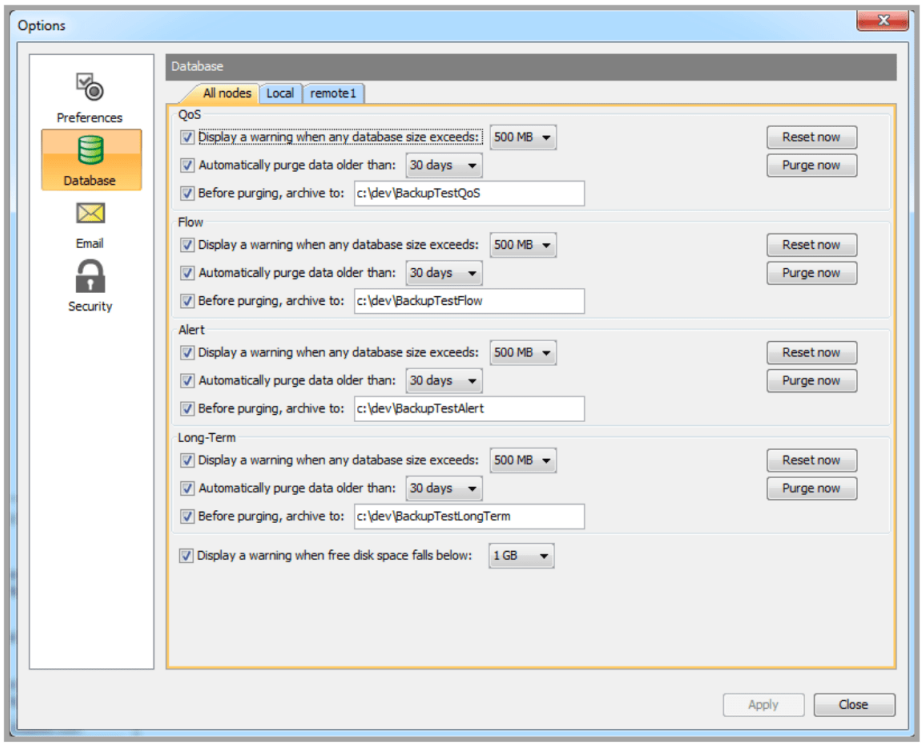
The Preferences section of the Options dialog allows you to use device names instead of hostnames, reset window sizes and warning dialogs. You can also set directory locations for the different files that LiveNX will save.

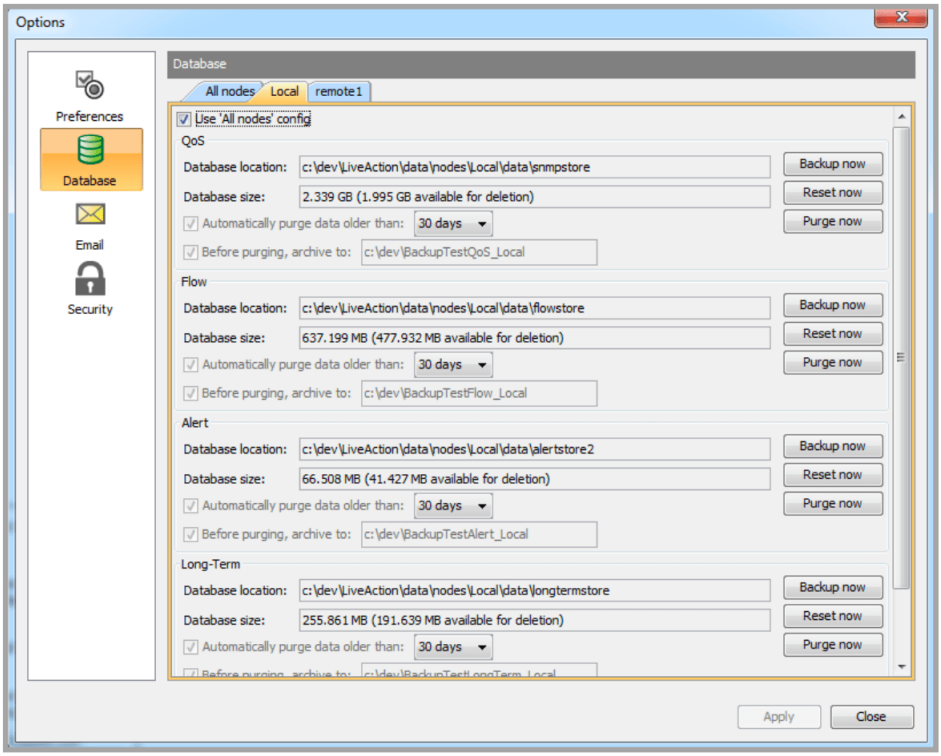
The device or hostname changes are visible in the System Hierarchy View and the System Topology.



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.





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.

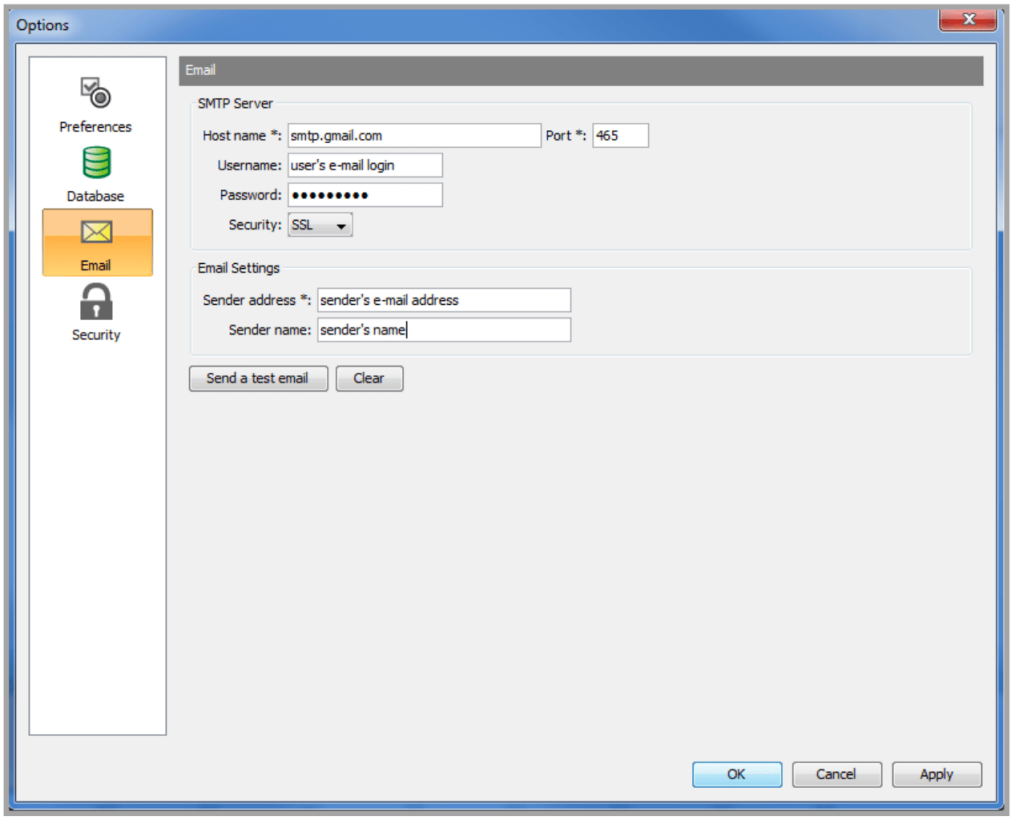
Note LiveNX supports an automatic purge to ensure that there is sufficient space to store about one minute worth of SNMP, Flow, Alert and Long-term data. This is not user-configurable, but the auto-purging of the four databases are done only as a last resort, to ensure that there is sufficient space 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.



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

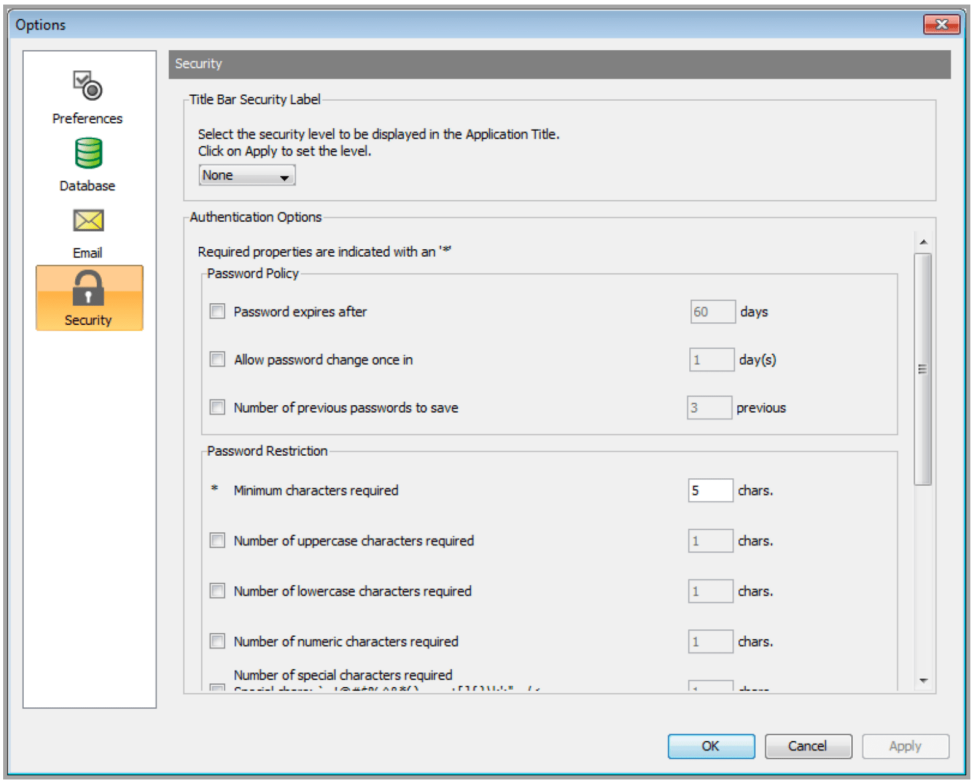
- Sender address—Enter the sender's e-mail address. • Sender's name—Enter the sender's name.

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.



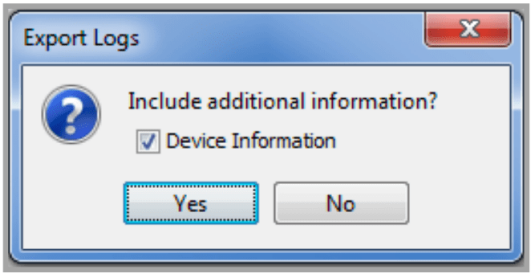
Export Server/Client /Nodes Logs

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.



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.

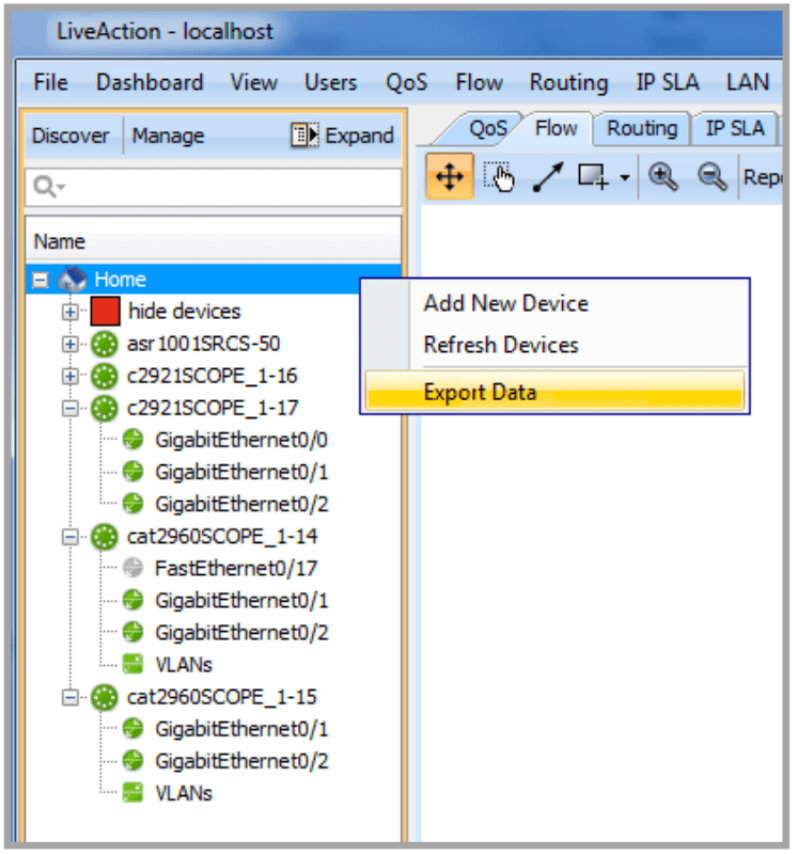
To get information from the LiveNX Nodes, go to the LiveAction Management Console and click on the Nodes tab. Right click on the status column of any Node with status = Connected and select Export Logs.

Export Device Data

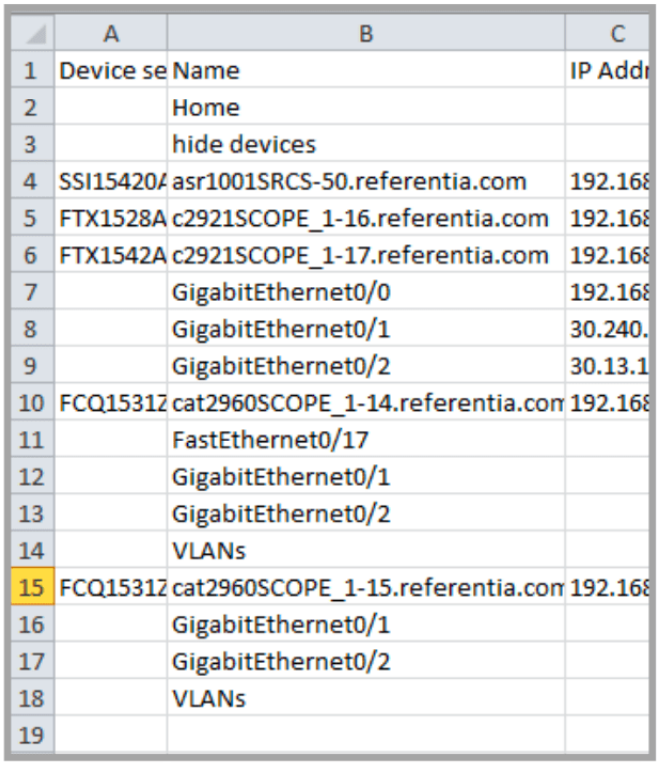
LiveNX uses the expand and collapse feature of the device tree in order for a user to hide certain information from exporting to a log file. To prevent certain devices from exporting to a log, create a group and then shrink the group, so no device are visible. To prevent certain interfaces from exporting 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.



	A	B	C
1	Device se	Name	IP Addı
2		Home	
3		hide devices	
4	SSI15420A	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	FCQ15317	cat2960SCOPE_1-14.referentia.com	192.168
11		FastEthernet0/17	
12		GigabitEthernet0/1	
13		GigabitEthernet0/2	
14		VLANs	
15	FCQ15317	cat2960SCOPE_1-15.referentia.com	192.168
16		GigabitEthernet0/1	
17		GigabitEthernet0/2	
18		VLANs	
19			