

LiveNX Semantic Tagging: Best-Practices Guide

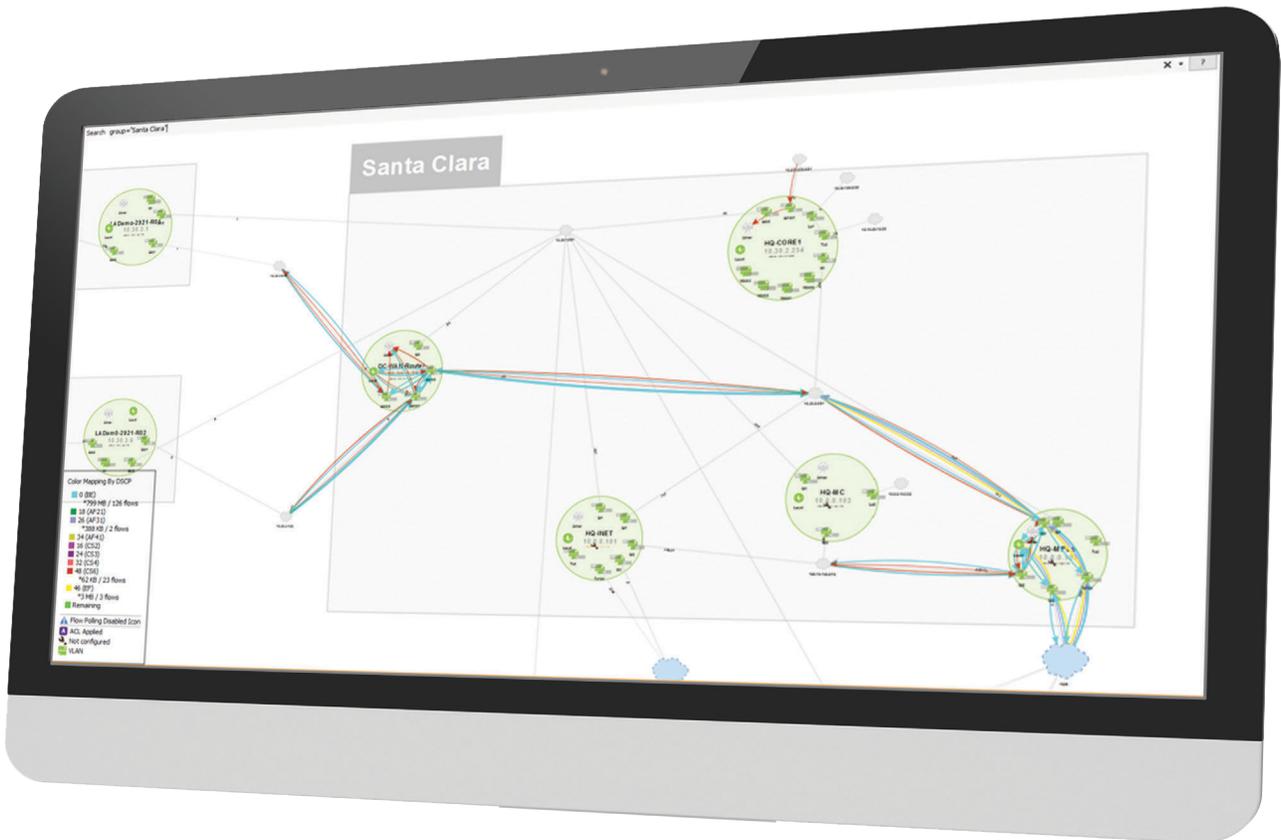


TABLE OF CONTENTS

Introduction.....	3
Groups.....	3
Sites and Site IPs	6
WAN and Service Provider.....	8
Label.....	9
Capacity.....	10
Device and Interface Tags.....	11
Reporting	12
Conclusion.....	13
More Information.....	13
About LiveAction.....	13

INTRODUCTION

Web search, a daily ritual in our connected lives is highly effective due to tagging of information. Wouldn't it be great if network admins had similar capability to search and ask questions related to the network?

LiveNX network semantics helps admins understand and troubleshoot their network better and faster. Using LiveNX's big data analytics platform, admins can tag network devices and interfaces to enable search, reporting and dashboard capabilities.

LiveNX provides a rich and flexible way to leverage network semantics. Admins 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 the admin create groups. Groups help visually and logically organize devices and enables 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 in Figure 1.

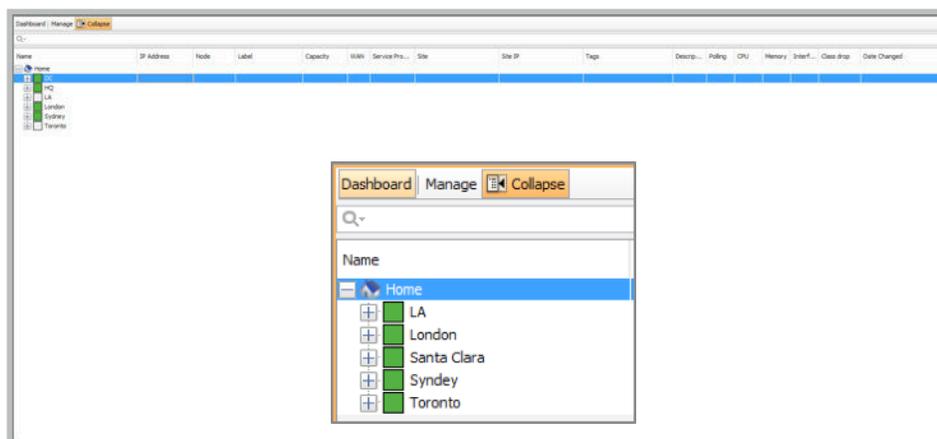
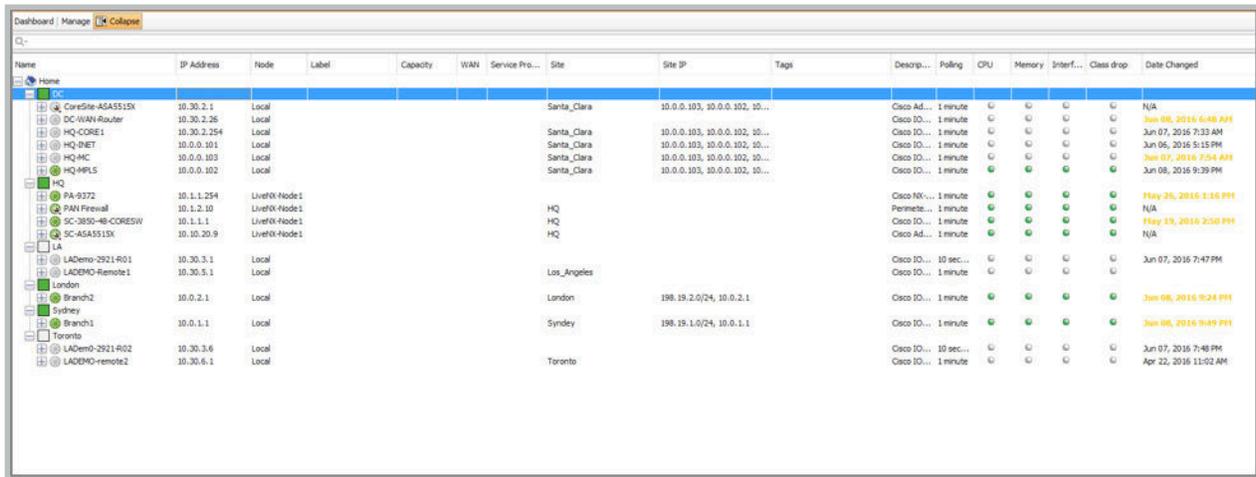


Figure 1. Groups

Each group contains network devices managed by LiveNX and can be seen by expanding the group as shown in Figure 2. Admins 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.



Name	IP Address	Node	Label	Capacity	WAN	Service Pro...	Site	Site IP	Tags	Descrip...	Poling	CPU	Memory	Interf...	Class drop	Date Changed
CoreSite-ASA5515X	10.30.2.1	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco Ad...	1 minute	🟢	🟢	🟢	🟢	N/A
DC-WAN-Router	10.30.2.26	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 08, 2016 6:48 AM
HQ-CORE1	10.30.2.254	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 07, 2016 7:33 AM
HQ-INET	10.0.0.101	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 06, 2016 5:15 PM
HQ-MC	10.0.0.103	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 07, 2016 7:54 AM
HQ-MPL5	10.0.0.102	Local					Santa_Clara	10.0.0.103, 10.0.0.102, 10...		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 08, 2016 9:39 PM
PA-9372	10.1.1.254	LiveNX-Node1					HQ			Cisco NX...	1 minute	🟢	🟢	🟢	🟢	May 25, 2016 1:16 PM
PA1-Firewall	10.1.2.10	LiveNX-Node1					HQ			Permit...	1 minute	🟢	🟢	🟢	🟢	N/A
SC-3850-48-CORESW	10.1.1.1	LiveNX-Node1					HQ			Cisco DO...	1 minute	🟢	🟢	🟢	🟢	May 19, 2016 2:50 PM
SC-ASA5515X	10.10.20.9	LiveNX-Node1					HQ			Cisco Ad...	1 minute	🟢	🟢	🟢	🟢	N/A
LA																
LADemo-2921-R01	10.30.3.1	Local					Los_Angeles			Cisco DO...	10 sec...	🟢	🟢	🟢	🟢	Jun 07, 2016 7:47 PM
LADemo-Remote1	10.30.5.1	Local					Los_Angeles			Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 07, 2016 7:47 PM
London																
Branch2	10.0.2.1	Local					London	198.19.2.0/24, 10.0.2.1		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 08, 2016 9:24 PM
Sydney																
Branch1	10.0.1.1	Local					Sydney	198.19.1.0/24, 10.0.1.1		Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Jun 08, 2016 9:49 PM
Toronto																
LADemo-2921-R02	10.30.3.6	Local					Toronto			Cisco DO...	10 sec...	🟢	🟢	🟢	🟢	Jun 07, 2016 7:48 PM
LADemo-remote2	10.30.6.1	Local					Toronto			Cisco DO...	1 minute	🟢	🟢	🟢	🟢	Apr 22, 2016 11:02 AM

Figure 2. Network Devices in Groups

LiveNX provides an intuitive and interactive topology as shown in Figure 3. 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.

Users 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 makes it easier to view all flow info to and from groups. Users 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. Users can simply click on the element to get additional details.

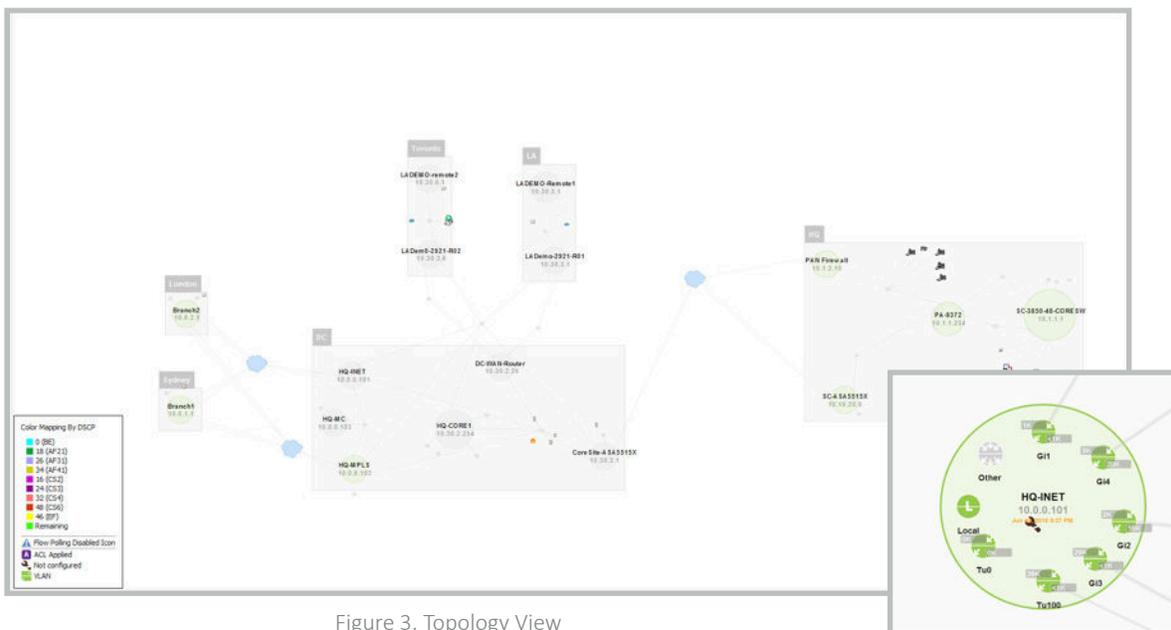


Figure 3. Topology View

Additionally, a search filter applied for 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. Figure 4 shows the flows related to group Santa Clara, when a filter for group=Santa_Clara is applied.

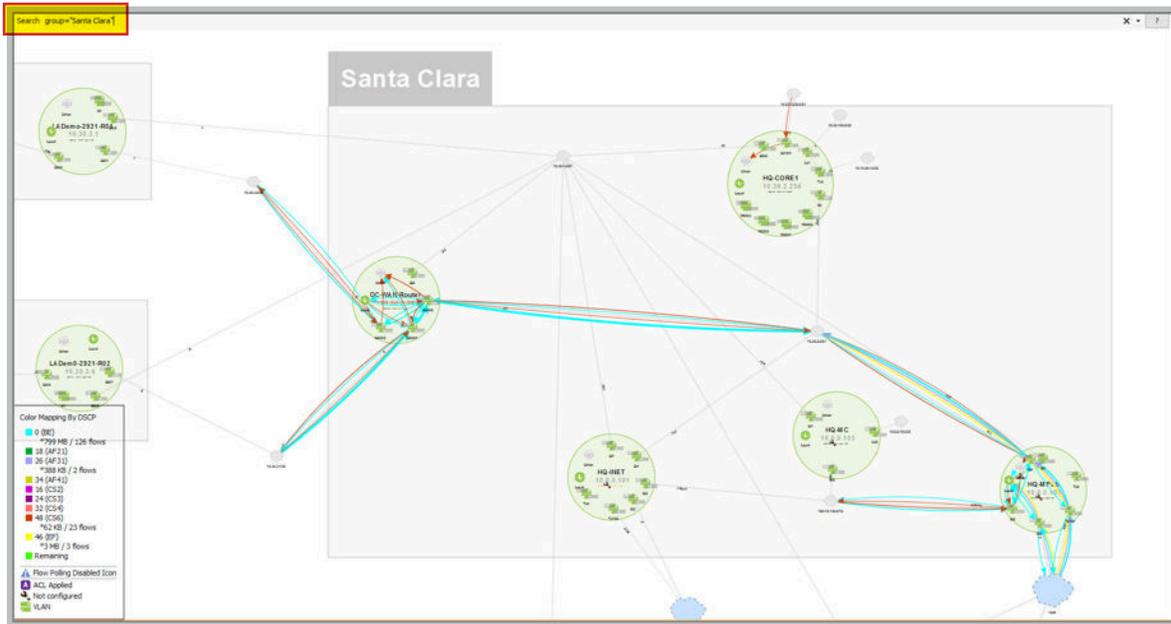


Figure 4. Group Flow Filter

Grouping devices is also important to help visualize the flows ingressing and egressing a collapsed group. The ingress and egress flows from a group can be to another device or another group (as you can see in Figure 5).

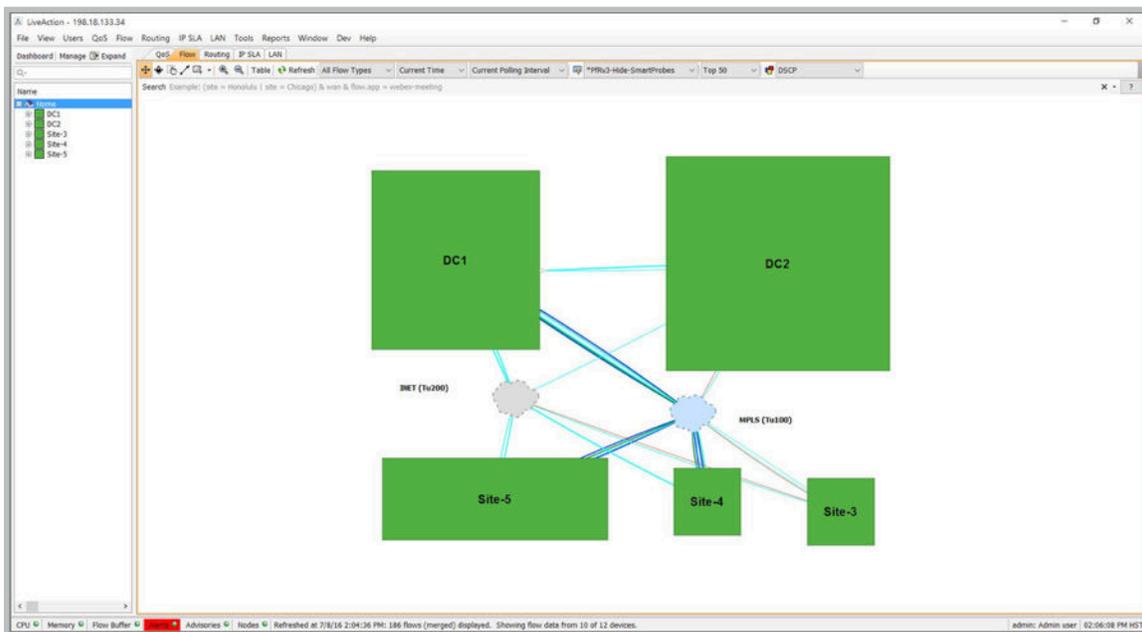


Figure 5. Ingress and Egress Flows from Groups

Collapsed groups also increase the performance of LiveNX by efficiently rendering the devices on the topology. Admins can simply zoom into a group to see the details, as shown in Figure 6.

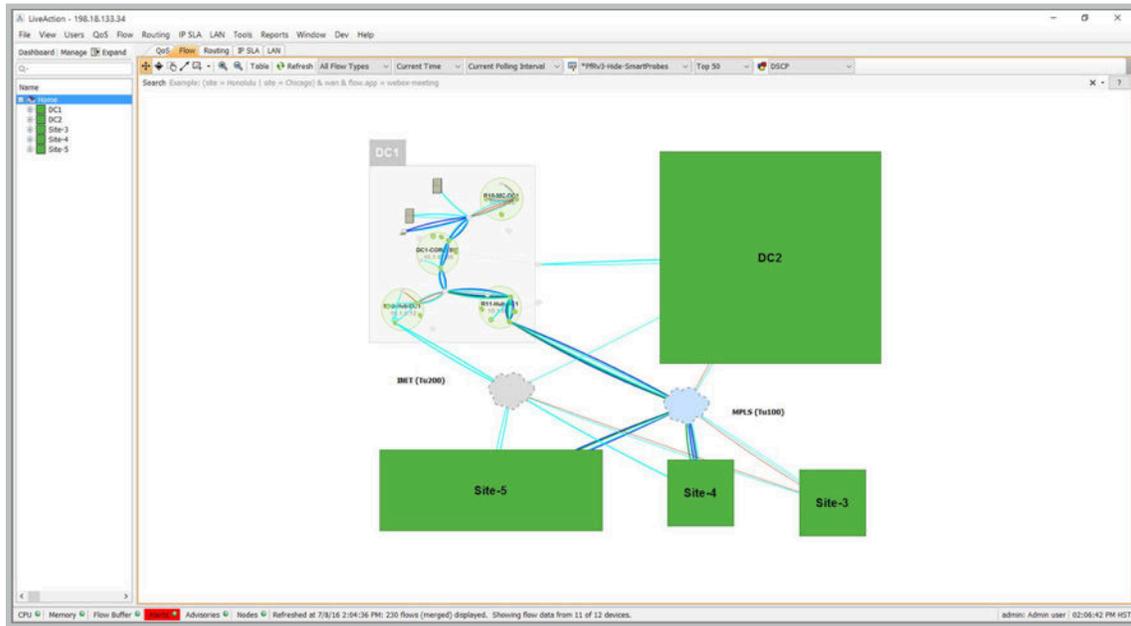


Figure 6. Expanded Group View

SITES AND SITE IPs'

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 useful for searching, running reports and observing data on the dashboard. LiveAction recommends that users assign network devices to a site and the site name correspond to the group name. For example, 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 Figure 7 are the same as the groups created in LiveNX.

Name	IP Address	Node	Label	Capacity	WAN	Service Pro...	Site	Site IP	Tags	Descrip...	Poling	CPU	Memory	Interf...	Class drop	Date Changed
DC																
HQ																
PA-9372	10.1.1.254	LiveNX-Node1					HQ			Cisco NX...	1 minute					May 26, 2016 1:16 PM
SC-3850-4S-CORESW	10.1.1.1	LiveNX-Node1					HQ			Cisco IO...	1 minute					May 13, 2016 2:58 PM
SC-45A5515X	10.10.20.9	LiveNX-Node1					HQ			Cisco Ad...	1 minute					N/A
LA																
LADemo-2921-R01	10.30.3.1	Local					Los_Angeles			Cisco IO...	10 sec...					Jun 07, 2016 7:47 PM
LACNO-Remote1	10.30.5.1	Local								Cisco IO...	1 minute					
Branch2	10.0.2.1	Local					London	198.19.2.0/24, 10.0.2.1		Cisco IO...	1 minute					Jan 08, 2016 9:24 PM
Branch1	10.0.1.1	Local					Sydney	198.19.1.0/24, 10.0.1.1		Cisco IO...	1 minute					Jan 08, 2016 9:49 PM
Toronto																
LADemo-2921-R02	10.30.3.6	Local								Cisco IO...	10 sec...					Jun 07, 2016 7:48 PM
LACNO-remote2	10.30.6.1	Local					Toronto			Cisco IO...	1 minute					Apr 22, 2016 11:02 AM

Figure 7. Sites

In addition to assigning a site to device(s), site also has a Site IP field as shown in Figure 7. 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.

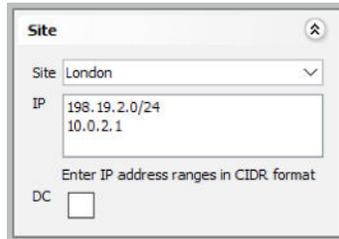


Figure 8. Site IP

When troubleshooting an issue between two sites, admins 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 in Figure 9a.

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 in Figure 9b.

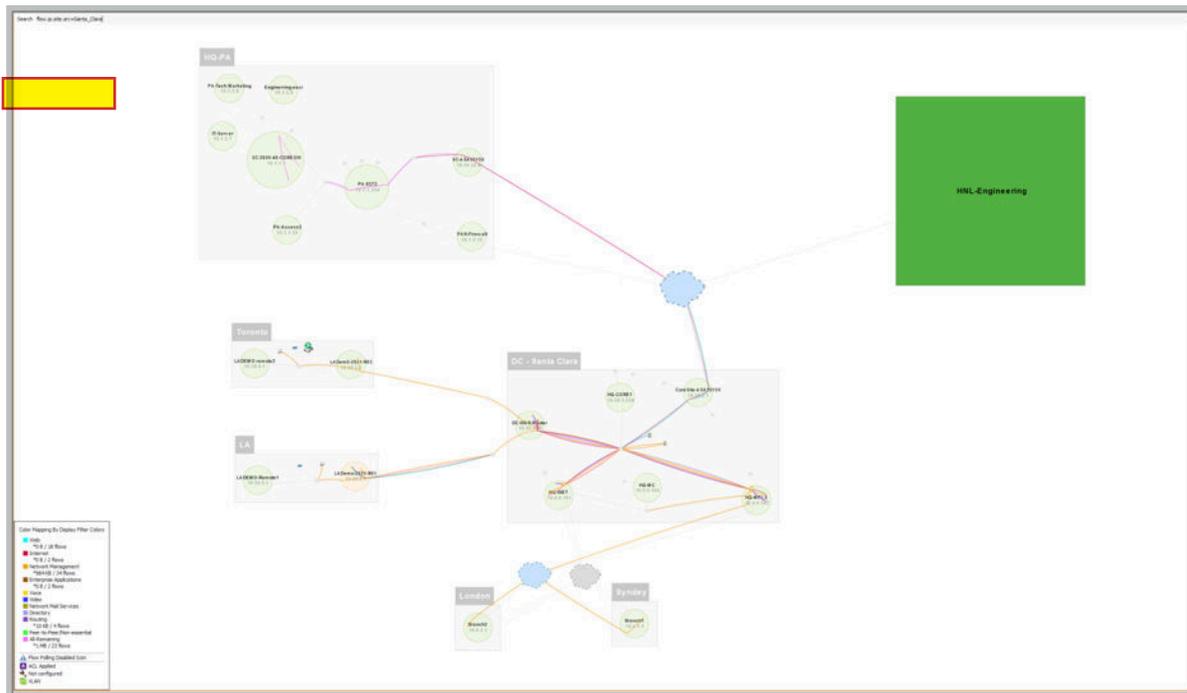


Figure 9a. Flow Query Search Based on Origin Site

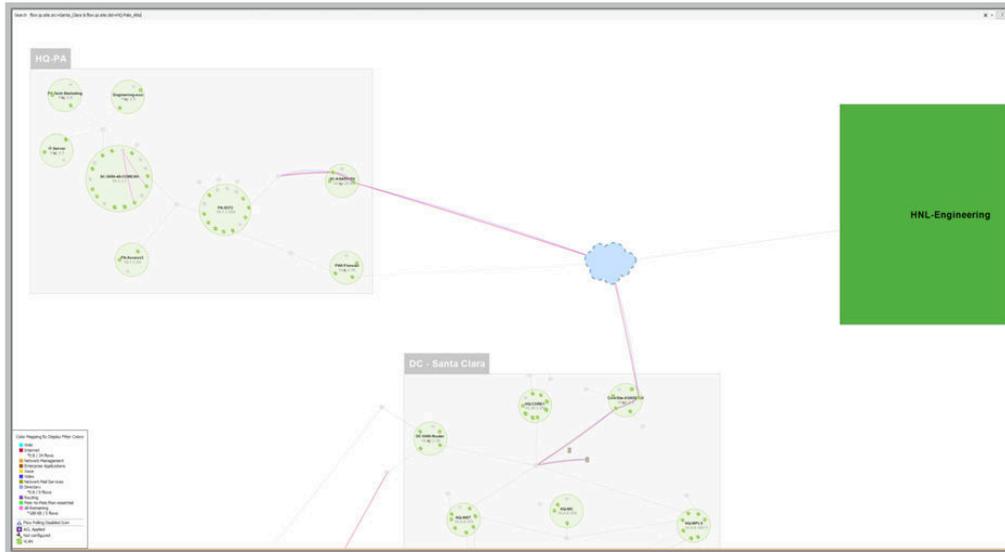


Figure 9b. Flow Query Search Based on Origin and Destination Site

WAN AND SERVICE PROVIDER

LiveAction recommends tagging all WAN links in the network. When filtering flows, admins can use the WAN filter to see traffic related to WAN flows only. Filtering traffic for WAN shows admins the usage of WAN links and the major consumers of bandwidth.

A WAN link can be identified by simply checking the WAN checkbox. In addition to the WAN checkbox, another label called “Service Provider” is available for further identification of the WAN link. Network admins 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.

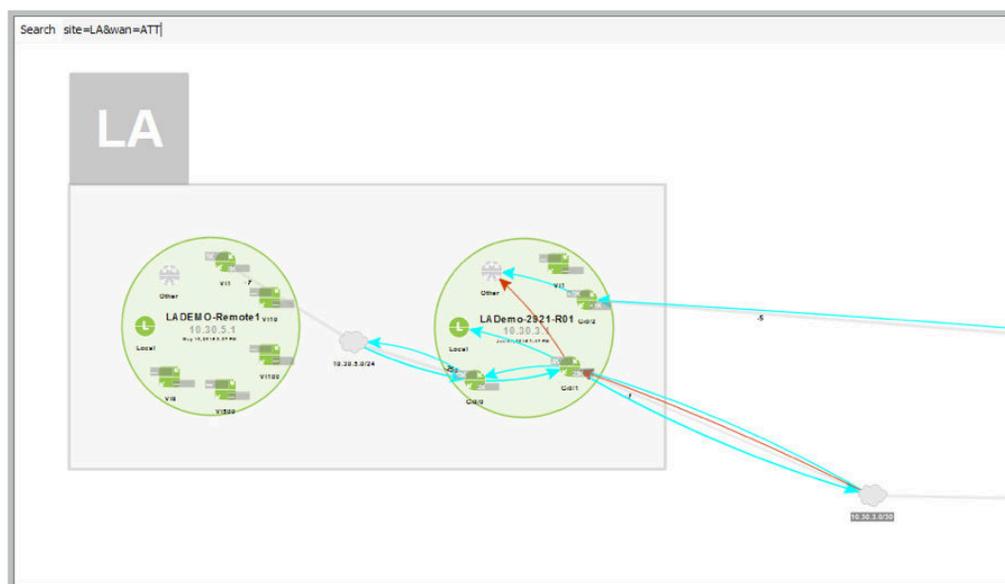
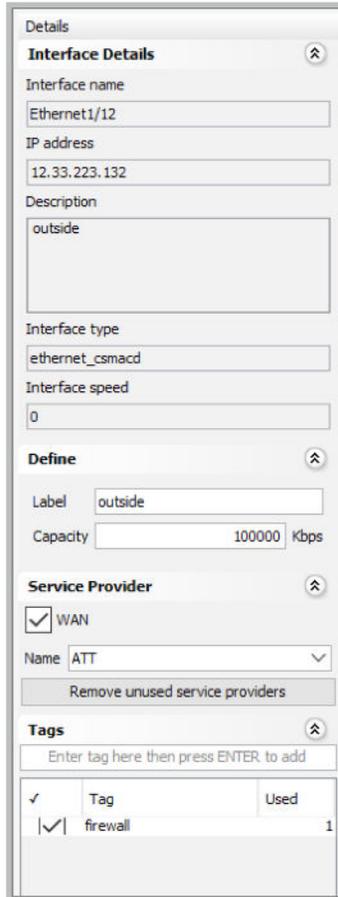


Figure 10. WAN and Service Provider

LABEL

Admins can also assign a label to interface(s). Labels are additional identifiers, which can be used to search and filter on the information available. Simply assign a label to the interface by selecting a previous label or adding a new one.



The screenshot shows a configuration page for an interface. It is divided into several sections:

- Interface Details:** Includes fields for Interface name (Ethernet1/12), IP address (12.33.223.132), Description (outside), Interface type (ethernet_csmacd), and Interface speed (0).
- Define:** Includes a Label field (outside) and a Capacity field (100000 Kbps).
- Service Provider:** Includes a checked checkbox for WAN, a Name dropdown menu (ATT), and a button labeled "Remove unused service providers".
- Tags:** Includes a text input field "Enter tag here then press ENTER to add" and a table of existing tags.

✓	Tag	Used
✓	firewall	1

Figure 11. Interface Tags, Labels

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 users 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.

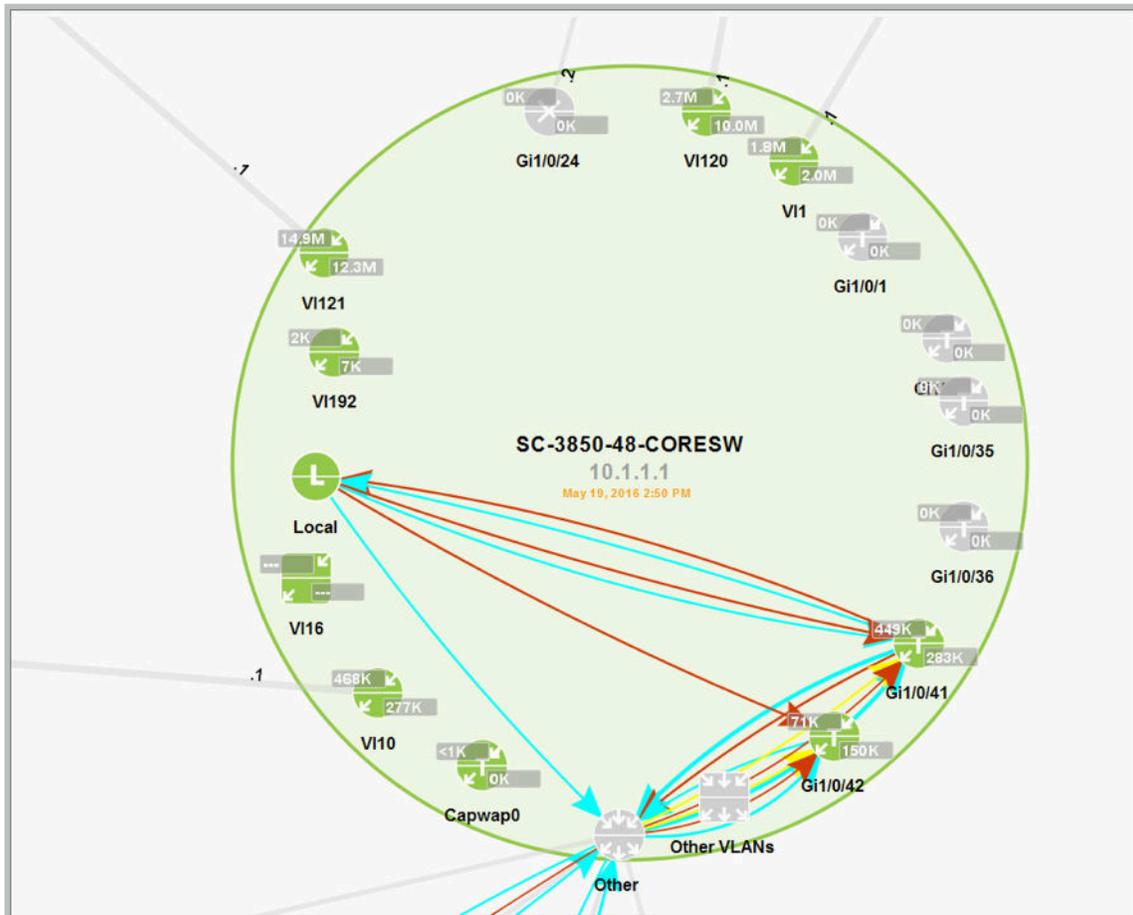


Figure 12. Interface Details

Admins can see interface details by simply zooming in on a network device on the topology. The topology shows the device with the bigger circle and 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. Admins 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. Figure 13 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.

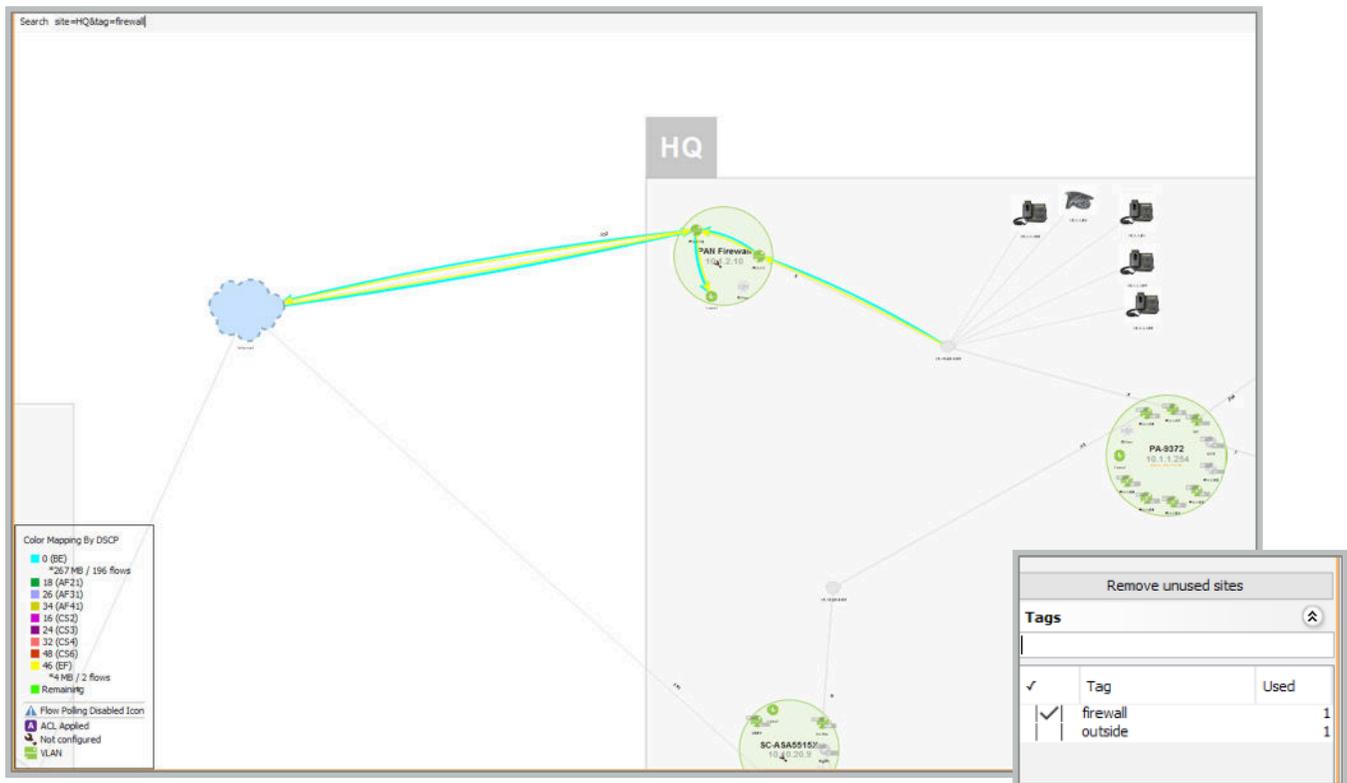


Figure 13. Filtering Flows Based on Tags

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 meaningful way for accurate decision making. For example, 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, as shown in Figure 14.

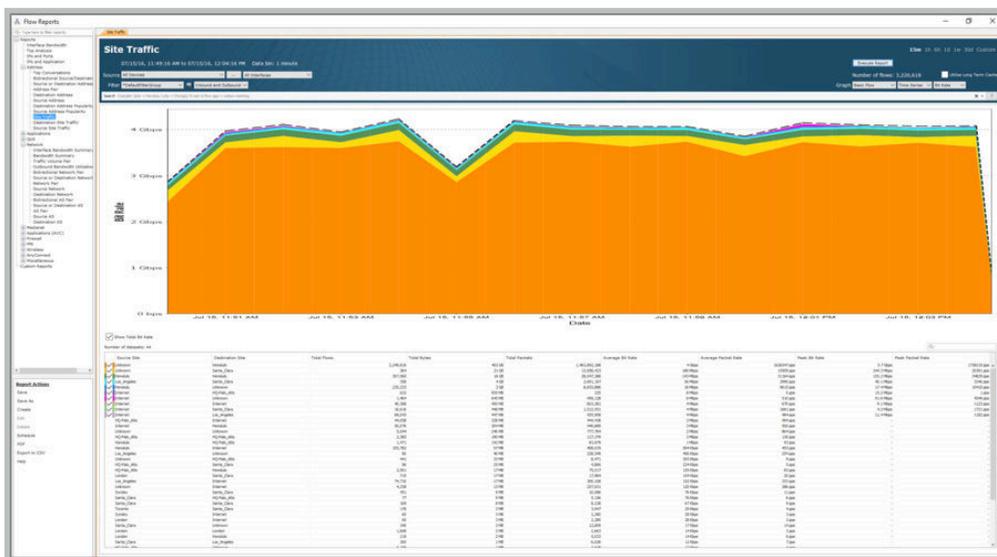


Figure 14. Site Report

Users 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 Figure 15 shows the traffic between those two sites only with the query `flow.ip.site.src=Santa_Clara & flow.ip.site.dst=HQ-Palo_Alto`

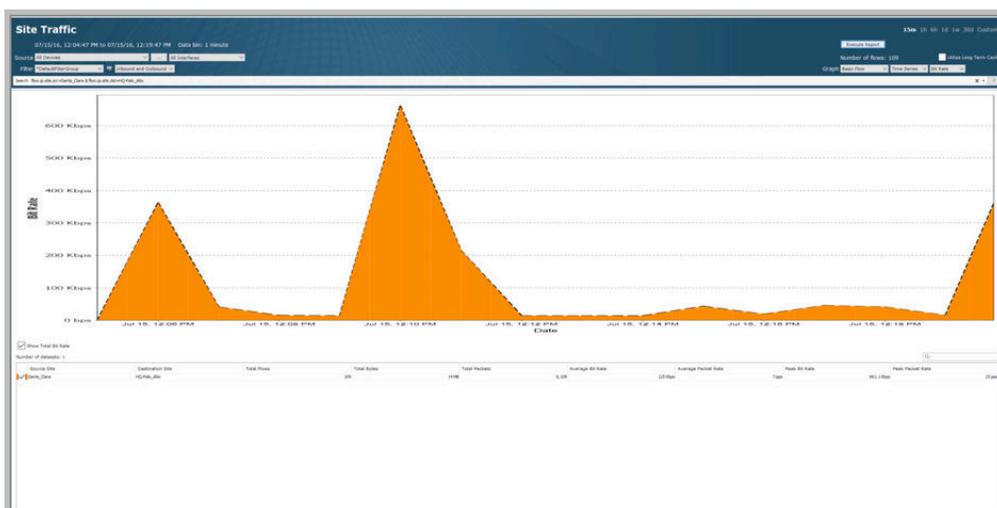


Figure 15. Site Report Between Two Specified Sites

CONCLUSION

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

- 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

MORE INFORMATION

[Network Performance Monitoring](#)

Learn how to quickly and cost-effectively monitor and manage network performance.

[Upcoming Webinars](#)

Check out our updated webinar schedule—gain insights from our special presenters about topics like QoS, Hybrid WAN Management, Capacity Planning and more.

[Additional Resources](#)

Case studies, white papers, eBooks and more are available for your learning on the LiveAction resources page.

[LiveNX and LiveUX Downloads](#)

Free downloads of [LiveNX](#) and [LiveUX](#) are available now. Visit our webpage to discover more details and benefits of LiveNX and LiveUX.

ABOUT LIVEACTION

LiveAction provides comprehensive and robust solutions for Network Performance Management. Key capabilities include Cisco Intelligent WAN visualization and service assurance, best-practice QoS policy management, and application-aware network performance management. LiveAction software's rich GUI and visualization provide IT teams with a deep understanding of the network while simplifying and accelerating management and troubleshooting tasks.

©2016 LiveAction, Inc. All rights reserved. LiveAction, the LiveAction logo and LiveNX Software are trademarks of LiveAction. Other company and product names are the trademarks of their respective companies.

LiveAction, Inc. · 3500 West Bayshore Road · Palo Alto, CA 94303 · USA · +1 (888) 881-1116