# LiveAction Training

*Lab Workbook Pt.2*

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

2019April15

## Table of Contents

**IMPORTANT INFORMATION – Please Read!**

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

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

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

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

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

# Lab .0

## Lab 0: Setup and Get Connected

# Lab 0.8:  Connect to the Lab Network

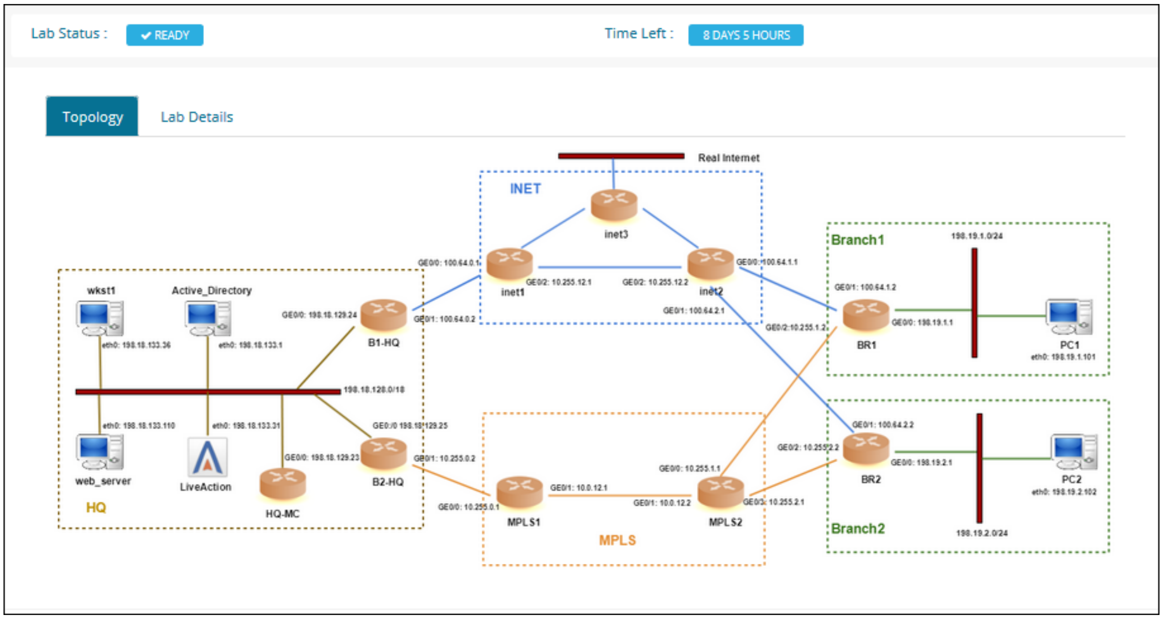
For this class, each attendee or Student will connect to and manage their own LiveNX installation.  In this lab you will connect to the classroom lab environment.  In some locations you may first be asked to connect your laptop to the Internet.

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

Local:
1 x PC Workstation to be used as a Management PC (YOUR Laptop)
1 x Installed LiveNX Client
1 x Browser

Remote Student Pod
1 x Windows Workstation accessed via RDC (optional) with an installed LiveNX Client and Browser
1 x LiveNX OVA Linux install
        1 LiveNX Server
        1 LiveNX Node (installed on LiveNX Server)

DIAGRAM



Lab Status : ✓ READY

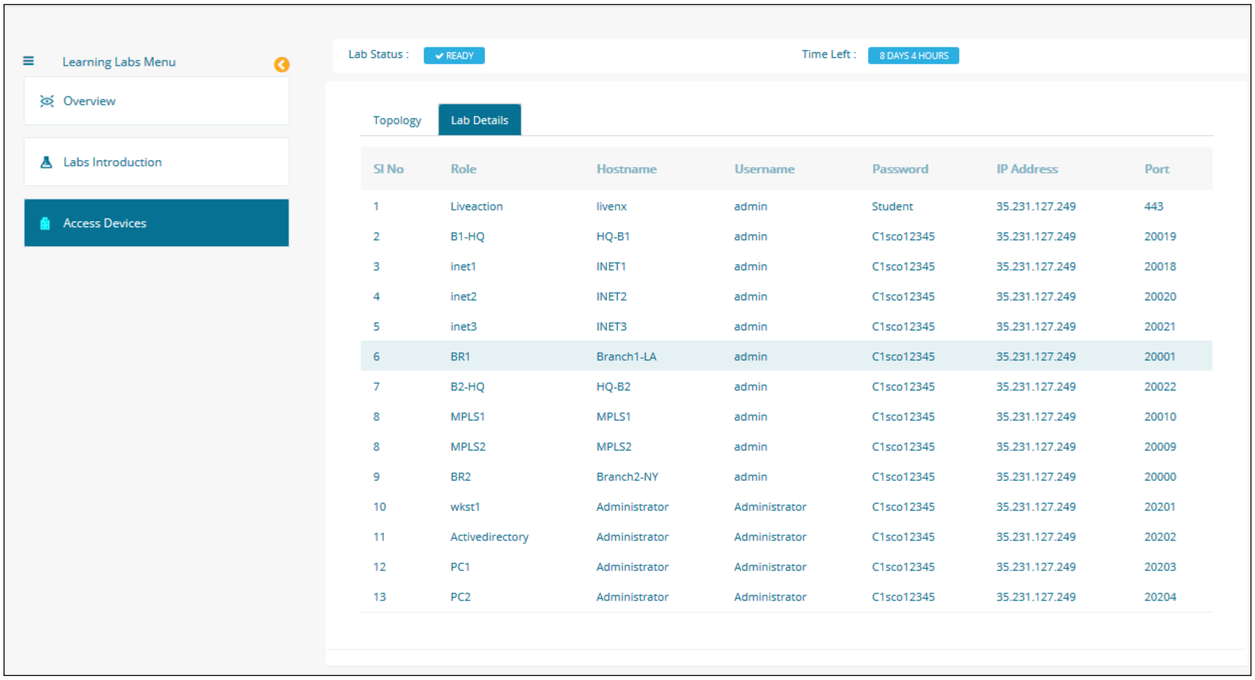
Time Left : 8 DAYS 5 HOURS

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

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

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

DIAGRAM



Lab Status : ✓ READY

Time Left : 8 DAYS 4 HOURS

| SI No | Role | Hostname | Username | Password | IP Address | Port |
|---|---|---|---|---|---|---|
| 1 | Liveaction | livenx | admin | Student | 35.231.127.249 | 443 |
| 2 | B1-HQ | HQ-B1 | admin | C1sco12345 | 35.231.127.249 | 20019 |
| 3 | inet1 | INET1 | admin | C1sco12345 | 35.231.127.249 | 20018 |
| 4 | inet2 | INET2 | admin | C1sco12345 | 35.231.127.249 | 20020 |
| 5 | inet3 | INET3 | admin | C1sco12345 | 35.231.127.249 | 20021 |
| 6 | BR1 | Branch1-LA | admin | C1sco12345 | 35.231.127.249 | 20001 |
| 7 | B2-HQ | HQ-B2 | admin | C1sco12345 | 35.231.127.249 | 20022 |
| 8 | MPLS1 | MPLS1 | admin | C1sco12345 | 35.231.127.249 | 20010 |
| 8 | MPLS2 | MPLS2 | admin | C1sco12345 | 35.231.127.249 | 20009 |
| 9 | BR2 | Branch2-NY | admin | C1sco12345 | 35.231.127.249 | 20000 |
| 10 | wkst1 | Administrator | Administrator | C1sco12345 | 35.231.127.249 | 20201 |
| 11 | Activedirectory | Administrator | Administrator | C1sco12345 | 35.231.127.249 | 20202 |
| 12 | PC1 | Administrator | Administrator | C1sco12345 | 35.231.127.249 | 20203 |
| 13 | PC2 | Administrator | Administrator | C1sco12345 | 35.231.127.249 | 20204 |

Lab Steps:

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

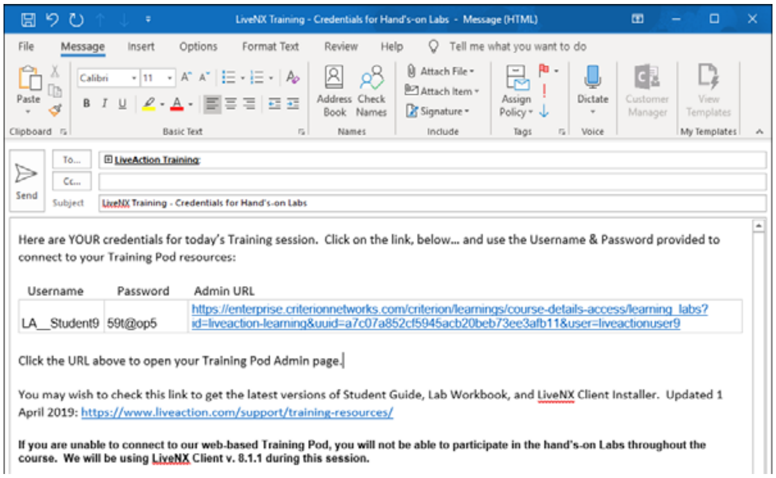
Note: **Make sure to consult the Infrastructure Diagram and worksheets, as well as specific classroom instructions for names, IP addresses, and other parameters.** The screen shots in this Lab Workbook are *examples* **which may not reflect the appropriate parameters for the classroom and/or your specific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

# Lab 0.9: Connecting to YOUR Training Pod

Throughout this Lab Workbook, you will be directed to connect to YOUR Pod resources… use the IP Address & Port information provided in YOUR assigned Web connection document.

The Instructor will have emailed credentials/login information to you prior to the start of the Training Session… similar to that below…

DIAGRAM



To: LiveAction Training;

Subject: LiveNX Training - Credentials for Hand's-on Labs

Here are YOUR credentials for today's Training session. Click on the link, below... and use the Username & Password provided to connect to your Training Pod resources:

| Username | Password | Admin URL |
|---|---|---|
| LA__Student9 | 59t@op5 | https://enterprise.criterionnetworks.com/criterion/learnings/course-details-access/learning_labs?id=liveaction-learning&uuid=a7c07a852cf5945acb20beb73ee3afb11&user=liveactionuser9 |

Click the URL above to open your Training Pod Admin page.

You may wish to check this link to get the latest versions of Student Guide, Lab Workbook, and LiveNX Client Installer. Updated 1 April 2019: https://www.liveaction.com/support/training-resources/

**If you are unable to connect to our web-based Training Pod, you will not be able to participate in the hand's-on Labs throughout the course. We will be using LiveNX Client v. 8.1.1 during this session.**

Lab Steps:

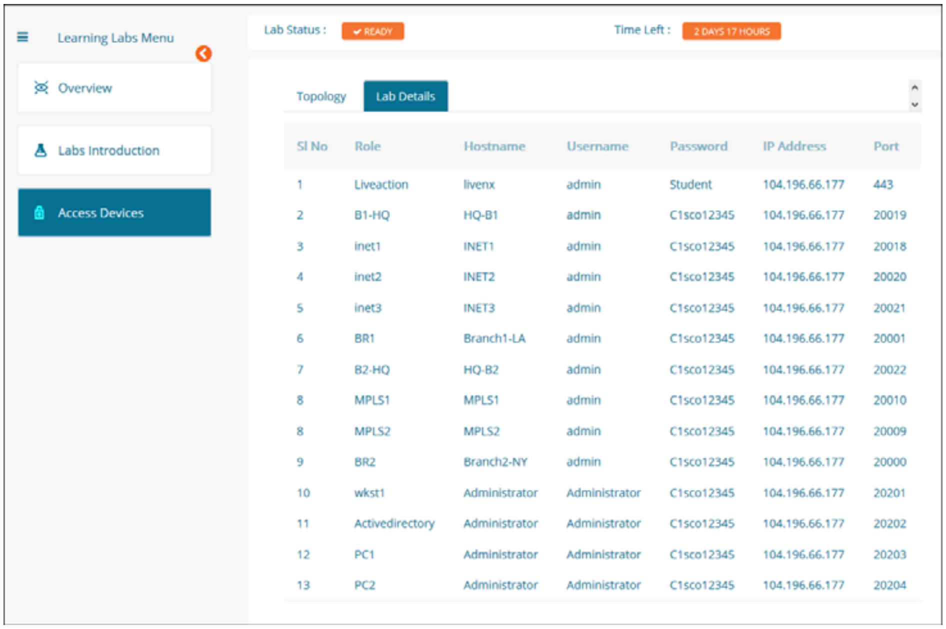
1. Click the URL provided in the email.

---

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

---

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



Lab Status : ✓ READY

Time Left : 2 DAYS 17 HOURS

| Sl No | Role | Hostname | Username | Password | IP Address | Port |
|---|---|---|---|---|---|---|
| 1 | Liveaction | livenx | admin | Student | 104.196.66.177 | 443 |
| 2 | B1-HQ | HQ-B1 | admin | C1sco12345 | 104.196.66.177 | 20019 |
| 3 | inet1 | INET1 | admin | C1sco12345 | 104.196.66.177 | 20018 |
| 4 | inet2 | INET2 | admin | C1sco12345 | 104.196.66.177 | 20020 |
| 5 | inet3 | INET3 | admin | C1sco12345 | 104.196.66.177 | 20021 |
| 6 | BR1 | Branch1-LA | admin | C1sco12345 | 104.196.66.177 | 20001 |
| 7 | B2-HQ | HQ-B2 | admin | C1sco12345 | 104.196.66.177 | 20022 |
| 8 | MPLS1 | MPLS1 | admin | C1sco12345 | 104.196.66.177 | 20010 |
| 8 | MPLS2 | MPLS2 | admin | C1sco12345 | 104.196.66.177 | 20009 |
| 9 | BR2 | Branch2-NY | admin | C1sco12345 | 104.196.66.177 | 20000 |
| 10 | wkst1 | Administrator | Administrator | C1sco12345 | 104.196.66.177 | 20201 |
| 11 | Activedirectory | Administrator | Administrator | C1sco12345 | 104.196.66.177 | 20202 |
| 12 | PC1 | Administrator | Administrator | C1sco12345 | 104.196.66.177 | 20203 |
| 13 | PC2 | Administrator | Administrator | C1sco12345 | 104.196.66.177 | 20204 |

# Lab 1

## Lab 1: QoS Configuration

# Lab 1.0: Introduction to QoS

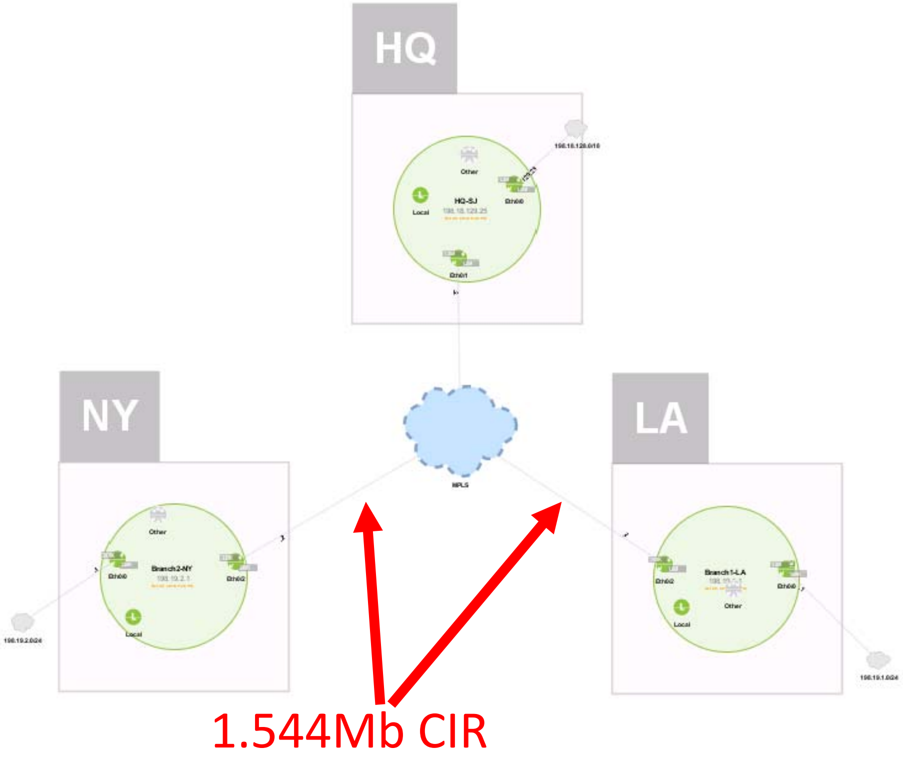
In this lab we are going to walk through the story of implementing QoS for a small WAN network using LiveNX. When complete we will have used LiveNX to:

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

Below is a diagram of sample network. There are three WAN locations. Each location has full-mesh connectivity provided by a MPLS network. The connectivity is designed as follows:

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

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

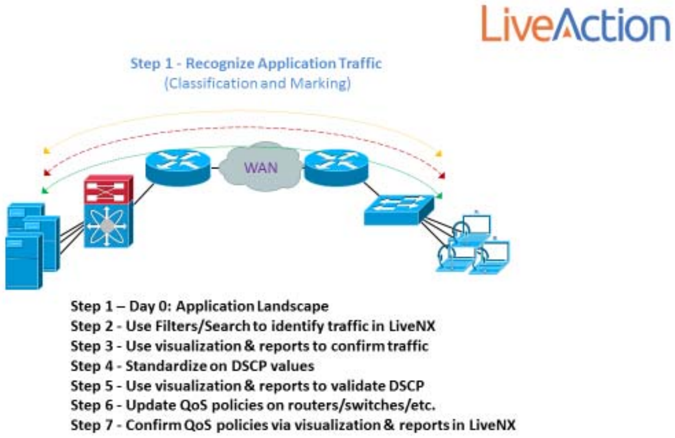


Remember from the presentation that QoS is done in 4 steps:

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

We will use LiveNX to walk through this story.

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



LiveAction

Step 1 - Recognize Application Traffic
(Classification and Marking)

Step 1 – Day 0: Application Landscape
Step 2 - Use Filters/Search to identify traffic in LiveNX
Step 3 - Use visualization & reports to confirm traffic
Step 4 - Standardize on DSCP values
Step 5 - Use visualization & reports to validate DSCP
Step 6 - Update QoS policies on routers/switches/etc.
Step 7 - Confirm QoS policies via visualization & reports in LiveNX

**Day 0 Tasks**

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

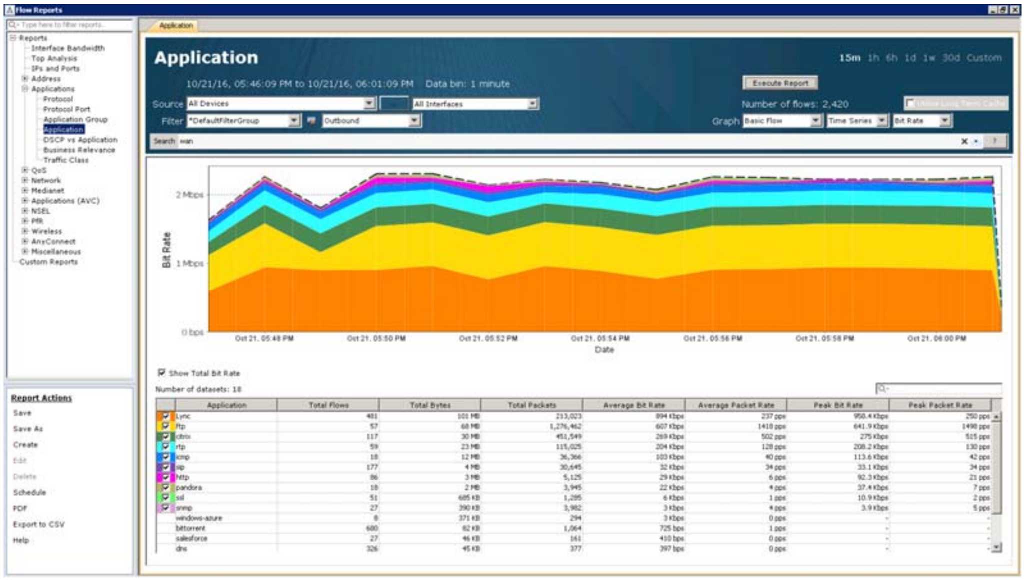
- Voice (rtp)
- Video (Lync)
- SIP
- Citrix
- NetFlow
- SNMP
- SSH
- Telnet
- Salesforce

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

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

# Lab 1.1:  Run Baseline Reports

1. From the LiveNX Client, Run the Reports > Flow > Applications > **Application**
   a. Keep all filters and report at their default settings
   b. Implement a Search of “wan”
   c. **Execute  Report**



Application

10/21/16, 05:46:09 PM to 10/21/16, 06:01:09 PM   Data bin: 1 minute

Source: All Devices   All Interfaces

Filter: *DefaultFilterGroup   Outbound

Number of flows: 2,420

Graph: Basic Flow   Time Series   Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 18

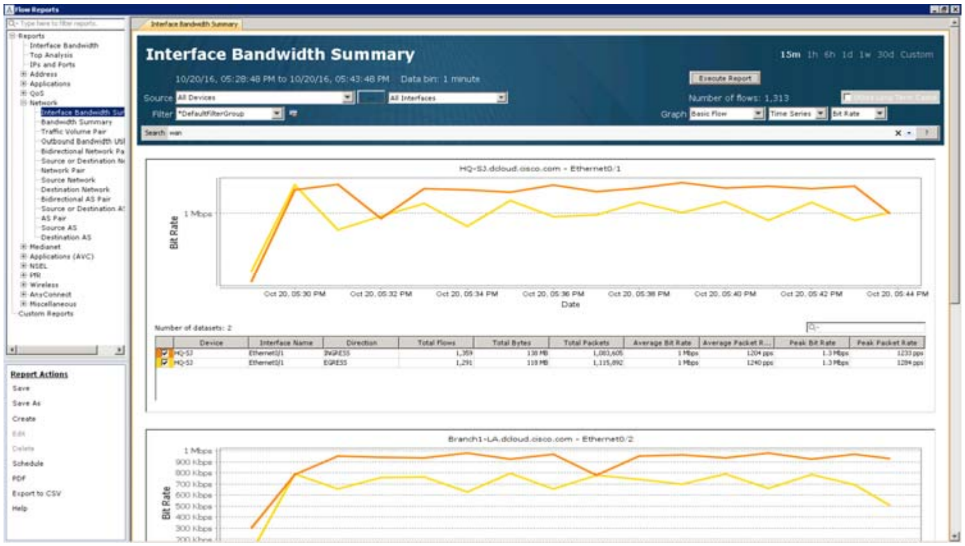
| | Application | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | Lync | 481 | 101 MB | 213,023 | 894 Kbps | 237 pps | 958.4 Kbps | 250 pps |
| ☑ | ftp | 57 | 68 MB | 1,276,462 | 607 Kbps | 1418 pps | 641.9 Kbps | 1490 pps |
| ☑ | citrix | 117 | 30 MB | 451,549 | 269 Kbps | 502 pps | 275 Kbps | 515 pps |
| ☑ | rtp | 59 | 23 MB | 115,025 | 204 Kbps | 128 pps | 208.2 Kbps | 130 pps |
| ☑ | icmp | 18 | 12 MB | 36,366 | 103 Kbps | 40 pps | 113.6 Kbps | 42 pps |
| ☑ | sip | 177 | 4 MB | 30,645 | 32 Kbps | 34 pps | 33.1 Kbps | 34 pps |
| ☑ | http | 86 | 3 MB | 5,125 | 29 Kbps | 6 pps | 92.3 Kbps | 21 pps |
| ☑ | pandora | 18 | 2 MB | 3,945 | 22 Kbps | 4 pps | 37.4 Kbps | 7 pps |
| ☑ | ssl | 51 | 685 KB | 1,295 | 6 Kbps | 1 pps | 10.9 Kbps | 2 pps |
| ☑ | snmp | 27 | 390 KB | 3,982 | 3 Kbps | 4 pps | 3.9 Kbps | 5 pps |
| | windows-azure | 8 | 371 KB | 294 | 3 Kbps | 0 pps | - | - |
| | bittorrent | 680 | 82 KB | 1,064 | 725 bps | 1 pps | - | - |
| | salesforce | 27 | 46 KB | 161 | 410 bps | 0 pps | - | - |
| | dns | 326 | 45 KB | 377 | 397 bps | 0 pps | - | - |

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

Review the applications on the network – all business critical applications are represented. Notice voice (rtp) & video (openwebnet) are top applications by volume in this network – this is often not the case in real networks.

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

2. Run the Reports > Flow > Bandwidth > **Interface Bandwidth Summary Report**
   a. Keep all filters and report at their default settings
   b. Implement a Search of “wan”
   c. **Execute Report**



**Interface Bandwidth Summary**

10/20/16, 05:28:48 PM to 10/20/16, 05:43:48 PM Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup

Number of flows: 1,313

Graph: Basic Flow | Time Series | Bit Rate

Search: wan

Number of datasets: 2

| | Device | Interface Name | Direction | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet R... | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | HQ-SJ | Ethernet0/1 | INGRESS | 1,359 | 138 MB | 1,083,605 | 1 Mbps | 1204 pps | 1.3 Mbps | 1233 pps |
| ☑ | HQ-SJ | Ethernet0/1 | EGRESS | 1,291 | 118 MB | 1,115,892 | 1 Mbps | 1240 pps | 1.3 Mbps | 1284 pps |

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

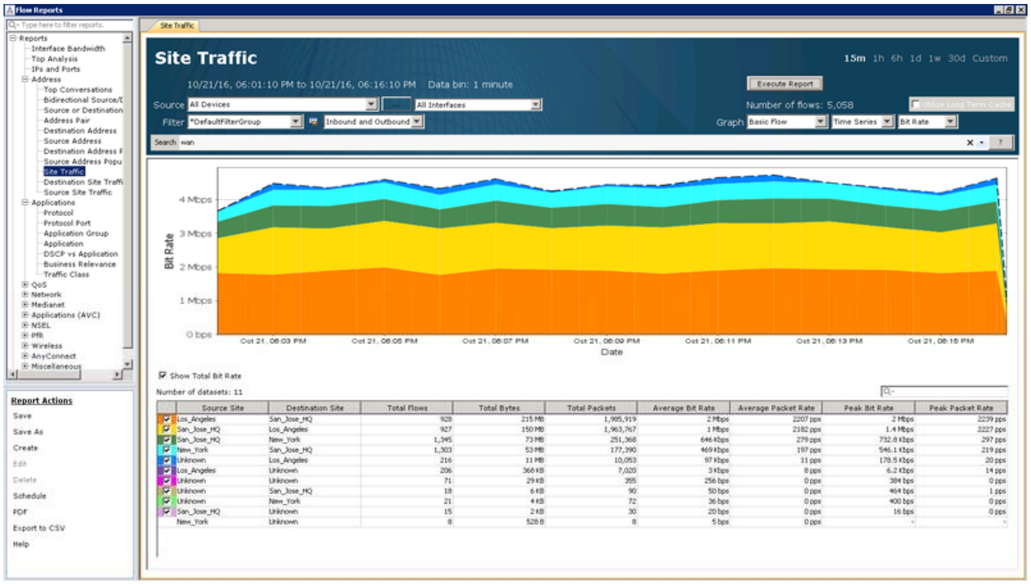
3. Re-run this report, but update the Search to: "wan & flow.app=rtp"

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

4. Re-run this report, but update the Search to: "wan & flow.app=openwebnet"

This provides an understanding of the utilization of just Video (Lync) on each WAN circuit.

5. Re-run this report, but update the Search to view other key applications as desired.
6. Run the Reports > Flow > Address > **Site Traffic**
   a. Keep all filters and report at their default settings
   b. Implement a Search of "wan"
   c. **Execute Report**



**Site Traffic**

10/21/16, 06:01:10 PM to 10/21/16, 06:16:10 PM Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup | Inbound and Outbound

Number of flows: 5,058

Graph: Basic Flow | Time Series | Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 11

| | Source Site | Destination Site | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | Los_Angeles | San_Jose_HQ | 928 | 215 MB | 1,985,919 | 2 Mbps | 2207 pps | 2 Mbps | 2239 pps |
| ☑ | San_Jose_HQ | Los_Angeles | 927 | 150 MB | 1,963,767 | 1 Mbps | 2182 pps | 1.4 Mbps | 2227 pps |
| ☑ | San_Jose_HQ | New_York | 1,345 | 73 MB | 251,368 | 646 Kbps | 279 pps | 732.8 Kbps | 297 pps |
| ☑ | New_York | San_Jose_HQ | 1,303 | 53 MB | 177,390 | 469 Kbps | 197 pps | 546.1 Kbps | 219 pps |
| ☑ | Unknown | Los_Angeles | 216 | 11 MB | 10,053 | 97 Kbps | 11 pps | 178.5 Kbps | 20 pps |
| ☑ | Los_Angeles | Unknown | 206 | 368 KB | 7,020 | 3 Kbps | 8 pps | 6.2 Kbps | 14 pps |
| ☑ | Unknown | Unknown | 71 | 29 KB | 355 | 256 bps | 0 pps | 384 bps | 0 pps |
| ☑ | Unknown | San_Jose_HQ | 18 | 6 KB | 90 | 50 bps | 0 pps | 464 bps | 1 pps |
| ☑ | Unknown | New_York | 21 | 4 KB | 72 | 36 bps | 0 pps | 400 bps | 0 pps |
| ☑ | San_Jose_HQ | Unknown | 15 | 2 KB | 30 | 20 bps | 0 pps | 16 bps | 0 pps |
| | New_York | Unknown | 8 | 528 B | 8 | 5 bps | 0 pps | - | - |

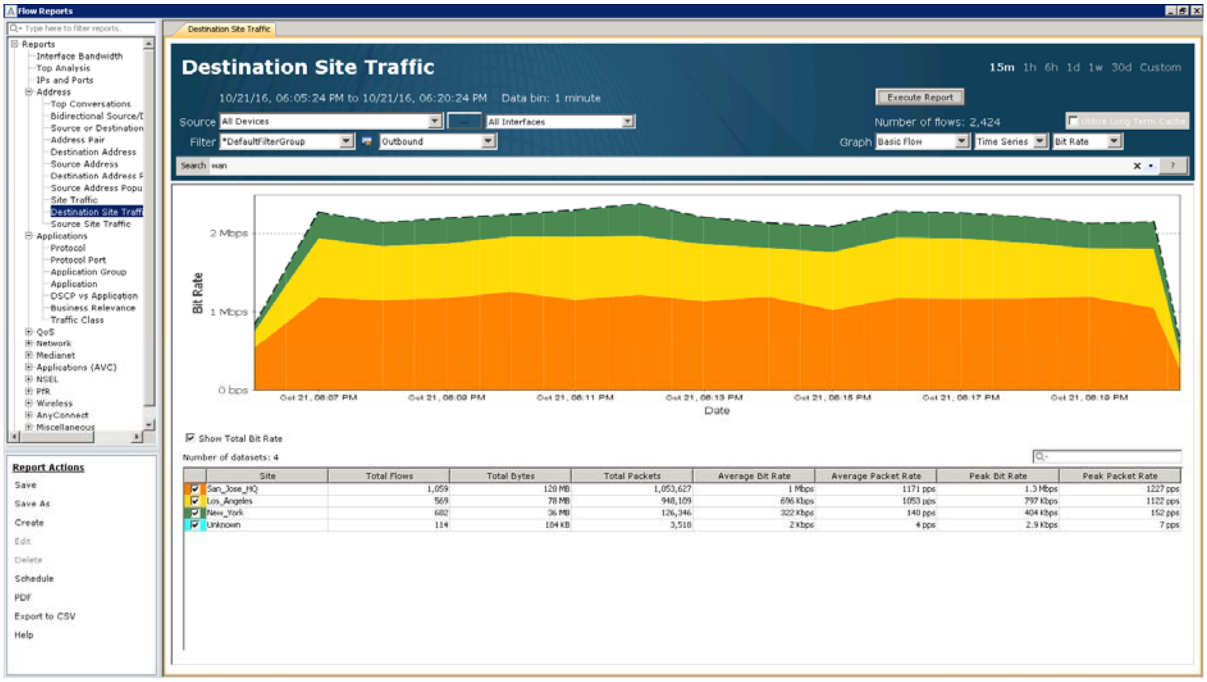
Observe the breakdown of bandwidth between site pairs.

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

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

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

9. Run the Reports > Flow > Address > **Destination Site Traffic**
    a. Keep all filters and report at their default settings
    b. Implement a Search of “wan”
    c. **Execute Report**



Destination Site Traffic

10/21/16, 06:05:24 PM to 10/21/16, 06:20:24 PM  Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup | Outbound

Number of flows: 2,424

Graph: Basic Flow | Time Series | Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 4

| | Site | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | San_Jose_HQ | 1,059 | 128 MB | 1,053,627 | 1 Mbps | 1171 pps | 1.3 Mbps | 1227 pps |
| ☑ | Los_Angeles | 569 | 78 MB | 948,109 | 696 Kbps | 1053 pps | 797 Kbps | 1122 pps |
| ☑ | New_York | 682 | 36 MB | 126,346 | 322 Kbps | 140 pps | 404 Kbps | 152 pps |
| ☑ | Unknown | 114 | 184 KB | 3,518 | 2 Kbps | 4 pps | 2.9 Kbps | 7 pps |

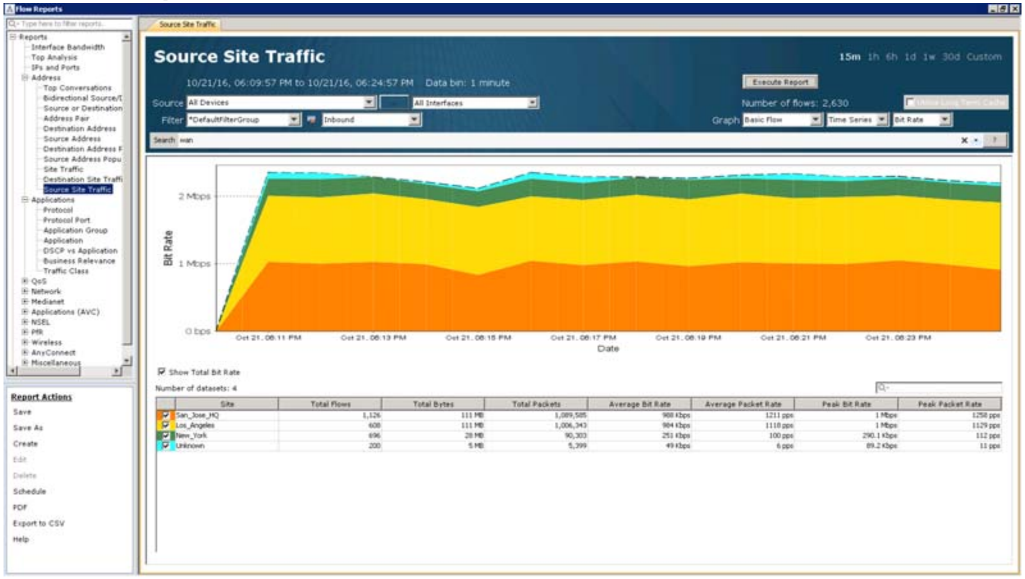
Observe which sites are being sent the most data.

10. Re-run this report, but update the Search to: “wan & flow.app=rtp”

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

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

12. Run the Reports > Flow > Address > **Source Site Traffic Report**
    a. Keep all filters and report at their default settings
    b. Implement a Search of “wan”
    c. **Execute Report**



Source Site Traffic

10/21/16, 06:09:57 PM to 10/21/16, 06:24:57 PM  Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup | Inbound

Number of flows: 2,630

Graph: Basic Flow | Time Series | Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 4

| | Site | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | San_Jose_HQ | 1,126 | 111 MB | 1,089,585 | 988 Kbps | 1211 pps | 1 Mbps | 1258 pps |
| ☑ | Los_Angeles | 608 | 111 MB | 1,006,343 | 984 Kbps | 1118 pps | 1 Mbps | 1129 pps |
| ☑ | New_York | 696 | 28 MB | 90,303 | 251 Kbps | 100 pps | 290.1 Kbps | 112 pps |
| ☑ | Unknown | 200 | 5 MB | 5,399 | 49 Kbps | 6 pps | 89.2 Kbps | 11 pps |

Observe which sites are sending the most data.

13. Re-run this report, but update the Search to: “wan & flow.app=rtp”

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

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

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

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

# Lab 1.2: Building Filters

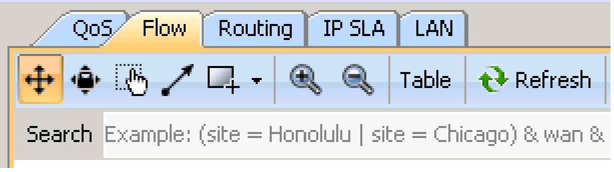
The reports we have used so far were using NBAR for recognizing specific types of traffic such as Voice (rtp) or Video (Lync). This can be an excellent way to see specific applications that are known by NBAR. In real networks though, NBAR is a great, but not a perfect solution for recognizing traffic.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

Many networks have not yet adopted NBAR so this data is unavailable, as well.

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

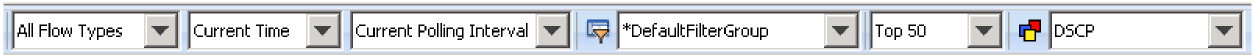
Lab Steps:

1. From the LiveAction map, select the Flow Tab



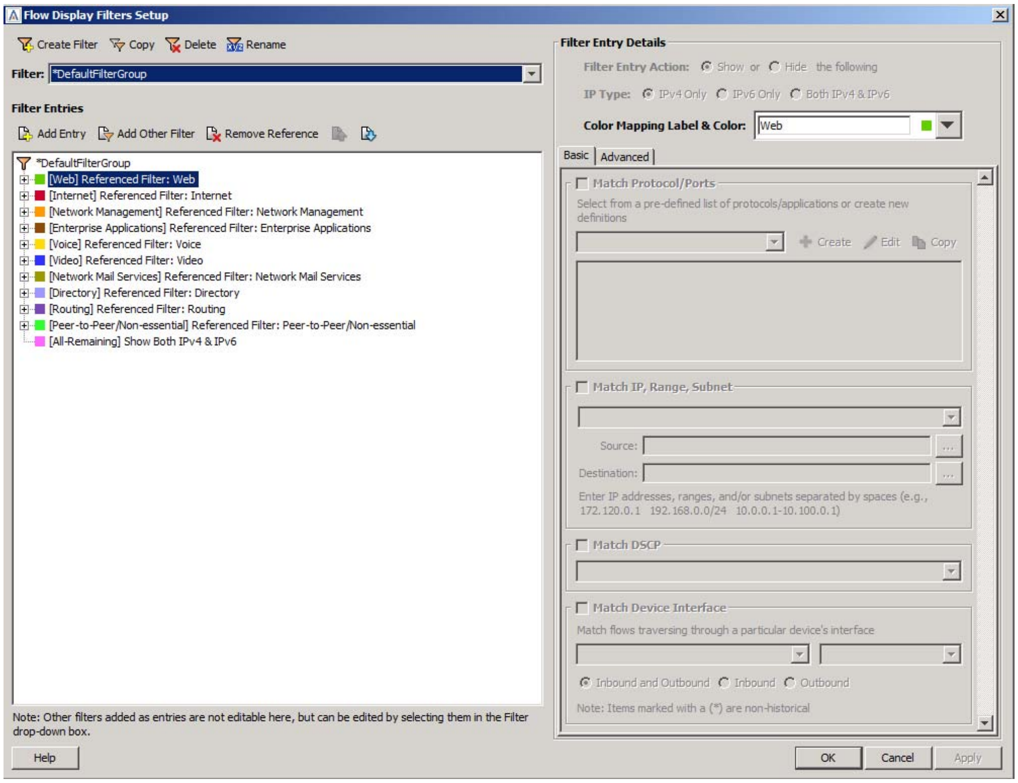
Search: Example: (site = Honolulu | site = Chicago) & wan &

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



All Flow Types | Current Time | Current Polling Interval | *DefaultFilterGroup | Top 50 | DSCP

3. The Display Filters Setup Dialog appears



Filter: *DefaultFilterGroup

*DefaultFilterGroup
- 🟩 [Web] Referenced Filter: Web
- 🟥 [Internet] Referenced Filter: Internet
- 🟧 [Network Management] Referenced Filter: Network Management
- 🟫 [Enterprise Applications] Referenced Filter: Enterprise Applications
- 🟨 [Voice] Referenced Filter: Voice
- 🟦 [Video] Referenced Filter: Video
- 🟫 [Network Mail Services] Referenced Filter: Network Mail Services
- 🟪 [Directory] Referenced Filter: Directory
- 🟪 [Routing] Referenced Filter: Routing
- 🟩 [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
- 🟪 [All-Remaining] Show Both IPv4 & IPv6

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: Web 🟩

□ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

□ Match IP, Range, Subnet

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ Match DSCP

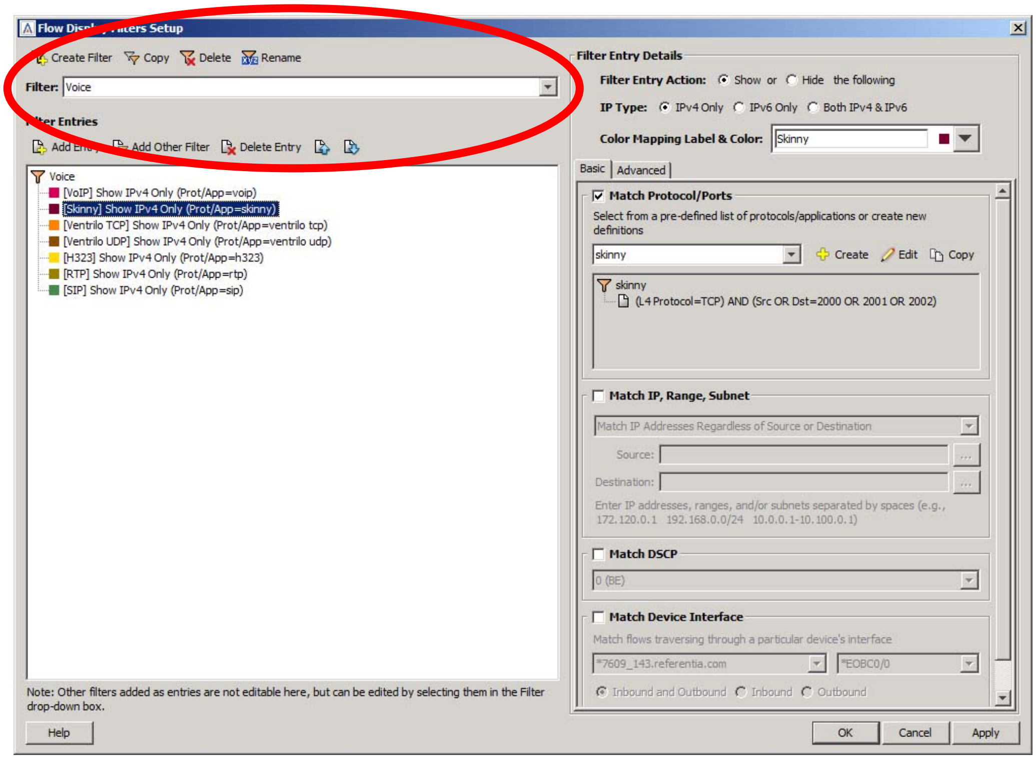
□ Match Device Interface

Match flows traversing through a particular device's interface

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

4. In the Filter selection pull-down, select the Voice Filter



Flow Disp... ...ters Setup

Create Filter | Copy | Delete | Rename

Filter: Voice

...ter Entries

Add Ent... | Add Other Filter | Delete Entry

Voice
- [VoIP] Show IPv4 Only (Prot/App=voip)
- [Skinny] Show IPv4 Only (Prot/App=skinny)
- [Ventrilo TCP] Show IPv4 Only (Prot/App=ventrilo tcp)
- [Ventrilo UDP] Show IPv4 Only (Prot/App=ventrilo udp)
- [H323] Show IPv4 Only (Prot/App=h323)
- [RTP] Show IPv4 Only (Prot/App=rtp)
- [SIP] Show IPv4 Only (Prot/App=sip)

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: Skinny

Basic | Advanced

☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

skinny | Create | Edit | Copy

skinny
(L4 Protocol=TCP) AND (Src OR Dst=2000 OR 2001 OR 2002)

☐ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

☐ Match DSCP

0 (BE)

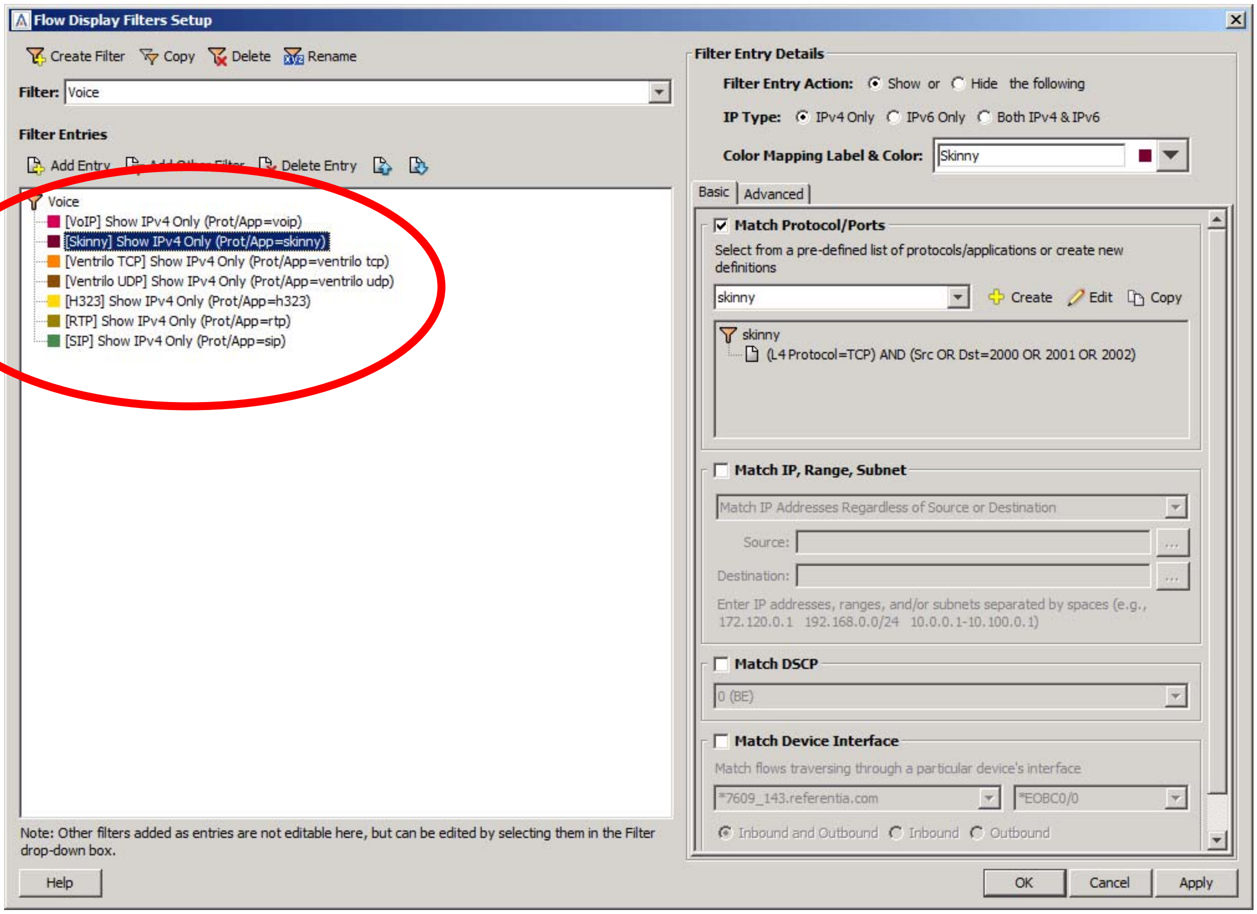
☐ Match Device Interface

Match flows traversing through a particular device's interface

*7609_143.referentia.com | *EOBC0/0

● Inbound and Outbound ○ Inbound ○ Outbound

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



Flow Display Filters Setup

Create Filter | Copy | Delete | Rename

Filter: Voice

Filter Entries

Add Entry | Add Other Filter | Delete Entry

Voice
- [VoIP] Show IPv4 Only (Prot/App=voip)
- [Skinny] Show IPv4 Only (Prot/App=skinny)
- [Ventrilo TCP] Show IPv4 Only (Prot/App=ventrilo tcp)
- [Ventrilo UDP] Show IPv4 Only (Prot/App=ventrilo udp)
- [H323] Show IPv4 Only (Prot/App=h323)
- [RTP] Show IPv4 Only (Prot/App=rtp)
- [SIP] Show IPv4 Only (Prot/App=sip)

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: Skinny

Basic | Advanced

☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

skinny | Create | Edit | Copy

skinny
(L4 Protocol=TCP) AND (Src OR Dst=2000 OR 2001 OR 2002)

☐ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

☐ Match DSCP

0 (BE)

☐ Match Device Interface

Match flows traversing through a particular device's interface

*7609_143.referentia.com | *EOBC0/0

● Inbound and Outbound ○ Inbound ○ Outbound

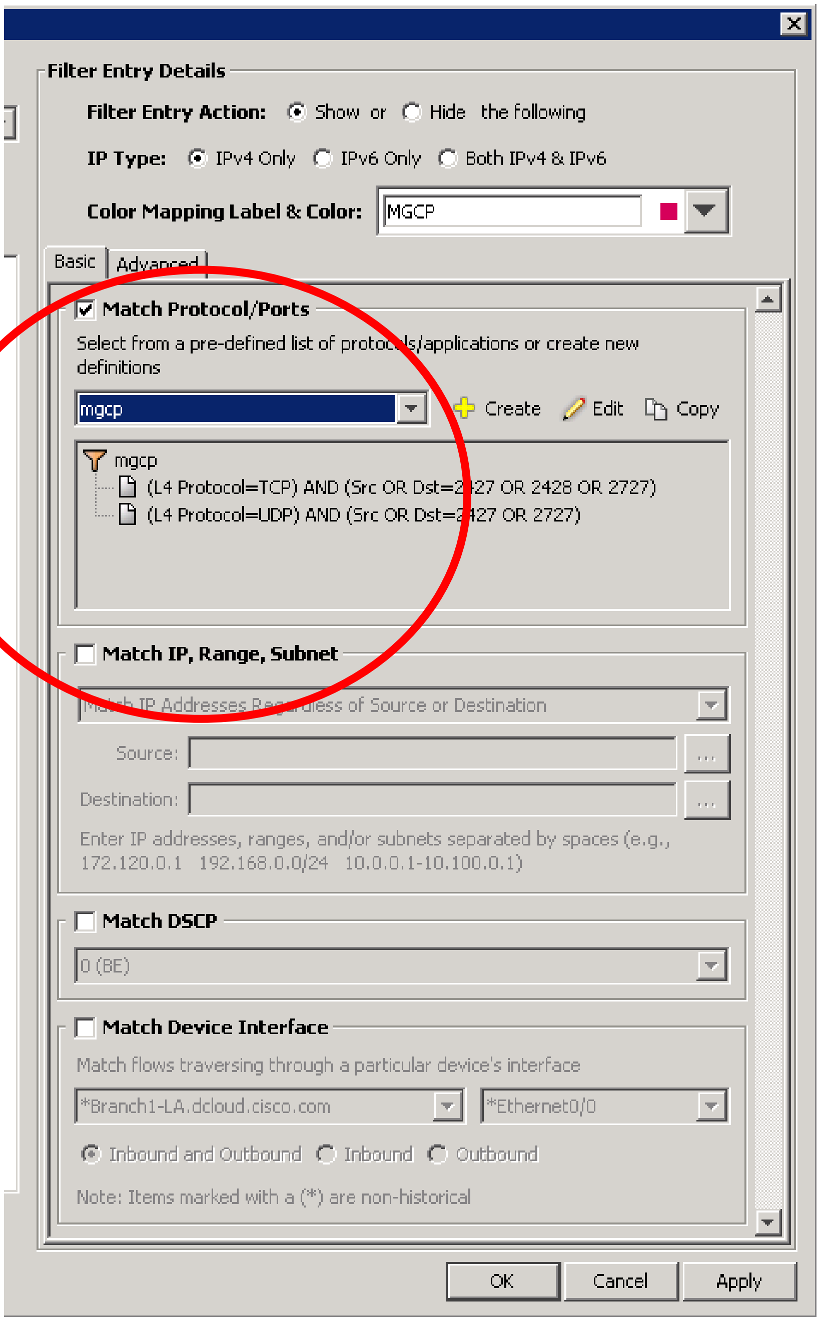
5. Delete unused Entries

   a. VoIP
   b. Ventrilo TCP
   c. Ventrilo UDP

6. Add Entry

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

7. Name it MGCP
8. Tick “Match Protocols/Ports”
9. In the dropdown, select MGCP



**Filter Entry Details**

**Filter Entry Action:** ● Show or ○ Hide the following

**IP Type:** ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

**Color Mapping Label & Color:** MGCP 🟥

Basic | Advanced

☑ **Match Protocol/Ports**

Select from a pre-defined list of protocols/applications or create new definitions

mgcp

mgcp
(L4 Protocol=TCP) AND (Src OR Dst=2427 OR 2428 OR 2727)
(L4 Protocol=UDP) AND (Src OR Dst=2427 OR 2727)

□ **Match IP, Range, Subnet**

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ **Match DSCP**

0 (BE)

□ **Match Device Interface**

Match flows traversing through a particular device's interface

*Branch1-LA.dcloud.cisco.com *Ethernet0/0

● Inbound and Outbound ○ Inbound ○ Outbound

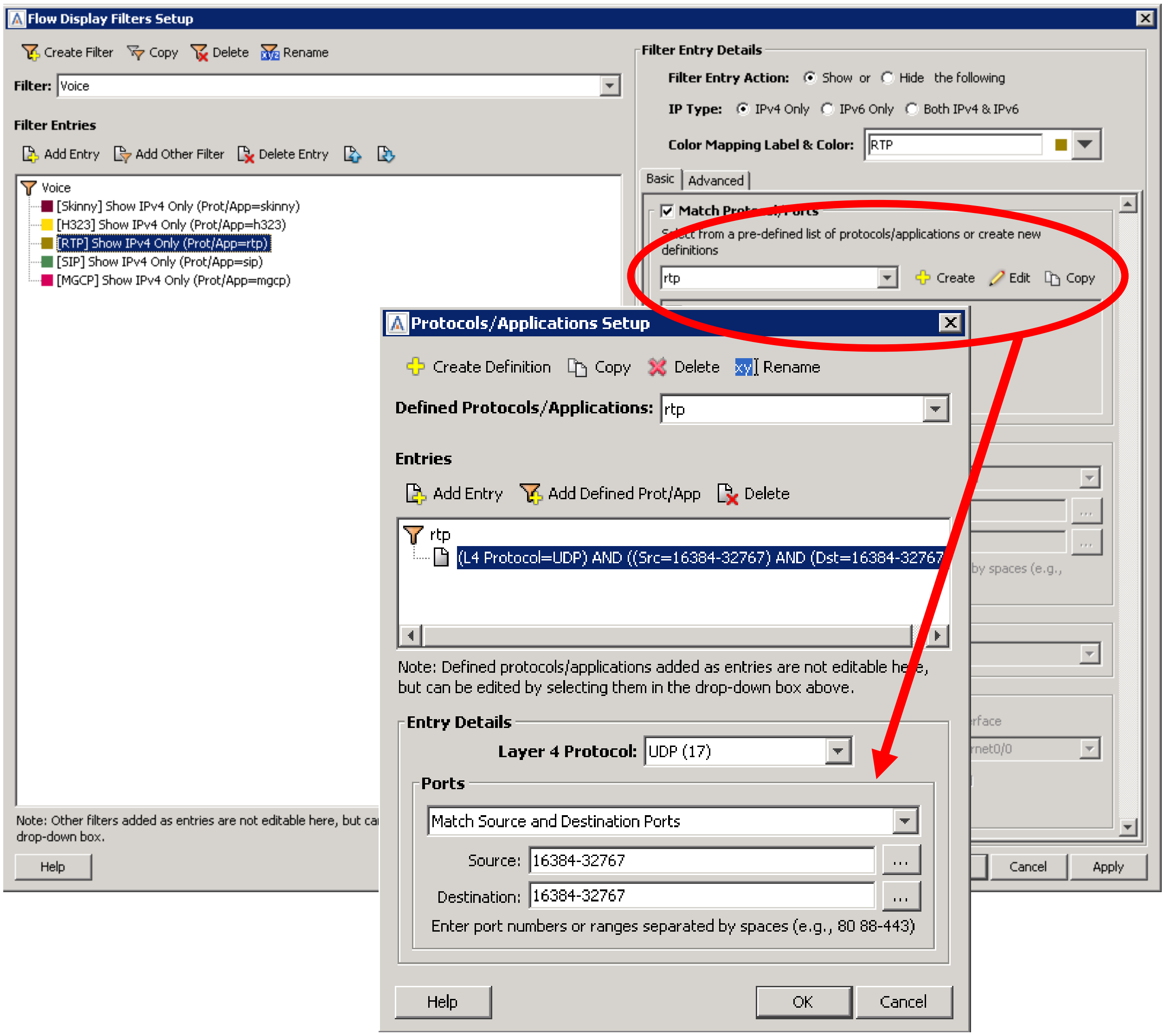
Note: Items marked with a (*) are non-historical

Edit Entries the following entries with these updates:

H323 - TCP/UDP = Src or Dst = 1718 1719 1720

SIP - TCP/UDP = Src or Dst = 5060 5061 5062

RTP - UDP = Src AND Dst = 16384-32767



Filter: Voice

Voice
- [Skinny] Show IPv4 Only (Prot/App=skinny)
- [H323] Show IPv4 Only (Prot/App=h323)
- [RTP] Show IPv4 Only (Prot/App=rtp)
- [SIP] Show IPv4 Only (Prot/App=sip)
- [MGCP] Show IPv4 Only (Prot/App=mgcp)

Note: Other filters added as entries are not editable here, but ca drop-down box.

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: RTP

☑ Match Protocols/Ports

Select from a pre-defined list of protocols/applications or create new definitions

rtp

Defined Protocols/Applications: rtp

rtp
- (L4 Protocol=UDP) AND ((Src=16384-32767) AND (Dst=16384-32767

Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.

Layer 4 Protocol: UDP (17)

Match Source and Destination Ports

Source: 16384-32767

Destination: 16384-32767

Enter port numbers or ranges separated by spaces (e.g., 80 88-443)

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

    a. MGCP - TCP/UDP = Src **OR** Dst = 2427 2727 & TCP = Src or Dst = 2428
    b. H323 - TCP/UDP = Src **OR** Dst = 1718 1719 1720
    c. SIP - TCP/UDP = Src **OR** Dst = 5060 5061 5062
    d. RTP - UDP = Src **AND** Dst = 16384-32767

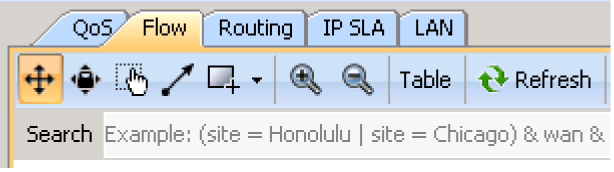
**Note: This updated voice filter will work well for our Lab purposes, but in a real networks, it would probably be best to also include IP addresses and/or subnets to these filters for eliminating any false positives.**

# Lab 1.3: Validating Filters

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

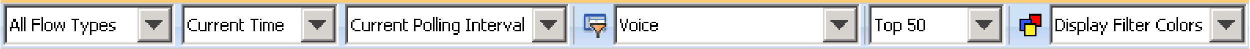
Lab Steps:

1. From the LiveNX Client map, select the Flow Tab



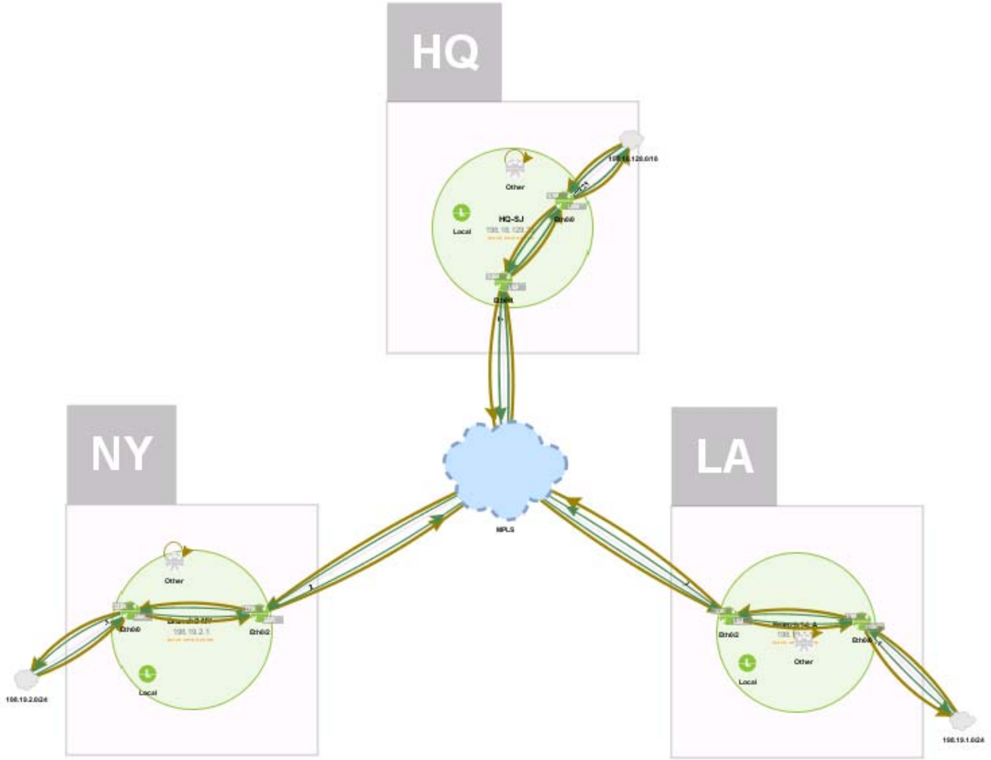
Search: Example: (site = Honolulu | site = Chicago) & wan &

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

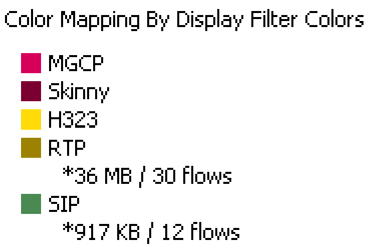


All Flow Types | Current Time | Current Polling Interval | Voice | Top 50 | Display Filter Colors

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



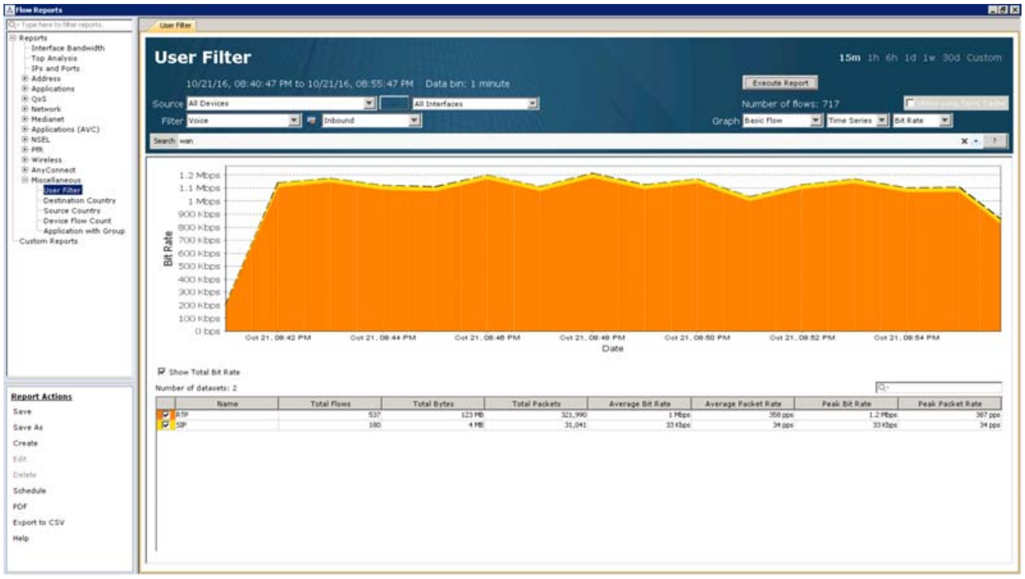
Confirm in the legend there is Voice traffic being matched.  You should see RTP & SIP being matched.



Color Mapping By Display Filter Colors

🟥 MGCP
🟫 Skinny
🟨 H323
🟫 RTP
*36 MB / 30 flows
🟩 SIP
*917 KB / 12 flows

3. Run the Miscellaneous > **User Filter** report
   a. Select the Voice filter, but leave all parameters at their default settings
   b. Implement a Search of “wan”
   c. **Execute Report**



User Filter

10/21/16, 08:40:47 PM to 10/21/16, 08:55:47 PM Data bin: 1 minute

Source: All Devices / All Interfaces

Filter: Voice / Inbound

Number of flows: 717

Graph: Basic Flow / Time Series / Bit Rate

Search: wan

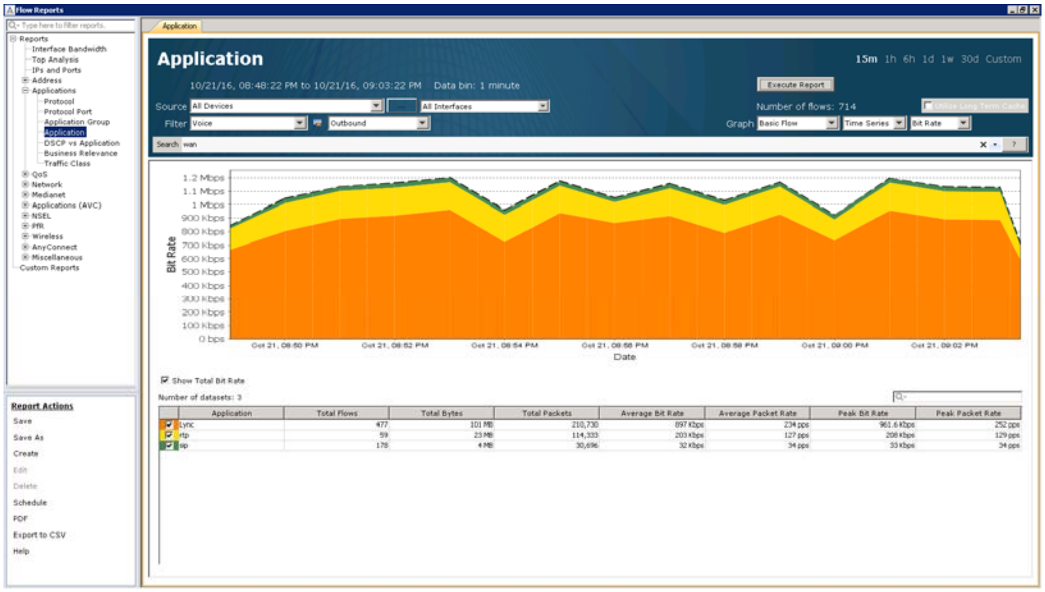
☑ Show Total Bit Rate

Number of datasets: 2

| | Name | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | RTP | 537 | 123 MB | 321,990 | 1 Mbps | 358 pps | 1.2 Mbps | 387 pps |
| ☑ | SIP | 180 | 4 MB | 31,041 | 33 Kbps | 34 pps | 33 Kbps | 34 pps |

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

4. Run the Reports > Flow > Applications > **Application** report
   a. Select the Voice filter, but leave all parameters at their default settings
   b. Implement a Search of “wan”
   c. **Execute Report**



Application

10/21/16, 08:48:22 PM to 10/21/16, 09:03:22 PM Data bin: 1 minute

Source: All Devices / All Interfaces

Filter: Voice / Outbound

Number of flows: 714

Graph: Basic Flow / Time Series / Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 3

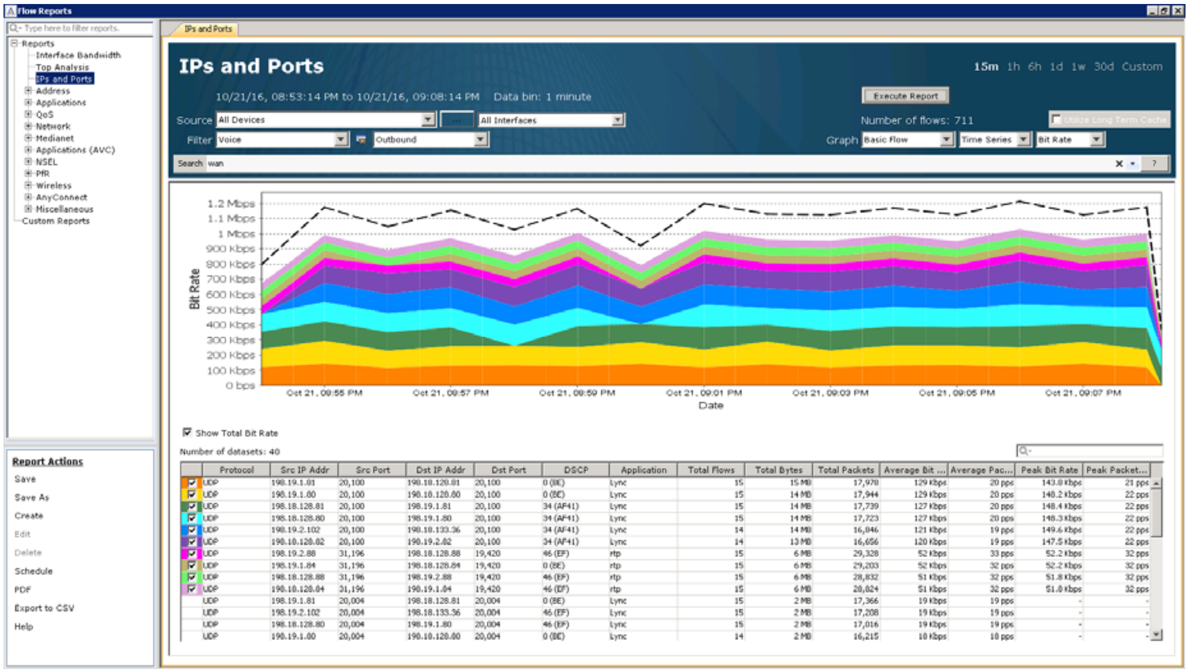
| | Application | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | Lync | 477 | 101 MB | 210,730 | 897 Kbps | 234 pps | 961.6 Kbps | 252 pps |
| ☑ | rtp | 59 | 23 MB | 114,333 | 203 Kbps | 127 pps | 208 Kbps | 129 pps |
| ☑ | sip | 178 | 4 MB | 30,696 | 32 Kbps | 34 pps | 33 Kbps | 34 pps |

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

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

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

5. Run the Reports > Flow > **IPs and Application** report
   a. Select the Voice filter, but leave all parameters at their default settings
   b. Implement a Search of "wan"
   c. **Execute Report**



IPs and Ports

10/21/16, 08:53:14 PM to 10/21/16, 09:08:14 PM    Data bin: 1 minute

Source: All Devices    All Interfaces

Filter: Voice    Outbound

Number of flows: 711

Graph: Basic Flow    Time Series    Bit Rate

Search: wan

☑ Show Total Bit Rate

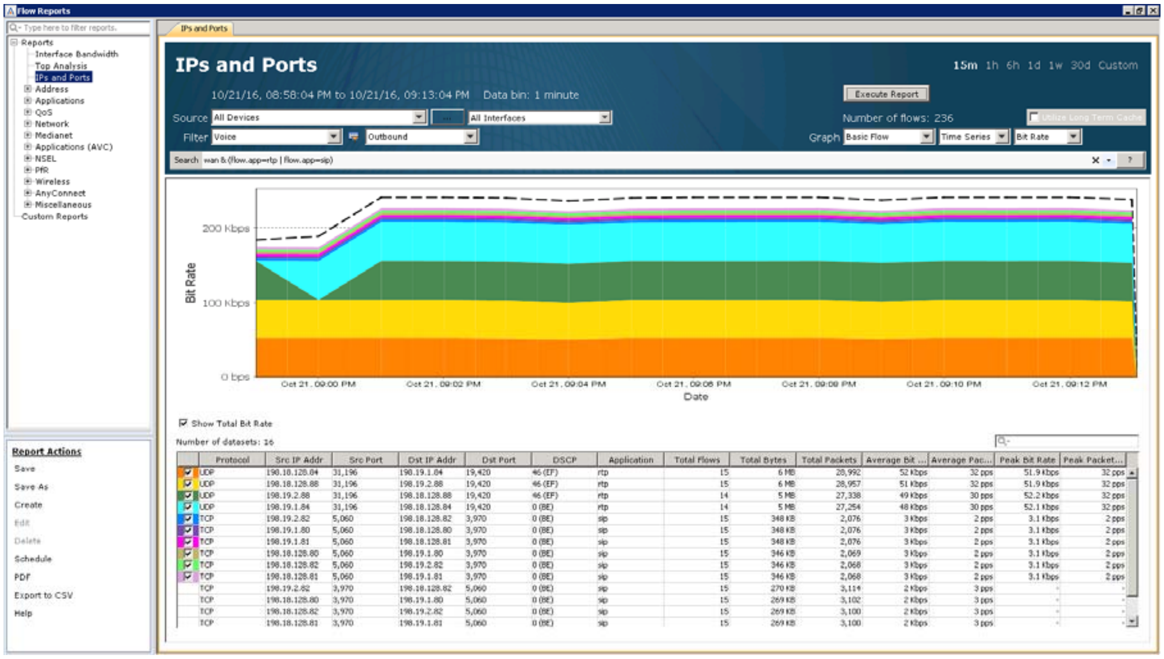
Number of datasets: 40

| | Protocol | Src IP Addr | Src Port | Dst IP Addr | Dst Port | DSCP | Application | Total Flows | Total Bytes | Total Packets | Average Bit ... | Average Pac... | Peak Bit Rate | Peak Packet... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | UDP | 198.19.1.81 | 20,100 | 198.18.128.81 | 20,100 | 0 (BE) | Lync | 15 | 15 MB | 17,978 | 129 Kbps | 20 pps | 143.8 Kbps | 21 pps |
| ☑ | UDP | 198.19.1.80 | 20,100 | 198.18.128.80 | 20,100 | 0 (BE) | Lync | 15 | 14 MB | 17,944 | 129 Kbps | 20 pps | 148.2 Kbps | 22 pps |
| ☑ | UDP | 198.18.128.81 | 20,100 | 198.19.1.81 | 20,100 | 34 (AF41) | Lync | 15 | 14 MB | 17,739 | 127 Kbps | 20 pps | 148.4 Kbps | 22 pps |
| ☑ | UDP | 198.18.128.80 | 20,100 | 198.19.1.80 | 20,100 | 34 (AF41) | Lync | 15 | 14 MB | 17,723 | 127 Kbps | 20 pps | 148.3 Kbps | 22 pps |
| ☑ | UDP | 198.19.2.102 | 20,100 | 198.18.133.36 | 20,100 | 34 (AF41) | Lync | 14 | 14 MB | 16,846 | 121 Kbps | 19 pps | 149.6 Kbps | 22 pps |
| ☑ | UDP | 198.18.128.82 | 20,100 | 198.19.2.82 | 20,100 | 34 (AF41) | Lync | 14 | 13 MB | 16,656 | 120 Kbps | 19 pps | 147.5 Kbps | 22 pps |
| ☑ | UDP | 198.19.2.88 | 31,196 | 198.18.128.88 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 29,328 | 52 Kbps | 33 pps | 52.2 Kbps | 32 pps |
| ☑ | UDP | 198.19.1.84 | 31,196 | 198.18.128.84 | 19,420 | 0 (BE) | rtp | 15 | 6 MB | 29,203 | 52 Kbps | 32 pps | 52.2 Kbps | 32 pps |
| ☑ | UDP | 198.18.128.88 | 31,196 | 198.19.2.88 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,832 | 51 Kbps | 32 pps | 51.8 Kbps | 32 pps |
| ☑ | UDP | 198.18.128.84 | 31,196 | 198.19.1.84 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,824 | 51 Kbps | 32 pps | 51.8 Kbps | 32 pps |
| | UDP | 198.19.1.81 | 20,004 | 198.18.128.81 | 20,004 | 0 (BE) | Lync | 15 | 2 MB | 17,366 | 19 Kbps | 19 pps | - | - |
| | UDP | 198.19.2.102 | 20,004 | 198.18.133.36 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,208 | 19 Kbps | 19 pps | - | - |
| | UDP | 198.18.128.80 | 20,004 | 198.19.1.80 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,016 | 19 Kbps | 19 pps | - | - |
| | UDP | 198.19.1.80 | 20,004 | 198.18.128.80 | 20,004 | 0 (BE) | Lync | 14 | 2 MB | 16,215 | 18 Kbps | 18 pps | - | - |

Notice the ports for Lync and rtp are in the same range of 16384-32767.

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

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



IPs and Ports

10/21/16, 08:58:04 PM to 10/21/16, 09:13:04 PM Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: Voice | Outbound

Number of flows: 236

Graph: Basic Flow | Time Series | Bit Rate

Search: wan & (flow.app=rtp | flow.app=sip)

☑ Show Total Bit Rate

Number of datasets: 16

| | Protocol | Src IP Addr | Src Port | Dst IP Addr | Dst Port | DSCP | Application | Total Flows | Total Bytes | Total Packets | Average Bit ... | Average Pac... | Peak Bit Rate | Peak Packet... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | UDP | 198.18.128.84 | 31,196 | 198.19.1.84 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,992 | 52 Kbps | 32 pps | 51.9 Kbps | 32 pps |
| ☑ | UDP | 198.18.128.88 | 31,196 | 198.19.2.88 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,957 | 51 Kbps | 32 pps | 51.9 Kbps | 32 pps |
| ☑ | UDP | 198.19.2.88 | 31,196 | 198.18.128.88 | 19,420 | 46 (EF) | rtp | 14 | 5 MB | 27,338 | 49 Kbps | 30 pps | 52.2 Kbps | 32 pps |
| ☑ | UDP | 198.19.1.84 | 31,196 | 198.18.128.84 | 19,420 | 0 (BE) | rtp | 14 | 5 MB | 27,254 | 48 Kbps | 30 pps | 52.1 Kbps | 32 pps |
| ☑ | TCP | 198.19.2.82 | 5,060 | 198.18.128.82 | 3,970 | 0 (BE) | sip | 15 | 348 KB | 2,076 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| ☑ | TCP | 198.19.1.80 | 5,060 | 198.18.128.80 | 3,970 | 0 (BE) | sip | 15 | 348 KB | 2,076 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| ☑ | TCP | 198.19.1.81 | 5,060 | 198.18.128.81 | 3,970 | 0 (BE) | sip | 15 | 348 KB | 2,076 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| ☑ | TCP | 198.18.128.80 | 5,060 | 198.19.1.80 | 3,970 | 0 (BE) | sip | 15 | 346 KB | 2,069 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| ☑ | TCP | 198.18.128.82 | 5,060 | 198.19.2.82 | 3,970 | 0 (BE) | sip | 15 | 346 KB | 2,068 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| ☑ | TCP | 198.18.128.81 | 5,060 | 198.19.1.81 | 3,970 | 0 (BE) | sip | 15 | 346 KB | 2,068 | 3 Kbps | 2 pps | 3.1 Kbps | 2 pps |
| | TCP | 198.19.2.82 | 3,970 | 198.18.128.82 | 5,060 | 0 (BE) | sip | 15 | 270 KB | 3,114 | 2 Kbps | 3 pps | - | - |
| | TCP | 198.18.128.80 | 3,970 | 198.19.1.80 | 5,060 | 0 (BE) | sip | 15 | 269 KB | 3,102 | 2 Kbps | 3 pps | - | - |
| | TCP | 198.18.128.82 | 3,970 | 198.19.2.82 | 5,060 | 0 (BE) | sip | 15 | 269 KB | 3,100 | 2 Kbps | 3 pps | - | - |
| | TCP | 198.18.128.81 | 3,970 | 198.19.1.81 | 5,060 | 0 (BE) | sip | 15 | 269 KB | 3,100 | 2 Kbps | 3 pps | - | - |

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

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

# Lab 2

## Lab 2:  Classification & Marking

# Lab 2.1: QoS Class Models

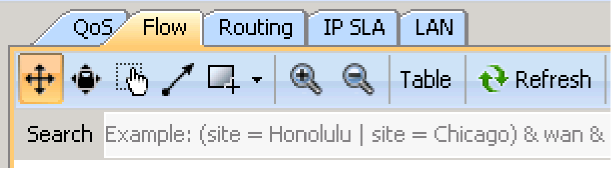
Now that we have used LiveNX's Filter and Search capabilities to accurately identify and understand the business critical traffic, we need to assign DSCP markings (QoS tags) on the traffic. In this lab, we are going to use the following 5 class QoS model:

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

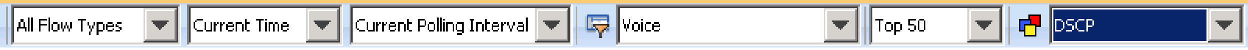
We need to now update the legends in LiveNX to understand these selected DSCP values of interest.

Lab Steps:

1. From the LiveNX Client, select the Flow Tab

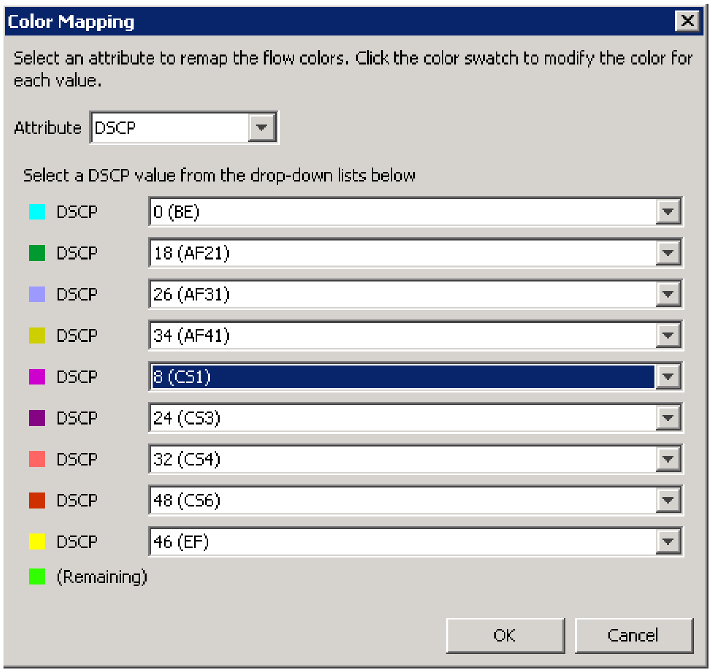


2. From the options at the top of the map, select the 🟥 icon:



3. Set the Attribute to DSCP

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



**Color Mapping**

Select an attribute to remap the flow colors. Click the color swatch to modify the color for each value.

Attribute DSCP

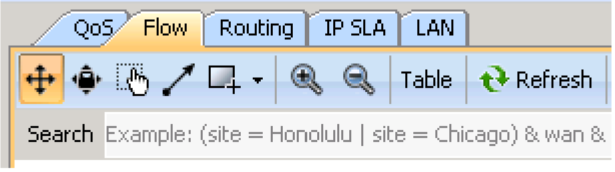
Select a DSCP value from the drop-down lists below

| | | |
|---|---|---|
| 🟦 | DSCP | 0 (BE) |
| 🟩 | DSCP | 18 (AF21) |
| 🟪 | DSCP | 26 (AF31) |
| 🟨 | DSCP | 34 (AF41) |
| 🟪 | DSCP | 8 (CS1) |
| 🟪 | DSCP | 24 (CS3) |
| 🟥 | DSCP | 32 (CS4) |
| 🟥 | DSCP | 48 (CS6) |
| 🟨 | DSCP | 46 (EF) |
| 🟩 | (Remaining) | |

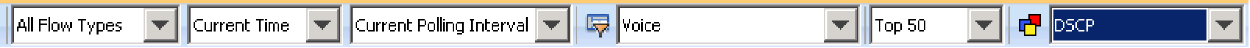
# Lab 2.2: Validate DSCP Markings

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

1. From the LiveAction map, select the Flow Tab

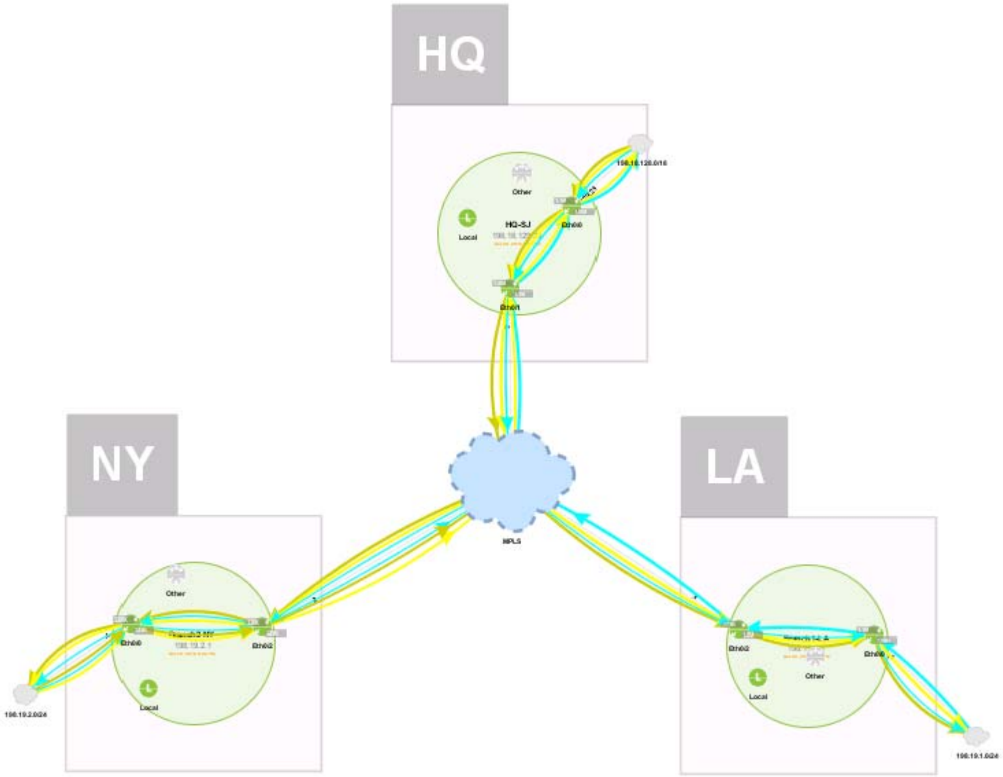


2. From the options at the top of the map, select the following options

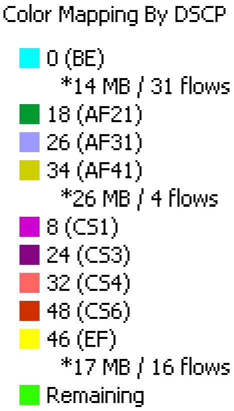


All Flow Types | Current Time | Current Polling Interval | Voice | Top 50 | DSCP

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



3. Confirm in the legend what DSCP values are seen.

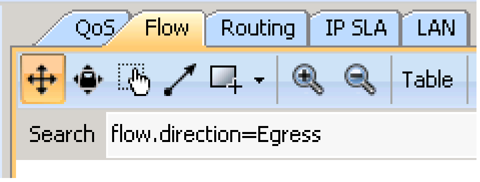


Color Mapping By DSCP

- 🟦 0 (BE)
  *14 MB / 31 flows
- 🟩 18 (AF21)
- 🟪 26 (AF31)
- 🟨 34 (AF41)
  *26 MB / 4 flows
- 🟪 8 (CS1)
- 🟪 24 (CS3)
- 🟥 32 (CS4)
- 🟥 48 (CS6)
- 🟨 46 (EF)
  *17 MB / 16 flows
- 🟩 Remaining

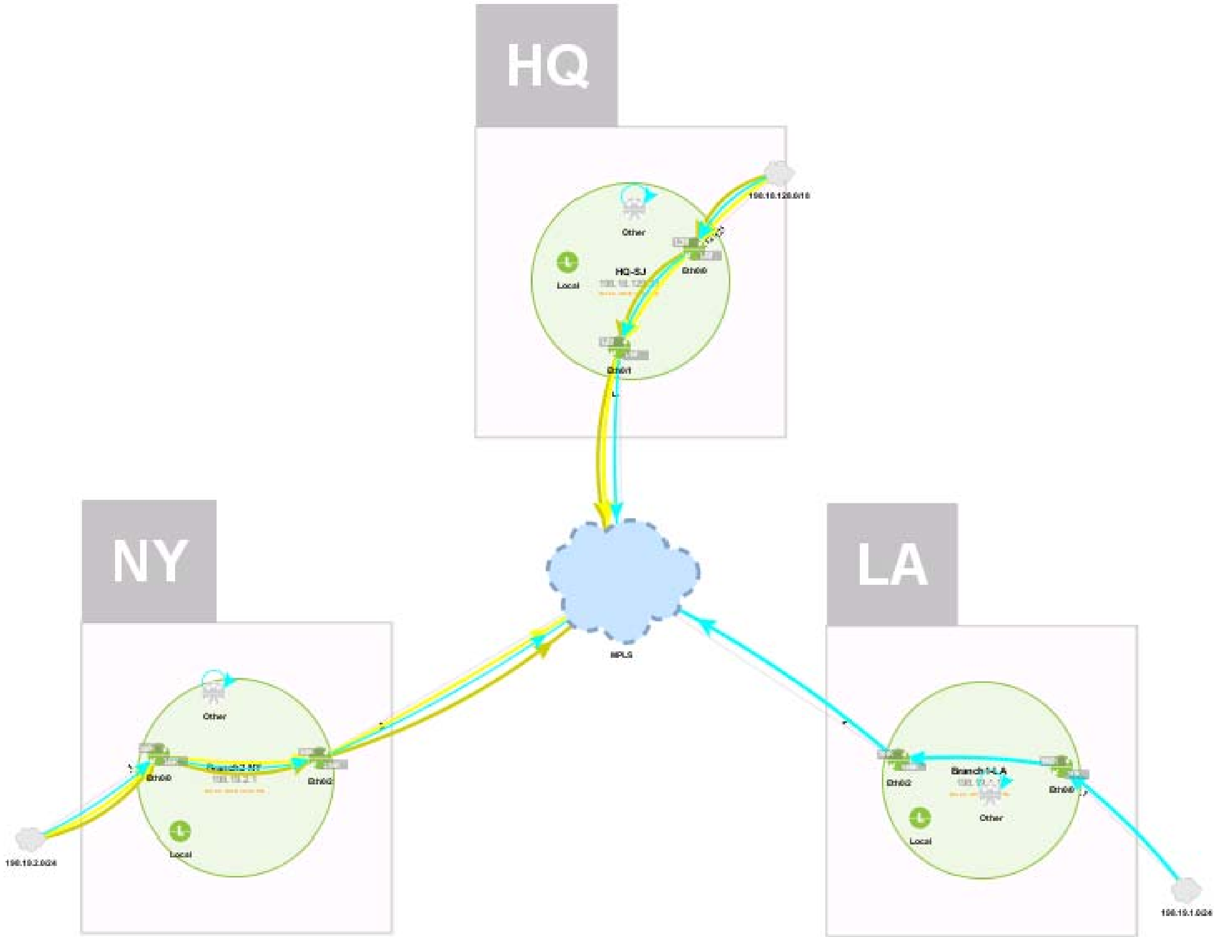
Since we have the Voice Filter in place, we would hope to only see EF and/or AF31 per the 5 Class QoS model that was chosen for this network. Because there are more values seen, we will further narrow the scope of the filter.

4. Update the Search to "flow.direction=Egress"



Search flow.direction=Egress

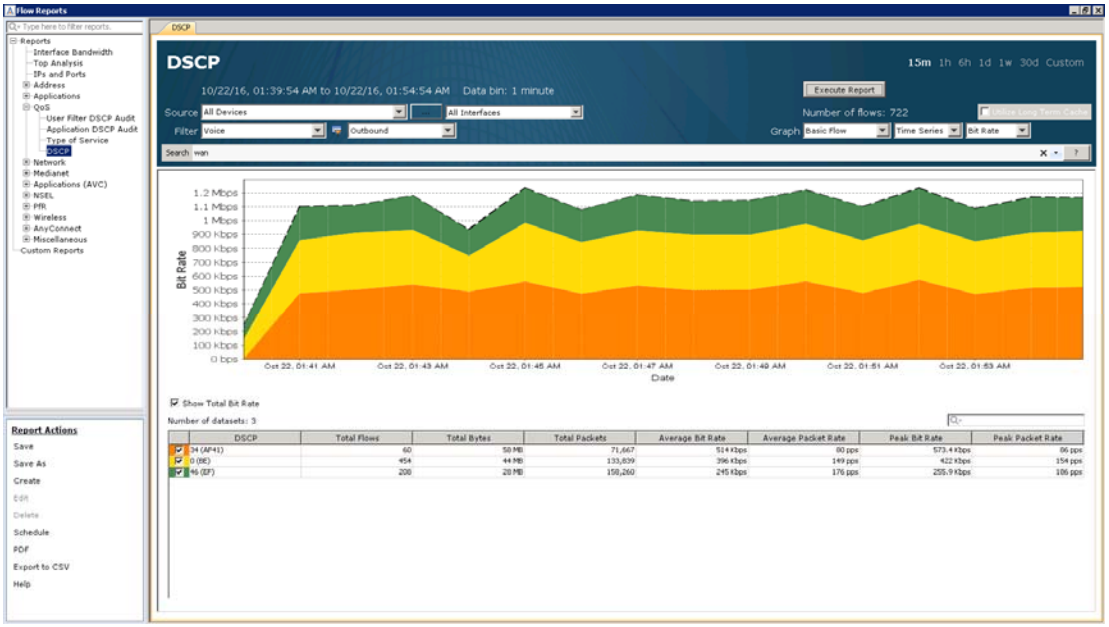
Notice that all traffic leaving LA is DSCP 0(BE) (light blue). That is *definitely not* correct.



**Note:** In subsequent labs the traffic specified in these labs may NOT be available due to timing of the replays, or traffic availability. You may try looking for alternate types of traffic. The intent of these labs is to demonstrate the settings and *process* for using filters, not necessarily the specific traffic found.

We’ll use LiveNX Client reports to investigate further.

5. Run the Reports > Flow > QoS > **DSCP** report
   a. Select the Voice filter, but leave all parameters at their default settings
   b. Implement a Search of “wan”
   c. **Execute Report**



DSCP

10/22/16, 01:39:54 AM to 10/22/16, 01:54:54 AM  Data bin: 1 minute

Source: All Devices  All Interfaces

Filter: Voice  Outbound

Number of flows: 722

Graph: Basic Flow  Time Series  Bit Rate

Search: wan

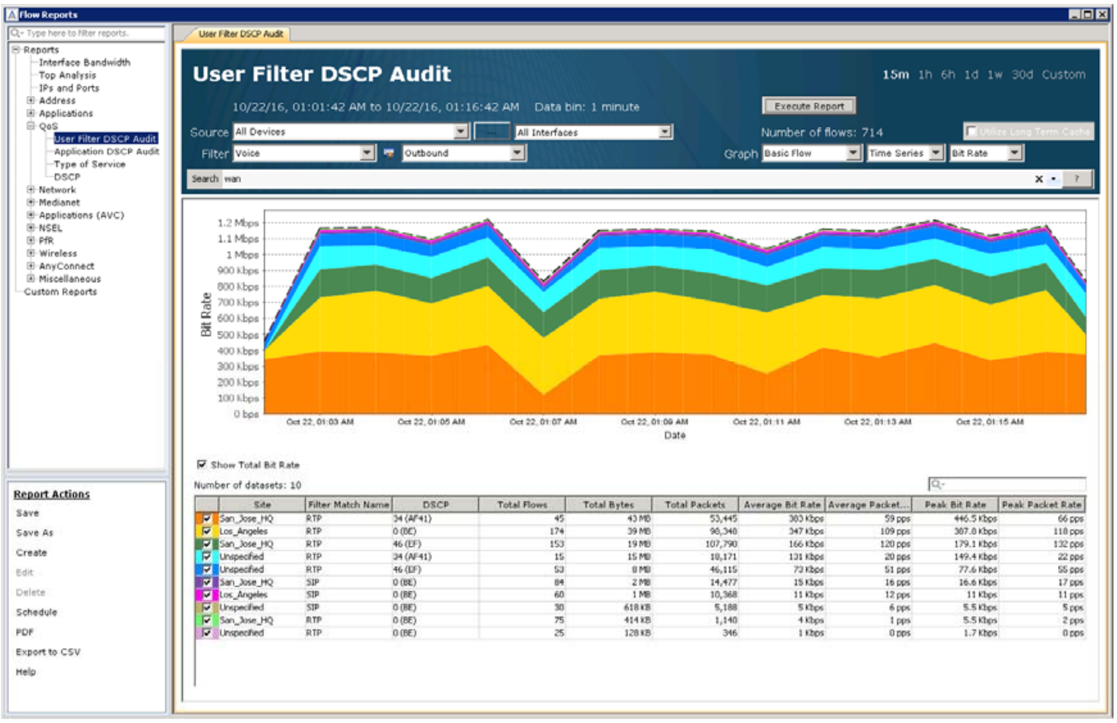
☑ Show Total Bit Rate

Number of datasets: 3

| | DSCP | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | 34 (AF41) | 60 | 58 MB | 71,667 | 514 Kbps | 80 pps | 573.4 Kbps | 86 pps |
| ☑ | 0 (BE) | 454 | 44 MB | 133,839 | 396 Kbps | 149 pps | 422 Kbps | 154 pps |
| ☑ | 46 (EF) | 208 | 28 MB | 158,260 | 245 Kbps | 176 pps | 255.9 Kbps | 186 pps |

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

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



User Filter DSCP Audit

10/22/16, 01:01:42 AM to 10/22/16, 01:16:42 AM   Data bin: 1 minute

Source: All Devices   All Interfaces

Number of flows: 714

Filter: Voice   Outbound

Graph: Basic Flow   Time Series   Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 10

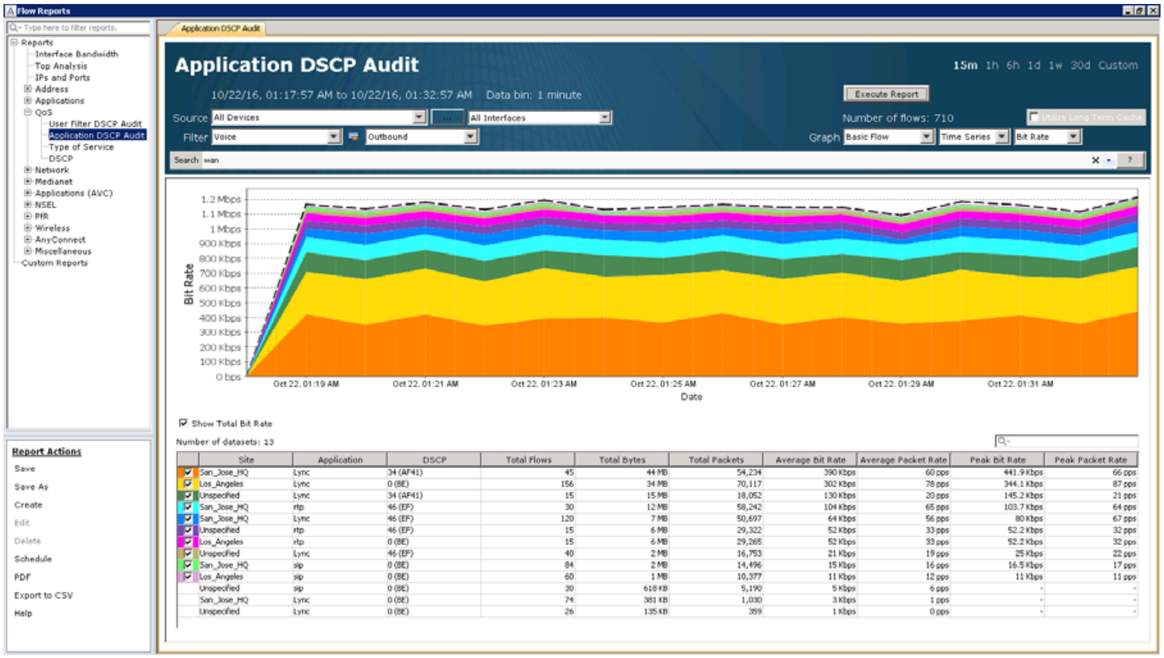
| | Site | Filter Match Name | DSCP | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet... | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | San_Jose_HQ | RTP | 34 (AF41) | 45 | 43 MB | 53,445 | 383 Kbps | 59 pps | 446.5 Kbps | 66 pps |
| ☑ | Los_Angeles | RTP | 0 (BE) | 174 | 39 MB | 98,340 | 347 Kbps | 109 pps | 387.8 Kbps | 118 pps |
| ☑ | San_Jose_HQ | RTP | 46 (EF) | 153 | 19 MB | 107,790 | 166 Kbps | 120 pps | 179.1 Kbps | 132 pps |
| ☑ | Unspecified | RTP | 34 (AF41) | 15 | 15 MB | 18,171 | 131 Kbps | 20 pps | 149.4 Kbps | 22 pps |
| ☑ | Unspecified | RTP | 46 (EF) | 53 | 8 MB | 46,115 | 73 Kbps | 51 pps | 77.6 Kbps | 55 pps |
| ☑ | San_Jose_HQ | SIP | 0 (BE) | 84 | 2 MB | 14,477 | 15 Kbps | 16 pps | 16.6 Kbps | 17 pps |
| ☑ | Los_Angeles | SIP | 0 (BE) | 60 | 1 MB | 10,368 | 11 Kbps | 12 pps | 11 Kbps | 11 pps |
| ☑ | Unspecified | SIP | 0 (BE) | 30 | 618 KB | 5,188 | 5 Kbps | 6 pps | 5.5 Kbps | 5 pps |
| ☑ | San_Jose_HQ | RTP | 0 (BE) | 75 | 414 KB | 1,140 | 4 Kbps | 1 pps | 5.5 Kbps | 2 pps |
| ☑ | Unspecified | RTP | 0 (BE) | 25 | 128 KB | 346 | 1 Kbps | 0 pps | 1.7 Kbps | 0 pps |

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

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

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

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



Application DSCP Audit

10/22/16, 01:17:57 AM to 10/22/16, 01:32:57 AM Data bin: 1 minute

Source: All Devices, All Interfaces

Filter: Voice, Outbound

Number of flows: 710

Graph: Basic Flow, Time Series, Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 13

| | Site | Application | DSCP | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | San_Jose_HQ | Lync | 34 (AF41) | 45 | 44 MB | 54,234 | 390 Kbps | 60 pps | 441.9 Kbps | 66 pps |
| ☑ | Los_Angeles | Lync | 0 (BE) | 156 | 34 MB | 70,117 | 302 Kbps | 78 pps | 344.1 Kbps | 87 pps |
| ☑ | Unspecified | Lync | 34 (AF41) | 15 | 15 MB | 18,052 | 130 Kbps | 20 pps | 145.2 Kbps | 21 pps |
| ☑ | San_Jose_HQ | rtp | 46 (EF) | 30 | 12 MB | 58,242 | 104 Kbps | 65 pps | 103.7 Kbps | 64 pps |
| ☑ | San_Jose_HQ | Lync | 46 (EF) | 120 | 7 MB | 50,697 | 64 Kbps | 56 pps | 80 Kbps | 67 pps |
| ☑ | Unspecified | rtp | 46 (EF) | 15 | 6 MB | 29,322 | 52 Kbps | 33 pps | 52.2 Kbps | 32 pps |
| ☑ | Los_Angeles | rtp | 0 (BE) | 15 | 6 MB | 29,265 | 52 Kbps | 33 pps | 52.2 Kbps | 32 pps |
| ☑ | Unspecified | Lync | 46 (EF) | 40 | 2 MB | 16,753 | 21 Kbps | 19 pps | 25 Kbps | 22 pps |
| ☑ | San_Jose_HQ | sip | 0 (BE) | 84 | 2 MB | 14,496 | 15 Kbps | 16 pps | 16.5 Kbps | 17 pps |
| ☑ | Los_Angeles | sip | 0 (BE) | 60 | 1 MB | 10,377 | 11 Kbps | 12 pps | 11 Kbps | 11 pps |
| | Unspecified | sip | 0 (BE) | 30 | 618 KB | 5,190 | 5 Kbps | 6 pps | - | - |
| | San_Jose_HQ | Lync | 0 (BE) | 74 | 381 KB | 1,030 | 3 Kbps | 1 pps | - | - |
| | Unspecified | Lync | 0 (BE) | 26 | 135 KB | 359 | 1 Kbps | 0 pps | - | - |

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

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

Also note where Video (MS-Lync) is showing as 46(EF).

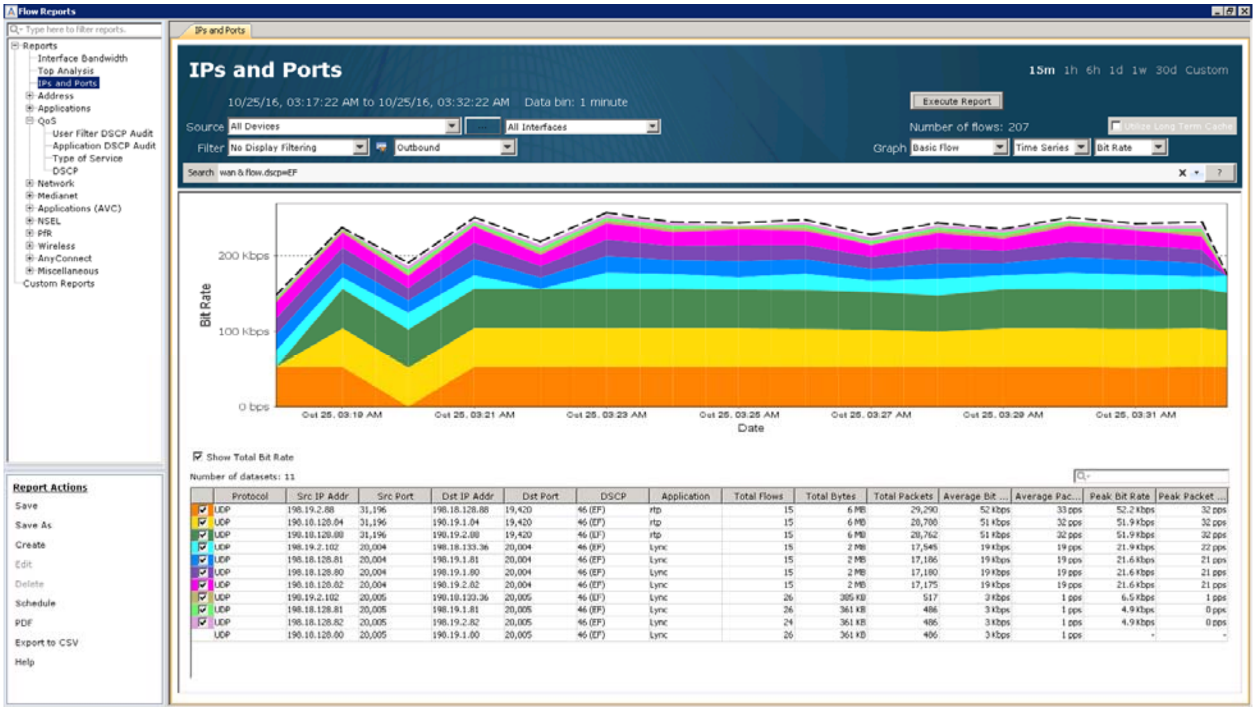
**Note: After validating the DSCP values using the Voice Filter, you would want to create more filters for the other priority applications of the network and repeat these steps.**

# Lab 2.3: Rogue DSCP Markings

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

Lab Steps:

1. Run the Reports > Flow > **IPs and Application** report.
   a. Select No Display Filter, but leave all parameters at their default settings
   b. Implement a Search of “wan & flow.dscp=EF”
   c. **Execute Report**



IPs and Ports

10/25/16, 03:17:22 AM to 10/25/16, 03:32:22 AM Data bin: 1 minute

Source: All Devices; All Interfaces

Filter: No Display Filtering; Outbound

Number of flows: 207

Graph: Basic Flow; Time Series; Bit Rate

Search: wan & flow.dscp=EF

☑ Show Total Bit Rate

Number of datasets: 11

| | Protocol | Src IP Addr | Src Port | Dst IP Addr | Dst Port | DSCP | Application | Total Flows | Total Bytes | Total Packets | Average Bit ... | Average Pac... | Peak Bit Rate | Peak Packet ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | UDP | 198.19.2.88 | 31,196 | 198.18.128.88 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 29,290 | 52 Kbps | 33 pps | 52.2 Kbps | 32 pps |
| ☑ | UDP | 198.18.128.84 | 31,196 | 198.19.1.84 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,708 | 51 Kbps | 32 pps | 51.9 Kbps | 32 pps |
| ☑ | UDP | 198.18.128.88 | 31,196 | 198.19.2.88 | 19,420 | 46 (EF) | rtp | 15 | 6 MB | 28,762 | 51 Kbps | 32 pps | 51.9 Kbps | 32 pps |
| ☑ | UDP | 198.19.2.102 | 20,004 | 198.18.133.36 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,545 | 19 Kbps | 19 pps | 21.9 Kbps | 22 pps |
| ☑ | UDP | 198.18.128.81 | 20,004 | 198.19.1.81 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,186 | 19 Kbps | 19 pps | 21.6 Kbps | 21 pps |
| ☑ | UDP | 198.18.128.80 | 20,004 | 198.19.1.80 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,180 | 19 Kbps | 19 pps | 21.6 Kbps | 21 pps |
| ☑ | UDP | 198.18.128.82 | 20,004 | 198.19.2.82 | 20,004 | 46 (EF) | Lync | 15 | 2 MB | 17,175 | 19 Kbps | 19 pps | 21.6 Kbps | 21 pps |
| ☑ | UDP | 198.19.2.102 | 20,005 | 198.18.133.36 | 20,005 | 46 (EF) | Lync | 26 | 385 KB | 517 | 3 Kbps | 1 pps | 6.5 Kbps | 1 pps |
| ☑ | UDP | 198.18.128.81 | 20,005 | 198.19.1.81 | 20,005 | 46 (EF) | Lync | 26 | 361 KB | 486 | 3 Kbps | 1 pps | 4.9 Kbps | 0 pps |
| ☑ | UDP | 198.18.128.82 | 20,005 | 198.19.2.82 | 20,005 | 46 (EF) | Lync | 24 | 361 KB | 486 | 3 Kbps | 1 pps | 4.9 Kbps | 0 pps |
| | UDP | 198.18.128.80 | 20,005 | 198.19.1.80 | 20,005 | 46 (EF) | Lync | 26 | 361 KB | 486 | 3 Kbps | 1 pps | - | - |

Notice the applications listed in this report.

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

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

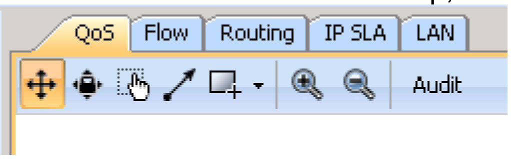
# Lab 2.4: Configure Classification & Marking Policies

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

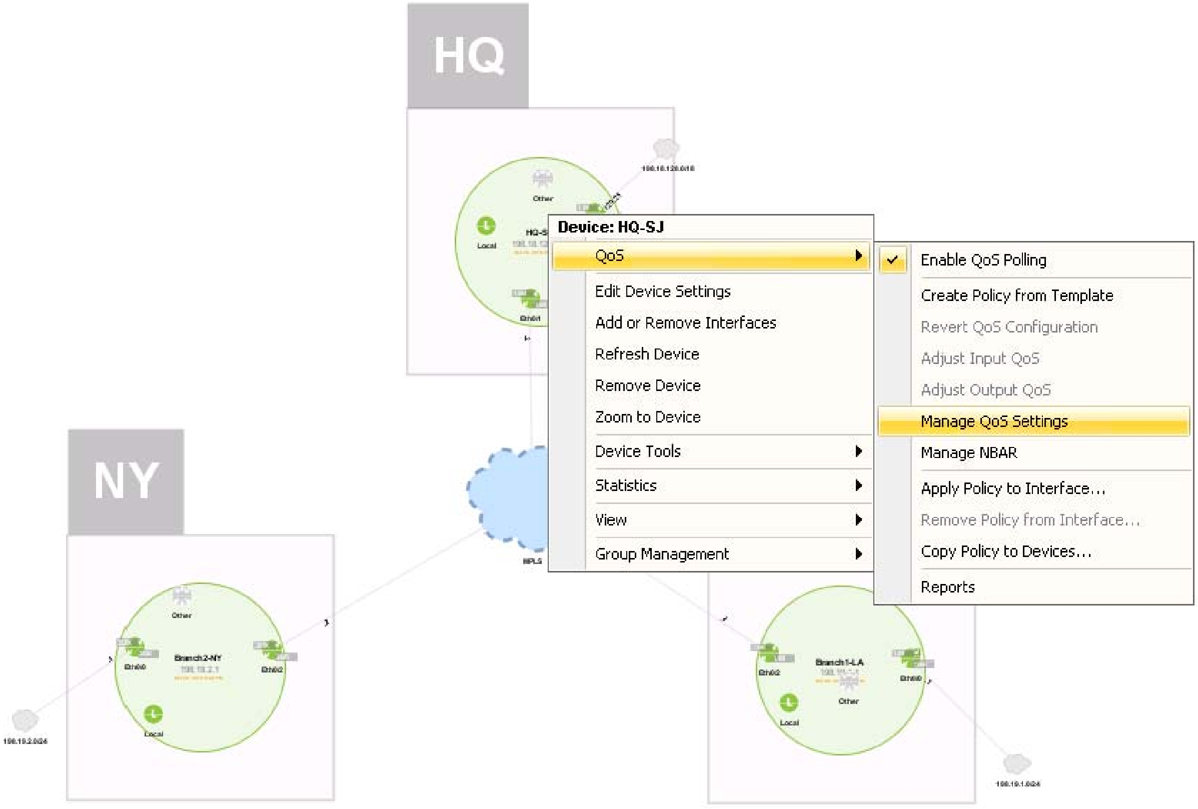
We will create a template QoS policy and apply this to the LAN interface of each of the routers to classify and mark the priority traffic properly.

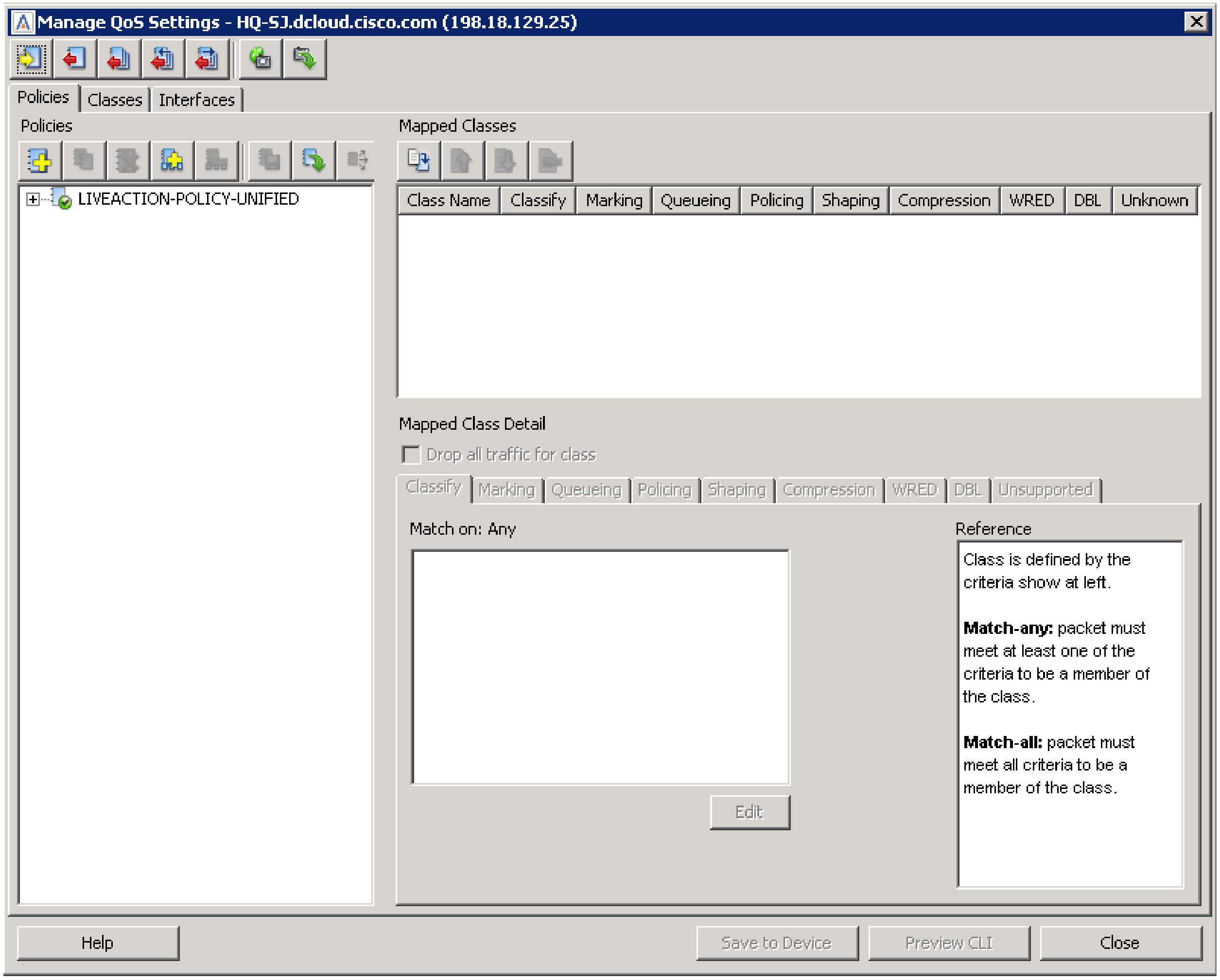
Lab Steps:

1. From the LiveAction map, select the QoS Tab



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





Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

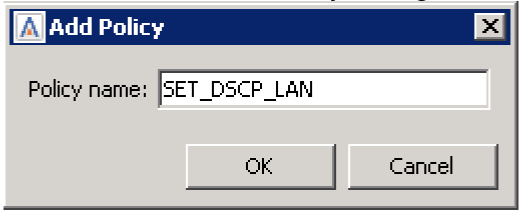
Policies | Classes | Interfaces
Policies
LIVEACTION-POLICY-UNIFIED
Mapped Classes
Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown
Mapped Class Detail
□ Drop all traffic for class
Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported
Match on: Any
Edit
Reference
Help
Save to Device
Preview CLI
Close

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

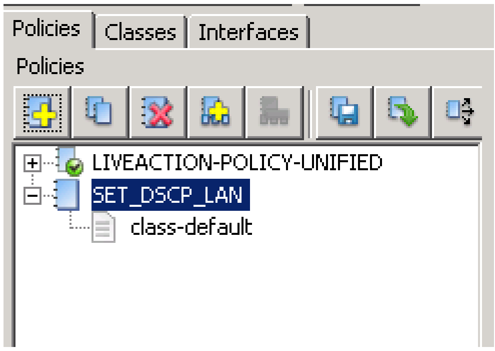
3. Select the Add Policy ➕ icon.
4. In the Add Policy dialog, enter the name “SET_DSCP_LAN”



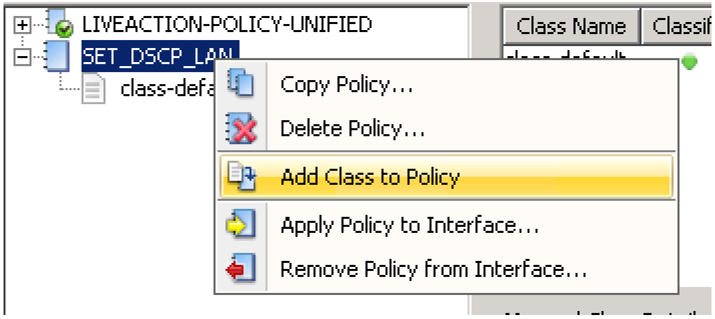
Add Policy

Policy name: SET_DSCP_LAN

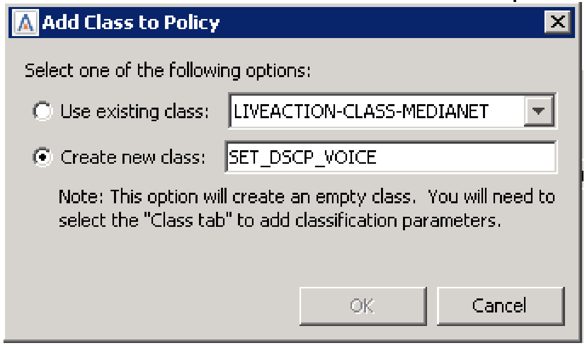
You can now see the new policy with its class-default appearing in the Policies list.



5. Right>Click on the SET_DSCP_LAN policy and select Add Class to Policy



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



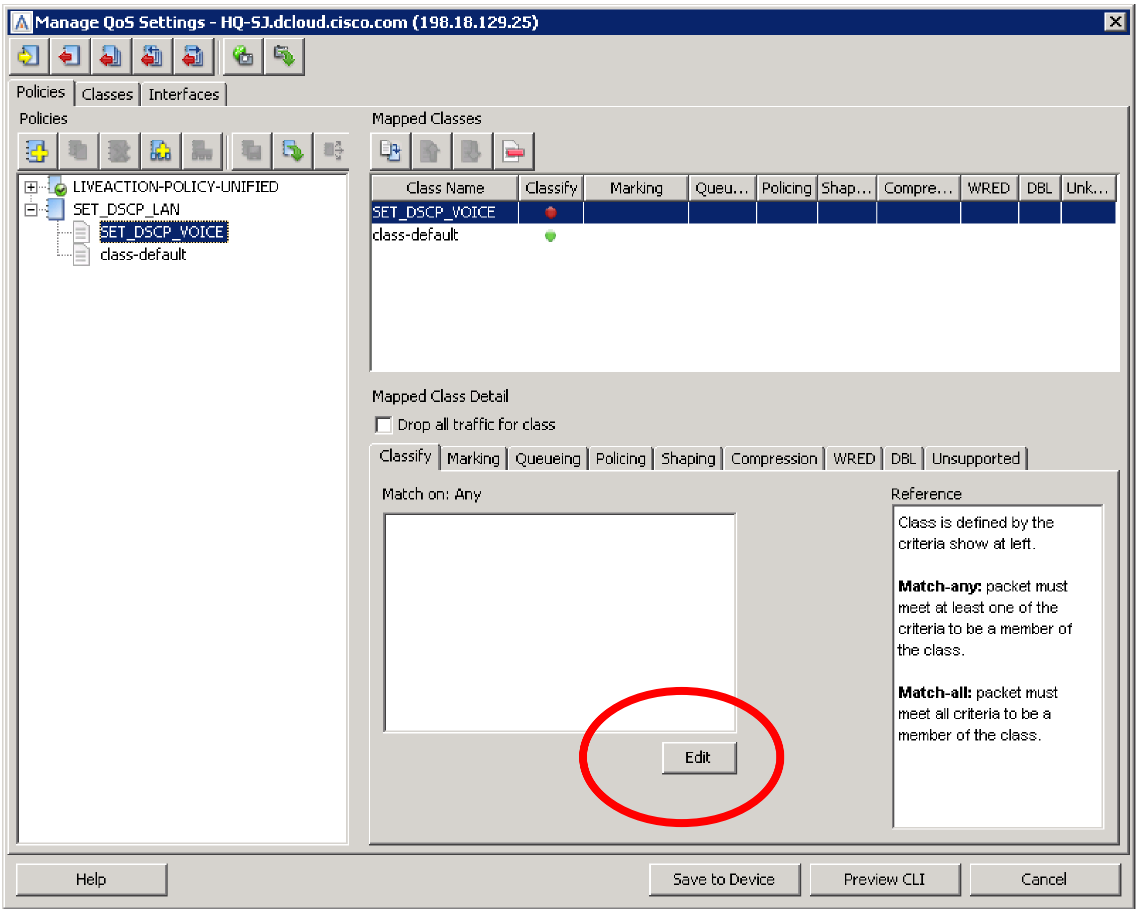
Select one of the following options:

○ Use existing class: LIVEACTION-CLASS-MEDIANET

● Create new class: SET_DSCP_VOICE

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

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



| Class Name | Classify | Marking | Queu... | Policing | Shap... | Compre... | WRED | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | | | | | | | | |
| class-default | ● | | | | | | | | |

Match on: Any

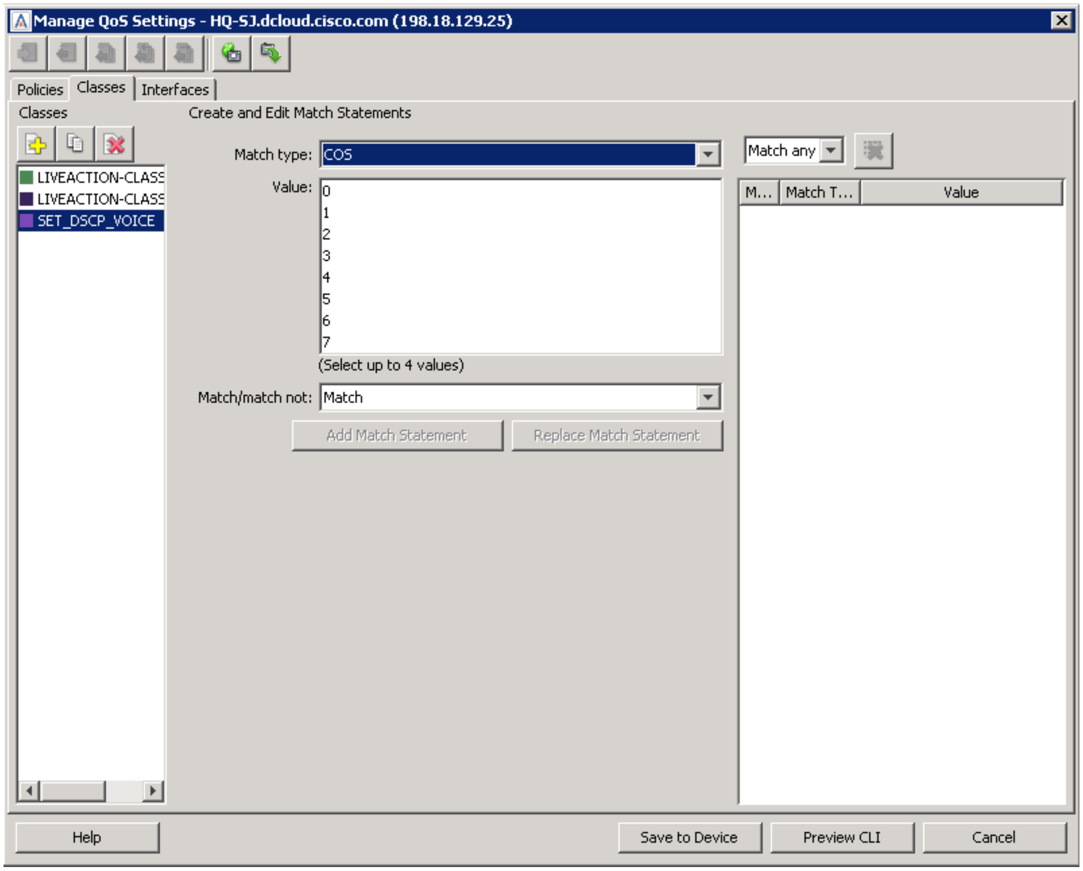
Reference

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

7. On the Classify Tab, select the Edit button



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Classes: LIVEACTION-CLASS, LIVEACTION-CLASS, SET_DSCP_VOICE

Create and Edit Match Statements

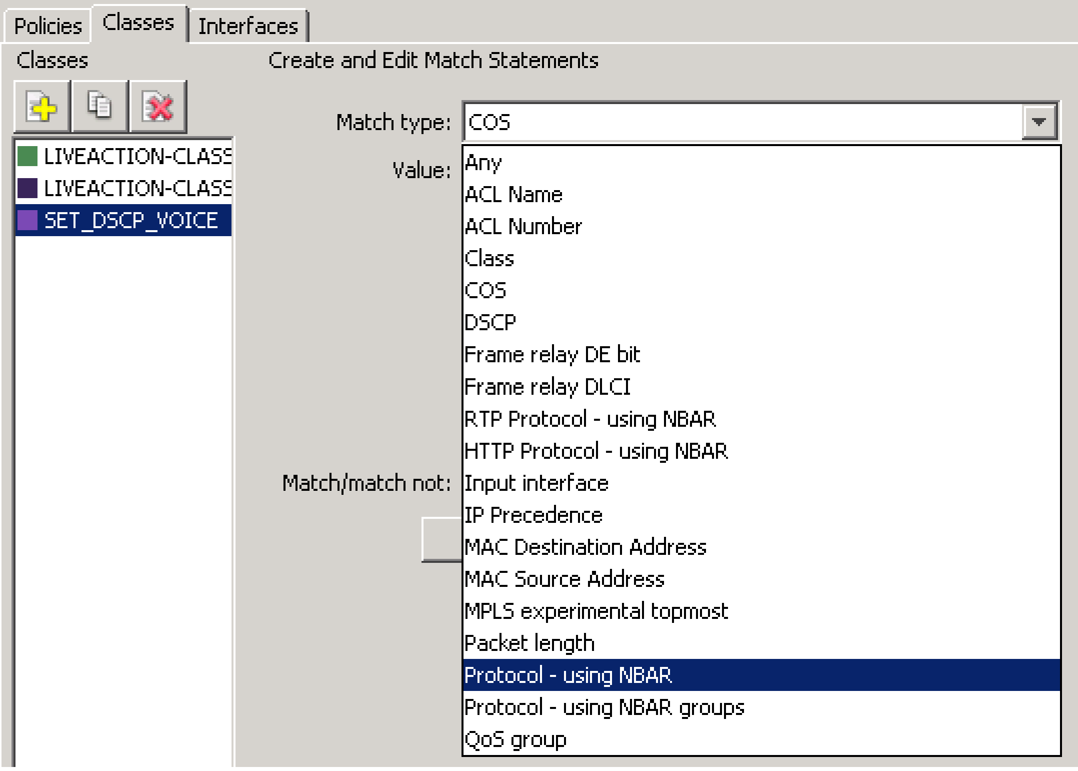
Match type: COS

Value: 0 1 2 3 4 5 6 7

(Select up to 4 values)

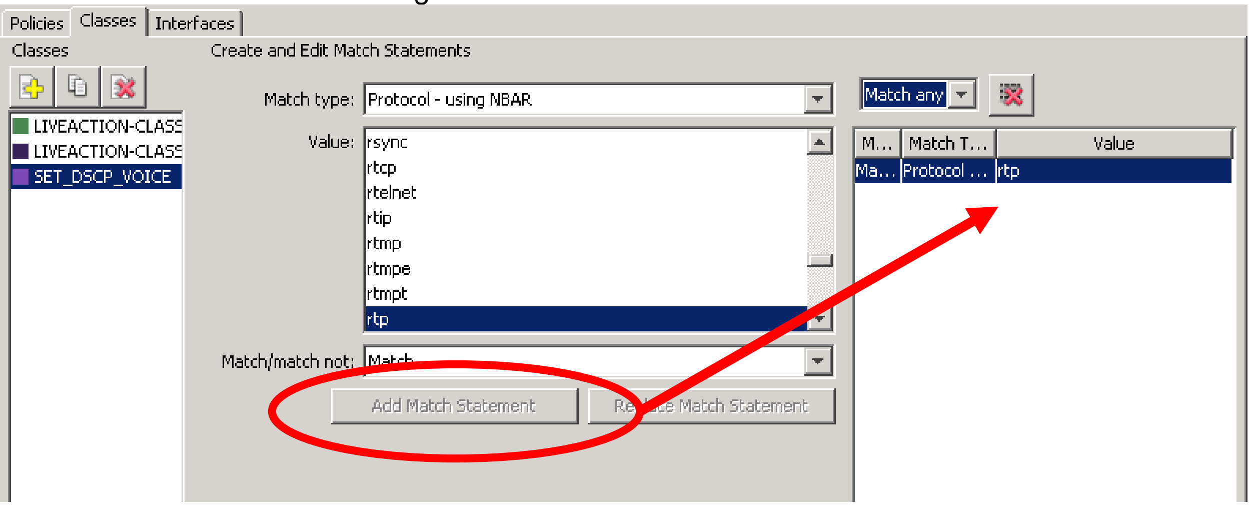
Match/match not: Match

8. Select the match type dropdown and select Protocol – using NBAR



Match type: COS

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



Classes

- LIVEACTION-CLASS
- LIVEACTION-CLASS
- SET_DSCP_VOICE

Create and Edit Match Statements

Match type: Protocol - using NBAR

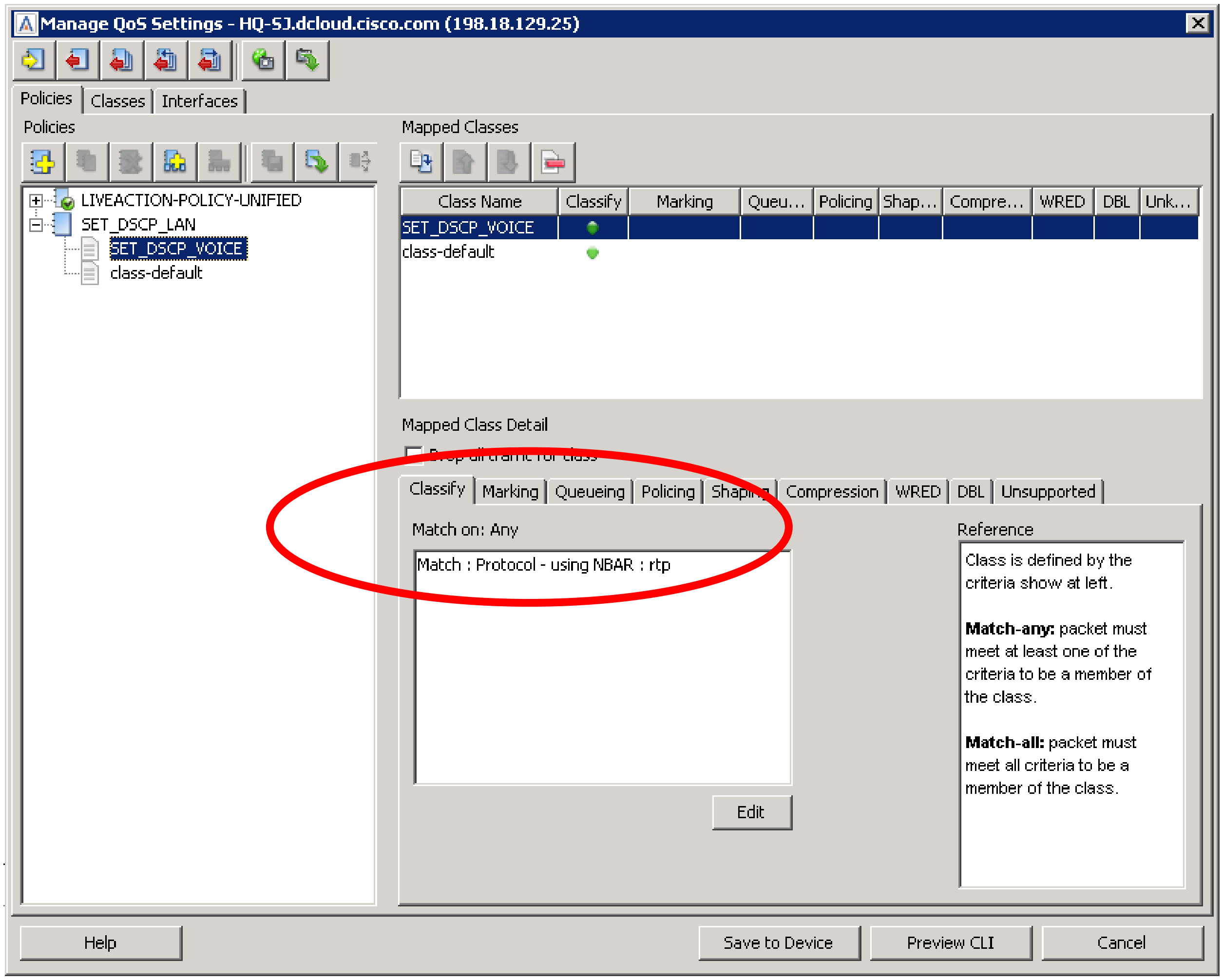
Value: rsync, rtcp, rtelnet, rtip, rtmp, rtmpe, rtmpt, rtp

Match/match not: Match

Match any

| M... | Match T... | Value |
|---|---|---|
| Ma... | Protocol ... | rtp |

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



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Policies

- LIVEACTION-POLICY-UNIFIED
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - class-default

Mapped Classes

| Class Name | Classify | Marking | Queu... | Policing | Shap... | Compre... | WRED | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | | | | | | | | |
| class-default | ● | | | | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Match on: Any

Match : Protocol - using NBAR : rtp

Reference

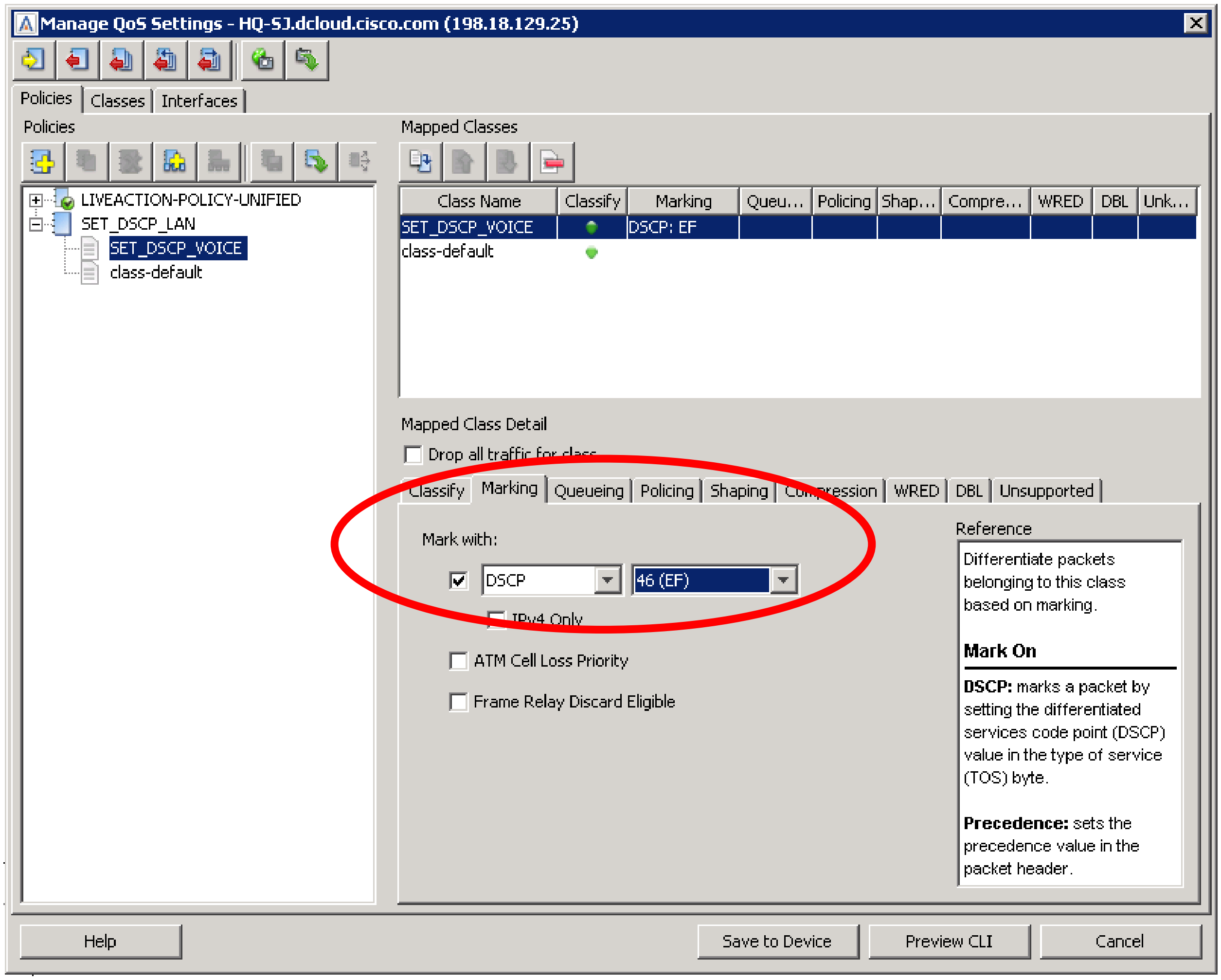
Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

11. Select the Marking tab.

12. Select the mark tick button and select the DSCP value of 46 (EF)



| Class Name | Classify | Marking | Queu... | Policing | Shap... | Compre... | WRED | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | DSCP: EF | | | | | | | |
| class-default | ● | | | | | | | | |

☐ Drop all traffic for class

Mark with:

☑ DSCP 46 (EF)

☐ IPv4 Only

☐ ATM Cell Loss Priority

☐ Frame Relay Discard Eligible

Differentiate packets belonging to this class based on marking.

**Mark On**

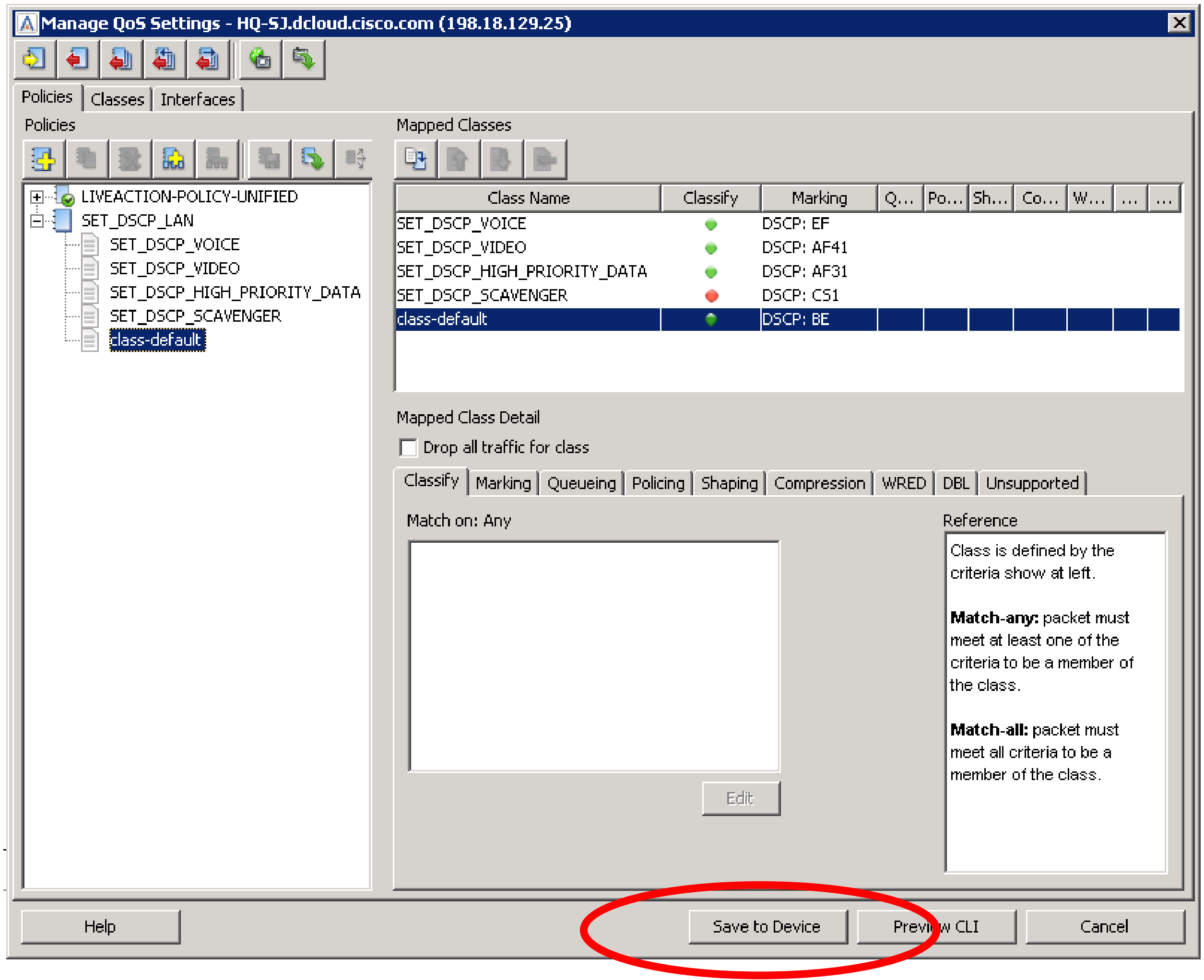
**DSCP:** marks a packet by setting the differentiated services code point (DSCP) value in the type of service (TOS) byte.

**Precedence:** sets the precedence value in the packet header.

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

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

When finished, the SET_DSCP_LAN policy should look like this:



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DATA
  - SET_DSCP_SCAVENGER
  - class-default

Mapped Classes

| Class Name | Classify | Marking | Q... | Po... | Sh... | Co... | W... | ... | ... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | 🟢 | DSCP: EF | | | | | | | |
| SET_DSCP_VIDEO | 🟢 | DSCP: AF41 | | | | | | | |
| SET_DSCP_HIGH_PRIORITY_DATA | 🟢 | DSCP: AF31 | | | | | | | |
| SET_DSCP_SCAVENGER | 🔴 | DSCP: CS1 | | | | | | | |
| class-default | 🟢 | DSCP: BE | | | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Match on: Any

Reference

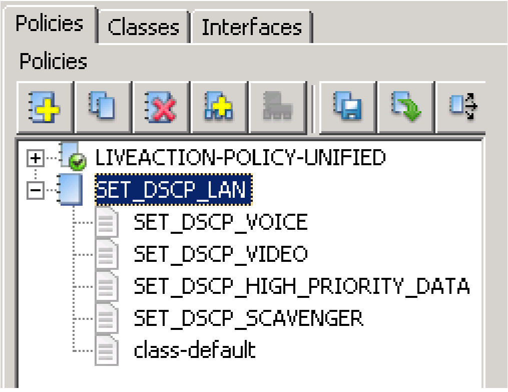
Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

14. Select Save to Device.

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



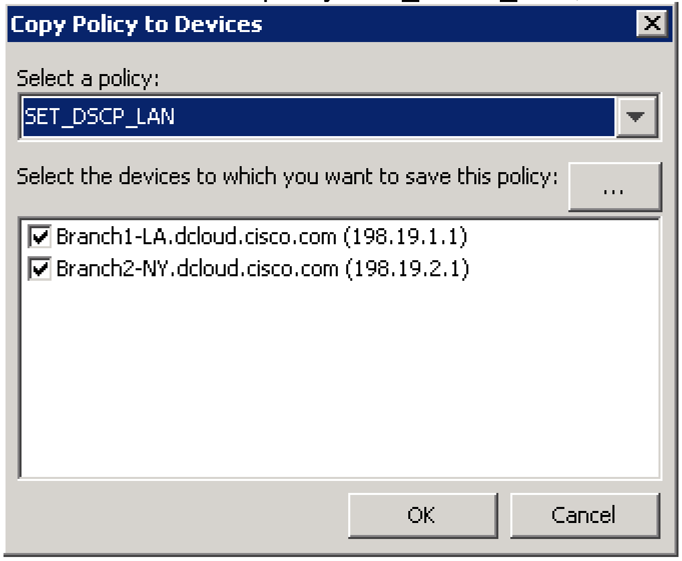
Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DATA
  - SET_DSCP_SCAVENGER
  - class-default

The Copy Policy to Devices dialog window appears.

16. Select the policy SET_DSCP_LAN, tick the two branch routers, and select OK.



Copy Policy to Devices

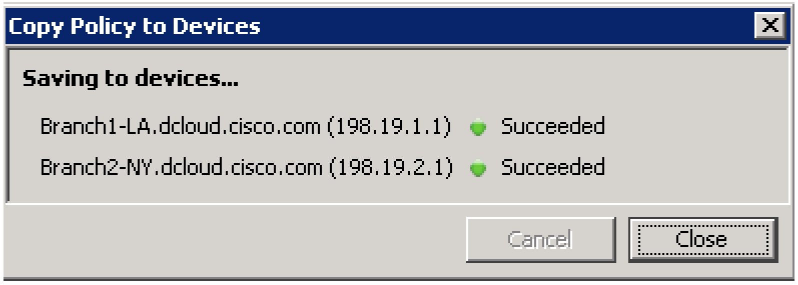
Select a policy: SET_DSCP_LAN

Select the devices to which you want to save this policy:

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)

The SET_DSCP_LAN policy will be copied to the other routers.

Validate the changes saved successfully.



Copy Policy to Devices

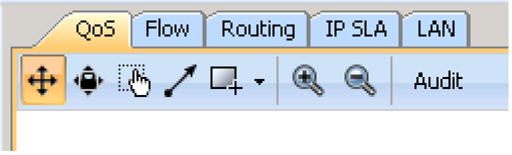
**Saving to devices...**

Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded
Branch2-NY.dcloud.cisco.com (198.19.2.1) ● Succeeded

17. Close the Manage QoS Dialog Window.

# Lab 2.5: Apply Marking Policies to Interface(s)

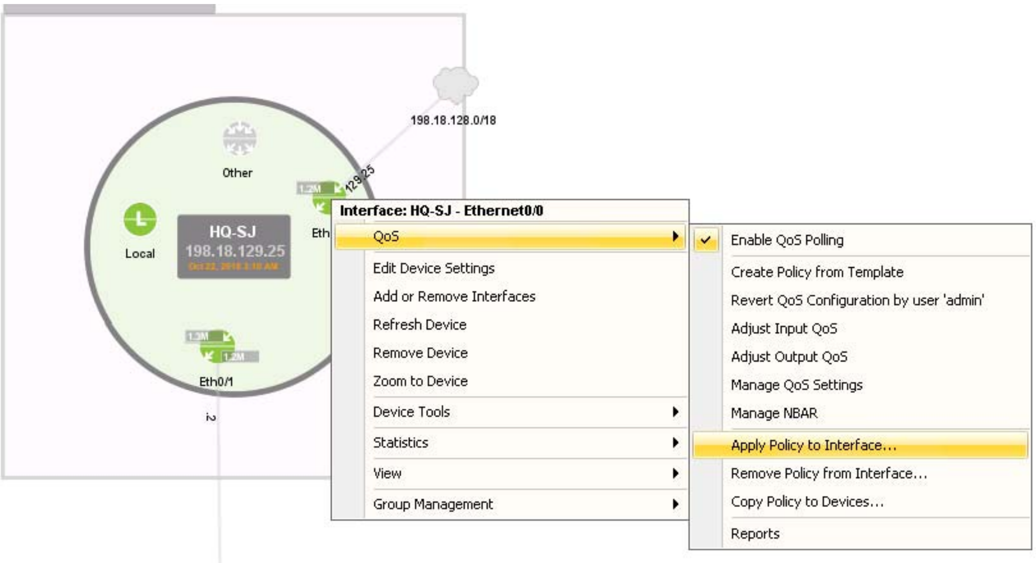
Lab Steps:



1. Select the **QoS** Tab

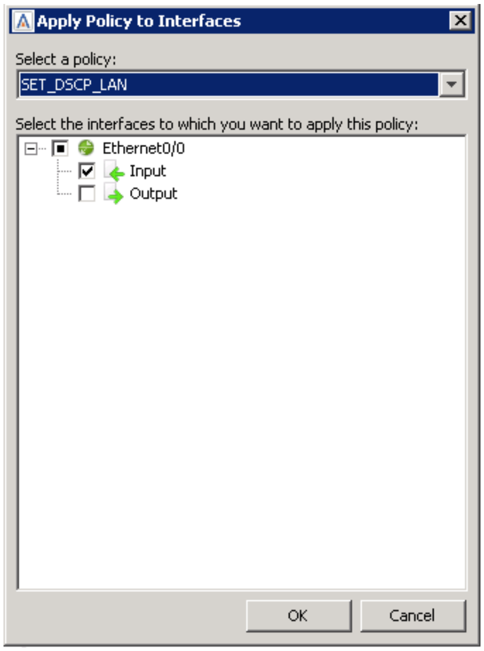
2. Right-click on the LAN interface on one of the routers and select QoS > Apply Policy to Interface.

**Note: The LAN interface will be GigabitEthernet1 on each of the routers in this lab.**



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

4. Click OK.



Apply Policy to Interfaces

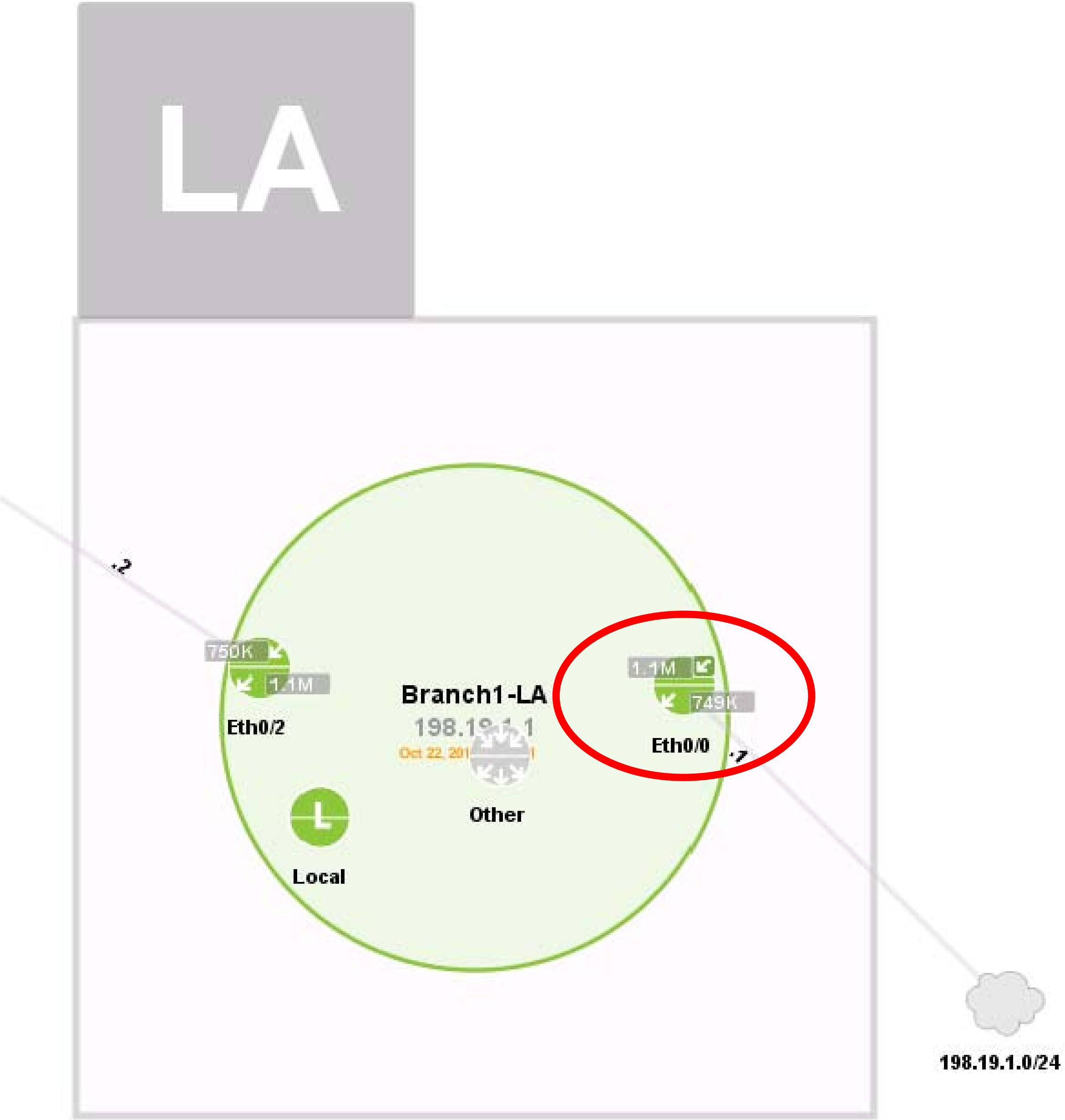
Select a policy: SET_DSCP_LAN

Select the interfaces to which you want to apply this policy:

- ■ Ethernet0/0
  - ☑ Input
  - □ Output

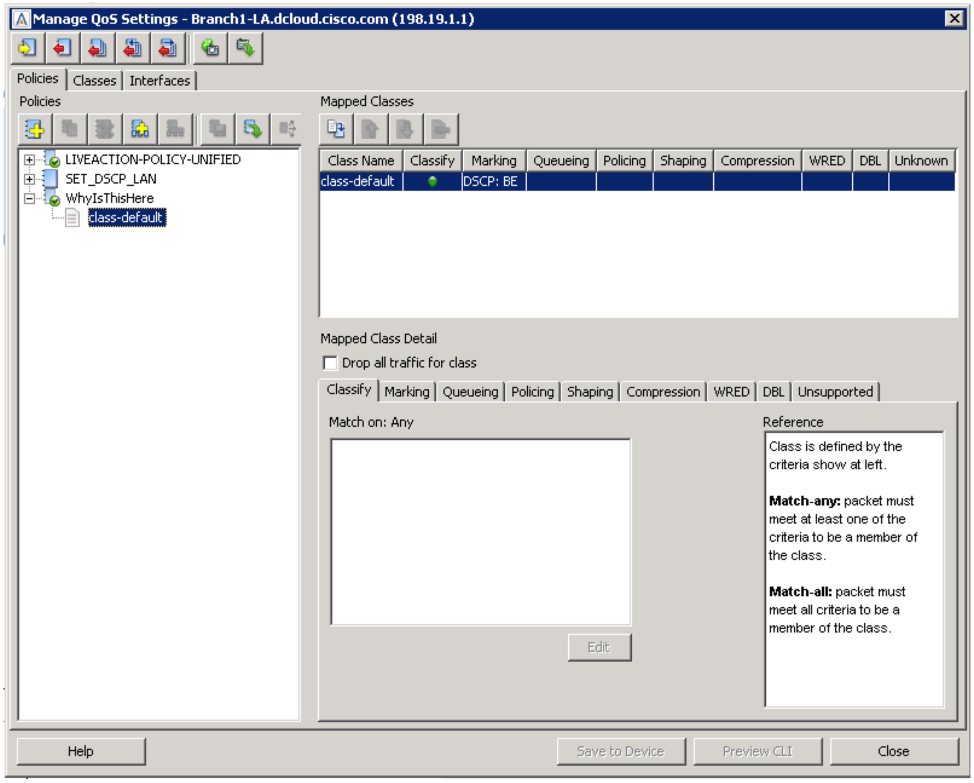
Follow these same steps to apply the SET_DSCP_LAN policy to **the other router's LAN interface.**

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



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

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



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Policies

- LIVEACTION-POLICY-UNIFIED
- SET_DSCP_LAN
- WhyIsThisHere
  - class-default

Mapped Classes

| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| class-default | ● | DSCP: BE | | | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Match on: Any

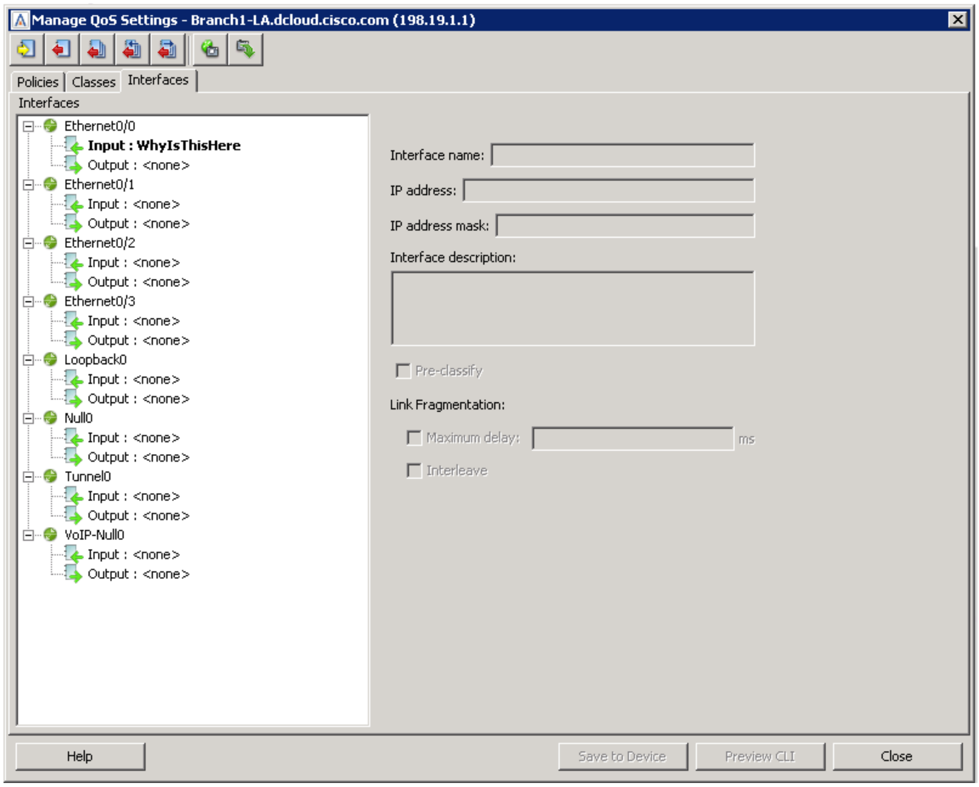
Reference

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

6. Select the Interface tab



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Interfaces

- Ethernet0/0
  - **Input : WhyIsThisHere**
  - Output : <none>
- Ethernet0/1
  - Input : <none>
  - Output : <none>
- Ethernet0/2
  - Input : <none>
  - Output : <none>
- Ethernet0/3
  - Input : <none>
  - Output : <none>
- Loopback0
  - Input : <none>
  - Output : <none>
- Null0
  - Input : <none>
  - Output : <none>
- Tunnel0
  - Input : <none>
  - Output : <none>
- VoIP-Null0
  - Input : <none>
  - Output : <none>

Interface name:

IP address:

IP address mask:

Interface description:

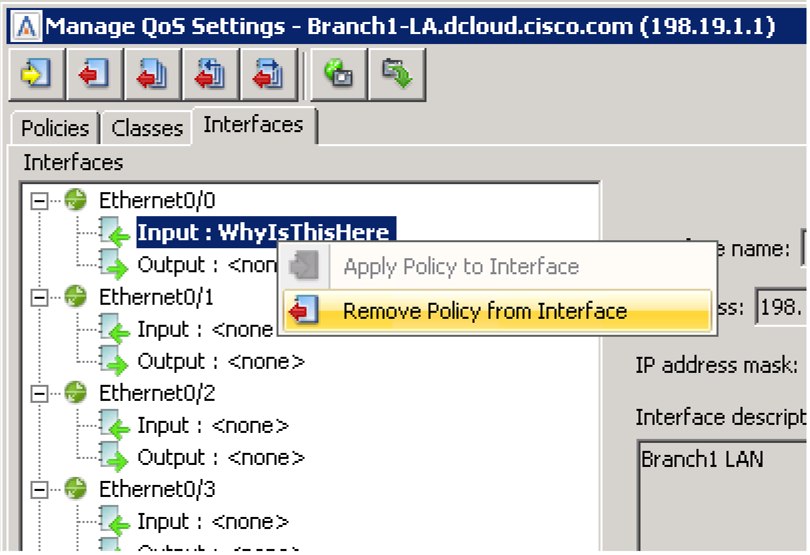
□ Pre-classify

Link Fragmentation:

□ Maximum delay: ms

□ Interleave

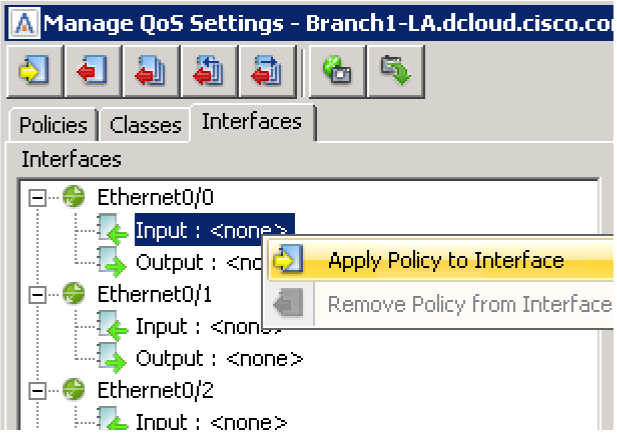
7. Right-click on the WhyIsThisHere policy that is highlighted on the input side of the GigabitEthernet1 interface.



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

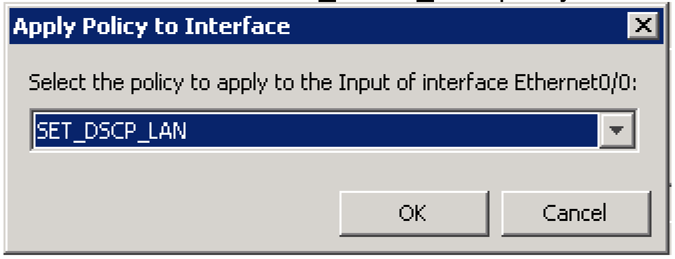
8. Select Remove Policy from Interface

9. Right-click on the input side of the GigabitEthernet1 interface and select Apply Policy to Interface.



Manage QoS Settings - Branch1-LA.dcloud.cisco.co

10. Select the SET_DSCP_LAN policy and select OK.

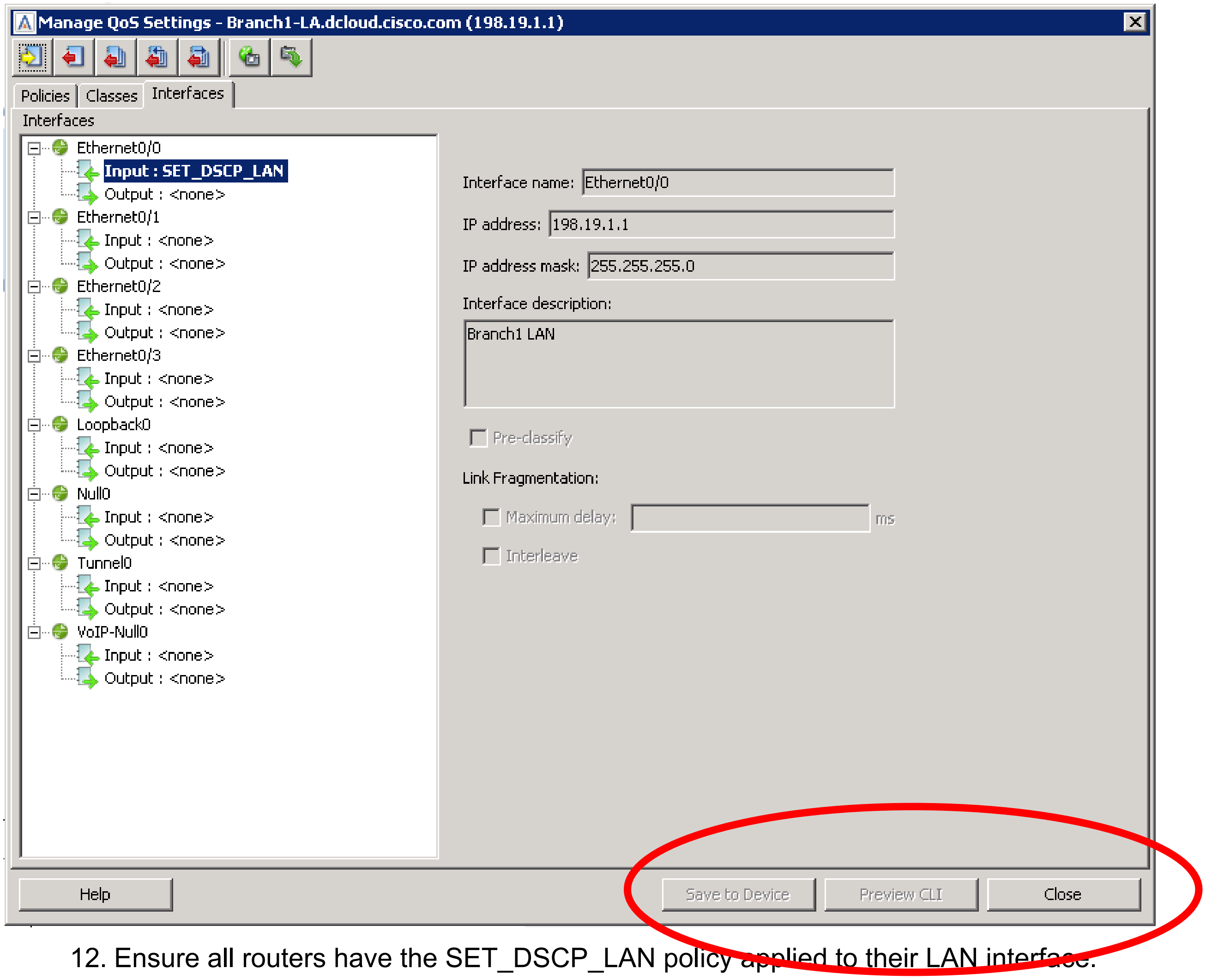


Apply Policy to Interface

Select the policy to apply to the Input of interface Ethernet0/0:

SET_DSCP_LAN

11. Select Save to Device and close the Manage QoS Settings dialog window.



Manage QoS Settings - Branch1-LA.dcloud.cisco.com (198.19.1.1)

Interface name: Ethernet0/0

IP address: 198.19.1.1

IP address mask: 255.255.255.0

Interface description: Branch1 LAN

□ Pre-classify

Link Fragmentation:

□ Maximum delay: ms

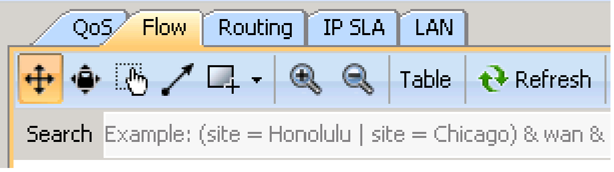
□ Interleave

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

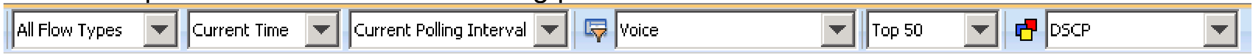
# Lab 2.6: Validate DSCP Settings

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

1. From the LiveAction map, select the Flow Tab

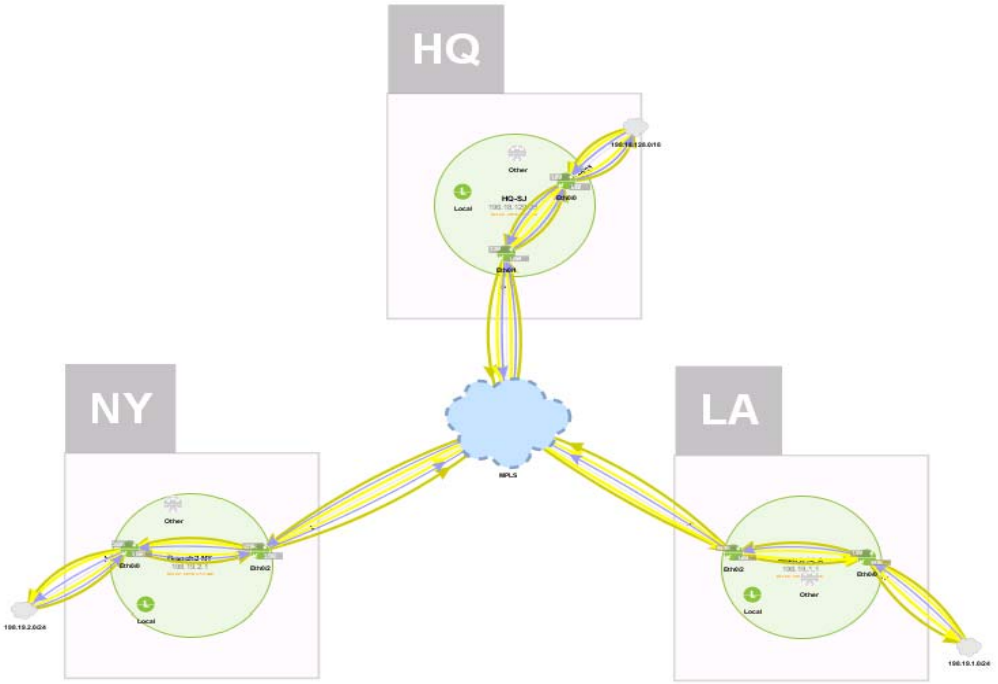


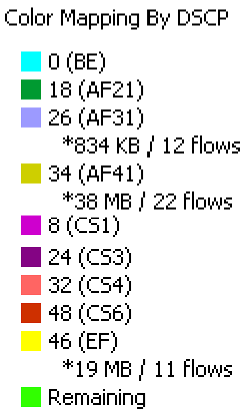
2. Update the filters to the following parameters



All Flow Types | Current Time | Current Polling Interval | Voice | Top 50 | DSCP

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





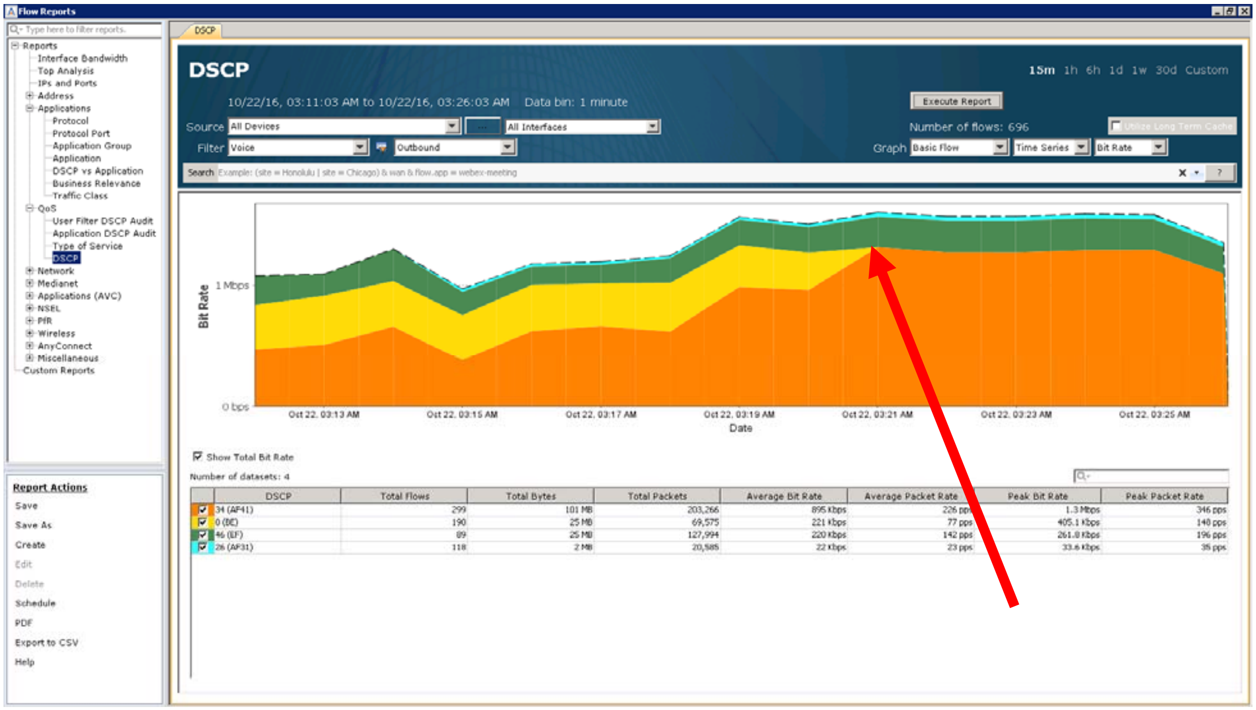
Color Mapping By DSCP

🟦 0 (BE)
🟩 18 (AF21)
🟪 26 (AF31)
*834 KB / 12 flows
🟨 34 (AF41)
*38 MB / 22 flows
🟪 8 (CS1)
🟪 24 (CS3)
🟥 32 (CS4)
🟥 48 (CS6)
🟨 46 (EF)
*19 MB / 11 flows
🟩 Remaining

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

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

3. Run the Reports > Flow > QOS > **DSCP** report
   a. Select the Voice filter, but leave all parameters at their default settings
   b. Implement a Search of “wan”
   c. **Execute Report**



DSCP

10/22/16, 03:11:03 AM to 10/22/16, 03:26:03 AM   Data bin: 1 minute

Source: All Devices, All Interfaces

Filter: Voice, Outbound

Number of flows: 696

Graph: Basic Flow, Time Series, Bit Rate

Search: Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

☑ Show Total Bit Rate

Number of datasets: 4

| | DSCP | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|
| ☑ | 34 (AF41) | 299 | 101 MB | 203,266 | 895 Kbps | 226 pps | 1.3 Mbps | 346 pps |
| ☑ | 0 (BE) | 190 | 25 MB | 69,575 | 221 Kbps | 77 pps | 405.1 Kbps | 140 pps |
| ☑ | 46 (EF) | 89 | 25 MB | 127,994 | 220 Kbps | 142 pps | 261.0 Kbps | 196 pps |
| ☑ | 26 (AF31) | 118 | 2 MB | 20,585 | 22 Kbps | 23 pps | 33.6 Kbps | 35 pps |

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

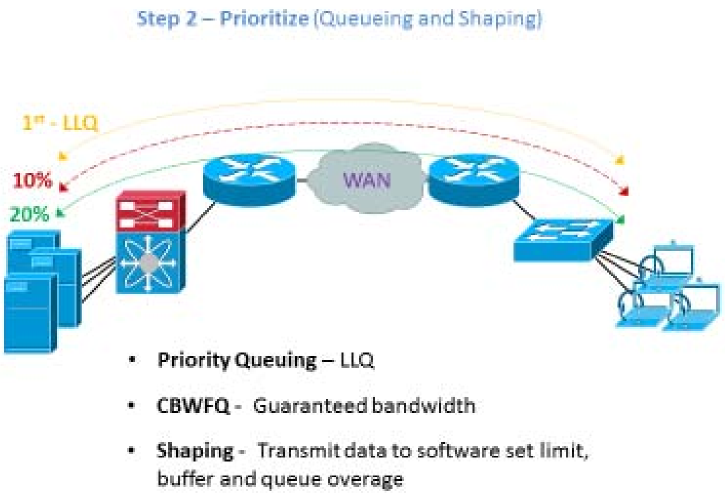
**Note:  For the sake of time in this lab, we are only going to focus on this one report. Remember that in a real network, you would repeat these steps for all important applications. We would use the same visualization and reports as we have used previously to validate QoS polices effectiveness for all priority traffic.**

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

# Lab 3

## Lab 3: QoS Prioritization & Queueing

# Lab 3.0: Intro to Prioritization



Step 2 – Prioritize (Queueing and Shaping)

- **Priority Queuing** – LLQ
- **CBWFQ** - Guaranteed bandwidth
- **Shaping** - Transmit data to software set limit, buffer and queue overage

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

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

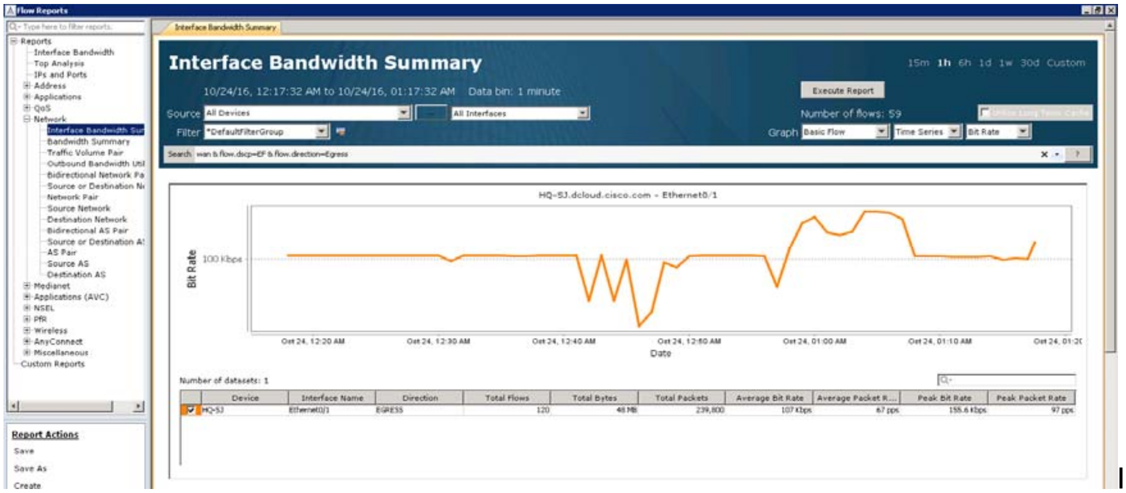
# Lab 3.1: Run the Reports!

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

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

Lab Steps:

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



Interface Bandwidth Summary

10/24/16, 12:17:32 AM to 10/24/16, 01:17:32 AM Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup

Number of flows: 59

Graph: Basic Flow | Time Series | Bit Rate

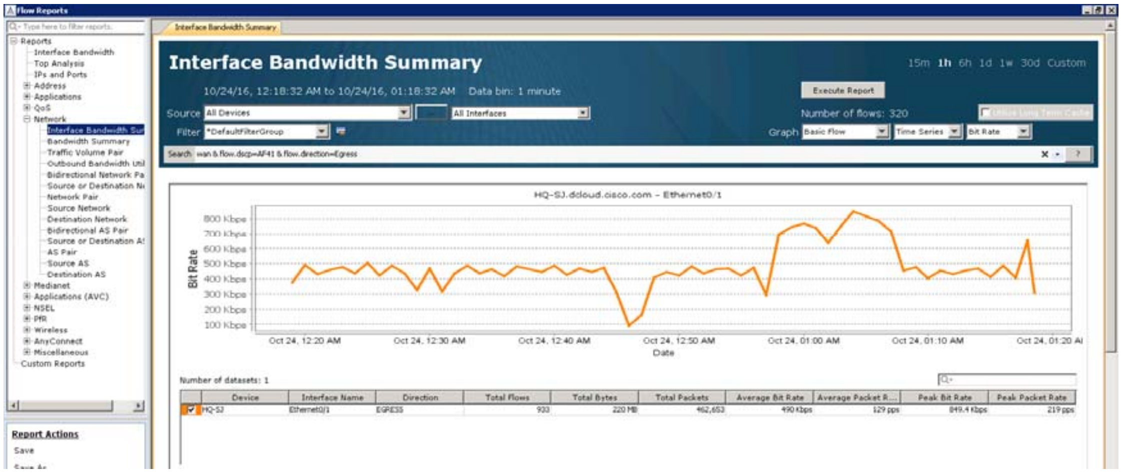
Search: wan & flow.dscp=EF & flow.direction=Egress

Number of datasets: 1

| | Device | Interface Name | Direction | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet R... | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | HQ-SJ | Ethernet0/1 | EGRESS | 120 | 48 MB | 239,800 | 107 Kbps | 67 pps | 155.6 Kbps | 97 pps |

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

2. Run the Flow > Network > **Interface Bandwidth Summary** report
   a. Leave all Filter parameters at their default settings
   b. Implement a Search of "wan & flow.dscp=AF41 & flow.direction=Egress"



Interface Bandwidth Summary

10/24/16, 12:18:32 AM to 10/24/16, 01:18:32 AM Data bin: 1 minute

Source: All Devices | All Interfaces

Filter: *DefaultFilterGroup

Number of flows: 320

Graph: Basic Flow | Time Series | Bit Rate

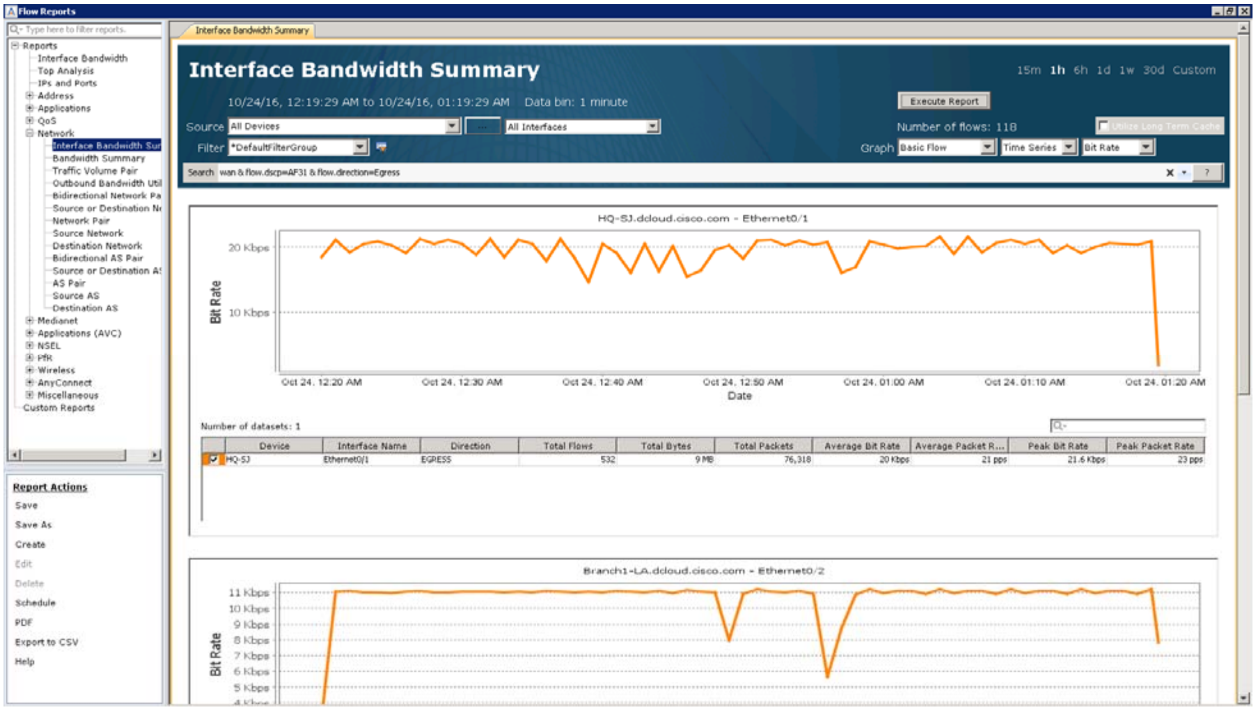
Search: wan & flow.dscp=AF41 & flow.direction=Egress

Number of datasets: 1

| | Device | Interface Name | Direction | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet R... | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | HQ-SJ | Ethernet0/1 | EGRESS | 933 | 220 MB | 462,653 | 490 Kbps | 129 pps | 849.4 Kbps | 219 pps |

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

3. Run the Flow > Network > **Interface Bandwidth Summary** Report
    a. Leave all Filter parameters at their default settings
    b. Implement a Search of “wan & flow.dscp=AF31 & flow.direction=Egress”



Interface Bandwidth Summary

10/24/16, 12:19:29 AM to 10/24/16, 01:19:29 AM Data bin: 1 minute

Source: All Devices, All Interfaces

Filter: *DefaultFilterGroup

Number of flows: 118

Graph: Basic Flow, Time Series, Bit Rate

Search: wan & flow.dscp=AF31 & flow.direction=Egress

Number of datasets: 1

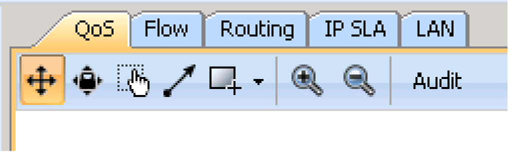
| | Device | Interface Name | Direction | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet R... | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | HQ-SJ | Ethernet0/1 | EGRESS | 532 | 9 MB | 76,318 | 20 Kbps | 21 pps | 21.6 Kbps | 23 pps |

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

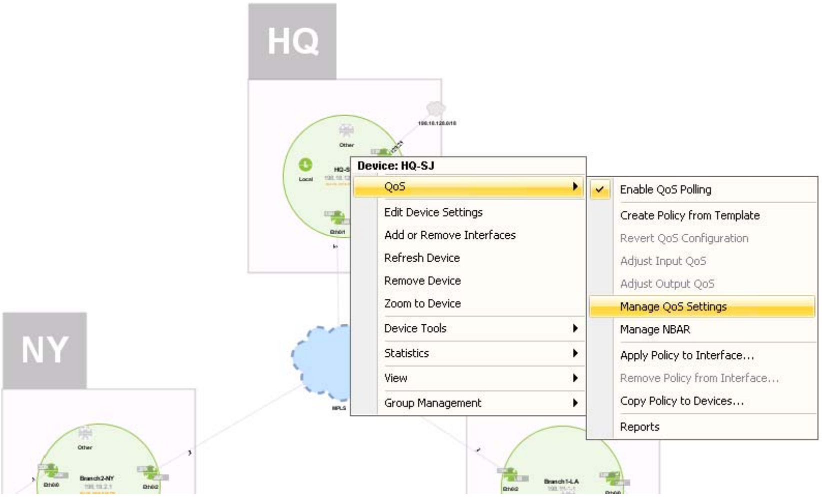
**Note: In a real network, it would be best to have at least two weeks of data to formulate the appropriate bandwidth allocations for the priority applications. Also remember that since Priority/LLQ queues have a built-in policer, one would want to over provision the settings based on these queues.**

# Lab 3.2: Building Queueing Policies

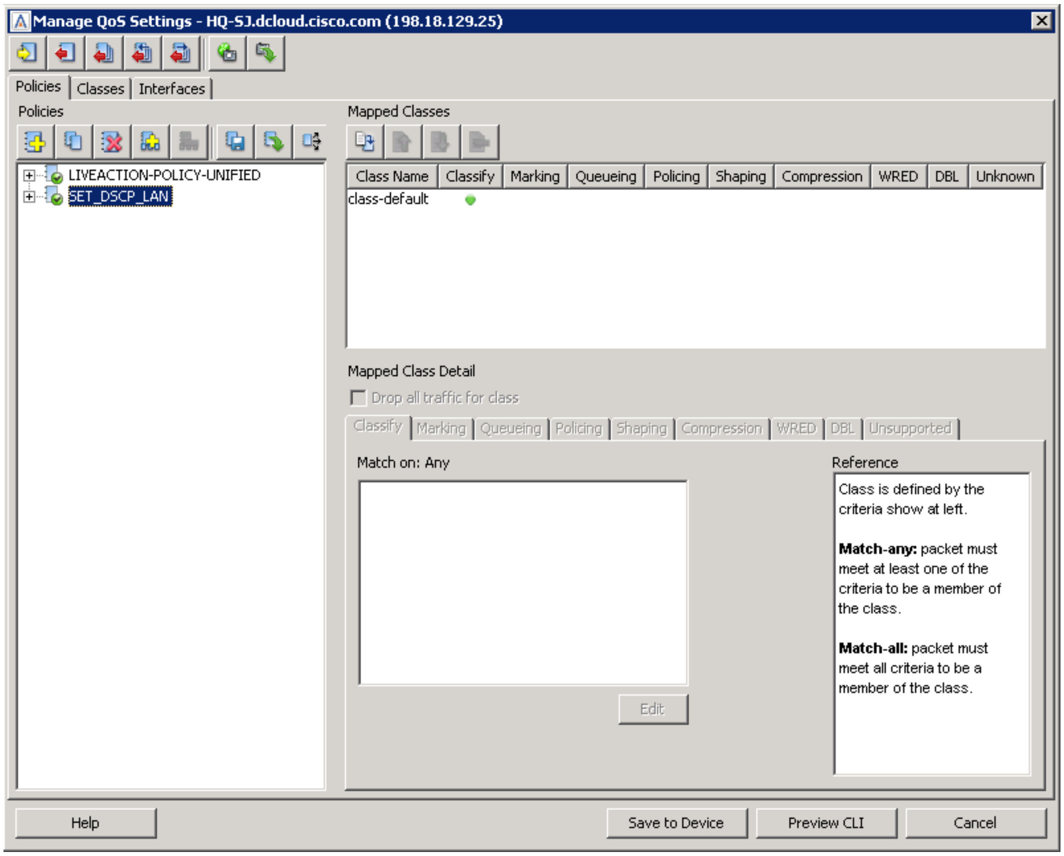
1. From the LiveAction map, select the QoS Tab



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



The Manage QoS Dialog Window will open

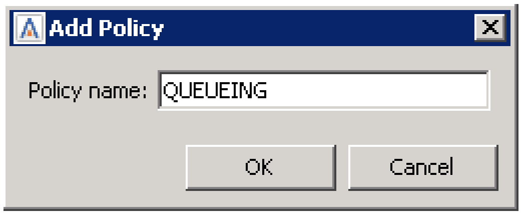


Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

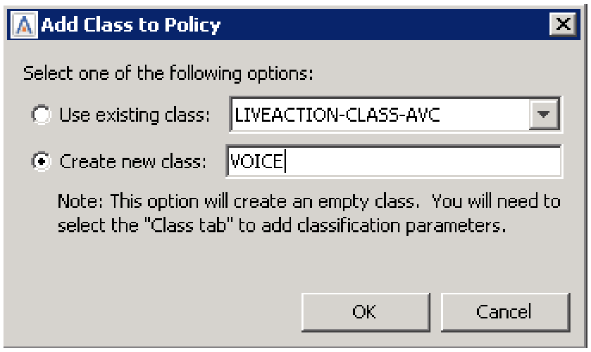
**Match-all:** packet must meet all criteria to be a member of the class.

3. Add a new Policy and name it QUEUEING.



Policy name: QUEUEING

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



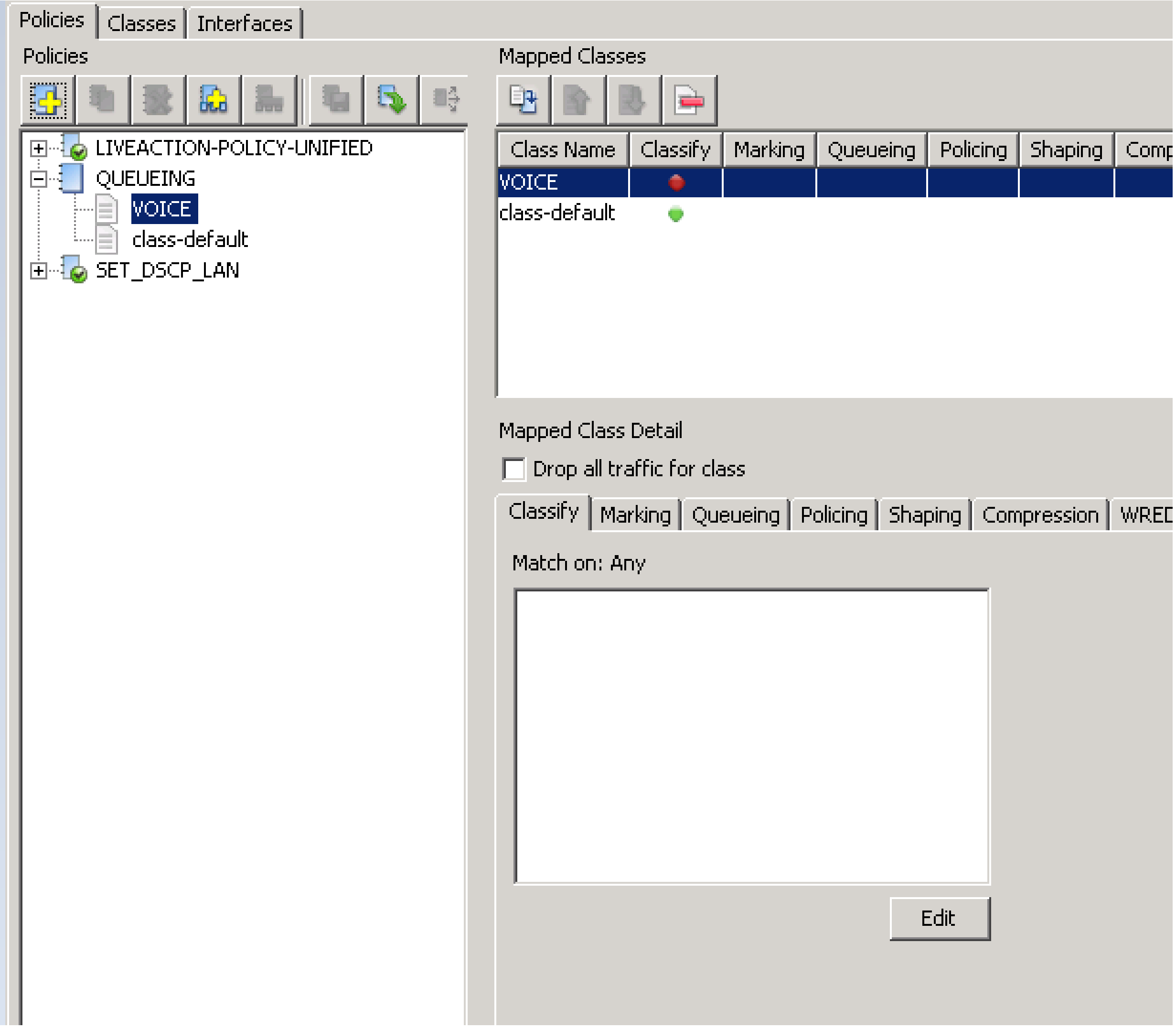
Select one of the following options:

○ Use existing class: LIVEACTION-CLASS-AVC

● Create new class: VOICE

Note: This option will create an empty class. You will need to select the "Class tab" to add classification parameters.

You should see the VOICE class inside the policy named QUEUEING



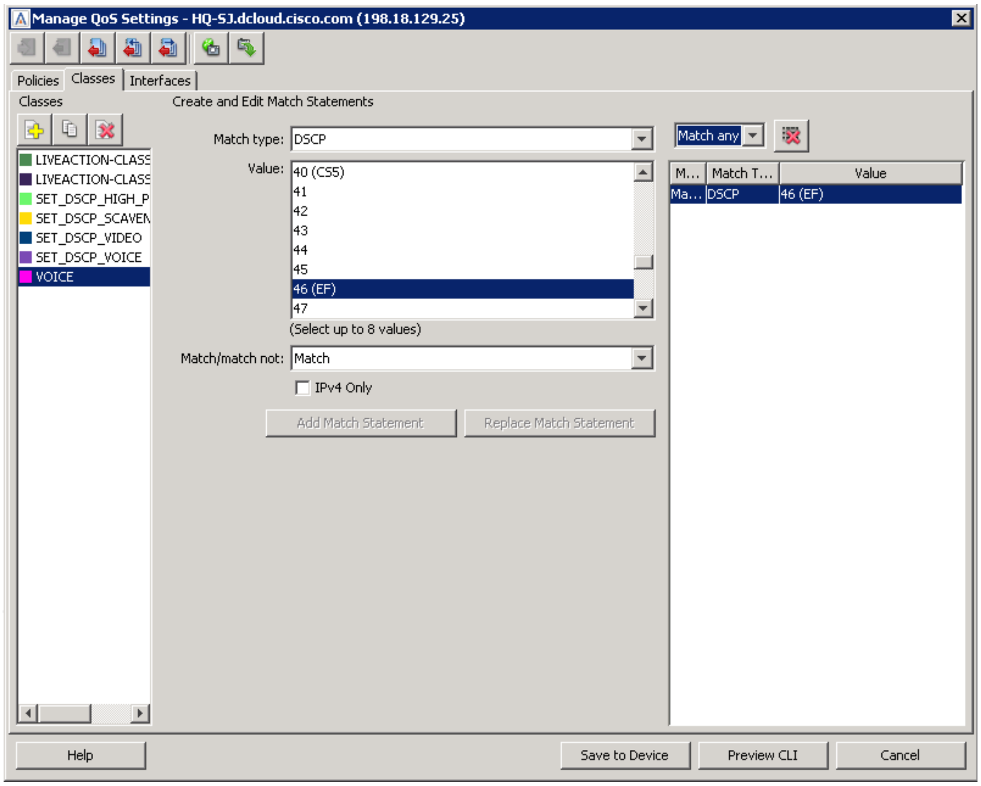
| Class Name | Classify | Marking | Queueing | Policing | Shaping | Comp |
|---|---|---|---|---|---|---|
| VOICE | ● | | | | | |
| class-default | ● | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Match on: Any

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



Classes:
- LIVEACTION-CLASS
- LIVEACTION-CLASS
- SET_DSCP_HIGH_P
- SET_DSCP_SCAVEN
- SET_DSCP_VIDEO
- SET_DSCP_VOICE
- VOICE

Match type: DSCP

Value: 40 (CS5), 41, 42, 43, 44, 45, 46 (EF), 47

(Select up to 8 values)

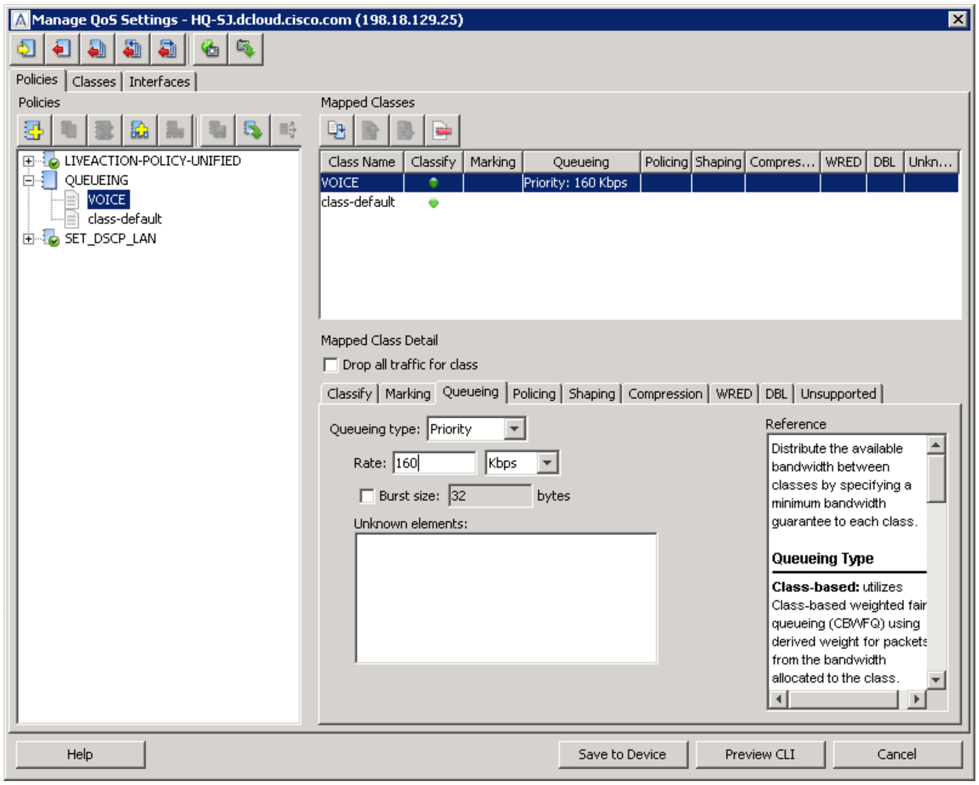
Match/match not: Match

☐ IPv4 Only

Match any

| M... | Match T... | Value |
|---|---|---|
| Ma... | DSCP | 46 (EF) |

6. Return to the Policies tab
7. Ensure the VOICE class of QUEUEING policy is highlighted and Select the Queueing tab.
8. Set the Queueing type to Priority and the bandwidth to 160 Kbps.



Policies:
- LIVEACTION-POLICY-UNIFIED
- QUEUEING
  - VOICE
  - class-default
- SET_DSCP_LAN

| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compres... | WRED | DBL | Unkn... |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority: 160 Kbps | | | | | | |
| class-default | ● | | | | | | | | |

☐ Drop all traffic for class

Queueing type: Priority

Rate: 160 Kbps

☐ Burst size: 32 bytes

Unknown elements:

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

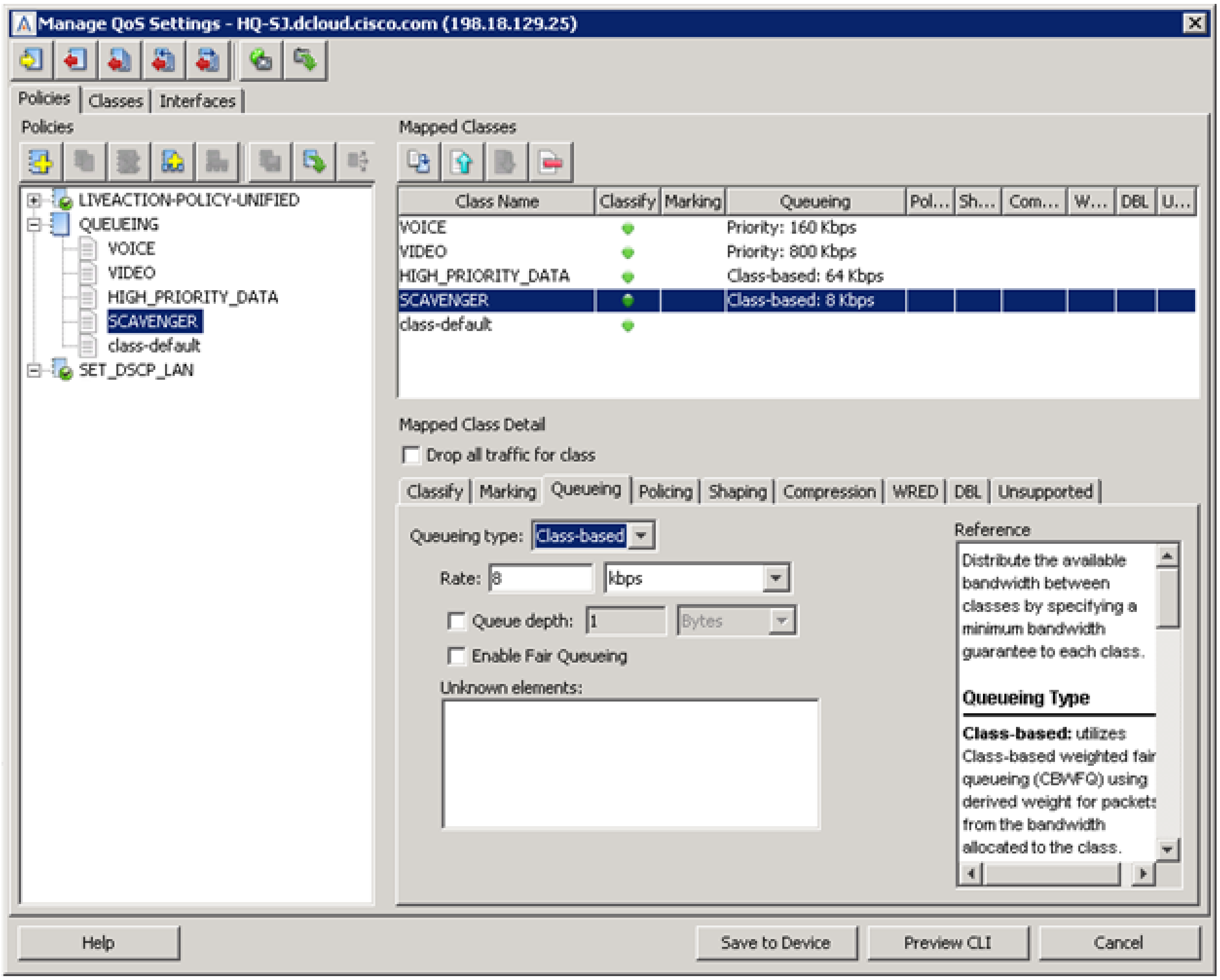
**Queueing Type**

**Class-based:** utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class.

9. K. Create the following classes in the QUEUEING policy based on the following table:

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

When finished, the QUEUEING policy should look similar to this:



Policies:

- LIVEACTION-POLICY-UNIFIED
- QUEUEING
  - VOICE
  - VIDEO
  - HIGH_PRIORITY_DATA
  - SCAVENGER
  - class-default
- SET_DSCP_LAN

Mapped Classes:

| Class Name | Classify | Marking | Queueing | Pol... | Sh... | Com... | W... | DBL | U... |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority: 160 Kbps | | | | | | |
| VIDEO | ● | | Priority: 800 Kbps | | | | | | |
| HIGH_PRIORITY_DATA | ● | | Class-based: 64 Kbps | | | | | | |
| SCAVENGER | ● | | Class-based: 8 Kbps | | | | | | |
| class-default | ● | | | | | | | | |

☐ Drop all traffic for class

Queueing type: Class-based

Rate: 8 kbps

☐ Queue depth: 1 Bytes

☐ Enable Fair Queueing

Unknown elements:

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

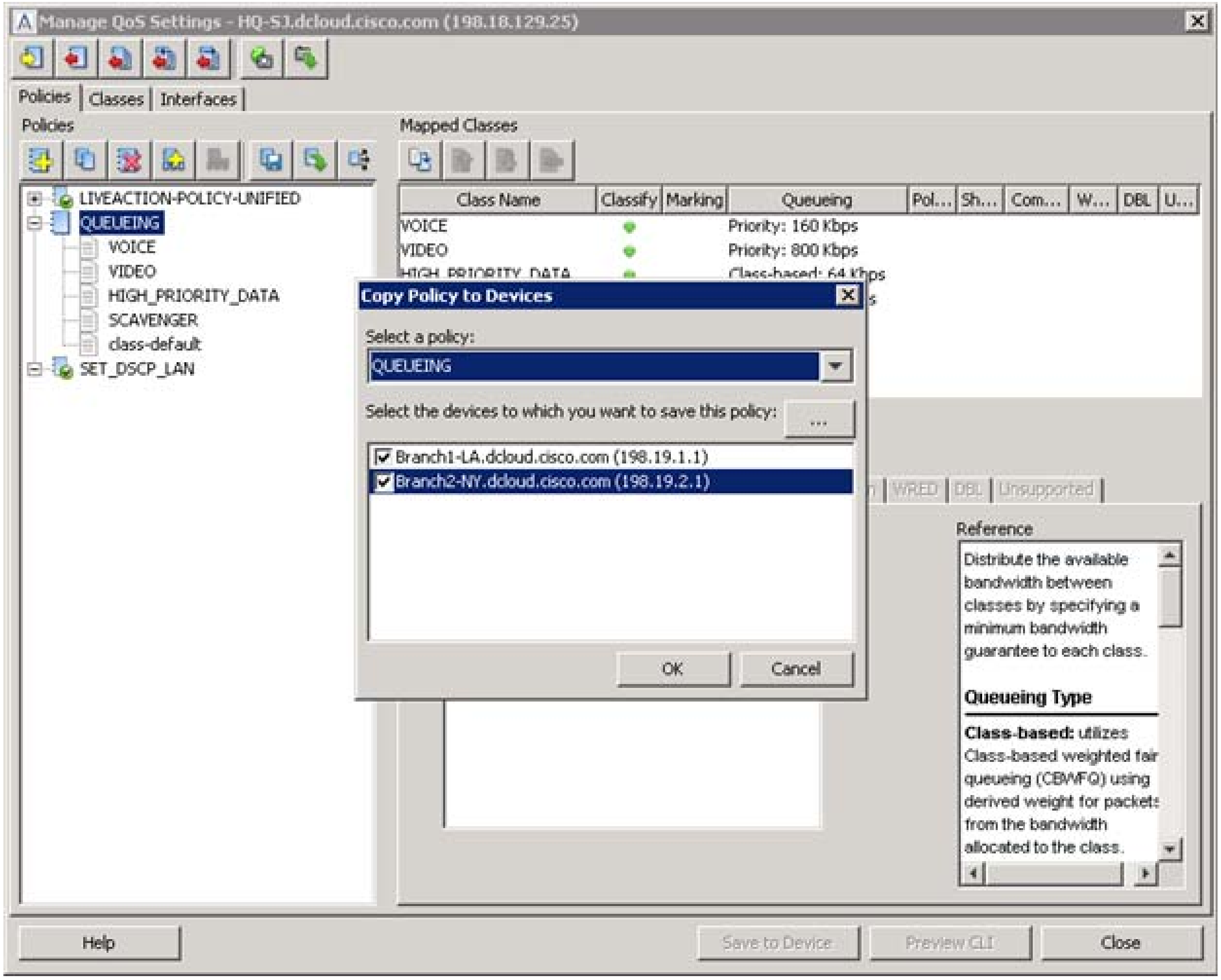
**Queueing Type**

**Class-based:** utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class.

10. Click **Save to Device.**

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

This will allow you to push the policy you just created to the other routers in the network.



| Class Name | Classify | Marking | Queueing | Pol... | Sh... | Com... | W... | DBL | U... |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority: 160 Kbps | | | | | | |
| VIDEO | ● | | Priority: 800 Kbps | | | | | | |
| HIGH_PRIORITY_DATA | ● | | Class-based: 64 Kbps | | | | | | |

Reference

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

**Queueing Type**

**Class-based:** utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class.

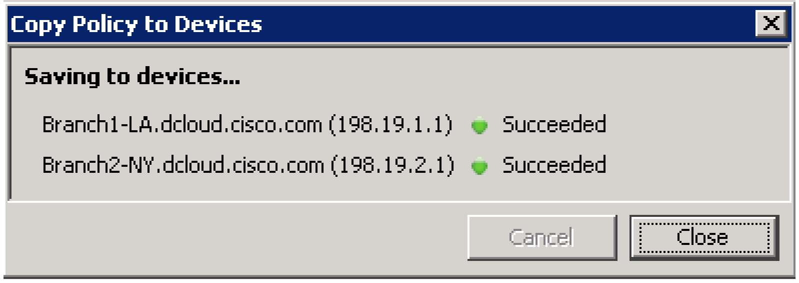
Copy Policy to Devices

Select a policy: QUEUEING

Select the devices to which you want to save this policy:

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)

12. Push the QUEUEING policy to the other routers



**Saving to devices...**

Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded
Branch2-NY.dcloud.cisco.com (198.19.2.1) ● Succeeded

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

# Lab 4

## Lab 4:  Shaping / Scaling

# Lab 4.0: Intro - Shaping (Scaling)

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

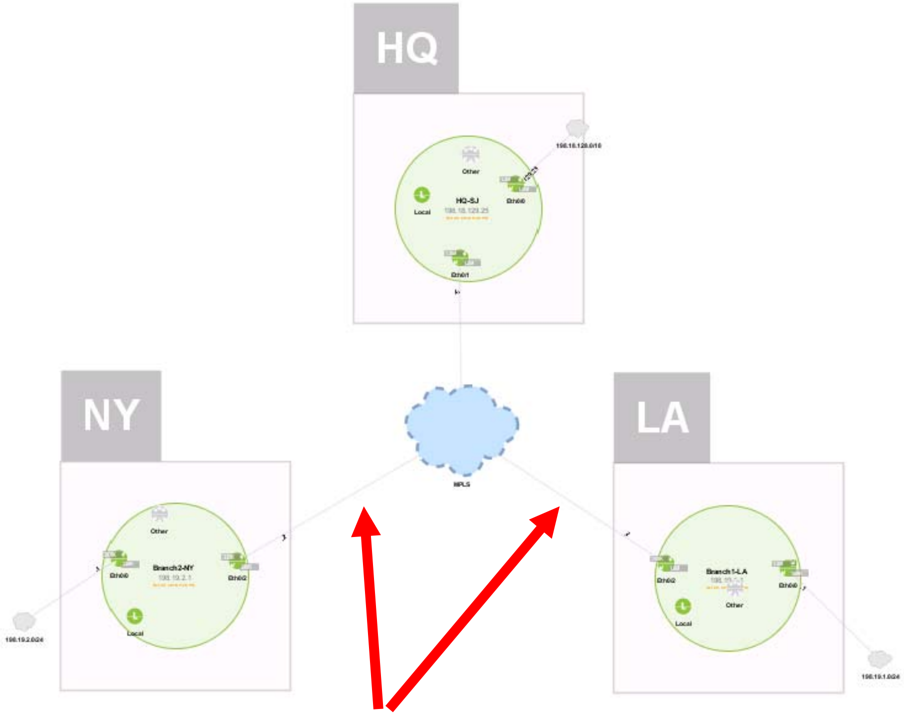
Below is a diagram of the lab network. The MPLS network in our lab does have CIRs in place with the following deign:

HQ - no provider CIR

NY - 1.5Mb provider CIR

LA - 1.5MB provider CIR

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



1.544Mb CIR

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

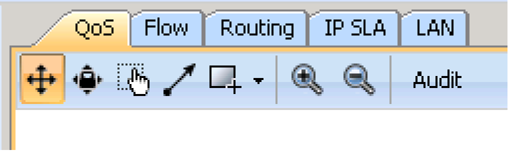
- HQ - Multi-class hierarchical shaping policy*
- NY - basic hierarchical shaping policy
- LA - basic hierarchical shaping policy

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

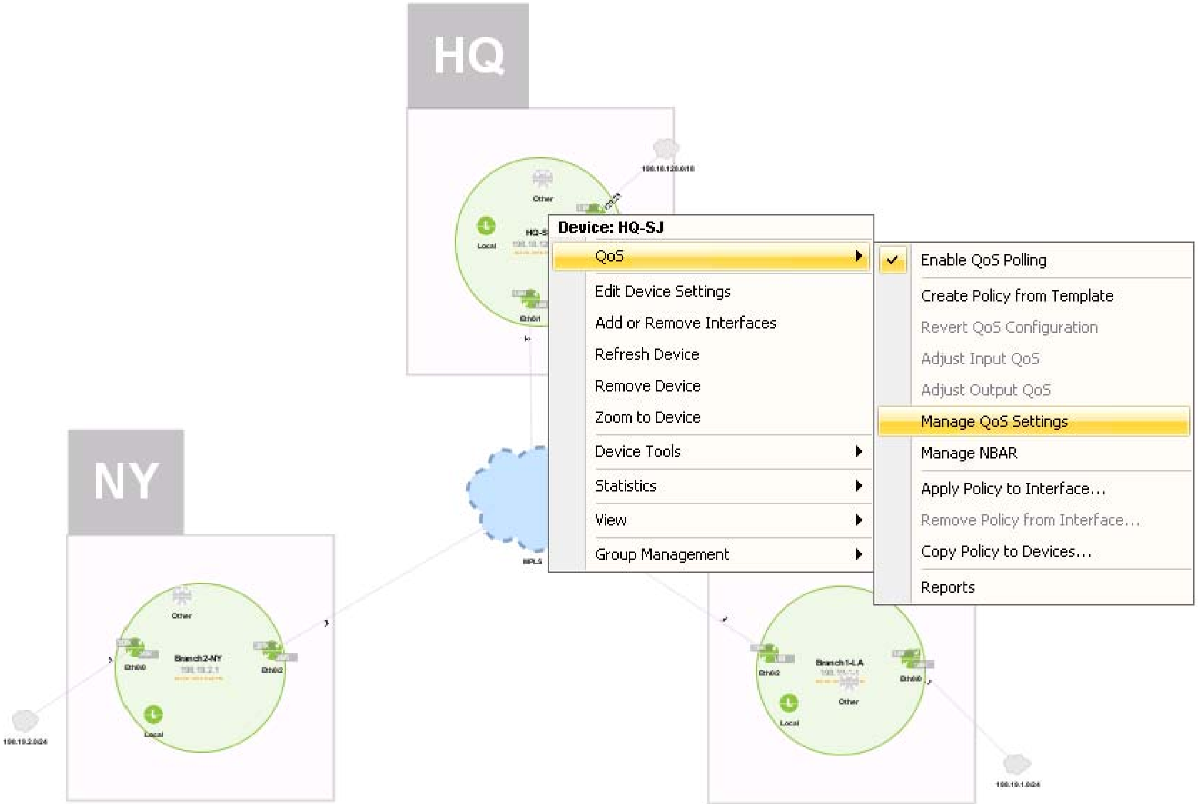
# Lab 4.1: Shaping (Scaling)

Lab Steps:

1. From the LiveAction map, select the QoS Tab

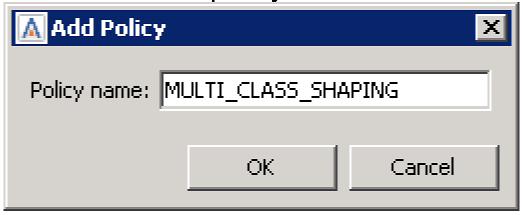


2. Right-click on the HQ router, select QoS > Manage QoS Settings



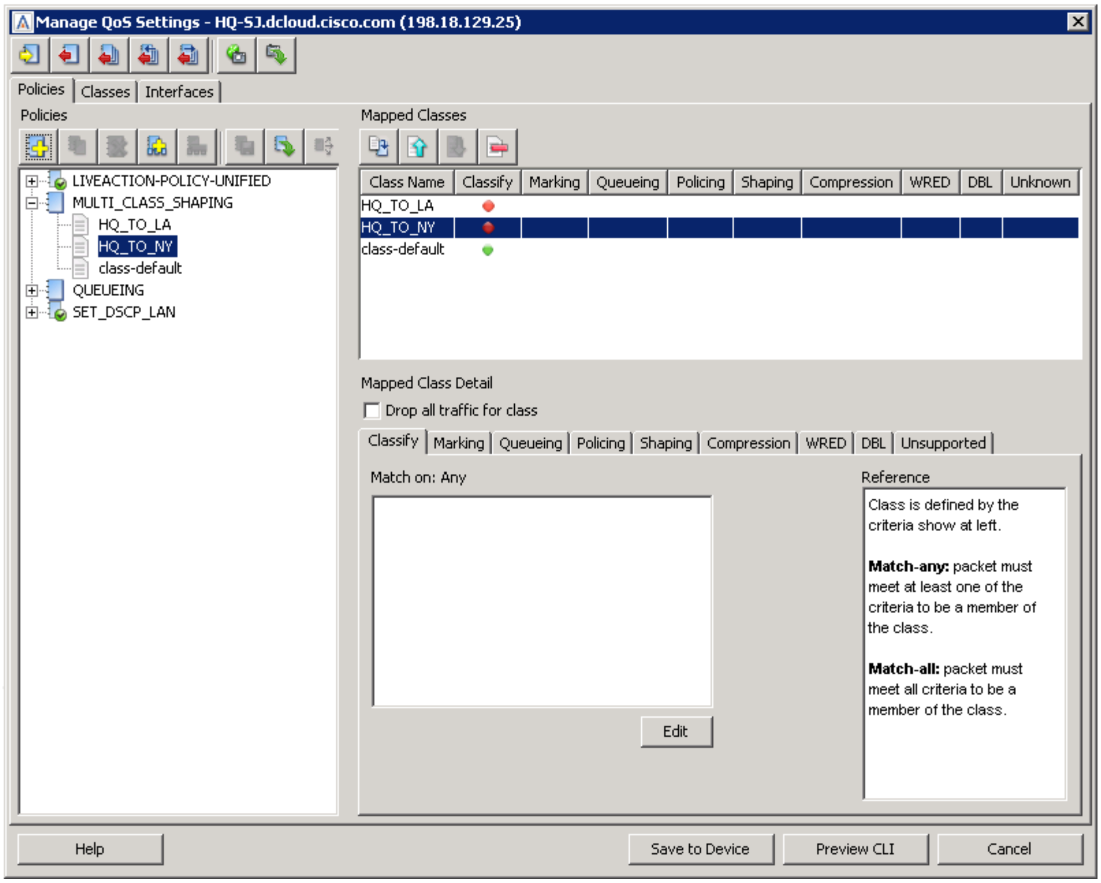
The Manage QoS Dialog Window will open

3. Create a new policy and name it MULTI_CLASS_SHAPING



Policy name: MULTI_CLASS_SHAPING

4. Create two classes within this Policy:
   - HQ_TO_NY
   - HQ_TO_LA



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| HQ_TO_LA | ● | | | | | | | | |
| HQ_TO_NY | ● | | | | | | | | |
| class-default | ● | | | | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Match on: Any

Reference

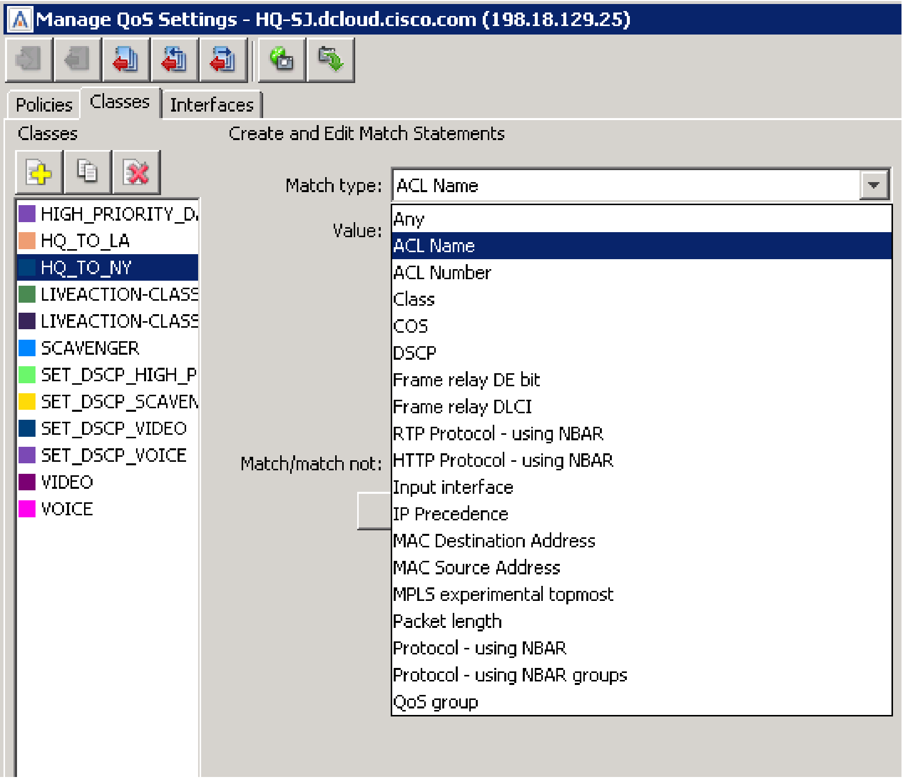
Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

**Note:** These classes each reference an access-list (ACL) for matching traffic from HQ to the respective remote sites. **These ACLs may NOT have been created… you may need to create 2 ACLs before continuing with the Lab.**

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



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

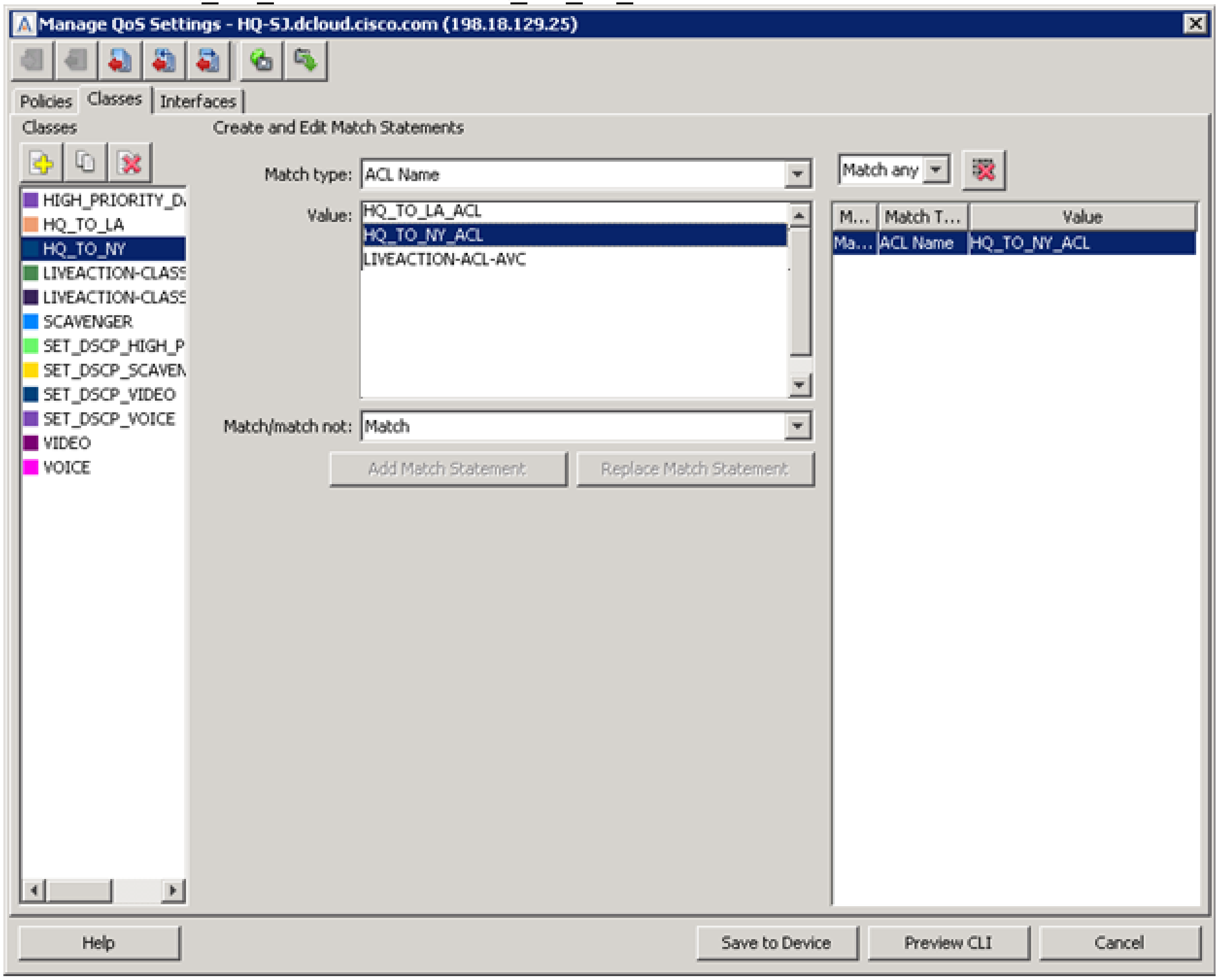
Match type: ACL Name

Value:

Match/match not:

**Note:** You may need to create the following ACLs on your Training Pod. Use the steps you learned in Lab Workbook Pt.1, to create the new ACLs. Create “HQ_TO_NY” from IP 198.18.129.0/24 to 198.19.2.0/24, and “HQ_TO_LA” from IP 198.19.129.0/24 to 198.19.1.0/24

6. Match the HQ_TO_NY class to the HQ_TO_NY_ACL
7. Match the HQ_TO_LA class to the HQ_TO_LA_ACL



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Classes

- HIGH_PRIORITY_D.
- HQ_TO_LA
- HQ_TO_NY
- LIVEACTION-CLASS
- LIVEACTION-CLASS
- SCAVENGER
- SET_DSCP_HIGH_P
- SET_DSCP_SCAVEN
- SET_DSCP_VIDEO
- SET_DSCP_VOICE
- VIDEO
- VOICE

Create and Edit Match Statements

Match type: ACL Name

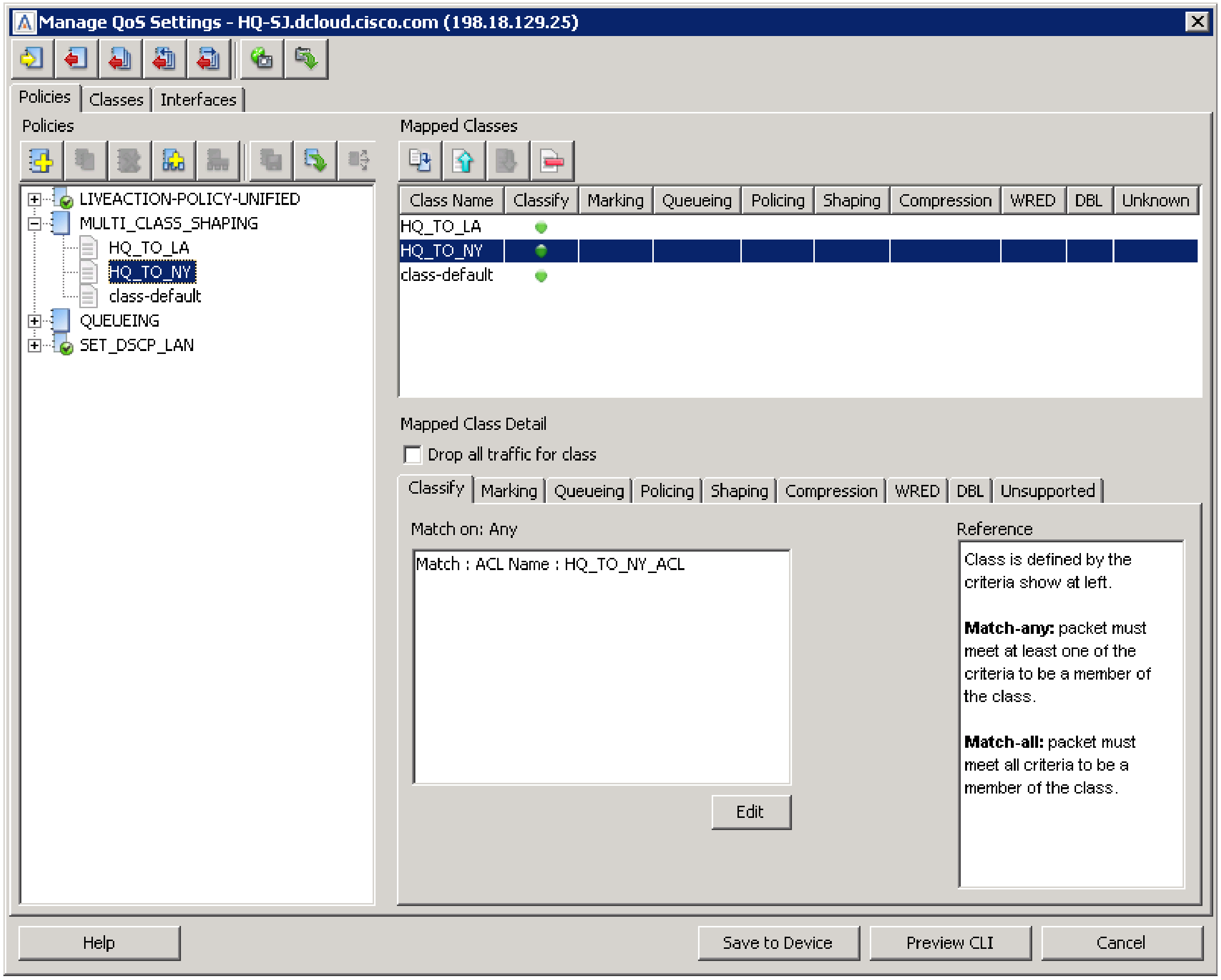
Value: HQ_TO_LA_ACL, HQ_TO_NY_ACL, LIVEACTION-ACL-AVC

Match/match not: Match

Match any

| M... | Match T... | Value |
|---|---|---|
| Ma... | ACL Name | HQ_TO_NY_ACL |

8. When finished, return to the Policy tab



| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| HQ_TO_LA | ● | | | | | | | | |
| HQ_TO_NY | ● | | | | | | | | |
| class-default | ● | | | | | | | | |

□ Drop all traffic for class

Match on: Any

Match : ACL Name : HQ_TO_NY_ACL

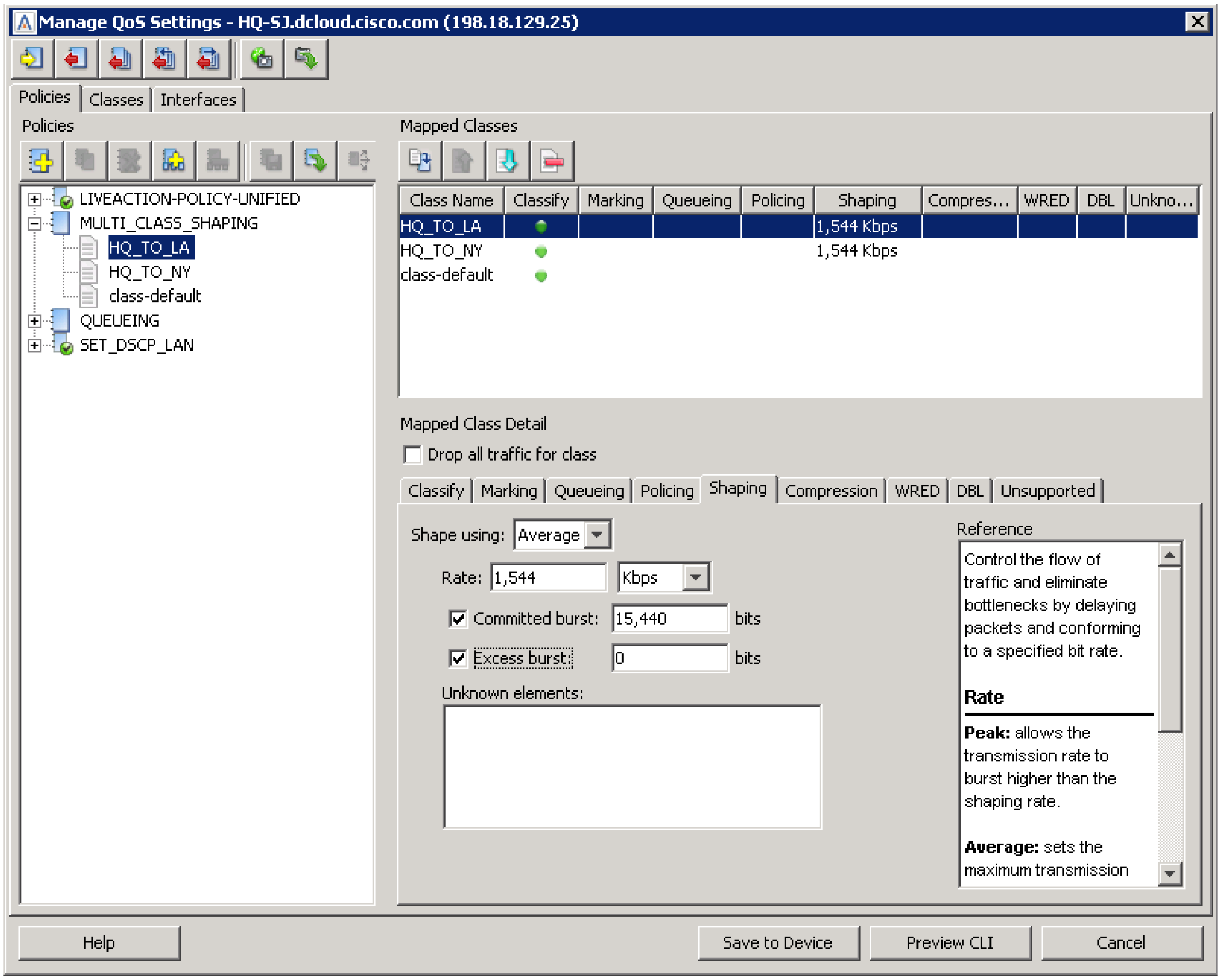
Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

9. Select the HQ_TO_NY class and select the shaping tab. Set its parameters to:
   - Shape using = Average
   - Rate = 1544 Kbps
   - Committed burst = 15,440
   - Excess burst = 0

10. Select the HQ_TO_LA class and select the shaping tab. Set its parameters to:
    - Shape using = Average
    - Rate = 1544 Kbps
    - Committed burst = 15,440
    - Excess burst = 0



| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compres... | WRED | DBL | Unkno... |
|---|---|---|---|---|---|---|---|---|---|
| HQ_TO_LA | ● | | | | 1,544 Kbps | | | | |
| HQ_TO_NY | ● | | | | 1,544 Kbps | | | | |
| class-default | ● | | | | | | | | |

□ Drop all traffic for class

Shape using: Average

Rate: 1,544 Kbps

☑ Committed burst: 15,440 bits

☑ Excess burst: 0 bits

Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

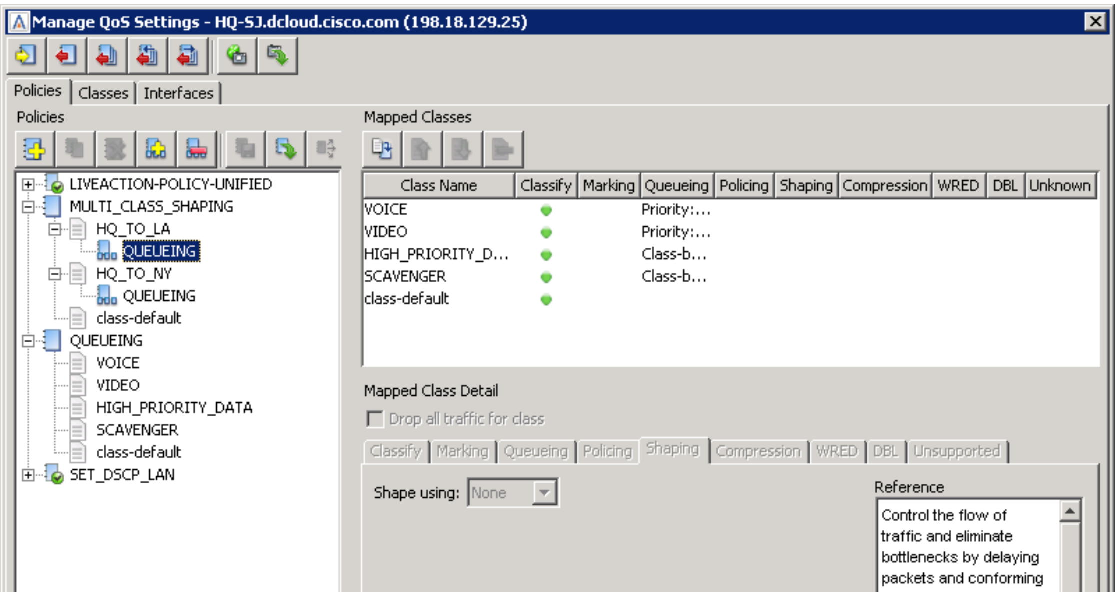
**Rate**

**Peak:** allows the transmission rate to burst higher than the shaping rate.

**Average:** sets the maximum transmission

11. Click-Drag-and-Drop the QUEUEING policy to  the class-default of the HQ_TO_NY policy
12. Click-Drag-and-Drop the QUEUEING policy to  the class-default of the HQ_TO_LA policy

When finished your view should look like this:



```
LIVEACTION-POLICY-UNIFIED
MULTI_CLASS_SHAPING
    HQ_TO_LA
        QUEUEING
    HQ_TO_NY
        QUEUEING
    class-default
QUEUEING
    VOICE
    VIDEO
    HIGH_PRIORITY_DATA
    SCAVENGER
    class-default
SET_DSCP_LAN
```

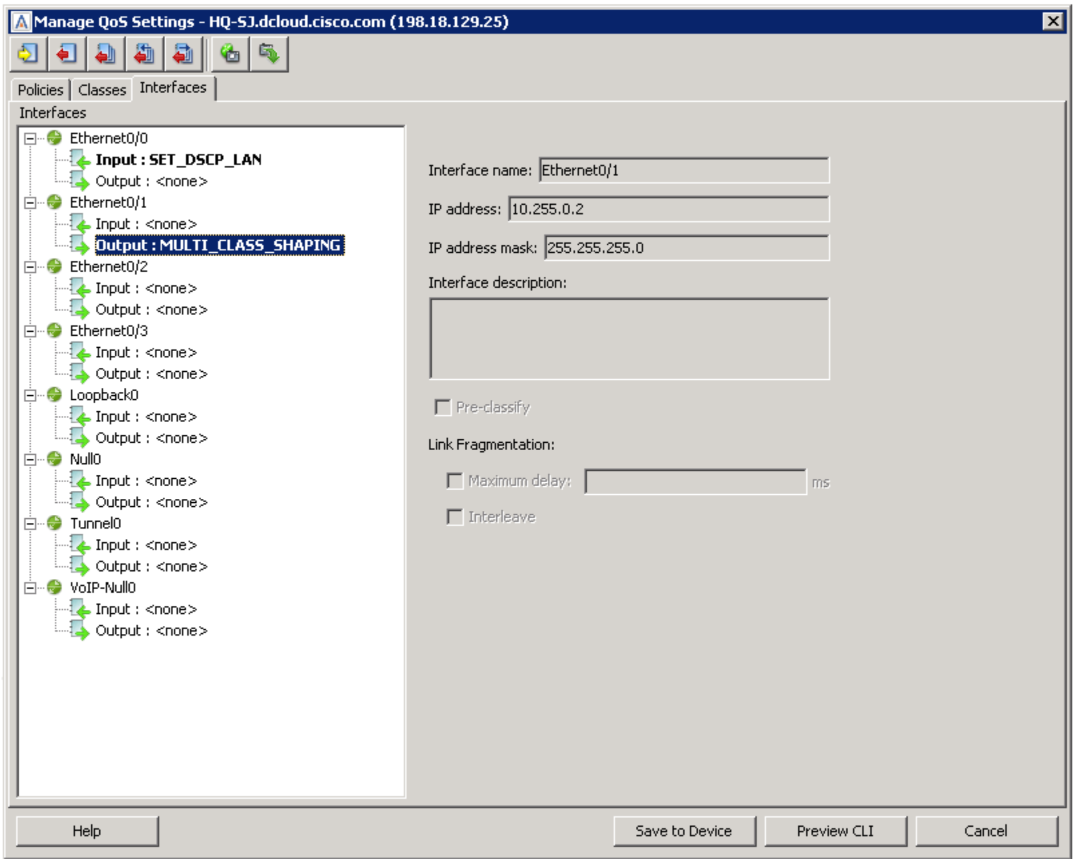
| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority:... | | | | | | |
| VIDEO | ● | | Priority:... | | | | | | |
| HIGH_PRIORITY_D... | ● | | Class-b... | | | | | | |
| SCAVENGER | ● | | Class-b... | | | | | | |
| class-default | ● | | | | | | | | |

□ Drop all traffic for class

Shape using: None

Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming

13. Select the interfaces tab and apply the MULTI_CLASS_SHAPING policy to the output of the GigabitEthernet1 interface.



```
Ethernet0/0
    Input : SET_DSCP_LAN
    Output : <none>
Ethernet0/1
    Input : <none>
    Output : MULTI_CLASS_SHAPING
Ethernet0/2
    Input : <none>
    Output : <none>
Ethernet0/3
    Input : <none>
    Output : <none>
Loopback0
    Input : <none>
    Output : <none>
Null0
    Input : <none>
    Output : <none>
Tunnel0
    Input : <none>
    Output : <none>
VoIP-Null0
    Input : <none>
    Output : <none>
```

Interface name: Ethernet0/1

IP address: 10.255.0.2

IP address mask: 255.255.255.0

Interface description:

□ Pre-classify

Link Fragmentation:

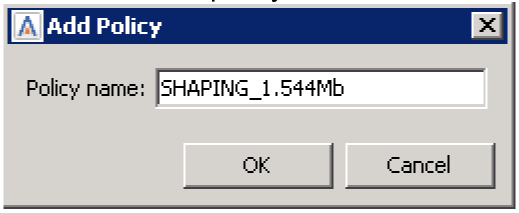
□ Maximum delay: ms

□ Interleave

14. Click Save to Device.

Next, we will build basic hierarchical polices on the remote routers.

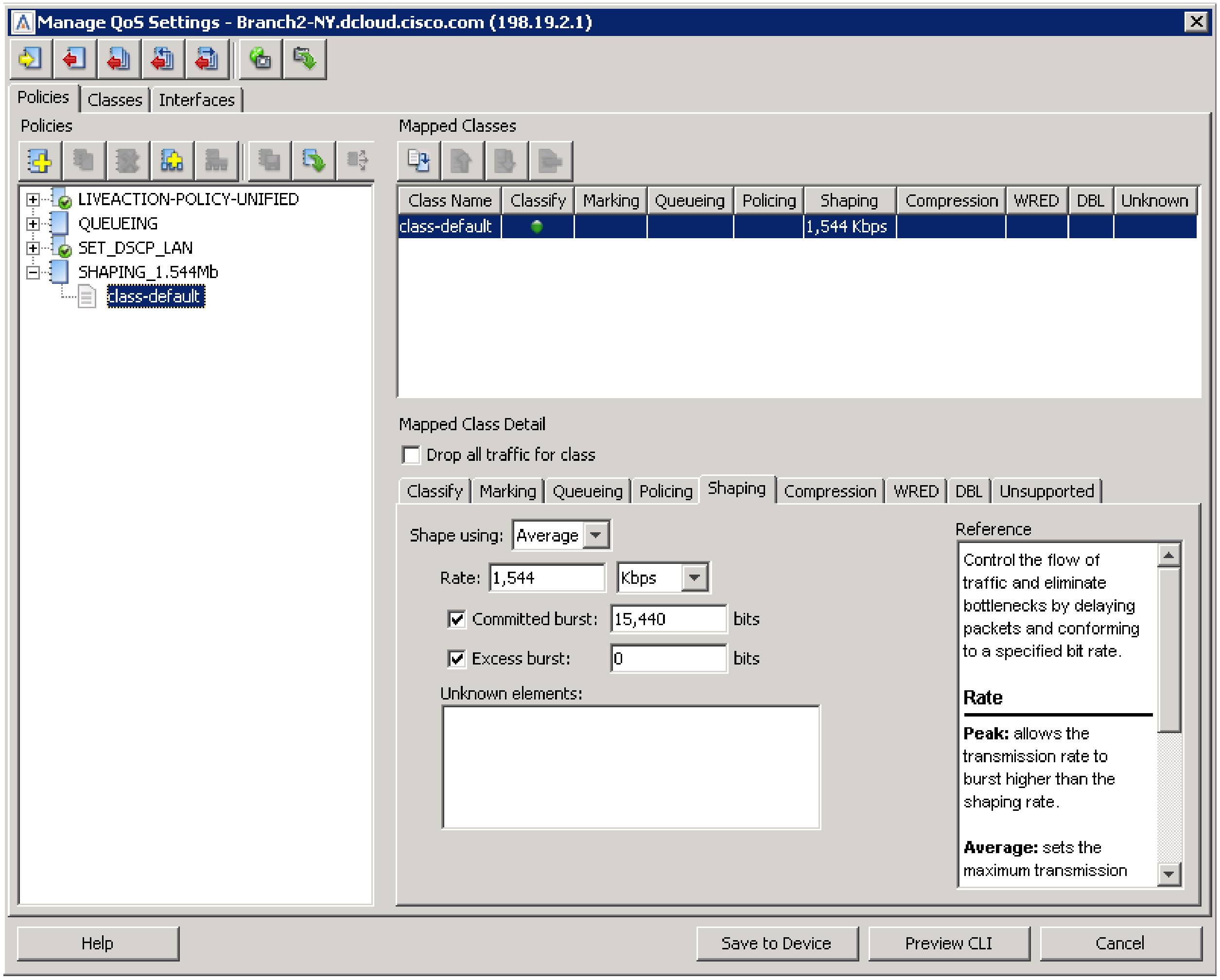
1. In LiveNX, select the QoS Tab
2. Right-click on the one of the remote routers, select QoS > Manage QoS Settings
3. Create a new policy and name it “SHAPING_1.544Mb”



Add Policy

Policy name: SHAPING_1.544Mb

4. Select its class-default and select the Shaping tab.
5. Implement a shaping policy with the following parameters:
   - Shape using = Average
   - Rate = 1544 Kbps
   - Committed burst = 15,440
   - Excess burst = 0



Manage QoS Settings - Branch2-NY.dcloud.cisco.com (198.19.2.1)

| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| class-default | ● | | | | 1,544 Kbps | | | | |

Mapped Class Detail

☐ Drop all traffic for class

Shape using: Average

Rate: 1,544 Kbps

☑ Committed burst: 15,440 bits

☑ Excess burst: 0 bits

Unknown elements:

Reference

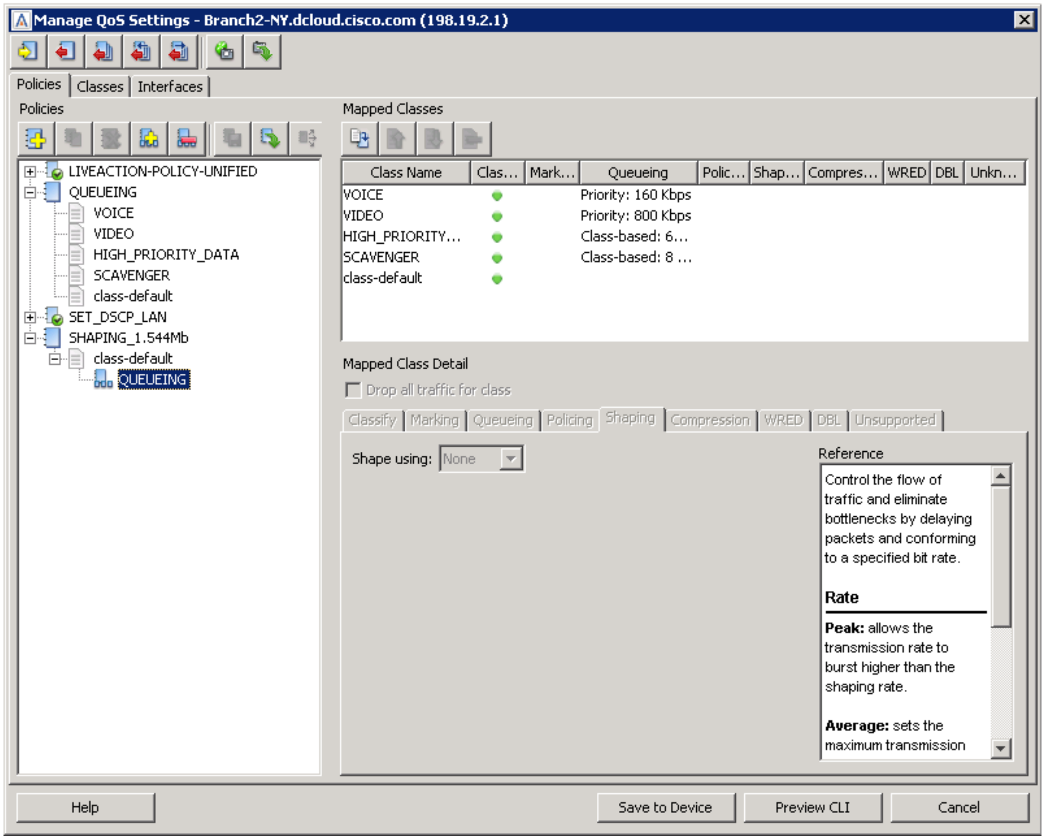
Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

**Rate**

**Peak:** allows the transmission rate to burst higher than the shaping rate.

**Average:** sets the maximum transmission

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



Manage QoS Settings - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- QUEUEING
  - VOICE
  - VIDEO
  - HIGH_PRIORITY_DATA
  - SCAVENGER
  - class-default
- SET_DSCP_LAN
- SHAPING_1.544Mb
  - class-default
    - QUEUEING

Mapped Classes

| Class Name | Clas… | Mark… | Queueing | Polic… | Shap… | Compres… | WRED | DBL | Unkn… |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority: 160 Kbps | | | | | | |
| VIDEO | ● | | Priority: 800 Kbps | | | | | | |
| HIGH_PRIORITY… | ● | | Class-based: 6… | | | | | | |
| SCAVENGER | ● | | Class-based: 8 … | | | | | | |
| class-default | ● | | | | | | | | |

Mapped Class Detail

□ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Shape using: None

Reference

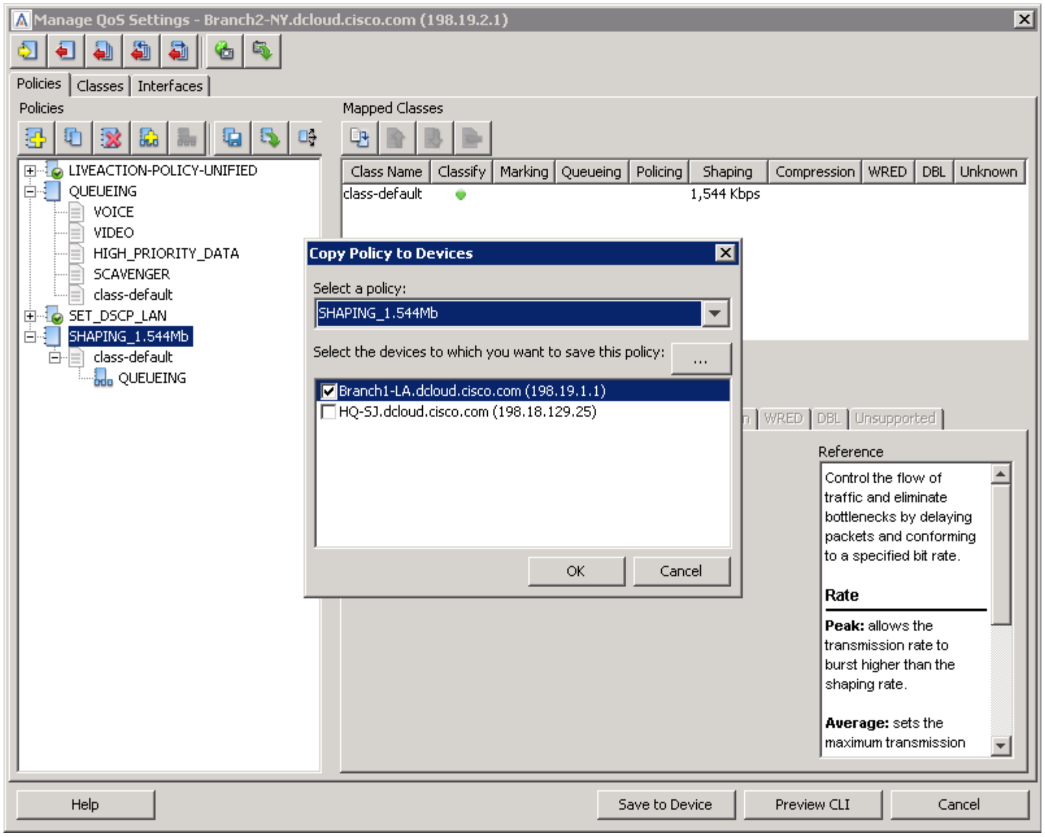
Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

**Rate**

**Peak:** allows the transmission rate to burst higher than the shaping rate.

**Average:** sets the maximum transmission

7. Copy the SHAPING_1.544Mb policy to the other remote router



Manage QoS Settings - Branch2-NY.dcloud.cisco.com (198.19.2.1)

Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- QUEUEING
  - VOICE
  - VIDEO
  - HIGH_PRIORITY_DATA
  - SCAVENGER
  - class-default
- SET_DSCP_LAN
- SHAPING_1.544Mb
  - class-default
    - QUEUEING

Mapped Classes

| Class Name | Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unknown |
|---|---|---|---|---|---|---|---|---|---|
| class-default | ● | | | | 1,544 Kbps | | | | |

Copy Policy to Devices

Select a policy: SHAPING_1.544Mb

Select the devices to which you want to save this policy: …

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
□ HQ-SJ.dcloud.cisco.com (198.18.129.25)

WRED | DBL | Unsupported

Reference

Control the flow of traffic and eliminate bottlenecks by delaying packets and conforming to a specified bit rate.

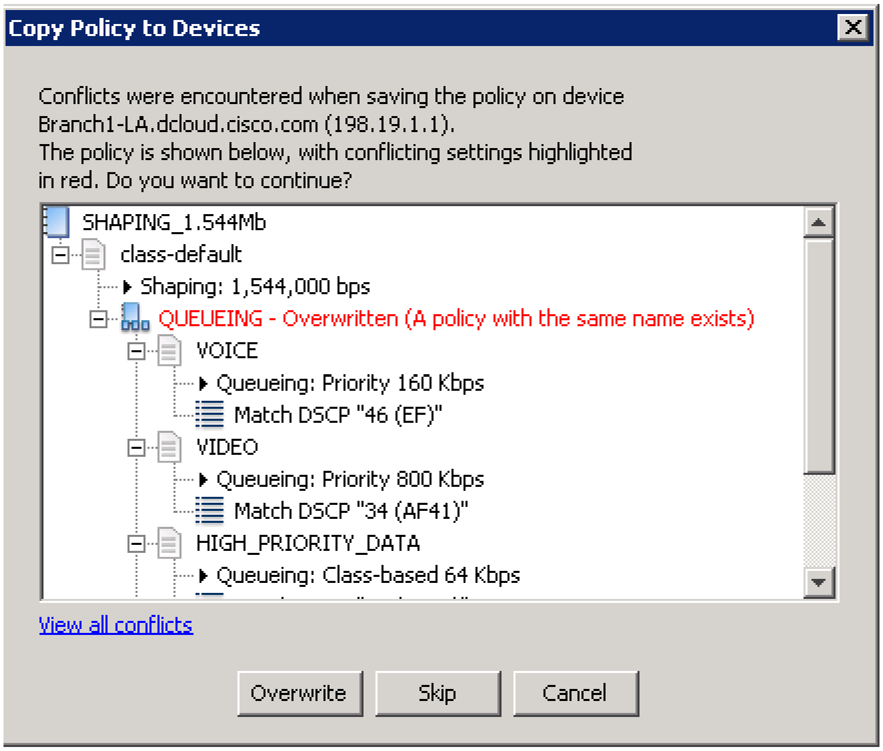
**Rate**

**Peak:** allows the transmission rate to burst higher than the shaping rate.

**Average:** sets the maximum transmission

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

8. Select Overwrite.

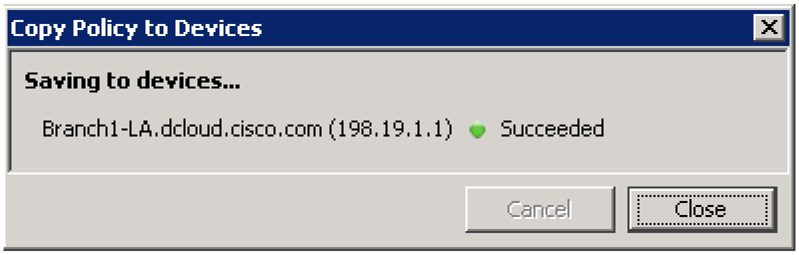


Copy Policy to Devices

Conflicts were encountered when saving the policy on device Branch1-LA.dcloud.cisco.com (198.19.1.1).
The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?

```
SHAPING_1.544Mb
  class-default
    Shaping: 1,544,000 bps
    QUEUEING - Overwritten (A policy with the same name exists)
      VOICE
        Queueing: Priority 160 Kbps
        Match DSCP "46 (EF)"
      VIDEO
        Queueing: Priority 800 Kbps
        Match DSCP "34 (AF41)"
      HIGH_PRIORITY_DATA
        Queueing: Class-based 64 Kbps
```

9. Validate the changes saved successfully.



Copy Policy to Devices

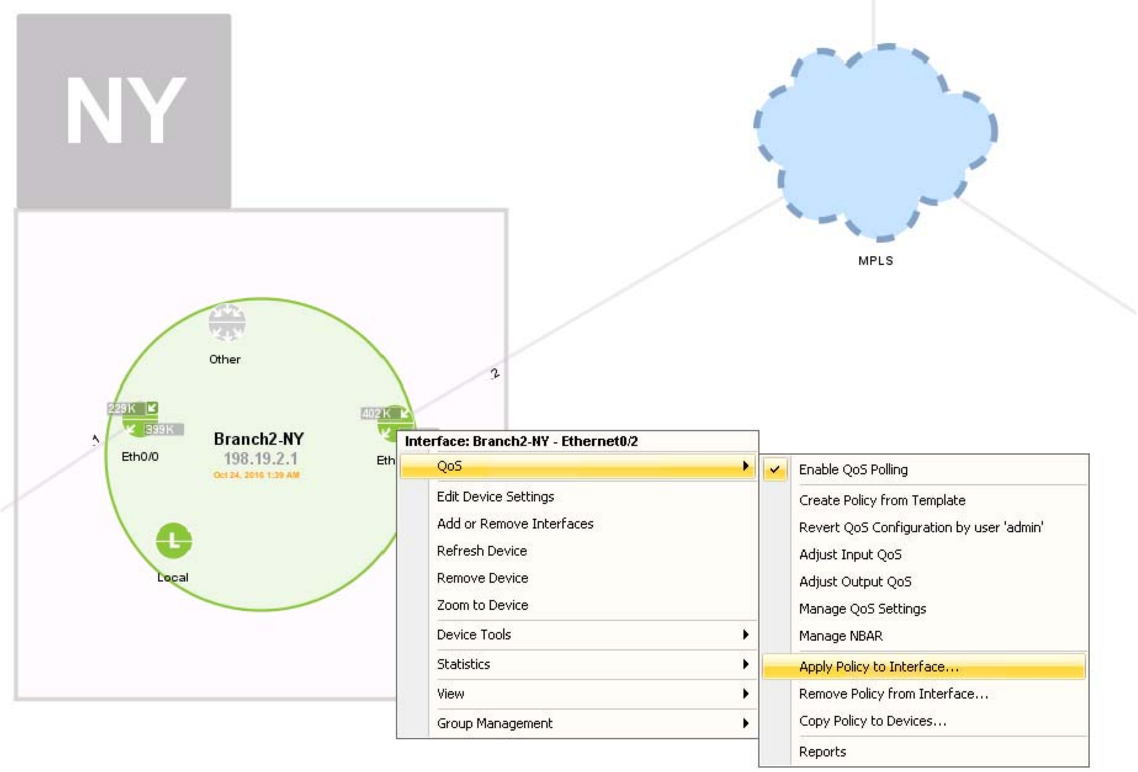
**Saving to devices...**

Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded

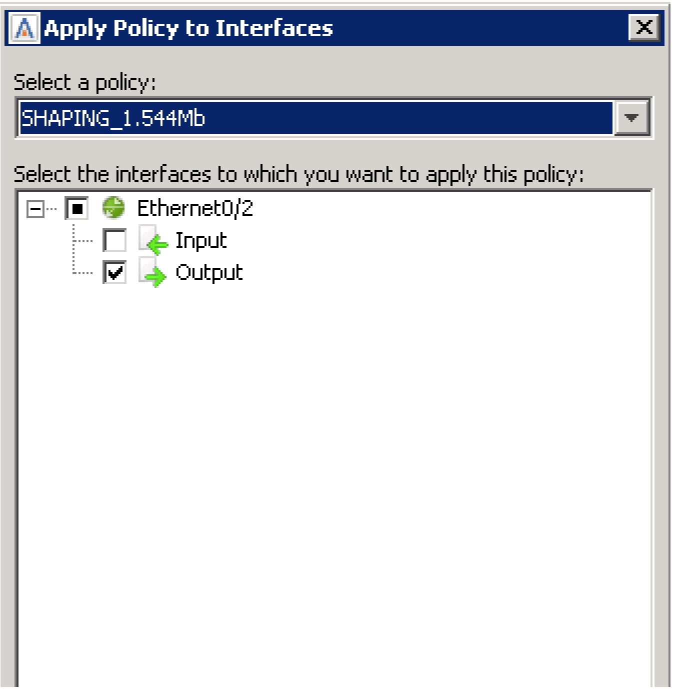
10. Save to Device and close the Manage QoS Settings dialog window.

11. Select the QoS Tab

12. Right-click on the WAN interface (GigEth1) on the NY router, select QoS > Apply Policy to Interface



13. Apply the SHAPING_1.544Mb policy to the output of Eth0/2.


Apply Policy to Interfaces

Select a policy: SHAPING_1.544Mb

Select the interfaces to which you want to apply this policy:

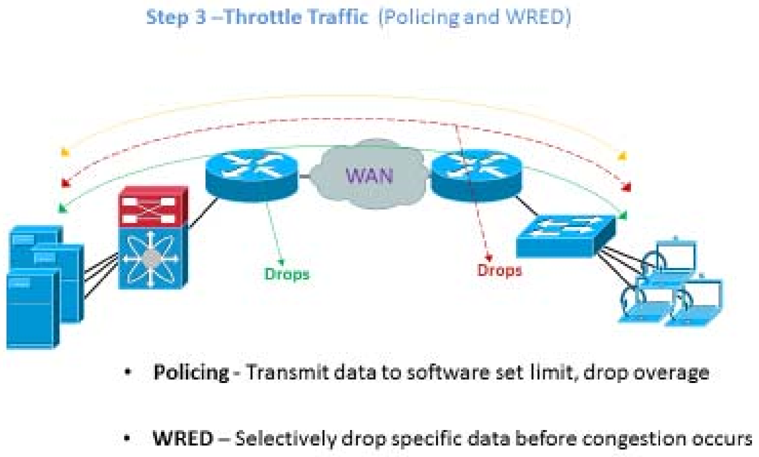
- ■ Ethernet0/2
  - □ Input
  - ☑ Output

14. C. Repeat this process and apply the SHAPING_1.544Mb policy to the LA router.

# Lab 5

## Lab 5:  Throttling Traffic

# Lab 5.0: Intro - Throttling / Policing

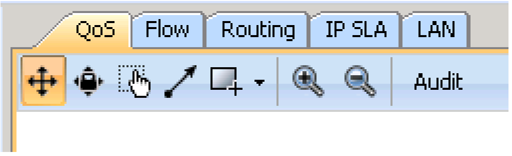


Step 3 –Throttle Traffic (Policing and WRED)

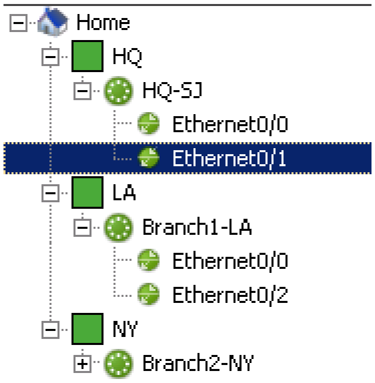
- **Policing** - Transmit data to software set limit, drop overage
- **WRED** – Selectively drop specific data before congestion occurs

Investigate the current traffic flows.

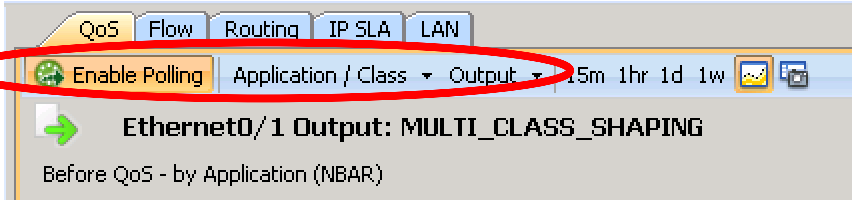
1. From the LiveNX Client, select the QoS Tab



2. Select GigabitEthernet1 from the HQ router
3. update the real-time view to the following:



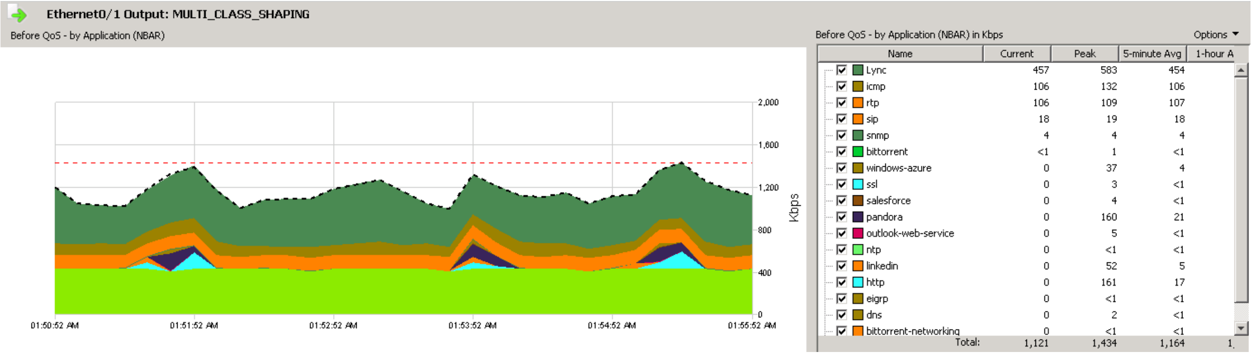
4. Update the real-time interface view to the following settings.



Ethernet0/1 Output: MULTI_CLASS_SHAPING

Before QoS - by Application (NBAR)

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



Ethernet0/1 Output: MULTI_CLASS_SHAPING

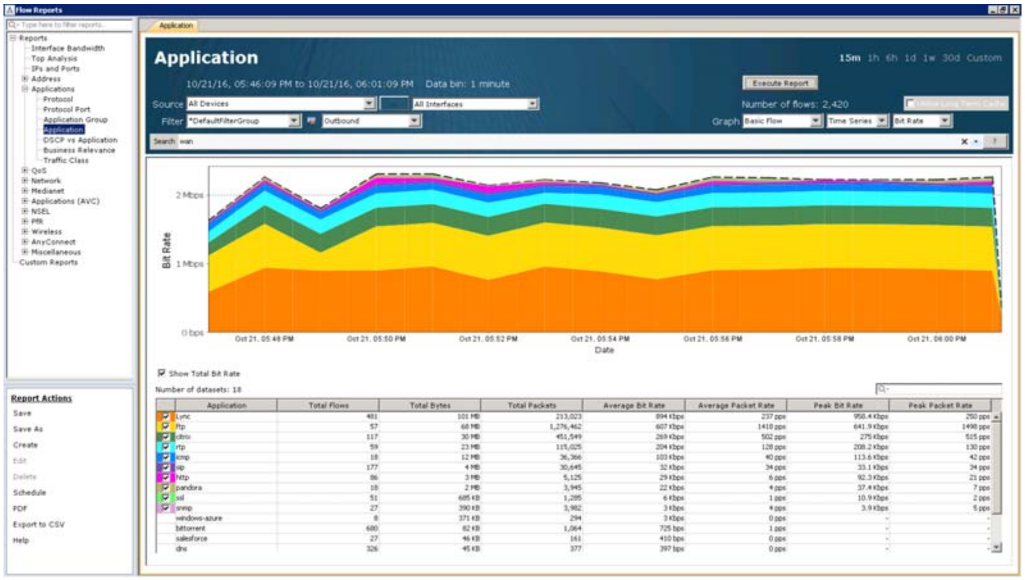
Before QoS - by Application (NBAR)

Before QoS - by Application (NBAR) in Kbps

| Name | Current | Peak | 5-minute Avg | 1-hour A |
|---|---|---|---|---|
| ☑ Lync | 457 | 583 | 454 | |
| ☑ icmp | 106 | 132 | 106 | |
| ☑ rtp | 106 | 109 | 107 | |
| ☑ sip | 18 | 19 | 18 | |
| ☑ snmp | 4 | 4 | 4 | |
| ☑ bittorrent | <1 | 1 | <1 | |
| ☑ windows-azure | 0 | 37 | 4 | |
| ☑ ssl | 0 | 3 | <1 | |
| ☑ salesforce | 0 | 4 | <1 | |
| ☑ pandora | 0 | 160 | 21 | |
| ☑ outlook-web-service | 0 | 5 | <1 | |
| ☑ ntp | 0 | <1 | <1 | |
| ☑ linkedin | 0 | 52 | 5 | |
| ☑ http | 0 | 161 | 17 | |
| ☑ eigrp | 0 | <1 | <1 | |
| ☑ dns | 0 | 2 | <1 | |
| ☑ bittorrent-networking | 0 | <1 | <1 | |
| Total: | 1,121 | 1,434 | 1,164 | 1, |

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

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



Application

10/21/16, 05:46:09 PM to 10/21/16, 06:01:09 PM Data bin: 1 minute

Source: All Devices, All Interfaces

Filter: *DefaultFilterGroup, Outbound

Number of flows: 2,420

Graph: Basic Flow, Time Series, Bit Rate

Search: wan

☑ Show Total Bit Rate

Number of datasets: 18

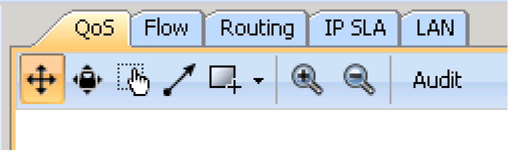
| Application | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|
| ☑ Lync | 481 | 101 MB | 213,023 | 894 Kbps | 237 pps | 958.4 Kbps | 250 pps |
| ☑ ftp | 57 | 68 MB | 1,276,462 | 607 Kbps | 1418 pps | 641.9 Kbps | 1498 pps |
| ☑ citrix | 117 | 30 MB | 451,549 | 269 Kbps | 502 pps | 275 Kbps | 515 pps |
| ☑ rtp | 59 | 23 MB | 115,025 | 204 Kbps | 128 pps | 208.2 Kbps | 130 pps |
| ☑ icmp | 18 | 12 MB | 36,366 | 103 Kbps | 40 pps | 113.6 Kbps | 42 pps |
| ☑ sip | 177 | 4 MB | 30,645 | 32 Kbps | 34 pps | 33.1 Kbps | 34 pps |
| ☑ http | 86 | 3 MB | 5,125 | 29 Kbps | 6 pps | 92.3 Kbps | 21 pps |
| ☑ pandora | 18 | 2 MB | 3,945 | 22 Kbps | 4 pps | 37.4 Kbps | 7 pps |
| ☑ ssl | 51 | 685 KB | 1,295 | 6 Kbps | 1 pps | 10.9 Kbps | 2 pps |
| ☑ snmp | 27 | 390 KB | 3,982 | 3 Kbps | 4 pps | 3.9 Kbps | 5 pps |
| windows-azure | 8 | 371 KB | 294 | 3 Kbps | 0 pps | - | - |
| bittorrent | 680 | 82 KB | 1,064 | 725 bps | 1 pps | - | - |
| salesforce | 27 | 46 KB | 161 | 410 bps | 0 pps | - | - |
| dns | 326 | 45 KB | 377 | 397 bps | 0 pps | - | - |

# Lab 5.1: Throttling / Policing

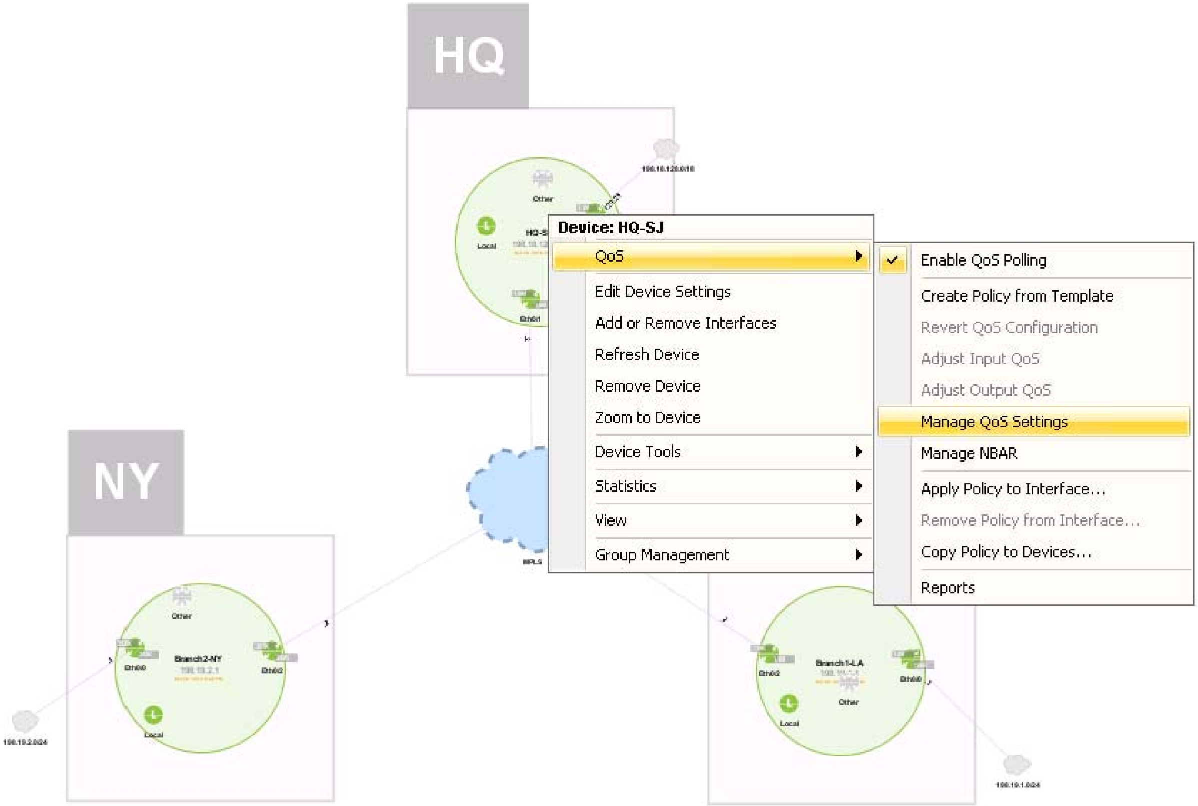
We'll implement a basic policing polity to throttle any scavenger (less than default) traffic.

Lab Steps:

1. From the LiveAction map, select the QoS Tab

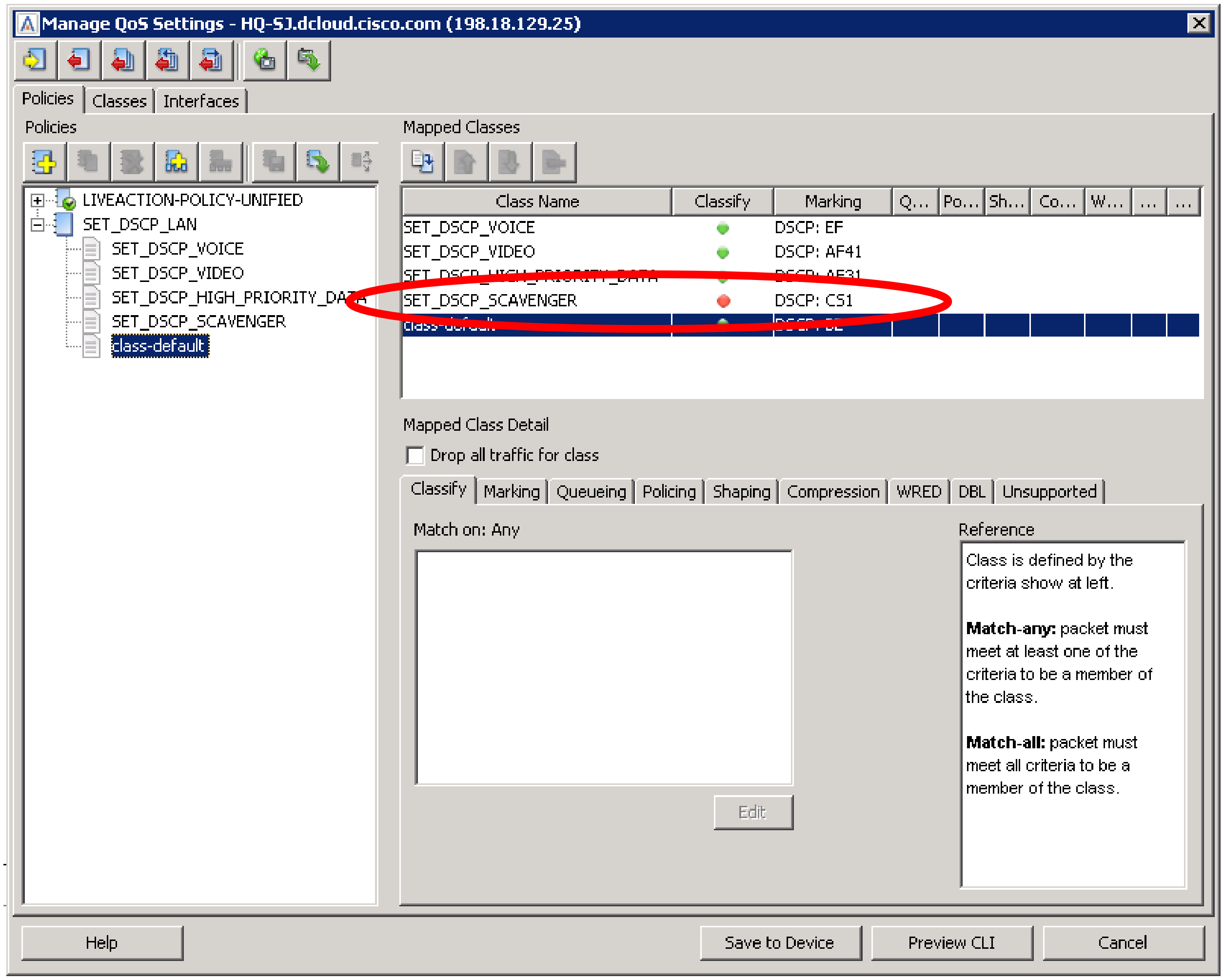


2. Right-click on the HQ router and select QoS > Manage QoS Settings



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

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



Policies:

- LIVEACTION-POLICY-UNIFIED
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DATA
  - SET_DSCP_SCAVENGER
  - class-default

Mapped Classes:

| Class Name | Classify | Marking | Q... | Po... | Sh... | Co... | W... | ... | ... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | DSCP: EF | | | | | | | |
| SET_DSCP_VIDEO | ● | DSCP: AF41 | | | | | | | |
| SET_DSCP_HIGH_PRIORITY_DATA | ● | DSCP: AF31 | | | | | | | |
| SET_DSCP_SCAVENGER | ● | DSCP: CS1 | | | | | | | |
| class-default | ● | DSCP: BE | | | | | | | |

☐ Drop all traffic for class

Match on: Any

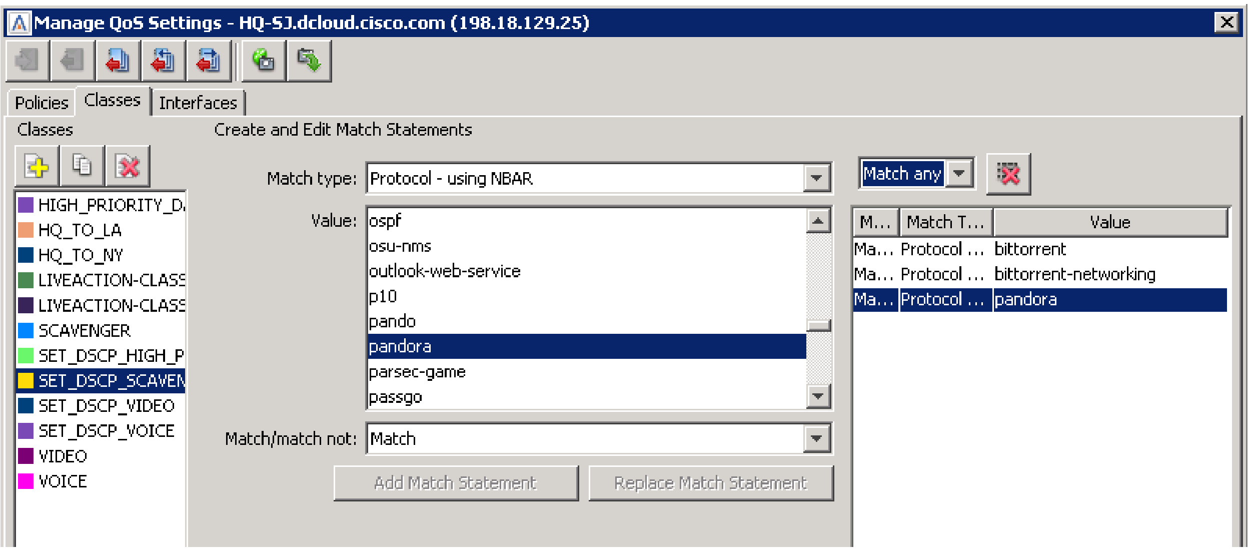
Reference

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

3. Update the SET_DSCP_SCAVENGER class with the following traffic:
   - Pandora
   - Bittorrent
   - Bittorrent-networking


Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)
Policies
Classes
Interfaces
Classes
Create and Edit Match Statements
Add Match Statement
Replace Match Statement

Classes:

- HIGH_PRIORITY_D...
- HQ_TO_LA
- HQ_TO_NY
- LIVEACTION-CLASS
- LIVEACTION-CLASS
- SCAVENGER
- SET_DSCP_HIGH_P
- SET_DSCP_SCAVEN
- SET_DSCP_VIDEO
- SET_DSCP_VOICE
- VIDEO
- VOICE

Match type: Protocol - using NBAR

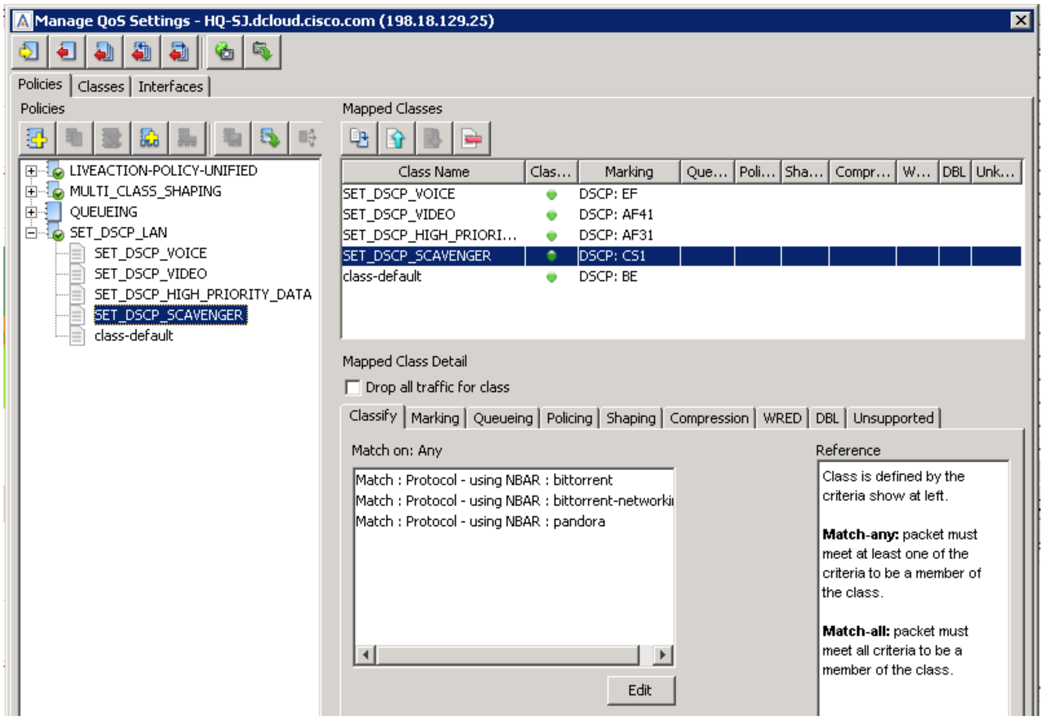
Value: ospf, osu-nms, outlook-web-service, p10, pando, pandora, parsec-game, passgo

Match/match not: Match

Match any

| M... | Match T... | Value |
|---|---|---|
| Ma... | Protocol ... | bittorrent |
| Ma... | Protocol ... | bittorrent-networking |
| Ma... | Protocol ... | pandora |

When finished, the SET_DSCP_LAN policy should look like this:



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- MULTI_CLASS_SHAPING
- QUEUEING
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DATA
  - SET_DSCP_SCAVENGER
  - class-default

Mapped Classes

| Class Name | Clas... | Marking | Que... | Poli... | Sha... | Compr... | W... | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | DSCP: EF | | | | | | | |
| SET_DSCP_VIDEO | ● | DSCP: AF41 | | | | | | | |
| SET_DSCP_HIGH_PRIORI... | ● | DSCP: AF31 | | | | | | | |
| SET_DSCP_SCAVENGER | ● | DSCP: CS1 | | | | | | | |
| class-default | ● | DSCP: BE | | | | | | | |

Mapped Class Detail

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

Match on: Any

Match : Protocol - using NBAR : bittorrent
Match : Protocol - using NBAR : bittorrent-networki
Match : Protocol - using NBAR : pandora

Edit

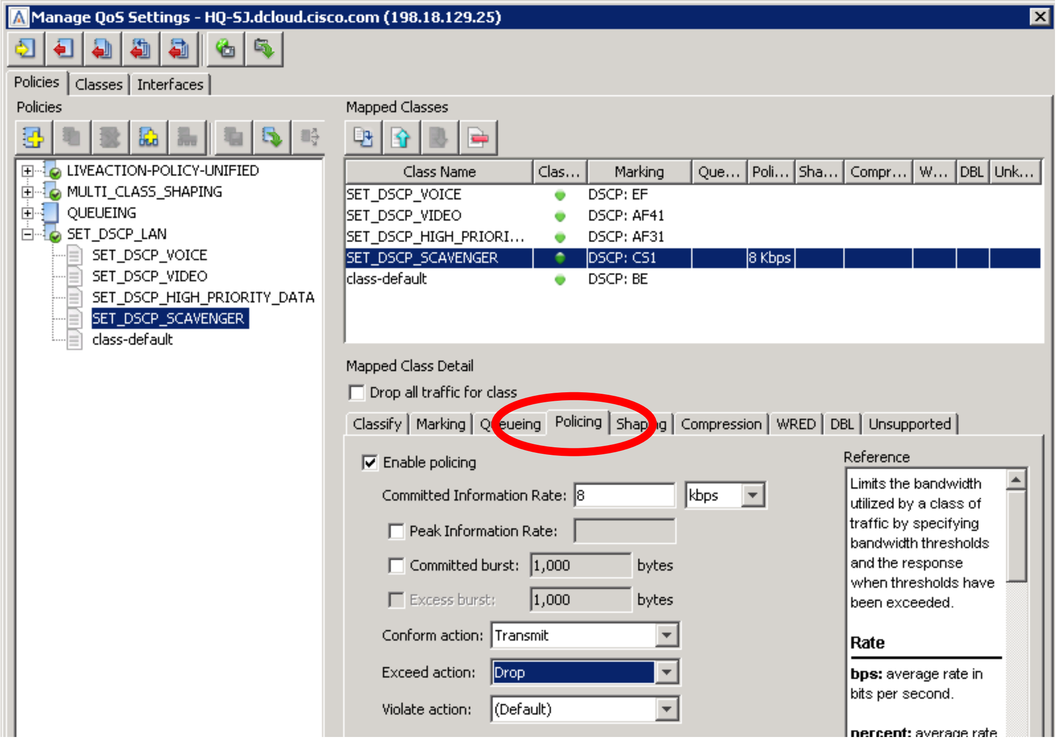
Reference

Class is defined by the criteria show at left.

**Match-any:** packet must meet at least one of the criteria to be a member of the class.

**Match-all:** packet must meet all criteria to be a member of the class.

4. Select the Policing tab and update the following settings:
   - Policing Enabled
   - Committed Information Rate = 8Kbps
   - Conform Action = Transmit
   - Exceed Action = Drop



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Policies | Classes | Interfaces

Policies

- LIVEACTION-POLICY-UNIFIED
- MULTI_CLASS_SHAPING
- QUEUEING
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DATA
  - SET_DSCP_SCAVENGER
  - class-default

Mapped Classes

| Class Name | Clas... | Marking | Que... | Poli... | Sha... | Compr... | W... | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | DSCP: EF | | | | | | | |
| SET_DSCP_VIDEO | ● | DSCP: AF41 | | | | | | | |
| SET_DSCP_HIGH_PRIORI... | ● | DSCP: AF31 | | | | | | | |
| SET_DSCP_SCAVENGER | ● | DSCP: CS1 | | 8 Kbps | | | | | |
| class-default | ● | DSCP: BE | | | | | | | |

Mapped Class Detail

☐ Drop all traffic for class

Classify | Marking | Queueing | Policing | Shaping | Compression | WRED | DBL | Unsupported

☑ Enable policing

Committed Information Rate: 8 kbps

☐ Peak Information Rate:

☐ Committed burst: 1,000 bytes

☐ Excess burst: 1,000 bytes

Conform action: Transmit

Exceed action: Drop

Violate action: (Default)

Reference

Limits the bandwidth utilized by a class of traffic by specifying bandwidth thresholds and the response when thresholds have been exceeded.

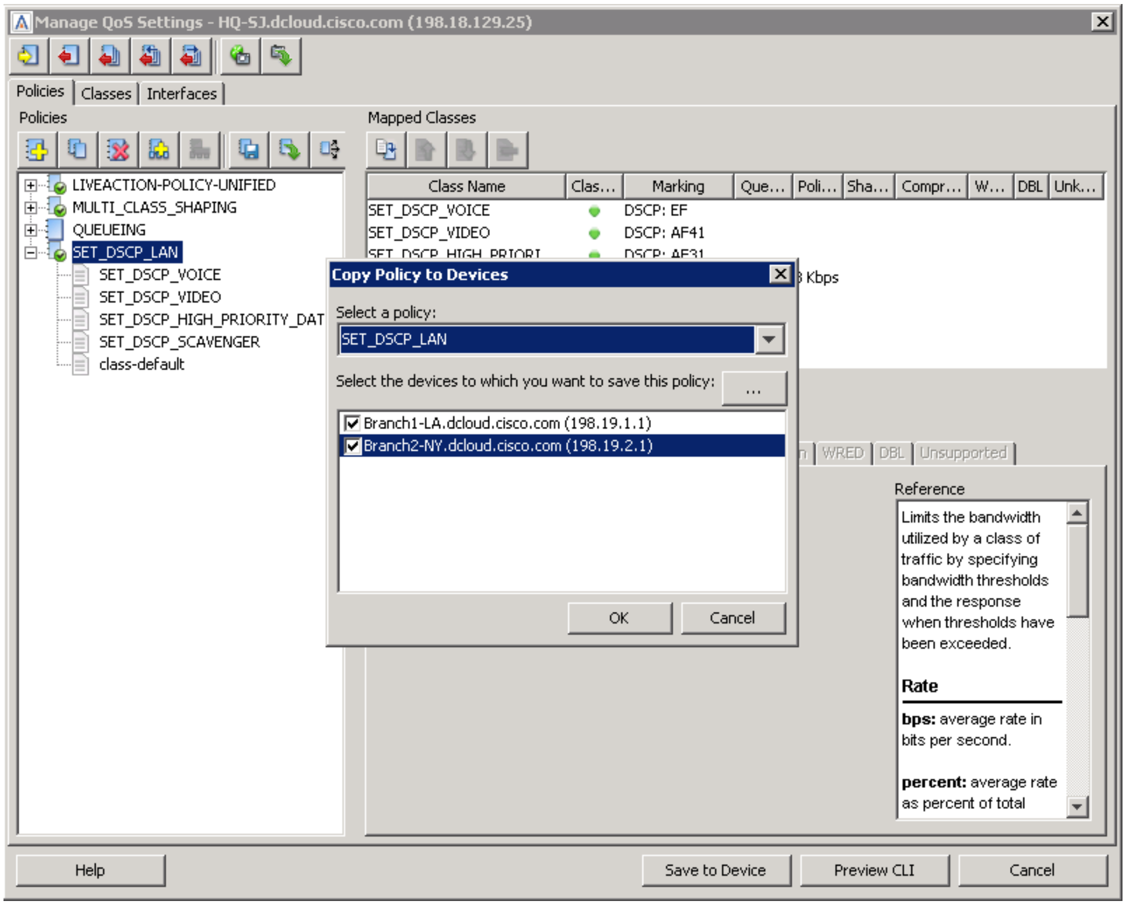
**Rate**

**bps:** average rate in bits per second.

**percent:** average rate

5. Select Save to Device.

6. Copy the SET_DSCP_LAN policy to the other available routers.



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

- LIVEACTION-POLICY-UNIFIED
- MULTI_CLASS_SHAPING
- QUEUEING
- SET_DSCP_LAN
  - SET_DSCP_VOICE
  - SET_DSCP_VIDEO
  - SET_DSCP_HIGH_PRIORITY_DAT
  - SET_DSCP_SCAVENGER
  - class-default

| Class Name | Clas... | Marking | Que... | Poli... | Sha... | Compr... | W... | DBL | Unk... |
|---|---|---|---|---|---|---|---|---|---|
| SET_DSCP_VOICE | ● | DSCP: EF | | | | | | | |
| SET_DSCP_VIDEO | ● | DSCP: AF41 | | | | | | | |
| SET_DSCP_HIGH_PRIORI | ● | DSCP: AF31 | | | | | | | |

Copy Policy to Devices

Select a policy: SET_DSCP_LAN

Select the devices to which you want to save this policy: ...

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)

Reference

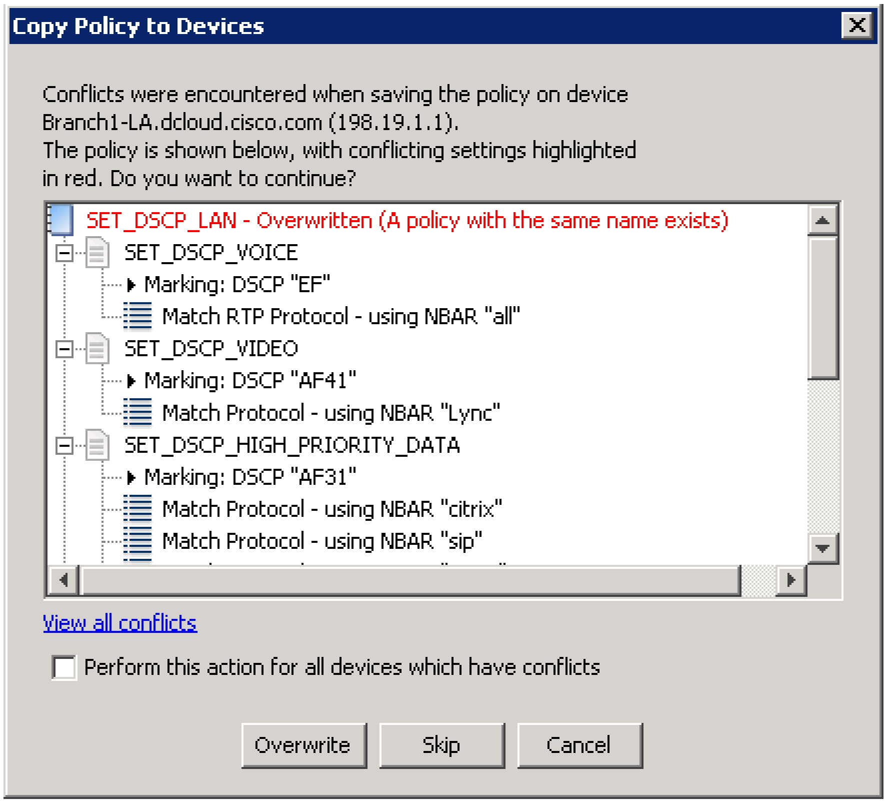
Limits the bandwidth utilized by a class of traffic by specifying bandwidth thresholds and the response when thresholds have been exceeded.

**Rate**

**bps:** average rate in bits per second.

**percent:** average rate as percent of total

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



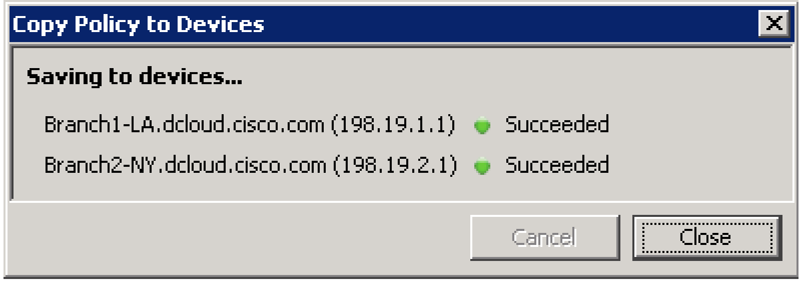
Copy Policy to Devices

Conflicts were encountered when saving the policy on device Branch1-LA.dcloud.cisco.com (198.19.1.1).
The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?

- SET_DSCP_LAN - Overwritten (A policy with the same name exists)
  - SET_DSCP_VOICE
    - Marking: DSCP "EF"
    - Match RTP Protocol - using NBAR "all"
  - SET_DSCP_VIDEO
    - Marking: DSCP "AF41"
    - Match Protocol - using NBAR "Lync"
  - SET_DSCP_HIGH_PRIORITY_DATA
    - Marking: DSCP "AF31"
    - Match Protocol - using NBAR "citrix"
    - Match Protocol - using NBAR "sip"

☐ Perform this action for all devices which have conflicts

7. Validate the changes saved successfully., Click Close,



Saving to devices...

Branch1-LA.dcloud.cisco.com (198.19.1.1) ● Succeeded

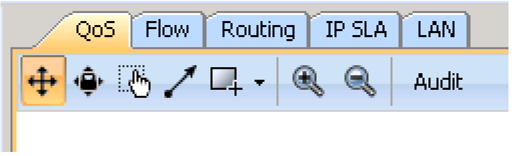
Branch2-NY.dcloud.cisco.com (198.19.2.1) ● Succeeded

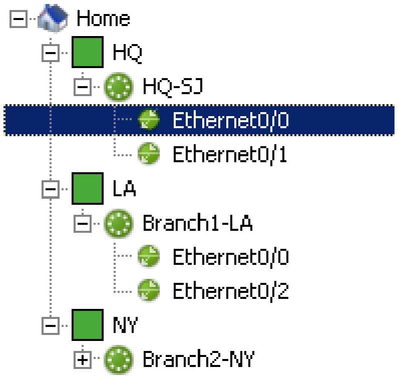
8. Close the Manage QoS Settings Dialog Window

# Lab 5.2:  Confirm policing Settings

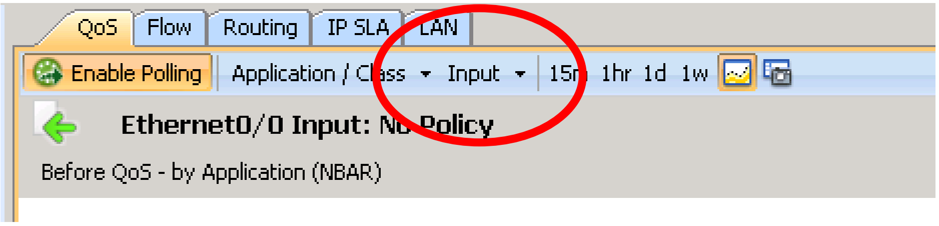
Lab Steps:

1. Select the QoS Tab.





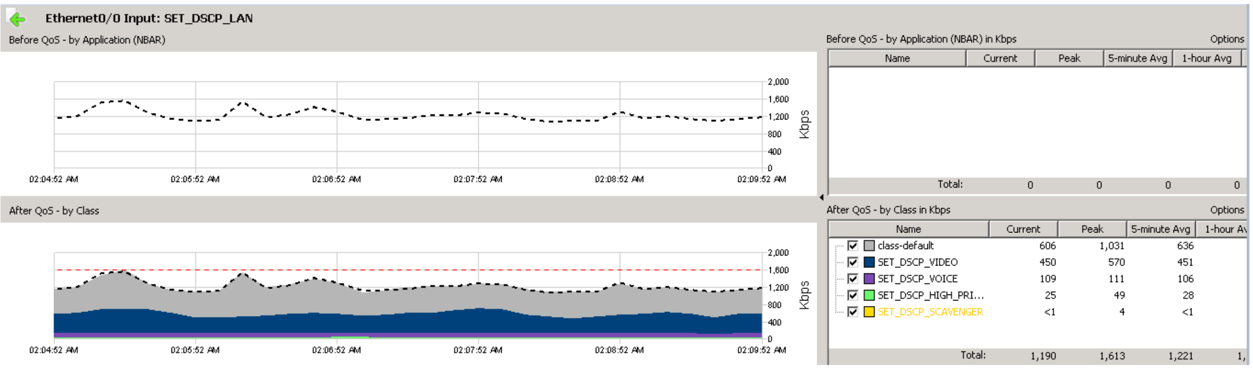
2. From the device list, select the HQ router's LAN interface – GigabitEthernet1
3. Update the real-time view's options to just include the input.



Ethernet0/0 Input: No Policy

Before QoS - by Application (NBAR)

**Note:  Notice how the SET_DSCP_SCAVENGER class is amber?  The amber confirms that drops are occurring inside the queue.**



Ethernet0/0 Input: SET_DSCP_LAN

Before QoS - by Application (NBAR)

After QoS - by Class

Before QoS - by Application (NBAR) in Kbps  Options

| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| Total: | 0 | 0 | 0 | 0 |

After QoS - by Class in Kbps  Options

| Name | Current | Peak | 5-minute Avg | 1-hour Av |
|---|---|---|---|---|
| ☑ class-default | 606 | 1,031 | 636 | |
| ☑ SET_DSCP_VIDEO | 450 | 570 | 451 | |
| ☑ SET_DSCP_VOICE | 109 | 111 | 106 | |
| ☑ SET_DSCP_HIGH_PRI... | 25 | 49 | 28 | |
| ☑ SET_DSCP_SCAVENGER | <1 | 4 | <1 | |
| Total: | 1,190 | 1,613 | 1,221 | 1, |

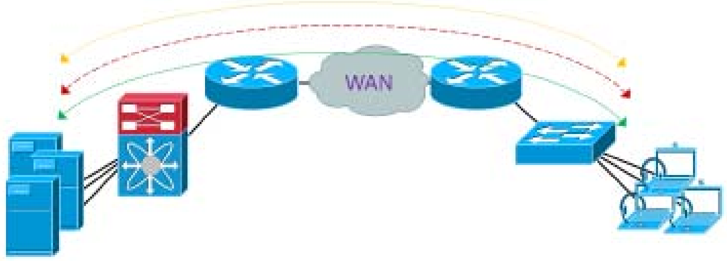
# Lab 6

## Lab 6:  Buffer tuning

# Lab 6.0: Intro – Buffer Tuning

**Buffer Tuning**

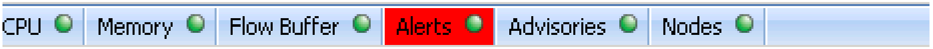
Step 4–Buffer Tuning
(Advanced)



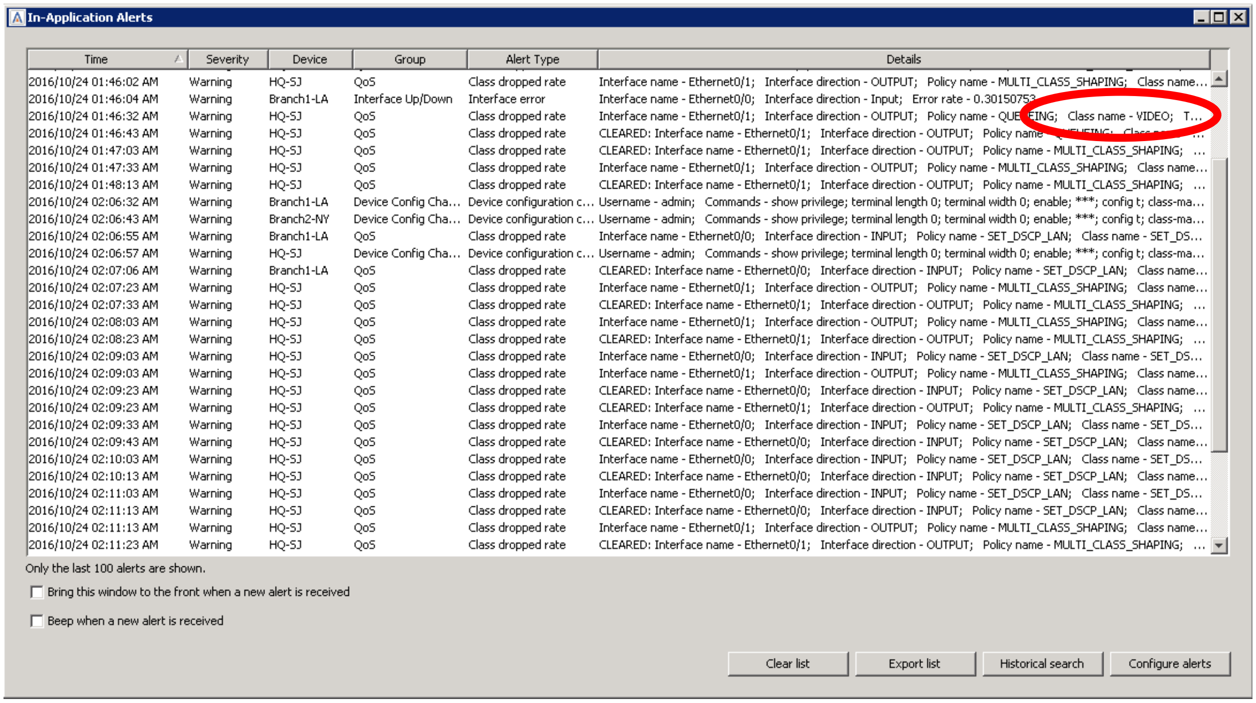
- **Queue-limit** – Buffer size that stores queue data during congestion
- **Priority queue BC** – Token bucket interval that schedules the releases data in priority

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

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

1. The first place to look for the issue is to review the in-application alerts.
   a. At the bottom left of the LiveNX window, note the Red Alert button.
   

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



In-Application Alerts

| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/24 01:46:02 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:46:04 AM | Warning | Branch1-LA | Interface Up/Down | Interface error | Interface name - Ethernet0/0; Interface direction - Input; Error rate - 0.30150753 |
| 2016/10/24 01:46:32 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VIDEO; T… |
| 2016/10/24 01:46:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class na… … |
| 2016/10/24 01:47:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 01:47:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:48:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:06:32 AM | Warning | Branch1-LA | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:43 AM | Warning | Branch2-NY | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:55 AM | Warning | Branch1-LA | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:06:57 AM | Warning | HQ-SJ | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:07:06 AM | Warning | Branch1-LA | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:07:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:07:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:08:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:08:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:10:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:10:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:11:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |

Only the last 100 alerts are shown.

☐ Bring this window to the front when a new alert is received

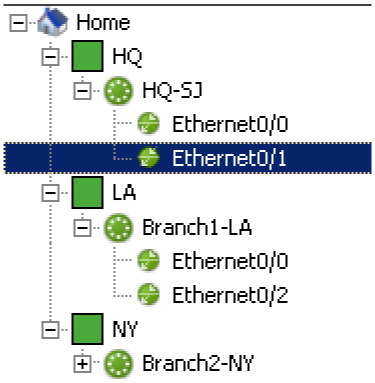
☐ Beep when a new alert is received

d. Are there any alerts class drop alerts from the VIDEO class?

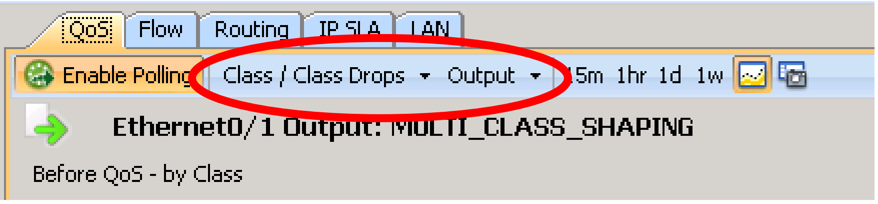
e. If not, we will want wait or do a Historic Search for class-dropped rate (see Appendix A.)

f. If there are any alerts for VIDEO, note the device and interface where the drop occurred. In this example, the device is HQ-SJ and the interface is GigabitEthernet1.

g. Select this interface from the device list.



h. From the real-time interface view, if necessary, update the view to:

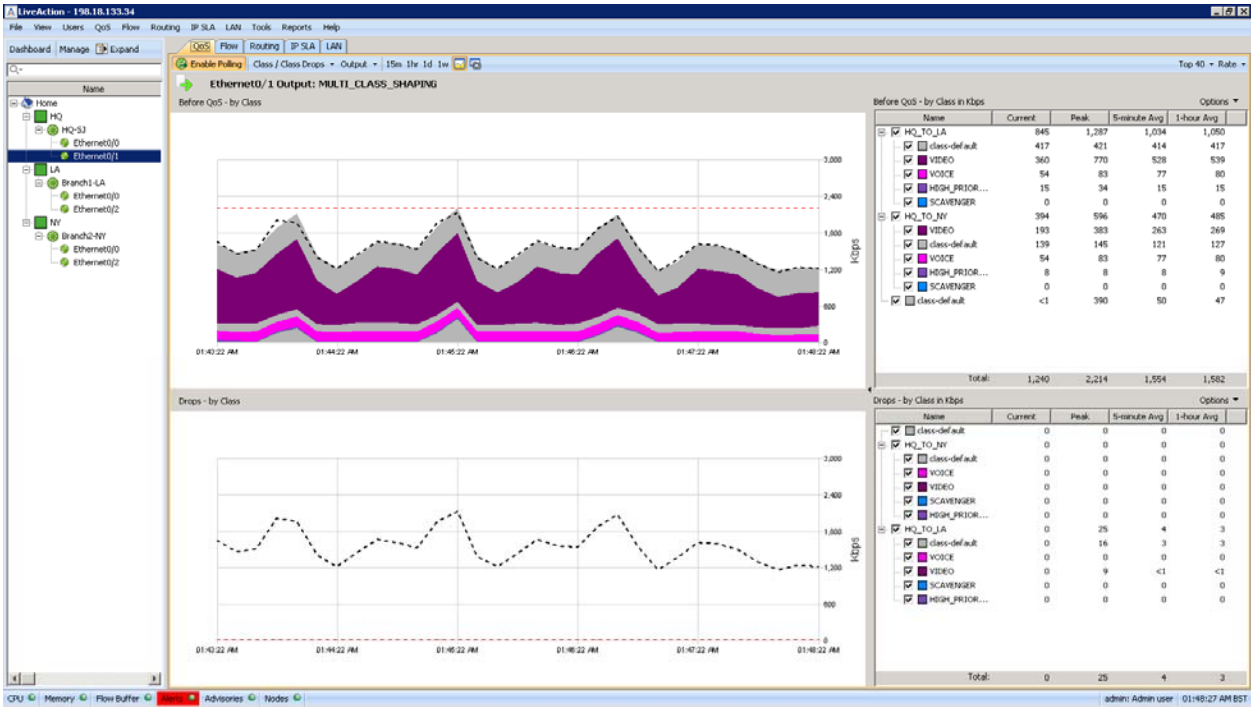


Class / Class Drops ▾ Output ▾

Ethernet0/1 Output: MULTI_CLASS_SHAPING

Before QoS - by Class

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



Ethernet0/1 Output: MULTI_CLASS_SHAPING

Before QoS - by Class in Kbps

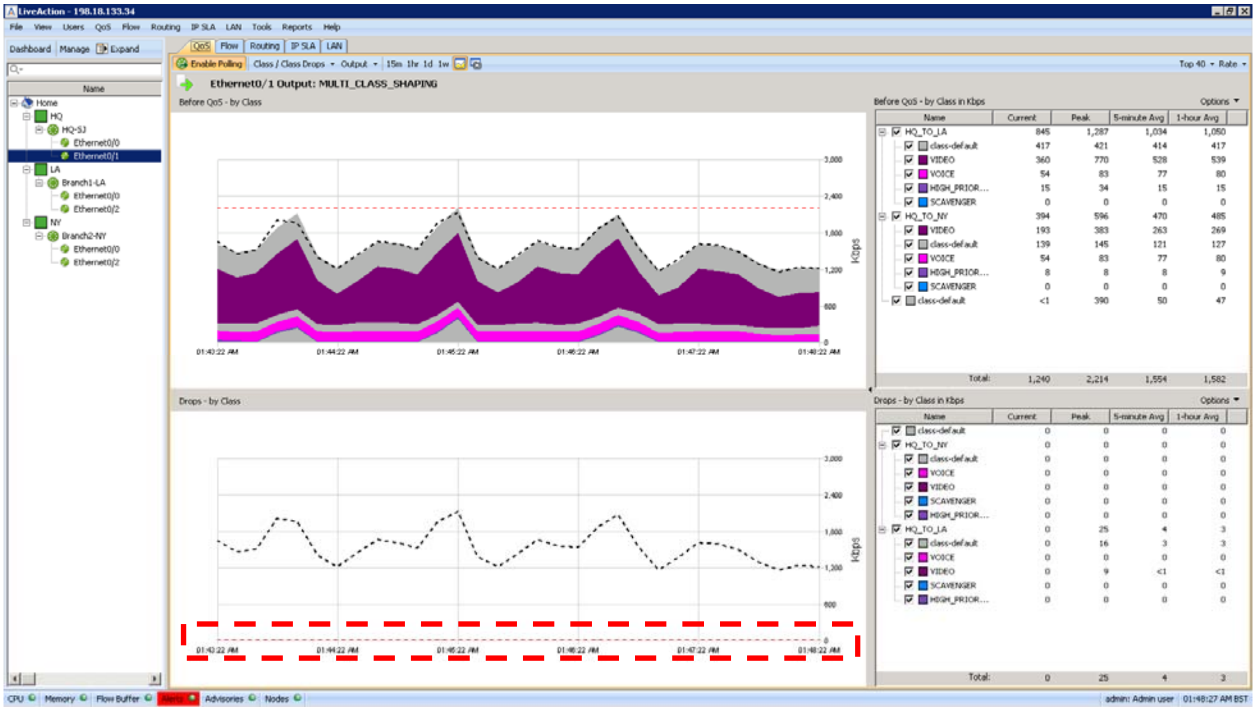
| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| ☑ HQ_TO_LA | 845 | 1,287 | 1,034 | 1,050 |
| ☑ class-default | 417 | 421 | 414 | 417 |
| ☑ VIDEO | 360 | 770 | 528 | 539 |
| ☑ VOICE | 54 | 83 | 77 | 80 |
| ☑ HIGH_PRIOR... | 15 | 34 | 15 | 15 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_NY | 394 | 596 | 470 | 485 |
| ☑ VIDEO | 193 | 383 | 263 | 269 |
| ☑ class-default | 139 | 145 | 121 | 127 |
| ☑ VOICE | 54 | 83 | 77 | 80 |
| ☑ HIGH_PRIOR... | 8 | 8 | 8 | 9 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ class-default | <1 | 390 | 50 | 47 |
| Total: | 1,240 | 2,214 | 1,554 | 1,582 |

Drops - by Class in Kbps

| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| ☑ class-default | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_NY | 0 | 0 | 0 | 0 |
| ☑ class-default | 0 | 0 | 0 | 0 |
| ☑ VOICE | 0 | 0 | 0 | 0 |
| ☑ VIDEO | 0 | 0 | 0 | 0 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HIGH_PRIOR... | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_LA | 0 | 25 | 4 | 3 |
| ☑ class-default | 0 | 16 | 3 | 3 |
| ☑ VOICE | 0 | 0 | 0 | 0 |
| ☑ VIDEO | 0 | 9 | <1 | <1 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HIGH_PRIOR... | 0 | 0 | 0 | 0 |
| Total: | 0 | 25 | 4 | 3 |

j. There have been minimal drops in the Video Class.

k. Click and drag your mouse on the bottom graph to make an outline of a box. When you let go the map should zoom in.



Ethernet0/1 Output: MULTI_CLASS_SHAPING

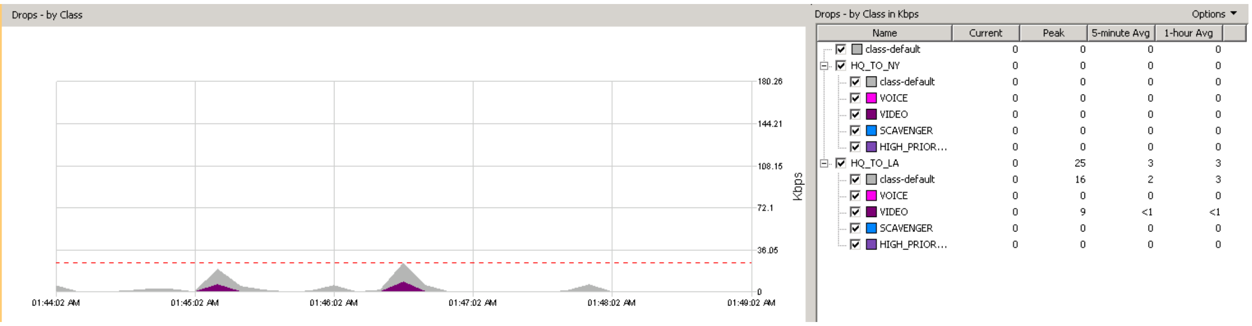
Before QoS - by Class in Kbps

| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| ☑ HQ_TO_LA | 845 | 1,287 | 1,034 | 1,050 |
| ☑ class-default | 417 | 421 | 414 | 417 |
| ☑ VIDEO | 360 | 770 | 528 | 539 |
| ☑ VOICE | 54 | 83 | 77 | 80 |
| ☑ HIGH_PRIOR... | 15 | 34 | 15 | 15 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_NY | 394 | 596 | 470 | 485 |
| ☑ VIDEO | 193 | 383 | 263 | 269 |
| ☑ class-default | 139 | 145 | 121 | 127 |
| ☑ VOICE | 54 | 83 | 77 | 80 |
| ☑ HIGH_PRIOR... | 8 | 8 | 8 | 9 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ class-default | <1 | 390 | 50 | 47 |
| Total: | 1,240 | 2,214 | 1,554 | 1,582 |

Drops - by Class in Kbps

| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| ☑ class-default | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_NY | 0 | 0 | 0 | 0 |
| ☑ class-default | 0 | 0 | 0 | 0 |
| ☑ VOICE | 0 | 0 | 0 | 0 |
| ☑ VIDEO | 0 | 0 | 0 | 0 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HIGH_PRIOR... | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_LA | 0 | 25 | 4 | 3 |
| ☑ class-default | 0 | 16 | 3 | 3 |
| ☑ VOICE | 0 | 0 | 0 | 0 |
| ☑ VIDEO | 0 | 9 | <1 | <1 |
| ☑ SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ HIGH_PRIOR... | 0 | 0 | 0 | 0 |
| Total: | 0 | 25 | 4 | 3 |

l. The zoomed-in graph shows the minimal drops happening in the VIDEO (purple) class and the class-default (grey). In this example there have been 9 drops at peak in the VIDEO class.



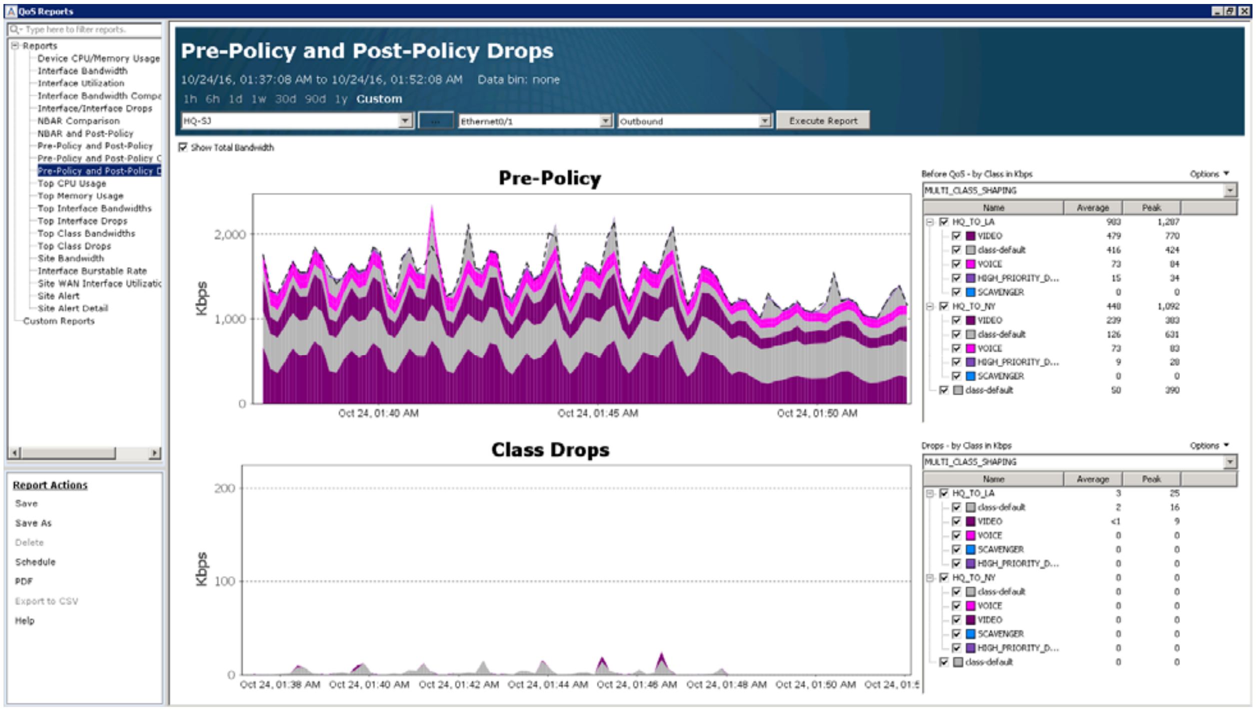
Drops - by Class in Kbps

| Name | Current | Peak | 5-minute Avg | 1-hour Avg |
|---|---|---|---|---|
| ☑ ▨ class-default | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_NY | 0 | 0 | 0 | 0 |
| ☑ ▨ class-default | 0 | 0 | 0 | 0 |
| ☑ 🟪 VOICE | 0 | 0 | 0 | 0 |
| ☑ 🟪 VIDEO | 0 | 0 | 0 | 0 |
| ☑ 🟦 SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ 🟪 HIGH_PRIOR... | 0 | 0 | 0 | 0 |
| ☑ HQ_TO_LA | 0 | 25 | 3 | 3 |
| ☑ ▨ class-default | 0 | 16 | 2 | 3 |
| ☑ 🟪 VOICE | 0 | 0 | 0 | 0 |
| ☑ 🟪 VIDEO | 0 | 9 | <1 | <1 |
| ☑ 🟦 SCAVENGER | 0 | 0 | 0 | 0 |
| ☑ 🟪 HIGH_PRIOR... | 0 | 0 | 0 | 0 |

m. To investigate the same type of drops from a historical report select the 15m icon.

n. The Pre-Policy and Post-Policy Drops report will open.

o. Click and drag your mouse on the bottom graph to make an outline of a box. When you let go the map should zoom in. Note that there are minimal VIDEO (purple) drops in this example too.



**Pre-Policy and Post-Policy Drops**

10/24/16, 01:37:08 AM to 10/24/16, 01:52:08 AM   Data bin: none

HQ-SJ   Ethernet0/1   Outbound

☑ Show Total Bandwidth

Before QoS - by Class in Kbps

MULTI_CLASS_SHAPING

| Name | Average | Peak |
|---|---|---|
| ☑ HQ_TO_LA | 903 | 1,207 |
| ☑ 🟪 VIDEO | 479 | 770 |
| ☑ ▨ class-default | 416 | 424 |
| ☑ 🟪 VOICE | 73 | 84 |
| ☑ 🟪 HIGH_PRIORITY_D... | 15 | 34 |
| ☑ 🟦 SCAVENGER | 0 | 0 |
| ☑ HQ_TO_NY | 448 | 1,092 |
| ☑ 🟪 VIDEO | 239 | 383 |
| ☑ ▨ class-default | 126 | 631 |
| ☑ 🟪 VOICE | 73 | 83 |
| ☑ 🟪 HIGH_PRIORITY_D... | 9 | 28 |
| ☑ 🟦 SCAVENGER | 0 | 0 |
| ☑ ▨ class-default | 50 | 390 |

Drops - by Class in Kbps

MULTI_CLASS_SHAPING

| Name | Average | Peak |
|---|---|---|
| ☑ HQ_TO_LA | 3 | 25 |
| ☑ ▨ class-default | 2 | 16 |
| ☑ 🟪 VIDEO | <1 | 9 |
| ☑ 🟪 VOICE | 0 | 0 |
| ☑ 🟦 SCAVENGER | 0 | 0 |
| ☑ 🟪 HIGH_PRIORITY_D... | 0 | 0 |
| ☑ HQ_TO_NY | 0 | 0 |
| ☑ ▨ class-default | 0 | 0 |
| ☑ 🟪 VOICE | 0 | 0 |
| ☑ 🟪 VIDEO | 0 | 0 |
| ☑ 🟦 SCAVENGER | 0 | 0 |
| ☑ 🟪 HIGH_PRIORITY_D... | 0 | 0 |
| ☑ ▨ class-default | 0 | 0 |

p. Remember we configured the VIDEO queue for each site to 800Kbps each.

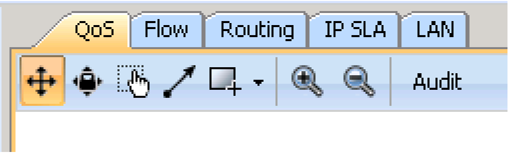
q. The Pre-Policy graph above shows 776 Kbps peak VIDEO traffic on the HQ_TO_LA child policy and 389 Kbps to the HQ_TO_NY child policy.

r. Neither of these are above the provisioned 800K. We need to implement some buffer tuning.

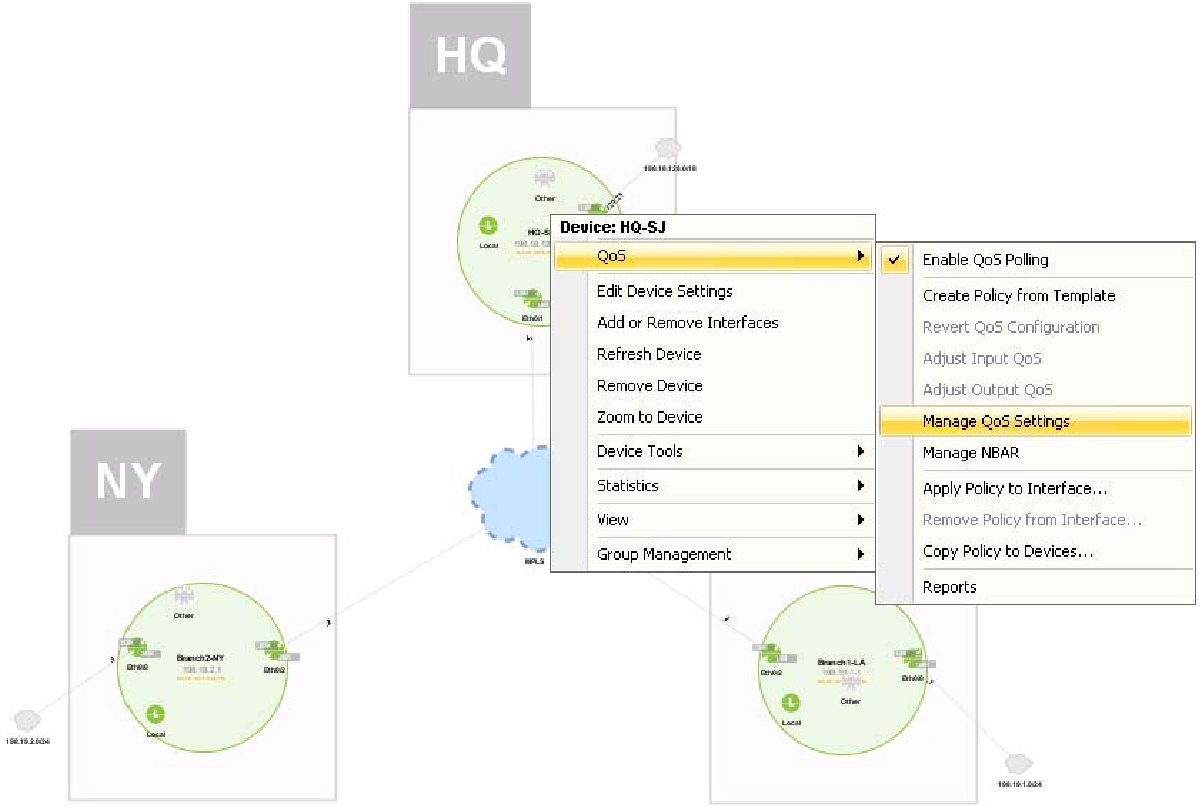
# Lab 6.1: Implementing Tuning

Lab Steps:

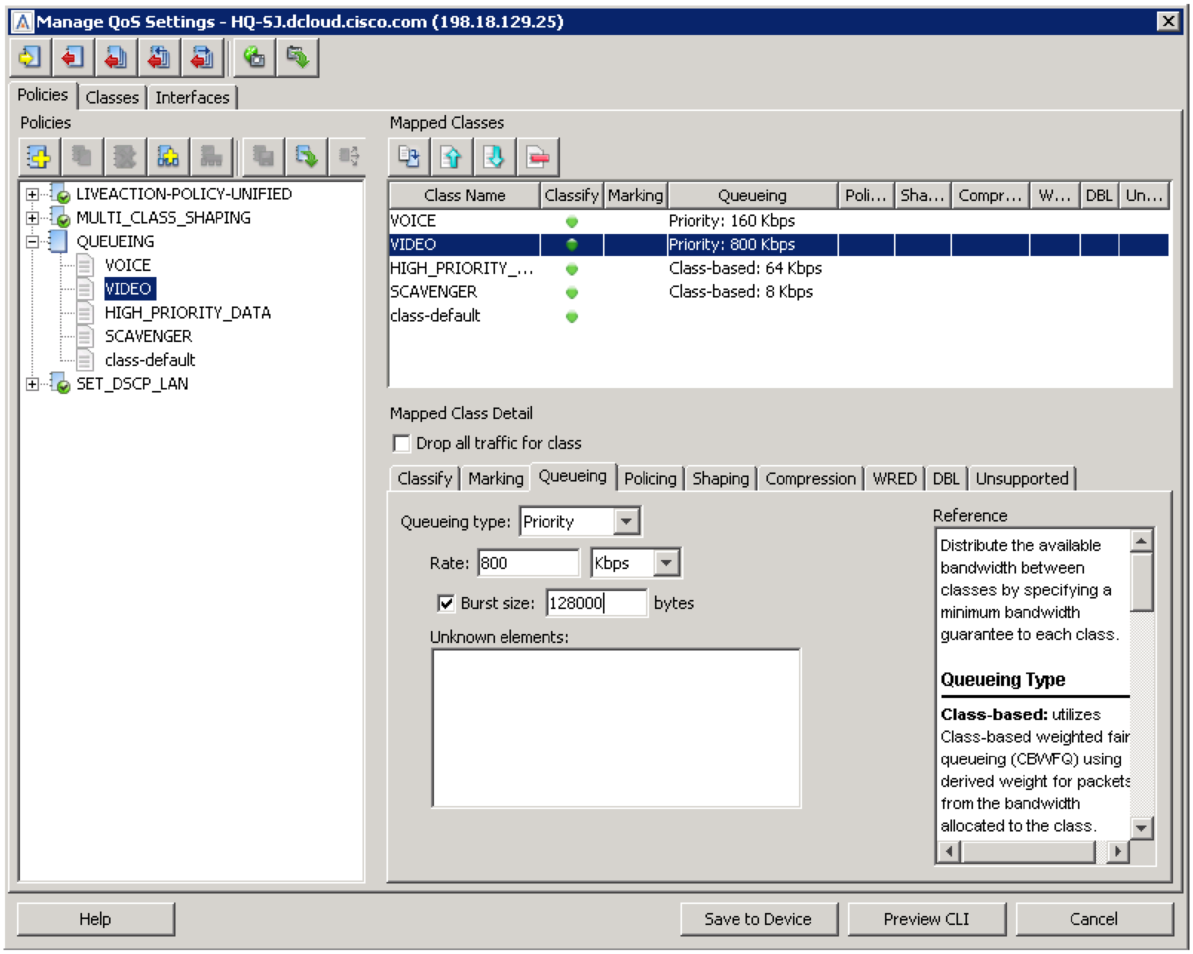
1. Select the QoS Tab



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



3. Expand the QUEUEING Policy
4. Select the VIDEO class.
5. Select the Queueing tab
6. Tick the Burst option and set it to 128000.



Manage QoS Settings - HQ-SJ.dcloud.cisco.com (198.18.129.25)

- LIVEACTION-POLICY-UNIFIED
- MULTI_CLASS_SHAPING
- QUEUEING
  - VOICE
  - VIDEO
  - HIGH_PRIORITY_DATA
  - SCAVENGER
  - class-default
- SET_DSCP_LAN

| Class Name | Classify | Marking | Queueing | Poli… | Sha… | Compr… | W… | DBL | Un… |
|---|---|---|---|---|---|---|---|---|---|
| VOICE | ● | | Priority: 160 Kbps | | | | | | |
| VIDEO | ● | | Priority: 800 Kbps | | | | | | |
| HIGH_PRIORITY_… | ● | | Class-based: 64 Kbps | | | | | | |
| SCAVENGER | ● | | Class-based: 8 Kbps | | | | | | |
| class-default | ● | | | | | | | | |

Mapped Class Detail

☐ Drop all traffic for class

Queueing type: Priority

Rate: 800 Kbps

☑ Burst size: 128000 bytes

Unknown elements:

Reference

Distribute the available bandwidth between classes by specifying a minimum bandwidth guarantee to each class.

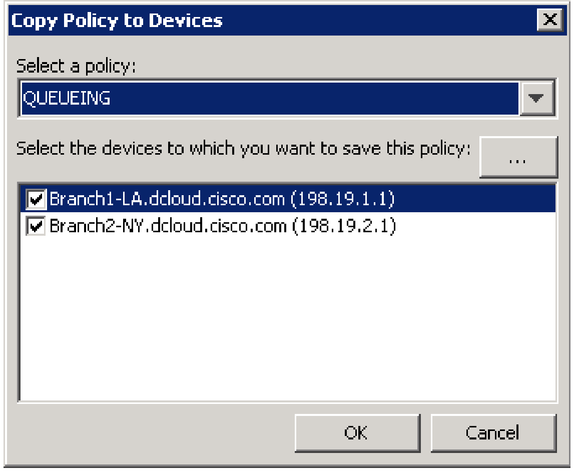
**Queueing Type**

**Class-based:** utilizes Class-based weighted fair queueing (CBWFQ) using derived weight for packets from the bandwidth allocated to the class.

To understand this value, please see the **TelePresence Network Systems 2.0 Design Guide** from www.cisco.com.

7. Select the Save to Device button.

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



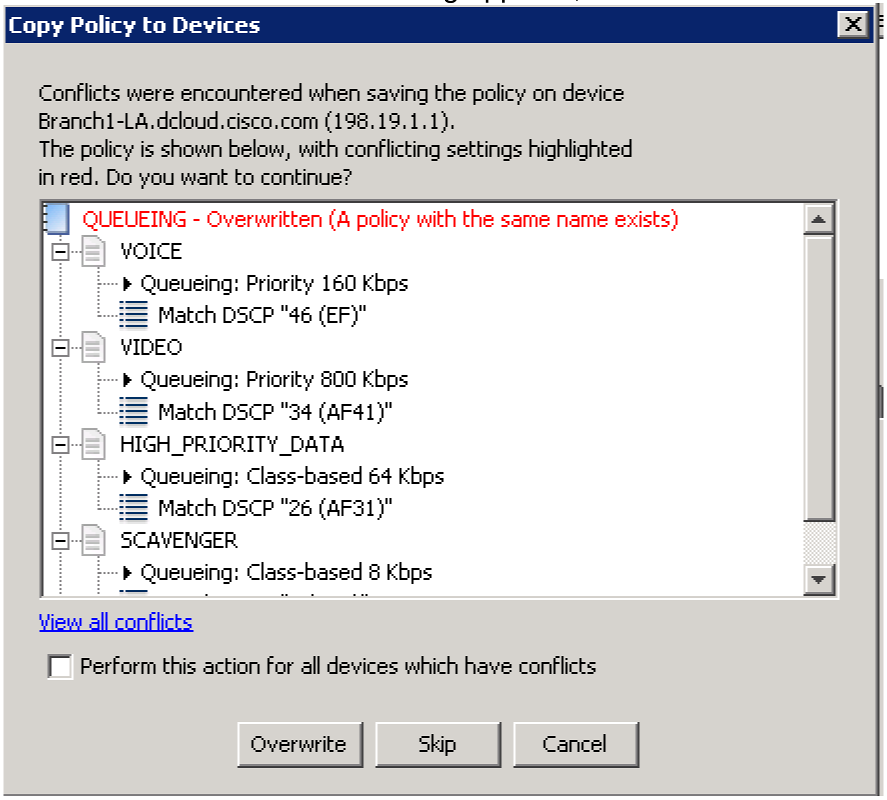
Copy Policy to Devices

Select a policy: QUEUEING

Select the devices to which you want to save this policy:

☑ Branch1-LA.dcloud.cisco.com (198.19.1.1)
☑ Branch2-NY.dcloud.cisco.com (198.19.2.1)

9. When the conflict warning appears, select overwrite.

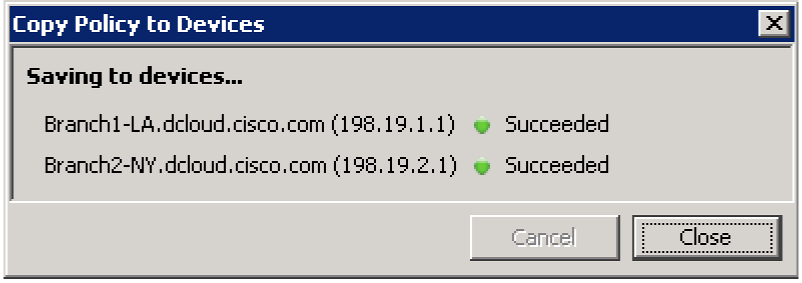


Copy Policy to Devices

Conflicts were encountered when saving the policy on device Branch1-LA.dcloud.cisco.com (198.19.1.1).
The policy is shown below, with conflicting settings highlighted in red. Do you want to continue?

```
QUEUEING - Overwritten (A policy with the same name exists)
  VOICE
    Queueing: Priority 160 Kbps
    Match DSCP "46 (EF)"
  VIDEO
    Queueing: Priority 800 Kbps
    Match DSCP "34 (AF41)"
  HIGH_PRIORITY_DATA
    Queueing: Class-based 64 Kbps
    Match DSCP "26 (AF31)"
  SCAVENGER
    Queueing: Class-based 8 Kbps
```

10. Validate the changes saved successfully.



Copy Policy to Devices

**Saving to devices...**

| | | |
|---|---|---|
| Branch1-LA.dcloud.cisco.com (198.19.1.1) | ● | Succeeded |
| Branch2-NY.dcloud.cisco.com (198.19.2.1) | ● | Succeeded |

11. Close the Manage QoS Settings Dialog window.

# Lab 7

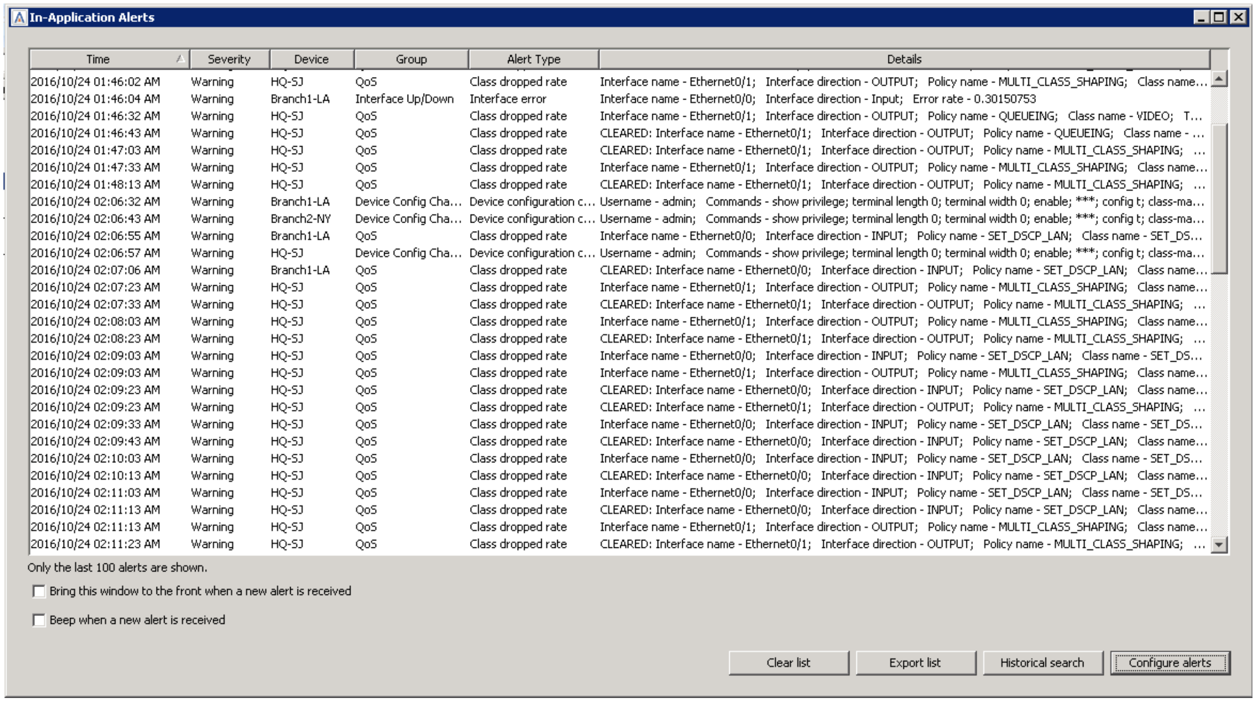
## Lab 7:  QoS Alerts

# Lab 7.1: Configure QoS Alerts

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

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

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



| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/24 01:46:02 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:46:04 AM | Warning | Branch1-LA | Interface Up/Down | Interface error | Interface name - Ethernet0/0; Interface direction - Input; Error rate - 0.30150753 |
| 2016/10/24 01:46:32 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VIDEO; T… |
| 2016/10/24 01:46:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - … |
| 2016/10/24 01:47:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 01:47:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:48:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:06:32 AM | Warning | Branch1-LA | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:43 AM | Warning | Branch2-NY | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:55 AM | Warning | Branch1-LA | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:06:57 AM | Warning | HQ-SJ | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:07:06 AM | Warning | Branch1-LA | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:07:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:07:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:08:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:08:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:10:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:10:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:11:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |

Only the last 100 alerts are shown.

☐ Bring this window to the front when a new alert is received

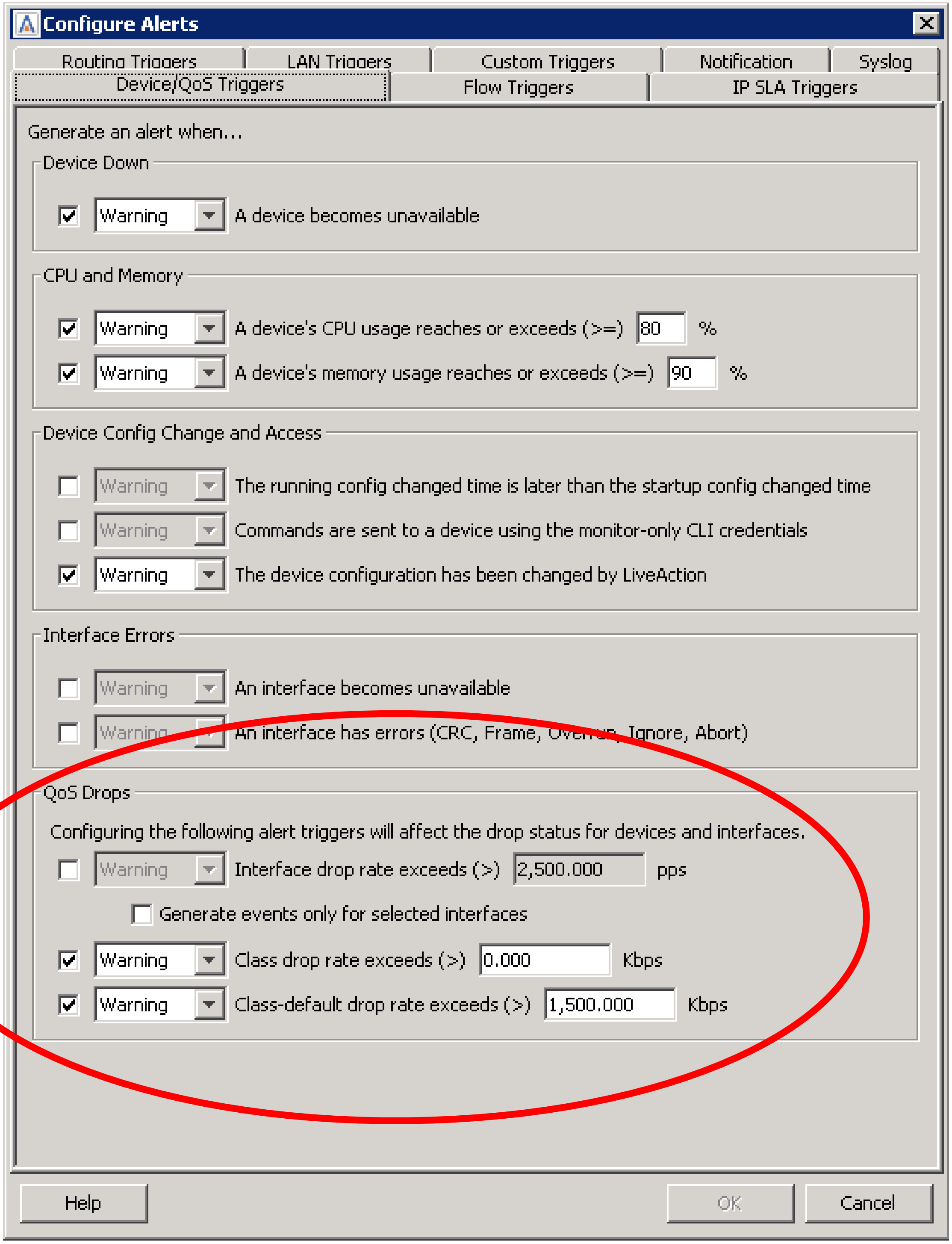
☐ Beep when a new alert is received

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

Lab Steps:

1. Tools > Configure Alerts

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



Generate an alert when...

Device Down

☑ Warning A device becomes unavailable

CPU and Memory

☑ Warning A device's CPU usage reaches or exceeds (>=) 80 %

☑ Warning A device's memory usage reaches or exceeds (>=) 90 %

Device Config Change and Access

☐ Warning The running config changed time is later than the startup config changed time

☐ Warning Commands are sent to a device using the monitor-only CLI credentials

☑ Warning The device configuration has been changed by LiveAction

Interface Errors

☐ Warning An interface becomes unavailable

☐ Warning An interface has errors (CRC, Frame, Overrun, Ignore, Abort)

QoS Drops

Configuring the following alert triggers will affect the drop status for devices and interfaces.

☐ Warning Interface drop rate exceeds (>) 2,500,000 pps

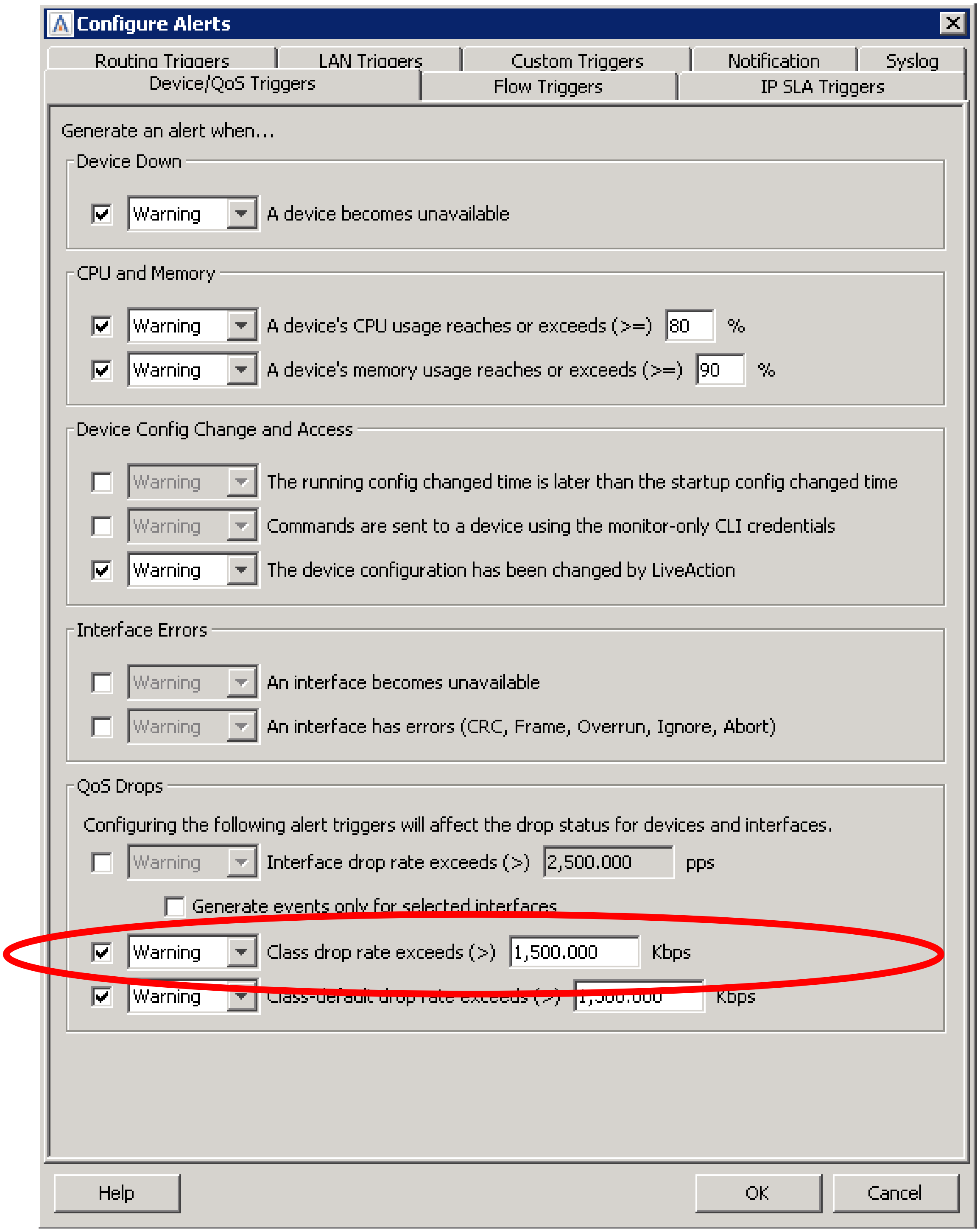
☐ Generate events only for selected interfaces

☑ Warning Class drop rate exceeds (>) 0.000 Kbps

☑ Warning Class-default drop rate exceeds (>) 1,500.000 Kbps

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

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



Generate an alert when...

Device Down

☑ Warning A device becomes unavailable

CPU and Memory

☑ Warning A device's CPU usage reaches or exceeds (>=) 80 %

☑ Warning A device's memory usage reaches or exceeds (>=) 90 %

Device Config Change and Access

□ Warning The running config changed time is later than the startup config changed time

□ Warning Commands are sent to a device using the monitor-only CLI credentials

☑ Warning The device configuration has been changed by LiveAction

Interface Errors

□ Warning An interface becomes unavailable

□ Warning An interface has errors (CRC, Frame, Overrun, Ignore, Abort)

QoS Drops

Configuring the following alert triggers will affect the drop status for devices and interfaces.

□ Warning Interface drop rate exceeds (>) 2,500.000 pps

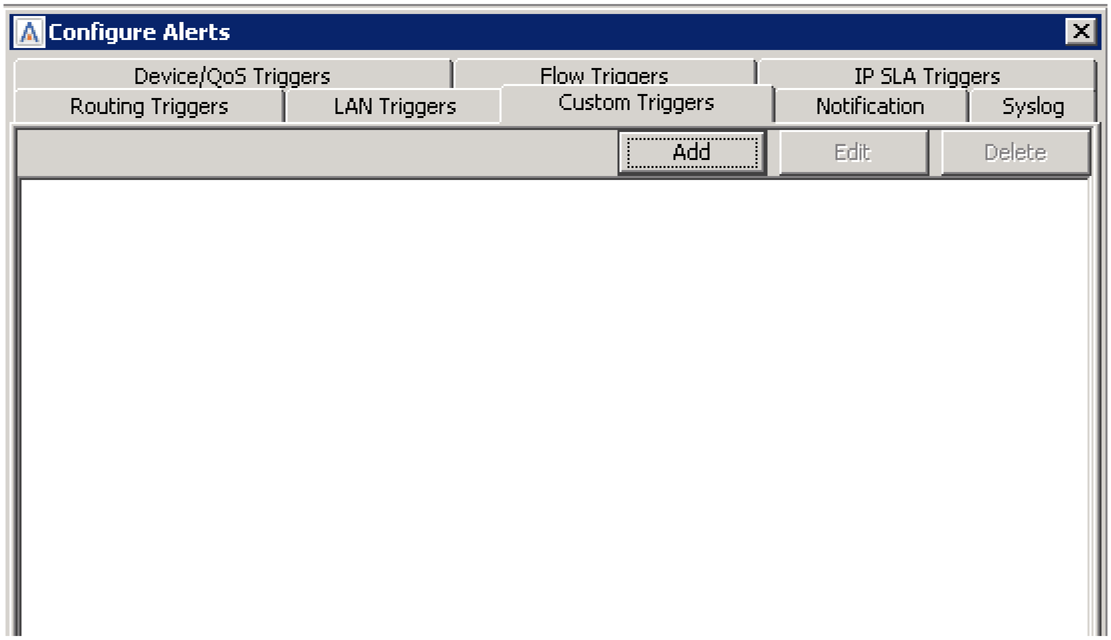
□ Generate events only for selected interfaces

☑ Warning Class drop rate exceeds (>) 1,500.000 Kbps

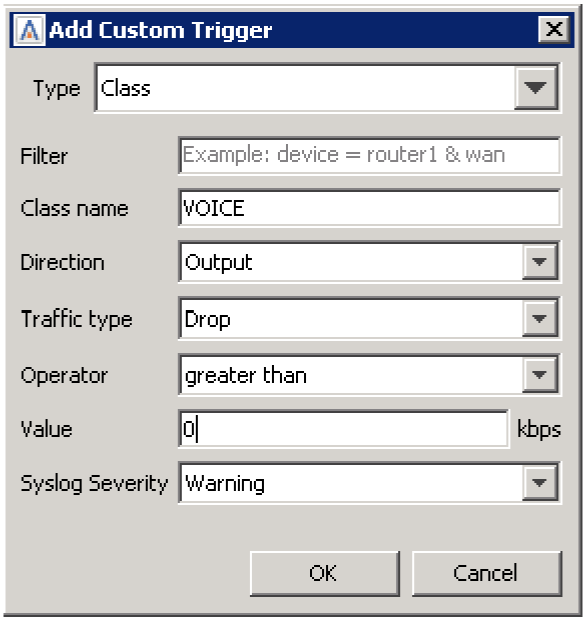
☑ Warning Class-default drop rate exceeds (>) 1,500.000 Kbps

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

2. Select the Custom Triggers tab.
3. Click Add.



4. Create a custom trigger type Class and set it with the following parameters:
   - Filter = *leave blank*
   - Class name = VOICE
   - Direction = Output
   - Traffic type = Drop
   - Operator = greater than
   - Value = 0



Type: Class

Filter: Example: device = router1 & wan

Class name: VOICE

Direction: Output

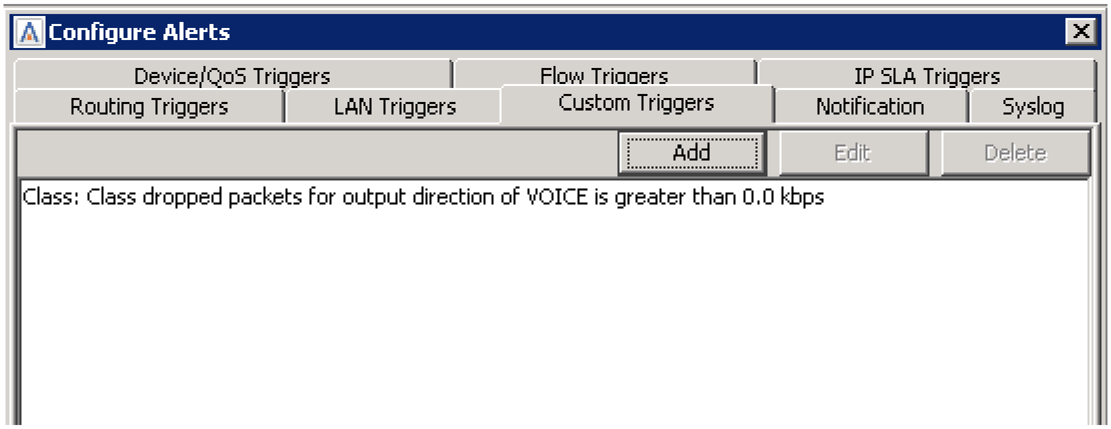
Traffic type: Drop

Operator: greater than

Value: 0 kbps

Syslog Severity: Warning

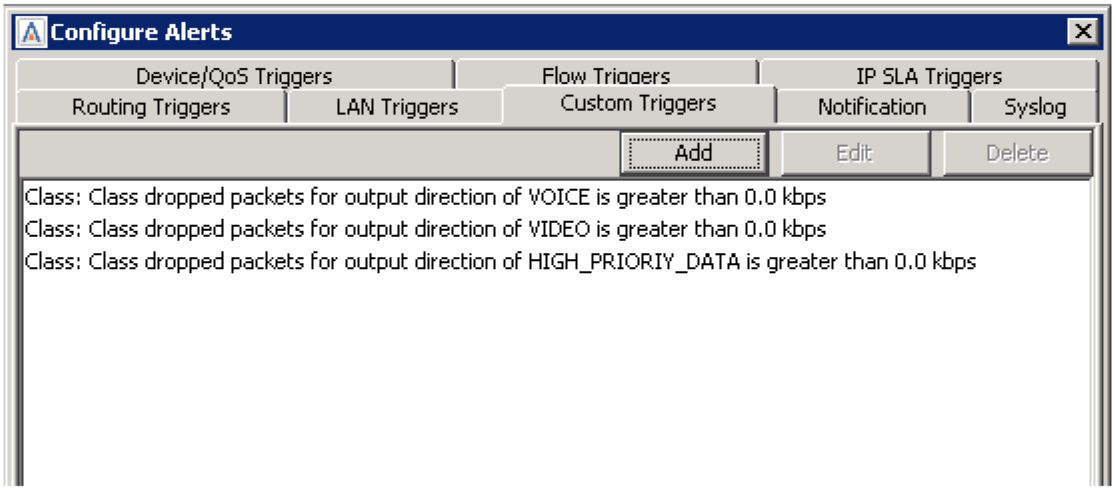
5. Click OK.



Class: Class dropped packets for output direction of VOICE is greater than 0.0 kbps

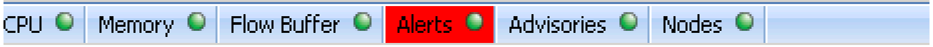
6. Repeat these steps and create a Custom trigger for the VIDEO and HIGH_PRIORITY_DATA classes.

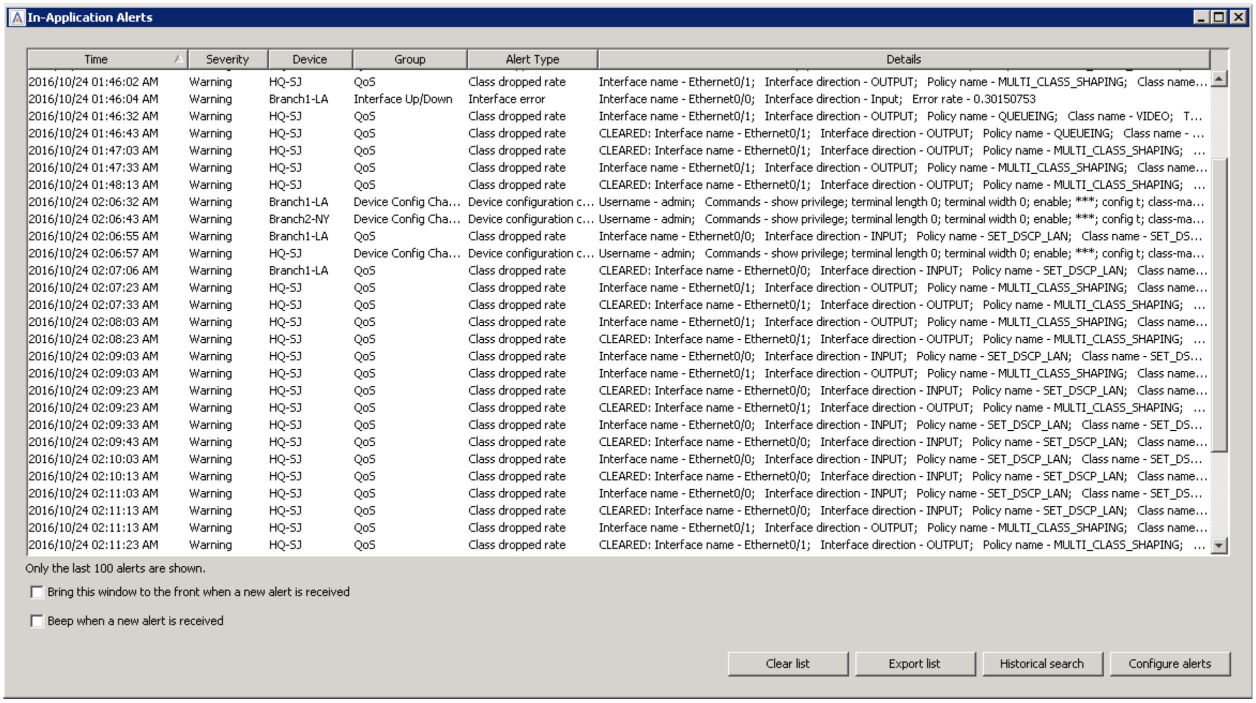
This will ensure these classes always alert when drops occur.



Class: Class dropped packets for output direction of VOICE is greater than 0.0 kbps
Class: Class dropped packets for output direction of VIDEO is greater than 0.0 kbps
Class: Class dropped packets for output direction of HIGH_PRIORIY_DATA is greater than 0.0 kbps

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





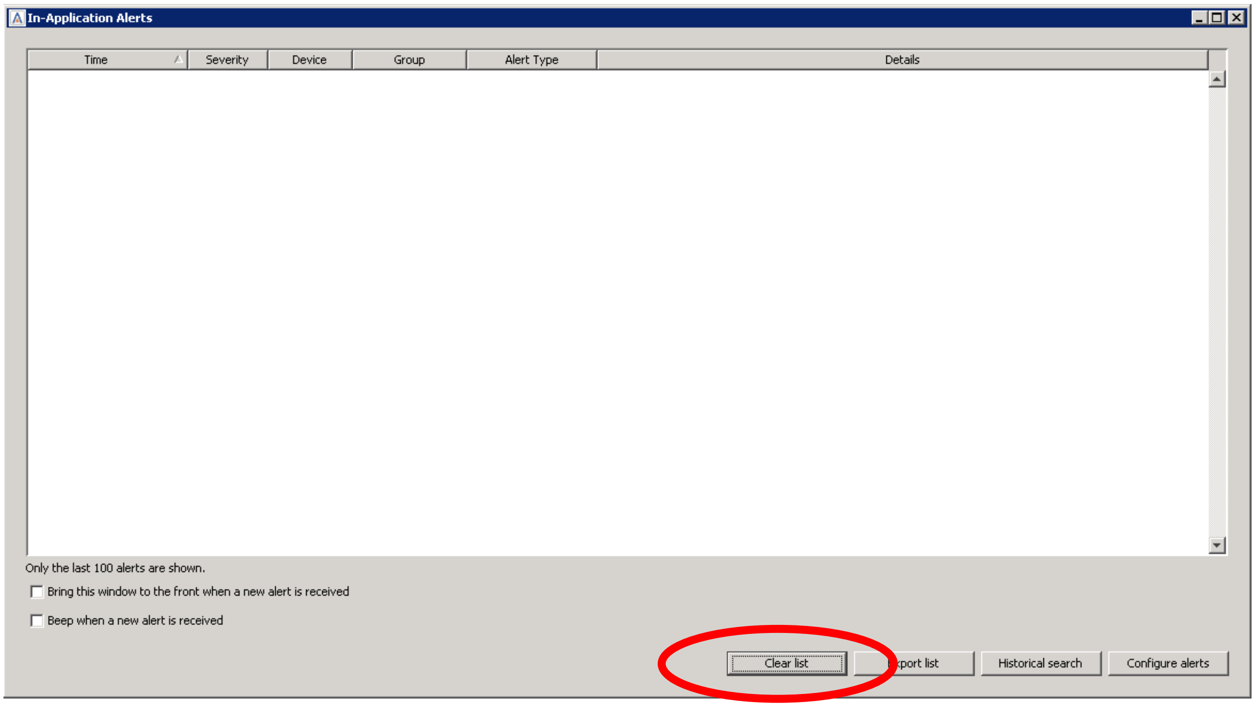
| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/24 01:46:02 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:46:04 AM | Warning | Branch1-LA | Interface Up/Down | Interface error | Interface name - Ethernet0/0; Interface direction - Input; Error rate - 0.30150753 |
| 2016/10/24 01:46:32 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - VIDEO; T… |
| 2016/10/24 01:46:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name - … |
| 2016/10/24 01:47:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 01:47:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 01:48:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:06:32 AM | Warning | Branch1-LA | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:43 AM | Warning | Branch2-NY | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:06:55 AM | Warning | Branch1-LA | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:06:57 AM | Warning | HQ-SJ | Device Config Cha… | Device configuration c… | Username - admin; Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma… |
| 2016/10/24 02:07:06 AM | Warning | Branch1-LA | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:07:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:07:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:08:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:08:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |
| 2016/10/24 02:09:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:09:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:10:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:10:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name - SET_DS… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0; Interface direction - INPUT; Policy name - SET_DSCP_LAN; Class name… |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; Class name… |
| 2016/10/24 02:11:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - MULTI_CLASS_SHAPING; … |

Only the last 100 alerts are shown.

☐ Bring this window to the front when a new alert is received

☐ Beep when a new alert is received

8. Click the Clear List Button



| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|

Only the last 100 alerts are shown.

☐ Bring this window to the front when a new alert is received

☐ Beep when a new alert is received

Monitor the system for any new QoS Alerts.

# Lab 8

## Lab 8:  Configure PfRv3 Monitoring

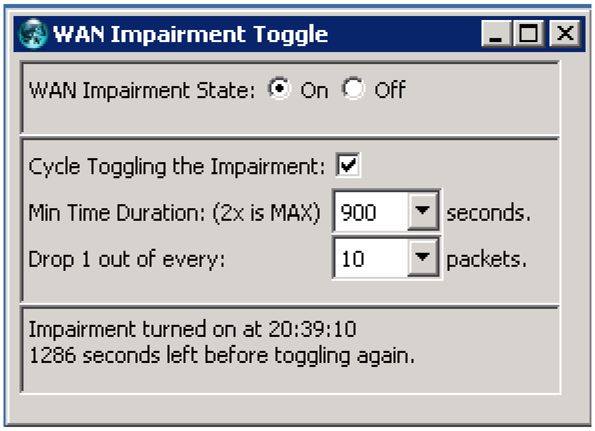
# Lab 8.1: Verify Traffic Generator

In this lab, we will configure LiveNX to monitor a PfRv3/ SD-WAN enabled network. The PfRv3 network is already completely configured and working, but LiveNX is freshly installed with no devices configured. We will configure LiveNX to monitor this PfRv3 environment.

Lab Steps:

1. Use an RDC to <ipaddress>:20201. (Administrator / C1sco12345)

**Note:** There is a WAN impairment tool application that should be running on the client PC. It will look like this. Note how it shows the number of seconds, before it wants to enable/disable impairment again.



WAN Impairment State: ● On ○ Off

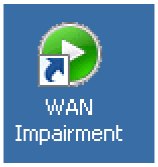
Cycle Toggling the Impairment: ☑

Min Time Duration: (2x is MAX) 900 seconds.

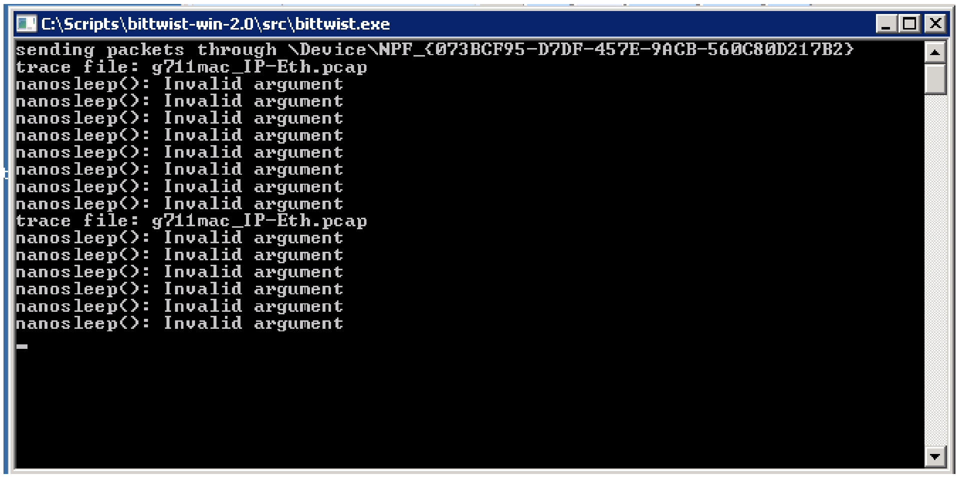
Drop 1 out of every: 10 packets.

Impairment turned on at 20:39:10
1286 seconds left before toggling again.

**Note:** If you do not see time incrementing, close the impairment tool and re-run it using this icon**.**



**Note:** You should also see an open CLI window. You may minimize, but leave this open.



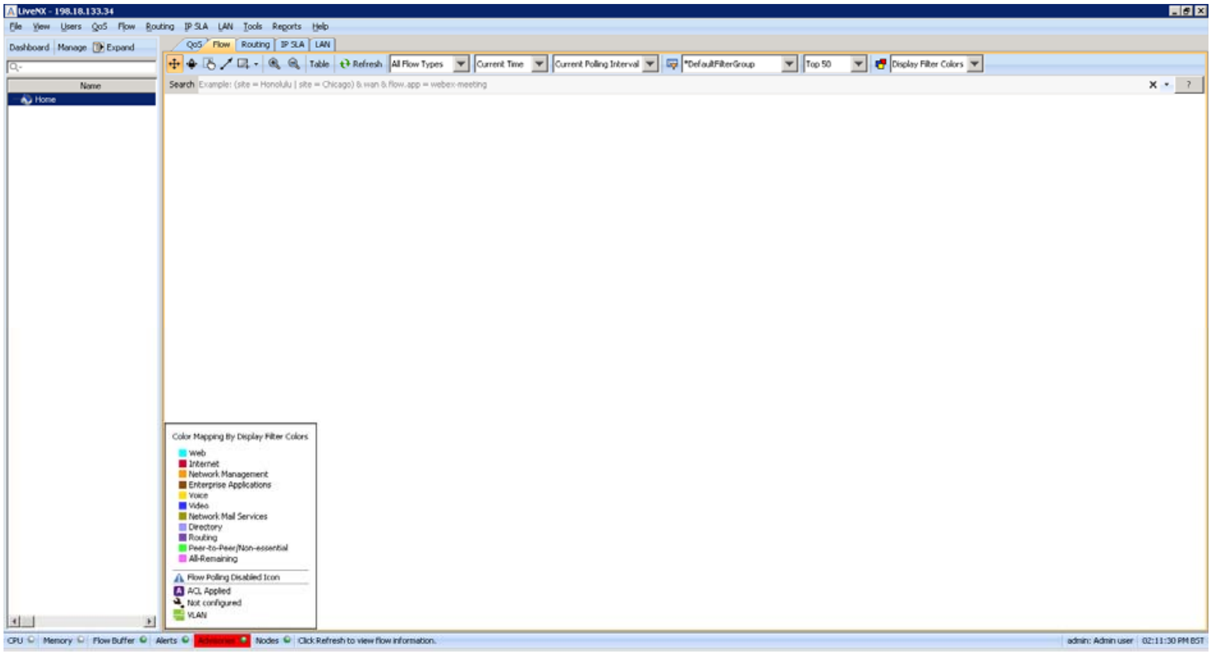
```
sending packets through \Device\NPF_{073BCF95-D7DF-457E-9ACB-560C80D217B2}
trace file: g711mac_IP-Eth.pcap
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
trace file: g711mac_IP-Eth.pcap
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
nanosleep(): Invalid argument
_
```

# Lab 8.2: Discover Devices

Our Training Pod for this sessions has not been configured. YOU need to add devices *& configure them for proper SDWAN operation. You are welcome to utilize the WebUI to perform the following steps.

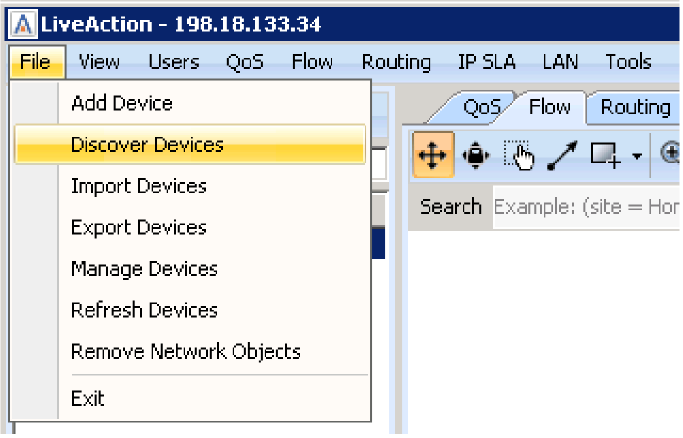
1. Log into the LiveNX Client:
   - Username = **admin**
   - Password = **Student**

You will notice that it is a fresh install.

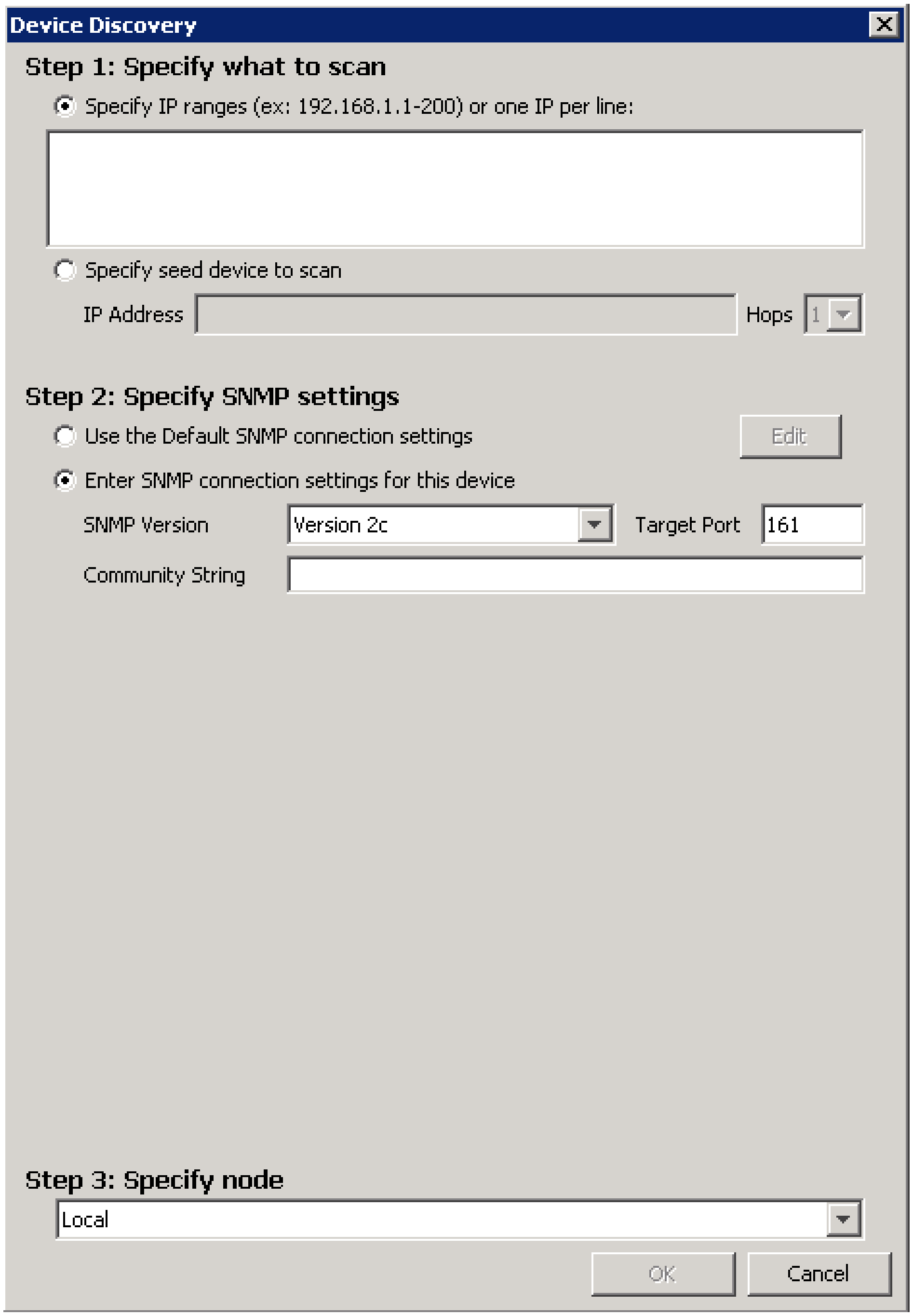

LiveNX - 198.18.133.34
File View Users QoS Flow Routing IP SLA LAN Tools Reports Help
Dashboard Manage Expand
QoS Flow Routing IP SLA LAN
Table Refresh All Flow Types Current Time Current Polling Interval *DefaultFilterGroup Top 50 Display Filter Colors
Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting
Name
Home
Color Mapping By Display Filter Colors
Web
Internet
Network Management
Enterprise Applications
Voice
Video
Network Mail Services
Directory
Routing
Peer-to-Peer/Non-essential
All-Remaining
Flow Polling Disabled Icon
ACL Applied
Not configured
VLAN
CPU Memory Flow Buffer Alerts Advisories Nodes Click Refresh to view flow information.
admin: Admin user 02:11:30 PM BST

Use Device Discovery to populate the Topology.

2. From the LiveNX client, select File > Discovery Devices.



**Note:** Your Instructor *may* give verbal instructions to use the Device Discovery via the WebUI… ask your Instructor why this may be beneficial. Most of the follow steps/entries will be similar.



Device Discovery

Step 1: Specify what to scan

● Specify IP ranges (ex: 192.168.1.1-200) or one IP per line:

○ Specify seed device to scan

IP Address | Hops 1

Step 2: Specify SNMP settings

○ Use the Default SNMP connection settings

● Enter SNMP connection settings for this device

SNMP Version: Version 2c | Target Port: 161

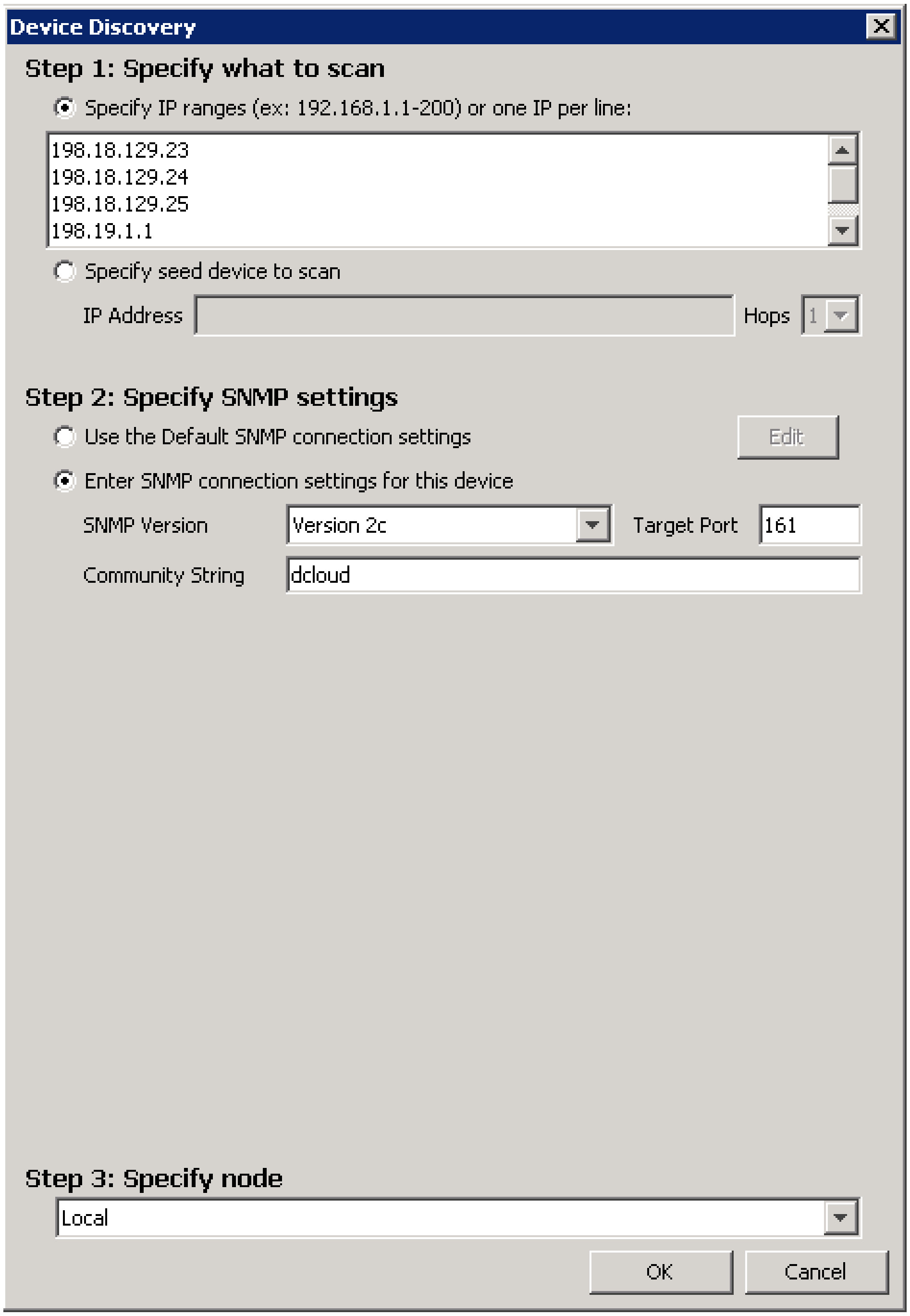
Community String:

Step 3: Specify node

Local

3. Step 1 - Specify IP ranges
   - 198.18.129.23-25
   - 198.19.1.1
   - 198.19.2.1

4. Step 2 – SNMP
   - Version = Version 2c
   - Communnity = dcloud
5. Step 3 - Select Local.
6. Click OK.



Device Discovery

Step 1: Specify what to scan

● Specify IP ranges (ex: 192.168.1.1-200) or one IP per line:

```
198.18.129.23
198.18.129.24
198.18.129.25
198.19.1.1
```

○ Specify seed device to scan

IP Address: Hops: 1

Step 2: Specify SNMP settings

○ Use the Default SNMP connection settings

● Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port: 161

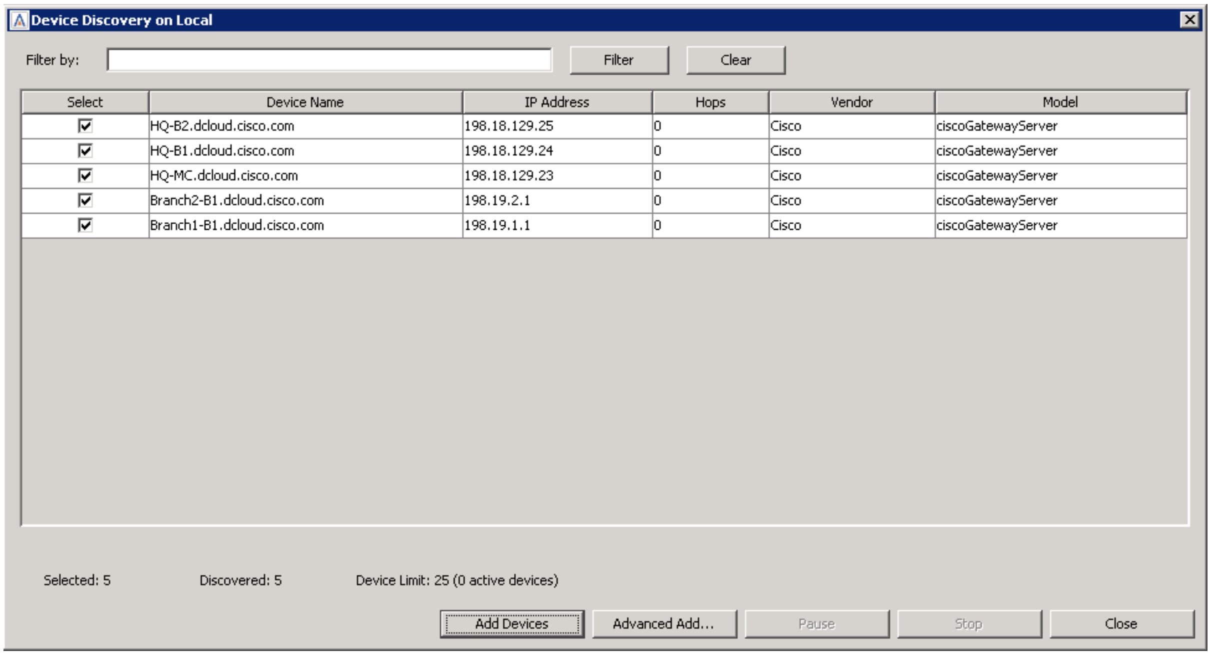
Community String: dcloud

Step 3: Specify node

Local

LiveNX will discover the devices via SNMP.

7. Select all devices and Add Devcies.



Device Discovery on Local

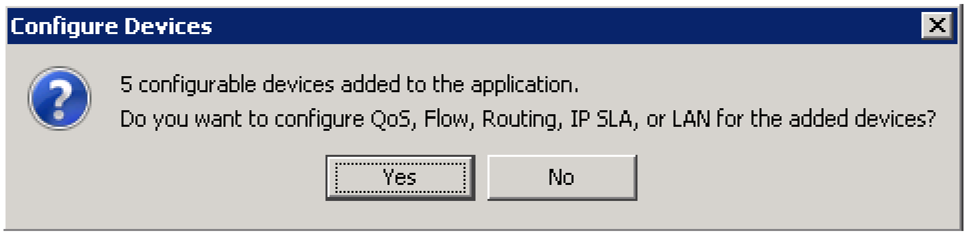
Filter by:

| Select | Device Name | IP Address | Hops | Vendor | Model |
|---|---|---|---|---|---|
| ☑ | HQ-B2.dcloud.cisco.com | 198.18.129.25 | 0 | Cisco | ciscoGatewayServer |
| ☑ | HQ-B1.dcloud.cisco.com | 198.18.129.24 | 0 | Cisco | ciscoGatewayServer |
| ☑ | HQ-MC.dcloud.cisco.com | 198.18.129.23 | 0 | Cisco | ciscoGatewayServer |
| ☑ | Branch2-B1.dcloud.cisco.com | 198.19.2.1 | 0 | Cisco | ciscoGatewayServer |
| ☑ | Branch1-B1.dcloud.cisco.com | 198.19.1.1 | 0 | Cisco | ciscoGatewayServer |

Selected: 5 Discovered: 5 Device Limit: 25 (0 active devices)

8. Select **No**.

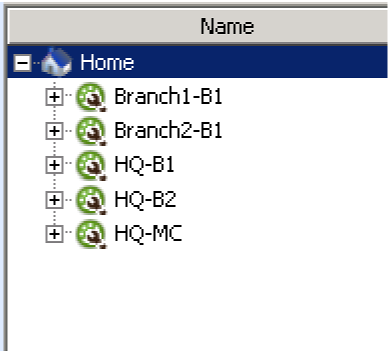
**Note: Since some of the devices discovered are Cisco devices, LiveNX offers the option to setup/enable various features as you add them to the Topology.**

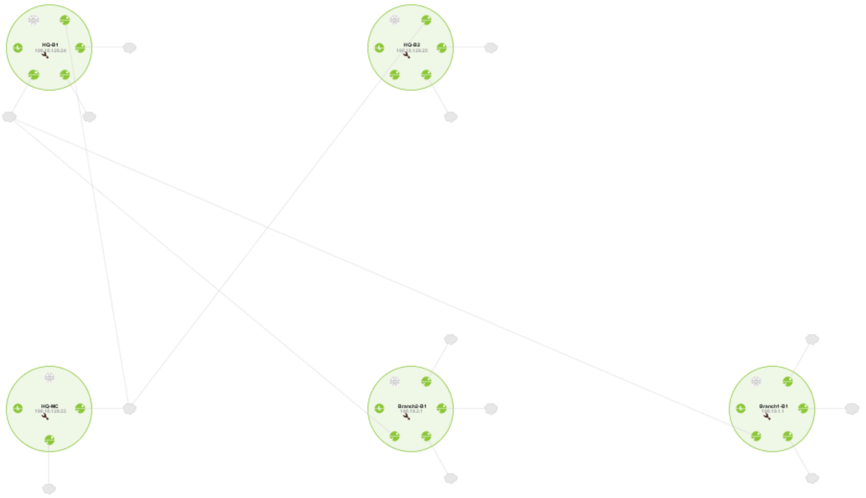


Configure Devices

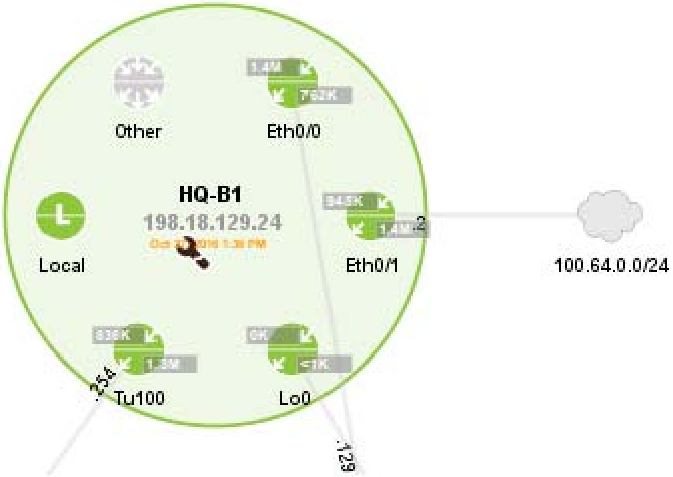
5 configurable devices added to the application.
Do you want to configure QoS, Flow, Routing, IP SLA, or LAN for the added devices?

The five discovered routers will appear in the LiveNX Home Tree View, and in the Topology Pane.





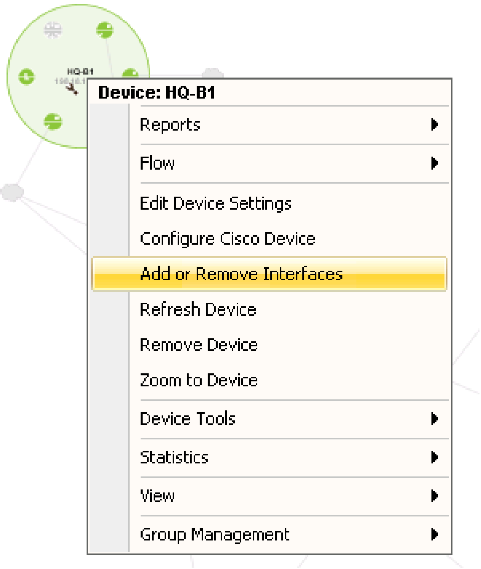
Notice there is a wrench icon on each device. This indicates that the devices are in “monitor only” mode.  Only SNMP and NetFlow statisitcs are available at this point. No flow or advanced collection is available.



# Lab 8.3: Configure Interfaces

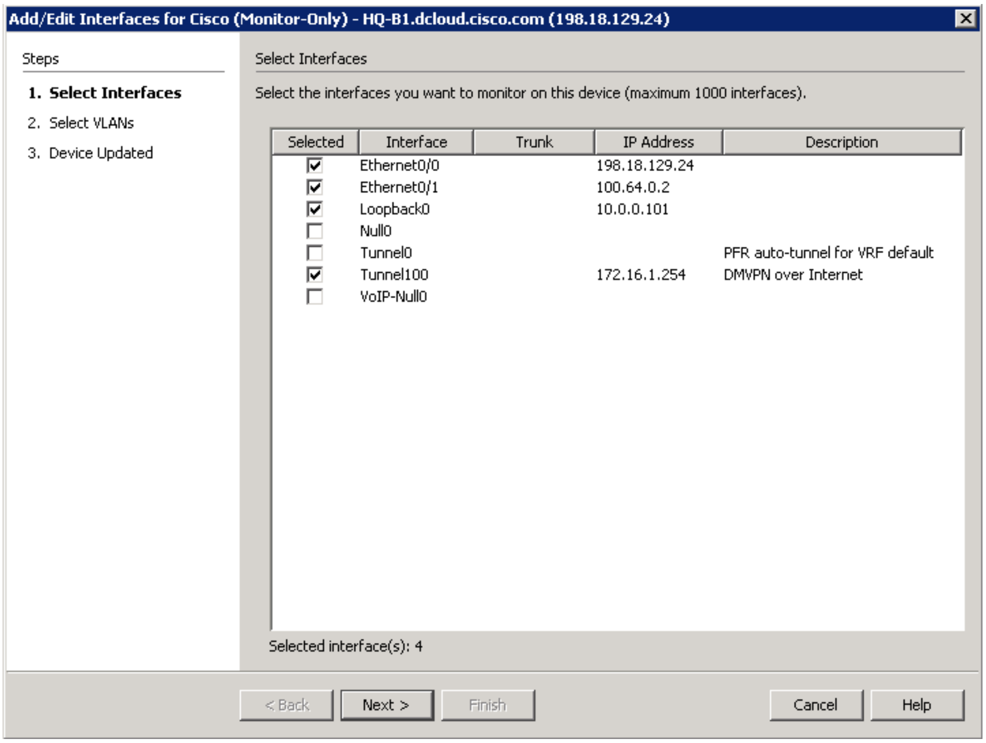
**Note: You *may* discover that some of the following configuration items have already been implemented… you should verify that all configurations match those described in the Labs.**

1. Righ-click on one of the routers and select Add or Remove Interfaces.



2. The Add/Edit Interfaces dialog will appear. Use the following table to select the interfaces of interest for each device.

| Device | Interface A | Interface B | Interface C | Interface D | Interface E | Interface F |
|---|---|---|---|---|---|---|
| Branch1-B1 | Loopback 0 | Tunnel100 | Tunnel101 | Eth0/0 | Eth0/1 | Eth0/2 |
| Branch2-B1 | Loopback 0 | Tunnel100 | Tunnel101 | Eth0/0 | Eth0/1 | Eth0/2 |
| HQ-B1 | Loopback 0 | Tunnel100 | | Eth0/0 | Eth0/1 | |
| HQ-B2 | Loopback 0 | | Tunnel101 | Eth0/0 | Eth0/1 | |
| HQ-MC | Loopback 0 | | | Eth0/0 | | |


Add/Edit Interfaces for Cisco (Monitor-Only) - HQ-B1.dcloud.cisco.com (198.18.129.24)

Steps

1. **Select Interfaces**
2. Select VLANs
3. Device Updated

Select Interfaces

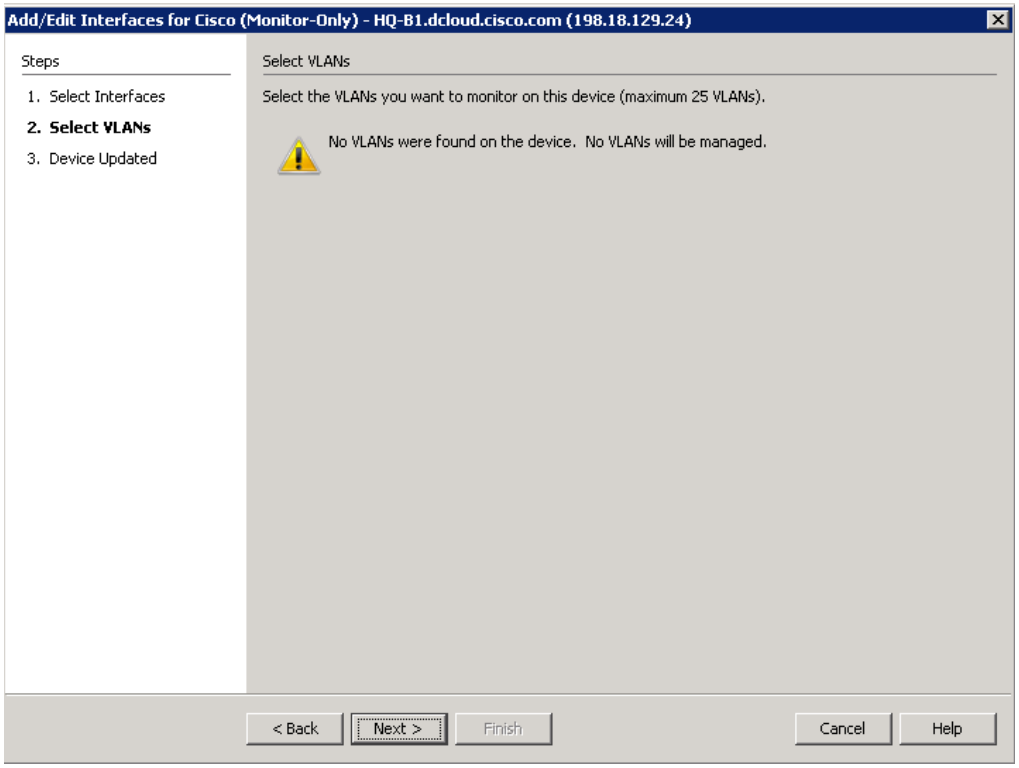
Select the interfaces you want to monitor on this device (maximum 1000 interfaces).

| Selected | Interface | Trunk | IP Address | Description |
|---|---|---|---|---|
| ☑ | Ethernet0/0 | | 198.18.129.24 | |
| ☑ | Ethernet0/1 | | 100.64.0.2 | |
| ☑ | Loopback0 | | 10.0.0.101 | |
| □ | Null0 | | | |
| □ | Tunnel0 | | | PFR auto-tunnel for VRF default |
| ☑ | Tunnel100 | | 172.16.1.254 | DMVPN over Internet |
| □ | VoIP-Null0 | | | |

Selected interface(s): 4

3. Select Next.

The select VLANs menu will appear.


Add/Edit Interfaces for Cisco (Monitor-Only) - HQ-B1.dcloud.cisco.com (198.18.129.24)

Steps

1. Select Interfaces
2. **Select VLANs**
3. Device Updated

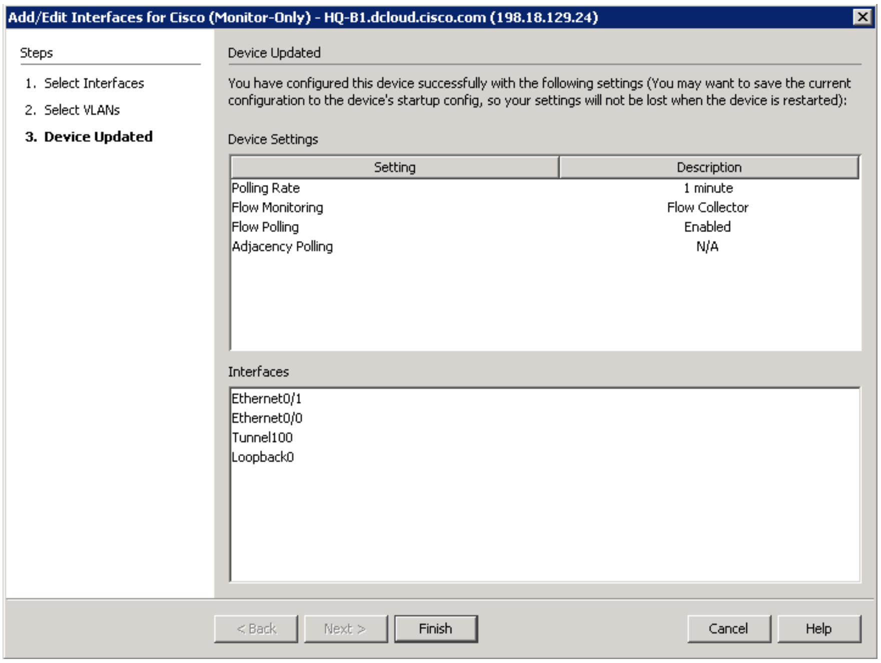
Select VLANs

Select the VLANs you want to monitor on this device (maximum 25 VLANs).

No VLANs were found on the device. No VLANs will be managed.

4. Select Next.

5. Select Finish.



Add/Edit Interfaces for Cisco (Monitor-Only) - HQ-B1.dcloud.cisco.com (198.18.129.24)

Steps

1. Select Interfaces
2. Select VLANs
3. **Device Updated**

Device Updated

You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):

Device Settings

| Setting | Description |
|---|---|
| Polling Rate | 1 minute |
| Flow Monitoring | Flow Collector |
| Flow Polling | Enabled |
| Adjacency Polling | N/A |

Interfaces

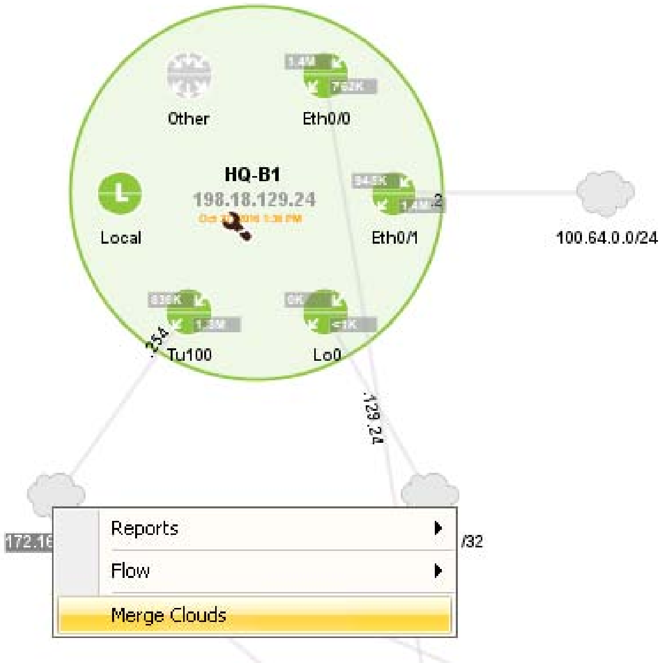
Ethernet0/1
Ethernet0/0
Tunnel100
Loopback0

The Topology will be updated with the selected interfaces.

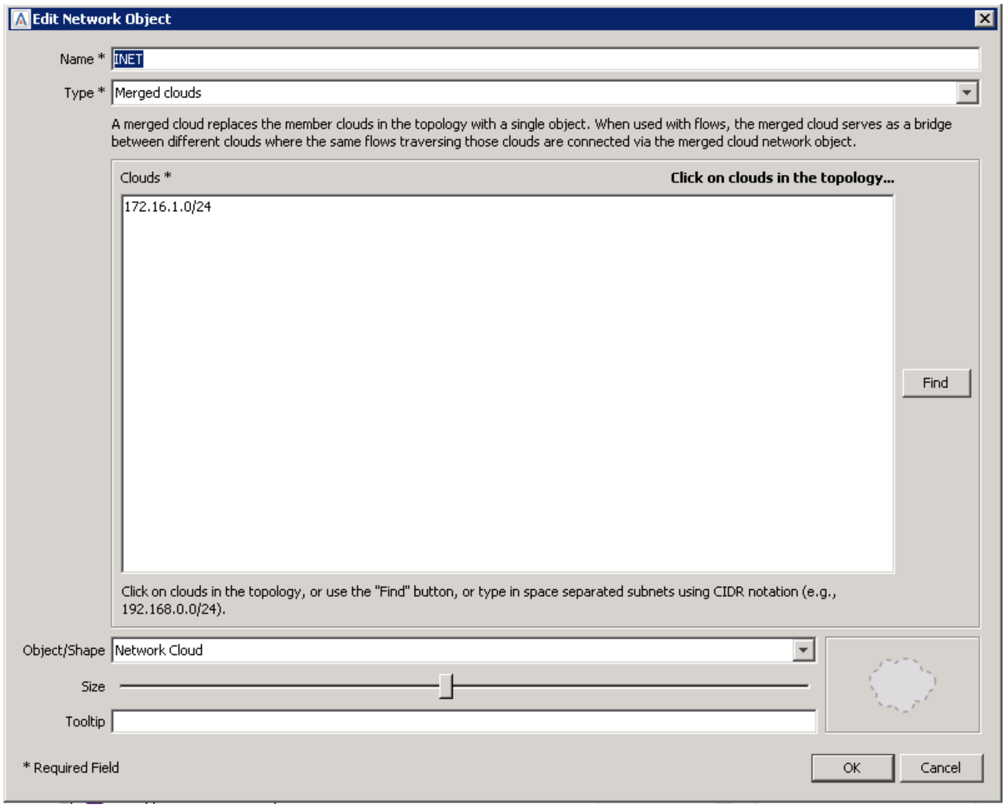
# Lab 8.4: Update Topology Map

In the next steps, we will update the map.

1. In the map, find the cloud attached to Router HQ-B1 interface Tu100, subnet 172.16.1.0/24
2. Right-Click on the cloud and select Merge Cloud.



The **Create Network Object** dialog will appear.



Edit Network Object

Name * INET

Type * Merged clouds

A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud network object.

Clouds * Click on clouds in the topology...

172.16.1.0/24

Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).

Object/Shape Network Cloud

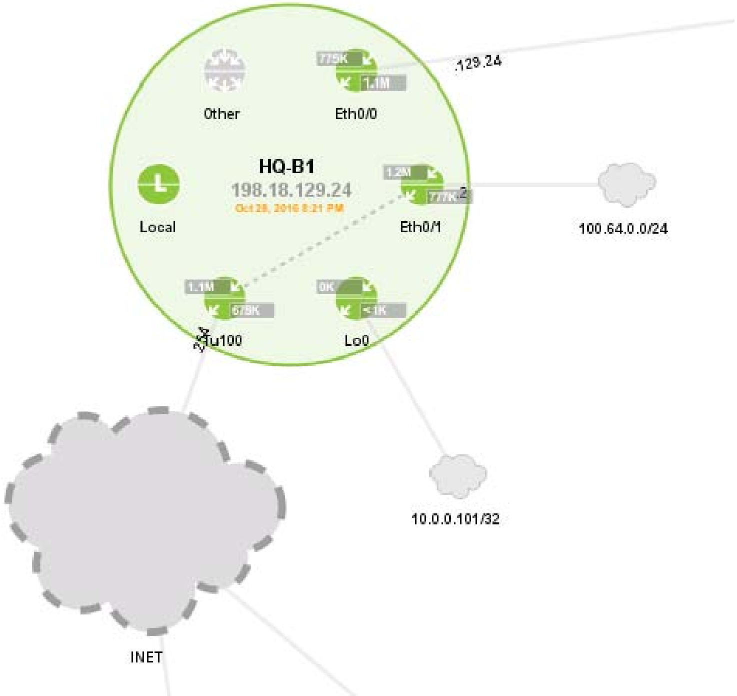
Size

Tooltip

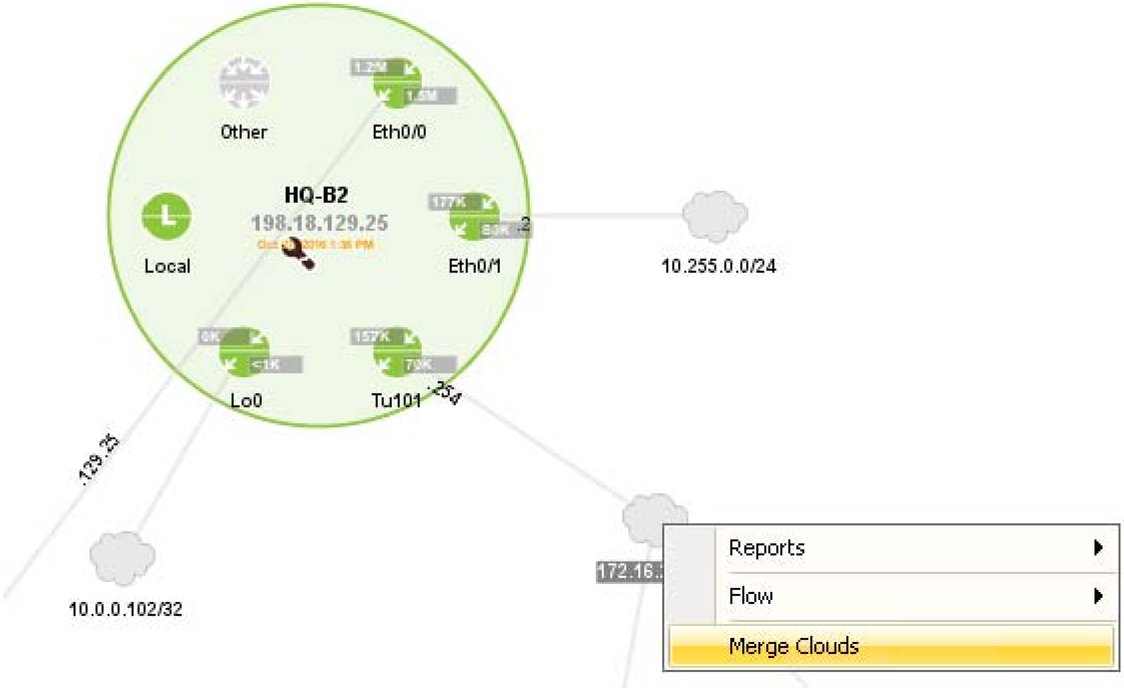
* Required Field

3. Update the name to: INET
4. Update Object/Shape: Network Cloud

A large grey cloud will appear on the Topology.

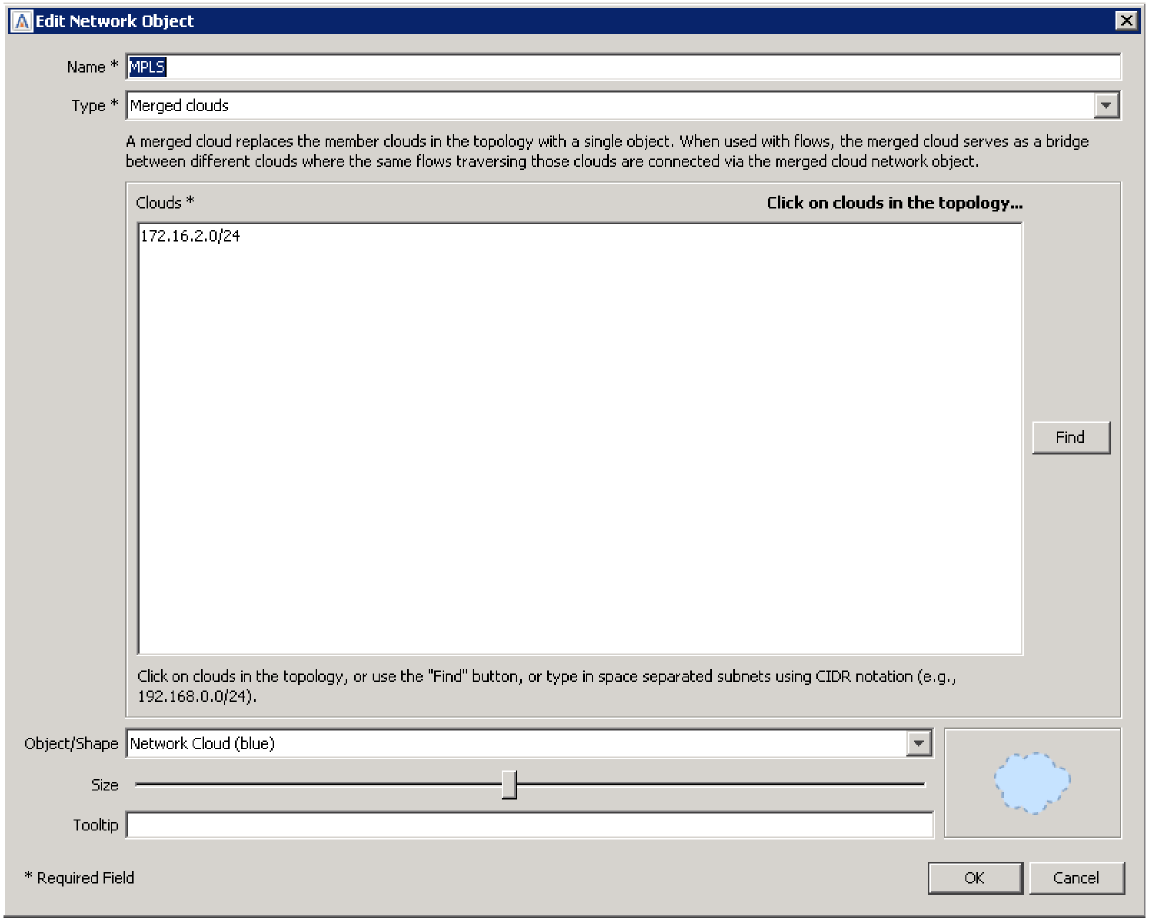


5. Locate the cloud attached to Router HQ-B2 interface Tu101, subnet 172.16.2.0/24
6. Right-Click on the cloud and select Merge Cloud.



The Create Network Object dialog will appear.

7. Update the name to = MPLS.



Edit Network Object

Name * MPLS

Type * Merged clouds

A merged cloud replaces the member clouds in the topology with a single object. When used with flows, the merged cloud serves as a bridge between different clouds where the same flows traversing those clouds are connected via the merged cloud network object.

Clouds * **Click on clouds in the topology...**

172.16.2.0/24

Click on clouds in the topology, or use the "Find" button, or type in space separated subnets using CIDR notation (e.g., 192.168.0.0/24).

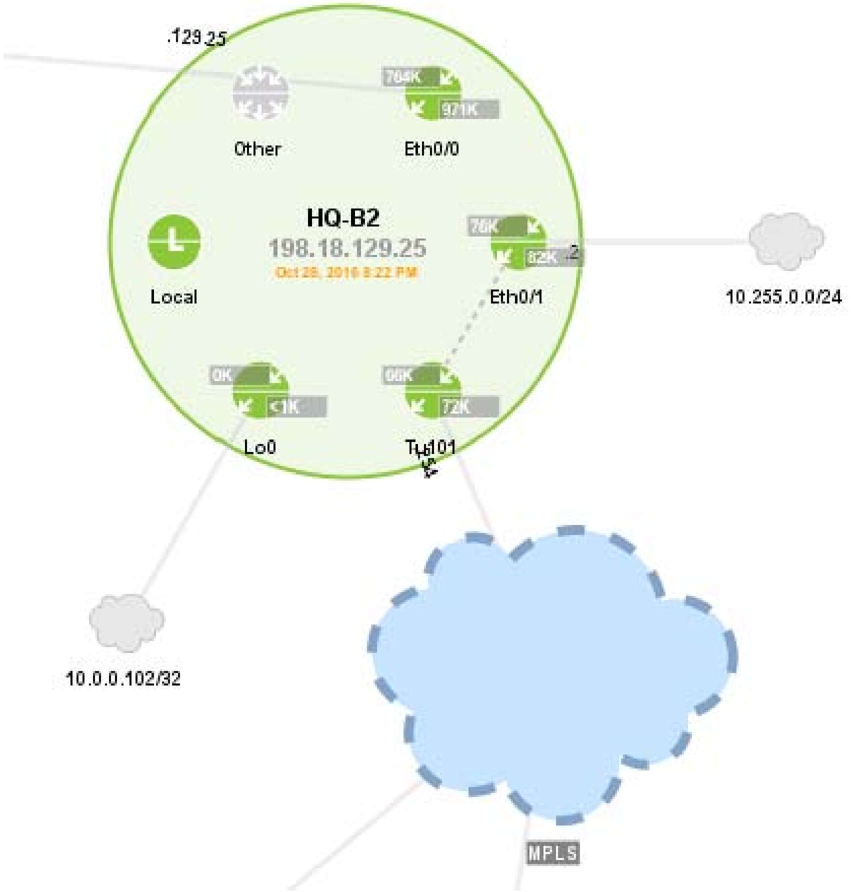
Object/Shape Network Cloud (blue)

Size

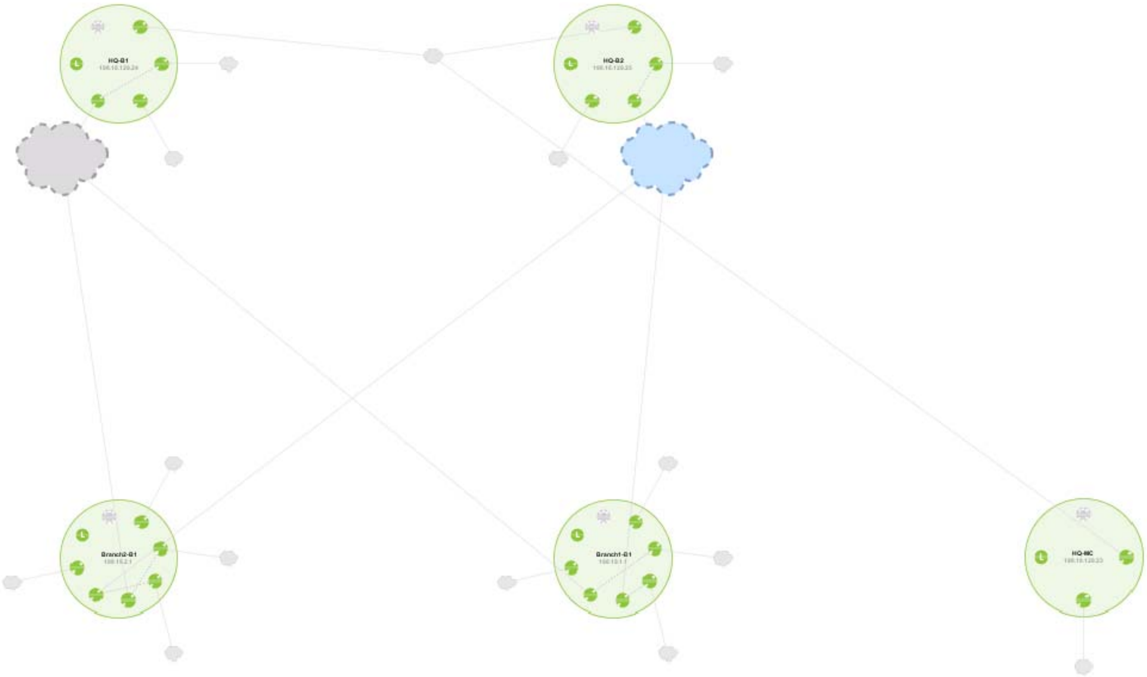
Tooltip

* Required Field

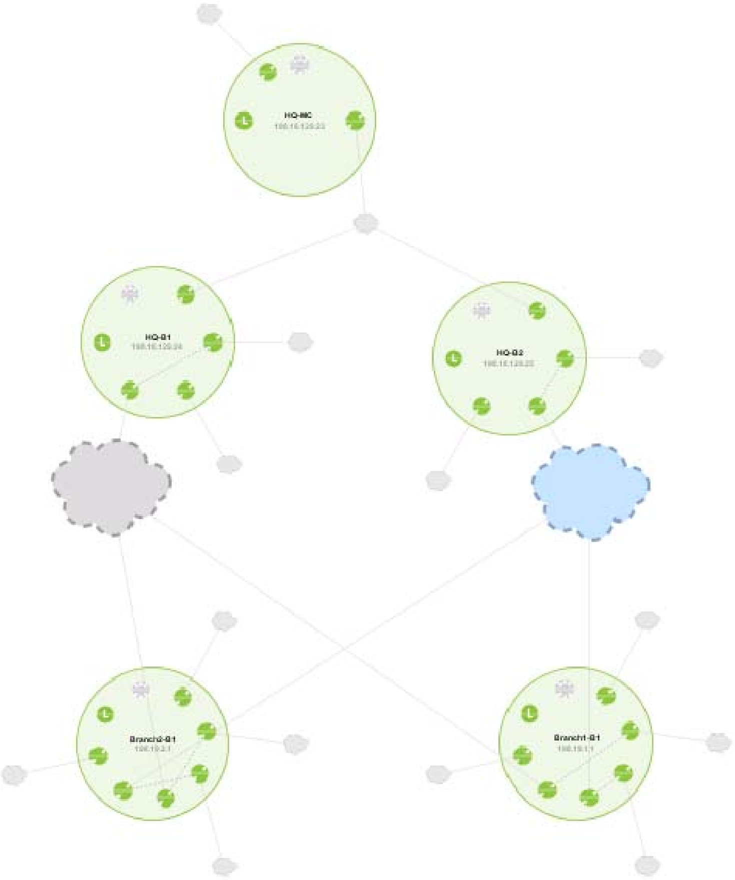
A large blue cloud will appear on the map.



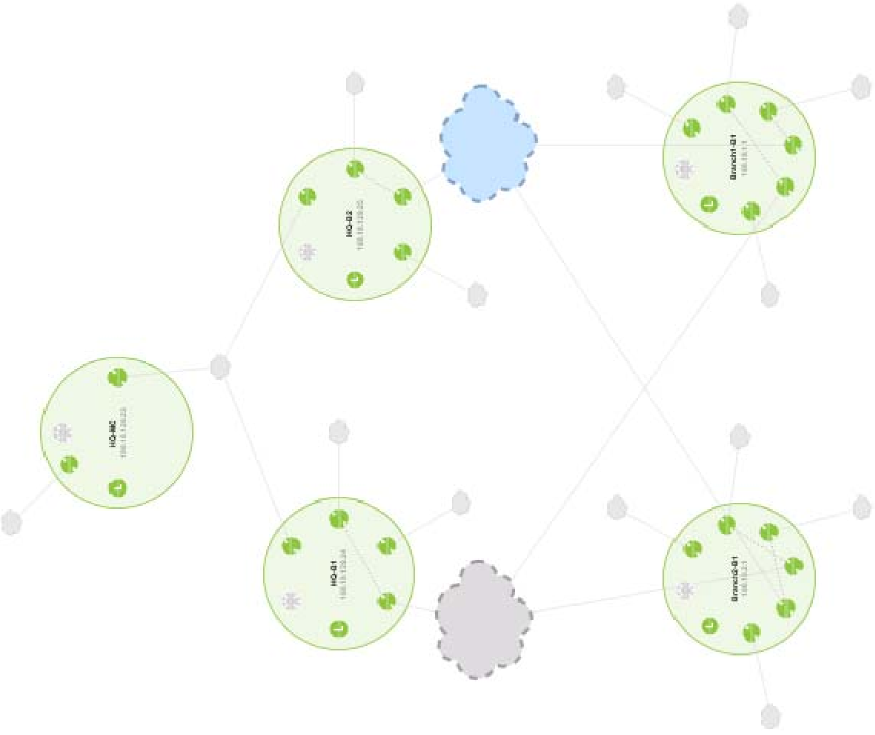
When you  review the map, it will look similar to the following.



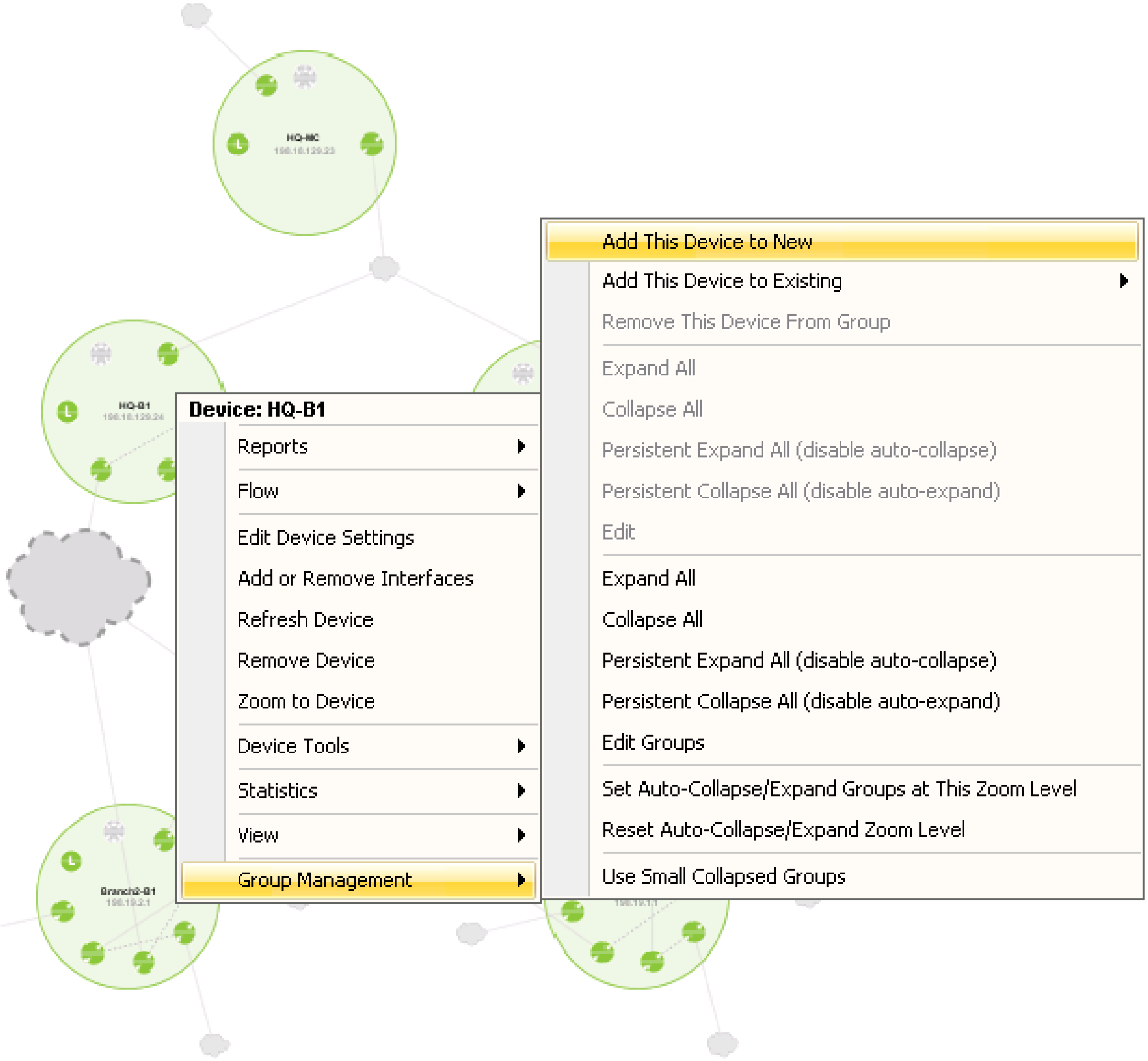
8. Re-arrange the map to make it similar to the examples below.



OR



9. Right-click on one of the routers and select Group Management > Add This Device to New

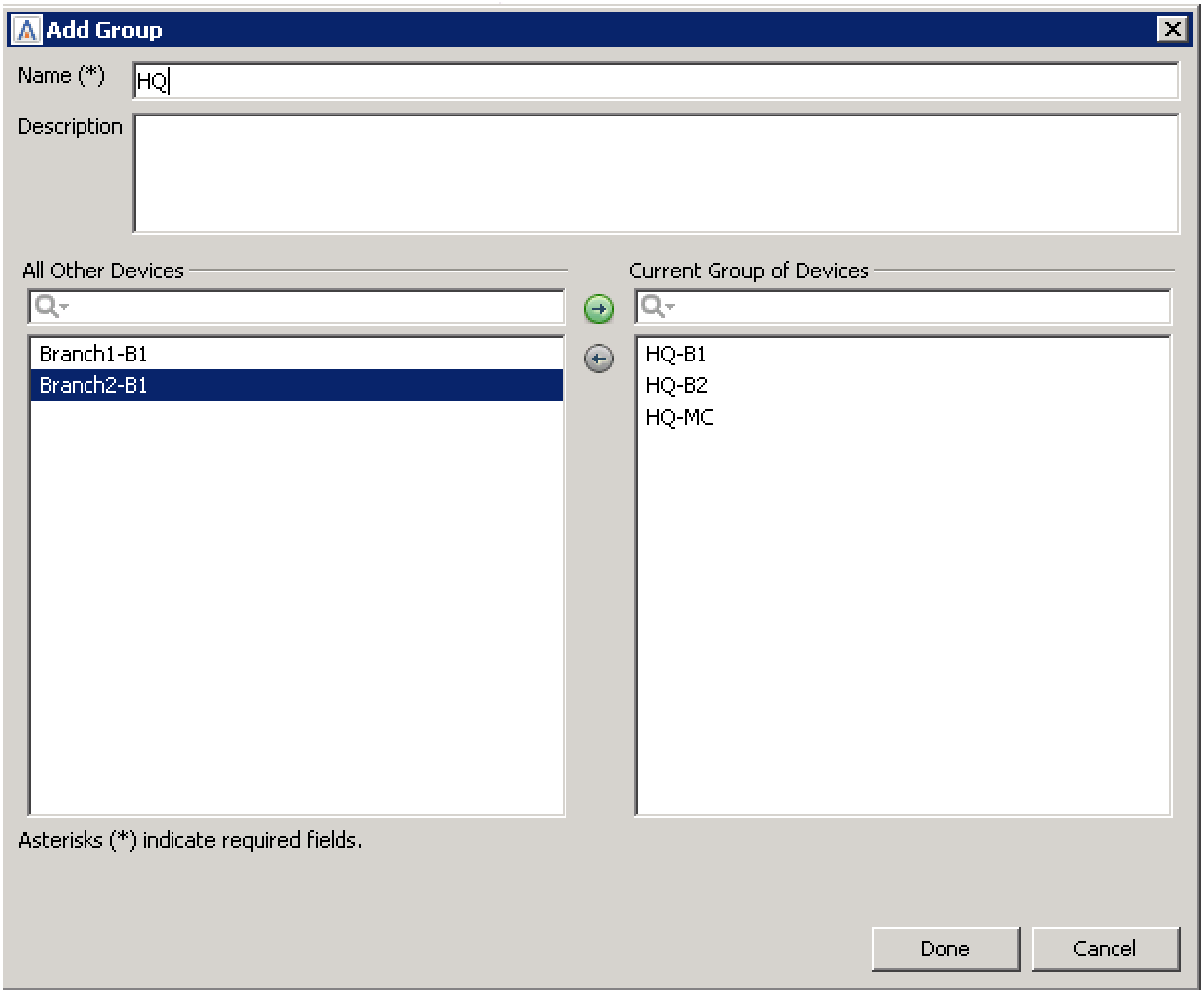

HQ-MC
HQ-B1
Branch2-B1
Device: HQ-B1
Reports
Flow
Edit Device Settings
Add or Remove Interfaces
Refresh Device
Remove Device
Zoom to Device
Device Tools
Statistics
View
Group Management
Add This Device to New
Add This Device to Existing
Remove This Device From Group
Expand All
Collapse All
Persistent Expand All (disable auto-collapse)
Persistent Collapse All (disable auto-expand)
Edit
Expand All
Collapse All
Persistent Expand All (disable auto-collapse)
Persistent Collapse All (disable auto-expand)
Edit Groups
Set Auto-Collapse/Expand Groups at This Zoom Level
Reset Auto-Collapse/Expand Zoom Level
Use Small Collapsed Groups

The Add Group dialog will appear.

10. Add a name to the group and move the respective devices to the Current Group od Devices field.

Use the following table as a guide.

| Device | Group |
|---|---|
| Branch1-B1 | Branch1 |
| Branch2-B1 | Branch2 |
| HQ-B1 | HQ |
| HQ-B2 | HQ |
| HQ-MC | HQ |



Name (*) HQ

Description

All Other Devices

Branch1-B1

Branch2-B1

Current Group of Devices

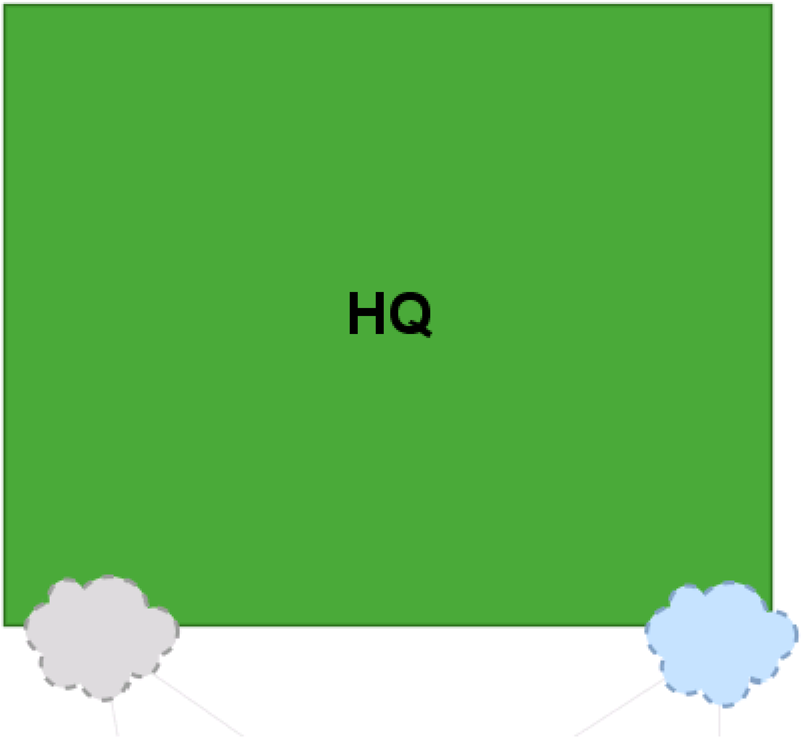
HQ-B1

HQ-B2

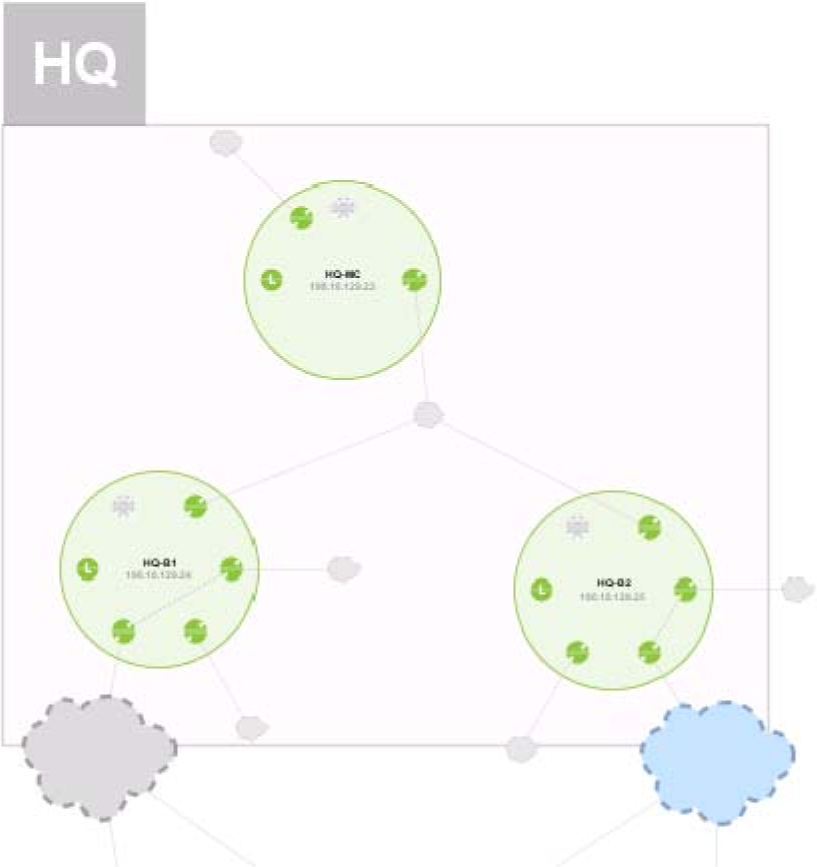
HQ-MC

Asterisks (*) indicate required fields.

11. On the map,  you will see a group appear.



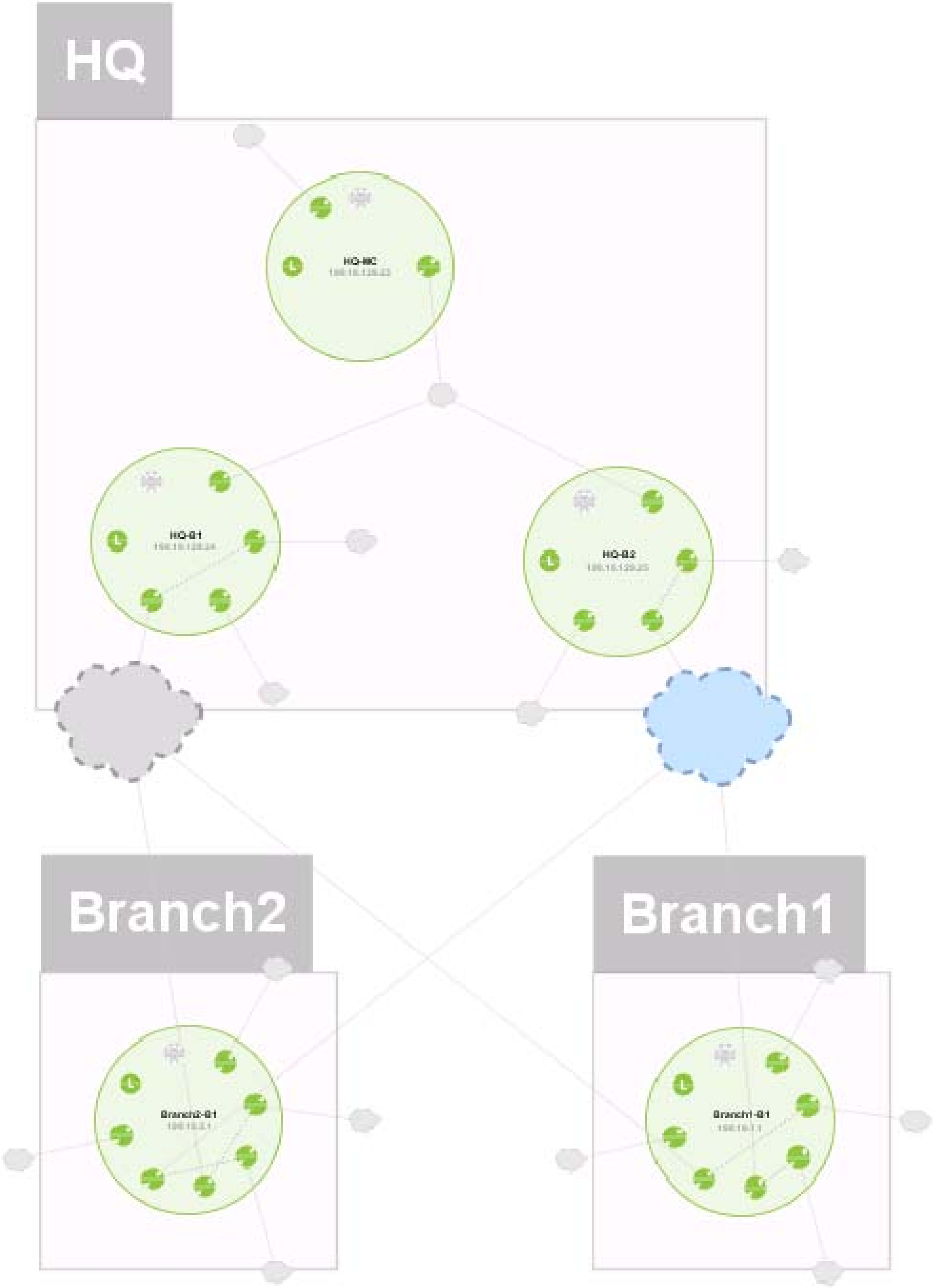
12. Double-click on the group to see the member devices again.



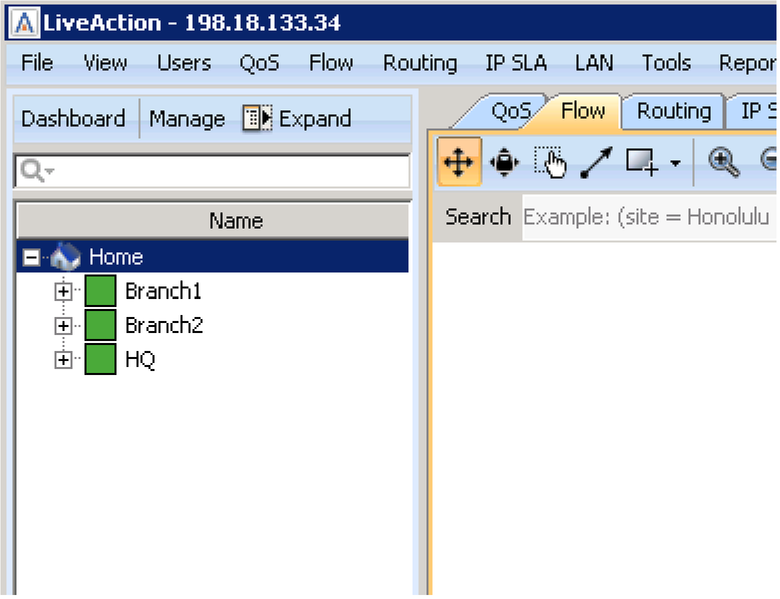
13. Add the other devices to their respective groups based on the following table:

| Device | Group |
|---|---|
| Branch1-B1 | Branch1 |
| Branch2-B1 | Branch2 |
| HQ-B1 | HQ |
| HQ-B2 | HQ |
| HQ-MC | HQ |

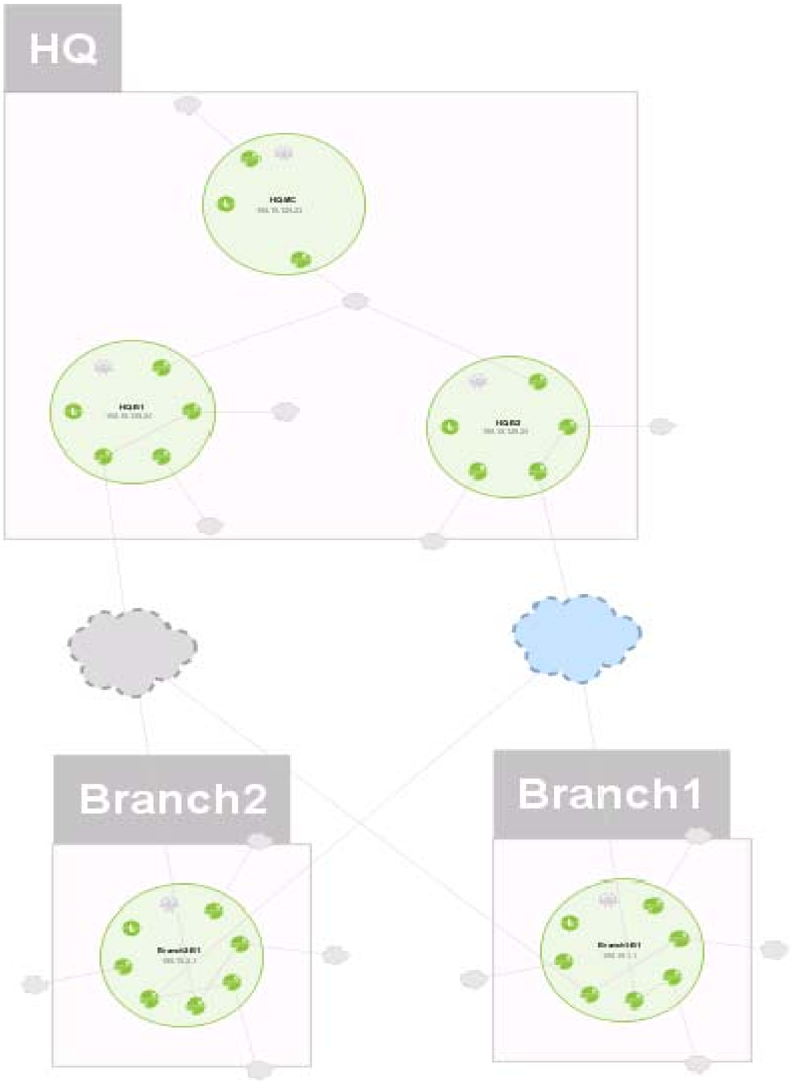
After all devices are put into groups, the map wil appear similar to the following



All devices will also appear in groups on the Device List.



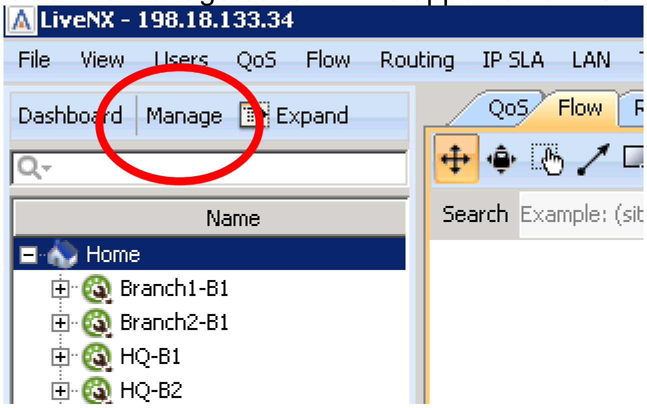
14. Continue to reogainze the map like the example shown below.



# Lab 8.5: Add CLI Access

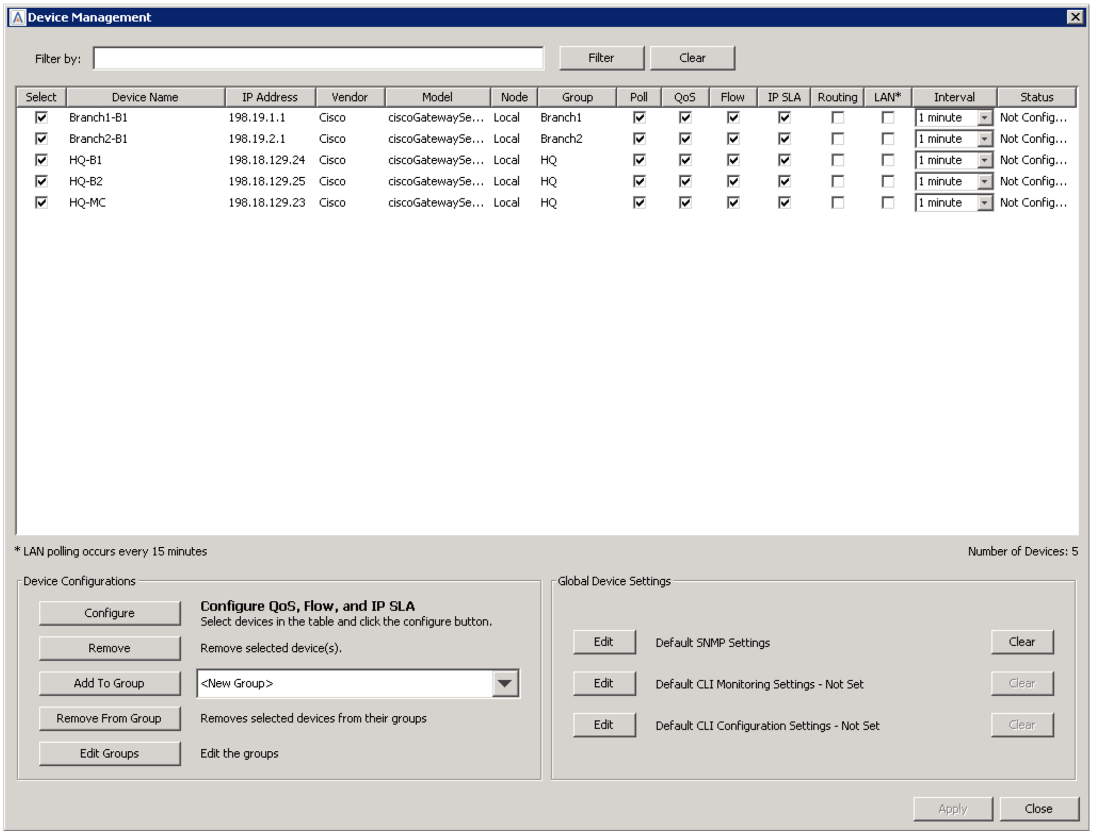
Now that the devices are being monitored and the map is organized we need to add CLI access to the routers.

1. Select the Manage button in the upper left of the LiveNX client.



The devices Management dialog will open.

2. Tick the select button for all five routers and select Configure.



| Select | Device Name | IP Address | Vendor | Model | Node | Group | Poll | QoS | Flow | IP SLA | Routing | LAN* | Interval | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Branch1-B1 | 198.19.1.1 | Cisco | ciscoGatewaySe... | Local | Branch1 | ☑ | ☑ | ☑ | ☑ | □ | □ | 1 minute | Not Config... |
| ☑ | Branch2-B1 | 198.19.2.1 | Cisco | ciscoGatewaySe... | Local | Branch2 | ☑ | ☑ | ☑ | ☑ | □ | □ | 1 minute | Not Config... |
| ☑ | HQ-B1 | 198.18.129.24 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 1 minute | Not Config... |
| ☑ | HQ-B2 | 198.18.129.25 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 1 minute | Not Config... |
| ☑ | HQ-MC | 198.18.129.23 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 1 minute | Not Config... |

* LAN polling occurs every 15 minutes

Number of Devices: 5

Device Configurations

Configure — **Configure QoS, Flow, and IP SLA**  
Select devices in the table and click the configure button.

Remove — Remove selected device(s).

Add To Group — <New Group>

Remove From Group — Removes selected devices from their groups

Edit Groups — Edit the groups

Global Device Settings

Edit — Default SNMP Settings — Clear

Edit — Default CLI Monitoring Settings - Not Set — Clear

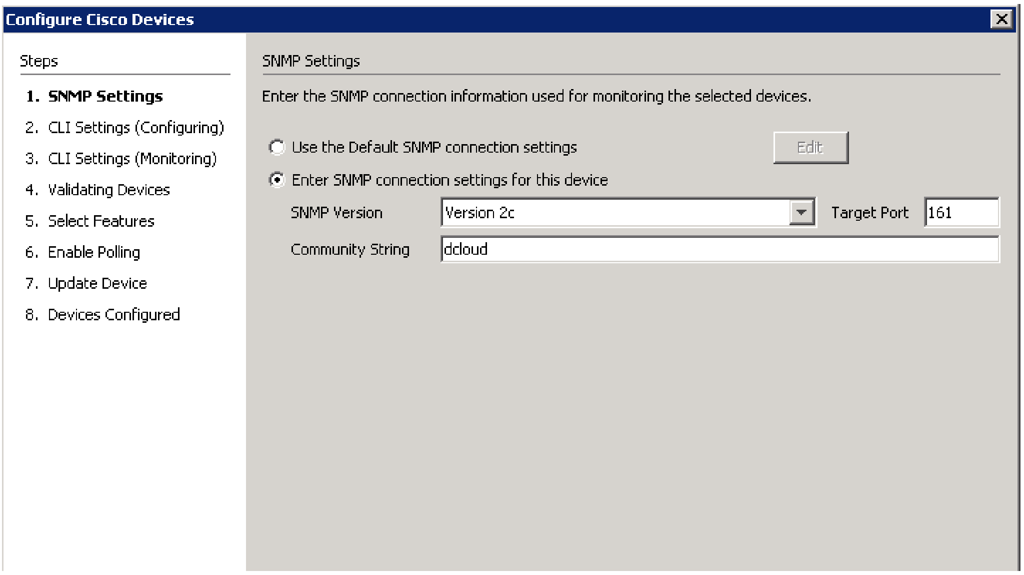
Edit — Default CLI Configuration Settings - Not Set — Clear

The Configure Cisco Devices dialog will appear.

3. Click; Use the Default…

   OR

4. Enter the SNMP credentials, and , select Next:
   a. SNMP Version = Version2c
   b. Community = dcloud



Enter the SNMP connection information used for monitoring the selected devices.

○ Use the Default SNMP connection settings

● Enter SNMP connection settings for this device

SNMP Version: Version 2c

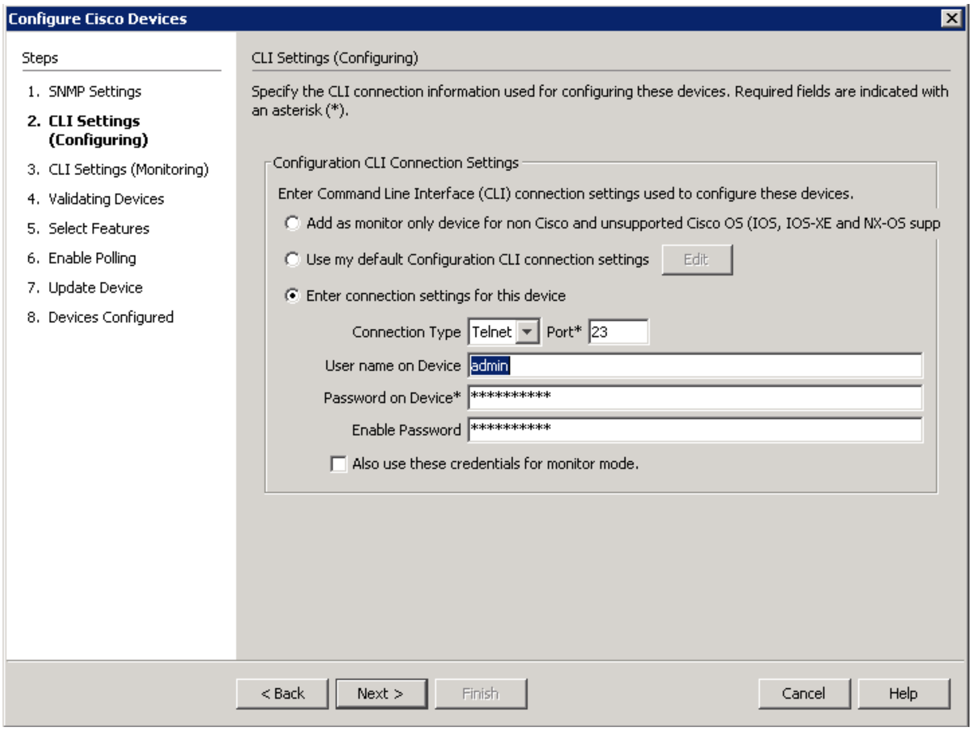
Target Port: 161

Community String: dcloud

5. Click Use my Default…

   OR

6. Enter the CLI configuration settings, and select Next.
   a. Type = **SSH** Port **22**
   b. Username = **admin**
   c. Password = **C1sco12345**
   d. Enable Password = **C1sco12345**



Configure Cisco Devices

Steps

1. SNMP Settings
2. **CLI Settings (Configuring)**
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

○ Use my default Configuration CLI connection settings [Edit]

● Enter connection settings for this device

Connection Type: Telnet  Port*: 23

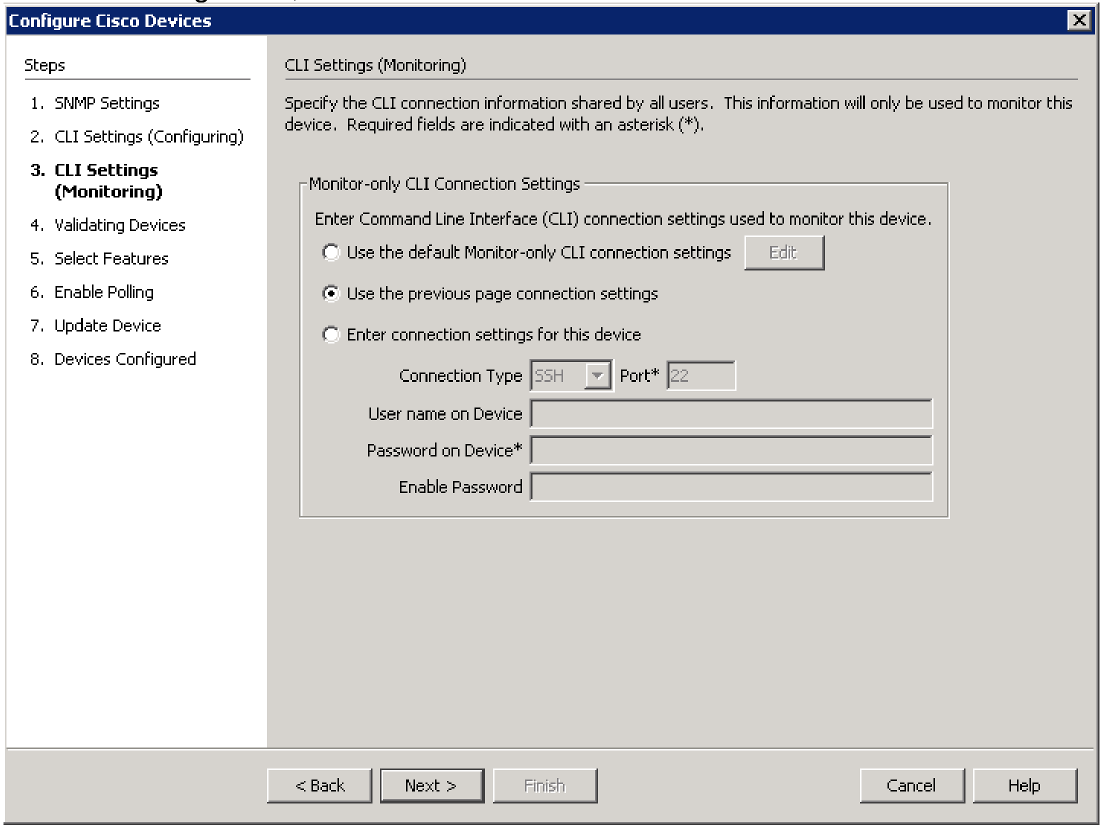
User name on Device: admin

Password on Device*: ***********

Enable Password: ***********

□ Also use these credentials for monitor mode.

7. For the CLI Monitoring settings page, select ”Use the previous page connection settings” and, select Next.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings [Edit]

● Use the previous page connection settings

○ Enter connection settings for this device

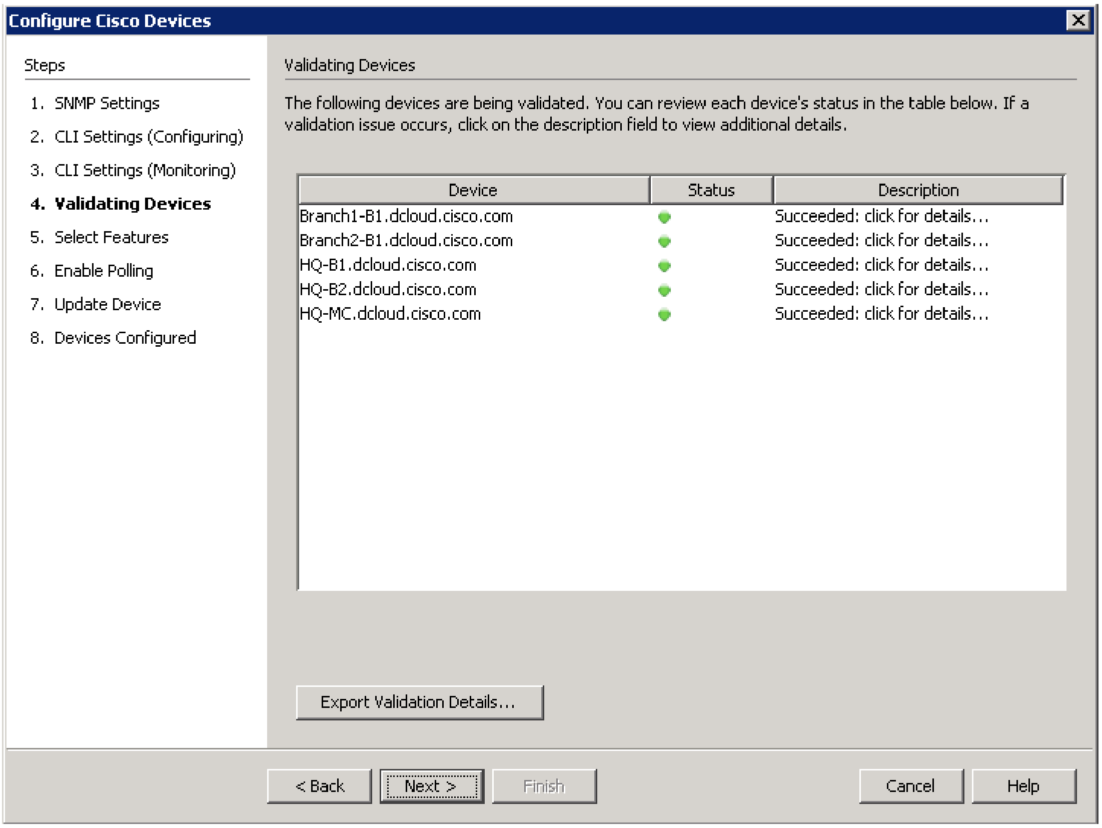
Connection Type: SSH  Port*: 22

User name on Device:

Password on Device*:

Enable Password:

8. The devices will be validated, select Next.

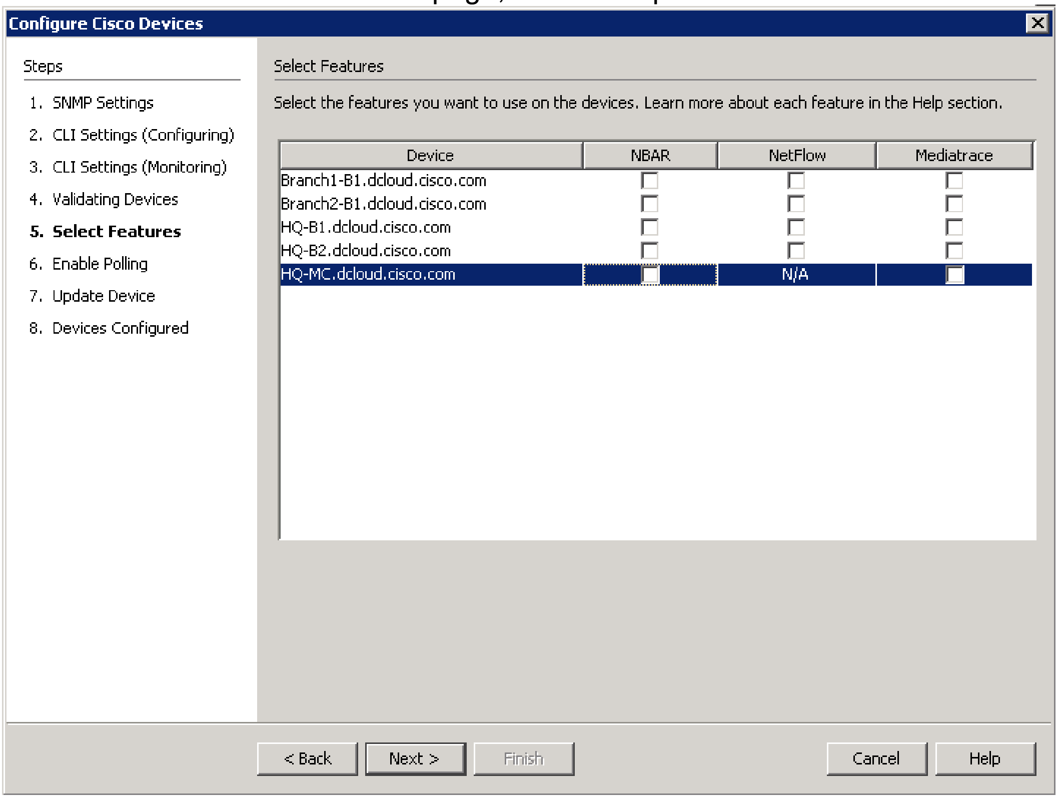


Validating Devices

The following devices are being validated. You can review each device's status in the table below. If a validation issue occurs, click on the description field to view additional details.

| Device | Status | Description |
|---|---|---|
| Branch1-B1.dcloud.cisco.com | ● | Succeeded: click for details... |
| Branch2-B1.dcloud.cisco.com | ● | Succeeded: click for details... |
| HQ-B1.dcloud.cisco.com | ● | Succeeded: click for details... |
| HQ-B2.dcloud.cisco.com | ● | Succeeded: click for details... |
| HQ-MC.dcloud.cisco.com | ● | Succeeded: click for details... |

9. On the Select Features page, untick all options and select Next.



Configure Cisco Devices

Steps

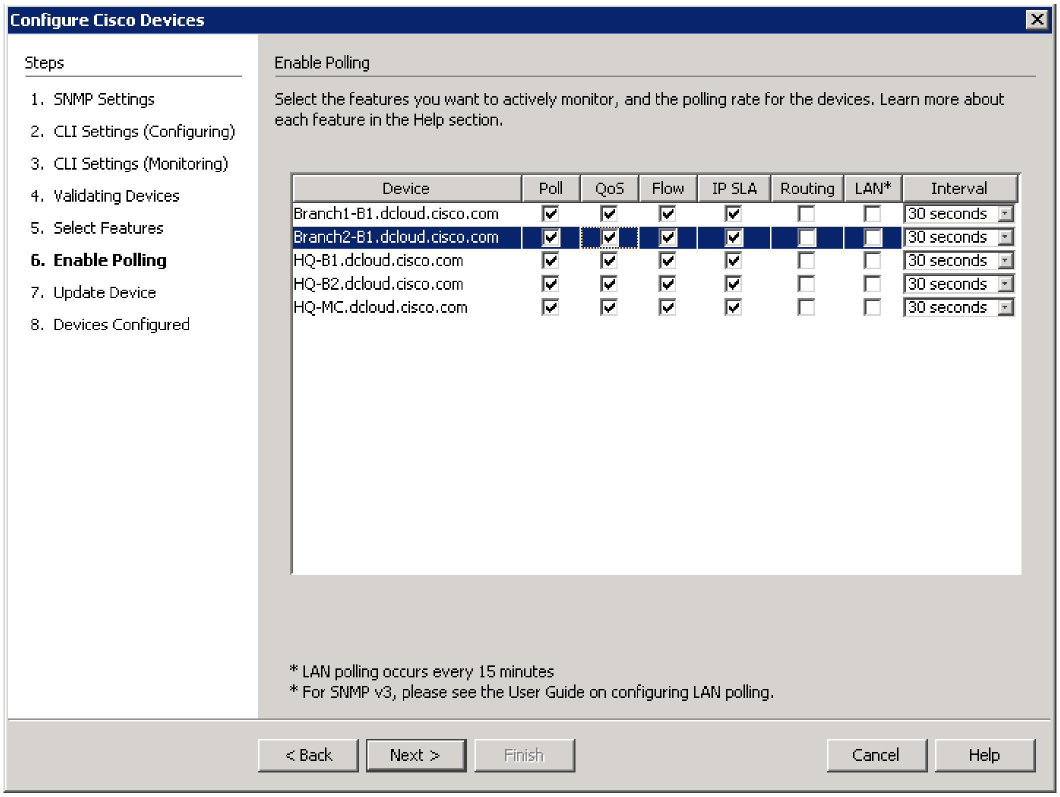
1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. **Select Features**
6. Enable Polling
7. Update Device
8. Devices Configured

Select Features

Select the features you want to use on the devices. Learn more about each feature in the Help section.

| Device | NBAR | NetFlow | Mediatrace |
|---|---|---|---|
| Branch1-B1.dcloud.cisco.com | □ | □ | □ |
| Branch2-B1.dcloud.cisco.com | □ | □ | □ |
| HQ-B1.dcloud.cisco.com | □ | □ | □ |
| HQ-B2.dcloud.cisco.com | □ | □ | □ |
| HQ-MC.dcloud.cisco.com | □ | N/A | □ |

10. On the Enable polling page
    a. Tick polling, QoS, Flow, and IP  SLA for all devices
    b. Set the interval to 30 seconds.
    c. Select Next



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. **Enable Polling**
7. Update Device
8. Devices Configured

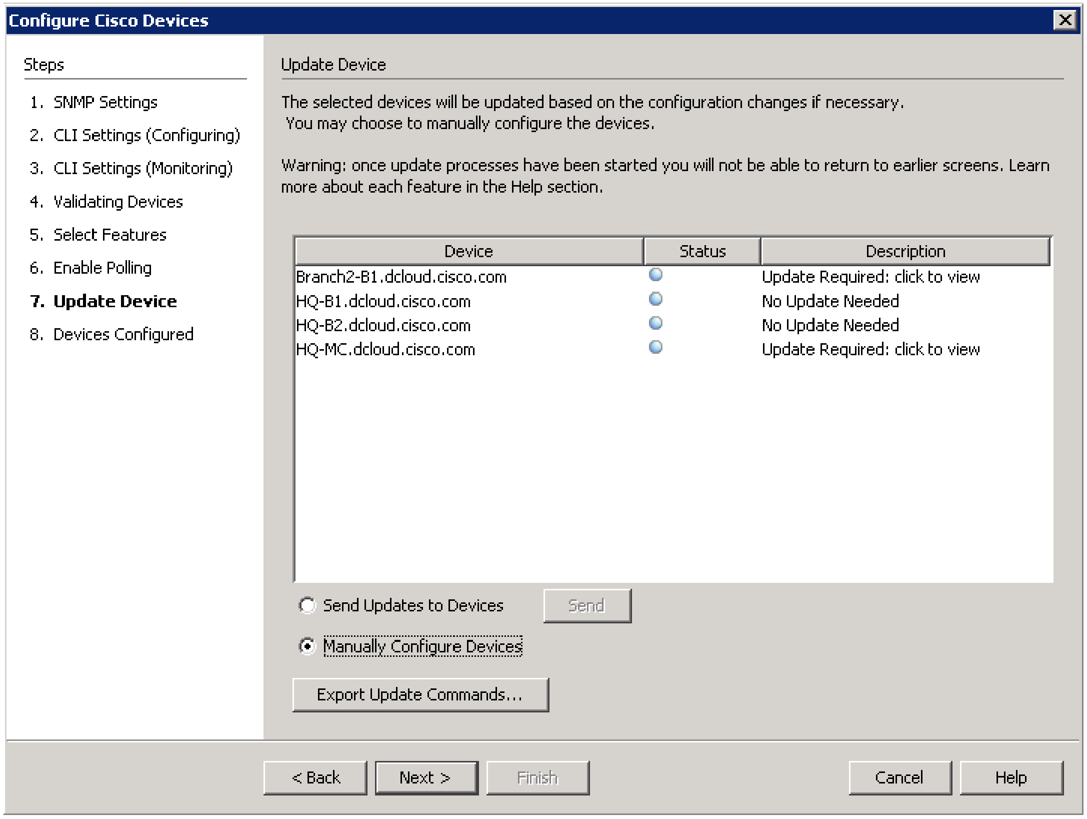
Enable Polling

Select the features you want to actively monitor, and the polling rate for the devices. Learn more about each feature in the Help section.

| Device | Poll | QoS | Flow | IP SLA | Routing | LAN* | Interval |
|---|---|---|---|---|---|---|---|
| Branch1-B1.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seconds |
| Branch2-B1.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seconds |
| HQ-B1.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seconds |
| HQ-B2.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seconds |
| HQ-MC.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seconds |

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.

11. On the Update Devices page, select “Manually Configure Devices”, and select Next.



Update Device

The selected devices will be updated based on the configuration changes if necessary.
You may choose to manually configure the devices.

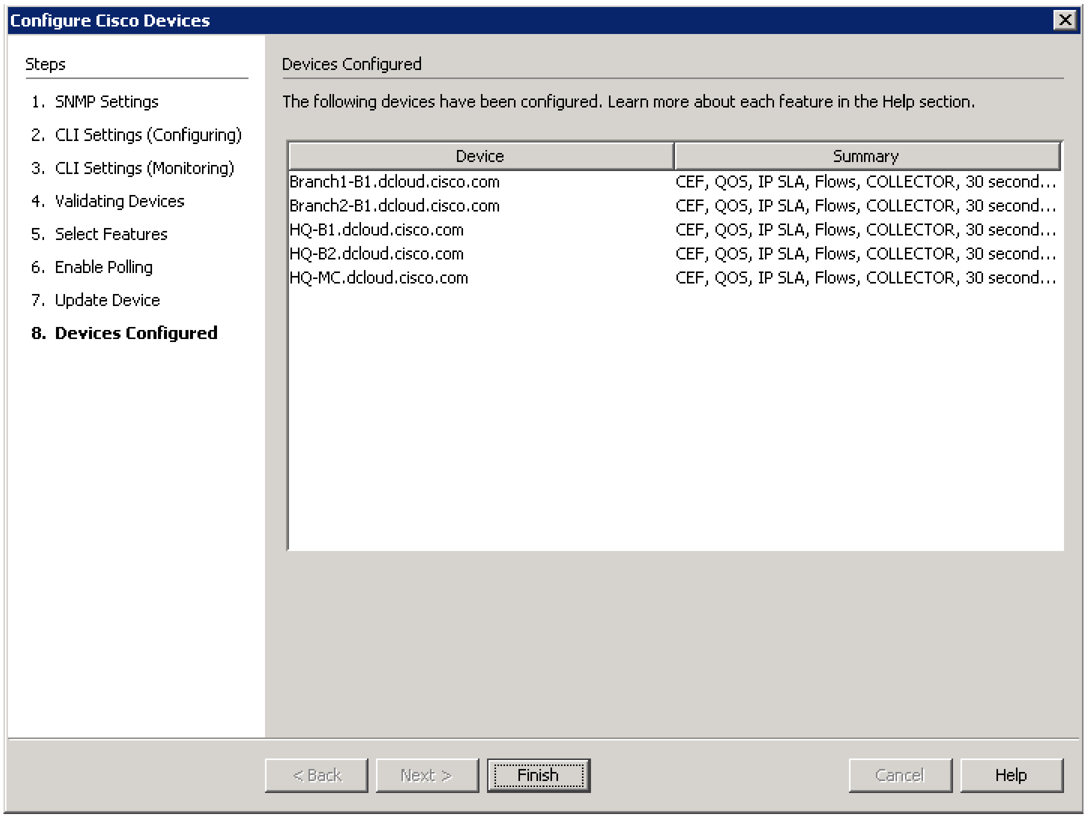
Warning: once update processes have been started you will not be able to return to earlier screens. Learn more about each feature in the Help section.

| Device | Status | Description |
|---|---|---|
| Branch2-B1.dcloud.cisco.com | ● | Update Required: click to view |
| HQ-B1.dcloud.cisco.com | ● | No Update Needed |
| HQ-B2.dcloud.cisco.com | ● | No Update Needed |
| HQ-MC.dcloud.cisco.com | ● | Update Required: click to view |

○ Send Updates to Devices

● Manually Configure Devices

12. Select Finish.

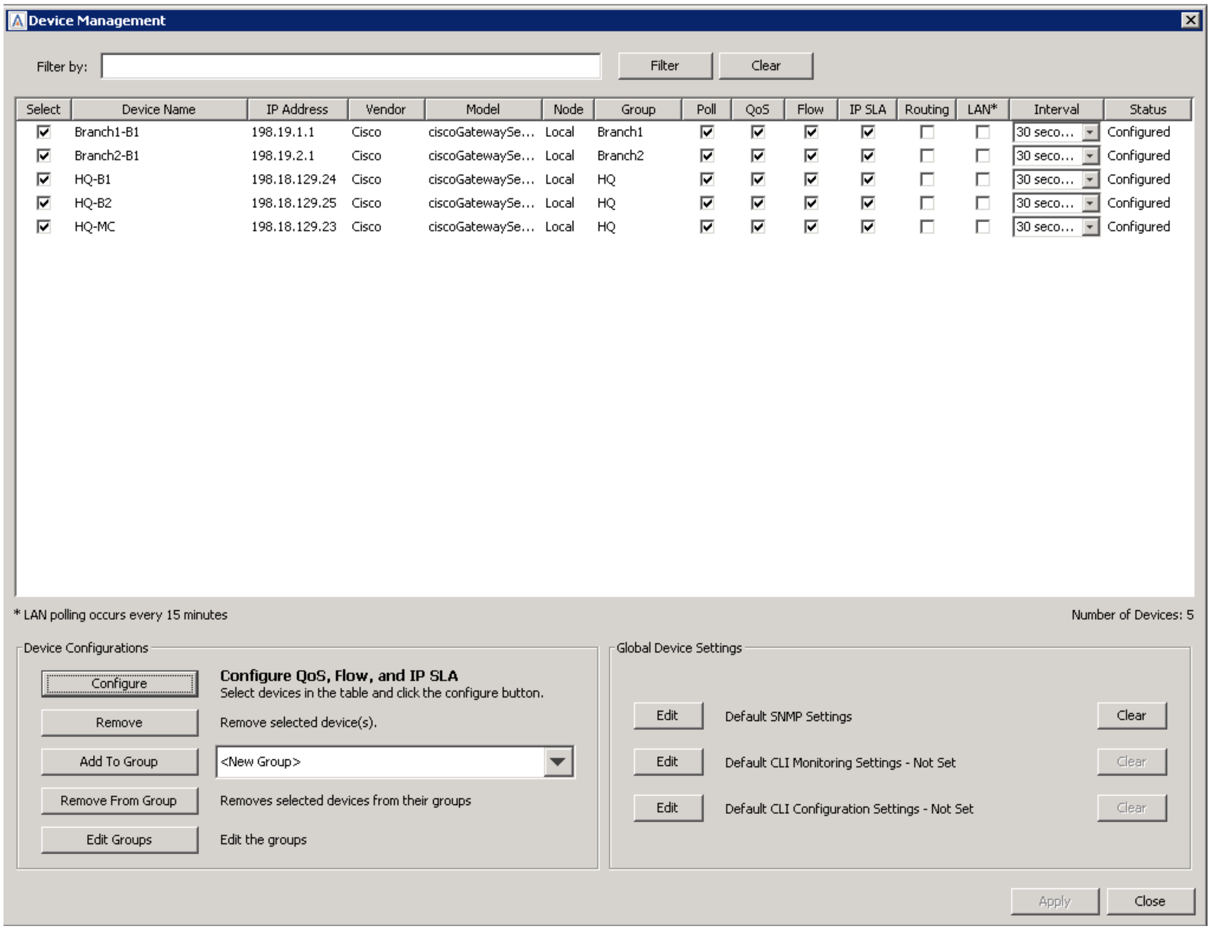


Devices Configured

The following devices have been configured. Learn more about each feature in the Help section.

| Device | Summary |
|---|---|
| Branch1-B1.dcloud.cisco.com | CEF, QOS, IP SLA, Flows, COLLECTOR, 30 second... |
| Branch2-B1.dcloud.cisco.com | CEF, QOS, IP SLA, Flows, COLLECTOR, 30 second... |
| HQ-B1.dcloud.cisco.com | CEF, QOS, IP SLA, Flows, COLLECTOR, 30 second... |
| HQ-B2.dcloud.cisco.com | CEF, QOS, IP SLA, Flows, COLLECTOR, 30 second... |
| HQ-MC.dcloud.cisco.com | CEF, QOS, IP SLA, Flows, COLLECTOR, 30 second... |

The Device Management dialog will appear again. Confirm the settings and select Close.



Filter by:

| Select | Device Name | IP Address | Vendor | Model | Node | Group | Poll | QoS | Flow | IP SLA | Routing | LAN* | Interval | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Branch1-B1 | 198.19.1.1 | Cisco | ciscoGatewaySe... | Local | Branch1 | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seco... | Configured |
| ☑ | Branch2-B1 | 198.19.2.1 | Cisco | ciscoGatewaySe... | Local | Branch2 | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seco... | Configured |
| ☑ | HQ-B1 | 198.18.129.24 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seco... | Configured |
| ☑ | HQ-B2 | 198.18.129.25 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seco... | Configured |
| ☑ | HQ-MC | 198.18.129.23 | Cisco | ciscoGatewaySe... | Local | HQ | ☑ | ☑ | ☑ | ☑ | □ | □ | 30 seco... | Configured |

* LAN polling occurs every 15 minutes

Number of Devices: 5

Device Configurations

**Configure QoS, Flow, and IP SLA**
Select devices in the table and click the configure button.

Remove selected device(s).

<New Group>

Removes selected devices from their groups

Edit the groups

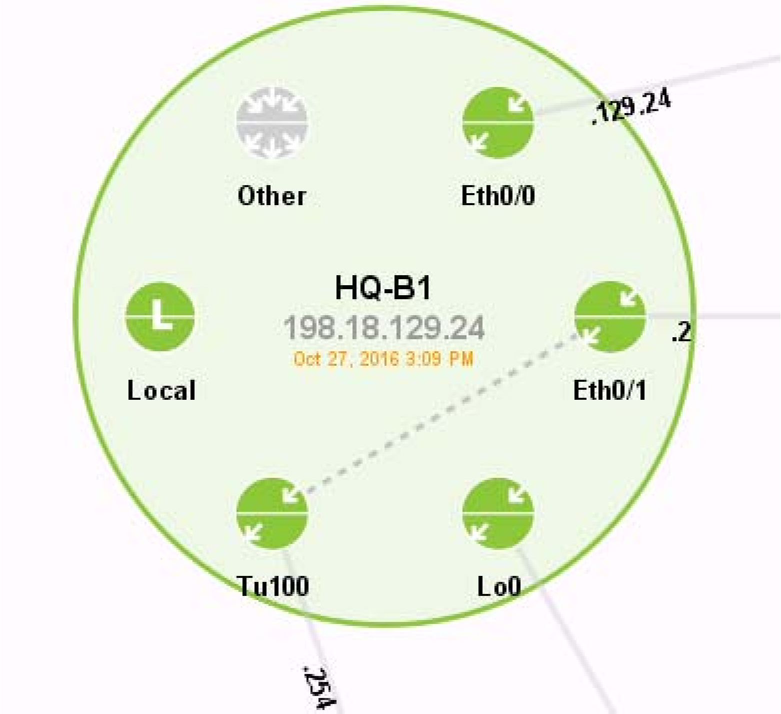
Global Device Settings

Default SNMP Settings

Default CLI Monitoring Settings - Not Set

Default CLI Configuration Settings - Not Set

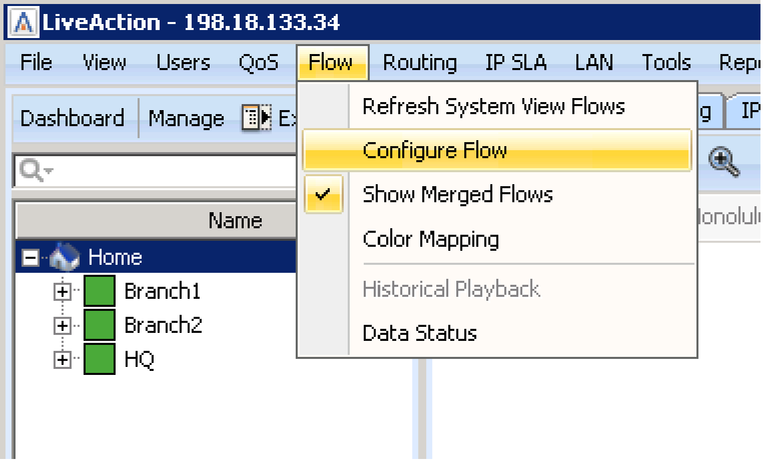
**Note: The wrench icon goes away after the CLI settings have been added.**



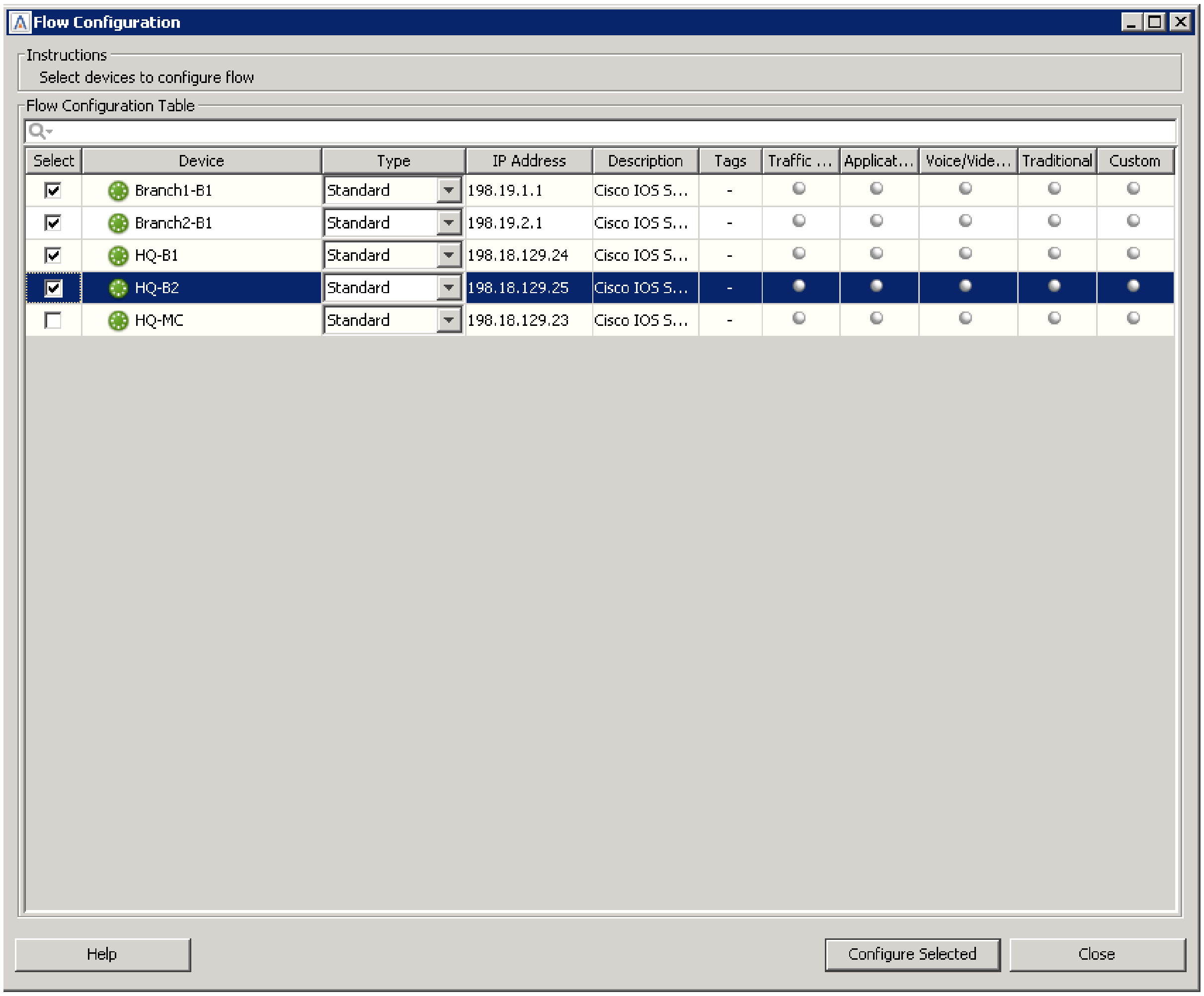
# Lab 8.6: Configure NetFlow

NetFlow needs to be configured. LiveNX can be used to accomplish this.

1. From the LiveNX client, select Flow > Configure Flow.



2. The Flow Configureation dialog will apear, tick Select for all of the devices, but for the HQ-MC, Configure Selected



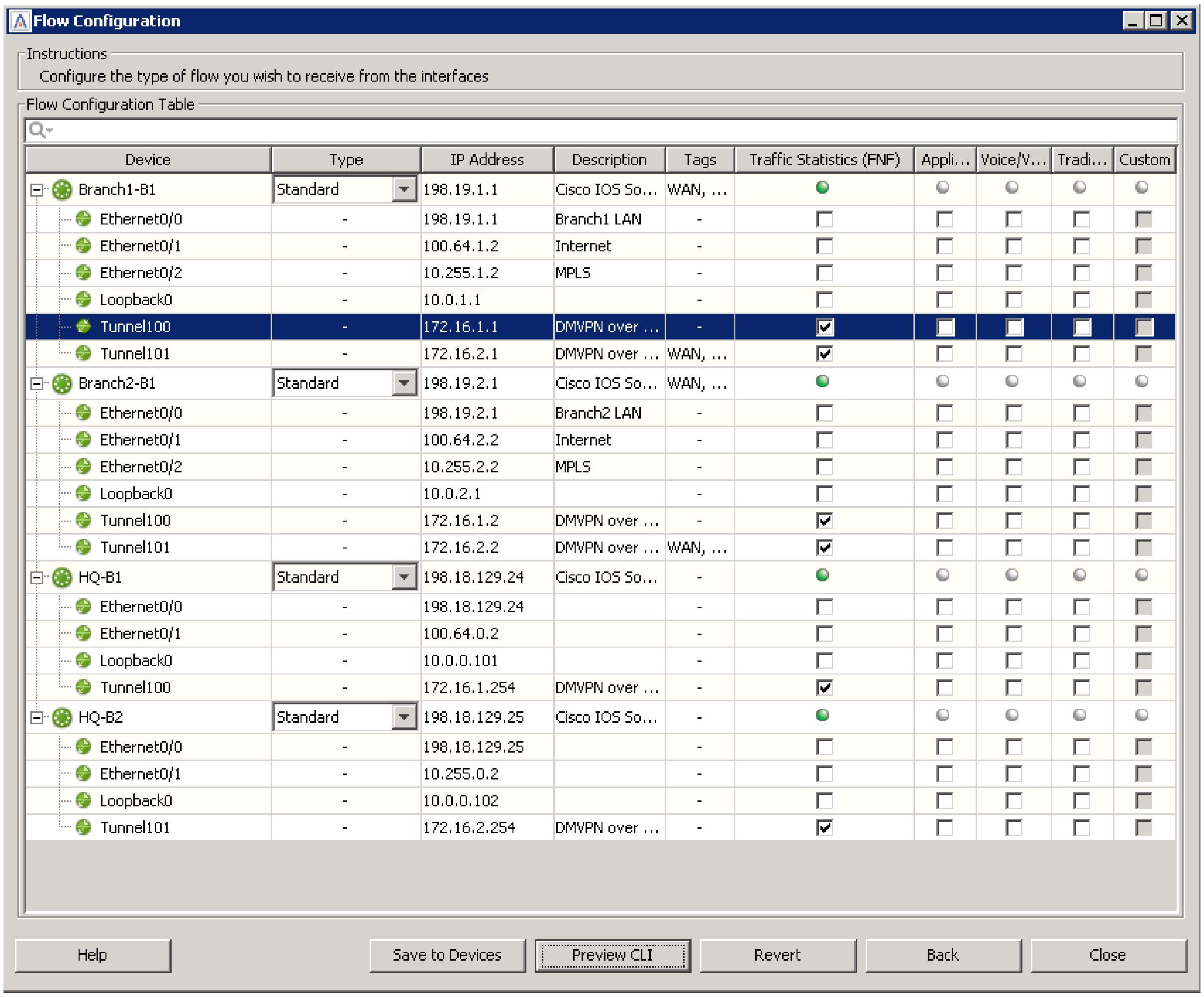
Instructions

Select devices to configure flow

Flow Configuration Table

| Select | Device | Type | IP Address | Description | Tags | Traffic ... | Applicat... | Voice/Vide... | Traditional | Custom |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Branch1-B1 | Standard | 198.19.1.1 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |
| ☑ | Branch2-B1 | Standard | 198.19.2.1 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |
| ☑ | HQ-B1 | Standard | 198.18.129.24 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |
| ☑ | HQ-B2 | Standard | 198.18.129.25 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |
| □ | HQ-MC | Standard | 198.18.129.23 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |

3. Tick the Traffic Statistics (FNF) option for all Tunnel interfaces.



Flow Configuration

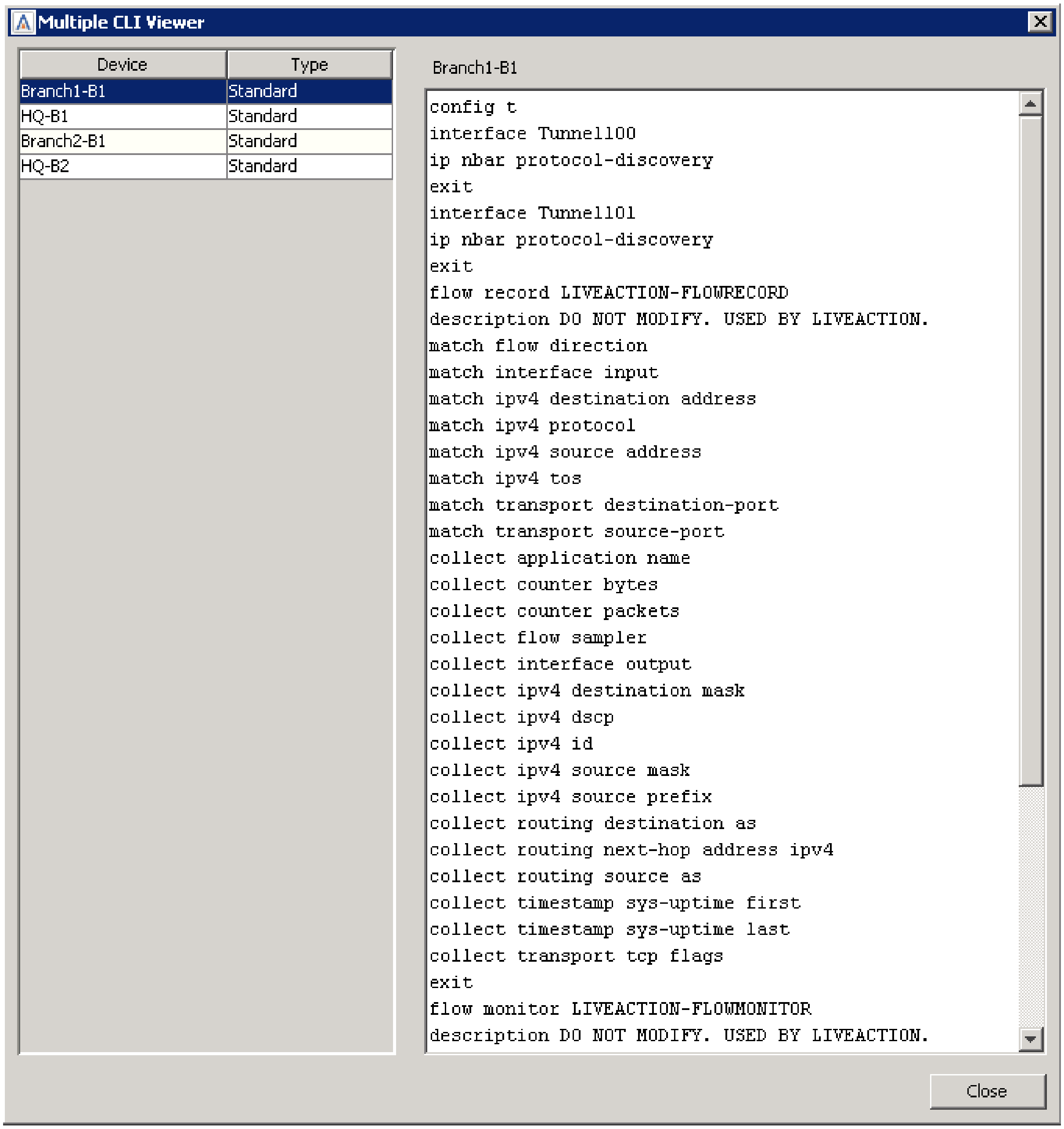
Instructions

Configure the type of flow you wish to receive from the interfaces

Flow Configuration Table

| Device | Type | IP Address | Description | Tags | Traffic Statistics (FNF) | Appli... | Voice/V... | Tradi... | Custom |
|---|---|---|---|---|---|---|---|---|---|
| Branch1-B1 | Standard | 198.19.1.1 | Cisco IOS So... | WAN, ... | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.19.1.1 | Branch1 LAN | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.1.2 | Internet | - | □ | □ | □ | □ | □ |
| Ethernet0/2 | - | 10.255.1.2 | MPLS | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.1.1 |  | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.1 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.1 | DMVPN over ... | WAN, ... | ☑ | □ | □ | □ | □ |
| Branch2-B1 | Standard | 198.19.2.1 | Cisco IOS So... | WAN, ... | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.19.2.1 | Branch2 LAN | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.2.2 | Internet | - | □ | □ | □ | □ | □ |
| Ethernet0/2 | - | 10.255.2.2 | MPLS | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.2.1 |  | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.2 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.2 | DMVPN over ... | WAN, ... | ☑ | □ | □ | □ | □ |
| HQ-B1 | Standard | 198.18.129.24 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.18.129.24 |  | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.0.2 |  | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.0.101 |  | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.254 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| HQ-B2 | Standard | 198.18.129.25 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.18.129.25 |  | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 10.255.0.2 |  | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.0.102 |  | - | □ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.254 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |

4. Click Preview CLI to review the Flexible NetFlow configuration created by LiveNX.

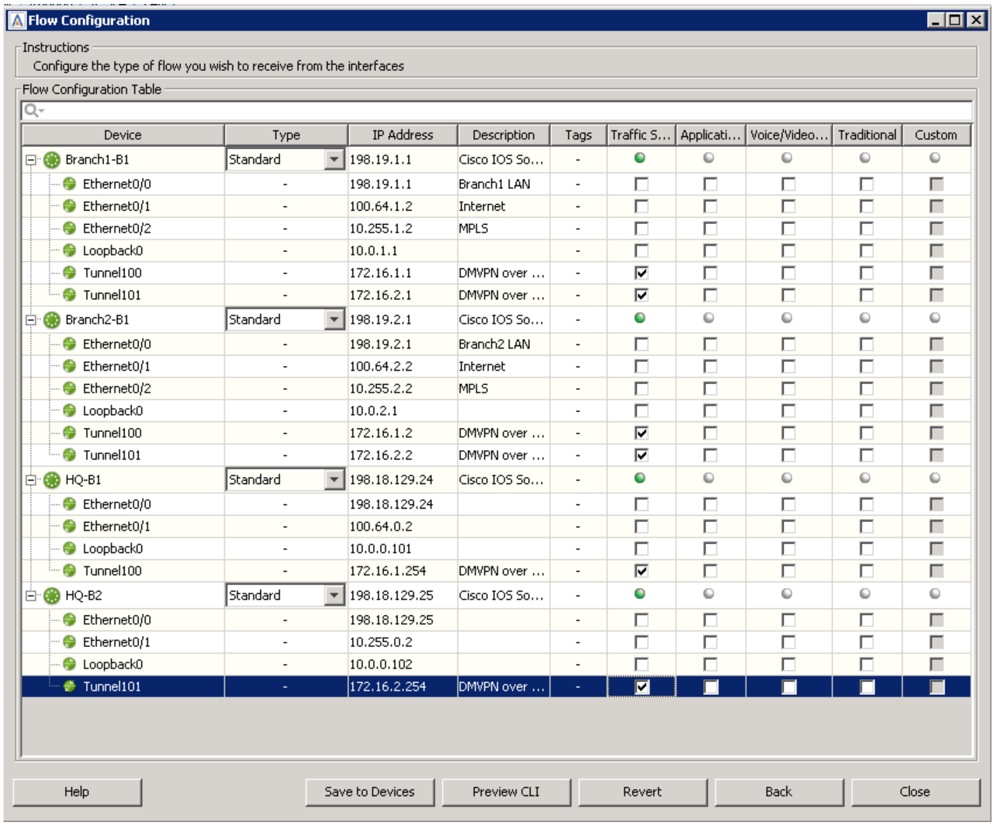


| Device | Type |
|---|---|
| Branch1-B1 | Standard |
| HQ-B1 | Standard |
| Branch2-B1 | Standard |
| HQ-B2 | Standard |

Branch1-B1

```
config t
interface Tunnel100
ip nbar protocol-discovery
exit
interface Tunnel101
ip nbar protocol-discovery
exit
flow record LIVEACTION-FLOWRECORD
description DO NOT MODIFY. USED BY LIVEACTION.
match flow direction
match interface input
match ipv4 destination address
match ipv4 protocol
match ipv4 source address
match ipv4 tos
match transport destination-port
match transport source-port
collect application name
collect counter bytes
collect counter packets
collect flow sampler
collect interface output
collect ipv4 destination mask
collect ipv4 dscp
collect ipv4 id
collect ipv4 source mask
collect ipv4 source prefix
collect routing destination as
collect routing next-hop address ipv4
collect routing source as
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect transport tcp flags
exit
flow monitor LIVEACTION-FLOWMONITOR
description DO NOT MODIFY. USED BY LIVEACTION.
```

5. Select Save to Devices.



Flow Configuration

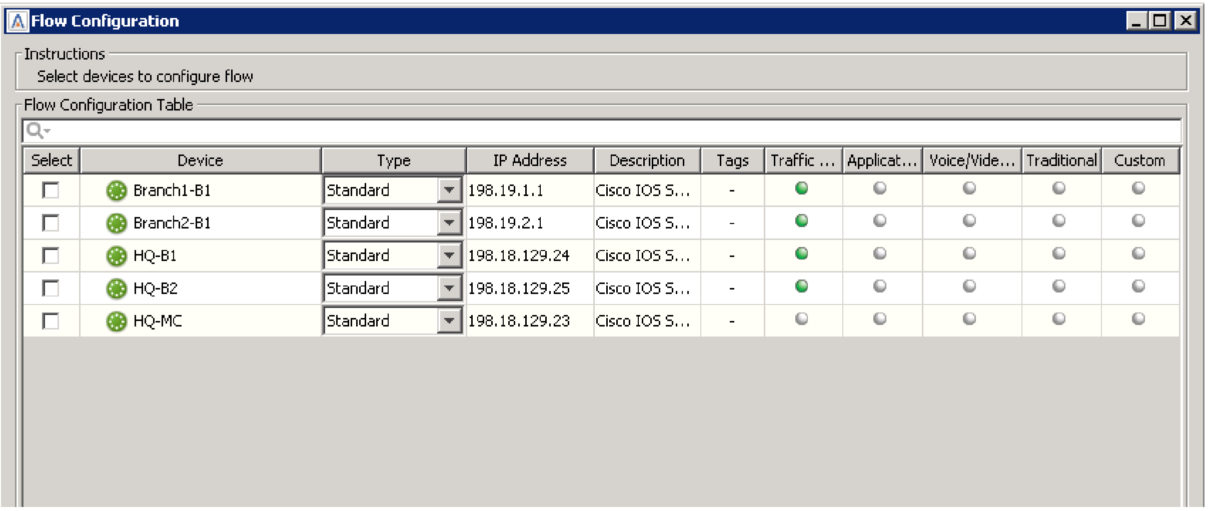
Instructions

Configure the type of flow you wish to receive from the interfaces

Flow Configuration Table

| Device | Type | IP Address | Description | Tags | Traffic S... | Applicati... | Voice/Video... | Traditional | Custom |
|---|---|---|---|---|---|---|---|---|---|
| Branch1-B1 | Standard | 198.19.1.1 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.19.1.1 | Branch1 LAN | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.1.2 | Internet | - | □ | □ | □ | □ | □ |
| Ethernet0/2 | - | 10.255.1.2 | MPLS | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.1.1 | | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.1 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.1 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| Branch2-B1 | Standard | 198.19.2.1 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.19.2.1 | Branch2 LAN | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.2.2 | Internet | - | □ | □ | □ | □ | □ |
| Ethernet0/2 | - | 10.255.2.2 | MPLS | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.2.1 | | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.2 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.2 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| HQ-B1 | Standard | 198.18.129.24 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.18.129.24 | | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 100.64.0.2 | | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.0.101 | | - | □ | □ | □ | □ | □ |
| Tunnel100 | - | 172.16.1.254 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |
| HQ-B2 | Standard | 198.18.129.25 | Cisco IOS So... | - | ● | ○ | ○ | ○ | ○ |
| Ethernet0/0 | - | 198.18.129.25 | | - | □ | □ | □ | □ | □ |
| Ethernet0/1 | - | 10.255.0.2 | | - | □ | □ | □ | □ | □ |
| Loopback0 | - | 10.0.0.102 | | - | □ | □ | □ | □ | □ |
| Tunnel101 | - | 172.16.2.254 | DMVPN over ... | - | ☑ | □ | □ | □ | □ |

LiveNX will push the NetFlow configuration to each device using the CLI settings already provided. Confirm each of the updated routers show a greem circle for the Traffic Statistics FNF column and select Close.



Flow Configuration

Instructions

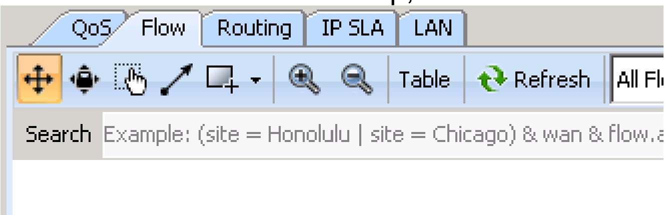
Select devices to configure flow

Flow Configuration Table

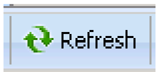
| Select | Device | Type | IP Address | Description | Tags | Traffic ... | Applicat... | Voice/Vide... | Traditional | Custom |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Branch1-B1 | Standard | 198.19.1.1 | Cisco IOS S... | - | ● | ○ | ○ | ○ | ○ |
| □ | Branch2-B1 | Standard | 198.19.2.1 | Cisco IOS S... | - | ● | ○ | ○ | ○ | ○ |
| □ | HQ-B1 | Standard | 198.18.129.24 | Cisco IOS S... | - | ● | ○ | ○ | ○ | ○ |
| □ | HQ-B2 | Standard | 198.18.129.25 | Cisco IOS S... | - | ● | ○ | ○ | ○ | ○ |
| □ | HQ-MC | Standard | 198.18.129.23 | Cisco IOS S... | - | ○ | ○ | ○ | ○ | ○ |

Confirm NetFlow collection.

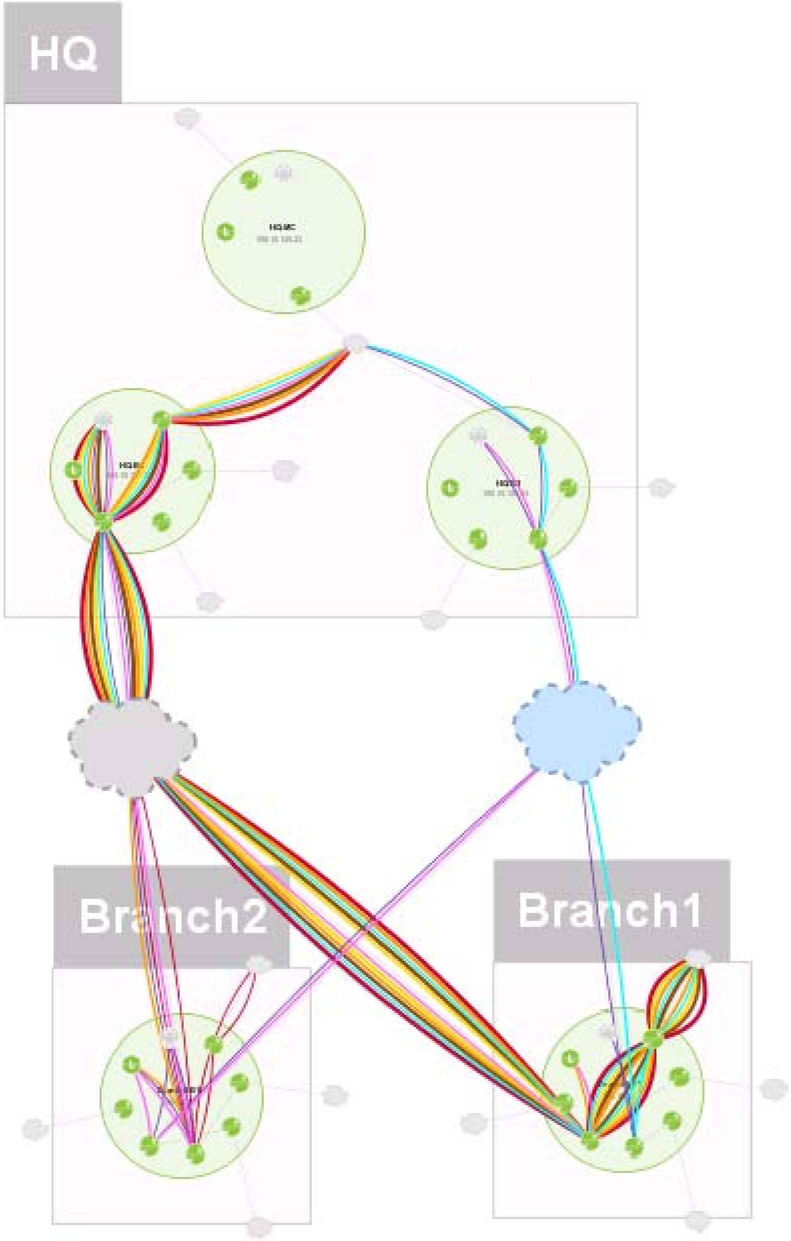
1. From the LiveNX map, select the Flow tab



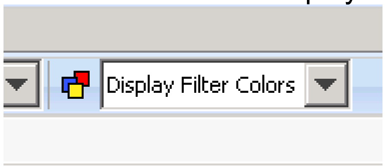
2. Select Refresh



NetFlow visualization data should appear across the map. Note it can sometimes take a couple of minutes for it to  appear

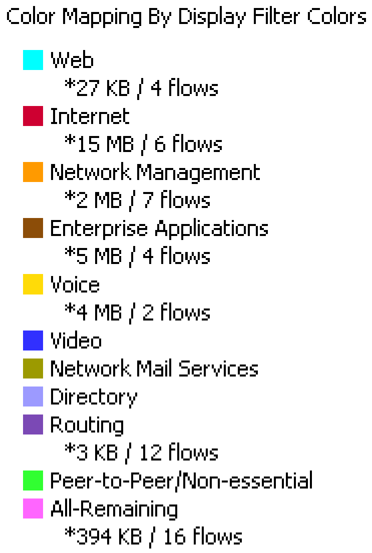


3. Select the Display Filter Colors pulldown.



Display Filter Colors

Notice the legend show the applications that are part of the default filter.



Color Mapping By Display Filter Colors

■ Web
*27 KB / 4 flows

■ Internet
*15 MB / 6 flows

■ Network Management
*2 MB / 7 flows

■ Enterprise Applications
*5 MB / 4 flows

■ Voice
*4 MB / 2 flows

■ Video

■ Network Mail Services

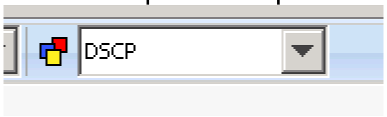
■ Directory

■ Routing
*3 KB / 12 flows

■ Peer-to-Peer/Non-essential

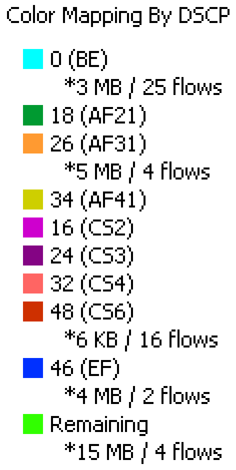
■ All-Remaining
*394 KB / 16 flows

4. Update the pulldown and select DSCP.



DSCP

Note the legend is now that of DSCP values.  This list needs to be updated as different DSCP values are being used  in this lab network.



Color Mapping By DSCP

■ 0 (BE)
*3 MB / 25 flows

■ 18 (AF21)

■ 26 (AF31)
*5 MB / 4 flows

■ 34 (AF41)

■ 16 (CS2)

■ 24 (CS3)

■ 32 (CS4)

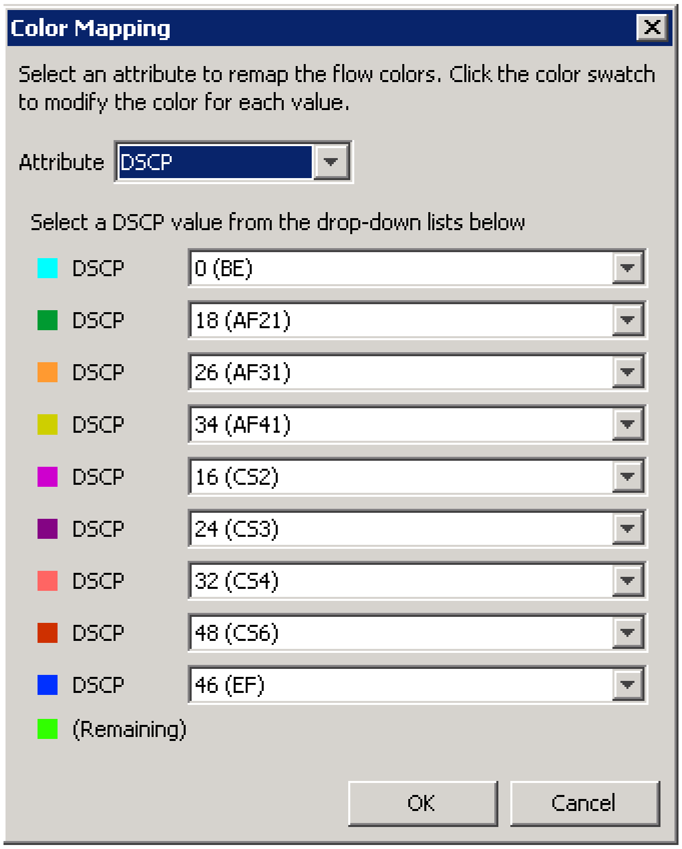
■ 48 (CS6)
*6 KB / 16 flows

■ 46 (EF)
*4 MB / 2 flows

■ Remaining
*15 MB / 4 flows

5. Select the icon to update the legend.

The Color Mapping dialog will appear.



**Color Mapping**

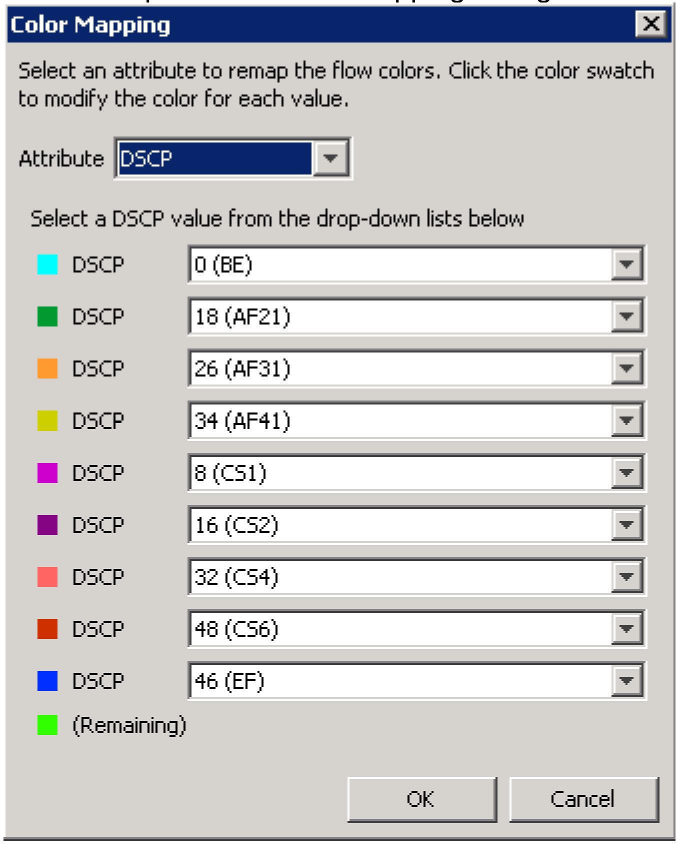
Select an attribute to remap the flow colors. Click the color swatch to modify the color for each value.

Attribute: DSCP

Select a DSCP value from the drop-down lists below

🟦 DSCP: 0 (BE)
🟩 DSCP: 18 (AF21)
🟧 DSCP: 26 (AF31)
🟨 DSCP: 34 (AF41)
🟪 DSCP: 16 (CS2)
🟪 DSCP: 24 (CS3)
🟥 DSCP: 32 (CS4)
🟥 DSCP: 48 (CS6)
🟦 DSCP: 46 (EF)
🟩 (Remaining)

6. Update the Color Mapping dialog as shown below.



**Color Mapping**

Select an attribute to remap the flow colors. Click the color swatch to modify the color for each value.

Attribute: DSCP

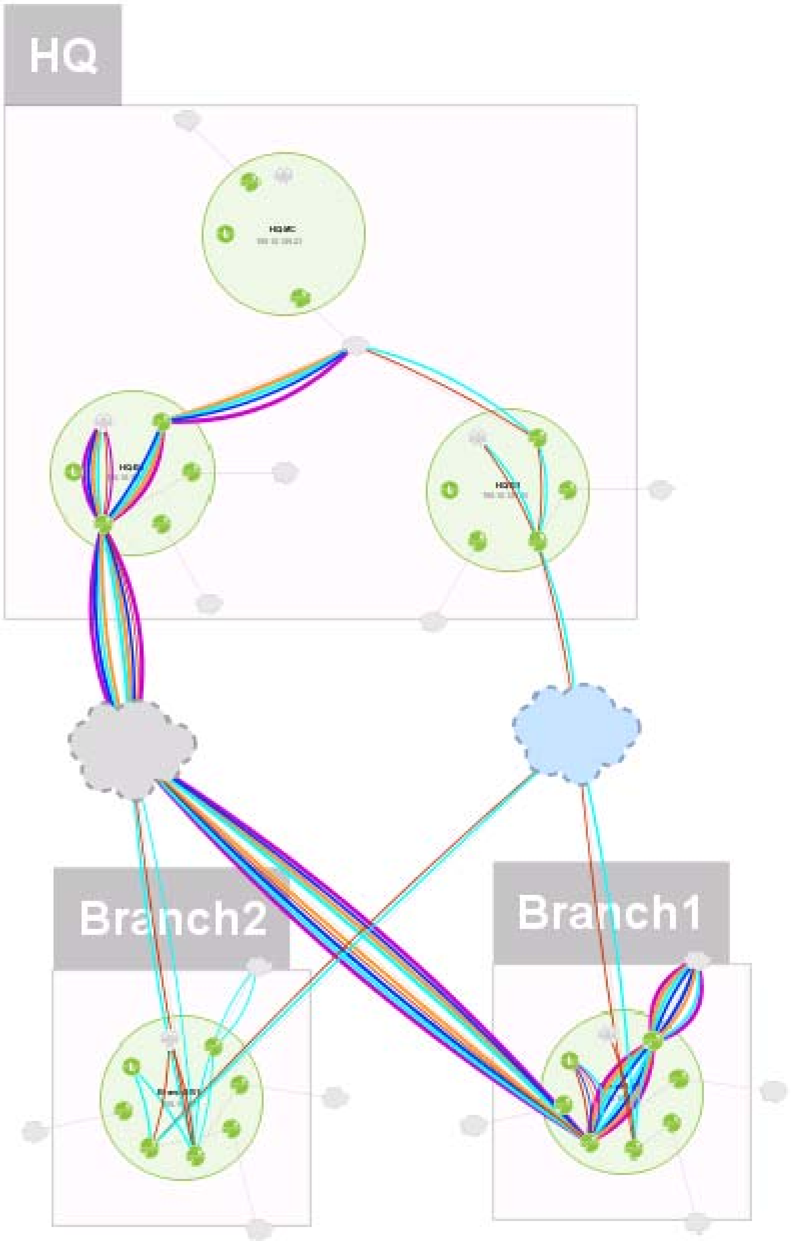
Select a DSCP value from the drop-down lists below

🟦 DSCP: 0 (BE)
🟩 DSCP: 18 (AF21)
🟧 DSCP: 26 (AF31)
🟨 DSCP: 34 (AF41)
🟪 DSCP: 8 (CS1)
🟪 DSCP: 16 (CS2)
🟥 DSCP: 32 (CS4)
🟥 DSCP: 48 (CS6)
🟦 DSCP: 46 (EF)
🟩 (Remaining)

Note the legend is now updated to the DSCP values used by this network. Note there is no “Remaining” Flow, it has all be accounted for in the legend.

Color Mapping By DSCP

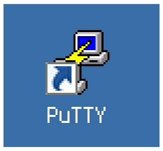
- 🟦 0 (BE)
  *4 MB / 58 flows
- 🟩 18 (AF21)
- 🟧 26 (AF31)
  *186 KB / 2 flows
- 🟨 34 (AF41)
- 🟪 8 (CS1)
  *432 B / 1 flow
- 🟪 16 (CS2)
- 🟥 32 (CS4)
- 🟥 48 (CS6)
  *334 KB / 15 flows
- 🟦 46 (EF)
  *288 B / 1 flow
- 🟩 Remaining



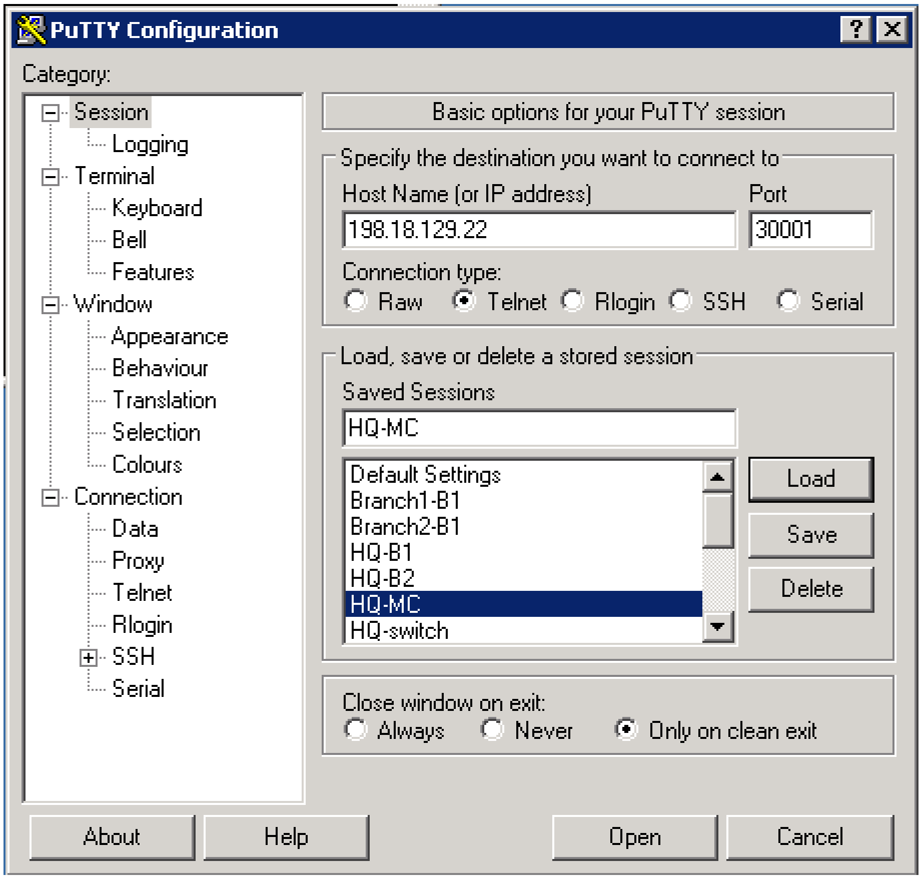
# Lab 8.7: Update Master Controller

Next, the PfR master controller needs to be updated to send PfR log data as NetFlow to LiveNX.

1. From the client PC, minimize the LiveNX client, and open Putty



2. Load HQ-MC or Telnet  to HQ-MC:
   a. IP Address = 198.18.129.22
   b. Port = 30001
   c. Username = admin
   d. Password = C1sco12345



Specify the destination you want to connect to

Host Name (or IP address): 198.18.129.22

Port: 30001

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

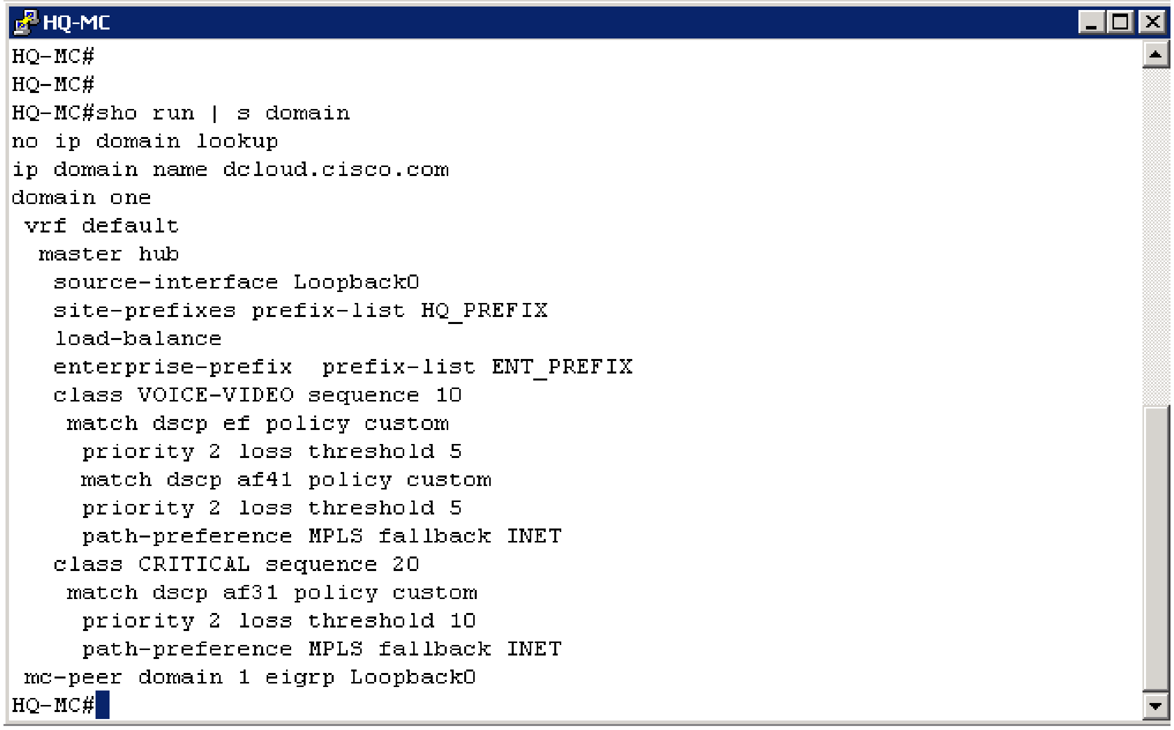
Load, save or delete a stored session

Saved Sessions: HQ-MC

Default Settings
Branch1-B1
Branch2-B1
HQ-B1
HQ-B2
HQ-MC
HQ-switch

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. run the command “show run | s domain”

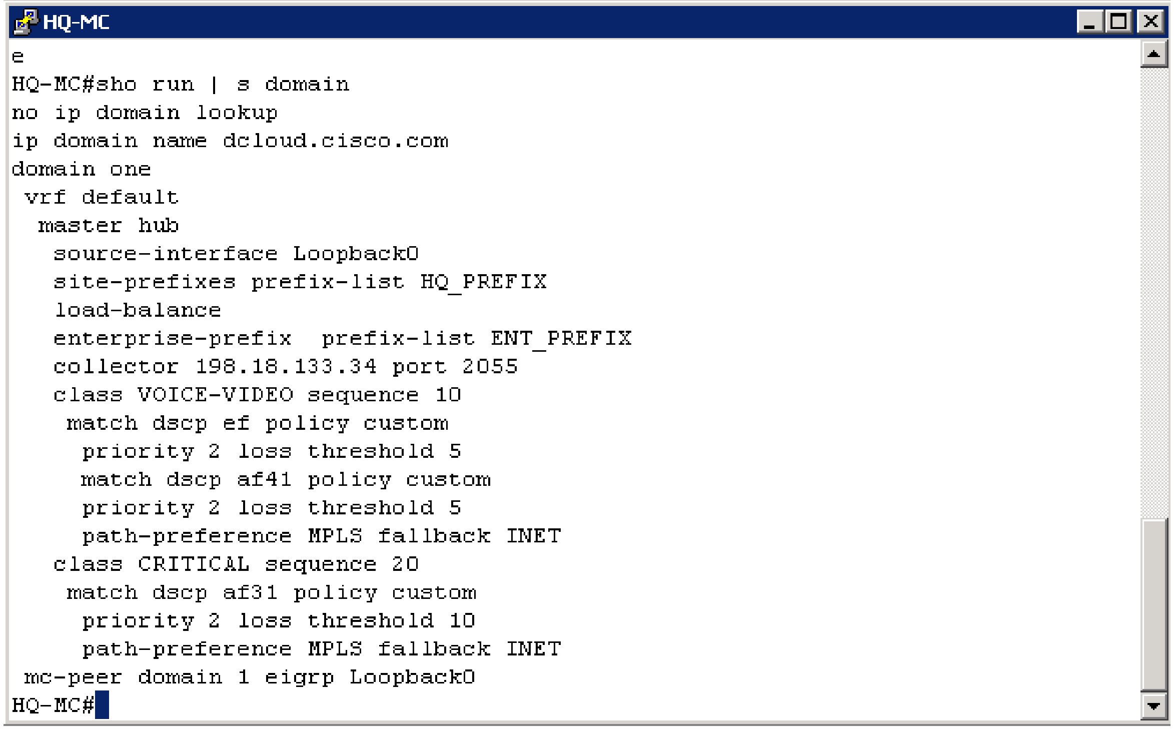


```
HQ-MC#
HQ-MC#
HQ-MC#sho run | s domain
no ip domain lookup
ip domain name dcloud.cisco.com
domain one
 vrf default
  master hub
   source-interface Loopback0
   site-prefixes prefix-list HQ_PREFIX
   load-balance
   enterprise-prefix  prefix-list ENT_PREFIX
   class VOICE-VIDEO sequence 10
    match dscp ef policy custom
     priority 2 loss threshold 5
     match dscp af41 policy custom
     priority 2 loss threshold 5
     path-preference MPLS fallback INET
   class CRITICAL sequence 20
    match dscp af31 policy custom
     priority 2 loss threshold 10
     path-preference MPLS fallback INET
 mc-peer domain 1 eigrp Loopback0
HQ-MC#
```

4. add the following configuration:

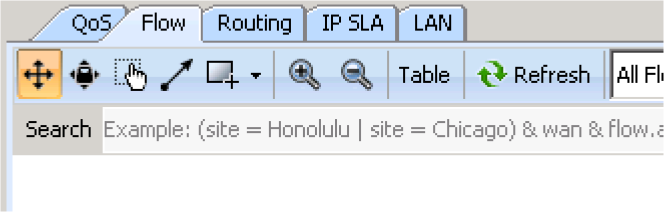
```
config t
domain one
vrf default
master hub
collector 198.18.133.34 port 2055
end
wr
```

5. After implementing these commands, re-issue “show run | s domain”

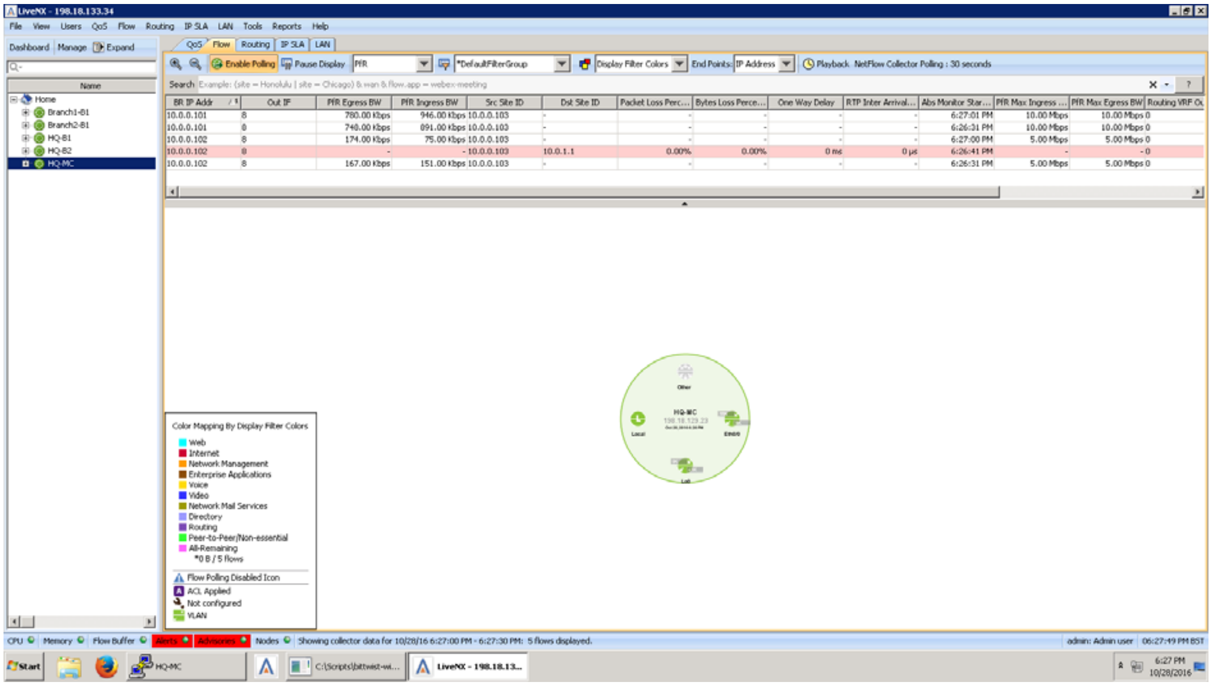


```
e
HQ-MC#sho run | s domain
no ip domain lookup
ip domain name dcloud.cisco.com
domain one
 vrf default
  master hub
   source-interface Loopback0
   site-prefixes prefix-list HQ_PREFIX
   load-balance
   enterprise-prefix  prefix-list ENT_PREFIX
   collector 198.18.133.34 port 2055
   class VOICE-VIDEO sequence 10
    match dscp ef policy custom
     priority 2 loss threshold 5
     match dscp af41 policy custom
     priority 2 loss threshold 5
     path-preference MPLS fallback INET
   class CRITICAL sequence 20
    match dscp af31 policy custom
     priority 2 loss threshold 10
     path-preference MPLS fallback INET
 mc-peer domain 1 eigrp Loopback0
HQ-MC#
```

6. From the LiveNX map, select the Flow tab



7. Double-click on one of the routers
8. Set the Flow type filter to PfR
9. Confirm PfR Flow data  is visable as in the example below shows.

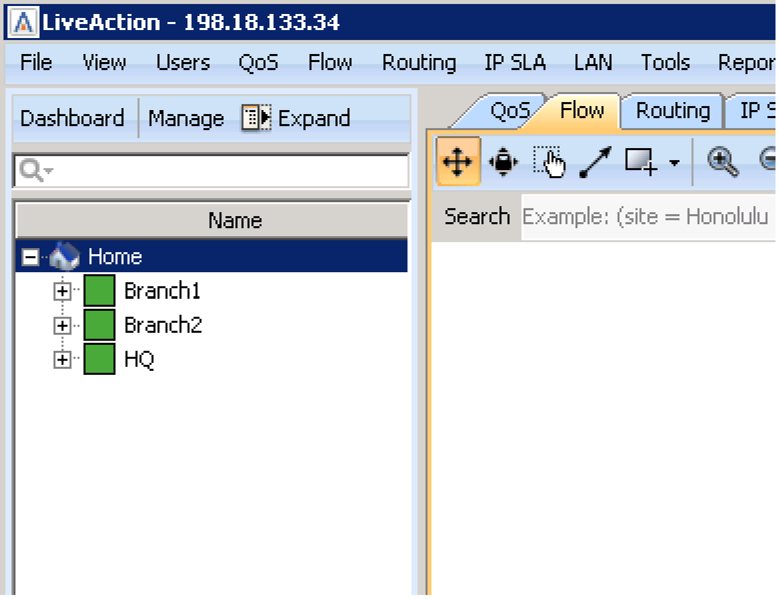


| BR IP Addr | Out IF | PfR Egress BW | PfR Ingress BW | Src Site ID | Dst Site ID | Packet Loss Perc... | Bytes Loss Perce... | One Way Delay | RTP Inter Arrival... | Abs Monitor Star... | PfR Max Ingress ... | PfR Max Egress BW | Routing VRF Ou |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.0.0.101 | 8 | 780.00 Kbps | 946.00 Kbps | 10.0.0.103 | - | - | - | - | - | 6:27:01 PM | 10.00 Mbps | 10.00 Mbps | 0 |
| 10.0.0.101 | 8 | 740.00 Kbps | 891.00 Kbps | 10.0.0.103 | - | - | - | - | - | 6:26:31 PM | 10.00 Mbps | 10.00 Mbps | 0 |
| 10.0.0.102 | 8 | 174.00 Kbps | 75.00 Kbps | 10.0.0.103 | - | - | - | - | - | 6:27:00 PM | 5.00 Mbps | 5.00 Mbps | 0 |
| 10.0.0.102 | 8 | - | - | 10.0.0.103 | 10.0.1.1 | 0.00% | 0.00% | 0 ms | 0 µs | 6:26:41 PM | - | - | 0 |
| 10.0.0.102 | 8 | 167.00 Kbps | 151.00 Kbps | 10.0.0.103 | - | - | - | - | - | 6:26:31 PM | 5.00 Mbps | 5.00 Mbps | 0 |

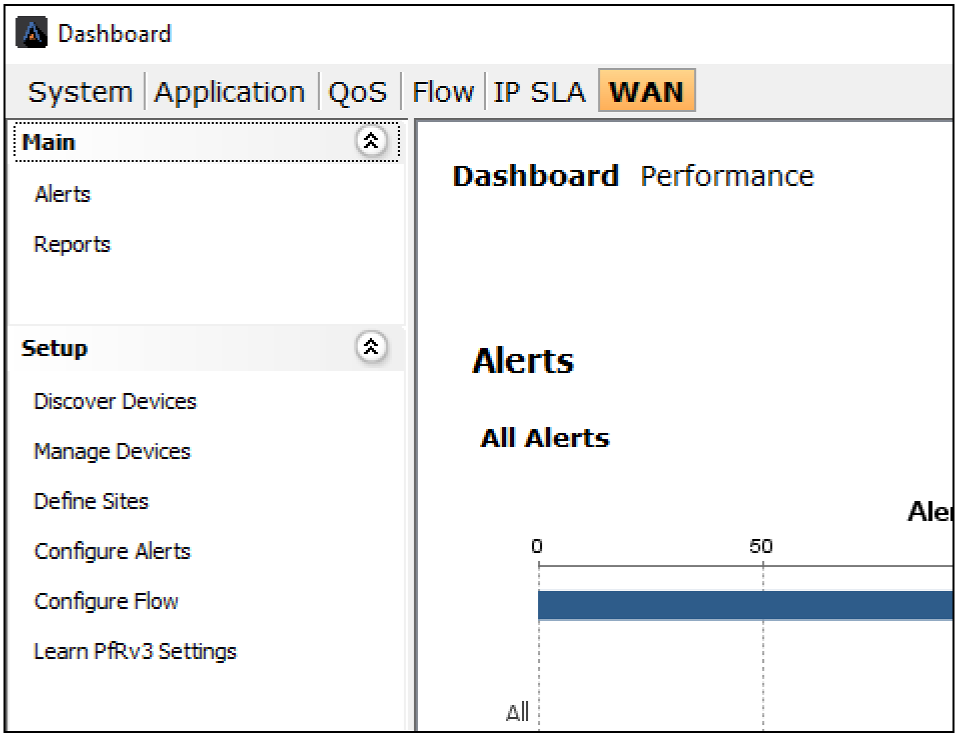
Showing collector data for 10/28/16 6:27:00 PM - 6:27:30 PM: 5 flows displayed.

After NetFlow is configured in the Network, the PfR dashboard needs to be configured.

1. From the LiveNX client, select the Dashboard

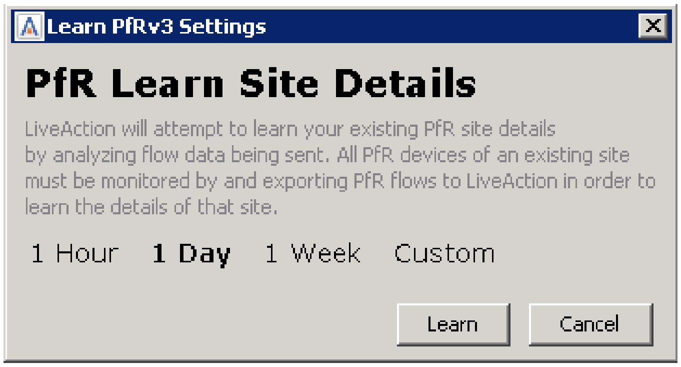

LiveAction - 198.18.133.34
File View Users QoS Flow Routing IP SLA LAN Tools Repor
Dashboard Manage Expand
Name
Home
Branch1
Branch2
HQ
QoS Flow Routing IP S
Search Example: (site = Honolulu

2. The Dashboard will open, select the WAN Dashboard.



3. From the WAN dashboard, select “Learn PfRv3 Settings”

4. The Learn PfRv3 Settings dialog will open. Choose 1 day and Learn.

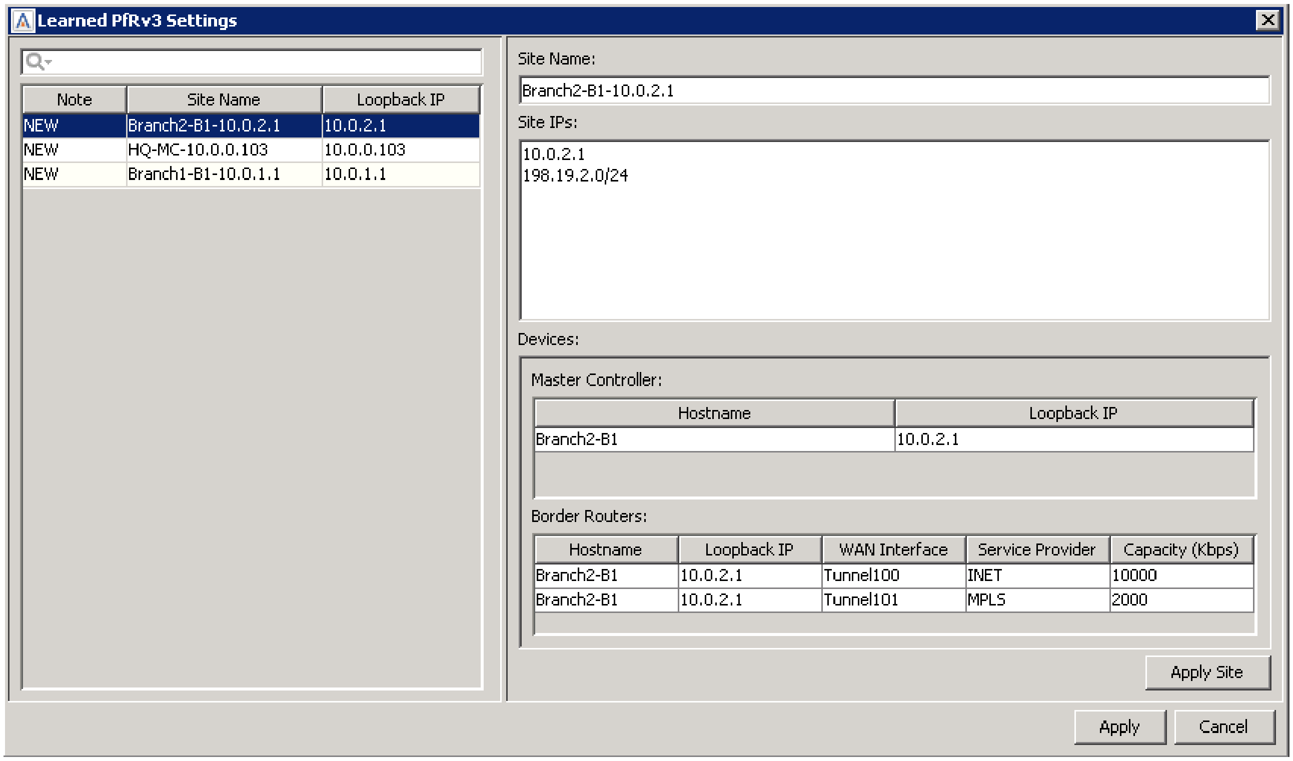


Learn PfRv3 Settings

PfR Learn Site Details

LiveAction will attempt to learn your existing PfR site details by analyzing flow data being sent. All PfR devices of an existing site must be monitored by and exporting PfR flows to LiveAction in order to learn the details of that site.

LiveNX will discover more semantic details about environment.



Learned PfRv3 Settings

| Note | Site Name | Loopback IP |
|---|---|---|
| NEW | Branch2-B1-10.0.2.1 | 10.0.2.1 |
| NEW | HQ-MC-10.0.0.103 | 10.0.0.103 |
| NEW | Branch1-B1-10.0.1.1 | 10.0.1.1 |

Site Name: Branch2-B1-10.0.2.1

Site IPs:

10.0.2.1
198.19.2.0/24

Devices:

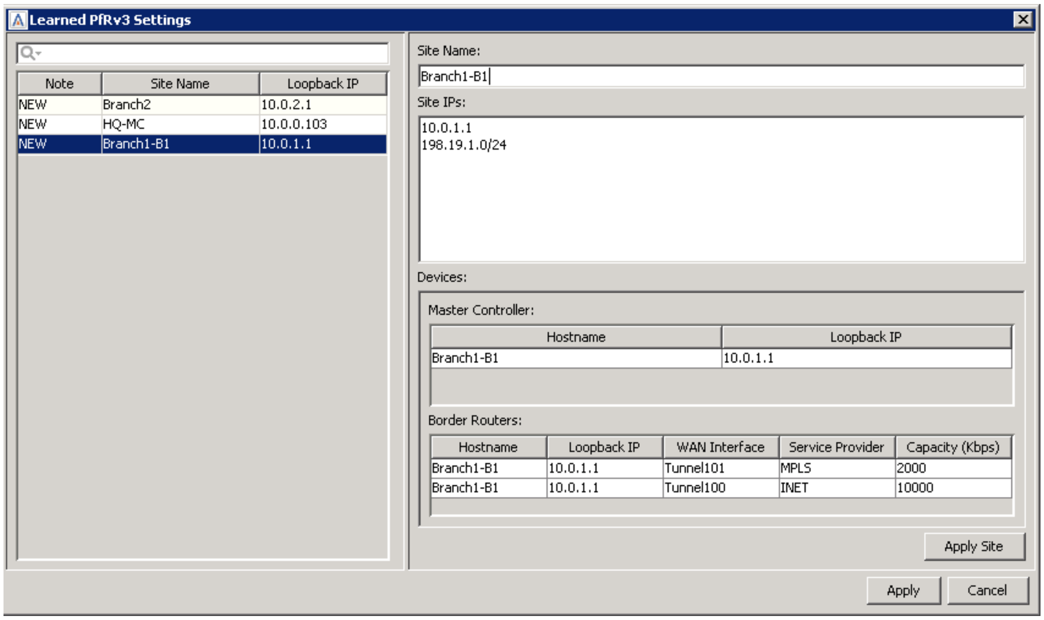
Master Controller:

| Hostname | Loopback IP |
|---|---|
| Branch2-B1 | 10.0.2.1 |

Border Routers:

| Hostname | Loopback IP | WAN Interface | Service Provider | Capacity (Kbps) |
|---|---|---|---|---|
| Branch2-B1 | 10.0.2.1 | Tunnel100 | INET | 10000 |
| Branch2-B1 | 10.0.2.1 | Tunnel101 | MPLS | 2000 |

5. Update the Site Name as follows:
   a. Branch2 = 10.0.2.1
   b. HQ-MC = 10.0.0.100
   c. Branch1 = 10.0.1.1
6. Select Apply.



| Note | Site Name | Loopback IP |
|---|---|---|
| NEW | Branch2 | 10.0.2.1 |
| NEW | HQ-MC | 10.0.0.103 |
| NEW | Branch1-B1 | 10.0.1.1 |

Site Name: Branch1-B1

Site IPs:
10.0.1.1
198.19.1.0/24

Devices:

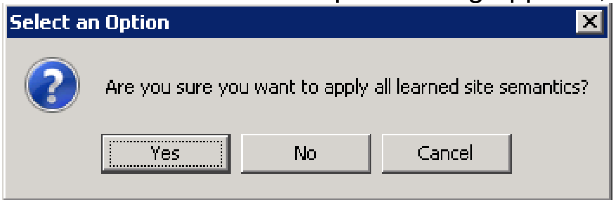
Master Controller:

| Hostname | Loopback IP |
|---|---|
| Branch1-B1 | 10.0.1.1 |

Border Routers:

| Hostname | Loopback IP | WAN Interface | Service Provider | Capacity (Kbps) |
|---|---|---|---|---|
| Branch1-B1 | 10.0.1.1 | Tunnel101 | MPLS | 2000 |
| Branch1-B1 | 10.0.1.1 | Tunnel100 | INET | 10000 |

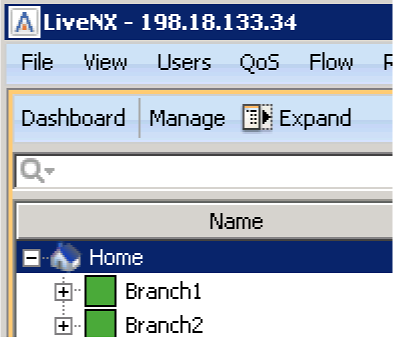
7. The Select an Option dialog appears, select Yes



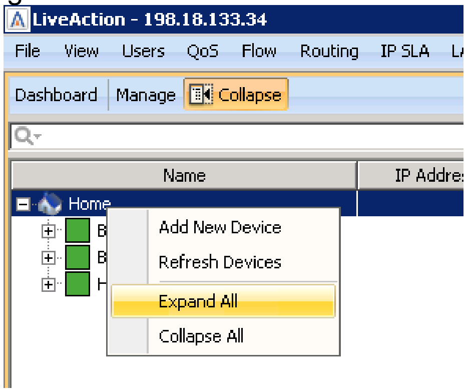
Are you sure you want to apply all learned site semantics?

8. Close the dashboard.

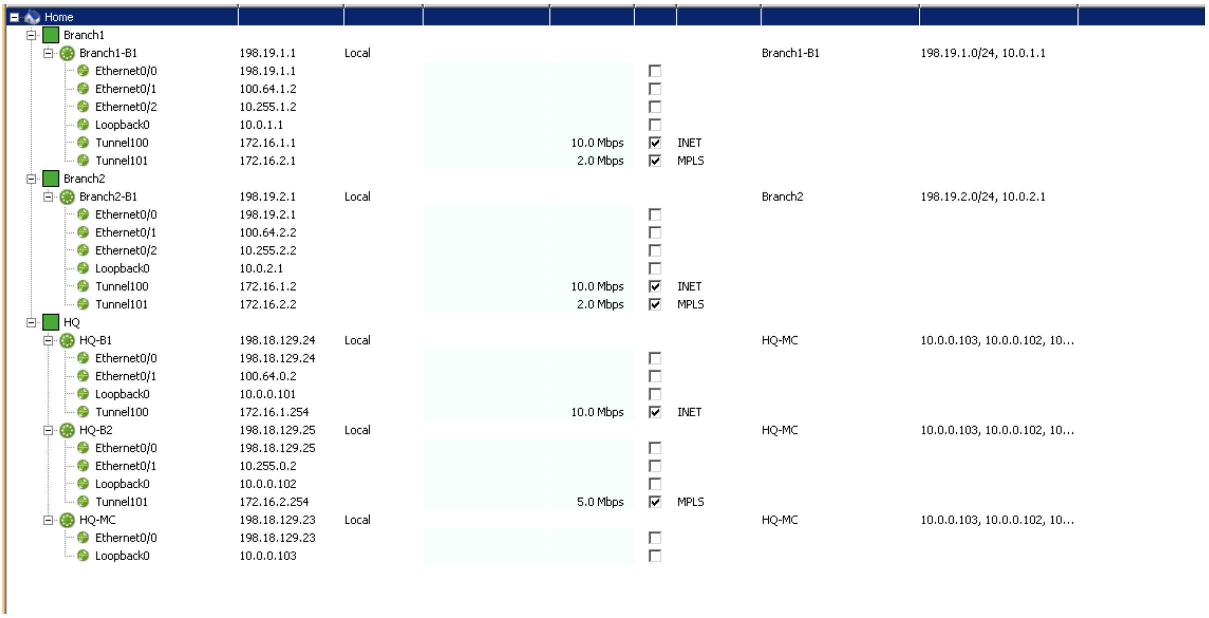
9. Select the Expand button at the top left of the LiveNX client.



10. Right-Click on the Home icon and select Expand all



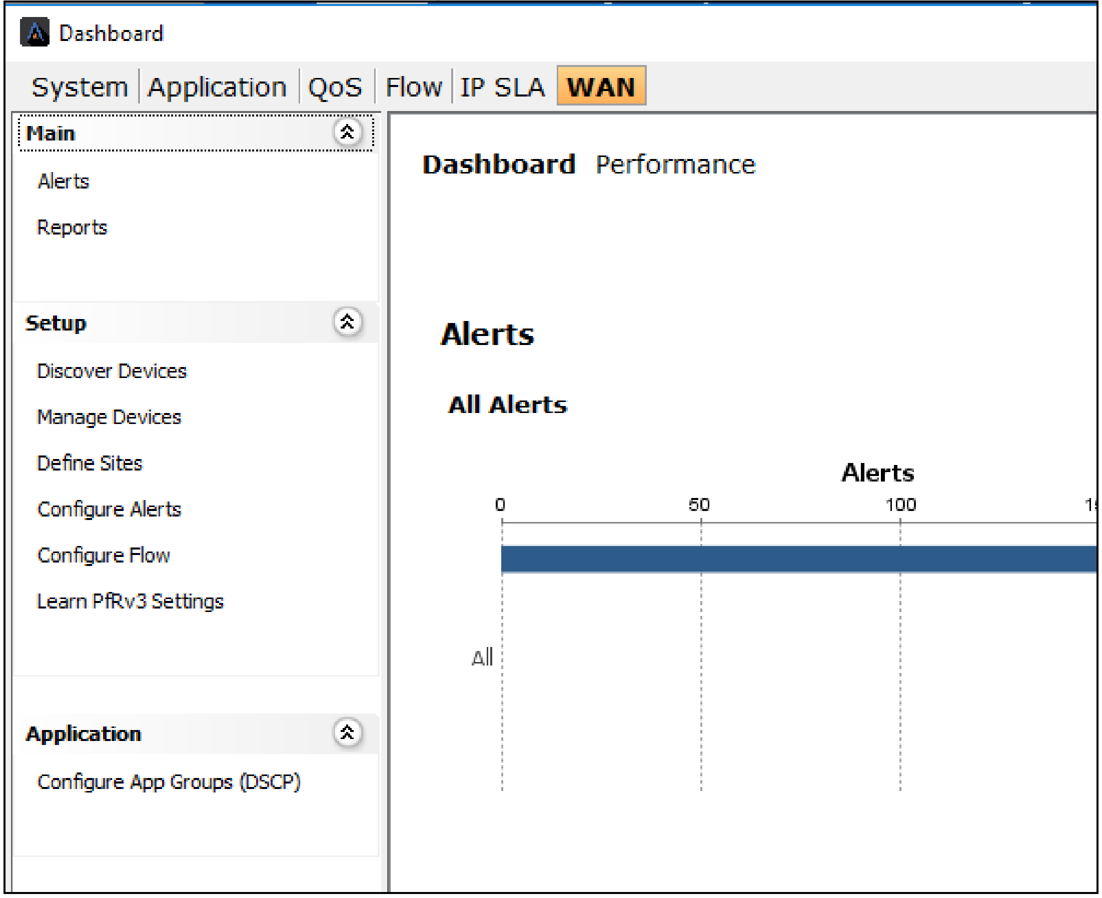
Note the semantic data that has been learned – capacity, WAN, Sites and IP networks



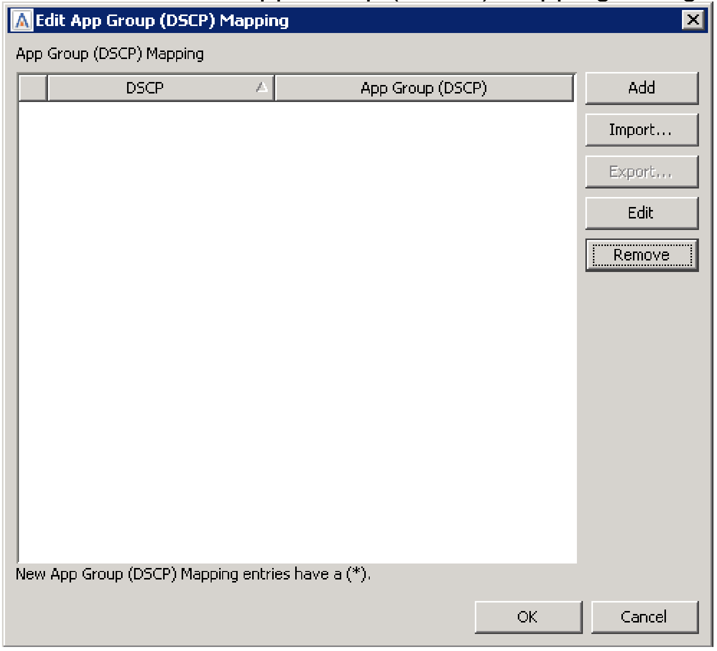
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Home | | | | | | | |
| Branch1 | | | | | | | |
| Branch1-B1 | 198.19.1.1 | Local | | | | Branch1-B1 | 198.19.1.0/24, 10.0.1.1 |
| Ethernet0/0 | 198.19.1.1 | | | ☐ | | | |
| Ethernet0/1 | 100.64.1.2 | | | ☐ | | | |
| Ethernet0/2 | 10.255.1.2 | | | ☐ | | | |
| Loopback0 | 10.0.1.1 | | | ☐ | | | |
| Tunnel100 | 172.16.1.1 | | 10.0 Mbps | ☑ | INET | | |
| Tunnel101 | 172.16.2.1 | | 2.0 Mbps | ☑ | MPLS | | |
| Branch2 | | | | | | | |
| Branch2-B1 | 198.19.2.1 | Local | | | | Branch2 | 198.19.2.0/24, 10.0.2.1 |
| Ethernet0/0 | 198.19.2.1 | | | ☐ | | | |
| Ethernet0/1 | 100.64.2.2 | | | ☐ | | | |
| Ethernet0/2 | 10.255.2.2 | | | ☐ | | | |
| Loopback0 | 10.0.2.1 | | | ☐ | | | |
| Tunnel100 | 172.16.1.2 | | 10.0 Mbps | ☑ | INET | | |
| Tunnel101 | 172.16.2.2 | | 2.0 Mbps | ☑ | MPLS | | |
| HQ | | | | | | | |
| HQ-B1 | 198.18.129.24 | Local | | | | HQ-MC | 10.0.0.103, 10.0.0.102, 10... |
| Ethernet0/0 | 198.18.129.24 | | | ☐ | | | |
| Ethernet0/1 | 100.64.0.2 | | | ☐ | | | |
| Loopback0 | 10.0.0.101 | | | ☐ | | | |
| Tunnel100 | 172.16.1.254 | | 10.0 Mbps | ☑ | INET | | |
| HQ-B2 | 198.18.129.25 | Local | | | | HQ-MC | 10.0.0.103, 10.0.0.102, 10... |
| Ethernet0/0 | 198.18.129.25 | | | ☐ | | | |
| Ethernet0/1 | 10.255.0.2 | | | ☐ | | | |
| Loopback0 | 10.0.0.102 | | | ☐ | | | |
| Tunnel101 | 172.16.2.254 | | 5.0 Mbps | ☑ | MPLS | | |
| HQ-MC | 198.18.129.23 | Local | | | | HQ-MC | 10.0.0.103, 10.0.0.102, 10... |
| Ethernet0/0 | 198.18.129.23 | | | ☐ | | | |
| Loopback0 | 10.0.0.103 | | | ☐ | | | |

Return to the PfR dashboard to configure PfRv3 Application Groups.

1. From the LiveNX client, select the Dashboard
2. The Dashboard will re-open, select the WAN Dashboard.



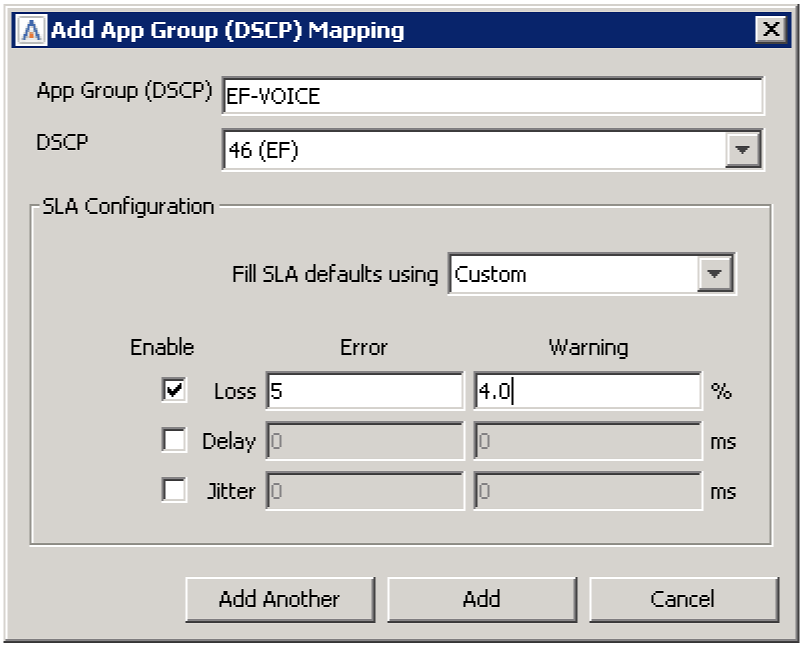
3. Select Configure App Groups (DSCP)
4. The Edit App Group (DSCP) Mapping dialog will appear, select Add.



New App Group (DSCP) Mapping entries have a (*).

The Add App Group (DSCP) mapping dialog will appear.

5. Populate the following data:
   a. App Group (DSCP) = EF-VOICE
   b. DSCP = 47
   c. Fill SLA defaults using = Custom
   d. Loss = 5.0 / 4.0
   e. Delay = N/A
   f. Jitter = N/A



Add App Group (DSCP) Mapping

App Group (DSCP): EF-VOICE

DSCP: 46 (EF)

SLA Configuration

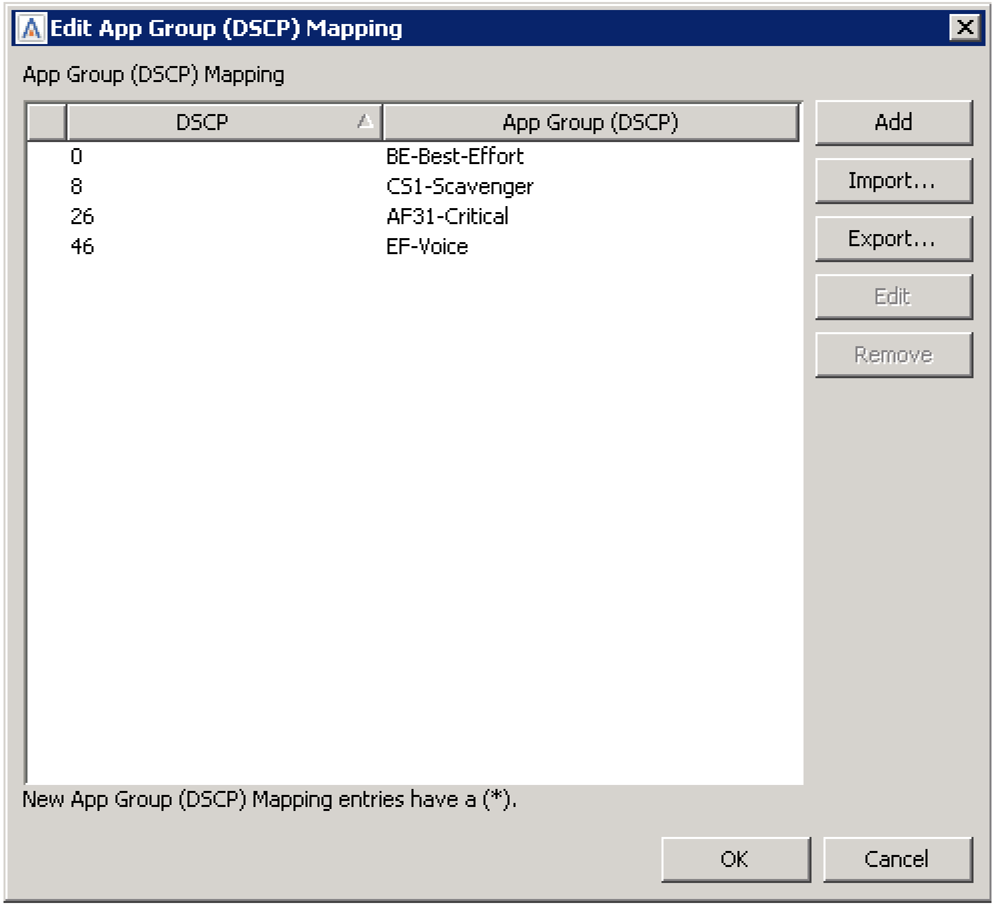
Fill SLA defaults using: Custom

| Enable | | Error | Warning | |
|---|---|---|---|---|
| ☑ | Loss | 5 | 4.0 | % |
| ☐ | Delay | 0 | 0 | ms |
| ☐ | Jitter | 0 | 0 | ms |

6. Select Add Another.
7. Create the following application groups based on the table below:

| App Group | Fill SLA default using | DSCP | Loss | Delay | Jitter |
|---|---|---|---|---|---|
| EF-VOICE | Custom | 47 (EF) | 5.0 / 4.0 | *n/a* | *n/a* |
| AF31-Critical | Custom | 26 (AF31) | 7.0 / 5.6 | *n/a* | *n/a* |
| CS1-Scavenger | Custom | 8 (CS1) | *n/a* | *n/a* | *n/a* |
| BE-Default | Custom | 0 (BE) | 10.0 / 8.0 | 500/400 | *n/a* |

When finished, the Edit App Group (DSCP) Mapping will appear as follows:



Edit App Group (DSCP) Mapping

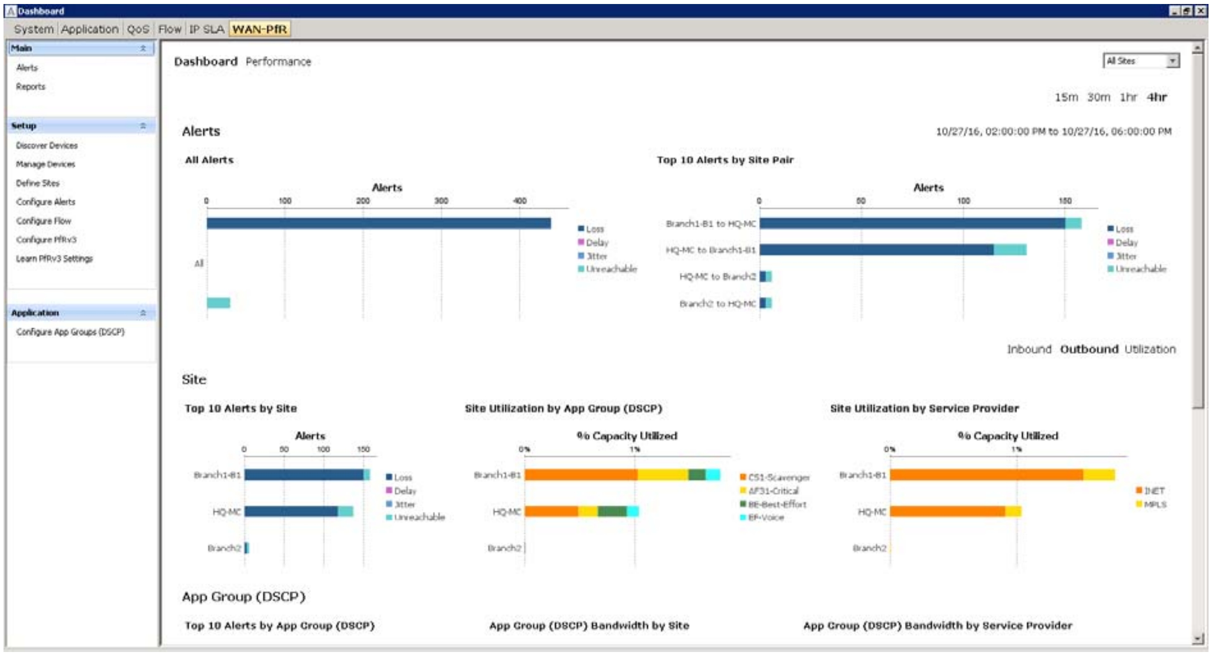
App Group (DSCP) Mapping

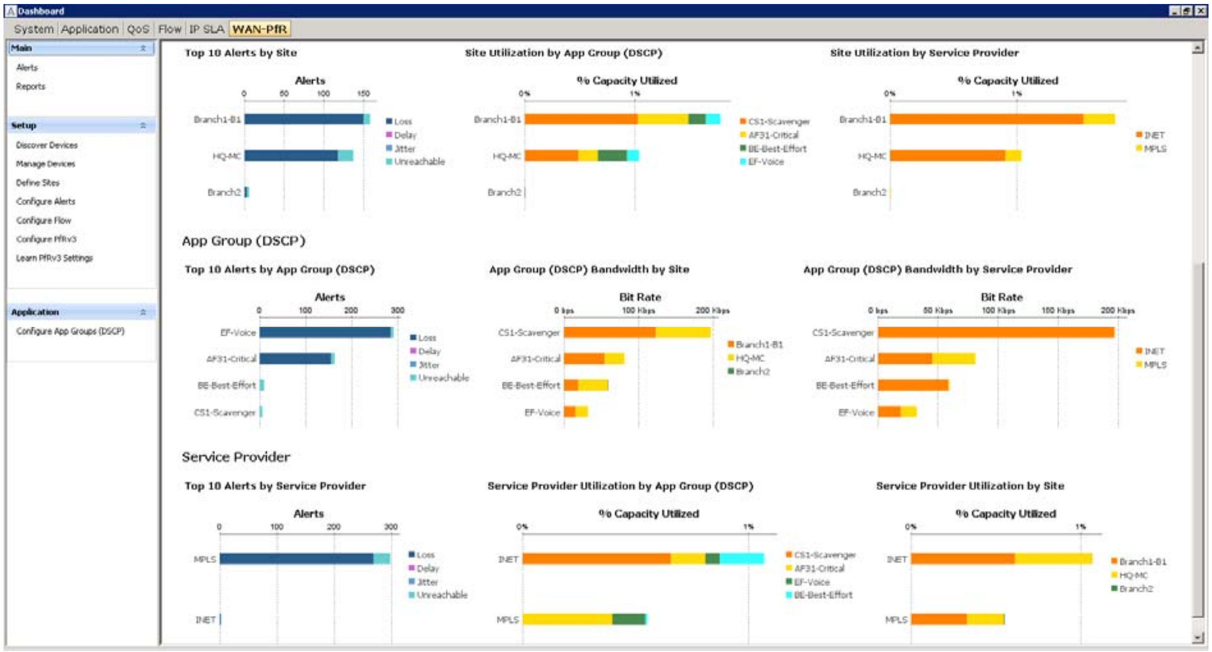
| DSCP | App Group (DSCP) |
|---|---|
| 0 | BE-Best-Effort |
| 8 | CS1-Scavenger |
| 26 | AF31-Critical |
| 46 | EF-Voice |

New App Group (DSCP) Mapping entries have a (*).

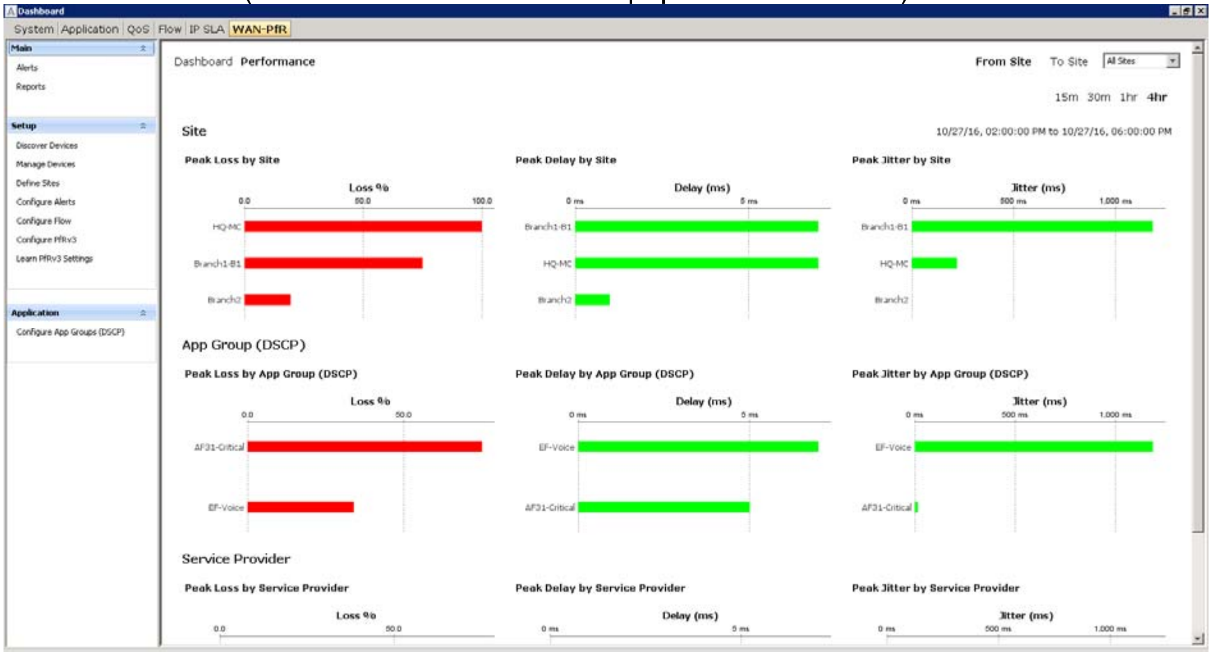
The PfR-WAN dashboard will begin to populate (this may  take 15 Minutes to populate the 1st time).  Below are a couple of screenshots of this dashboard.

Note the Dashboard/ Performance options at the top left of the window. The dashboard will show alerts and bandwidth utilization of the IWAN environment.



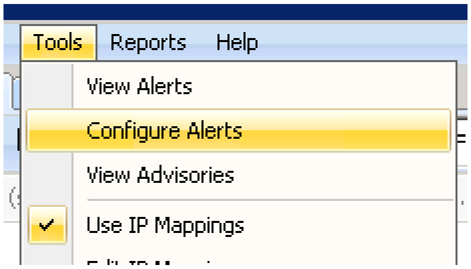


8. Select the Performance link. The dashboard will show the performance statistics of the network. (this make take 15 Minute  to populate the 1st time )



Validate PfR Alerting is enabled.

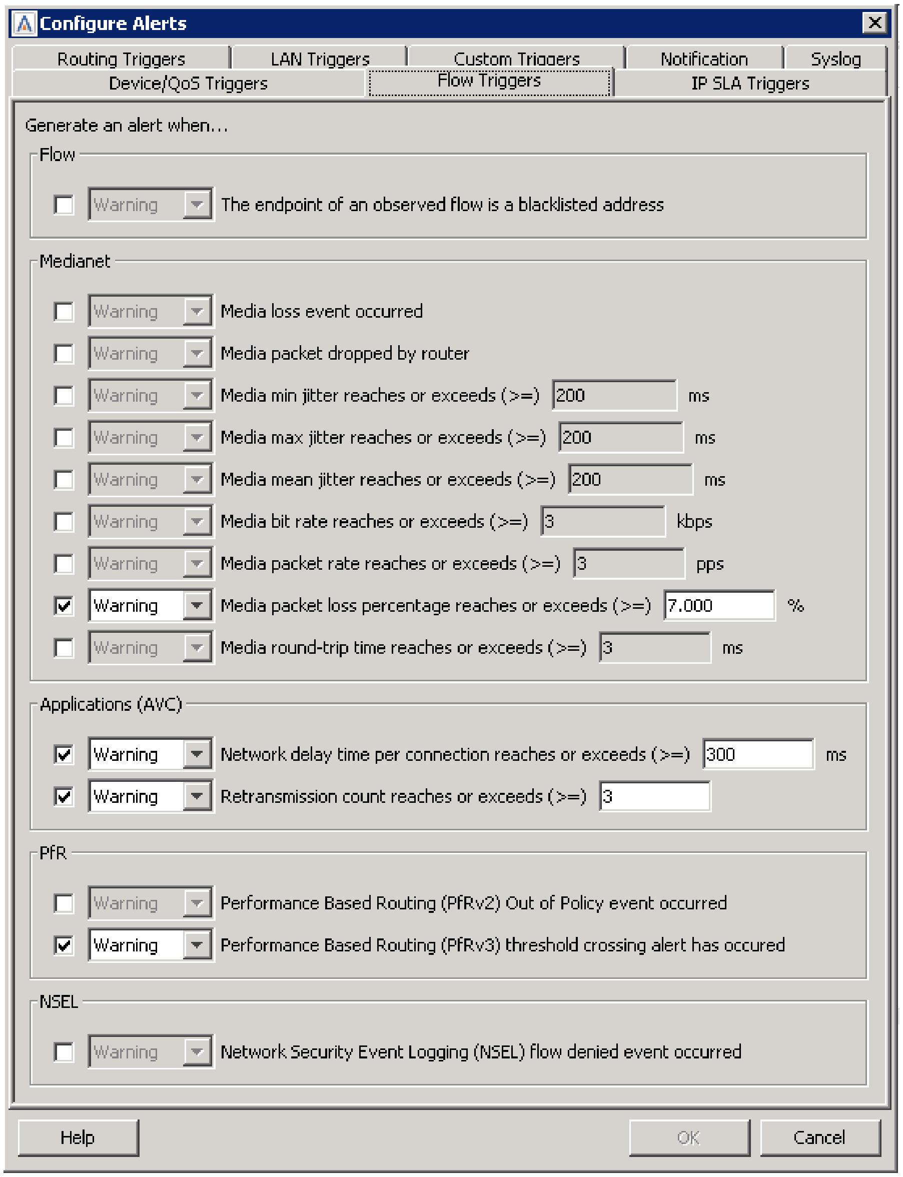
9. Select  Tools > Configure Alerts



The Configure Alert dialog will open.

10. Select the Flow Triggers tab

11. Ensure PfRv3 Alerts are selected.



Generate an alert when...

Flow

- ☐ Warning The endpoint of an observed flow is a blacklisted address

Medianet

- ☐ Warning Media loss event occurred
- ☐ Warning Media packet dropped by router
- ☐ Warning Media min jitter reaches or exceeds (>=) 200 ms
- ☐ Warning Media max jitter reaches or exceeds (>=) 200 ms
- ☐ Warning Media mean jitter reaches or exceeds (>=) 200 ms
- ☐ Warning Media bit rate reaches or exceeds (>=) 3 kbps
- ☐ Warning Media packet rate reaches or exceeds (>=) 3 pps
- ☑ Warning Media packet loss percentage reaches or exceeds (>=) 7.000 %
- ☐ Warning Media round-trip time reaches or exceeds (>=) 3 ms

Applications (AVC)

- ☑ Warning Network delay time per connection reaches or exceeds (>=) 300 ms
- ☑ Warning Retransmission count reaches or exceeds (>=) 3

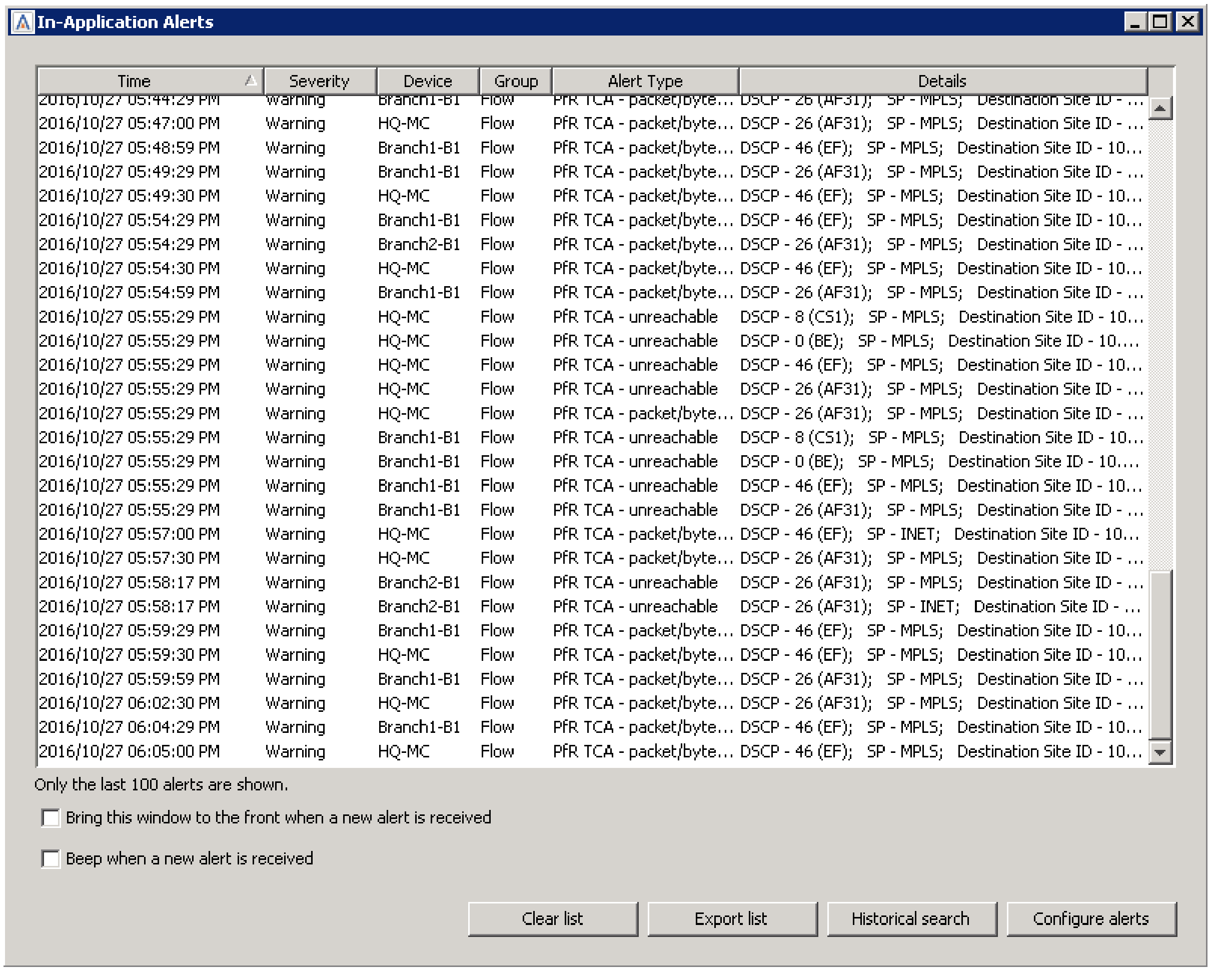
PfR

- ☐ Warning Performance Based Routing (PfRv2) Out of Policy event occurred
- ☑ Warning Performance Based Routing (PfRv3) threshold crossing alert has occured

NSEL

- ☐ Warning Network Security Event Logging (NSEL) flow denied event occurred

If PfRv3 alerting is enabled, the In-Application Alerts will show PfRv3 TCA alerts. Below is an example.



| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/27 05:44:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:47:00 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:48:59 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:49:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:49:30 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:54:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:54:29 PM | Warning | Branch2-B1 | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:54:30 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:54:59 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:55:29 PM | Warning | HQ-MC | Flow | PfR TCA - unreachable | DSCP - 8 (CS1); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:55:29 PM | Warning | HQ-MC | Flow | PfR TCA - unreachable | DSCP - 0 (BE); SP - MPLS; Destination Site ID - 10.… |
| 2016/10/27 05:55:29 PM | Warning | HQ-MC | Flow | PfR TCA - unreachable | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:55:29 PM | Warning | HQ-MC | Flow | PfR TCA - unreachable | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:55:29 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:55:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - unreachable | DSCP - 8 (CS1); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:55:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - unreachable | DSCP - 0 (BE); SP - MPLS; Destination Site ID - 10.… |
| 2016/10/27 05:55:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - unreachable | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:55:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - unreachable | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:57:00 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - INET; Destination Site ID - 10… |
| 2016/10/27 05:57:30 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:58:17 PM | Warning | Branch2-B1 | Flow | PfR TCA - unreachable | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 05:58:17 PM | Warning | Branch2-B1 | Flow | PfR TCA - unreachable | DSCP - 26 (AF31); SP - INET; Destination Site ID - … |
| 2016/10/27 05:59:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:59:30 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 05:59:59 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 06:02:30 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 26 (AF31); SP - MPLS; Destination Site ID - … |
| 2016/10/27 06:04:29 PM | Warning | Branch1-B1 | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |
| 2016/10/27 06:05:00 PM | Warning | HQ-MC | Flow | PfR TCA - packet/byte… | DSCP - 46 (EF); SP - MPLS; Destination Site ID - 10… |

Only the last 100 alerts are shown.

□ Bring this window to the front when a new alert is received

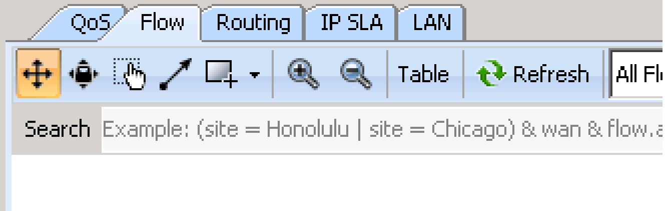
□ Beep when a new alert is received

# Lab 8.8: Setup PfRv3 Filters

Set up LiveNX Filters for PfRv3 for NetFlow reports and visualization. These Filters will be used to hide PfR Smart Probe data, to ensure the focus is on actual end-user traffic.

**Note: The filter configurations *may* already be in place as these devices were pre-configured. Verify the settings as described in these Labs.**

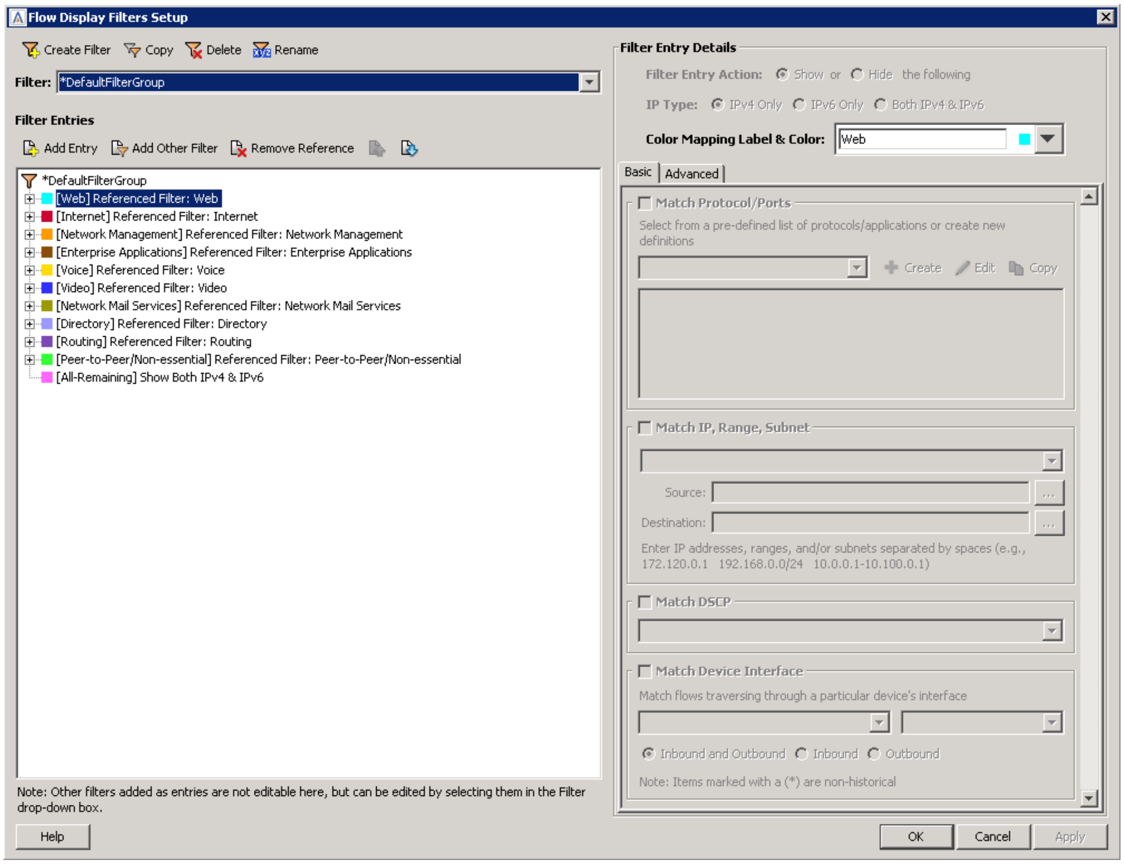
1. From the LiveNX map, select the Flow tab



Search Example: (site = Honolulu | site = Chicago) & wan & flow.a

2. From the LiveNX map, select the icon

The Flow Display Filter Setup dialog page opens



Filter: *DefaultFilterGroup

Filter Entries

- *DefaultFilterGroup
  - [Web] Referenced Filter: Web
  - [Internet] Referenced Filter: Internet
  - [Network Management] Referenced Filter: Network Management
  - [Enterprise Applications] Referenced Filter: Enterprise Applications
  - [Voice] Referenced Filter: Voice
  - [Video] Referenced Filter: Video
  - [Network Mail Services] Referenced Filter: Network Mail Services
  - [Directory] Referenced Filter: Directory
  - [Routing] Referenced Filter: Routing
  - [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
  - [All-Remaining] Show Both IPv4 & IPv6

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: Web

□ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

□ Match IP, Range, Subnet

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ Match DSCP

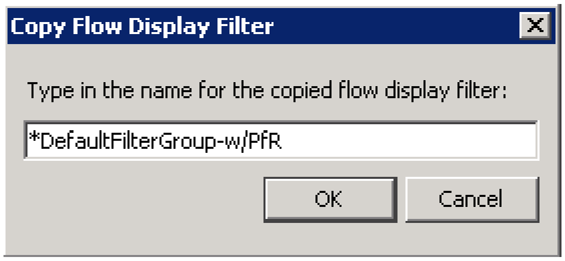
□ Match Device Interface

Match flows traversing through a particular device's interface

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

3. Select the copy Copy icon.
4. Name this copied *DefaultFilterGroup-w/PfR

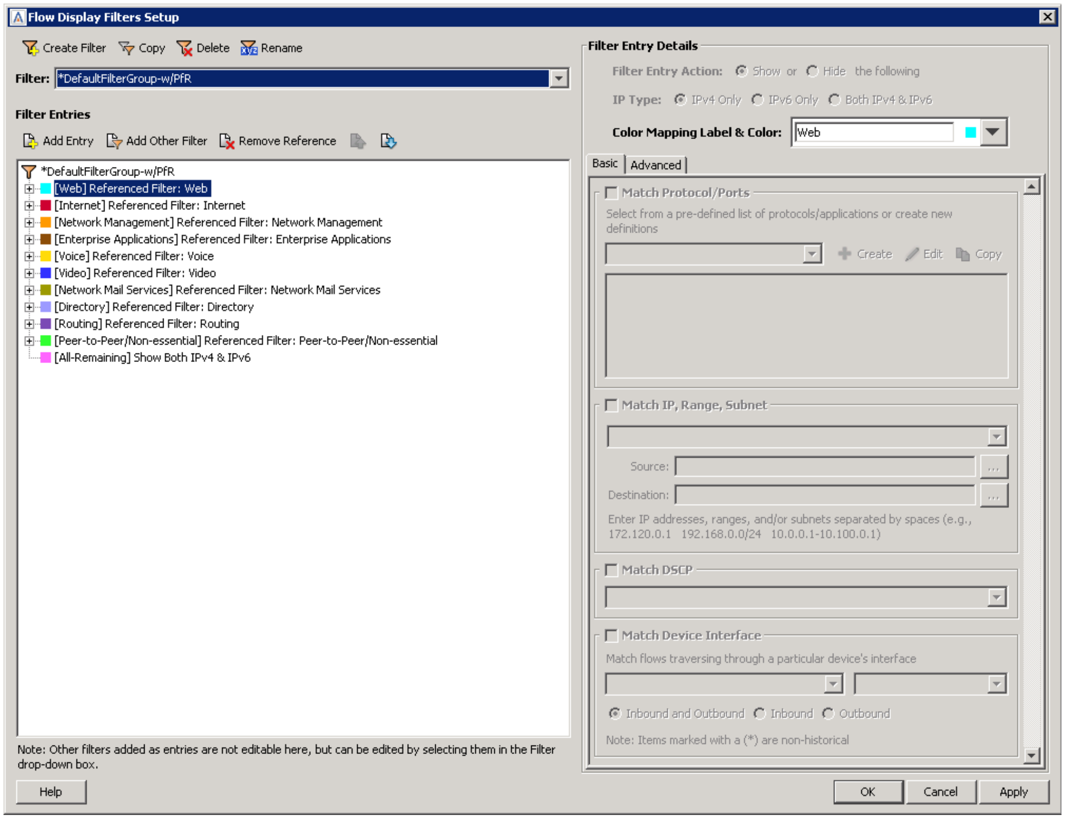


Copy Flow Display Filter

Type in the name for the copied flow display filter:

*DefaultFilterGroup-w/PfR

5. Change back to *DefaultFilterGroup



Flow Display Filters Setup

Filter: *DefaultFilterGroup-w/PfR

Filter Entries

- *DefaultFilterGroup-w/PfR
  - [Web] Referenced Filter: Web
  - [Internet] Referenced Filter: Internet
  - [Network Management] Referenced Filter: Network Management
  - [Enterprise Applications] Referenced Filter: Enterprise Applications
  - [Voice] Referenced Filter: Voice
  - [Video] Referenced Filter: Video
  - [Network Mail Services] Referenced Filter: Network Mail Services
  - [Directory] Referenced Filter: Directory
  - [Routing] Referenced Filter: Routing
  - [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
  - [All-Remaining] Show Both IPv4 & IPv6

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: Web

□ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

□ Match IP, Range, Subnet

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ Match DSCP

□ Match Device Interface

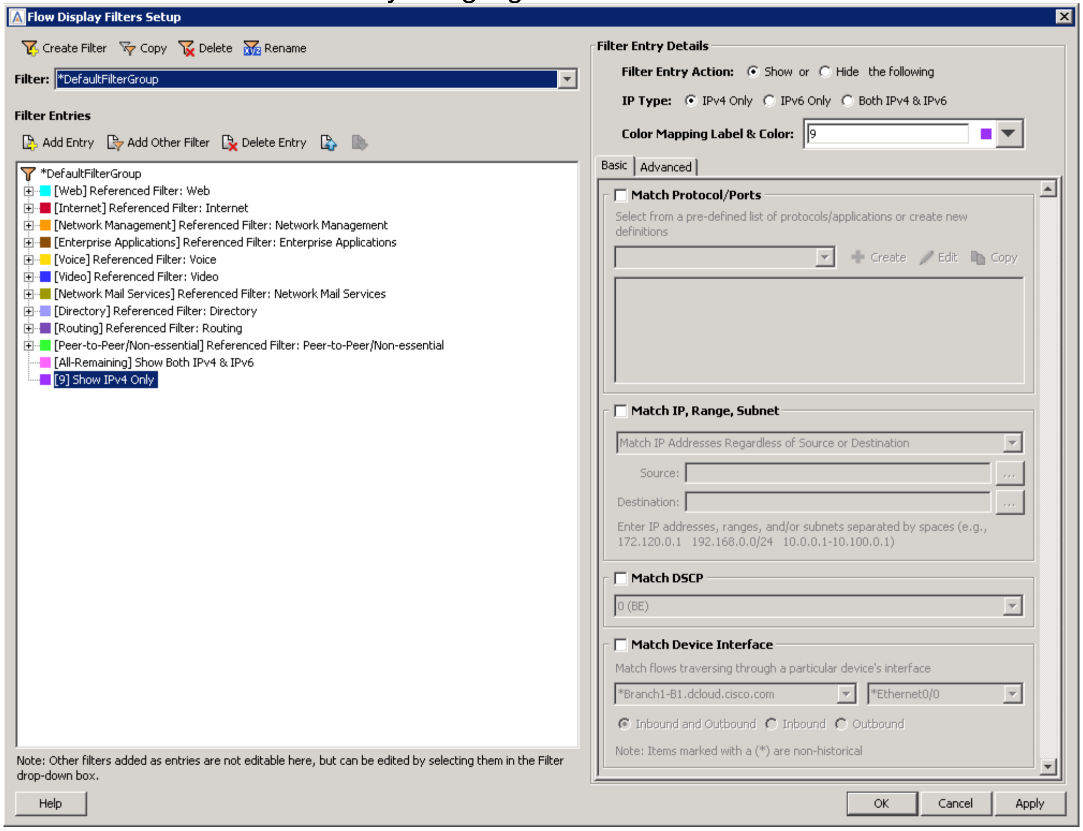
Match flows traversing through a particular device's interface

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

6. On the *DefaultFilterGroup, Select Add Entry.

7. Ensure the new entry is highlighted.



Flow Display Filters Setup

Filter: *DefaultFilterGroup

Filter Entries

- *DefaultFilterGroup
  - [Web] Referenced Filter: Web
  - [Internet] Referenced Filter: Internet
  - [Network Management] Referenced Filter: Network Management
  - [Enterprise Applications] Referenced Filter: Enterprise Applications
  - [Voice] Referenced Filter: Voice
  - [Video] Referenced Filter: Video
  - [Network Mail Services] Referenced Filter: Network Mail Services
  - [Directory] Referenced Filter: Directory
  - [Routing] Referenced Filter: Routing
  - [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
  - [All-Remaining] Show Both IPv4 & IPv6
  - [9] Show IPv4 Only

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: 9

□ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

□ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ Match DSCP

0 (BE)

□ Match Device Interface

Match flows traversing through a particular device's interface

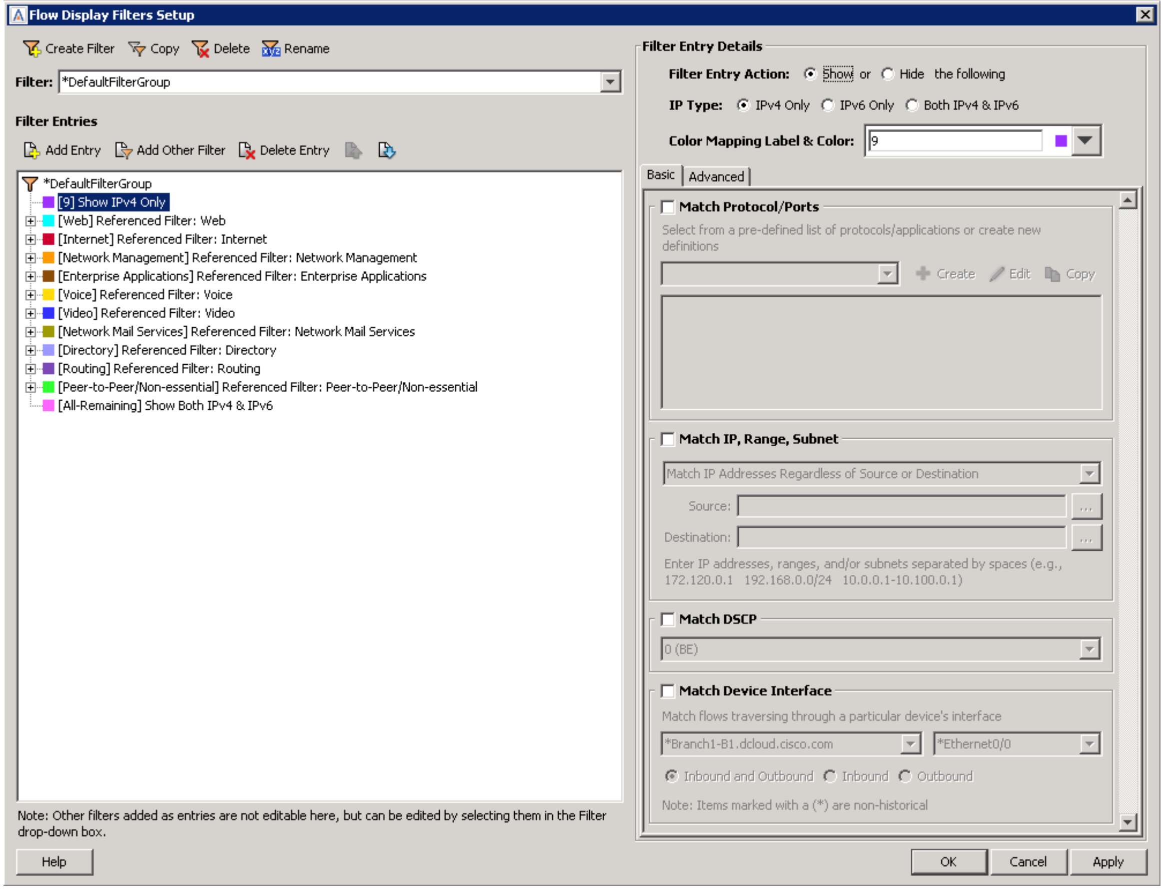
*Branch1-B1.dcloud.cisco.com

*Ethernet0/0

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

8. Move this new Entry up to the top of the list by selecting the icon multiple times.



Flow Display Filters Setup

Filter: *DefaultFilterGroup

Filter Entries

*DefaultFilterGroup
- [9] Show IPv4 Only
- [Web] Referenced Filter: Web
- [Internet] Referenced Filter: Internet
- [Network Management] Referenced Filter: Network Management
- [Enterprise Applications] Referenced Filter: Enterprise Applications
- [Voice] Referenced Filter: Voice
- [Video] Referenced Filter: Video
- [Network Mail Services] Referenced Filter: Network Mail Services
- [Directory] Referenced Filter: Directory
- [Routing] Referenced Filter: Routing
- [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
- [All-Remaining] Show Both IPv4 & IPv6

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: 9

□ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

□ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

□ Match DSCP

0 (BE)

□ Match Device Interface

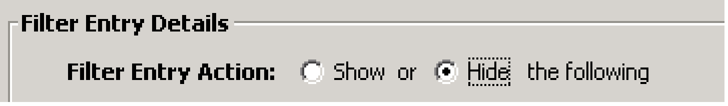
Match flows traversing through a particular device's interface

*Branch1-B1.dcloud.cisco.com *Ethernet0/0

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

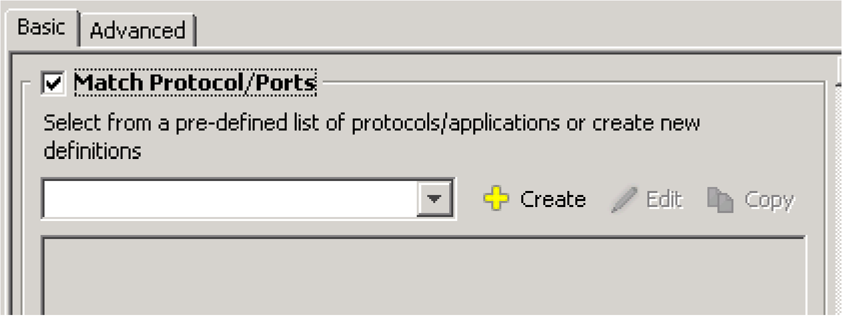
9. Once the new Entry is at the top of the list, select Hide for this new Entry



Filter Entry Details

Filter Entry Action: ○ Show or ● Hide the following

10. Tick Match Protocol/Ports

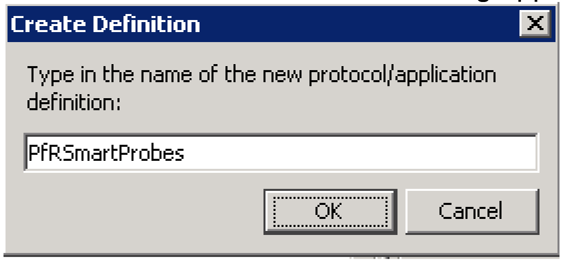


☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

11. Select Create.

12. The Create Definition Dialog appears, name the new definition, PfRSmartProbes.



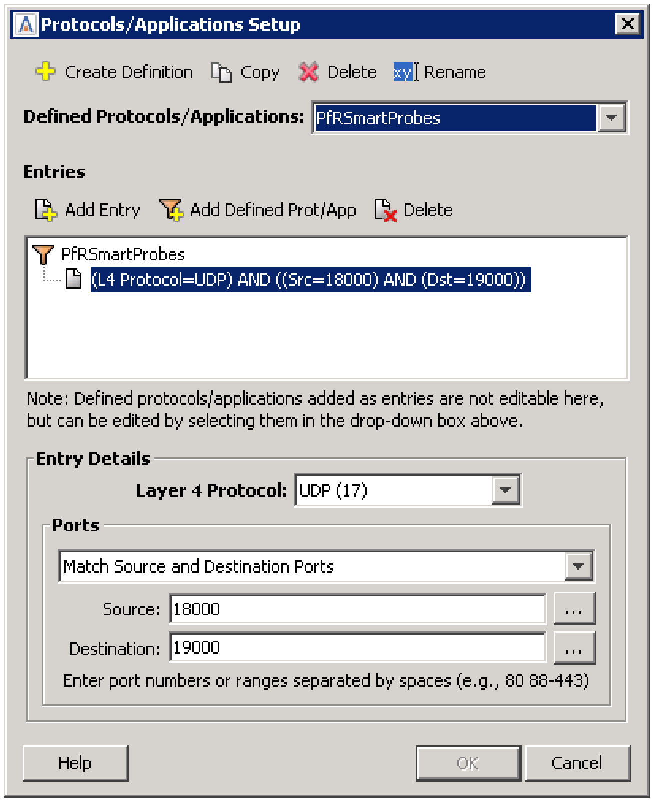
Create Definition

Type in the name of the new protocol/application definition:

PfRSmartProbes

The Filter needs to focus on:

I. Layer4 Protocol = UDP
II. Match Source and Destination Ports
III. Source Port = 18000
IV. Destination Port = 19000



Defined Protocols/Applications: PfRSmartProbes

Entries

PfRSmartProbes
(L4 Protocol=UDP) AND ((Src=18000) AND (Dst=19000))

Note: Defined protocols/applications added as entries are not editable here, but can be edited by selecting them in the drop-down box above.

Entry Details

Layer 4 Protocol: UDP (17)

Ports

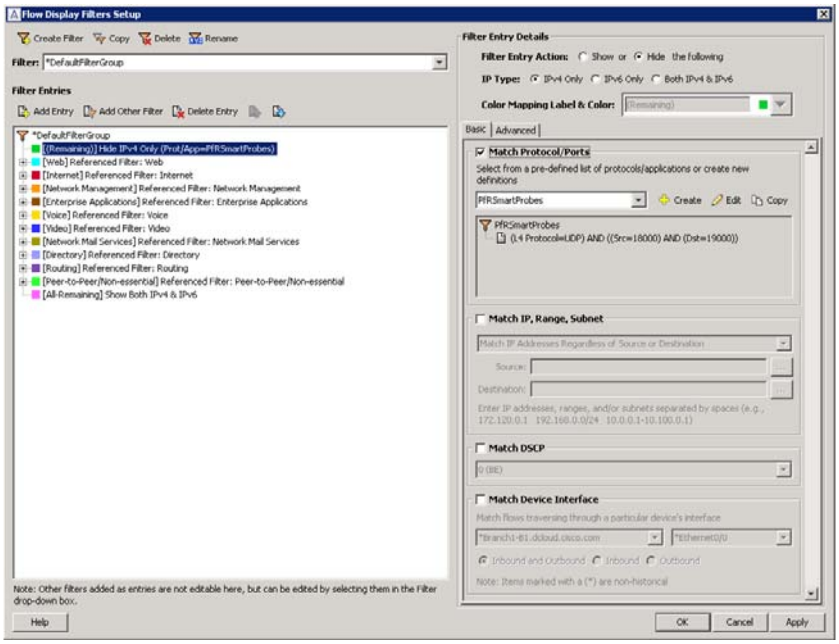
Match Source and Destination Ports

Source: 18000

Destination: 19000

Enter port numbers or ranges separated by spaces (e.g., 80 88-443)

When finished, the Filter should look like the following:



Filter: *DefaultFilterGroup

Filter Entries

*DefaultFilterGroup
🟩 [(Remaining)] Hide IPv4 Only (Prot/App=PfRSmartProbes)
🟦 [Web] Referenced Filter: Web
🟥 [Internet] Referenced Filter: Internet
🟧 [Network Management] Referenced Filter: Network Management
🟫 [Enterprise Applications] Referenced Filter: Enterprise Applications
🟨 [Voice] Referenced Filter: Voice
🟦 [Video] Referenced Filter: Video
🟫 [Network Mail Services] Referenced Filter: Network Mail Services
🟦 [Directory] Referenced Filter: Directory
🟪 [Routing] Referenced Filter: Routing
🟩 [Peer-to-Peer/Non-essential] Referenced Filter: Peer-to-Peer/Non-essential
🟪 [All-Remaining] Show Both IPv4 & IPv6

Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter drop-down box.

Filter Entry Details

Filter Entry Action: ○ Show or ● Hide the following

IP Type: ● IPv4 Only ○ IPv6 Only ○ Both IPv4 & IPv6

Color Mapping Label & Color: (Remaining) 🟩

☑ Match Protocol/Ports

Select from a pre-defined list of protocols/applications or create new definitions

PfRSmartProbes

PfRSmartProbes
(L4 Protocol=UDP) AND ((Src=18000) AND (Dst=19000))

☐ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source:

Destination:

Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)

☐ Match DSCP

0 (BE)

☐ Match Device Interface

Match flows traversing through a particular device's interface

*Branch1-81.dcloud.cisco.com *Ethernet0/0

● Inbound and Outbound ○ Inbound ○ Outbound

Note: Items marked with a (*) are non-historical

13. Select Apply
14. Select Ok

# Lab 9

## Lab 9:  SD-WAN Troubleshooting

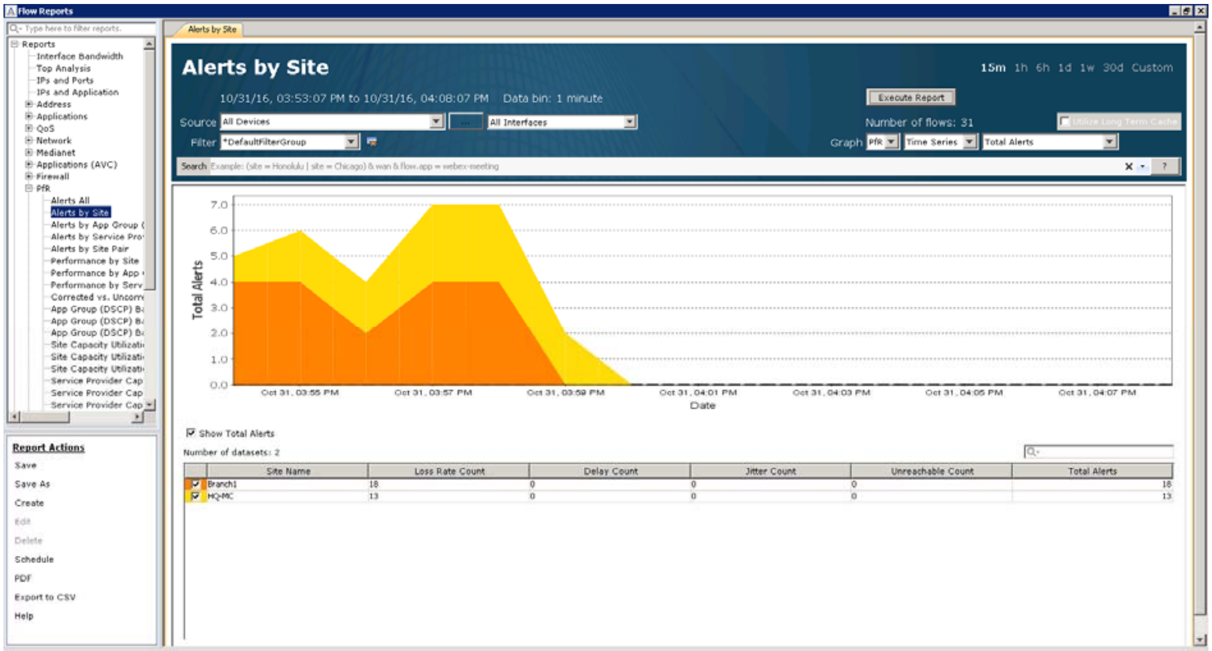
# Lab 9.1: Monitor SD-WAN

We will next use several LiveNX Flow that are useful for IWAN monitoring.

**Note: Keep all filters and report at their default settings**

1. Run the Flow > PfR > Alerts by Site Report
2. Run the Flow > PfR > Alerts by App Group (DSCP) Report
3. Run the Flow > PfR > Alerts by Service Provider Report
4. Run the Flow > PfR > Alerts by Site Pair Report

These reports will each break down the PfR Alerts from different perspectives.



Alerts by Site

10/31/16, 03:53:07 PM to 10/31/16, 04:08:07 PM Data bin: 1 minute

Source All Devices All Interfaces

Filter *DefaultFilterGroup

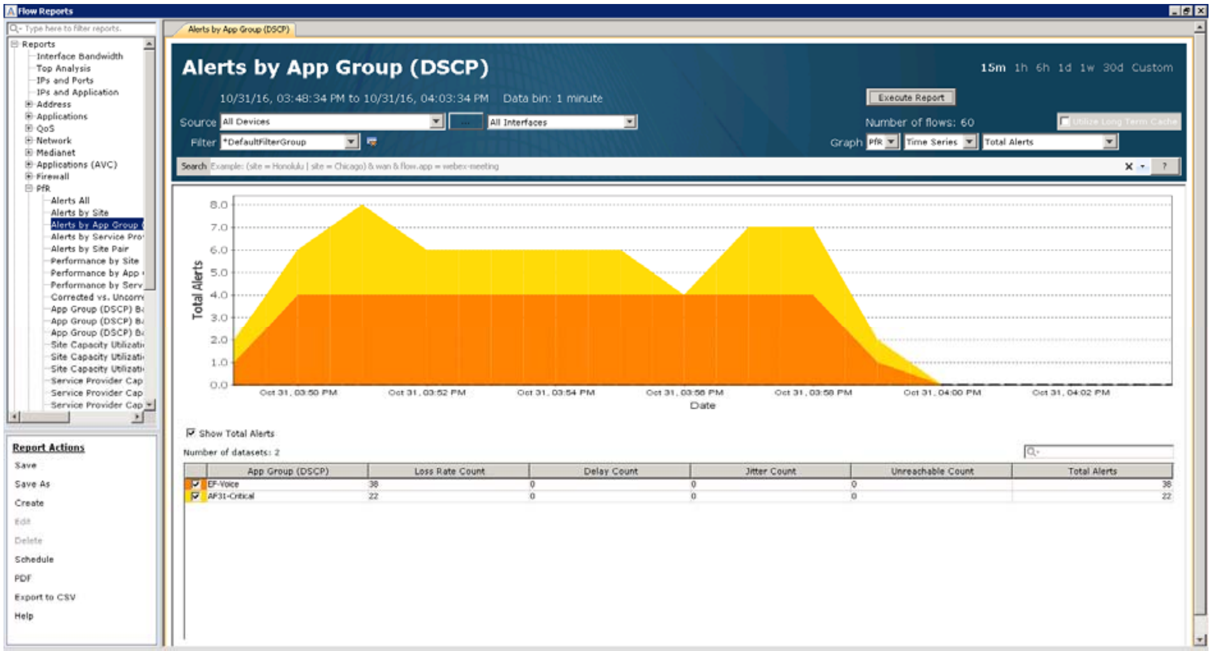
Number of flows: 31

Graph PfR Time Series Total Alerts

☑ Show Total Alerts

Number of datasets: 2

| | Site Name | Loss Rate Count | Delay Count | Jitter Count | Unreachable Count | Total Alerts |
|---|---|---|---|---|---|---|
| ☑ | Branch1 | 18 | 0 | 0 | 0 | 18 |
| ☑ | HQ-MC | 13 | 0 | 0 | 0 | 13 |



Alerts by App Group (DSCP)

10/31/16, 03:48:34 PM to 10/31/16, 04:03:34 PM Data bin: 1 minute

Source All Devices All Interfaces

Filter *DefaultFilterGroup

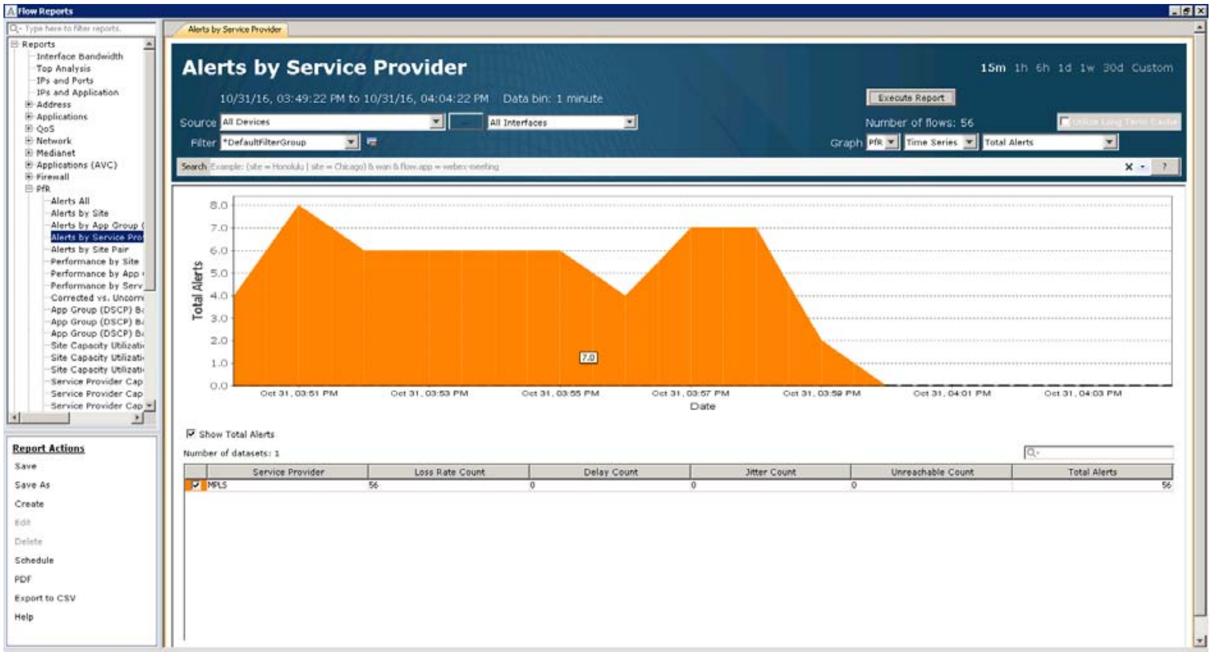
Number of flows: 60

Graph PfR Time Series Total Alerts

☑ Show Total Alerts

Number of datasets: 2

| | App Group (DSCP) | Loss Rate Count | Delay Count | Jitter Count | Unreachable Count | Total Alerts |
|---|---|---|---|---|---|---|
| ☑ | EF-Voice | 38 | 0 | 0 | 0 | 38 |
| ☑ | AF31-Critical | 22 | 0 | 0 | 0 | 22 |



Alerts by Service Provider

10/31/16, 03:49:22 PM to 10/31/16, 04:04:22 PM Data bin: 1 minute

Source All Devices All Interfaces

Filter *DefaultFilterGroup

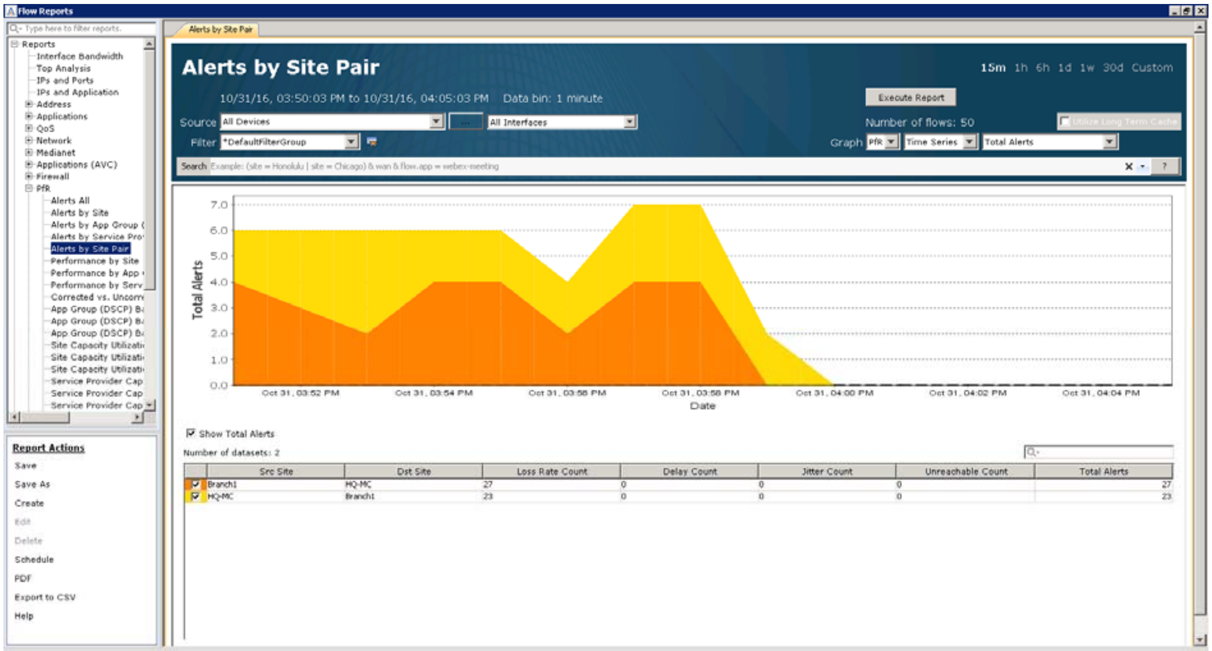
Number of flows: 56

Graph PfR Time Series Total Alerts

☑ Show Total Alerts

Number of datasets: 1

| | Service Provider | Loss Rate Count | Delay Count | Jitter Count | Unreachable Count | Total Alerts |
|---|---|---|---|---|---|---|
| ☑ | MPLS | 56 | 0 | 0 | 0 | 56 |



Alerts by Site Pair

10/31/16, 03:50:03 PM to 10/31/16, 04:05:03 PM Data bin: 1 minute

Source All Devices All Interfaces

Filter *DefaultFilterGroup

Number of flows: 50

Graph PfR Time Series Total Alerts

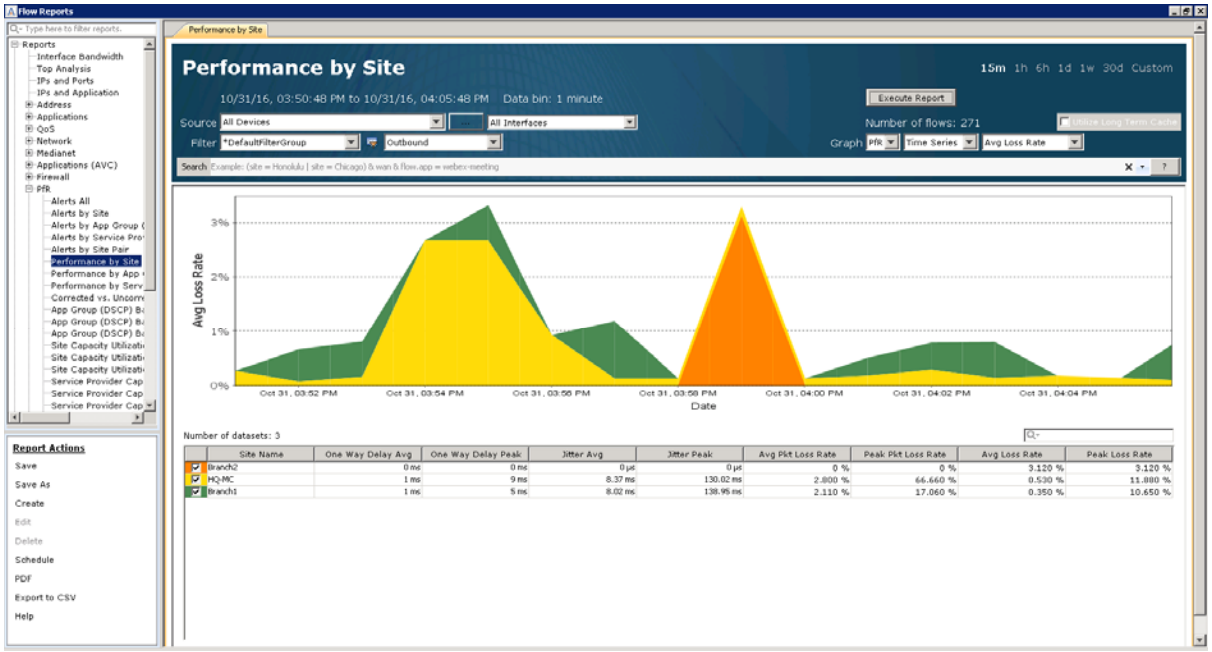
☑ Show Total Alerts

Number of datasets: 2

| | Src Site | Dst Site | Loss Rate Count | Delay Count | Jitter Count | Unreachable Count | Total Alerts |
|---|---|---|---|---|---|---|---|
| ☑ | Branch1 | HQ-MC | 27 | 0 | 0 | 0 | 27 |
| ☑ | HQ-MC | Branch1 | 23 | 0 | 0 | 0 | 23 |

5. Keep all filters and report at their default settings
6. Run the Flow > PfR > Performance by Site Report
7. Run the Flow > PfR > Performance by App Group (DSCP) Report
8. Run the Flow > PfR > Performance by Service Provider Report

These reports will each break down the PfR Performance from different perspectives.



Performance by Site

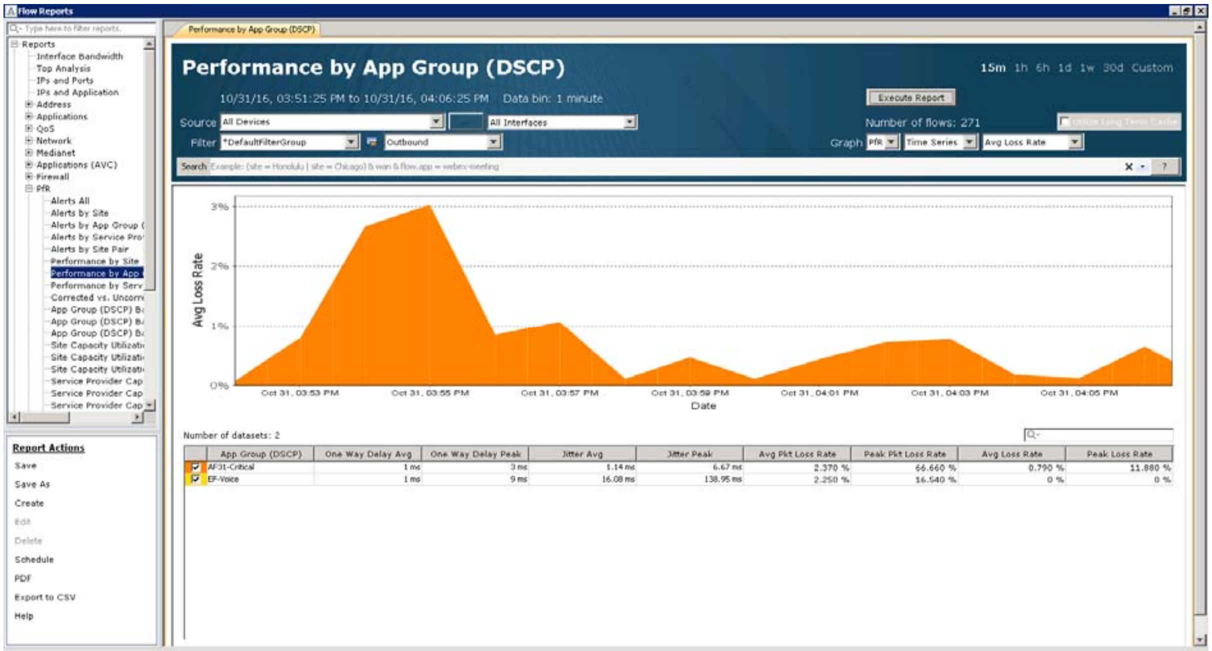
10/31/16, 03:50:48 PM to 10/31/16, 04:05:48 PM   Data bin: 1 minute

Source: All Devices   All Interfaces   Number of flows: 271

Filter: *DefaultFilterGroup   Outbound   Graph: PfR   Time Series   Avg Loss Rate

Number of datasets: 3

| | Site Name | One Way Delay Avg | One Way Delay Peak | Jitter Avg | Jitter Peak | Avg Pkt Loss Rate | Peak Pkt Loss Rate | Avg Loss Rate | Peak Loss Rate |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | Branch2 | 0 ms | 0 ms | 0 µs | 0 µs | 0 % | 0 % | 3.120 % | 3.120 % |
| ☑ | HQ-MC | 1 ms | 9 ms | 8.37 ms | 130.02 ms | 2.800 % | 66.660 % | 0.530 % | 11.880 % |
| ☑ | Branch1 | 1 ms | 5 ms | 8.02 ms | 138.95 ms | 2.110 % | 17.060 % | 0.350 % | 10.650 % |



Performance by App Group (DSCP)

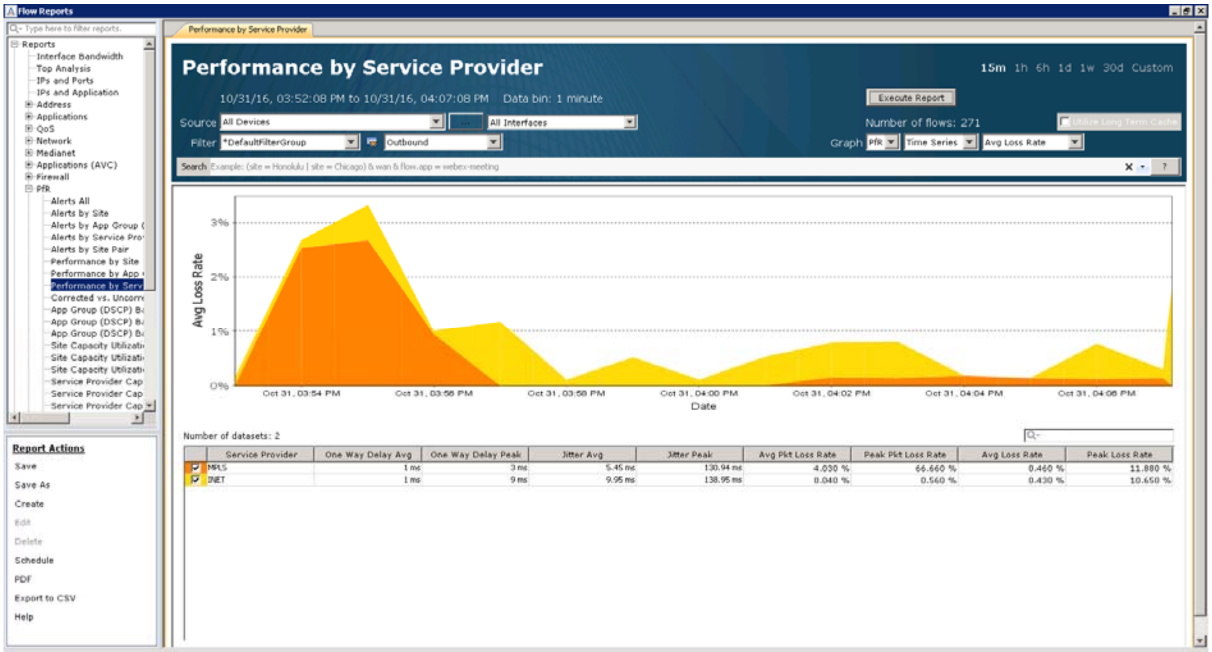
10/31/16, 03:51:25 PM to 10/31/16, 04:06:25 PM   Data bin: 1 minute

Source: All Devices   All Interfaces   Number of flows: 271

Filter: *DefaultFilterGroup   Outbound   Graph: PfR   Time Series   Avg Loss Rate

Number of datasets: 2

| | App Group (DSCP) | One Way Delay Avg | One Way Delay Peak | Jitter Avg | Jitter Peak | Avg Pkt Loss Rate | Peak Pkt Loss Rate | Avg Loss Rate | Peak Loss Rate |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | AF31-Critical | 1 ms | 3 ms | 1.14 ms | 6.67 ms | 2.370 % | 66.660 % | 0.790 % | 11.880 % |
| ☑ | EF-Voice | 1 ms | 9 ms | 16.08 ms | 138.95 ms | 2.250 % | 16.540 % | 0 % | 0 % |



Performance by Service Provider

10/31/16, 03:52:08 PM to 10/31/16, 04:07:08 PM Data bin: 1 minute

Source All Devices … All Interfaces

Filter *DefaultFilterGroup Outbound

Number of flows: 271

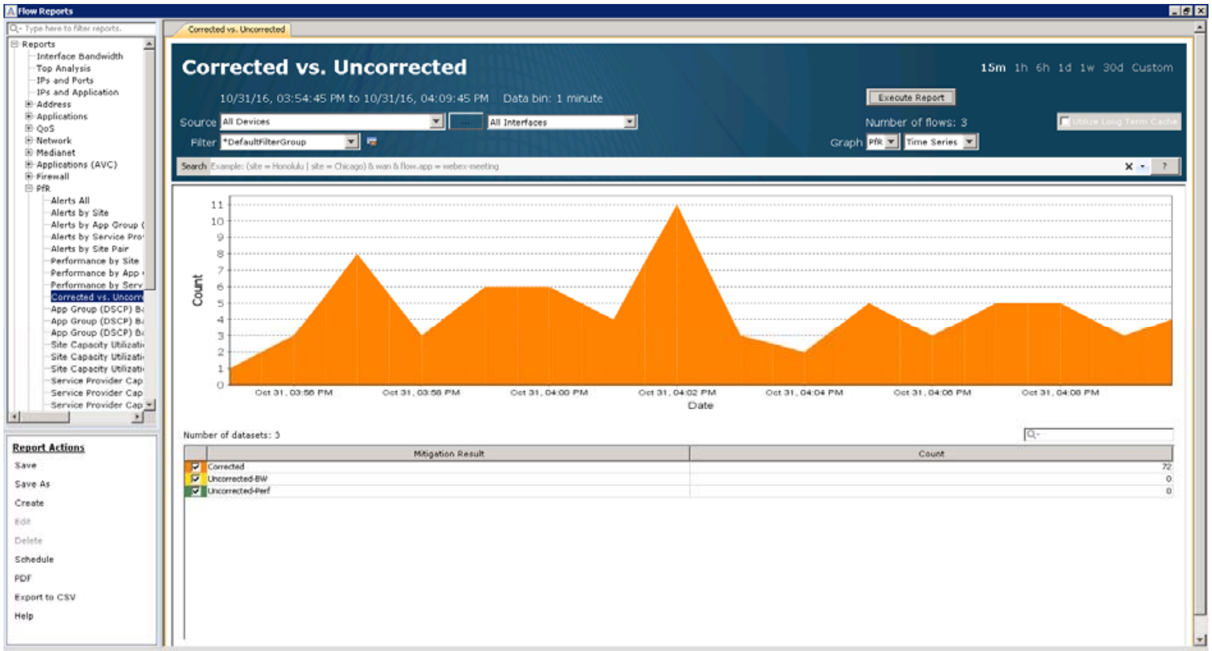
Graph PfR Time Series Avg Loss Rate

Number of datasets: 2

| | Service Provider | One Way Delay Avg | One Way Delay Peak | Jitter Avg | Jitter Peak | Avg Pkt Loss Rate | Peak Pkt Loss Rate | Avg Loss Rate | Peak Loss Rate |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | MPLS | 1 ms | 3 ms | 5.45 ms | 130.94 ms | 4.030 % | 66.660 % | 0.460 % | 11.880 % |
| ☑ | INET | 1 ms | 9 ms | 9.95 ms | 138.95 ms | 0.040 % | 0.560 % | 0.430 % | 10.650 % |

9. Run the Flow > PfR > Corrected vs. Uncorrected Report

This report shows the number of RCAs (route changes) vs IMEs (Immitigable event)



Corrected vs. Uncorrected

10/31/16, 03:54:45 PM to 10/31/16, 04:09:45 PM Data bin: 1 minute

Source All Devices … All Interfaces

Filter *DefaultFilterGroup

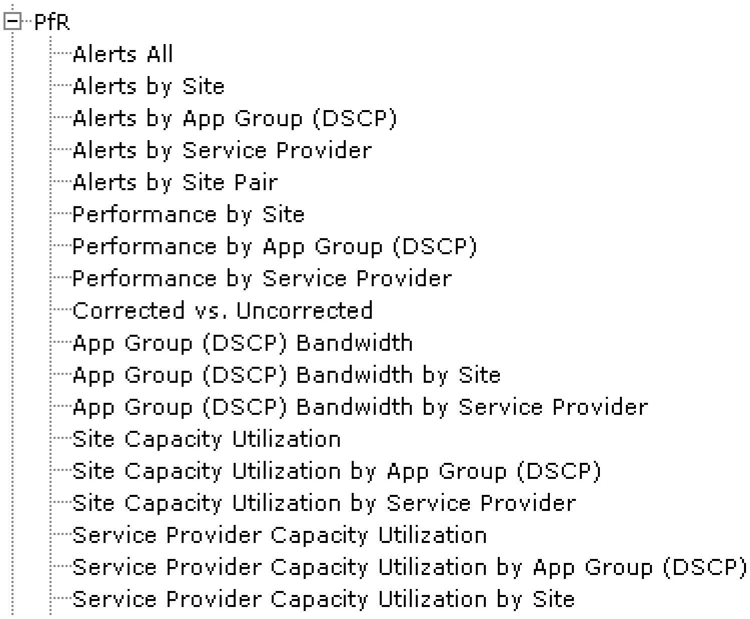
Number of flows: 3

Graph PfR Time Series

Number of datasets: 3

| | Mitigation Result | Count |
|---|---|---|
| ☑ | Corrected | 72 |
| ☑ | Uncorrected-BW | 0 |
| ☑ | Uncorrected-Perf | 0 |

Note that there are several more PfR Reports. Please review each of these reports

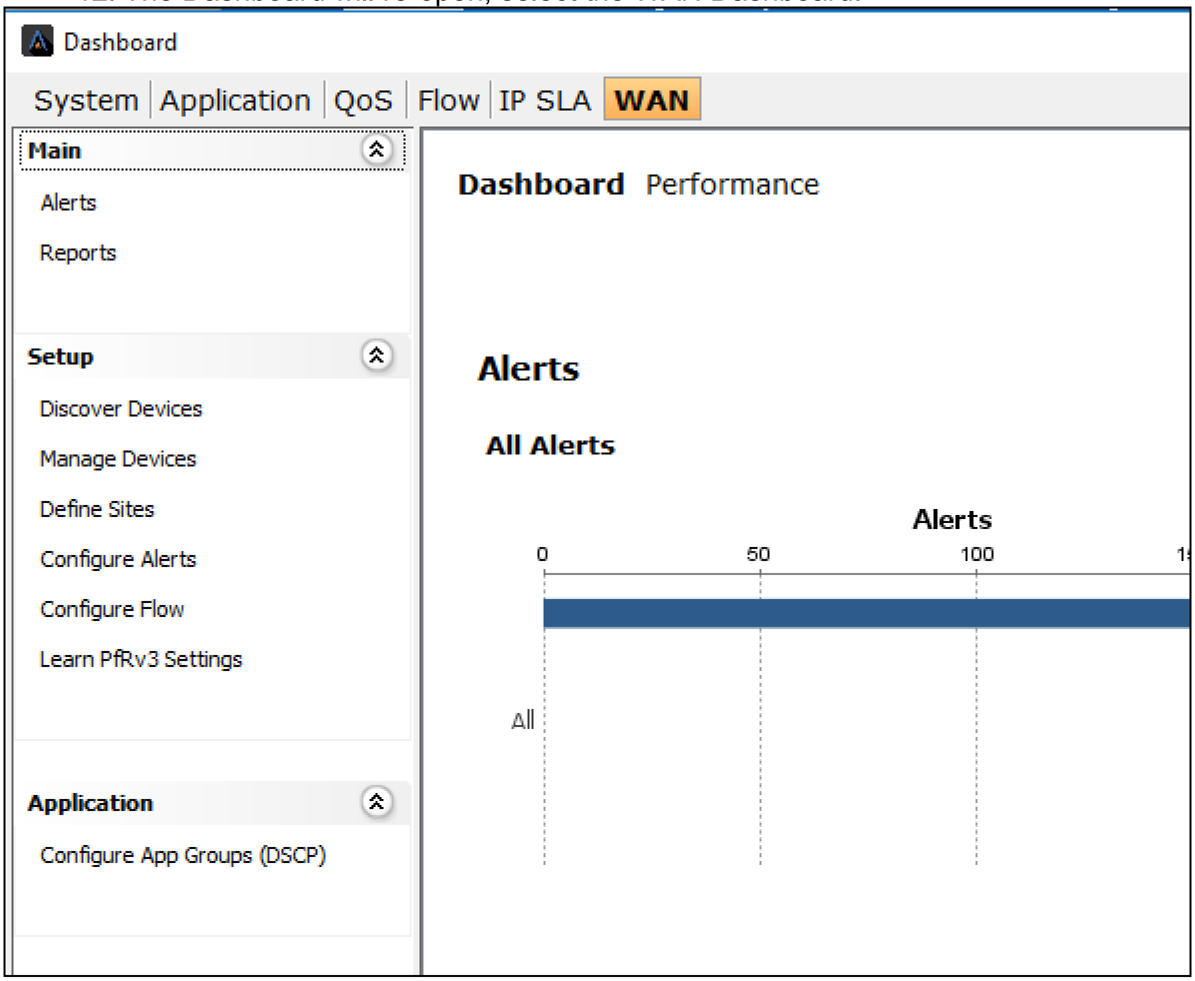


PfR
- Alerts All
- Alerts by Site
- Alerts by App Group (DSCP)
- Alerts by Service Provider
- Alerts by Site Pair
- Performance by Site
- Performance by App Group (DSCP)
- Performance by Service Provider
- Corrected vs. Uncorrected
- App Group (DSCP) Bandwidth
- App Group (DSCP) Bandwidth by Site
- App Group (DSCP) Bandwidth by Service Provider
- Site Capacity Utilization
- Site Capacity Utilization by App Group (DSCP)
- Site Capacity Utilization by Service Provider
- Service Provider Capacity Utilization
- Service Provider Capacity Utilization by App Group (DSCP)
- Service Provider Capacity Utilization by Site

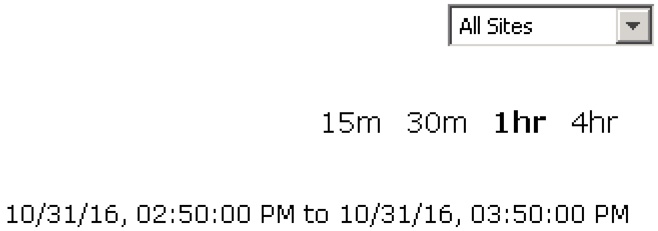
10. Return to the PfR dashboard to review network utilization.

11. From the LiveNX client, select the Dashboard

12. The Dashboard will re-open, select the WAN Dashboard.



13. Set the time range of the WAN-PfR dashboard to 1hr.

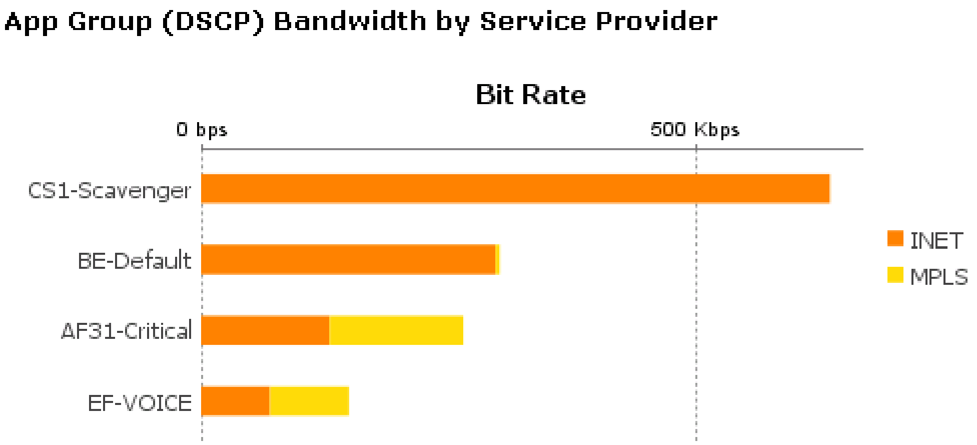


All Sites

15m 30m **1hr** 4hr

10/31/16, 02:50:00 PM to 10/31/16, 03:50:00 PM

14. Review the App Group (DSCP) Bandwidth by Service Provider widget.

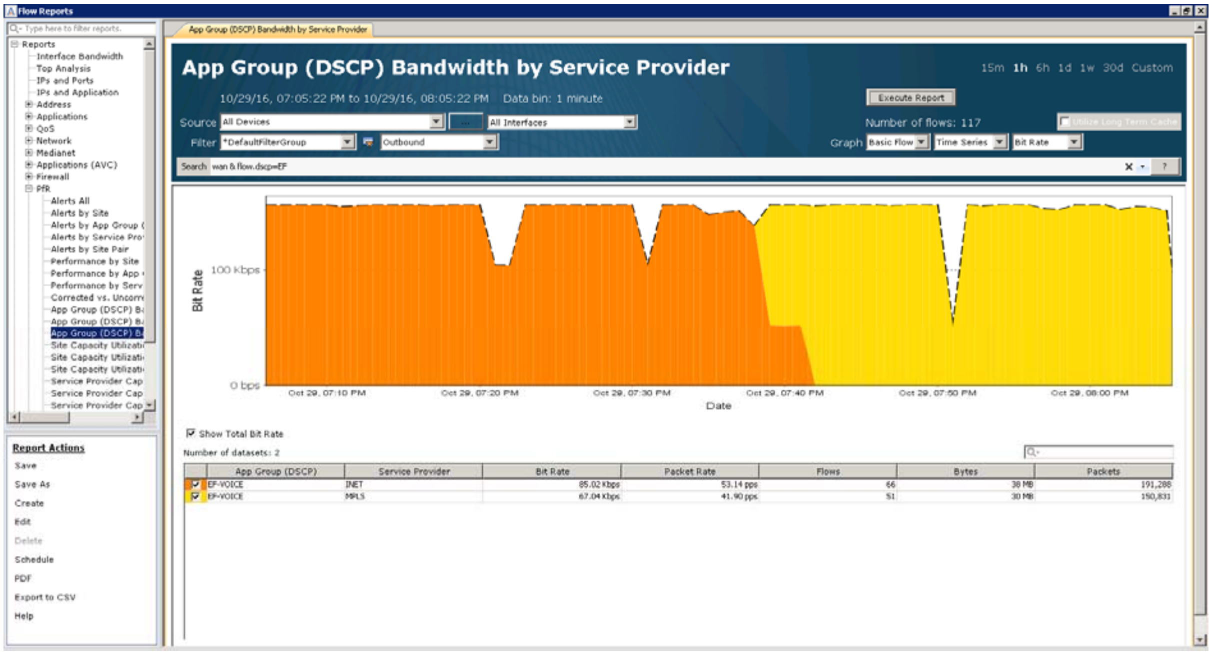


15. Note how AF31-Critical and EF-Voice show ~50% utilization on INET and MPLS

16. Double-click on the EF-Voice bar graph

17. This will open the App Group (DSCP) Bandwidth by Service Provider Report

18. Update the Search to “wan & flow.dscp=EF”



App Group (DSCP) Bandwidth by Service Provider

10/29/16, 07:05:22 PM to 10/29/16, 08:05:22 PM Data bin: 1 minute

Source: All Devices; All Interfaces

Filter: *DefaultFilterGroup; Outbound

Number of flows: 117

Graph: Basic Flow; Time Series; Bit Rate

Search: wan & flow.dscp=EF

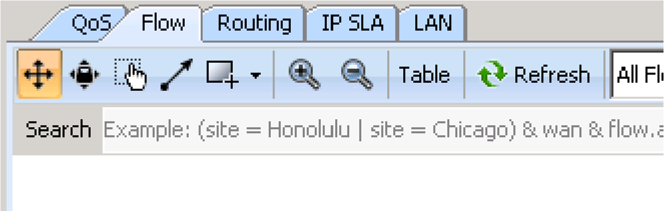
☑ Show Total Bit Rate

Number of datasets: 2

| | App Group (DSCP) | Service Provider | Bit Rate | Packet Rate | Flows | Bytes | Packets |
|---|---|---|---|---|---|---|---|
| ☑ | EF-VOICE | INET | 85.02 Kbps | 53.14 pps | 66 | 38 MB | 191,288 |
| ☑ | EF-VOICE | MPLS | 67.04 Kbps | 41.90 pps | 51 | 30 MB | 150,831 |

Note the time when the bandwidth graph changes colours. This shows when any PfR route changes have occurred. We will use the time in the next step.

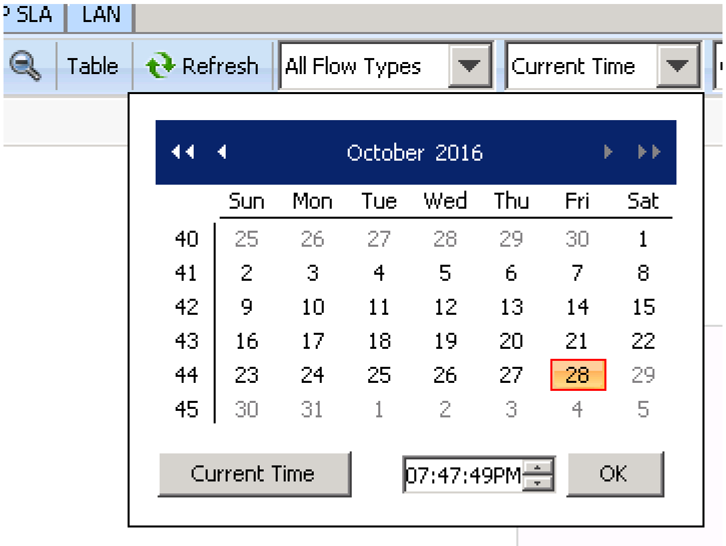
19. From the LiveNX map, select the Flow tab



Search: Example: (site = Honolulu | site = Chicago) & wan & flow.a

20. Select the Current Time pull-down

21. Set the time based of the map based the data captured in the App Group (DSCP) Bandwidth by Service Provider Report.



October 2016

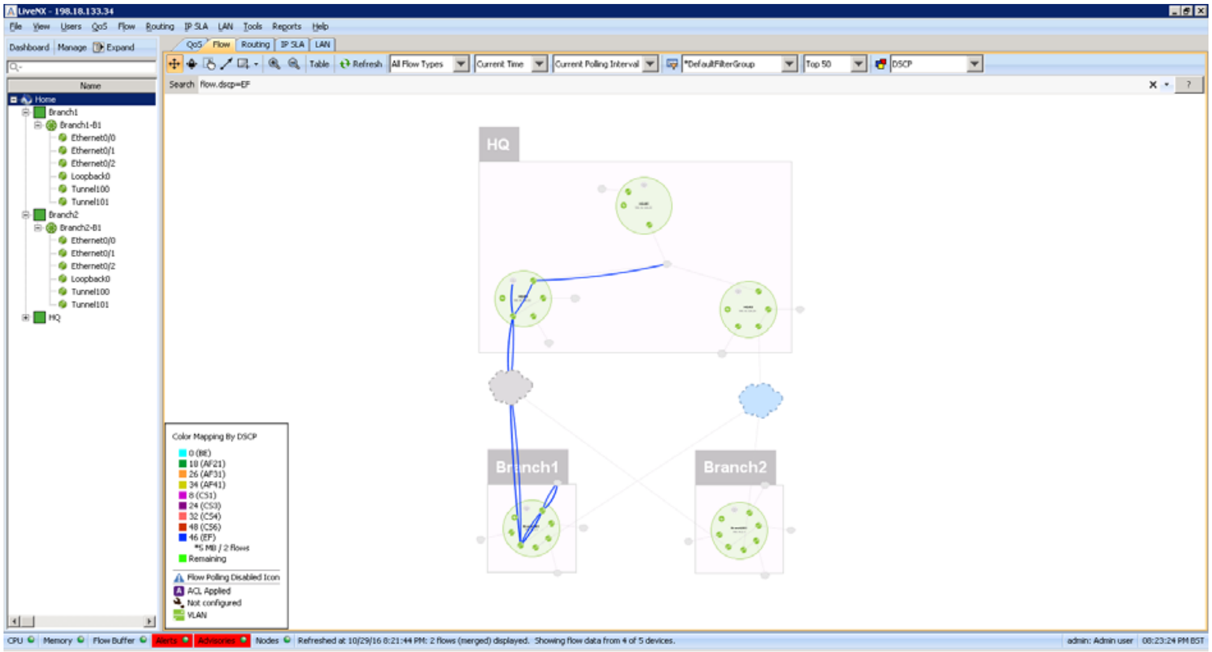
| | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|---|---|---|---|---|---|---|---|
| 40 | 25 | 26 | 27 | 28 | 29 | 30 | 1 |
| 41 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 42 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 43 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 44 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 45 | 30 | 31 | 1 | 2 | 3 | 4 | 5 |

07:47:49PM

22. Set the map's Filter to *DefaultFilterGroup and Search to “flow.dscp=EF”

By adjusting the time according to the App Group (DSCP) Bandwidth by Service Provider Report, you will be able to visualize the path changes of the EF (Voice) traffic in the network.

In this example, the EF traffic is on the INET path.



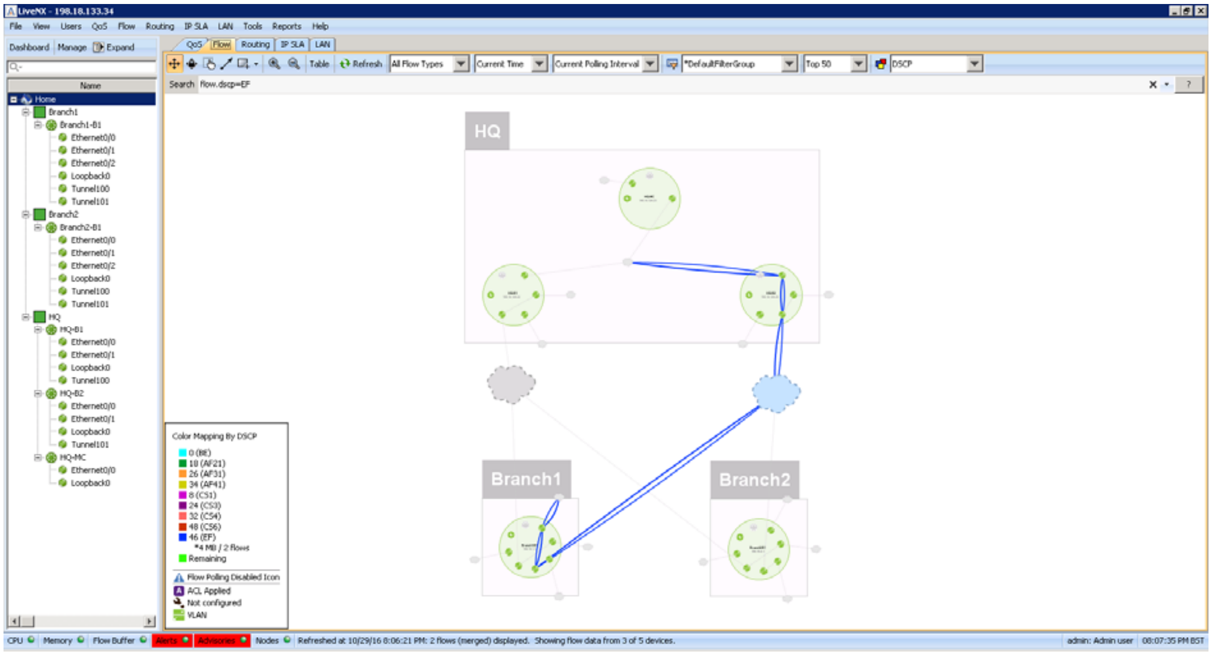
All Flow Types | Current Time | Current Polling Interval | *DefaultFilterGroup | Top 50 | DSCP

Search Flow.dscp=EF

Refreshed at 10/29/16 8:21:44 PM: 2 flows (merged) displayed. Showing flow data from 4 of 5 devices.

admin: Admin user | 08:23:24 PM BST

In this example, the EF traffic is on the MPLS path.



All Flow Types | Current Time | Current Polling Interval | *DefaultFilterGroup | Top 50 | DSCP

Search Flow.dscp=EF

Refreshed at 10/29/16 8:06:21 PM: 2 flows (merged) displayed. Showing flow data from 3 of 5 devices.

admin: Admin user | 08:07:35 PM BST

# Lab A

## Lab A:  Appendix

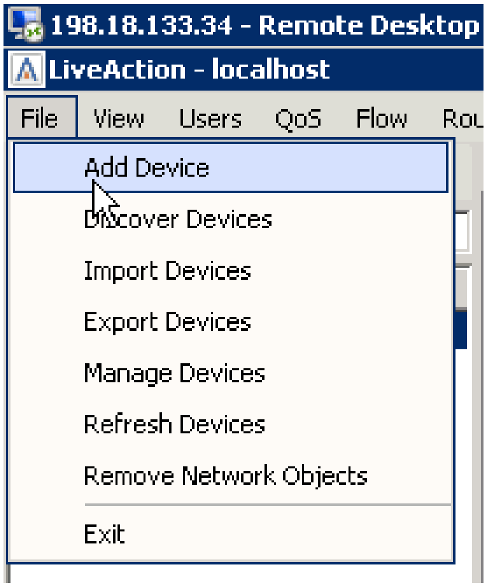
# Lab A.1: Add Initial Device

Step 2 – Add Devices into LiveAction

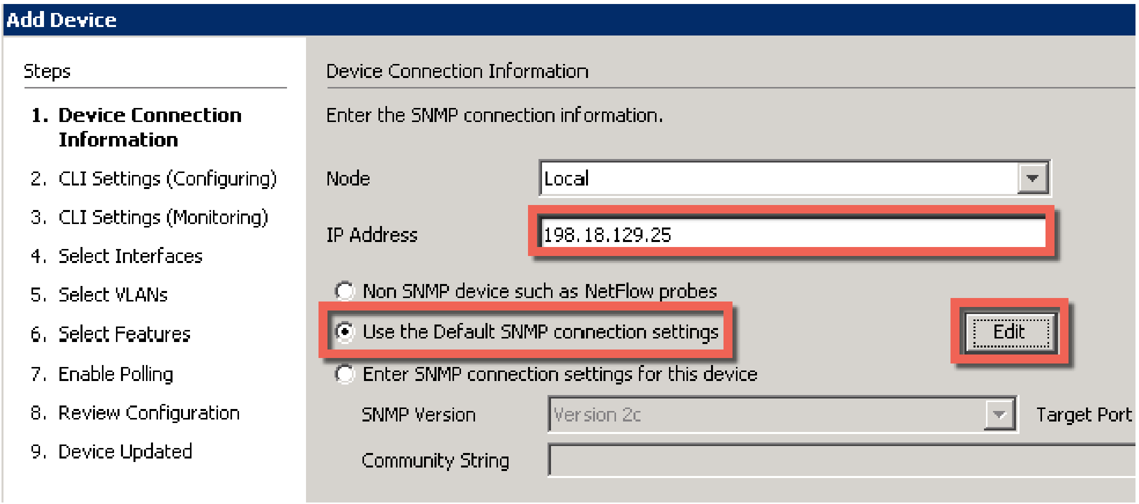
Adding devices into LiveAction and managing them properly is very important to the overall usability of LiveAction itself.

- Your task in this section will be to add 3 devices into LiveAction, managing the correct interfaces and configuring NetFlow on the devices.

To add a single device into LiveAction go to File and then Add Device



For the first device we will be adding into LiveAction use: 198.18.129.25 in the IP Address field. Select "Use the Default SNMP connection settings" then select Edit.


Add Device

Steps

1. **Device Connection Information**
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

Device Connection Information

Enter the SNMP connection information.

Node: Local

IP Address: 198.18.129.25

○ Non SNMP device such as NetFlow probes

● Use the Default SNMP connection settings

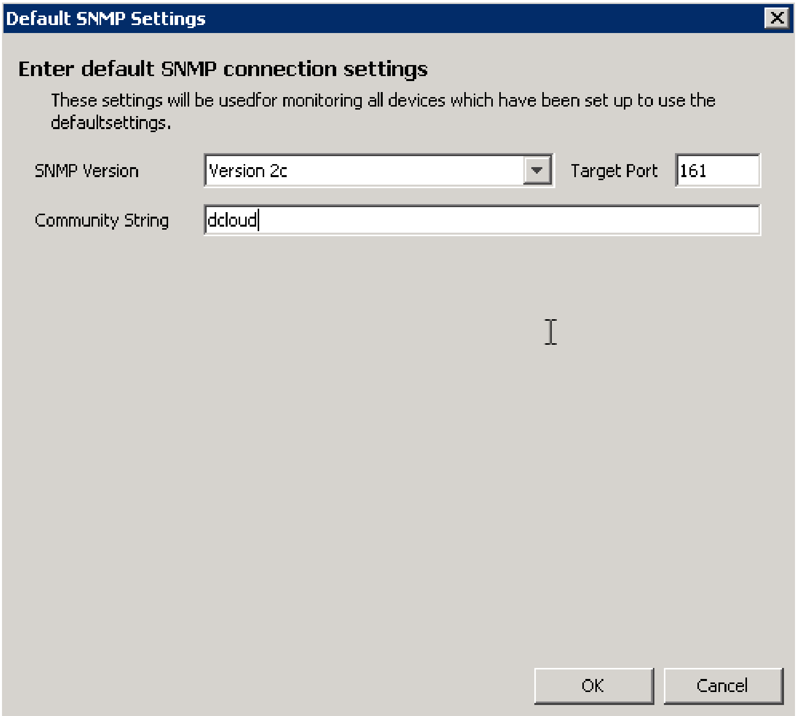
○ Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port

Community String

On the Default SNMP Settings window use the Community String of "dcloud" and then select OK. Setting the default community string will allow you to use them on multiple devices.



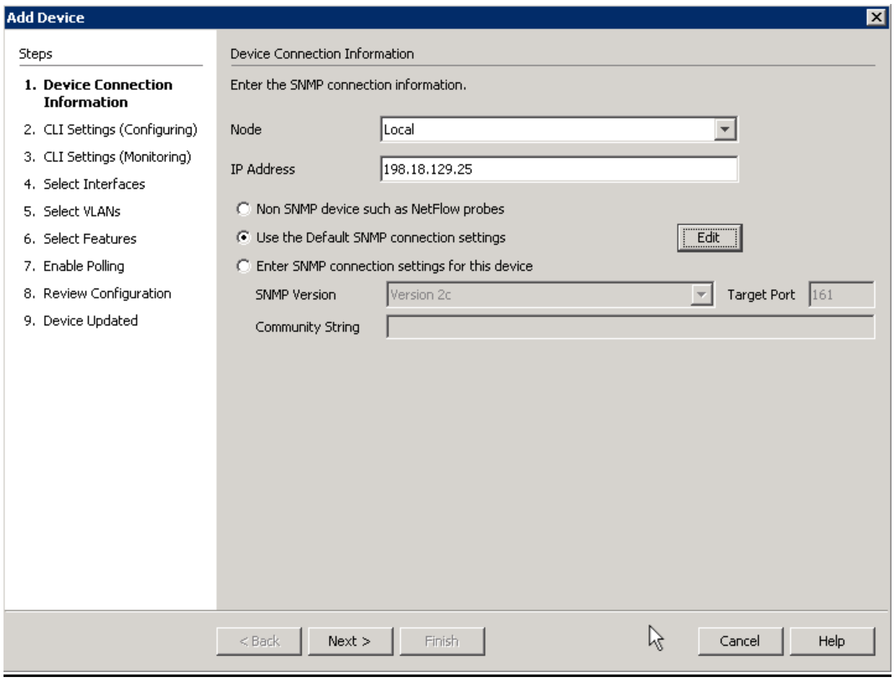
Default SNMP Settings

Enter default SNMP connection settings

These settings will be usedfor monitoring all devices which have been set up to use the defaultsettings.

SNMP Version: Version 2c
Target Port: 161
Community String: dcloud

Select Next



Add Device

Device Connection Information

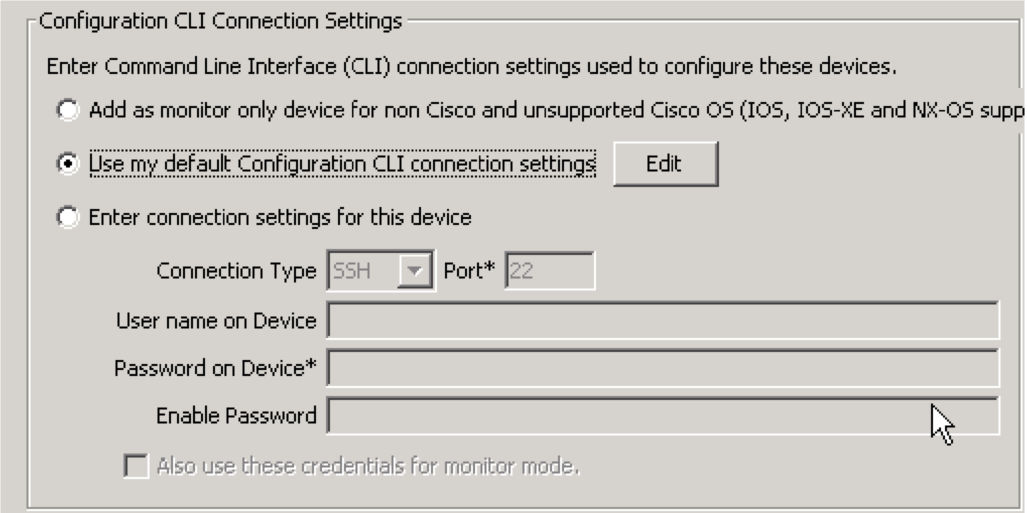
Enter the SNMP connection information.

Node: Local
IP Address: 198.18.129.25

○ Non SNMP device such as NetFlow probes
● Use the Default SNMP connection settings
○ Enter SNMP connection settings for this device

SNMP Version: Version 2c
Target Port: 161
Community String:

On the next window select “Use my default Configuration CLI connection settings” and then select “Edit”



Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

● Use my default Configuration CLI connection settings

○ Enter connection settings for this device

Connection Type: SSH  Port*: 22

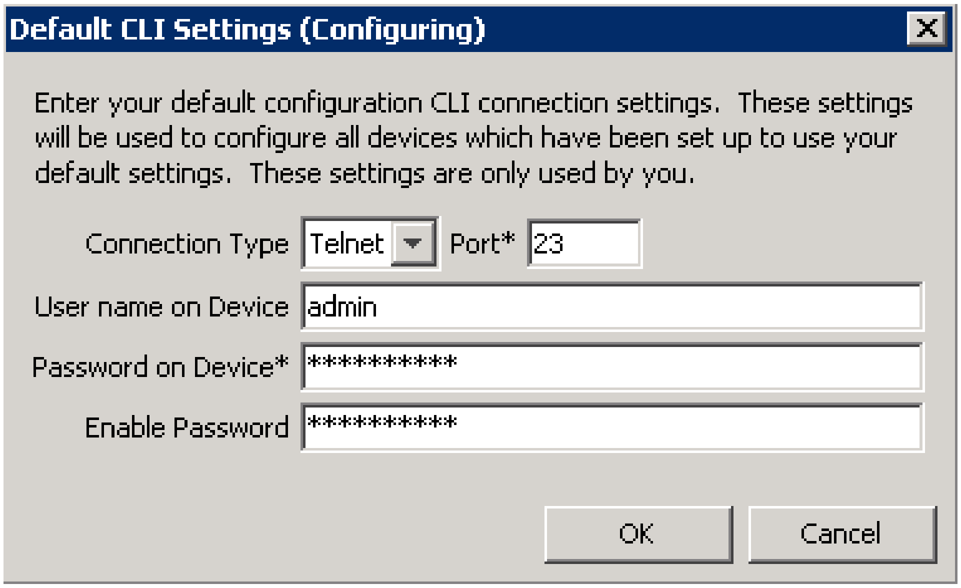
User name on Device:

Password on Device*:

Enable Password:

□ Also use these credentials for monitor mode.

On the Default CLI Settings select “Telnet” as the connection type. Then use the username of “admin” and for the password and enable password use “C1sco12345”. Select OK. Setting the user credentials will allow you to use them for multiple devices.



Default CLI Settings (Configuring)

Enter your default configuration CLI connection settings. These settings will be used to configure all devices which have been set up to use your default settings. These settings are only used by you.

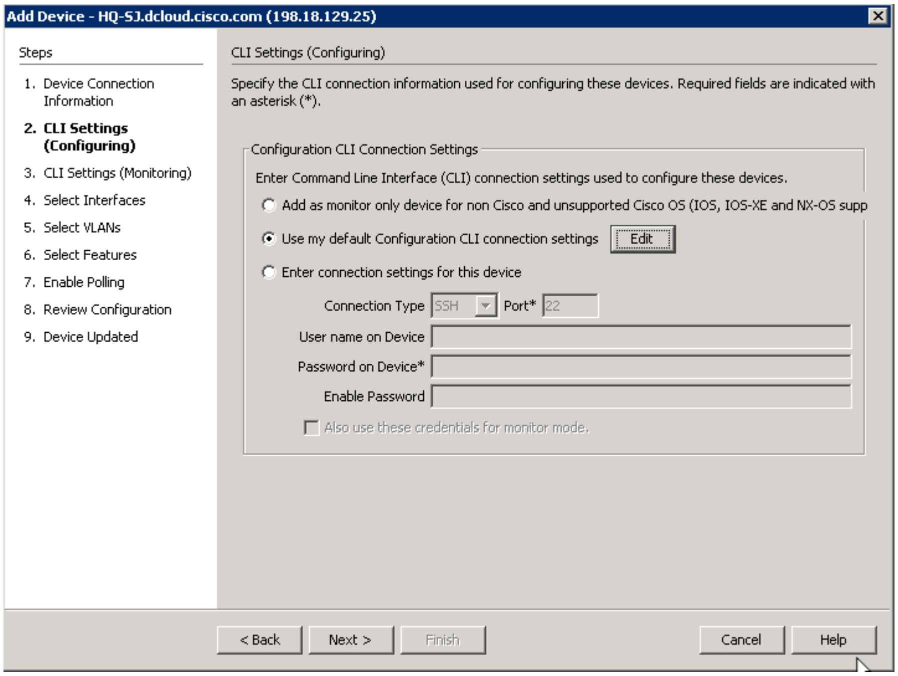
Connection Type: Telnet  Port*: 23

User name on Device: admin

Password on Device*: **********

Enable Password: **********

Select Next to continue.


Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. **CLI Settings (Configuring)**
3. CLI Settings (Monitoring)
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

● Use my default Configuration CLI connection settings [Edit]

○ Enter connection settings for this device

Connection Type SSH Port* 22

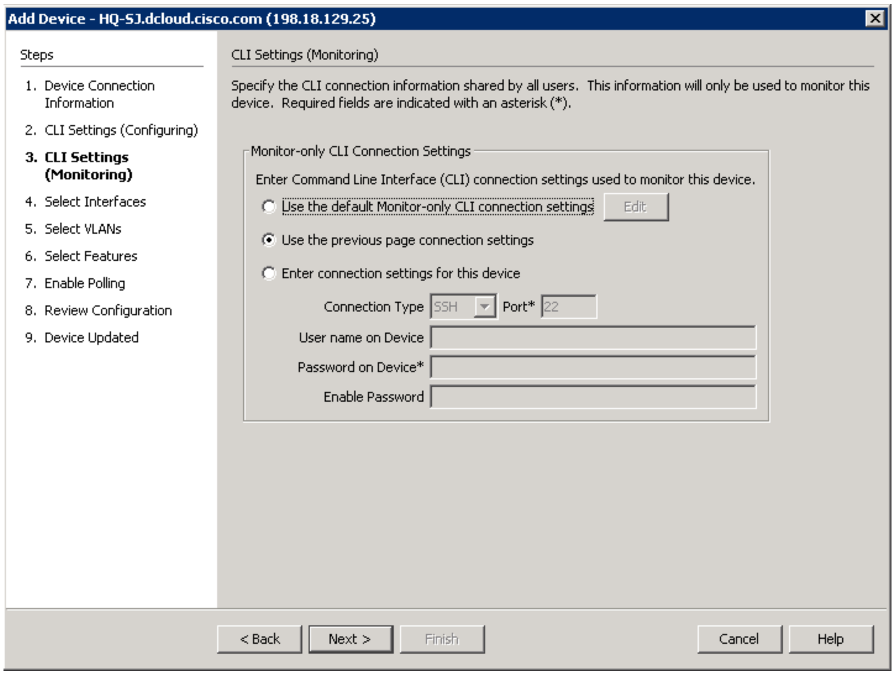
User name on Device

Password on Device*

Enable Password

□ Also use these credentials for monitor mode.

On the CLI Settings for Monitoring select “Use the previous page connection settings” and then select Next.


Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Select Interfaces
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings [Edit]

● Use the previous page connection settings

○ Enter connection settings for this device

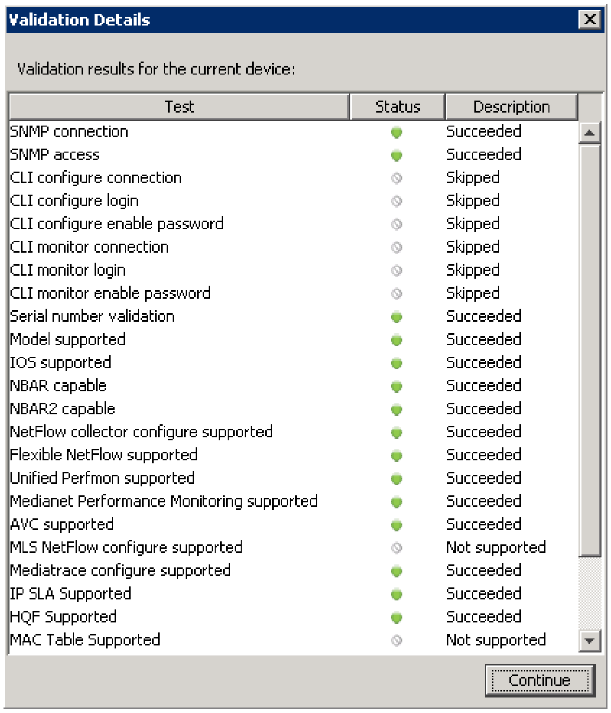
Connection Type SSH Port* 22

User name on Device

Password on Device*

Enable Password

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

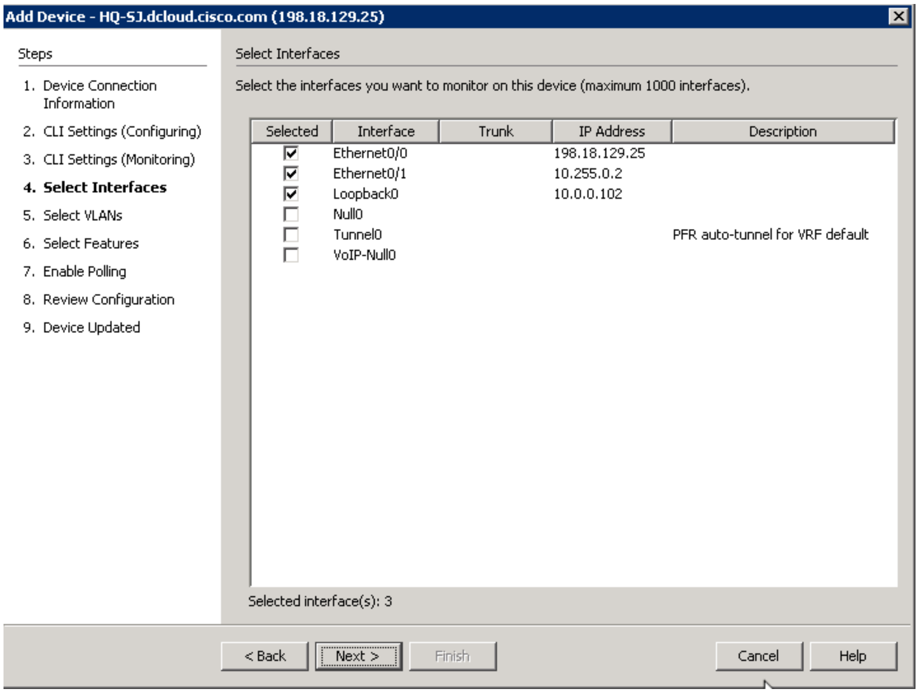


**Validation Details**

Validation results for the current device:

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

On the select interfaces window you can notice 3 interfaces are already selected. LiveAction automatically selects the interfaces based on the highest bit rate. Select Next to continue.



**Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)**

Steps

1. Device Connection Information
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. **Select Interfaces**
5. Select VLANs
6. Select Features
7. Enable Polling
8. Review Configuration
9. Device Updated

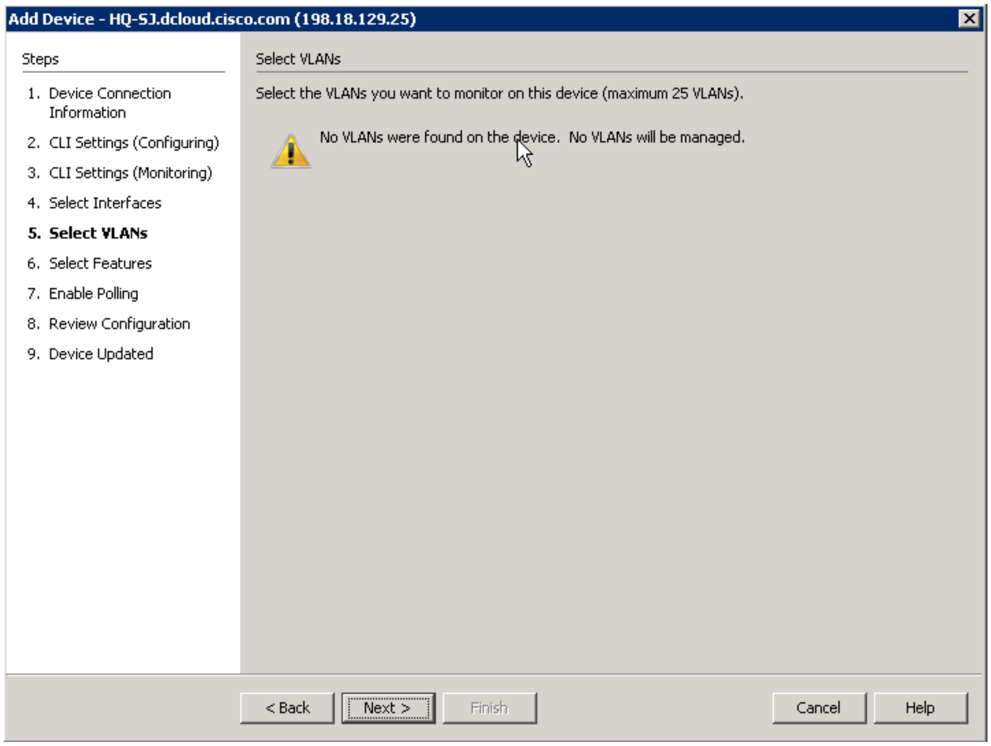
Select Interfaces

Select the interfaces you want to monitor on this device (maximum 1000 interfaces).

| Selected | Interface | Trunk | IP Address | Description |
|---|---|---|---|---|
| ☑ | Ethernet0/0 | | 198.18.129.25 | |
| ☑ | Ethernet0/1 | | 10.255.0.2 | |
| ☑ | Loopback0 | | 10.0.0.102 | |
| ☐ | Null0 | | | |
| ☐ | Tunnel0 | | | PFR auto-tunnel for VRF default |
| ☐ | VoIP-Null0 | | | |

Selected interface(s): 3

Select Next on the select VLANs window.

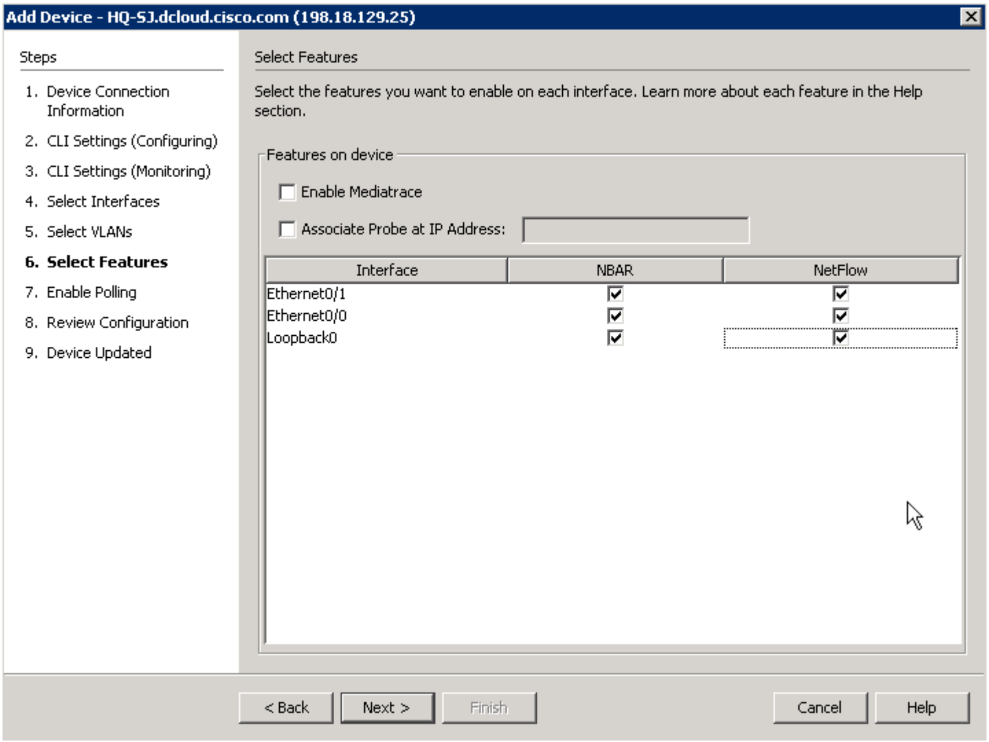

Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Select VLANs

Select the VLANs you want to monitor on this device (maximum 25 VLANs).

No VLANs were found on the device.  No VLANs will be managed.

Check NBAR and NetFlow for all interfaces and then select Next


Add Device - HQ-SJ.dcloud.cisco.com (198.18.129.25)

Select Features

Select the features you want to enable on each interface. Learn more about each feature in the Help section.

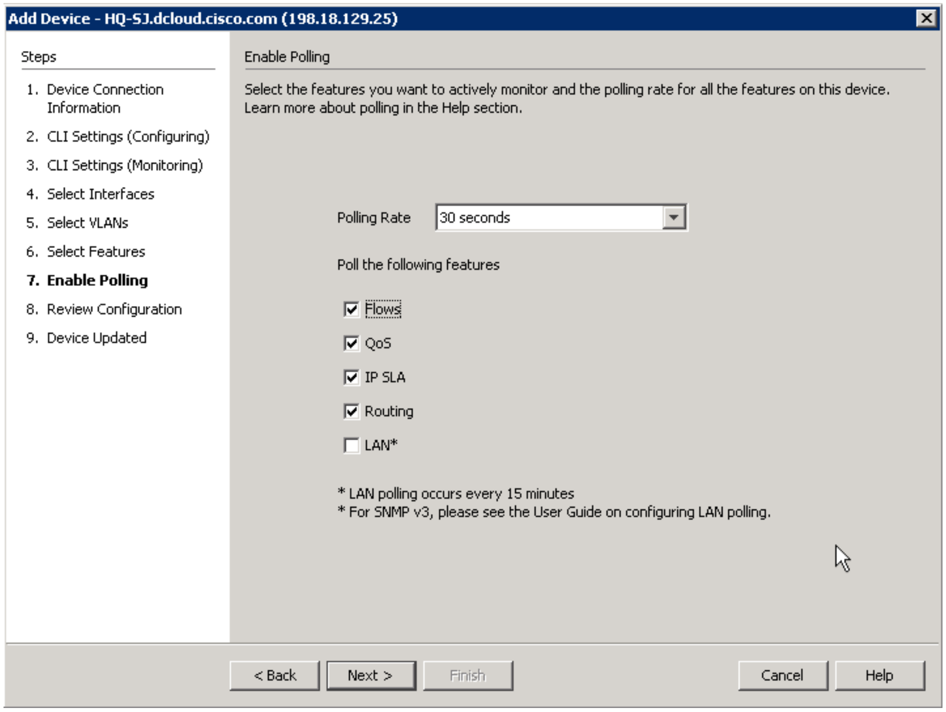
Features on device

□ Enable Mediatrace

□ Associate Probe at IP Address:

| Interface | NBAR | NetFlow |
|---|---|---|
| Ethernet0/1 | ☑ | ☑ |
| Ethernet0/0 | ☑ | ☑ |
| Loopback0 | ☑ | ☑ |

On the enable polling window change the polling rate to 30 seconds, and check all features except LAN.



Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section.

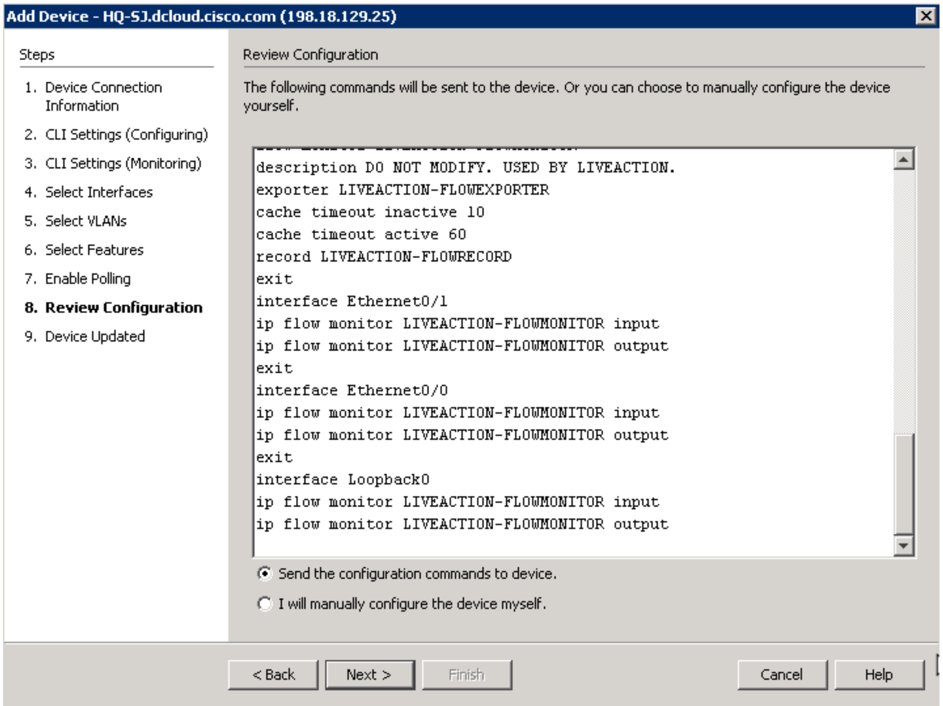
Polling Rate: 30 seconds

Poll the following features

☑ Flows
☑ QoS
☑ IP SLA
☑ Routing
□ LAN*

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.

Before sending the NetFlow configurations to the device, you can verify the configurations that LiveAction created. Select Next to push the configurations to the device.

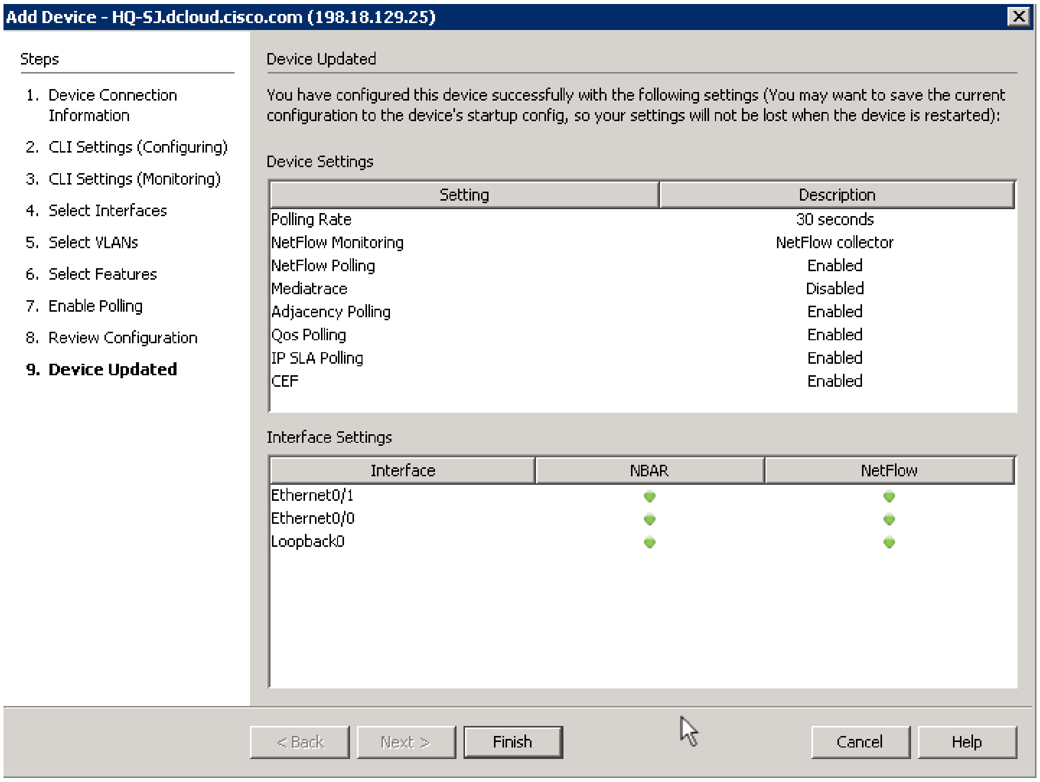


The following commands will be sent to the device. Or you can choose to manually configure the device yourself.

```
description DO NOT MODIFY. USED BY LIVEACTION.
exporter LIVEACTION-FLOWEXPORTER
cache timeout inactive 10
cache timeout active 60
record LIVEACTION-FLOWRECORD
exit
interface Ethernet0/1
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
exit
interface Ethernet0/0
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
exit
interface Loopback0
ip flow monitor LIVEACTION-FLOWMONITOR input
ip flow monitor LIVEACTION-FLOWMONITOR output
```

● Send the configuration commands to device.
○ I will manually configure the device myself.

Once completed you will just need to select Finish to add the device into LiveAction.



Device Updated

You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):

Device Settings

| Setting | Description |
|---|---|
| Polling Rate | 30 seconds |
| NetFlow Monitoring | NetFlow collector |
| NetFlow Polling | Enabled |
| Mediatrace | Disabled |
| Adjacency Polling | Enabled |
| Qos Polling | Enabled |
| IP SLA Polling | Enabled |
| CEF | Enabled |

Interface Settings

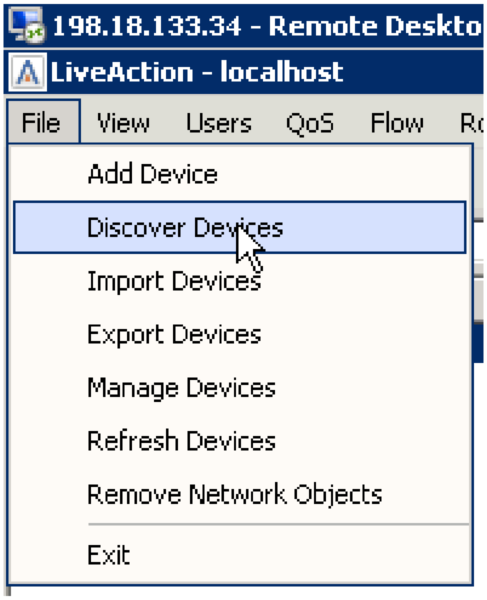
| Interface | NBAR | NetFlow |
|---|---|---|
| Ethernet0/1 | ● | ● |
| Ethernet0/0 | ● | ● |
| Loopback0 | ● | ● |

# Lab A.2:  Using Device Discovery

As we discovered in the prior Lab, the LiveNX Server in your topology has had a single device pre-installed.  The Appendix in this Lab Workbook details the step-by-step instructions to install the Server, Client, and adding an initial device.  In the following Labs you will add additional devices to your Topology, configure those devices to send flow and SNMP data to the LiveNX Server, and discover what data your LiveNX solution is gathering.

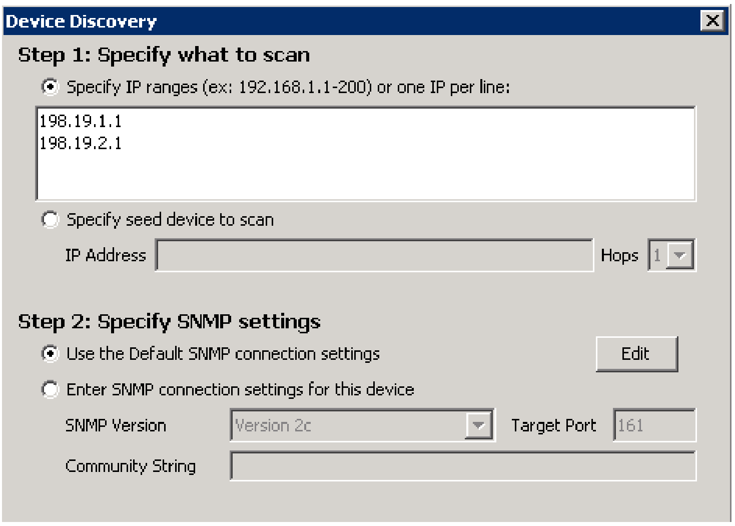
Lab Steps:
Adding several devices at once is as easy as adding a single device at a time. To do this:

1. Select File and Discover Devices.



2. Specify the following IP addresses:
   198.19.1.1
   198.19.2.1

3. **Select** Use the default SNMP connection settings.


Device Discovery

Step 1: Specify what to scan

● Specify IP ranges (ex: 192.168.1.1-200) or one IP per line:

198.19.1.1
198.19.2.1

○ Specify seed device to scan

IP Address   Hops 1

Step 2: Specify SNMP settings

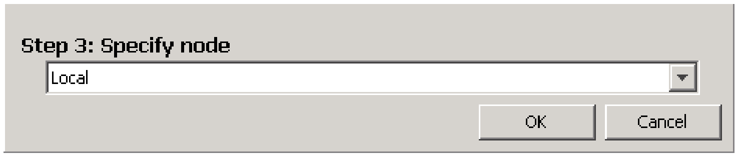
● Use the Default SNMP connection settings   Edit

○ Enter SNMP connection settings for this device

SNMP Version Version 2c   Target Port 161

Community String

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

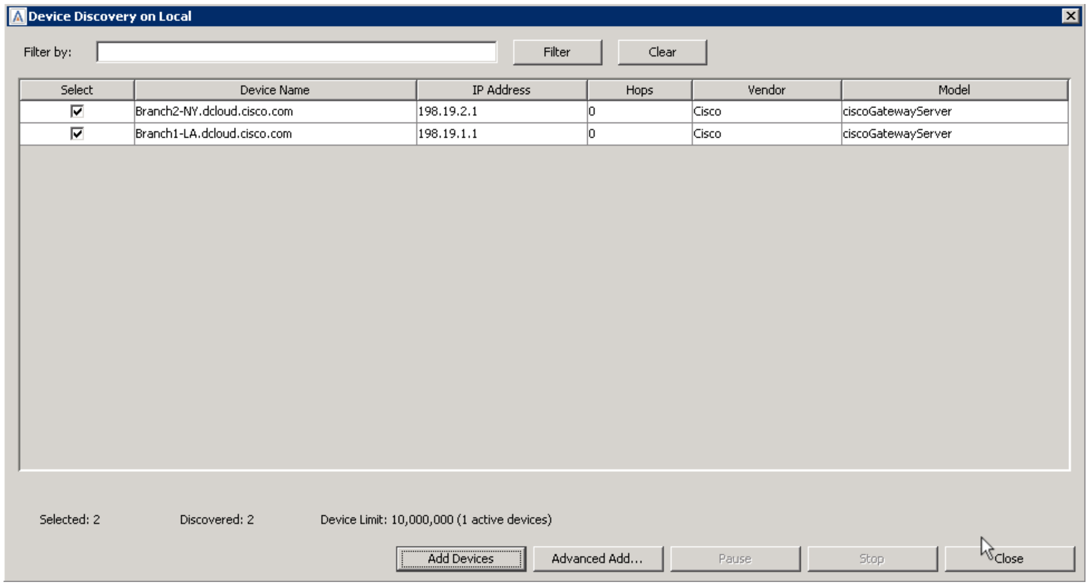


Step 3: Specify node

Local

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

**Note: LiveNX may NOT be able to discover both routers as specified in the above steps. In that case you will need to use the Add Device wizard (See Appendix A2) to add the 2nd device.**



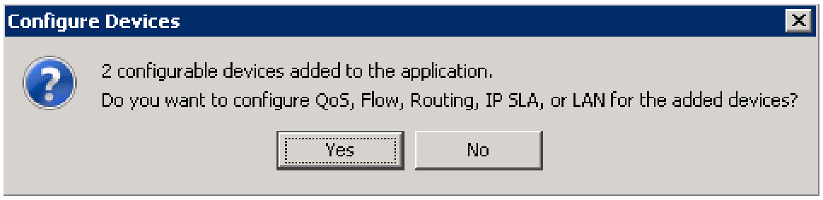
Device Discovery on Local

Filter by:

| Select | Device Name | IP Address | Hops | Vendor | Model |
|---|---|---|---|---|---|
| ☑ | Branch2-NY.dcloud.cisco.com | 198.19.2.1 | 0 | Cisco | ciscoGatewayServer |
| ☑ | Branch1-LA.dcloud.cisco.com | 198.19.1.1 | 0 | Cisco | ciscoGatewayServer |

Selected: 2 Discovered: 2 Device Limit: 10,000,000 (1 active devices)

6. Select Yes on the configure devices dialog.

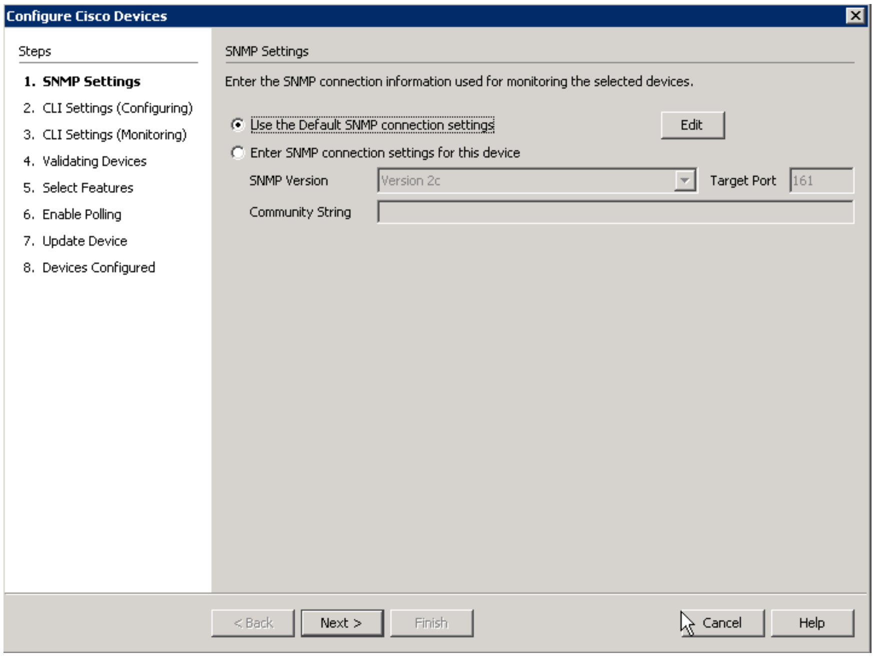


Configure Devices

2 configurable devices added to the application.
Do you want to configure QoS, Flow, Routing, IP SLA, or LAN for the added devices?

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

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



Configure Cisco Devices

Steps

1. **SNMP Settings**
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

SNMP Settings

Enter the SNMP connection information used for monitoring the selected devices.

● Use the Default SNMP connection settings

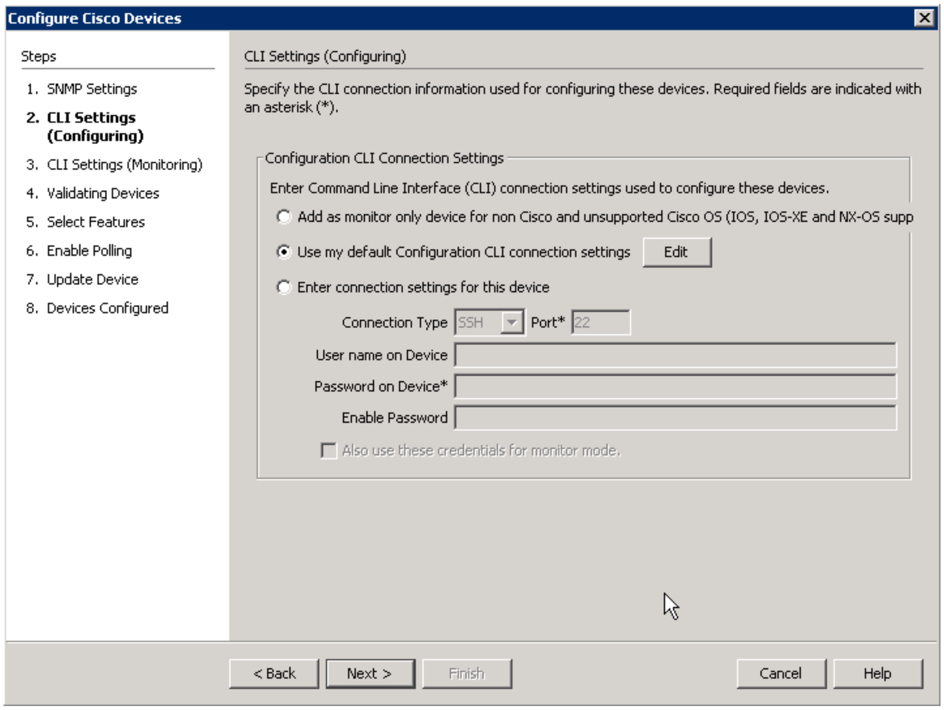
○ Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port: 161

Community String:

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



Configure Cisco Devices

Steps

1. SNMP Settings
2. **CLI Settings (Configuring)**
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Configuring)

Specify the CLI connection information used for configuring these devices. Required fields are indicated with an asterisk (*).

Configuration CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to configure these devices.

○ Add as monitor only device for non Cisco and unsupported Cisco OS (IOS, IOS-XE and NX-OS supp

● Use my default Configuration CLI connection settings

○ Enter connection settings for this device

Connection Type: SSH

Port*: 22

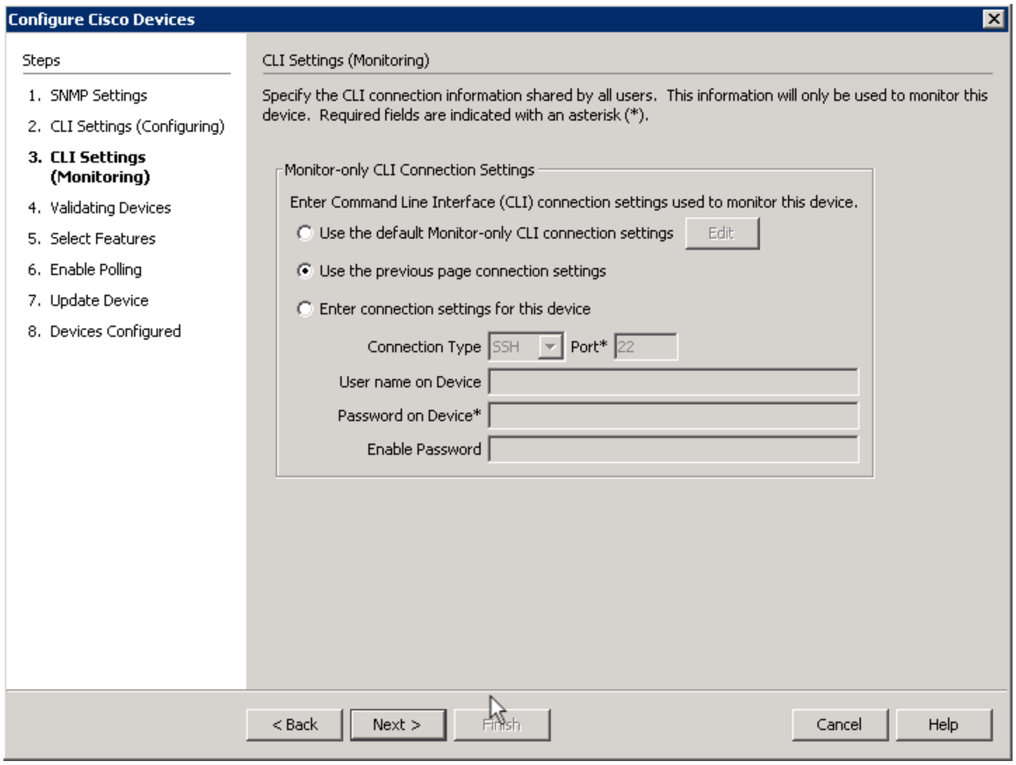
User name on Device:

Password on Device*:

Enable Password:

□ Also use these credentials for monitor mode.

10. Select Use the previous page connection settings.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. **CLI Settings (Monitoring)**
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

CLI Settings (Monitoring)

Specify the CLI connection information shared by all users. This information will only be used to monitor this device. Required fields are indicated with an asterisk (*).

Monitor-only CLI Connection Settings

Enter Command Line Interface (CLI) connection settings used to monitor this device.

○ Use the default Monitor-only CLI connection settings

● Use the previous page connection settings

○ Enter connection settings for this device

Connection Type SSH Port* 22

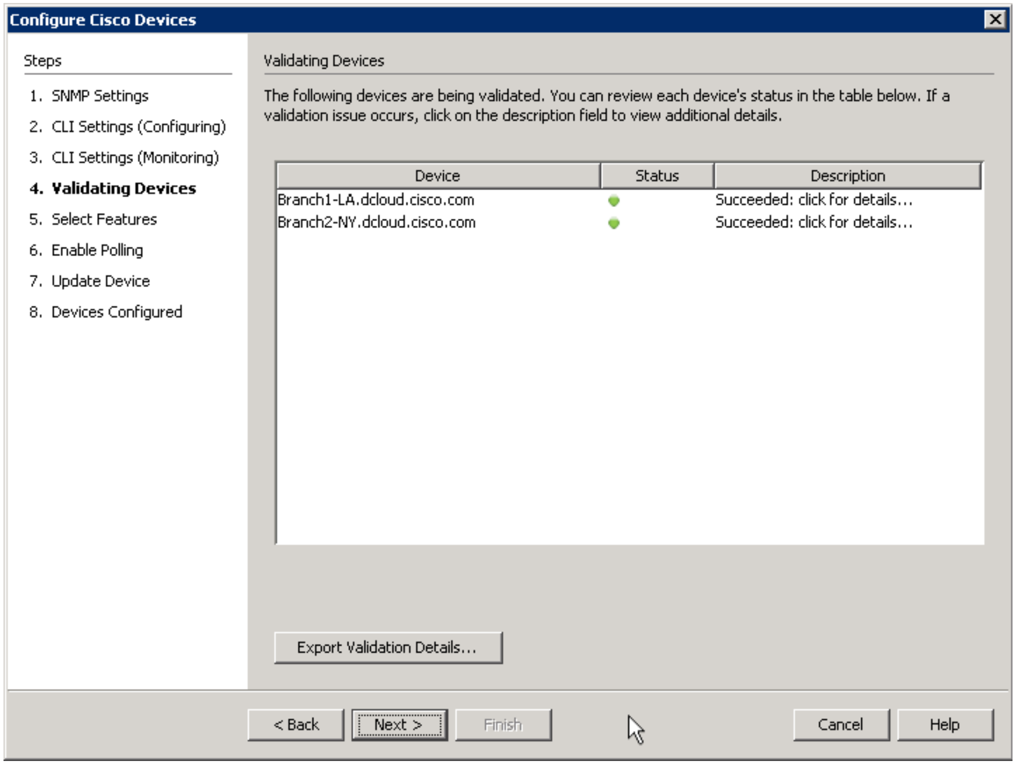
User name on Device

Password on Device*

Enable Password

11. Click Next

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



Configure Cisco Devices

Steps

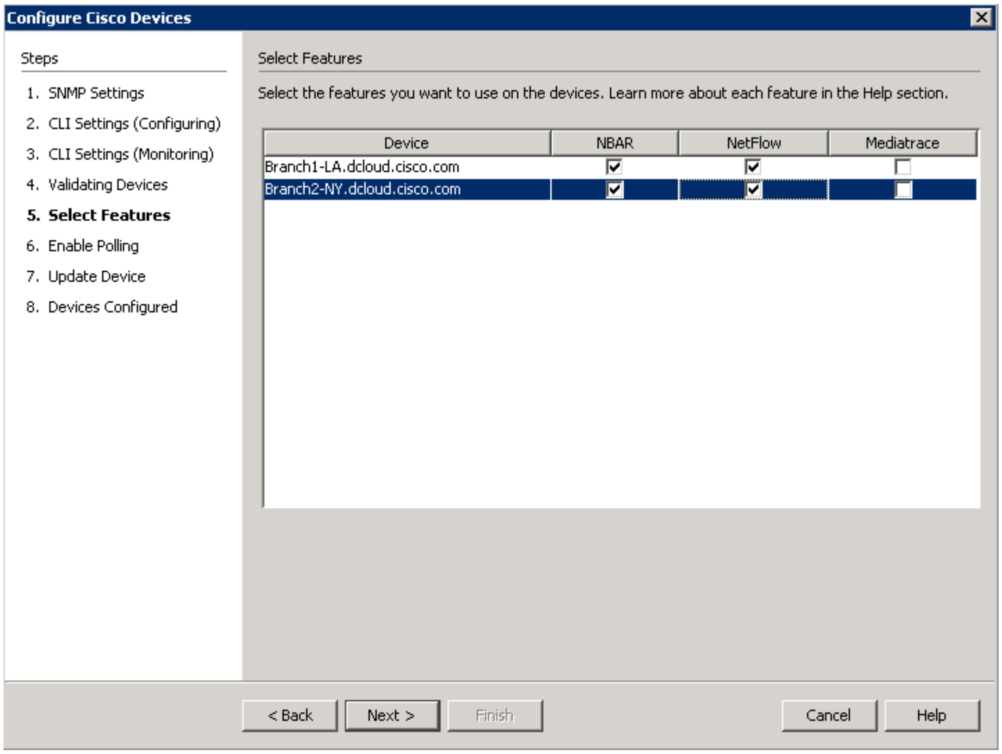
1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. **Validating Devices**
5. Select Features
6. Enable Polling
7. Update Device
8. Devices Configured

Validating Devices

The following devices are being validated. You can review each device's status in the table below. If a validation issue occurs, click on the description field to view additional details.

| Device | Status | Description |
|---|---|---|
| Branch1-LA.dcloud.cisco.com | ● | Succeeded: click for details... |
| Branch2-NY.dcloud.cisco.com | ● | Succeeded: click for details... |

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



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. **Select Features**
6. Enable Polling
7. Update Device
8. Devices Configured

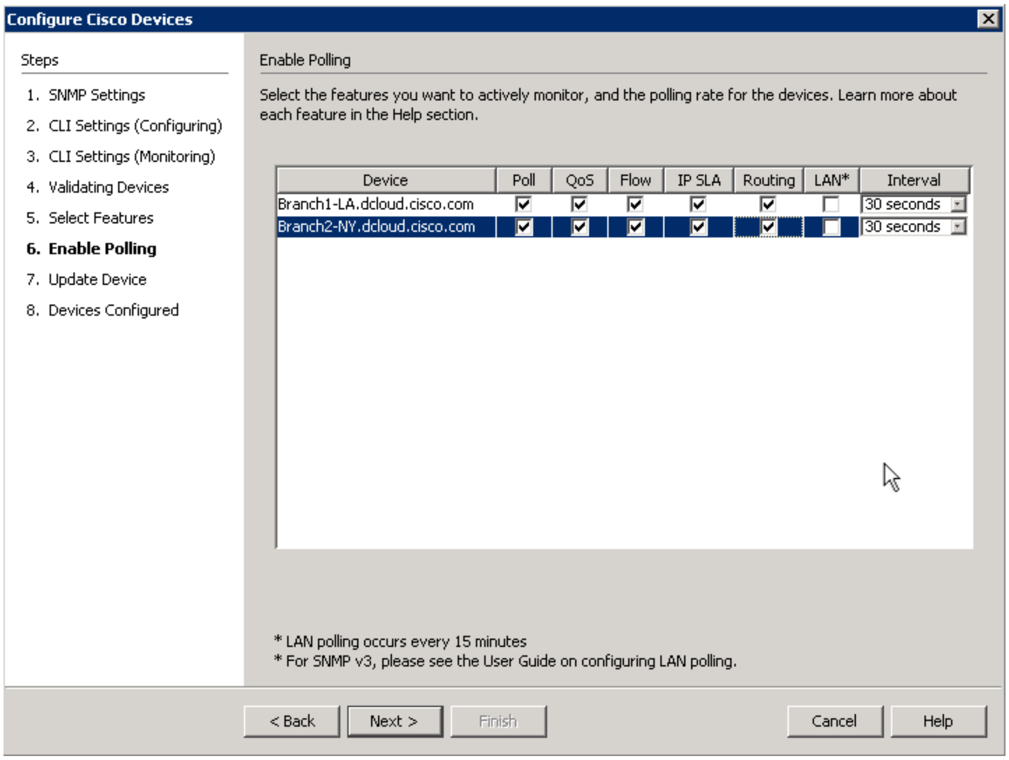
Select Features

Select the features you want to use on the devices. Learn more about each feature in the Help section.

| Device | NBAR | NetFlow | Mediatrace |
|---|---|---|---|
| Branch1-LA.dcloud.cisco.com | ☑ | ☑ | □ |
| Branch2-NY.dcloud.cisco.com | ☑ | ☑ | □ |

14. Select all technologies excepting LAN.

15. Set the interval to 30 seconds for each device, Click Next.



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. **Enable Polling**
7. Update Device
8. Devices Configured

Enable Polling

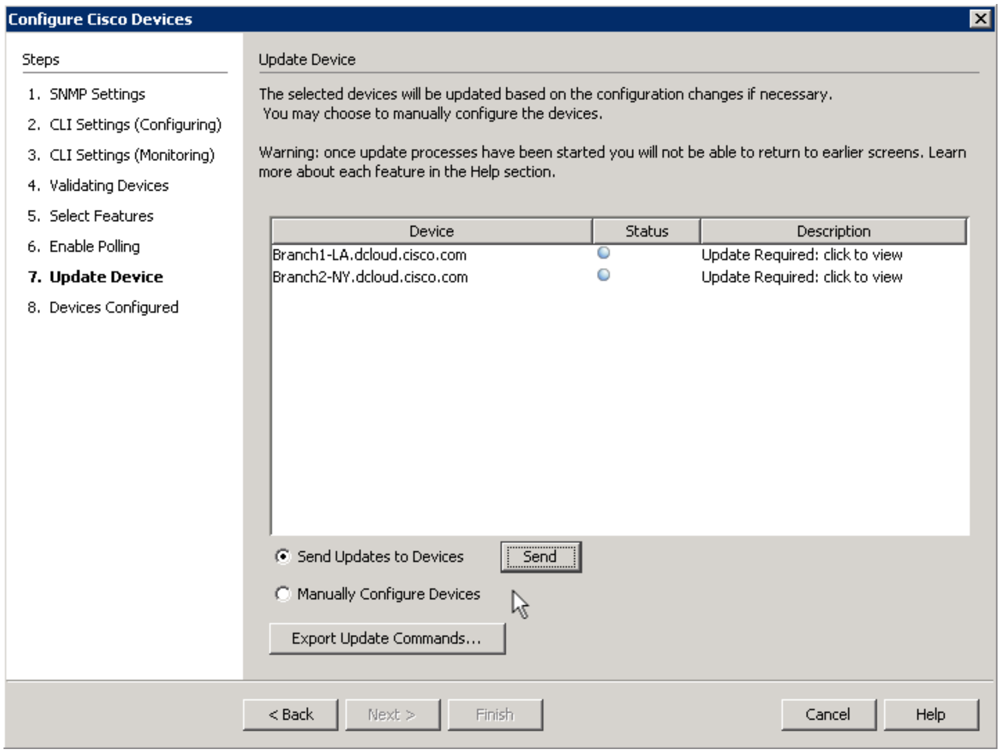
Select the features you want to actively monitor, and the polling rate for the devices. Learn more about each feature in the Help section.

| Device | Poll | QoS | Flow | IP SLA | Routing | LAN* | Interval |
|---|---|---|---|---|---|---|---|
| Branch1-LA.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | ☑ | □ | 30 seconds |
| Branch2-NY.dcloud.cisco.com | ☑ | ☑ | ☑ | ☑ | ☑ | □ | 30 seconds |

* LAN polling occurs every 15 minutes
* For SNMP v3, please see the User Guide on configuring LAN polling.

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

16. Select Send Updates to Devices and click Send.



The selected devices will be updated based on the configuration changes if necessary.
You may choose to manually configure the devices.

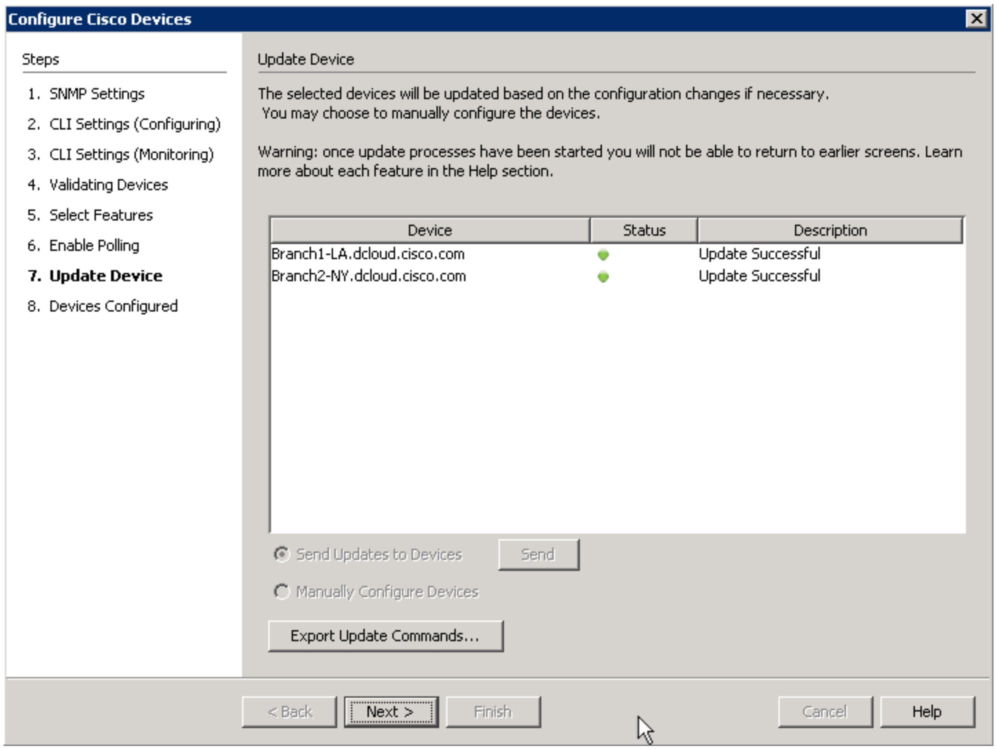
Warning: once update processes have been started you will not be able to return to earlier screens. Learn more about each feature in the Help section.

| Device | Status | Description |
|---|---|---|
| Branch1-LA.dcloud.cisco.com | ● | Update Required: click to view |
| Branch2-NY.dcloud.cisco.com | ● | Update Required: click to view |

● Send Updates to Devices

○ Manually Configure Devices

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



The selected devices will be updated based on the configuration changes if necessary.
You may choose to manually configure the devices.

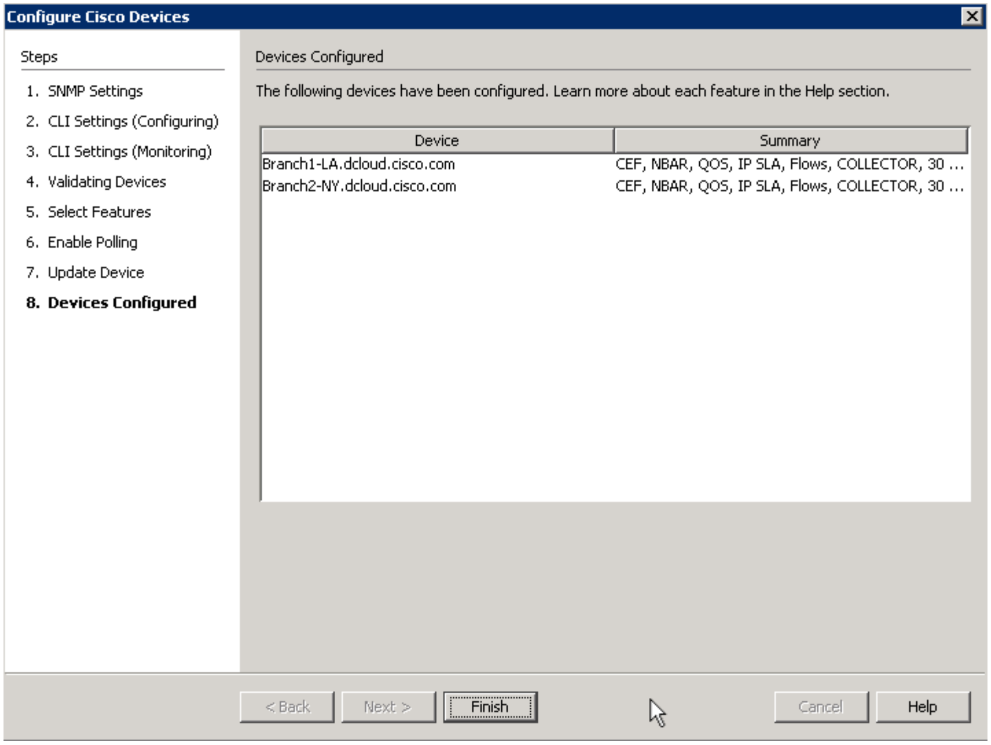
Warning: once update processes have been started you will not be able to return to earlier screens. Learn more about each feature in the Help section.

| Device | Status | Description |
|---|---|---|
| Branch1-LA.dcloud.cisco.com | ● | Update Successful |
| Branch2-NY.dcloud.cisco.com | ● | Update Successful |

● Send Updates to Devices

○ Manually Configure Devices

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



Configure Cisco Devices

Steps

1. SNMP Settings
2. CLI Settings (Configuring)
3. CLI Settings (Monitoring)
4. Validating Devices
5. Select Features
6. Enable Polling
7. Update Device
8. **Devices Configured**

Devices Configured

The following devices have been configured. Learn more about each feature in the Help section.

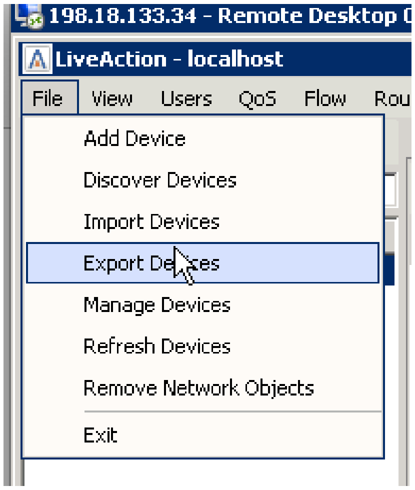
| Device | Summary |
|---|---|
| Branch1-LA.dcloud.cisco.com | CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 ... |
| Branch2-NY.dcloud.cisco.com | CEF, NBAR, QOS, IP SLA, Flows, COLLECTOR, 30 ... |

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

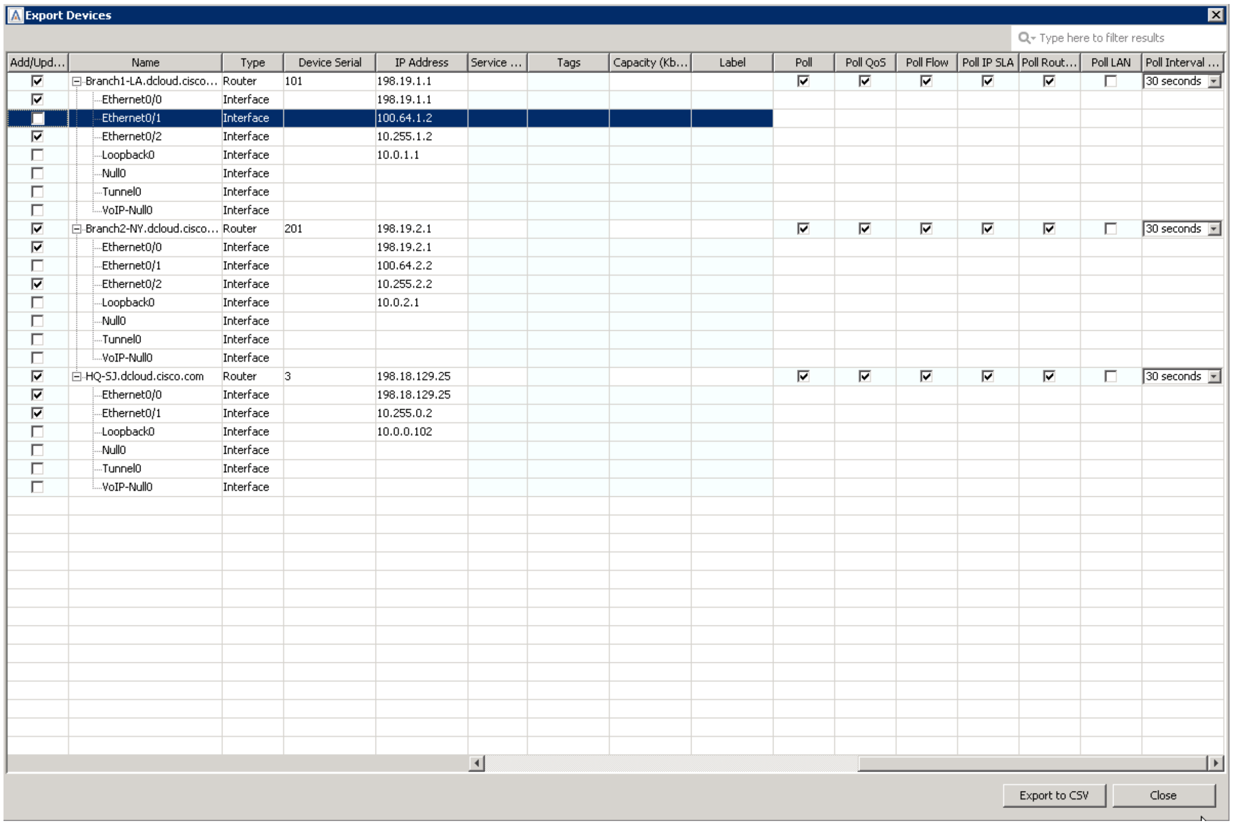
# Lab A.3: Export/Import Device Configuration

Lab Steps:

1. From the File Menu select Export Devices.



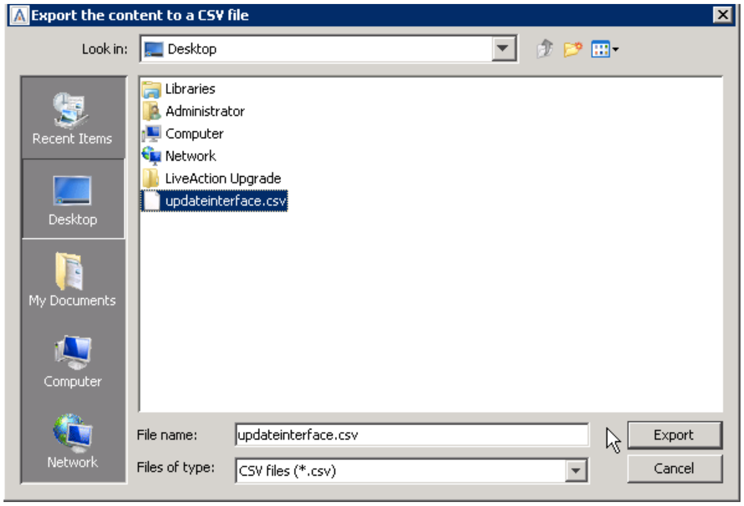
2. Deselect GigabitEthernet1 and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.



| Add/Upd... | Name | Type | Device Serial | IP Address | Service ... | Tags | Capacity (Kb... | Label | Poll | Poll QoS | Poll Flow | Poll IP SLA | Poll Rout... | Poll LAN | Poll Interval ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ⊟ Branch1-LA.dcloud.cisco... | Router | 101 | 198.19.1.1 | | | | | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | 30 seconds |
| ☑ | Ethernet0/0 | Interface | | 198.19.1.1 | | | | | | | | | | | |
| ☐ | Ethernet0/1 | Interface | | 100.64.1.2 | | | | | | | | | | | |
| ☑ | Ethernet0/2 | Interface | | 10.255.1.2 | | | | | | | | | | | |
| ☐ | Loopback0 | Interface | | 10.0.1.1 | | | | | | | | | | | |
| ☐ | Null0 | Interface | | | | | | | | | | | | | |
| ☐ | Tunnel0 | Interface | | | | | | | | | | | | | |
| ☐ | VoIP-Null0 | Interface | | | | | | | | | | | | | |
| ☑ | ⊟ Branch2-NY.dcloud.cisco... | Router | 201 | 198.19.2.1 | | | | | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | 30 seconds |
| ☑ | Ethernet0/0 | Interface | | 198.19.2.1 | | | | | | | | | | | |
| ☐ | Ethernet0/1 | Interface | | 100.64.2.2 | | | | | | | | | | | |
| ☑ | Ethernet0/2 | Interface | | 10.255.2.2 | | | | | | | | | | | |
| ☐ | Loopback0 | Interface | | 10.0.2.1 | | | | | | | | | | | |
| ☐ | Null0 | Interface | | | | | | | | | | | | | |
| ☐ | Tunnel0 | Interface | | | | | | | | | | | | | |
| ☐ | VoIP-Null0 | Interface | | | | | | | | | | | | | |
| ☑ | ⊟ HQ-SJ.dcloud.cisco.com | Router | 3 | 198.18.129.25 | | | | | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | 30 seconds |
| ☑ | Ethernet0/0 | Interface | | 198.18.129.25 | | | | | | | | | | | |
| ☑ | Ethernet0/1 | Interface | | 10.255.0.2 | | | | | | | | | | | |
| ☐ | Loopback0 | Interface | | 10.0.0.102 | | | | | | | | | | | |
| ☐ | Null0 | Interface | | | | | | | | | | | | | |
| ☐ | Tunnel0 | Interface | | | | | | | | | | | | | |
| ☐ | VoIP-Null0 | Interface | | | | | | | | | | | | | |

3. Select Export to csv.

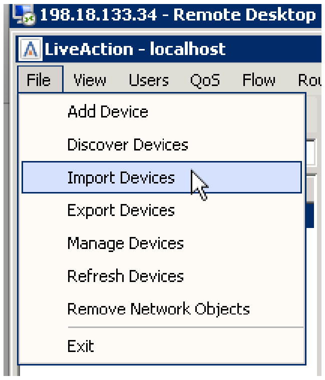
4. On the Export window give the file a name.
5. Export the csv to the desktop, or appropriate directory.



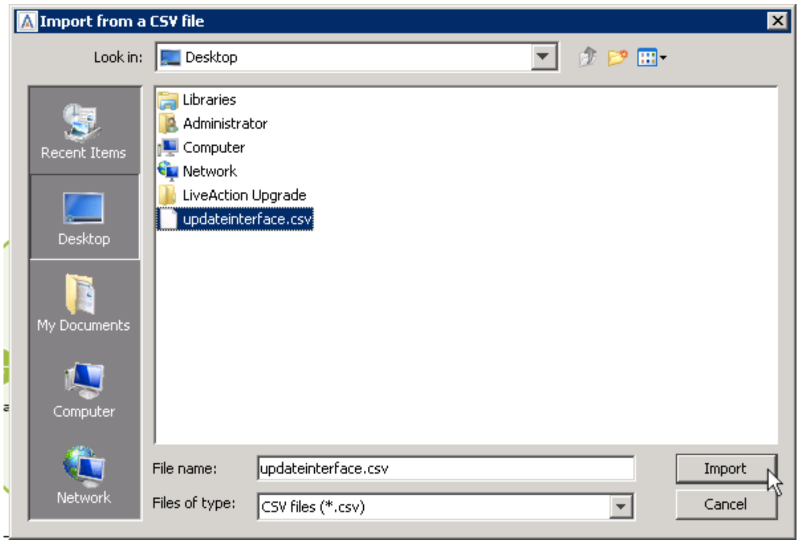
File name: updateinterface.csv

Files of type: CSV files (*.csv)

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



8. Select the file you previously exported.

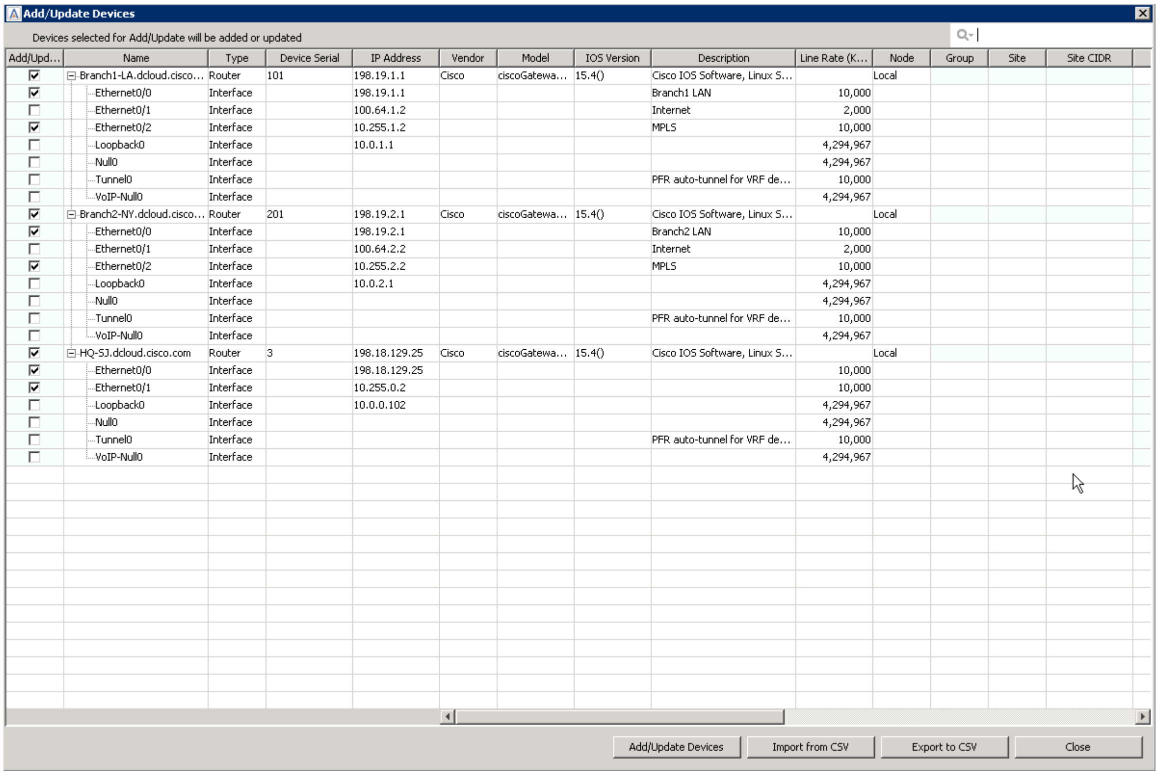


Look in: Desktop

File name: updateinterface.csv

Files of type: CSV files (*.csv)

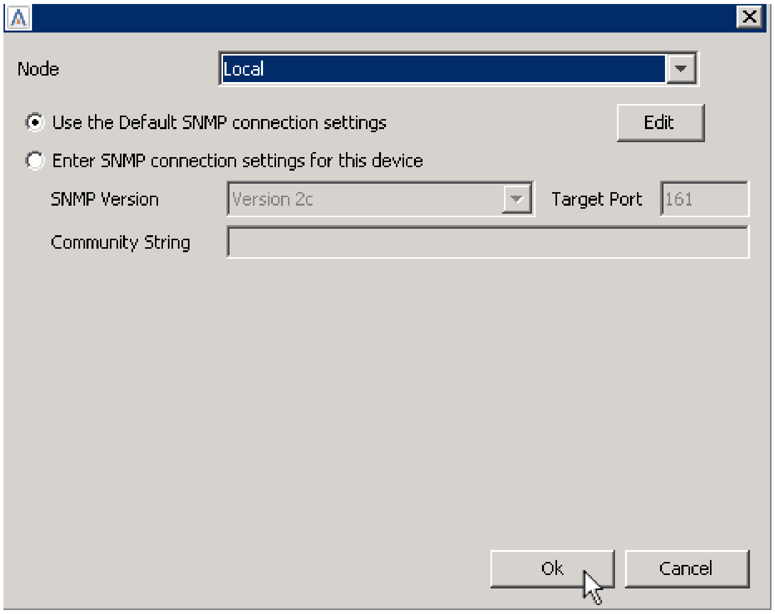
9. Click Add/Update Devices.



Devices selected for Add/Update will be added or updated

| Add/Upd… | Name | Type | Device Serial | IP Address | Vendor | Model | IOS Version | Description | Line Rate (K… | Node | Group | Site | Site CIDR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | ⊟ Branch1-LA.dcloud.cisco… | Router | 101 | 198.19.1.1 | Cisco | ciscoGatewa… | 15.4() | Cisco IOS Software, Linux S… | | Local | | | |
| ☑ | Ethernet0/0 | Interface | | 198.19.1.1 | | | | Branch1 LAN | 10,000 | | | | |
| □ | Ethernet0/1 | Interface | | 100.64.1.2 | | | | Internet | 2,000 | | | | |
| ☑ | Ethernet0/2 | Interface | | 10.255.1.2 | | | | MPLS | 10,000 | | | | |
| □ | Loopback0 | Interface | | 10.0.1.1 | | | | | 4,294,967 | | | | |
| □ | Null0 | Interface | | | | | | | 4,294,967 | | | | |
| □ | Tunnel0 | Interface | | | | | | PFR auto-tunnel for VRF de… | 10,000 | | | | |
| □ | VoIP-Null0 | Interface | | | | | | | 4,294,967 | | | | |
| ☑ | ⊟ Branch2-NY.dcloud.cisco… | Router | 201 | 198.19.2.1 | Cisco | ciscoGatewa… | 15.4() | Cisco IOS Software, Linux S… | | Local | | | |
| ☑ | Ethernet0/0 | Interface | | 198.19.2.1 | | | | Branch2 LAN | 10,000 | | | | |
| □ | Ethernet0/1 | Interface | | 100.64.2.2 | | | | Internet | 2,000 | | | | |
| ☑ | Ethernet0/2 | Interface | | 10.255.2.2 | | | | MPLS | 10,000 | | | | |
| □ | Loopback0 | Interface | | 10.0.2.1 | | | | | 4,294,967 | | | | |
| □ | Null0 | Interface | | | | | | | 4,294,967 | | | | |
| □ | Tunnel0 | Interface | | | | | | PFR auto-tunnel for VRF de… | 10,000 | | | | |
| □ | VoIP-Null0 | Interface | | | | | | | 4,294,967 | | | | |
| ☑ | ⊟ HQ-SJ.dcloud.cisco.com | Router | 3 | 198.18.129.25 | Cisco | ciscoGatewa… | 15.4() | Cisco IOS Software, Linux S… | | Local | | | |
| ☑ | Ethernet0/0 | Interface | | 198.18.129.25 | | | | | 10,000 | | | | |
| ☑ | Ethernet0/1 | Interface | | 10.255.0.2 | | | | | 10,000 | | | | |
| □ | Loopback0 | Interface | | 10.0.0.102 | | | | | 4,294,967 | | | | |
| □ | Null0 | Interface | | | | | | | 4,294,967 | | | | |
| □ | Tunnel0 | Interface | | | | | | PFR auto-tunnel for VRF de… | 10,000 | | | | |
| □ | VoIP-Null0 | Interface | | | | | | | 4,294,967 | | | | |

10. Click OK to use the Default SNMP settings.



Node: Local

● Use the Default SNMP connection settings

○ Enter SNMP connection settings for this device

SNMP Version: Version 2c

Target Port: 161

Community String:

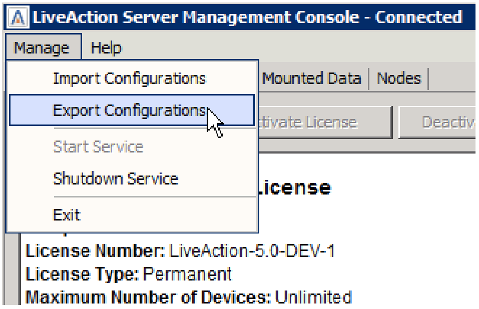
Your Topology Pane will now show the appropriate devices/configurations.

# Lab A.4: Saving Server Configurations

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

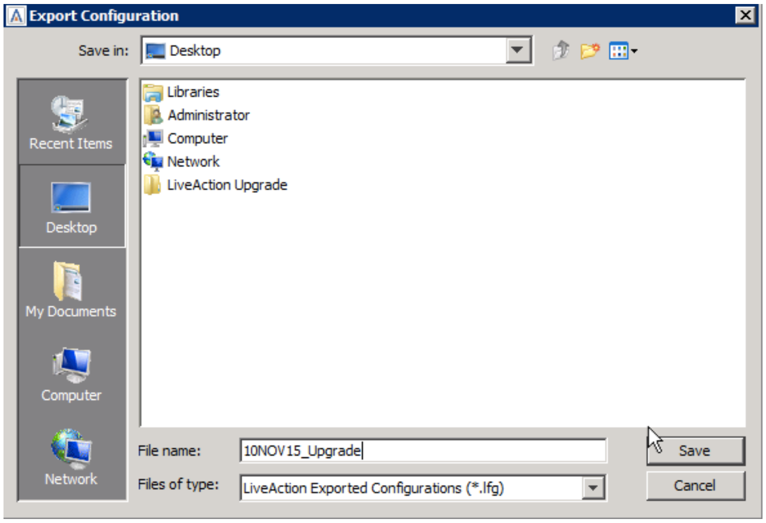
Lab Steps:

1. Open the LiveNX Server Management Console, select Manage and Export Configurations.



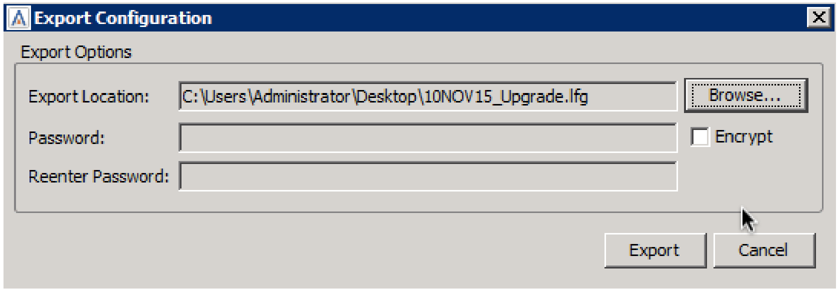
License Number: LiveAction-5.0-DEV-1
License Type: Permanent
Maximum Number of Devices: Unlimited

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



File name: 10NOV15_Upgrade
Files of type: LiveAction Exported Configurations (*.lfg)

3. Click Export to save the file.



Export Location: C:\Users\Administrator\Desktop\10NOV15_Upgrade.lfg
Password:
Reenter Password:
☐ Encrypt

If upgrading the LiveNX Server… After backing up your configuration select Manage, Shutdown Service. When the service is shutdown close the Management Console.

# Lab A.5: Connect via Remote Desktop Connection

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

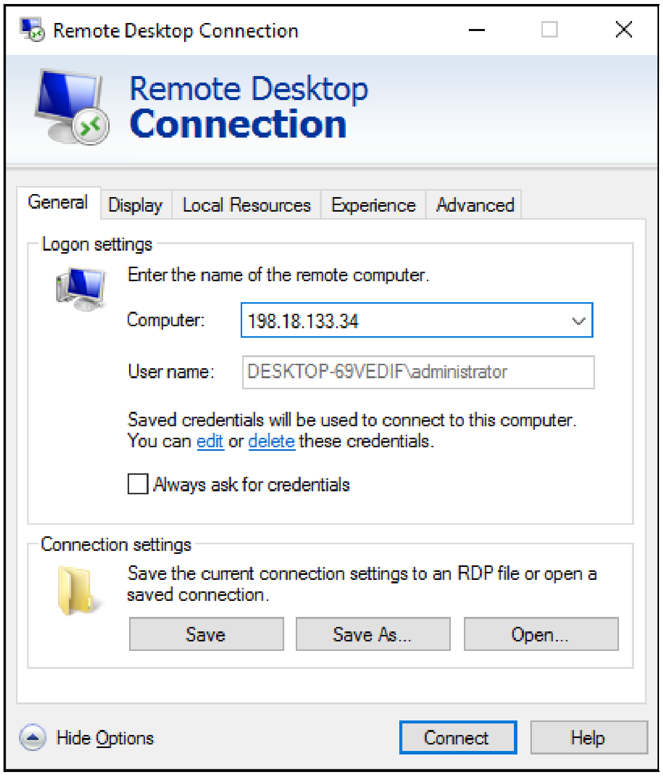
To connect useing Microsoft Remote Desktop on Windows, or a compatible Remote Desktop client on Linux and Macintosh, follow the steps below. On Windows you can typically find Remote Desktop in START > ALL PROGRAMS > ACCESSORIES.

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

Lab Steps:

4. Connect to the virtual Windows 7 Workstation using the IP Address, username, and password pre-printed on the Class Worksheet, unless otherwise instructed.
5. Launch a Remote Desktop client. BEFORE connecting, click the Options button and go to the General tab. (On Macintosh this will be the Preferences menu and Login tab.)

DIAGRAM



Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: 198.18.133.34

User name: DESKTOP-69VEDIF\administrator

Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

□ Always ask for credentials

Connection settings

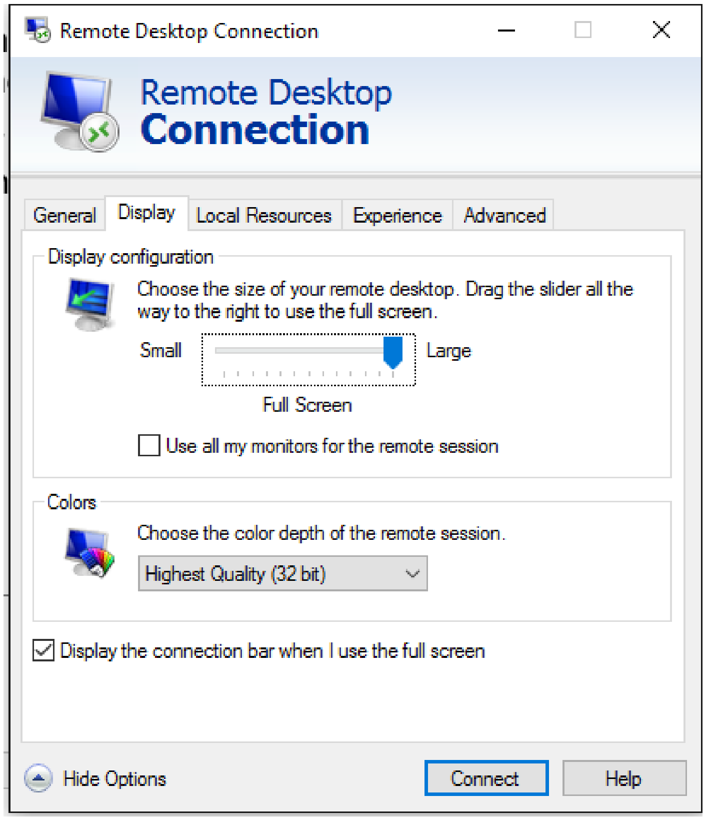
Save the current connection settings to an RDP file or open a saved connection.

   a. Enter the following fields:
      •Computer: **<ipaddress>:20201** (or otherwise defined by instructor)
      •User name: **administrator** (or otherwise defined by instructor)

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

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

DIAGRAM



Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Full Screen

□ Use all my monitors for the remote session

Colors

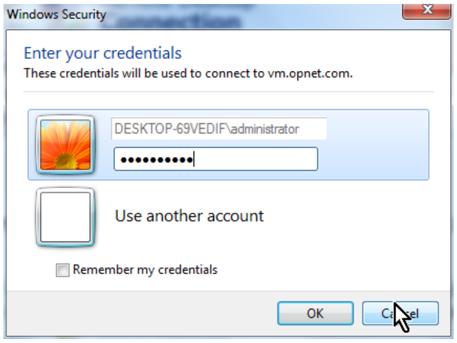
Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

7. Select Connect.
8. Enter the RDC password: **C1sco12345** (or otherwise defined by instructor).

DIAGRAM



Enter your credentials

These credentials will be used to connect to vm.opnet.com.

DESKTOP-69VEDIF\administrator

••••••••••

□ Remember my credentials

9. Click OK.

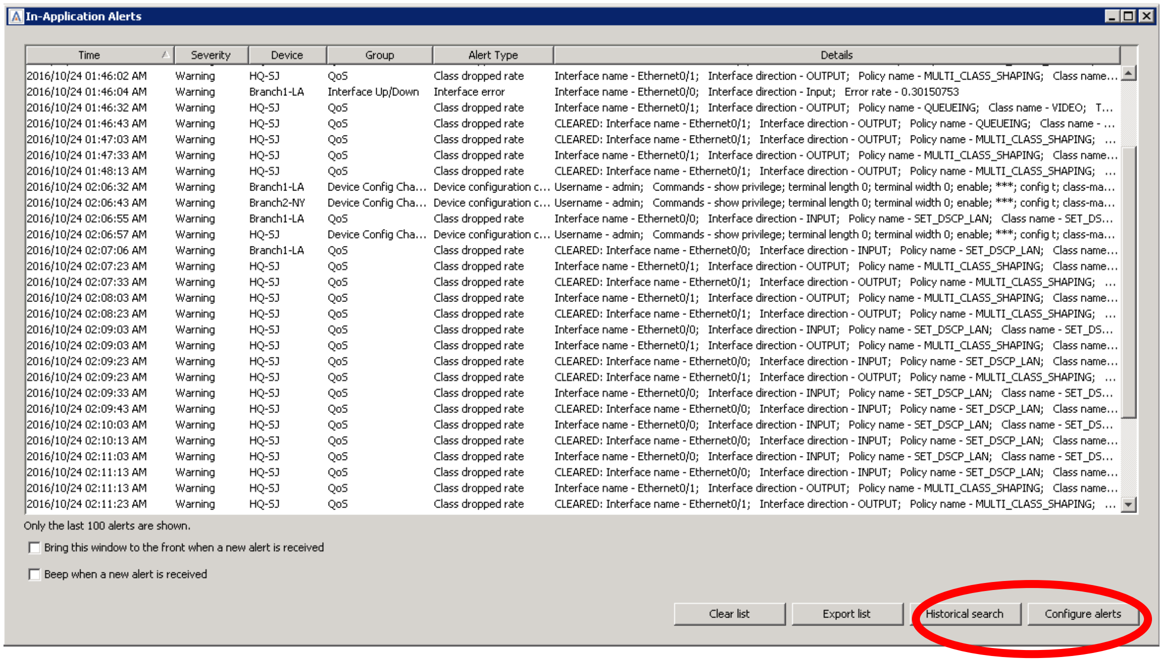
Once successfully connected to your Pod you will see the Windows7 Desktop, and be able to access the LiveNX Server, Client, and other pod resources.

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

# Lab A.6:  Search Alert History

LiveNX's In Application Alert view only show the past 100 events.  To see older events:

1. Select the Historical search.



In-Application Alerts

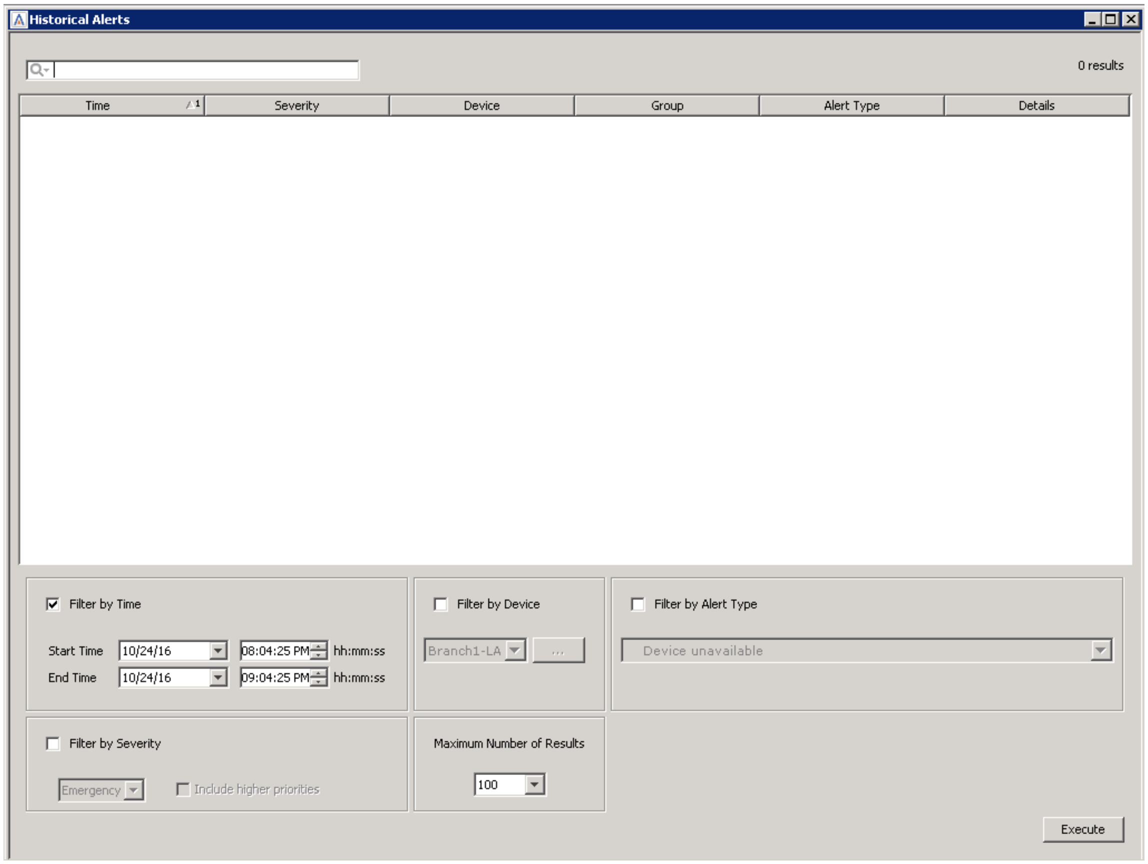
| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/24 01:46:02 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 01:46:04 AM | Warning | Branch1-LA | Interface Up/Down | Interface error | Interface name - Ethernet0/0;  Interface direction - Input;  Error rate - 0.30150753 |
| 2016/10/24 01:46:32 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - QUEUEING;  Class name - VIDEO;  T... |
| 2016/10/24 01:46:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - QUEUEING;  Class name - ... |
| 2016/10/24 01:47:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |
| 2016/10/24 01:47:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 01:48:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |
| 2016/10/24 02:06:32 AM | Warning | Branch1-LA | Device Config Cha... | Device configuration c... | Username - admin;  Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma... |
| 2016/10/24 02:06:43 AM | Warning | Branch2-NY | Device Config Cha... | Device configuration c... | Username - admin;  Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma... |
| 2016/10/24 02:06:55 AM | Warning | Branch1-LA | QoS | Class dropped rate | Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name - SET_DS... |
| 2016/10/24 02:06:57 AM | Warning | HQ-SJ | Device Config Cha... | Device configuration c... | Username - admin;  Commands - show privilege; terminal length 0; terminal width 0; enable; ***; config t; class-ma... |
| 2016/10/24 02:07:06 AM | Warning | Branch1-LA | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name... |
| 2016/10/24 02:07:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 02:07:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |
| 2016/10/24 02:08:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 02:08:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name - SET_DS... |
| 2016/10/24 02:09:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name... |
| 2016/10/24 02:09:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |
| 2016/10/24 02:09:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name - SET_DS... |
| 2016/10/24 02:09:43 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name... |
| 2016/10/24 02:10:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name - SET_DS... |
| 2016/10/24 02:10:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name... |
| 2016/10/24 02:11:03 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name - SET_DS... |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/0;  Interface direction - INPUT;  Policy name - SET_DSCP_LAN;  Class name... |
| 2016/10/24 02:11:13 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  Class name... |
| 2016/10/24 02:11:23 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1;  Interface direction - OUTPUT;  Policy name - MULTI_CLASS_SHAPING;  ... |

Only the last 100 alerts are shown.

□ Bring this window to the front when a new alert is received

□ Beep when a new alert is received

. The Historical Alerts Dialog appears.



Historical Alerts

0 results

| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|

☑ Filter by Time

Start Time 10/24/16 08:04:25 PM hh:mm:ss

End Time 10/24/16 09:04:25 PM hh:mm:ss

□ Filter by Device

Branch1-LA

□ Filter by Alert Type

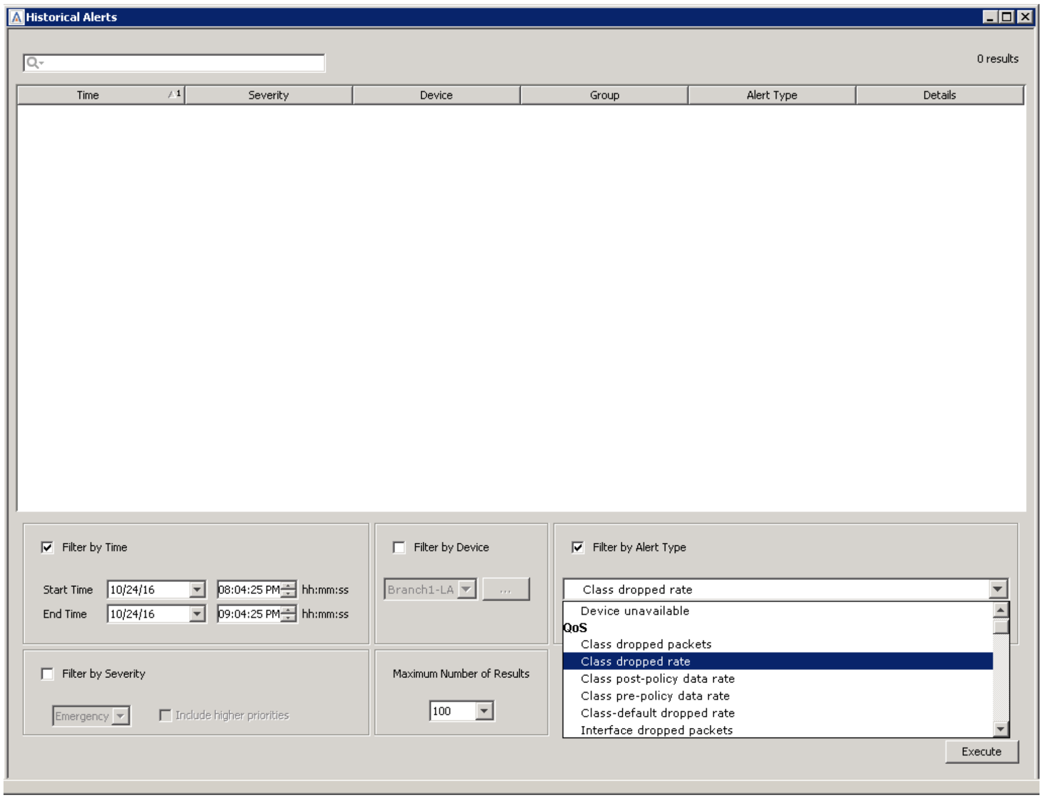
Device unavailable

□ Filter by Severity

Emergency □ Include higher priorities

Maximum Number of Results 100

2. Select the time range, device, number of results, and Alert Type filters
3. To look specifically for QoS alerts set Filter by Alert type to “Class Drop Rate”:



Historical Alerts

0 results

| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|

☑ Filter by Time

Start Time 10/24/16 08:04:25 PM hh:mm:ss

End Time 10/24/16 09:04:25 PM hh:mm:ss

☐ Filter by Device

Branch1-LA

☑ Filter by Alert Type

Class dropped rate

Device unavailable
QoS
Class dropped packets
Class dropped rate
Class post-policy data rate
Class pre-policy data rate
Class-default dropped rate
Interface dropped packets

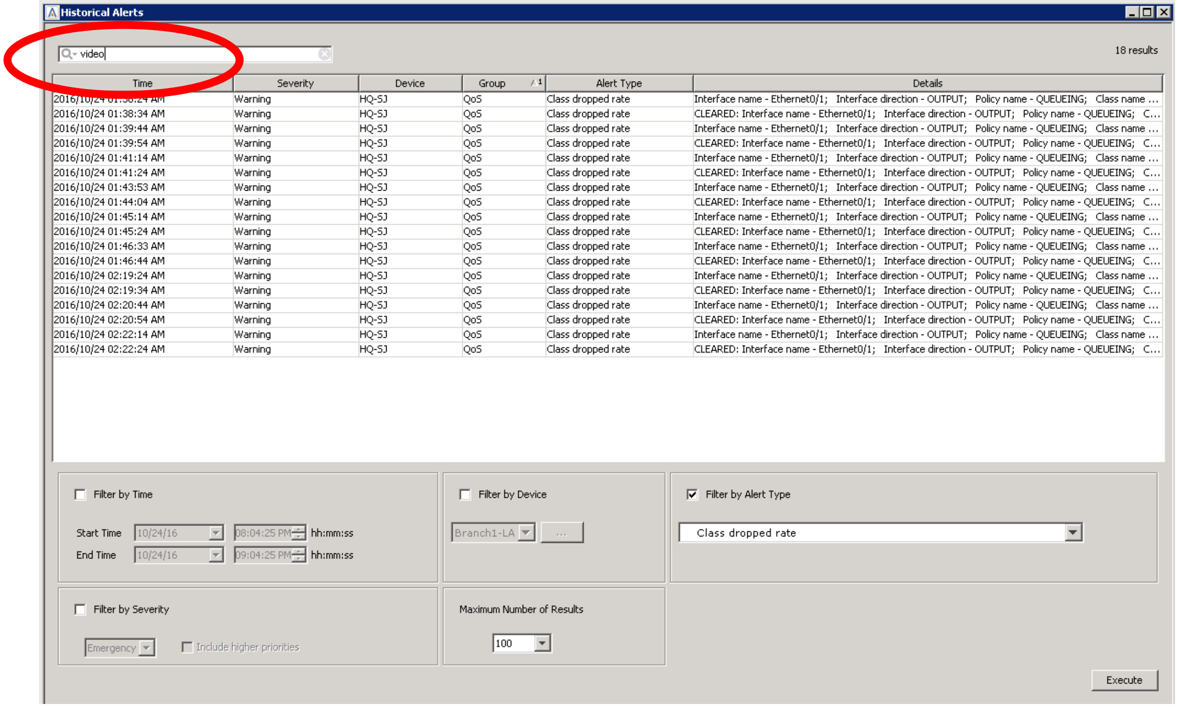
☐ Filter by Severity

Emergency ☐ Include higher priorities

Maximum Number of Results

100

4. Use the filter to find the class of interest. In this example the search was for the term “video”.



Historical Alerts

video

18 results

| Time | Severity | Device | Group | Alert Type | Details |
|---|---|---|---|---|---|
| 2016/10/24 01:38:24 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:38:34 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 01:39:44 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:39:54 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 01:41:14 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:41:24 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 01:43:53 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:44:04 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 01:45:14 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:45:24 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 01:46:33 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 01:46:44 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 02:19:24 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 02:19:34 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 02:20:44 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 02:20:54 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |
| 2016/10/24 02:22:14 AM | Warning | HQ-SJ | QoS | Class dropped rate | Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; Class name ... |
| 2016/10/24 02:22:24 AM | Warning | HQ-SJ | QoS | Class dropped rate | CLEARED: Interface name - Ethernet0/1; Interface direction - OUTPUT; Policy name - QUEUEING; C... |

☐ Filter by Time

Start Time 10/24/16 08:04:25 PM hh:mm:ss

End Time 10/24/16 09:04:25 PM hh:mm:ss

☐ Filter by Device

Branch1-LA

☑ Filter by Alert Type

Class dropped rate

☐ Filter by Severity

Emergency ☐ Include higher priorities

Maximum Number of Results

100

The results are for past issues with the VIDEO class.