# LiveAction Training

*Lab Workbook Pt.2*

## 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 0.1:  Connect to the Lab Network

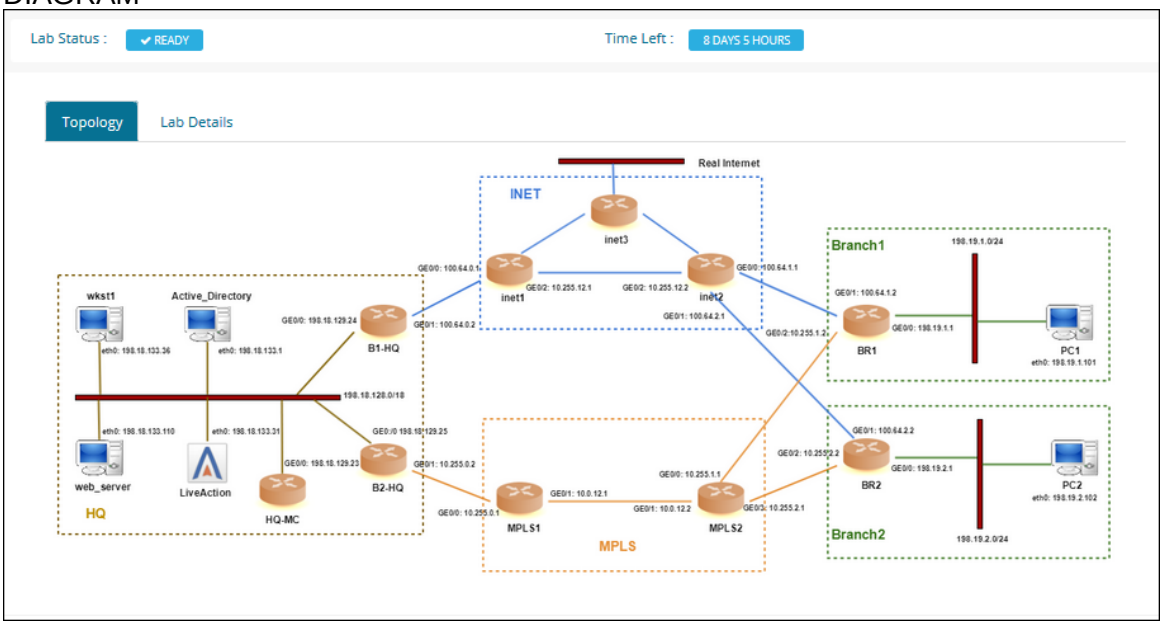
For this class, each attendee or Student will connect to and manage their own LiveNX installation.  In this lab you will connect to the classroom lab environment.  In some locations you may first be asked to connect your laptop to the Internet.

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




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

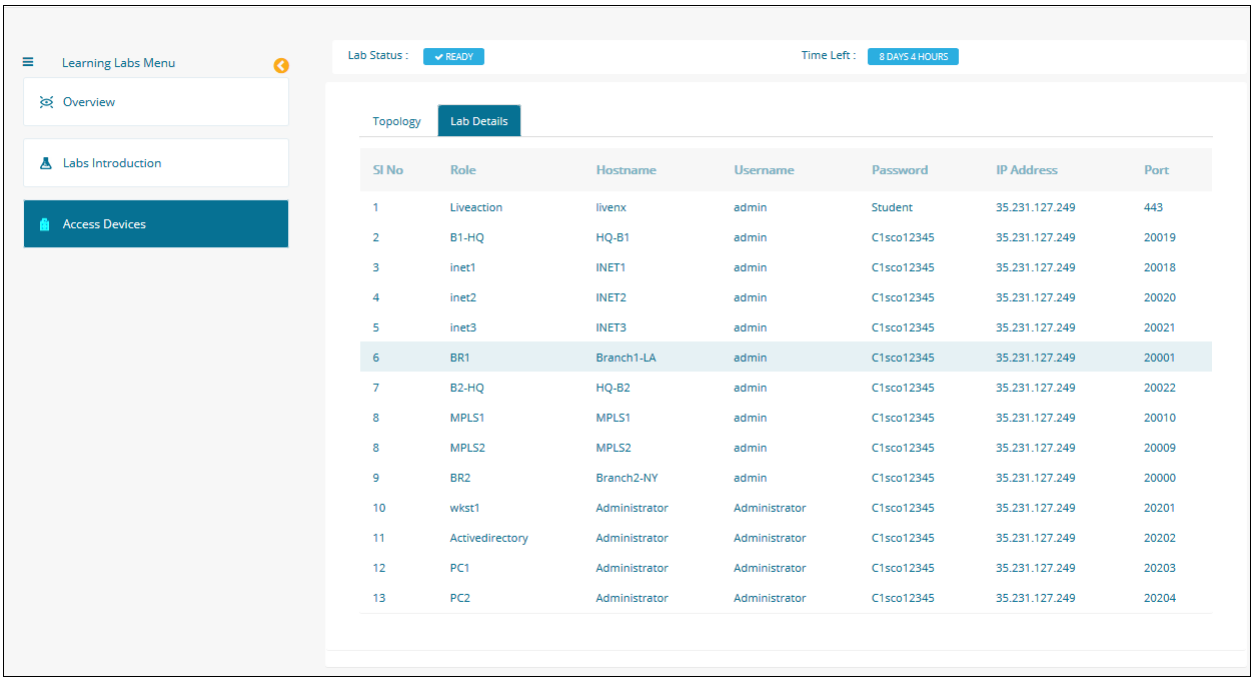
---

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




| Sl 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.

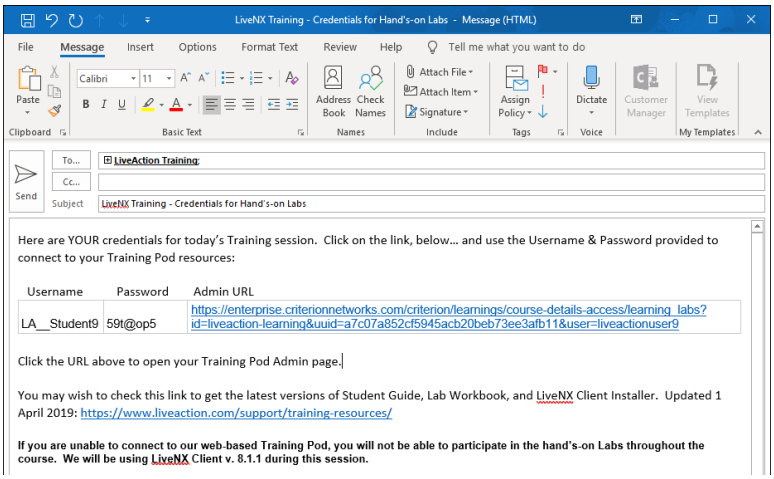
Note: **Make sure to consult the Infrastructure Diagram and worksheets, as well as specific classroom instructions for names, IP addresses, and other parameters.** The screen shots in this Lab Workbook are *examples* **which may not reflect the appropriate parameters for the classroom and/or your specific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

# Lab 0.2: 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

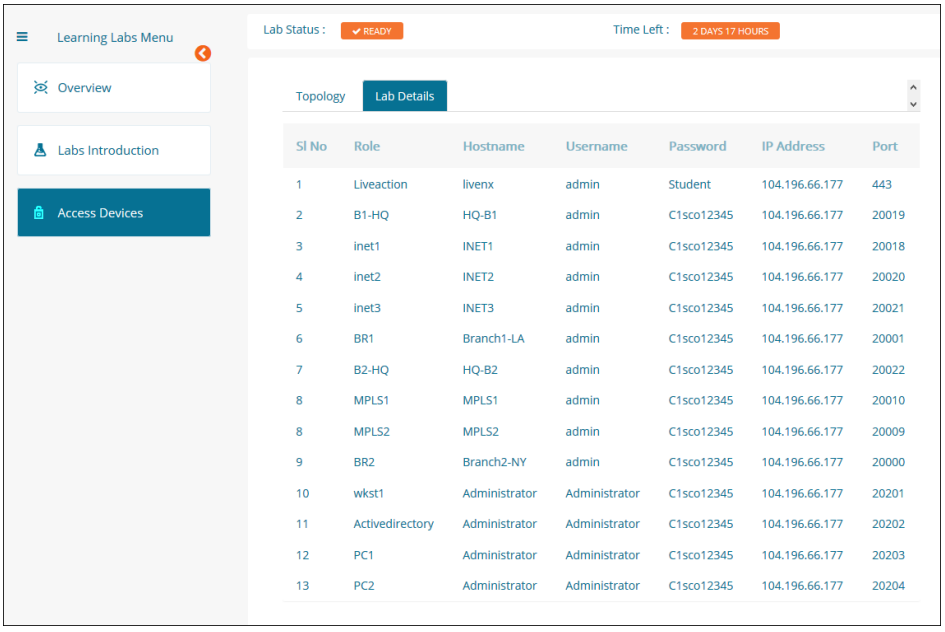



Lab Steps:

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 1

## Lab 1:  QoS Configuration

# Lab 1.0:  Introduction to QoS

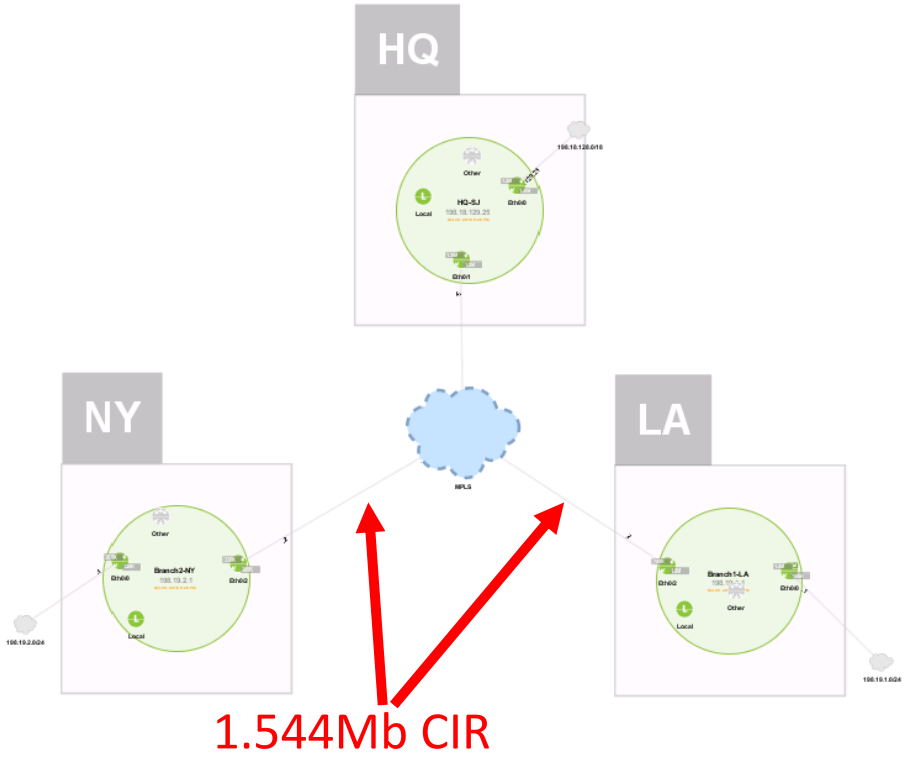
In this lab we are going to walk through the story of implementing QoS for a small WAN network using LiveNX. When complete we will have used LiveNX to:

- 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.

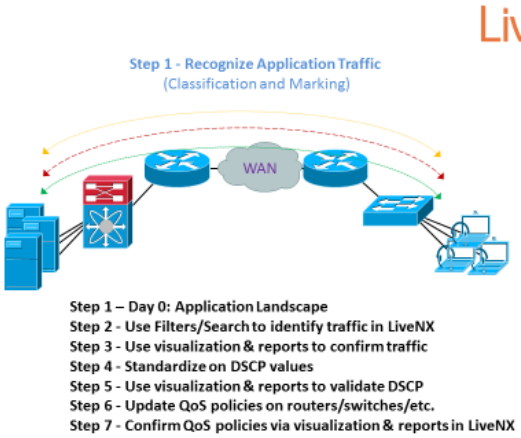



Remember from the presentation that QoS is done in 4 steps:

- 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.




**Day 0 Tasks**

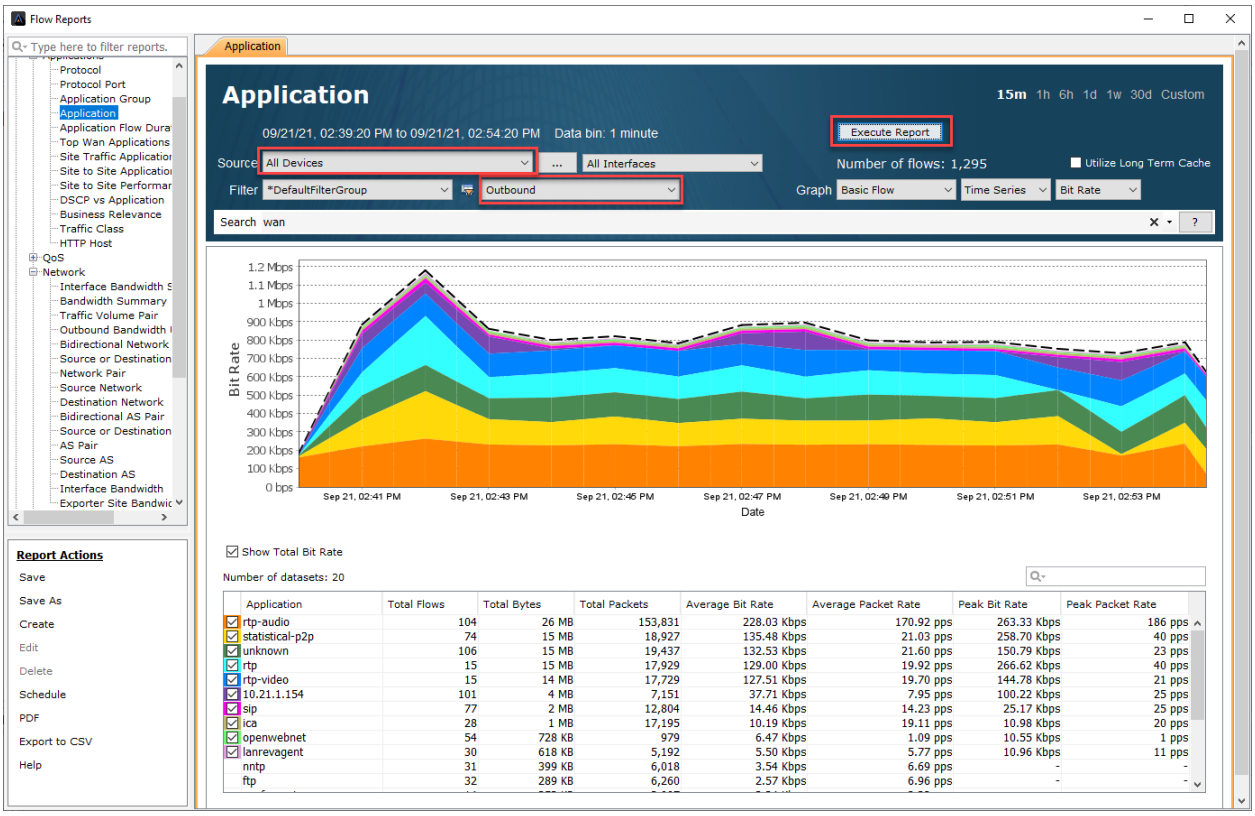
The first item that must be understood to successfully implement QoS is to understand a business's critical applications. In our sample network the following applications have been defined as the highest priority:

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

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

# Lab 1.1: Run Baseline Reports

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**



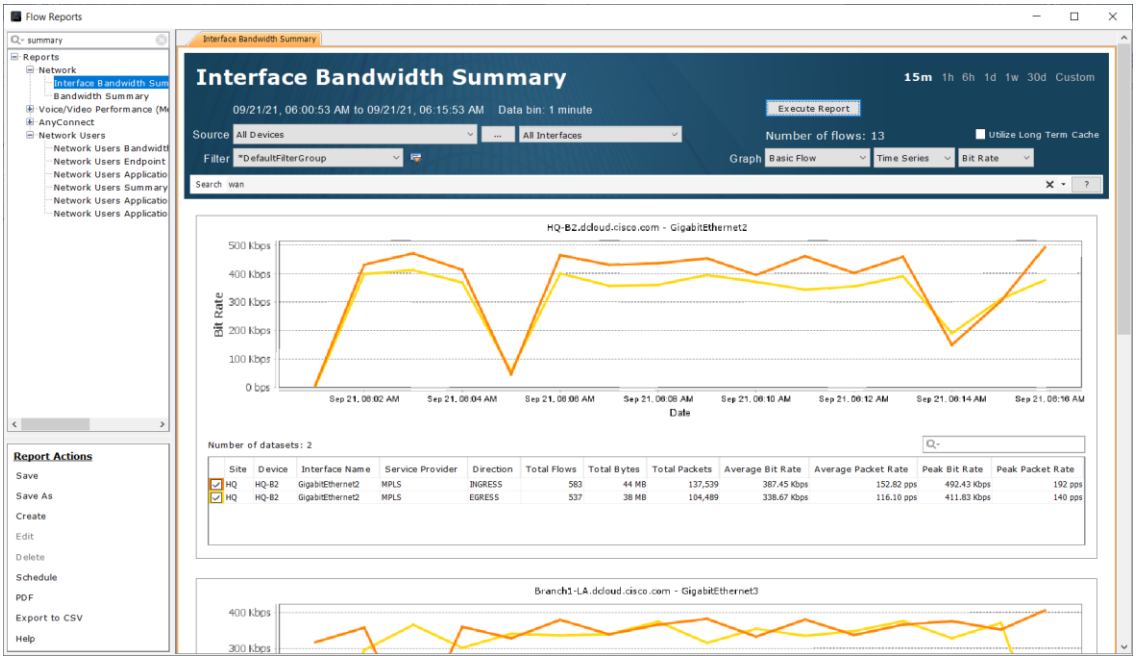

| Application | Total Flows | Total Bytes | Total Packets | Average Bit Rate | Average Packet Rate | Peak Bit Rate | Peak Packet Rate |
|---|---|---|---|---|---|---|---|
| rtp-audio | 104 | 26 MB | 153,831 | 228.03 Kbps | 170.92 pps | 263.33 Kbps | 186 pps |
| statistical-p2p | 74 | 15 MB | 18,927 | 135.48 Kbps | 21.03 pps | 258.70 Kbps | 40 pps |
| unknown | 106 | 15 MB | 19,437 | 132.53 Kbps | 21.60 pps | 150.79 Kbps | 23 pps |
| rtp | 15 | 15 MB | 17,929 | 129.00 Kbps | 19.92 pps | 266.62 Kbps | 40 pps |
| rtp-video | 15 | 14 MB | 17,729 | 127.51 Kbps | 19.70 pps | 144.78 Kbps | 21 pps |
| 10.21.1.154 | 101 | 4 MB | 7,151 | 37.71 Kbps | 7.95 pps | 100.22 Kbps | 25 pps |
| sip | 77 | 2 MB | 12,804 | 14.46 Kbps | 14.23 pps | 25.17 Kbps | 25 pps |
| ica | 28 | 1 MB | 17,195 | 10.19 Kbps | 19.11 pps | 10.98 Kbps | 20 pps |
| openwebnet | 54 | 728 KB | 979 | 6.47 Kbps | 1.09 pps | 10.55 Kbps | 1 pps |
| lanrevagent | 30 | 618 KB | 5,192 | 5.50 Kbps | 5.77 pps | 10.96 Kbps | 11 pps |
| nntp | 31 | 399 KB | 6,018 | 3.54 Kbps | 6.69 pps | - | - |
| ftp | 32 | 289 KB | 6,260 | 2.57 Kbps | 6.96 pps | - | - |

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

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




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"

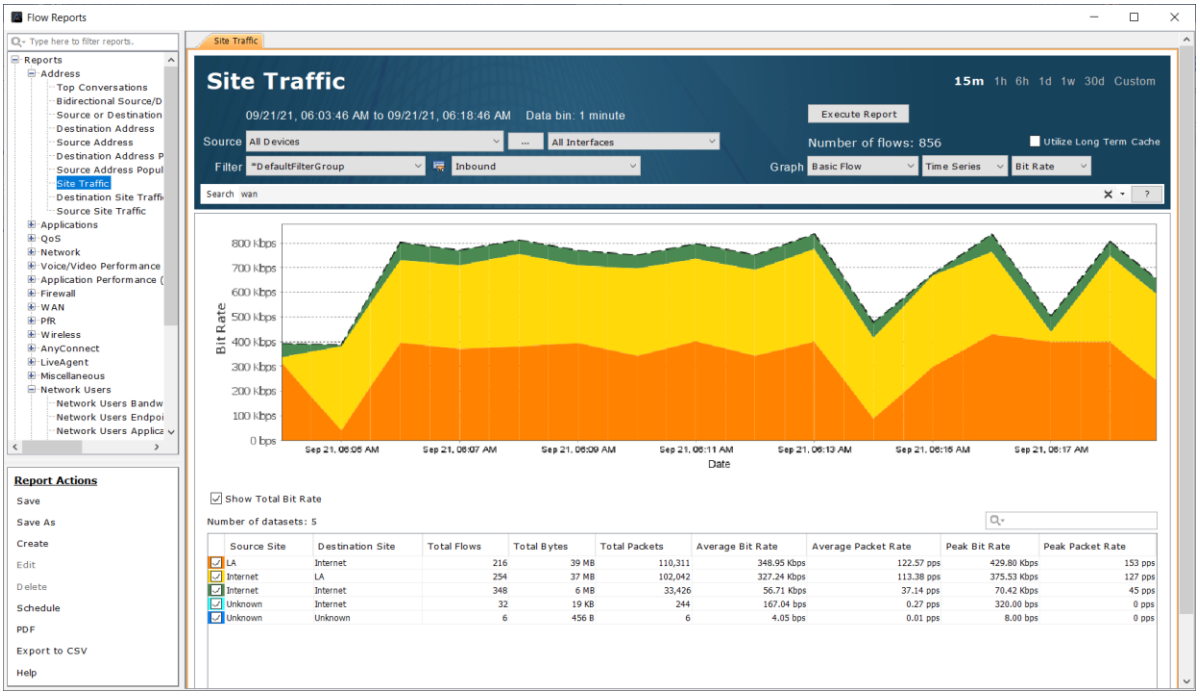
This provides an understanding of the utilization of just Voice (rtp) on each WAN circuit.

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**

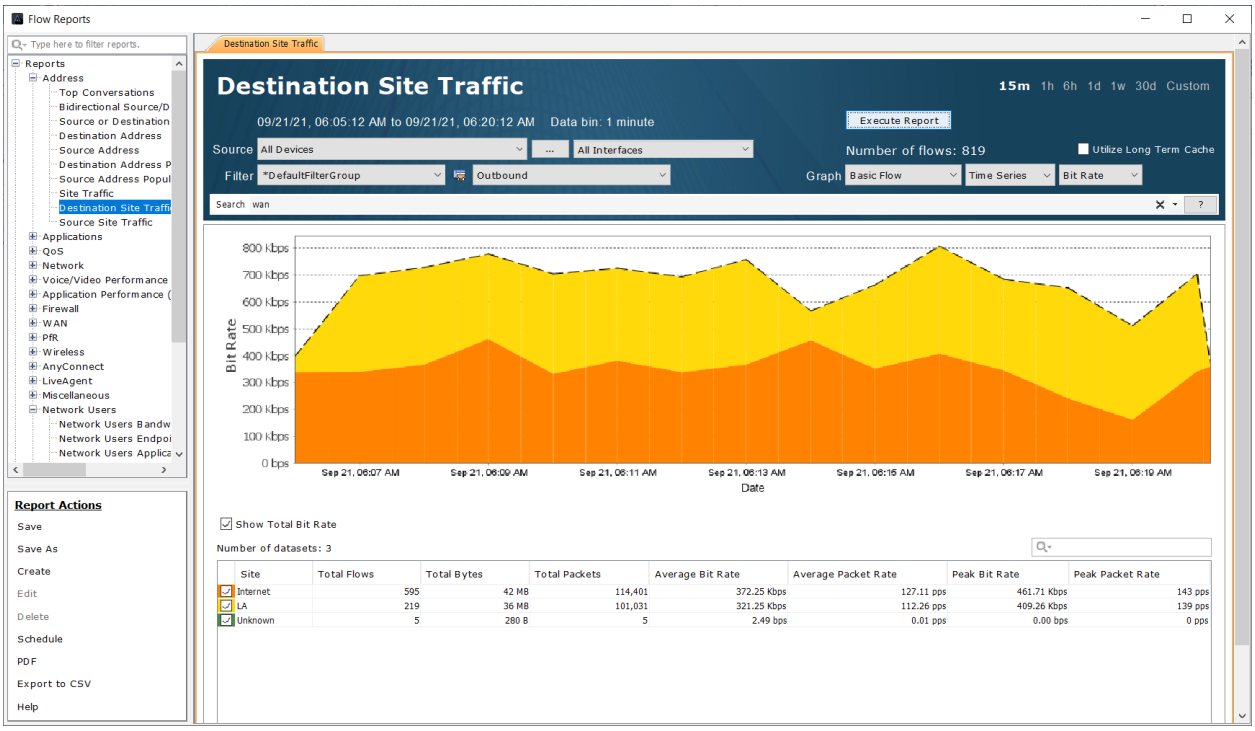


Observe the breakdown of bandwidth between site pairs.

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**

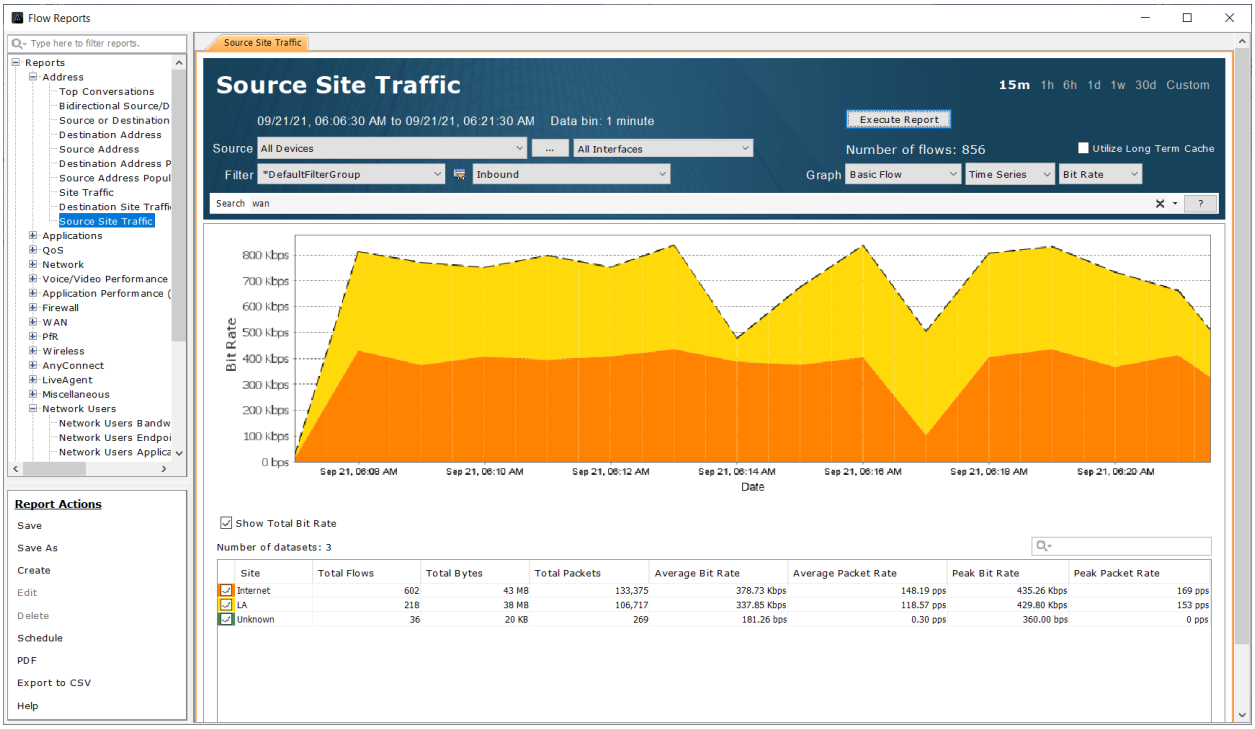



Observe which sites are being sent the most data.

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**




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.

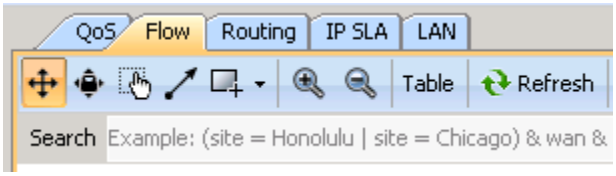
# Lab 1.2: Building Filters

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.

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.

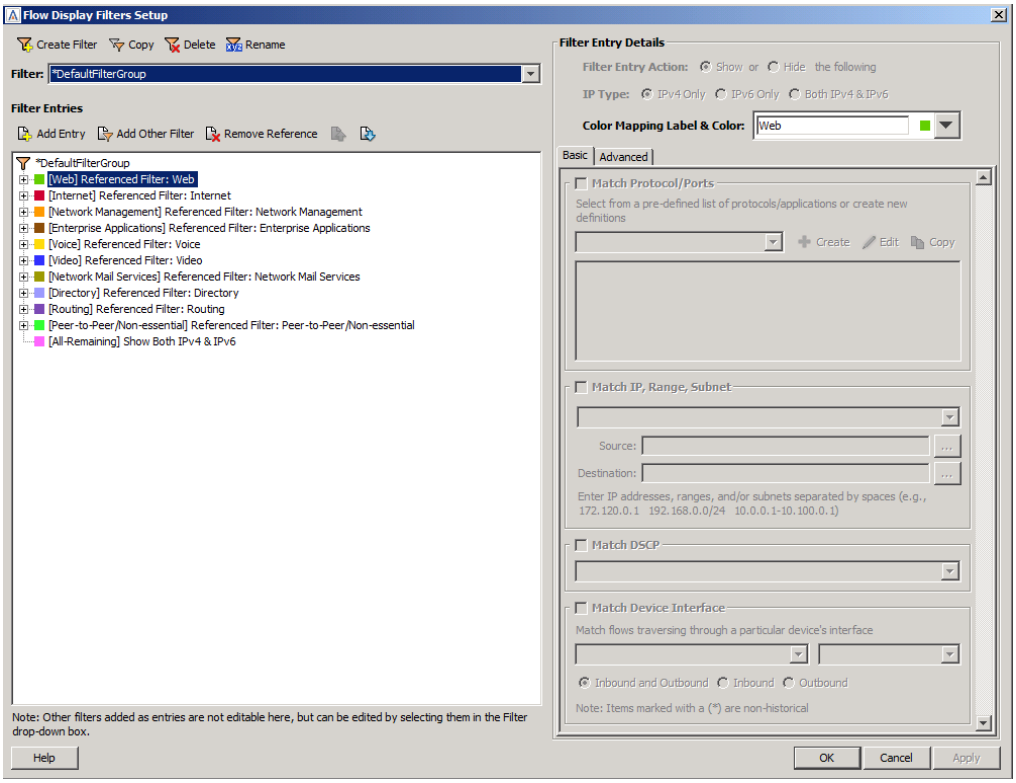
Lab Steps:

1. From the LiveAction map, select the **Flow** Tab

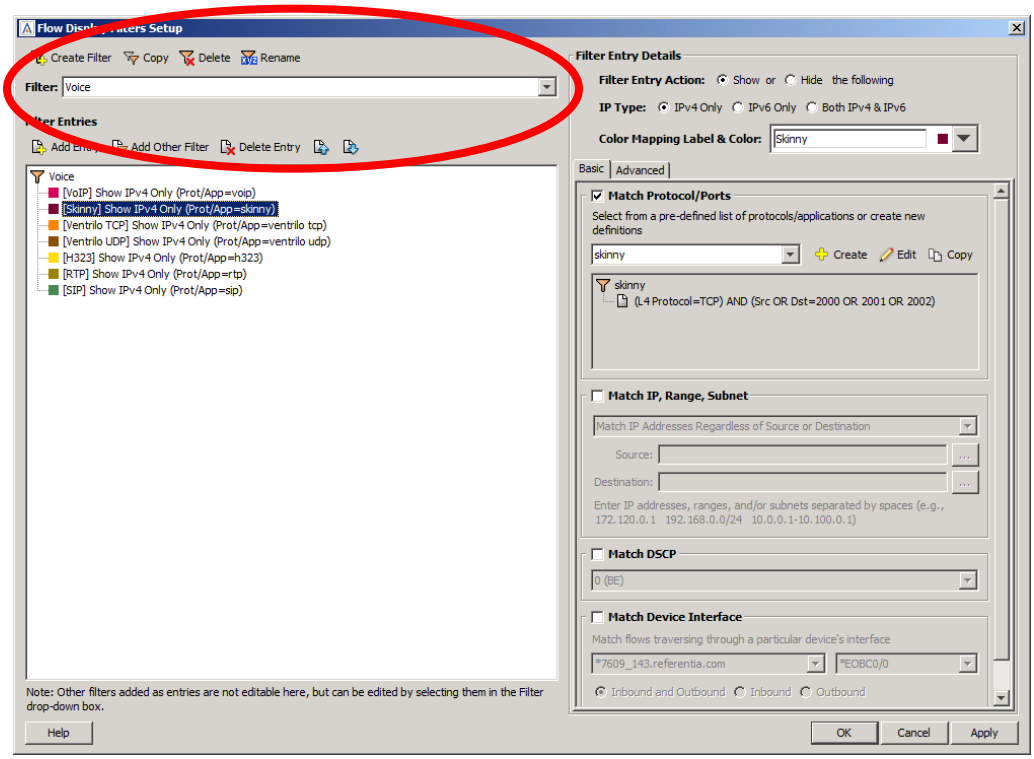



2. To Edit or Create a filter, click the  icon from the options at the top of the map:

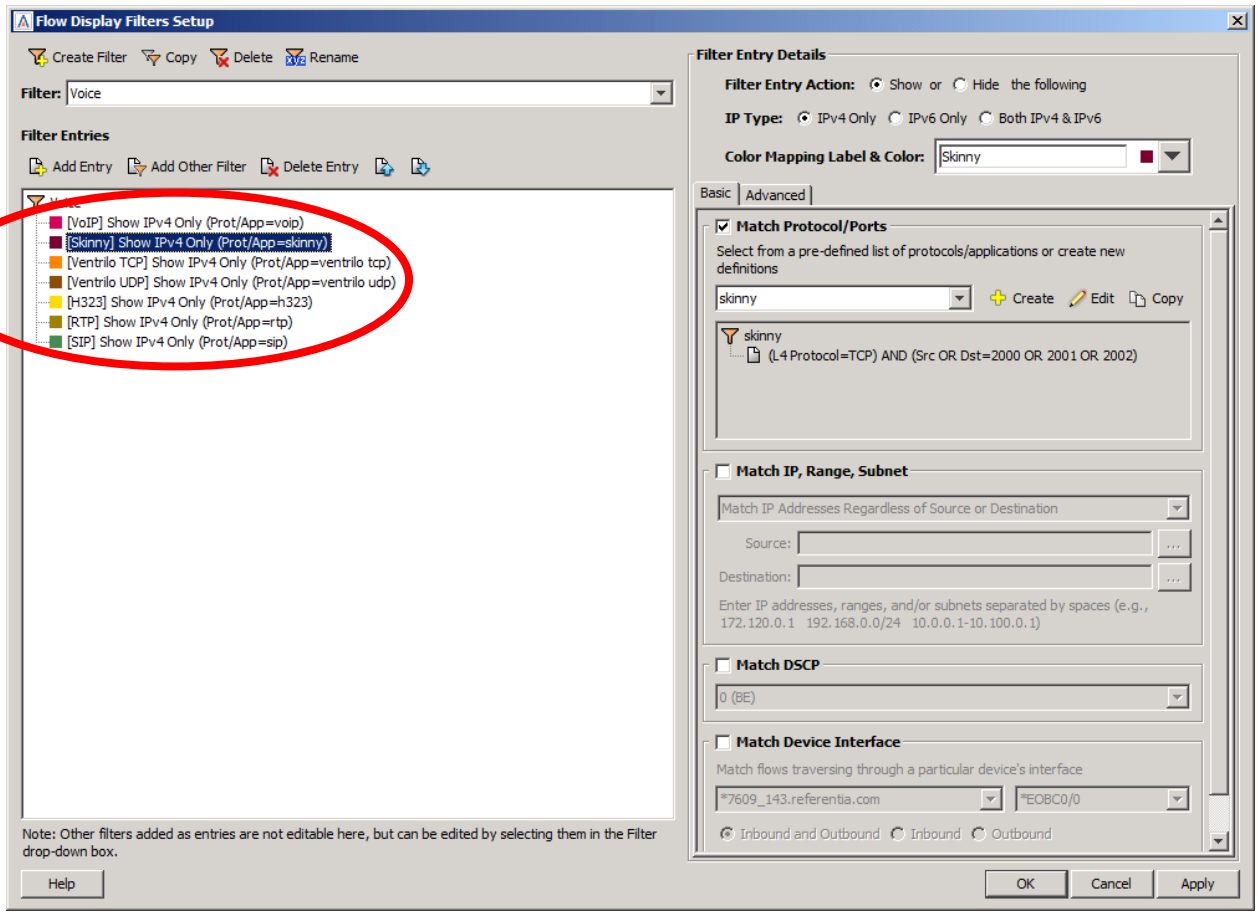

3. The **Display Filters Setup** Dialog appears




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



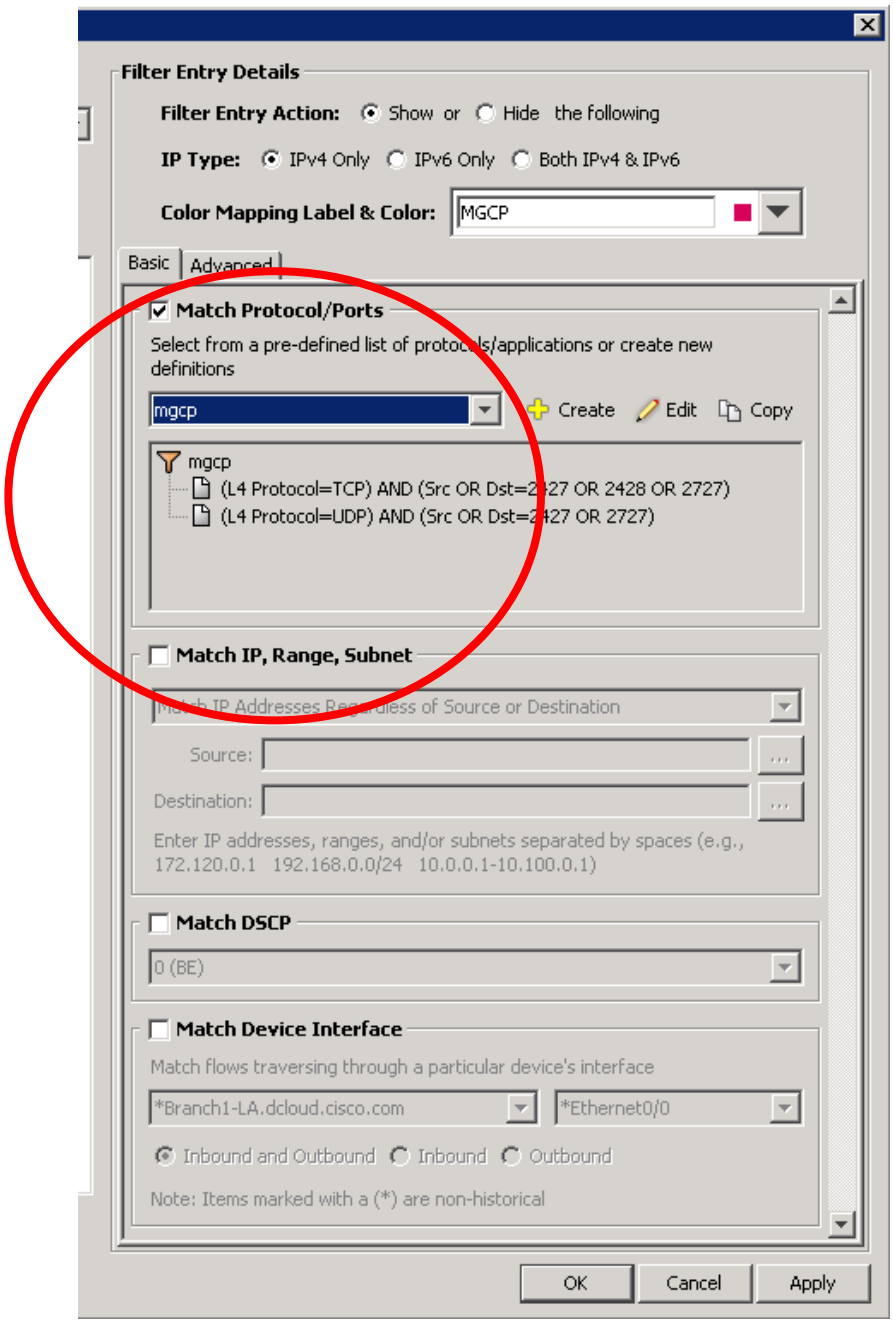

In its default form, the **Voice** filter is not built for any specific Vendor's solution. We will modify this filter to make it useful in a **Cisco CallManager** environment. We will **Delete**, **Add**, and **Edit** the entries of the filter.



5. To delete unused Entries simply select it and click **Delete Entry** above the list of entries.
    a. Delete VoIP
    b. Delete Ventrilo TCP
    c. Delete Ventrilo UDP
6. To add and entry simply click **Add** above the list of entries.

**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

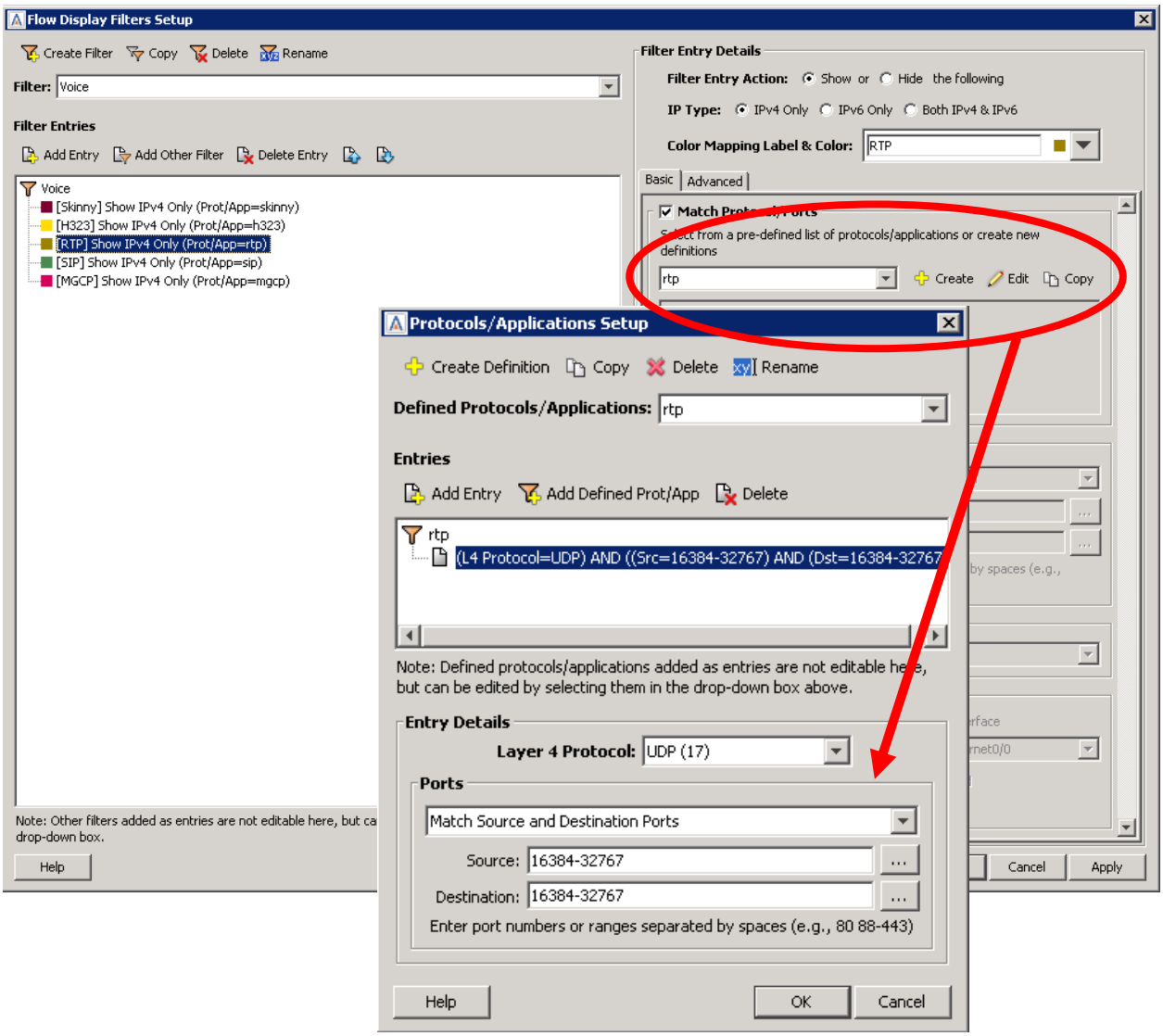


Edit Entries the following entries with these updates:

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




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

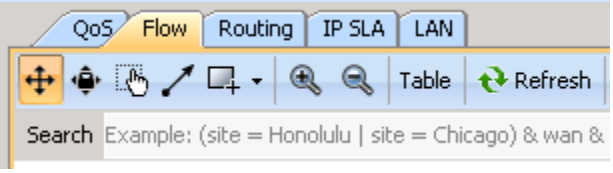
**Note: This updated voice filter will work well for our Lab purposes, but in a real networks, it would probably be best to also include IP addresses and/or subnets to these filters for eliminating any false positives.**

# Lab 1.3: Validating Filters

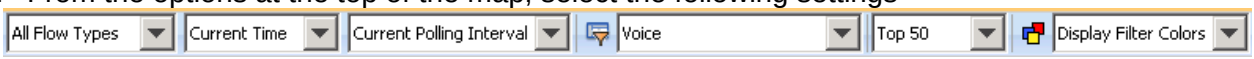
The example Filter we created should show us the Voice traffic in our network. The following reports will allow us to confirm the traffic.

Lab Steps:

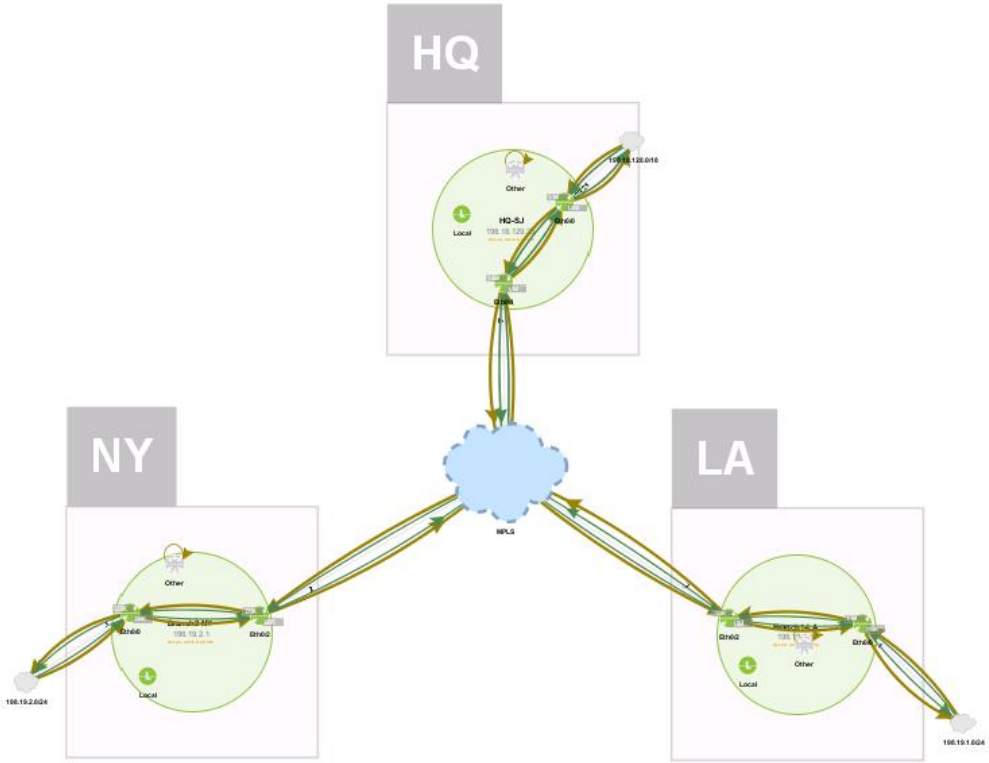
1. From the LiveNX Client map, select the Flow Tab



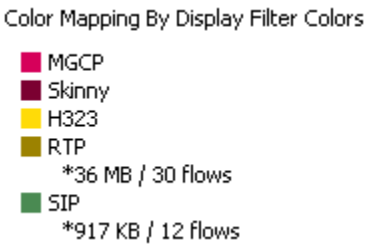

2. From the options at the top of the map, select the following settings



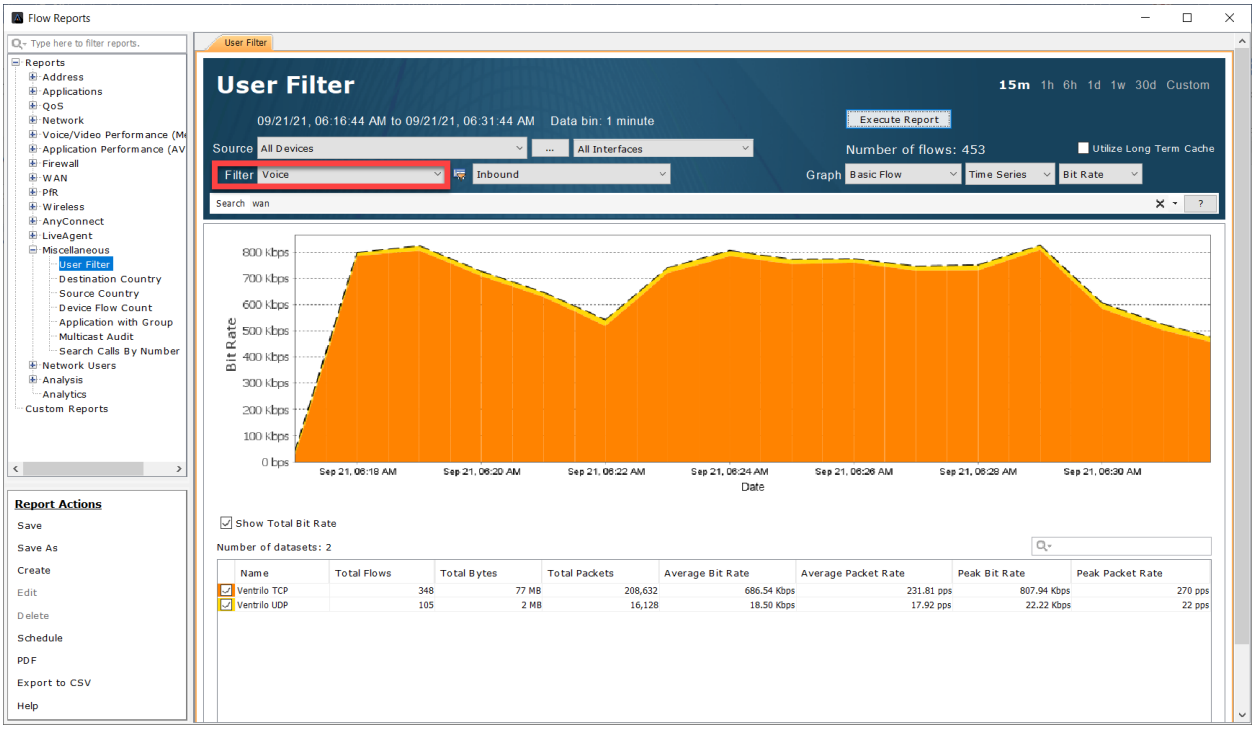

You should be presented with a Flow visualization similar to the following diagram




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

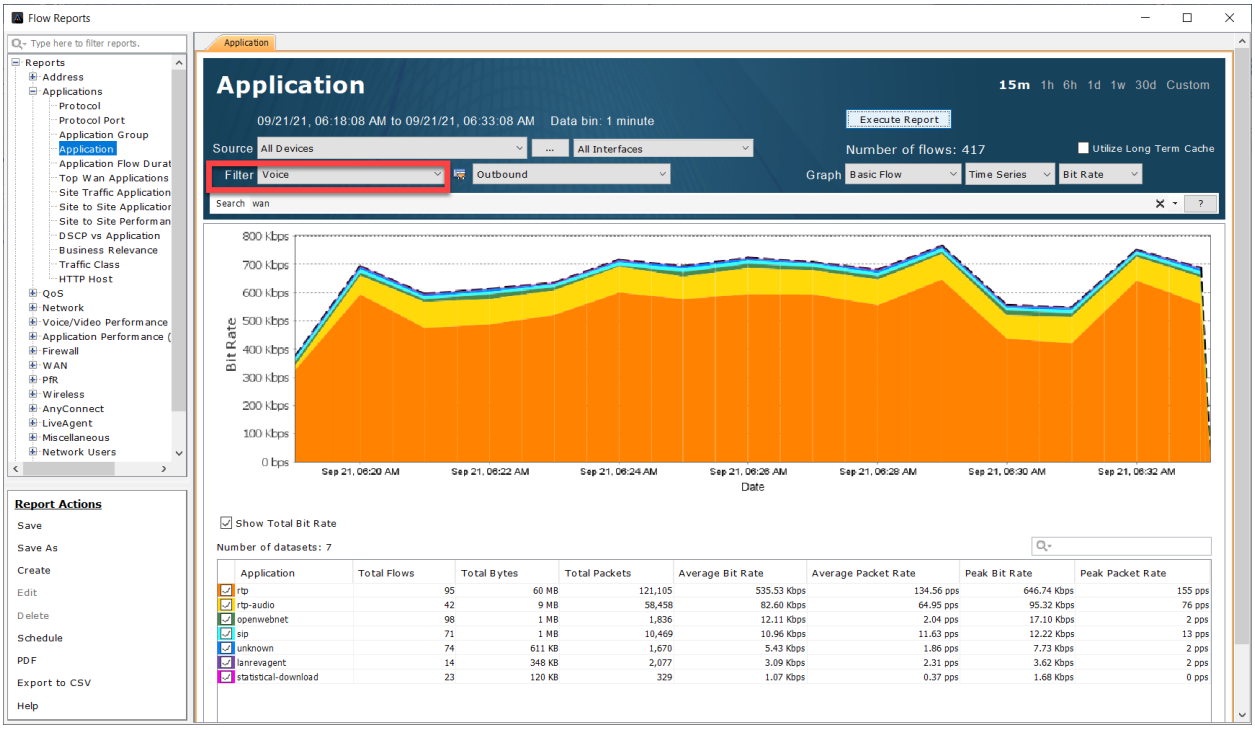


3. Run the Miscellaneous > **User Filter** report
    a. Select the Voice filter, but leave all parameters at their default settings
    b. Implement a Search of “wan”
    c. **Execute Report**




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**

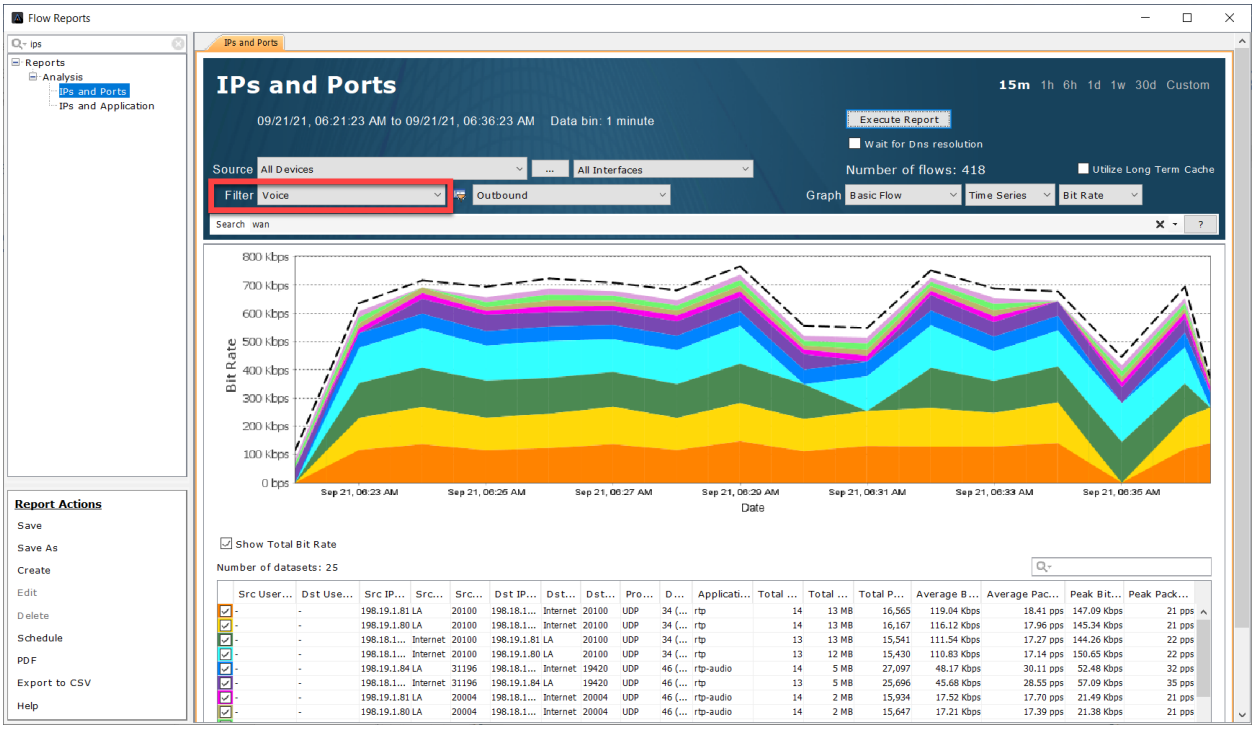



Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically “WAN” interfaces.

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?

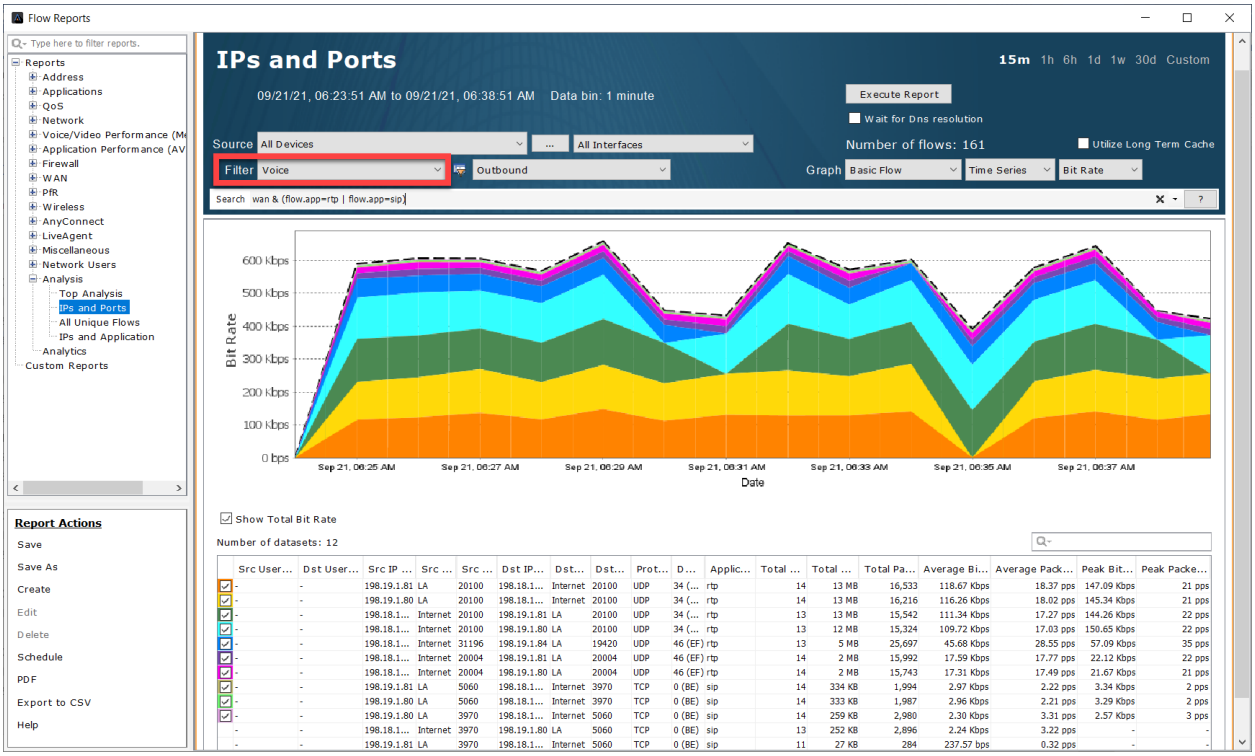
5. Run the Reports > Flow > Analysis > **IPs and Ports** report
    a. Select the Voice filter, but leave all parameters at their default settings
    b. Implement a Search of “wan”
    c. **Execute Report**




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)".




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

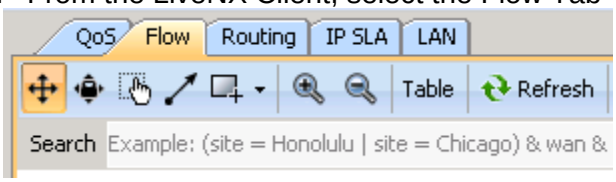
Now that we have used LiveNX's Filter and Search capabilities to accurately identify and understand the business critical traffic, we need to assign DSCP markings (QoS tags) on the traffic. In this lab, we are going to use the following 5 class QoS model:

| 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 |

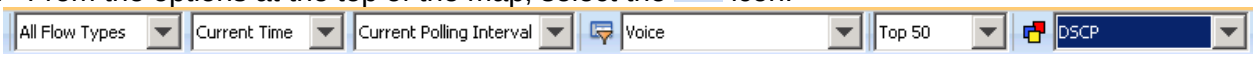
We need to now update the legends in LiveNX to understand these selected DSCP values of interest.

Lab Steps:

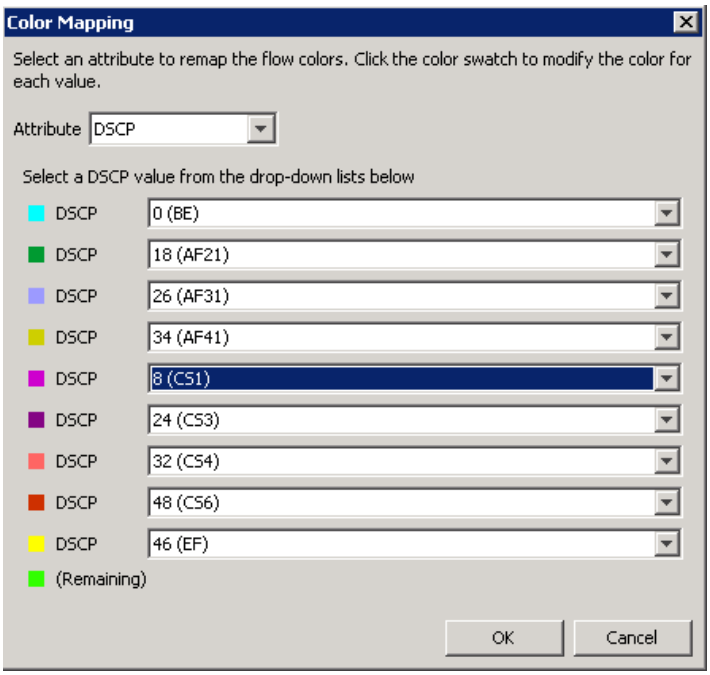
1. From the LiveNX Client, select the Flow Tab




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



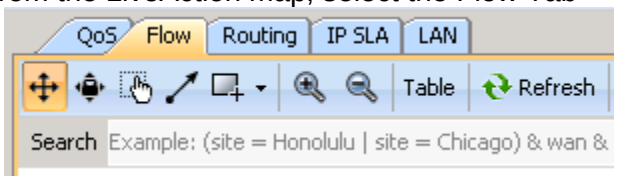

3. Set the Attribute to DSCP
4. Update the values to match those selected for the lab's 5 class QoS model.



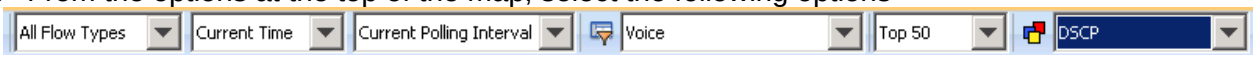
# Lab 2.2: Validate DSCP Markings

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

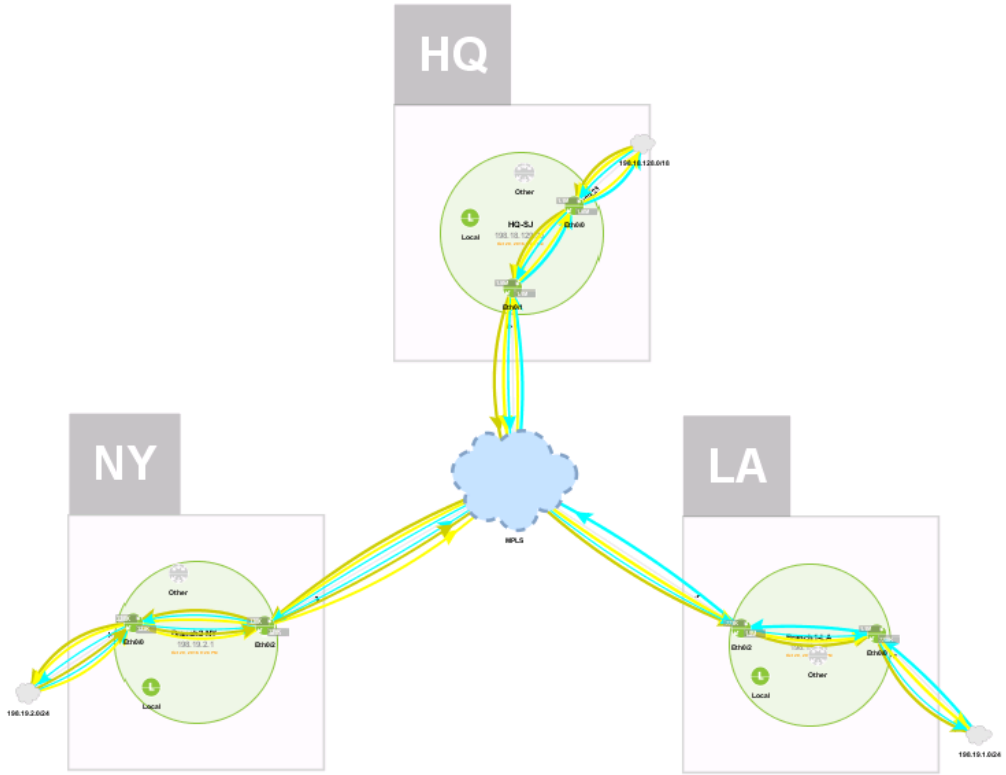
1. From the LiveAction map, select the Flow Tab



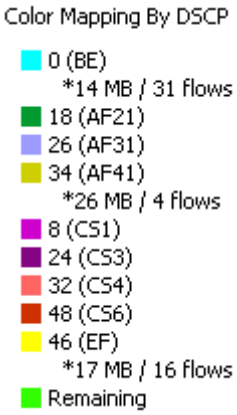

2. From the options at the top of the map, select the following options




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

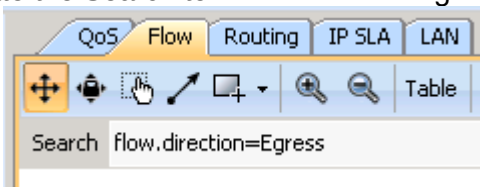



3. Confirm in the legend what DSCP values are seen.

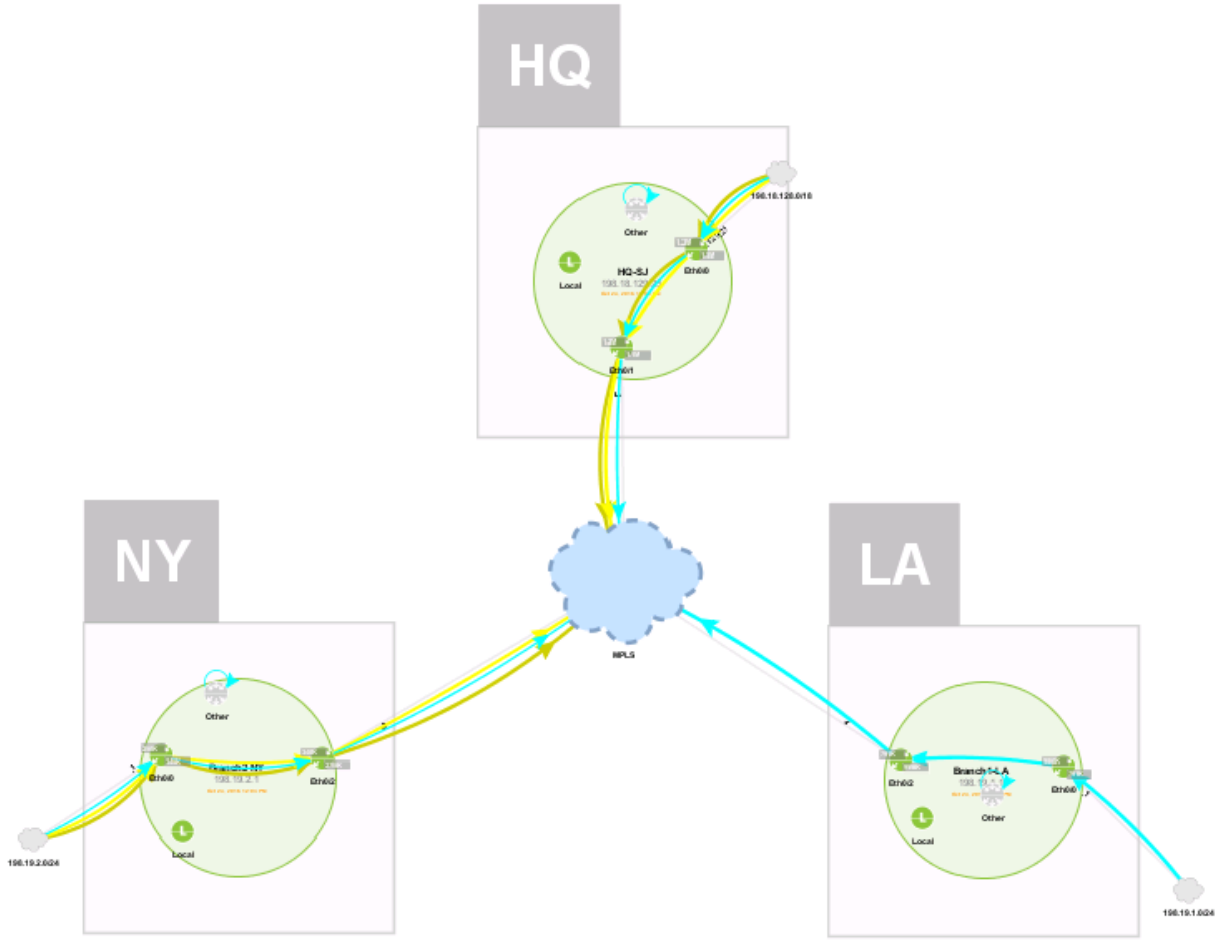


Since we have the Voice Filter in place, we would hope to only see EF and/or AF31 per the 5 Class QoS model that was chosen for this network. Because there are more values seen, we will further narrow the scope of the filter.

4. Update the Search to “flow.direction=Egress”



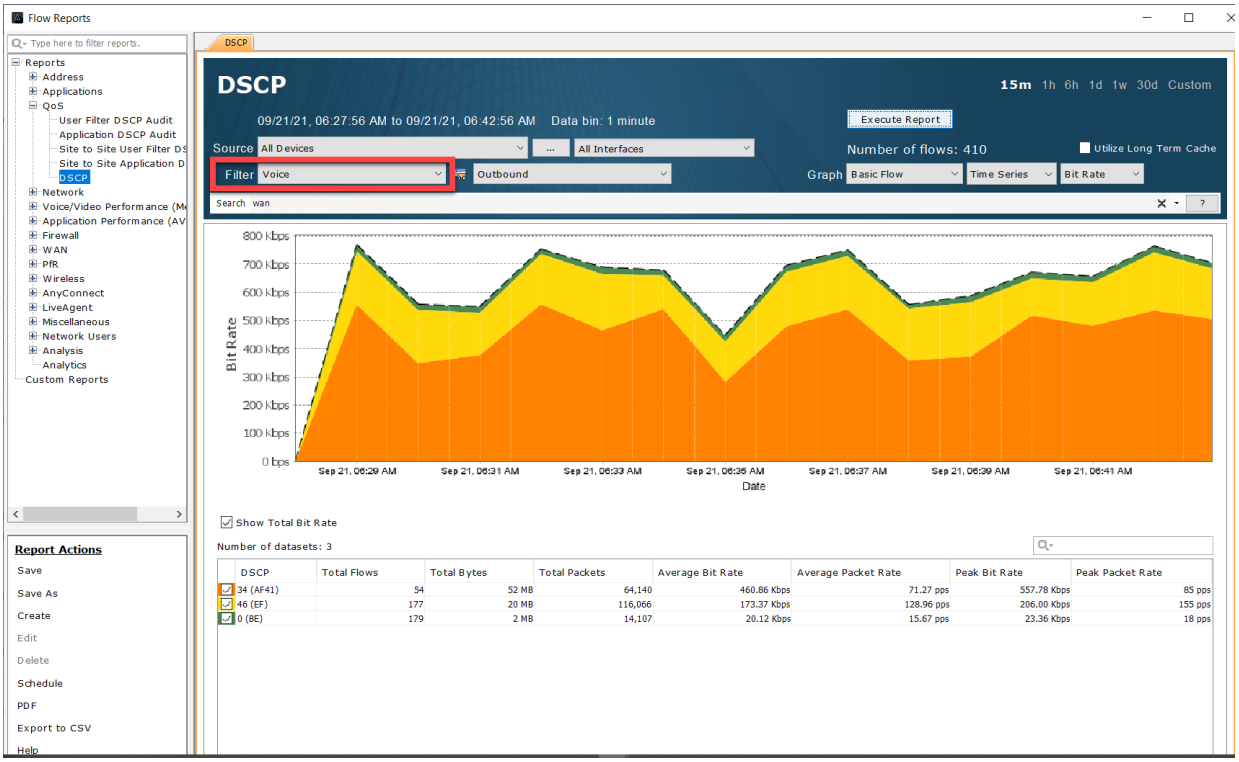

Notice that all traffic leaving LA is DSCP 0(BE) (light blue). That is *definitely not* correct.




**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.

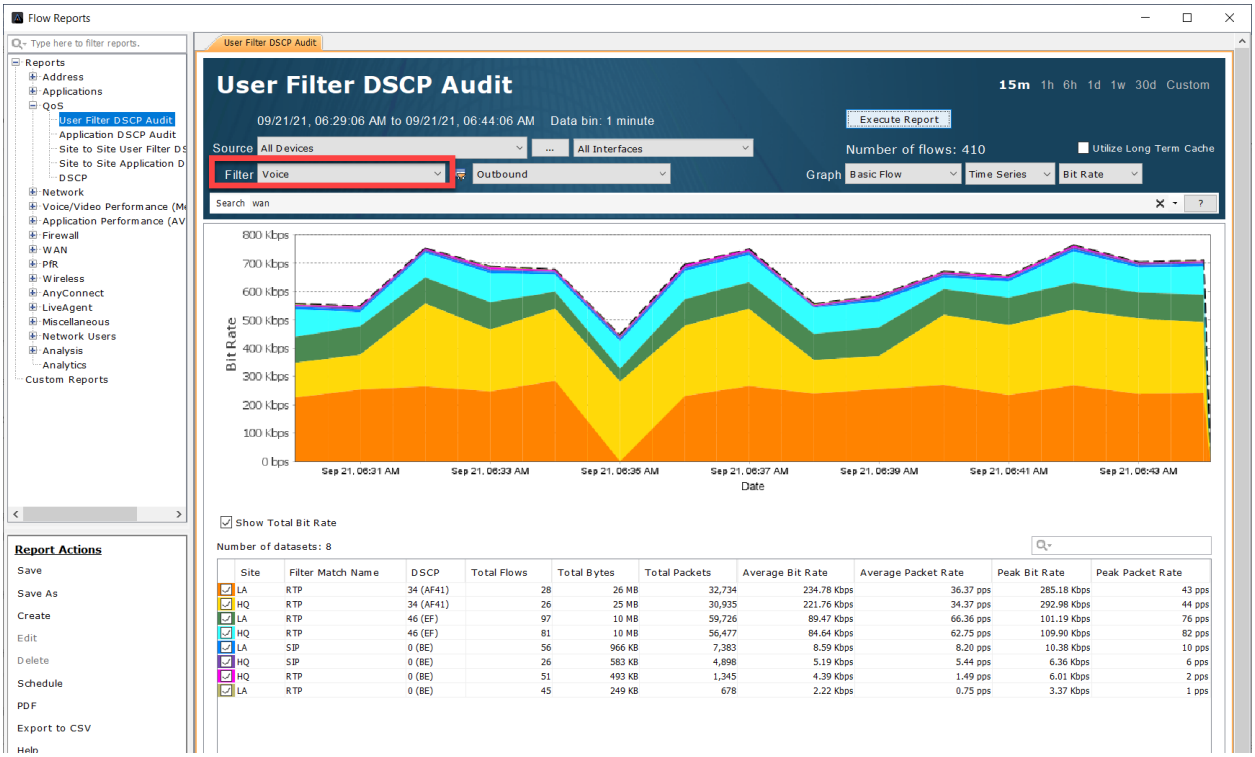
We'll use LiveNX Client reports to investigate further.

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**




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**

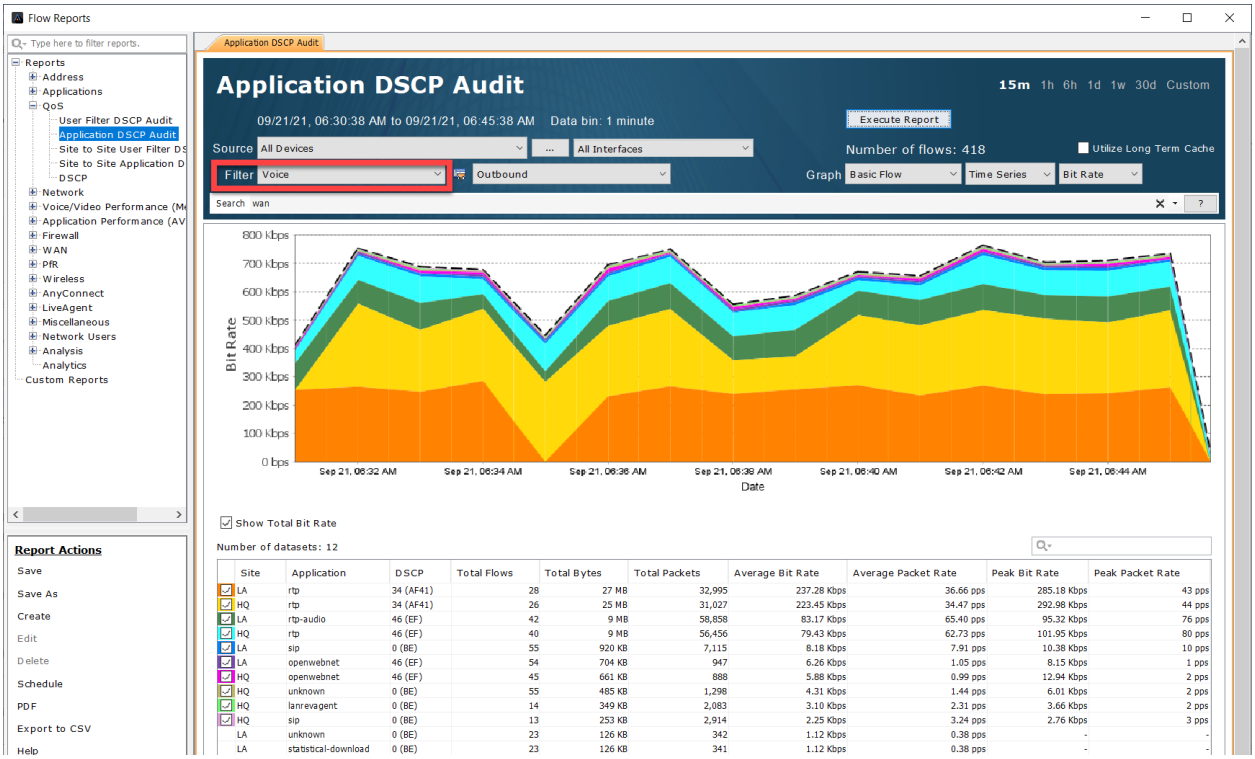



Notice that this report is looking at All Devices and All Interfaces in the outbound direction, but specifically “WAN” interfaces. It is showing the Source Site, the Filter match, and the DSCP value of the match.

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**




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).

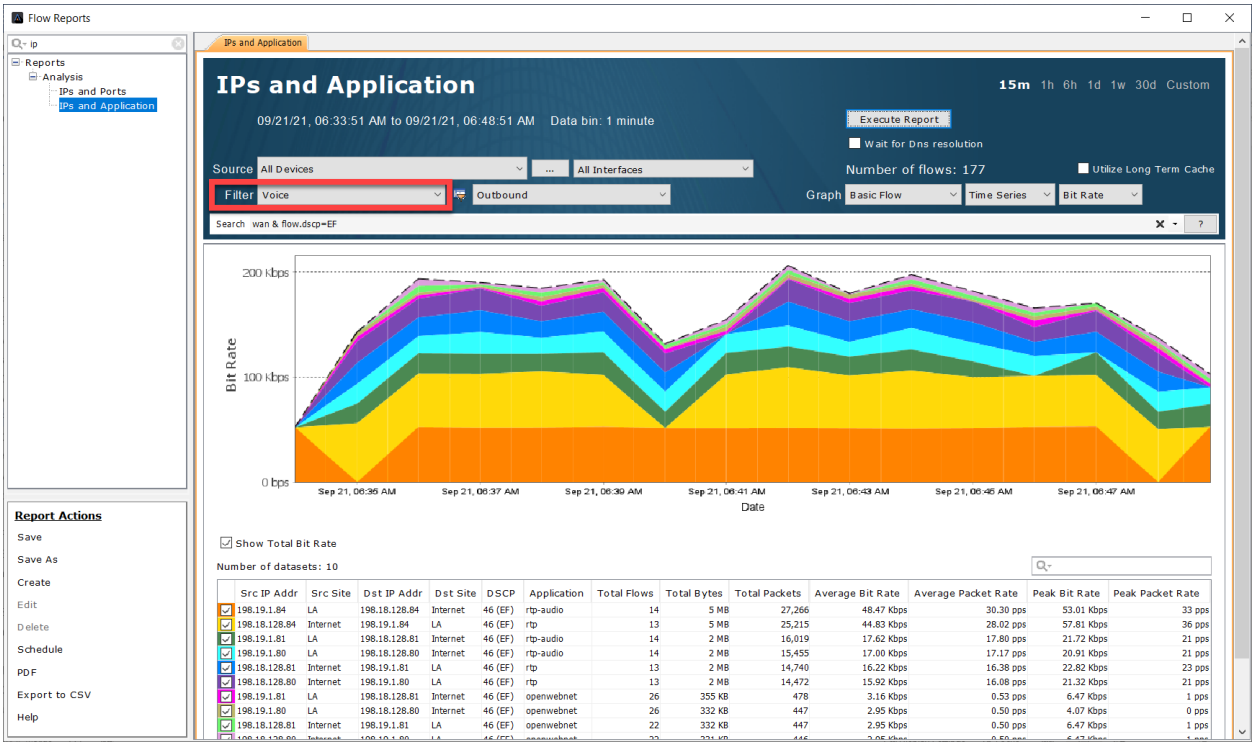
**Note: After validating the DSCP values using the Voice Filter, you would want to create more filters for the other priority applications of the network and repeat these steps.**

# 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 > Analysis > **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**




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.

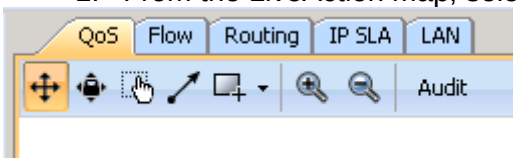
# Lab 2.4: Configure Classification & Marking Policies

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.

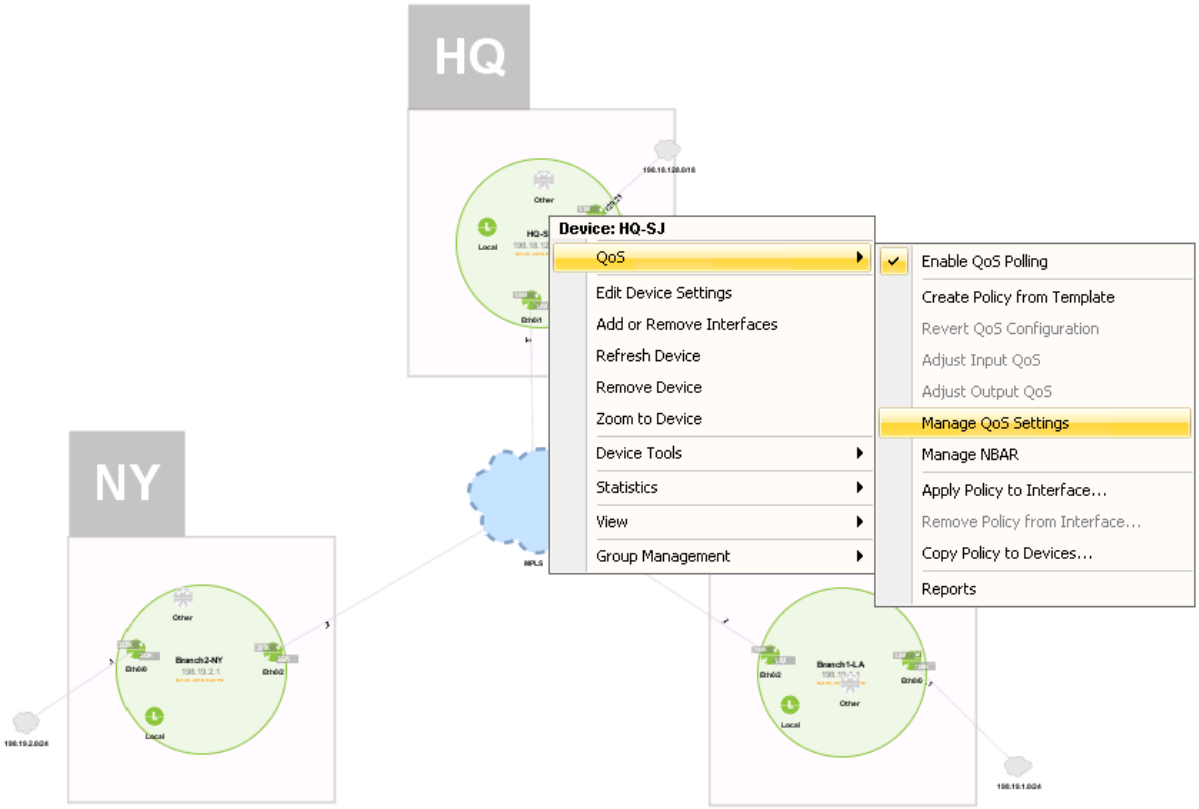
We will create a template QoS policy and apply this to the LAN interface of each of the routers to classify and mark the priority traffic properly.

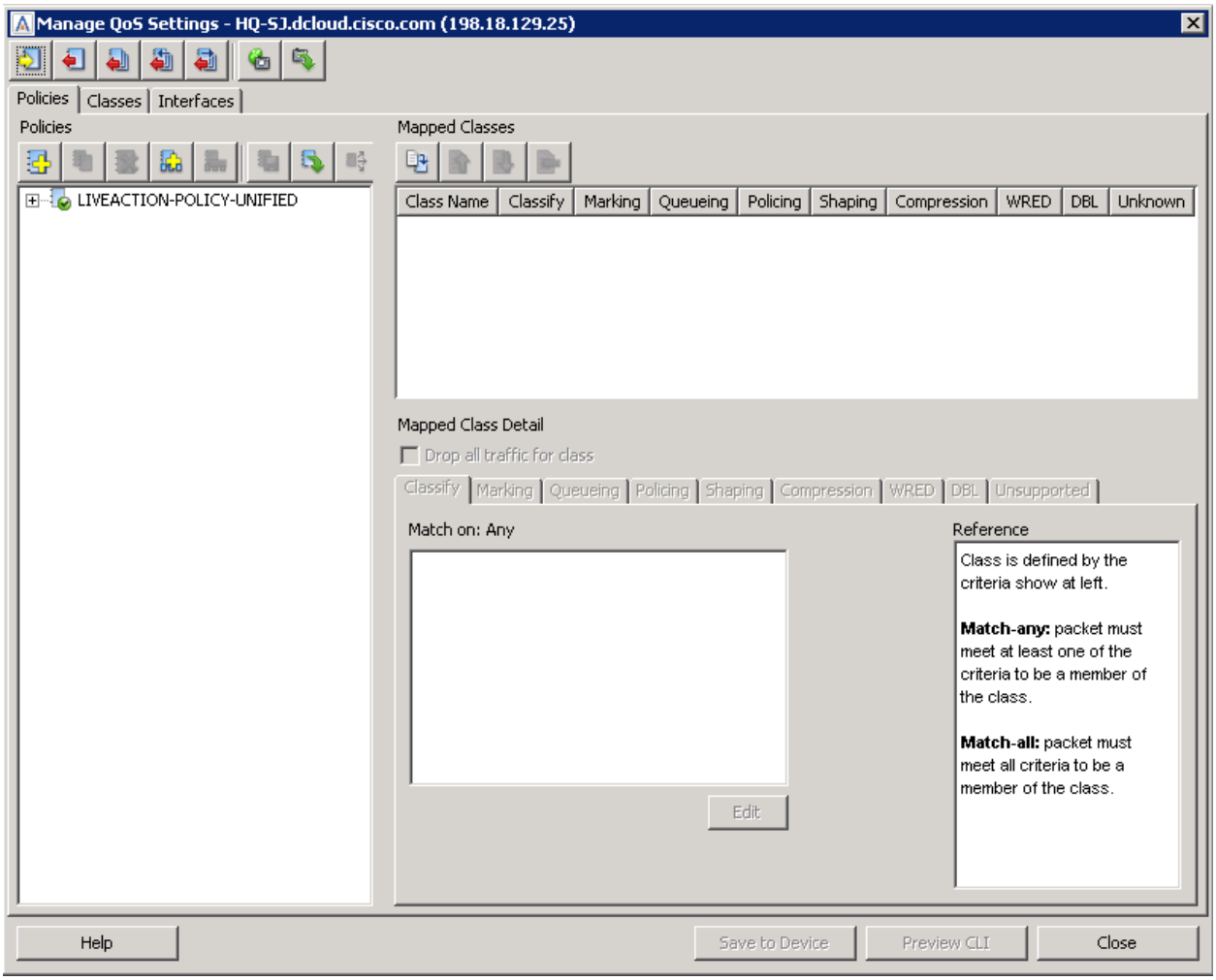
Lab Steps:

1. From the LiveAction map, select the QoS Tab

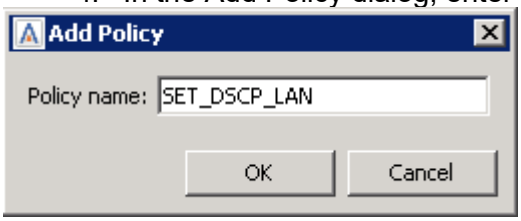



2. Right-click on the HQ router, select QoS > Manage QoS Settings

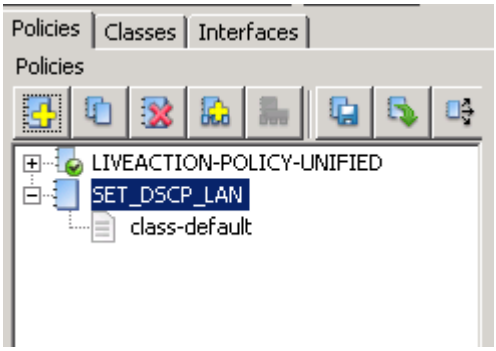




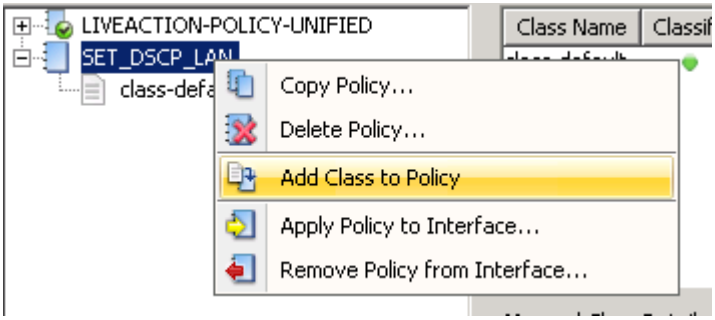

3. Select the Add Policy  icon.
4. In the Add Policy dialog, enter the name “SET_DSCP_LAN”



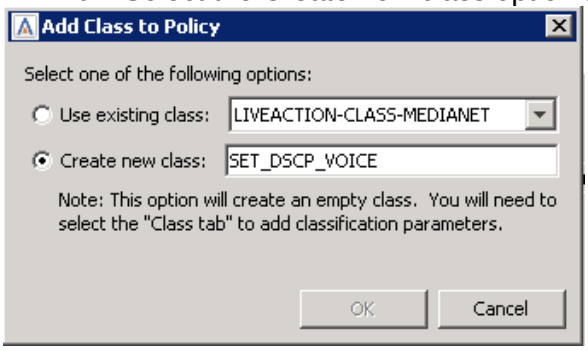

You can now see the new policy with its class-default appearing in the Policies list.



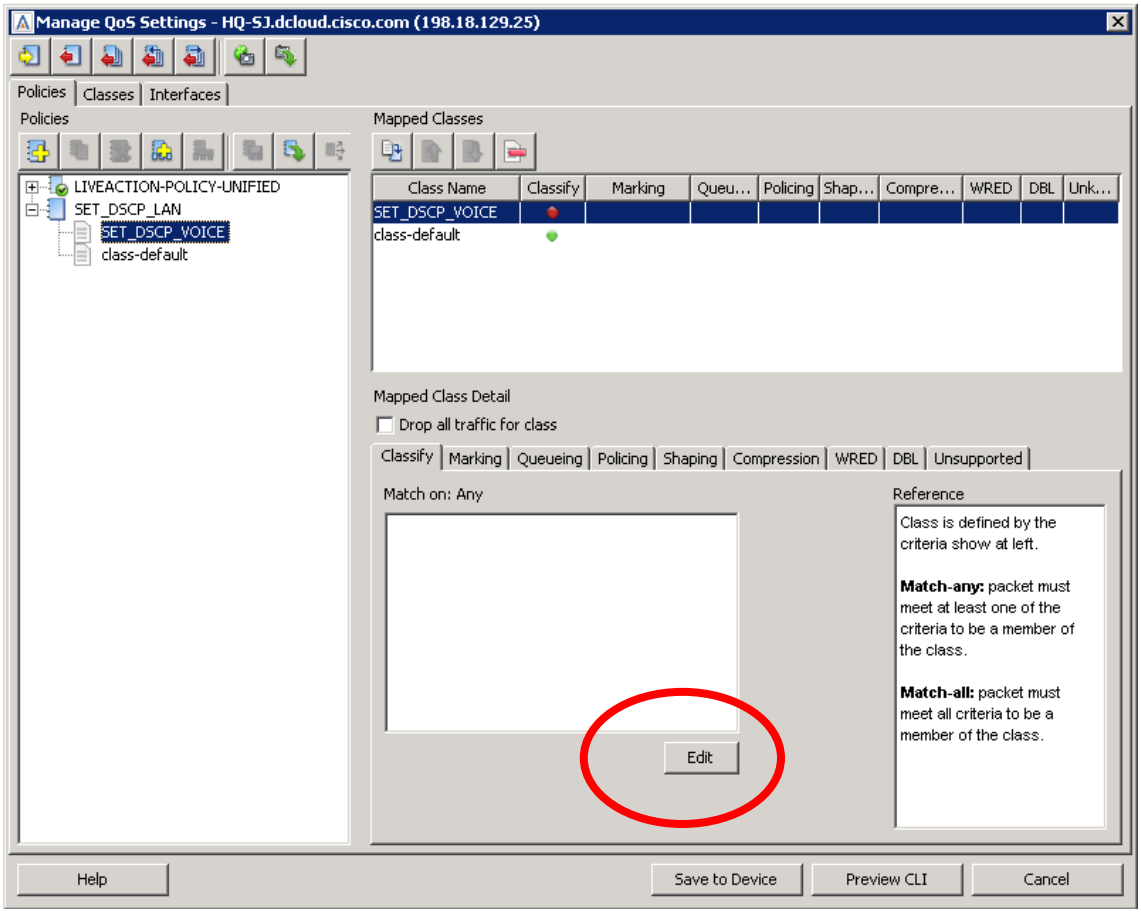
5. Right>Click on the SET_DSCP_LAN policy and select Add Class to Policy



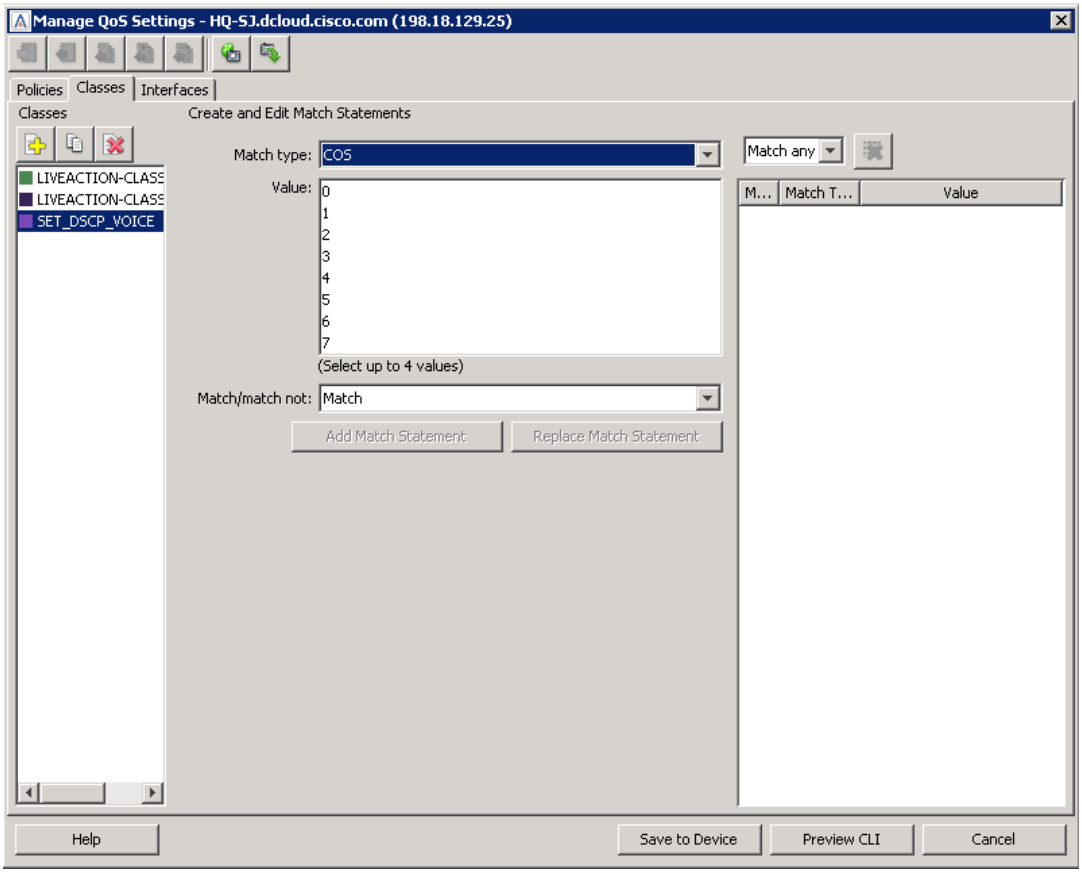

6. Select the Create new class option and name the new class SET_DSCP_VOICE



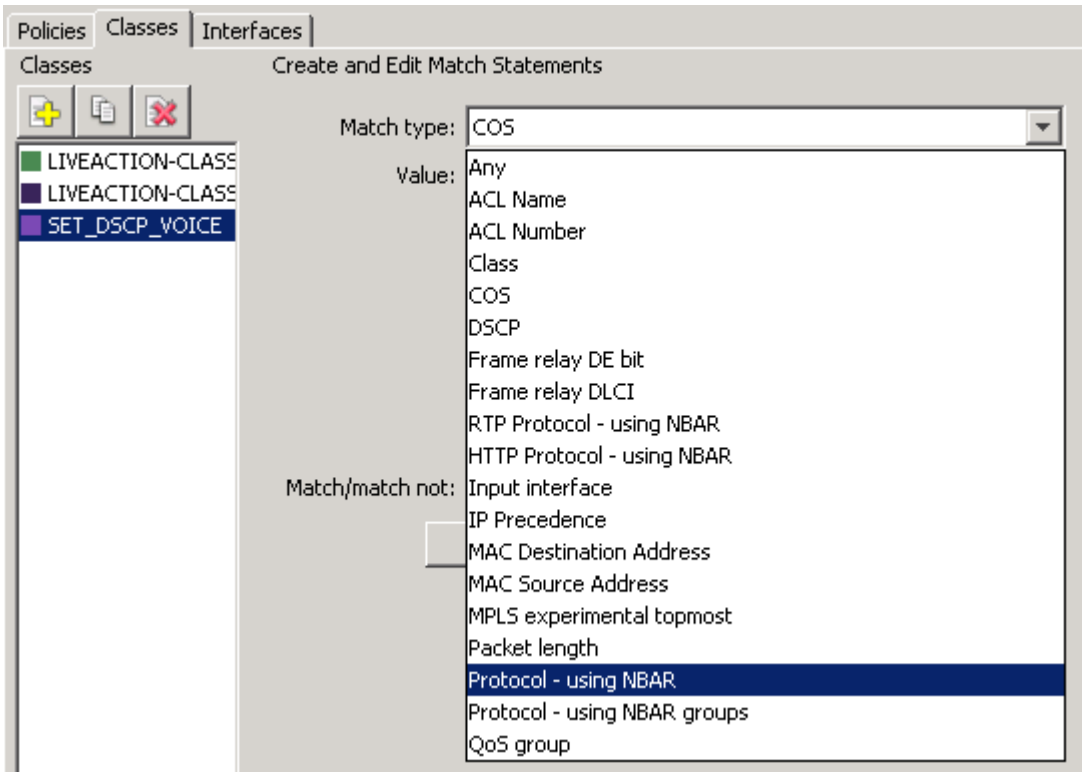

You will see the new class SET_DSCP_VOICE appear under the SET_DSCP_LAN policy



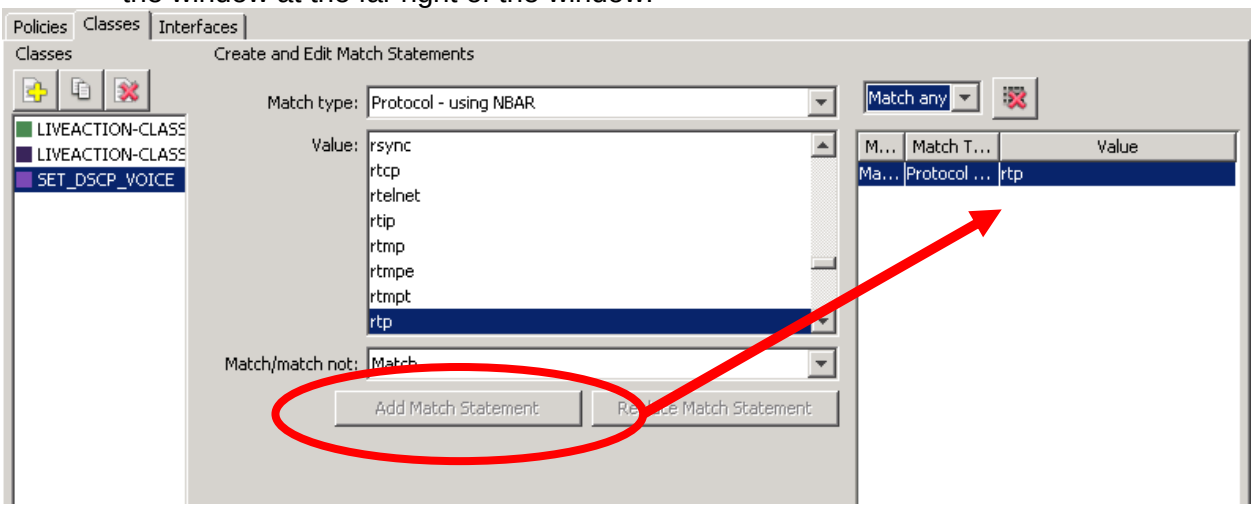

7. On the Classify Tab, select the Edit button



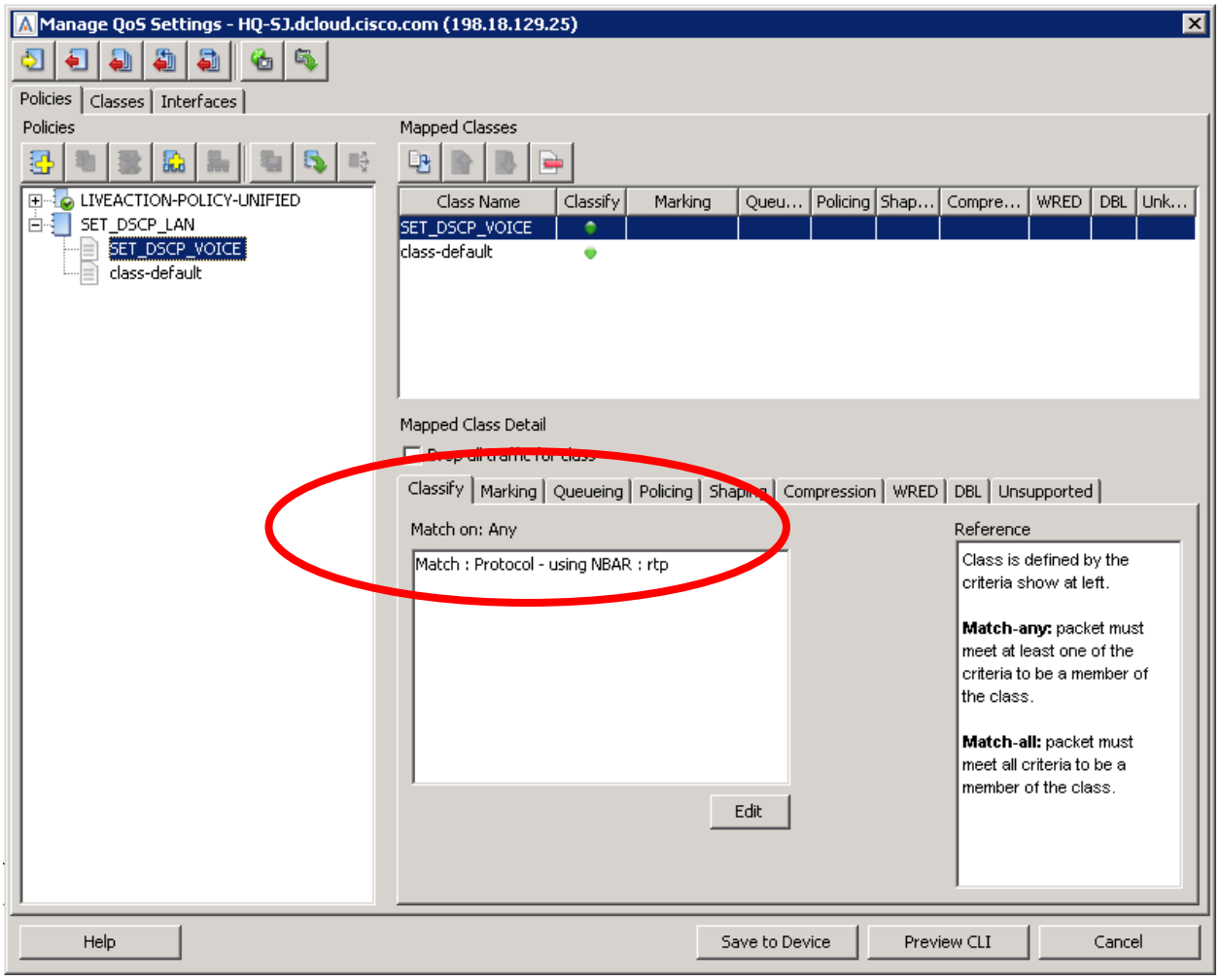

8. Select the **Match Type** dropdown and select **Protocol – using NBAR**



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.

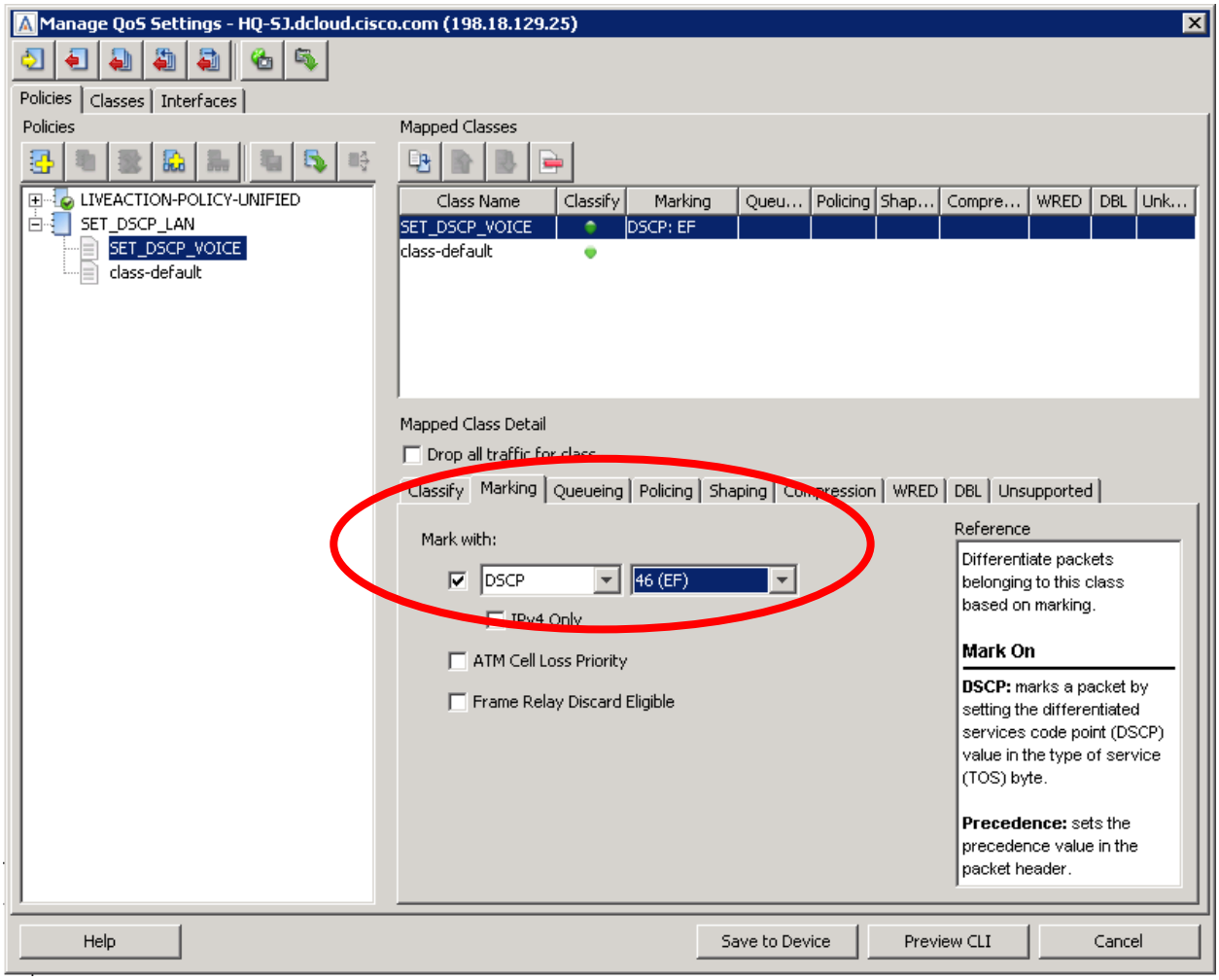



10. Select the **Policies** tab at the top left of the screen. Notice the **NBAR protocol match** on the classify tab




11. Select the **Marking** tab.

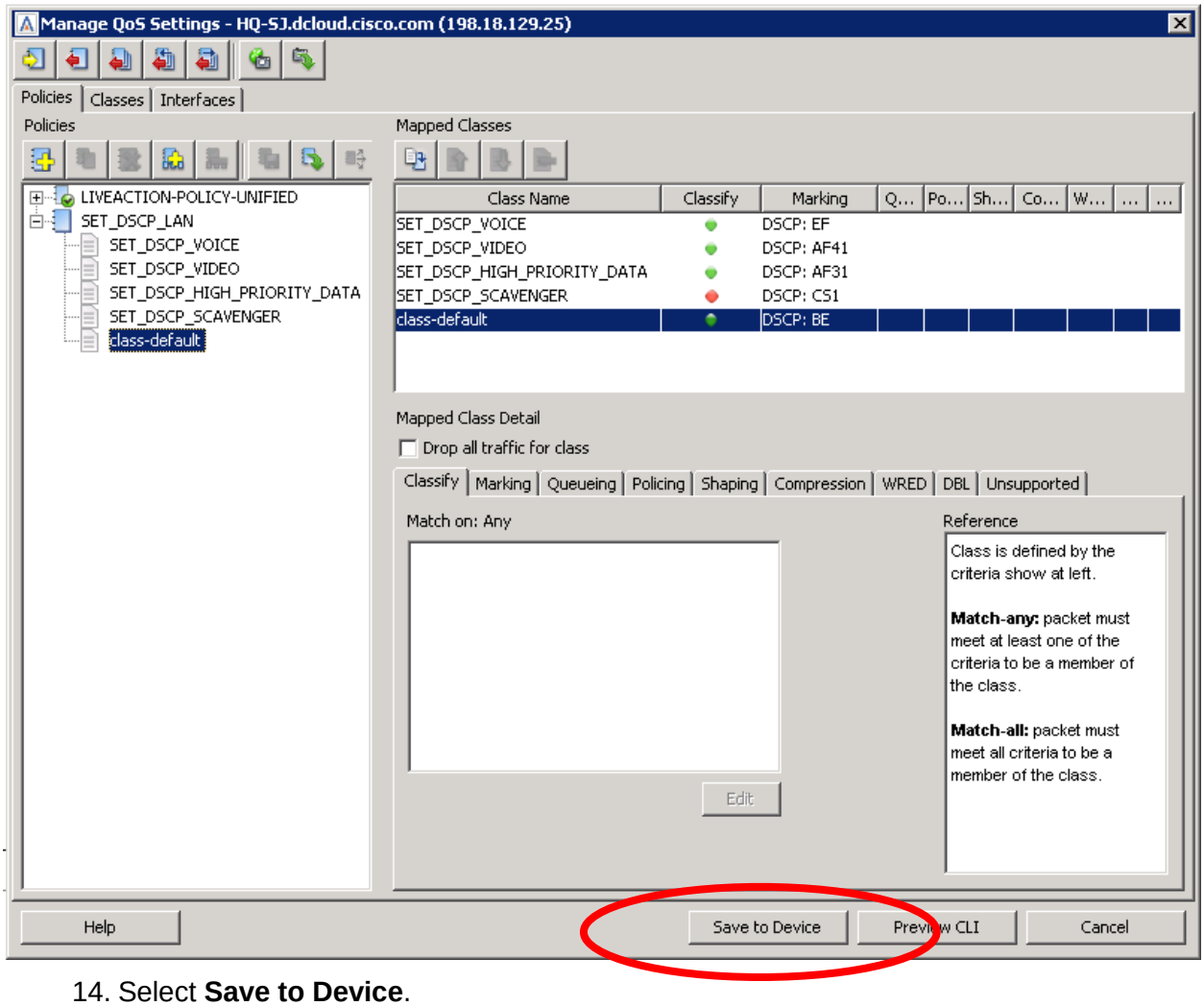
12. Select the **Mark With** check box and select the DSCP value of 46 (EF)




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:

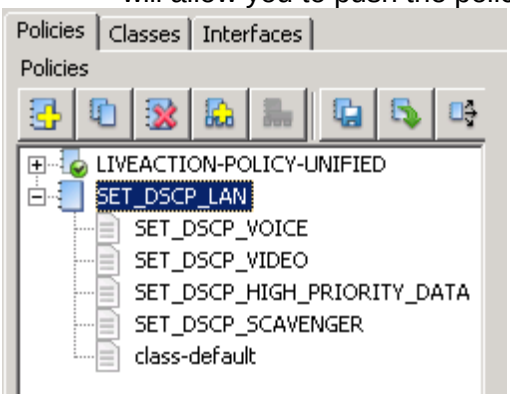
| Class Name | DSCP | NBAR Protocol(s) |
|---|---|---|
| **SET_DSCP_VOICE** | EF (46) | rtp |
| **SET_DSCP_VIDEO** | AF41 (34) | Ms-Lync |
| **SET_DSCP_HIGH_PRIORITY DATA** | AF31 (26) | SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce |
| **SET_DSCP_SCAVENGER** | CS1 (8) | *Leave blank for now* |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

When finished, the **SET_DSCP_LAN** policy should look like this:



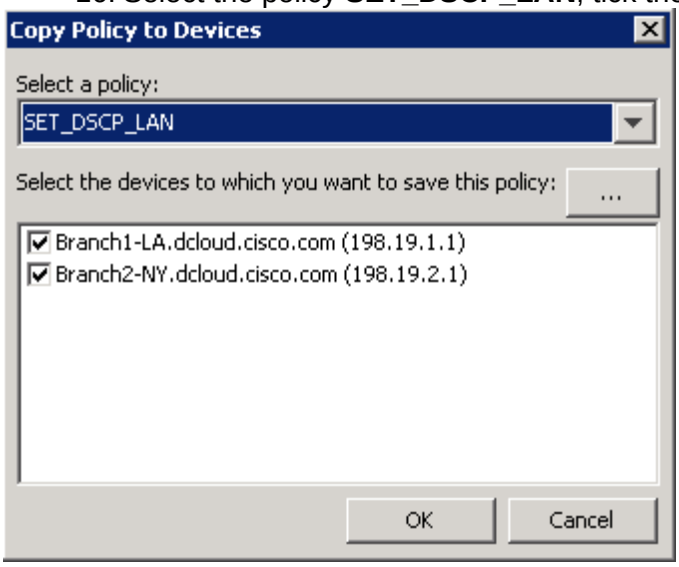

14. Select **Save to Device**.

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



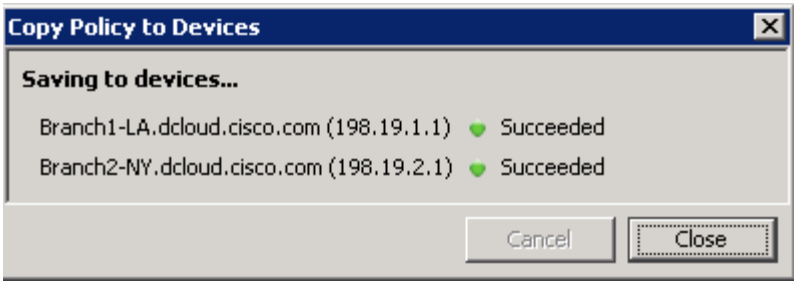

The **Copy Policy to Devices** dialog window appears.

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




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

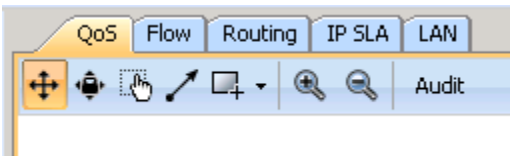
Validate the changes saved successfully.




17. Close the **Manage QoS** Dialog Window.

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

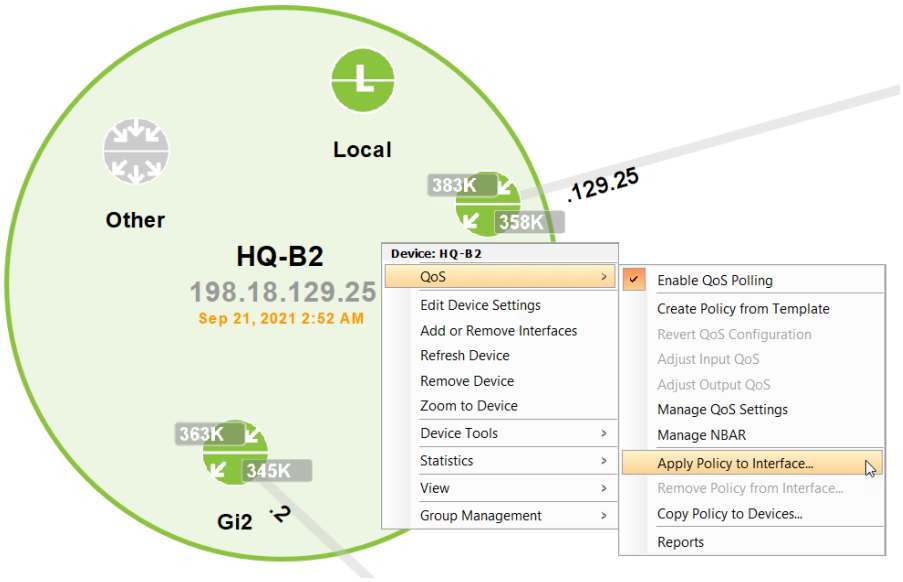
Lab Steps:



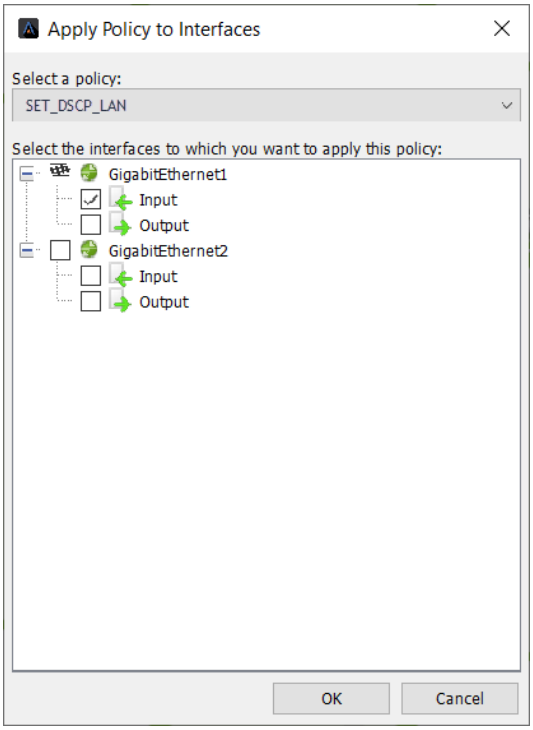

1. Select the **QoS** Tab

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.**

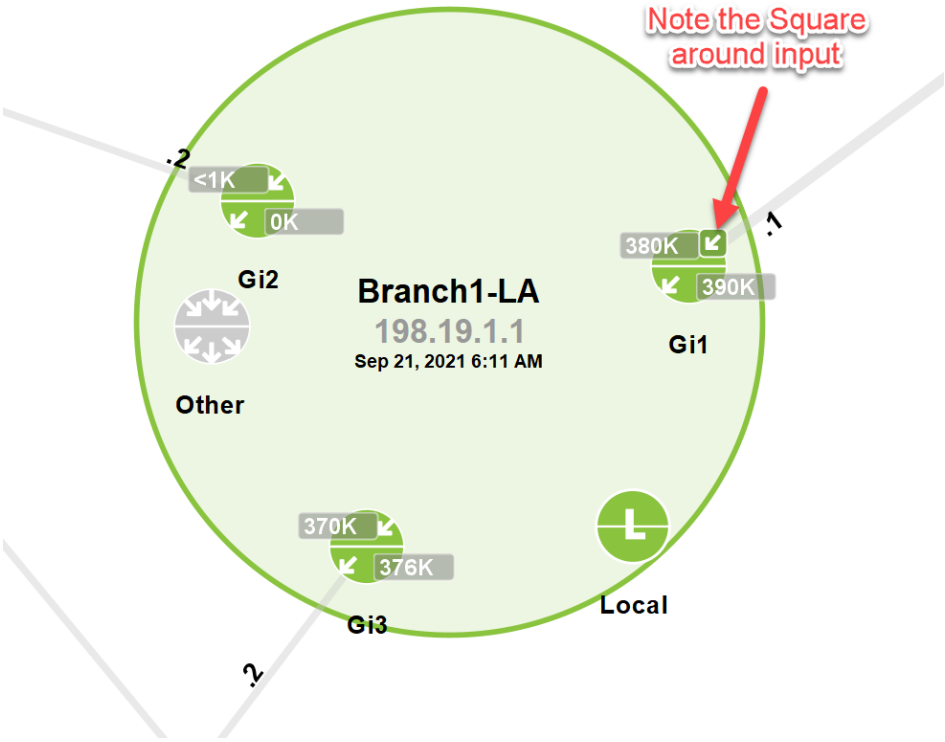



3. Select the **SET_DSCP_LAN** policy and tick to apply it in the **input** direction.
4. Click OK.



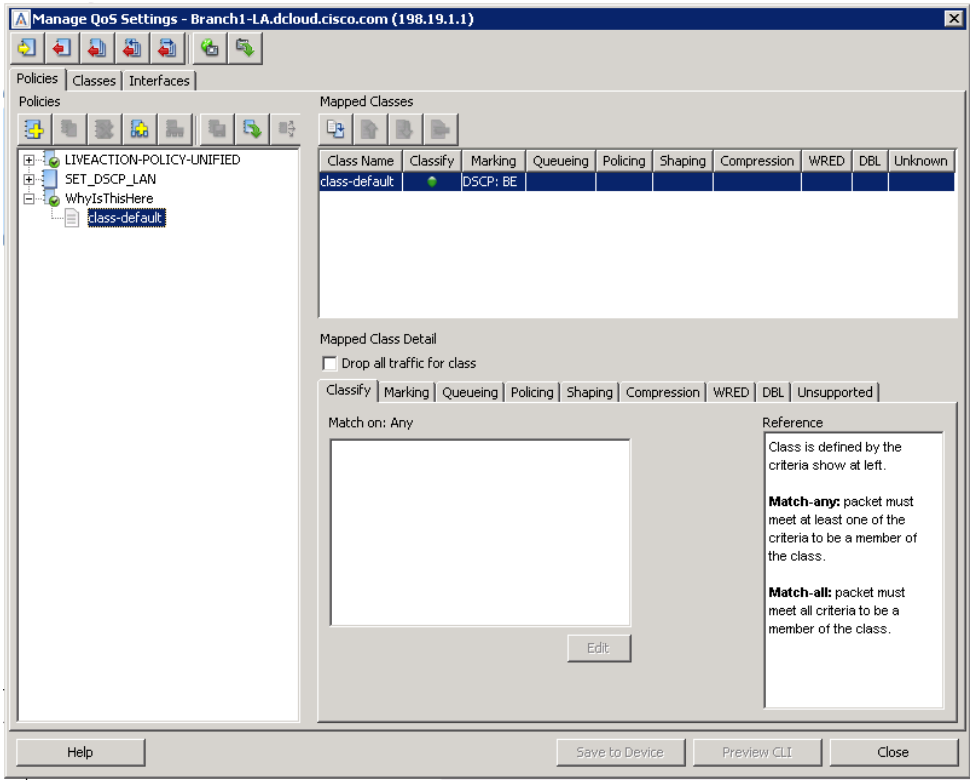

Follow these same steps to apply the **SET_DSCP_LAN** policy to **the other router's LAN interface.**

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

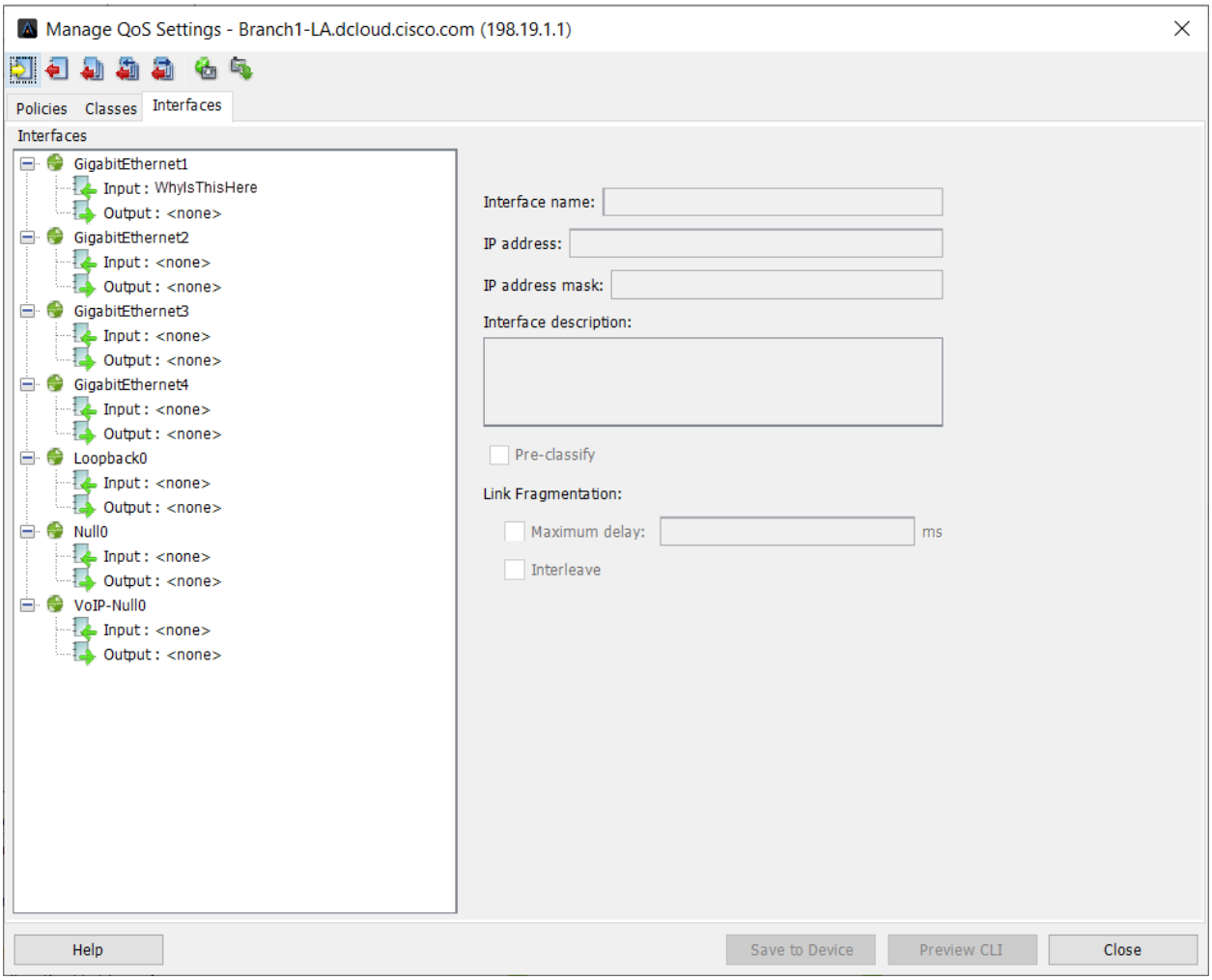



5. Right-click on the LA router and select **QoS > Manage QoS Settings**.

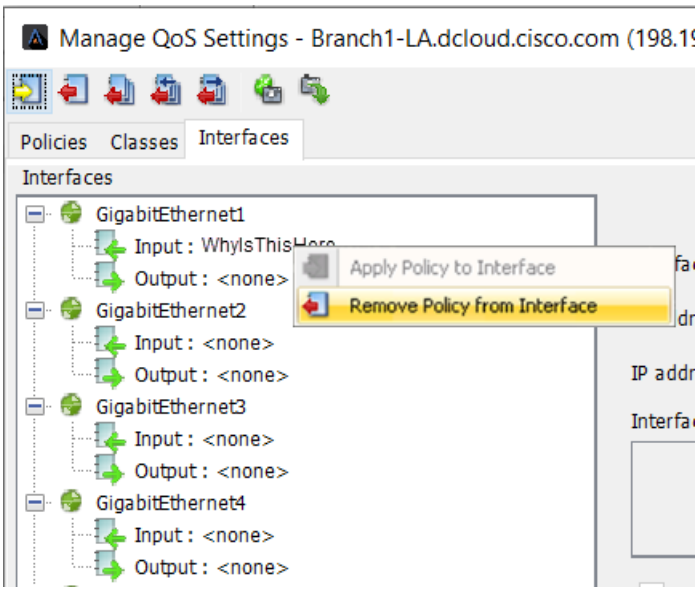
Notice how it has a policy on it called “**WhyIsThisHere**”. Notice how the class-default of this policy is marking traffic as 0 (BE). No wonder we were seeing Voice (rtp) leaving this site as BE!



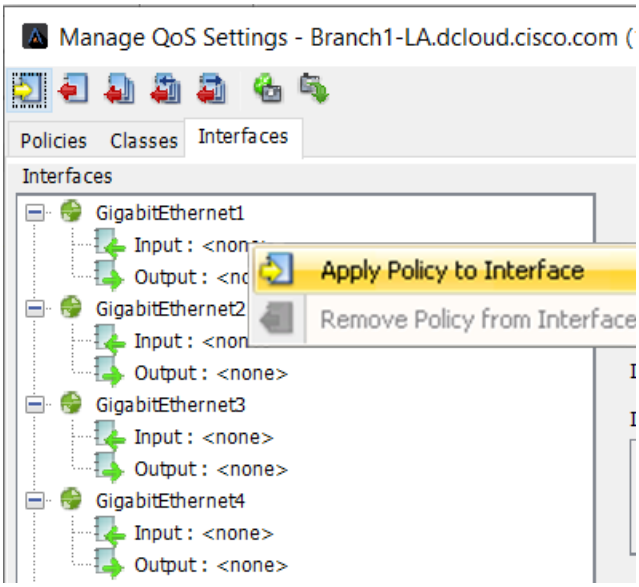

6. Select the Interface tab



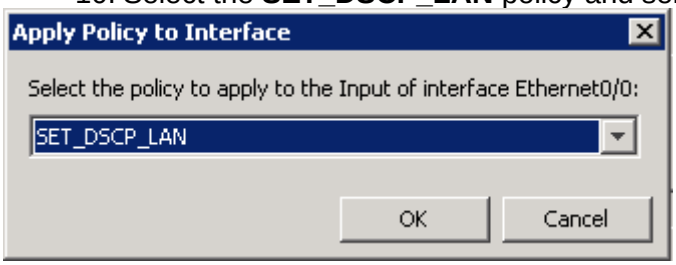

7. Right-click on the WhyIsThisHere policy that is highlighted on the input side of the GigabitEthernet1 interface.



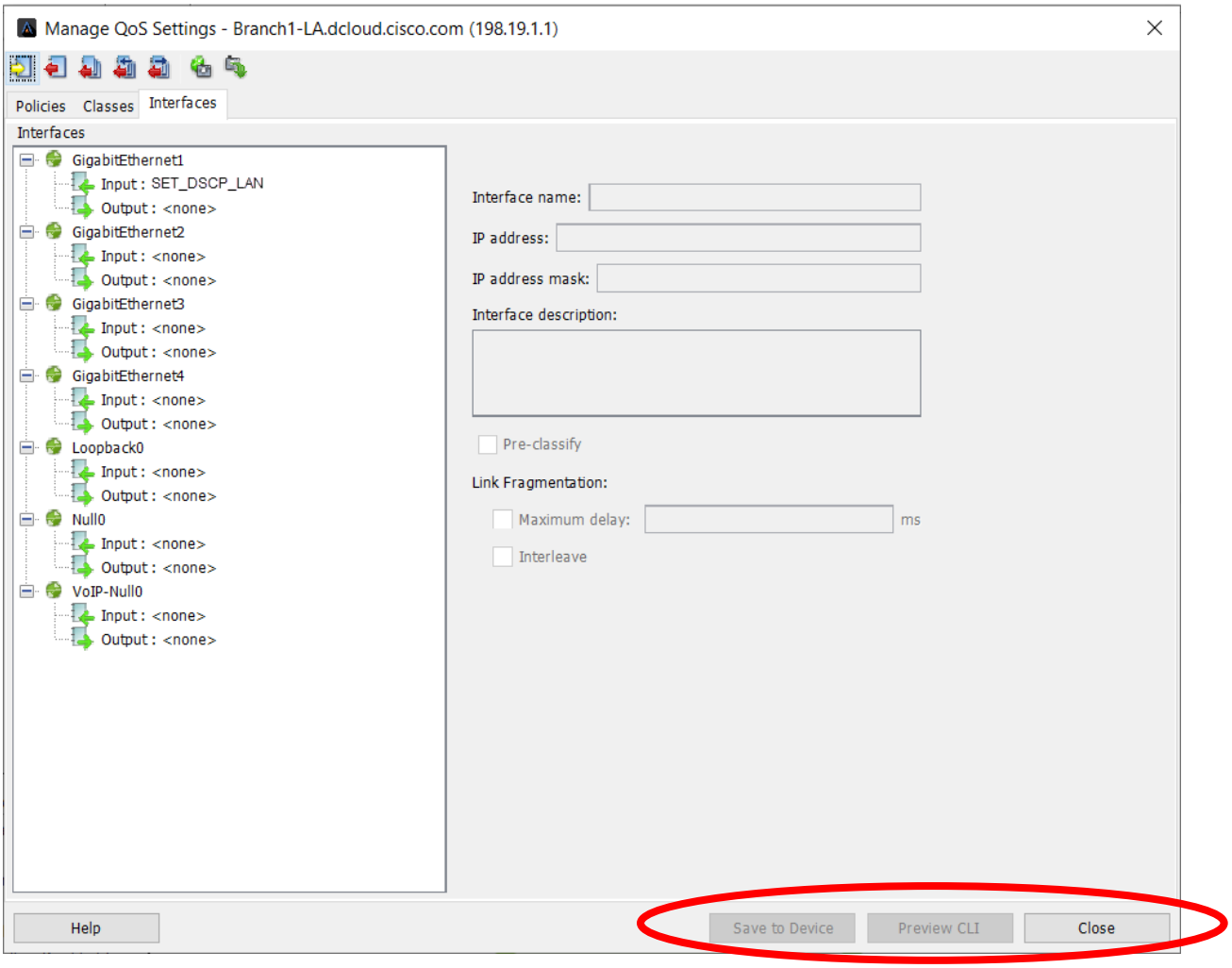

8. Select Remove Policy from Interface
9. **Right-click** on the input side of the **GigabitEthernet1** interface and select **Apply Policy to Interface**.




10. Select the **SET_DSCP_LAN** policy and select OK.




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

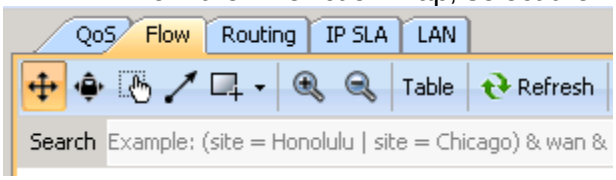



12. Ensure all routers have the **SET_DSCP_LAN** policy applied to their **LAN** interface.

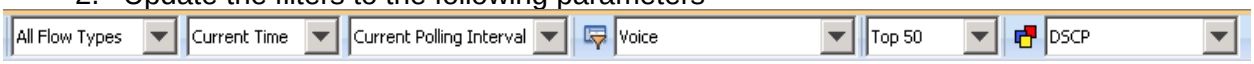
# Lab 2.6: Validate DSCP Settings

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

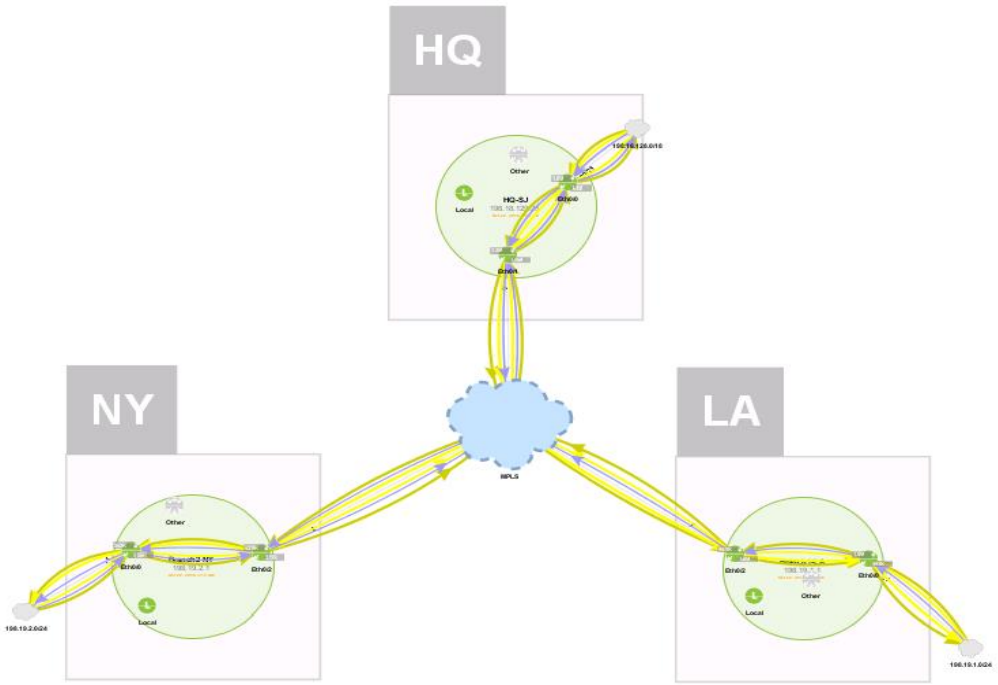
1. From the LiveAction map, select the **Flow** Tab




2. Update the filters to the following parameters




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



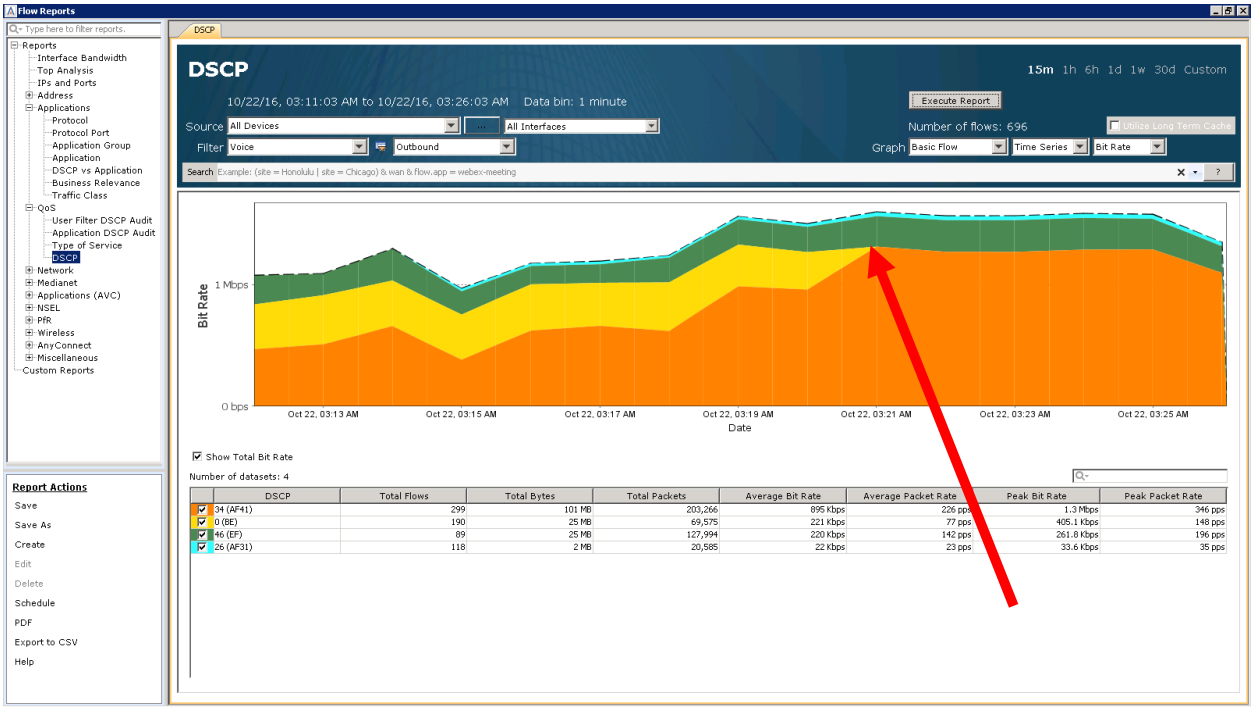

Color Mapping By DSCP

- 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**




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

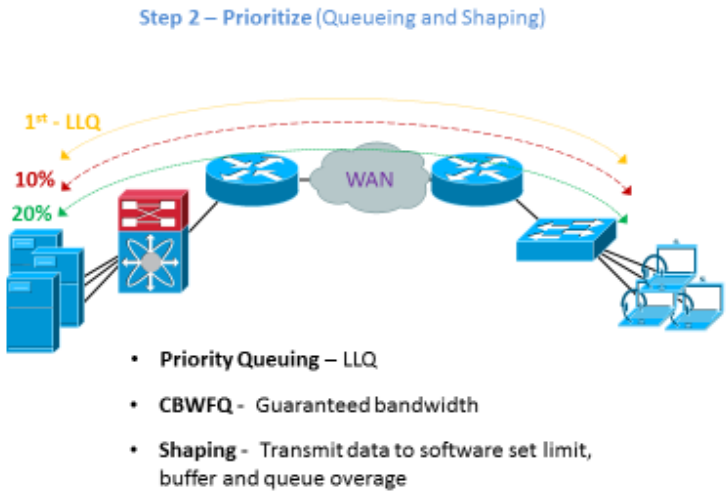
**Note: For the sake of time in this lab, we are only going to focus on this one report. Remember that in a real network, you would repeat these steps for all important applications. We would use the same visualization and reports as we have used previously to validate QoS polices effectiveness for all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




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?

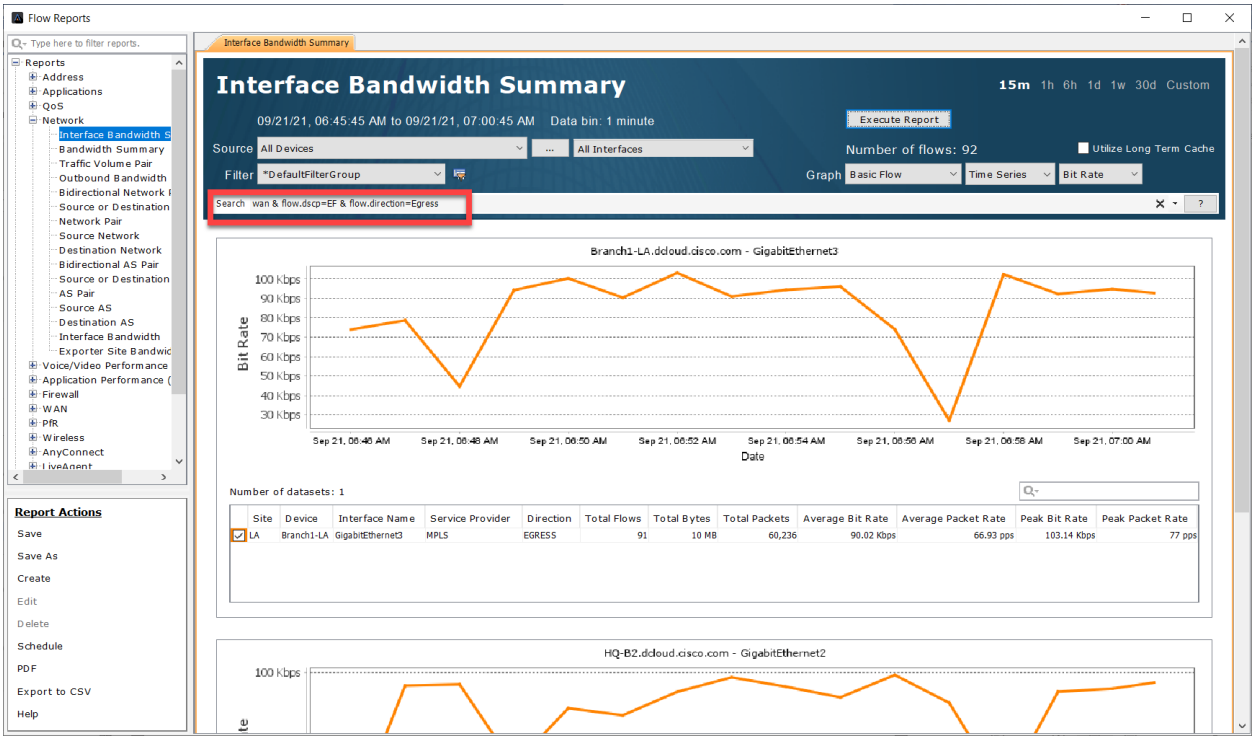
# Lab 3.1: Run the Reports!

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.

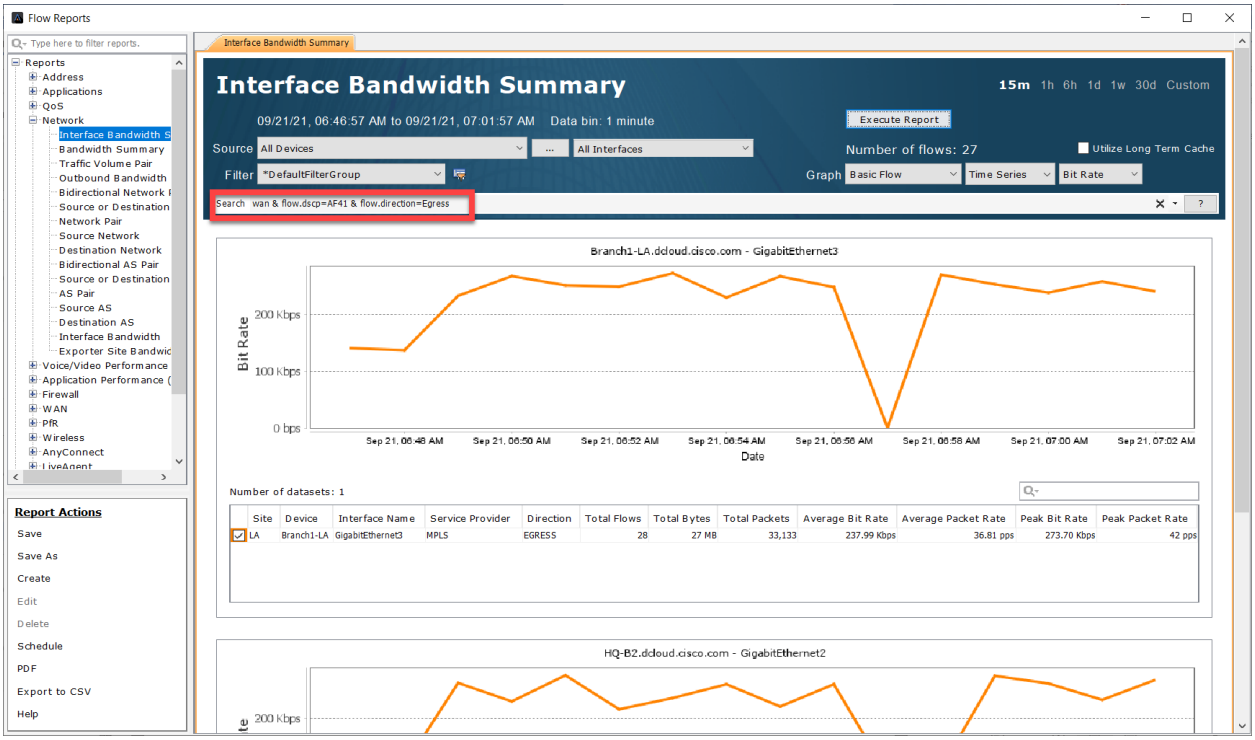
Lab Steps:

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**



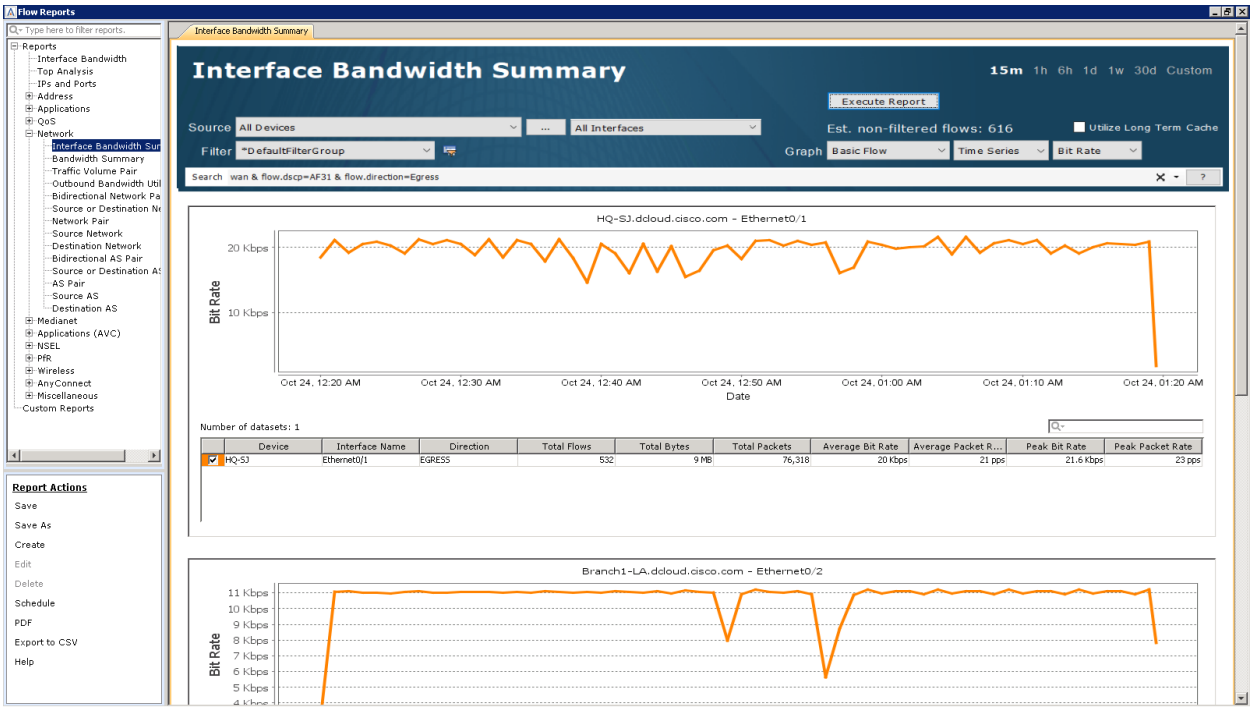

Notice how this shows a bandwidth graph of the data being transmitted out of each WAN interface. In this example, we are focused on Voice (rtp)/ EF traffic. This is the capacity planning data we need for Voice.

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**"




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**"

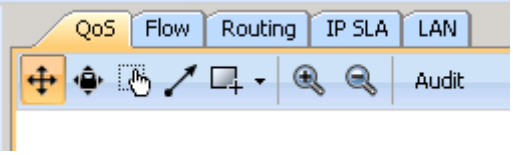



Notice how this shows a bandwidth graph of the data being transmitted out each WAN interface. In this example, we are focused on High Priority Data/ AF31 traffic. This is the capacity planning data we need for the High Priority Data.

**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.**

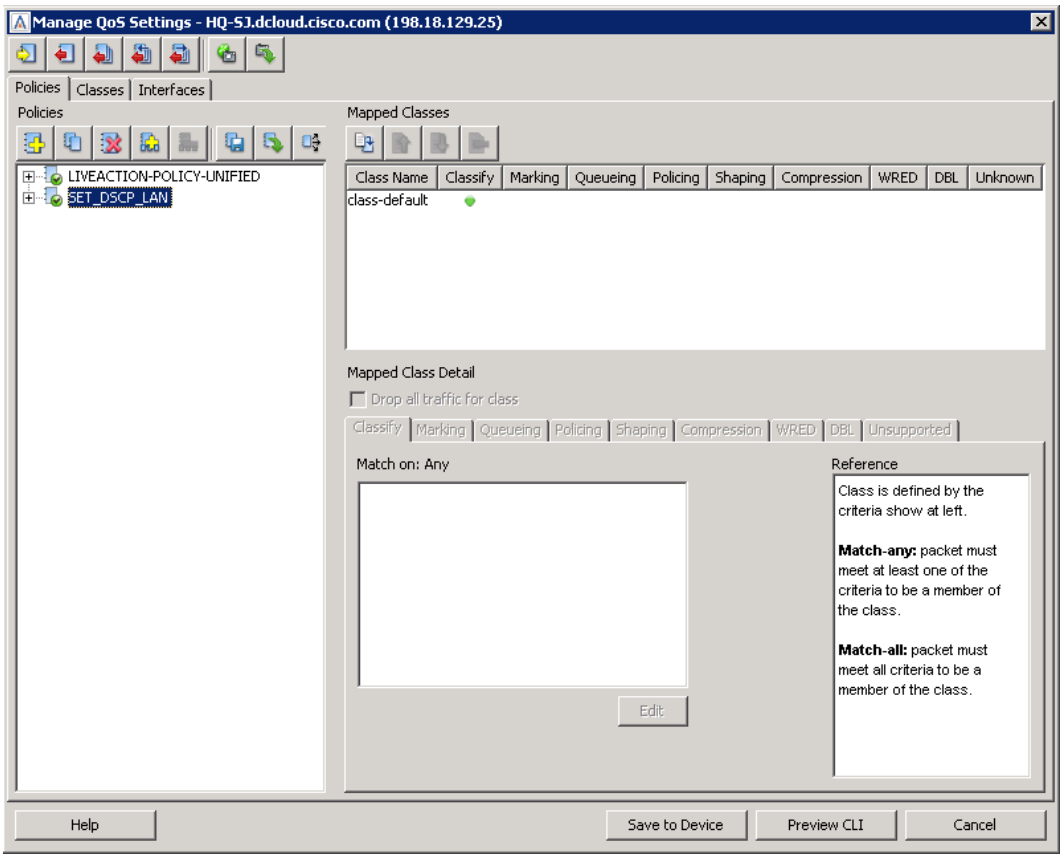
# Lab 3.2: Building Queueing Policies

1. From the LiveAction map, select the QoS Tab

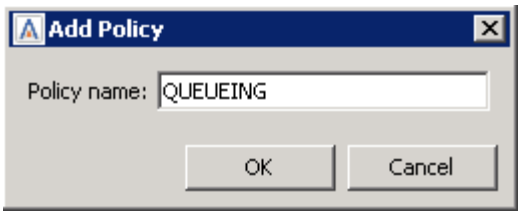



2. **Right-click** the HQ router, select **QoS > Manage QoS Settings**

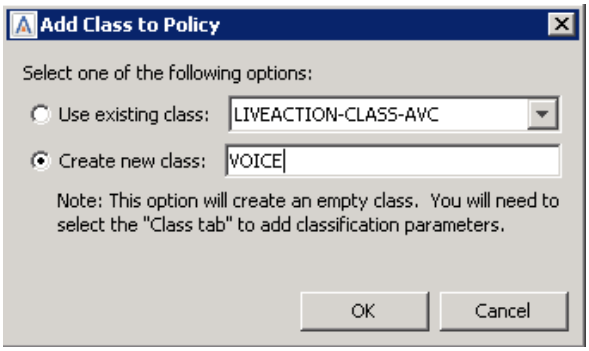

The **Manage QoS** Dialog Window will open



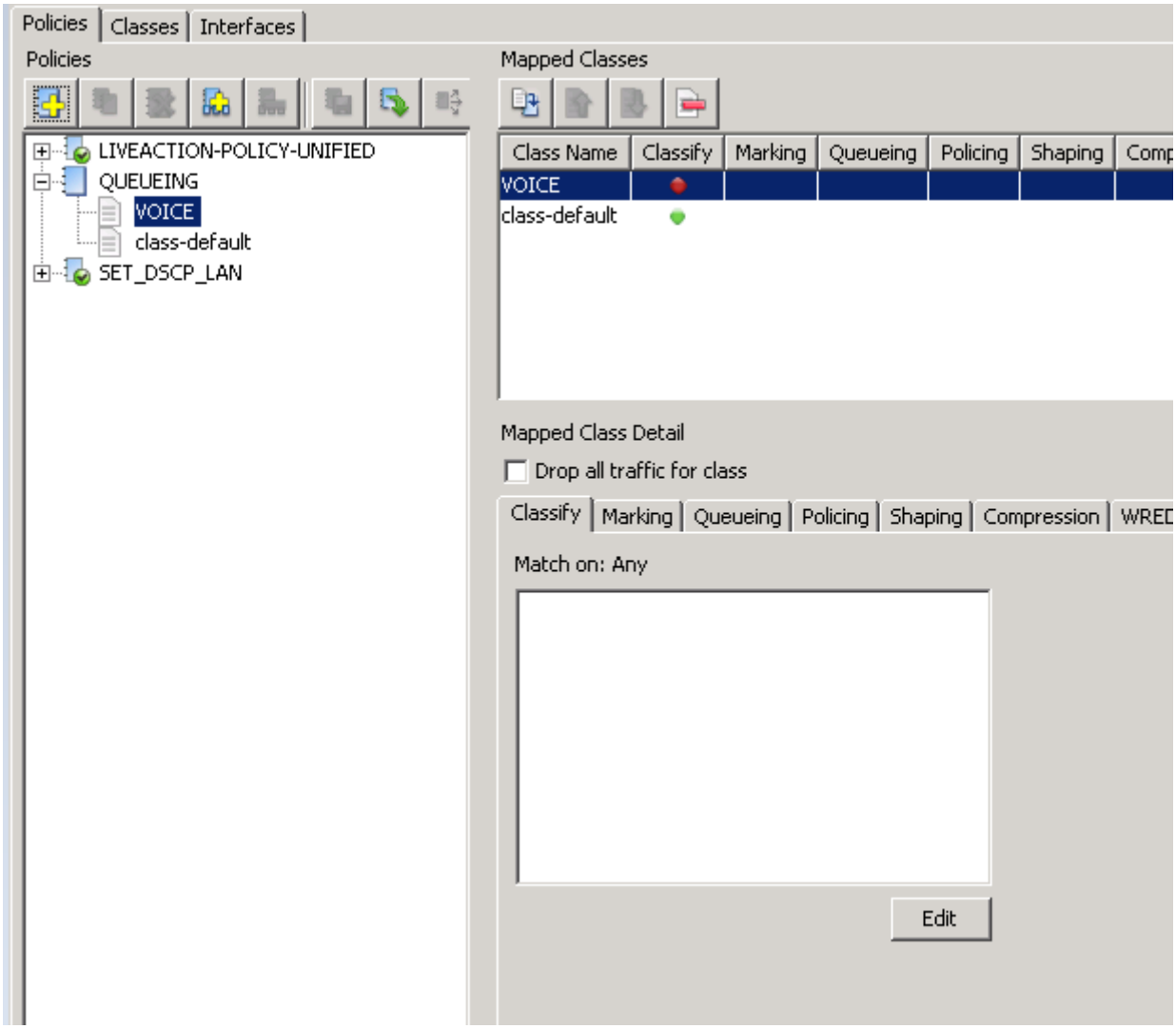
3. **Add** a new Policy and name it **QUEUEING**.



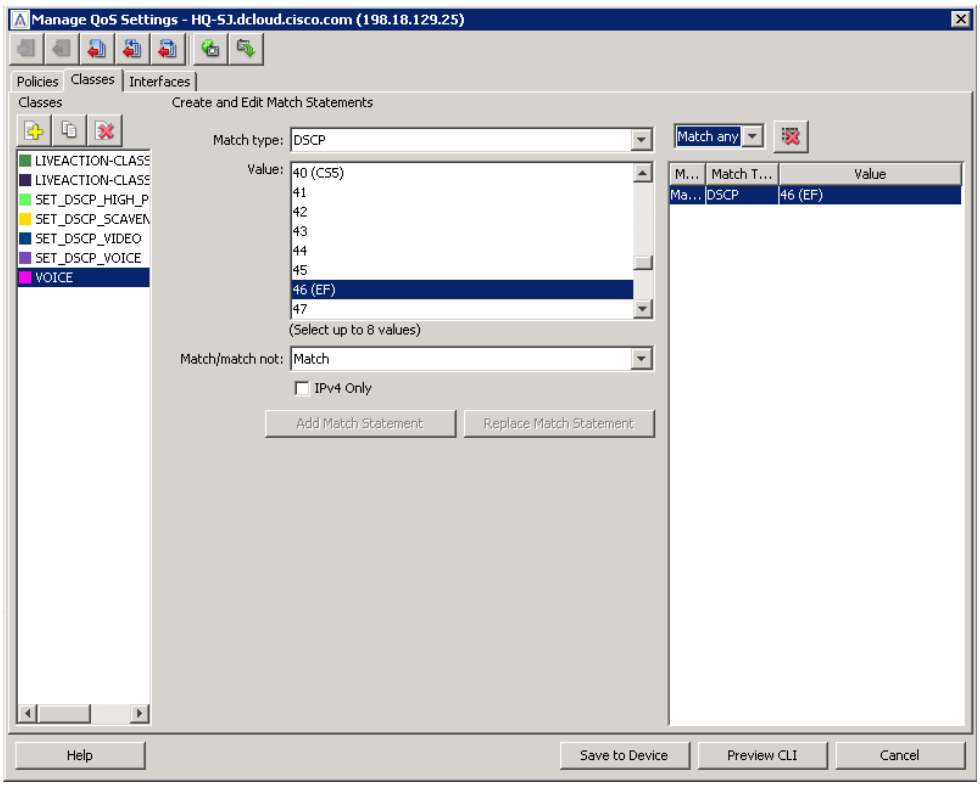

4. Create a **new class** for the QUEUEING policy and name it **VOICE**.



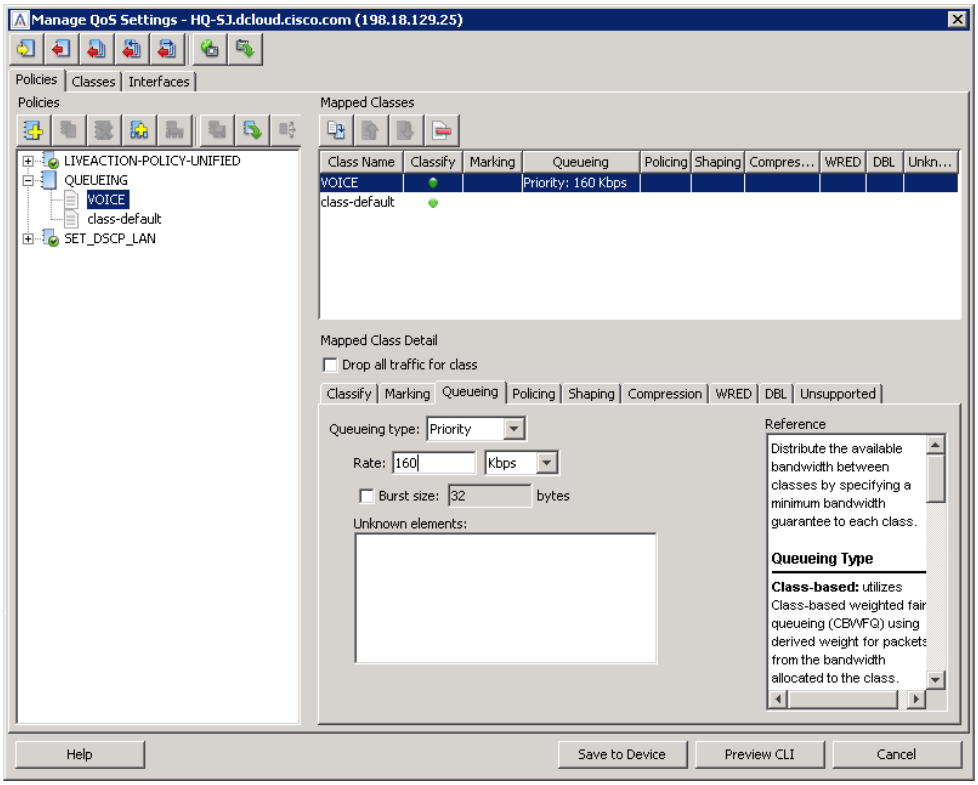

You should see the **VOICE** class inside the policy named **QUEUEING**



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



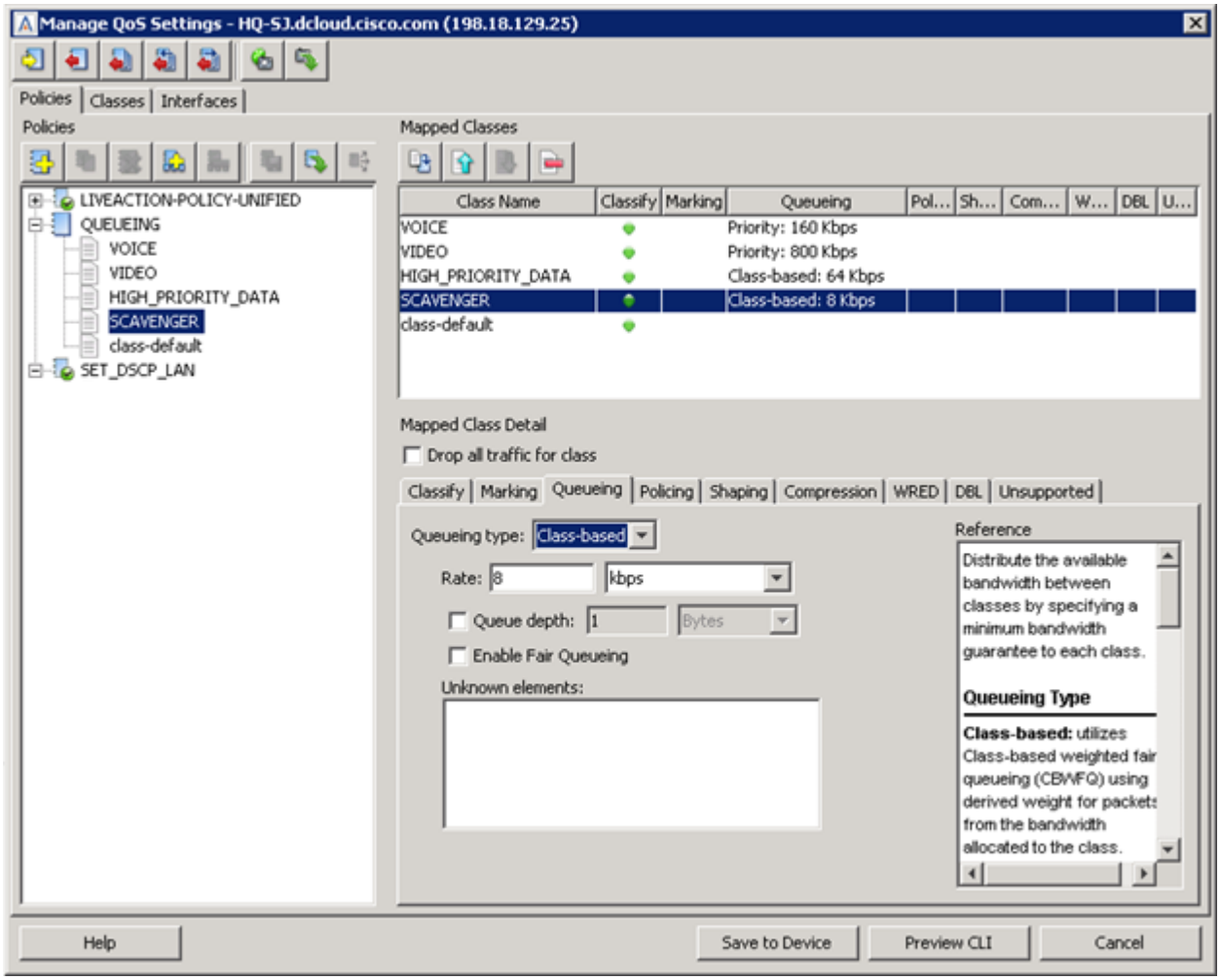

6. **Return** to the **Policies** tab
7. Ensure the **VOICE class** of **QUEUEING** policy is highlighted and select the **Queueing** tab.
8. Set the **Queueing type** to **Priority** and the bandwidth to **160 Kbps**.



9. **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 |

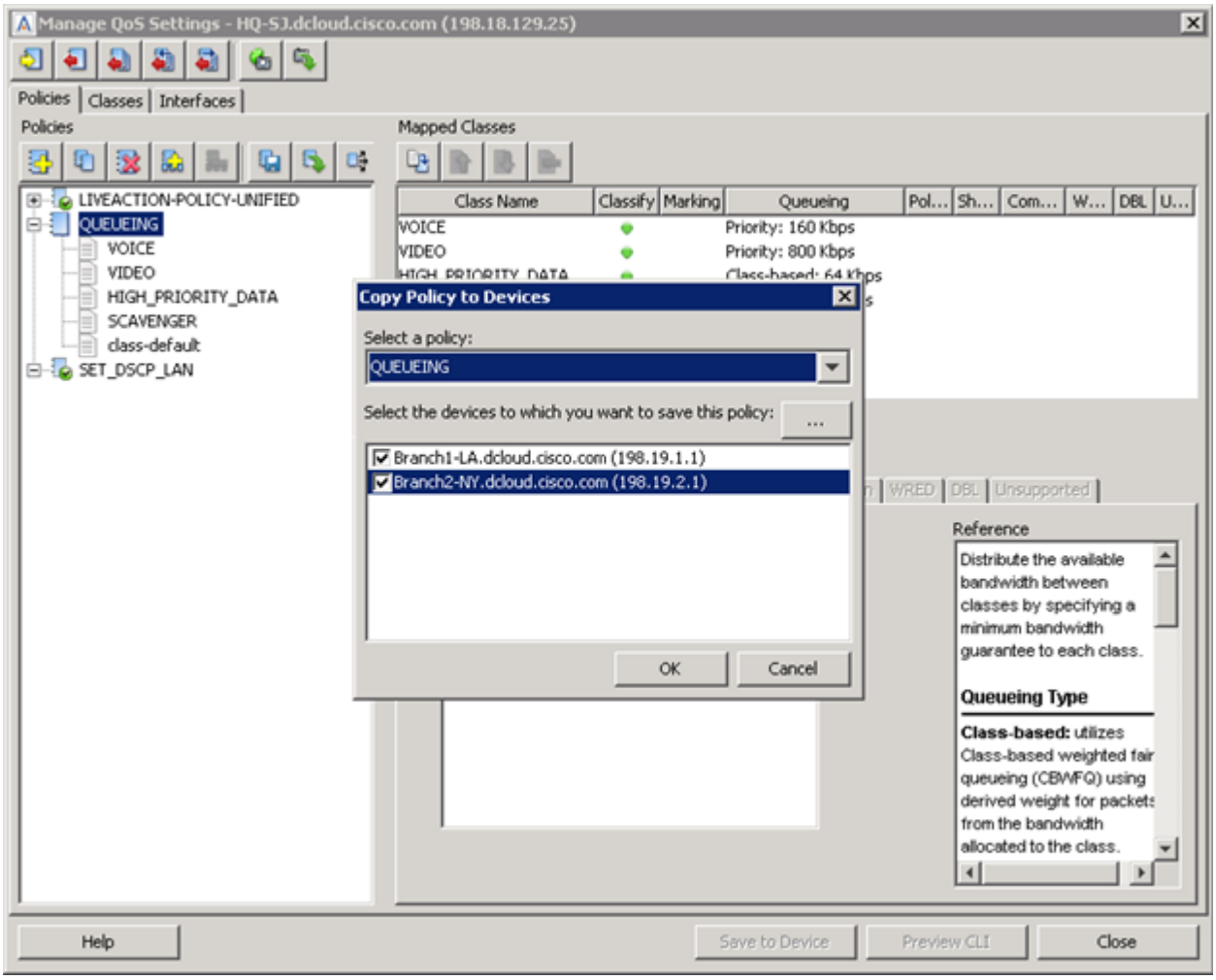
When finished, the **QUEUEING** policy should look similar to this:



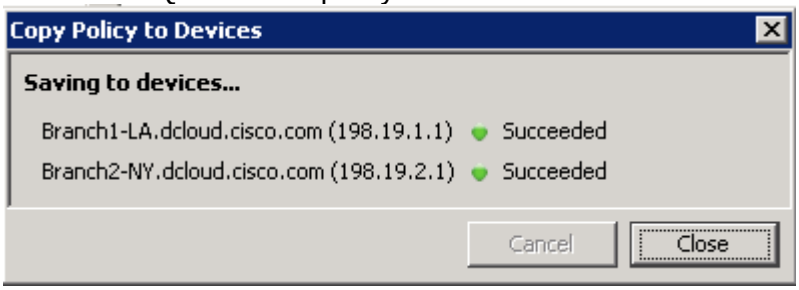

10. Click **Save to Device.**

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.




12. **Push** the QUEUEING policy to the other routers




**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.

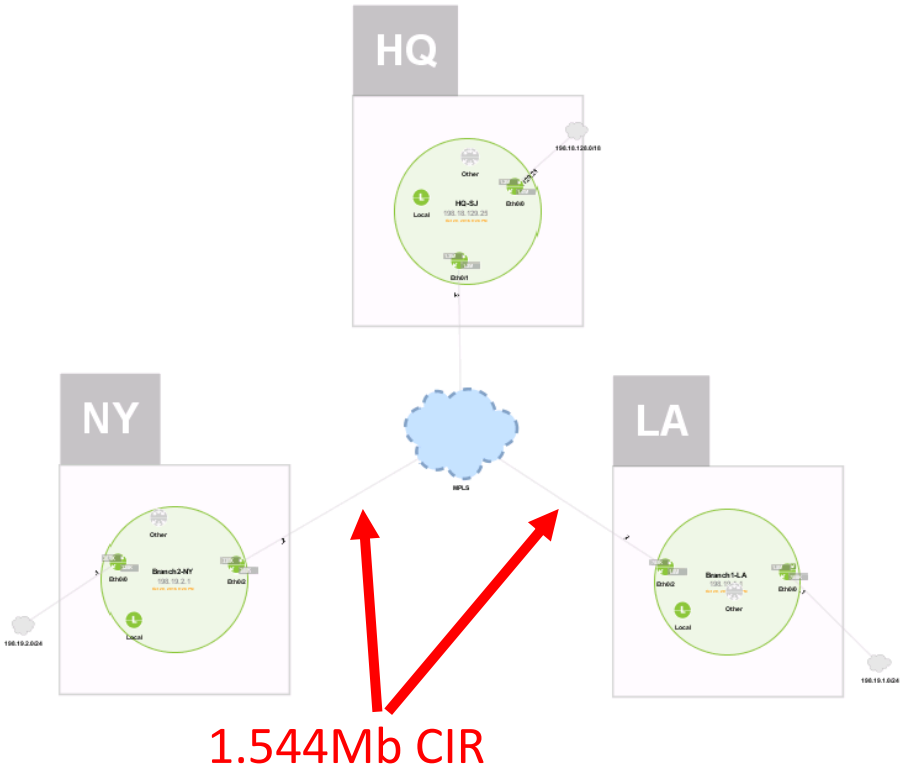
Below is a diagram of the lab network.  The MPLS network in our lab does have CIRs in place with the following deign:

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.




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

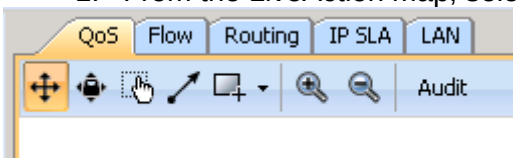
- HQ - Multi-class hierarchical shaping policy*
- NY - basic hierarchical shaping policy
- LA - basic hierarchical shaping policy

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

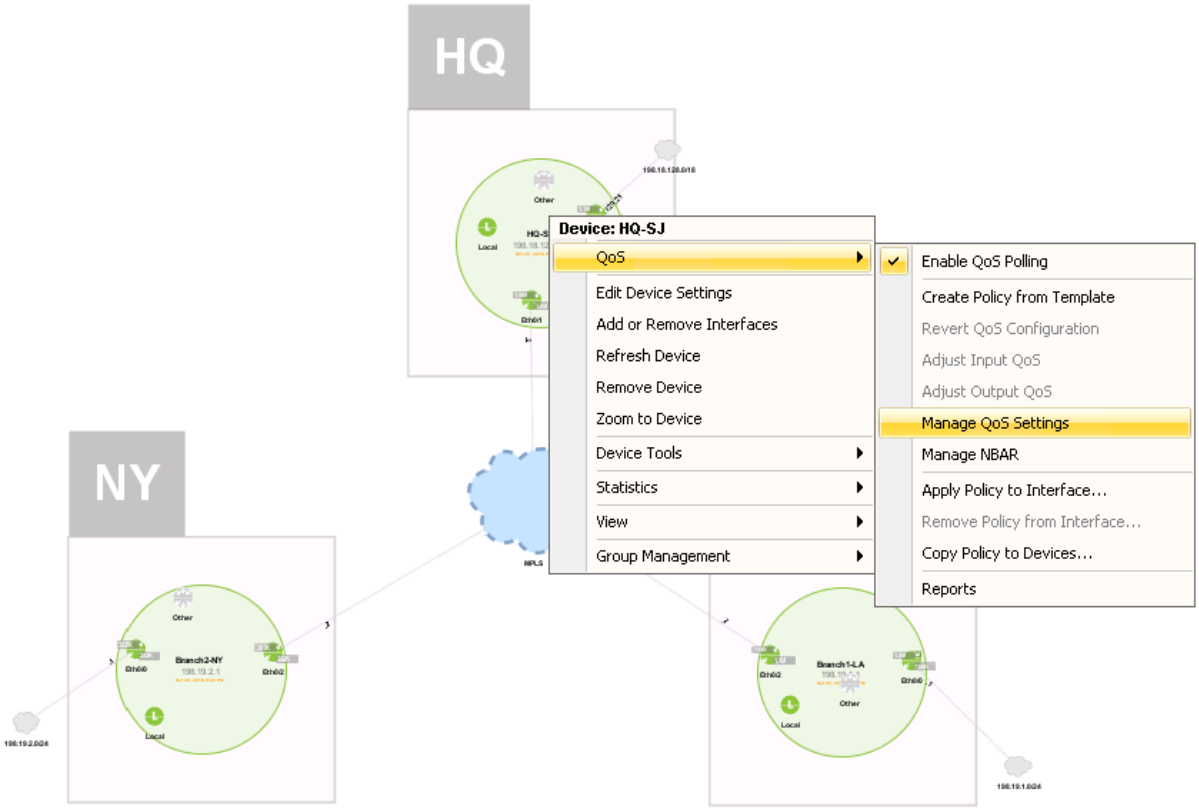
# Lab 4.1: Shaping (Scaling)

Lab Steps:

1. From the LiveAction map, select the QoS Tab

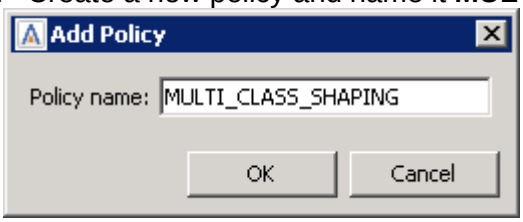



2. Right-click on the HQ router, select QoS > Manage QoS Settings

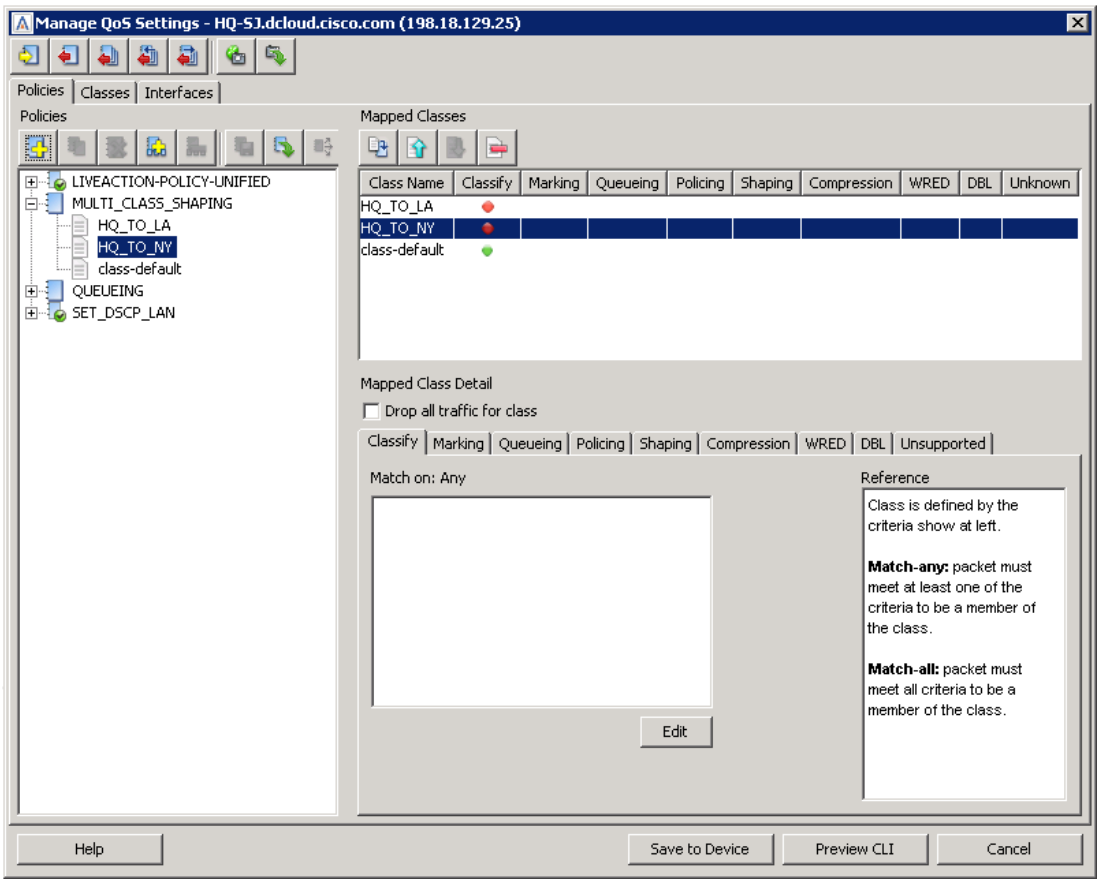



The Manage QoS Dialog Window will open

3. Create a new policy and name it **MULTI_CLASS_SHAPING**

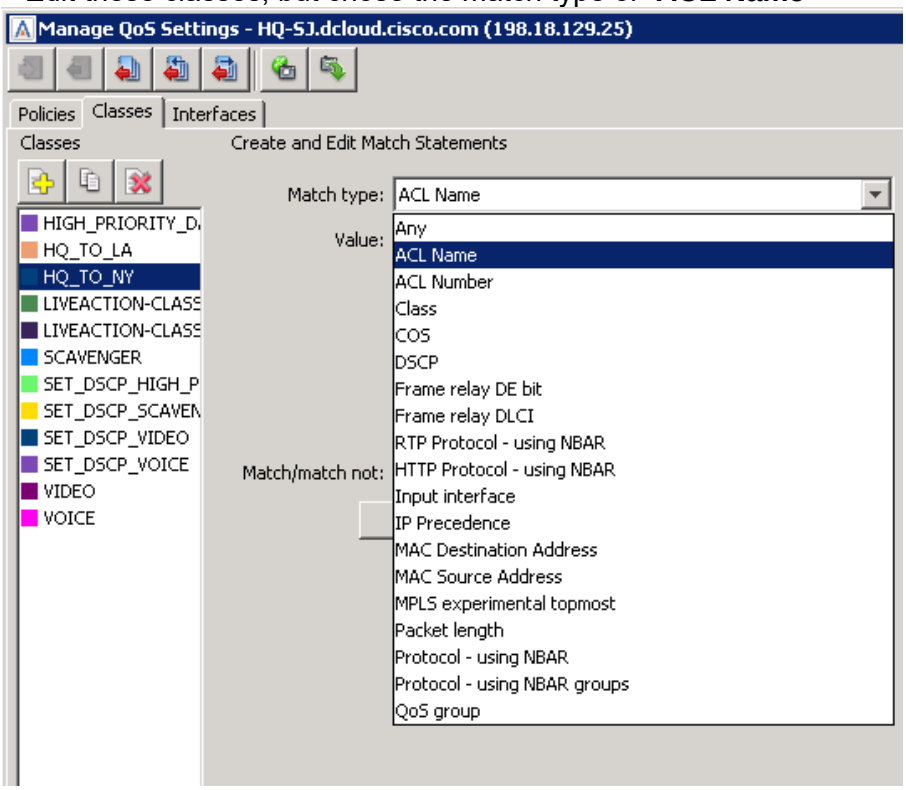



4. Create two classes within this Policy:
   - **HQ_TO_NY**
   - **HQ_TO_LA**



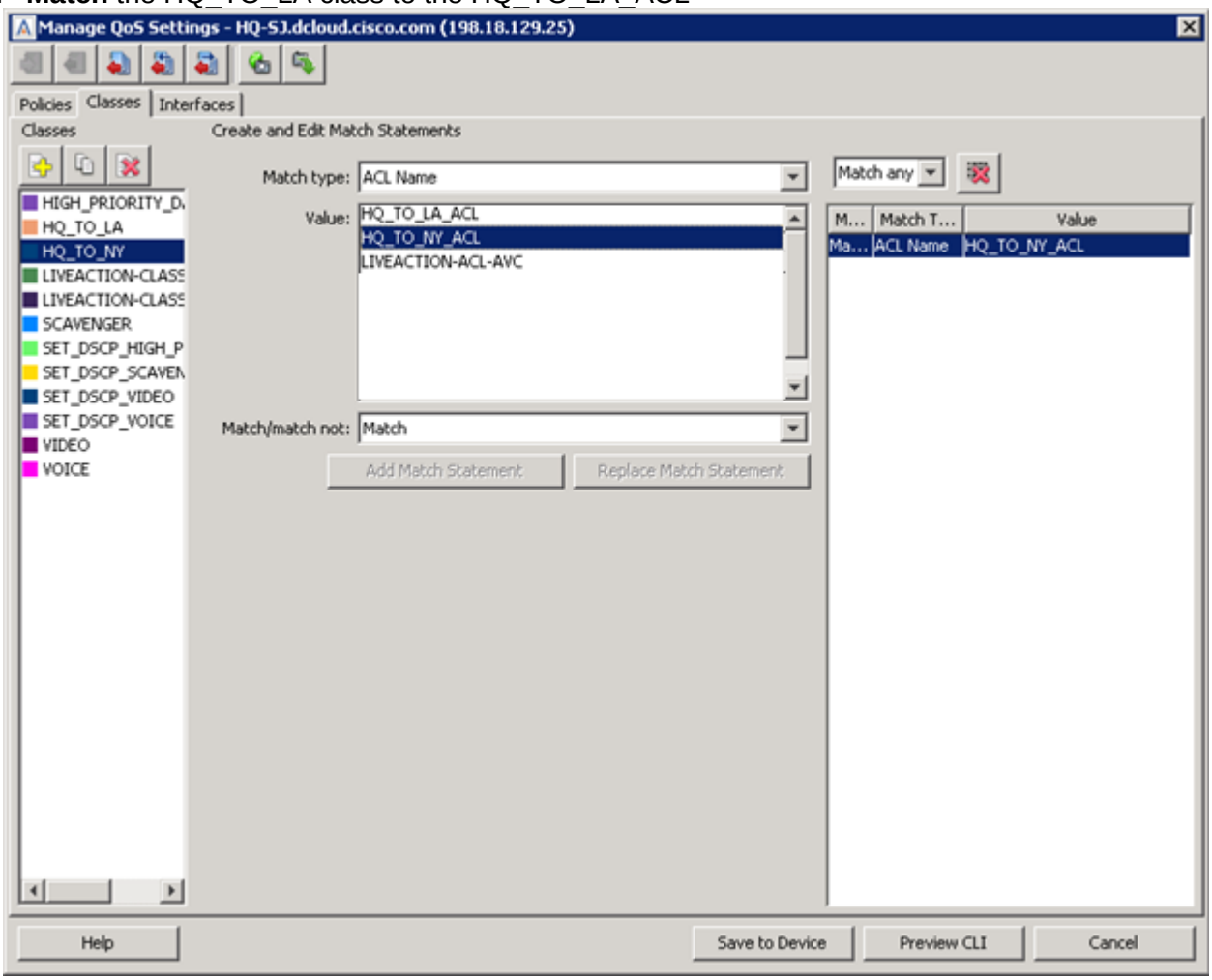

**Note:** These classes each reference an access-list (ACL) for matching traffic from HQ to the respective remote sites. **These ACLs may NOT have been created… you may need to create 2 ACLs before continuing with the Lab.**

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

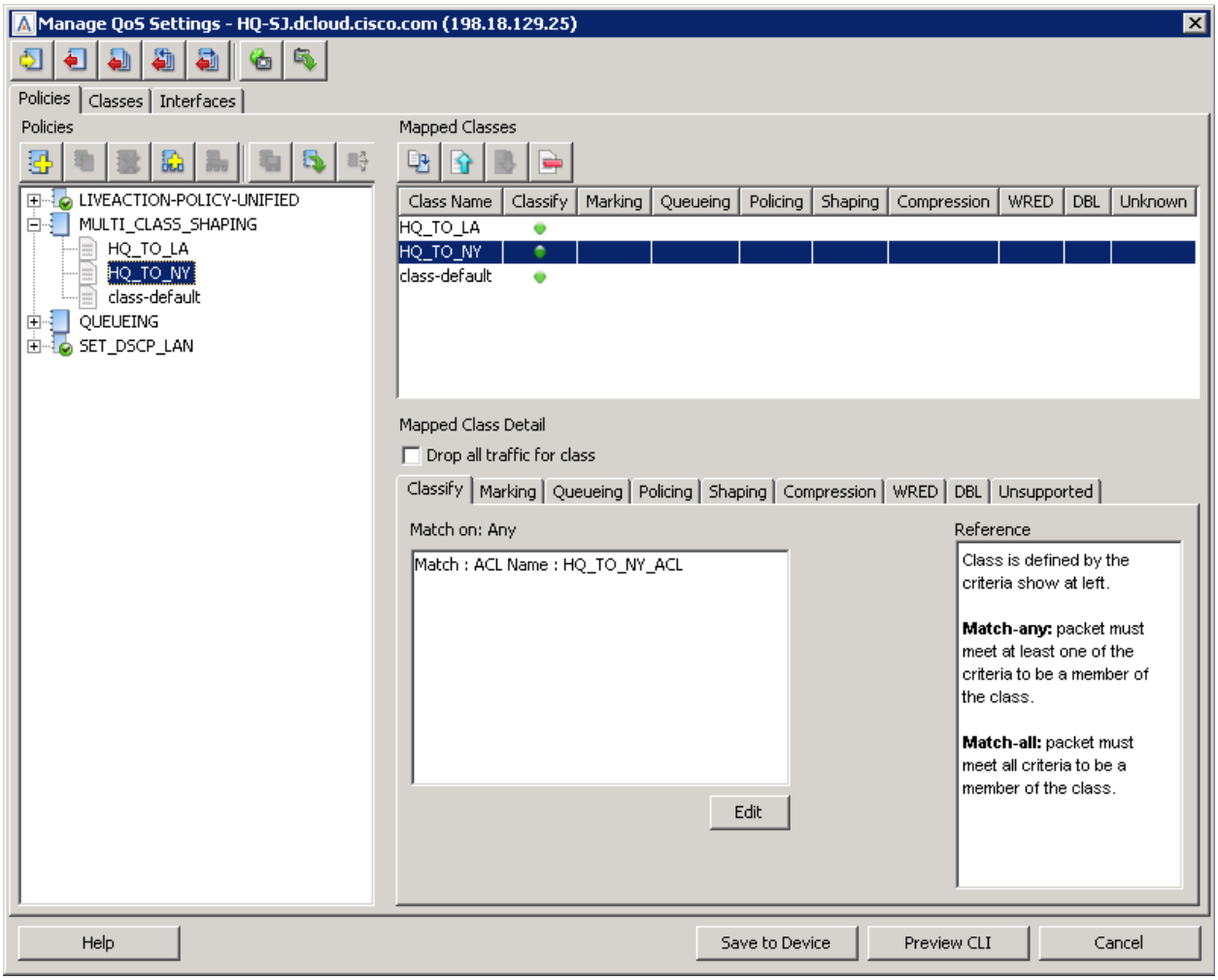


**Note:** You may need to create the following ACLs on your Training Pod. Use the steps you learned in Lab Workbook Pt.1, to create the new ACLs. Create “HQ_TO_NY” from IP 198.18.129.0/24 to 198.19.2.0/24, and “HQ_TO_LA” from IP 198.19.129.0/24 to 198.19.1.0/24

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

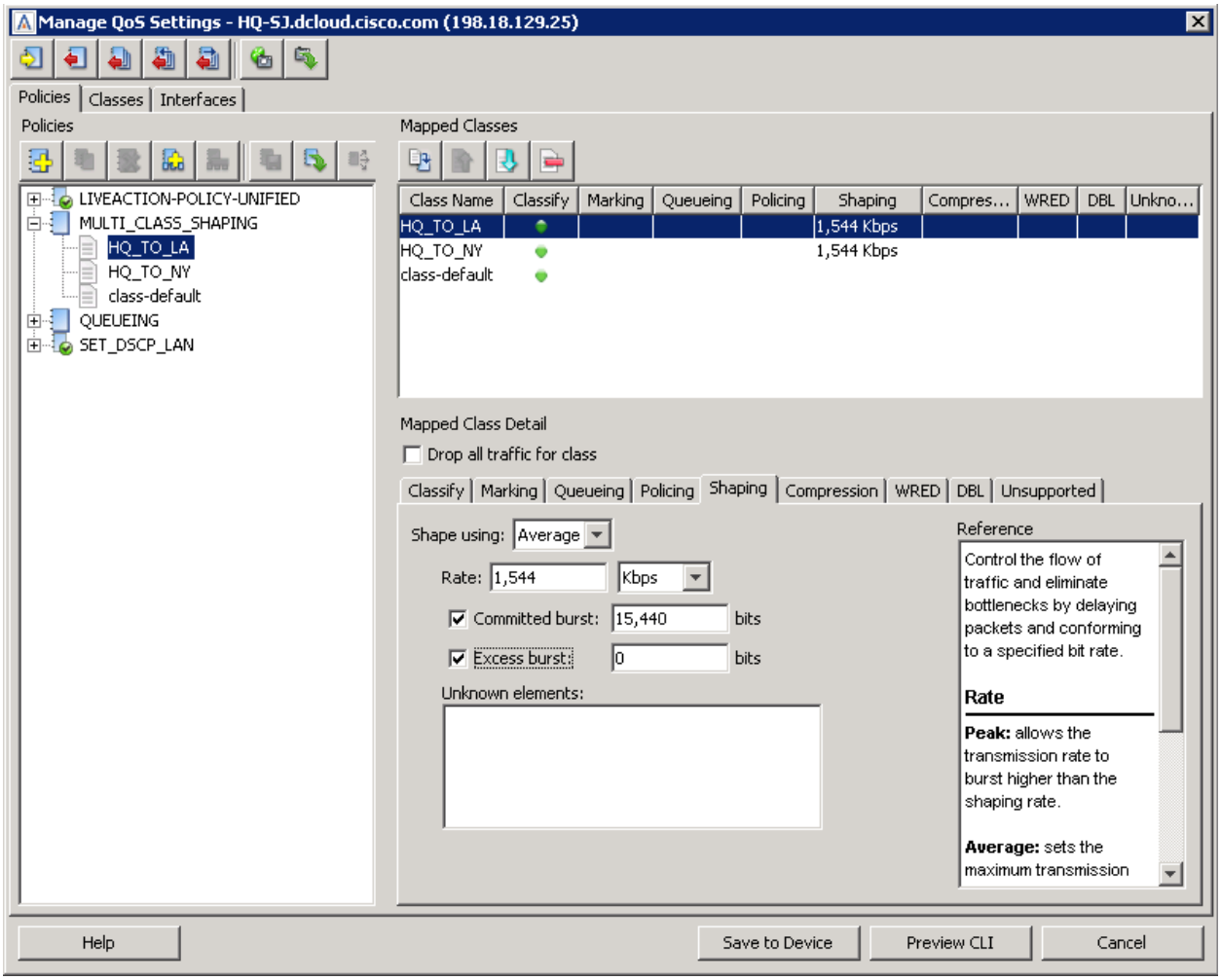



8. When finished, return to the **Policy** tab



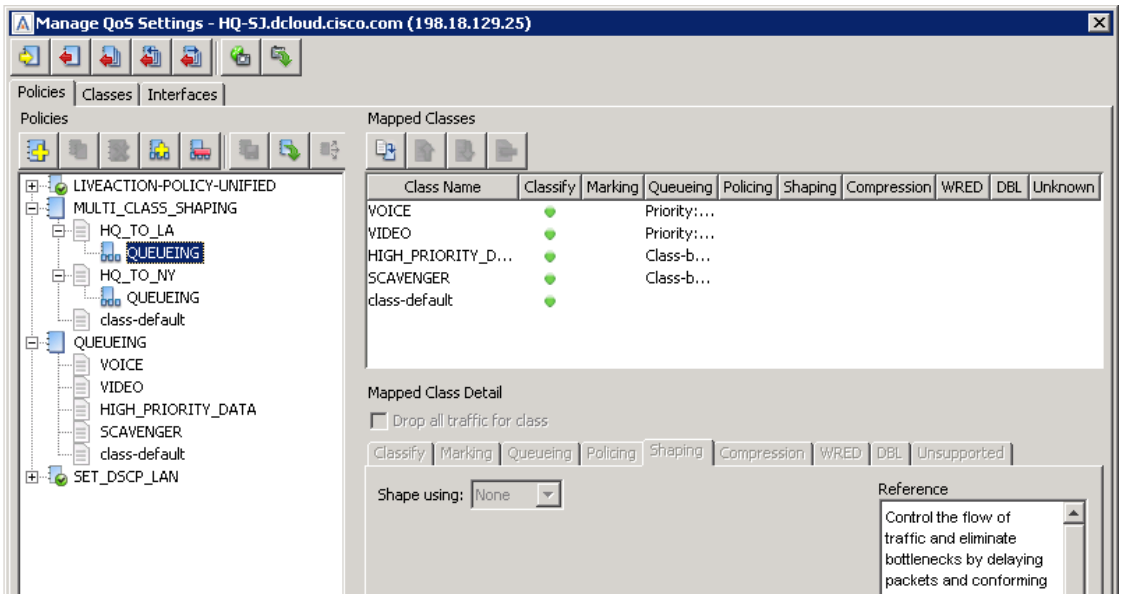

9. Select the **HQ_TO_NY** class and select the **shaping** tab. Set its parameters to:
    - Shape using = Average
    - Rate = 1544 Kbps
    - Committed burst = 15,440
    - Excess burst = 0

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

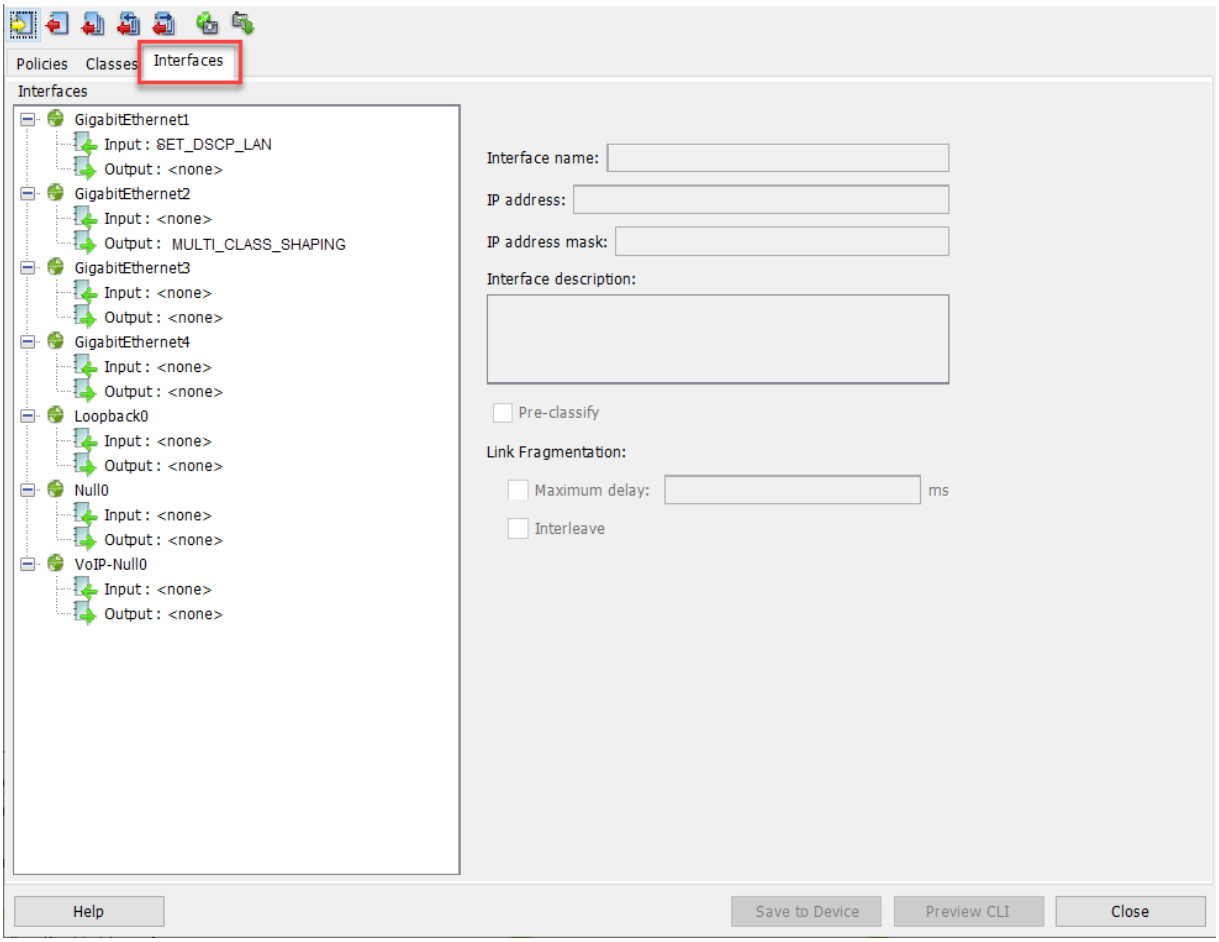



11. **Click-Drag-and-Drop** the QUEUEING **policy** to the **class-default** of the HQ_TO_NY policy
12. **Click-Drag-and-Drop** the QUEUEING **policy** to the **class-default** of the HQ_TO_LA policy

When finished your view should look like this:



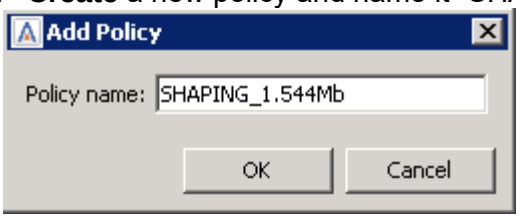

13. Select the interfaces tab and **apply** the MULTI_CLASS_SHAPING policy to the **output** of the GigabitEthernet2 interface.



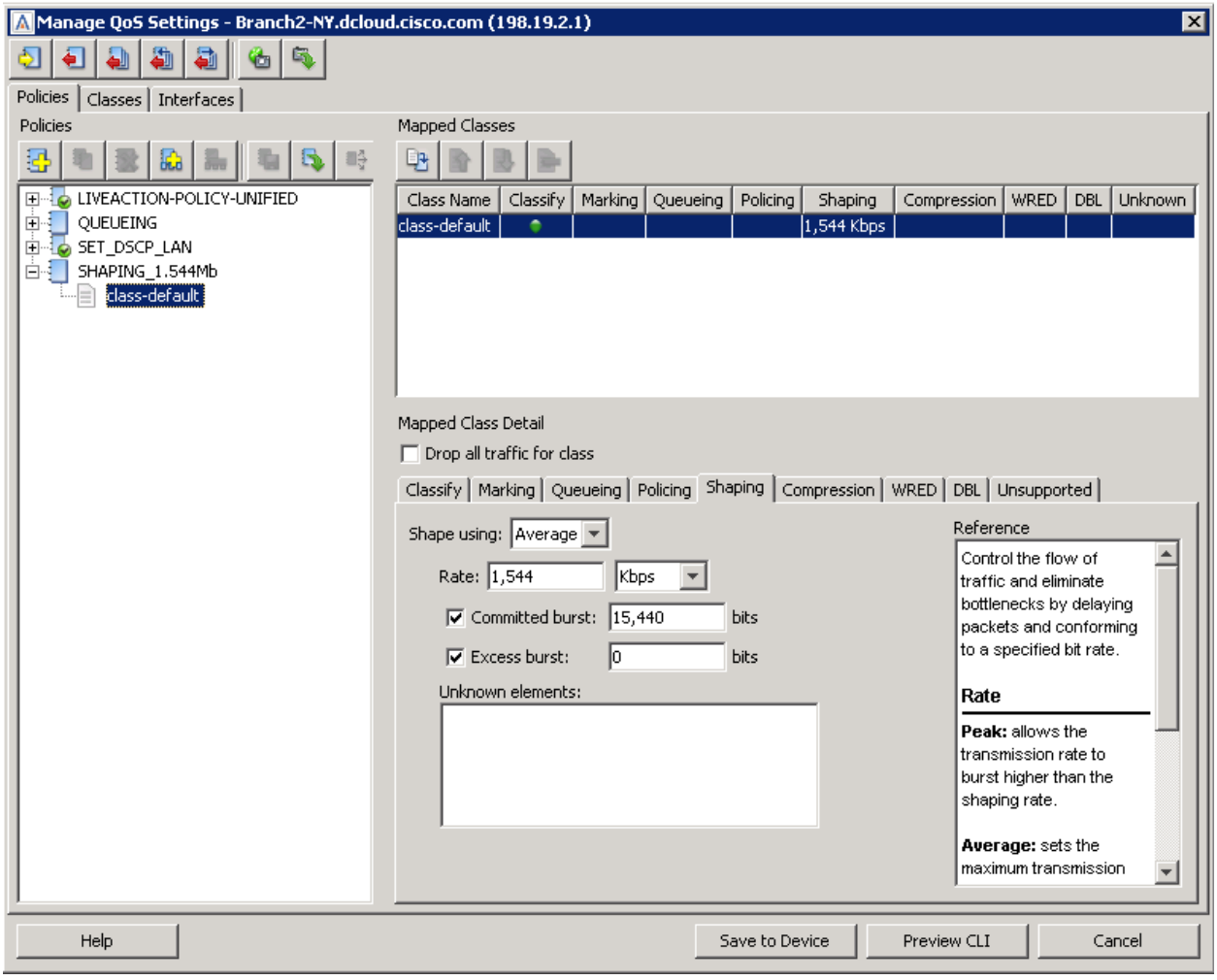

14. Click **Save to Device**.

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

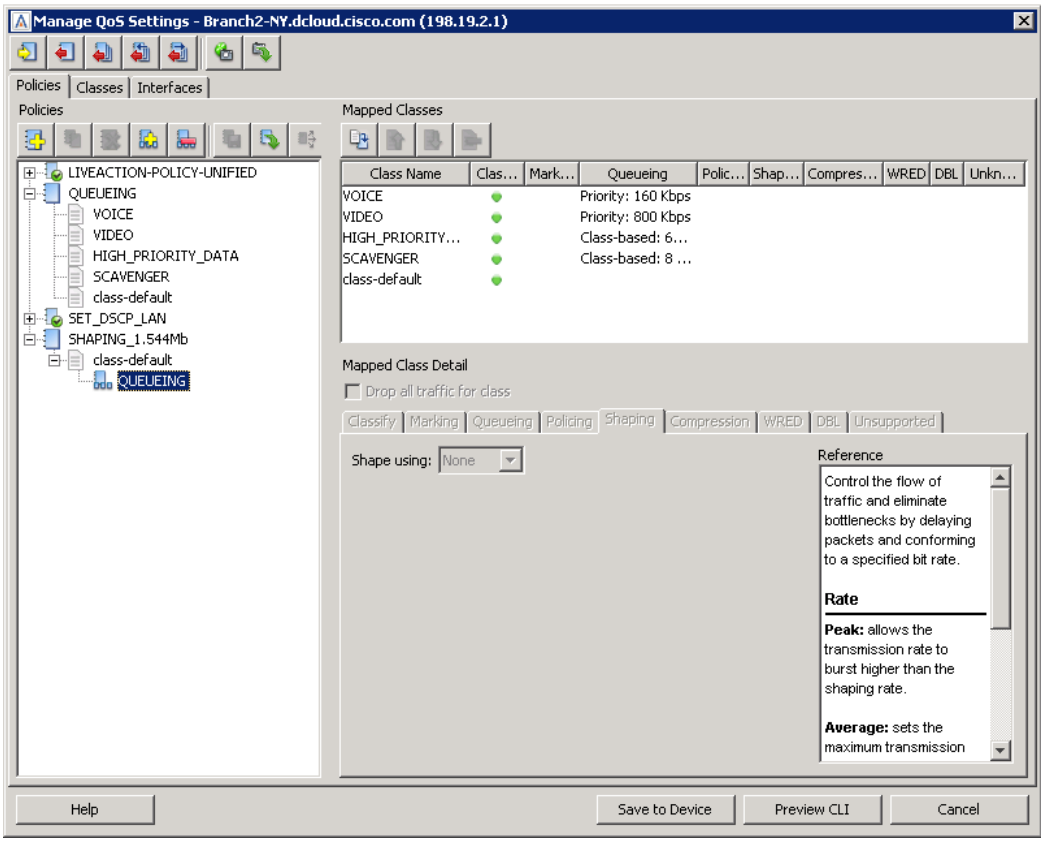
1. In LiveNX, select the **QoS Tab**
2. **Right-click** on the one of the **remote** routers, select **QoS > Manage QoS Settings**
3. **Create** a new policy and name it “SHAPING_1.544Mb”



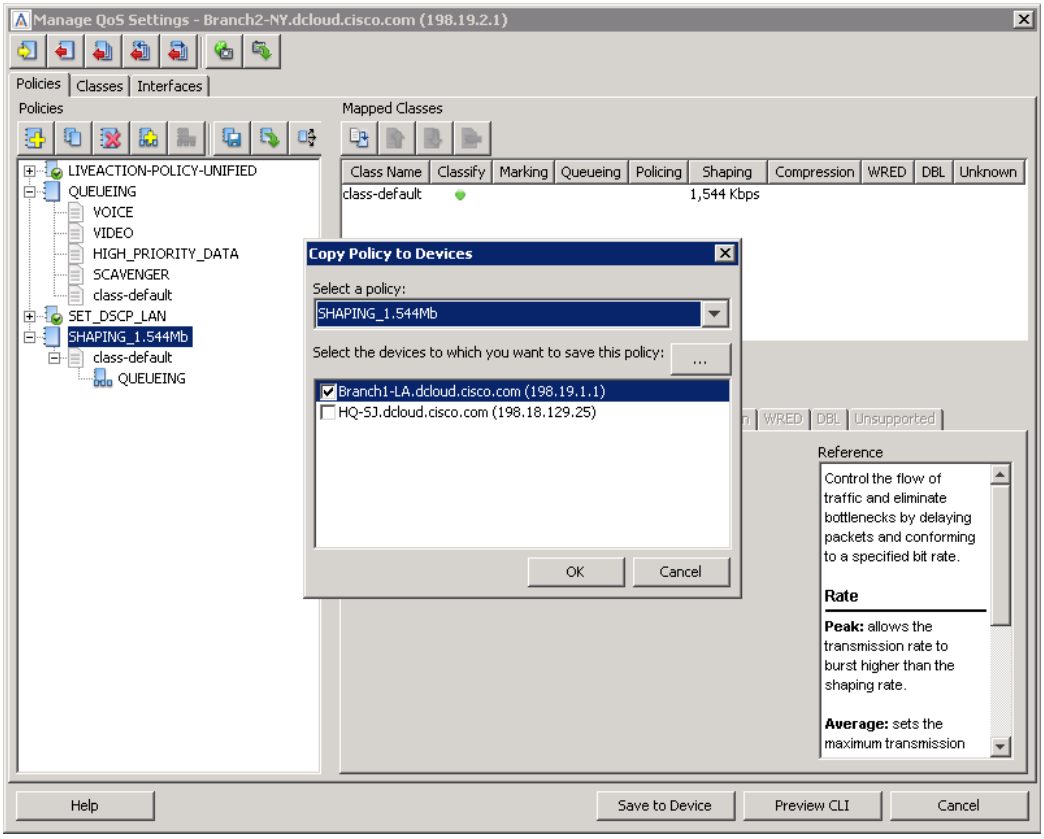

4. Select its **class-default** and select the **Shaping** tab.
5. Implement a **shaping policy** with the following parameters:
   - Shape using = Average
   - Rate = 1544 Kbps
   - Committed burst = 15,440
   - Excess burst = 0



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

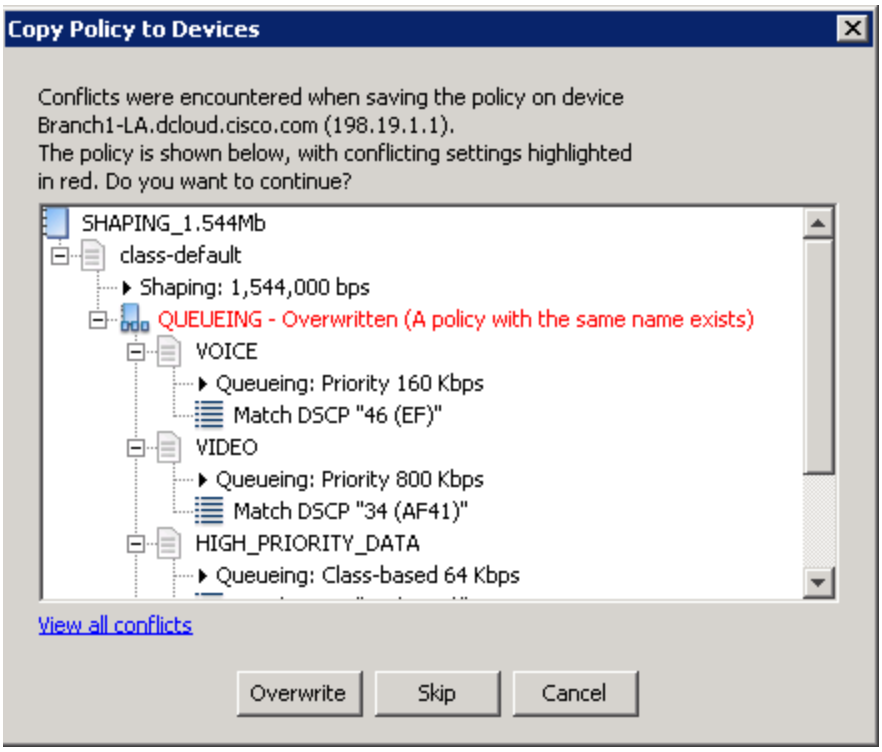



7. Copy the SHAPING_1.544Mb policy to **the other remote router**

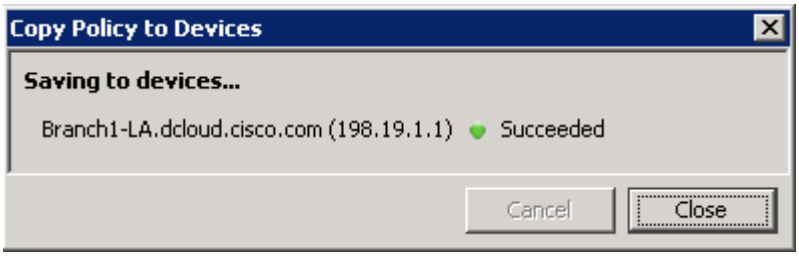


You will be warned there is a conflict. This is because a policy named QUEUEING already exist on the other remote router.

8. Select **Overwrite**.



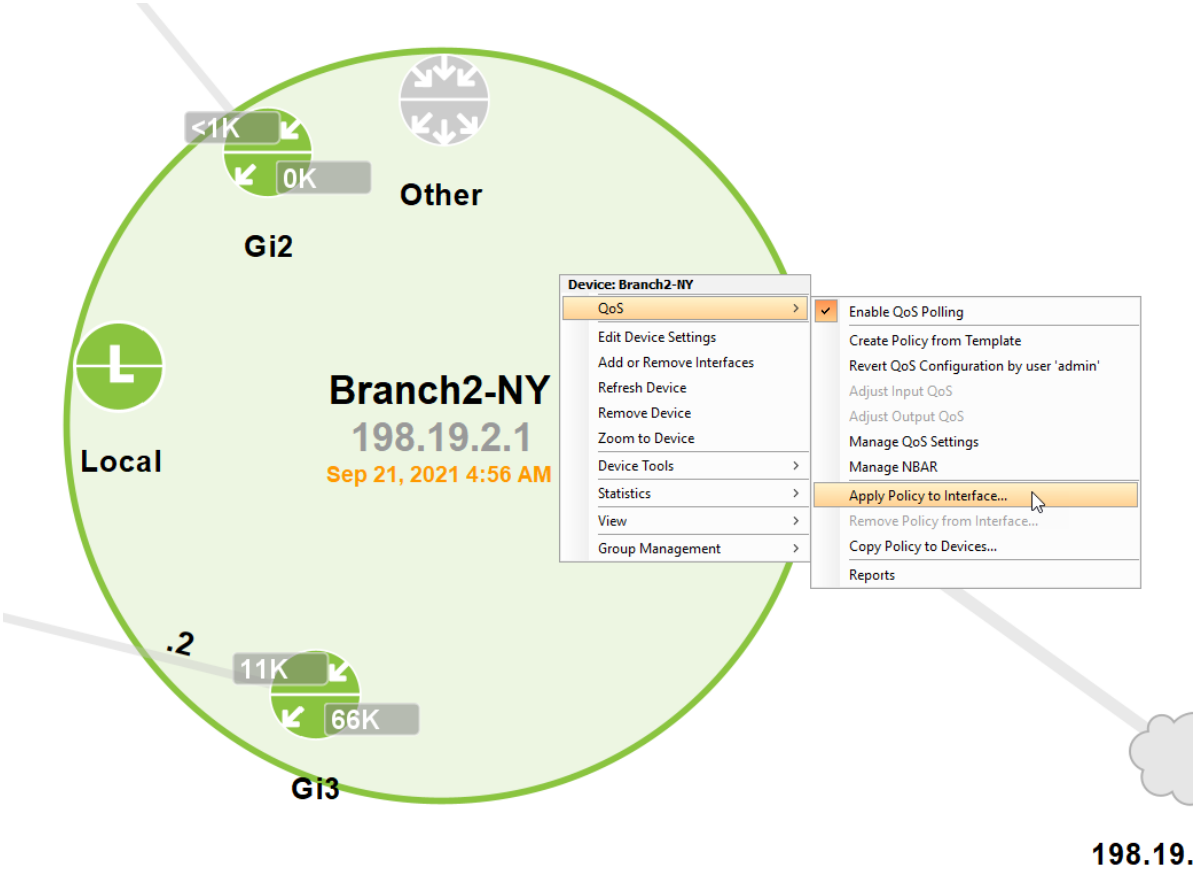

9. Validate the changes saved successfully.



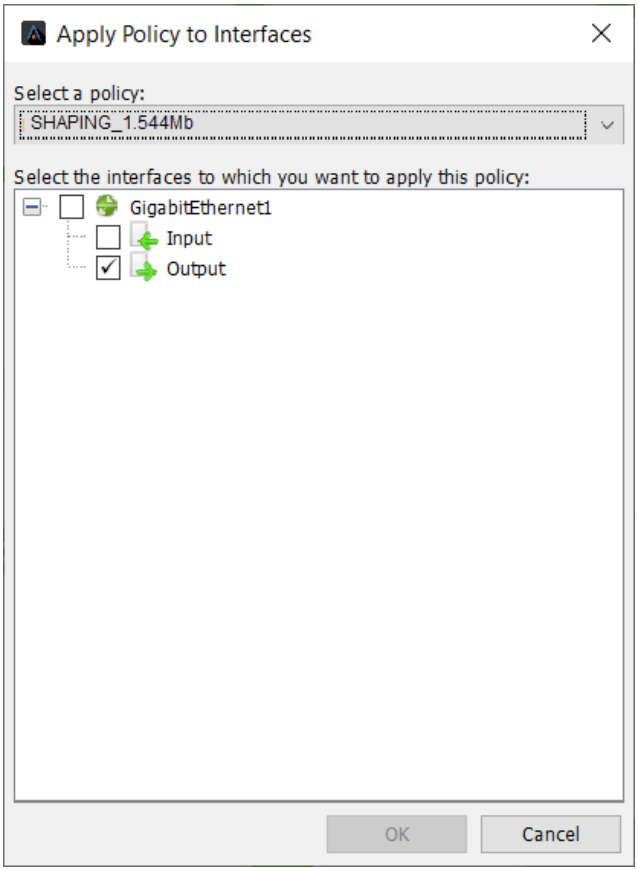

10. **Save to Device** and close the Manage QoS Settings dialog window.

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 GigabitEthernet3.

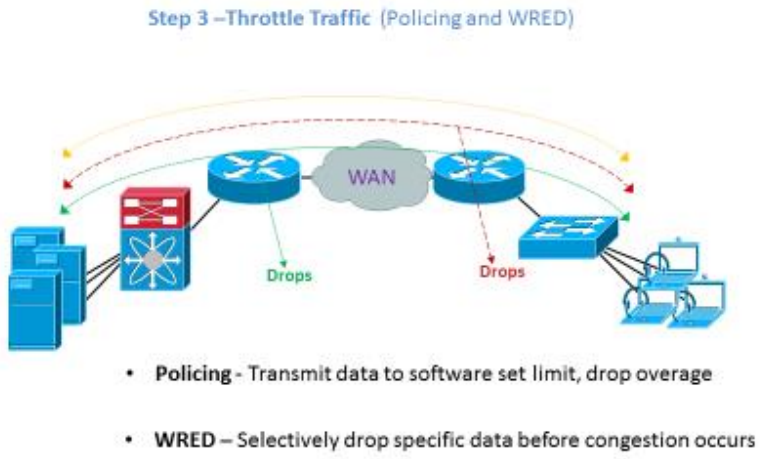



14. Repeat this process and apply the SHAPING_1.544Mb policy to the **other remote router**.

# Lab 5

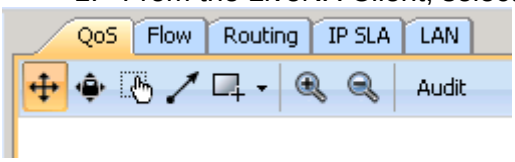
## Lab 5:  Throttling Traffic

# Lab 5.0: Intro - Throttling / Policing

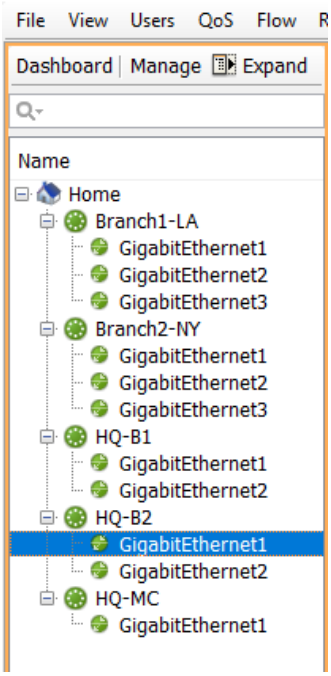



Investigate the current traffic flows.

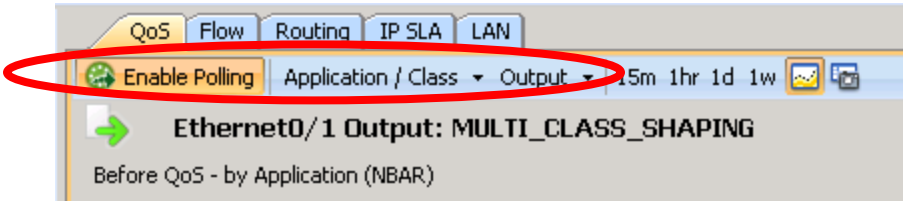
1. From the LiveNX Client, select the **QoS** Tab



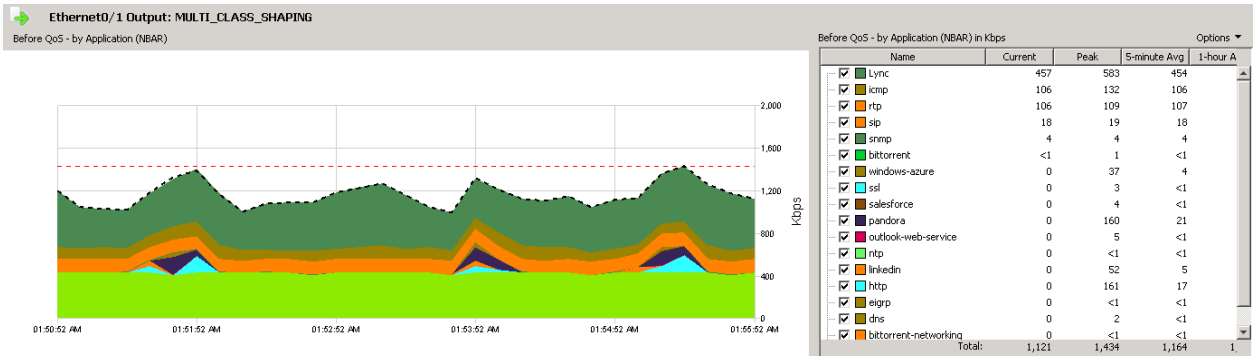

2. Select **GigabitEthernet1** from the **HQ-B2** router



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

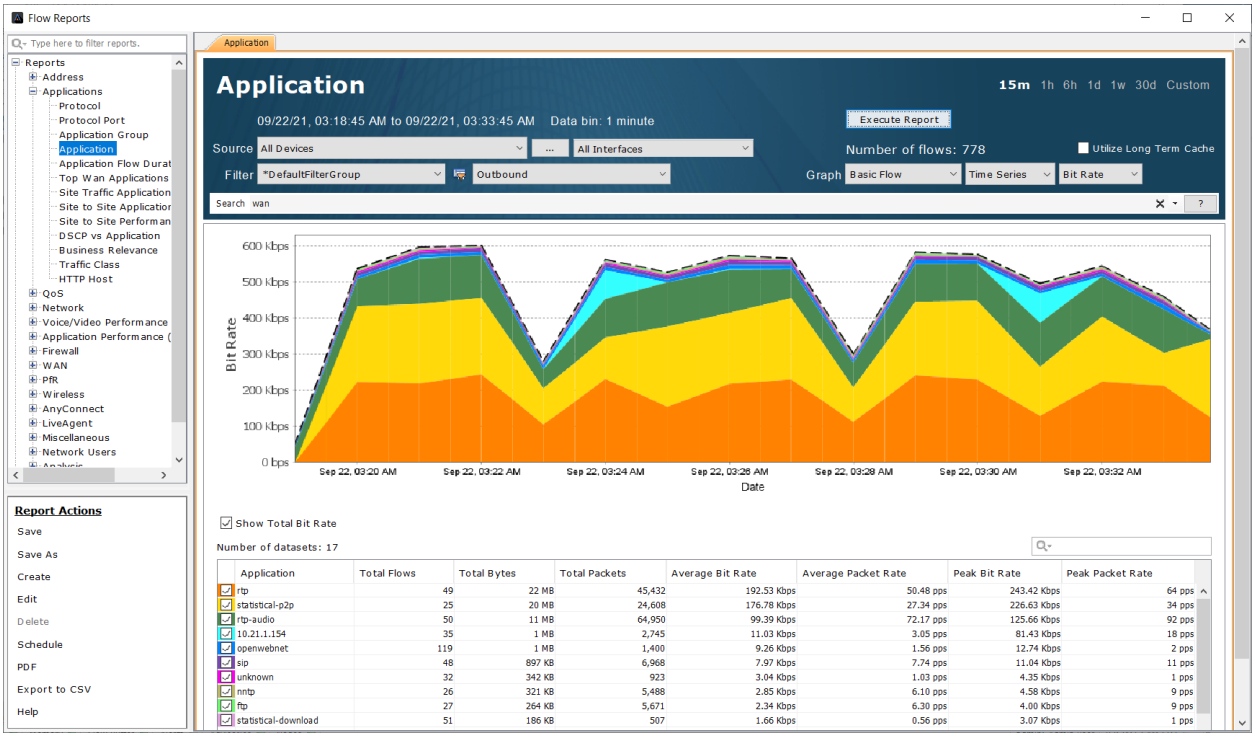



Notice the applications listed in the NBAR view at the top right of the page:




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

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

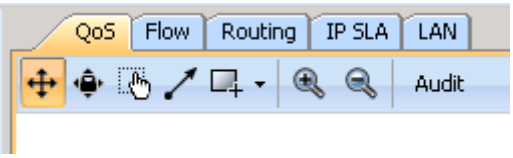


# Lab 5.1: Throttling / Policing

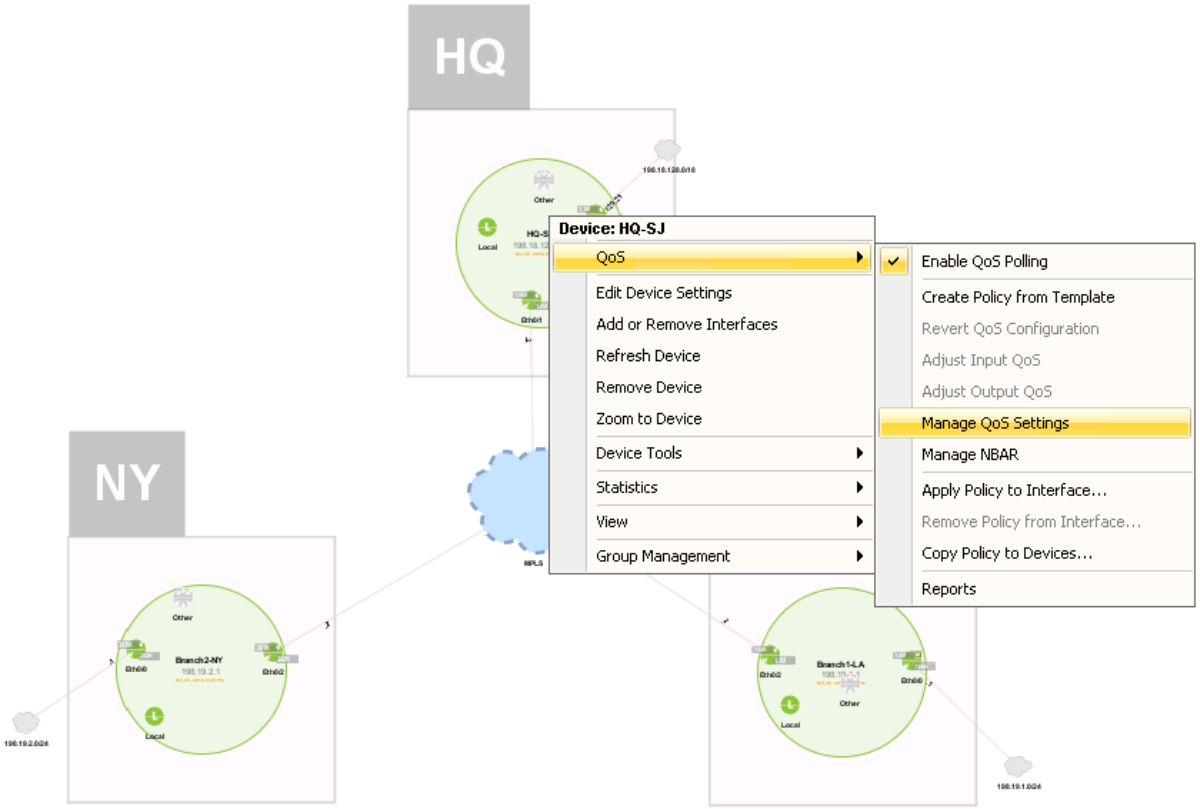
We'll implement a basic policing polity to throttle any scavenger (less than default) traffic.

Lab Steps:

1. From the LiveAction map, select the **QoS** Tab

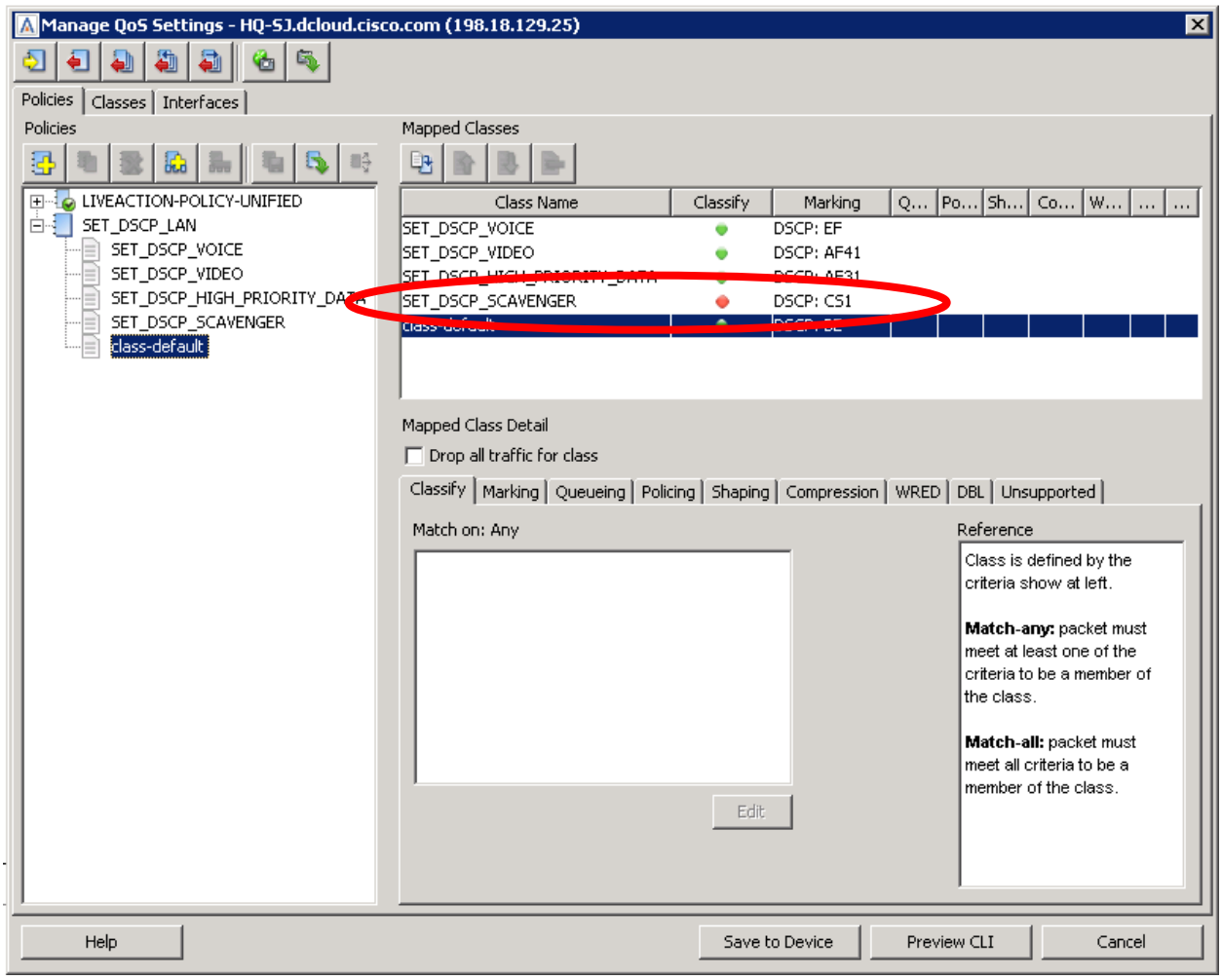



2. Right-click on the **HQ-B2** router and select **QoS > Manage QoS Settings**

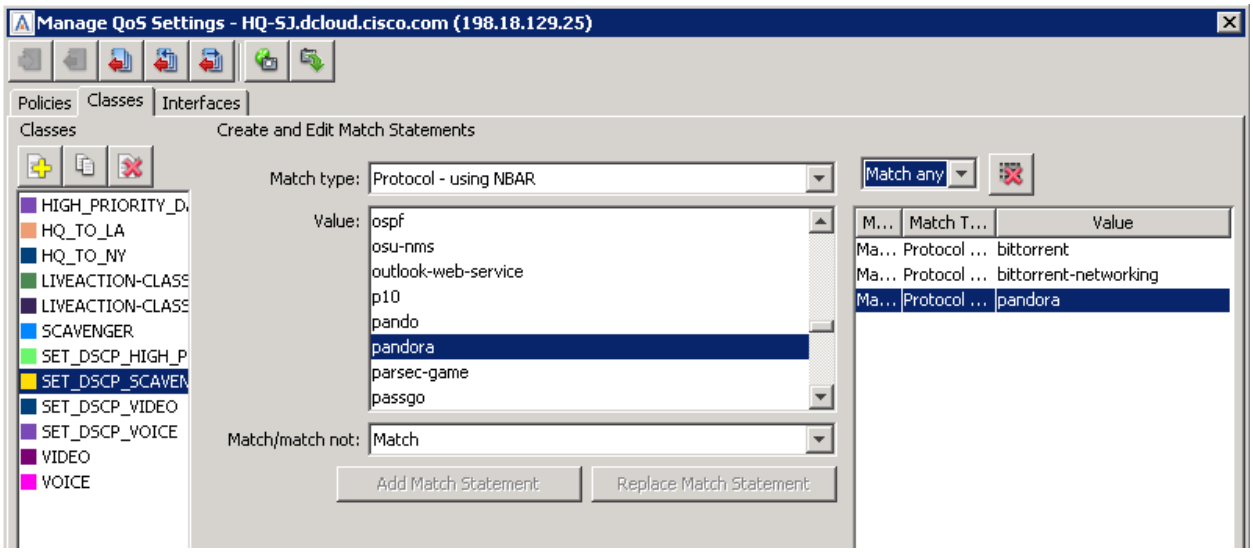



Remember how we created a SET_DSCP_SCAVENGER class as part of the SET_DSCP_LAN policy? But also remember how we did not assign any classification to this class?

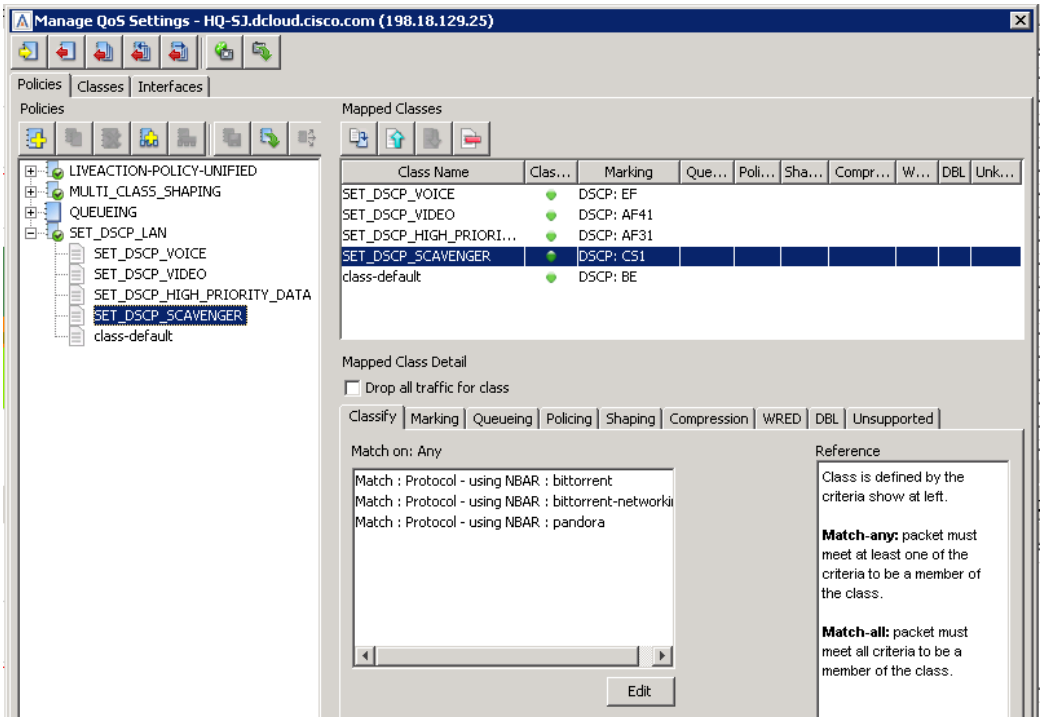
| Class Name | DSCP | NBAR Protocol(s) |
|---|---|---|
| **SET_DSCP_VOICE** | EF (46) | rtp |
| **SET_DSCP_VIDEO** | AF41 (34) | Lync |
| **SET_DSCP_HIGH_PRIORITY_DATA** | AF31 | SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce |
| **SET_DSCP_SCAVENGER** | CS1 (8) | *Leave blank for now* |
| **Best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



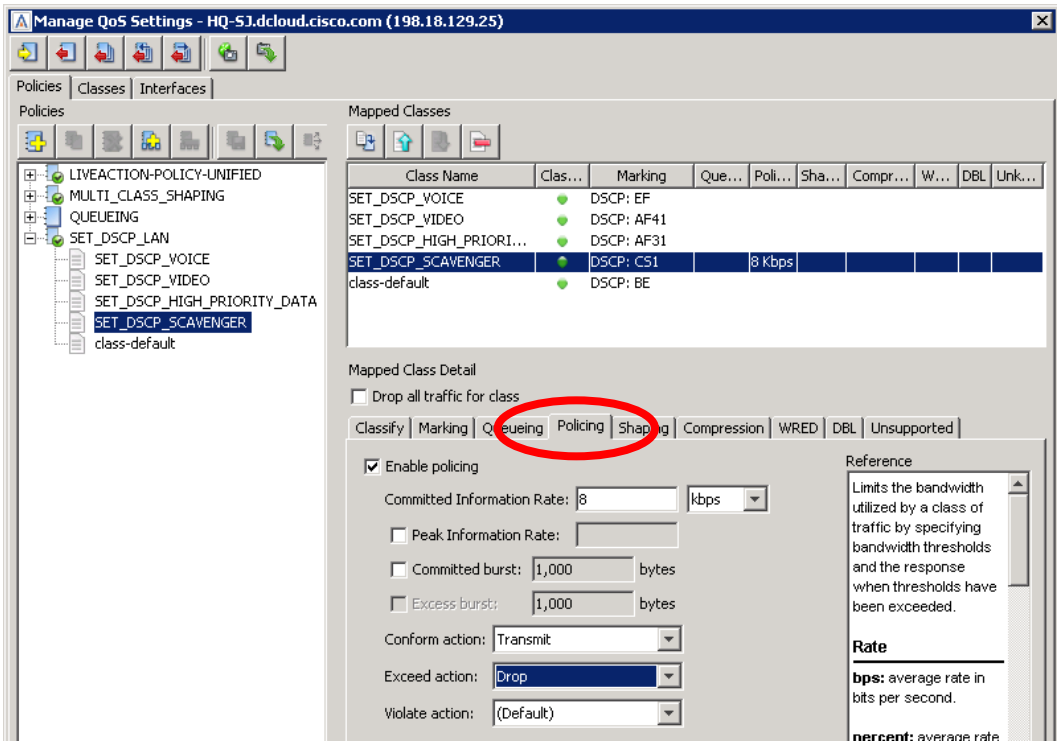

3. Update the **SET_DSCP_SCAVENGER** class with the following traffic:
    - Pandora
    - Bittorrent
    - Bittorrent-networking



When finished, the SET_DSCP_LAN policy should look like this:

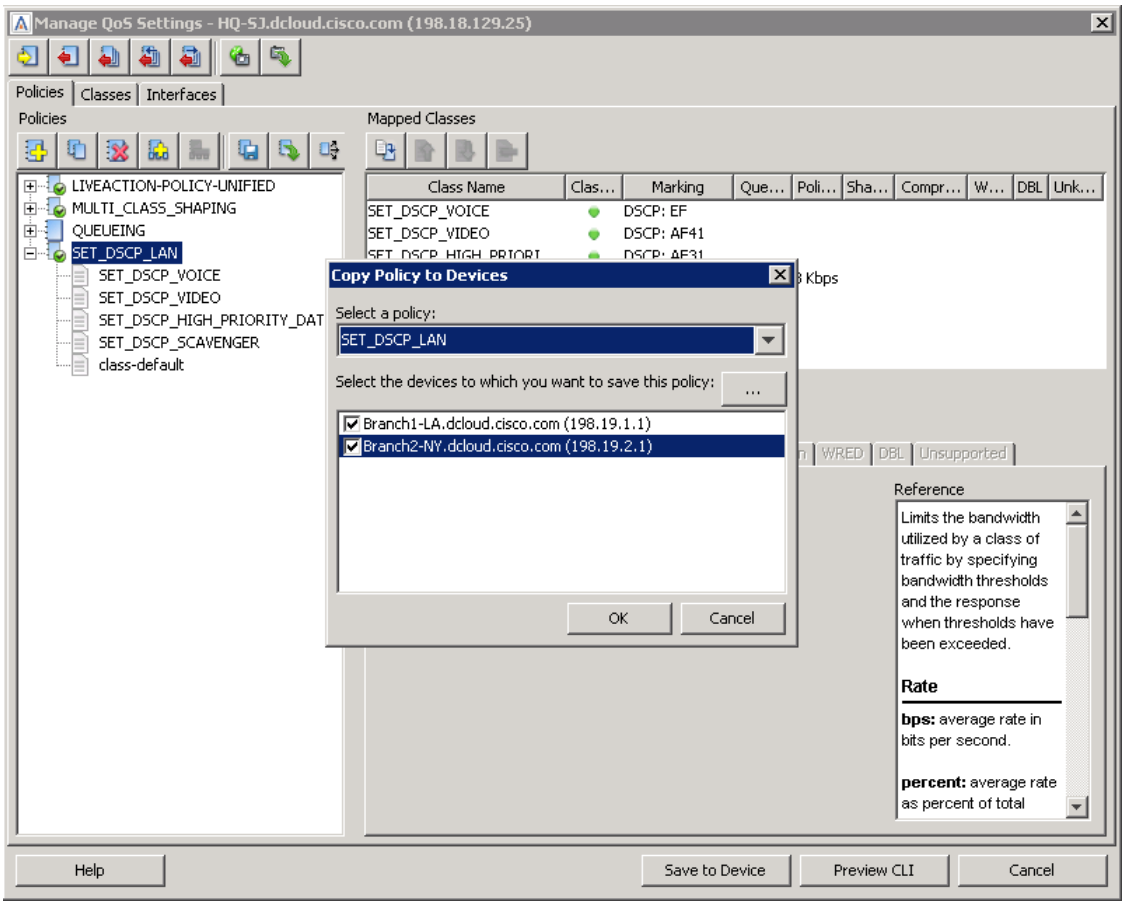



4. Select the **Policing** tab and **update** the following settings:
    - Policing Enabled
    - Committed Information Rate = 8Kbps
    - Conform Action = Transmit
    - Exceed Action = Drop

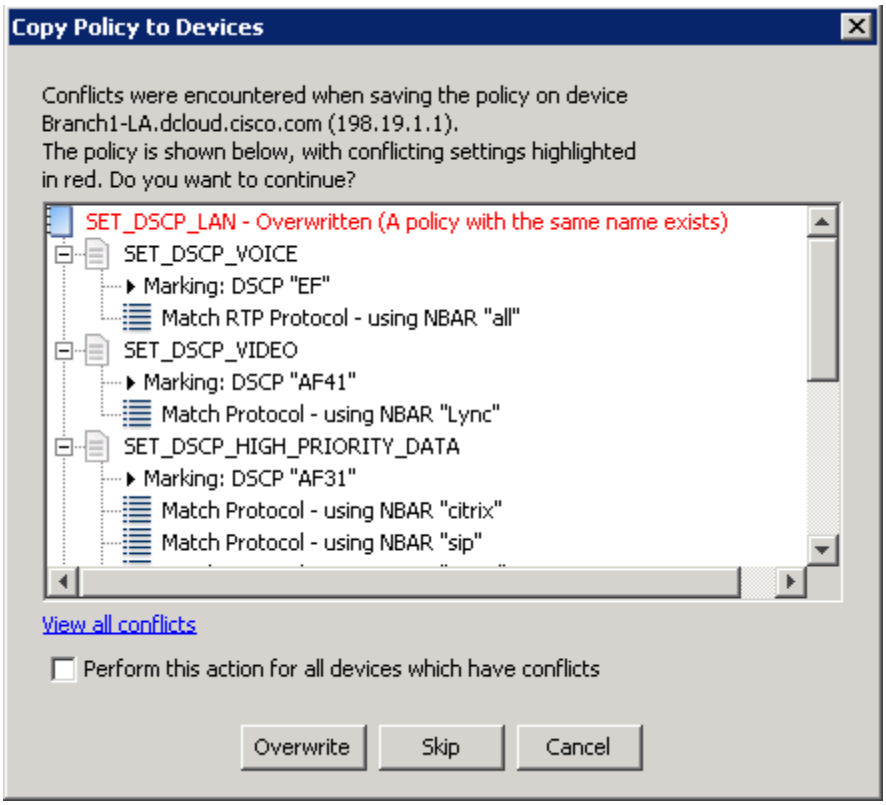



5. Select **Save to Device**.

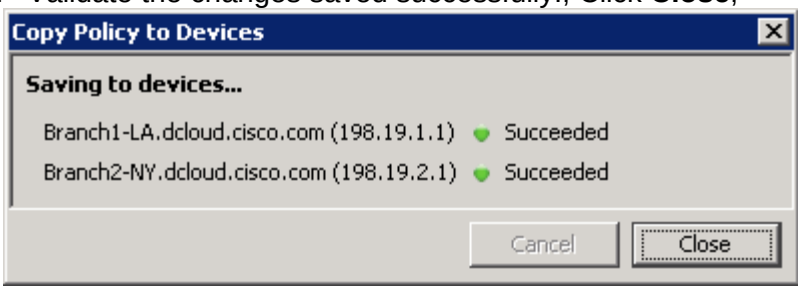
6. **Copy** the SET_DSCP_LAN policy to the **other available routers**.




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



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

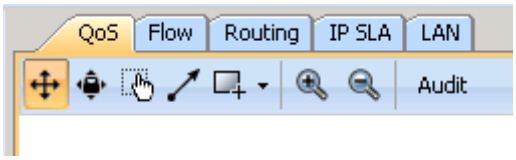


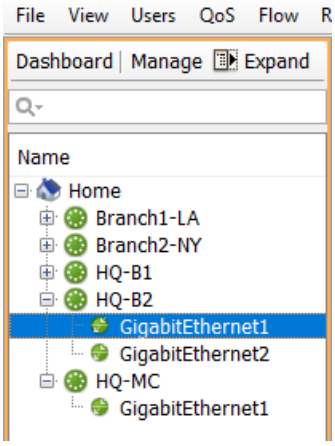

8. Close the **Manage QoS Settings** Dialog Window

# Lab 5.2: Confirm policing Settings

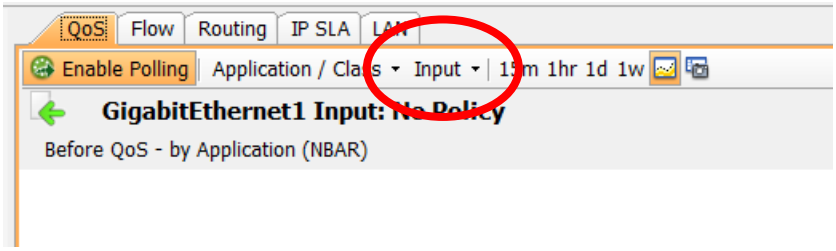
Lab Steps:

1. Select the QoS Tab.

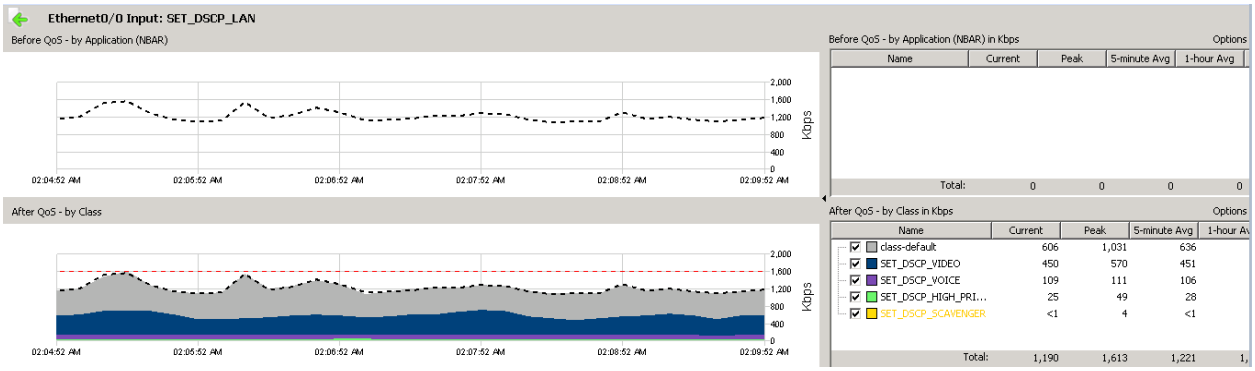



2. From the device list, select the HQ-B2 router's **LAN interface** – GigabitEthernet1
3. Update the real-time view's options to just include the **input**.




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

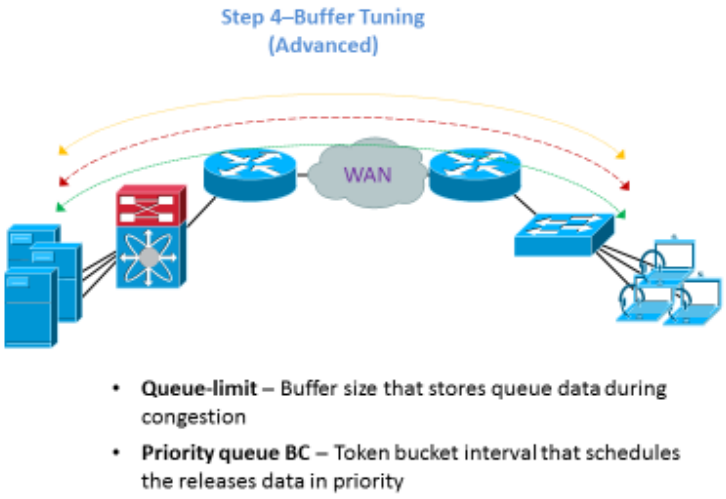


# Lab 6

## Lab 6:  Buffer tuning

# Lab 6.0: Intro – Buffer Tuning

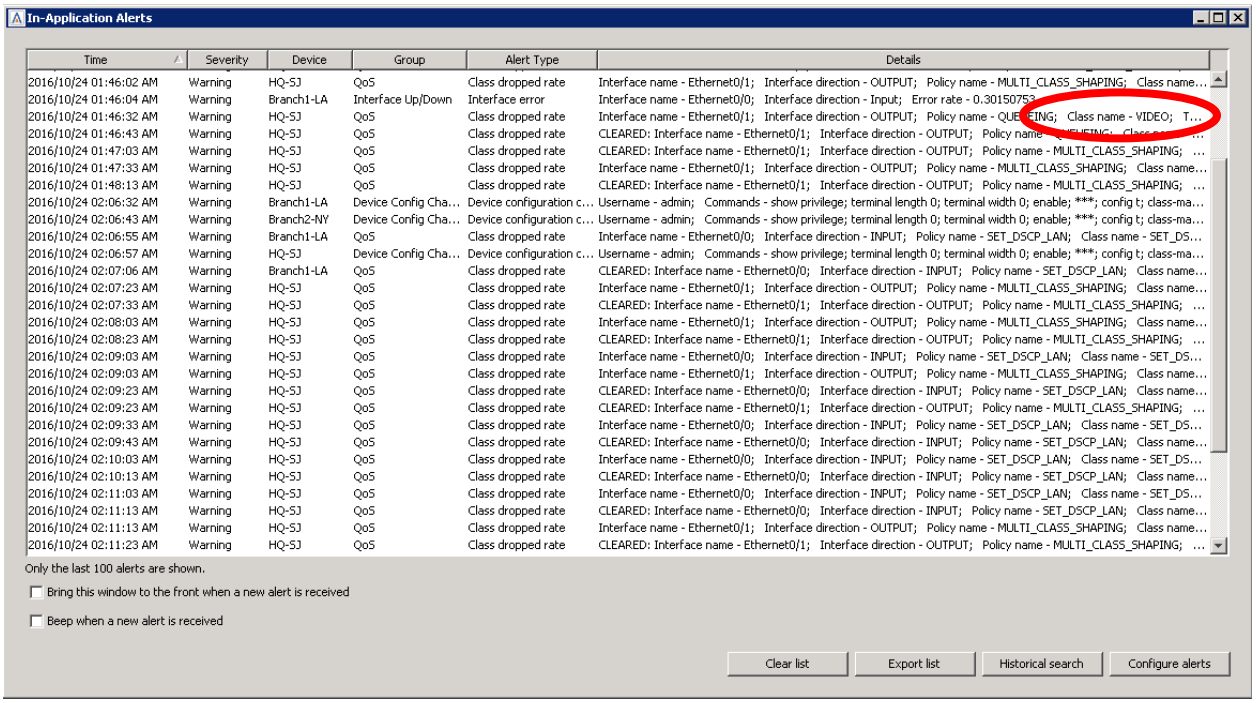
**Buffer Tuning**



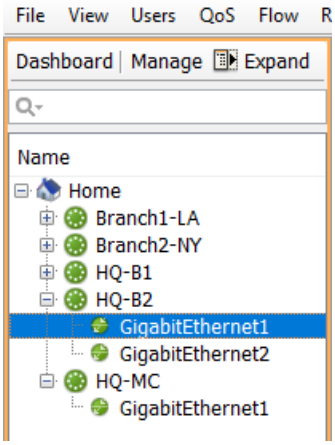

Buffer tuning is an advanced QoS topic that LiveNX can greatly assist with simplifying the implementation and validation. It should be noted that buffer tuning should usually only be implemented for important, bursty traffic classes like video, desktop replacement applications (VDI), or transactional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

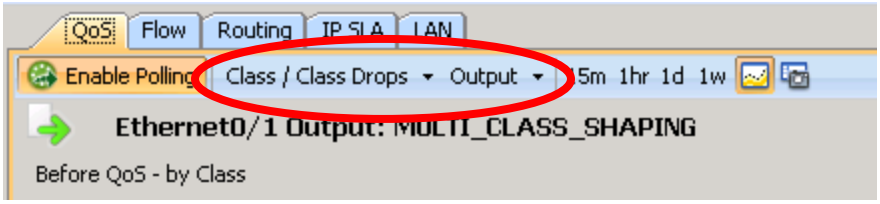
1. The first place to look for the issue is to review the in-application alerts.
   a. At the bottom left of the LiveNX window, note the Red Alert button.
   
   
   b. Double click the alert button
   c. The In-Application Alert view appears



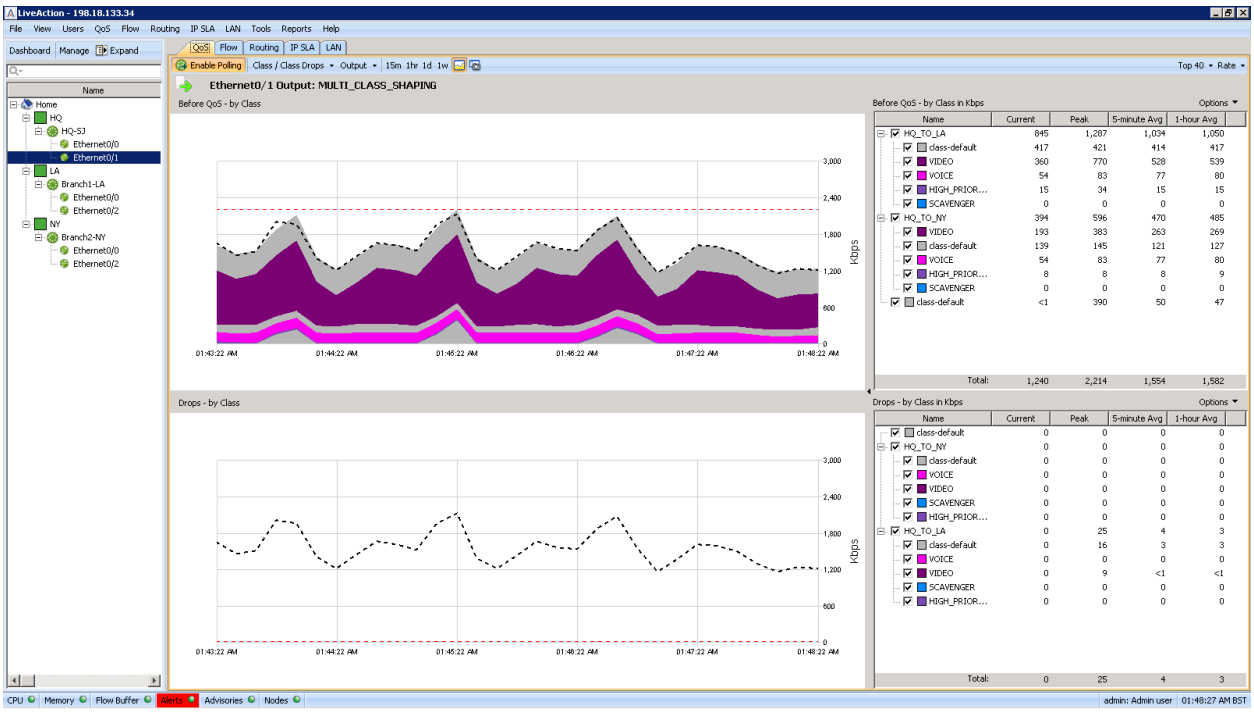

d. Are there any alerts class drop alerts from the VIDEO class?
e. If not, we will want to wait or do a Historic Search for class-dropped rate (see Appendix A.)
f. If there are any alerts for VIDEO, note the device and interface where the drop occurred. In this example, the device is HQ-SJ and the interface is GigabitEthernet1.
g. Select this interface from the device list.




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

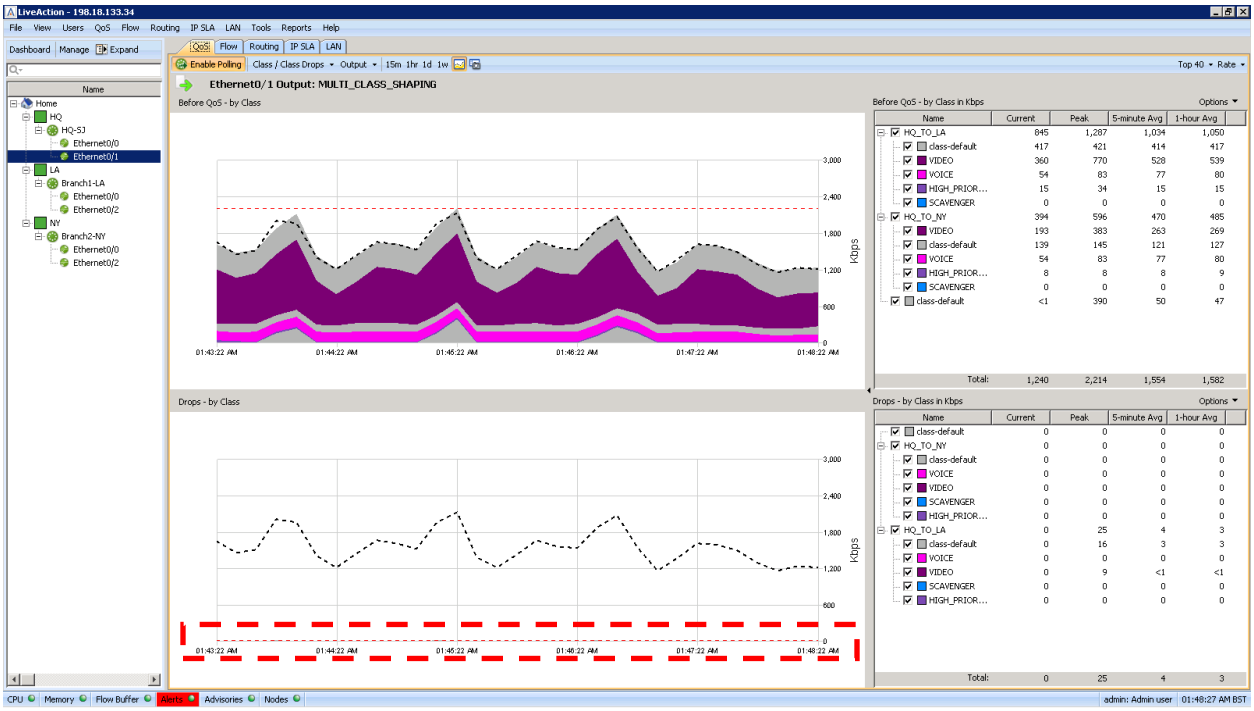



i. The bottom section of the window is a **QoS drops** report. Note if there have been any QoS drops in the VIDEO class.

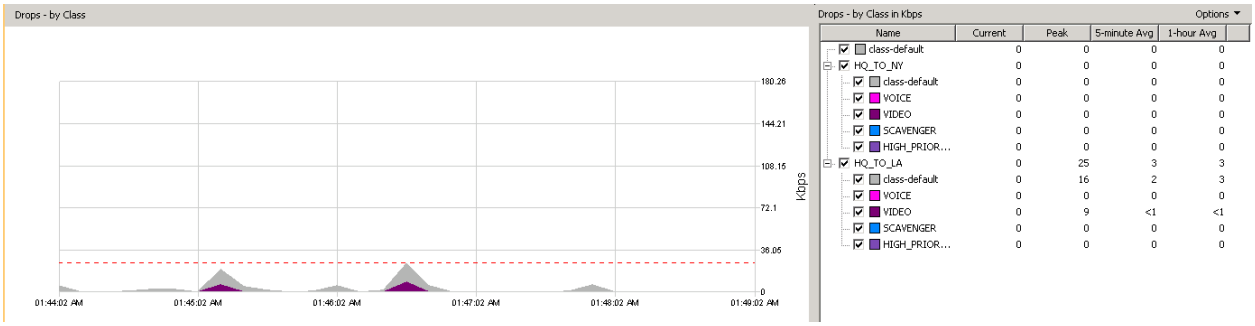



j. There have been minimal drops in the Video Class.

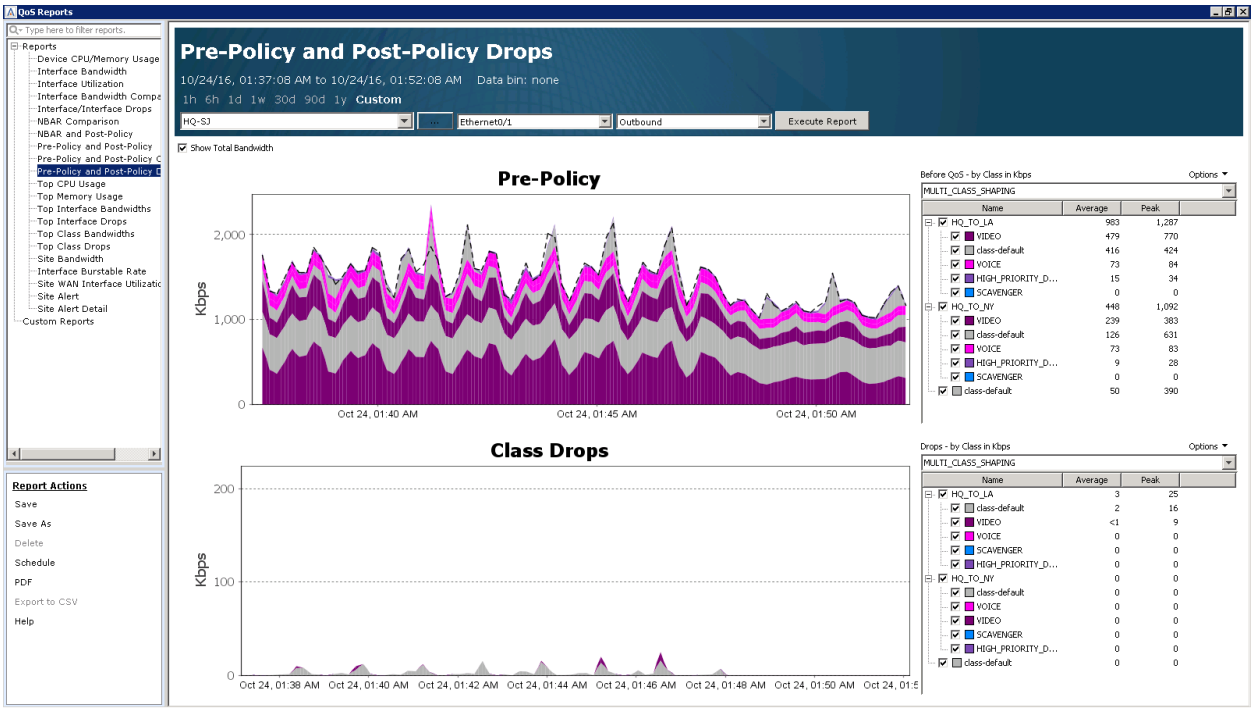
k. Click and drag your mouse on the bottom graph to make an outline of a box. When you let go the map should zoom in.




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.




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.

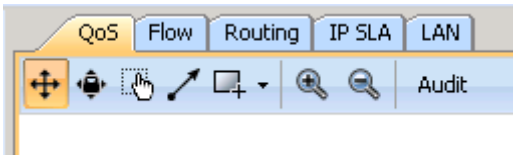



p. Remember we configured the VIDEO queue for each site to 800Kbps each.
q. The Pre-Policy graph above shows 776 Kbps peak VIDEO traffic on the HQ_TO_LA child policy and 389 Kbps to the HQ_TO_NY child policy.
r. Neither of these are above the provisioned 800K. We need to implement some buffer tuning.

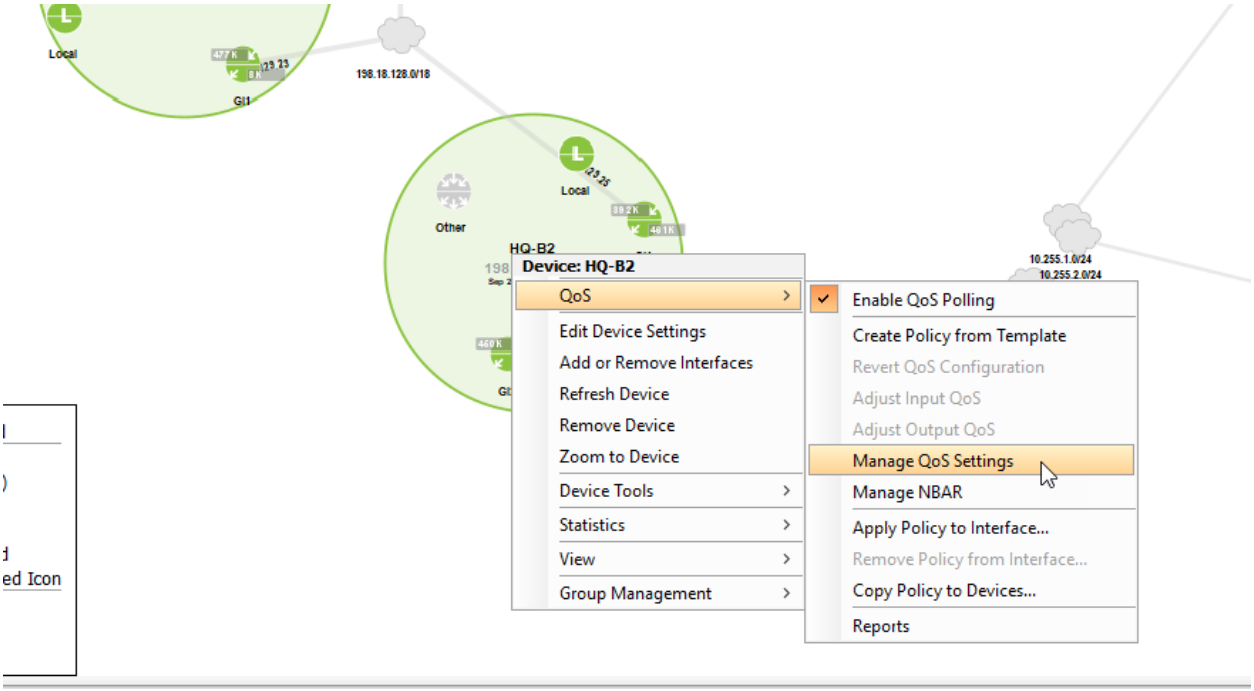
# Lab 6.1: Implementing Tuning

Lab Steps:

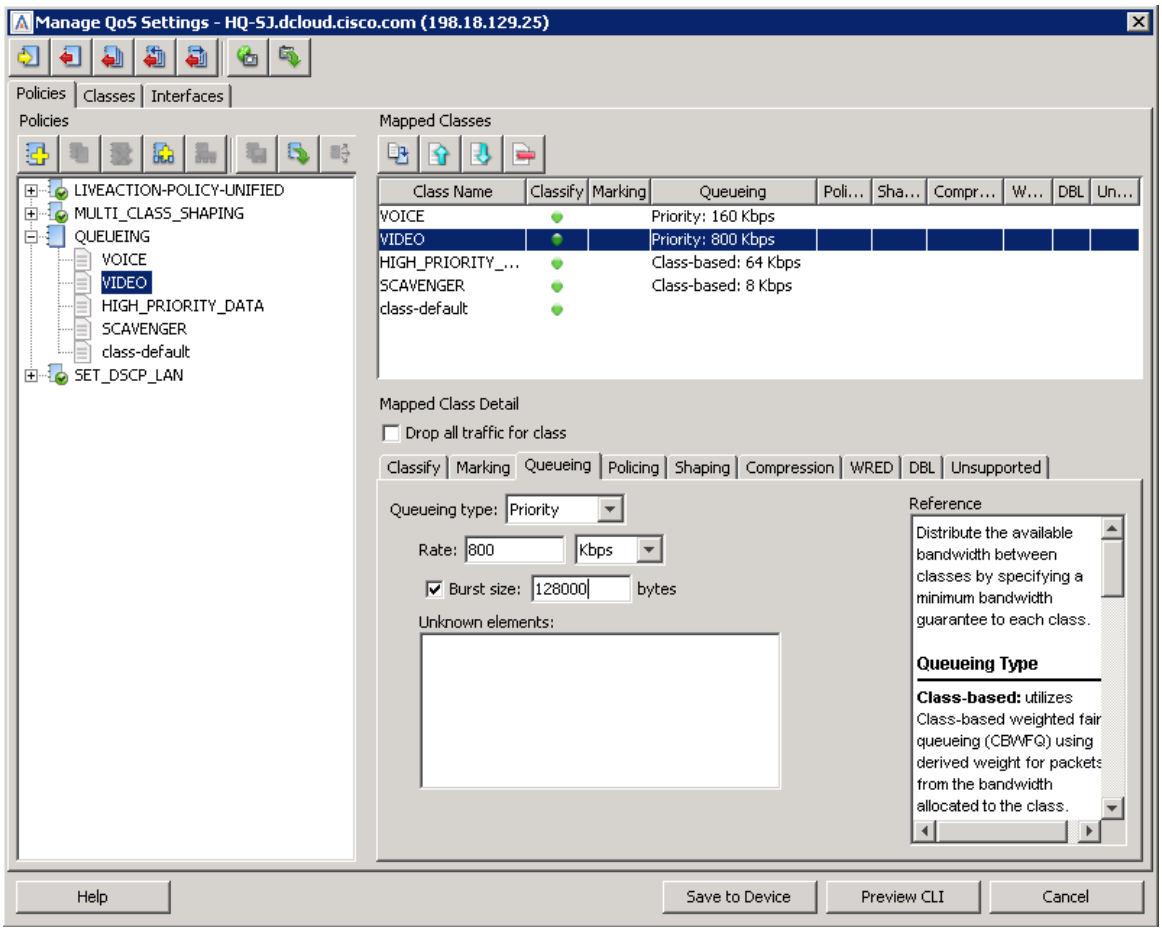
1. Select the **QoS** Tab




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

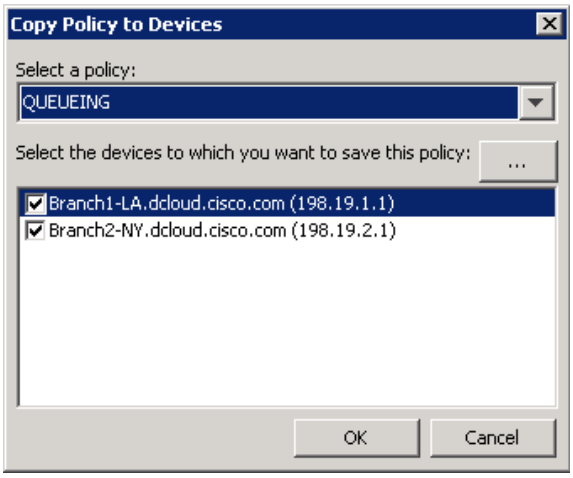


3. **Expand** the QUEUEING Policy
4. **Select** the VIDEO class.
5. **Select** the Queueing tab
6. Tick the **Burst option** and set it to **128000**.

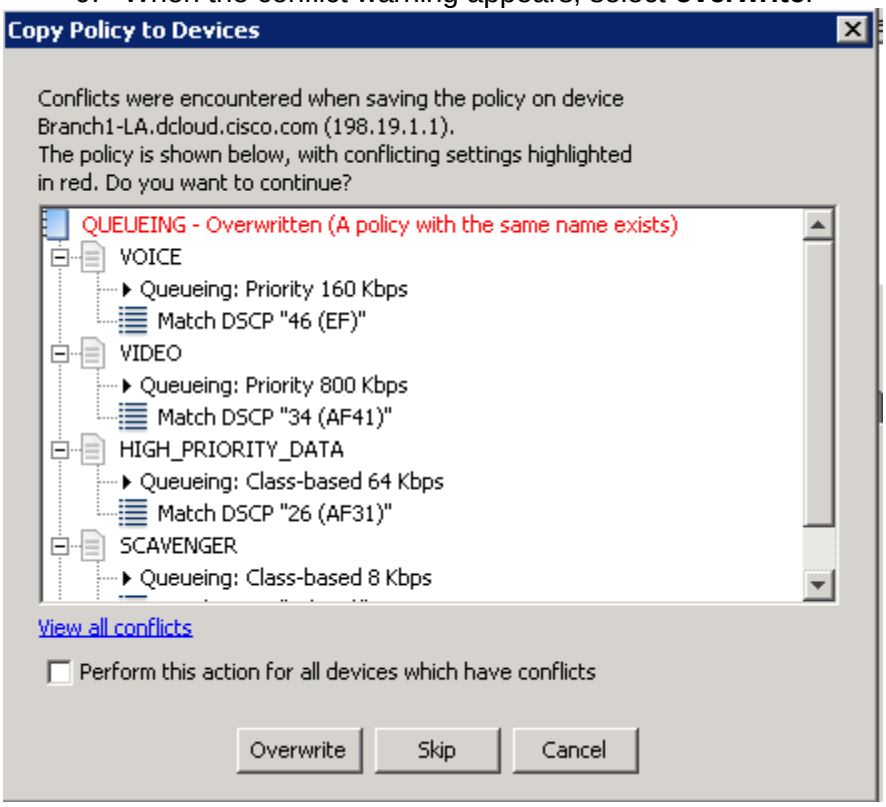



To understand this value, please see the **TelePresence Network Systems 2.0 Design Guide** from www.cisco.com.

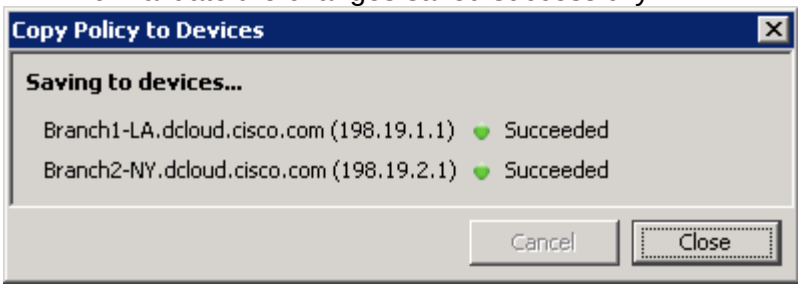
7. Select the **Save to Device** button.
8. Copy the QUEUEING policy to the **other devices via Copy Policy to Devices** icon.



9. When the conflict warning appears, select **overwrite**.




10. Validate the changes saved successfully.




11. Close the **Manage QoS Settings** Dialog window.

# Lab 7

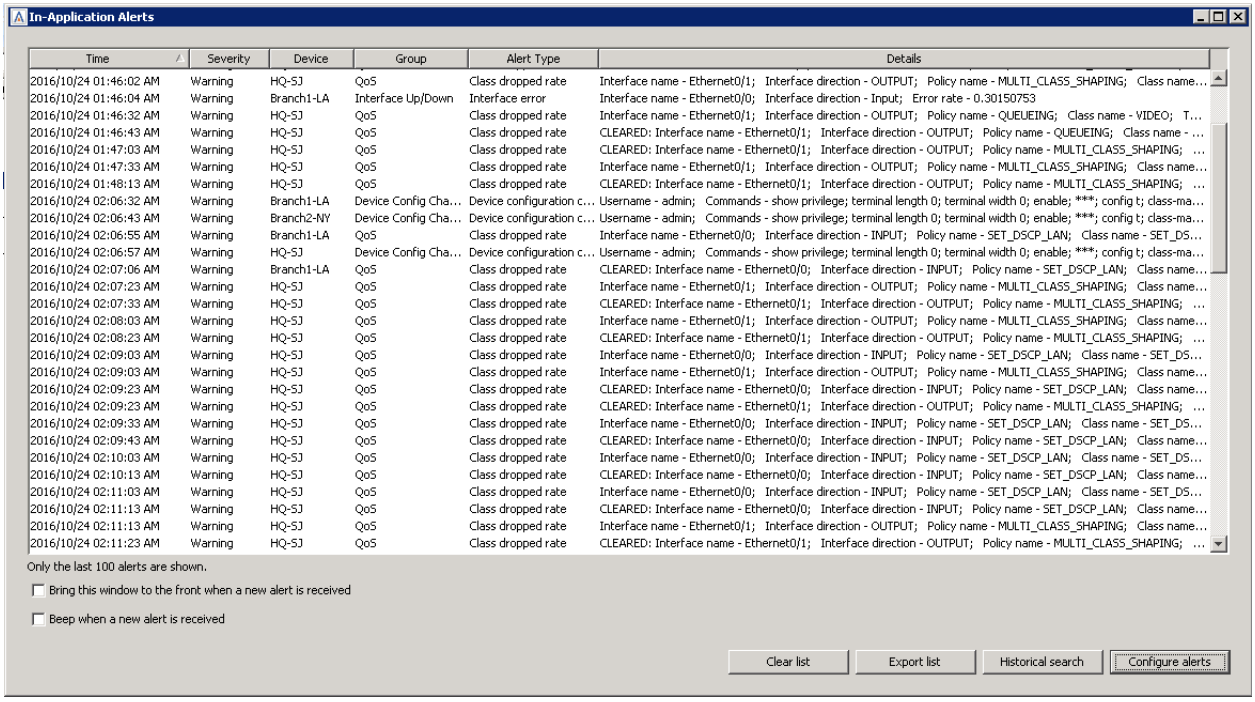
Lab 7:  QoS Alerts

# 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:

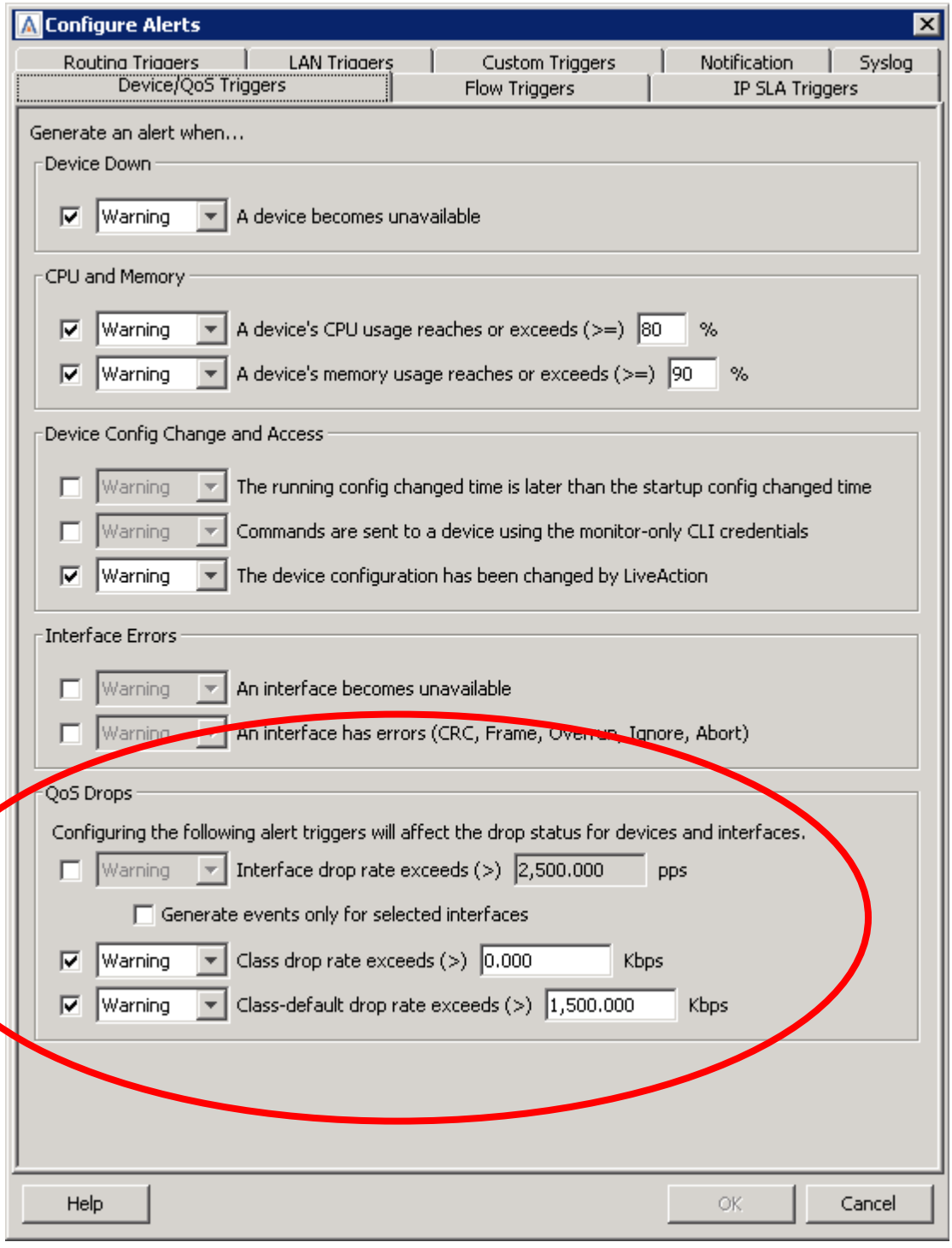



The following Lab directs you to create an Alert when QoS problems are detected.

Lab Steps:

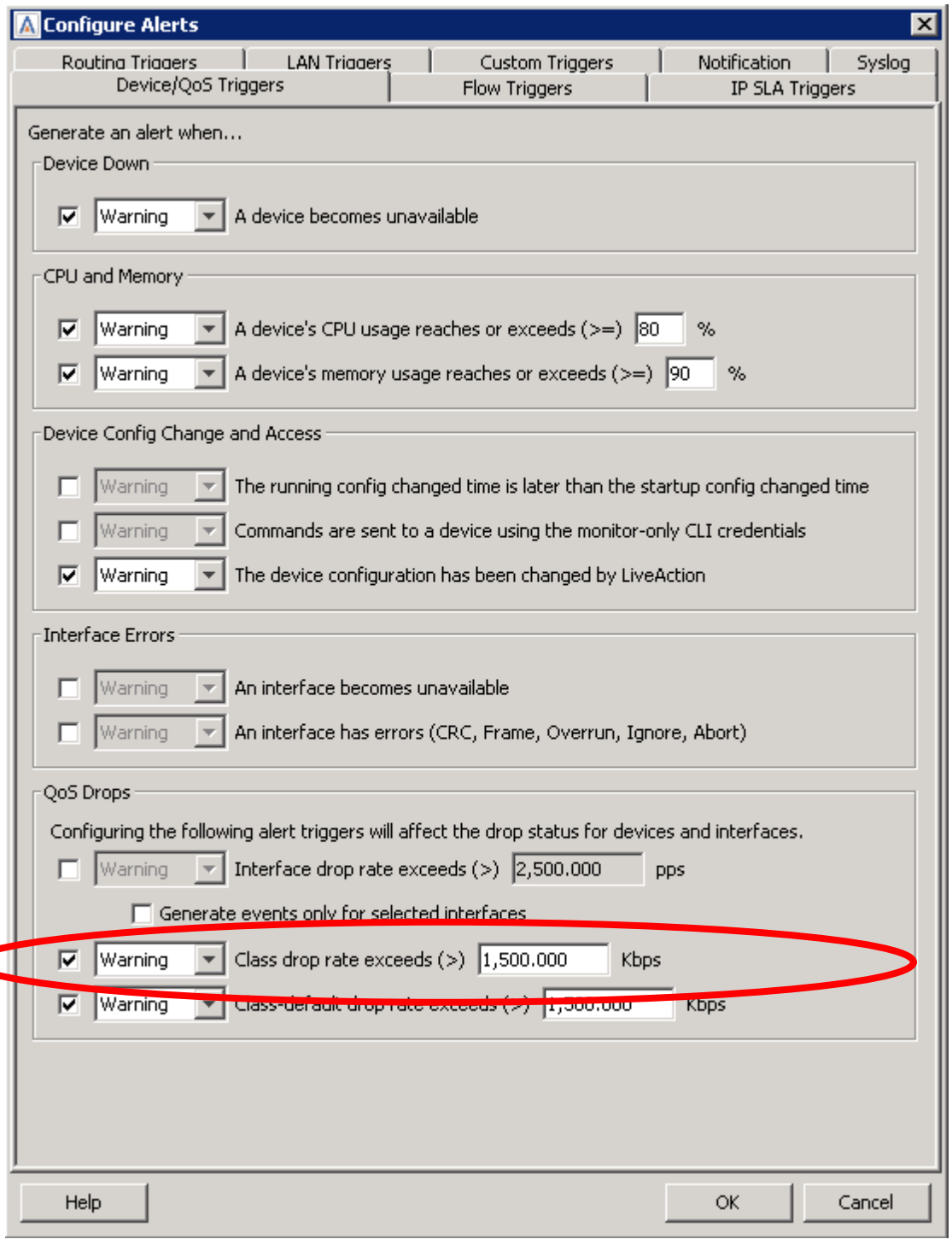
1. **Tools > Configure Alerts**

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



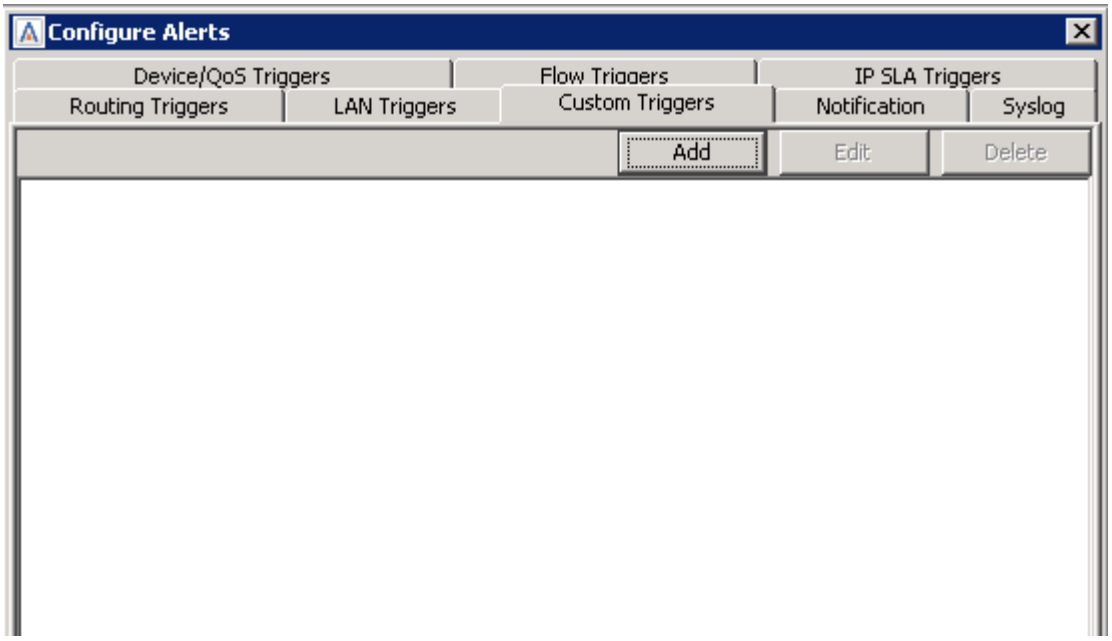

**Note: If a network uses policers, it is often best to tune the global Class drop rate exceeds setting.**

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.

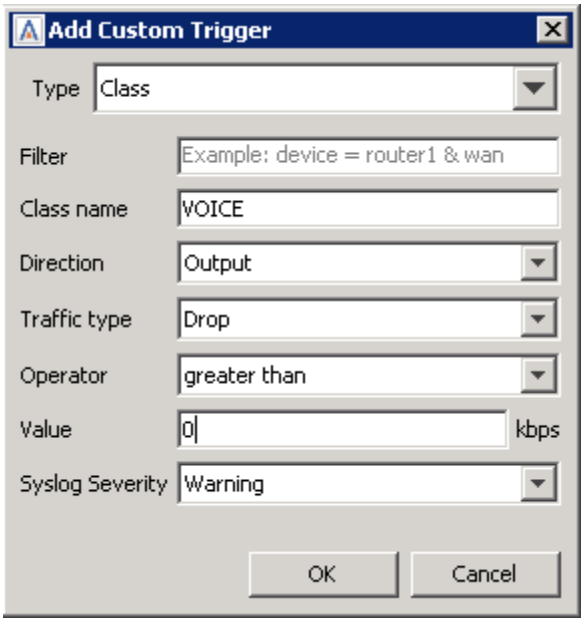


To modify this condition and ensure VIOCE and VIDEO classes still alert if there are any drops:

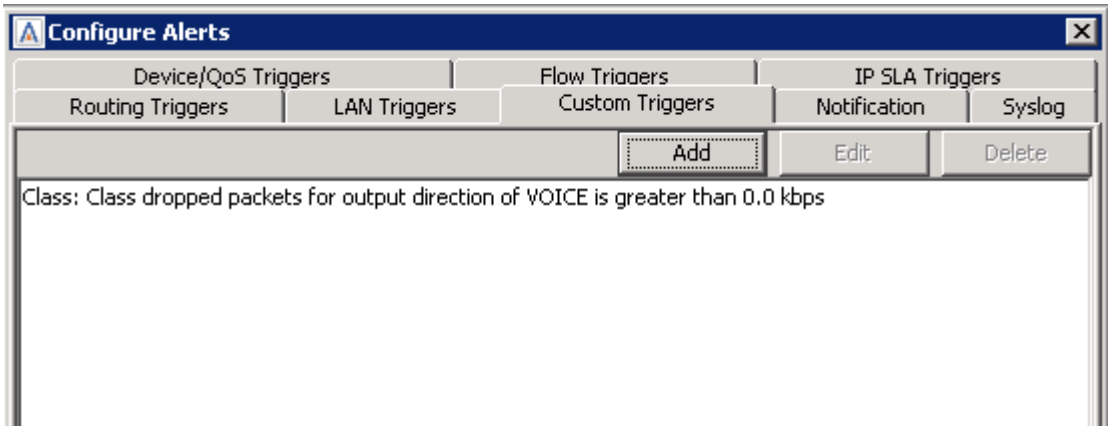
2. Select the **Custom Triggers** tab.
3. Click **Add**.




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

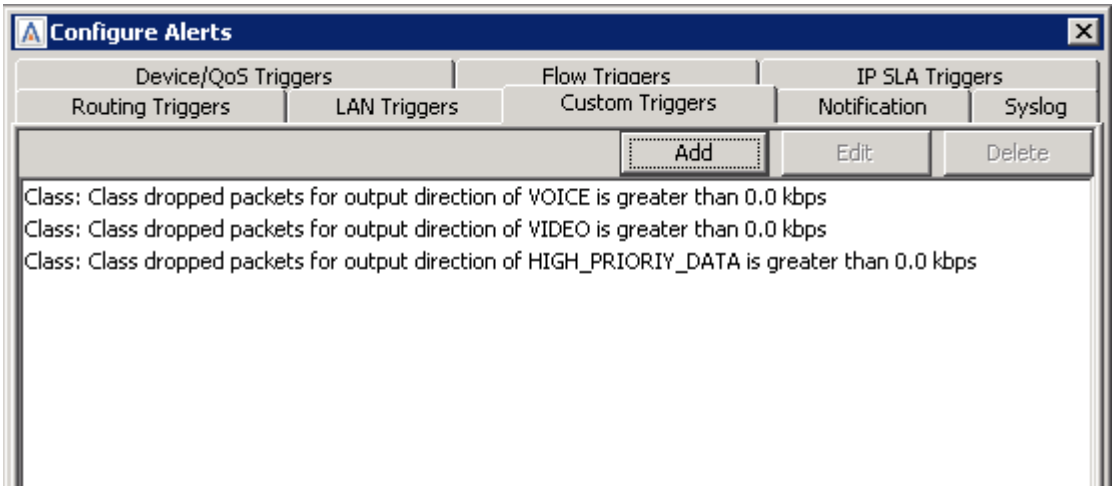



5. Click OK.

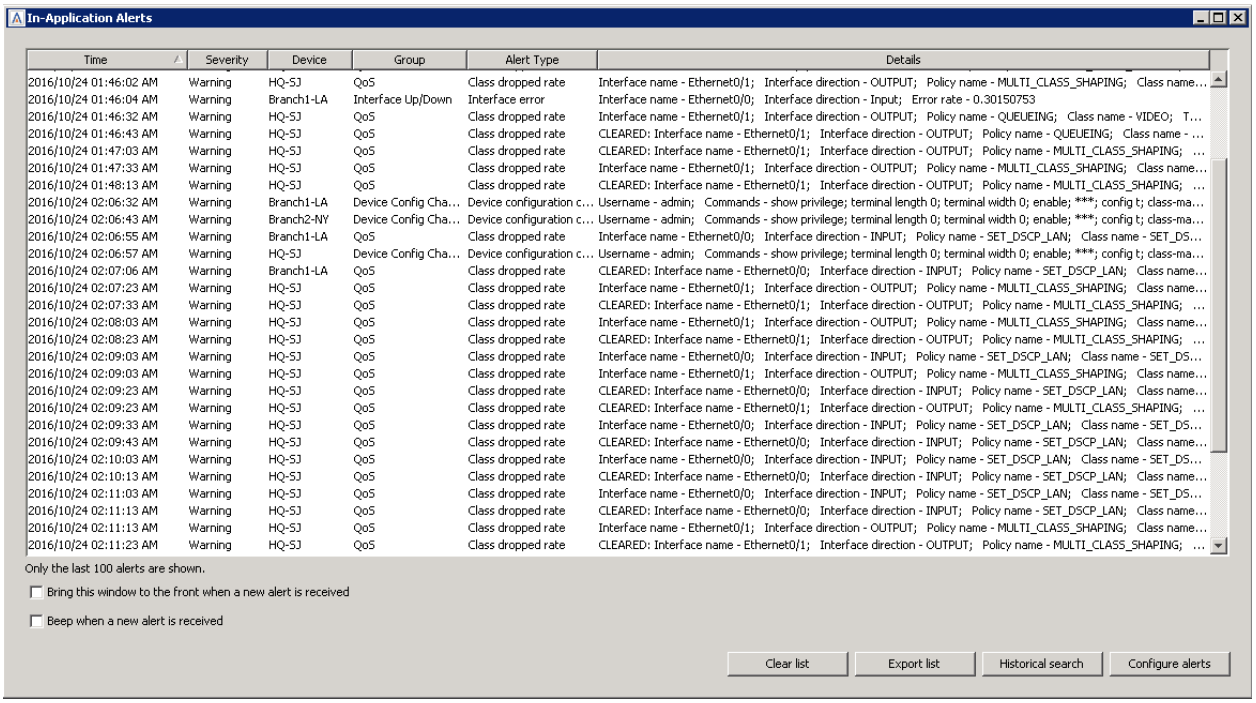



6. Repeat these steps and create a Custom trigger for the VIDEO and HIGH_PRIORITY_DATA classes.

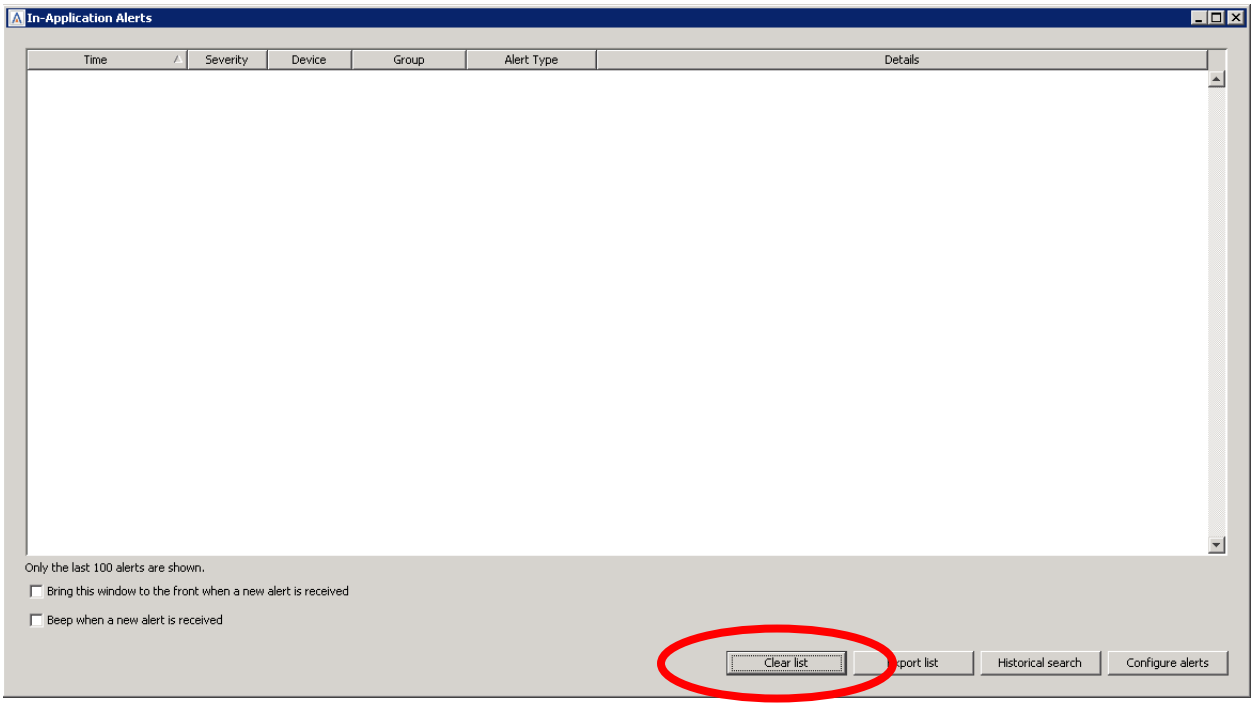
This will ensure these classes always alert when drops occur.




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.




8. Click the **Clear List** Button




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

# Lab A

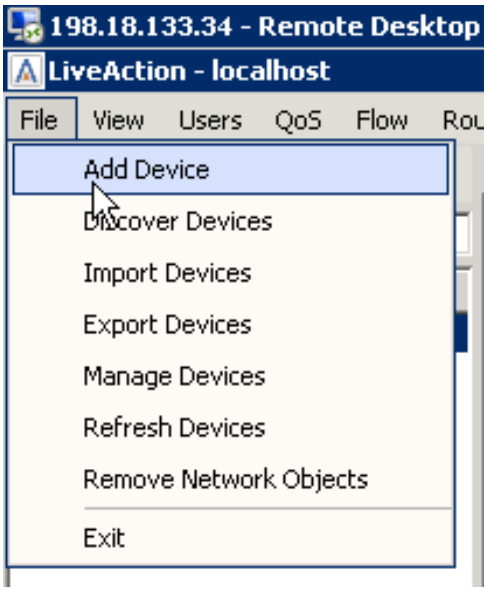
## Lab A:  Appendix

# Lab A.1:  Add Device

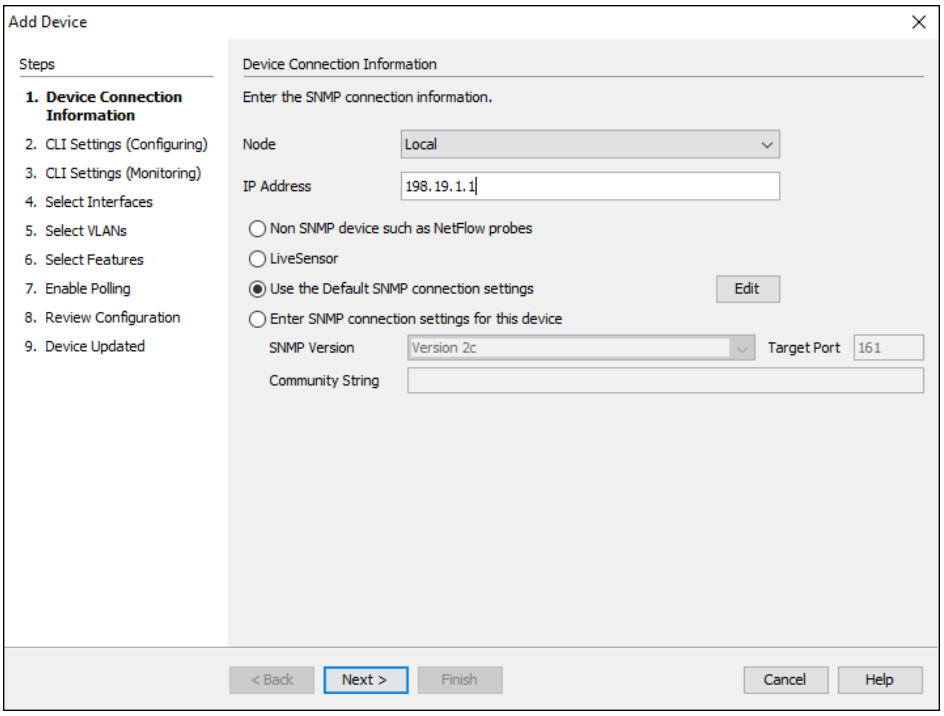
Adding devices into LiveAction and managing them properly is very important to the overall usability of LiveAction itself.

Lab Steps:

9. Select File, **Add Device**

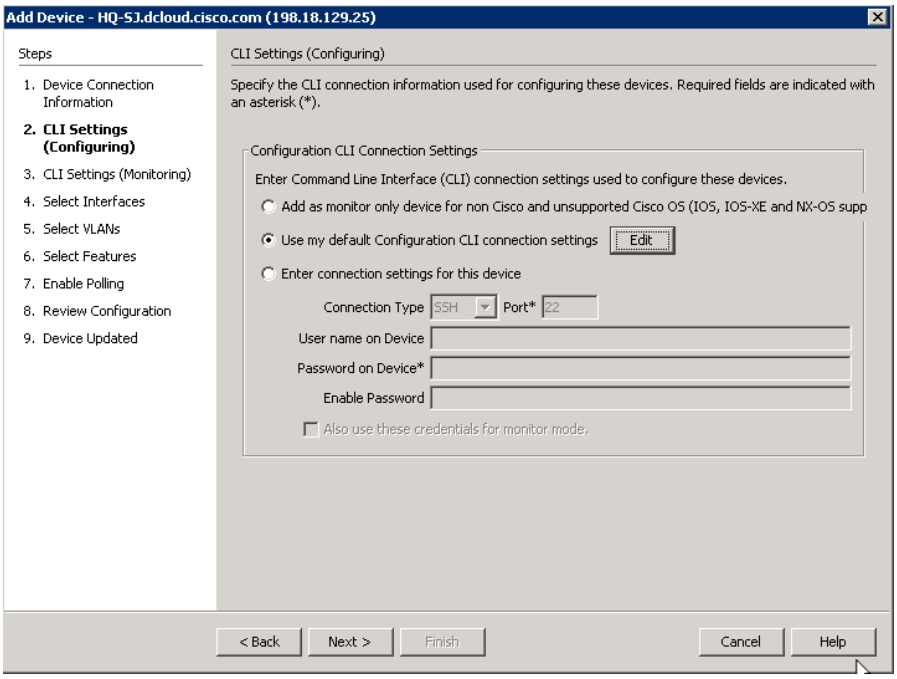



10. Enter 198.19.1.1 in the IP Address field.
11. Select “Use the Default SNMP connection settings”.

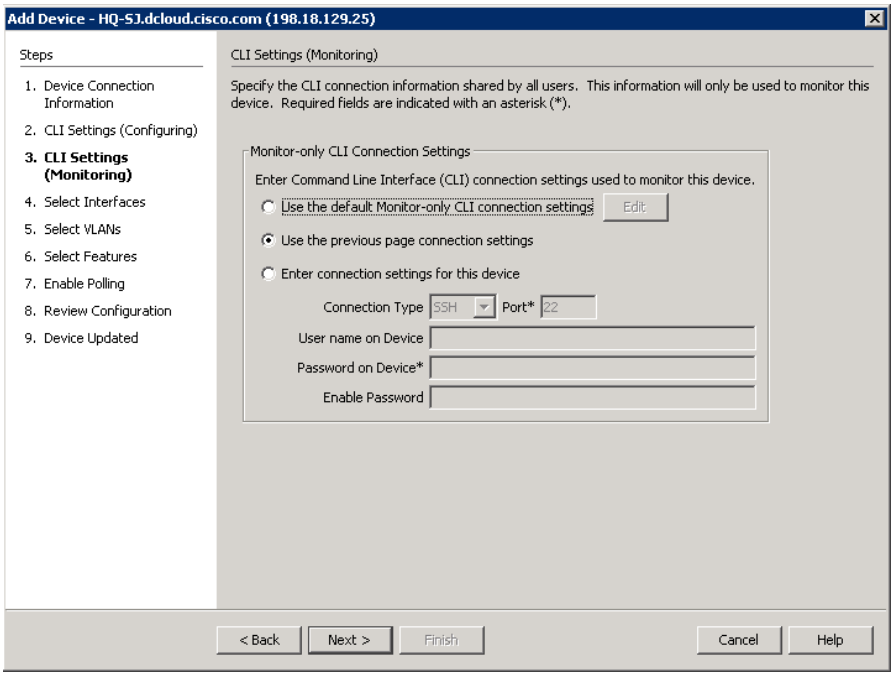



12. Click Next.

13. Select “Use my default Configuration CLI connection settings”.




14. Click Next.

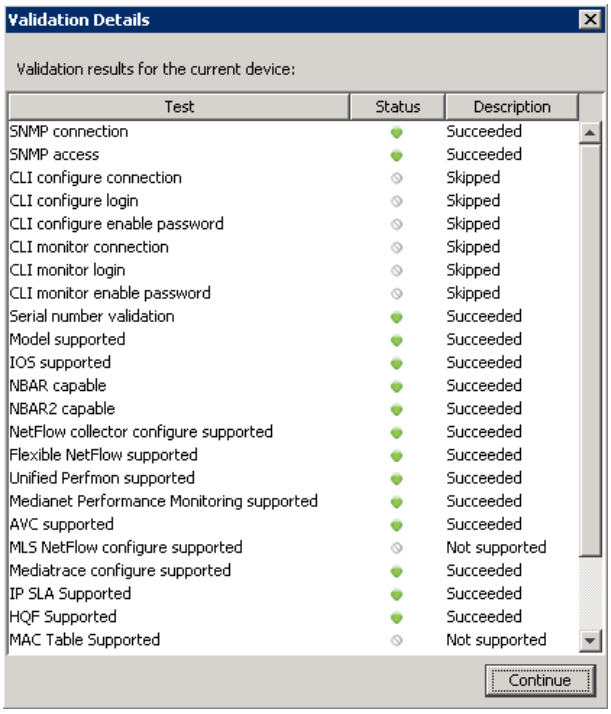



15. Select “Use the previous page connection settings”.

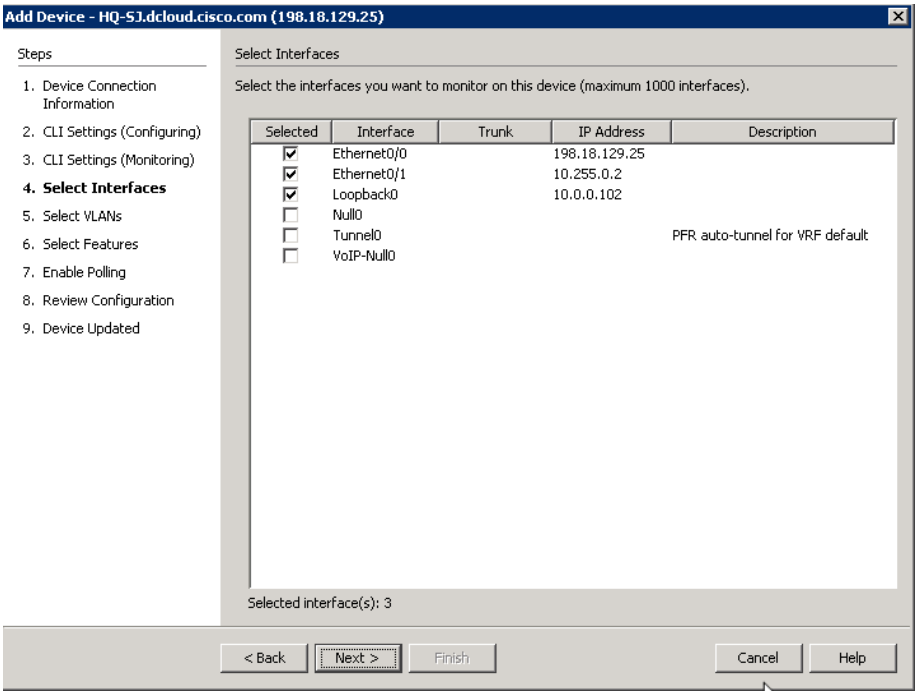
16. Click Next.

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

17. Click Continue.

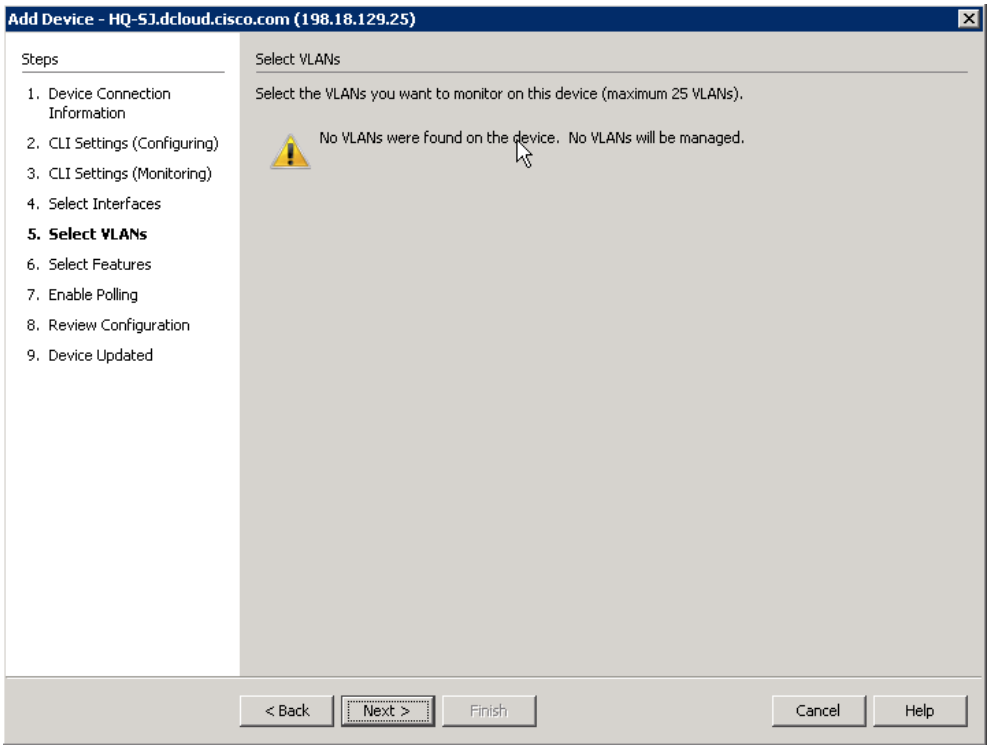



On the select interfaces window you may notice 3 interfaces are already selected. LiveAction automatically selects the interfaces based on the highest bit rate.



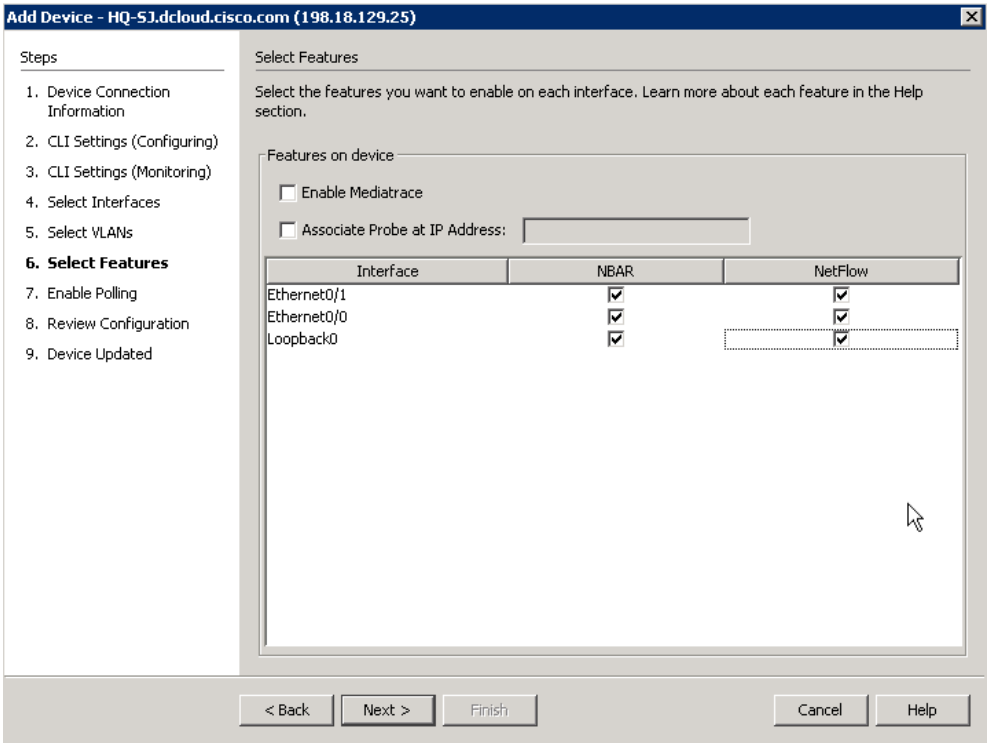

18. Click Next.

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




19. Click Next.

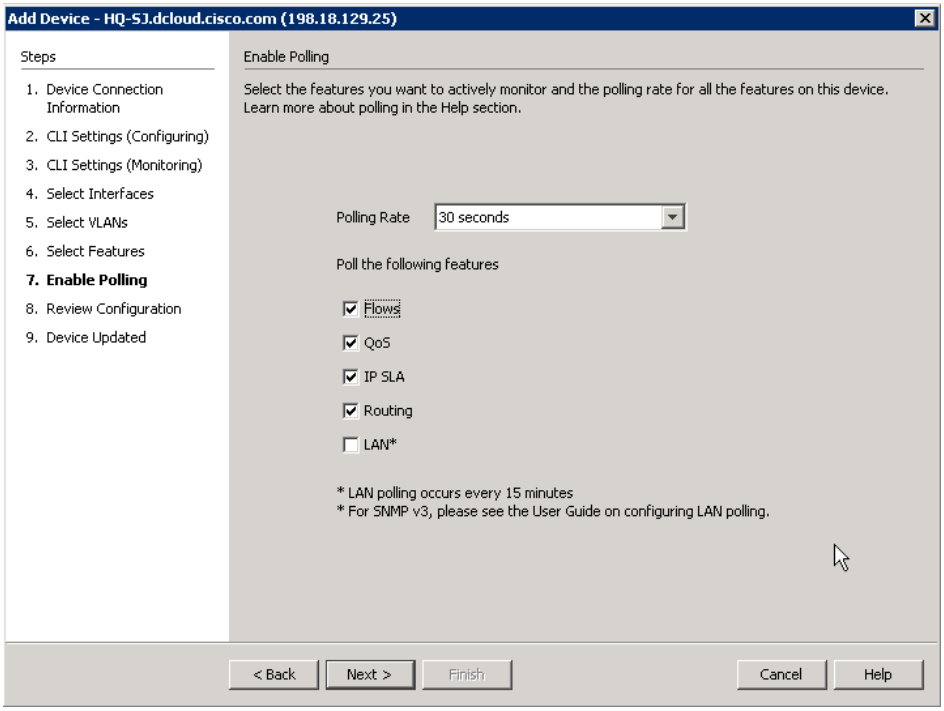
The **Select Features** dialog allows you to turn-on specific Cisco technologies using the templates included in LiveNX. This dialog displays the current IOS configuration of the device you are currently viewing. Leave this screen **AS-IS**.



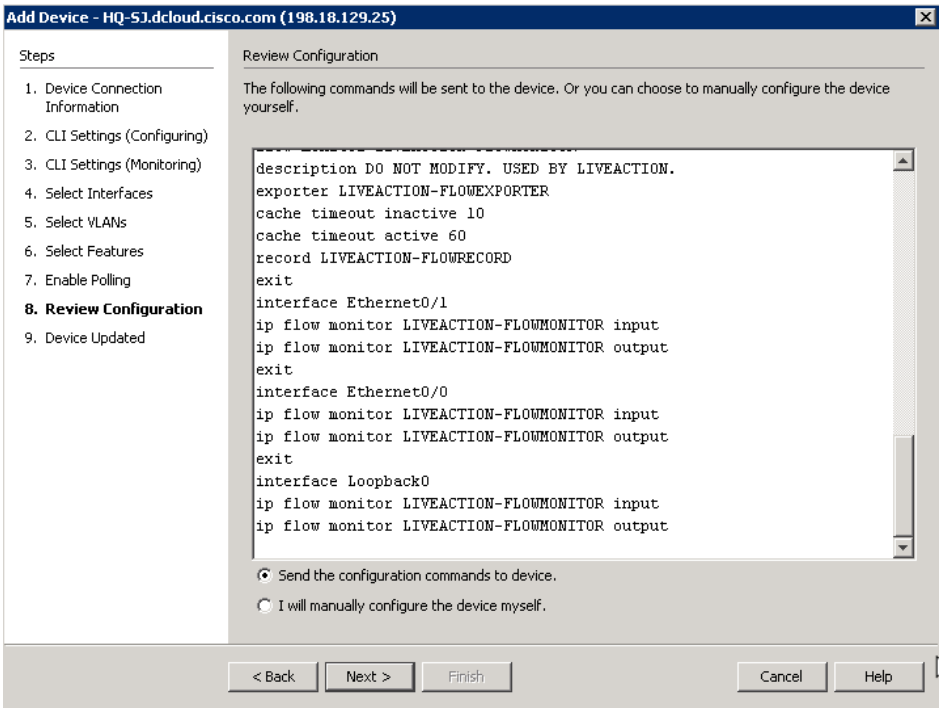

20. Click Next.

21. Change the polling rate to 30 seconds.

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



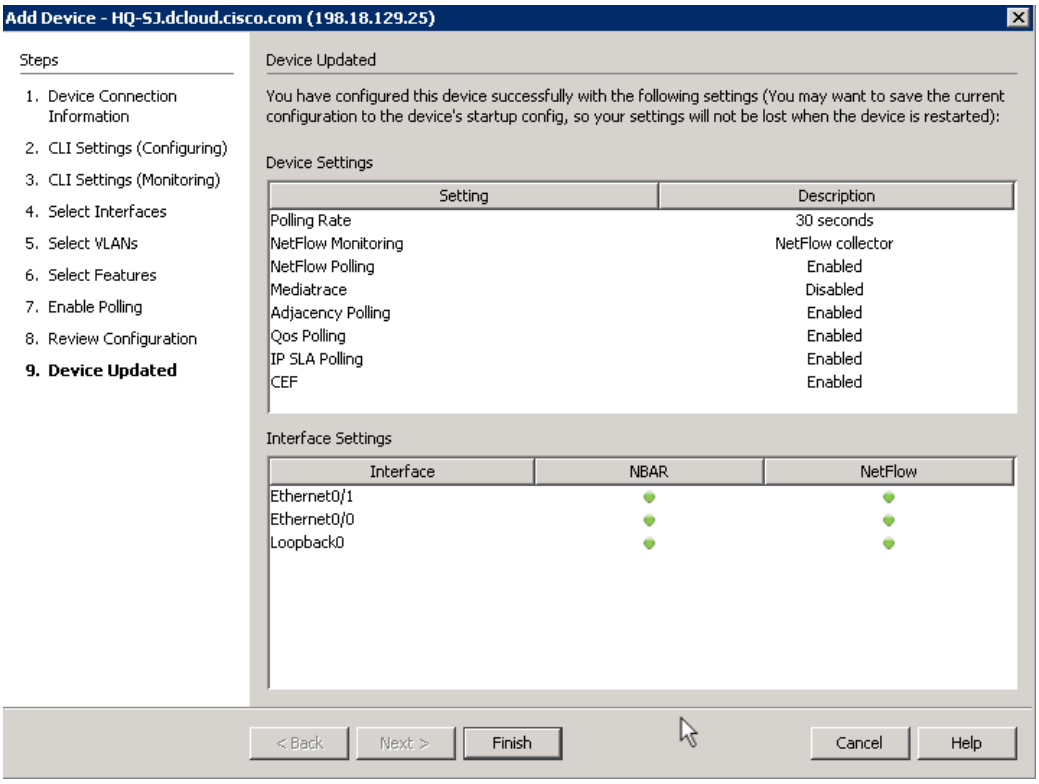

**Note: Any changes to the Select Features dialog will generate a CLI push to update the current configuration. Before sending the NetFlow configurations to the device, you can verify the configurations that LiveAction created.**




23. Select “Send the configuration…” radio button, if available.

24. Click Next.

25. Click Finish.



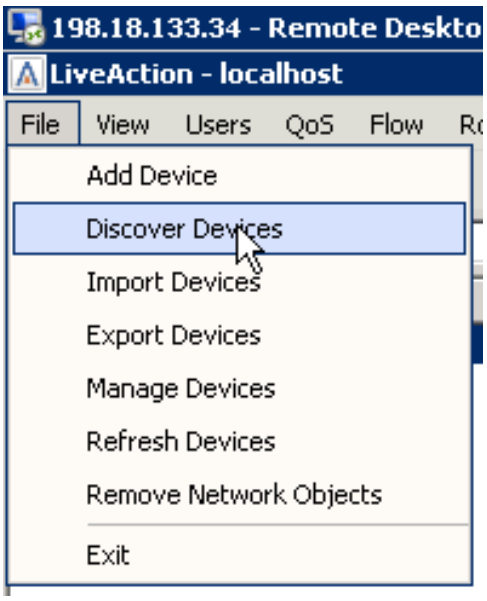

The device will be added to the Topology Pane in LiveNX. Note that LiveNX will not automatically position a new device with reference to any existing devices… you may need to scroll-about in the Topology Pane to locate your new device(s).

# Lab A.2: Client Device Discovery

As we discovered in a prior Lab, the LiveNX Server in your topology has had device(s) pre-installed. In the following Lab you may add additional devices to your Topology, configure those devices to send flow and SNMP data to the LiveNX Server, and discover what data your LiveNX solution is gathering.

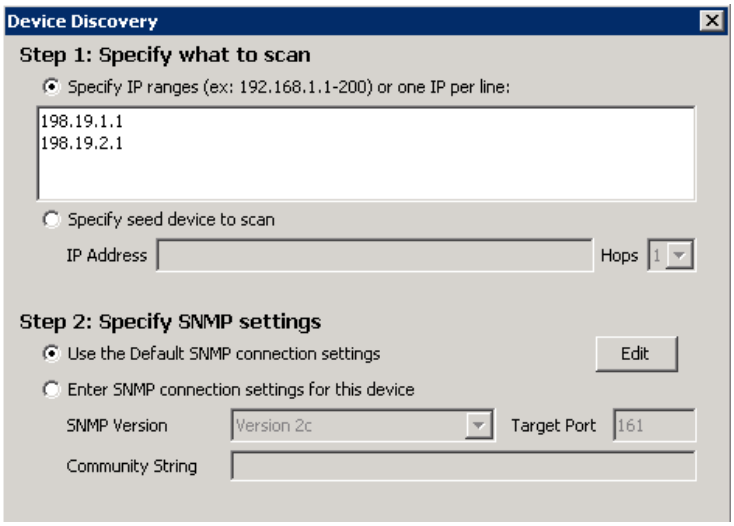
Lab Steps:
Adding several devices at once is as easy as adding a single device at a time. To do this:

26. Select File and Discover Devices.




27. Specify the following IP addresses:
    198.19.1.1
    198.19.2.1

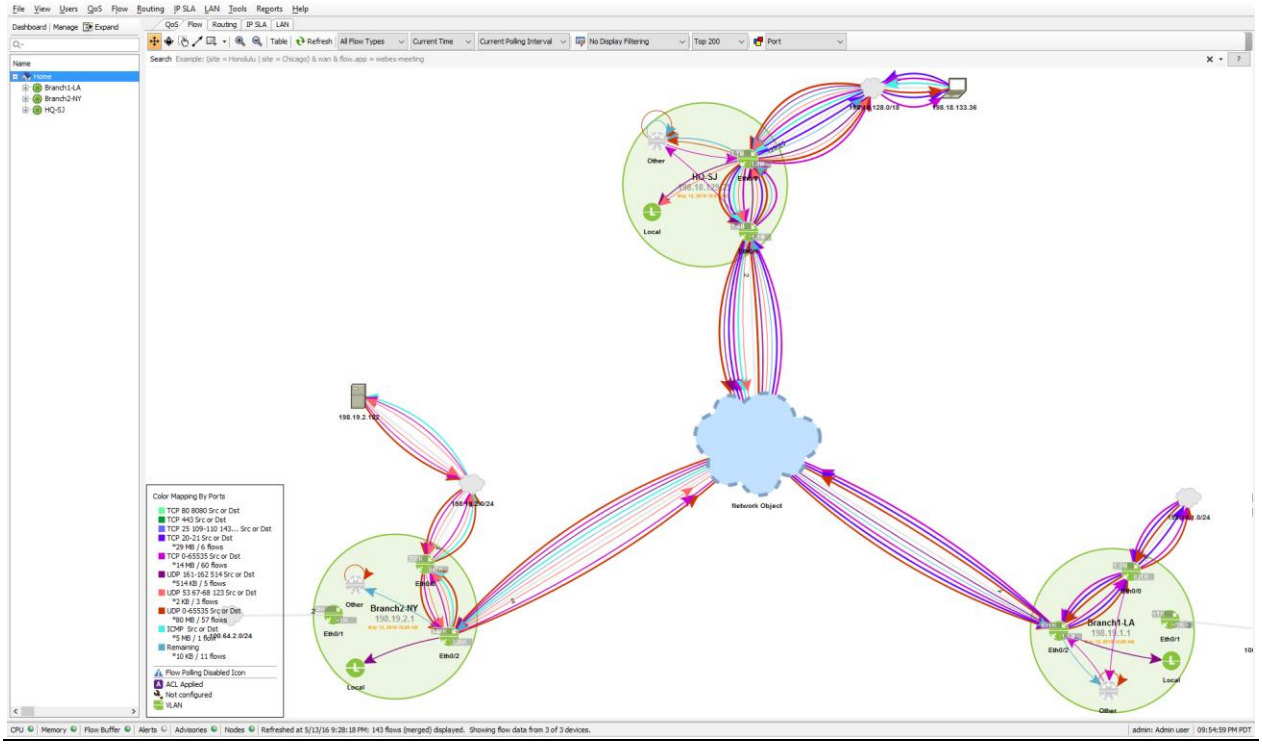
28. **Select** Use the default SNMP connection settings.

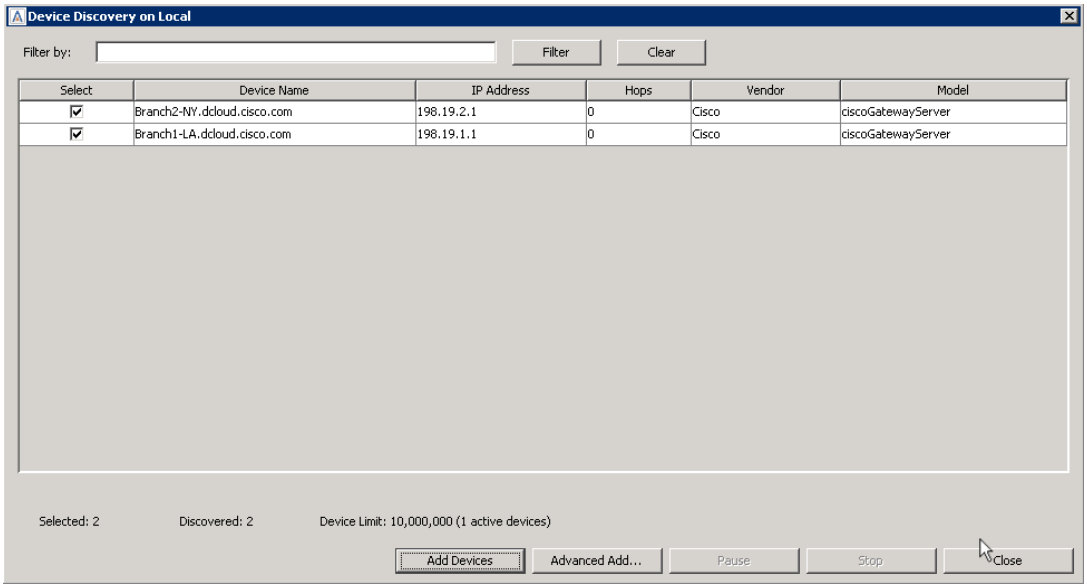


**Note: In the Lab infrastructure we are utilizing the Local LiveNX Node included with the Server installation. If you require access to a Remote Node to access the subnets or addressing in "Step 1: Specify what to scan" you would use the Specify node drop-down at the bottom of this dialog box.**

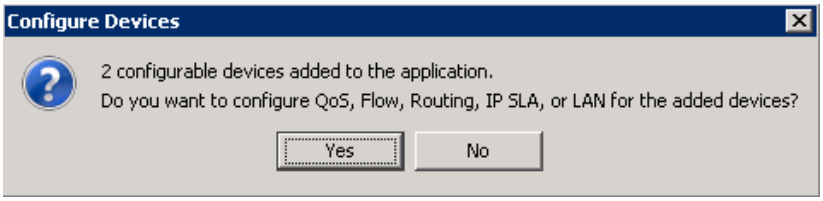

29. Click OK.
30. Verify that both devices were found, and then select Add Devices.

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



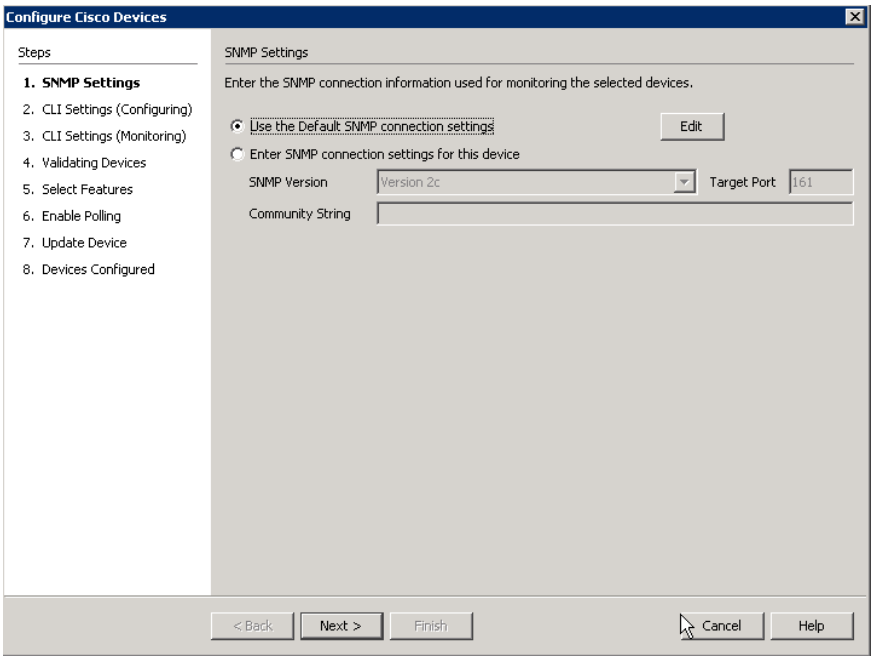



31. Select Yes on the configure devices dialog.



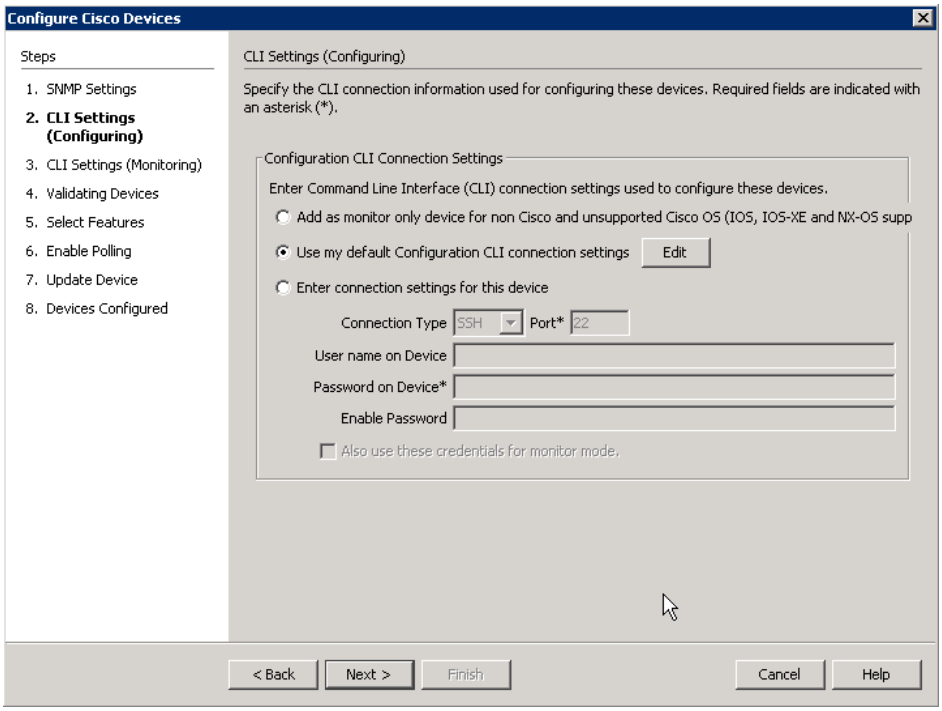
32. Use the default SNMP connection settings and then select Next

**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.**

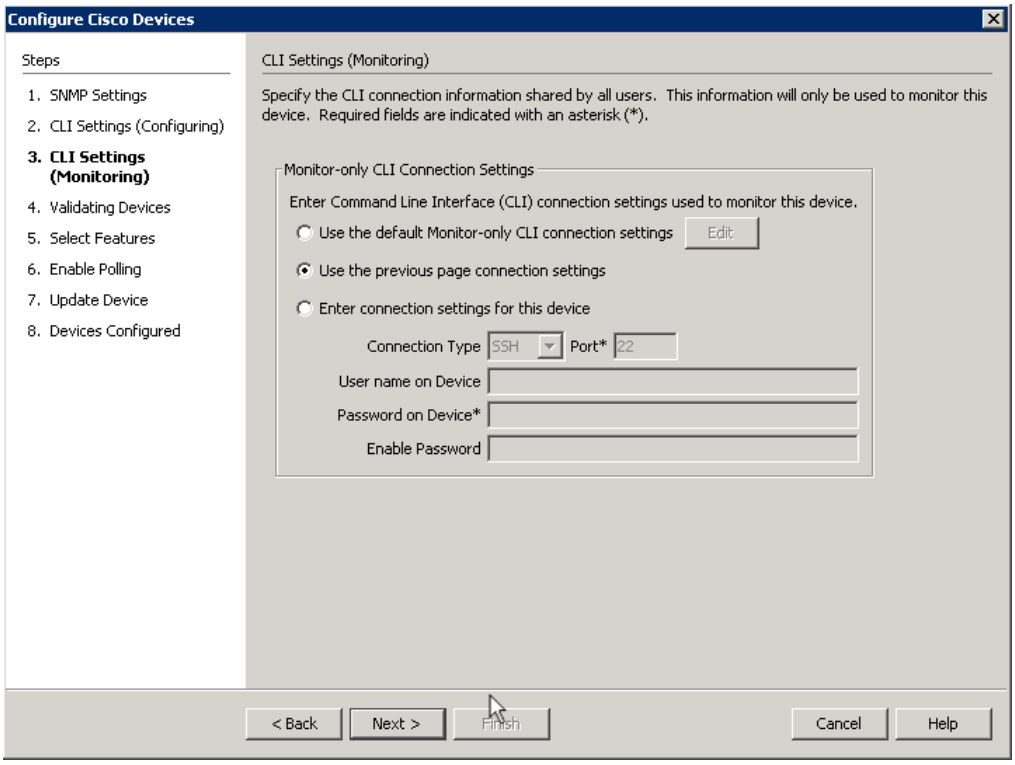



33. Select Use my default Configuration CLI connection settings.

34. Click next.

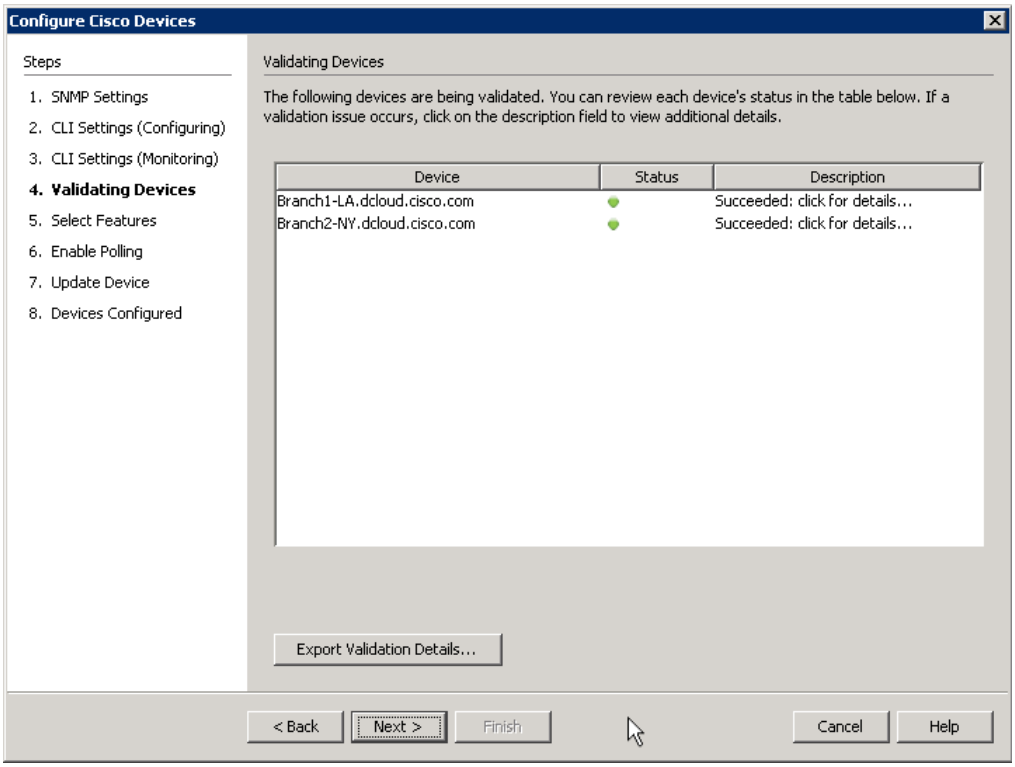


35. Select Use the previous page connection settings.

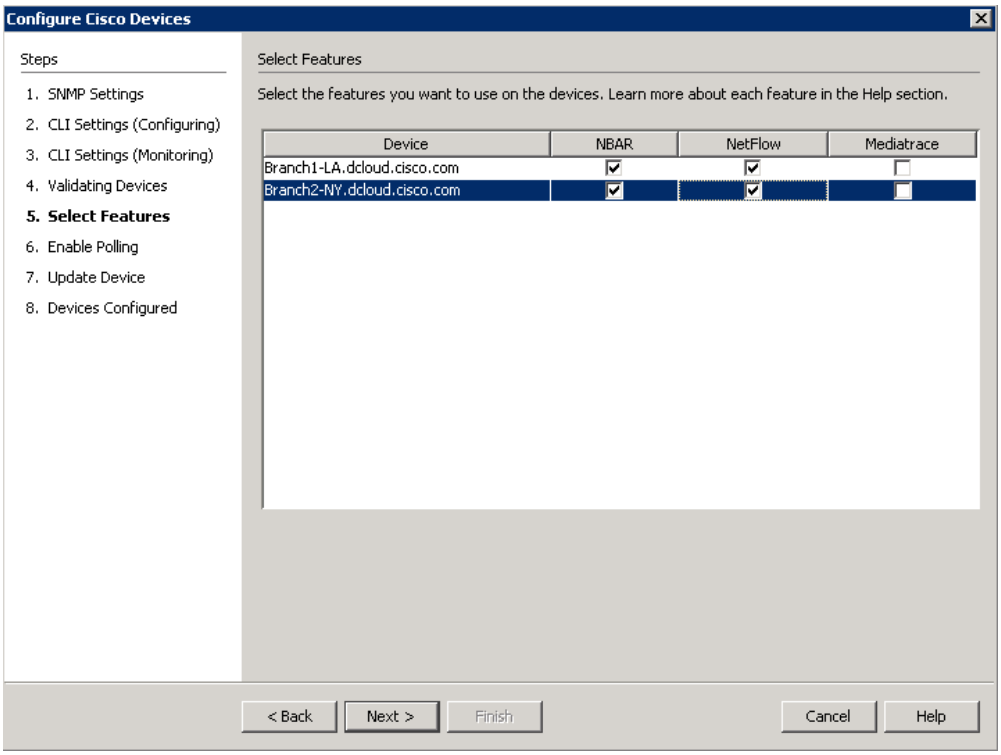



36. Click Next

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

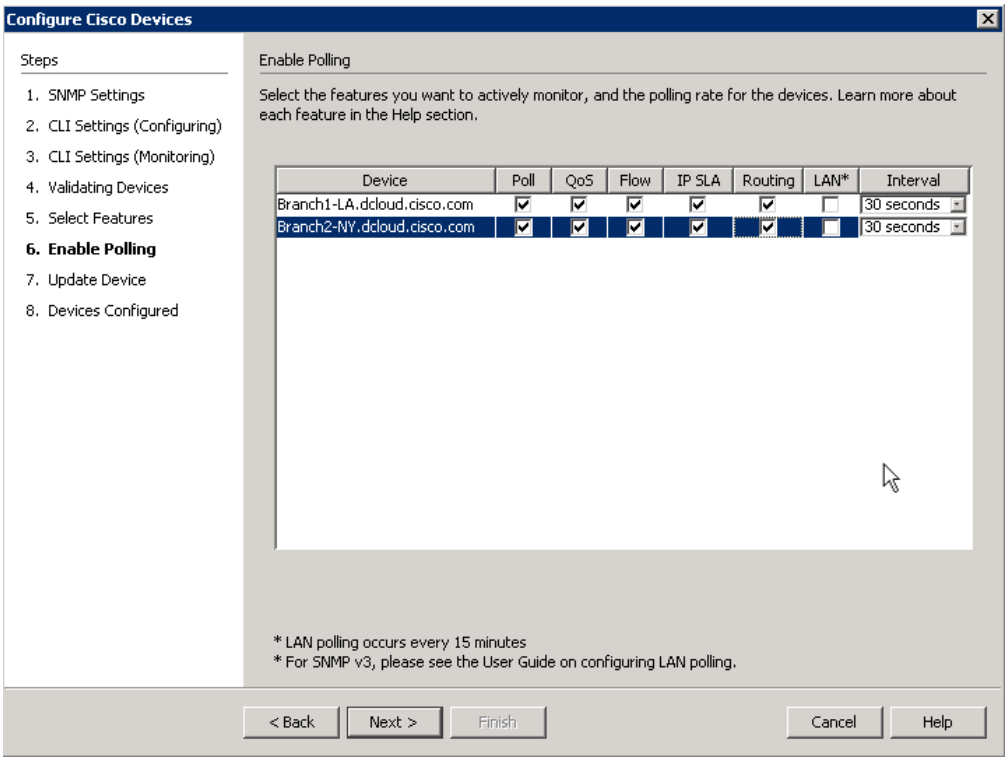


38. Select NBAR and NetFlow for both devices, Click Next.



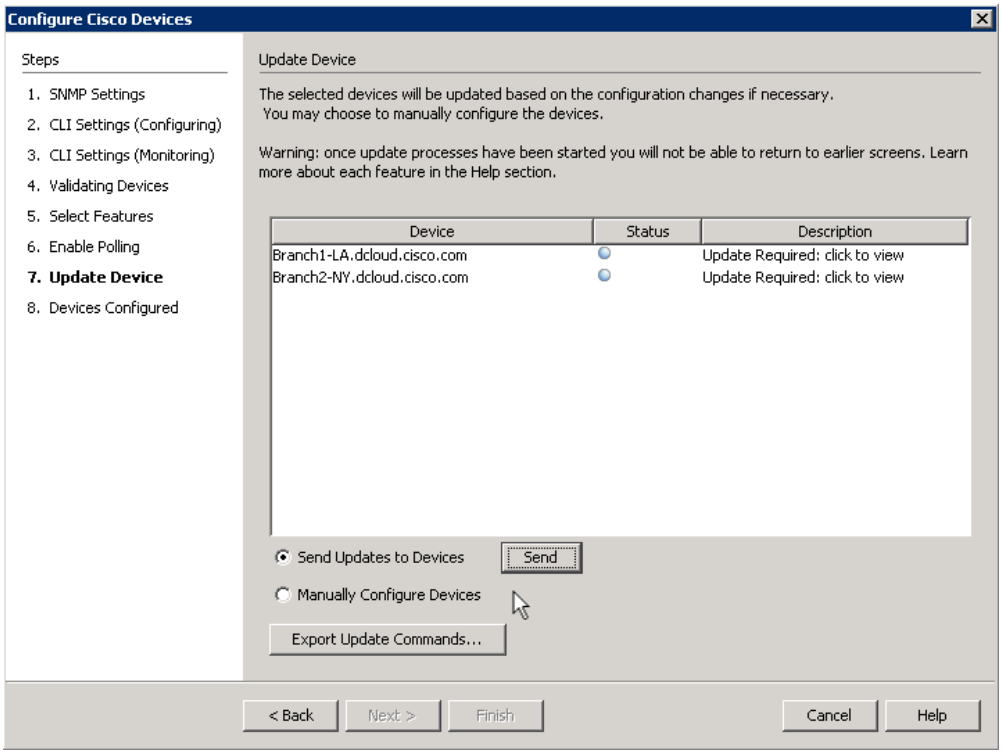

39. Select all technologies excepting LAN.

40. Set the interval to 30 seconds for each device, Click Next.

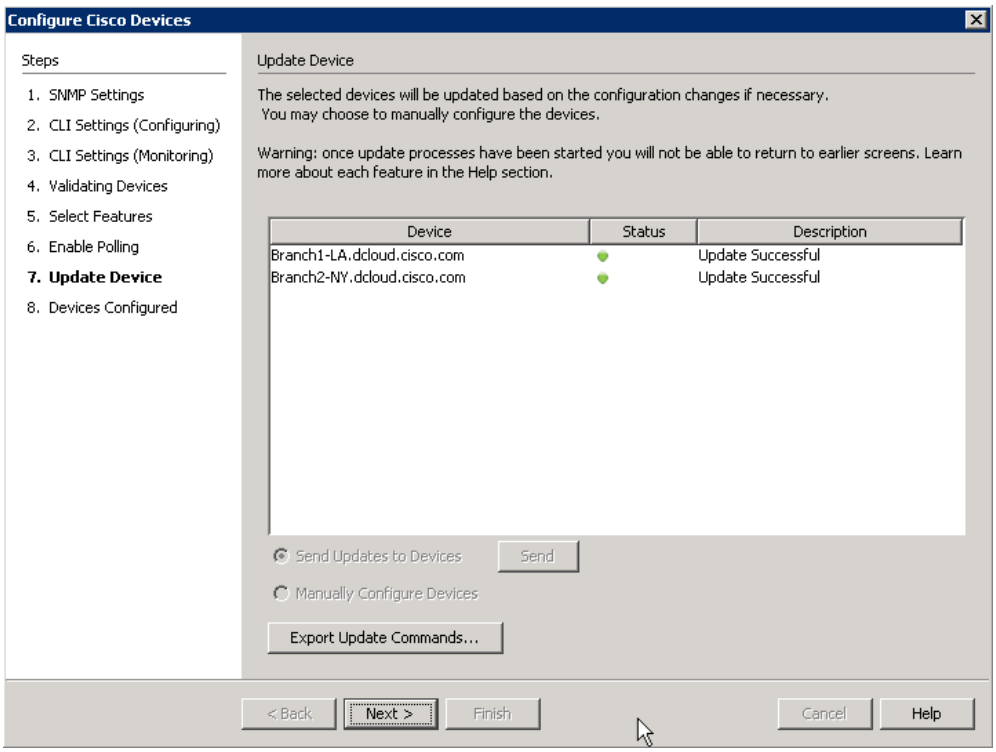



**Note: For our class Labs we are gathering data every 30 seconds to reduce wait time when we make changes. In a production environment this may generate more network traffic than desired.**

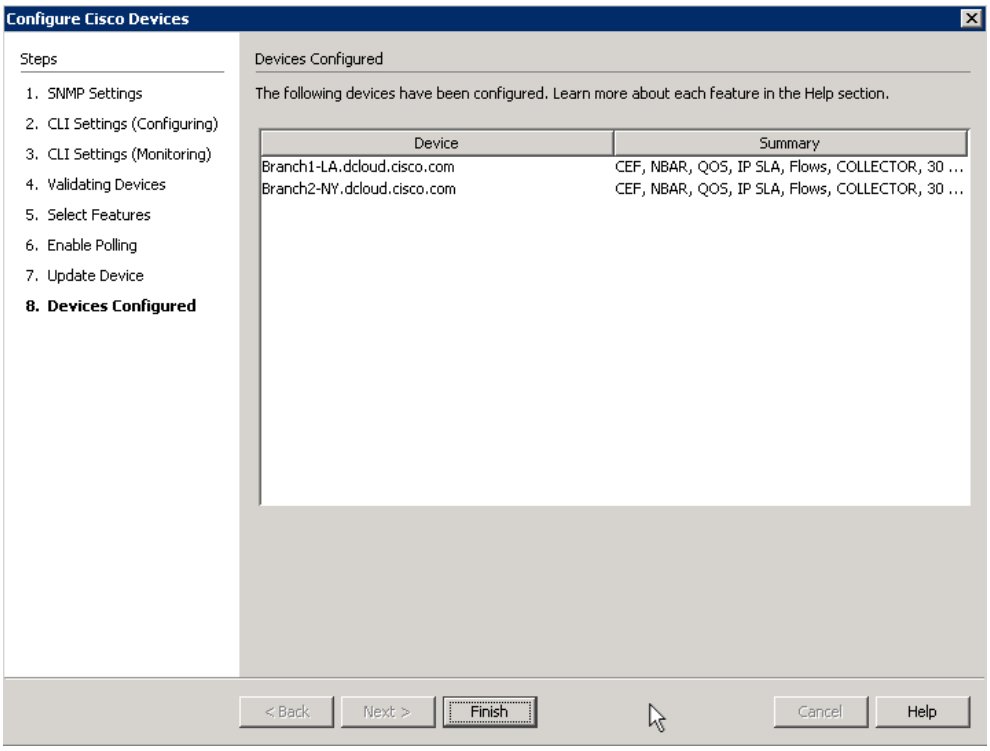
41. Select Send Updates to Devices and click Send.




42. Once the updates are pushed successfully, click next.



43. Click finish to add the devices into the topology.

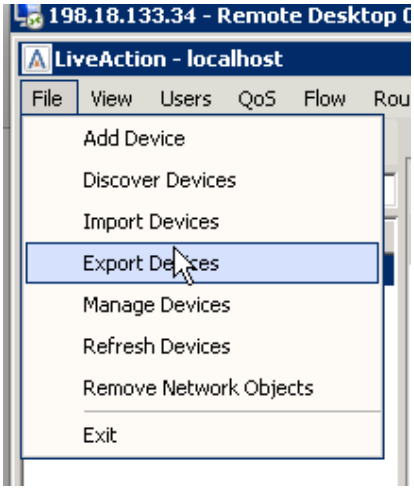



Now that you have added three devices to the topology, they should look familiar to the image below. What is important to remember is that you should only bring in interfaces that will have interesting traffic, to you, traversing them. We will not need all the interfaces that have been included, so in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

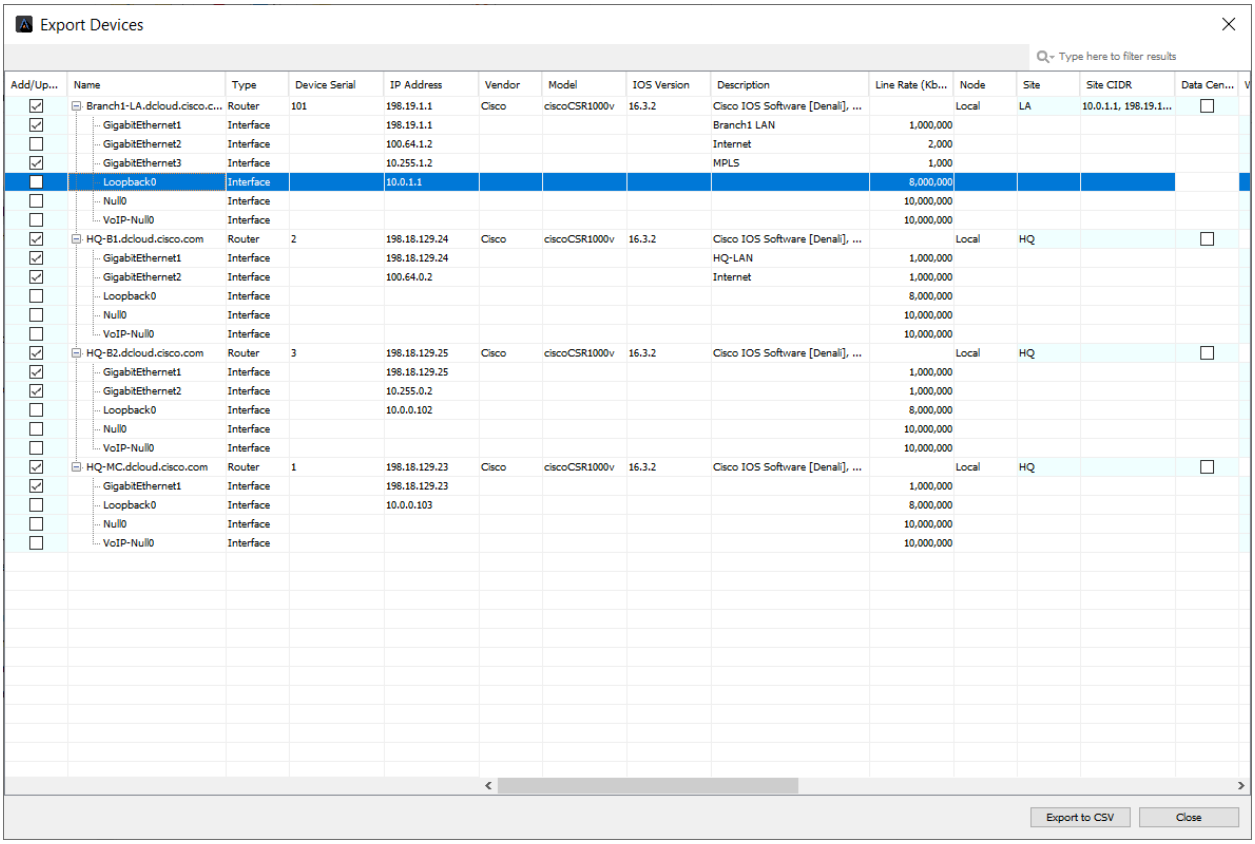
# Lab A.3: Export/Import Device Configuration

Lab Steps:

44. From the File Menu select Export Devices.

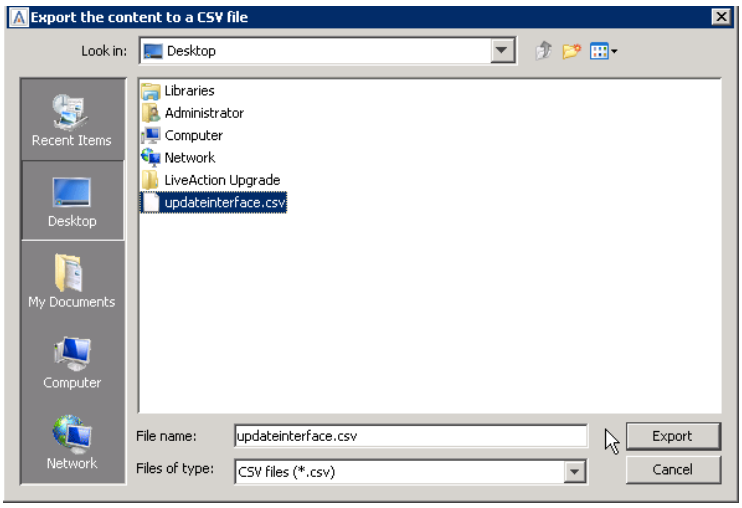



45. Deselect **GigabitEthernet2** and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

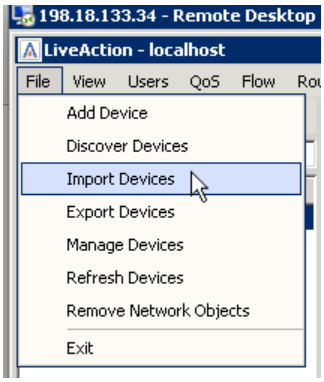



46. Select Export to csv.

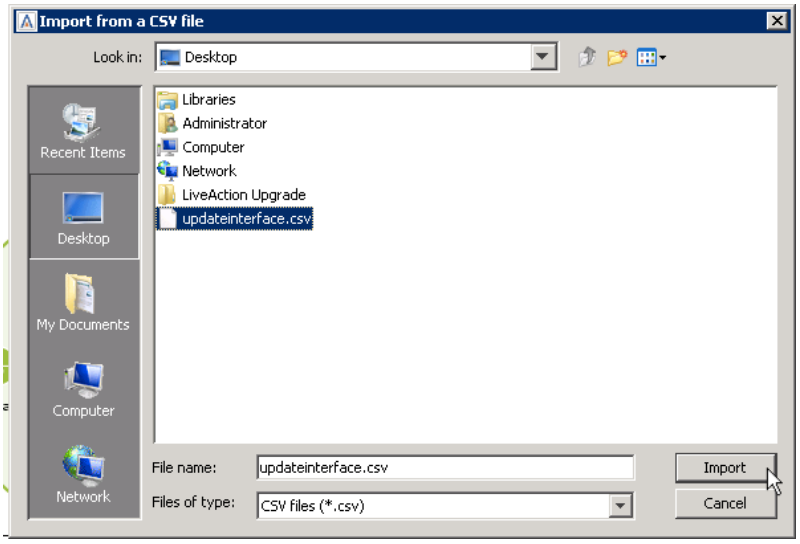
47. On the Export window give the file a name.
48. Export the csv to the desktop, or appropriate directory.



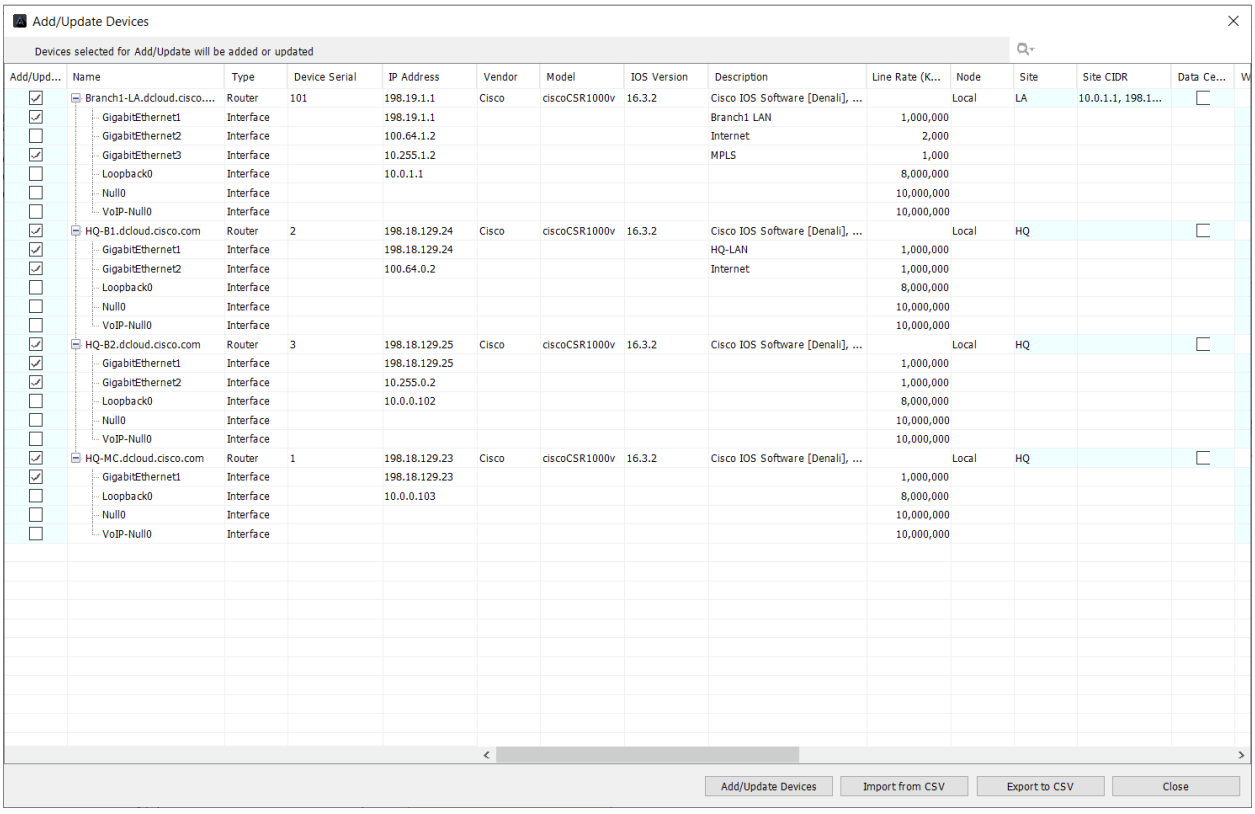

49. Close the export devices window.
50. Select File and Import Devices.



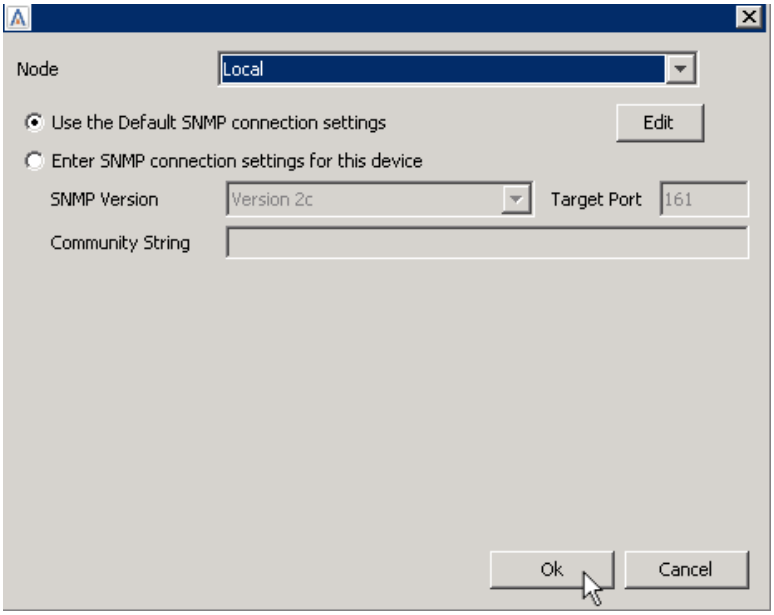

51. Select the file you previously exported.




52. Click Add/Update Devices.




53. Click OK to use the Default SNMP settings.



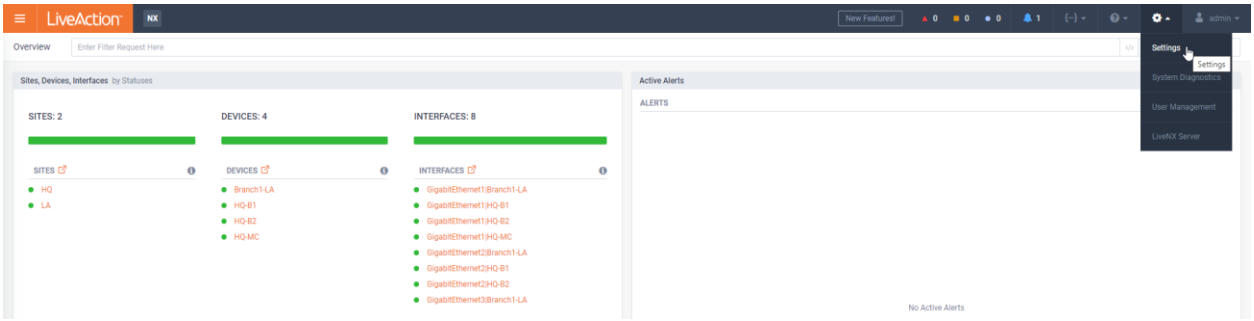

Your Topology Pane will now show the appropriate devices/configurations.

# Lab A.4:  Saving Server Configurations

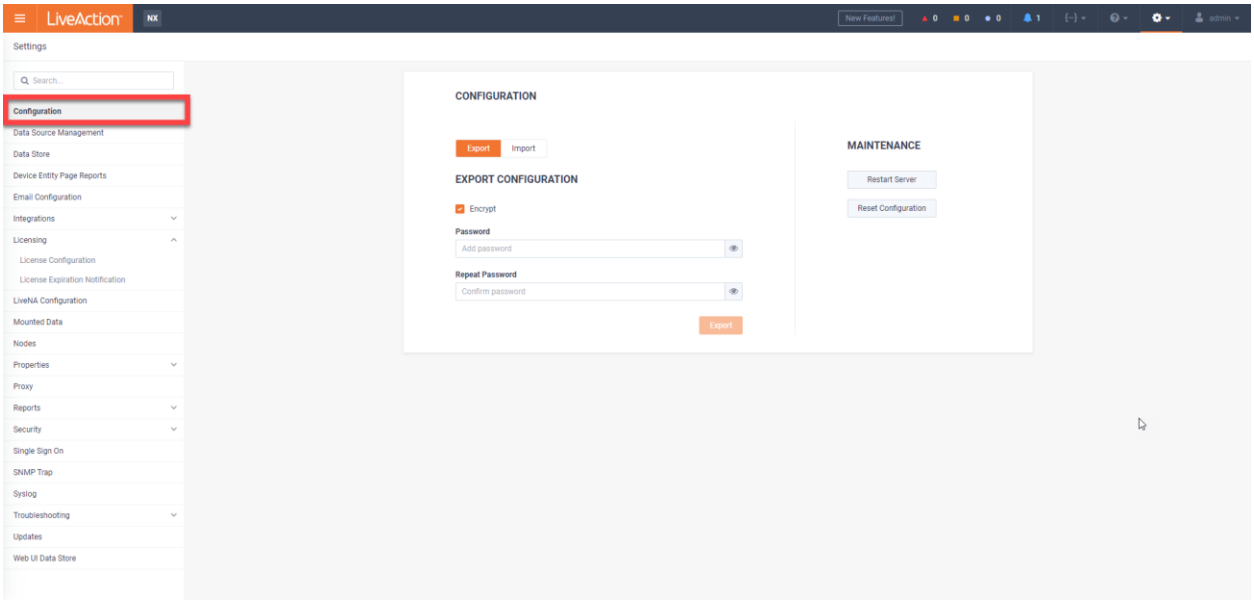
Prior to upgrading the LiveAction Software, or to retain existing Server configuration for use in the case of a hardware failure or misconfiguration, the current configuration file may be Exported to a local or network drive.

Lab Steps:

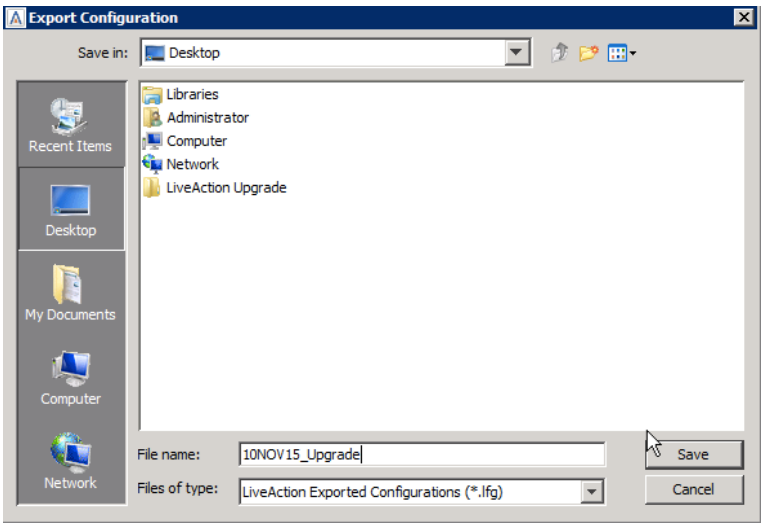
54. Open the LiveNX WebUI, select **Settings**.




55. Select **Configuration**.




56. Click **Export**.
57. Enter encryption password if preferred.




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

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

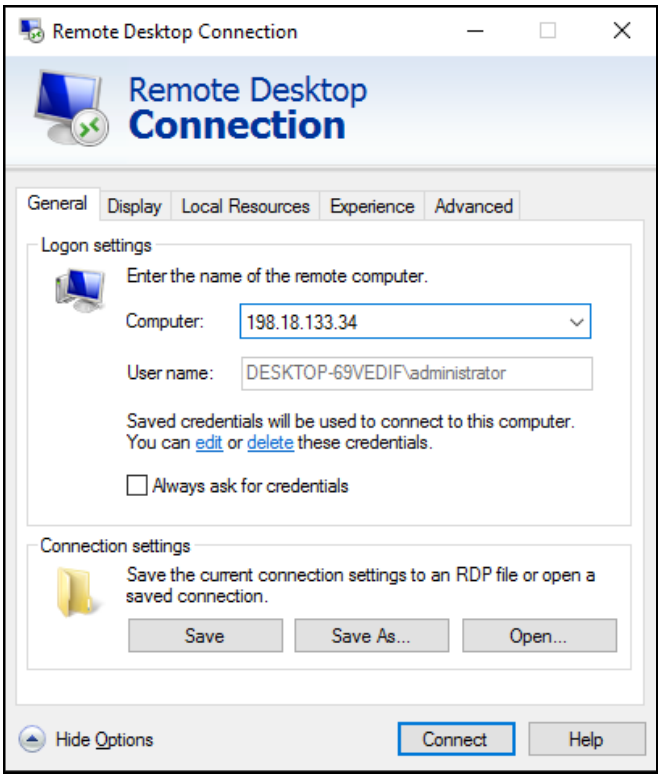
**Note: Use the information from the Lab Details table to connect to the desired device.**

Lab Steps:

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

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

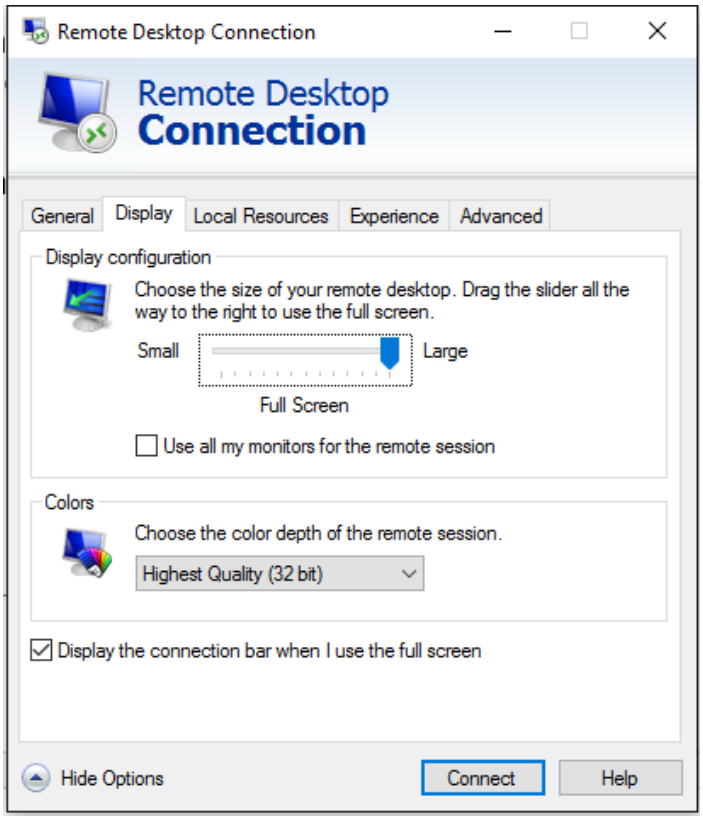
DIAGRAM




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

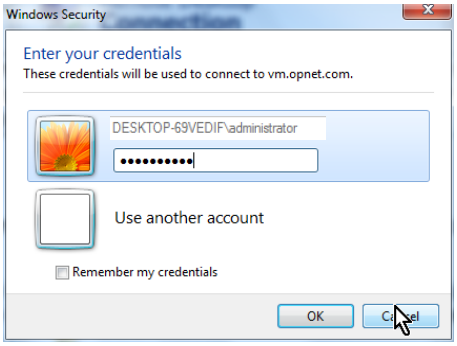
61. Set the RDC session properties on the Display tab so that your video is a minimum of 1200x800 resolution… this may NOT be changed once the connection is active. See next page for example.

DIAGRAM




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

DIAGRAM




64. Click OK.

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

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