Table of Contents

Lab 1: QoS Configuration .............................................................................................................. 5
Lab 1.0: Introduction to QoS ...................................................................................................... 6
Lab 1.1: Run Baseline Reports ................................................................................................. 8
Lab 1.2: Building Filters ......................................................................................................... 13
Lab 1.3: Validating Filters .................................................................................................... 19
Lab 2: Classification & Marking ............................................................................................... 23
  Lab 2.1: QoS Class Models .................................................................................................. 24
  Lab 2.2: Validate DSCP Markings ....................................................................................... 26
  Lab 2.3: Rogue DSCP Markings .......................................................................................... 31
  Lab 2.4: Configure Classification & Marking Policies ............................................................ 32
  Lab 2.5: Apply Marking Policies to Interface(s) .................................................................... 40
  Lab 2.6: Validate DSCP Settings .......................................................................................... 46
Lab 3: QoS Prioritization & Queueing ......................................................................................... 49
  Lab 3.0: Intro to Prioritization ............................................................................................. 50
  Lab 3.1: Run the Reports! ..................................................................................................... 51
  Lab 3.2: Building Queueing Policies .................................................................................... 54
Lab 4: Shaping / Scaling .............................................................................................................. 60
  Lab 4.0: Intro - Shaping (Scaling) ....................................................................................... 60
  Lab 4.1: Shaping (Scaling) .................................................................................................. 62
Lab 5: Throttling Traffic .............................................................................................................. 80
  Lab 5.0: Intro - Throttling / Policing ..................................................................................... 81
  Lab 5.1: Throttling / Policing ............................................................................................... 83
  Lab 5.2: Confirm policing Settings ........................................................................................ 88
Lab 6: Buffer Tuning .................................................................................................................... 90
  Lab 6.0: Intro – Buffer Tuning ............................................................................................. 91
  Lab 6.1: Implementing Tuning ............................................................................................... 96
Lab 7: QoS Alerts ...................................................................................................................... 100
  Lab 7.1: Configure QoS Alerts ............................................................................................. 101
Appendices ................................................................................................................................... 108
  Appendix 1: Add Device ................................................................................................... 109
  Appendix 2: Client Device Discovery .................................................................................... 115
  Appendix 3: Export/Import Device Configuration ................................................................. 123
  Appendix 4: Saving Server Configurations .......................................................................... 127
  Appendix 5: Connect via Remote Desktop Connection .......................................................... 129
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 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 two branch locations with connections back to HQ via two MPLS Networks. The connectivity is designed as follows:

- HQ-B1 - no provider CIR
- HQ-B2 - 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.

Figure 1

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.

**Figure 2**

**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

This Lab uses the WebUI.

- From the LiveNX Client, Run the Reports > Flow > Applications > **Application**
  - Keep all filters and report at their default settings (All Devices, Outbound)
  - Implement a Search of “wan” by entering **wan** in the flex search bar.
  - Then click **Execute Report**

Figure 3

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

Review the applications on the network – examples of business-critical applications are represented. Notice the ratios of these examples may not be representative of real networks.

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

Run the Reports > Flow > Network > **Interface Bandwidth Summary Report**
  a. Keep all filters and report at their default settings
  b. **Execute Report**
Figure 4

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

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

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

Re-run this report but update the Search to: “flow.app=10.21.1.154”

This provides an understanding of the utilization of an as yet unidentified application on each WAN circuit.
Re-run this report but update the Search to view other key applications as desired.

Run the Report **Site Traffic**

a. Keep all filters and report at their default settings
b. In the report settings select **WAN Devices**, and **All WAN Interfaces**.

c. **Execute Report**
Observe the breakdown of bandwidth between site pairs.

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

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

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

Run the Reports > Flow > Address > **Destination Site Traffic**

- a. Keep all filters and report at their default settings
- b. In the report settings select **WAN Devices**, and **All WAN Interfaces**.
- c. **Execute Report**

Observe which sites are being sent the most data.
Re-run this report, but update the Search to: “flow.app=rtp”
This provides an understanding of which sites are receiving the most Voice (rtp).

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

Run the Reports > Flow > Address > **Source Site Traffic Report**

- Keep all filters and report at their default settings
- In the report settings select **WAN Devices**, and **All WAN Interfaces**.
- **Execute Report**

Observe which sites are sending the most data.

Re-run this report, but update the Search to: **“flow.app=rtp”**
This provides an understanding of which sites are sending most Voice (rtp).

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 to keep this understanding in mind as we continue through the lifecycle of the QoS project and beyond.
Lab 1.2: Building Filters

This Lab uses the Engineering Console.

The reports we have used so far were using NBAR for recognizing specific types of traffic such as Voice (rtp). 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, Custom Applications and Application Groups provide an excellent way to administratively define application definitions. As an example, we are now going to build custom applications and an Application Group 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:

- From the LiveAction map, select the Flow Tab

  ![Figure 10](image)

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

  ![Figure 11](image)

  - The Display Filters Setup Dialog appears
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.
Figure 14

- Delete unused Entries
  - VoIP
  - Ventrilo TCP
  - Ventrilo UDP
- Add Entry

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

- Name it MGCP
- Tick “Match Protocols/Ports"
- In the dropdown, select MGCP
- Also select Match DSCP = 31
Edit Entries the following entries with these updates:

- **H323** - TCP/UDP = Src or Dst = 1718 1719 1720 and DSCP = 46
- **SIP** - TCP/UDP = Src or Dst = 5060 5061 5062 and DSCP = 46
- **Skinny** – TCP = Src OR Dst = 2000 2001 2002 and DSCP = 46
- **RTP** - UDP = Src AND Dst = 16384-32767 and DSCP = 34
Figure 16

Figure 17

- When finished, you should have something that looks like the following:
• MGCP - TCP/UDP = Src OR Dst = 2427 2727 & TCP = Src or Dst = 2428 and DSCP=31
• H323 - TCP/UDP = Src OR Dst = 1718 1719 1720 and DSCP=46
• Skinny – TCP = Src OR Dst = 2000 2001 2002 and DSCP=46
• SIP - TCP/UDP = Src OR Dst = 5060 5061 5062 and DSCP=26
• RTP - UDP = Src AND Dst = 16384-32767 and DSCP=34

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

This Lab uses the WebUI and Engineering Console.

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:

- From the LiveNX Client map, select the Flow Tab

![Figure 18](image1)

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

![Figure 19](image2)

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

![Figure 20](image3)

Confirm in the legend there is Voice traffic being matched. You should see RTP & SIP being matched.
Run the Miscellaneous > **User Filter** report

a. Select the Voice filter, but leave all parameters at their default settings
b. In the report settings select **WAN Devices**, and **All WAN Interfaces**.

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.

Run the Reports > Flow > Applications > Application report

a. Select the Voice filter, but leave all parameters at their default settings
b. In the report settings select WAN Devices, and All WAN Interfaces.

c. Execute Report

Figure 24

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?

Run the Reports > Flow > Analysis > IPs and Ports report

a. Select the Voice filter, but leave all parameters at their default settings
b. In the report settings select WAN Devices, and All WAN Interfaces.

c. Execute Report

Figure 25
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.

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

Figure 26

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

**This Lab uses the Engineering Console.**

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:

<table>
<thead>
<tr>
<th>Class Type/Name</th>
<th>5 Class Model</th>
<th>Business Critical Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF (46)</td>
<td>rtp</td>
</tr>
<tr>
<td>Video</td>
<td>AF41 (34)</td>
<td>openwebnet</td>
</tr>
<tr>
<td>High Priority Data</td>
<td>AF31</td>
<td>SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1 (8)</td>
<td>Unknown yet</td>
</tr>
<tr>
<td>Best Effort</td>
<td>BE (0)</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Figure 27

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

Lab Steps:

- From the LiveNX Client, select the Flow Tab

Figure 28

- From the options at the top of the map, select the icon:

Figure 29

- Set the Attribute to DSCP

Update the values to match those selected for the lab’s 5 class QoS model.
### Color Mapping

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

#### Attribute: DSCP

Select a DSCP value from the drop-down lists below:

- DSCP 0 (BE)
- DSCP 18 (AF21)
- DSCP 26 (AF31)
- DSCP 34 (AF41)
- DSCP 42 (AF51)
- DSCP 24 (CS3)
- DSCP 32 (CS4)
- DSCP 40 (CS6)
- DSCP 46 (EF)
- (Remainng)

![Color Mapping Dialog Box](Figure 30)

---

**Lab 2.1: QoS Class Models**

© Copyright LiveAction 2022
Lab 2.2: Validate DSCP Markings

This Lab uses the WebUI and the Engineering Console.

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

- From the LiveAction map, select the Flow Tab

![Flow Tab]

Figure 31

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

All Flow Types, Current Time, Current Poling Interval, Top 50, DSCP

You should be presented with a Flow visualization like the following diagram

![Flow Visualization]

Figure 32

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.

Update the Search to “flow.direction=Egress”

You will see the DSCP markings that are exiting each router. It looks like LA has only BE traffic. Let’s look further into exactly what protocols are using each DSCP.
Note: In the following labs the traffic shown in these images may not reflect what you see in your lab. 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 Engineering Client reports to investigate further.

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

![DSCP Report](image)

Figure 36

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.

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

- Run the Reports > Flow > QoS > Application DSCP Audit report.
  - Select the Voice filter, but leave all parameters at their default settings
  - Implement a Search of "wan"
  - 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 (openwebnet) 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:

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

![Flow 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:

- From the LiveAction map, select the QoS Tab

![QoS Tab](image)

Figure 40

Right-click on the HQ-B2 router, select QoS > Manage QoS Settings

![Manage QoS Settings](image)

Figure 41
Select the Add Policy icon.

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.

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

On the Classify Tab, select the Edit button.
**Figure 48**

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

**Figure 49**

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

- Select the Marking tab.

Select the Mark With check box and select the DSCP value of 46 (EF)
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:

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>NBAR Protocol(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SET_DSCP_VOICE</td>
<td>EF (46)</td>
<td>rtp</td>
</tr>
<tr>
<td>SET_DSCP_VIDEO</td>
<td>AF41 (34)</td>
<td>MS-Lync</td>
</tr>
<tr>
<td>SET_DSCP_HIGH_PRIORITY_DATA</td>
<td>AF31 (26)</td>
<td>SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce</td>
</tr>
<tr>
<td>SET_DSCP_SCAVENGER</td>
<td>CS1 (8)</td>
<td>Leave blank for now</td>
</tr>
<tr>
<td>Best Effort</td>
<td>BE (0)</td>
<td>n/a</td>
</tr>
</tbody>
</table>
When finished, the **SET_DSCP_LAN** policy should look like this:

![Policy Configuration Screenshot](image)

Figure 54

Select **Save to Device**.

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.

![Policy Copy Dialog](image)

Figure 55

The **Copy Policy to Devices** dialog window appears.
Select the policy **SET_DSCP_LAN**, check HQ-B2 and the two branch routers, and select **OK**.

![Figure 56](nxof-2.lwa.2.0.0.png)

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

Validate the changes saved successfully.

![Figure 57](nxof-2.lwa.2.0.0.png)

Close the **Copy Policy to Devices** dialog window.

Close the **Manage QoS** dialog window.

You will be prompted to save these changes to the startup configuration, click **Yes**.

You can click **Yes** three times, or select the **Do not show again** option.
Lab 2.5: Apply Marking Policies to Interface(s)

Lab Steps:

- Select the QoS Tab

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

**Note:** The LAN interface will be GigabitEthernet2 on each of the routers in this lab.

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

Figure 62
Select the Interface tab

Figure 63
Right-click on the WhyIsThisHere policy that is highlighted on the input side of the GigabitEthernet2 interface.
Figure 64
Select Remove Policy from Interface

**Right-click** on the input side of the GigabitEthernet2 interface and select **Apply Policy to Interface**.

Figure 65
Select the **SET_DSCP_LAN** policy and select OK.

Figure 66
Select **Save to Device** and close the Manage QoS Settings dialog window. When prompted, save from current running configuration to startup configuration.
Figure 67

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.

- From the LiveAction map, select the **Flow Tab**

![Flow Tab](image)

**Figure 68**

Update the filters to the following parameters

![Filter Configuration](image)

**Figure 69**

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

![DSCP Filter Result](image)

**Figure 70**
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. Therefore, 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).

Run the Reports > Flow > QOS > DSCP report

- Select the Voice filter, but leave all parameters at their default settings
- Implement a Search of "wan"
- 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: QoS Prioritization & Queueing
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:

- Run the Reports > Flow > Network > Interface Bandwidth Summary report
  - Leave all Filter parameters at their default settings.
  - Implement a Search of “wan & flow.dscp=EF & flow.direction=Egress”
  - 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.

Run the Flow > Network > Interface Bandwidth Summary report

- Leave all Filter parameters at their default settings
  - Implement a Search of “wan & flow.dscp=AF41 & 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 Video (MS-Lync)/AF41 traffic. This is the capacity planning data we need for Video.

Run the Flow > Network > Interface Bandwidth Summary Report

- Leave all Filter parameters at their default settings
- 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

- From the LiveAction map, select the QoS Tab

Right-click the HQ-B1 router, select QoS > Manage QoS Settings

The Manage QoS Dialog Window will open
Add a new Policy and name it **QUEUEING**.

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

You should see the **VOICE** class inside the policy named **QUEUEING**.
Update the Classes tab of the VOICE class to match **DSCP 46 (EF)** traffic
Return to the Policies tab

Ensure the VOICE class of QUEUEING policy is highlighted and select the Queueing tab.

Set the Queueing type to Priority and the bandwidth to 160 Kbps.
Create the following classes in the QUEUEING policy based on the following table:

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Match DSCP</th>
<th>Queueing</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOICE</td>
<td>EF (46)</td>
<td>Priority – 160K</td>
</tr>
<tr>
<td>VIDEO</td>
<td>AF41 (34)</td>
<td>Priority – 800K</td>
</tr>
<tr>
<td>HIGH_PRIORITY DATA</td>
<td>AF31 (26)</td>
<td>Class Based – 64K</td>
</tr>
<tr>
<td>SCAVENGER</td>
<td>CS1 (8)</td>
<td>Class Based – 8K</td>
</tr>
<tr>
<td>Best Effort</td>
<td>BE (0)</td>
<td>n/a</td>
</tr>
</tbody>
</table>

When finished, the QUEUEING policy should look like this:

Click **Save to Device**.

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.
Push the QUEUEING policy to the other routers

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

If you encounter a conflict – select **Overwrite**.
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 design:

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 Steps:

- Right Click on HQ-B1 and select **Manage ACL’s**. We will create some ACL’s first. We will create two ACL’s:
  - HQ_TO_NY_ACL
  - HQ_TO_LA_ACL
- Click on **Create ACL**.
- Select **Extended** as the ACL Type. Let’s do the **HQ_TO_NY_ACL** first.
- Create a rule allowing **198.18.129.0/24** to **198.19.2.0/24**
- Click **OK**. If you want to Preview the commands that will be sent to CLI click **Preview CLI**. Then click **Save To Device**.
- Next, create another ACL called **HQ_TO_LA_ACL**.
• **Create Rule** entry with source IP `198.19.129.0/24` and destination IP `198.19.1.0/24`.

• **Click OK**, then **Save to Device**. (Preview the CLI commands if you want to)
• **You should see the two ACLs now created.**
Click Close.

From the LiveAction map, make sure you are still in the QoS Tab.

Right-click on the HQ-B1 router, select QoS > Manage QoS Settings.

The Manage QoS Dialog Window will open.
Create a new policy and name it **MULTI_CLASS_SHAPING**

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

Edit these classes, but chose the match type of **ACL Name**
Match the HQ_TO_NY class to the HQ_TO_NY_ACL

Match the HQ_TO_LA class to the HQ_TO_LA_ACL
When finished, return to the **Policy** tab
Select the **HQ_TO_NY** class and select the **shaping** tab. Set its parameters to:

- Shape using = Average
- Rate = 1,000 Kbps
- Committed burst = 10,000
- Excess burst = 0

Select the **HQ_TO_LA** class and select the **shaping** tab. Set its parameters to:

- Shape using = Average
- Rate = 1,000 Kbps
- Committed burst = 10,000
- Excess burst = 0
Click-Drag-and-Drop the QUEUEING policy to the HQ_TO_NY policy under MULTI_CLASS_SHAPING.

Click-Drag-and-Drop the QUEUEING policy to the HQ_TO_LA policy under MULTI_CLASS_SHAPING.

When finished your view should look like this:
Select the `interfaces` tab and apply the MULTI_CLASS_SHAPING policy to the output of the GigabitEthernet3 interface.

Make sure you select the `MULTI_CLASS_SHAPING` policy.
Click Save to Device.
You will see the Saving information box appear.

Then Click Close. The **Would you like to save the current running configuration to the startup configuration, i.e., “copy run start”** dialogue box appear. Click Yes.

Go back into HQ-B1 Manage **QoS Settings**. Then click the **Copy Policy to Devices** box and select the **MULTI_CLASS_SHAPING** policy, and check **HQ-B2** as the destination device.
When you hit OK, you will see the Copy Status box appear. If you get a Copy QoS Policy to Device Conflict, select Overwrite.
Next, we will build basic hierarchical policies on the remote routers.

In LiveNX and select the **QoS Tab**

**Right-click** on **Branch1-LA**, select **QoS > Manage QoS Settings**

Create a new policy and name it “SHAPING_1.544Mb”

Select its **class-default** and select the **Shaping** tab.

Implement a **shaping policy** with the following parameters:

- **Shape using** = Average
- **Rate** = 1544 Kbps
- **Committed burst** = 15,440
- **Excess burst** = 0
Click-Drag-and-Drop the QUEUEING policy onto the class-default of the SHAPING_1.544Mb policy.
Copy the SHAPING_1.544Mb policy to the other remote router.

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

Select **Overwrite**.

Validate the changes saved successfully.
Save to Device and Copy to Startup Config. Then close the Manage QoS Settings dialog window.
In LiveNX console, select the QoS Tab

**Right-click** on the WAN interface (GigabitEthernet4) on the NY router, select **QoS > Apply Policy to Interface**

**Apply** the SHAPING_1.544Mb policy to the **output** of GigabitEthernet4.

Repeat this process and apply the **SHAPING_1.544Mb** policy to the other WAN interface (GigabitEthernet3).

Once you are complete with **Branch1-LA**, do the same with **Branch2-NY** and apply the policy to **both WAN Interfaces** (GigabitEthernet3 and GigabitEthernet4).

You can verify that the configuration is complete and correct by reviewing the **Interfaces** tab of each router.
Lab 5

Lab 5: Throttling Traffic
Investigate the current traffic flows.

- From the LiveNX Client, select the QoS Tab

Select **GigabitEthernet3** from the **HQ-B2** router

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, on our business network?
Run a **Flow > Application** report to see the same type of data.
Lab 5.1: Throttling / Policing

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

Lab Steps:

- From the LiveAction map, select the QoS Tab

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.

<table>
<thead>
<tr>
<th>Class Name</th>
<th>DSCP</th>
<th>NBAR Protocol(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SET_DSCP_VOICE</td>
<td>EF (46)</td>
<td>rtp</td>
</tr>
<tr>
<td>SET_DSCP_VIDEO</td>
<td>AF41 (34)</td>
<td>Lync</td>
</tr>
<tr>
<td>SET_DSCP_HIGH_PRIORITY DATA</td>
<td>AF31</td>
<td>SIP, SNMP, NetFlow, SSH, Telnet, Citrix, Salesforce</td>
</tr>
<tr>
<td>SET_DSCP_SCAVENGER</td>
<td>CS1 (8)</td>
<td>Leave blank for now</td>
</tr>
<tr>
<td>Best Effort</td>
<td>BE (0)</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Update the **SET_DSCP_SCAVENGER** class with the following traffic:

- Bittorrent
- Bittorrent-networking
When finished, the SET_DSCP_LAN policy should look like this:

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

Select **Save to Device**.

**Copy** the SET_DSCP_LAN policy to the other available routers.
Note: You will get a conflict warning... simply select Overwrite.

Validate the changes saved successfully., Click Close,
Close the Manage QoS Settings Dialog Window

Lab 5.2: Confirm policing Settings

Lab Steps:

- Select the QoS Tab.

From the device list, select the HQ-B2 router's LAN interface – GigabitEthernet2

Update the real-time view’s options to just include the input.
Note: If any of the policies are exceeded, they will show as AMBER. The amber confirms that drops are occurring inside the queue.
Lab 6

Lab 6: 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 Alert button. Yours may or may not be red.
   b. Double click the alert button
   c. The In-Application Alert view appears
d. Are there any alerts class drop alerts from the VOICE 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 VOICE, note the device and interface where the drop occurred. In this example, the device is Branch1-LA, and the interface is GigabitEthernet4, and the direction is egress (output).

g. Select this interface from the device list.

h. From the real-time interface view, if necessary, update the view to Class/Class Drops, and Output.

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 VOICE 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 VOICE (purple) class and the class-default (grey). In this example there have been 7 drops at peak in the VOICE class.
m. To investigate the same type of drops from a historical report select the 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 VOICE queue for each site to 800Kbps each.

q. The Pre-Policy graph above shows 742 Kbps peak VOICE traffic on the SHAPING_1.544Mb policy.
This is above the provisioned 160K. We need to implement some buffer tuning.
Lab Steps:

- Select the **QoS** Tab

Right-click the **HQ-B2** router and select **QoS > Manage QoS Settings**
Expand the QUEUEING Policy

Select the VOICE class.

Select the Queueing tab

Tick the **Burst option** and set it to **128000**.

Select the **Save to Device** button.

Copy the QUEUEING policy to the **other devices via Copy Policy to Devices** icon.
When the conflict warning appears, select **overwrite**.

Validate the changes saved successfully.
Close the Manage QoS Settings Dialog window.

Accept the suggestion to copy the current running configuration to the startup config.
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.
Ignore the message regarding reporting in the WebUI. This is normal – and reporting as we need it will still work here.

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:

Select the **Custom Triggers** tab.

Click **Add**.

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

Click **OK**.
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.

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.
Monitor the system for any new QoS Alerts.

Click the Clear List Button
Appendix 1: Add Device

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

Lab Steps:

- Select File, **Add Device**

  ![Add Device](image)

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

  ![Add Device Steps](image)

- Click Next.
- Select “Use my default Configuration CLI connection settings”.

- Click Next.

- Select “Use the previous page connection settings”.

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

- 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.

- 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.

- 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.

- Click Next.
- Change the polling rate to 30 seconds.
• 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.

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

• Click Next.

• 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).
Appendix 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:

- Select File and Discover Devices.

  ![Remote Desktop](Image)

  - Specify the following IP addresses:
    - 198.19.1.1
    - 198.19.2.1

  - 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.

- Click OK.
- 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.
• Select Yes on the configure devices dialog.
• 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.

• Select Use my default Configuration CLI connection settings.
• Click next.
Select Use the previous page connection settings.

Click Next

After verifying that the device validation is successful, Click Next.
Select NBAR and NetFlow for both devices, Click Next.

- Select all technologies excepting LAN.
- 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.

- Select Send Updates to Devices and click Send.
Once the updates are pushed successfully, click next.
• 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.
Appendix 3: Export/Import Device Configuration

Lab Steps:

- From the File Menu select Export Devices.

- Deselect GigabitEthernet3 and Loopback0 from the 198.19.1.1 and 198.19.2.1 devices.

- Select Export to csv.
• On the Export window give the file a name.
• Export the csv to the desktop, or appropriate directory.

• Close the export devices window.
• Select File and Import Devices.

• Select the file you previously exported.
• Click Add/Update Devices.

• Click OK to use the Default SNMP settings.
Your Topology Pane will now show the appropriate devices/configurations.
Appendix 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:

- Open the LiveNX WebUI, select Settings.

- Select Configuration.

- Click Export.

- Enter encryption password if preferred.
Select an appropriate place to save the file, give the file a name, then click Save.
Appendix 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.

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

Diagram

- Enter the following fields:
  - Computer: `<ipaddress>:20201`
    (From your Lab Access worksheet)
  - Username: `administrator` (or otherwise defined by instructor)
- 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.
• Select Connect.
• Enter the workstation password: C1sco12345 (or otherwise defined by instructor).

• 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.