Managing Cisco Webex QoS with LiveNX

Cisco Webex (Webex) is a cloud-based, on-demand collaboration, online meeting, web and video conferencing service. While Webex is a simple application to use, protecting its voice and video call quality across the enterprise network can be challenging to manage. Fortunately, a network administrator can effectively implement Webex QoS protection by leveraging LiveAction's application-aware network performance management platform, LiveNX, with QoS control tools.

Table of Contents

Cisco Webex and LiveAction

LiveNX is an award-winning network performance management solution with patented visualization capabilities that utilize Cisco's advanced IOS features to help implement management controls through its console. It provides a complete management solution for monitoring, troubleshooting and provisioning Webex QoS to ensure that bandwidth is properly allocated to support the needs of the business. Users can take advantage of LiveNX to go back in time (think 'network DVR') and perform analysis and troubleshooting for real-time or historic Webex calls using the Medianet Performance Monitor Path Analysis feature.

Protecting critical Webex traffic throughout the managed network can easily be done with LiveNX. This document will cover the following simple steps:

- How to use LiveNX to identify Webex traffic
- How to use LiveNX to implement QoS markings on Webex traffic
- How to use LiveNX to prioritize Webex traffic at the WAN edge and Internet perimeter via QoS policy
- How to use LiveNX to monitor performance of Webex

By using NBAR2 (protocol pack 28 or higher), Cisco's next generation network-based application recognition technology built into IOS, Webex QoS management can be further simplified to uniquely identify Webex communication without having to configure and manage complex access control lists (ACLs) in the network infrastructure. This can translate to 50 percent faster (or higher) QoS deployments and reduce the chance of mistakes during configuration. LiveAction highly recommends updating to this protocol pack to simplify Webex QoS deployments. (See Appendix D for further details.)

Cisco Webex QoS Technical Overview

Webex is a cloud-based, on-demand video and web conferencing solution. Communication occurs between users via Webex software running on a user's PC, MAC or mobile device (Windows, iPhone/iPad, Android). Other communication devices may also communicate via Webex (PSTN, IP phones, IP video conference unit). Since Webex is a cloud-based solution, the resiliency of the communication technologies is dependent on several factors, including, but not limited to: Wi-Fi reliability, last mile Internet reliability and capacity, and corporate network converged media (VoIP and video) readiness. This document will focus on QoS management and monitoring in the areas of the IP network where LiveNX can help with Webex performance.

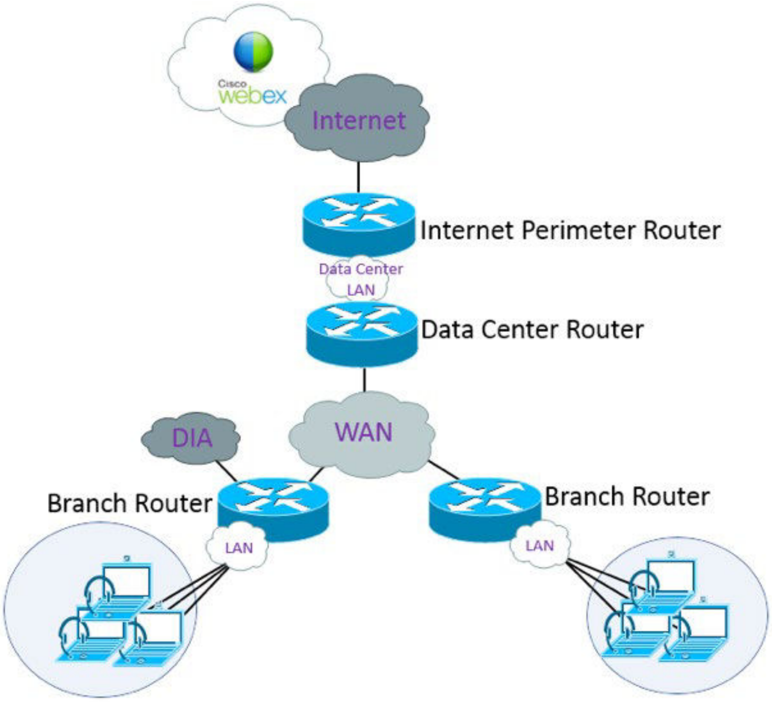
For optimum performance, the network must recognize Webex traffic, mark it with a DSCP (Differentiated Services Code Point) value, and prioritize the flows as they traverse the network. Without proper protection, congestion can cause performance impacts to both Webex communication traffic on highly utilized enterprise networks. This congestion typically occurs at the WAN edge and Internet perimeter.

The management and configuration of QoS in networks can be very complex to operate, manage and validate. It can require reviewing hundreds of lines of CLI commands to understand the configuration and performance of QoS policies on just one device alone. Therefore, understanding end-to-end QoS policy on an enterprise network can become extremely difficult at best. LiveNX has been designed to streamline the implementation and management of QoS in network environments and can be used to easily deploy this complex set of technologies to the network infrastructure.

This document will provide the configuration parameters required for Webex traffic. It will also detail the required steps of implementing QoS in a network infrastructure. Finally, it will highlight how a network infrastructure's QoS can be configured, monitored, and validated using LiveNX.

Cisco Webex QoS Design

The following diagram shows a typical Webex enterprise deployment:



A typical, managed enterprise network has the following components that must be considered when protecting and prioritizing Webex media traffic. These include:

- **WAN Edge** — The WAN edge requires QoS policies for marking DSCP values and prioritizing Webex traffic. These policies both protect the Webex traffic leaving the branch office and data center and ensure the upstream service provider recognizes Webex as priority traffic.
- **Internet Perimeter** — QoS policies for the Internet perimeter are a critical component for successful Webex communication. Even though the Internet does not have QoS across its backbone, careful consideration should be given to the QoS options available on the managed equipment that terminates the Internet. If the proper equipment is utilized, network engineers can successfully protect Webex traffic both leaving and entering managed networks. For example, traditional Cisco routers have the ability to both recognize and prioritize Webex traffic that other equipment does not provide. With the proper configurations in place (as outlined in this document), enterprises can often enjoy service from these public connections at near business-class quality.

How Does QoS Work?

QoS is a performance measurement that uses a suite of technologies to manage bandwidth usage as data crosses computer networks. Its most common use is for the protection of real-time voice or video communications and high priority data applications. QoS technologies, or tools, each have specific roles that are used in conjunction with one another to build end-to-end network QoS policies.

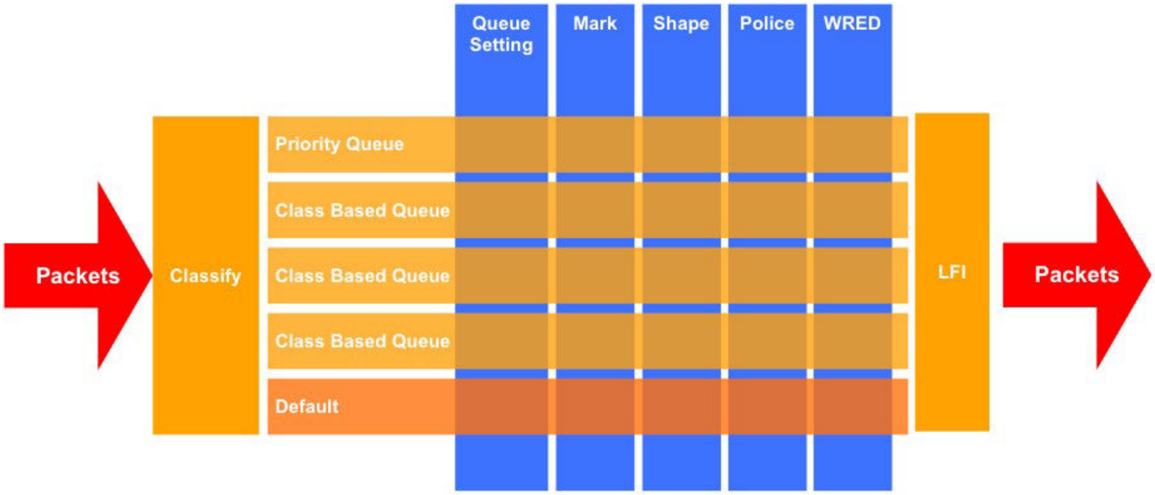
The two most common QoS tools used to handle traffic are Classification and Queuing. Classification identifies and marks traffic to ensure network devices know how to identify and prioritize data as it traverses a network. Queues are buffers in devices that hold data to be processed and provide bandwidth reservation and prioritization of traffic as it enters or leaves a network device. If the queues are not emptied (due to higher priority traffic going first), they overflow and drop traffic.

Policing and Shaping are also commonly used QoS technologies that limit the bandwidth utilized by administratively defining traffic types. Policing enforces bandwidth to a specified limit. If applications try to use more bandwidth than that which is allocated, the traffic is dropped or remarked. Shaping, on the other hand, puts traffic into a buffer. This buffer can then utilize Queuing to prioritize data as it leaves the buffer.

The WRED (Weighted Random Early Detection) is a Queuing technology that can then be used to provide a congestion avoidance mechanism that will drop lower priority TCP data in an attempt to protect higher priority data from the adverse effects of congestion.

Finally, link-specific fragmentation and compression tools are often used on lower bandwidth WANs to ensure real-time applications do not suffer from high jitter and delay.

Table 1: Packet flow through a typical QoS policy.



LiveNX Overview

LiveNX is an application-aware network performance management platform that graphically displays how networks and applications are performing using SNMP and the latest advanced NetFlow capabilities now embedded in Cisco devices. In addition to showing application and network performance, LiveNX provides the ability to control application performance via its graphical QoS management capabilities. The next section will highlight how easily QoS can be configured to manage and control Webex media traffic. Moreover, this document will describe how the platform and tools can be used to confirm the application performance of Webex using the latest Medianet technology now available in some Cisco devices.

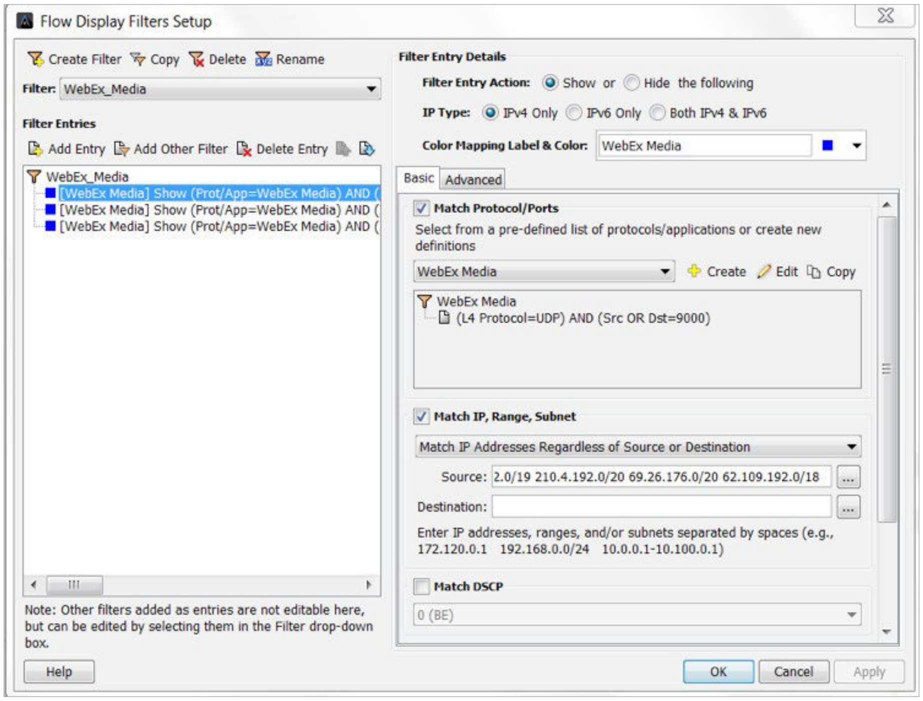
Using LiveNX to Identify Webex Traffic

The first step in deploying QoS for Webex is to validate the TCP and UDP port numbers that the Webex application will use. Webex media traffic can typically be easily identified as it defaults to using UDP 9000.

There are two primary ways LiveNX can be used to identify and monitor Webex traffic. These are often best used in conjunction:

1. Utilize a Filter — This filter should utilize both IP addresses/networks and ports.

- The port should be UDP 9000.
- The public IP addresses published for Webex conference servers are:
  - 64.68.96.0/19 66.114.160.0/20 66.163.32.0/19 173.39.224.0/19 173.243.0.0/20 207.182.160.0/19 209.197.192.0/19 216.151.128.0/19 114.29.192.0/19 210.4.192.0/20 69.26.176.0/20 62.109.192.0/18 69.26.160.0/20 64.68.96.0/19 66.114.160.0/20 66.163.32.0/19 173.39.224.0/19 173.243.0.0/20 207.182.160.0/19 209.197.192.0/19 216.151.128.0/19 114.29.192.0/19 210.4.192.0/20 69.26.176.0/20 62.109.192.0/18 69.26.160.0/20



Filter: WebEx_Media

Filter Entries

WebEx_Media
- [WebEx Media] Show (Prot/App=WebEx Media) AND (
- [WebEx Media] Show (Prot/App=WebEx Media) AND (
- [WebEx Media] Show (Prot/App=WebEx Media) AND (

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

Filter Entry Details

Filter Entry Action: ● Show or ○ Hide the following

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

Color Mapping Label & Color: WebEx Media

Basic | Advanced

☑ Match Protocol/Ports

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

WebEx Media

WebEx Media
(L4 Protocol=UDP) AND (Src OR Dst=9000)

☑ Match IP, Range, Subnet

Match IP Addresses Regardless of Source or Destination

Source: 2.0/19 210.4.192.0/20 69.26.176.0/20 62.109.192.0/18

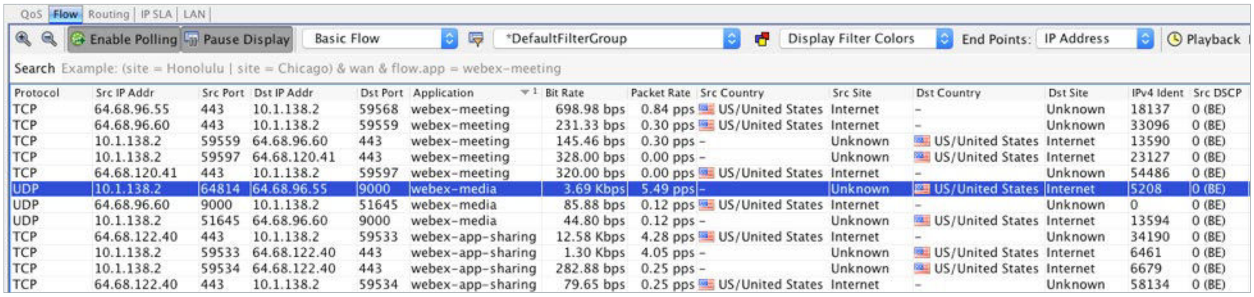
Destination:

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

☐ Match DSCP

0 (BE)

2. Utilize NBAR — Cisco has updated its NBAR2 application recognition technology to granularly recognize Webex media. By using NBAR2 protocol pack 28 (or higher) on the application Cisco routers and in LiveNX, it is possible to easily recognize and protect Webex traffic. Note the following screenshot of the raw Flow data being received from a Cisco router. The application column is populated via NBAR running on the router. Notice how the Cisco router is detecting different types of Webex traffic, specifically webex-media (udp 9000).

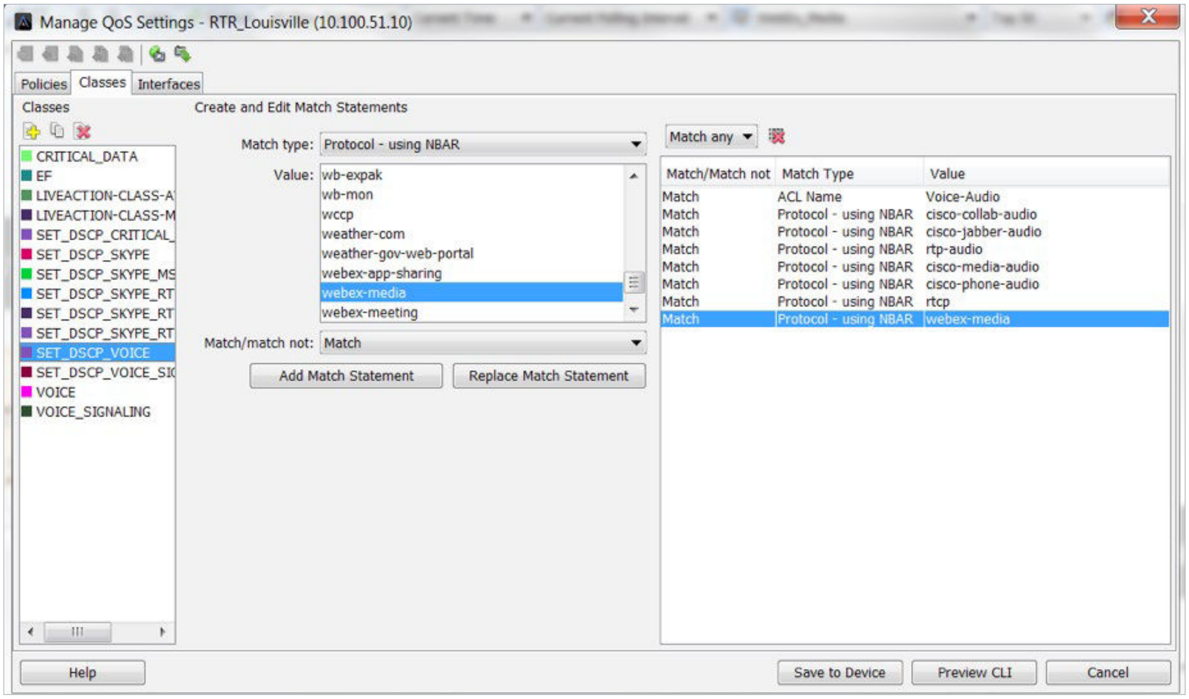


Search Example: (site = Honolulu | site = Chicago) & wan & flow.app = webex-meeting

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Bit Rate	Packet Rate	Src Country	Src Site	Dst Country	Dst Site	IPv4 Ident	Src DSCP
TCP	64.68.96.55	443	10.1.138.2	59568	webex-meeting	698.98 bps	0.84 pps	US/United States	Internet	-	Unknown	18137	0 (BE)
TCP	64.68.96.60	443	10.1.138.2	59559	webex-meeting	231.33 bps	0.30 pps	US/United States	Internet	-	Unknown	33096	0 (BE)
TCP	10.1.138.2	59559	64.68.96.60	443	webex-meeting	145.46 bps	0.30 pps	-	Unknown	US/United States	Internet	13590	0 (BE)
TCP	10.1.138.2	59597	64.68.120.41	443	webex-meeting	328.00 bps	0.00 pps	-	Unknown	US/United States	Internet	23127	0 (BE)
TCP	64.68.120.41	443	10.1.138.2	59597	webex-meeting	320.00 bps	0.00 pps	US/United States	Internet	-	Unknown	54486	0 (BE)
UDP	10.1.138.2	64814	64.68.96.55	9000	webex-media	3.69 Kbps	5.49 pps	-	Unknown	US/United States	Internet	5208	0 (BE)
UDP	64.68.96.60	9000	10.1.138.2	51645	webex-media	85.88 bps	0.12 pps	US/United States	Internet	-	Unknown	0	0 (BE)
UDP	10.1.138.2	51645	64.68.96.60	9000	webex-media	44.80 bps	0.12 pps	-	Unknown	US/United States	Internet	13594	0 (BE)
TCP	64.68.122.40	443	10.1.138.2	59533	webex-app-sharing	12.58 Kbps	4.28 pps	US/United States	Internet	-	Unknown	34190	0 (BE)
TCP	10.1.138.2	59533	64.68.122.40	443	webex-app-sharing	1.30 Kbps	4.05 pps	-	Unknown	US/United States	Internet	6461	0 (BE)
TCP	10.1.138.2	59534	64.68.122.40	443	webex-app-sharing	282.88 bps	0.25 pps	-	Unknown	US/United States	Internet	6679	0 (BE)
TCP	64.68.122.40	443	10.1.138.2	59534	webex-app-sharing	79.65 bps	0.25 pps	US/United States	Internet	-	Unknown	58134	0 (BE)

Using LiveNX to Implement QoS Markings on Webex Traffic

The LiveNX Engineering console has a QoS management GUI that allows users to visually manage QoS policies on several Cisco devices. You can create, edit and deploy QoS policies visually. The following screenshots show an example of adding the NBAR protocol match of "webex-media" to a class named SET_DSCP_VOICE. This class is setting the DSCP value of the "webex-media" to 46 (EF). The DSCP value used for Webex should always be chosen in accordance to any QoS configurations required by the Service Provider.



Classes

- CRITICAL_DATA
- EF
- LIVEACTION-CLASS-A
- LIVEACTION-CLASS-M
- SET_DSCP_CRITICAL_
- SET_DSCP_SKYPE
- SET_DSCP_SKYPE_MS
- SET_DSCP_SKYPE_RT
- SET_DSCP_SKYPE_RT
- SET_DSCP_SKYPE_RT
- SET_DSCP_VOICE
- SET_DSCP_VOICE_SI
- VOICE
- VOICE_SIGNALING

Create and Edit Match Statements

Match type: Protocol - using NBAR

Value: wb-expak, wb-mon, wccp, weather-com, weather-gov-web-portal, webex-app-sharing, webex-media, webex-meeting

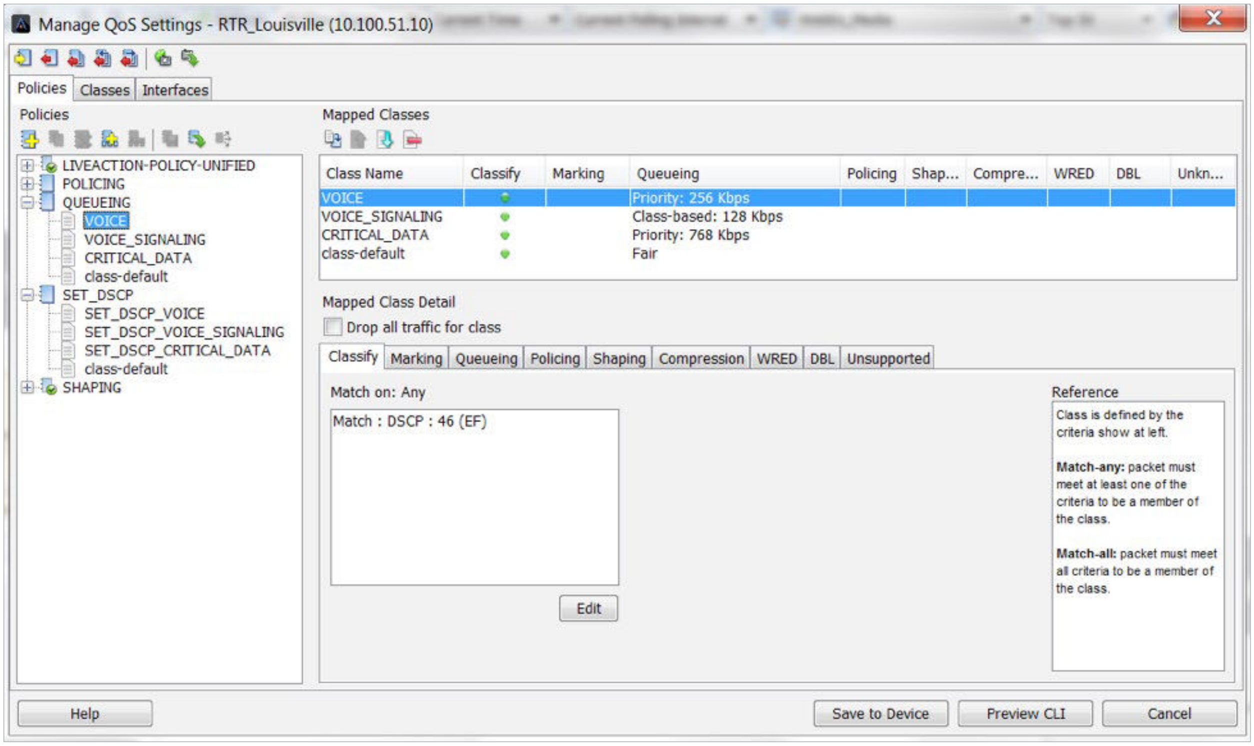
Match/match not: Match

Match any

Match/Match not	Match Type	Value
Match	ACL Name	Voice-Audio
Match	Protocol - using NBAR	cisco-collab-audio
Match	Protocol - using NBAR	cisco-jabber-audio
Match	Protocol - using NBAR	rtp-audio
Match	Protocol - using NBAR	cisco-media-audio
Match	Protocol - using NBAR	cisco-phone-audio
Match	Protocol - using NBAR	rtcp
Match	Protocol - using NBAR	webex-media

Using LiveNX to Prioritize Webex Communication at the WAN Edge

Webex traffic should be prioritized on the WAN edge. If Webex-media is matched and marked with the DSCP, it can then be easily prioritized utilizing traditional QoS configurations. Below is a screenshot of how this could be accomplished via the LiveNX GUI.



Manage QoS Settings - RTR_Louisville (10.100.51.10)

Class Name	Classify	Marking	Queueing	Policing	Shap...	Compre...	WRED	DBL	Unkn...
VOICE	●		Priority: 256 Kbps						
VOICE_SIGNALING	●		Class-based: 128 Kbps						
CRITICAL_DATA	●		Priority: 768 Kbps						
class-default	●		Fair						

Mapped Class Detail

☐ Drop all traffic for class

Match on: Any

Match : DSCP : 46 (EF)

Reference

Class is defined by the criteria show at left.

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

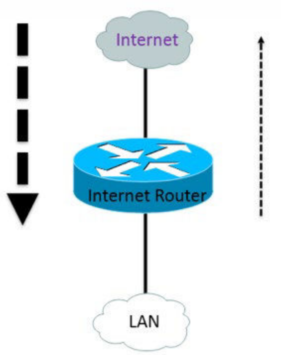
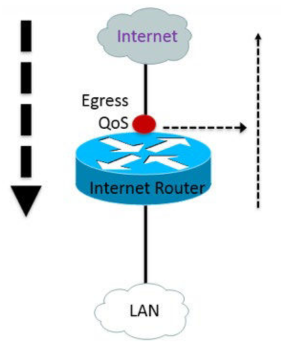
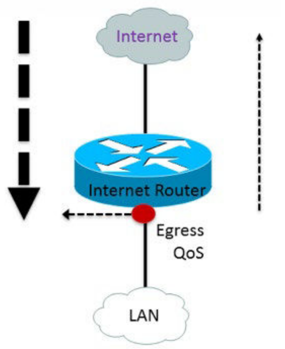
Match-all: packet must meet all criteria to be a member of the class.

All WAN devices should have an appropriate Shaping and Queuing configuration to prioritize traffic in accordance to any Service Provider requirements. Below is an example of a Cisco IOS configuration that uses a commonly used QoS configuration framework:

```
policy-map QUEUING
 class VOIP
  priority percent 20
 class VIDEO
   bandwidth percent 30
class MGMT_DATA
  bandwidth percent 5
 class CALL_SIGNALING
  bandwidth percent 5
 class CRITICAL_DATA
  bandwidth percent 10
 class class-default
   fair-queue
!
policy-map Internet_Shaping_2Mb
 class class-default
  shape average 2000000 20000 0
  service-policy QUEUING
!
interface GigabitEthernet0
description WAN-Interface
service-policy output Internet_Shaping_2Mb
```

Using LiveNX to Prioritize Webex Communication at the Internet Perimeter

One of the most important QoS considerations for protecting Webex traffic is prioritizing critical traffic on the Internet perimeter. Even though there is typically no QoS prioritization across the Internet itself, if the appropriate QoS configuration is implemented on the perimeter WAN router, excellent performance of real-time traffic like Webex can be achieved.

	On a typical Internet connection, the traffic being transmitted to the Internet is often much less than the traffic being downloaded from the Internet.
	The priority traffic being transmitted to the Internet (like Webex) can be prioritized with a QoS policy, like what would be utilized by a typical WAN router.
	The key to the successful protection of priority media applications, like Webex on the Internet, is controlling the other traffic being downloaded from the Internet. A very effective way to do this is by using a QoS policy on the egress of the Internet perimeter router's LAN interface. This QoS policy's Shaper is set to 95 percent of the targeted download bandwidth CIR. This policy works effectively for real-time, Internet-based traffic because most media is UDP-based, but most Internet traffic is TCP-based. When TCP becomes congested, it will limit its transmission rate via a windowing mechanism called Slow Start. By using a Shaper set to 95 percent of the target rate, the router becomes the logical congestion point of the circuit. The TCP traffic will be throttled effectively by the Shaper and the child Queuing policy will protect the priority UDP-based Webex media traffic.

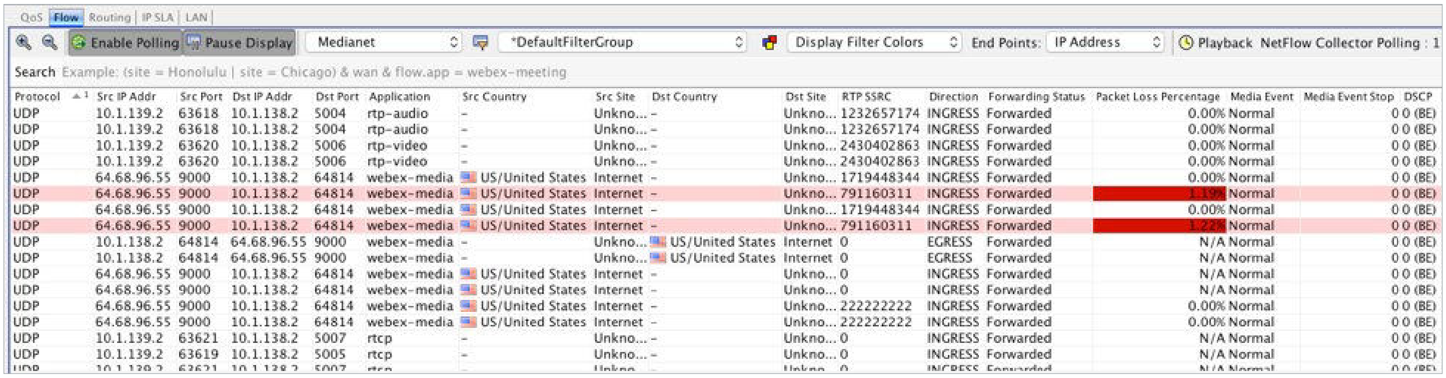
Below is an example of this type of a Cisco IOS QoS configuration placed on the Internet perimeter router’s LAN interface. This policy is very similar to that of a traditional WAN egress policy. However, this policy is set in the outbound direction of the LAN interface, and the shaper is set to 95 percent of the bandwidth of the target download CIR.

```
policy-map QUEUING
 class VOIP
  priority percent 20
 class VIDEO
   bandwidth percent 30
class MGMT_DATA
  bandwidth percent 5
 class CALL_SIGNALING
  bandwidth percent 5
 class CRITICAL_DATA
  bandwidth percent 10
 class class-default
   fair-queue
!
policy-map RIS_Shaping_2Mb
 class class-default
  shape average 1900000 19000 0 !← 95%
   service-policy QUEUING
!
interface GigabitEthernet1
Description LAN-Interface
service-policy output RIS_Shaping_2Mb
```

Using LiveNX to Monitor Webex Performance Traffic

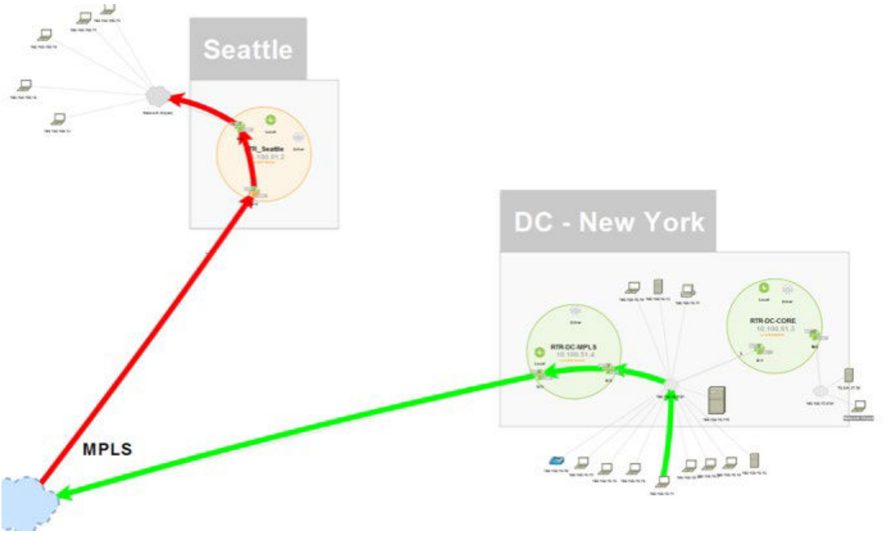
LiveNX takes advantage of Cisco’s Performance Monitor feature. Performance Monitor tracks jitter and packet loss of voice and video over IP. Since Webex is encapsulated as RTP, Performance Monitor can track it as well. LiveNX will collect the Performance Monitor statistics via NetFlow and can then report, visualize and alert when there are problem calls.

Below is a screenshot showing the ‘webex-media’ conversation experiencing an issue with packet loss.



Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	Src Country	Src Site	Dst Country	Dst Site	RTP SSRC	Direction	Forwarding Status	Packet Loss Percentage	Media Event	Media Event Stop	DSCP
UDP	10.1.139.2	63618	10.1.138.2	5004	rtp-audio	-	Unkno...	-	Unkno...	1232657174	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	10.1.139.2	63618	10.1.138.2	5004	rtp-audio	-	Unkno...	-	Unkno...	1232657174	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	10.1.139.2	63620	10.1.138.2	5006	rtp-video	-	Unkno...	-	Unkno...	2430402863	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	10.1.139.2	63620	10.1.138.2	5006	rtp-video	-	Unkno...	-	Unkno...	2430402863	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	1719448344	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	791160311	INGRESS	Forwarded	1.19%	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	1719448344	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	791160311	INGRESS	Forwarded	1.22%	Normal		0 0 (BE)
UDP	10.1.138.2	64814	64.68.96.55	9000	webex-media	-	Unkno...	US/United States	Internet	0	EGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	10.1.138.2	64814	64.68.96.55	9000	webex-media	-	Unkno...	US/United States	Internet	0	EGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	0	INGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	0	INGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	222222222	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	64.68.96.55	9000	10.1.138.2	64814	webex-media	US/United States	Internet	-	Unkno...	222222222	INGRESS	Forwarded	0.00%	Normal		0 0 (BE)
UDP	10.1.139.2	63621	10.1.138.2	5007	rtcp	-	Unkno...	-	Unkno...	0	INGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	10.1.139.2	63619	10.1.138.2	5005	rtcp	-	Unkno...	-	Unkno...	0	INGRESS	Forwarded	N/A	Normal		0 0 (BE)
UDP	10.1.139.2	63621	10.1.138.2	5007	rtcp	-	Unkno...	-	Unkno...	0	INGRESS	Forwarded	N/A	Normal		0 0 (BE)

The following is a Performance Monitor visualization showing the hop-by-hop performance of a call. In this example, the call began well (green), but its performance was degraded by the MPLS provider (red). The routers detected this and sent that information via NetFlow.



More Information

Visit our website:
https://www.liveaction.com/solutions/qos-monitoring-control
Find out more about Cisco QoS including best practices, the latest tools for monitoring and creating new policies, and a schedule for QoS webinars.

Get a copy of our complete QoS Handbook:
https://www.liveaction.com/resources/white-papers/cisco-qos-handbook
Follow the above link if you want additional copies or printable PDF versions of this document.

Download a trial edition of LiveNX:
www.liveaction.com/download
Register for a free trial download of LiveNX for monitoring and configuring Cisco QoS. Be sure to check often for periodic specials including free licenses on selected items.

About LiveAction

LiveAction simplifies the management of complex networks by providing real-time visualization and analytics for SD-WAN, Voice, Video, and Quality of Service monitoring. Our platforms are LiveNX™ designed for large enterprises and LiveSP™ designed for Service Providers. Savvius, a LiveAction company, offers Omnipliance and Omnipeek for powerful packet capture and analytics, providing the unparalleled visibility needed to anticipate and resolve network performance issues. Learn more at www.liveaction.com. Follow us on Twitter, Facebook, and LinkedIn.

LiveAction
3500 West Bayshore Rd
Palo Alto, CA 94303

Phone + eFAX: +1 888-881-1116
Email: sales@liveaction.com
Website: www.liveaction.com

© 2018 LiveAction, Inc. All rights reserved. LiveAction, the LiveAction logo and LiveAction Software, LiveNX, LiveSensor, LiveInsight, and LiveUX are trademarks of LiveAction, Inc. Information subject to change without notice.