End-to-End QoS for Video Across the Cambium Wireless Fabric

AS MORE PEOPLE WORK, LEARN AND RECREATE FROM HOME, IT IS ESSENTIAL THAT NETWORKS SUPPORT A HIGH-QUALITY END USER EXPERIENCE.

Introduction

THE YEAR 2020 brought about many changes due to the impact of COVID-19. A key change has been a shift from in person to remote functioning. Working and learning remotely, or virtually, has become the new normal for many. These changes have had a significant impact on day-to-day communications and collaboration. Video conferencing applications such as Zoom, Google Meet, Webex and Microsoft Teams have risen to the task as key tools in enabling remote operation, resulting in an explosion in video conferencing traffic on networks. In many cases, businesses and schools use three or more different video conferencing platforms to address all their needs.

A Cambium survey of US K-12 education CIOs highlights the heavy use of these applications.

Video Conferencing Apps in Use

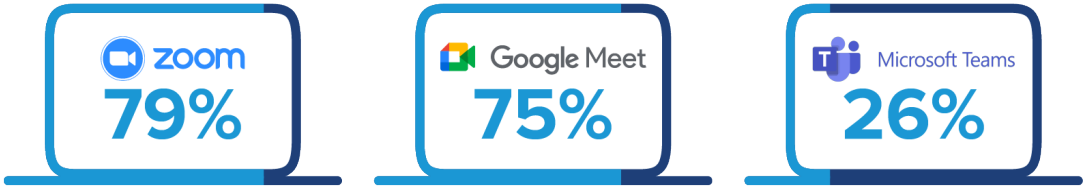


Figure 1. Most used video conferencing apps in US K-12, November 2020

According to research from Forbes:

- Zoom had over 300 million meeting participants per day in 2020
- Google Meet had over 100 million meeting participants per day in 2020
- Microsoft Teams had over 75 million active daily users in 2020
- Cisco Webex currently has over 300 million users

Businesses and employees benefit from the use of video conferencing, with estimates of $11,000 annual savings per employee by having a remote work force that uses video conferencing. Employees are also saving money and time by telecommuting to the office. Travel costs have been reduced by 30% or more, and the need for business travel has been reduced by 47%. (Stone, K. The State of Video Conferencing in 2020 [50 Statistics] | GetVoIP)

It is imperative that the video conferencing applications perform at a higher level to deliver a good Quality of Experience to the end-user. This application note will introduce the concepts of Quality of Experience, the system and network influence factors related to the end-user Quality of Experience, why they are important for video conferencing, and how Cambium solutions can be set up to ensure quality video performance over a wireless fabric.

Impact of Collaboration and Video Conferencing Tools on Wi-Fi Networks

WITH BUSINESSES AND SCHOOLS relying heavily on team collaboration and video conferencing platforms, it can present a challenge for IT administrators as they are required to support this new critical dynamic in network traffic. Left unchecked, video conferencing applications compete with traditional business applications such as email, productivity applications, SaaS and in-house applications for bandwidth. To ensure high quality video and audio for all users will require an understanding of factors which affect the quality of a conference call. Network administrators will rely on network management systems and tools to gain visibility in traffic flows and then be able to detect bottlenecks and manage network traffic to ensure high performance of the video conferencing apps.

How Latency, Jitter, and Packet Loss Impact the Client Experience

THERE ARE SEVERAL NETWORK METRICS that impact the quality of the video conference experience, including latency, jitter, and packet loss. The quality of a video conference will degrade if the network cannot provide an appropriate level of service for these parameters.

Latency is the time it takes a data packet to travel from a sender to a receiver on a network. Each step the data packet takes through the network adds time to the latency. When network path latency occurs, performance will be affected. On a video conferencing call, high latency can cause the audio and video to become out of sync, giving the effect of a poorly dubbed foreign film.

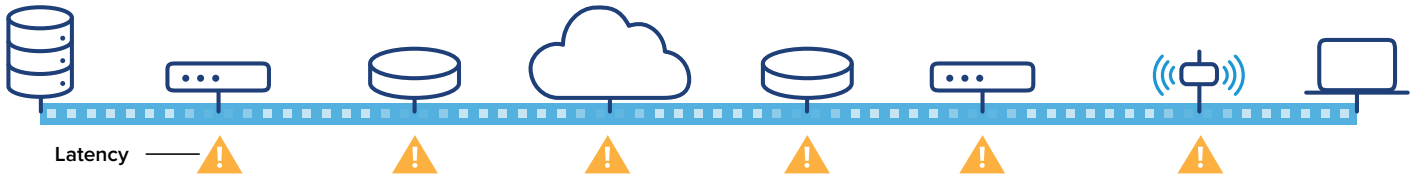


Figure 2. Latency is added at every network device.

Jitter is the variation in how much time (latency) a data packet takes to travel from sender to receiver. Many factors such as poor hardware performance, not enough bandwidth, and not implementing packet prioritization can cause some packets to take longer to travel across the network than other packets, increasing jitter and decreasing the quality of a video conference call.

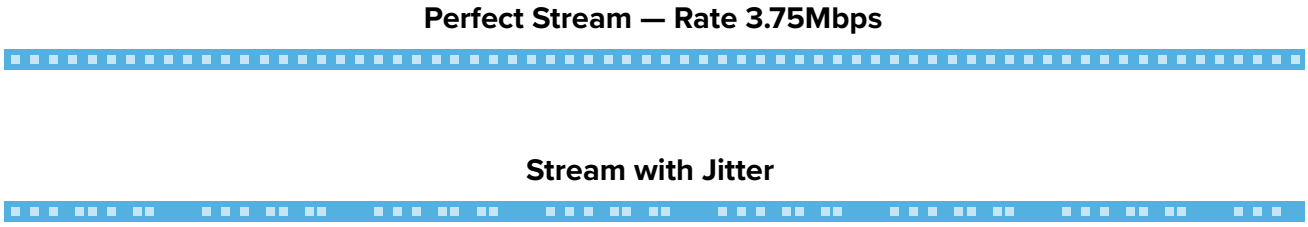


Figure 3. Jitter

Packet loss occurs when one or more data packets travelling across a network fail to reach their destination. Packet loss is usually caused by errors in data transmission, network congestion and/or problems with network hardware. When packet loss percentages in a video conference call exceed 2.5%, the end user experience will degrade.

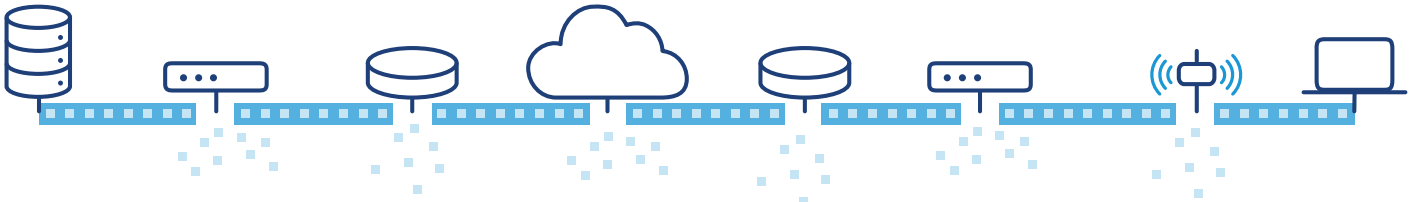


Figure 4. Packet Loss

To achieve a good quality of experience during a video conference call, network latency should not surpass 150ms one way and 300ms round trip. Jitter should be below 30ms, and packet loss should be below 1%. If network latency rises above 250ms, or jitter is above 30ms or packet loss is above 2%, the quality of experience will suffer and will be very noticeable to the end user.

Optimizing Video Conferencing Network Traffic - QoS / DSCP

WHEN OPTIMIZING VIDEO CONFERENCNG network traffic, network administrators not only need to consider factors such as network bandwidth, network congestion, and network hardware resources, all of which will have an effect on quality of experience, they must also consider other network traffic that the video conferencing traffic will have to contend with.

Left unchecked, recreational applications like video streaming services (Netflix & Hulu) and file transfer services (BitTorrent & Dropbox) and online video games will consume network bandwidth and will likely have a negative effect on business applications such as video conferencing. Using Application Policies and Deep Packet Inspection in XMS-Cloud, Network administrators can identify and assign a higher QoS or DSCP value to video conferencing traffic at the Wi-Fi access point, ensuring that this traffic gets a higher priority, thus eliminating any additional latency that may be caused by queueing due to other applications.

If QoS is implemented, as packets leave the AP, they are 802.1p tagged with a QoS value. When the return traffic comes into the AP from the wired network, they are prioritized and sent out on the wireless network according to the QoS value.

If DSCP is implemented, as packets leave the AP, they are 802.1p tagged with a DSCP value. This value prioritizes the packet as it goes through your LAN devices network devices such as switches and routers. When the return traffic comes back through the router, the DSCP values are reassigned (as they have probably been dropped as the packet has traveled through the cloud), and the packet is prioritized as it goes through switches, into the AP and onto the wireless network.

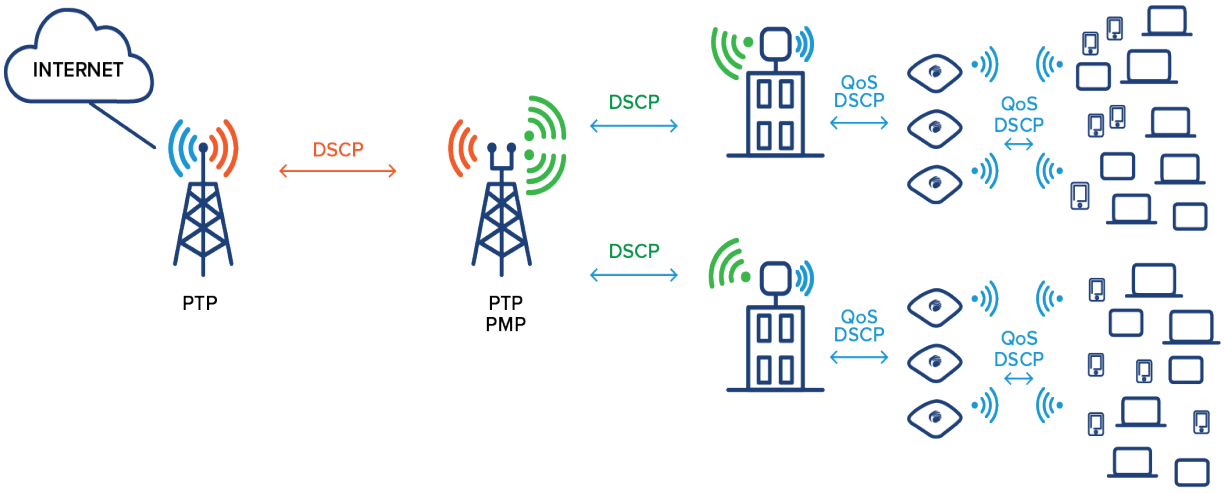


Figure 5. QoS & DSCP through the network

Network Management System

THE NETWORK MANAGEMENT SYSTEM (NMS) is a crucial component in the overall quality of experience for video conferencing calls. The NMS will provide for device discovery, automate device configuration and provisioning, device monitoring, network performance monitoring and analytics, reporting, notifications and automated alerts. Cambium Networks Enterprise Management System, XMS-Cloud, provides all this plus the capability of configuring QoS and DSCP for over 2,400 applications. This next section covers how to configure QoS and DSCP for video conferencing applications such as Zoom and Microsoft Teams.

Configuring QoS / DSCP Values in XMS-Cloud

CAMBIUM NETWORKS' XMS-CLOUD management system provides tools to assist the network administrator in mitigating latency, jitter and packet loss across the Wi-Fi network.

SSIDs

SSIDs CAN BE ASSIGNED a separate QoS priority from 0 – 3, where 3 is the highest and 2 is the default.

Application Control

APPLICATION CONTROL POLICIES ALLOW you to assign QoS or DSCP values to prioritize specific application traffic such as Zoom, Microsoft Teams, or Webex, to enhance the quality of the application performance.

QoS

QoS VALUES RANGE FROM 0 – 3, with 0 being the lowest priority and 3 being the highest priority. If you configure a QoS for an application, as upstream traffic leaves the access point, it is assigned a priority tag and receives priority as it passes through network appliances such as switches and routers on its way to the internet.

When downstream internet traffic enters your network through the router, the incoming packets are assigned a priority based on their SSID or priority tag. Higher priority traffic will have a shorter wait time before gaining access to the air.

DSCP

DIFFERENTIATED SERVICES CODE POINT (DSCP) is a value (0 – 64) assigned to specified network traffic allowing networking equipment to prioritize traffic based on the DSCP value. Assigning a higher DSCP value to video conferencing traffic will eliminate additional latency as the traffic will always be placed at the front of the queue as it passes through network routers, switches and Wi-Fi access points. By default, DSCP 48 is used for voice traffic and is set to QoS level 3 – the highest level.

Set Up Zoom Application QoS / DSCP Policies in XMS-Cloud

OPEN an existing Profile and go to the Policies page.

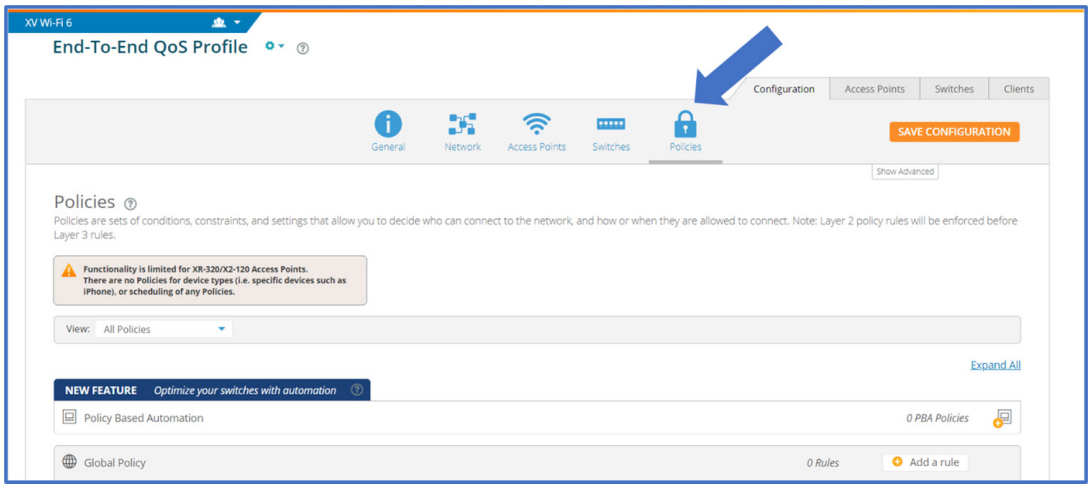


Figure 6. Go to the Policies page in the Profile.

To create an **SSID Policy**, click **New SSID Policy** button, click the SSID dropdown box and select the SSID you will create the QoS policy for. Click the **Create Policy** button.

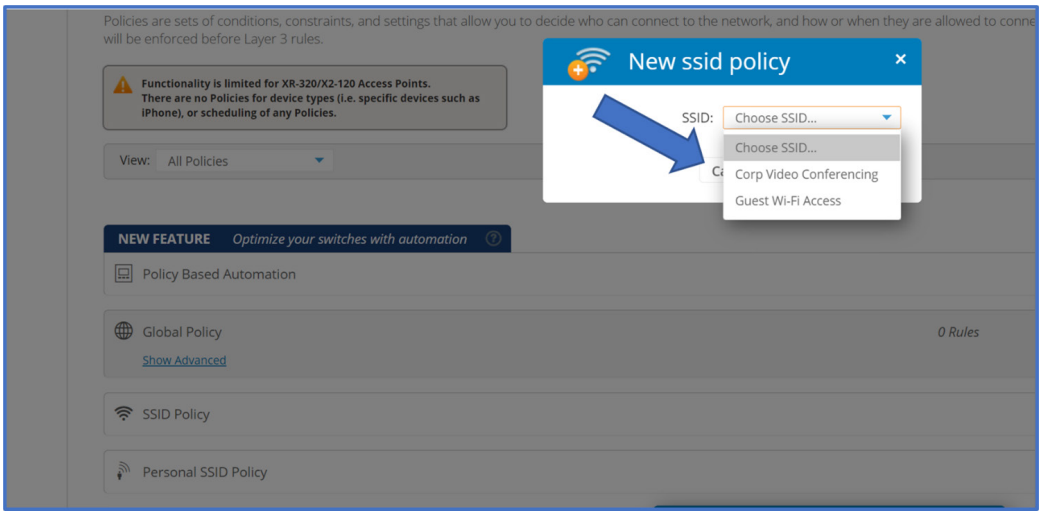


Figure 7. Create new SSID policy.

To add a **Policy rule**, on the new SSID Policy that you just created, click the **Add a rule** button.

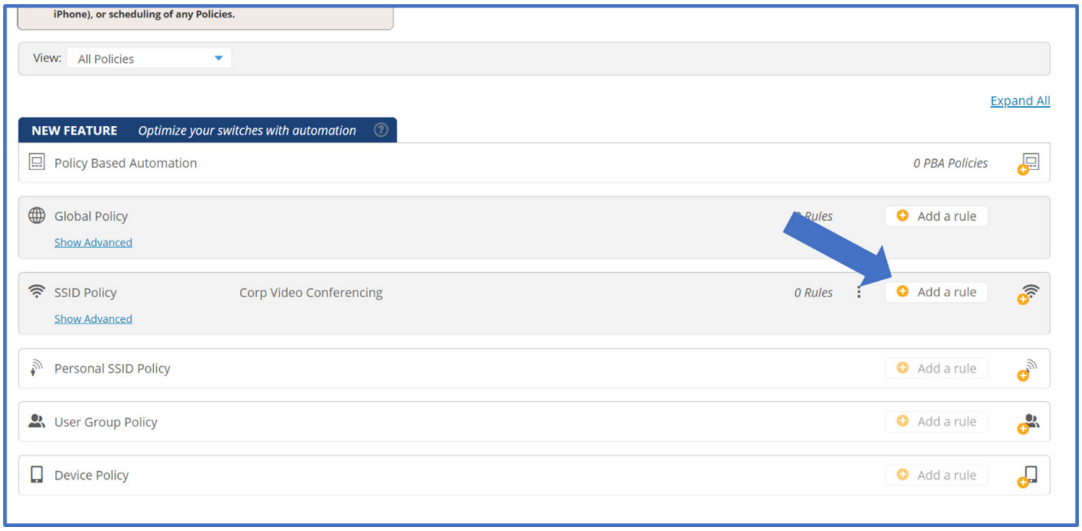


Figure 8. Add a rule

Click the **Application Control** button, then for **Action**, select **Allow**.

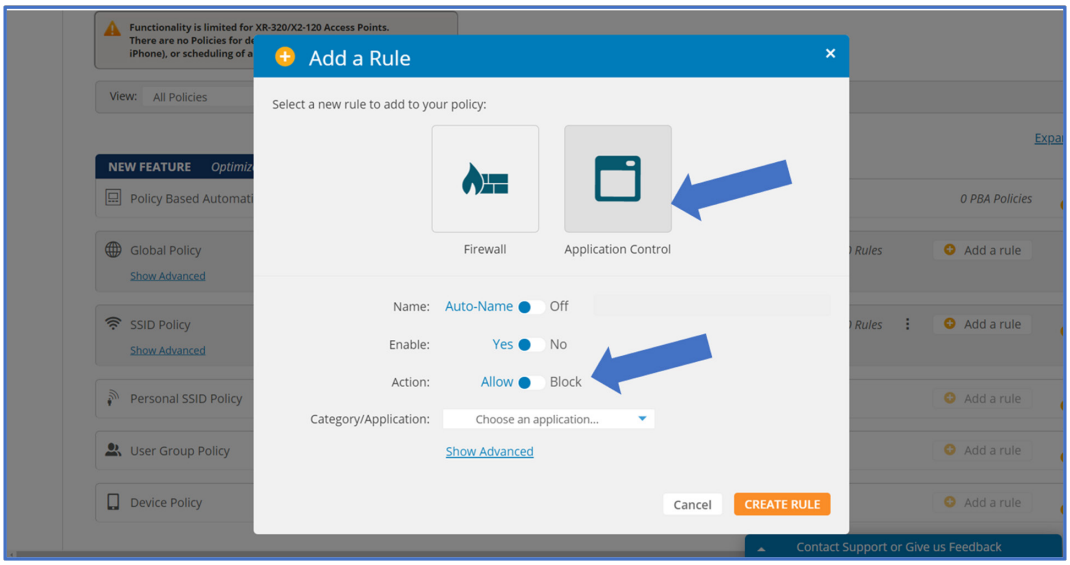


Figure 9. Create Applcation Policy rule.

For **Category/Application**, select **Zoom**.

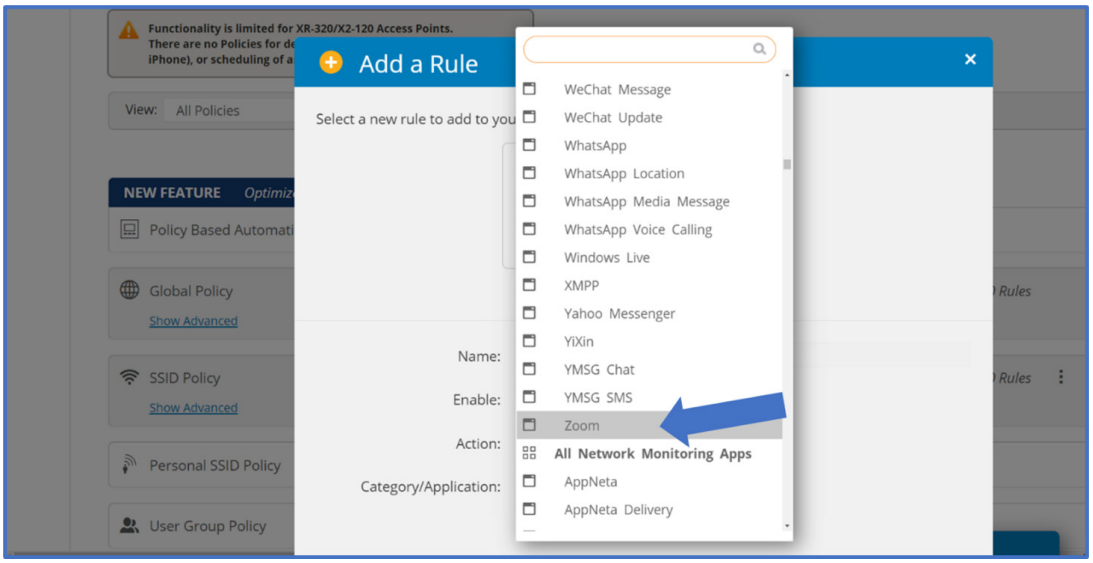


Figure 10. Select Zoom application.

Click the **Show Advanced** link. To configure a QoS setting, for **QoS**, enter **3** for the highest QoS priority.

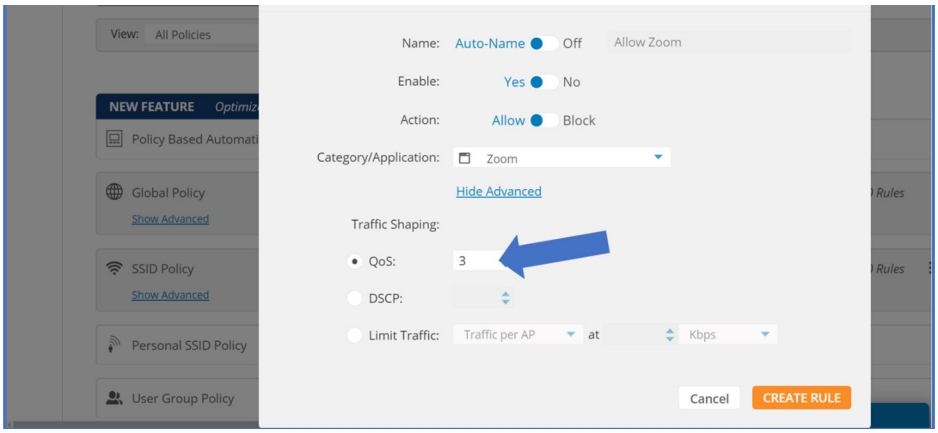


Figure 11. Set QoS level to "3"

Or to configure a **DSCP** priority, select the DSCP radio dial and enter **56**, which is the Zoom recommended setting for audio.

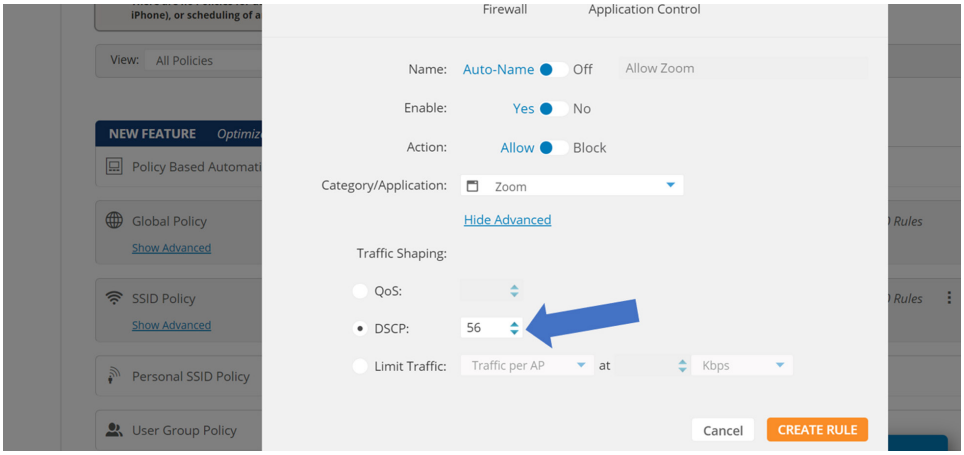


Figure 12. Set DSCP value to "56"

Optimizing Traffic on the Cambium PMP / PTP 450

DSCP TAGGED TRAFFIC from the Wi-Fi access point makes it simple for Cambium PMP/ PTP 450 devices to identify and prioritize this traffic via existing DiffServ to ToS mapping.

But then a new problem arises in that this only solves prioritizing the traffic in the upstream direction. When the return downlink traffic comes, the DSCP is generally stripped during route through the cloud, and being 0, will default to lowest priority in the downlink over the RF link. This means that general user traffic can greatly impact the quality of the video and audio of the meeting.

To solve this, we have implemented a feature on the upstream device (which is the AP in the PMP system) to track these data flows in the upstream and properly re-apply the DSCP in the downstream before forwarding packets over the RF with proper prioritization. With this in place, we now can have end to end Cambium prioritization solution with Cambium XV and XD access points starting the identification and PMP 450 / PTP 450 keeping the proper priority in place in both directions.

The feature was made as generic as possible so as to not be specific to "Zoom Meetings". The same problem can apply to many other traffic flows, including other video conferencing solutions such as MS Teams and Webex. Since the 450 implementation relies on DSCP, it is up to a device beneath the SM device to get the traffic onto a known DSCP before sending into our SM.

Please note that this feature is closely related to both DiffServ as well as each SM's number of enabled Data channels. While this feature allows for setting Low, Medium, High and Ultra High options, it will only work if the proper number of data channels are configured. Otherwise, the QoS to Data Channel mapping will operate in the same way it does today with mapping of ToS to Data Channels:

Priority Levels Enabled	ToS to Data Channel Mapping
1	ToS 0-7 → single, Low priority DC
2	ToS 0-3 (Low and Medium) → Low DC, ToS 4-7 (High and Ultra High) → High DC
3	ToS 0-1 (Low) → Low DC ToS 2-3 (Medium) → Medium DC ToS 4-7 (High and Ultra High) → High Priority DC
4	ToS 0-1 (Low) → Low DC ToS 2-3 (Medium) → Medium DC ToS 4-5 (High) → High Priority DC ToS 6-7 (Ultra High) → Ultra High DC

Figure 13. ToS to enabled Data Channel mapping in PMP 450 / PTP 450

Technical Description

THE FEATURE HAS TWO IMPLEMENTATIONS depending on whether it is a PMP or PTP link. As it is a pure SW feature, it is supported on all 450 HW variants. The implementation between PMP and PTP are extremely similar with some key differences that affect what devices are performing certain roles. For PMP, there is a definite presumed assumption of what constitutes the "Uplink" direction. This is always going to be the Access Point. In order to allow the most flexibility of our customers to fine tune this, in the PMP setup, the configuration for this feature is done on the SM's QoS page and the actual tracking and restoring of DSCP per configured stream is handled on the AP.

For PTP, there is no assumption that can be made about which end of the link is in the "Uplink" direction. A valid installation scenario may be as shown below, where the BHS is actually the "Upstream" device. In order to support this, the configuration is always done on the BHM device, but there is an additional configuration item called "Role" in which the user will have to state what side of the link which the BHM operates, either Upstream or Downstream. For PTP, the Upstream device will handle the tracking and restoring of DSCP per configured stream. So, it follows that on PTP, you may have the configuration AND tracking operation handled both on the BHM if that is the Upstream device.

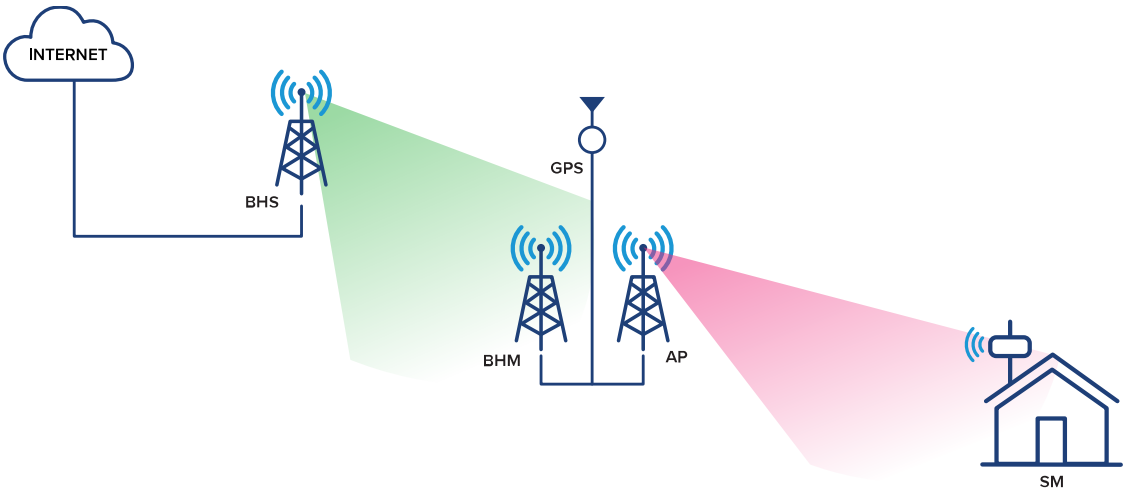


Figure 14. DSCP flow on PMP 450 / PTP 450 devices

In this figure, the configuration would be done on the BHM and the SM while the BHS and AP would handle the tracking and restoration of DSCP. Upstream direction is from the house to the Internet while Downstream is from Internet to the House.

Flow

The traffic flow and feature operation are as follows:

1. Traffic enters the PMP SM already marked on a specific targeted DSCP, such as 45. The PMP SM has been configured to prioritize DSCP 45 at a "High" priority level. The default mapping of DSCP 45 is 1, which normally would be mapped to the Low priority Data channel. But due to this configuration, IPv4 traffic matching DSCP 45 will be routed to the High Priority channel.
2. Traffic enters the PMP AP on High Priority channel. Since 45 is configured to be tracked, the AP collects information about the stream including Source LUID, Source IP, Destination IP, Protocol, Source Port, and Destination Port. These properties are captured and stored for return traffic analysis.
3. Traffic enters the BHM. The PTP BHM has been configured to track DSCP 45 and play the "Downstream Role". The BHM sends the traffic up to the BHS over the High Priority Data Channel.
4. Traffic enters the BHS. Since the BHS is the "Upstream" PTP role device, it performs the same operation as the PMP AP did, tracking the DSCP 45 traffic with the same information, Source LUID (For BHM this will always be the RF LUID), Source IP, Destination IP, Protocol, Source Port, and

Destination port.

5. Traffic leaves the BHS still with DSCP 45 to the “Internet”
6. Traffic processed by end destination and return traffic generated, most certainly with DSCP set to 0.
7. Traffic enters the BHS in the downstream direction with DSCP 0. Since BHS is the Upstream Role, it analyzes the traffic to see if it matches the stored tuple, except in reverse direction.
8. If there is a match, the BHS places the traffic onto DSCP 45 by updating the IP header and adjusting the IP and packet checksums
9. Traffic is now sent to BHM via High Priority Data Channel
10. Traffic enters PMP AP. Since it has already been put on DSCP 45 by the BHM, the PMP AP doesn’t have to do anything involving a lookup, it forwards the traffic to the SM via the High Priority data channel as defined by the configuration.
11. Traffic enters PMP SM and is sent into the House network.

Note that if there is no PTP link with this feature above the PMP AP, then in Step 10, the AP will perform the lookup and packet modification that the BHS did in Step 7.
Without this feature, the downstream direction would have all been using Low Priority channel as the return traffic DSCP will typically come in as 0 and map to the low priority data channel.

Configuration

THE CONFIGURATION OF THIS FEATURE, as mentioned before is on the PMP SM and PTP BHS with a minor difference being that the PTP has an additional option called “Role” for the BHM device to play.

PMP Configuration:

The PMP Configuration is found on the SM’s Configuration ➔ DiffServ page

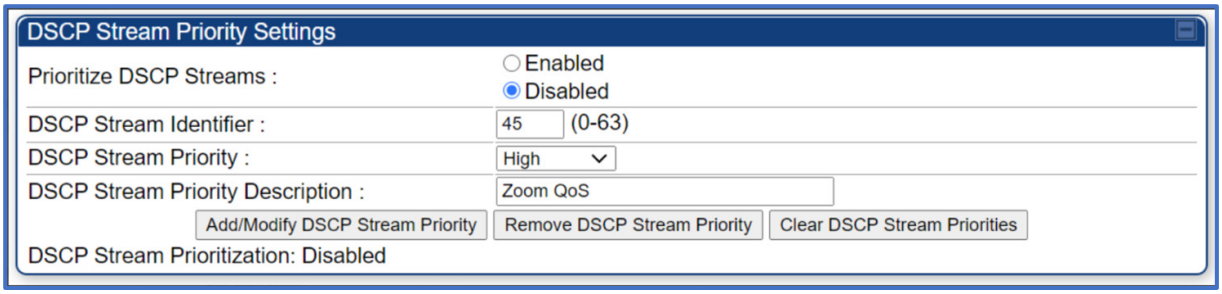


Figure 15. DSCP stream priority settings

The first option is the enable/disable the feature for this SM’s link. This option is controlled by the overall DiffServ page’s “Save Changes” button. To configure specific mappings, the next 3 entries are used as well as the associated buttons.

To add a new, or modify an existing, mapping, enter the values in the boxes and click the Add/Modify DSCP Stream Priority button. Adding DSCP 45, for High, for “Zoom Meetings” will look like this:

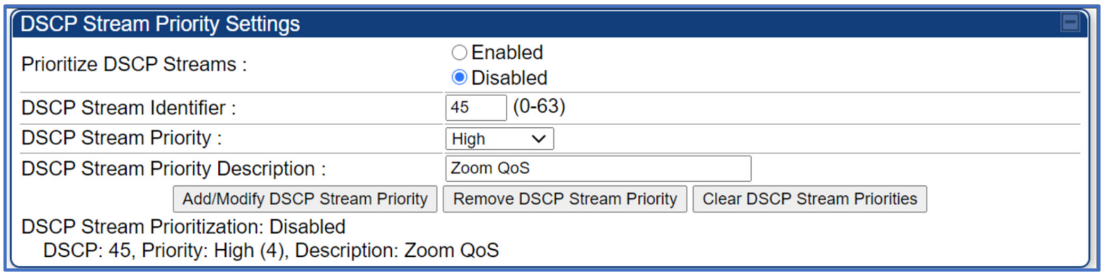


Figure 16. Add/Modify DSCP stream priority

To modify this to change the priority or the description, make the change and use the Add/Modify DSCP Stream Priority button again:

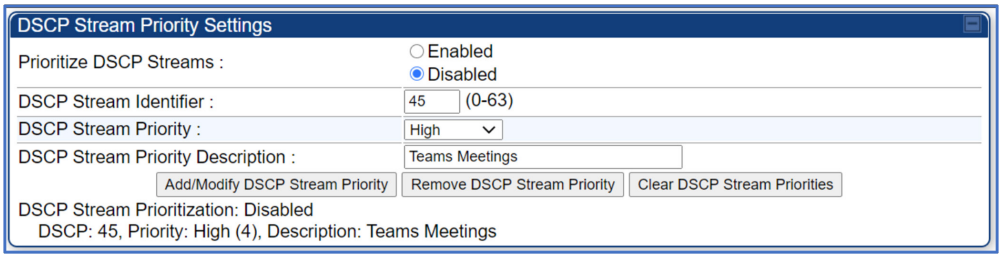


Figure 17. Modify priority

Note that up to 10 entries can be configured per SM and the Description field can be up to 32 characters long.

To remove a mapping, simply enter the DSCP (other options don't matter) and click the "Remove DSCP Stream Priority button.
To clear all entries, just press the "Clear DSCP Stream Priorities button.

The SM's configuration is sent to the AP at registration time as well as any time that there is a change made to the configuration. There is no Reboot Required when making changes to this configuration. The configuration will be seen on the AP's DiffServ page, grouped per SM, to note that there is an overlay being used for a particular SM link:

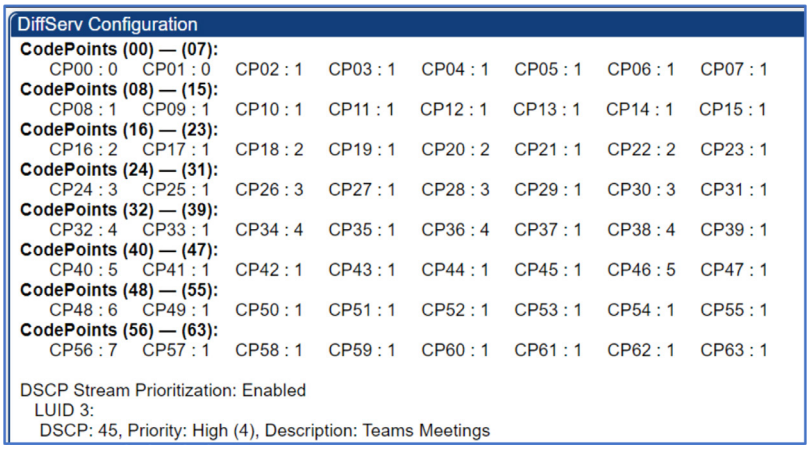


Figure 18. AP DiffServ configuration page

If there were multiple SMs with this feature enabled, each of them would show up on this page. And you can have different Priorities for each SM even on the same DSCP.

Also, on the PMP AP, since it is the Upstream Device, you can see the captured Tuples of a tracked stream. This can be found on the new Logs ➔ DSCP Priority Streams page.

Here is an example of a Zoom Meeting being tracked and prioritized:

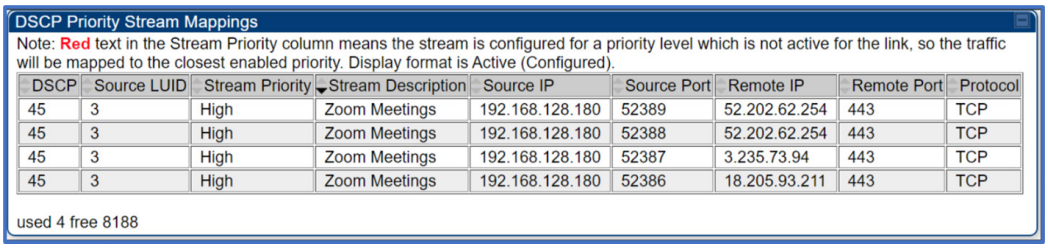
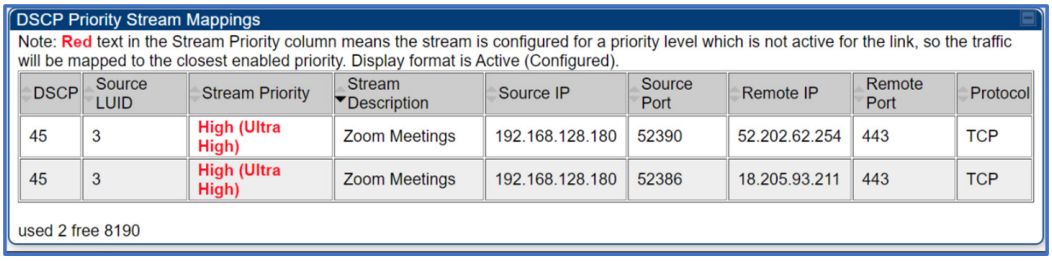


Figure 19. Tracking a Zoom call

You can see here, all of this data is for LUID 3 DSCP 45, for our “Zoom Meetings” stream. All of this is from the same Source IP (my iPad), but using different source ports and remote IPs, and a mixture of TCP and UDP traffic. This view is with “admin” login. With “engineering” login, we show a few more columns which will be covered below. By default, each entry will timeout after 5 minutes of inactivity at which point, it will need to be relearned in the uplink in order to be properly handled in the downlink.

Also, please note the “Stream Priority” column along with the Note above the table. As was mentioned earlier, the configuration of this feature allows setting of all 4 possible QoS levels, Low, Medium, High, and Ultra High. However, on PMP Canopy systems, all of these channels may not be present when the SM is in session, depending on the configuration of the device. If there is a mismatch from the config to what Priority channels are actually available, the data will be mapped as described above and the page will look similar to this:


DSCP Priority Stream Mappings

Note: Red text in the Stream Priority column means the stream is configured for a priority level which is not active for the link, so the traffic will be mapped to the closest enabled priority. Display format is Active (Configured).

DSCP	Source LUID	Stream Priority	Stream Description	Source IP	Source Port	Remote IP	Remote Port	Protocol
45	3	High (Ultra High)	Zoom Meetings	192.168.128.180	52390	52.202.62.254	443	TCP
45	3	High (Ultra High)	Zoom Meetings	192.168.128.180	52386	18.205.93.211	443	TCP

used 2 free 8190

Figure 20. DSCP priority mappings

As you can see here, I have changed the configuration of the stream to Ultra High, but that QoS level is not available, as this link only has 2 QoS levels, Low and High. So, this “Ultra High” traffic is actually going over the “High” priority channel.

A good way to track the operation of this feature is to use the Statistics ➔ Data Channels page to see traffic on the desired priority level in both directions, and then changing the configuration on the fly to watch the traffic move to different priority levels. With this method, it is very easy to see the priority channel change as the configuration changes with constant DSCP uplink marked traffic.

PTP Configuration

FOR PTP MODE, THE OPERATION and GUI is the same except that the Configuration is on the PTP BHM always and has an extra configuration item called “Role.” The DSCP Streams Priority Mappings Log page will be on the “Upstream” Role Device; think of the PTP “Upstream” Role Device as acting like the PMP AP and the PTP “Downstream” Role Device acting as the PMP SM as far as the feature operation is concerned. The configuration for this will be found on the PTP BHM Configuration ➔ DiffServ page.

PTP Configuration Example: In this example, the BHM is the “Downstream” device.

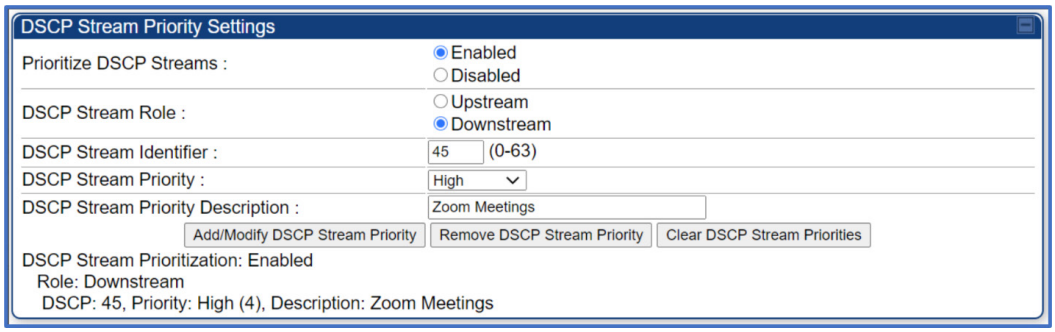
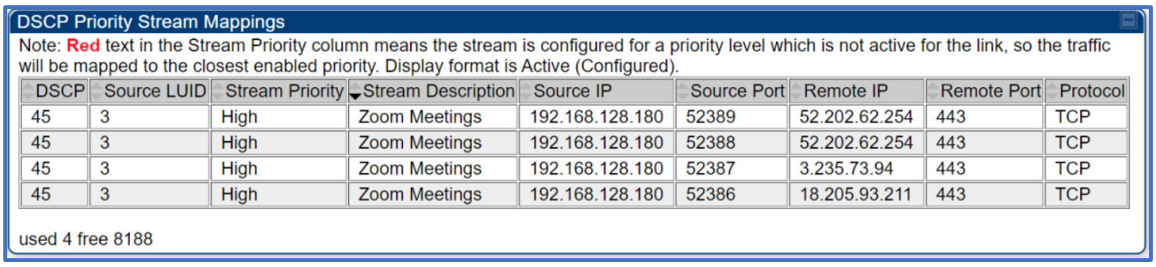


Figure 21. DSCP priority settings in the BHM

And in this case, the BHS will be the "Upstream" device and thus, will contain the Logs ➔ DSCP Priority Streams tracking table, which will look the same as the PMP AP:



DSCP Priority Stream Mappings

Note: **Red** text in the Stream Priority column means the stream is configured for a priority level which is not active for the link, so the traffic will be mapped to the closest enabled priority. Display format is Active (Configured).

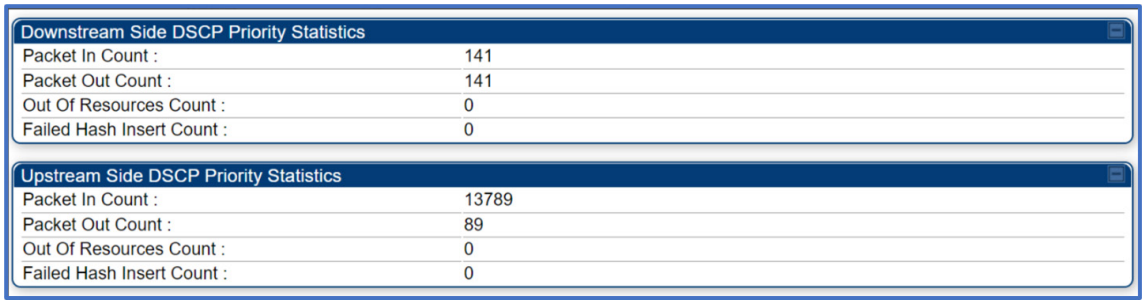
DSCP	Source LUID	Stream Priority	Stream Description	Source IP	Source Port	Remote IP	Remote Port	Protocol
45	3	High	Zoom Meetings	192.168.128.180	52389	52.202.62.254	443	TCP
45	3	High	Zoom Meetings	192.168.128.180	52388	52.202.62.254	443	TCP
45	3	High	Zoom Meetings	192.168.128.180	52387	3.235.73.94	443	TCP
45	3	High	Zoom Meetings	192.168.128.180	52386	18.205.93.211	443	TCP

used 4 free 8188

Figure 22. DSCP priority settings in the BSM

Statistics and Extra Mapping Data - Engineering User Display

There is a page for engineering user to track statistics for packets processed as well as any issues with using the tracking table. You can find them in Statistics ➔ DSCP Priority Stats, and it simply tracks packets in and out of each direction as well as any errors acquiring resources for tracking. Those resource counters should only increment if the table gets full. This is only available to engineering user for now:



Downstream Side DSCP Priority Statistics

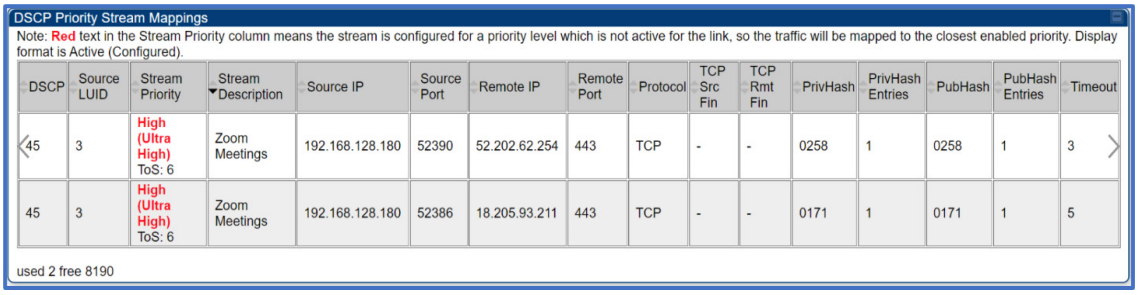
Packet In Count :	141
Packet Out Count :	141
Out Of Resources Count :	0
Failed Hash Insert Count :	0

Upstream Side DSCP Priority Statistics

Packet In Count :	13789
Packet Out Count :	89
Out Of Resources Count :	0
Failed Hash Insert Count :	0

Figure 23. Tracking statistics

Also, when logged in as engineering user, the DSCP Priority Stream Mappings table shows a few extra items, as mentioned above. Here is an example



DSCP Priority Stream Mappings

Note: **Red** text in the Stream Priority column means the stream is configured for a priority level which is not active for the link, so the traffic will be mapped to the closest enabled priority. Display format is Active (Configured).

DSCP	Source LUID	Stream Priority	Stream Description	Source IP	Source Port	Remote IP	Remote Port	Protocol	TCP Src Fin	TCP Rmt Fin	PrivHash	PrivHash Entries	PubHash	PubHash Entries	Timeout
45	3	High (Ultra High) ToS: 6	Zoom Meetings	192.168.128.180	52390	52.202.62.254	443	TCP	-	-	0258	1	0258	1	3
45	3	High (Ultra High) ToS: 6	Zoom Meetings	192.168.128.180	52386	18.205.93.211	443	TCP	-	-	0171	1	0171	1	5

used 2 free 8190

Figure 24. More DSCP statistics

Here you can see the ToS value being used across the radio link. Normally 6 would map to an Ultra High channel, but in this case, only High is available, so that is being used. Note that this ToS value is not actually used or inserted into the packet. Other new columns include Priv and Pub Hash values and entries and TCP Src/Rmt Fin. For TCP links, we will track the FIN packets so that we can accelerate the timeout of the mapping. Once a FIN is seen in either direction, the timeout will accelerate to 1 minute.

For the Hash columns, the Priv and Pub Hash values are the index into our hash table for each side of the link. Currently these will be the same, as we hash on Remote IP and Remote Port. The Entries columns shows how many entries are in that Hash index. In order to operate efficiently, the entries column should

remain a pretty low number (< 10). If these numbers get too large, it will increase the search time which can cause other issues.

Conclusion

VIDEO CONFERENCING APPLICATIONS AND SERVICES are very important in work and educational spaces as more and more people are working and learning remotely. It is imperative that the applications perform at a high level to ensure a good Quality of Experience to the end-user. This application note introduced the concepts of Quality of Experience, the system and network influence factors related to the end-user Quality of Experience, why they are important for video conferencing, and how Cambium solutions can be set up to ensure quality video performance over a wireless fabric.