Cisco Unified Wireless QoS Tech Note

Document ID: 116056

Contributed by Nick Tate and Nicolas Darchis, Cisco TAC Engineers.
Jul 02, 2015

Contents

Introduction

This document describes techniques to handle Quality of Service (QoS) on a Cisco Wireless LAN Controller (WLC) and the infrastructure devices to which the controller connects. QoS for Cisco wireless products is an often overlooked area that becomes more critical with the increase in data rates.

The QoS checklist is a quick guide that explains how to set up QoS correctly. Subsequent sections of this document explain settings and other information about wired networks, so that wireless QoS can be fully realized.

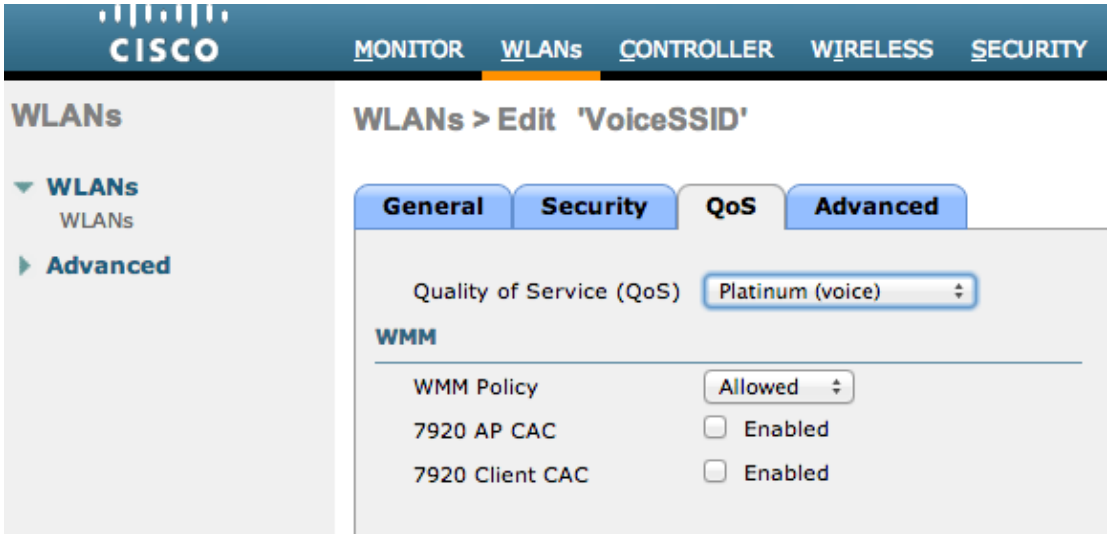
If you are familiar with QoS terms and wireless technology, start with the checklist; otherwise, read the explanations first.

If you are familiar with wired QoS but not with wireless QoS, be sure to read the explanations on Wi-Fi Multimedia (WMM) in order to understand why wireless QoS is much more critical than wired QoS.

QoS Checklist

1. Expand **WLANs**, and click the **QoS** tab.
2. For each WLAN, choose **Allowed** from the WMM Policy drop-down list .
3. For each WLAN, choose the appropriate QoS level from the Quality of Service (QoS) drop-down list:

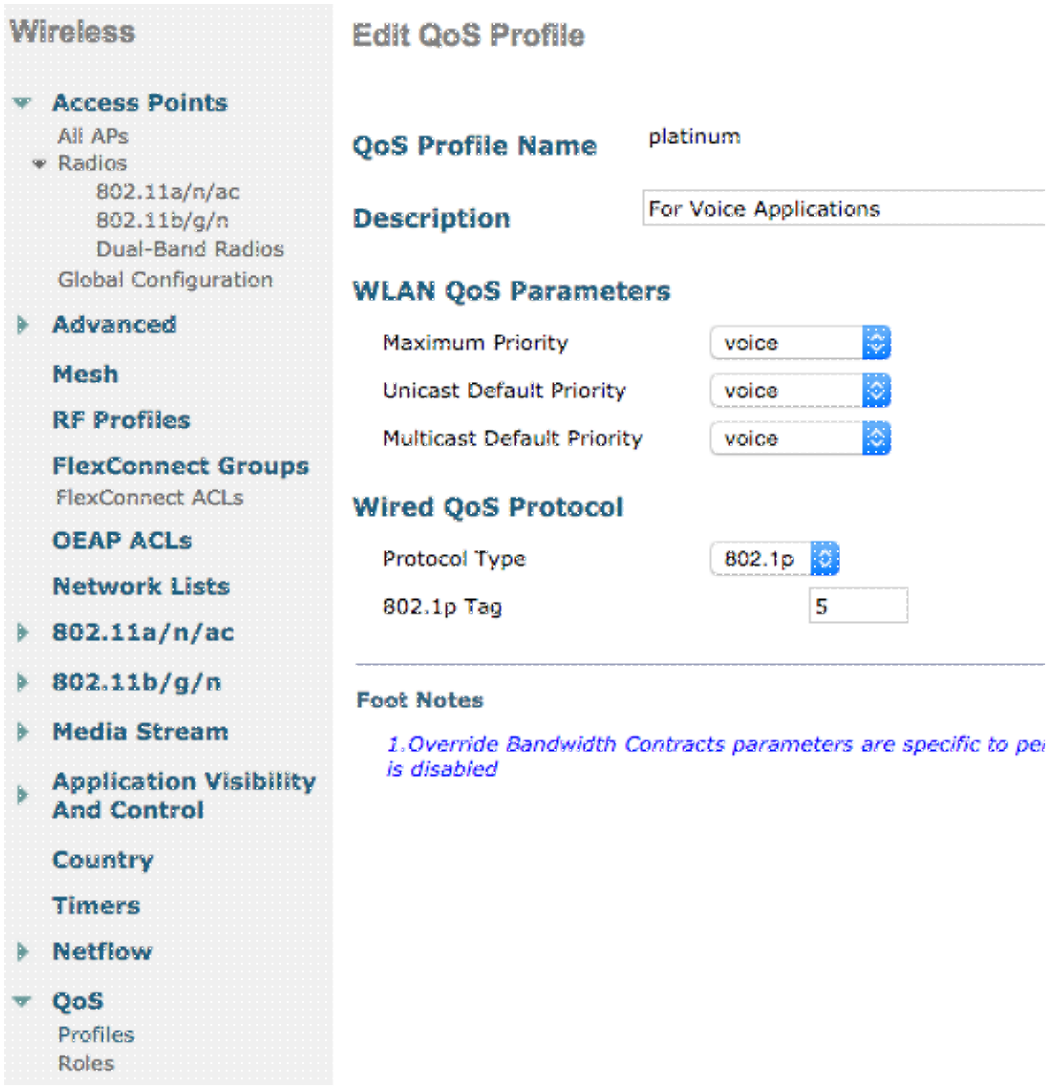
    - Choose Platinum for wireless VoIP comunications with other types of traffic.
    - Choose Gold only for video streaming networks with no voice traffic.
    - Choose Silver for all general purpose data networks with no voice or video traffic.
    - Choose Bronze for all guest networks.



4. On the Wireless menu, click **QoS**, and click **Profiles**.

5. Choose **802.1p** from the Protocol Type drop-down list, and enter the appropriate tag in the **802.1p Tag** field:

   - Platinum = 5
   - Gold = 4
   - Silver = 3
   - Bronze = 1



Note: In versions before Version 7.5, it was recommended to set the .1p tag to 6 for voice (although this would actually mark it with CoS 5 in reality). Versions after Version 7.5 default to 5 for platinum .1p. This is a cosmetic change only, behavior stays the same.

Additional guidelines include:

- If you rely on Class of Service (CoS), all interfaces should be tagged. None should be set to VLAN 0, because that indicates they are in the native VLAN.
- If you rely on CoS, switchports connected to the WLC should be trunk ports set with the **mls qos trust cos** command.
- Switchports connected to local mode access points (APs) and Hybrid Remote Edge Access Point (H-REAP)/FlexConnect APs with no locally switching Wireless LANs (WLANs) should be access ports set with the **mls qos trust dscp** command.
- If you rely on CoS, switchports connected to H-REAP/FlexConnect APs with at least one locally switched WLAN should be trunk ports set with the **mls qos trust cos** command.

WMM

Enable WMM on a WLAN in order to create the simplest implementation of QoS; this option is on the QoS tab in the WLAN configuration menu. Other WMM policy settings are:

- **Disabled** - WMM is not in use on the WLAN.

- **Required** - Clients must support WMM or they are not permitted to access the WLAN.
- **Allowed** - Clients that support WMM may use it, while those that do not support WMM can still connect to the network.

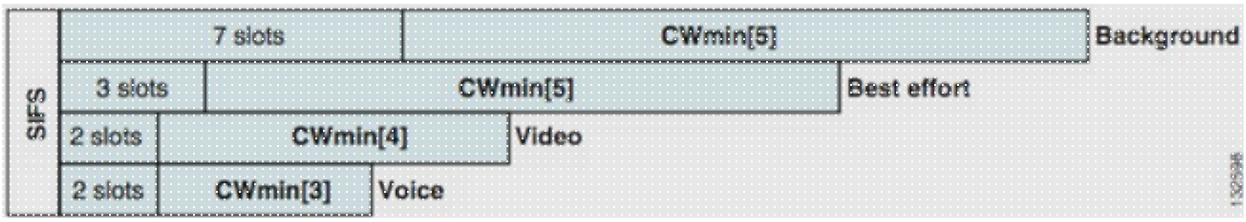
WMM is a Wi-Fi alliance certification, which is a subset of the full 802.11e IEEE standard.

WMM allows wireless stations (clients and APs) to prioritize and classify each packet they send into one of four access classes:

- Voice (AC_VO)
- Video (AC_VI)
- Best Effort (AC_BE)
- Background (AC_BK)

For ease of computation, look at 802.11b only as the numbers skew when dealing with 802.11a/g/n. Without WMM, all packets are given the same preference in the wireless contention algorthim, Distributed Coordination Function (DCF). Before a packet is transmitted, the station calculates a random backoff timer, which the station must have before it attempts to send the packet. Without WWM and with standard DCF, every transmission has the same priority because they are all given the same backoff variable. The variable is a random backoff between 0 and 31, where the top end doubles, up to a maximum of 1023, if a collision occurs and the packet must be retried.

Note: The image that follows is for reference purposes only and does not reflect the WLC values.



With WMM, packets in the different access class queues are prioritized based upon different random backoff variables.

The current backoff numbers are as follows:

- **AC_VO** – ranges between 3 and 7
- **AC_VI** – ranges between 7 and 15
- **AC_BE** and **AC_BK** – range between 15 and 1,023

Thus, a station with higher priority traffic to send is much more likely to have its message sent first and is allowed to retry more often in the case of collisions.

WMM also shortens the Interframe Spacing requirements for high priority packets so that voice and video can be sent in bursts without the need to wait as much for lower priority data inbetween. Additionally, WMM is needed in order to obtain 802.11n and 802.11ac data rates. This means that with WMM disabled or for non-WMM clients, the maximum usable data rate is 54 Mbps.

This modification of the DCF is called Enhanced Distributed Channel Access (EDCA) and is essentially what the WMM certification took out of the 802.11e, which proposed a second medium access mechanism.

CoS and DSCP Switch Operation

Differentiated Services Code Point (DSCP) is a tag in layer 3 of the IP header, so it always survives throughout the journey of the packet. DSCP contains a hex/decimal value but is usually translated into a friendly name.

For example, a voice packet is usually tagged Expedited Forwarding (EF), which has a decimal value of 46. This table gives the correspondance:

DSCP Name	Binary	Decimal	IP Precedence
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

Call signaling is often tagged as CS3, while voice is EF. You usually need to remember the friendly names rather than the actual values.

IP phones or even software applications send voice traffic tagged as EF.

CoS is a layer 2 tag, also called 802.1p, that sits in the 802.1q VLAN tag header; therefore, it is present only when a VLAN tag is present, such as on trunk ports. For this reason, it is a non-surviving tag that disappears when the packet is routed to another subnet or when the packet goes through an access port.

It is perfectly acceptable for both values to coexist, and they always coexist on trunk ports.

When you enter the **mls qos trust dscp** command on a port, the switch uses the DSCP value on incoming packets in order to put the packets in the right queue (internal voice, video, or best effort queue). When the packet is resent on another port, the switch sets the CoS tag to match the DSCP so there is no conflict between the two values; if the CoS tag is present, it is a trunk port.

When you enter the **mls qos trust cos** command on a port, the switch uses the CoS marking on incoming packets in order to put the packet in the right queue. When the packet is resent, the switch makes the DSCP

value correspond to the CoS.

With this system, you cannot have a mismatch, because one value is always rewritten in order to match the other one (the trusted one). So, you can trust DSCP on access ports and CoS on trunk ports. The CoS value is rewritten by the switch on egressing on a trunk port, even if the value was not present when ingressing from an access port.

As soon as you enter the **mls qos** command globally on a switch, the switch requires you to run the **mls qos trust cos** or **mls qos trust dscp** command on switchports. If you do not, both CoS and DSCP values are overwritten to 0. Without the global configuration from the **mls qos** command, any tag stays as is, but the switch does not use priority queues at all.

Different UP Markings for the Same Traffic Class

Voice is tagged as CoS 5 over a wired network, but as 6 on WMM/802.11e. This is often confused between the 802.1p standard and the WMM standard. More and more vendors actually break the 802.11e/WMM standard as they tag voice as UP 5 over the air (Microsoft with Lync is a famous example), so they basically use the 802.1p table instead of 802.11e over the air. This is something to be aware of as Cisco still respects the 802.11e standard and tags voice as 6 over the air. This is another reason to trust DSCP over CoS.

This is why, for added flexbility, the first maintenance release of the 8.1 WLC software adds the support of a manual QoS map. This means that instead of using a static mapping table as before (for example, an UP of 5 will not be tagged as voice in the wired DSCP, but video instead), the administrator can decide to keep trusting the original DSCP value. As such, for the most classic use case, you can decide to trust the DSCP EF that a Microsoft Lync Windows clients will send and keep it tagged as voice rather than noticing it is sent with UP 5 and downgrading it to a video DSCP over the network.

QoS Profiles

The first role of a WMM profile (platinum, gold, silver, bronze) is to set the ceiling (the maximum level of QoS that clients are allowed to use). For example, if you set a silver profile on a WLAN, clients can send background traffic or best effort traffic but are not allowed to send voice or video. If voice or video is sent, they are treated like best effort.

Similarly, if you set platinum, the clients are allowed to use any QoS tag/class. That does not mean that everything is considered as voice. It means that, if the laptop sends voice traffic, it is treated as such, and, if the laptop sends best effort (as the majority of laptops send), it is also treated as best effort.

Another role of WMM profiles is to define the tag of non-QoS traffic. If WMM is set to allowed, clients are still allowed to send non-QoS frames. Do not confuse two different situations:

- If a laptop supports WMM (as the vast majority of laptops do) and sends QoS data frame, it uses a tag of 0 if it is not tagging traffic.
- If a laptop does not support WMM and sends simple data frames with no QoS field, the WLC translates those data frames into the QoS profile. For example, data frames are translated as voice tags if you configure platinum.

QoS profiles let you take the WMM values used in the wireless space and translate them into QoS marks on a wired network. The configuration on the WLC uses the 802.11e-recommended mappings which are how WMM is defined, such that Voice = Platinum = 6, Video = Gold = 5, Best Effort = Silver = 3, Background = Bronze = 1.

On the wired side, Cisco routers and switches can operate on DSCP at layer 3 or CoS markings at layer 2. The CoS markings are present in the 802.1p/q tag that is added to packets in order to mark the VLAN to which the packet belongs. This 802.1q tag is 16 bits long; 12 bits are used for the VLAN ID (0 through 4095), one bit is not used, and three bits are used for CoS markings (0-7). Because CoS values 6 and 7 have special significance on the wired network, Cisco does not send out the WMM values defined as 6, 5, 3, and 1 for platinum, gold, silver, and bronze. Instead, Cisco translates them into the CoS values of 5, 4, 0, and 1, as shown in this table:

Access Classh	Quality of Service	WMM Values	Cisco-Translated CoS values
Voice	WMM Platinum	802.11e 6	802.1p 5
Video	WMM Gold	802.11e 5	802.1p 4
Best Effort	WMM Silver	802.11e 0	802.1p 0
Background	WMM Bronze	802.11e 1	802.1p 1

Wireless traffic that is associated with a higher priority QoS profile is given a higher priority tag on the wired side. The CoS value assigned based on the WMM to 802.11e to 802.1q marking is maintained by both the AP and the WLC so that the Control and Provisioning of Wireless Access Points (CAPWAP) packets are given the same level of wired QoS as the packet, once the CAPWAP header is stripped off by the WLC and sent on to the wired network.

Similarly, traffic from the wired network that is in route to a wireless client has a CoS value associated with it that Cisco copies to the CAPWAP packets that go to the AP. The AP then uses the CoS value in order to determine the proper WMM queue to use.

Tagged WLC Interfaces

It is common to leave the WLC Management Interface on an untagged/native VLAN. Because of the CoS tagging discussed previously, this is not a wise choice if you enable 802.1p marking on the WLC. Without that 802.1q tag, there is nowhere to put the CoS markings, and QoS fails on the Management Interface.

Even if you do not put any WLANs on the Management Interface, you might still encounter QoS issues with:

- CAPWAP control packets sent by the WLC to its APs
- Inner WLC communications
- Backend authentication that originates from the Management Interface

Therefore, ensure all of your WLC interfaces are on tagged VLANs.

DSCP Recommendation

Due to the fact that more and more vendors use 802.1p-like markings over the air rather than the original 802.11e table (that is, voice is sent as 5 UP instead of 6), Cisco now recommends to trust DSCP end-to-end in order to avoid confusion and mismatches. DSCP also offers more values and choices, is more resilient to native VLANs, and is therefore more reliable to be preserved throughout the network.

Post Release 7.2 Behavior Change

Before the WLC Release 7.2, there was no capping of the inner CAPWAP DSCP value. The first thing to insist on is that the inner DSCP value did not change and is still not modified as of Release 8.1. So if an end station (wireless or wired) sends a DSCP packet on a Gold (=video) WLAN, Gold marking between the AP and WLC is enforced, but the original packet keeps its original DSCP tagging.

What is now modified is wired to wireless packets that come with a DSCP value higher than the WLAN can tolerate. The WLC, that now trusts DSCP, rewrites the DSCP value of the outer CAPWAP encapsulation in order to match the WLAN maximum. The same rewrite takes place in the other direction as well.

Related Information

- **QoS on Wireless LAN Controllers and Lightweight APs Configuration Example**
- **QOS on 8.0 - Video That Explains the DSCP Capping Behavior of WLC**
- **Technical Support & Documentation - Cisco Systems**

Updated: Jul 02, 2015 Document ID: 116056