Understand & Troubleshoot QoS over Wireless 9800 WLC (Quick Reference)

Contents

Introduction

This document describes QoS on 9800 wireless LAN Controllers

Prerequisites

Requirements

This document covers how to prioritize and tag the traffic in both upstream and downstream. It explains the best practice configuration for voice traffic on Wireless LAN Controller (WLC) and troubleshooting techniques for a common voice-related issues.

Components Used

9800 WLC based on 17.12 Cisco IOS® XE release.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

A brief description of IEEE 802.11e standard and Wi-Fi Multimedia (WMM)

WMM is a Wi-Fi Alliance based on the IEEE 802.11e standard. WMM provides Quality of service (QoS) features by prioritizing the traffic according to four Access Categories: Voice, Video, Best Effort, and Background based on the Enhanced Distributed Channel Access (EDCA) method.

Enabling WMM is essential for achieving optimal performance in Wi-Fi networks, particularly in environments where high-bandwidth, low-latency applications are prevalent. For example, in 802.11n networks, WMM is required to fully leverage the capabilities of this high-speed Wi-Fi standard.

WMM Queues and Enhanced Distributed Channel Access (EDCA)

Generally speaking, any station must listen to the medium to check if it is idle before sending the frames. Once the frame is sent, the station listens to the medium to see if a collision has occurred.

Wireless clients can not detect the collisions. For this, CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used. It uses a fixed and random timer (CWmin, CWmax) and every frame that is sent must be acknowledged so that we know there is no collision and all clients can send their traffic.

As we mentioned earlier, we have four Access Categories (Queues), each of the queues uses different timers. Frames with the higher priority are sent statistically earlier, and the lower priority frames have backoff parameters making them statistically be sent afterwards.

In summary, the existence of the four queues alone does not guarantee Quality of Service (QoS); what truly matters is how the traffic within each queue is effectively managed.

QoS Implementation

By default, without Quality of Service (QoS) configured, network traffic is treated equally, with a best-effort delivery model. This means that all traffic, regardless of its type or importance, has the same priority and chance of being delivered at any given time. However, when QoS features are enabled and properly configured, priority can be assigned to specific types of network traffic, such as Voice and Video.

Configuring QoS involves two main components: Classification and Marking.

Classification:

Classification involves identifying and categorizing network traffic based on specific criteria, such as the type of application, source/destination IP address, protocol, or port number. Traffic is divided into classes or queues:

1. Voice: AC_VO
2. Video: AC_VI

3. Best-effort: AC_BE
4. Background: AC_BK

Marking:

Once the traffic is classified into queues marking involves assigning QoS markings or tags to packets to indicate their priority level.

There are several ways to mark the traffic. The main two standards are layer 2 802.1p CoS (Class of Service) and layer 3 DSCP (Differentiated Services Code Point).

Layer 2 "802.1p" CoS (Class of Service)

In the 802.1p standard,there are seven levels of CoS, each represented by a 3-bit field that can take on values ranging from 0 to 7. These values signify the priority of the traffic, with 0 being the lowest priority and 7 being the highest priority.

Note: 802.1p is a sub-set of the 802.1q standard, it is presented only when a VLAN tag is there, such as on trunk ports.

Table 1: 802.1P and WMM Classification

802.1P Priority	Access Category_WMM Designation	Access Category "AC"	QoS
1	AC_BK	Background	Bronze
2	AC_BK	Background	Bronze
0	AC_BE	Best Effort	Silver
3	AC_BE	Best Effort	Silver
4	AC_VI	Video	Gold
5	AC_VI	Video	Gold
6	AC_VO	Voice	Platinum
7	AC_VO	Voice	Platinum

Layer 3 DSCP (Differentiated Services Code Point)

DSCP is a layer 3 tag on the IP header, it uses 6-bits allowing 64 different values (0 to 63).

Table 2: DSCP and WMM Classification

DSCP	Access Category_WMM Designation	Access Category "AC"	QoS
0-7	AC_BE	Best Effort	Silver
24-31	AC_BE	Best Effort	Silver
8-15	AC_BK	Background	Bronze
16-23	AC_BK	Background	Bronze
32-39	AC_VI	Video	Gold
40-47	AC_VI	Video	Gold
48-55	AC_VO	Voice	Platinum
56-63	AC_VO	Voice	Platinum

The predominant DSCP values include 46 (EF) for Voice, 34 (AF41) for Video, and 0 (BE) designated for best effort.

Default DSCP-to-UP Mapping

As we discussed earlier UP is a 3-bits field within the Ethernet frame, while DSCP is 6-bits in the IP header.

How can you calculate the Layer 2 User Priority (UP) value from the Layer 3 Differentiated Services Code Point (DSCP) value?

Currently, there is no specific standard for this mapping however, a common method is used and known as 'Default DSCP-to-UP Mapping'.

DSCP-to-UP Mapping method derives the UP values from the 3 msb of the DSCP packet and then maps it on the correct Access category.

This method is used by Microsoft Windows machines yield to well-known issue which is covered in more details in Example #2: A Well-Known Microsoft Windows Client Issue In DSCP To UP Mapping

Table 3: Default DSCP-to-UP mapping

DSCP	DSCP (binary)	802.11e UP (binary)	802.11e UP (decimal)	Access Category Assignment
56-63	111000 - 111111	111	7	Voice
48-55	110000 - 110111	110	6	
40-47	101000 - 101111	101	5	Video
32-39	100000 - 100111	100	4	
24-31	011000 - 011111	011	3	Best Effort
0-7	000000 – 000101	000	0	
16-23	010000 - 010111	010	2	Background
8-15	001111 - 001111	001	1	

Packet Flow and QoS Trust

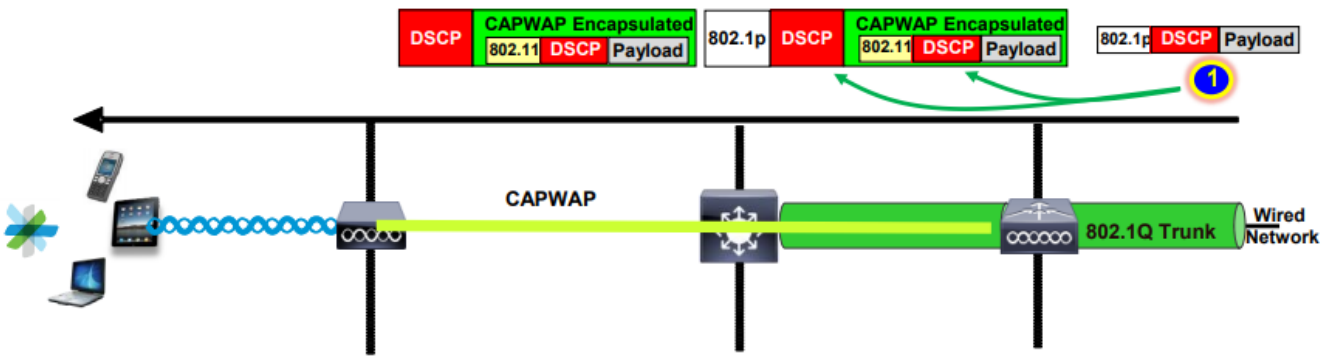
This section covers packet flow and QoS trust in these different scenarios:

1. Central Switching- Downstream Trust.
2. Central Switching- Upstream Trust.
3. FlexConnect locally Switching Trust.

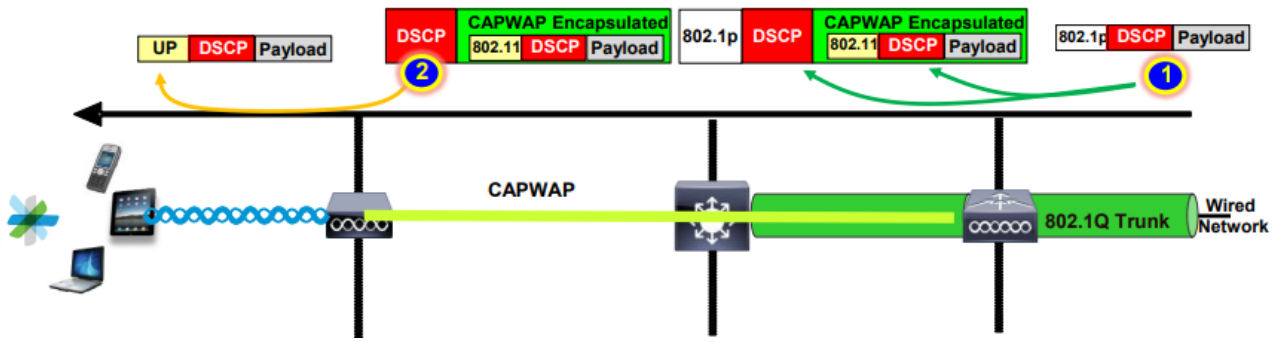
Central Switching- Downstream Trust

- Downstream- traffic from Wired to Wireless.
- The downstream traffic is CAPWAP encapsulated.

1- An Ethernet frame is received on the WLC 802.1q trunk port. The WLC uses the inner DSCP value sent from the wired network and maps it to the outer DSCP in the CAPWAP header, it caps the outer DSCP to a max value as per the QoS profile configured on the WLC.



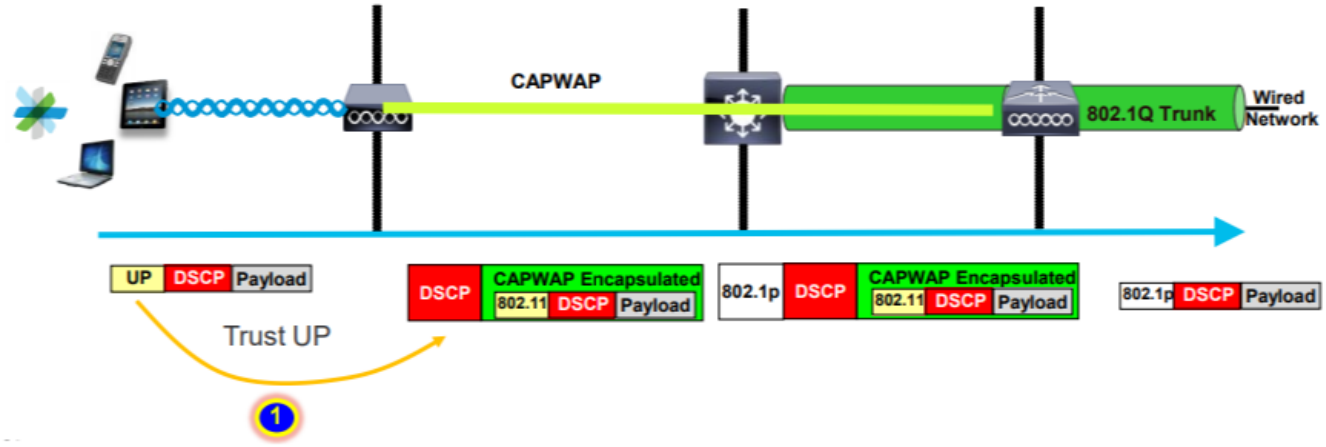
2- Once this Ethernet frame is received by the AP, the AP maps the outer DSCP value to UP value and sends it to the wireless client with the right AC.



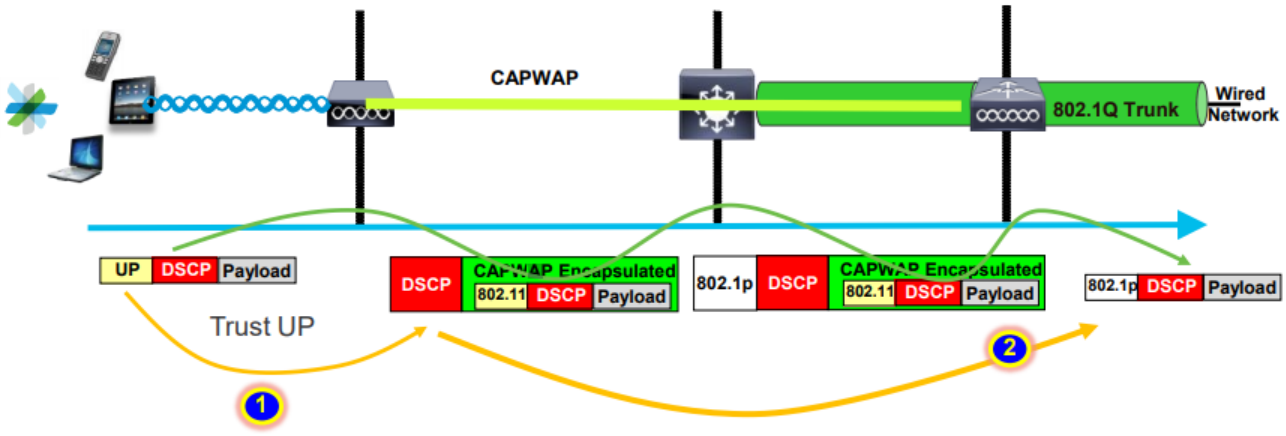
Central Switching- Upstream Trust

- Upstream- traffic from Wireless to wired.

1. The Wireless client sends the 802.11e (WMM) frame and this is received by the AP.



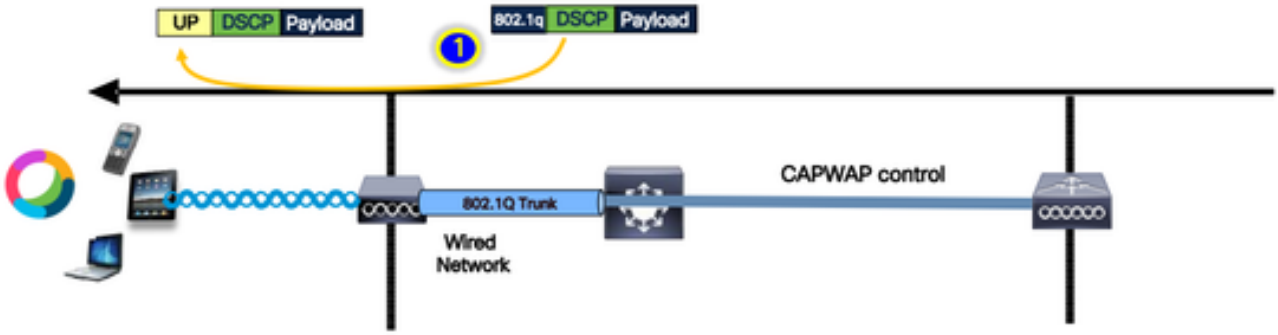
2- The AP encapsulates the original packet into a CAPWAP header and maps the UP to an outer DSCP value as long as the QoS profile configured on WLC allows that QoS level. The packet is sent to the wired network with the original DSCP value.



Flexconnect locally Switching Trust

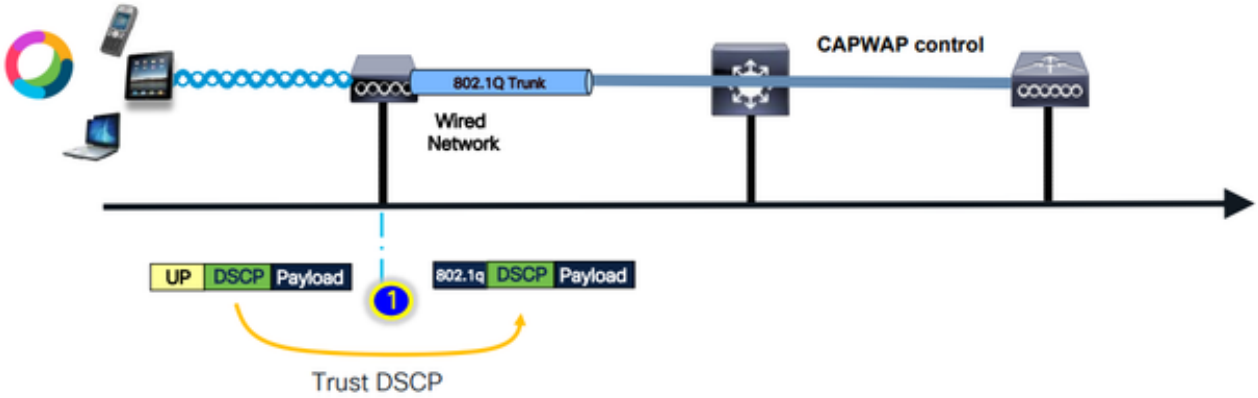
- Flexconnect locally Switching- Downstream trust

For locally switched VLANs, the FlexConnect AP takes the DSCP value of the IP packet, processes any QoS policy (for example AVC policy), maps it to the 802.11e UP value on the wireless frame and queues the frame . It then sends it to the client.



- Flexconnect locally Switching- Upstream trust

The client sends the frame and it is received by the AP. The AP looks at the original packet DSCP value to apply any QoS policy before sending the packet to the wired.



Common Issues For Upstream Traffic

Traffic in Upstream scenario - between the wireless client and the AP - is out of control; meaning that you have no control over the QoS sent from the client over the air.

For a working scenario, the client is expected to send a packet with correct UP and DSCP values so that traffic is in the correct Access-Category.

What occurs if the client transmits traffic with an incorrect UP value?

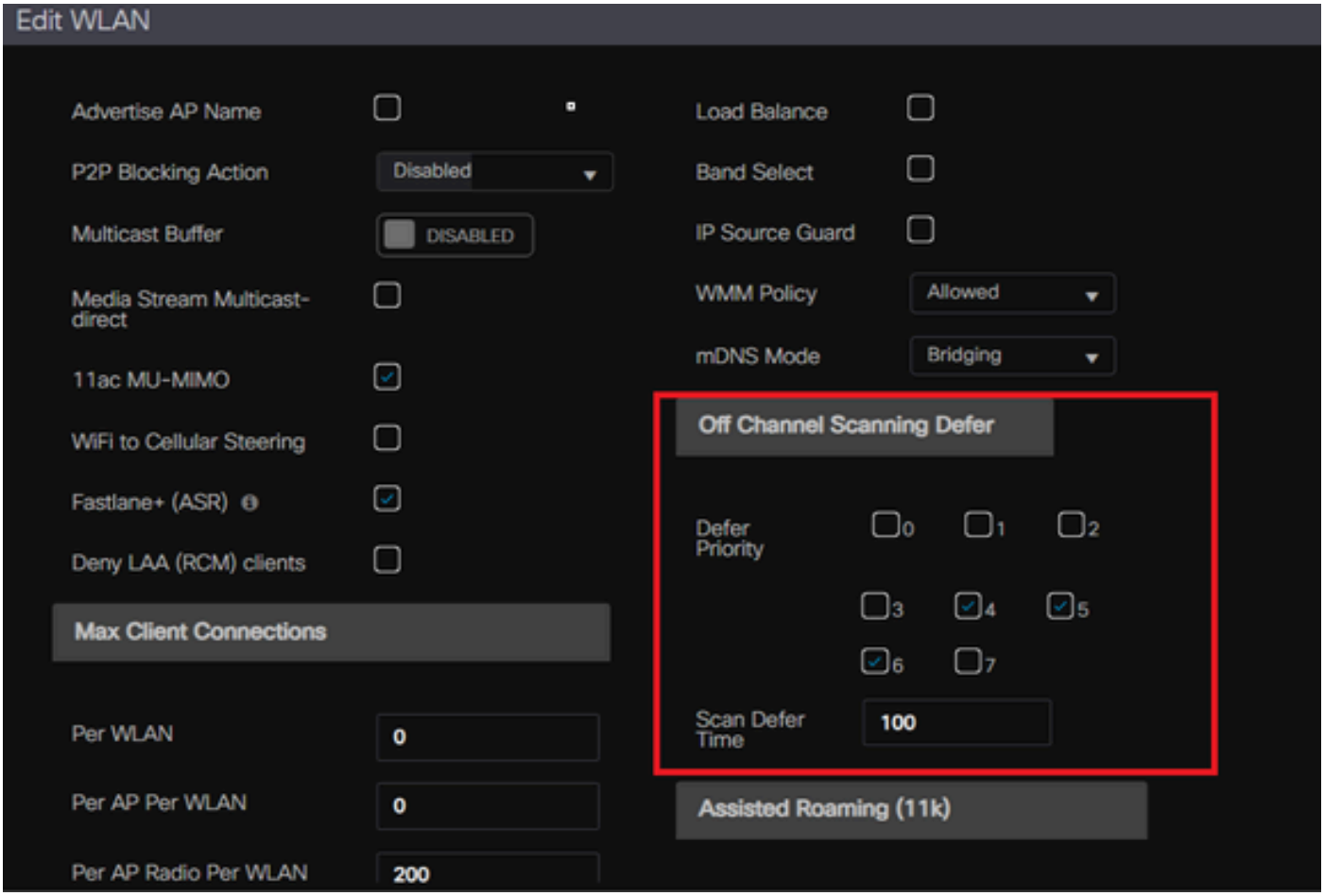
Example #1: When the client transmits traffic with a UP value of "2"

Note: APs go off-channel to scan to gather information needed for the RRM algorithm. This for sure impacts sensitive traffic such as voice and video.

Off Channel Scanning Defer option is configured under the WLAN Advanced tab. By default it is enabled

for UP classes 4, 5, and 6, with a time threshold of 100 millseconds, it means that the AP does not go off-channel to scan for a period of 100ms after seeing sensitive traffic (voice or video).

Assume wireless client is using voice application, the expected UP value is "6" however, the client sent the packet with wrong UP value “2". AP then goes off-channel scanning and this impacts the client performance and experience.



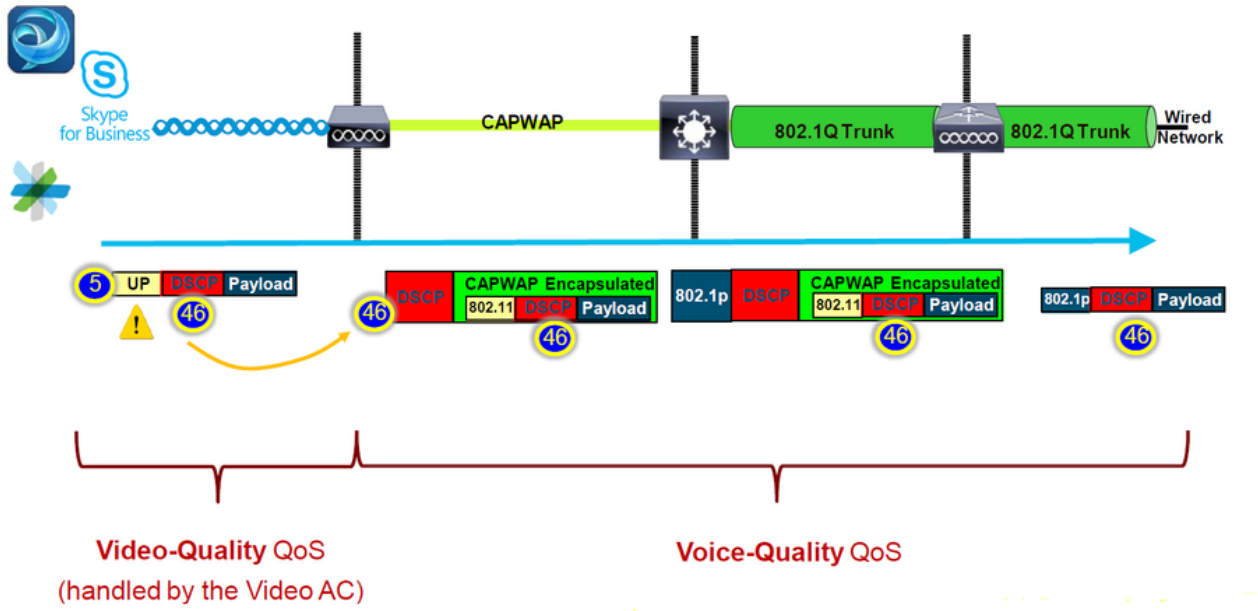
Can you enable Defer Scanning for low UP priority?

The answer is yes. Enabling Defer Scanning for low UP priority traffic effectively prevents the Access Point from conducting off-channel scans, thereby impacting the operation of the RRM and rogue detection algorithms. To address this challenge, an alternative approach is required to facilitate channel scanning while still prioritizing critical traffic.

Example #2: A Well-Known Microsoft Windows Client Issue In DSCP To UP Mapping

A common issue observed in MS Windows machines occurs when the default mapping between DHCP and UP values is utilized. In this mapping, the User Priority (UP) is determined from the three most significant bits (msb) of the Differentiated Services Code Point (DSCP) value. For instance, for voice traffic with a DSCP value of EF (101110), it would be mapped to UP 5 (101).

By default, APs in Upstream trust the UP value; causing the voice traffic to be treated in the Video Access Category (AC_VI) with DSCP value as 34 rather than the Voice Access Category (AC_VO) with DSCP value as 46, for which it is intended. For this, the Voice frames have longer wait times and a greater chance of retries.

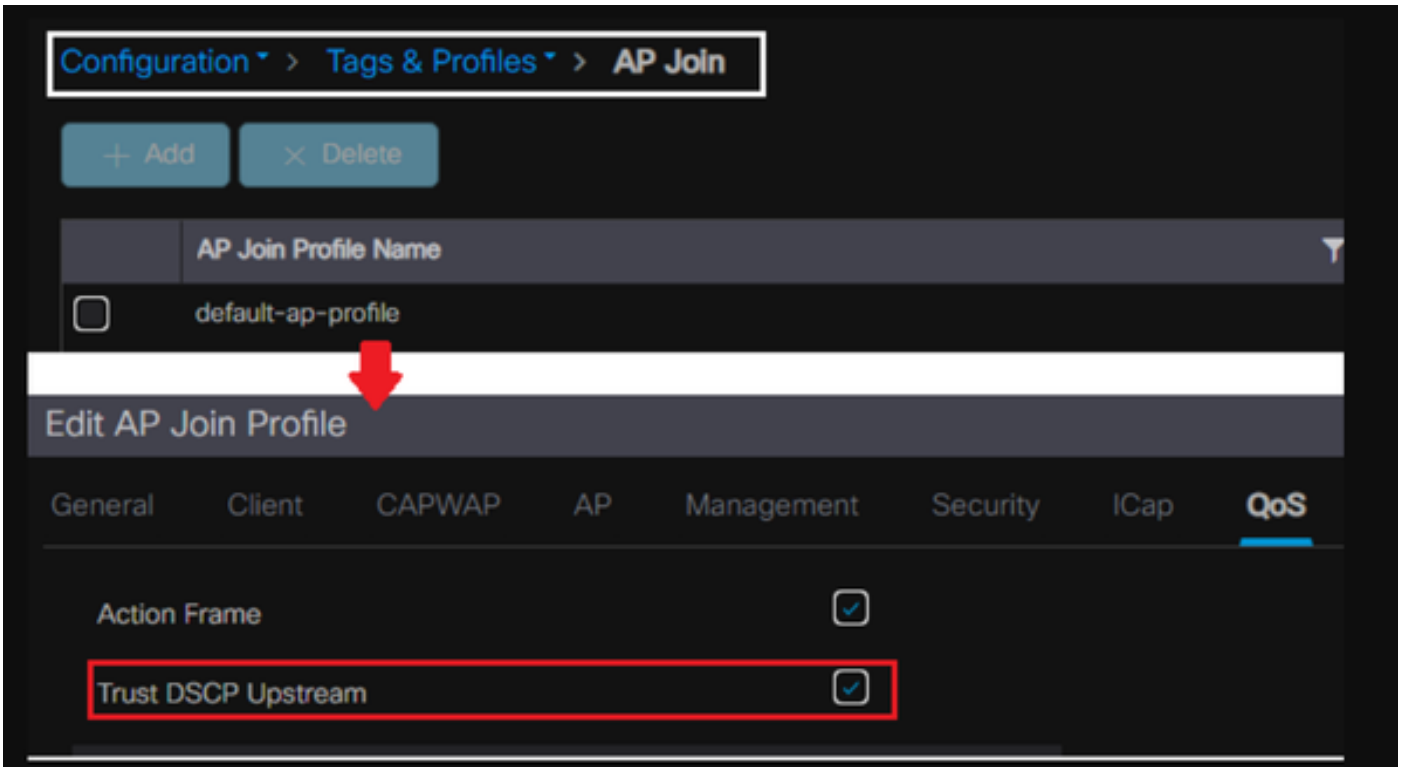


Is there a way to fix this?

The answer is yes if MS windows machine send voice traffic with the correct DSCP value.

How can it be fixed?

By using the“trust DSCP Upstream“ option on the WLC. This option forces the AP to trust the inner DSCP in the Upstream instead of the UP.



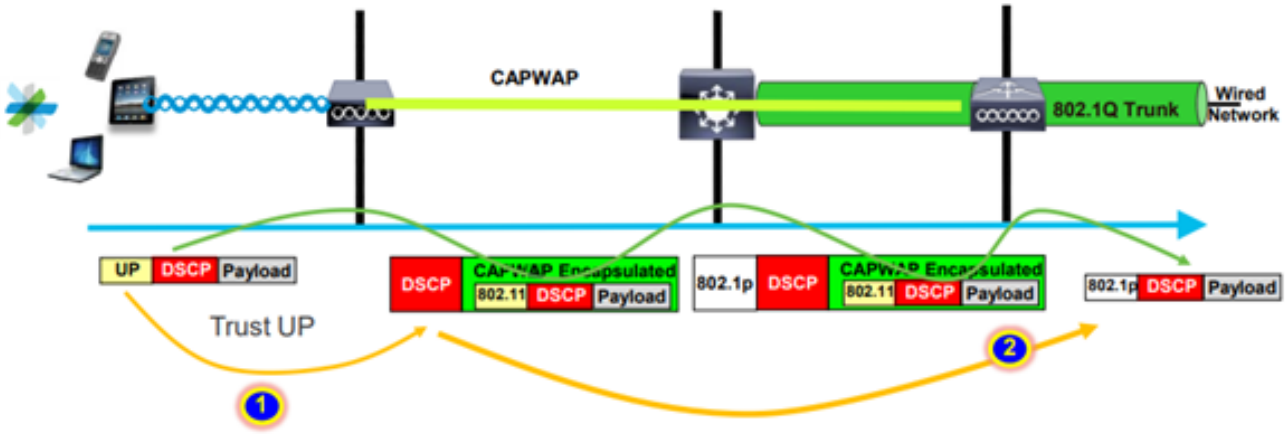
For further instructions on configuring your Windows machine to either override or tag the traffic, Please refer to ["How To Enable DSCP Tagging on Windows Machines"]

Which protocol to trust : DSCP or COS?

Which trust type to select for the WLC Switch Port?

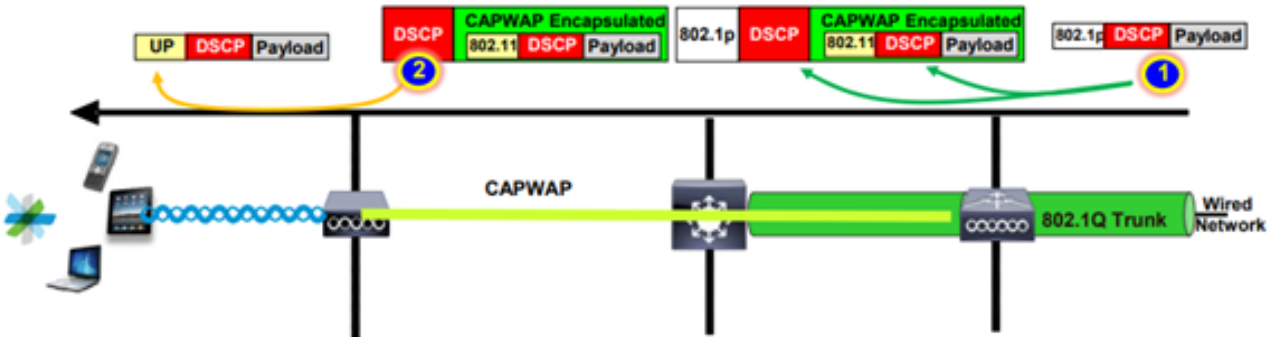
Actually, we can choose any of the trust options. However, you have to keep in mind that for the Upstream scenario if you choose to trust CoS; the switch rewrites the outer DSCP value based on the CoS-DSCP mapping table configured on the switch.

However, if you choose to trust DSCP; the switch does not rewrite the outer DSCP value as it trusts the incoming inner DSCP.



For the downstream scenario, the switch where the WLC is connected adds the 802.1p value based on the DSCP-CoS mapping table configured on it. If you choose to trust CoS; the outer DSCP value is changed based on the incoming 802.1p value.

However, if you choose to trust DSCP the Switch does not rewrite the outer DSCP value.



As an example on the above; Wireless client connected to an SSID mapped to the management interface on the native VLAN.

What happens if you choose to trust CoS on the WLC Switch port?

Client traffic reaches the trunk port, it is not tagged to 802.1q as it is a native untagged VLAN.

What can you do to fix this?

You can use the DSCP trust option instead of CoS which is generally the recommendation.

Wireless LAN Controller QoS Best Practices

Metal QoS profiles

We can configure four main QoS profiles on the WLC (Platinum, Gold, Silver, Bronze).

- Platinum/voice – ensures a high quality of service for voice over wireless
- Gold/video – supports high-quality video applications
- Silver/best effort – supports normal bandwidth for clients; this is the default setting
- Bronze/background – provides the lowest bandwidth for guest services.

The main purpose of these QoS profile is to limit the maximum outer DSCP value on the CAPWAP header for both Upstream and Downstream without affecting the inner DSCP.

Note: The inner DSCP value is modified by AVC.

For locally switched traffic, the QoS profile is applied to downstream traffic based on the UP value. if this value is higher than the default WLAN value the default WLAN value is used.

For upstream traffic, if the client sends a UP value that is higher than the default WLAN value; the default WLAN value is used.

For more details about the 9800 WLC best practice config guide Wireless QoS for the Catalyst 9800 Wireless Controller

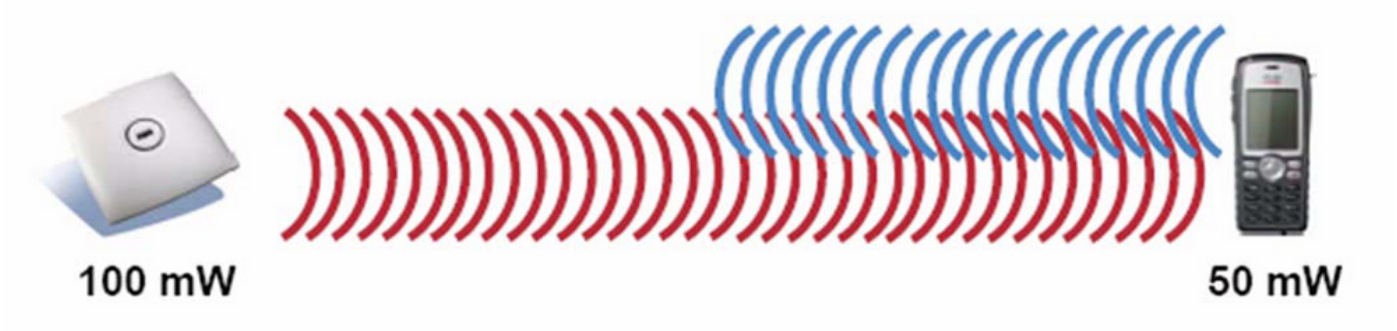
Troubleshooting steps:

1. Understand the problem.
2. Create a solid Action plan.
    - Ask Troubleshooting questions and a Network Topology Diagram.
    - Collect logs and debugs.
    - Ask for PI Heat-Maps.
3. Check WLC configurations.
4. Analyze the debugs
5. Use the VoWLAN checklist to confirm if the best practices were followed.

Understanding One-Way Audio

Mainly this issue happens when we have asymmetric power between the client and the AP.

APs can transmit with maximum power, however wireless devices such as Cisco phones can transmit with less power causing Cisco phones to hear the downstream frames from the AP, but AP does not hear the frames in Upstream from phones.



It is recommended not to configure the AP TX power higher than the maximum supported TX power on the wireless device.

- Action plan:
  - Check the client connection and make sure it is stable and no disconnections.
  - Check RF environment (AP power, signal strength ...etc).
  - Collect OTA captures to check audio traffic; single direction traffic is seen.

- Best practices:
  - Enable DTPC: it helps CCX Clients to adjust their TX power to match AP power.
  - Check volume settings in the client device.

Understanding Choppy and Robotic Audio

Both "Choppy" and "Robotic" audio happens when we have high packet loss or packet is being delayed.

Choppy voice describes gaps and delay in the sound. These are examples of a choppy and robotic records.

- Action plan:
  - Check client connection and make sure it is stable and no disconnections.
  - Check RF environment (high channel utilization, noise and interference devices ...etc).
  - Collect Captures through the path to check for packet drops.
- Best practices:
  - Check QoS configurations on WLC.
  - Make sure QoS is configured on the wired side.

Understanding Gaps and no audio when roaming

Sometimes users reports gaps and loss of audio connection when they are roaming from one location to another.

- Action plan:
  - Check RF environment and confirm you have a good coverage cell between APs.
  - Get PI heat MAP.
  - Collect Captures through the path to check for packet drops.
- Best practices:
  - Check the client connection and make sure it is stable and no disconnections.
  - Make sure RSSI value on the destination AP greater or equal -67

References

Wireless QoS recommendations

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html

Application Visibility and Control Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-avc-deployment-guide-rel-17-1.pdf