Wi-Fi CERTIFIED QoS Management™

Technology Overview

January 2024

The following document and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch are subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

Introduction

Wi-Fi CERTIFIED QoS Management™ is an optional Wi-Fi Alliance® certification program that improves the Wi-Fi® user experience in real-time applications, such as online gaming and augmented and virtual reality (AR/VR). Wi-Fi QoS Management™ technology extends features of Wi-Fi CERTIFIED WMM™ — and also leverages the scheduled access capabilities of Wi-Fi 6 and Wi-Fi 7 — to simplify the prioritization and management of latency-sensitive internet protocol (IP) traffic in Wi-Fi networks. Program features enable IP data flows to be classified, mapped to one of the quality of service (QoS) access categories defined by WMM®, and scheduled appropriately. This helps ensure that traffic for real-time applications and services is inserted into queues with higher priority and (when available) scheduled according to each flow's characteristics and QoS key performance indicators (KPIs), resulting in a better experience for end users.

Wi-Fi QoS Management is an ideal complement to Wi-Fi 7 because it helps manage the use of Wi-Fi 7's key features, such as Multi-Link Operation (MLO) and Multiple Resource Units (M-RU), to robustly achieve the QoS KPIs required for each flow. For example, once the necessary prioritization and KPIs for a flow with stringent QoS requirements have been exchanged using Wi-Fi QoS Management features, the flow can be intelligently scheduled across all available MLO links with flexible M-RU resource allocation. This facilitates reduction of channel access delay and improvement in link capacity, particularly in the presence of interference or congestion, to help ensure the flow's KPIs are met.

Wi-Fi technology is used for an expanding range of applications and services with a variety of QoS requirements. All of these benefit from higher throughput and lower latency. Some services, such as video streaming, use large playback buffers to help tolerate short-term variations in link quality, but still require a minimum average throughput to avoid service interruption. More advanced services that rely on real-time interactions via audio and video — such as voice-over-IP (VoIP), online gaming, enterprise videoconferencing, live streaming, and AR/VR—have higher demands to avoid latency and jitter and require high instantaneous throughput to deliver a quality experience. Good service delivery entails consistently applied QoS treatment policies that deliver reliable service even when the Wi-Fi environment experiences dynamic changes, such as peaks in traffic demand and interference. The Wi-Fi QoS Management™ certification program delivers a consistent, end-to-end QoS treatment in Wi-Fi networks, providing robust service delivery and quality experiences in real-time applications.

This paper provides a detailed technical overview of the features of the Wi-Fi QoS Management program, their applicability to use cases, and implementation considerations.

Key Capabilities

- Leverages QoS-aware capabilities to bring quality end-to-end connectivity
- Extends features of WMM for simplified QoS traffic categorization and prioritization
- Utilizes mirrored QoS and flow classifiers to enable client devices to request prioritization of IP data flows
- Gives network managers the ability to apply QoS policies to IP data flows

Benefits

- Delivers a consistent, end-to-end approach to QoS management in Wi-Fi networks
- Brings greater quality service in latency-sensitive applications used in residential, public, and enterprise settings
- Provides noticeable improvement to quality of experience for users
- Complements and provides benefits for all Wi-Fi generations

Defining the Wi-Fi QoS Management program

Wi-Fi QoS Management certification is available for client devices and access points (APs). The program comprises four main features, which are based on capabilities defined in IEEE Std 802.11-2020 and the 802.11ax-2021 and 802.11be amendments:

- Mirrored Stream Classification Service (MSCS) enables a client device to manage AP QoS treatment of downlink IP flows using QoS mirroring
- Stream Classification Service (SCS) enables a client device to manage AP treatment of downlink IP data flows based on IP tuple and IPsec child security association (SA) classifiers, and, for Wi-Fi 6 and Wi-Fi 7 devices, of uplink IP data flows based on traffic identifier (TID)
- Differentiated Service Code Point (DSCP) mapping enables a network manager to configure mapping tables between the DSCP marking in IP packet headers and the over-the-air QoS treatment on both APs and client devices
- DSCP Policy enables the network to manage a client device's treatment of uplink IP flows using DSCP marking policies

These features leverage WMM, which is based on IEEE 802.11 QoS mechanisms. To best understand the benefits provided by Wi-Fi QoS Management, it is important to become familiar with the basics of the WMM program.

WMM certification program background

The Wi-Fi ecosystem already has ubiquitous support for WMM, which adopted the four QoS access categories established in the IEEE 802.11 standard: Voice, Video, Best Effort, and Background. These categories are used to prioritize traffic, both in terms of over-the-air channel access and transmit queuing. The Wi-Fi QoS Management program builds on WMM by enabling both APs and client devices to request identified IP flows to be assigned to an access category for specific QoS treatment.

The baseline mechanism provided by WMM[1] enables prioritized, differentiated QoS treatment based on enhanced distributed channel access (EDCA). Prioritized and differentiated QoS refers to the prioritization of data flows with respect to each other. Prioritized QoS provides an appropriate baseline for Wi-Fi networks because it is scalable, does not require prediction of traffic patterns, and is effective even when networks experience dynamic changes in data rate, channel load, and interference.

WMM access categories

The four WMM access categories, presented in order of channel access priority, are:

- Voice
- Video
- Best effort
- Background

These access categories provide differentiated QoS treatment through independent transmit queues and unique channel access parameters.

[1] *For additional information about WMM, see https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm-programs*

Transmit queues

Each of the four access categories includes two User Priority (UP) levels and has its own independent transmit queue, as shown in Figure 1. This means that when the transmitting device is queueing a mixture of data packets assigned to different access categories, high priority data packets reach the front of the queue for transmission, even when other lower priority data packets are already pending transmission. This minimizes latency caused by "head-of-line blocking," where the first packet holds up the remaining packets in a queue, within the transmitting device. Since the receiving device handles in-order delivery of packets for each UP individually, high priority data packets received with a given UP are made available to applications without delay, even when previously transmitted packets assigned to other UPs are pending successful retransmission.

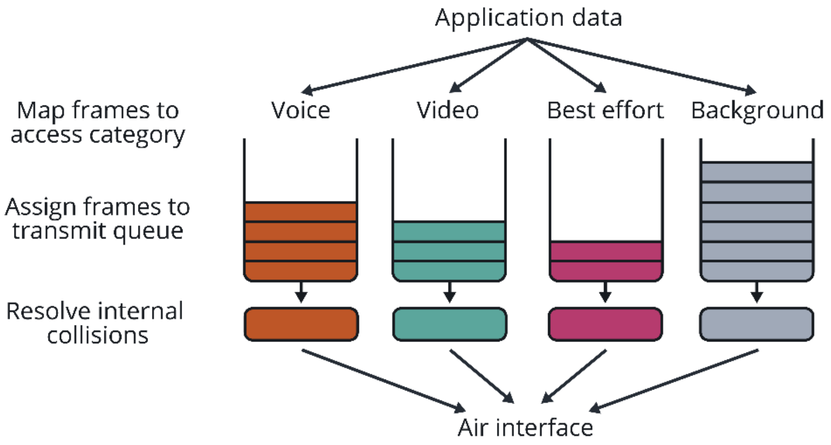

Application data
Map frames to access category
Voice
Video
Best effort
Background
Assign frames to transmit queue
Resolve internal collisions
Air interface

Figure 1: Transmitter data path with WMM access categories

Unique channel access parameters

Each access category is associated with a set of EDCA parameters: contention window minimum (CWmin), contention window maximum (CWmax), arbitration interframe space number (AIFSN), and transmission opportunity (TXOP) limit. As shown in Figure 2, these access parameters influence the backoff delay before a device contends for the medium to transmit a data packet from the corresponding queue.

By default, the Voice access category has the highest statistical priority to gain access to the channel, but the maximum duration of a single channel access is relatively short, since it is intended for low-bandwidth, low latency applications. The Video, Best Effort, and Background access categories have — in that order — relatively lower statistical channel access priority by default, but the maximum duration of a single channel access is longer since they are intended for higher bandwidth applications. This statistically prioritized channel access applies internally within a device between access categories transmitted by that device. Such prioritization also applies between different Wi-Fi devices that are sharing the channel using the same mechanism — including between devices in different basic service sets (BSSs) and/or networks.

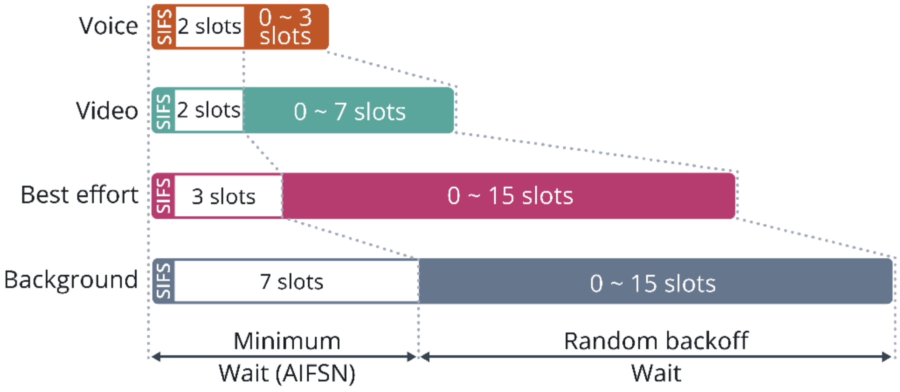


Figure 2: Backoff delay for channel access with WMM access categories

User Priority

A device transmitting an IP packet assigns its access category based on the packet's UP, using the fixed mapping table defined by WMM, replicated in Table 1 below. A packet's UP needs to be determined based on the higher layer QoS requirements of the application or service.

Most commonly, applications and services signal this intent via DSCP marking within the IP packet header, which can then be mapped to a UP. However, there are many scenarios in which the appropriate DSCP marking is not, or cannot, be applied. Wi-Fi QoS Management addresses these scenarios with features such as MSCS, SCS and DSCP Policy. In addition, implementation diversity in the industry has resulted in inconsistent mapping of DSCP values to UPs. Wi-Fi QoS Management addresses this inconsistency by standardizing the default DSCP mapping.

User Priority	Access Category
6 or 7	Voice (VO)
4 or 5	Video (VI)
0 or 3	Best Effort (BE)
1 or 2	Background (BK)

Table 1: UP to WMM access category mapping

WMM with multi-user and scheduled access

WMM access categories are the fundamental basis of channel access for all Wi-Fi generations, including Wi-Fi 6 and Wi-Fi 7. When the advanced multiple access technologies of Wi-Fi 6 and Wi-Fi 7, such as orthogonal frequency division multiple access (OFDMA) and multi-user, multiple-input, multiple-output (MU-MIMO) are also used, the assignment of data flows to WMM access categories also influences how those data flows are aggregated and scheduled for transmission. With these technologies, the AP's scheduler can facilitate transmission of both downlink and uplink flows — the latter by utilizing trigger-based uplink access.

With Wi-Fi 7's MLO feature, packets of a given flow can be transmitted over any or all of the links enabled between the AP and station (STA). All QoS Management features are managed and executed at the multi-link device (MLD) layer. However, WMM's underlying EDCA parameters (Cwmin/max, AIFSN, and TXOP Limit) are defined for each link separately.

Wi-Fi QoS Management features

Wi-Fi QoS Management provides new and convenient mechanisms for application and service QoS requirements to be signaled and negotiated, as well as mechanisms to ensure the mapping of DSCP values to UPs are consistently applied and managed. A detailed discussion of the features follows.

Mirrored Stream Classification Service

Wi-Fi QoS Management APs and client devices are required to support MSCS, as defined in IEEE 802.11-2020. MSCS provides a simple means for a client device to request its AP to assign downlink IP flows destined to that client device to the desired access categories. MSCS is based on the concept of "mirrored," or "reflective," QoS, where the AP derives QoS rules for downlink IP flows by monitoring the corresponding uplink IP flows sent by the client device. The AP does this by monitoring the IP header and the UP value in the 802.11 MAC header.

MSCS is designed for situations where the downlink IP flows that ingress the AP do not have appropriate DSCP marking, and therefore simple DSCP-to-UP Mapping does not achieve the required QoS prioritization on the Wi-Fi link. Lack of appropriate DSCP marking is a frequent scenario for downlink IP flows that originate on the public internet since it is common for intermediate nodes or internet service providers (ISPs) to reset to zero or modify any DSCP marking that might have been set by the source server.

As described in the section below, the procedure to activate MSCS is simple and lightweight. This involves a single request/response exchange to negotiate the MSCS parameters, which is done either at association or at any time post-association. Unlike some alternative approaches, the client device does not need to request QoS treatment for each flow individually and does not need to determine an IP tuple classifier for each IP flow. Therefore, MSCS is particularly efficient in scenarios where applications and services generate many short-lived IP sessions and/or the IP tuples of data flows are a-priori unknown, for example, due to DNS load balancing.

MSCS capability signaling

Wi-Fi QoS Management APs and client devices indicate support for MSCS in the Extended Capabilities element (defined in IEEE 802.11-2020) in (Re)Association Request and Response frames. APs also indicate support for MSCS in Beacon and Probe Response frames.

MSCS setup procedures

MSCS activation is always initiated by the client device, either by sending an MSCS Request frame to the AP post-association, or — if supported by the client device — sending a request embedded in a (Re)Association Request frame at association time. In either case, the request frame contains an MSCS Descriptor element which specifies the parameters below.

Request Type

The Request Type is set to “add” when the client device is requesting activation of MSCS, or to “change” when the client device is requesting modification of MSCS parameters when MSCS is already activated, or to “remove” to deactivate MSCS.

User Priority Bitmap

The UP Bitmap indicates a list of UPs — in the range 0 to 7 — which are to be monitored by the AP in received uplink packets to determine downlink QoS rules.

Typically, a client device would set this bitmap to indicate UPs 4, 5, 6, and 7 only, which corresponds to the Video and Voice access categories. This is done so that the AP generates downlink QoS rules based on uplink IP flows that the client device sends in Video and Voice access categories but does not generate rules for uplink IP flows that are sent using Best Effort or Background access categories. This helps avoid excessive processing overhead on the AP, for instance, where the AP would generate unnecessary rules corresponding to downlink Best Effort and Background IP flows that do not require special QoS treatment.

In use cases where the client device also wants certain downlink IP flows to be deprioritized, the client device might also include UPs 1 and 2, the Background access category, in the bitmap and use those UPs when sending the corresponding uplink IP flows.

User Priority Limit

The UP Limit indicates a maximum limit for the UP values that the AP applies in downlink QoS rules. Typically, a client device sets this value to 7, which is the highest possible UP value, so that all UPs in the bitmap are mirrored as-is. There may be cases where a lower limit is negotiated. For example, an enterprise network might have a network policy that allows MSCS mirroring only up to UP 5, the Video access category, to preserve Voice for predetermined mission-critical business applications. In such a case, QoS rules generated by the AP based on uplink IP flows sent using UP 6 or 7 would be capped and assigned to UP 5.

Stream timeout

Stream timeout indicates a minimum period of time for which the AP is required to maintain a downlink QoS rule, from the time at which the rule was generated or most recently updated. Typically, a client device sets this value to 60 seconds or less, so that the AP implementation can efficiently delete downlink QoS rules pertaining to IP flows that are no longer active.

In general, AP implementations are expected to maintain downlink QoS rules corresponding to downlink IP flows that are currently active. If an AP does delete a rule for a downlink IP flow that is still active, then the subsequent reception of a packet in the corresponding uplink IP flow from the client device will cause the AP to generate a new rule for that downlink flow.

Traffic classification (TCLAS) Mask element

The TCLAS Mask element indicates a list of IP header fields that the AP is to use to define a downlink QoS rule. A client device sets the frame classifier type in the TCLAS Mask element to 4, indicating IP and higher layer parameters. The device then typically sets the Classifier Mask bitmap to indicate the QoS rules are to be defined based on the full IP 5-tuple (Source and Destination IP Address and Ports, and Protocol / Next Header). The same list applies for both IPv4 and IPv6 flows. The TCLAS Mask element does not specify the actual IP tuple values for any particular flow; it simply specifies the list of IP header fields that are used to uniquely identify and classify each flow.

In some use cases, an alternative TCLAS Mask parameter list might be beneficial. For example, if applications on the client device intend to create a large number of short-lived connections to the same remote IP address and port using different local ports, and the uplink UP for all those connections is the same, then the client device might omit Destination Port from the list in the TCLAS Mask element in order to help minimize the number of downlink QoS rules generated by the AP.

The client device must ensure that the UP used when transmitting uplink packets that the AP will consider part of the same uplink IP flow does not rapidly fluctuate on a packet-to-packet basis. Otherwise, the UP assigned to the corresponding downlink QoS rule will be unstable. The client device should specify TCLAS Mask parameters that are specific enough to avoid such instability.

If the AP accepts the request from the client device, it activates MSCS for that client device, or updates the MSCS parameters if already activated. It then responds by including an MSCS Descriptor element indicating "success" in the (Re)Association Response frame, if requested at association, or indicating Success in an MSCS Response frame, if requested post-association. The AP maintains the MSCS state for each client device individually, meaning the negotiated MSCS parameters and generated downlink QoS rules are specific to each client device.

If the AP does not accept the request, it provides a status code that might indicate the reason for rejection, such as insufficient processing resources, or unsupported TCLAS Mask parameters. The AP then optionally specifies an alternative set of MSCS parameters that it would be prepared to accept. For example, if the client device requests a UP Limit of 7 but the network policy only allows MSCS mirroring up to UP 5, the AP might indicate a UP Limit of 5 in its rejection response. Then, if the client device still wants to activate MSCS, it can send a new request in which the requested UP Limit is 5.

If network policies completely prohibit the use of MSCS, perhaps because the policy requires DSCP-to-UP Mapping to be strictly applied to all downlink IP flows, the AP might reject MSCS requests. However, if the network policies only specify QoS treatment for certain IP flows but not for other IP flows, it is possible for those policies to coexist with MSCS. In such a case, the AP might accept the MSCS request made by a client and continue to abide by the network policies for those specific flows, while using the MSCS rules to set the UP for other downlink IP flows.

MSCS termination procedures and roaming

An AP or client device can terminate an active MSCS at any time. An AP terminates MSCS with a client device by sending an unsolicited MSCS Response frame to that client device, including a status code value that might indicate the reason for the termination. Examples of termination reasons include exhausted processing resources due to an excessive number of QoS rules generated or insufficient network capacity to support the QoS rules generated. A client device terminates MSCS by sending an MSCS Request frame with Request Type set to "remove."

Any active MSCS between an AP and client device is implicitly terminated at such time that the client device is no longer associated with the AP, or reassociates with the same AP. While it is possible that some network architectures might exchange MSCS QoS rules between APs when a client device roams — or potentially derive network-wide QoS policies based on MSCS rules — in general it should not be expected that MSCS rules or states propagate beyond a single BSS (or, for a Wi-Fi 7 case, a single AP MLD). If a client device has activated MSCS with an AP and then roams to another BSS in the network where it wishes to continue to use MSCS, in general the client device needs to request activation of MSCS with the new AP in the target BSS during or immediately after the roam (re)association. This applies regardless of whether the target BSS is operated by the same physical AP, except for a Wi-Fi 7 case where MSCS applies to all links of an ML association. Downlink IP flows are not assigned the expected UP immediately after a roam until the client device has sent at least one packet to the target BSS in the corresponding uplink IP flow so that the AP can generate the corresponding rule.

MSCS rule derivation

Once MSCS is activated at the AP for a given client device, the AP monitors the uplink packets received from that client device. UPs are indicated in the TID subfield of the QoS Control field of the 802.11 MAC header. If an individually addressed unicast QoS Data frame containing an IP packet is received from the client device with a UP that matches a value in the UP Bitmap, the AP generates or updates a corresponding downlink QoS rule by extracting the values of IP header fields from that received packet, as specified in the TCLAS Mask.

Consider the case where the MSCS parameters negotiated with the client device are as follows:

- UP Bitmap = {4, 5, 6, 7}
- UP Limit = 5
- TCLAS Mask = {IP Version, Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol / Next Header}

When the AP receives the uplink QoS Data frame shown in Figure 3 from that client device, where the indicated UP in the QoS Control field is 7, it generates a downlink QoS rule as follows:

{IPver=4; SrcIPAddr=WAN_IPADDR; DstIPAddr=STA_IPADDR; SrcPort=WAN_PORT; DstPort=STA_PORT; ProtNxtHdr=6} ➔ UP=5

The Destination IP Address and Port in the received uplink frame are used as the Source IP Address and Port in the downlink QoS rule classifier, and vice versa. The UP assigned to the rule is determined as the minimum of the UP of the uplink packet (7) and the negotiated UP Limit (5).

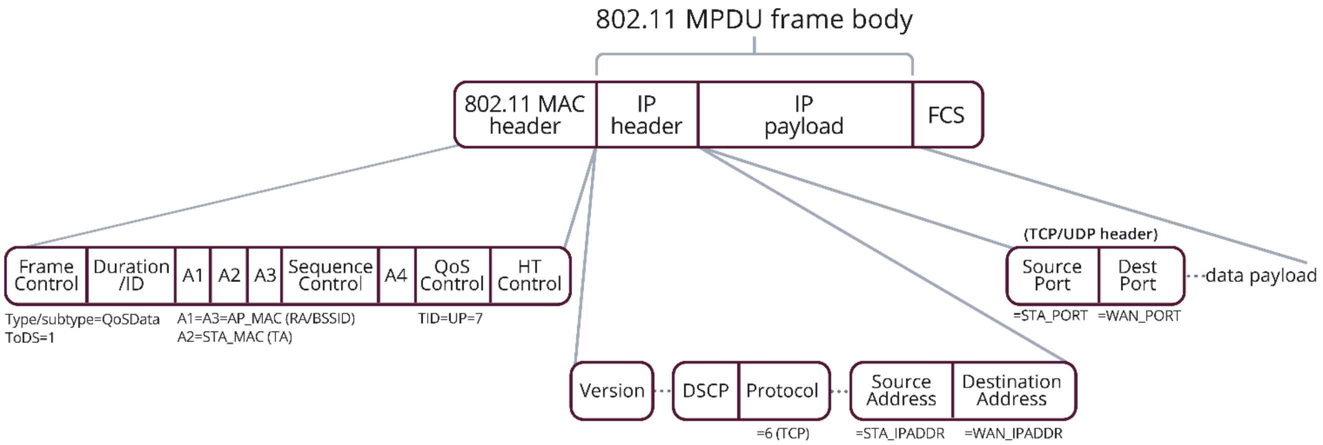


Figure 3: Example of an IEEE 802.11 QoS Data frame containing an IP packet sent by a client device to an AP

If another uplink packet with the same IP tuple values is received, the UP of that packet is used to update the UP assigned to the rule, if it is different to the rule's current UP assignment. This means that the client device can cause the AP to dynamically modify the QoS treatment of a downlink IP flow simply by changing the UP— or, indirectly, the DSCP marking — of the corresponding uplink IP flow it transmits.

AP implementations can use various optimizations to minimize packet processing overhead and the number of rules generated, such as:

- An AP does not need to generate a downlink QoS rule based on an uplink packet with Destination IP Address set to a multicast IP group address, since no valid downlink IP packet will have an IP group address as its Source IP Address
- An AP does not need to generate a downlink QoS rule corresponding to a downlink IP flow for which a higher precedence network policy applies
- An AP can delete a rule if the Stream Timeout period has expired since the rule was created or the UP corresponding to the rule was last updated

MSCS rule execution

If MSCS is activated at an AP for a given client device, the AP attempts to classify the downlink IP packets destined for that client device by matching their IP headers against the MSCS downlink QoS rules. Figure 4 shows an example where a downlink packet is assigned to UP 5, or the Video access category, based on the MSCS rule derivation described above.

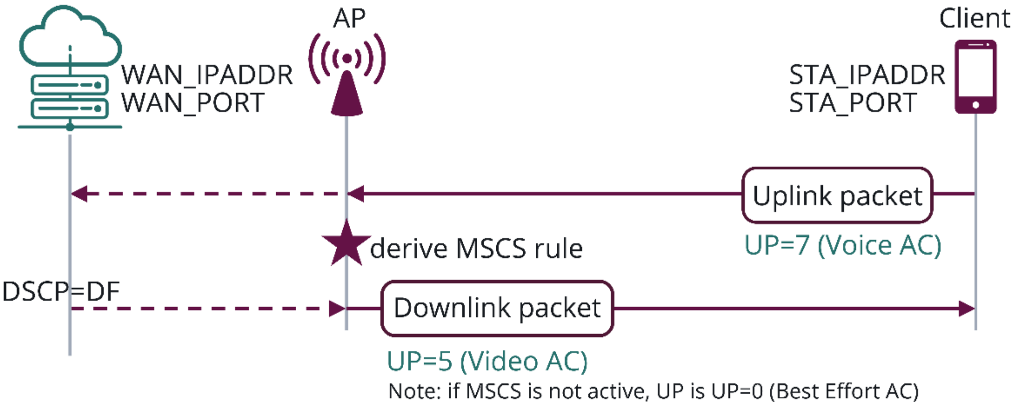


Figure 4: Example of MSCS rule derivation and execution

If the AP is configured with a network policy that uses mechanisms outside the scope of this program and that applies to a downlink IP packet, then that policy can take precedence for UP assignment over MSCS QoS rules. This might also include network control protocols such as Internet Control Message Protocol, DNS, and DHCP. If the downlink IP packet matches a TCLAS classifier associated with a traffic stream or SCS rule (see Stream Classification section), it also takes precedence for UP assignment over MSCS QoS rules. Note this does not apply to any traffic streams negotiated for WMM-Admission Control or WMM-Power Save, since they are not associated with TCLAS classifiers. If those higher precedence rules do not apply to the downlink IP packet and it matches an MSCS rule, then the AP assigns the UP specified in the rule to that packet. If the downlink IP packet does not match any of the above policies or rules, by default its UP will be assigned based on DSCP mapping. See the QoS Map section for more information.

Applicability of MSCS

MSCS can be used to manage the QoS treatment of all downlink IP flows that have a corresponding uplink IP flow with symmetric IP addresses and ports.

In the case of Transmission Control Protocol (TCP) protocol, which is stateful and inherently bidirectional, the same socket, or IP address and port, is used for both transmit and receive, and the corresponding downlink and uplink IP flows together form a TCP session. The QoS treatment of downlink packets of all TCP sessions can be managed using MSCS. Even if the transfer of user data is essentially downlink only, any uplink packet sent to establish or maintain the TCP session, such as synchronize (SYN) or acknowledge (ACK), is sufficient for the AP to generate the correct downlink IP rule, as long as it is sent using the appropriate UP.

Similarly, although the Quick UDP Internet Connection (QUIC) protocol uses User Datagram Protocol (UDP) as the underlying layer 4 protocol, it creates stateful bidirectional sessions using symmetric ports, and the QoS treatment of downlink packets of all QUIC sessions can also be managed using MSCS.

In practice, many other UDP based protocols also share these characteristics since, even if they do not necessarily establish formal bidirectional sessions, they do require downlink IP packets to traverse network address translation (NAT) or other stateful firewalls that typically exist between the peers.

For instance, in the case where a peer device behind a firewall uses a STUN server to establish a peer-to-peer VoIP call with another remote peer, that device uses the same socket, or local IP address and port, for both transmission and reception of VoIP packets. This is so that the initial packets it transmits to the remote peer will cause its local firewall to accept and forward packets subsequently received from the remote peer. The flows in both directions will have symmetric IP addresses and ports, and the initial outbound VoIP packets are sufficient for the AP to generate the correct rule for QoS treatment of the inbound downlink VoIP packets from the peer using MSCS.

In the case of virtual private network (VPN) connections — such as using IPsec — TCP or UDP encapsulation is often used to facilitate NAT traversal, and the outer IP addresses and ports are typically symmetric. In many cases, the VPN client uses a constant UP to send all uplink VPN packets, irrespective of the nature of the payload or any DSCP marking on inner IP headers within the VPN tunnel. For example, if the VPN is primarily carrying video traffic, the VPN client might use UP 4 or 5, or the Video access category, to send all uplink VPN packets. In this case, if MSCS is activated, the corresponding downlink VPN packets would also be sent using the same UP and access category.

Alternatively, if the VPN client dynamically changes the UP used to send the uplink VPN packets on a packet-to-packet basis, then downlink UP assignment based on MSCS rules would result in instability in the QoS treatment of the downlink VPN packets. In such cases, it is recommended that SCS rules are activated to assign constant UP values (see Stream Classification Service section). Another possible option is to establish multiple VPN connections to carry each of the inner flows with different QoS requirements. If the IP 5-tuple of each VPN connection is non-identical, the QoS treatment of the downlink packets for each VPN connection can be managed using MSCS.

Note that, in use cases where the VPN endpoints perform (outer) DSCP marking and that marking is preserved end-to-end across the network, DSCP mapping can be used to assign the UP without using either MSCS or SCS.

Stream Classification Service (SCS)

Wi-Fi QoS Management APs and client devices optionally support SCS, as defined in IEEE 802.11-2020 and extended in IEEE 802.11be.

For downlink flows, SCS is similar to MSCS in the sense that it also allows a client device to request its AP to assign downlink IP flows destined to that client device to the desired access categories. However, whereas with MSCS the AP implicitly derives QoS rules by monitoring the corresponding uplink IP flows, with SCS the request from the STA explicitly provides the AP with the IP classifier and UP for each downlink IP flow. MSCS and SCS are complementary and designed to be used independently or together. SCS can be used to specify QoS rules for certain downlink IP flows that MSCS does not address — for example, downlink flows for which there is no corresponding uplink flow with symmetric addresses/ports, or downlink flows that require different QoS treatment but have the same IP 5-tuple, and so need to be classified based on additional IP header parameters. SCS also allows traffic characteristics (e.g., traffic data rate and burst size) and QoS KPIs (e.g., latency bound) to be specified by the client device in its request as inputs to the AP's downlink scheduler.

For uplink flows, SCS allows a Wi-Fi 6 or Wi-Fi 7 client device to request its Wi-Fi 6 or Wi-Fi 7 AP to schedule resources using trigger frames. The request includes the traffic characteristics and QoS KPIs of the flow, as well as the required cadence of trigger frames that schedule resources for that flow, as inputs to the AP's uplink scheduler.

SCS capability signaling

Wi-Fi QoS Management APs and client devices indicate support for SCS in the Extended Capabilities element in (Re)Association Request and Response frames. APs also indicate support for SCS in Beacon and Probe Response frames.

If the AP or client device also supports QoS Management SCS Traffic Description, then it additionally indicates support for this in the Wi-Fi Alliance Capabilities element and, if it is a Wi-Fi 7 device, also in the EHT Capabilities element. These elements are carried in the same frames as described above.

SCS setup procedures

Activation of SCS rules is always initiated by the client device sending an SCS Request frame to the AP post-association, containing one or more SCS Descriptor elements. Each element corresponds to one SCS rule and specifies the parameters below.

Request Type

The Request Type is set to “add” when the client device is requesting activation of an SCS rule, or to “change” when the client device is requesting modification of an SCS rule that is already activated, or to “remove” to deactivate an SCS rule.

For downlink SCS rules, the “change” request type can be used to change the UP and/or any QoS Characteristics of the flow. However, if the IP classifier of the flow has changed, the SCS rule should instead be removed and a new SCS rule added containing the new TCLAS classifier.

For uplink SCS rules, the “change” request type can be used to change the UP/TID and/or any QoS Characteristics of the flow.

SCSID

The SCSID field indicates an index value, selected determined by the client device, that is a unique identifier of the SCS rule between the AP and the client device.

TCLAS element(s) (and TCLAS Processing element)

The TCLAS element(s) indicate the IP classifier of a downlink SCS rule, as chosen by the client device.

A client device specifies an IP 5-tuple (or partial IP tuple) classifier by including one TCLAS element with Frame Classifier Type of 4 (IP and higher layer parameters). Note that unlike the TCLAS Mask element used in MSCS, this TCLAS element explicitly specifies the IP version (IPv4 or IPv6) and the tuple field values that the classifier matches.

A client device can optionally specify a classifier comprised of both an IP tuple and an IPsec Security Parameter Index (SPI) value, by also including a second TCLAS element with Frame Classifier Type of 10 (IP extensions and higher layer parameters) and Protocol Instance of 0, together with a TCLAS Processing element with Processing value of 0 (match all). If the IPsec packets use ESP protocol (per IETF RFC 4303), the Filter Mask and Filter Value specify the SPI field in the first four octets of the ESP protocol header. If the IPsec packets use UDP protocol with ESP encapsulation (per IETF RFC 3948), the Filter Mask and Filter Value specify the four-octet SPI field offset by eight octets from the start of the UDP header.

For uplink SCS rules, no IP tuple classifier is specified, and therefore the TCLAS element is not included.

User Priority

For downlink SCS rules, the UP is specified in the Intra-Access Category Priority element within the SCS Descriptor element and specifies the UP to be assigned to IP packets matching the classifier.

For uplink SCS rules, since the AP does not perform UP assignment, the Intra-Access Category Priority element is not included. However, the UP /TID of the uplink flow is specified in the QoS Characteristics element (see below) within the SCS Descriptor element so that the AP can schedule resources for the flow using trigger frames where the corresponding RU allocation has an appropriate Preferred AC value.

QoS Characteristics element

For downlink SCS rules, a QoS Characteristics element can be optionally included within the SCS Descriptor element and indicates the traffic characteristics and QoS KPIs for that flow.

For uplink SCS rules, a QoS Characteristics element is always included and indicates the traffic characteristics, QoS KPIs, and required cadence of trigger frames that schedule resources for that flow.

The QoS Characteristics element can only be included when both the AP and client device support QoS Management SCS Traffic Description. Hence, if this is not the case, uplink SCS rules cannot be established.

Table 2 gives a summary of the key fields in the QoS Characteristics element.

Field	Presence in Element	Description
UP / TID	Always present	Indicates direction of the SCS rule (uplink or downlink). If QoS Characteristics element is absent, the SCS rule is in downlink direction.
Minimum / Maximum Service Interval	Always present	The UP that is used for the flow. For a downlink flow, this is equal to the UP in the Intra-Access Category Priority element.
Minimum Data Rate	Always present	The minimum required throughput for the IP flow over the Wi-Fi link, averaged over bursts in the traffic flow.
Delay Bound **and** **MSDU Delivery Info**	Always present Optionally present	The maximum acceptable latency for packets in the flow over the Wi-Fi link. If the MSDU Delivery Info field is also present, it indicates the measurement duration and confidence level for which the Delay Bound is specified. For example, if Delay Bound of 10 ms and MSDU Delivery Ratio of 99% are indicated, it is expected that 99% of packets in the flow will have latency less than 10 ms.
Service Start Time and Service Start Time LinkID	Optionally present	The time at which a (future) burst of packets in the flow is expected to be ready for transmission over the Wi-Fi link, referenced to the TSF of the BSS (or, in MLD case, the link specified by the Service Start Time LinkID field). Note: This is particularly useful to minimize the latency of isochronous uplink SCS flows, by helping the AP to optimize the timing of trigger frames to align with the timing of bursts of packets in the flow.
Mean Data Rate	Optionally present	The mean desired throughput for the IP flow over the Wi-Fi link. This desired mean throughput is larger than the minimum required throughput indicated in the Minimum Data Rate field
MSDU Lifetime	Optionally present	The maximum latency over the Wi-Fi link for which a received packet in the IP flow is useful. Note: If a packet is pending transmission for longer than this period, the transmitter can decide to drop the packet.

Table 2: Fields of the QoS Characteristics element

If the AP accepts a request for an SCS rule from the client device, it activates and begins executing (see below) the SCS rule for that client device or updates the parameters of the rule if it was already activated. It then responds by indicating success for that SCSID in an SCS Response frame.

If the AP does not accept the request for that SCS rule, it provides a status code for that SCSID that might indicate the reason for rejection, such as insufficient processing resources, unsupported TCLAS parameters, or other reasons such as conflict with a local policy. If the request contained a QoS Characteristics element, the rejection might indicate alternative parameters for this element that might be accepted by the AP.

SCS termination procedures and roaming

An AP or client device can terminate an active SCS rule at any time. An AP terminates an SCS rule with a client device by sending an unsolicited SCS Response frame to that client device, including an SCS Status duple containing the SCSID of that rule and a status code value that might indicate the reason for the termination. Examples of termination reasons include exhausted processing resources, insufficient network capacity to support the QoS rule, or a conflict with network policies (which, presumably, did not conflict at the time the SCS rule was originally accepted by the AP). A client device terminates an SCS rule by sending an SCS Request frame with an SCS Descriptor element containing the SCSID of that rule with request type set to "remove".

Similar to MSCS, any active SCS rules between an AP and client device are implicitly terminated at such time that the client device is no longer associated with the AP, or reassociates with the same AP. While some network implementations might derive network-wide QoS policies based on SCS rules, in general it should not be expected that SCS rules or states propagate beyond a single BSS (or, for a Wi-Fi 7 case, a single AP MLD). If a client device has activated one or more SCS rules with an AP and then roams to another BSS in the network where it wishes to continue to use those SCS rules, in general the client device needs to request activation of the SCS rules with the new AP in the target BSS immediately after the roam (re)association. This applies regardless of whether the target BSS is operated by the same physical AP, except for a Wi-Fi 7 case where SCS applies to all links of an ML association.

SCS rule execution

If a downlink SCS rule is activated at an AP for a given client device, the AP attempts to classify the downlink IP packets destined for that client device by matching against the classifier of that rule. An example of a downlink SCS rule that causes downlink IPsec packets from a server with IPv6 address of WAN_IPADDR to a client device with IPv6 address of STA_IPADDR using ESP protocol with SPI value of 0x1234 to be assigned to UP 5 is shown below.

{IPver=6; SrcIPAddr=WAN_IPADDR; DstIPAddr=STA_IPADDR; SrcPort=WAN_PORT; ProtNxtHdr=50; FilterMask=0xFFFFFFFF; FilterValue=0x12345678} ➔ UP=5

If a QoS Characteristics element is included in a downlink SCS rule, the AP is expected to schedule the classified IP packets such that the delay bound and minimum data rate parameters are met.

If a downlink IP packet matches multiple SCS rules, the rule with the most granular classifier is used (see IEEE 802.11-2020 for details). If both MSCS and SCS are simultaneously activated, the AP first attempts to match a downlink IP packet to the SCS rules; if a matching rule does not exist, it then attempts to match the packet to the rules derived from MSCS mirroring. If there is no matching SCS or MSCS rule, and no other network policy is configured that takes precedence, then by default the packet's UP will be assigned based on DSCP mapping.

If an uplink SCS rule is activated at an AP for a given client device, the AP is expected to schedule trigger frames with RU allocation for the client device and the corresponding Preferred AC such that the delay bound, minimum data rate, and minimum/maximum service interval parameters in the QoS Characteristics element are met.

Applicability of SCS

Since an SCS request explicitly specifies the classifier for a rule, it does not (unlike MSCS) require a corresponding uplink IP flow with symmetric IP addresses and ports to exist, and it allows a different UP to be assigned to the downlink flow compared to the uplink flow (if it exists).

With SCS the client device needs to explicitly request a rule for each downlink IP flow individually. The complexity and overhead of SCS signaling can be high if a large number of flows need to be managed simultaneously and/or the IP flows are short-lived. In some use cases, partial IP tuple classifiers can help reduce the amount of signaling, e.g., by omitting (wildcard) Destination Port in the TCLAS element classifier if the application creates many short-lived connections from the same remote IP address and port to different local ports, all of which require the same QoS treatment. In addition, since it is possible to simultaneously activate MSCS and SCS, it is only necessary to request SCS rules for downlink IP flows that will not be appropriately handled by rules derived from MSCS mirroring.

The client device should ensure that it terminates SCS rules for IP flows that are no longer active, to avoid excessive processing overhead on the AP (or the AP rejecting new requests due to exhausted classification resources).

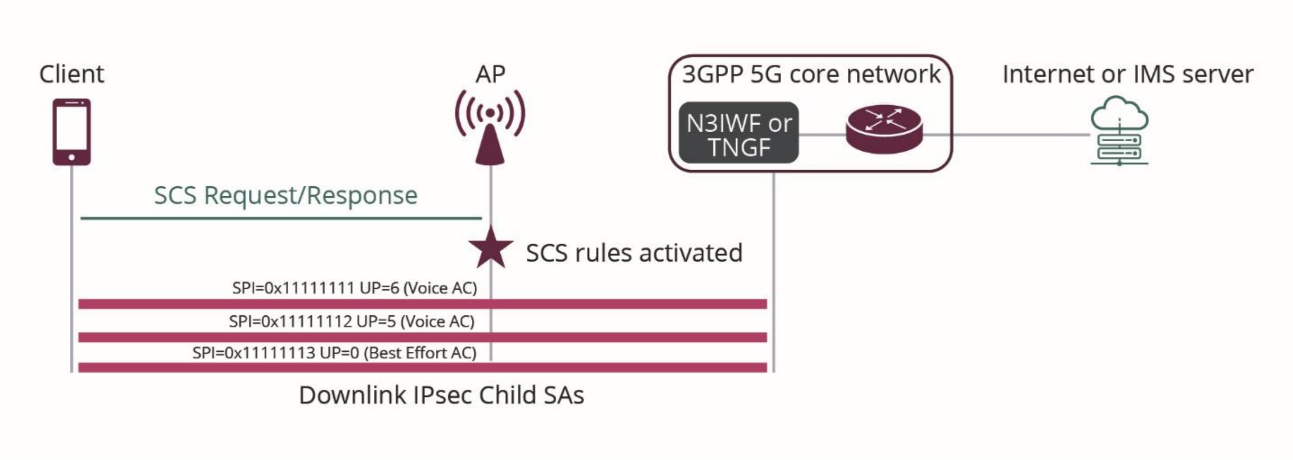


Figure 5: Example of SCS rule derivation and execution

Since SCS allows a rule classifier to be defined based on parameters in protocol/extension headers (in addition to IP tuple parameters), it can support use cases such as QoS differentiation in Wi-Fi access to 3GPP 5G core networks, where IPsec with multiple child SAs is used between the client device and the N3IWF or TNGF gateway (see 3GPP TS 24.502). For example, as shown in Figure 5, the client device might send an SCS request to its AP at the time the child SAs are initiated and the corresponding SPI values, and the 5G QoS Identifiers (5QIs) of the QoS flows associated with each child SA (which can be mapped to a UP for each child SA), are known by the client device.

DSCP mapping

In managed enterprise and carrier Wi-Fi networks, it is common for the network manager to configure certain DSCP marking policies as part of network wide QoS management. Downlink traffic might be DSCP marked at source for servers managed by the enterprise or carrier. Alternatively, downlink traffic might be DSCP marked at ingress to the network based on classification rules for traffic originating from third party servers on the public internet. In some cases, the network manager can also manage the DSCP marking of uplink traffic at source using Group Policy Objects (GPO) or Mobile Device Management (MDM) tools deployed on managed client devices. As discussed in the context of MSCS, some mobile applications apply specific DSCP marking to QoS sensitive uplink flows by default, even in the absence of GPO or MDM policies.

In these situations, the network manager typically wants to manage the mapping between DSCP values and UPs on both APs and client devices to achieve differentiated QoS for flows with prioritized DSCP marking even under varying network load. Wi-Fi QoS Management certified APs and client devices are required to support the default DSCP-to-UP Mapping table defined in IETF RFC 8325, and also to support the QoS Map feature defined in IEEE 802.11 to indicate exceptions to that default mapping. This applies to both downlink and uplink IP packets.

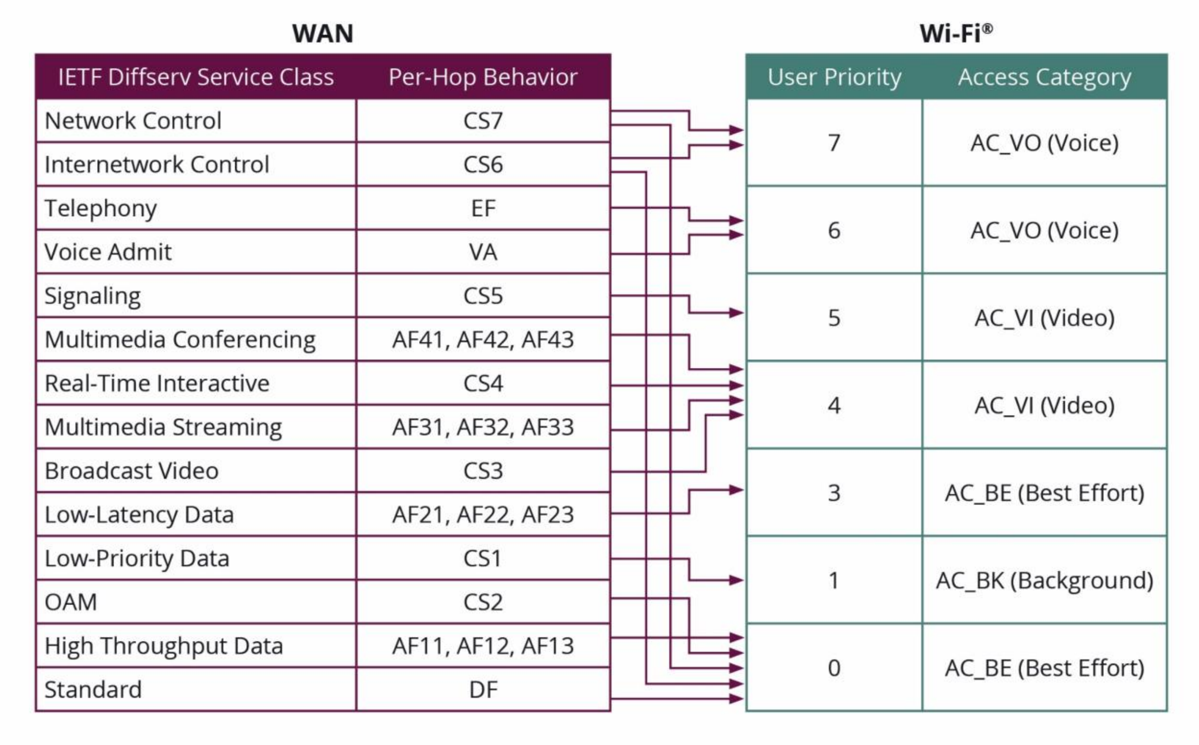
DSCP-to-UP mapping execution

When no other UP assignment policies such as vendor-specific classifiers, virtual local area network (VLAN) tag mapping, or MSCS rules apply, an AP or client device determines the UP by examining the DSCP value in the IP header of the packet in the following manner:

> When the QoS Map feature is not enabled, the device is required to use the mapping table in Figure 5 based on IETF RFC 8325. In cases where a given DSCP value maps to multiple UP values, the device can use either value depending on its local policy. If the DSCP marking of a packet is not specified in this

figure, the default UP mapping is not defined. There is an exception: for APs it is recommended that DSCP values not authorized for use over the network are mapped to UP 0.

The DSCP-to-UP Mapping table defined in RFC 8325 addresses inconsistencies in legacy mapping tables. Some legacy implementations perform the mapping simply by using the three most significant bits of the DSCP value, also known as the deprecated “preference” value, as the UP. This results in voice flows that are marked DSCP Expedited Forwarding (EF) being allocated to UP 5, the Video access category, instead of UP 6 or 7, the Voice access category. Other legacy implementations use the example mapping tables included in earlier versions of the IEEE 802.11 standard. This results in video flows that are marked DSCP CS4[2] being allocated to UP 6, or the Voice access category, instead of UP 4 or 5, the Video access category. The use of the RFC 8325 mapping table by default ensures consistency between QoS treatment over Wi-Fi and the networking industry consensus on QoS traffic marking.



WAN

IETF Diffserv Service Class	Per-Hop Behavior
Network Control	CS7
Internetwork Control	CS6
Telephony	EF
Voice Admit	VA
Signaling	CS5
Multimedia Conferencing	AF41, AF42, AF43
Real-Time Interactive	CS4
Multimedia Streaming	AF31, AF32, AF33
Broadcast Video	CS3
Low-Latency Data	AF21, AF22, AF23
Low-Priority Data	CS1
OAM	CS2
High Throughput Data	AF11, AF12, AF13
Standard	DF

Wi-Fi®

User Priority	Access Category
7	AC_VO (Voice)
6	AC_VO (Voice)
5	AC_VI (Video)
4	AC_VI (Video)
3	AC_BE (Best Effort)
1	AC_BK (Background)
0	AC_BE (Best Effort)

Figure 6: DSCP-to-UP Mapping based on RFC 8325

When the QoS Map feature is enabled on a Wi-Fi QoS Management AP or client device and a non-default DSCP-to-UP Mapping table is configured, the device must use that table for its own transmissions, instead of the IETF RFC 8325 default mapping table. A non-default mapping table might be used as part of network management to avoid excessive use of a high priority access category, and/or to specify the mapping for non-standard local use DSCP values that are in use on the network.

QoS Map signaling and configuration

A Wi-Fi QoS Management AP and client device advertise support for QoS Map in the Extended Capabilities element. The means by which the network manager configures a QoS Map table on an AP is not defined but is typically performed using vendor-specific or standards-based (e.g., see Wi-Fi Data Elements™ and Wi-Fi EasyMesh™) management interfaces. To configure a non-default DSCP-to-UP Mapping table on a client device, the AP either includes the QoS Map table in the (Re)Association Response frame at association or includes the table in a QoS Map Configure frame sent to the client device post-association. The QoS Map element present in these frames defines the DSCP-to-UP Mapping table in the form of non-overlapping ranges of DSCP values.

[2] CS4 is a DSCP name associated to DSCP value 32, as defined in IETF per RFC 4594.

These DSCP values map to each UP value, together with a list of exceptions for specific DSCP values, or ranges of values, for which a specific UP mapping is defined.

QoS Map lifetime and roaming

When QoS Map is used to configure a non-default DSCP-to-UP Mapping table on a client device, the configuration applies for the duration of the client device association to that BSS (or, for a Wi-Fi 7 case, that AP MLD). Therefore, if the network configures a client device using QoS Map and that client device then roams to another BSS (or AP MLD) in the network, the AP in the target BSS (or the target AP MLD) should configure the same mapping table using QoS Map during or immediately after the roam (re)association so that the client device continues to perform consistent DSCP-to-UP Mapping after the roam.

Applicability of QoS Map

The QoS Map feature allows the network manager to manage the QoS treatment of both downlink IP packets sent by APs, and uplink IP packets sent by the client device with a given DSCP marking. For downlink traffic, the network manager can configure DSCP (re)marking of IP flows within the network infrastructure as needed. For uplink traffic, the client device might determine the (initial) DSCP marking based on vendor-specific application or operating system policies, or based on policies determined by the network manager and configured by the DSCP Policy feature (see DSCP Policy section below).

DSCP Policy

Wi-Fi QoS Management APs and client devices optionally support the DSCP Policy feature, as defined in the QoS Management specification. The DSCP Policy feature enables an AP to request a client device to apply DSCP marking to specific uplink traffic flows, which are identified by a classifier based on IP tuple, port range and/or destination domain name. The DSCP Policy feature can be used in conjunction with QoS Map, where the former specifies the DSCP marking rules and the latter provides the mapping from DSCP marking to UP.

The DSCP Policy feature allows finer-grained QoS management for uplink IP flows. For example, it enables configuration of policies that cause IP flows that would otherwise be marked with the same DSCP value (e.g., Default Forwarding) to instead be marked with different DSCP values, and therefore assigned to different UPs. It can be used in combination with GPO or MDM tools for dynamic policy management on managed client devices and can also be used with unmanaged client devices on guest or public networks.

DSCP Policy capability signaling

Wi-Fi QoS Management APs and client devices indicate support for DSCP Policy in the Wi-Fi Alliance Capabilities element in (Re)Association Request and Response frames. APs also indicate support for DSCP Policy in Beacon and Probe Response frames.

DSCP Policy setup procedures

An AP activates DSCP policies on a client device by sending a DSCP Policy Request frame to the client device post-association, containing one or more QoS Management elements. The request frame can be sent unsolicited, or can be sent in response to a DSCP Policy Query frame sent by the client device (which might indicate classifier(s) of policies the client device is interested in). Each Wi-Fi QoS Management element in the DSCP Policy Request frame corresponds to one DSCP policy and specifies the parameters below.

Request Type

The Request Type (in the DSCP Policy attribute) is set to “add/update” when the AP is requesting activation of a new DSCP policy or update of an existing policy, or to “remove” when the AP is requesting removal of an existing DSCP policy.

DSCP Policy ID

The DSCP Policy ID (in the DSCP Policy attribute) indicates an index value, determined by the network, that is a unique identifier of the DSCP policy between the network and the client device.

DSCP

The DSCP value (in the DSCP Policy attribute) specifies the DSCP marking to be applied to IP packets matching the classifier.

TCLAS, Domain Name and Port Range attributes

One or more of the TCLAS attribute, Domain Name attribute and Port Range attribute is included by the AP to specify the classifier for the DSCP policy. If a TCLAS attribute is included, the classifier includes (partial) IP tuple parameters of the uplink flow, such as the destination IP address and/or port. If a Domain Name attribute is included, the classifier includes a domain name that is matched to the FQDN of the remote host of the uplink flow on a label-wise suffix match basis. If a Port Range attribute is included, the classifier includes a destination port range.

If the client device accepts a DSCP policy, it activates the policy, or if it was already activated, updates the DSCP marking for that policy. It then responds by indicating Success for that DSCP Policy ID in a DSCP Policy Response frame.

If the client device does not accept the request for that DSCP Policy, it provides a status code for that DSCP Policy ID that might indicate the reason for rejection, such as insufficient processing resources, unsupported classifier parameters, or other reasons such as conflict with a client device policy (e.g., local app/OS policy, or policy remotely configured by an MDM tool).

Configuration of DSCP policies can be split across multiple request and response frames. The AP can indicate that it has more policies for the client device that are not included within a given DSCP Request frame by setting the "More" indication; similarly, the client device can indicate its interest in receiving more policies by indicating "More" in a DSCP Response frame.

DSCP policy termination procedures and roaming

An AP or client device can terminate an active DSCP policy at any time. A client device terminates a DSCP policy by sending an unsolicited DSCP Policy Response frame to the AP indicating either "Reset" if all policies are being terminated or indicating the DSCP Policy ID of the policy and a status code that indicates the reason for the termination – either that the client device now has insufficient processing resources to handle the policy, or another reason such as conflict with a client device policy which, presumably, did not exist when the client device originally accepted the policy. An AP terminates a DSCP policy by sending a DSCP Policy Request frame indicating either "Reset" if all policies are to be terminated, or containing a QoS Management element indicating the DSCP Policy ID of the policy and Request Type set to "remove".

Unlike MSCS, SCS and QoS Map, DSCP policies continue to apply across roams between BSSs within the same ESS. DSCP policies are implicitly terminated at such time that the client device is no longer associated with the network. Any AP in the network can modify or terminate DSCP policies that were previously activated on client devices – either by specifying the corresponding DSCP Policy IDs if known by the AP, e.g., in a centralized management implementation, or, if the AP does not know those DSCP Policy IDs, by using the "Reset" indication to terminate all policies and activate new ones using DSCP Policy IDs determined by this AP.

DSCP Policy execution

If one or more DSCP policies are activated at a client device, the client device performs DSCP marking for the uplink IP flows it sends to the network, in accordance with the classifiers specified in those policies. An example of a DSCP policy that causes uplink IP packets sent to a remote host with example.com domain suffix on port 443 to be marked with DSCP 46 (EF) is shown below.

{DomainName=example.com; PortRange={443,443}} ➔ DSCP=46

If an uplink IP packet matches multiple DSCP policies, the policy with the most granular classifier is used (see Wi-Fi QoS Management Specification for details). If there is a tie and domain name classifiers are specified, the policy specifying the lowest level domain is used.

Applicability of DSCP Policy

Since the client device is typically an IP endpoint, an implementation might efficiently execute DSCP policies by setting the DSCP option on sockets that match the classifier to the corresponding value. Alternatively, execution of IP tuple based policies might be implemented by per-packet classification and (re)marking.

A DSCP policy that specifies a domain name classifier is applicable when the application layer identifies the corresponding remote host by an FQDN. Such classifiers can be useful when DNS load balancing is used so the remote host's IP address may not be known by the network a-priori.

If the application layer only identifies the remote host by IP address, then flows to that host will not match a DSCP policy with a domain name classifier; a DSCP policy that specifies an IP tuple based classifier must be used instead.

3GPP 5G QoS to Wi-Fi QoS Mapping

The QoS Management specification defines a default mapping table between 3GPP 5G QoS parameters (5QI, Priority Level, Packet Delay Budget, Guaranteed Flow Bit Rate, etc.) and Wi-Fi QoS parameters (UP, Delay Bound, Minimum Data Rate, etc.).

This mapping can be used by a client device to determine the parameters in an SCS request when the client device is connected to a 3GPP 5G core network over Wi-Fi access.

In addition, the mapping can be used by a gateway device with 3GPP backhaul when forwarding packets from the 3GPP network into the Wi-Fi network.

Deployment of QoS mechanisms

The efficient use of unlicensed spectrum used by Wi-Fi requires good faith use of mechanisms that enable prioritized access to that spectrum. Therefore, it is important that all entities that leverage Wi-Fi QoS Management features do so in a reasonable and responsible manner.

Network IT managers should implement mechanisms that assign the appropriate UP to the corresponding traffic flow to facilitate maximum network efficiency. Since the highest priority access categories use smaller contention windows (CWmin, CWmax), the probability of collision increases when the traffic volume using those access categories increases. Network efficiency can degrade substantially in such scenarios, even when the number of contending transmitters is small. In addition, since the highest priority access category is, by default, associated with a short TXOP length, use of that category can substantially decrease the throughput achieved in the presence of contending devices since the total airtime obtained is reduced.

Developers of applications and services that use Wi-Fi can help ensure appropriate and effective use of these mechanisms by leveraging industry best practices when assigning DSCP marking to IP flows, per the service classes defined in IETF RFC 4594. Client device operating systems can help ensure that applications use appropriate access categories for uplink traffic and negotiate activation of MSCS and/or SCS with the AP when QoS sensitive services are active. This helps guarantee that the same access categories are used for the corresponding downlink traffic.

AP implementations can help ensure suitable network policies are configured for downlink traffic and monitor use of high priority access categories. APs can then take suitable action, such as modifying network policies, MSCS activations, QoS Map tables and DSCP policies if excessive use of those access categories is detected, causing unacceptable impact on network performance or medium access fairness.

The features defined in the Wi-Fi QoS Management program are focused on enabling the appropriate assignment of UPs and access categories to IP flows, as well as the exchange of traffic characteristics and QoS KPIs to assist the AP's scheduler and queue management, in order to achieve prioritized, differentiated QoS. Other complementary QoS treatment mechanisms such as explicit reservation of over-the-air resources, and core network traffic management such as packet shaping, might be managed by other network policies and/or protocols, including WMM-Admission Control.

Wi-Fi QoS Management use cases

Online gaming

An online gaming application on a mobile client device communicates with one or more servers to synchronize game play across all users. The game leverages APIs provided by the client device's operating system to set the UP with which uplink IP flow is sent to its AP and toward the online servers. For example, the application could set UP 6, or the Voice access category, for latency-sensitive data flows, UP 5, or the Video access category, for a real-time video streaming flow, and UP 0, or the Best Effort access category, for a non-real-time media assets flow, such as game updates that run in the background while the user plays the game.

The applications on the client device achieve prioritized QoS treatment for uplink IP flows based on the device's rules. The rules may be strictly local to the device or apply industry general best practices, such as RFC 4594. For example, the latency-sensitive data flows may match the definition of RFC 4594 Telephony class, which applies to jitter sensitive traffic with small, fixed size packets emitted at a constant rate.

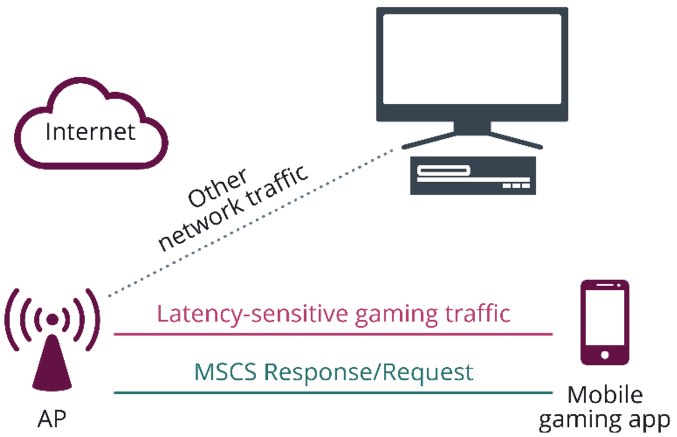


Figure 7: QoS in mobile gaming

In this example, the DSCP markings of all the corresponding downlink IP flows that arrive at the AP from the internet are equal to 0, the QoS behavior Default Forwarding. If the AP were to assign the UP of each flow based on the DSCP marking, then all the flows would be sent in the Best Effort access category. As a result, particularly when the channel is loaded, the game metadata and real-time video sessions might not achieve their latency, jitter, and throughput requirements. However, since the client device activated MSCS, the AP sets the UPs of the downlink flows based on the UPs of the corresponding uplink flows. These are determined by the client device application instead of the downlink DSCP marking. Therefore, the user experience of the game is consistently high.

The Wi-Fi QoS Management program enables the client gaming application to influence the prioritization of IP data flows to maximize performance in that application. As a result, the game meets the requirements for low latency, low or no jitter, and high throughput, giving the user a consistently good playing experience.

Enterprise videoconferencing and remote training

Enterprises deploy various network services, including videoconferencing for mission critical communications and collaboration, and video streaming services for employee training. In environments with frequent videoconferencing and remote training, network administrators are tasked with ensuring high quality service in those applications. To do so, the network administrator may typically configure DSCP marking on the network and, where possible, on managed client devices so that videoconferencing flows are marked with the Assured Forwarding (AF) behavior class AF41 and EF, for Video and Voice, respectively, while the video streaming flows are marked AF31.[3] Default DSCP-to-UP Mapping ensures that the AP and client devices send the video flows in the Video access category, and the voice flows in the Voice access category. During a busy hour of peak network activity, the network is close to capacity and the videoconferencing service quality is at risk of degrading. Administrators trigger a network policy which configures the APs and client devices with a QoS Map, which maps the DSCP AF31 video streaming flow to UP 0, the Best Effort access category, instead of UP 4, the Video access category. This reduces the priority of the video streaming service with minimal impact on that service, to

[3] AF41 and AF31 are values as defined in RFC 4594.

preserve sufficient network capacity and channel access priority for the mission critical videoconferencing service.

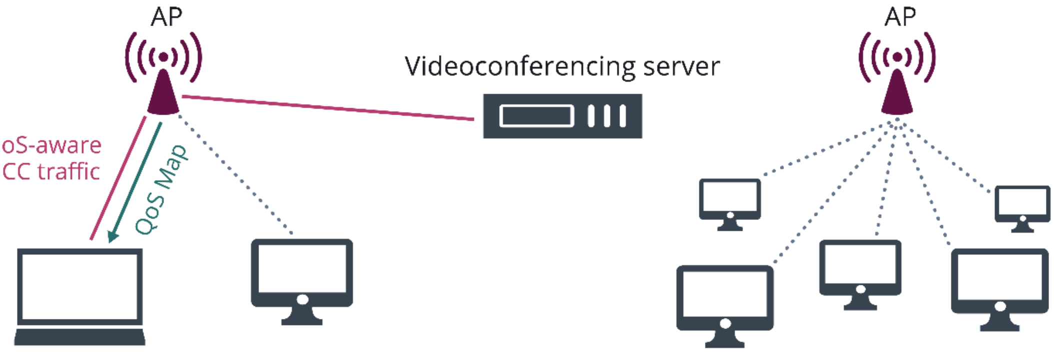


Figure 8: QoS in videoconferencing and remote training

QoS support in Wi-Fi access to 3GPP 5G core networks

When a client device accesses a 3GPP 5G core network over Wi-Fi, there may be multiple simultaneous data flows that require different QoS treatment, unlike 3G and 4G Wi-Fi Calling, for which QoS treatment is typically only needed for a single voice data flow. Downlink and uplink data flows with different QoS profiles are assigned to different IPsec child SAs between the Wi-Fi client device and the core network. Since the client device is aware of these mappings, SCS provides a convenient method for the client device to request the AP to apply appropriate QoS treatment for each downlink child SA, based on its unique index (SPI). For uplink child SAs, the client device can assign the appropriate QoS treatment for each child SA autonomously, e.g., using DSCP marking. As a result, QoS sensitive traffic such as gaming, voice and video will be prioritized bidirectionally over other bulk data traffic.

AR service in a sports stadium

When a service with demanding QoS requirements such as AR-enhanced gameplay is deployed in a sports stadium, the throughput and delay KPIs must be met in the presence of heavy traffic load from other applications such as social network live streaming and web. The DSCP Policy feature provides a way for the stadium's network to dynamically request the client devices to apply specific DSCP marking to different uplink traffic flows including the AR flows. In conjunction with the QoS Map feature, this allows the network to control relative prioritization of the traffic flows in the network to ensure the KPIs of the AR service are met.

VR gaming

A user wears a VR headset (and possibly also sensor-equipped gloves or hand controllers) to play a multiplayer VR game at home. Other uses in the same home, and in adjacent houses, are streaming video and surfing the web. The VR headset provides an immersive, first-person perspective of in-game action. Multiple QoS-sensitive flows are generated between the VR headset and a cloud server, and possibly also between the VR headset and a VR rendering device on the local network or the cloud. These real-time flows include bidirectional multi-channel HD audio, haptic data, pose and controller data, and possibly very high resolution and high frame rate video. If the QoS requirements for these flows (such as strict latency bounds) are not met, it can lead to a poor user experience and potentially contribute to so-called "VR sickness".

The VR headset (as the client device) sends SCS requests to its AP, including QoS Characteristics, which indicate the QoS requirements for each individual flow. For example, one of the SCS descriptors describes a downlink real-time audio flow, indicating its TCLAS classifier, requesting UP 6 (voice), and indicating the flow data rate is 2 Mbps and the latency bound is 15 ms at the 99th percentile. Another of the SCS descriptors describes an uplink pose and controller data flow, indicating it will use UP 6 (voice), that the flow rate is 2 Mbps, the latency bound is 2 ms at the 90th percentile, and the service interval ranges between 2 ms and 20 ms.

The AP's scheduler then performs classification and prioritization for the downlink flows and schedules transmission of trigger frames for the uplink flows in order to ensure the indicated QoS KPIs are achieved and the user has a positive experience of the VR game even in the presence of the other users' traffic.

Summary

The increased bandwidth and faster speeds delivered by Wi-Fi networks have enabled applications such as high-definition video, advanced telemedicine, ultra low latency gaming, and AR/VR. This trend will continue as video traffic growth increases. To deliver good quality of experience in these applications it is essential that Wi-Fi networks support a range of service categories that differentiate and prioritize data flows for such applications. Wi-Fi networks that give equal priority access to all connected devices and data flows cannot provide the throughput and stability required when traffic demands exceed the available bandwidth. This negatively impacts the user experience. Access to additional spectrum and newer Wi-Fi generations, such as Wi-Fi 6 and Wi-Fi 7, provide capabilities to better handle traffic with very low latency requirements, and Wi-Fi QoS management further improves the user experience by ensuring the interactions among the participants of real-time applications, such as voice-over-Wi-Fi videoconferencing, AR/VR, telemedicine, and interactive gaming, are timely and avoid skipping audio or stalled video.

The features of the Wi-Fi QoS Management certification program provide simple, flexible standardized mechanisms to enable robust delivery of an expanding range of services with low latency requirements. The program helps devices leverage knowledge of application-specific QoS requirements both on clients and on the network. With appropriate use, these features provide strong benefits across a wide range of Wi-Fi deployments, including residential, enterprise, and public networks.

About Wi-Fi Alliance®

www.wi-fi.org

Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®. Members of our collaboration forum come together from across the Wi-Fi ecosystem with the shared vision to connect everyone and everything, everywhere, while providing the best possible user experience. Since 2000, Wi-Fi Alliance has completed more than 80,000 Wi-Fi certifications. The Wi-Fi CERTIFIED® seal of approval designates products with proven interoperability, backward compatibility, and the highest industry-standard security protections in place. Today, Wi-Fi carries more than half of the internet's traffic in an ever-expanding variety of applications. Wi-Fi Alliance continues to drive the adoption and evolution of Wi-Fi, which billions of people rely on every day.

Follow Wi-Fi Alliance:

wi-fi.org/beacon
wi-fi.org/signal
facebook.com/wificertified
twitter.com/wifialliance
linkedin.com/company/wi-fi-alliance
youtube.com/wifialliance