Diffserv to IEEE 802.11 Mapping
draft-ietf-tsvwg-ieee-802-11-10

Abstract

   As internet traffic is increasingly sourced-from and destined-to
   wireless endpoints, it is crucial that Quality of Service be aligned
   between wired and wireless networks; however, this is not always the
   case by default. This document specifies a set of Differentiated
   Services Code Point (DSCP) to IEEE 802.11 User Priority (UP) mappings
   to reconcile the marking recommendations offered by the IETF and the
   IEEE so as to maintain consistent QoS treatment between wired and
   IEEE 802.11 wireless networks.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on June 18, 2018.

Table of Contents

1. Introduction

   IEEE 802.11 [IEEE.802.11-2016] wireless has become the preferred
   medium for endpoints connecting to business and private networks.
   However, the wireless medium defined by IEEE 802.11
   [IEEE.802.11-2016] presents several design challenges for ensuring
   end-to-end quality of service. Some of these challenges relate to
   the nature of the IEEE 802.11 Radio Frequency (RF) medium itself,
   being a half-duplex and shared medium, while other challenges relate
   to the fact that the IEEE 802.11 standard is not administered by the
   same standards body as IP networking standards. While the IEEE has
   developed tools to enable QoS over wireless networks, little guidance
   exists on how to maintain consistency of QoS treatment between wired
   IP and wireless IEEE 802.11 networks. The purpose of this document
   is to provide such guidance.

1.1. Related work

   Several RFCs outline Diffserv QoS recommendations over IP networks,
   including:

   o [RFC2474] specifies the Diffserv Codepoint Field. This RFC also
      details Class Selectors, as well as the Default Forwarding (DF)
      treatment.

   o [RFC2475] defines a Diffserv architecture

   o [RFC3246] specifies the Expedited Forwarding (EF) Per-Hop Behavior
      (PHB)

o [RFC2597] specifies the Assured Forwarding (AF) PHB.

o [RFC3662] specifies a Lower Effort Per-Domain Behavior (PDB)

o [RFC4594] presents Configuration Guidelines for Diffserv Service
   Classes

o [RFC5127] presents the Aggregation of Diffserv Service Classes

o [RFC5865] specifies a DSCP for Capacity Admitted Traffic

Note: [RFC4594] is intended to be viewed as a framework for
supporting Diffserv in any network, including wireless networks;
thus, it describes different types of traffic expected in IP networks
and provides guidance as to what DSCP marking(s) should be associated
with each traffic type. As such, this document draws heavily on
[RFC4594], as well as [RFC5127], and [RFC8100].

In turn, the relevant standard for wireless QoS is IEEE 802.11, which
is being progressively updated; the current version of which (at the
time of writing) is [IEEE.802.11-2016].

1.2. Interaction with RFC 7561

There is also a recommendation from the Global System for Mobile
Communications Association (GSMA) on DSCP to UP Mapping for IP Packet
eXchange (IPX), specifically their Guidelines for IPX Provider
networks [GSMA-IPX_Guidelines]. These GSMA Guidelines were developed
without reference to existing IETF specifications for various
services, referenced in Section 1.1. In turn, [RFC7561] was written
based on these GSMA Guidelines, as explicitly called out in [RFC7561]
Section 4.2. Thus, [RFC7561] conflicts with the overall Diffserv
traffic-conditioning service plan, both in the services specified and
the code points specified for them. As such, these two plans cannot
be normalized. Rather, as discussed in [RFC2474] Section 2, the two
domains (IEEE 802.11 and GSMA) are different Differentiated Services
Domains separated by a Differentiated Services Boundary. At that
boundary, code points from one domain are translated to code points
for the other, and maybe to Default (zero) if there is no
corresponding service to translate to.

1.3. Applicability Statement

This document is applicable to the use of Differentiated Services
that interconnect with IEEE 802.11 wireless LANs (referred to as Wi-
Fi, throughout this document, for simplicity). These guidelines are
applicable whether the wireless access points (APs) are deployed in
an autonomous manner, managed by (centralized or distributed) WLAN

controllers or some hybrid deployment option. This is because in all
these cases, the wireless access point is the bridge between wired
and wireless media.

This document applies to IP networks using WiFi infrastructure at the
link layer. Such networks typically include wired LANs with wireless
access points at their edges, however, such networks can also include
Wi-Fi backhaul, wireless mesh solutions or any other type of AP-to-AP
wireless network that extends the wired network infrastructure.

1.4. Document Organization

This document is organized as follows:

o Section 1 introduces the wired-to-wireless QoS challenge,
   references related work, outlines the organization of the
   document, and specifies both the requirements language and the
   terminology used in this document.

o Section 2 begins the discussion with a comparison of IETF Diffserv
   QoS and Wi-Fi QoS standards and highlights discrepancies between
   these that require reconciliation.

o Section 3 presents the marking and mapping capabilities that
   wireless access points and wireless endpoint devices are
   recommended to support.

o Section 4 presents DSCP-to-UP mapping recommendations for each of
   the [RFC4594] service classes, which are primarily applicable in
   the downstream (wired-to-wireless) direction.

o Section 5, in turn, considers upstream (wireless-to-wired) QoS
   options, their respective merits and recommendations.

o Section 6 (in the form of an Appendix) presents a brief overview
   of how QoS is achieved over IEEE 802.11 wireless networks, given
   the shared, half-duplex nature of the wireless medium.

o Section 7 on notes IANA considerations

o Section 8 presents security considerations relative to DSCP-to-UP,
   UP-to-DSCP mapping and remarking

1.5. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in BCP

14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

1.6. Terminology Used in this Document

Key terminology used in this document includes:

AC: Access Category. A label for the common set of enhanced
distributed channel access (EDCA) parameters that are used by a
quality-of-service (QoS) station (STA) to contend for the channel
in order to transmit medium access control (MAC) service data
units (MSDUs) with certain priorities. [IEEE.802.11-2016]
Section 3.2.

AIFS: Arbitration Interframe Space. Interframe space used by QoS
stations before transmission of data and other frame types defined
by [IEEE.802.11-2016] Section 10.3.2.3.6.

AP: Access Point. An entity that contains one station (STA) and
provides access to the distribution services, via the wireless
medium (WM) for associated STAs. An AP comprises a STA and a
distribution system access function (DSAF) [IEEE.802.11-2016]
Section 3.1.

BSS: Basic Service Set. Informally, a wireless cell; formally, a
set of stations that have successfully synchronized using the JOIN
service primitives and one STA that has used the START primitive.
Alternatively, a set of STAs that have used the START primitive
specifying matching mesh profiles where the match of the mesh
profiles has been verified via the scanning procedure. Membership
in a BSS does not imply that wireless communication with all other
members of the BSS is possible. Defined in [IEEE.802.11-2016]
Section 3.1.

Contention Window: See CW.

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance.
A media access control method in which carrier sensing is used,
but nodes attempt to avoid collisions by transmitting only when
the channel is sensed to be "idle". When these do transmit, nodes
transmit their packet data in its entirety.

CSMA/CD: Carrier Sense Multiple Access with Collision Detection.
A media access control method (used most notably in early Ethernet
technology) for local area networking. It uses a carrier-sensing
scheme in which a transmitting station detects collisions by
sensing transmissions from other stations while transmitting a
frame. When this collision condition is detected, the station

stops transmitting that frame, transmits a jam signal, and then
waits for a random time interval before trying to resend the
frame.

CW: Contention Window. Limits a CWMin and CWMax, from which a
random backoff is computed.

CWMax: Contention Window Maximum. The maximum value (in unit of
Slot Time) that a contention window can take.

CWMin: Contention Window Minimum. The minimum value that a
contention window can take.

DCF: Distributed Coordinated Function. A class of coordination
function where the same coordination function logic is active in
every station (STA) in the basic service set (BSS) whenever the
network is in operation.

DIFS: Distributed (Coordination Function) Interframe Space. A
unit of time during which the medium has to be detected as idle
before a station should attempt to send frames, as per
[IEEE.802.11-2016] Section 10.3.2.3.5.

DSCP: Differentiated Service Code Point [RFC2474] and [RFC2475].
The DSCP is carried in the first 6 bits of the IPv4 and IPv6 Type
of Service (TOS) Byte (the remaining 2 bits are used for IP
Explicit Congestion Notification [RFC3168]).

EIFS: Extended Interframe Space. A unit of time that a station
has to defer before transmitting a frame if the previous frame
contained an error, as per [IEEE.802.11-2016] Section 10.3.2.3.7.

HCF: Hybrid Coordination Function A coordination function that
combines and enhances aspects of the contention based and
contention free access methods to provide quality-of-service (QoS)
stations (STAs) with prioritized and parameterized QoS access to
the wireless medium (WM), while continuing to support non-QoS STAs
for best-effort transfer. [IEEE.802.11-2016] Section 3.1.

IFS: Interframe Space. Period of silence between transmissions
over 802.11 networks. [IEEE.802.11-2016] describes several types
of Interframe Spaces.

Random Backoff Timer: A pseudorandom integer period of time (in
units of Slot Time) over the interval (0,CW), where CWmin is-less-
than-or-equal-to CW, which in turn is less-than-or-equal-to CWMax.
Stations desiring to initiate transfer of data frames and-or
Management frames using the DCF shall invoke the carrier sense

mechanism to determine the busy-or-idle state of the medium. If
the medium is busy, the STA shall defer until the medium is
determined to be idle without interruption for a period of time
equal to DIFS when the last frame detected on the medium was
received correctly, or after the medium is determined to be idle
without interruption for a period of time equal to EIFS when the
last frame detected on the medium was not received correctly.
After this DIFS or EIFS medium idle time, the STA shall then
generate a random backoff period for an additional deferral time
before transmitting. [IEEE.802.11-2016] Section 10.3.3.

RF: Radio Frequency.

SIFS: Short Interframe Space. An IFS used before transmission of
specific frames as defined in [IEEE.802.11-2016]
Section 10.3.2.3.3.

Slot Time: A unit of time used to count time intervals in 802.11
networks, and defined in [IEEE.802.11-2016] Section 10.3.2.13.

Trust: From a QoS-perspective, trust refers to the accepting of
the QoS markings of a packet by a network device. Trust is
typically extended at Layer 3 (by accepting the DSCP), but may
also be extended at lower layers, such as at Layer 2 by accepting
User Priority markings. For example, if an access point is
configured to trust DSCP markings and it receives a packet marked
EF, then it would treat the packet with the Expedite Forwarding
PHB and propagate the EF marking value (DSCP 46) as it transmits
the packet. Alternatively, if a network device is configured to
operate in an untrusted manner, then it would remark packets as
these entered the device, typically to DF (or to a different
marking value at the network administrator's preference). Note:
The terms "trusted" and "untrusted" are used extensively in
[RFC4594].

UP: User Priority. A value associated with a medium access
control (MAC) service data unit (MSDU) that indicates how the MSDU
is to be handled. The UP is assigned to an MSDU in the layers
above the MAC [IEEE.802.11-2016] Section 3.1. The UP defines a
level of priority for the associated frame, on a scale of 0 to 7.

Wi-Fi: An interoperability certification defined by the Wi-Fi
Alliance. However, this term is commonly used, including in the
present document, to be the equivalent of IEEE 802.11.

Wireless: In the context of this document, "wireless" refers to
the media defined in IEEE 802.11 [IEEE.802.11-2016], and not 3G/4G
LTE or any other radio telecommunications specification.

2. Service Comparison and Default Interoperation of Diffserv and IEEE
    802.11

   (Section 6 provides a brief overview of IEEE 802.11 QoS.)

   The following comparisons between IEEE 802.11 and Diffserv services
   should be noted:

   o [IEEE.802.11-2016] does not support an EF PHB service [RFC3246],
      as it is not possible to assure that a given access category will
      be serviced with strict priority over another (due to the random
      element within the contention process)

   o [IEEE.802.11-2016] does not support an AF PHB service [RFC2597],
      again because it is not possible to assure that a given access
      category will be serviced with a minimum amount of assured
      bandwidth (due to the non-deterministic nature of the contention
      process)

   o [IEEE.802.11-2016] loosely supports a [RFC2474] Default Forwarding
      service via the Best Effort Access Category (AC_BE)

   o [IEEE.802.11-2016] loosely supports a [RFC3662] Lower Effort PDB
      service via the Background Access Category (AC_BK)

   As such, these high-level considerations should be kept in mind when
   mapping from Diffserv to [IEEE.802.11-2016] (and vice-versa);
   however, access points may or may not always be positioned at
   Diffserv domain boundaries, as will be discussed next.

2.1. Diffserv Domain Boundaries

   It is important to recognize that the wired-to-wireless edge may or
   may not function as an edge of a Diffserv domain or a domain
   boundary.

   In most commonly-deployed WLAN models, the wireless access point
   represents not only the edge of the Diffserv domain, but also the
   edge of the network infrastructure itself. As such, only client
   endpoint devices (and no network infrastructure devices) are
   downstream from the access points in these deployment models. Note:
   security considerations and recommendations for hardening such Wifi-
   at-the-edge deployment models are detailed in Section 8; these
   recommendations include mapping network control protocols (which are
   not used downstream from the AP in this deployment model) to UP 0.

   Alternatively, in other deployment models, such as Wi-Fi backhaul,
   wireless mesh infrastructures, wireless AP-to-AP deployments, or in

cases where a Wi-Fi link connects to a device providing service via
another technology (e.g. Wi-Fi to Bluetooth or Zigbee router), the
wireless access point extends the network infrastructure and thus,
typically, the Diffserv domain. In such deployments, both client
devices and infrastructure devices may be expected downstream from
the access points, and as such network control protocols are
RECOMMENDED to be mapped to UP 7 in this deployment model, as is
discussed in Section 4.1.1.

Thus, as can be seen from these two examples, the QoS treatment of
packets at the access point will depend on the position of the AP in
the network infrastructure and on the WLAN deployment model.

However, regardless of the access point being at the Diffserv
boundary or not, Diffserv to [IEEE.802.11-2016] (and vice-versa)
marking-specific incompatibilities exist that must be reconciled, as
will be discussed next.

2.2. EDCF Queuing

[IEEE.802.11-2016] displays a reference implementation queuing model
in Figure 10-24, which depicts four transmit queues, one per access
category.

However, in practical implementations, it is common for WLAN network
equipment vendors to implement dedicated transmit queues on a per-UP
(versus a per access category) basis, which are then dequeued into
their associated access category in a preferred (or even in a strict
priority manner). For example, it is common for vendors to dequeue
UP 5 ahead of UP 4 to the hardware performing the EDCA function
(EDCAF) for the Video Access Category (AC_VI).

Some of the recommendations made in Section 4 make reference to this
common implementation model of queuing per UP.

2.3. Default DSCP-to-UP Mappings and Conflicts

While no explicit guidance is offered in mapping (6-Bit) Layer 3 DSCP
values to (3-Bit) Layer 2 markings (such as IEEE 802.1D, 802.1p or
802.11e), a common practice in the networking industry is to map
these by what we will refer to as 'Default DSCP-to-UP Mapping' (for
lack of a better term), wherein the 3 Most Significant Bits (MSB) of
the DSCP are used as the corresponding L2 markings.

Note: There are mappings provided in [IEEE.802.11-2016] Annex V
Tables V-1 and V2, but it bears mentioning that these mappings are
provided as examples (as opposed to explicit recommendations).
Furthermore, some of these mappings do not align with the intent and

recommendations expressed in [RFC4594], as will be discussed in this
and the following section (Section 2.4).

However, when this default DSCP-to-UP mapping method is applied to
packets marked per [RFC4594] recommendations and destined to 802.11
WLAN clients, it will yield a number of inconsistent QoS mappings,
specifically:

o Voice (EF-101110) will be mapped to UP 5 (101), and treated in the
   Video Access Category (AC_VI), rather than the Voice Access
   Category (AC_VO), for which it is intended

o Multimedia Streaming (AF3-011xx0) will be mapped to UP3 (011) and
   treated in the Best Effort Access Category (AC_BE), rather than
   the Video Access Category (AC_VI), for which it is intended

o Broadcast Video (CS3-011000) will be mapped to UP3 (011) and
   treated in the Best Effort Access Category (AC_BE), rather than
   the Video Access Category (AC_VI), for which it is intended

o OAM traffic (CS2-010000) will be mapped to UP 2 (010) and treated
   in the Background Access Category (AC_BK), which is not the intent
   expressed in [RFC4594] for this service class

It should also be noted that while [IEEE.802.11-2016] defines an
intended use for each access category through the AC naming
convention (for example, UP 6 and UP 7 belong to AC_VO, the Voice
Access Category), [IEEE.802.11-2016] does not:

o define how upper layer markings (such as DSCP) should map to UPs
   (and hence to ACs)

o define how UPs should translate to other medium Layer 2 QoS
   markings

o strictly restrict each access category to applications reflected
   in the AC name

2.4. Default UP-to-DSCP Mappings and Conflicts

In the opposite direction of flow (the upstream direction, that is,
from wireless-to-wired), many APs use what we will refer to as
'Default UP-to-DSCP Mapping' (for lack of a better term), wherein
DSCP values are derived from UP values by multiplying the UP values
by 8 (i.e. shifting the 3 UP bits to the left and adding three
additional zeros to generate a DSCP value). This derived DSCP value
is then used for QoS treatment between the wireless access point and
the nearest classification and marking policy enforcement point

(which may be the centralized wireless LAN controller, relatively
deep within the network). Alternatively, in the case where there is
no other classification and marking policy enforcement point, then
this derived DSCP value will be used on the remainder of the Internet
path.

It goes without saying that when 6 bits of marking granularity are
derived from 3, then information is lost in translation. Servicing
differentiation cannot be made for 12 classes of traffic (as
recommended in [RFC4594]), but for only 8 (with one of these classes
being reserved for future use (i.e. UP 7 which maps to DSCP CS7).

Such default upstream mapping can also yield several inconsistencies
with [RFC4594], including:

o Mapping UP 6 ([RFC4594] Voice) to CS6, which [RFC4594] recommends
   for Network Control

o Mapping UP 4 ([RFC4594] Multimedia Conferencing and/or Real-Time
   Interactive) to CS4, thus losing the ability to differentiate
   between these two distinct service classes, as recommended in
   [RFC4594] Sections 4.3 and 4.4

o Mapping UP 3 ([RFC4594] Multimedia Streaming and/or Broadcast
   Video) to CS3, thus losing the ability to differentiate between
   these two distinct service classes, as recommended in [RFC4594]
   Sections 4.5 and 4.6

o Mapping UP 2 ([RFC4594] Low-Latency Data and/or OAM) to CS2, thus
   losing the ability to differentiate between these two distinct
   service classes, as recommended in [RFC4594] Sections 4.7 and 3.3,
   and possibly overwhelming the queues provisioned for OAM (which is
   typically lower in capacity [being network control traffic], as
   compared to Low-Latency Data queues [being user traffic])

o Mapping UP 1 ([RFC4594] High-Throughput Data and/or Low-Priority
   Data) to CS1, thus losing the ability to differentiate between
   these two distinct service classes, as recommended in [RFC4594]
   Sections 4.8 and 4.10, and causing legitimate business-relevant
   High-Throughput Data to receive a [RFC3662] Lower Effort PDB, for
   which it is not intended

The following sections address these limitations and concerns in
order to reconcile [RFC4594] and [IEEE.802.11-2016]. First
downstream (wired-to-wireless) DSCP-to-UP mappings will be aligned
and then upstream (wireless-to-wired) models will be addressed.

3. Wireless Device Marking and Mapping Capability Recommendations

This document assumes and RECOMMENDS that all wireless access points
(as the interconnects between wired-and-wireless networks) support
the ability to:

o   mark DSCP, per Diffserv standards

o   mark UP, per the [IEEE.802.11-2016] standard

o   support fully-configurable mappings between DSCP and UP

o   process DSCP markings set by wireless endpoint devices

This document further assumes and RECOMMENDS that all wireless
endpoint devices support the ability to:

o   mark DSCP, per Diffserv standards

o   mark UP, per the [IEEE.802.11-2016] standard

o   support fully-configurable mappings between DSCP (set by
    applications in software) and UP (set by the operating system and/
    or wireless network interface hardware drivers)

Having made the assumptions and recommendations above, it bears
mentioning while the mappings presented in this document are
RECOMMENDED to replace the current common default practices (as
discussed in Section 2.3 and Section 2.4), these mapping
recommendations are not expected to fit every last deployment model,
and as such MAY be overridden by network administrators, as needed.

4. DSCP-to-UP Mapping Recommendations

The following section specifies downstream (wired-to-wireless)
mappings between [RFC4594] Configuration Guidelines for Diffserv
Service Classes and [IEEE.802.11-2016]. As such, this section draws
heavily from [RFC4594], including service class definitions and
recommendations.

This section assumes [IEEE.802.11-2016] wireless access points and/or
WLAN controllers that support customizable, non-default DSCP-to-UP
mapping schemes.

This section also assumes that [IEEE.802.11-2016] access points and
endpoint devices differentiate UP markings with corresponding queuing
and dequeuing treatments, as described in Section 2.2.

4.1. Network Control Traffic

Network control traffic is defined as packet flows that are essential
for stable operation of the administered network [RFC4594] Section 3.
Network control traffic is different from user application control
(signaling) that may be generated by some applications or services.
Network control traffic MAY be split into two service classes:

o Network Control, and

o Operations Administration and Management (OAM)

4.1.1. Network Control Protocols

The Network Control service class is used for transmitting packets
between network devices (e.g. routers) that require control (routing)
information to be exchanged between nodes within the administrative
domain, as well as across a peering point between different
administrative domains.

[RFC4594] Section 3.2 recommends that Network Control traffic be
marked CS6 DSCP. Additionally, as stated in [RFC4594] Section 3.1:
"CS7 DSCP value SHOULD be reserved for future use, potentially for
future routing or control protocols."

By default (as described in Section 2.3), packets marked DSCP CS7
will be mapped to UP 7 and serviced within the Voice Access Category
(AC_VO). This represents the RECOMMENDED mapping for CS7, that is,
packets marked to CS7 DSCP are RECOMMENDED to be mapped to UP 7.

However, by default (as described in Section 2.3), packets marked
DSCP CS6 will be mapped to UP 6 and serviced within the Voice Access
Category (AC_VO); such mapping and servicing is a contradiction to
the intent expressed in [RFC4594] Section 3.2. As such, it is
RECOMMENDED to map Network Control traffic marked CS6 to UP 7 (per
[IEEE.802.11-2016] Section 10.2.4.2, Table 10-1), thereby admitting
it to the Voice Access Category (AC_VO), albeit with a marking
distinguishing it from (data-plane) voice traffic.

It should be noted that encapsulated routing protocols for
encapsulated or overlay networks (e.g., VPN, Network Virtualization
Overlays, etc.) are not network control traffic for any physical
network at the AP, and hence SHOULD NOT be marked with CS6 in the
first place.

Addtionally, and as previously noted, the Security Considerations
section (Section 8) contains additional recommendations for hardening
Wifi-at-the-edge deployment models, where, for example, network

control protocols are not expected to be sent nor recevied between
APs and downstream endpoint client devices.

4.1.2. Operations Administration Management (OAM)

The OAM (Operations, Administration, and Management) service class is
recommended for OAM&P (Operations, Administration, and Management and
Provisioning). The OAM service class can include network management
protocols, such as SNMP, SSH, TFTP, Syslog, etc., as well as network
services, such as NTP, DNS, DHCP, etc. [RFC4594] Section 3.3
recommends that OAM traffic be marked CS2 DSCP.

By default (as described in Section 2.3), packets marked DSCP CS2
will be mapped to UP 2 and serviced with the Background Access
Category (AC_BK). Such servicing is a contradiction to the intent
expressed in [RFC4594] Section 3.3. As such, it is RECOMMENDED that
a non-default mapping be applied to OAM traffic, such that CS2 DSCP
is mapped to UP 0, thereby admitting it to the Best Effort Access
Category (AC_BE).

4.2. User Traffic

User traffic is defined as packet flows between different users or
subscribers. It is the traffic that is sent to or from end-terminals
and that supports a very wide variety of applications and services
[RFC4594] Section 4.

Network administrators can categorize their applications according to
the type of behavior that they require and MAY choose to support all
or a subset of the defined service classes.

4.2.1. Telephony

The Telephony service class is recommended for applications that
require real-time, very low delay, very low jitter, and very low
packet loss for relatively constant-rate traffic sources (inelastic
traffic sources). This service class SHOULD be used for IP telephony
service. The fundamental service offered to traffic in the Telephony
service class is minimum jitter, delay, and packet loss service up to
a specified upper bound. [RFC4594] Section 4.1 recommends that
Telephony traffic be marked EF DSCP.

Traffic marked to DSCP EF will map by default (as described in
Section 2.3) to UP 5, and thus to the Video Access Category (AC_VI),
rather than to the Voice Access Category (AC_VO), for which it is
intended. Therefore, a non-default DSCP-to-UP mapping is
RECOMMENDED, such that EF DSCP is mapped to UP 6, thereby admitting
it into the Voice Access Category (AC_VO).

Similarly, the [RFC5865] VOICE-ADMIT DSCP (44/101100) is RECOMMENDED
to be mapped to UP 6, thereby admitting it also into the Voice Access
Category (AC_VO).

4.2.2. Signaling

The Signaling service class is recommended for delay-sensitive
client-server (e.g. traditional telephony) and peer-to-peer
application signaling. Telephony signaling includes signaling
between IP phone and soft-switch, soft-client and soft-switch, and
media gateway and soft-switch as well as peer-to-peer using various
protocols. This service class is intended to be used for control of
sessions and applications. [RFC4594] Section 4.2 recommends that
Signaling traffic be marked CS5 DSCP.

While Signaling is recommended to receive a superior level of service
relative to the default class (i.e. AC_BE), it does not require the
highest level of service (i.e. AC_VO). This leaves only the Video
Access Category (AC_VI), which it will map to by default (as
described in Section 2.3). Therefore it is RECOMMENDED to map
Signaling traffic marked CS5 DSCP to UP 5, thereby admitting it to
the Video Access Category (AC_VI).

Note: Signaling traffic is not control plane traffic from the
perspective of the network (but rather is data plane traffic); as
such, it does not merit provisioning in the Network Control service
class (marked CS6 and mapped to UP 6). However, Signaling traffic is
control-plane traffic from the perspective of the voice/video
telephony overlay-infrastructure. As such, Signaling should be
treated with preferential servicing vs. other data plane flows. This
may be achieved in common WLAN deployments by mapping Signaling
traffic marked CS5 to UP 5. On APs supporting per-UP EDCAF queuing
logic (as described in Section 2.2) this will result in preferential
treatment for Signaling traffic versus other video flows in the same
access category (AC_VI), which are marked to UP 4, as well as
preferred treatment over flows in the Best Effort (AC_BE) and
Background (AC_BK) access categories.

4.2.3. Multimedia Conferencing

The Multimedia Conferencing service class is recommended for
applications that require real-time service for rate-adaptive
traffic. [RFC4594] Section 4.3 recommends Multimedia Conferencing
traffic be marked AF4x (that is, AF41, AF42 and AF43, according to
the rules defined in [RFC2475]).

The primary media type typically carried within the Multimedia
Conferencing service class is video; as such, it is RECOMMENDED to

   map this class into the Video Access Category, which it does by
   default (as described in Section 2.3). Specifically, it is
   RECOMMENDED to map AF41, AF42 and AF43 to UP 4, thereby admitting
   Multimedia Conferencing into the Video Access Category (AC_VI).

4.2.4. Real-Time Interactive

   The Real-Time Interactive service class is recommended for
   applications that require low loss and jitter and very low delay for
   variable rate inelastic traffic sources. Such applications may
   include inelastic video-conferencing applications, but may also
   include gaming applications (as pointed out in [RFC4594] Sections 2.1
   through 2.3, and Section 4.4). [RFC4594] Section 4.4 recommends
   Real-Time Interactive traffic be marked CS4 DSCP.

   The primary media type typically carried within the Real-Time
   Interactive service class is video; as such, it is RECOMMENDED to map
   this class into the Video Access Category, which it does by default
   (as described in Section 2.3). Specifically, it is RECOMMENDED to
   map CS4 to UP 4, thereby admitting Real-Time Interactive traffic into
   the Video Access Category (AC_VI).

4.2.5. Multimedia-Streaming

   The Multimedia Streaming service class is recommended for
   applications that require near-real-time packet forwarding of
   variable rate elastic traffic sources. Typically these flows are
   unidirectional. [RFC4594] Section 4.5 recommends Multimedia
   Streaming traffic be marked AF3x (that is, AF31, AF32 and AF33,
   according to the rules defined in [RFC2475]).

   The primary media type typically carried within the Multimedia
   Streaming service class is video; as such, it is RECOMMENDED to map
   this class into the Video Access Category, which it will by default
   (as described in Section 2.3). Specifically, it is RECOMMENDED to
   map AF31, AF32 and AF33 to UP 4, thereby admitting Multimedia
   Streaming into the Video Access Category (AC_VI).

4.2.6. Broadcast Video

   The Broadcast Video service class is recommended for applications
   that require near-real-time packet forwarding with very low packet
   loss of constant rate and variable rate inelastic traffic sources.
   Typically these flows are unidirectional. [RFC4594] Section 4.6
   recommends Broadcast Video traffic be marked CS3 DSCP.

   As directly implied by the name, the primary media type typically
   carried within the Broadcast Video service class is video; as such,

it is RECOMMENDED to map this class into the Video Access Category;
however, by default (as described in Section 2.3), this service class
will map to UP 3, and thus the Best Effort Access Category (AC_BE).
Therefore, a non-default mapping is RECOMMENDED, such that CS4 maps
to UP 4, thereby admitting Broadcast Video into the Video Access
Category (AC_VI).

4.2.7. Low-Latency Data

The Low-Latency Data service class is recommended for elastic and
time-sensitive data applications, often of a transactional nature,
where a user is waiting for a response via the network in order to
continue with a task at hand. As such, these flows are considered
foreground traffic, with delays or drops to such traffic directly
impacting user-productivity. [RFC4594] Section 4.7 recommends Low-
Latency Data be marked AF2x (that is, AF21, AF22 and AF23, according
to the rules defined in [RFC2475]).

By default (as described in Section 2.3), Low-Latency Data will map
to UP 2 and thus to the Background Access Category (AC_BK), which is
contrary to the intent expressed in [RFC4594].

Mapping Low-Latency Data to UP 3 may allow such to receive a superior
level of service via per-UP transmit queues servicing the EDCAF
hardware for the Best Effort Access Category (AC_BE), as described in
Section 2.2. Therefore it is RECOMMENDED to map Low-Latency Data
traffic marked AF2x DSCP to UP 3, thereby admitting it to the Best
Effort Access Category (AC_BE).

4.2.8. High-Throughput Data

The High-Throughput Data service class is recommended for elastic
applications that require timely packet forwarding of variable rate
traffic sources and, more specifically, is configured to provide
efficient, yet constrained (when necessary) throughput for TCP
longer-lived flows. These flows are typically non-user-interactive.
According to [RFC4594] Section 4.8, it can be assumed that this class
will consume any available bandwidth and that packets traversing
congested links may experience higher queuing delays or packet loss.
It is also assumed that this traffic is elastic and responds
dynamically to packet loss. [RFC4594] Section 4.8 recommends High-
Throughput Data be marked AF1x (that is, AF11, AF12 and AF13,
according to the rules defined in [RFC2475]).

By default (as described in Section 2.3), High-Throughput Data will
map to UP 1 and thus to the Background Access Category (AC_BK), which
is contrary to the intent expressed in [RFC4594].

Unfortunately, there really is no corresponding fit for the High-
Throughput Data service class within the constrained 4 Access
Category [IEEE.802.11-2016] model. If the High-Throughput Data
service class is assigned to the Best Effort Access Category (AC_BE),
then it would contend with Low-Latency Data (while [RFC4594]
recommends a distinction in servicing between these service classes)
as well as with the default service class; alternatively, if it is
assigned to the Background Access Category (AC_BK), then it would
receive a less-then-best-effort service and contend with Low-Priority
Data (as discussed in Section 4.2.10).

As such, since there is no directly corresponding fit for the High-
Throughout Data service class within the [IEEE.802.11-2016] model, it
is generally RECOMMENDED to map High-Throughput Data to UP 0, thereby
admitting it to the Best Effort Access Category (AC_BE).

4.2.9. Standard Service Class

The Standard service class is recommended for traffic that has not
been classified into one of the other supported forwarding service
classes in the Diffserv network domain. This service class provides
the Internet's "best-effort" forwarding behavior. [RFC4594]
Section 4.9 states that the "Standard service class MUST use the
Default Forwarding (DF) PHB."

The Standard Service Class loosely corresponds to the
[IEEE.802.11-2016] Best Effort Access Category (AC_BE) and therefore
it is RECOMMENDED to map Standard Service Class traffic marked DF
DSCP to UP 0, thereby admitting it to the Best Effort Access Category
(AC_BE). This happens to correspond to the default mapping (as
described in Section 2.3).

4.2.10. Low-Priority Data

The Low-Priority Data service class serves applications that the user
is willing to accept without service assurances. This service class
is specified in [RFC3662] and [I-D.ietf-tsvwg-le-phb].

[RFC3662] and [RFC4594] both recommend Low-Priority Data be marked
CS1 DSCP.

Note: This marking recommendation may change in the future, as
[I-D.ietf-tsvwg-le-phb] defines a Lower Effort (LE) per-hop behavior
(PHB) and states: "The RECOMMENDED codepoint for the LE PHB is
'000010'.

The Low-Priority Data service class loosely corresponds to the
[IEEE.802.11-2016] Background Access Category (AC_BK) and therefore

it is RECOMMENDED to map Low-Priority Data traffic marked CS1 DSCP to
UP 1, thereby admitting it to the Background Access Category (AC_BK).
This happens to correspond to the default mapping (as described in
Section 2.3).

4.3. DSCP-to-UP Mapping Recommendations Summary

Figure 1 summarizes the [RFC4594] DSCP marking recommendations mapped
to [IEEE.802.11-2016] UP and access categories applied in the
downstream direction (i.e. from wired-to-wireless networks).

```
+----------------------------------------------------------------------+
| IETF Diffserv | PHB  |Reference|           IEEE 802.11                |
| Service Class |      |   RFC   |User Priority|  Access Category       |
|===============+======+=========+=============+======================= |
|               |      |         |     7       |     AC_VO (Voice)      |
|Network Control| CS7  | RFC2474 |          OR                          |
|(reserved for  |      |         |     0       | AC_BE (Best Effort)|
| future use)   |      |         |See Security Considerations-Sec.8 |
+---------------+------+---------+-------------+--------------------+
|               |      |         |     7       |     AC_VO (Voice)      |
|Network Control| CS6  | RFC2474 |          OR                          |
|               |      |         |     0       | AC_BE (Best Effort)|
|               |      |         |See Security Considerations-Sec.8 |
+---------------+------+---------+-------------+--------------------+
|   Telephony   |  EF  | RFC3246 |     6       |     AC_VO (Voice)      |
+---------------+------+---------+-------------+--------------------+
|  VOICE-ADMIT  |  VA  | RFC5865 |     6       |     AC_VO (Voice)      |
|               |      |         |             |                    |
+---------------+------+---------+-------------+--------------------+
|   Signaling   | CS5  | RFC2474 |     5       |     AC_VI (Video)      |
+---------------+------+---------+-------------+--------------------+
|   Multimedia  | AF41 |         |             |                    |
|  Conferencing | AF42 | RFC2597 |     4       |     AC_VI (Video)      |
|               | AF43 |         |             |                    |
+---------------+------+---------+-------------+--------------------+
|   Real-Time   | CS4  | RFC2474 |     4       |     AC_VI (Video)      |
|   Interactive |      |         |             |                    |
+---------------+------+---------+-------------+--------------------+
|   Multimedia  | AF31 |         |             |                    |
|   Streaming   | AF32 | RFC2597 |     4       |     AC_VI (Video)      |
|               | AF33 |         |             |                    |
+---------------+------+---------+-------------+--------------------+
|Broadcast Video| CS3  | RFC2474 |     4       |     AC_VI (Video)      |
+---------------+------+---------+-------------+--------------------+
|     Low-      | AF21 |         |             |                    |
|   Latency     | AF22 | RFC2597 |     3       | AC_BE (Best Effort)|
```

Data	AF23			
OAM	CS2	RFC2474	0	AC_BE (Best Effort)
High-Throughput Data	AF11 AF12 AF13	RFC2597	0	AC_BE (Best Effort)
Standard	DF	RFC2474	0	AC_BE (Best Effort)
Low-Priority Data	CS1	RFC3662	1	AC_BK (Background)

Note: All unused codepoints are RECOMMENDED to be mapped to UP 0
(See Security Considerations Section - Section 8)

Figure 1: Summary of Downstream DSCP to IEEE 802.11 UP and AC Mapping
Recommendations

5. Upstream Mapping and Marking Recommendations

In the upstream direction (i.e. wireless-to-wired), there are three
types of mapping that may be implemented:

o DSCP-to-UP mapping within the wireless client operating system,
   and

o UP-to-DSCP mapping at the wireless access point, or

o DSCP-Passthrough at the wireless access point (effectively a 1:1
   DSCP-to-DSCP mapping)

As an alternative to the latter two options, the network
administrator MAY choose to use the wireless-to-wired edge as a
Diffserv boundary and explicitly set (or reset) DSCP markings
according to administrative policy, thus making the wireless edge a
Diffserv policy enforcement point; this approach is RECOMMENDED
whenever the APs support the required classification and marking
capabilities.

Each of these options will now be considered.

5.1. Upstream DSCP-to-UP Mapping within the Wireless Client Operating System

Some operating systems on wireless client devices utilize a similar default DSCP-to-UP mapping scheme as described in Section 2.3. As such, this can lead to the same conflicts as described in that section, but in the upstream direction.

Therefore, to improve on these default mappings, and to achieve parity and consistency with downstream QoS, it is RECOMMENDED that wireless client operating systems utilize instead the same DSCP-to-UP mapping recommendations presented in Section 4, with the explicit RECOMMENDATION that packets requesting a marking of CS6 or CS7 DSCP SHOULD be mapped to UP 0 (and not to UP 7). Furthermore, in such cases the wireless client operating system SHOULD remark such packets to DSCP 0. This is because CS6 and CS7 DSCP, as well as UP 7 markings, are intended for network control protocols and these SHOULD NOT be sourced from wireless client endpoint devices. This recommendation is detailed in the Security Considerations section (Section 8).

5.2. Upstream UP-to-DSCP Mapping at the Wireless Access Point

UP-to-DSCP mapping generates a DSCP value for the IP packet (either an unencapsulated IP packet or an IP packet encapsulated within a tunneling protocol such as CAPWAP - and destined towards a wireless LAN controller for decapsulation and forwarding) from the Layer 2 [IEEE.802.11-2016] UP marking. This is typically done in the manner described in Section 2.4.

It should be noted that any explicit remarking policy to be performed on such a packet only takes place at the nearest classification and marking policy enforcement point, which may be:

o At the wireless access point

o At the wired network switch port

o At the wireless LAN controller

As such, UP-to-DSCP mapping allows for wireless L2 markings to affect the QoS treatment of a packet over the wired IP network (that is, until the packet reaches the nearest classification and marking policy enforcement point).

It should be further noted that nowhere in the [IEEE.802.11-2016] specifications is there an intent expressed for UP markings to be used to influence QoS treatment over wired IP networks. Furthermore,

[RFC2474], [RFC2475] and [RFC8100] all allow for the host to set DSCP
markings for end-to-end QoS treatment over IP networks. Therefore,
wireless access points MUST NOT leverage Layer 2 [IEEE.802.11-2016]
UP markings as set by wireless hosts and subsequently perform a UP-
to-DSCP mapping in the upstream direction. But rather, if wireless
host markings are to be leveraged (as per business requirements,
technical constraints and administrative policies), then it is
RECOMMENDED to pass through the Layer 3 DSCP markings set by these
wireless hosts instead, as is discussed in the next section.

5.3. Upstream DSCP-Passthrough at the Wireless Access Point

It is generally NOT RECOMMENDED to pass through DSCP markings from
unauthenticated and unauthorized devices, as these are typically
considered untrusted sources.

When business requirements and/or technical constraints and/or
administrative policies require QoS markings to be passed through at
the wireless edge, then it is RECOMMENDED to pass through Layer 3
DSCP markings (over Layer 2 [IEEE.802.11-2016] UP markings) in the
upstream direction, with the exception of CS6 and CS7 (as will be
discussed further), for the following reasons:

o [RFC2474], [RFC2475] and [RFC8100] all allow for hosts to set DSCP
   markings to achieve an end-to-end differentiated service

o [IEEE.802.11-2016] does not specify that UP markings are to be
   used to affect QoS treatment over wired IP networks

o Most present wireless device operating systems generate UP values
   by the same method as described in Section 2.3 (i.e. by using the
   3 MSB of the encapsulated 6-bit DSCP); then, at the access point,
   these 3-bit markings are converted back into DSCP values,
   typically in the default manner described in Section 2.4; as such,
   information is lost in the translation from a 6-bit marking to a
   3-bit marking (which is then subsequently translated back to a
   6-bit marking); passing through the original (encapsulated) DSCP
   marking prevents such loss of information

o A practical implementation benefit is also realized by passing
   through the DSCP set by wireless client devices, as enabling
   applications to mark DSCP is much more prevalent and accessible to
   programmers of applications running on wireless device platforms,
   vis-a-vis trying to explicitly set UP values, which requires
   special hooks into the wireless device operating system and/or
   hardware device drivers, many of which do not support such
   functionality

CS6 and CS7 are exceptions to this pass through recommendation because wireless hosts SHOULD NOT use them (see Section 5.1) and traffic with those two markings poses a threat to operation of the wired network (see Section 8.2). CS6 and CS7 SHOULD NOT be passed through to the wired network in the upstream direction unless the access point has been specifically configured to do that by a network administrator or operator.

5.4. Upstream DSCP Marking at the Wireless Access Point

An alternative option to mapping is for the administrator to treat the wireless edge as the edge of the Diffserv domain and explicitly set (or reset) DSCP markings in the upstream direction according to administrative policy. This option is RECOMMENDED over mapping, as this typically is the most secure solution, as the network administrator directly enforces the Diffserv policy across the IP network (versus an application developer and/or the wireless endpoint device operating system developer, who may be functioning completely independently of the network administrator).

6. IEEE 802.11 QoS Overview

QoS is enabled on wireless networks by means of the Hybrid Coordination Function (HCF). To give better context to the enhancements in HCF that enable QoS, it may be helpful to begin with a review of the original Distributed Coordination Function (DCF).

6.1. Distributed Coordination Function (DCF)

As has been noted, the Wi-Fi medium is a shared medium, with each station-including the wireless access point-contending for the medium on equal terms. As such, it shares the same challenge as any other shared medium in requiring a mechanism to prevent (or avoid) collisions which can occur when two (or more) stations attempt simultaneous transmission.

The IEEE Ethernet working group solved this challenge by implementing a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) mechanism that could detect collisions over the shared physical cable (as collisions could be detected as reflected energy pulses over the physical wire). Once a collision was detected, then a pre-defined set of rules was invoked that required stations to back off and wait random periods of time before re-attempting transmission. While CSMA/CD improved the usage of Ethernet as a shared medium, it should be noted the ultimate solution to solving Ethernet collisions was the advance of switching technologies, which treated each Ethernet cable as a dedicated collision domain.

However, unlike Ethernet (which uses physical cables), collisions cannot be directly detected over the wireless medium, as RF energy is radiated over the air and colliding bursts are not necessarily reflected back to the transmitting stations. Therefore, a different mechanism is required for this medium.

As such, the IEEE modified the CSMA/CD mechanism to adapt it to wireless networks to provide Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). The original CSMA/CA mechanism used in IEEE 802.11 was the Distributed Coordination Function. DCF is a timer-based system that leverages three key sets of timers, the slot time, interframe spaces and contention windows.

6.1.1. Slot Time

The slot time is the basic unit of time measure for both DCF and HCF, on which all other timers are based. The slot time duration varies with the different generations of data-rates and performances described by the [IEEE.802.11-2016] standard. For example, the [IEEE.802.11-2016] standard specifies the slot time to be 20 us ([IEEE.802.11-2016] Table 15-5) for legacy implementations (such as IEEE 802.11b, supporting 1, 2, 5.5 and 11 Mbps data rates), while newer implementations (including IEEE 802.11g, 802.11a, 802.11n and 802.11ac, supporting data rates from 6.5 Mbps to over 2 Gbps per spatial stream) define a shorter slot time of 9 us ([IEEE.802.11-2016], Section 17.4.4, Table 17-21).

6.1.2. Interframe Spaces

The time interval between frames that are transmitted over the air is called the Interframe Space (IFS). Several IFS are defined in [IEEE.802.11-2016], with the most relevant to DCF being the Short Interframe Space (SIFS), the DCF Interframe Space (DIFS) and the Extended Interframe Space (EIFS).

The SIFS is the amount of time in microseconds required for a wireless interface to process a received RF signal and its associated [IEEE.802.11-2016] frame and to generate a response frame. Like slot times, the SIFS can vary according to the performance implementation of the [IEEE.802.11-2016] standard. The SIFS for IEEE 802.11a, 802.11n and 802.11ac (in 5 GHz) is 16 us ([IEEE.802.11-2016], Section 17.4.4, Table 17-21).

Additionally, a station must sense the status of the wireless medium before transmitting. If it finds that the medium is continuously idle for the duration of a DIFS, then it is permitted to attempt transmission of a frame (after waiting an additional random backoff period, as will be discussed in the next section). If the channel is

found busy during the DIFS interval, the station must defer its
transmission until the medium is found idle for the duration of a
DIFS interval. The DIFS is calculated as:

    DIFS = SIFS + (2 * Slot time)

However, if all stations waited only a fixed amount of time before
attempting transmission then collisions would be frequent. To offset
this, each station must wait, not only a fixed amount of time (the
DIFS), but also a random amount of time (the random backoff) prior to
transmission. The range of the generated random backoff timer is
bounded by the Contention Window.

6.1.3. Contention Windows

Contention windows bound the range of the generated random backoff
timer that each station must wait (in addition to the DIFS) before
attempting transmission. The initial range is set between 0 and the
Contention Window minimum value (CWmin), inclusive. The CWmin for
DCF (in 5 GHz) is specified as 15 slot times ([IEEE.802.11-2016],
Section 17.4.4, Table 17-21).

However, it is possible that two (or more) stations happen to pick
the exact same random value within this range. If this happens then
a collision may occur. At this point, the stations effectively begin
the process again, waiting a DIFS and generate a new random backoff
value. However, a key difference is that for this subsequent
attempt, the Contention Window approximatively doubles in size (thus
exponentially increasing the range of the random value). This
process repeats as often as necessary if collisions continue to
occur, until the maximum Contention Window size (CWmax) is reached.
The CWmax for DCF is specified as 1023 slot times
([IEEE.802.11-2016], Section 17.4.4, Table 17-21).

At this point, transmission attempts may still continue (until some
other pre-defined limit is reached), but the Contention Window sizes
are fixed at the CWmax value.

Incidentally it may be observed that a significant amount of jitter
can be introduced by this contention process for wireless
transmission access. For example, the incremental transmission delay
of 1023 slot times (CWmax) using 9 us slot times may be as high as 9
ms of jitter per attempt. And, as previously noted, multiple
attempts can be made at CWmax.

6.2. Hybrid Coordination Function (HCF)

   Therefore, as can be seen from the preceding description of DCF,
   there is no preferential treatment of one station over another when
   contending for the shared wireless media; nor is there any
   preferential treatment of one type of traffic over another during the
   same contention process. To support the latter requirement, the IEEE
   enhanced DCF in 2005 to support QoS, specifying HCF in IEEE 802.11,
   which was integrated into the main IEEE 802.11 standard in 2007.

6.2.1. User Priority (UP)

   One of the key changes to the [IEEE.802.11-2016] frame format is the
   inclusion of a QoS Control field, with 3 bits dedicated for QoS
   markings. These bits are referred to the User Priority (UP) bits and
   these support eight distinct marking values: 0-7, inclusive.

   While such markings allow for frame differentiation, these alone do
   not directly affect over-the-air treatment. Rather it is the non-
   configurable and standard-specified mapping of UP markings to
   [IEEE.802.11-2016] Access Categories (AC) that generate
   differentiated treatment over wireless media.

6.2.2. Access Category (AC)

   Pairs of UP values are mapped to four defined access categories that
   correspondingly specify different treatments of frames over the air.
   These access categories (in order of relative priority from the top
   down) and their corresponding UP mappings are shown in Figure 2
   (adapted from [IEEE.802.11-2016], Section 10.2.4.2, Table 10-1).

```
+------------------------------------------+
|   User    |  Access    | Designative     |
| Priority  | Category   | (informative)   |
|===========+============+=================|
|    7      |   AC_VO    |    Voice        |
+-----------+------------+-----------------+
|    6      |   AC_VO    |    Voice        |
+-----------+------------+-----------------+
|    5      |   AC_VI    |    Video        |
+-----------+------------+-----------------+
|    4      |   AC_VI    |    Video        |
+-----------+------------+-----------------+
|    3      |   AC_BE    |  Best Effort    |
+-----------+------------+-----------------+
|    0      |   AC_BE    |  Best Effort    |
+-----------+------------+-----------------+
|    2      |   AC_BK    |  Background     |
+-----------+------------+-----------------+
|    1      |   AC_BK    |  Background     |
+------------------------------------------+
```

  Figure 2: IEEE 802.11 Access Categories and User Priority Mappings

   The manner in which these four access categories achieve
   differentiated service over-the-air is primarily by tuning the fixed
   and random timers that stations have to wait before sending their
   respective types of traffic, as will be discussed next.

6.2.3. Arbitration Inter-Frame Space (AIFS)

   As previously mentioned, each station must wait a fixed amount of
   time to ensure the medium is idle before attempting transmission.
   With DCF, the DIFS is constant for all types of traffic. However,
   with [IEEE.802.11-2016] the fixed amount of time that a station has
   to wait will depend on the access category and is referred to as an
   Arbitration Interframe Space (AIFS). AIFS are defined in slot times
   and the AIFS per access category are shown in Figure 3 (adapted from
   [IEEE.802.11-2016], Section 9.4.2.29, Table 9-137).

```
+-------------------------------------------+
|   Access   |  Designative  |     AIFS     |
|  Category  |  (informative)|  (slot times)|
|===========+================+=============|
|   AC_VO    |     Voice     |      2       |
+-----------+----------------+-------------+
|   AC_VI    |     Video     |      2       |
+-----------+----------------+-------------+
|   AC_BE    |  Best Effort  |      3       |
+-----------+----------------+-------------+
|   AC_BK    |  Background    |      7       |
+-----------+----------------+-------------+
```

Figure 3: Arbitration Interframe Spaces by Access Category

6.2.4. Access Category Contention Windows (CW)

Not only is the fixed amount of time that a station has to wait
skewed according to [IEEE.802.11-2016] access category, but so are
the relative sizes of the Contention Windows that bound the random
backoff timers, as shown in Figure 4 (adapted from
[IEEE.802.11-2016], Section 9.4.2.29, Table 9-137).

```
+---------------------------------------------------------+
|   Access   |  Designative  |    CWmin    |    CWmax    |
|  Category  |  (informative)|  (slot times)|(slot times)|
|===========+================+============|============|
|   AC_VO    |     Voice     |      3      |      7      |
+-----------+----------------+-----------+------------+
|   AC_VI    |     Video     |      7      |     15      |
+-----------+----------------+-----------+------------+
|   AC_BE    |  Best Effort  |     15      |    1023     |
+-----------+----------------+-----------+------------+
|   AC_BK    |  Background    |     15      |    1023     |
+-----------+----------------+-----------+------------+
```

Figure 4: Contention Window Sizes by Access Category

When the fixed and randomly generated timers are added together on a
per access category basis, then traffic assigned to the Voice Access
Category (i.e. traffic marked to UP 6 or 7) will receive a
statistically superior service relative to traffic assigned to the
Video Access Category (i.e. traffic marked UP 5 and 4), which, in
turn, will receive a statistically superior service relative to
traffic assigned to the Best Effort Access Category traffic (i.e.

traffic marked UP 3 and 0), which finally will receive a
statistically superior service relative to traffic assigned to the
Background Access Category traffic (i.e. traffic marked to UP 2 and
1).

6.3. **IEEE 802.11u QoS Map Set**

IEEE 802.11u [IEEE.802-11u.2011] is an addendum that has now been
included within the main [IEEE.802.11-2016] standard, and which
includes, among other enhancements, a mechanism by which wireless
access points can communicate DSCP to/from UP mappings that have been
configured on the wired IP network. Specifically, a QoS Map Set
information element (described in [IEEE.802.11-2016] Section 9.4.2.95
and commonly referred to as the QoS Map element) is transmitted from
an AP to a wireless endpoint device in an association / re-
association Response frame (or within a special QoS Map Configure
frame).

The purpose of the QoS Map element is to provide the mapping of
higher layer Quality of Service constructs (i.e. DSCP) to User
Priorities. One intended effect of receiving such a map is for the
wireless endpoint device (that supports this function and is
administratively configured to enable it) to perform corresponding
DSCP-to-UP mapping within the device (i.e. between applications and
the operating system / wireless network interface hardware drivers)
to align with what the APs are mapping in the downstream direction,
so as to achieve consistent end-to-end QoS in both directions.

The QoS Map element includes two key components:

1) each of the eight UP values (0-7) are associated with a range of
DSCP values, and

2) (up to 21) exceptions from these range-based DSCP to/from UP
mapping associations may be optionally and explicitly specified.

In line with the recommendations put forward in this document, the
following recommendations apply when the QoS Map element is enabled:

1) each of the eight UP values (0-7) are RECOMMENDED to be mapped to
DSCP 0 (as a baseline, so as to meet the recommendation made in
Section 8.2

2) (up to 21) exceptions from this baseline mapping are RECOMMENDED
to be made in line with Section 4.3, to correspond to the Diffserv
Codepoints that are in use over the IP network.

It is important to note that the QoS Map element is intended to be
transmitted from a wireless access point to a non-AP station. As
such, the model where this element is used is that of a network where
the AP is the edge of the Diffserv domain. Networks where the AP
extends the Diffserv domain by connecting other APs and
infrastructure devices through the IEEE 802.11 medium are not
included in the cases covered by the presence of the QoS Map element,
and therefore are not included in the present recommendation.

7. IANA Considerations

This memo asks the IANA for no new parameters.

8. Security Considerations

The recommendations in this document concern widely-deployed wired
and wireless network functionality, and for that reason do not
present additional security concerns that do not already exist in
these networks. In fact, several of the recommendations made in this
document serve to protect wired and wireless networks from potential
abuse, as is discussed further in this section.

8.1. General QoS Security Recommendations

It may be possible for a wired or wireless device (which could be
either a host or a network device) to mark packets (or map packet
markings) in a manner that interferes with or degrades existing QoS
policies. Such marking or mapping may be done intentionally or
unintentionally by developers and/or users and/or administrators of
such devices.

To illustrate: A gaming application designed to run on a smart-phone
or tablet may request that all its packets be marked DSCP EF and/or
UP 6. However, if the traffic from such an application is forwarded
without change over a business network, then this could interfere
with QoS policies intended to provide priority services for business
voice applications.

To mitigate such scenarios it is RECOMMENDED to implement general QoS
security measures, including:

o Setting a traffic conditioning policy reflective of business
   objectives and policy, such that traffic from authorized users
   and/or applications and/or endpoints will be accepted by the
   network; otherwise packet markings will be "bleached" (i.e.
   remarked to DSCP DF and/or UP 0). Additionally, Section 5.3 made
   it clear that it is generally NOT RECOMMENDED to pass through DSCP
   markings from unauthorized and/or unauthenticated devices, as

these are typically considered untrusted sources. This is
especially relevant for IoT deployments, where tens-of-billions of
devices are being connected to IP networks with little or no
security capabilities (making such vulernable to be utilized as
agents for DDoS attacks, the effects of which can be amplified
with preferential QoS treatments, should the packet markings of
such devices be trusted).

o Policing EF marked packet flows, as detailed in [RFC2474]
   Section 7 and [RFC3246] Section 3.

In addition to these general QoS security recommendations, WLAN-
specific QoS security recommendations can serve to further mitigate
attacks and potential network abuse.

8.2. WLAN QoS Security Recommendations

The wireless LAN presents a unique DoS attack vector, as endpoint
devices contend for the shared media on a completely egalitarian
basis with the network (as represented by the AP). This means that
any wireless client could potentially monopolize the air by sending
packets marked to preferred UP values (i.e. UP values 4-7) in the
upstream direction. Similarly, airtime could be monopolized if
excessive amounts of downstream traffic were marked/mapped to these
same preferred UP values. As such, the ability to mark/map to these
preferred UP values (of UP 4-7) should be controlled.

If such marking/mapping were not controlled, then, for example, a
malicious user could cause WLAN DoS by flooding traffic marked CS7
DSCP downstream. This codepoint would map by default (as described
in Section 2.3) to UP 7 and would be assigned to the Voice Access
Category (AC_VO). Such a flood could cause Denial-of-Service to not
only wireless voice applications, but also to all other traffic
classes. Similarly, an uninformed application developer may request
all traffic from his/her application to be marked CS7 or CS6,
thinking this would acheive in the best overall servicing of their
application traffic, while not realizing that such a marking (if
honored by the client operating system) could cause not only WLAN
DoS, but also IP network instability, as the traffic marked CS7 or
CS6 finds its way into queues intended for servicing (relatively low-
bandwidth) network control protocols, potentially starving legitimate
network control protocols in the process.

Therefore, to mitigate such an attack, it is RECOMMENDED that all
packets marked to Diffserv Codepoints not authorized or explicitly
provisioned for use over the wireless network by the network
administrator be mapped to UP 0; this recommendation applies both at
the access point (in the downstream direction) and within the

wireless endpoint device operating system (in the upstream
direction).

Such a policy of mapping unused codepoints to UP 0 would also prevent
an attack where non-standard codepoints were used to cause WLAN DoS.
Consider the case where codepoints are mapped to UP values using a
range function (e.g. DSCP values 48-55 all map to UP 6), then an
attacker could flood packets marked, for example to DSCP 49, in
either the upstream or downstream direction over the WLAN, causing
DoS to all other traffic classes in the process.

In the majority of WLAN deployments, the AP represents not only the
edge of the Diffserv domain, but also the edge of the network
infrastructure itself; that is, only wireless client endpoint devices
are downstream from the AP. In such a deployment model, CS6 and CS7
also fall into the category of codepoints that are not in use over
the wireless LAN (since only wireless endpoint client devices are
downstream from the AP in this model and these devices do not
[legitimately] participate in network control protocol exchanges).
As such, it is RECOMMENDED that CS6 and CS7 DSCP be mapped to UP 0 in
these Wifi-at-the-edge deployment models. Otherwise, it would be
easy for a malicious application developer, or even an inadvertently
poorly-programmed IoT device, to cause WLAN DoS and even wired IP
network instability by flooding traffic marked CS6 DSCP, which would
by default (as described in Section 2.3) be mapped to UP 6, causing
all other traffic classes on the WLAN to be starved, as well
hijacking queues on the wired IP network that are intended for the
servicing of routing protocols. To this point, it was also
recommended in Section 5.1 that packets requesting a marking of CS6
or CS7 DSCP SHOULD be remarked to DSCP 0 and mapped to UP 0 by the
wireless client operating system.

Finally, it should be noted that the recommendations put forward in
this document are not intended to address all attack vectors
leveraging QoS marking abuse. Mechanisms that may further help
mitigate security risks of both wired and wireless networks deploying
QoS include strong device- and/or user-authentication, access-
control, rate limiting, control-plane policing, encryption and other
techniques; however, the implementation recommendations for such
mechanisms are beyond the scope of this document to address in
detail. Suffice it to say that the security of the devices and
networks implementing QoS, including QoS mapping between wired and
wireless networks, merits consideration in actual deployments.

9. Acknowledgements

The authors wish to thank David Black, Gorry Fairhurst, Ruediger
Geib, Vincent Roca, Brian Carpenter, David Blake, Cullen Jennings,
David Benham and the TSVWG.

The authors also acknowledge a great many inputs, notably from David
Kloper, Mark Montanez, Glen Lavers, Michael Fingleton, Sarav
Radhakrishnan, Karthik Dakshinamoorthy, Simone Arena, Ranga Marathe,
Ramachandra Murthy and many others.

10. References

10.1. Normative References

[IEEE.802.11-2016]
            "Information technology - Telecommunications and
            information exchange between systems - Local and
            metropolitan area networks - Specific requirements - Part
            11: Wireless LAN Medium Access Control (MAC) and Physical
            Layer (PHY) specifications", IEEE Standard 802.11, 2016,
            <https://standards.ieee.org/findstds/
            standard/802.11-2016.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <https://www.rfc-editor.org/info/rfc2119>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black,
            "Definition of the Differentiated Services Field (DS
            Field) in the IPv4 and IPv6 Headers", RFC 2474,
            DOI 10.17487/RFC2474, December 1998,
            <https://www.rfc-editor.org/info/rfc2474>.

[RFC2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski,
            "Assured Forwarding PHB Group", RFC 2597,
            DOI 10.17487/RFC2597, June 1999,
            <https://www.rfc-editor.org/info/rfc2597>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition
            of Explicit Congestion Notification (ECN) to IP",
            RFC 3168, DOI 10.17487/RFC3168, September 2001,
            <https://www.rfc-editor.org/info/rfc3168>.

   [RFC3246] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec,
              J., Courtney, W., Davari, S., Firoiu, V., and D.
              Stiliadis, "An Expedited Forwarding PHB (Per-Hop
              Behavior)", RFC 3246, DOI 10.17487/RFC3246, March 2002,
              <https://www.rfc-editor.org/info/rfc3246>.

   [RFC3662] Bless, R., Nichols, K., and K. Wehrle, "A Lower Effort
              Per-Domain Behavior (PDB) for Differentiated Services",
              RFC 3662, DOI 10.17487/RFC3662, December 2003,
              <https://www.rfc-editor.org/info/rfc3662>.

   [RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration
              Guidelines for DiffServ Service Classes", RFC 4594,
              DOI 10.17487/RFC4594, August 2006,
              <https://www.rfc-editor.org/info/rfc4594>.

   [RFC5865] Baker, F., Polk, J., and M. Dolly, "A Differentiated
              Services Code Point (DSCP) for Capacity-Admitted Traffic",
              RFC 5865, DOI 10.17487/RFC5865, May 2010,
              <https://www.rfc-editor.org/info/rfc5865>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

   [GSMA-IPX_Guidelines]
              "Guidelines for IPX Provider networks (Previously Inter-
              Service Provider IP Backbone Guidelines) Version 11.0",
              GSMA Official Document, November 2014,
              <https://www.gsma.com/newsroom/wp-content/uploads/
              IR.34-v11.0.pdf>.

   [I-D.ietf-tsvwg-le-phb]
              Bless, R., "A Lower Effort Per-Hop Behavior (LE PHB)",
              draft-ietf-tsvwg-le-phb-02 (work in progress), June 2017.

   [IEEE.802-11u.2011]
              "Information technology - Telecommunications and
              information exchange between systems - Local and
              metropolitan area networks - Specific requirements - Part
              11: Wireless LAN Medium Access Control (MAC) and Physical
              Layer (PHY) specifications", IEEE Standard 802.11, 2011,
              <http://standards.ieee.org/getieee802/
              download/802.11u-2011.pdf>.

   [RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z.,
              and W. Weiss, "An Architecture for Differentiated
              Services", RFC 2475, DOI 10.17487/RFC2475, December 1998,
              <https://www.rfc-editor.org/info/rfc2475>.

   [RFC5127] Chan, K., Babiarz, J., and F. Baker, "Aggregation of
              Diffserv Service Classes", RFC 5127, DOI 10.17487/RFC5127,
              February 2008, <https://www.rfc-editor.org/info/rfc5127>.

   [RFC7561] Kaippallimalil, J., Pazhyannur, R., and P. Yegani,
              "Mapping Quality of Service (QoS) Procedures of Proxy
              Mobile IPv6 (PMIPv6) and WLAN", RFC 7561,
              DOI 10.17487/RFC7561, June 2015,
              <https://www.rfc-editor.org/info/rfc7561>.

   [RFC8100] Geib, R., Ed. and D. Black, "Diffserv-Interconnection
              Classes and Practice", RFC 8100, DOI 10.17487/RFC8100,
              March 2017, <https://www.rfc-editor.org/info/rfc8100>.

Appendix A. Change Log

   Initial Version: July 2015

Authors' Addresses

   Tim Szigeti
   Cisco Systems
   Vancouver, British Columbia V6K 3L4
   Canada

   Email: szigeti@cisco.com

   Jerome Henry
   Cisco Systems
   Research Triangle Park, North Carolina 27709
   USA

   Email: jerhenry@cisco.com

   Fred Baker
   Santa Barbara, California 93117
   USA

   Email: FredBaker.IETF@gmail.com