Transport Working Group   T. Szigeti
Internet-Draft   F. Baker
Intended status: Informational   Cisco Systems
Expires: September 15, 2016   March 14, 2016

                Guidelines for DiffServ to IEEE 802.11 Mapping
                    draft-szigeti-tsvwg-ieee-802-11-01

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 is due to the fact that two independent
   standards bodies provide QoS guidance on wired and wireless networks:
   specifically, the IETF specifies standards and design recommendations
   for wired IP networks, while a separate and autonomous standards-
   body, the IEEE, administers the standards for wireless 802.11
   networks. The purpose of this document is to propose a set
   Differentiated Services Code Point (DSCP) to IEEE 802.11 User
   Priority (UP) mappings to reconcile the marking recommendations
   offered by these two standards bodies, and, as such, to optimize
   wired-and-wireless interconnect QoS.

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 http://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 September 15, 2016.

Copyright Notice

Table of Contents

1. Introduction

   Wireless has become the medium of choice for endpoints connecting to
   business and private networks. However, the wireless medium defined
   by IEEE 802.11 [IEEE.802-11.2012] presents several design challenges
   for ensuring end-to-end quality of service. Some of these challenges
   relate to the nature of 802.11 RF medium itself, being a half-duplex
   and shared media, while other challenges relate to the fact that the
   802.11 standard is not administered by the standards body that
   administers the rest of the IP network. While the IEEE has developed
   tools to enable QoS over wireless networks, little guidance exists on
   how to optimally interconnect wired IP and wireless 802.11 networks,
   which is the aim of this document.

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] details the Assured Forwarding (AF) PHB.

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

o [RFC4594] presents Configuration Guidelines for DiffServ Service
   Classes

o [RFC5127] discusses the Aggregation of Diffserv Service Classes

o [RFC5865] introduces a DSCP for Capacity Admitted Traffic

This draft draws heavily on [RFC4594], [RFC5127], and
[I-D.ietf-tsvwg-diffserv-intercon].

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 802.11-2012.

1.2. Interaction with RFC 7561

There is also a recommendation from GSMA, Mapping Quality of Service
(QoS) Procedures of Proxy Mobile IPv6 (PMIPv6) and WLAN [RFC7561].
The GSMA specification was developed without reference to the service
plan documented in Section 1.1, and conflicts both in the services
specified and the code points specified for them. As such, the two
plans cannot be normalized. Rather, as discussed in [RFC2474]
section 2, the two domains (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 primarily applies to wired IP networks that have
wireless access points at their edges, but can also be applied to Wi-
Fi backhaul, wireless mesh solutions or any other type of AP-to-AP
wireless network that serves to extend the IP network infrastructure.

1.4. Document Organization

This document is organized as follows:

o Section 1 outlines the abstract, related work, organization and
   the requirements language of 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] traffic 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, security considerations,
   acknowledgements and references, respectively

1.5. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL", and "NOT
RECOMMENDED" in this document are to be interpreted as described in
[RFC2119].

2. 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 should be
noted:

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

   o 802.11 does not support a [RFC2597] AF PHB service, again because
      it is not possible to guarantee 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 802.11 loosely supports a [RFC2474] Default Forwarding service via
      the Best Effort Access Category (AC_BE)

   o 802.11 loosely supports a [RFC3662] Lower PDB service via the
      Background Access Category (AC_BK)

   As such, these are high-level considerations that need to be kept in
   mind when mapping from DiffServ to 802.11 (and vice-versa); however,
   some additional marking-specific incompatibilities must also be
   reconciled, as will be discussed next.

2.1. 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 transcribed to generate the corresponding L2 markings.

   Note: There are example mappings in IEEE 802.11 (in the Annex V
   Tables V-1 and V2), but these mappings are provided as examples (vs.
   as recommendations). Furthermore, some of these mappings do not
   align with the intent and recommendations expressed in [RFC4594], as
   will be discussed in the following section.

   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 sub-optimal 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 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 traffic class

It should also be noted that while IEEE 802.11 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),
802.11 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

2.2. 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).

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 (Voice) to CS6, which [RFC4594] recommends for
   Network Control

o Mapping UP 4 (Multimedia Conferencing and/or Real-Time
   Interactive) to CS4, thus losing the ability to distinguish
   between these two distinct traffic classes

o Mapping UP 3 (Multimedia Streaming and/or Broadcast Video) to CS3,
   thus losing the ability to distinguish between these two distinct
   traffic classes

o Mapping UP 2 (Low-Latency Data and/or OAM) to CS2, thus losing the
   ability to distinguish between these two distinct traffic classes,
   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 (High-Throughput Data and/or Low-Priority Data) to
   CS1, thus losing the ability to distinguish between these two
   distinct traffic classes and causing legitimate business-relevant
   High-Throughput Data to receive a [RFC3662] Lower PDB, for which
   it is not intended

Thus, the next sections of this draft seek to address these
limitations and concerns and reconcile the intents of [RFC4594] and
IEEE 802.11. First the 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 bridges between wired-and-wireless networks) support the
ability to:

o mark DSCP, per DiffServ standards

o mark UP, per the 802.11 standard

o support fully-configurable mappings between DSCP and UP

o trust the DSCP markings set by wireless endpoint devices (as
   discussed in Section 5.3)

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 802.11 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 2.1 and Section 2.2), 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 proposes downstream (wired-to-wireless) mappings between [RFC4594] Configuration Guidelines for DiffServ Service Classes and IEEE 802.11. As such, this section draws heavily from [RFC4594], including traffic class definitions and recommendations.

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

4.1. Network Control Traffic

Network control traffic is defined as packet flows that are essential for stable operation of the administered network. 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 (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. The RECOMMENDED DSCP marking for Network Control is CS6.

Before discussing a mapping recommendation for Network Control traffic marked CS6 DSCP, it is interesting to note a relevant recommendation from [RFC4594] pertaining to traffic marked CS7 DSCP: in [RFC4594] Section 3.1 it is RECOMMENDED that packets marked CS7 DSCP (a codepoint that SHOULD be reserved for future use) be dropped or remarked at the edge of the DiffServ domain.

Following this recommendation, it is RECOMMENDED that all packets marked to DiffServ Codepoints not in use over the wireless network be dropped or remarked at the edge of the DiffServ domain.

It is important to note that the wired-to-wireless edge may or may not equate to the edge of the DiffServ domain; as such, this recommendation may or may not apply at the wired-to-wireless edge.

For example, in most commonly deployed 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, and in line with the above recommendation, traffic marked CS7 DSCP SHOULD be dropped or remarked at this edge (as it is typically unused, as CS7 SHOULD be reserved for future use). So too SHOULD Network Control traffic marked CS6 DSCP, considering that only client devices (and no network infrastructure devices) are downstream from the wireless access points in these deployment models. In such cases, no Network Control traffic would be (legitimately) expected to be sent or received from wireless client endpoint devices, and thus this recommendation would apply.

Alternatively, in other deployment models, such as Wi-Fi backhaul, wireless mesh infrastructures, or any other type of wireless AP-to-AP deployments, the wireless access point extends the network infrastructure and thus, typically, the DiffServ domain. In such cases, the above recommendation would not apply, as the wired-to-wireless edge does not represent the edge of the DiffServ domain. Furthermore, as these deployment models require Network Control traffic to be propagated across the wireless network, it is RECOMMENDED to map Network Control traffic marked CS6 to UP 7 (per IEEE 802.11-2012, Section 9.2.4.2, Table 9-1), thereby admitting it to the Voice Access Category (AC_VO).

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 RECOMMENDED DSCP marking for OAM is CS2.

By default, 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. 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. The RECOMMENDED DSCP marking for Telephony
is EF.

Traffic marked to DSCP EF will map by default 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 (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. The RECOMMENDED DSCP marking for Signaling is CS5.

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. However,
to better differentiate inelastic video flows from elastic video and
signaling flows (as will be discussed next), it is RECOMMENDED to map
Signaling traffic marked CS5 DSCP to UP 4, thereby admitting it to
the Video Access Category (AC_VI).

4.2.3. Inelastic Video Classes

Both the Real-Time Interactive and Broadcast Video traffic classes
are considered to be inelastic, in that the traffic in these classes
does not have the ability (or the business requirement precludes the

use of the ability) to change encoding, resolution, frame or
transmission rates to dynamically adapt to network conditions such as
congestion and/or packet loss. The Real-Time Interactive and
Broadcast Video traffic classes are intended for bi-directional and
unidirectional inelastic video flows (respectively).

Specifically, the Real-Time Interactive traffic 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). The RECOMMENDED DSCP marking for
Real-Time Interactive traffic is CS4.

Similarly, 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. The RECOMMENDED DSCP marking for Broadcast Video is CS3.

While considering Table 1 it may seem superfluous to make a
distinction between inelastic video classes (by mapping these to UP
5) and elastic video classes (by mapping these to UP 4), as both are
destined to be serviced within the same Video Access Category
(AC_VI). However, a subtlety in implementation merits consideration
and provides the rationale behind this recommendation.

IEEE 802.11-2012 illustrates a reference implementation model in
Figure 9-19 which depicts four transmit queues, one per access
category. In practical implementation, however, it is common for
network vendors to actually implement dedicated transmit queues on a
per-UP basis, which are then dequeued into their associated access
category in a preferred (or even strict priority manner). For
example, (and specific to this example): it is common for network
vendors to dequeue UP 5 ahead of UP 4 to the hardware performing the
EDCA function (EDCAF) for the Video Access Category (AC_VI). As
such, inelastic video flows can benefit from this differentiation in
servicing.

A corollary benefit may also be realized in the upstream direction,
for if inelastic video flows are marked to a separate UP from elastic
video (or signaling) flows, then these can likewise be differentiated
from each other and serviced accordingly in the upstream direction.

For these reasons it is RECOMMENDED to map inelastic video traffic
marked CS4 and CS3 DSCP to UP 5, thereby admitting it to the Video
Access Category (AC_VI).

4.2.4. Elastic Video Classes

In contrast to Real-Time Interactive and Broadcast Video, the
Multimedia Conferencing and Multimedia Streaming traffic classes are
intended for bi-directional and unidirectional elastic video flows
(respectively).

Specifically, the Multimedia Conferencing service class is
RECOMMENDED for applications that require real-time service for rate-
adaptive traffic. The RECOMMENDED DSCP markings for Multimedia
Conferencing are AF41, AF42 and AF43.

Similarly, the Multimedia Streaming The Multimedia Streaming service
class is RECOMMENDED for applications that require near-real-time
packet forwarding of variable rate elastic traffic sources. The
RECOMMENDED DSCP markings for Multimedia Streaming are AF31, AF32 and
AF33.

In line with the recommendation made in the previous section, and to
preclude the default mapping of Multimedia Streaming to UP 3 (and
hence to AC_BE), it is RECOMMENDED to map inelastic video/multimedia
traffic classes marked AF4x and AF3x DSCP to UP 4, thereby admitting
these to the Video Access Category (AC_VI).

4.2.5. 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 may be considered
foreground traffic, with delays or drops to such traffic directly
impacting user-productivity. The RECOMMENDED DSCP markings for Low-
Latency Data are AF21, AF22 and AF23.

In line with the recommendations made in Section 4.2.3, mapping Low-
Latency Data to UP 3 may allow such to receive a superior level of
service via transmit queues servicing the EDCAF hardware for the Best
Effort Access Category (AC_BE), as well as providing for a
distinction between such traffic vs. Default Forwarding traffic in
the upstream direction. 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).

4.2.6. 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.
Per [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. The RECOMMENDED DSCP markings for High-Throughput Data
are AF11, AF12 and AF13.

Unfortunately, there really is no corresponding fit for the High-
Throughput Data traffic class within the constrained 4 Access
Category 802.11 model. If the High-Throughput Data traffic 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 traffic classes) as well as
with the default traffic 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 4.2.8).

As such, administrators MAY map High-Throughput Data to UP 0, when
their business-requirements and/or administrative-preference is to
treat this traffic class the same as the default Standard Service
Class (as discussed in Section 4.2.7).

Alternatively, an administrator may interpret [RFC4594] to imply that
since the High-Throughput Data traffic class may receive higher
queuing delays and/or packet loss, as well as that this traffic is
elastic and responds dynamically to packet loss ([RFC4594]
-Section 4.8), that such traffic may be adequately serviced in the
Background Access Category (AC_BK). In such cases, High-Throughput
Data MAY be mapped to UP 2, so as to receive a differentiated service
(via transmit queues servicing the EDCAF hardware) within the
Background Access Category (AC_BK), as discussed in Section 4.2.3.

4.2.7. 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. The RECOMMENDED
DSCP marking for the Standard Service Class is DF.

The Standard Service Class loosely corresponds to the 802.11 Best
Effort Access Category (AC_BK) 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).

4.2.8. Low-Priority Data

The Low-Priority Data service class serves applications that the user
is willing to accept service without guarantees. This service class
is specified in [RFC3662].

The Low-Priority Data service class loosely corresponds to the 802.11
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).

4.3. DSCP-to-UP Mapping Recommendations Summary

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

IETF DiffServ Service Class	DSCP	PHB Used	IEEE 802.11		
			User Priority	Access Category	
Network Control	CS6	RFC2474	(See Section 4.1.1)		
Telephony	EF	RFC3246	6	AC_VO (Voice)	
VOICE-ADMIT	44	RFC5865	6	AC_VO (Voice)	
Signaling	CS5	RFC2474	4	AC_VI (Video)	
Multimedia Conferencing	AF41 AF42 AF43	RFC2597	4	AC_VI (Video)	
Real-Time Interactive	CS4	RFC2474	5	AC_VI (Video)	
Multimedia Streaming	AF31 AF32 AF33	RFC2597	4	AC_VI (Video)	
Broadcast Video	CS3	RFC2474	5	AC_VI (Video)	
Low-Latency Data	AF21 AF22 AF23	RFC2597	3	AC_BE (Best Effort)	
OAM	CS2	RFC2474	0	AC_BE (Best Effort)	
High-Throughput Data	AF11 AF12 AF13	RFC2597	0 OR 2	AC_BE (Best Effort) OR AC_BK (Background)	
Standard	DF	RFC2474	0	AC_BE (Best Effort)	
Low-Priority Data	CS1	RFC3662	1	AC_BK (Background)	

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

5. Upstream Mapping Recommendations

   In the upstream direction, there are three types of mapping that may
   occur:

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

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

   o DSCP-Trust at the wireless access point

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 2.1. 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
   such wireless client operating systems utilize instead the same DSCP-
   to-UP mapping recommendations presented in Section 4 and/or fully
   customizable UP markings.

5.2. 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 UP markings of the wireless frame.

   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 noted that nowhere in the IEEE 802.11 specifications is
there an intent expressed for 802.11 UP to be used to influence QoS
treatment over wired IP networks. Furthermore, both [RFC2474] and
[RFC2475] allow for the host to set DSCP markings for QoS treatment
over IP networks. Therefore, it is NOT RECOMMENDED that wireless
access points trust UP markings as set by these hosts and
subsequently perform a UP-to-DSCP mapping in the upstream direction,
but rather, if wireless host markings are to be trusted (as per
business requirements, technical constraints and administrative
preference), then it is RECOMMENDED to trust the DSCP markings set by
these wireless hosts.

5.3. DSCP-Trust at the Wireless Access Point

On wireless access points that can trust DSCP markings of packets
encapsulated within wireless frames it is RECOMMENDED to trust DSCP
markings in the upstream direction, for the following reasons:

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

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

o Most wireless device operating systems generate UP values by the
   same method as described in Section 3.1 (i.e. by using the 3 MSB
   of the encapsulated 6-bit DSCP); then, at the access point, these
   3-bit mappings are converted back into DSCP values, either by the
   default operation described in Section 3.2 or by a customized
   mapping as described in Section 4; in either case, information is
   lost in the transitions from 6-bit marking to 3-bit marking and
   then back to 6-bit marking; trusting the encapsulated DSCP
   prevents this loss of information

o A practical implementation benefit is also realized by trusting
   the DSCP set by wireless client devices, as enabling applications
   to mark DSCP is much more prevalent and accessible to programmers
   of wireless applications 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 (at
   the time of writing) have little or no resources to support such
   functionality

6. Appendix: 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 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 802.11 standard. For example, the IEEE 802.11-2012
standard specifies the slot time to be 20 us (IEEE 802.11-2012
Table 16-2) for legacy implementations (such as 802.11b, supporting
1, 2, 5.5 and 11 Mbps data rates), while newer implementations
(including 802.11g, 80.11a, 802.11n and 802.11ac, supporting data

rates from 500 Mbps to over 1 Gbps) define a shorter slot time of 9
us (IEEE 802.11-2012, Section 18.4.4, Table 18-17).

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
802.11, with the two most relevant to DCF being the Short Interframe
Space (SIFS) and the DCF Interframe Space (DIFS).

The SIFS is the amount of time in microseconds required for a
wireless interface to process a received RF signal and its associated
802.11 frame and to generate a response frame. Like slot times, the
SIFS can vary according to the performance implementation of the
802.11 standard. The SIFS for 802.11a, 802.11n and 802.11ac (in 5
Ghz) is 16 us (IEEE 802.11-2012, Section 18.4.4, Table 18-17).

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- 2012,
Section 18.4.4, Table 18-17).

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 will 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 802.11-2012,
Section 18.4.4, Table 18-17).

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 802.11, which
was integrated into the main 802.11 standard in 2007.

6.2.1. User Priority (UP)

One of the key changes to the 802.11 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 802.11
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 802.11-2012, Section 9.2.4.2, Table 9-1).

```
+-------------------------------------------+
|   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 air is clear before attempting transmission. With
   DCF, the DIFS is constant for all types of traffic. However, with
   802.11 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
   802.11-2012, Section 8.4.2.31, Table 8-105).

```
+-------------------------------------------+
|  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 802.11 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 802.11-2012,
   Section 8.4.2.31, Table 8-105).

```
+--------------------------------------------------------+
|  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 proposed addendum to the IEEE
   802.11 standard 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
   802.11u-2011 Section 7.3.2.95) 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 Set information element is to provide the mapping of
   higher layer Quality of Service constructs (i.e. DSCP) to User
   Priorities so that a wireless endpoint device (that supports this
   function and is administratively configured to enable it) can 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.

   The QoS Map Set information 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 this QoS Map Set information
   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 4.1.1 (that packets marked to unused DiffServ Codepoints be
   remarked at the edge of the DiffServ domain), and

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

7. IANA Considerations

   This memo asks the IANA for no new parameters.

8. Security Considerations

   The recommendation offered in Section 4.1.1 (of dropping or remarking
   packets marked with DiffServ Codepoints not in use at the edge of the
   DiffServ domain) is to address a Denial-of-Service attack vector that
   exists at wired-to-wireless edges due to the requirement of trusting
   traffic markings to ensure end-to-end QoS. For example, consider a
   malicious user flooding traffic marked CS7 or CS6 DSCP toward the
   WLAN. These codepoints would map by default to UP 7 and UP 6
   (respectively), both of which would be assigned to the Voice Access
   Category (AC_VO). Such a flood could cause a Denial-of-Service to
   wireless voice applications.

8.1. Privacy Considerations

9. Acknowledgements

   The authors wish to thank TSVWG reviewers.

   The authors acknowledge a great many inputs, notably from Jerome
   Henry, 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

   [I-D.ietf-tsvwg-diffserv-intercon]
              Geib, R. and D. Black, "Diffserv interconnection classes
              and practice", draft-ietf-tsvwg-diffserv-intercon-03 (work
              in progress), October 2015.

   [IEEE.802-11.2012]
              "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, 2012,
              <http://standards.ieee.org/getieee802/
              download/802.11-2012.pdf>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
              RFC2119, March 1997,
              <http://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,
              <http://www.rfc-editor.org/info/rfc2474>.

   [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,
              <http://www.rfc-editor.org/info/rfc2475>.

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

   [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,
              <http://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,
              <http://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,
              <http://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,
              <http://www.rfc-editor.org/info/rfc5865>.

10.2. Informative References

   [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>.

   [RFC5127] Chan, K., Babiarz, J., and F. Baker, "Aggregation of
              Diffserv Service Classes", RFC 5127, DOI 10.17487/RFC5127,
              February 2008, <http://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,
              <http://www.rfc-editor.org/info/rfc7561>.

Appendix A. Change Log

   Initial Version: July 2015

Authors' Addresses

   Tim Szigeti
   Cisco Systems
   Vancouver, British Columbia V7X 1J1
   Canada

   Email: szigeti@cisco.com

   Fred Baker
   Cisco Systems
   Santa Barbara, California 93117
   USA

   Email: fred@cisco.com