                  A Lower Effort Per-Hop Behavior (LE PHB)
                        draft-ietf-tsvwg-le-phb-08

Abstract

   This document specifies properties and characteristics of a Lower
   Effort (LE) per-hop behavior (PHB). The primary objective of this LE
   PHB is to protect best-effort (BE) traffic (packets forwarded with
   the default PHB) from LE traffic in congestion situations, i.e., when
   resources become scarce, best-effort traffic has precedence over LE
   traffic and may preempt it. Alternatively, packets forwarded by the
   LE PHB can be associated with a scavenger service class, i.e., they
   scavenge otherwise unused resources only. There are numerous uses
   for this PHB, e.g., for background traffic of low precedence, such as
   bulk data transfers with low priority in time, non time-critical
   backups, larger software updates, web search engines while gathering
   information from web servers and so on. This document recommends a
   standard DSCP value for the LE PHB. This specification obsoletes RFC
   3662 and updates the DSCP recommended in RFC 4594 and RFC 8325 to use
   the DSCP assigned in this specification.

Status of This Memo

Table of Contents

1. Introduction

   This document defines a Differentiated Services per-hop behavior
   [RFC2474] called "Lower Effort" (LE), which is intended for traffic
   of sufficiently low urgency that all other traffic takes precedence
   over the LE traffic in consumption of network link bandwidth. Low
   urgency traffic has a low priority for timely forwarding, which does
   not necessarily imply that it is generally of minor importance. From
   this viewpoint, it can be considered as a network equivalent to a
   background priority for processes in an operating system. There may
   or may not be memory (buffer) resources allocated for this type of
   traffic.

   Some networks carry packets that ought to consume network resources
   only when no other traffic is demanding them. In this point of view,
   packets forwarded by the LE PHB scavenge otherwise unused resources
   only, which led to the name "scavenger service" in early Internet2
   deployments (see Appendix A). Other commonly used names for LE PHB
   type services are "Lower-than-best-effort" or "Less-than-best-
   effort". Alternatively, the effect of this type of traffic on all
   other network traffic is strictly limited ("no harm" property). This
   is distinct from "best-effort" (BE) traffic since the network makes
   no commitment to deliver LE packets. In contrast, BE traffic
   receives an implied "good faith" commitment of at least some
   available network resources. This document proposes a Lower Effort
   Differentiated Services per-hop behavior (LE PHB) for handling this
   "optional" traffic in a differentiated services node.

2. 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.

3. Applicability

   A Lower Effort PHB is applicable for many applications that otherwise
   use best-effort delivery. More specifically, it is suitable for
   traffic and services that can tolerate strongly varying throughput
   for their data flows, especially periods of very low throughput or
   even starvation (i.e., long interruptions due to significant or even
   complete packet loss). Therefore, an application sending an LE

marked flow needs to be able to tolerate short or (even very) long
interruptions due to the presence of severe congestion conditions
during the transmission of the flow. Thus, there ought to be an
expectation that packets of the LE PHB could be excessively delayed
or dropped when any other traffic is present. The LE PHB is suitable
for sending traffic of low urgency across a Differentiated Services
(DS) domain or DS region.

Just like best-effort traffic, LE traffic SHOULD be congestion
controlled (i.e., use a congestion controlled transport or implement
an appropriate congestion control method [RFC2914] [RFC8085]). Since
LE traffic could be starved completely for a longer period of time,
transport protocols or applications (and their related congestion
control mechanisms) SHOULD be able to detect and react to such a
starvation situation. An appropriate reaction would be to resume the
transfer instead of aborting it, i.e., an LE optimized transport
ought to use appropriate retry and timeout limits in order to avoid
the loss of the connection due to the mentioned starvation periods.
While it is desirable to achieve a quick resumption of the transfer
as soon as resources become available again, it may be difficult to
achieve this in practice. Congestion control is not only useful to
let the flows within the LE behavior aggregate adapt to the available
bandwidth that may be highly fluctuating, but is also essential if LE
traffic is mapped to the default PHB in DS domains that do not
support LE. In this case, use of background transport protocols,
e.g., similar to LEDBAT [RFC6817], is expedient.

Use of the LE PHB might assist a network operator in moving certain
kinds of traffic or users to off-peak times. Alternatively, or in
addition, packets can be designated for the LE PHB when the goal is
to protect all other packet traffic from competition with the LE
aggregate while not completely banning LE traffic from the network.
An LE PHB SHOULD NOT be used for a customer's "normal Internet"
traffic nor should packets be "downgraded" to the LE PHB instead of
being dropped, particularly when the packets are unauthorized
traffic. The LE PHB is expected to have applicability in networks
that have at least some unused capacity at certain periods.

The LE PHB allows networks to protect themselves from selected types
of traffic as a complement to giving preferential treatment to other
selected traffic aggregates. LE ought not to be used for the general
case of downgraded traffic, but could be used by design, e.g., to
protect an internal network from untrusted external traffic sources.
In this case there is no way for attackers to preempt internal (non
LE) traffic by flooding. Another use case in this regard is
forwarding of multicast traffic from untrusted sources. Multicast
forwarding is currently enabled within domains only for specific
sources within a domain, but not for sources from anywhere in the

Internet. A main problem is that multicast routing creates traffic
sources at (mostly) unpredictable branching points within a domain,
potentially leading to congestion and packet loss. In the case of
multicast traffic packets from untrusted sources are forwarded as LE
traffic, they will not harm traffic from non-LE behavior aggregates.
A further related use case is mentioned in [RFC3754]: preliminary
forwarding of non-admitted multicast traffic.

There is no intrinsic reason to limit the applicability of the LE PHB
to any particular application or type of traffic. It is intended as
an additional traffic engineering tool for network administrators.
For instance, it can be used to fill protection capacity of
transmission links that is otherwise unused. Some network providers
keep link utilization below 50% to ensure that all traffic is
forwarded without loss after rerouting caused by a link failure (cf.
Section 6 of [RFC3439]). LE marked traffic can utilize the normally
unused capacity and will be preempted automatically in case of link
failure when 100% of the link capacity is required for all other
traffic. Ideally, applications mark their packets as LE traffic,
since they know the urgency of flows.

Example uses for the LE PHB:

o For traffic caused by world-wide web search engines while they
   gather information from web servers.

o For software updates or dissemination of new releases of operating
   systems.

o For reporting errors or telemetry data from operating systems or
   applications.

o For backup traffic or non-time critical synchronization or
   mirroring traffic.

o For content distribution transfers between caches.

o For preloading or prefetching objects from web sites.

o For network news and other "bulk mail" of the Internet.

o For "downgraded" traffic from some other PHB when this does not
   violate the operational objectives of the other PHB.

o For multicast traffic from untrusted (e.g., non-local) sources.

[4](). PHB Description

The LE PHB is defined in relation to the default PHB (best-effort).
A packet forwarded with the LE PHB SHOULD have lower precedence than
packets forwarded with the default PHB, i.e., in the case of
congestion, LE marked traffic SHOULD be dropped prior to dropping any
default PHB traffic. Ideally, LE packets would be forwarded only
when no packet with any other PHB is awaiting transmission. This
means that in case of link resource contention LE traffic can be
starved completely, which may not be always desired by the network
operator's policy. The used scheduler to implement the LE PHB may
reflect this policy accordingly.

A straightforward implementation could be a simple priority scheduler
serving the default PHB queue with higher priority than the lower-
effort PHB queue. Alternative implementations may use scheduling
algorithms that assign a very small weight to the LE class. This,
however, could sometimes cause better service for LE packets compared
to BE packets in cases when the BE share is fully utilized and the LE
share not.

If a dedicated LE queue is not available, an active queue management
mechanism within a common BE/LE queue could also be used. This could
drop all arriving LE packets as soon as certain queue length or
sojourn time thresholds are exceeded.

Since congestion control is also useful within the LE traffic class,
Explicit Congestion Notification [RFC3168] SHOULD be used for LE
packets, too.

[5](). Traffic Conditioning Actions

If possible, packets SHOULD be pre-marked in DS-aware end systems by
applications due to their specific knowledge about the particular
precedence of packets. There is no incentive for DS domains to
distrust this initial marking, because letting LE traffic enter a DS
domain causes no harm. Thus, any policing such as limiting the rate
of LE traffic is not necessary at the DS boundary.

As for most other PHBs an initial classification and marking can be
also performed at the first DS boundary node according to the DS
domain's own policies (e.g., as protection measure against untrusted
sources). However, non-LE traffic (e.g., BE traffic) SHOULD NOT be
remarked to LE on a regular basis without consent or knowledge of the
user. See also remarks with respect to downgrading in Section 3 and
Section 8.

6. **Recommended DS Codepoint**

   The RECOMMENDED codepoint for the LE PHB is '000001'.

   Earlier specifications [RFC4594] recommended to use CS1 as codepoint
   (as mentioned in [RFC3662]). This is problematic since it may cause
   a priority inversion in Diffserv domains that treat CS1 as originally
   proposed in [RFC2474], resulting in forwarding LE packets with higher
   precedence than BE packets. Existing implementations SHOULD
   transition to use the unambiguous LE codepoint '000001' whenever
   possible.

   This particular codepoint was chosen due to measurements on the
   currently observable DSCP remarking behavior in the Internet
   [ietf99-secchi]. Since some network domains set the former IP
   precedence bits to zero, it is possible that some other standardized
   DSCPs get mapped to the LE PHB DSCP if it were taken from the DSCP
   standards action pool 1 (xxxxx0).

7. **Deployment Considerations**

   In order to enable LE support, DS nodes typically only need

   o A BA classifier (Behavior Aggregate classifier, see [RFC2475])
      that classifies packets according to the LE DSCP

   o A dedicated LE queue

   o A suitable scheduling discipline, e.g., simple priority queueing

   Alternatively, implementations could use active queue management
   mechanisms instead of a dedicated LE queue, e.g., dropping all
   arriving LE packets when certain queue length or sojourn time
   thresholds are exceeded.

   Internet-wide deployment of the LE PHB is eased by the following
   properties:

   o No harm to other traffic: since the LE PHB has the lowest
      forwarding priority it does not consume resources from other PHBs.
      Deployment across different provider domains with LE support
      causes no trust issues or attack vectors to existing (non LE)
      traffic. Thus, providers can trust LE markings from end-systems,
      i.e., there is no need to police or remark incoming LE traffic.

   o No PHB parameters or configuration of traffic profiles: the LE PHB
      itself possesses no parameters that need to be set or configured.

Similarly, since LE traffic requires no admission or policing, it
is not necessary to configure traffic profiles.

o No traffic conditioning mechanisms: the LE PHB requires no traffic
   meters, droppers, or shapers. See also [Section 5](#) for further
   discussion.

Operators of DS domains that cannot or do not want to implement the
LE PHB (e.g., because there is no separate LE queue available in the
corresponding nodes) SHOULD NOT drop packets marked with the LE DSCP.
They SHOULD map packets with this DSCP to the default PHB and SHOULD
preserve the LE DSCP marking. DS domains operators that do not
implement the LE PHB should be aware that they violate the "no harm"
property of LE. See also [Section 8](#) for further discussion of
forwarding LE traffic with the default PHB instead.

8. Remarking to other DSCPs/PHBs

"DSCP bleaching", i.e., setting the DSCP to '000000' (default PHB) is
NOT RECOMMENDED for this PHB. This may cause effects that are in
contrast to the original intent in protecting BE traffic from LE
traffic (no harm property). In the case that a DS domain does not
support the LE PHB, its nodes SHOULD treat LE marked packets with the
default PHB instead (by mapping the LE DSCP to the default PHB), but
they SHOULD do so without remarking to DSCP '000000'. The reason for
this is that later traversed DS domains may then have still the
possibility to treat such packets according to the LE PHB.

Operators of DS domains that forward LE traffic within the BE
aggregate need to be aware of the implications, i.e., induced
congestion situations and quality-of-service degradation of the
original BE traffic. In this case, the LE property of not harming
other traffic is no longer fulfilled. To limit the impact in such
cases, traffic policing of the LE aggregate MAY be used.

In case LE marked packets are effectively carried within the default
PHB (i.e., forwarded as best-effort traffic) they get a better
forwarding treatment than expected. For some applications and
services, it is favorable if the transmission is finished earlier
than expected. However, in some cases it may be against the original
intention of the LE PHB user to strictly send the traffic only if
otherwise unused resources are available. In case LE traffic is
mapped to the default PHB, LE traffic may compete with BE traffic for
the same resources and thus adversely affect the original BE
aggregate. Applications that want to ensure the lower precedence
compared to BE traffic even in such cases SHOULD use additionally a
corresponding Lower-than-Best-Effort transport protocol [RFC6297],
e.g., LEDBAT [RFC6817].

A DS domain that still uses DSCP CS1 for marking LE traffic
(including Low Priority-Data as defined in [RFC4594] or the old
definition in [RFC3662]) SHOULD remark traffic to the LE DSCP
'000001' at the egress to the next DS domain. This increases the
probability that the DSCP is preserved end-to-end, whereas a CS1
marked packet may be remarked by the default DSCP if the next domain
is applying Diffserv-intercon [RFC8100].

9. Multicast Considerations

Basically the multicast considerations in [RFC3754] apply. However,
using the Lower Effort PHB for multicast requires to pay special
attention to the way how packets get replicated inside routers. Due
to multicast packet replication, resource contention may actually
occur even before a packet is forwarded to its output port and in the
worst case, these forwarding resources are missing for higher
prioritized multicast or even unicast packets.

Several forwarding error correction coding schemes such as fountain
codes (e.g., [RFC5053]) allow reliable data delivery even in
environments with a potential high amount of packet loss in
transmission. When used for example over satellite links or other
broadcast media, this means that receivers that lose 80% of packets
in transmission simply need 5 times as long to receive the complete
data than those receivers experiencing no loss (without any receiver
feedback required).

Superficially viewed, it may sound very attractive to use IP
multicast with the LE PHB to build this type of opportunistic
reliable distribution in IP networks, but it can only be usefully
deployed with routers that do not experience forwarding/replication
resource starvation when a large amount of packets (virtually) need
to be replicated to links where the LE queue is full.

Thus, packet replication of LE marked packets should consider the
situation at the respective output links: it is a waste of internal
forwarding resources if a packet is replicated to output links that
have no resources left for LE forwarding. In those cases a packet
would have been replicated just to be dropped immediately after
finding a filled LE queue at the respective output port. Such
behavior could be avoided for example by using a conditional internal
packet replication: a packet would then only be replicated in case
the output link is not fully used. This conditional replication,
however, is probably not widely implemented.

While the resource contention problem caused by multicast packet
replication is also true for other Diffserv PHBs, LE forwarding is
special, because often it is assumed that LE packets get only

   forwarded in case of available resources at the output ports. The
   previously mentioned redundancy data traffic could nicely use the
   varying available residual bandwidth being utilized the by LE PHB,
   but only if the previously specific requirements in the internal
   implementation of the network devices are considered.

10. The Update to RFC 4594

   [RFC4594] recommended to use CS1 as codepoint in section 4.10,
   whereas CS1 was defined in [RFC2474] to have a higher precedence than
   CS0, i.e., the default PHB. Consequently, Diffserv domains
   implementing CS1 according to [RFC2474] will cause a priority
   inversion for LE packets that contradicts with the original purpose
   of LE. Therefore, every occurrence of the CS1 DSCP is replaced by
   the LE DSCP.

   Changes:

   o This update to RFC 4594 removes the following entry from figure 3:

```
    |---------------+---------+-------------+------------------------|
    | Low-Priority  |  CS1    |   001000    | Any flow that has no BW |
    |     Data      |         |             | assurance               |
     ------------------------------------------------------------------
```

      and replaces this by the following entry:

```
    |---------------+---------+-------------+------------------------|
    | Low-Priority  |   LE    |   000001    | Any flow that has no BW |
    |     Data      |         |             | assurance               |
     ------------------------------------------------------------------
```

   o This update to RFC 4594 extends the Notes text below figure 3 that
      currently states "Notes for Figure 3: Default Forwarding (DF) and
      Class Selector 0 (CS0) provide equivalent behavior and use the
      same DS codepoint, '000000'." to state "Notes for Figure 3:
      Default Forwarding (DF) and Class Selector 0 (CS0) provide
      equivalent behavior and use the same DS codepoint, '000000'. The
      prior recommendation to use the CS1 DSCP for Low-Priority Data has
      been replaced by the current recommendation to use the LE DSCP,
      '000001'."

   o This update to RFC 4594 removes the following entry from figure 4:

```
    |---------------+------+------------------+---------+--------+----|
    | Low-Priority  | CS1  | Not applicable   | RFC3662 |  Rate  | Yes|
    |     Data      |      |                  |         |        |    |
     ------------------------------------------------------------------
```

and replaces this by the following entry:

```
|---------------+------+------------------+--------+--------+----|
| Low-Priority  | LE   | Not applicable   | RFCXXXX |  Rate  | Yes|
|     Data      |      |                  |        |        |    |
 -----------------------------------------------------------------
```

o Section 2.3 of [RFC4594] specifies: "In network segments that use
   IP precedence marking, only one of the two service classes can be
   supported, High-Throughput Data or Low-Priority Data. We
   RECOMMEND that the DSCP value(s) of the unsupported service class
   be changed to 000xx1 on ingress and changed back to original
   value(s) on egress of the network segment that uses precedence
   marking. For example, if Low-Priority Data is mapped to Standard
   service class, then 000001 DSCP marking MAY be used to distinguish
   it from Standard marked packets on egress." This document removes
   this recommendation, because by using the herein defined LE DSCP
   such remarking is not necessary. So even if Low-Priority Data is
   unsupported (i.e., mapped to the default PHB) the LE DSCP should
   be kept across the domain as RECOMMENDED in Section 8. That
   removed text is replaced by: "In network segments that use IP
   Precedence marking, the Low-Priority Data service class receives
   the same Diffserv QoS as the Standard service class when the LE
   DSCP is used for Low-Priority Data traffic. This is acceptable
   behavior for the Low-Priority Data service class, although it is
   not the preferred behavior."

o This document removes the following line of RFC 4594,
   Section 4.10: "The RECOMMENDED DSCP marking is CS1 (Class Selector
   1)." and replaces this with the following text: "The RECOMMENDED
   DSCP marking is LE (Lower Effort), which replaces the prior
   recommendation for CS1 (Class Selector 1) marking."

11. The Update to RFC 8325

   Section 4.2.10 of RFC 8325 [RFC8325] specifies "[RFC3662] and
   [RFC4594] both recommend Low-Priority Data be marked CS1 DSCP."
   which is updated to "[RFC3662] recommends that Low-Priority Data be
   marked CS1 DSCP. [RFC4594] as updated by [RFCXXXX] recommends Low-
   Priority Data be marked LE DSCP."

   This document removes the following paragraph of RFC 8325,
   Section 4.2.10 because this document makes the anticipated change:
   "Note: This marking recommendation may change in the future, as [LE-
   PHB] defines a Lower Effort (LE) PHB for Low-Priority Data traffic
   and recommends an additional DSCP for this traffic."

Section 4.2.10 of RFC 8325 [RFC8325] specifies "therefore, it is
RECOMMENDED to map Low-Priority Data traffic marked CS1 DSCP to UP 1"
which is updated to "therefore, it is RECOMMENDED to map Low-Priority
Data traffic marked with LE DSCP or legacy CS1 DSCP to UP 1"

This update to RFC 8325 replaces the following entry from figure 1:

```
+---------------+------+---------+------------+-------------------+
| Low-Priority  | CS1  | RFC 3662 |    1       | AC_BK (Background) |
|    Data       |      |         |            |                   |
+---------------+------+---------+------------+-------------------+
```

by the following entries:

```
+---------------+------+---------+------------+-------------------+
| Low-Priority  | LE   | RFCXXXX |    1       | AC_BK (Background) |
|    Data       |      |         |            |                   |
+---------------+------+---------+------------+-------------------+
| Low-Priority  | CS1  | RFC 3662 |    1       | AC_BK (Background) |
| Data (legacy) |      |         |            |                   |
+---------------+------+---------+------------+-------------------+
```

12. The Update to draft-ietf-tsvwg-rtcweb-qos

Section 5 of [I-D.ietf-tsvwg-rtcweb-qos] describes the Recommended
DSCP Values for WebRTC Applications

This update to [I-D.ietf-tsvwg-rtcweb-qos] replaces all occurrences
of CS1 with LE in Table 1:

Flow Type	Very Low	Low	Medium	High
Audio	LE (1)	DF (0)	EF (46)	EF (46)
Interactive Video with or without Audio	LE (1)	DF (0)	AF42, AF43 (36, 38)	AF41, AF42 (34, 36)
Non-Interactive Video with or without Audio	LE (1)	DF (0)	AF32, AF33 (28, 30)	AF31, AF32 (26, 28)
Data	LE (1)	DF (0)	AF11	AF21

and updates the following paragraph:

"The above table assumes that packets marked with CS1 are treated as
"less than best effort", such as the LE behavior described in
[RFC3662]. However, the treatment of CS1 is implementation
dependent. If an implementation treats CS1 as other than "less than
best effort", then the actual priority (or, more precisely, the per-
hop-behavior) of the packets may be changed from what is intended.
It is common for CS1 to be treated the same as DF, so applications
and browsers using CS1 cannot assume that CS1 will be treated
differently than DF [RFC7657]. However, it is also possible per
[RFC2474] for CS1 traffic to be given better treatment than DF, thus
caution should be exercised when electing to use CS1. This is one of
the cases where marking packets using these recommendations can make
things worse."

as follows:

"The above table assumes that packets marked with LE are treated as
lower effort (i.e., "less than best effort"), such as the LE behavior
described in [RFCXXXX]. However, the treatment of LE is
implementation dependent. If an implementation treats LE as other
than "less than best effort", then the actual priority (or, more
precisely, the per- hop-behavior) of the packets may be changed from
what is intended. It is common for LE to be treated the same as DF,
so applications and browsers using LE cannot assume that LE will be
treated differently than DF [RFC7657]. During development of this
document, the CS1 DSCP was recommended for "very low" application
priority traffic; implementations that followed that recommendation
SHOULD be updated to use the LE DSCP instead of the CS1 DSCP."

13. IANA Considerations

This document assigns the Differentiated Services Field Codepoint
(DSCP) '000001' from the Differentiated Services Field Codepoints
(DSCP) registry (https://www.iana.org/assignments/dscp-registry/dscp-
registry.xhtml) (Pool 3, Codepoint Space xxxx01, Standards Action) to
the LE PHB. This document suggests to use a DSCP from Pool 3 in
order to avoid problems for other PHB marked flows to become
accidentally remarked as LE PHB, e.g., due to partial DSCP bleaching.
See [RFC8436] for re-classifying Pool 3 for Standards Action.

IANA is requested to update the registry as follows:

o Name: LE

o Value (Binary): 000001

o Value (Decimal): 1

o Reference: [RFC number of this memo]

14. Security Considerations

There are no specific security exposures for this PHB. Since it
defines a new class of low forwarding priority, remarking other
traffic as LE traffic may lead to quality-of-service degradation of
such traffic. Thus, any attacker that is able to modify the DSCP of
a packet to LE may carry out a downgrade attack. See the general
security considerations in [RFC2474] and [RFC2475].

With respect to privacy, an attacker could use the information from
the DSCP to infer that the transferred (probably even encrypted)
content is considered of low priority or low urgency by a user, in
case the DSCP was set on the user's request. However, this disclosed
information is only useful if some form of identification happened at
the same time, see [RFC6973] for further details on general privacy
threats.

15. References

15.1. Normative References

[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>.

15.2. Informative References

[carlberg-lbe-2001]
           Carlberg, K., Gevros, P., and J. Crowcroft, "Lower than
           best effort: a design and implementation", SIGCOMM
           Computer Communications Review Volume 31, Issue 2
           supplement, April 2001,
           <https://doi.org/10.1145/844193.844208>.

[chown-lbe-2003]
          Chown, T., Ferrari, T., Leinen, S., Sabatino, R., Simar,
          N., and S. Venaas, "Less than Best Effort: Application
          Scenarios and Experimental Results", In Proceedings of the
          Second International Workshop on Quality of Service in
          Multiservice IP Networks (QoS-IP 2003), Lecture Notes in
          Computer Science, vol 2601. Springer, Berlin,
          Heidelberg Pages 131-144, February 2003,
          <https://doi.org/10.1007/3-540-36480-3_10>.

[draft-bless-diffserv-lbe-phb-00]
          Bless, R. and K. Wehrle, "A Lower Than Best-Effort Per-Hop
          Behavior", draft-bless-diffserv-lbe-phb-00 (work in
          progress), September 1999, <https://tools.ietf.org/html/
          draft-bless-diffserv-lbe-phb-00>.

[I-D.ietf-tsvwg-rtcweb-qos]
          Jones, P., Dhesikan, S., Jennings, C., and D. Druta, "DSCP
          Packet Markings for WebRTC QoS", draft-ietf-tsvwg-rtcweb-
          qos-18 (work in progress), August 2016.

[ietf99-secchi]
          Secchi, R., Venne, A., and A. Custura, "Measurements
          concerning the DSCP for a LE PHB", Presentation held at
          99th IETF Meeting, TSVWG, Prague , July 2017,
          <https://datatracker.ietf.org/meeting/99/materials/slides-
          99-tsvwg-sessb-31measurements-concerning-the-dscp-for-a-
          le-phb-00>.

[RFC2914] Floyd, S., "Congestion Control Principles", BCP 41,
          RFC 2914, DOI 10.17487/RFC2914, September 2000,
          <https://www.rfc-editor.org/info/rfc2914>.

[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,
          <http://www.rfc-editor.org/info/rfc3168>.

[RFC3439] Bush, R. and D. Meyer, "Some Internet Architectural
          Guidelines and Philosophy", RFC 3439,
          DOI 10.17487/RFC3439, December 2002,
          <https://www.rfc-editor.org/info/rfc3439>.

[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>.

   [RFC3754] Bless, R. and K. Wehrle, "IP Multicast in Differentiated
              Services (DS) Networks", RFC 3754, DOI 10.17487/RFC3754,
              April 2004, <http://www.rfc-editor.org/info/rfc3754>.

   [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>.

   [RFC5053] Luby, M., Shokrollahi, A., Watson, M., and T. Stockhammer,
              "Raptor Forward Error Correction Scheme for Object
              Delivery", RFC 5053, DOI 10.17487/RFC5053, October 2007,
              <https://www.rfc-editor.org/info/rfc5053>.

   [RFC6297] Welzl, M. and D. Ros, "A Survey of Lower-than-Best-Effort
              Transport Protocols", RFC 6297, DOI 10.17487/RFC6297, June
              2011, <http://www.rfc-editor.org/info/rfc6297>.

   [RFC6817] Shalunov, S., Hazel, G., Iyengar, J., and M. Kuehlewind,
              "Low Extra Delay Background Transport (LEDBAT)", RFC 6817,
              DOI 10.17487/RFC6817, December 2012,
              <http://www.rfc-editor.org/info/rfc6817>.

   [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J.,
              Morris, J., Hansen, M., and R. Smith, "Privacy
              Considerations for Internet Protocols", RFC 6973,
              DOI 10.17487/RFC6973, July 2013,
              <https://www.rfc-editor.org/info/rfc6973>.

   [RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage
              Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085,
              March 2017, <https://www.rfc-editor.org/info/rfc8085>.

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

   [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>.

   [RFC8325] Szigeti, T., Henry, J., and F. Baker, "Mapping Diffserv to
              IEEE 802.11", RFC 8325, DOI 10.17487/RFC8325, February
              2018, <https://www.rfc-editor.org/info/rfc8325>.

   [RFC8436] Fairhurst, G., "Update to IANA Registration Procedures for
              Pool 3 Values in the Differentiated Services Field
              Codepoints (DSCP) Registry", RFC 8436,
              DOI 10.17487/RFC8436, August 2018,
              <https://www.rfc-editor.org/info/rfc8436>.

Appendix A. History of the LE PHB

   A first version of this PHB was suggested by Roland Bless and Klaus
   Wehrle in September 1999 [draft-bless-diffserv-lbe-phb-00], named "A
   Lower Than Best-Effort Per-Hop Behavior". After some discussion in
   the Diffserv Working Group Brian Carpenter and Kathie Nichols
   proposed a "bulk handling" per-domain behavior and believed a PHB was
   not necessary. Eventually, "Lower Effort" was specified as per-
   domain behavior and finally became [RFC3662]. More detailed
   information about its history can be found in Section 10 of
   [RFC3662].

   There are several other names in use for this type of PHB or
   associated service classes. Well-known is the QBone Scavenger
   Service (QBSS) that was proposed in March 2001 within the Internet2
   QoS Working Group. Alternative names are "Lower-than-best-effort"
   [carlberg-lbe-2001] or "Less-than-best-effort" [chown-lbe-2003].

Appendix B. Acknowledgments

   Since text is borrowed from earlier Internet-Drafts and RFCs the co-
   authors of previous specifications are acknowledged here: Kathie
   Nichols and Klaus Wehrle. David Black, Toerless Eckert, Gorry
   Fairhurst, Ruediger Geib, and Spencer Dawkins provided helpful
   comments and (also text) suggestions.

Appendix C. Change History

   This section briefly lists changes between Internet-Draft versions
   for convenience.

   Changes in Version 08:

   o revised two sentences as suggested by Spencer Dawkins

   Changes in Version 07:

   o revised some text for clarification according to comments from
      Spencer Dawkins

   Changes in Version 06:

o added Multicast Considerations section with input from Toerless
   Eckert

o incorporated suggestions by David Black with respect to better
   reflect legacy CS1 handling

Changes in Version 05:

o added scavenger service class into abstract

o added some more history

o added reference for "Myth of Over-Provisioning" in RFC3439 and
   references to presentations w.r.t. codepoint choices

o added text to update draft-ietf-tsvwg-rtcweb-qos

o revised text on congestion control in case of remarking to BE

o added reference to DSCP measurement talk @IETF99

o small typo fixes

Changes in Version 04:

o Several editorial changes according to review from Gorry Fairhurst

o Changed the section structure a bit (moved subsections 1.1 and 1.2
   into own sections 3 and 7 respectively)

o updated section 2 on requirements language

o added updates to RFC 8325

o tried to be more explicit what changes are required to RFCs 4594
   and 8325

Changes in Version 03:

o Changed recommended codepoint to 000001

o Added text to explain the reasons for the DSCP choice

o Removed LE-min,LE-strict discussion

o Added one more potential use case: reporting errors or telemetry
   data from OSs

   o Added privacy considerations to the security section (not worth an
      own section I think)

   o Changed IANA considerations section

   Changes in Version 02:

   o Applied many editorial suggestions from David Black

   o Added Multicast traffic use case

   o Clarified what is required for deployment in section 1.2
      (Deployment Considerations)

   o Added text about implementations using AQMs and ECN usage

   o Updated IANA section according to David Black's suggestions

   o Revised text in the security section

   o Changed copyright Notice to pre5378Trust200902

   Changes in Version 01:

   o Now obsoletes RFC 3662.

   o Tried to be more precise in section 1.1 (Applicability) according
      to R. Geib's suggestions, so rephrased several paragraphs. Added
      text about congestion control

   o Change section 2 (PHB Description) according to R. Geib's
      suggestions.

   o Added RFC 2119 language to several sentences.

   o Detailed the description of remarking implications and
      recommendations in Section 8.

   o Added Section 10 to explicitly list changes with respect to RFC
      4594, because this document will update it.

Appendix D. Note to RFC Editor

   This section lists actions for the RFC editor during final
   formatting.

   o Please replace the occurrences of RFCXXXX in Section 10 and
      Section 11 with the assigned RFC number for this document.

   o Delete [Appendix C](#).

   o Delete this section.

Author's Address

   Roland Bless
   Karlsruhe Institute of Technology (KIT)
   Kaiserstr. 12
   Karlsruhe 76131
   Germany

   Phone: +49 721 608 46413
   Email: roland.bless@kit.edu