

Internet Engineering Task Force (IETF)  
Request for Comments: 8622  
Obsoletes: 3662  
Updates: 4594, 8325  
Category: Standards Track  
ISSN: 2070-1721

R. Bless  
KIT  
June 2019

## A Lower-Effort Per-Hop Behavior (LE PHB) for Differentiated Services

### Abstract

This document specifies properties and characteristics of a Lower-Effort Per-Hop Behavior (LE 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, BE 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 Differentiated Services Code Point (DSCP) value for the LE PHB.

This specification obsoletes RFC 3662 and updates the DSCP recommended in RFCs 4594 and 8325 to use the DSCP assigned in this specification.

### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8622>.

## Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

## Table of Contents

1. Introduction .....	3
2. Requirements Language .....	3
3. Applicability .....	3
4. PHB Description .....	6
5. Traffic-Conditioning Actions .....	7
6. Recommended DSCP .....	7
7. Deployment Considerations .....	8
8. Re-marking to Other DSCPs/PHBs .....	9
9. Multicast Considerations .....	10
10. The Updates to RFC 4594 .....	11
11. The Updates to RFC 8325 .....	12
12. IANA Considerations .....	13
13. Security Considerations .....	14
14. References .....	15
14.1. Normative References .....	15
14.2. Informative References .....	15
Appendix A. History of the LE PHB .....	18
Acknowledgments .....	18
Author's Address .....	18

## 1. Introduction

This document defines a Differentiated Services (DS) per-hop behavior [RFC2474] called "Lower-Effort Per-Hop Behavior" (LE PHB), 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; note, however, that this 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. From this point of view, packets forwarded by the LE PHB scavenge otherwise-unused resources only; this led to the name "scavenger service" in early Internet2 deployments (see Appendix A). Other commonly used names for LE PHB types of services are "Lower than best effort" [Carlberg-LBE-2001] or "Less than best effort" [Chown-LBE-2003]. In summary, with the above-mentioned feature, the LE PHB has two important properties: it should scavenge residual capacity, and it must be preemptable by the default PHB (or other elevated PHBs) in case they need more resources. Consequently, the effect of this type of traffic on all other network traffic is strictly limited (the "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 an LE DS PHB for handling this "optional" traffic in a DS 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

An LE PHB is applicable for many applications that otherwise use BE 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. Whether or not a lack of progress is considered to be a failure is application dependent (e.g., if a transport connection fails due to timing out, the application may try several times to reestablish the transport connection in order to resume the application session before finally giving up). The LE PHB is suitable for sending traffic of low urgency across a DS domain or DS region.

Just like BE 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 strategies (e.g., exponential back-off with an upper bound) as well as corresponding retry and timeout limits in order to avoid the loss of the connection due to the above-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. In the case of a lack of a transport protocol and congestion control that are adapted to LE, applications can also use existing common transport protocols and implement session resumption by trying to reestablish failed connections. Congestion control is not only useful for letting the flows within the LE Behavior Aggregate (BA) adapt to the available bandwidth, which may be highly fluctuating; it is also essential if LE traffic is mapped to the default PHB in DS domains that do not support LE. In this case, the use of background transport protocols, e.g., similar to Low Extra Delay Background Transport (LEDBAT) [RFC6817], is expedient.

The use of the LE PHB might assist a network operator in moving certain kinds of traffic or users to off-peak times. Furthermore, 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 and packets **SHOULD NOT** 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 during 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 be used for the general case of downgraded traffic, but it 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 the forwarding of multicast traffic from untrusted sources. Multicast forwarding is currently enabled within domains only for specific sources within a domain -- not for sources from anywhere in the Internet. One major 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 where multicast traffic packets from untrusted sources are forwarded as LE traffic, they will not harm traffic from non-LE BAs. 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 the case of link failure when 100% of the link capacity is required for all other traffic. Ideally, applications mark their packets as LE traffic, because they know the urgency of flows. Since LE traffic may be starved for longer periods of time, it is probably less suitable for real-time and interactive applications.

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, 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 (BE). 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 the case of link resource contention LE traffic can be starved completely, which may not always be desired by the network operator's policy. A scheduler used 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 LE 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 is 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 (ECN) [RFC3168] SHOULD be used for LE packets, too. More specifically, an LE implementation SHOULD also apply Congestion Experienced (CE) marking for ECT-marked packets ("ECT" stands for ECN-Capable Transport), and transport protocols used for LE SHOULD support and employ ECN. For more information on the benefits of using ECN, see [RFC8087].

## 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 also be performed at the first DS boundary node according to the DS domain's own policies (e.g., as a protection measure against untrusted sources). However, non-LE traffic (e.g., BE traffic) **SHOULD NOT** be re-marked to LE. Re-marking traffic from another PHB results in that traffic being "downgraded". This changes the way the network treats this traffic, and it is important not to violate the operational objectives of the original PHB. See Sections 3 and 8 for notes related to downgrading.

## 6. Recommended DSCP

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

Earlier specifications (e.g., [RFC4594]) recommended the use of Class Selector 1 (CS1) as the 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 Differentiated Services Code Point (DSCP) re-marking 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) [RFC2474] [RFC8436].

## 7. Deployment Considerations

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

- o A BA 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 re-mark 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 domain 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 of the LE PHB.



## 8. Re-marking 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 to protect BE traffic from LE traffic (the "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 re-marking to DSCP '000000'. This is because DS domains that are traversed later may then still have the opportunity 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 QoS 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 the case that LE-marked packets are effectively carried with the default PHB (i.e., forwarded as BE 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 the case that 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 additionally use a corresponding lower-than-BE 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 re-mark 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 re-marked by the default DSCP if the next domain is applying Diffserv-Interconnection [RFC8100].

## 9. Multicast Considerations

Basically, the multicast considerations in [RFC3754] apply. However, using the LE PHB for multicast requires paying special attention to 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. In the worst case, these forwarding resources are missing for higher-priority multicast or even unicast packets.

Several forward error correction coding schemes, such as fountain codes (e.g., [RFC5053]), allow reliable data delivery even in environments with a potentially 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 five times longer 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, a packet replication mechanism for 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 cases where 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 only get forwarded in the case of available resources at the output ports. The previously mentioned redundancy data traffic could suitably use the varying available residual bandwidth being utilized by the LE PHB, but only if the specific requirements stated above for conditional replication in the internal implementation of the network devices are considered.

## 10. The Updates to RFC 4594

[RFC4594] recommended the use of CS1 as the codepoint in its 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 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 its Figure 3:

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

and replaces it with the following entry:

Low-Priority Data	LE	000001	Any flow that has no BW 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 DSCP, '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 its Figure 4:

Low-Priority Data	CS1	Not applicable	RFC3662	Rate	Yes
----------------------	-----	----------------	---------	------	-----

and replaces it with the following entry:

Low-Priority Data	LE	Not applicable	RFC 8622	Rate	Yes
----------------------	----	----------------	----------	------	-----

- o Section 2.3 of [RFC4594] specifies the following: "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 LE DSCP defined herein, such re-marking 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 the following: "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 in Section 4.10 of RFC 4594: "The RECOMMENDED DSCP marking is CS1 (Class Selector 1)." and replaces it 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 Updates to RFC 8325

Section 4.2.10 of RFC 8325 [RFC8325] specifies that "[RFC3662] and [RFC4594] both recommend Low-Priority Data be marked CS1 DSCP." This is updated to "[RFC3662] recommends that Low-Priority Data be marked CS1 DSCP. [RFC4594], as updated by RFC 8622, recommends that Low-Priority Data be marked LE DSCP."

This document removes the following paragraph in Section 4.2.10 of [RFC8325], 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 that "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 its Figure 1:

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

with the following entries:

Low-Priority Data	LE	RFC 8622	1	AC_BK (Background)
Low-Priority Data (legacy)	CS1	RFC 3662	1	AC_BK (Background)

## 12. 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 Pool 3 Codepoints", Codepoint Space xxxx01, Standards Action) [RFC8126] to the LE PHB. This document uses a DSCP from Pool 3 in order to avoid problems for other PHB-marked flows, where they could become accidentally re-marked as LE PHB, e.g., due to partial DSCP bleaching. See [RFC8436] regarding reclassifying Pool 3 for Standards Action.

IANA has updated this registry as follows:

- o Name: LE
- o Value (Binary): 000001
- o Value (Decimal): 1
- o Reference: RFC 8622

### 13. Security Considerations

There are no specific security exposures for this PHB. Since it defines a new class that is of low forwarding priority, re-marking other traffic as LE traffic may lead to QoS 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 if the DSCP was set per the user's request. On the one hand, this disclosed information is useful only if correlation with metadata (such as the user's IP address) and/or other flows reveal a user's identity. On the other hand, it might help an observer (e.g., a state-level actor) who is interested in learning about the user's behavior from observed traffic: LE-marked background traffic (such as software downloads, operating system updates, or telemetry data) may be less interesting for surveillance than general web traffic. Therefore, the LE marking may help the observer to focus on potentially more interesting traffic (however, the user may exploit this particular assumption and deliberately hide interesting traffic in the LE aggregate). Apart from such considerations, the impact of disclosed information by the LE DSCP is likely negligible in most cases, given the numerous traffic analysis possibilities and general privacy threats (e.g., see [RFC6973]).

## 14. References

### 14.1. 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, <<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>>.
- [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>>.
- [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>>.

### 14.2. Informative References

- [Carlberg-LBE-2001] Carlberg, K., Gevros, P., and J. Crowcroft, "Lower than best effort: a design and implementation", ACM SIGCOMM Computer Communication Review, Volume 31 Issue 2 supplement, DOI 10.1145/844193.844208, April 2001, <<https://dl.acm.org/citation.cfm?doid=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", 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, DOI 10.1007/3-540-36480-3\_10, February 2003, <[https://link.springer.com/chapter/10.1007%2F3-540-36480-3\\_10](https://link.springer.com/chapter/10.1007%2F3-540-36480-3_10)>.

**[Diffserv-LBE-PHB]**

Bless, R. and K. Wehrle, "A Lower Than Best-Effort Per-Hop Behavior", Work in Progress, draft-bless-diffserv-lbe-phb-00, September 1999.

**[IETF99-Secchi]**

Secchi, R., Venne, A., and A. Custura, "Measurements concerning the DSCP for a LE PHB", Presentation held at the 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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://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, <<https://www.rfc-editor.org/info/rfc6817>>.
- [RFC6973] Cooper, A., Tschafenig, 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>>.
- [RFC8087] Fairhurst, G. and M. Welzl, "The Benefits of Using Explicit Congestion Notification (ECN)", RFC 8087, DOI 10.17487/RFC8087, March 2017, <<https://www.rfc-editor.org/info/rfc8087>>.
- [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>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/info/rfc8126>>.
- [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 draft version of this PHB was suggested by Roland Bless and Klaus Wehrle in September 1999 [Diffserv-LBE-PHB], 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].

## Acknowledgments

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

## Author's Address

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

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