INTAREA Group
Internet-Draft
Updates: 4884 (if approved)
Intended status: Standards Track
Expires: 21 February 2026

R. Bonica
HPE
X. He
China Telecom
X. Min
ZTE Corporation
T. Mizrahi
Huawei

20 August 2025

ICMP Extension Structure Length Field
draft-ietf-intarea-icmp-exten-hdr-len-08

Abstract

The ICMP Extension Structure (RFC4884) does not have a length field. Therefore, unless the length of the Extension Structure can be inferred from other data in the ICMP message, the Extension Structure must be the last item in the ICMP message.

This document updates RFC 4884 to define a length field for the ICMP Extension Structure. When length information is provided, receivers can use it to parse ICMP messages. Specifically, receivers can use length information to determine the offset at which the item after the ICMP Extension Structure begins.

Status of This Memo

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

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

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

This Internet-Draft will expire on 21 February 2026.

Table of Contents

1. Introduction

The ICMP Extension Structure [RFC4884] has variable length. However, it does not include a field that reflects its length. Therefore, implementations can parse the ICMP Extension Structure only when it appears at the end of an ICMP message.

It is good practice for a variable-length data structure to include a field that reflects its length. This allows implementations to parse the structure even when it does not appear at the end of a message. The ICMP Extension Structure includes reserved bits that are available for this purpose.

This document adds a length field to the ICMP Extension Header. It does not define data items that might follow the ICMP Extension Structure.

The specifications of this document apply to all ICMP Extension Structures, regardless of whether they appear in ICMPv4 [RFC0792] or ICMPv6 [RFC4443] messages.

This document UPDATES [RFC4884].

2. Conventions and Definitions

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. The ICMP Extension Structure

An ICMP Extension Structure contains exactly one Extension Header followed by one or more objects. The Extension Header format is defined in Section 7 of [RFC4884]. This document modifies the Extension Header format by allocating the lower 8 bits of the reserved field for a new length field. Figure 1 depicts the updated Extension Header format.

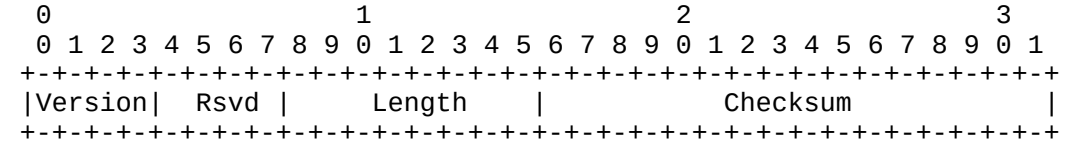

Figure 1: ICMP Extension Header As Updated By This Document

Version: 4 bits.

* ICMP Extension Header version number. This is version 2 as per [RFC4884].

Reserved (Rsvd): 4 bits

* MUST be set to 0 by the sender and MUST be ignored by the receiver.

Length: 8 bits

* This field represents the length of the ICMP Extension Structure, including all options and optional padding, but excluding the ICMP Extension Header. The length is measured in 4-byte words. Legacy implementations set this field to 0 as per section 7 of [RFC4884]. Therefore, implementation SHOULD NOT drop packets if this field is set to 0.

Checksum: 16 bits

* As per [RFC4884], the checksum is the one's complement of the one's complement sum of the data structure, with the checksum field replaced by zero for the purpose of computing the checksum. An all-zero value means that no checksum was transmitted. See Section 5.2 of [RFC4884] for a description of how this field is used.

The ICMP Extension Structure MUST be zero-padded so that it ends on a 4-byte boundary. If it does not end on a 4-byte boundary, the receiving node will parse the ICMP message incorrectly and may discard it.

The receiver MUST silently discard an ICMP message in the following cases:

* The length field in the ICMP Extension Header indicates that the ICMP Extension Structure is too large to fit in the ICMP message.

* The length field in the final ICMP Extension Object indicates that the final ICMP Extension Object is too large to fit in the ICMP Extension Structure.

* The final three bytes of the ICMP Extension Structure are neither padding (i.e., zeros) nor part of a well-formed ICMP Extension Object.

4. Backwards Compatibility

Legacy implementations that do not support the mechanism defined in this document set the length field to zero when sending a packet and ignore the length field in received ICMP messages.

Such implementations require one of the following:

* The ICMP Extension Structure is final item in the ICMP packet.

* The length of the ICMP Extension Structure can be inferred from other fields in the packet.

Currently, no mechanisms rely on the ICMP extension structure length field. Should such mechanisms be defined in the future, backward compatibility with legacy implementations should be discussed for each case.

5. UPDATES to RFC 4884

5.1. Length Field

In Section 7 of [RFC4884], an ICMP Extension Header contains a 12-bit reserved field.

Section 3 of this document allocates the lower 8 bits of that field for a new length field. Figure 1 provides a diagram of the updated ICMP Extension header.

5.2. Malformed Extension Headers

[RFC4884] offered no advice regarding the processing of malformed ICMP Extension Headers.

Section 3 of this document offers the following advice:

The receiver MUST silently discard an ICMP message in the following cases:

* The length field in the ICMP Extension Header indicates that the ICMP Extension Structure is too large to fit in the ICMP message.

* The length field in the ICMP Extension Structure is less than to the total length of ICMP Extension Objects.

* The final three bytes of the ICMP Extension Structure are neither padding (i.e., zeros) nor part of a well-formed ICMP Extension Object.

5.3. Padding Requirement

In [RFC4884], the ICMP Extension Structure was not required to end on a 4-byte boundary.

Section 3 of this document adds the following requirement:

The ICMP Extension Structure MUST be zero-padded so that it ends on a 4-byte boundary. If it does not end on a 4-byte boundary, the receiving node will parse the ICMP message incorrectly and may discard it.

5.4. Ignore Reserved Field

[RFC4884] describes the reserved field of the ICMP Extension Header as follows:

Must be set to 0.

Section 3 of this document describes the reserved field as follows:

MUST be set to 0 by the sender and MUST be ignored by the receiver.

6. IANA Considerations

This document requires no IANA actions.

7. Security Considerations

This document introduces no security vulnerabilities. However, it does inherit security considerations from [RFC4884].

8. Acknowledgements

Thanks to Tom Herbert, Jen Linkova, Erik Vynke and Michael Welzl for their review and helpful suggestions.

9. Normative References

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/rfc/rfc792>.

[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/rfc/rfc2119>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/rfc/rfc4443>.

[RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, DOI 10.17487/RFC4884, April 2007, <https://www.rfc-editor.org/rfc/rfc4884>.

[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/rfc/rfc8174>.

Authors' Addresses

Ron Bonica
HPE
United States of America
Email: rbonica@juniper.net

Xiaoming He
China Telecom
China
Email: hexm4@chinatelecom.cn

Xiao Min
ZTE Corporation
China
Email: xiao.min2@zte.com.cn

Tal Mizrahi
Huawei
Israel
Email: tal.mizrahi.phd@gmail.com