INTAREA Working Group
Internet-Draft
Updates: 4884 (if approved)
Intended status: Standards Track
Expires: 28 August 2026

X. Min
ZTE Corp.
R. Bonica
HPE
G. Mirsky
Ericsson

24 February 2026

ICMP Query for IP Node Information
draft-xbm-intarea-icmp-query-00

Abstract

This document introduces two new ICMP messages. They are called the ICMP Query Request and the ICMP Query Response. The ICMP Query Request requests information. The ICMP Query Response provides information in response to an ICMP Query Request.

This document updates RFC 4884.

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 28 August 2026.

Copyright Notice

Table of Contents

1. Introduction

This document introduces two new ICMP messages. They are called the ICMP Query Request and the ICMP Query Response. The ICMP Query Request requests information. The ICMP Query Response provides information in response to an ICMP Query Request.

Both messages are specified for ICMPv4 [RFC792] and ICMPv6 [RFC4443]. Both messages include an ICMP Extension Structure [RFC4884]. ICMP Extension Objects in the Query Request message determine which information is requested. ICMP Extension Objects in the Query Response message provide the requested information.

To prevent denial of service attacks, the ICMP Query Response message MUST NOT be longer than the corresponding ICMP Query Request message.

This document updates [RFC4884].

2. Conventions Used in This Document

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. ICMP Query Request

The ICMP Query Request message is defined for both ICMPv4 and ICMPv6. Like any ICMP message, the ICMP Query Request message is encapsulated in an IP header. The ICMPv4 version of the Query Request message is encapsulated in an IPv4 header, while the ICMPv6 version is encapsulated in an IPv6 header.

The ICMP Query Request message has the following format:

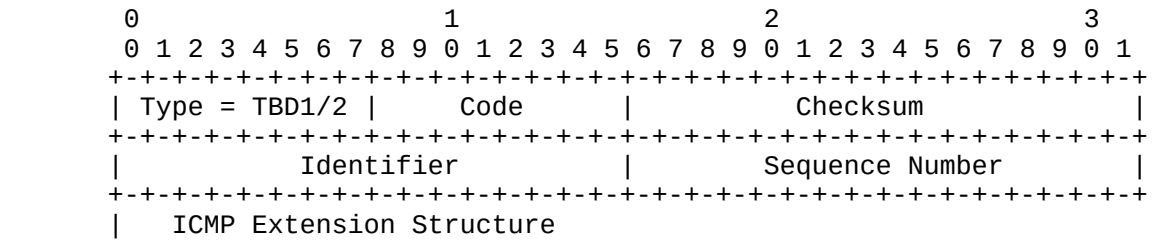

Figure 1: ICMP Query Request Message

IP Header fields:

* Source Address: The Source Address identifies the ICMP Querying node. It MUST be a valid IP unicast address.

* Destination Address: The Destination Address identifies the ICMP Queried node. It MUST be a valid IP unicast address.

ICMP fields:

* Type: ICMP Query Request. The value is TBD1 for ICMP and TBD2 for ICMPv6.

* Code: MUST be set to 0 and MUST be ignored upon receipt.

* Checksum: The same as defined in [RFC4443].

* Identifier: An Identifier aids in matching ICMP Query Replies to ICMP Query Requests.

* Sequence Number: A Sequence Number to aid in matching ICMP Query Replies to ICMP Query Requests.

* Following the ICMP Query Request header, it’s an ICMP Extension Structure as specified in Sections 7 and 8 of [RFC4884], continuing to the end of the packet.

Nothing can be added after the ICMP Extension Structure.

3.1. Query Request Objects

One or more Query Request Objects MUST be encapsulated in an ICMP Extension Structure of the ICMP Query Request message.

Each Query Request Object has the following format:

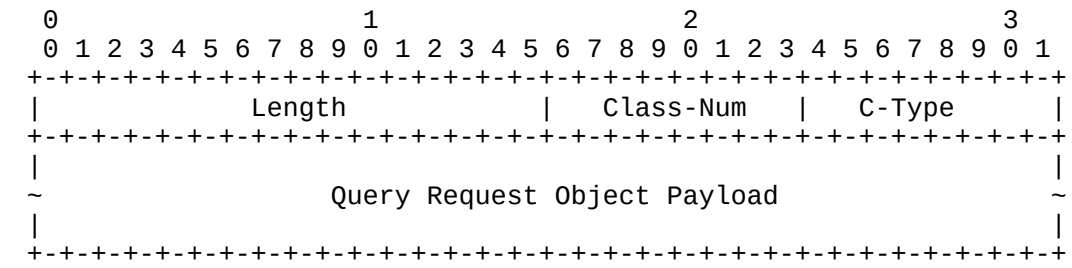

Figure 2: Query Request Object

Object fields:

* Class-Num: Indicates the class of IP node information to be queried. The value will be requested by a separate document.

* C-Type: Indicates the sub-type of IP node information to be queried. The value will be requested by a separate document.

* Length: Length of the object, measured in octets, including the Object Header and payload.

* Object payload: Following the Query Request Object Header is the Query Request Object Payload, which is used to define the scope of IP node information to be queried. The length of this field is variable. The value will be defined by a separate document.

3.2. Pad Objects

One or more Pad Objects MAY be encapsulated in an ICMP Extension Structure of the ICMP Query Request message.

Each Pad Object has the following format:

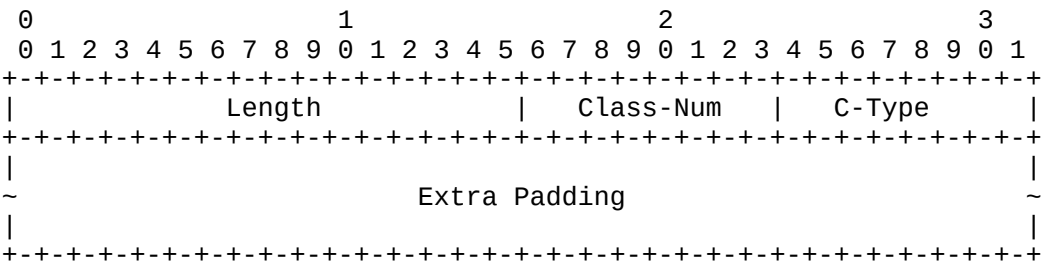

Figure 3: Pad Object

Object fields:

* Class-Num: Indicates that it’s a Pad Object. The value is TBD5.

* C-Type: The value is 0.

* Length: Length of the object, measured in octets, including the Object Header and payload.

* Object payload: Following the Pad Object Header is the Pad Object Payload, which SHOULD be filled by a sequence of pseudorandom numbers, or MAY be filled with all zeros. An implementation MUST control the content of the Pad Object Payload field..

4. ICMP Query Response

The ICMP Query Response message is defined for both ICMPv4 and ICMPv6. Like any ICMP message, the ICMP Query Response message is encapsulated in an IP header. The ICMPv4 version of the Query Response message is encapsulated in an IPv4 header, while the ICMPv6 version is encapsulated in an IPv6 header.

The ICMP Query Response message has the following format:

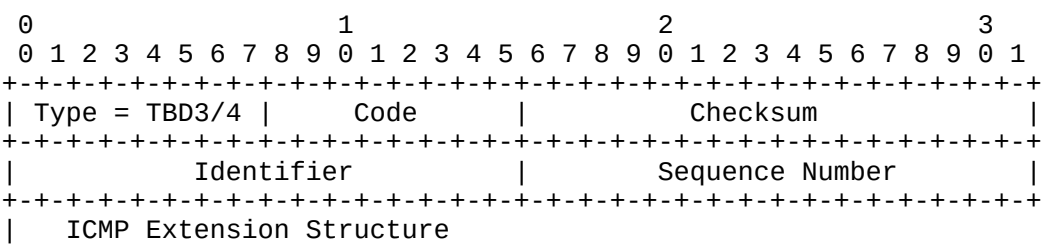

Figure 4: ICMP Query Response Message

IP Header fields:

* Source Address: Copied from the Destination Address field of the invoking ICMP Query Request packet.

* Destination Address: Copied from the Source Address field of the invoking ICMP Query Request packet.

ICMP fields:

* Type: ICMP Query Response. The value is TBD3 for ICMPv4 and TBD4 for ICMPv6.

* Code: The values are (0) No Error, (1) Malformed Query, (2) Unrecognized Query Request Object, and (3) Request Denied. See Section 5 for details.

* Checksum: The same as defined in [RFC4443].

* Identifier: Copied from the Identifier field of the invoking ICMP Query Request message.

* Sequence Number: Copied from the Sequence Number field of the invoking ICMP Query Request message.

* Following the ICMP Query Response header, it’s an ICMP Extension Structure as specified in Sections 7 and 8 of [RFC4884], continuing to the end of the packet.

Nothing can be added after the ICMP Extension Structure.

4.1. Query Response Objects

One or more Query Response Objects MUST be encapsulated in an ICMP Extension Structure of the ICMP Query Response message.

Each Query Response Object has the following format:

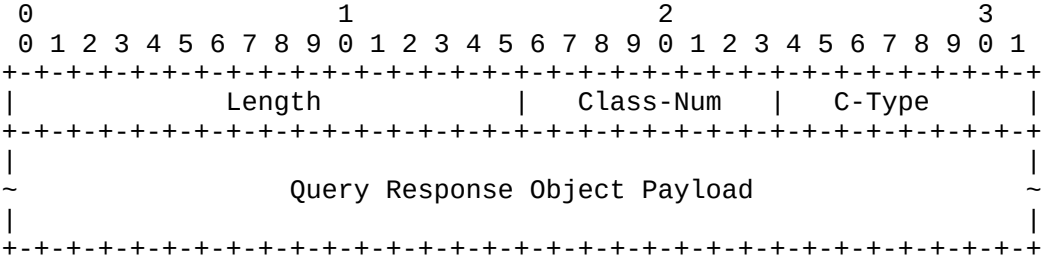

Figure 5: Query Response Object

Object fields:

* Class-Num: Indicates the class of replied IP node information. The value will be requested by a separate document.

* C-Type: Indicates the sub-type of replied IP node information. The value will be requested by a separate document.

* Length: Length of the object, measured in octets, including the Object Header and payload.

* Object payload: Following the Query Response Object Header is the Query Response Object Payload, which is the replied IP node information. The length of this field is variable. The value will be defined by a separate document.

5. Code Field Processing

The Code field in the ICMP Query Response MUST be set to (1) Malformed Query if any of the following conditions apply:

* The ICMP Query Request does not include an ICMP Extension Structure.

* The ICMP Extension Structure checksum is 0 or incorrect.

* The ICMP Query Request is otherwise malformed.

The Code field in the ICMP Query Response MUST be set to (2) Unrecognized Query Request Object if any of the following conditions apply:

* The ICMP Extension Structure of the ICMP Query Request does not include a Query Request Object.

* None of the Class-Num of the Query Request Object is recognized.

* None of the C-Type of the Query Request Object is recognized.

6. Updates to RFC 4884

Section 4.6 of [RFC4884] provides a list of extensible ICMP messages (i.e., messages that can carry the ICMP Extension Structure). This document adds the ICMP Query Request message and the ICMP Query Response message to that list.

7. IANA Considerations

This document requests the following actions from IANA:

* Add the following ICMPv4 Type to the "ICMP Type Numbers" registry:

  - TBD1 Query Request

  Add the following Code to the "Type TBD1 - Query Request" subregistry:

  - (0) No Error

* Add the following ICMPv6 Type to the "ICMPv6 'type' Numbers" registry:

  - TBD2 Query Request

  - As ICMPv6 distinguishes between informational and error messages, and this is an informational message, the value must be assigned from the range 128-255.

  Add the following Code to the "Type TBD2 - Query Request" subregistry:

  - (0) No Error

* Add the following ICMPv4 Type to the "ICMP Type Numbers" registry:

  - TBD3 Query Response

  Add the following Codes to the "Type TBD3 - Query Response" subregistry:

  - (0) No Error

  - (1) Malformed Query

  - (2) Unrecognized Query Request Object

  - (3) Request Denied

* Add the following ICMPv6 Type to the "ICMPv6 'type' Numbers" registry:

  - TBD4 Query Response

- As ICMPv6 distinguishes between informational and error messages, and this is an informational message, the value must be assigned from the range 128-255.

Add the following Codes to the "Type TBD4 - Query Response" subregistry:

- (0) No Error

- (1) Malformed Query

- (2) Unrecognized Query Request Object

- (3) Request Denied

* Add the following Class-Num to the "ICMP Extension Object Classes and Class Sub-types" registry:

  - (TBD5) Pad Object

  Add the following C-type to the "Sub-types - Class TBD5 - Pad Object" subregistry:

  - (0) Reserved

  C-Type values are assigned on a First Come First Serve (FCFS) basis with a range of 0-255.

All codes mentioned above are assigned on an FCFS basis with a range of 0-255.

8. Security Considerations

Security issues discussed in [RFC4884] apply to this document.

This document recommends using IP Authentication Header [RFC4302] or IP Encapsulating Security Payload Header [RFC4303] to provide integrity protection for replied IP node information.

This document recommends using IP Encapsulating Security Payload Header [RFC4303] to provide privacy protection for replied IP node information.

This document recommends that the network operators establish policies that restrict access to ICMP Query functionality. In order to enforce these policies, nodes that support ICMP Query functionality MUST support the following configuration options:

* Enable/disable ICMP Query functionality. By default, ICMP Query functionality is disabled.

* Define the prefixes from which ICMP Query Request messages are permitted.

In order to protect local resources, implementations SHOULD rate-limit incoming ICMP Query Request messages.

To avoid the potential amplification attack, an implementation that supports this specification MUST ensure that the Query Response message must never be larger than the Query Request message.

9. Acknowledgements

TBA.

10. References

10.1. 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>.

[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/info/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/info/rfc4884>.

[RFC792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

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

10.2. Informative References

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

Authors' Addresses

Xiao Min
ZTE Corp.
Nanjing
China
Phone: +86 18061680168
Email: xiao.min2@zte.com.cn

Ron Bonica
HPE
United States of America
Email: ronald.bonica@hpe.com

Greg Mirsky
Ericsson
United States of America
Email: gregimirsky@gmail.com