int-area
Internet-Draft
Obsoletes: 8335 (if approved)
Updates: 4884 (if approved)
Intended status: Standards Track
Expires: 16 October 2026

B. Fenner, Ed.
Arista Networks
R. Bonica
Juniper Networks
R. Thomas
Arista Networks
J. Linkova
Google
C. Lenart
Verizon
M. Boucadair
Orange
14 April 2026

PROBE: A Utility for Probing Interfaces
draft-ietf-intarea-rfc8335bis-03

Abstract

This document describes a network diagnostic tool called PROBE. PROBE is similar to PING in that it can be used to query the status of a probed interface, but it differs from PING in that it does not require bidirectional connectivity between the probing and probed interfaces. Instead, PROBE requires bidirectional connectivity between the probing interface and a proxy interface. The proxy interface can reside on the same node as the probed interface, or it can reside on a node to which the probed interface is directly connected. This document updates RFC 4884 and obsoletes RFC 8335.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://fenner.github.io/probe-clarification/draft-ietf-intarea-rfc8335bis.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-intarea-rfc8335bis/.

Discussion of this document takes place on the Internet Area Area mailing list (mailto:int-area@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/int-area/. Subscribe at https://www.ietf.org/mailman/listinfo/int-area/.

Source for this draft and an issue tracker can be found at https://github.com/fenner/probe-clarification.

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 16 October 2026.

Copyright Notice

Copyright (c) 2026 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Network operators use PING [RFC2151] to test bidirectional connectivity between two interfaces. For the purposes of this document, these interfaces are called the probing and probed interfaces. PING sends an ICMP [RFC0792] [RFC4443] Echo Request message from the probing interface to the probed interface. The probing interface resides on a probing node while the probed interface resides on a probed node.

If the probed interface receives the ICMP Echo Request message, it returns an ICMP Echo Reply. When the probing interface receives the ICMP Echo Reply, it has verified bidirectional connectivity between the probing and probed interfaces. Specifically, it has verified that:

* The probing node can reach the probed interface.

* The probed interface is active.

* The probed node can reach the probing interface.

* The probing interface is active.

This document describes a network diagnostic tool called PROBE. PROBE is similar to PING in that it can be used to query the status of a probed interface, but it differs from PING in that it does not require bidirectional connectivity between the probing and probed interfaces. Instead, PROBE requires bidirectional connectivity between the probing interface and a proxy interface. The proxy interface can reside on the same node as the probed interface, or it can reside on a node to which the probed interface is directly connected. A list of use cases for this characteristic can be found in Section 5 of this document.

Like PING, PROBE executes on a probing node. It sends an ICMP Extended Echo Request message from a local interface, called the probing interface, to a proxy interface. The proxy interface resides on a proxy node.

The ICMP Extended Echo Request contains an ICMP Extension Structure and the ICMP Extension Structure contains an Interface Identification Object. The Interface Identification Object identifies the probed interface. The probed interface can reside on or be directly connected to the proxy node.

When the proxy interface receives the ICMP Extended Echo Request, the proxy node executes access control procedures. If access is granted, the proxy node determines the status of the probed interface and returns an ICMP Extended Echo Reply message. The ICMP Extended Echo Reply indicates the status of the probed interface.

If the probed interface resides on the proxy node, PROBE determines the status of the probed interface as it would determine its oper-status [RFC8343]. If oper-status is equal to 'up' (1), PROBE reports that the probed interface is active. Otherwise, PROBE reports that the probed interface is inactive.

If the probed interface resides on a node that is directly connected to the proxy node, and the probed interface appears in the IPv4 Address Resolution Protocol (ARP) table [RFC0826] or IPv6 Neighbor Cache [RFC4861], PROBE reports interface reachability. Otherwise, PROBE reports that the table entry does not exist.

1.1. Terminology

This document uses the following terms:

* Probing interface: The interface that sends the ICMP Extended Echo Request.

* Probing node: The node upon which the probing interface resides.

* Proxy interface: The interface to which the ICMP Extended Echo Request message is sent.

* Proxy node: The node upon which the proxy interface resides.

* Probed interface: The interface whose status is being queried.

* Probed node: The node upon which the probed interface resides. If the proxy interface and the probed interface reside upon the same node, the proxy node is also the probed node. Otherwise, the proxy node is directly connected to the probed node.

1.2. 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.

1.3. A note on this document’s use of ICMP Extensions

This document defines a unique use of ICMP Extensions [RFC4884]. Normally, ICMP Extensions are defined to start at a given point and continue to the end of the packet. However, when the extension object is an Interface Identification Object as defined in this memo, the extension structure (including the checksum) consists only of that single ICMP Extension Object. This is done to maintain compatibility with the initial set of implementations of RFC8335, which behave this way. The ICMP Extension Structure checksum covers only the Interface Identification Object. Any data following it is not covered by this checksum but is covered by the ICMP header checksum, which protects the entire ICMP message (see Section 10 for further discussion). New uses of ICMP Extensions, and in fact uses of Extended Echo using some object other than the Interface Identification Object, SHOULD NOT behave this way. Uses other than defined in this memo SHOULD treat the ICMP Extension Structure as extending to the end of the packet as [RFC4884] defines.

2. ICMP Extended Echo Request

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

Figure 1 depicts the ICMP Extended Echo Request message.

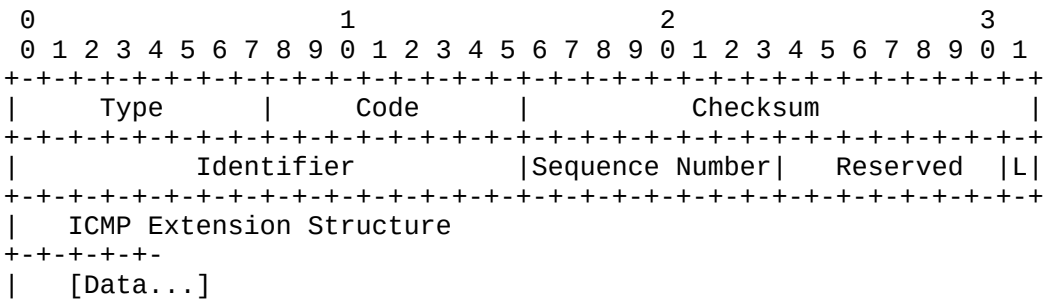

Figure 1: ICMP Extended Echo Request Message

IP Header fields:

* Source Address: The Source Address identifies the probing interface. It MUST be a valid IPv4 or IPv6 unicast address.

* Destination Address: The Destination Address identifies the proxy interface. It MUST be a unicast address.

ICMP fields:

* Type: Extended Echo Request. The value for ICMPv4 is 42. The value for ICMPv6 is 160.

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

* Checksum: For ICMPv4, see [RFC0792]. For ICMPv6, see [RFC4443].

* Identifier: An Identifier to aid in matching Extended Echo Replies to Extended Echo Requests. May be 0.

* Sequence Number: A Sequence Number to aid in matching Extended Echo Replies to Extended Echo Requests. May be 0.

* Reserved: This field MUST be set to 0 and ignored upon receipt.

* L (local): The L-bit is set if the probed interface resides on the proxy node. The L-bit is clear if the probed interface is directly connected to the proxy node.

* ICMP Extension Structure: The ICMP Extension Structure contains an Interface Identification Object that identifies the probed interface. The checksum in the ICMP Extension structure covers the Interface Identification Object but not any (optional) data that follows.

Section 7 of [RFC4884] defines the ICMP Extension Structure. As per RFC 4884, the Extension Structure contains exactly one Extension Header followed by one or more objects. When applied to the ICMP Extended Echo Request message, the Extension Object(s) define the operation to perform. In the PROBE application, the ICMP Extension Structure MUST contain exactly one instance of the Interface Identification Object (Section 2.1), and the ICMP Extension Structure does not cover the rest of the packet; it ends at the end of the single Interface Identification Object, and what follows is simply optional data. The behavior when it contains a different Extension Object is not defined by this memo.
[I-D.ietf-6man-icmpv6-reflection] is an example of a document which defines a different Extension Object and the corresponding behavior.

If the L-bit is set, the Interface Identification Object can identify the probed interface by name, index, or address. If the L-bit is clear, the Interface Identification Object MUST identify the probed interface by address.

If the Interface Identification Object identifies the probed interface by address, that address can be a member of any address family. For example, an ICMPv4 Extended Echo Request message can carry an Interface Identification Object that identifies the probed interface by IPv4, IPv6, or IEEE 802 address. Likewise, an ICMPv6 Extended Echo Request message can carry an Interface Identification Object that identifies the probed interface by IPv4, IPv6, or IEEE 802 address.

The Interface Identification Object MAY be followed by an optional data section, which is not interpreted but is simply present to be copied to the ICMP Extended Echo Reply.

The size of the resulting packet MUST NOT exceed the outgoing interface MTU.

2.1. Interface Identification Object

The Interface Identification Object identifies the probed interface by name, index, or address. Like any other ICMP Extension Object, it contains an Object Header and Object Payload. The Object Header contains the following fields:

* Class-Num: Interface Identification Object. The value is 3.

* C-Type: Values are (1) Identifies Interface by Name, (2) Identifies Interface by Index, and (3) Identifies Interface by Address.

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

If the Interface Identification Object identifies the probed interface by name, the Object Payload MUST be the interface name as defined in [RFC8343]. If the Object Payload would not otherwise terminate on a 32-bit boundary, it MUST be padded with ASCII NUL characters, adjusting the Length accordingly.

If the Interface Identification Object identifies the probed interface by index, the length is equal to 8 and the payload contains the if-index [RFC8343].

If the Interface Identification Object identifies the probed interface by address, the payload is as depicted in Figure 2.

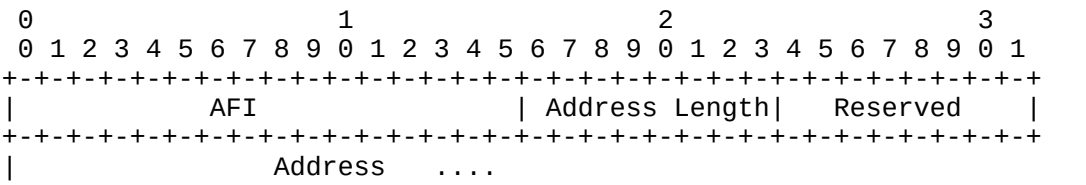

Figure 2: Interface Identification Object - C-Type 3 Payload

Payload fields are defined as follows:

* Address Family Identifier (AFI): This 16-bit field identifies the type of address represented by the Address field. All values found in the IANA registry of Address Family Numbers (available from [IANA.address-family-numbers]) are valid in this field.

* Address Length: Number of significant bytes contained by the Address field. (The Address field contains significant bytes and padding bytes.)

* Reserved: This field MUST be set to 0 and ignored upon receipt.

* Address: This variable-length field represents an address associated with the probed interface. If the address field would not otherwise terminate on a 32-bit boundary, it MUST be padded with zeroes.

3. ICMP Extended Echo Reply

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

Figure 3 depicts the ICMP Extended Echo Reply message.

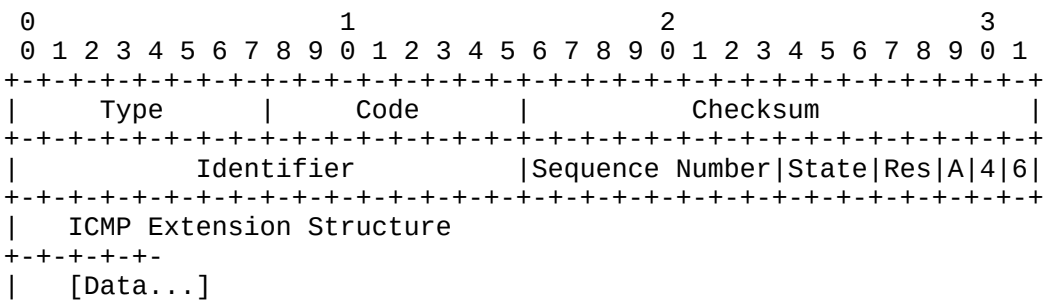

Figure 3: ICMP Extended Echo Reply Message

IP Header fields:

* Source Address: Copied from the Destination Address field of the invoking Extended Echo Request message.

* Destination Address: Copied from the Source Address field of the invoking Extended Echo Request message.

ICMP fields:

* Type: Extended Echo Reply. The value for ICMPv4 is 43. The value for ICMPv6 is 161.

* Code: Values are (0) No Error, (1) Malformed Query, (2) No Such Interface, (3) No Such Table Entry, and (4) Multiple Interfaces Satisfy Query.

* Checksum: For ICMPv4, see [RFC0792]. For ICMPv6, see [RFC4443].

* Identifier: Copied from the Identifier field of the invoking Extended Echo Request packet.

* Sequence Number: Copied from the Sequence Number field of the invoking Extended Echo Request packet.

* State: If Code is not equal to 0, this field MUST be set to 0 and ignored upon receipt. Likewise, if the probed interface resides upon the proxy node, this field MUST be set to 0 and ignored upon receipt. Otherwise, this field reflects the state of the ARP table or Neighbor Cache entry associated with the probed interface. Values are (0) Reserved, (1) Incomplete, (2) Reachable, (3) Stale, (4) Delay, (5) Probe, and (6) Failed.

* Res: This field MUST be set to 0 and ignored upon receipt.

* A (Active): The A-bit is set if the Code is equal to 0, the probed interface resides on the proxy node, and the probed interface is active. Otherwise, the A-bit is clear.

* 4 (IPv4): The 4-bit is set if the A-bit is also set and IPv4 is running on the probed interface. Otherwise, the 4-bit is clear.

* 6 (IPv6): The 6-bit is set if the A-bit is also set and IPv6 is running on the probed interface. Otherwise, the 6-bit is clear.

4. ICMP Message Processing

When a node receives an ICMP Extended Echo Request message and any of the following conditions apply, the node MUST silently discard the incoming message:

* The node does not recognize ICMP Extended Echo Request messages.

* The node has not explicitly enabled ICMP Extended Echo functionality.

* The incoming ICMP Extend Echo Request carries a Source Address that is not explicitly authorized for the L-bit setting of the incoming ICMP Extended Echo Request.

* The incoming ICMP Extend Echo Request carries a Source Address that is not explicitly authorized for the incoming ICMP Extended Echo Request type (i.e., by name, by if-index, or by address).

* The Source Address of the incoming message is not a unicast address.

* The Destination Address of the incoming message is a multicast address.

Otherwise, when a node receives an ICMPv4 Extended Echo Request, it MUST format the IPv4 header of an ICMPv4 Extended Echo Reply as follows:

* TTL is 255

* Protocol is ICMP

* Indicate that the packet is not source fragmented and must not be on-path fragmented with the following values:

  - Don’t Fragment (DF) flag is 1

  - More Fragments flag is 0

  - Fragment Offset is 0

When a node receives an ICMPv6 Extended Echo Request, it MUST format the IPv6 header of an ICMPv6 Extended Echo Reply as follows:

* Hop Limit is 255

* Next Header is ICMPv6

* Indicate that the packet is not source fragmented

  - Do not include an IPv6 Fragmentation Header

In either case, the responding node MUST do the following:

* Copy the Source Address from the Extended Echo Request message to the Destination Address of the Extended Echo Reply.

* Copy the Destination Address from the Extended Echo Request message to the Source Address of the Extended Echo Reply.

* Set the DiffServ codepoint to CS0 [RFC4594].

* Set the ICMP Type to Extended Echo Reply.

* Copy the Identifier from the Extended Echo Request message to the Extended Echo Reply.

* Copy the Sequence Number from the Extended Echo Request message to the Extended Echo Reply.

* Set the Code field as described in Section 4.1.

* Set the State field to 0.

* Clear the A-bit, the 4-bit, and the 6-bit.

* If (1) the Code Field is equal to (0) No Error, (2) the L-bit is set, and (3) the probed interface is active, set the A-bit. Also, set the 4-bit and the 6-bit as appropriate.

* If the Code field is equal to (0) No Error and the L-bit is clear, then set the State field to reflect the state of the ARP table or Neighbor Cache entry that represents the probed interface.

* Copy the ICMP Extension Structure, ICMP Extension Object, and Data (if any) from the Extended Echo Request message.

* Set the Checksum appropriately.

* Forward the ICMP Extended Echo Reply to its destination. The size of the resulting packet MUST NOT exceed the outgoing interface MTU.

4.1. Code Field Processing

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

* The ICMP Extended Echo Request does not include an ICMP Extension Structure.

* The ICMP Extension Structure does not include exactly one Interface Identification Object.

* The ICMP Extension Structure checksum is 0 or incorrect.

* The L-bit is clear and the Interface Identification Object identifies the probed interface by name or if-index.

* The query is otherwise malformed.

The Code field MUST be set to (2) No Such Interface if the L-bit is set and the ICMP Extension Structure does not identify an interface that resides on the proxy node.

The Code field MUST be set to (3) No Such Table Entry if the L-bit is clear and the address found in the Interface Identification Object does not appear in the IPv4 Address Resolution Protocol (ARP) table or the IPv6 Neighbor Cache.

The Code field MUST be set to (4) Multiple Interfaces Satisfy Query if any of the following conditions apply:

* The L-bit is set and the ICMP Extension Structure identifies more than one interface that resides in the proxy node.

* The L-bit is clear and the address found in the Interface Identification Object maps to multiple IPv4 ARP or IPv6 Neighbor Cache entries.

Otherwise, the Code field MUST be set to (0) No Error.

5. Use Cases

In the scenarios listed below, network operators can use PROBE to determine the status of a probed interface but cannot use PING for the same purpose. In all scenarios, assume bidirectional connectivity between the probing and proxy interfaces. However, bidirectional connectivity between the probing and probed interfaces is lacking.

* The probed interface is unnumbered.

* The probing and probed interfaces are not directly connected to one another. The probed interface has an IPv6 link-local address but does not have a more globally scoped address.

* The probing interface runs IPv4 only while the probed interface runs IPv6 only.

* The probing interface runs IPv6 only while the probed interface runs IPv4 only.

* For lack of a route, the probing node cannot reach the probed interface.

5.1. Caveats

A limitation of PROBE is that if probing a link-local destination with the L-bit clear, and the same link-local address is used by multiple neighbors, you may get one of three code values in response:

* No Such Table Entry, if none of the neighbors are currently in the table.

* No Error, if one neighbor is currently in the table, but there is no indication as to which neighbor.

* Multiple Interfaces Satisfy Query, if more than one such neighbor is in the table.

Similarly, when identifying a local interface by link-local address (the L-bit is set), and the same link-local address is assigned to multiple interfaces, you will get a response with the code Multiple Interfaces Satisfy Query, with no indication which interface is active or able to pass traffic.

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 Extended Echo Request message and the ICMP Extended Echo Reply message to that list.

7. Change History

7.1. Changes from RFC 8335

This document updates [RFC8335] to clarify the handling of extra data beyond the ICMP Extension Structure, that data is echoed in the response packet, and checksum handling in the ICMP Extension Structure.

Specifically,

* Updated Figure 1 to reflect the presence of the ICMP Extension Object and additional data.

* Updated Section 2 to mention the ICMP Extension Structure checksum, and extra verbosity about how the Extension Structure does not cover the rest of the packet.

* Updated Figure 3 to reflect the presence of the ICMP Extension Structure and additional data.

* Added a step in Section 4 about copying data from the request to the response.

* Added a step in Section 4.1 about validating the ICMP Extension Structure checksum.

* Added section Appendix A.1 to suggest human-readable display of PROBE responses

* Clarified in Section 2.1 that the length of an ifName Object is adjusted when padding is added.

7.2. Changes from draft-fenner-intarea-probe-clarification-00

* Changed "NULL" to "NUL" when referring to the ASCII control character, per RFC20.

* Consistently refer to interface name and index using their yang names, not SNMP names.

* Added [] around the Data following the ICMP Extension Structure in Figure 1 and Figure 3 to indicate that it is optional.

7.3. Changes from draft-fenner-intarea-probe-clarification-01

* Updated the section on ICMP Extension header format to say that different ICMP Extension Option headers may be present, and if they are, the mechanism is not as specified in this memo.

7.4. Changes from draft-fenner-intarea-probe-clarification-02

* Made a stronger statement about not copying this behavior in Section 1.3

* Renamed to rfc8335bis and made WG document

7.5. Changes from draft-int-intarea-rfc8335bis-00

* Changed "For the operations in this memo" to "In the PROBE application" to better align with draft-ietf-6man-icmpv6-reflection

7.6. Changes from draft-int-intarea-rfc8335bis-01

* None

7.7. Changes from draft-int-intarea-rfc8335bis-02

* Added reference to draft-ietf-6man-icmpv6-reflection

* Updated some "RFC NNN" references to bibliography references

* Add MUST NOT exceed MTU.

* Added details of IPv4/IPv6 headers and avoidance of fragmentation to Section 4

* Added IP address and interface index considerations to Section 10

* Add new Section 9 (Manageability Considerations) immediately before Section 10, per RFC 5706 Section 4.3 guidance.

* Add to Section 10 details of Amplification risk, Covert channel potential, On-path attacker modification, ICMP header checksum scope.

* Broaden VPN isolation language to cover network instances and logical network elements.

* Clarify the wording of Section 1.3, including further wording about the checksum coverage.

8. IANA Considerations

IANA is requested to update the references for the below actions from [RFC8335] to refer to this document.

IANA has performed the following actions:

* Added the following to the "ICMP Type Numbers" registry:

  42 Extended Echo Request

  Added the following to the "Type 42 - Extended Echo Request" subregistry:

  (0) No Error

* Added the following to the "ICMPv6 ’type’ Numbers" registry:

  160 Extended Echo Request

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

  Added the following to the "Type 160 - Extended Echo Request" subregistry:

  (0) No Error

* Added the following to the "ICMP Type Numbers" registry:

  43 Extended Echo Reply

  Added the following to the "Type 43 - Extended Echo Reply" subregistry:

(0) No Error
(1) Malformed Query
(2) No Such Interface
(3) No Such Table Entry
(4) Multiple Interfaces Satisfy Query

* Added the following to the "ICMPv6 'type' Numbers" registry:

  161 Extended Echo Reply

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

  Added the following to the "Type 161 - Extended Echo Reply" subregistry:

  (0) No Error
  (1) Malformed Query
  (2) No Such Interface
  (3) No Such Table Entry
  (4) Multiple Interfaces Satisfy Query

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

  (3) Interface Identification Object

  Added the following C-types to the "Sub-types - Class 3 - Interface Identification Object" subregistry:

  (0) Reserved
  (1) Identifies Interface by Name
  (2) Identifies Interface by Index
  (3) Identifies Interface by Address

  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.

9. Manageability Considerations

This section discusses manageability aspects of PROBE. PROBE is an on-demand diagnostic tool analogous to PING. It does not run autonomously, does not maintain persistent protocol state, and does not require a formal information model or data-model definition. The subsections below address the aspects of [RFC5706] that are applicable to PROBE.

9.1. Control of Function and Policy

Nodes that support ICMP Extended Echo functionality MUST support the configuration parameters specified in Section 10. In particular, an operator MUST be able to:

* Enable or disable Extended Echo functionality on the node. By default, ICMP Extended Echo functionality is disabled.

* Define the permitted L-bit settings. By default, the option to set the L-bit is enabled and the option to clear the L-bit is disabled.

* Define the enabled query types (by name, by index, or by address). By default, all query types are disabled.

* For each enabled query type, control the source prefixes from which ICMP Extended Echo Requests are permitted.

* Control acceptance of ICMP messages on a per-interface basis.

These parameters are local to each node and take effect immediately; no protocol restart or network-wide coordination is required. An operator must explicitly enable the feature and configure authorized source prefixes before a node will respond to any Extended Echo Request.

No MIB module or YANG data model is defined for these parameters. A YANG model may be defined in a separate document in the future.

9.2. Monitoring and Verifying Operation

Correct operation of PROBE can be verified by sending an ICMP Extended Echo Request to a proxy node and examining the Code field of the ICMP Extended Echo Reply (Section 4.1). A Code of 0 (No Error) with the expected interface status confirms correct operation. Non-zero Code values indicate specific error conditions enumerated in Section 4.1.

The PROBE application described in Appendix A sends iterative queries and reports per-query results including round-trip time. This round-trip time reflects the path latency between the probing node and the proxy node, not a property of the probed interface itself.

Implementations MAY log received Extended Echo Requests at a debug level and MAY maintain counters of received, accepted, and discarded Extended Echo Requests as part of their general ICMP statistics, to assist operators in troubleshooting access-control configuration and detecting unexpected traffic.

9.3. Deployment and Backward Compatibility

PROBE is deployed on individual nodes and invoked on demand by operators or network management applications. It does not require network-wide signaling, discovery, or coordination. Operators deploying PROBE SHOULD:

* Enable Extended Echo functionality only on nodes that require diagnostic access.

* Restrict permitted source prefixes to authorized management networks.

* Apply rate-limiting to Extended Echo Requests consistent with existing ICMP rate-limiting policies.

This document obsoletes [RFC8335]. All known implementations of [RFC8335] are compatible with this document. The differences between this document and [RFC8335] are clarifications of the packet format and processing rules and not changes to on-the-wire behavior. Nodes implementing this document interoperate with nodes implementing [RFC8335] without any transition mechanism or behavioral migration.

9.4. Impact on Network Operation

Each PROBE invocation generates one ICMP Extended Echo Request and one ICMP Extended Echo Reply. Each query is independent; there is no persistent session or periodic message exchange. The processing cost on the proxy node is comparable to that of a standard ICMP Echo Request.

Frequent automated use of PROBE (e.g., by a management application polling many interfaces) could increase ICMP traffic on the network. Operators SHOULD apply rate-limiting at the responder (Section 10) consistent with their existing ICMP rate-limiting policies to bound this load.

10. Security Considerations

The following are legitimate uses of PROBE:

* to determine the operational status of an interface.

* to determine which protocols (e.g., IPv4 or IPv6) are active on an interface.

However, malicious parties can use PROBE to obtain additional information. For example, a malicious party can use PROBE to discover interface names. Having discovered an interface name, the malicious party may be able to infer additional information. Additional information may include:

* interface bandwidth

* the type of device that supports the interface (e.g., vendor identity)

* the operating system version that the above-mentioned device executes

Addresses and interface index values can also give away information that might not want to be shared. For example, a malicious party can use PROBE to determine that a given IP address is assigned to any interface on the probed node, or if interface index values are assigned densely, it can determine how many interfaces exist on the probed node.

Understanding these risks, network operators establish policies that restrict access to ICMP Extended Echo functionality. In order to enforce these policies, nodes that support ICMP Extended Echo functionality MUST support the following configuration options:

* Enable/disable ICMP Extended Echo functionality. By default, ICMP Extend Echo functionality is disabled.

* Define enabled L-bit settings. By default, the option to set the L-bit is enabled and the option to clear the L-bit is disabled.

* Define enabled query types (i.e., by name, by index, or by address); by default, all query types are disabled.

* For each enabled query type, define the prefixes from which ICMP Extended Echo Request messages are permitted.

* For each interface, determine whether ICMP Echo Request messages are accepted.

When a node receives an ICMP Extended Echo Request message that it is not configured to support, it MUST silently discard the message. See Section 4 for details.

PROBE must not leak information across network instance boundaries. Therefore, when a node receives an ICMP Extended Echo Request and the proxy interface and the probed interface are in different Virtual Private Networks (VPNs), network instances [RFC8529], or logical network elements [RFC8530], the node MUST return an ICMP Extended Echo Reply with error code equal to (2) No Such Interface.

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

PROBE does not present a significant amplification risk. The ICMP Extended Echo Reply is not meaningfully larger than the corresponding ICMP Extended Echo Request; therefore, PROBE is not a useful amplification vector.

As with any ICMP message that carries an opaque data payload, the optional data field could theoretically be used as a covert channel. The rate-limiting recommended above bounds the throughput of any such channel.

An on-path attacker can modify ICMP Extended Echo Request or Reply messages to return incorrect interface status information. This risk is shared with all ICMP messages and is not unique to PROBE. When integrity protection of PROBE messages is required, IPsec [RFC4301] SHOULD be used.

The ICMP header checksum provides integrity protection for the entire ICMP message, including any data following the ICMP Extension Structure. However, this is a non-cryptographic checksum intended for error detection, not protection against intentional modification.

11. References

11.1. 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>.

[RFC0826] Plummer, D., "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, DOI 10.17487/RFC0826, November 1982, <https://www.rfc-editor.org/rfc/rfc826>.

[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>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/rfc/rfc4861>.

[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>.

[RFC8335] Bonica, R., Thomas, R., Linkova, J., Lenart, C., and M. Boucadair, "PROBE: A Utility for Probing Interfaces", RFC 8335, DOI 10.17487/RFC8335, February 2018, <https://www.rfc-editor.org/rfc/rfc8335>.

[RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018, <https://www.rfc-editor.org/rfc/rfc8343>.

11.2. Informative References

[I-D.ietf-6man-icmpv6-reflection]
Mizrahi, T., hexiaoming, X., Zhou, T., Bonica, R. P., and X. Min, "Internet Control Message Protocol (ICMPv6) Reflection", Work in Progress, Internet-Draft, draft-ietf-6man-icmpv6-reflection-19, 15 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-icmpv6-reflection-19>.

[IANA.address-family-numbers]
IANA, "Address Family Numbers", <https://www.iana.org/assignments/address-family-numbers>.

[RFC2151] Kessler, G. and S. Shepard, "A Primer On Internet and TCP/IP Tools and Utilities", FYI 30, RFC 2151, DOI 10.17487/RFC2151, June 1997, <https://www.rfc-editor.org/rfc/rfc2151>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/rfc/rfc4301>.

[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/rfc/rfc4594>.

[RFC5706] Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", RFC 5706, DOI 10.17487/RFC5706, November 2009, <https://www.rfc-editor.org/rfc/rfc5706>.

[RFC8529] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Data Model for Network Instances", RFC 8529, DOI 10.17487/RFC8529, March 2019, <https://www.rfc-editor.org/rfc/rfc8529>.

[RFC8530] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Model for Logical Network Elements", RFC 8530, DOI 10.17487/RFC8530, March 2019, <https://www.rfc-editor.org/rfc/rfc8530>.

Appendix A. The PROBE Application

The PROBE application accepts input parameters, sets a counter, and enters a loop to be exited when the counter is equal to 0. On each iteration of the loop, PROBE emits an ICMP Extended Echo Request, decrements the counter, sets a timer, and waits. The ICMP Extended Echo Request includes an Identifier and a Sequence Number.

If an ICMP Extended Echo Reply carrying the same Identifier and Sequence Number arrives, PROBE relays information returned by that message to its user. However, on each iteration of the loop, PROBE waits for the timer to expire regardless of whether an Extended Echo Reply message arrives.

PROBE accepts the following parameters:

* Count

* Wait

* Probing Interface Address

* Hop Count

* Proxy Interface Address

* Local

* Probed Interface Identifier

Count is a positive integer whose default value is 3. Count determines the number of times that PROBE iterates through the above-mentioned loop.

Wait is a positive integer whose minimum and default values are 1. Wait determines the duration of the above-mentioned timer, measured in seconds.

Probing Interface Address specifies the Source Address of the ICMP Extended Echo Request. The Probing Interface Address MUST be a unicast address and MUST identify an interface that resides on the probing node.

The Proxy Interface Address identifies the interface to which the ICMP Extended Echo Request message is sent. It must be an IPv4 or IPv6 unicast address. If it is an IPv4 address, PROBE emits an ICMPv4 message. If it is an IPv6 address, PROBE emits an ICMPv6 message.

Local is a boolean value. It is TRUE if the proxy and probed interfaces both reside on the same node. Otherwise, it is FALSE.

The Probed Interface Identifier identifies the probed interface. It is one of the following:

* an interface name;

* an address from any address family (e.g., IPv4, IPv6, IEEE 802, 48-bit MAC, or 64-bit MAC); or

* an if-index.

If the Probed Interface Identifier is an address, it does not need to be of the same address family as the proxy interface address. For example, PROBE accepts an IPv4 Proxy Interface Address and an IPv6 Probed Interface Identifier.

A.1. Information Display

For the PING application, the primary available piece of information is the fact that we received an ICMP Echo Reply. Therefore, the appropriate information to display is all of the available information about the received reply, e.g., size, ttl, etc. However, with PROBE, the primary piece of information is the reported status of the probed interface: the code, status, A, 4, and 6 fields. It's appropriate to convert the combination of the returned values into a "human-readable" response.

For example, an application may perform these steps:

* If the code field is non-zero, print the code value as described in Section 3.

* If the code field is zero, then if the L field sent is zero, print the state value as described in Section 3.

* Otherwise, the L field sent is 1; print the state represented by the A, 4, and 6 bits. Sample textual translations for these bits are shown in Table 1.

A	4	6	Text
0	0	0	Interface inactive
1	0	0	Interface active, with no ipv4 or ipv6 running
1	0	1	Interface active, with ipv6 running
1	1	0	Interface active, with ipv4 running
1	1	1	Interface active, with ipv4 and ipv6 running

Table 1: Sample translations for bit settings

Acknowledgments

Thanks to Sowmini Varadhan, Jeff Haas, Carlos Pignataro, Jonathan Looney, Dave Thaler, Mikio Hara, Joel Halpern, Yaron Sheffer, Stefan Winter, Jean-Michel Combes, Amanda Barber, Joe Touch, Sue Hares, Xaio Min, Tony Przygienda, Nick Buraglio and Tal Mizrahi for their thoughtful review of this document.

Authors' Addresses

Bill Fenner (editor)
Arista Networks
5453 Great America Parkway
Santa Clara, California 95054
United States of America
Email: fenner@fenron.com

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia 20171
United States of America
Email: rbonica@juniper.net

Reji Thomas
Arista Networks
Global Tech Park
Bangalore 560103
Karnataka
India
Email: reji.thomas@arista.com

Jen Linkova
Google
1600 Amphitheatre Parkway
Mountain View, California 94043
United States of America
Email: furry@google.com

Chris Lenart
Verizon
22001 Loudoun County Parkway
Ashburn, Virginia 20147
United States of America

Email: chris.lenart@verizon.com

Mohamed Boucadair
Orange
Rennes 35000
France
Email: mohamed.boucadair@orange.com