Internet Engineering Task Force (IETF)
Request for Comments: 8335
Updates: 4884
Category: Standards Track
ISSN: 2070-1721

R. Bonica
R. Thomas
Juniper Networks
J. Linkova
Google
C. Lenart
Verizon
M. Boucadair
Orange

February 2018

PROBE: A Utility for Probing Interfaces

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.

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/rfc8335.

Copyright Notice

Copyright (c) 2018 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.

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 [RFC792] [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. Section 5 of this document describes scenarios in which this characteristic is useful.

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 directly connect 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 [RFC7223]. 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 [RFC826] 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.

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.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |     Code      |          Checksum             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Identifier          |Sequence Number|   Reserved  |L|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   ICMP Extension Structure
```

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 RFC 792. For ICMPv6, see RFC 4443.

- 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 identifies the probed interface.

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 ICMP Extension Structure MUST contain exactly one instance of the Interface Identification Object (see Section 2.1).

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.

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 [RFC7223]. If the Object Payload would not otherwise terminate on a 32-bit boundary, it MUST be padded with ASCII NULL characters.

If the Interface Identification Object identifies the probed interface by index, the length is equal to 8 and the payload contains the if-index [RFC7223].

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             AFI               | Address Length|   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Address   ....
```

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 <https://www.iana.org/assignments/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.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |     Code      |          Checksum             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Identifier          |Sequence Number|State|Res|A|4|6|
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 RFC 792. For ICMPv6, see RFC 4443.

- 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 ifName, by IfIndex, 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 an ICMP Extended Echo Reply as follows:

- Don’t Fragment (DF) flag is 1

- More Fragments flag is 0

- Fragment Offset is 0

- TTL is 255

- Protocol is ICMP

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

- Hop Limit is 255
- Next Header is ICMPv6

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.
- Set the Checksum appropriately.
- Forward the ICMP Extended Echo Reply to its destination.

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 L-bit is clear and the Interface Identification Object identifies the probed interface by ifName or ifIndex.
- 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.

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. IANA Considerations

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.

8. 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

Understanding this risk, 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 about one Virtual Private Network (VPN) into another. Therefore, when a node receives an ICMP Extended Echo Request and the proxy interface is in a different VPN than the probed interface, 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.

9. References

9.1. Normative References

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

[RFC826] Plummer, D., "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/info/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/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>.

[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/info/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/info/rfc4884>.

[RFC7223] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014, <https://www.rfc-editor.org/info/rfc7223>.

[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>.

9.2. Informative References

[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/info/rfc2151>.

[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>.

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.

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, and Joe Touch for their thoughtful review of this document.

Authors' Addresses

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia 20171
United States of America

Email: rbonica@juniper.net

Reji Thomas
Juniper Networks
Elnath-Exora Business Park Survey
Bangalore, Karnataka 560103
India

Email: rejithomas@juniper.net

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