An Acceptable Use Policy for New ICMP Types and Codes

Abstract

   In this document we provide a basic description of ICMP's role in the
   IP stack and some guidelines for future use.

   This document is motivated by concerns about lack of clarity
   concerning when to add new Internet Control Message Protocol (ICMP)
   types and/or codes. These concerns have highlighted a need to
   describe policies for when adding new features to ICMP is desirable
   and when it is not.

Status of This Memo

   This memo documents an Internet Best Current Practice.

   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
   BCPs is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7279.

Table of Contents

1. Introduction

   There has been some recent concern expressed about a lack of clarity
   around when new message types and codes should be added to ICMP
   (including ICMPv4 [RFC0792] and ICMPv6 [RFC4443]). We lay out a
   policy regarding when (and when not) to move functionality into ICMP.

   This document is the result of discussions among ICMP experts within
   the Operations and Management (OPS) area's IP Diagnostics Technical
   Interest Group [DIAGNOSTICS] and concerns expressed by the OPS area
   leadership.

   Note that this document does not supercede the "IANA Allocation
   Guidelines For Values In the Internet Protocol and Related Headers"
   [RFC2780], which specifies best practices and processes for the
   allocation of values in the IANA registries but does not describe the
   policies to be applied in the standards process.

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in [RFC2119].

2. Acceptable Use Policy

   In this document, we describe an acceptable use policy for new ICMP
   message types and codes, and provide some background about the
   policy.

In summary, any future message types added to ICMP should be limited
to two broad categories:

1. to inform a datagram's originator that a forwarding plane anomaly
    has been encountered downstream. The datagram originator must be
    able to determine whether or not the datagram was discarded by
    examining the ICMP message.

2. to discover and convey dynamic information about a node (other
    than information usually carried in routing protocols), to
    discover and convey network-specific parameters, and to discover
    on-link routers and hosts.

Normally, ICMP SHOULD NOT be used to implement a general-purpose
routing or network management protocol. However, ICMP does have a
role to play in conveying dynamic information about a network, which
would belong in category 2 above.

2.1. Classification of Existing Message Types

This section provides a rough breakdown of existing message types
according to the taxonomy described in Section 2 at the time of
publication.

IPv4 forwarding plane anomaly reporting:

    3:    Destination Unreachable

    4:    Source Quench (Deprecated)

    6:    Alternate Host Address (Deprecated)

    11:   Time Exceeded

    12:   Parameter Problem

    31:   Datagram Conversion Error (Deprecated)

IPv4 router or host discovery:

    0:    Echo Reply

    5:    Redirect

    8:    Echo

    9:    Router Advertisement

   10: Router Solicitation

   13: Timestamp

   14: Timestamp Reply

   15: Information Request (Deprecated)

   16: Information Reply (Deprecated)

   17: Address Mask Request (Deprecated)

   18: Address Mask Reply (Deprecated)

   30: Traceroute (Deprecated)

   32: Mobile Host Redirect (Deprecated)

   33: IPv6 Where-Are-You (Deprecated)

   34: IPv6 I-Am-Here (Deprecated)

   35: Mobile Registration Request (Deprecated)

   36: Mobile Registration Reply (Deprecated)

   37: Domain Name Request (Deprecated)

   38: Domain Name Reply (Deprecated)

   39: SKIP (Deprecated)

   40: Photuris

   41: ICMP messages utilized by experimental mobility protocols
        such as Seamoby

   Please note that some ICMP message types were formally deprecated by
   [RFC6918].

   IPv6 forwarding plane anomaly reporting:

   1: Destination Unreachable

   2: Packet Too Big

   3:   Time Exceeded

   4:   Parameter Problem

   150: ICMP messages utilized by experimental mobility protocols
        such as Seamoby

   IPv6 router or host discovery:

   128: Echo Request

   129: Echo Reply

   130: Multicast Listener Query

   131: Multicast Listener Report

   132: Multicast Listener Done

   133: Router Solicitation

   134: Router Advertisement

   135: Neighbor Solicitation

   136: Neighbor Advertisement

   137: Redirect Message

   138: Router Renumbering

   139: ICMP Node Information Query

   140: ICMP Node Information Response

   141: Inverse Neighbor Discovery Solicitation Message

   142: Inverse Neighbor Discovery Advertisement Message

   143: Version 2 Multicast Listener Report

   144: Home Agent Address Discovery Request Message

   145: Home Agent Address Discovery Reply Message

   146: Mobile Prefix Solicitation

        147: Mobile Prefix Advertisement

        148: Certification Path Solicitation Message

        149: Certification Path Advertisement Message

        150: ICMP messages utilized by experimental mobility protocols
             such as Seamoby

        151: Multicast Router Advertisement

        152: Multicast Router Solicitation

        153: Multicast Router Termination

        154: FMIPv6 Messages

        155: RPL Control Message

2.1.1. ICMP Use as a Routing Protocol

   As mentioned in Section 2, using ICMP as a general-purpose routing or
   network management protocol is not advisable and SHOULD NOT be used
   that way.

   ICMP has a role in the Internet as an integral part of the IP layer;
   it is not as a routing protocol or as a transport protocol for other
   layers including routing information. From a more pragmatic
   perspective, some of the key characteristics of ICMP make it a less-
   than-ideal choice for a routing protocol. These key characteristics
   include that ICMP is frequently filtered, is not authenticated, and
   is easily spoofed. In addition, specialist hardware processing of
   ICMP would disrupt the deployment of an ICMP-based routing or
   management protocol.

2.1.2. A Few Notes on RPL

   RPL, the IPv6 routing protocol for low-power and lossy networks (see
   [RFC6550]) uses ICMP as a transport. In this regard, it is an
   exception among the ICMP message types. Note that, although RPL is
   an IP routing protocol, it is not deployed on the general Internet;
   it is limited to specific, contained networks.

   This should be considered anomalous and is not a model for future
   ICMP message types. That is, ICMP is not intended as a transport for
   other protocols and SHOULD NOT be used in that way in future
   specifications. In particular, while it is adequate to use ICMP as a
   discovery protocol, it does not extend to full routing capabilities.

2.2. Applications Using ICMP

   Some applications make use of ICMP error notifications, or even
   deliberately create anomalous conditions in order to elicit ICMP
   messages. These ICMP messages are then used to generate feedback to
   the higher layer. Some of these applications include some of the
   most widespread examples, such as PING, TRACEROUTE, and Path MTU
   Discovery (PMTUD). These uses are considered acceptable because they
   use existing ICMP message types and do not change ICMP functionality.

2.3. Extending ICMP

   ICMP multi-part messages are specified in [RFC4884] by defining an
   extension mechanism for selected ICMP messages. This mechanism
   addresses a fundamental problem in ICMP extensibility. An ICMP
   multi-part message carries all of the information that ICMP messages
   carried previously, as well as additional information that
   applications may require.

   Some currently defined ICMP extensions include ICMP extensions for
   Multiprotocol Label Switching [RFC4950] and ICMP extensions for
   interface and next-hop identification [RFC5837].

   Extensions to ICMP SHOULD follow the requirements provided in
   [RFC4884].

2.4. ICMPv4 vs. ICMPv6

   Because ICMPv6 is used for IPv6 Neighbor Discovery, deployed IPv6
   routers, IPv6-capable security gateways, and IPv6-capable firewalls
   normally support administrator configuration of how specific ICMPv6
   message types are handled. By contrast, deployed IPv4 routers,
   IPv4-capable security gateways, and IPv4-capable firewalls are less
   likely to allow an administrator to configure how specific ICMPv4
   message types are handled. So, at present, ICMPv6 messages usually
   have a higher probability of travelling end-to-end than ICMPv4
   messages.

3. ICMP's Role in the Internet

   ICMP was originally intended to be a mechanism for gateways or
   destination hosts to report error conditions back to source hosts in
   ICMPv4 [RFC0792]; ICMPv6 [RFC4443] is modeled after it. ICMP is also
   used to perform IP-layer functions, such as diagnostics (e.g., PING).

   ICMP is defined to be an integral part of IP and must be implemented
   by every IP module. This is true for ICMPv4 as an integral part of
   IPv4 (see the Introduction of [RFC0792]), and for ICMPv6 as an

integral part of IPv6 (see Section 2 of [RFC4443]). When first
defined, ICMP messages were thought of as IP messages that didn't
carry any higher-layer data. It could be conjectured that the term
"control" was used because ICMP messages were not "data" messages.

The word "control" in the protocol name did not describe ICMP's
function (i.e., it did not "control" the Internet); rather, it was
used to communicate about the control functions in the Internet. For
example, even though ICMP included a redirect message type that
affects routing behavior in the context of a LAN segment, it was not
and is not used as a generic routing protocol.

4. Security Considerations

This document describes a high-level policy for adding ICMP types and
codes. While special attention must be paid to the security
implications of any particular new ICMP type or code, this
recommendation presents no new security considerations.

From a security perspective, ICMP plays a part in the Photuris
protocol [RFC2521]. But more generally, ICMP is not a secure
protocol and does not include features to be used to discover network
security parameters or to report on network security anomalies in the
forwarding plane.

Additionally, new ICMP functionality (e.g., ICMP extensions, or new
ICMP types or codes) needs to consider potential ways that ICMP can
be abused (e.g., Smurf IP DoS [CA-1998-01]).

5. Acknowledgments

This document was originally proposed by, and received substantial
review and suggestions from, Ron Bonica. Discussions with Pascal
Thubert helped clarify the history of RPL's use of ICMP. We are very
grateful for the review, feedback, and comments from Ran Atkinson,
Tim Chown, Joe Clarke, Adrian Farrel, Ray Hunter, Hilarie Orman, Eric
Rosen, JINMEI Tatuya, and Wen Zhang, which resulted in a much
improved document.

6. References

6.1. Normative references

   [RFC0792]   Postel, J., "Internet Control Message Protocol", STD 5,
               RFC 792, September 1981.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control
              Message Protocol (ICMPv6) for the Internet Protocol
              Version 6 (IPv6) Specification", RFC 4443, March 2006.

   [RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro,
              "Extended ICMP to Support Multi-Part Messages", RFC 4884,
              April 2007.

6.2. Informative references

   [CA-1998-01]
              CERT, "Smurf IP Denial-of-Service Attacks", CERT Advisory
              CA-1998-01, January 1998,
              <http://www.cert.org/advisories/CA-1998-01.html>.

   [DIAGNOSTICS]
              "IP Diagnostics Technical Interest Group", ,
              <https://svn.tools.ietf.org/area/ops/trac/wiki/
              TIG_DIAGNOSTICS>.

   [RFC2521] Karn, P. and W. Simpson, "ICMP Security Failures
              Messages", RFC 2521, March 1999.

   [RFC2780] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For
              Values In the Internet Protocol and Related Headers", BCP
              37, RFC 2780, March 2000.

   [RFC4950] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "ICMP
              Extensions for Multiprotocol Label Switching", RFC 4950,
              August 2007.

   [RFC5837] Atlas, A., Bonica, R., Pignataro, C., Shen, N., and JR.
              Rivers, "Extending ICMP for Interface and Next-Hop
              Identification", RFC 5837, April 2010.

   [RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R.,
              Levis, P., Pister, K., Struik, R., Vasseur, JP., and R.
              Alexander, "RPL: IPv6 Routing Protocol for Low-Power and
              Lossy Networks", RFC 6550, March 2012.

   [RFC6918] Gont, F. and C. Pignataro, "Formally Deprecating Some
              ICMPv4 Message Types", RFC 6918, April 2013.

Authors' Addresses

    Melinda Shore
    No Mountain Software
    PO Box 16271
    Two Rivers, AK 99716
    US

    Phone: +1 907 322 9522
    EMail: melinda.shore@nomountain.net

    Carlos Pignataro
    Cisco Systems, Inc.
    7200-12 Kit Creek Road
    Research Triangle Park, NC 27709
    US

    EMail: cpignata@cisco.com