              An Acceptable Use Policy for New ICMP Types and Codes
                         draft-shore-icmp-aup-01

Abstract

   Some recent proposals to add new Internet Control Message Protocol
   (ICMP) types and/or codes have highlighted a need to describe
   policies for when adding new features to ICMP is desirable and when
   it is not. In this document we provide a basic description of ICMP's
   role in the IP stack and some guidelines for the future.

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 http://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 January 14, 2013.

Copyright Notice

   described in the Simplified BSD License.

Table of Contents

1. Introduction

There have been some recent proposals to add new message types and codes to ICMP [RFC792]. Not all of these proposal are consistent with the design and intent of ICMP, and so we attempt to lay out a description of when (and when not) to move functionality into ICMP.

This document is the result of discussions within the IETF Operations area "ICMP Society," and concerns expressed by the OPS area leadership.

2. Acceptable use policy

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

In summary, we propose that 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 on-link routers and hosts

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.

IPV4 forwarding plane anomaly reporting

3:    Destination unreachable

4:    Source quench (deprecated)

5:    Redirect

6:    Alternate host address

11   Time exceeded

12   Parameter problem

31:   Datagram converson error

32:   Mobile host redirect

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

IPv4 router or host discovery

0:    Echo reply

8:    Echo

9:    Router advertisement

10:    Router solicitation

13:    Timestamp

14:    Timestamp reply

15:    Information request

16:    Information reply

17:    Address mask request

18:    Address mask reply

30:    Traceroute

33:    IPv6 Where-Are-You

34:    IPv6 I-Am-Here

35:    Mobile registration request

36:    Mobile registration reply

37:    Domain name request

38:    Domain name reply

39:    SKIP

40:    Photuris

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

IPv6 forwarding plane anomaly reporting

1:    Destination unreachable

2:    Packet too big

3:    Time exceeded

4:    Parameter problem

137:   Redirect message

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

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

3. **ICMP's role in the internet**

   ICMP was originally intended to be a mechanism for routers to report
   error conditions back to hosts [RFC792]. The word "control" in the
   protocol name did not describe ICMP's function (i.e. it did not
   "control" the internet), but rather that it was used to communicate
   about the control functions in the internet. For example, even
   though ICMP included a redirect message type, it was and is not used
   as a routing protocol.

   Most likely because of the presence of the word "control" in the
   protocol name, ICMP is often understood to be a control protocol,
   borrowing some terminology from circuit networks and the PSTN. That
   is probably not correct - it might be more correct to describe it as
   being closer to a management plane protocol, given the data plane/
   control plane/ management plane taxonomy often used in describing
   telephony protocols. However, layering in IP networks is not very
   clean and there's often some intermingling of function that can tend
   to lead to confusion about where to place new functions.

   In following sections we provide some background on the differences
   between control and management traffic.

4. **Management vs control**

   In this section we attempt to draw a distinction between management
   and control planes, acknowledging in advance that this may serve to
   muddle the differences even further. Ultimately the difference may
   not matter that much for the purpose of creating a policy for adding
   new types to ICMP, but because that terminology has become
   ubiquitous, even in IETF discussions, and because it has come up in
   prior discussions of ICMP policies, it seems worthwhile to take a few
   paragraph to describe what they are and what they are not.

   The terms "management plane" and "control plane" came into use to
   describe one aspect of layering in telecommunications networks. It
   is particularly important, in the context of this discussion, to
   understand that "control plane" in telecomm networks almost always
   refers to 'signaling,' or call control and network control
   information. This includes "call" establishment and teardown, route
   establishment and teardown, requesting QoS or other parameters, and
   so on.

   "Management," on the other hand, tends to fall under the rubric
   "OAM," or "Operations, Administration, and Management." typical
   functions include fault management and performance monitoring
   (Service Level Agreement [SLA] compliance), discovery, etc.

   The correct answer to the question of where ICMP fits into the
   management/control/data taxonomy is that it doesn't, at least not
   neatly. While some of the message types are unambiguously management
   message (ICMP type 3, or "unreachable" messages), others are less
   clearly identifiable. For example, the "redirect" (ICMP type 5)
   message can be construed to contain control (in this case, routing)
   information, even though it is in some very real sense an error
   message.

   At this time,

   o   there are many, many other protocols that can be (and are) used
       for control traffic, whether they're routing protocols, telephony
       signaling protocols, QoS protocols, middlebox protocols, AAA
       protocols, etc.

   o   the transport characteristics needed by control traffic can be
       incompatible with the ICMP protocol standard -- for example, they
       may require reliable delivery, very large payloads, or have
       security requirements that cannot be met.

   and because of this we propose that any future message types added to
   ICMP must conform to the policy proposed in Section 2. ICMP should

   not be used as a routing or network management protocol.

5. Security considerations

   This document attempts to describe 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,
   specific security considerations are outside the scope of this paper.

6. IANA considerations

   There are no actions required by IANA.

7. Acknowledgments

   This document was originally proposed by, and received substantial
   review and suggestions from, Ron Bonica.

8. Informative references

[RFC792]   Postel, J., "INTERNET CONTROL MESSAGE PROTOCOL", RFC 792,
            September 1981.

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@cisc.com