Network Working Group
Internet Draft

Steven M. Bellovin
AT&T Labs Research

Expiration Date: August 2002

December 2001

A "Reason" Field for ICMP "Administratively Prohibited" Messages

draft-bellovin-adminprohib-00.txt

1. Status of this Memo

2. Abstract

The current ICMP "Administratively Prohibited" message conveys one bit of information: we don't like your packet. This memo proposes adding additional information to help hosts retry other possible packets.

3. Introduction

The current ICMP "Administratively Prohibited" message conveys one bit of information: we don't like your packet. Sometimes, more is needed. For example, attempts to deploy systems that use the ECN bit [RFC3168] have run into trouble with some firewalls. Unfortunately, all the firewalls can do is silently drop the packet, send a TCP Reset packet (which is, arguably, in violation of [RFC793], or send an ICMP "Administratively Denied" message [RFC1716]. But that gives the sender too little information on what the cause of the failure was, and hence no indication on how to recover.

4. An Unused Field

The ICMP Destination Unreachable message [RFC792] has a field that is unused except in the case of Path MTU Discovery messages [RFC1191]. We suggest that this field (bytes 5-8 of the ICMP header) be used to signal which fields of the original packet caused it to be rejected. Each byte is a byte offset from the start of the IP header to an

offending field. A value of zero ends the field, since we believe that byte 0 of the IP header is unlikely to cause offense beyond what would be noted by a Parameter Problem message.

Since the field is currently defined as "unused", it is possible that it contains random garbage. Accordingly, receivers MUST ignore any such fields if any of them reach beyond the IP and next-layer headers.

Senders SHOULD fill in as many fields as they can identify as causing problems. For example, if a packet were rejected because of an access control list that matched on source host, destination host, and destination port, the field would contain bytes of 12 (the source address offset), 16 (destination address), and 22 (destination port), as well as a 0 pad byte.

5. IP Version 6

This draft only applies to ICMP for IPv4. A later version may describe the corresponding IPv6 message.

6. Security Considerations

Many security boxes prefer to give as little information as possible. They are welcome to leave the field at 0, if they wish.

7. References

[RFC793] "Transmission Control Protocol". J. Postel. September 1981.

[RFC792] "Internet Control Message Protocol". J. Postel. September 1981.

[RFC1191] "Path MTU discovery". J.C. Mogul and S.E. Deering. November 1990.

[RFC1716] "Towards Requirements for IP Routers". P. Almquist and F. Kastenholz. November 1994.

[RFC3168] "The Addition of Explicit Congestion Notification (ECN) to IP". K. Ramakrishnan, S. Floyd, and D. Black. September 2001

8. Author Information

Steven M. Bellovin
AT&T Labs Research
Shannon Laboratory
180 Park Avenue
Florham Park, NJ 07932
Phone: +1 973-360-8656
email: bellovin@acm.org