Transable Area Working Group   F. Gont
(tsvwg)   UTN/FRH
Internet-Draft   January 27, 2011
Updates: 792, 1122, 1812
(if approved)
Intended status: Standards Track
Expires: July 31, 2011

                 Deprecation of ICMP Source Quench messages
                   draft-ietf-tsvwg-source-quench-00.txt

Abstract

   This document formally deprecates the use of ICMP Source Quench
   messages by transport protocols, formally updating RFC 792, RFC 1122,
   and RFC 1812. Additionally, it requests that the status of RFC 1016
   be changed to "Historic".

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The ICMP specification [RFC0792] defined the ICMPv4 Source Quench
message (type 4, code 0), which was meant as a mechanism for
congestion control. ICMP Source Quench has been known to be an
ineffective (and unfair) antidote for congestion, and generation of
ICMP Source Quench messages by routers has been formally deprecated
by [RFC1812] since 1995. However, reaction to ICMP Source Quench
messages in transport protocols has never been formally deprecated.

This document formally deprecates reaction to ICMP Source Quench
messages by transport protocols such as TCP, formally updating
[RFC0792], [RFC1122], and [RFC1812]. Additionally, it requests that
the status of [RFC1016] be changed to "Historic".

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 RFC 2119 [RFC2119].

2. ICMP Source Quench messages

The ICMP specification [RFC0792] defined the ICMP Source Quench
message (type 4, code 0), which was meant to provide a mechanism for
congestion control. The Host Requirements RFC [RFC1122] stated in
Section 4.2.3.9 that hosts MUST react to ICMP Source Quench messages
by slowing transmission on the connection, and further added that the
RECOMMENDED procedure was to put the corresponding connection in the
slow-start phase of TCP's congestion control algorithm [RFC5681].

[RFC1812] noted that research suggested that ICMP Source Quench was
an ineffective (and unfair) antidote for congestion, and formally
deprecated the generation of ICMP Source Quench messages by routers,
stating that routers SHOULD NOT send ICMP Source Quench messages in
response to congestion.

[RFC5927] discussed the use of ICMP Source Quench messages for
performing "blind throughput-reduction" attacks, and noted that most
TCP implementations silently ignore ICMP Source Quench messages.

We note that TCP implements its own congestion control mechanisms
[RFC5681] [RFC3168], that do not depend on ICMP Source Quench
messages.

It is interesting to note that ICMPv6 [RFC4443] does not specify a
"Source Quench" message.

3. Updating RFC 1122

This document hereby updates Section 3.2.2.3 of [RFC1122] as follows:

A host SHOULD NOT send ICMP Source Quench messages.

If a Source Quench message is received, the IP layer MAY silently
discard it.

Section 4.2.3.9 of [RFC1122] is updated as follows:

TCP SHOULD silently discard any received ICMP Source Quench
messages.

4. Updating RFC 1812

This document hereby updates Section 4.3.3.3 of [RFC1812] as follows:

A router SHOULD ignore any ICMP Source Quench messages it
receives.

5. General Advice to Transport Protocols

If a Source Quench message is received by a transport-protocol
instance (e.g., a TCP connection), it SHOULD be silently ignored.

6. Changing the status of RFC 1016 Historic

This document requests the RFC Editor to change the status of
[RFC1016] to "Historic".

7. Security Considerations

ICMP Source Quench messages could be leveraged for performing blind
throughput-reduction attacks against TCP and similar protocols. This
attack vector, along with possible countermeasures, have been
discussed in great detail in [RFC5927] and [CPNI-TCP]. However, as
noted in [RFC5927] and [CPNI-TCP], virtually all current versions of
popular TCP implementations already silently ignore ICMP Source
Quench messages.

Silently ignoring ICMP Source Quench messages, as specified in this document, eliminates the aforementioned attack vector.

If deemed necessary, ICMP Source Quench messages could be filtered at firewalls.

8. IANA Considerations

This document has no actions for IANA. The RFC-Editor can remove this section before publication of this document as an RFC.

9. Acknowledgements

The author of this document would like to thank (in alphabetical order) Fred Baker, David Black, Scott Bradner, James Carlson, Antonio De Simone, Gorry Fairhurst, Alfred Hoenes, Mahesh Jethanandani, Dan Wing, and Andrew Yourtchenko, for providing valuable feedback on earlier versions of this document.

This document has benefited from discussions within the TCPM Working Group while working on [RFC5927].

10. References

10.1. Normative References

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

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7,
           RFC 793, September 1981.

[RFC1016] Prue, W. and J. Postel, "Something a host could do with
           source quench: The Source Quench Introduced Delay
           (SQuID)", RFC 1016, July 1987.

[RFC1122] Braden, R., "Requirements for Internet Hosts -
           Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers",
           RFC 1812, June 1995.

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

   [RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition
              of Explicit Congestion Notification (ECN) to IP",
              RFC 3168, September 2001.

   [RFC5681] Allman, M., Paxson, V., and E. Blanton, "TCP Congestion
              Control", RFC 5681, September 2009.

10.2. Informative References

   [CPNI-TCP]
              CPNI, "Security Assessment of the Transmission Control
              Protocol (TCP)", 2009, <http://www.cpni.gov.uk/Docs/
              tn-03-09-security-assessment-TCP.pdf>.

   [FreeBSD] The FreeBSD Project, "http://www.freebsd.org".

   [Linux]   The Linux Project, "http://www.kernel.org".

   [NetBSD]   The NetBSD Project, "http://www.netbsd.org".

   [OpenBSD] The OpenBSD Project, "http://www.openbsd.org".

   [OpenSolaris]
              OpenSolaris, "http://www.opensolaris.org".

   [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.

   [RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927, July 2010.

Appendix A. Survey of support of ICMP Source Quench in some popular TCP/IP implementations

   A large number of implementations completely ignore ICMP Source
   Quench messages meant for TCP connections. This behavior has been
   implemented in, at least, Linux [Linux] since 2004, and in FreeBSD
   [FreeBSD], NetBSD [NetBSD], OpenBSD [OpenBSD], and Solaris 10 since
   2005. Additionally, OpenSolaris [OpenSolaris] has always shipped
   with support for ICMP Source Quench messages disabled.

Appendix B. Changes from previous versions of the draft (to be removed by the RFC Editor before publishing this document as an RFC)

B.1. **Changes from draft-gont-tsvwg-source-quench-01**

   o Addresses nits and editorial chagnes suggested by Gorry Fairhurst.

   o Added the status of Solaris and OpenSolaris to Appendix A.

   o Document resubmitted as draft-ietf.

B.2. **Changes from draft-gont-tsvwg-source-quench-00**

   o This revision reflects the recent discussion about ICMP Source
      Quench messages on the tsvwg mailing-list. A detailed list of the
      changes is available at:
      http://www.ietf.org/mail-archive/web/tsvwg/current/msg10407.html

Author's Address

   Fernando Gont
   Universidad Tecnologica Nacional / Facultad Regional Haedo
   Evaristo Carriego 2644
   Haedo, Provincia de Buenos Aires 1706
   Argentina

   Phone: +54 11 4650 8472
   Email: fernando@gont.com.ar
   URI: http://www.gont.com.ar