Internet Engineering Task Force (IETF)
Request for Comments: 6633
Updates: 792, 1122, 1812
Category: Standards Track
ISSN: 2070-1721

F. Gont
UTN-FRH / SI6 Networks

May 2012

Deprecation of ICMP Source Quench Messages

Abstract

This document formally deprecates the use of ICMP Source Quench messages by transport protocols, formally updating RFC 792, RFC 1122, and RFC 1812.

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 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/rfc6633.

Table of Contents

1. Introduction

The ICMP specification [RFC0792] defined the ICMP 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 [RFC0793], formally updating [RFC0792], [RFC1122], and [RFC1812]. Additionally, it provides a recommendation against the implementation of [RFC1016]. The rationale for these specification updates is as follows:

- Processing of ICMP Source Quench messages by routers has been deprecated for nearly 17 years [RFC1812].

- Virtually all popular host implementations have removed support for ICMP Source Quench messages since (at least) 2005 [RFC5927].

- Widespread deployment of ICMP filtering makes it impossible to rely on ICMP Source Quench messages for congestion control.

- The IETF has moved away from ICMP Source Quench messages for congestion control (e.g., note the development of Explicit Congestion Notification (ECN) [RFC3168] and the fact that ICMPv6 [RFC4443] does not even specify a Source Quench message).

> ICMP Source Quench messages are not normally seen in the deployed Internet and were considered rare at least as far back as 1994 [Floyd1994].

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. 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], which 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 MUST 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 MUST silently discard any received ICMP Source Quench messages.

The consensus of the TSV WG was that there are no valid reasons for a host to generate or react to an ICMP Source Quench message in the current Internet. The recommendation that a sender "MUST NOT" send an ICMP Source Quench message is because there is no known valid reason for a host to generate this message. The only known impact of a sender ignoring this requirement is that it may necessarily consume network and endpoint resources. Discarding ICMP Source Quench messages at the Internet layer (rather than at the transport layer) is a performance optimization that is permitted by this update.

4. Updating RFC 1812

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

> A router MUST ignore any ICMP Source Quench messages it receives.

The consensus of the TSV WG was that there are no valid reasons for a router to react to ICMP Source Quench messages in the current Internet.

5. Clarification for UDP, SCTP, and DCCP

UDP [RFC0768] did not explicitly specify support for ICMP Source Quench messages. Hereby, we clarify that UDP endpoints MUST silently discard received ICMP Source Quench messages.

It is understood that SCTP [RFC4960] and DCCP [RFC4340] did not specify support for processing received ICMP Source Quench messages. Hereby, we clarify that DCCP and SCTP endpoints MUST silently discard received ICMP Source Quench messages.

6. General Advice to Transport Protocols

If a Source Quench message is received by any other transport-protocol instance, it MUST be silently ignored.

The TSV WG is not aware of any mechanism that requires processing of these messages and therefore expects other transports to follow the recommendations in Section 3. Note that since generation of ICMP Source Quench messages has been deprecated for many years, and since this document additionally deprecates reaction to ICMP Source Quench messages by IETF-specified transports, future applications cannot expect to receive these messages.

7. Recommendation Regarding RFC 1016

[RFC1016] describes an experimental approach to the handling of ICMP Source Quench messages in hosts that was considered in 1987. Even though RFC 1016 has never been on the IETF Standards Track, for clarity and avoidance of doubt we note that the approach described in [RFC1016] MUST NOT be implemented.

8. 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, has been discussed in great detail in [RFC5927] and [CPNI-TCP]. Silently ignoring ICMP Source Quench messages, as specified in this document, eliminates the aforementioned attack vector.

For current TCP implementations, receipt of an ICMP Source Quench message should not result in security issues because, as noted in [RFC5927] and [CPNI-TCP], virtually all current versions of popular TCP implementations already silently ignore ICMP Source Quench messages. This is also the case for SCTP and DCCP implementations.

Hosts, security gateways, and firewalls MUST silently discard received ICMP Source Quench packets and SHOULD log such drops as a security fault with at least minimal details (IP Source Address, IP Destination Address, ICMP message type, and date/time the packet was seen).

> We note that security devices such as the Snort Network Intrusion Detection System (NIDS) have logged ICMP Source Quench messages as such for more than ten years [Anderson2002].

9. IANA Considerations

IANA has marked ICMP type 4 (Source Quench) as "Deprecated" in the ICMP Parameters registry [ICMPPARREG] with a reference to this document.

10. Acknowledgements

The author of this document would like to thank Ran Atkinson, who contributed text that was incorporated into this document and also provided valuable feedback on earlier versions of this document.

The author of this document would like to thank (in alphabetical order) Fred Baker, David Black, Scott Bradner, James Carlson, Antonio De Simone, Wesley Eddy, Gorry Fairhurst, Alfred Hoenes, Mahesh

Jethanandani, Kathleen Moriarty, Carlos Pignataro, James Polk, Anantha Ramaiah, Randall Stewart, Dan Wing, and Andrew Yourtchenko, for providing valuable feedback on earlier versions of this document. This document has also benefited from discussions within the TCPM Working Group while working on [RFC5927].

Fernando Gont wishes to thank Jorge Oscar Gont, Nelida Garcia, and Guillermo Gont for their love and support.

Fernando Gont's attendance to IETF meetings was supported by ISOC's "Fellowship to the IETF" program.

11. References

11.1. Normative References

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[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.

[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.

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, March 2006.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

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

11.2. Informative References

[Anderson2002] Anderson, D., Fong, M., and A. Valdes, "Heterogeneous Sensor Correlation: A Case Study of Live Traffic Analysis", Proceedings of the 3rd Annual IEEE Information Assurance Workshop New York, NY, USA, 2002.

[CPNI-TCP] CPNI, "Security Assessment of the Transmission Control Protocol (TCP)", 2009, <http://www.gont.com.ar/papers/tn-03-09-security-assessment-TCP.pdf>.

[Floyd1994] Floyd, S., "TCP and Explicit Congestion Notification", ACM CCR New York, NY, Volume 24, Issue 5, October 1994.

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

[ICMPPARREG] IANA, "Internet Control Message Protocol (ICMP) Parameters", <http://www.iana.org/assignments/icmp-parameters>.

[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>.

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

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

[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.

Author's Address

Fernando Gont
UTN-FRH / SI6 Networks
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
EMail: fgont@si6networks.com
URI: http://www.si6networks.com