Internet Engineering Task Force
INTERNET-DRAFT
draft-floyd-tsvwg-ecn-nonce-00a.ps
Expires: May 2007

S. Floyd
ICIR

26 November 2006

Why RFC 3540 on the ECN Nonce Should Progress to Proposed Standard

Abstract

The Proposed Standard document RFC 3168, "The Addition of Explicit Congestion Notification (ECN) to IP", defines the semantics of all four codepoints in the ECN Field in the IP header. Section 11.2 of [RFC3168] says that "the use of two ECT codepoints, ECT(0) and ECT(1), can provide a one-bit ECN nonce in packet headers [SCWA99]." The use of the ECN nonce for DCCP is specified in the Proposed Standard documents RFC 4340, RFC 4341, and RFC 4342. The use of the ECN nonce for TCP is specified in RFC 3540, which has been Experimental since June 2003 [RFC3540].

Recent documents [BJSK06] have proposed that RFC 3540 remain at Experimental, instead of advancing to Proposed Standard, This document argues that the RFC 3540 should advance to Proposed Standard, and contends that the ECN Nonce is a valuable addition to the Internet architecture.

1. Introduction

RFC 3168 defined the semantics of the four codepoints in the ECN field in the IP header, providing for a one-bit ECN nonce. RFC 3540 specifies how this ECN nonce could be used by TCP end-nodes to allow the sender to protect against receivers lying about whether data packets were dropped or ECN-marked. However, the ECN nonce itself does not offer protection against transport-level senders that do not respond to reported congestion events.

[BJSK06] specifies a proposal for alternate semantics for the ECN field in the IP header, called re-ECN. [BJSK06] states that "the most immediate priority for the authors is to delay any move of the ECN nonce to Proposed Standard status", where "the ECN nonce" refers to RFC 3540. The argument for this position is given in Appendix I of RFC 3540.

On paths where re-ECN is successfully deployed at some pair of ingress and egress routers, re-ECN is intended to allow the re-ECN routers to protect against either sending or receiving end-nodes not responding properly to ECN-marked packets marked between the ingress and egress re-ECN routers.

Re-ECN would not be able to offer protection on paths where re-ECN was not used by a pair of ingress and egress re-ECN routers. Re-ECN would also not be able to offer protection against end-nodes not responding to packets ECN-marked between the transport sender and the ingress re-ECN router, or to packets ECN-marked between the egress re-ECN router and the transport receiver.

In addition, re-ECN would not be able to protect against end-nodes not responding

properly to packets dropped on a path, regardless of whether the packets were dropped between the ingress and egress re-ECN routers, or whether the packets were dropped elsewhere on the end-to-end path. It would be possible to specify a transport-level mechanism that used a transport-level nonce (e.g., in the TCP, SCTP, and/or DCCP packet headers) to allow senders to protect against receivers lying about whether packets were dropped in the network, but such a mechanism would have to be designed and standardized.

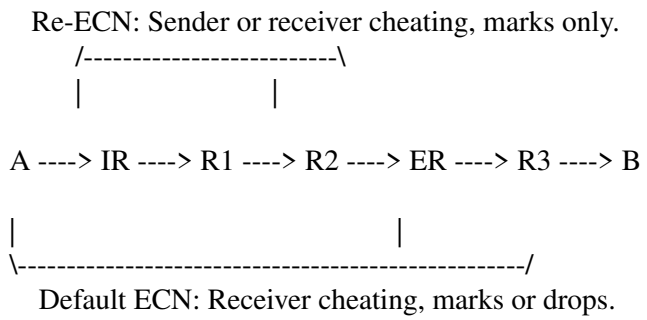

Figure 1: A path between end-nodes A and B.
Ingress and egress re-ECN routers IR and ER.
Routers R1, R2, and R3.

Figure 1 gives a simple figure comparing the functionality of Default ECN and re-ECN. Re-ECN is intended to allow the re-ECN routers together to protect against senders or receivers cheating about data packets ECN-marked between IR and ER. Default ECN with the ECN nonce is designed to allow senders to protect against receivers cheating about data packets dropped or ECN-marked anywhere along the end-to-end path.

Appendix I of [BJSK06] states that "delaying the ECN nonce is justified because the applicability of the ECN nonce seems too limited for it to consume a two-bit codepoint in the IP header." We disagree.

2. Informative References

[BJSK06] Briscoe, B., A. Jacquet, A. Salvatori, and M. Koyabe, Re-ECN: Adding Accountability for Causing Congestion to TCP/IP, internet draft draft-briscoe-tsvwg-re-ecn-tcp-03.txt, work in progress, October 2006.

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

[RFC3540] Spring, N., Wetherall, D., and D. Ely, "Robust Explicit Congestion Notification (ECN) Signaling with Nonces", RFC 3540, June 2003.

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

[RFC4341] Floyd, S., and E. Kohler, Profile for Datagram Congestion Control Protocol (DCCP) Congestion Control ID 2: TCP-like Congestion Control, RFC 4341, March 2006.

[RFC4342] Floyd, S., E. Kohler, and J. Padhye, Profile for Datagram Congestion Control Protocol (DCCP) Congestion Control ID 3: TCP-Friendly Rate Control (TFRC). RFC 4342, March 2006.

[SCWA99] Stefan Savage, Neal Cardwell, David Wetherall, Tom Anderson, TCP Congestion Control with a Misbehaving Receiver, ACM Computer Communications Review, October 1999.

AUTHORS' ADDRESSES

Sally Floyd
Phone: +1 (510) 666-2989
ICIR (ICSI Center for Internet Research)
Email: floyd@icir.org
URL: http://www.icir.org/floyd/