Network Working Group
Request for Comments: 3228
BCP: 57
Category: Best Current Practice

B. Fenner
AT&T Research

February 2002

IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)

Status of this Memo

Copyright Notice

Abstract

This memo requests that the IANA create a registry for fields in the IGMP (Internet Group Management Protocol) protocol header, and provides guidance for the IANA to use in assigning parameters for those fields.

Table of Contents

1. Introduction

This memo requests that the IANA create a registry for fields in the IGMP protocol header.

The terms "Specification Required", "Expert Review", "IESG Approval", "IETF Consensus", and "Standards Action", are used in this memo to refer to the processes described in [2].

2. IANA Considerations for fields in the IPv4 IGMP header

The IPv4 IGMP header [1] contains the following fields that carry values assigned from IANA-managed name spaces: Type and Code. Code field values are defined relative to a specific Type value.

Values for the IPv4 IGMP Type fields are allocated using an IESG Approval or Standards Action processes. Code Values for existing IPv4 IGMP Type fields are allocated using IESG Approval or Standards Action processes. The policy for assigning Code values for new IPv4 IGMP Types should be defined in the document defining the new Type value.

3. Assignments for testing and experimentation

Instead of suggesting temporary assignments as in [3], this document follows the lead of [4] and assigns a range of values for experimental use. The IGMP Code values 240-255 inclusive (0xf0 - 0xff) are reserved for protocol testing and experimentation.

Systems should silently ignore IGMP messages with unknown Code values.

4. Security Considerations

Security analyzers such as firewalls and network intrusion detection monitors often rely on unambiguous interpretations of the fields described in this memo. As new values for the fields are assigned, existing security analyzers that do not understand the new values may fail, resulting in either loss of connectivity if the analyzer declines to forward the unrecognized traffic, or loss of security if it does forward the traffic and the new values are used as part of an attack. This vulnerability argues for high visibility (which the Standards Action and IETF Consensus processes ensure) for the assignments whenever possible.

5. Normative References

[1] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[2] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

6. Informative References

[3] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", BCP 37, RFC 2780, March 2000.

[4] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", Work in Progress.

7. Author's Address

Bill Fenner
AT&T Labs -- Research
75 Willow Rd
Menlo Park, CA 94025
USA

EMail: fenner@research.att.com

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.