INTAREA Working Group A. Ghule
Internet-Draft R. Bonica
Intended status: Experimental Juniper Networks
Expires: February 8, 2020 August 7, 2019

Use of The IPv4 Reserved-flag for OAM
draft-aghule-intarea-oam-01

Abstract

This document defines new IPv4 Operations and Management (OAM) capabilities. In order to support these capabilities, this document defines a new interpretation of the IPv4 Reserved-flag.

Table of Contents

1. Problem Statement

This document defines new IPv4 [RFC0791] Operations and Management (OAM) capabilities. In order to support these capabilities, this document defines a new interpretation of the IPv4 Reserved-flag.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Redefining the IPv4 Reserved-Bit

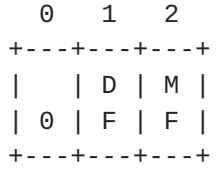

Figure 1: Current Defintion Of The IPv4 Flags Field

Figure 1 depicts the IPv4 Flags field, as defined in [RFC0791]. It contains the following fields:

o Bit 0: reserved, must be zero

o Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment.

o Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.

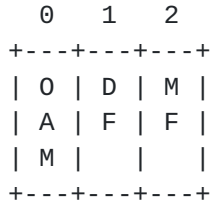

Figure 2: Redefintion Of The IPv4 Flags Field

Figure 2 depicts a redefinition of the IPv4 flags field. It contains the following fields:

o Bit 0: OAM 0 = No OAM Action, 1 = OAM Action

o Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment.

o Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.

In the redefinition, the Reserved-flag is replaced by an OAM flag.

4. OAM Flag Processing

4.1. At Network Ingress Nodes

When a packet enters a provider network, the network ingress router can subject the packet to policy. Policy includes match conditions and actions. If the packet satisfies match conditions, the policy can execute the following actions:

o Set the OAM-bit

o Recompute the IPv4 header checksum

If the ingress node sets the OAM bit, it MAY execute any of the OAM actions described in Section 4.2.

4.2. At Network Interior Nodes

When a network interior node receives a packet and its OAM bit is set, it MAY execute any combination of the following OAM actions.

Action	Notes
Log the packet	The processing node creates a log entry. The log entry reflects the time at which it was created. It also reflects the time at which the packet arrived.
Count the packet	The processing node increments a counter.
Send an ICMP OAM message	The processing node sends an ICMP OAM message to the packet's source. The OAM message indicates the time at which the packet arrived.
Send telemetry	The processing node sends telemetry to a monitoring station. Telemetry includes the packet and the time at which the packet arrived.

Table 1: OAM Actions

The action taken depends on local configuration. By default, no action is taken

4.3. At Network Egress Nodes

When a network egress node receives a packet and the OAM bit is set, it MAY execute any of the OAM actions described in Section 4.2. It SHOULD clear the OAM bit. If it clears the OAM bit, it MUST recompute the IPv4 Header Checksum.

5. The ICMP OAM Message

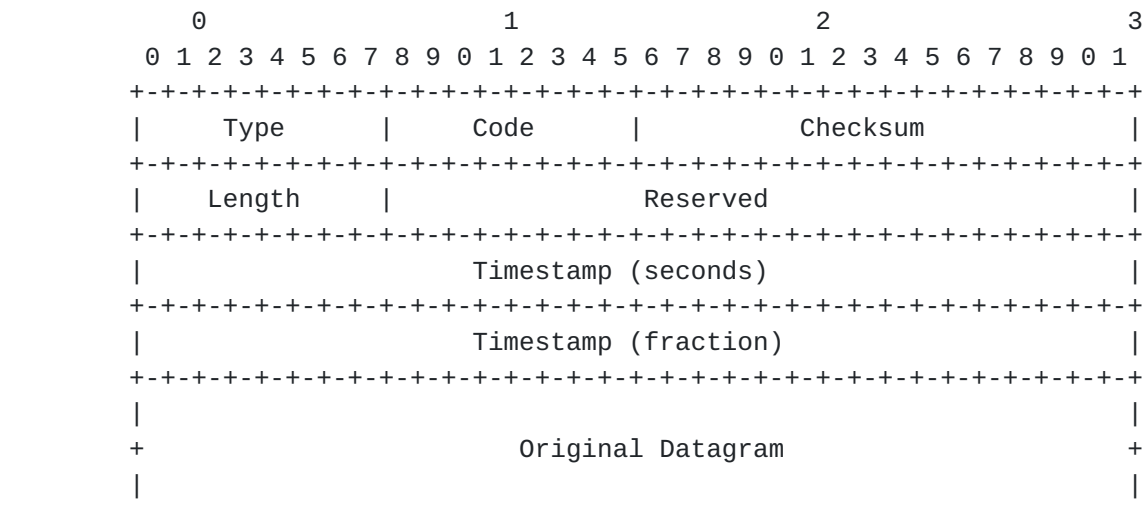

Figure 3

Figure 3 depicts the ICMP OAM message. The ICMP OAM message contains the following fields:

- Type - OAM. Value TBD by IANA.
- Code - MUST be set to (0) No Error.
- Checksum - See [RFC0792]
- Reserved - MUST be set to 0 and MUST be ignored upon receipt.
- Length - Represents the length of the padded "original datagram" field, measured in 32-bit words.
- Timestamp (seconds) - Represents the time at which the original packet arrived in Network Time Protocol (NTP) [RFC5905] format.
- Timestamp (fraction) - Represents the time at which the original packet arrived in NTP [RFC5905] format.
- Original Datagram - As much of invoking packet as possible without the ICMPv6 packet exceeding the minimum ICMP MTU (576 bytes). The original datagram MUST be zero padded to the nearest 32-bit boundary.

ICMP OAM messages SHOULD be rate limited by the sender.

The Timestamp fields SHOULD be as accurate as possible. They SHOULD reflect the time at which the original packet arrived, not the time at which the ICMPv6 OAM message was sent.

6. IANA Considerations

IANA is requested to add an entry to the ICMP Type registry (https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types). The ICMP message name is OAM and its value is TBD by IANA.

7. Security Considerations

All OAM actions elicited by the OAM bit must be rate-limited, so that they cannot be used as denial of service attack vectors.

8. Acknowledgements

The authors wish to acknowledge Ross Callon for his contributions to this document.

9. References

9.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[InfRef] , 2004.

Authors' Addresses

Ashish Ghule
Juniper Networks
Bangalore, KA 56009
India

Email: aghule@juniper.net

Ron Bonica
Juniper Networks
Herndon, Virginia 20171
USA

Email: rbonica@juniper.net