

INTAREA Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: February 8, 2020

A. Ghule  
R. Bonica  
Juniper Networks  
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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 8, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|                      |  |                   |
|----------------------|--|-------------------|
| <a href="#">1.</a>   | Problem Statement . . . . .                | <a href="#">2</a> |
| <a href="#">2.</a>   | Requirements Language . . . . .            | <a href="#">2</a> |
| <a href="#">3.</a>   | Redefining the IPv4 Reserved-Bit . . . . . | <a href="#">2</a> |
| <a href="#">4.</a>   | OAM Flag Processing . . . . .              | <a href="#">3</a> |
| <a href="#">4.1.</a> | At Network Ingress Nodes . . . . .         | <a href="#">3</a> |
| <a href="#">4.2.</a> | At Network Interior Nodes . . . . .        | <a href="#">3</a> |
| <a href="#">4.3.</a> | At Network Egress Nodes . . . . .          | <a href="#">4</a> |
| <a href="#">5.</a>   | The ICMP OAM Message . . . . .             | <a href="#">4</a> |
| <a href="#">6.</a>   | IANA Considerations . . . . .              | <a href="#">6</a> |
| <a href="#">7.</a>   | Security Considerations . . . . .          | <a href="#">6</a> |
| <a href="#">8.</a>   | Acknowledgements . . . . .                 | <a href="#">6</a> |
| <a href="#">9.</a>   | References . . . . .                       | <a href="#">6</a> |
| <a href="#">9.1.</a> | Normative References . . . . .             | <a href="#">6</a> |
| <a href="#">9.2.</a> | Informative References . . . . .           | <a href="#">6</a> |
|                      | Authors' Addresses . . . . .               | <a href="#">7</a> |

**[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**

```

      0   1   2
    +---+---+---+
    |   | D | M |
    | 0 | F | F |
    +---+---+---+

```

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.

| 0             | 1 | 2 |
|---------------|---|---|
| +---+---+---+ |   |   |
| O             | D | M |
| A             | F | F |
| M             |   |   |
| +---+---+---+ |   |   |

Figure 2: Redefinition 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**



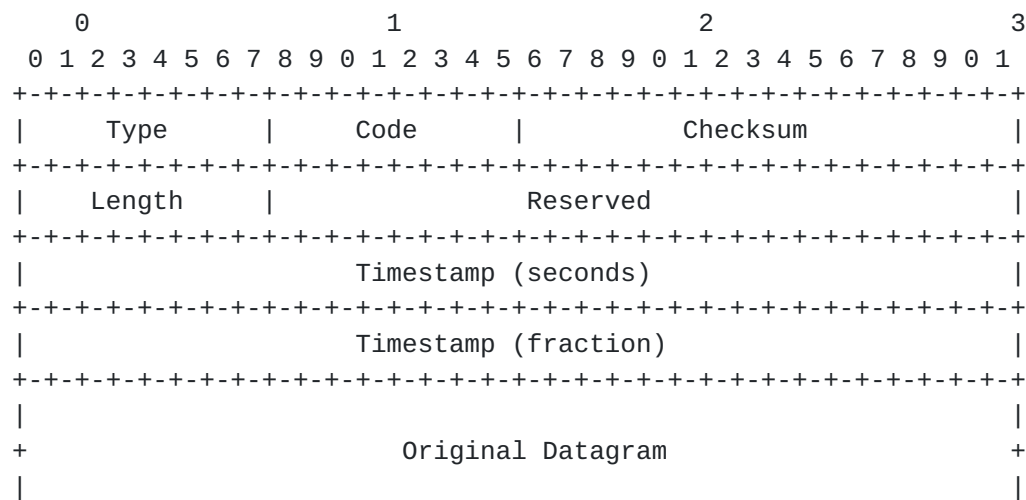


Figure 3

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

- o Type - OAM. Value TBD by IANA.
- o Code - MUST be set to (0) No Error.
- o Checksum - See [[RFC0792](#)]
- o Reserved - MUST be set to 0 and MUST be ignored upon receipt.
- o Length - Represents the length of the padded "original datagram" field, measured in 32-bit words.
- o Timestamp (seconds) - Represents the time at which the original packet arrived in Network Time Protocol (NTP) [[RFC5905](#)] format.
- o Timestamp (fraction) - Represents the time at which the original packet arrived in NTP [[RFC5905](#)] format.
- o 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](mailto:aghule@juniper.net)

Ron Bonica  
Juniper Networks  
Herndon, Virginia 20171  
USA

Email: [rbonica@juniper.net](mailto:rbonica@juniper.net)

