| | | |
|---|---|---|
| Open Shortest Path First IGP | P. Jakma | |
| Working Group | DCS, Uni. of Glasgow | |
| Internet-Draft | M. Bhatia | |
| Updates: 2328 (if approved) | Alcatel-Lucent | |
| Intended status: Standards Track | October 13, 2010 | |
| Expires: April 16, 2011 | | |

TOC

**Stronger, Automatic Integrity Checks for OSPF Packets**
**draft-jakma-ospf-integrity-00**

**Abstract**

This document describes an extension to OSPFv2 and OSPFv3 to allow a stronger integrity check to be applied to the protocol packets, than the default OSPF checksum, which is known to be weak.
The extension allows OSPF speakers to negotiate the use of a CRC integrity check, as a new psuedo-authentication type.

**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 http://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 April 16, 2011.

**Copyright Notice**

---

**Table of Contents**



---

## 1. Requirements Language

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

---

## 2. Introduction

TOC

The integrity of Open Shortest Path First versions 2 (OSPFv2)[RFC2328] (Moy, J., "OSPF Version 2," April 1998.) and 3 (OSPFv3)[RFC5340] (Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6," July 2008.) packets is protected either through the standard internet protocol checksum, or through some cryptographic integrity scheme within OSPF, or, more rarely, through IPSec. This provides a check against errors that can not be caught by the link-layer integrity

checks, e.g. errors in lower layers of the software stack or in hardware of the host.
The internet protocol checksum is known to have weaknesses[partridge] (Stone, J., Greenwald, M., Partridge, C., and J. Hughes, “Performance of checksums and CRC's over real data,” 1998.). In particular it can not detect re-ordered words and certain patterns of bit flips. If stronger integrity checks are desired, the only option is to use cryptographic HMACs, either with MD5 (all conforming [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.) implementations) or, if supported, the stronger algorithms specified by [RFC5709] (Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, “OSPFv2 HMAC-SHA Cryptographic Authentication,” October 2009.). There are some disadvantages though to using the existing support for cryptographic HMACs purely for integrity checking. The algorithms require more computation, which may be noticable on less powerful and/or energy-sensitive platforms. Additionally, the need to configure key material is an additional administrative burden.
This documents extends OSPF to allow for the automatic and backward compatible use of stronger integrity checks. Backward compatibility implies the default null authentication type must be used and extended.

---

## 3. Stronger Checksum mechanism for OSPFv2

TOC

The null authentication mode of OSPFv2 is extended to make use of the authentication data field of the OSPFv2 packet header. Where previously this field was ignored for null authentication, now an OPTIONAL "Null Authentication Data" structure is recognised there.
Implementations MUST provide a means to disable this extension, in case there are non-conforming RFC2328 implementations. Implementations MAY wish to generate a CRC32 checksum by default via this extension, and SHOULD attempt to verify any received, regardless of whether they generate the same or not.

---

### 3.1. Null Authentication Data

TOC

---

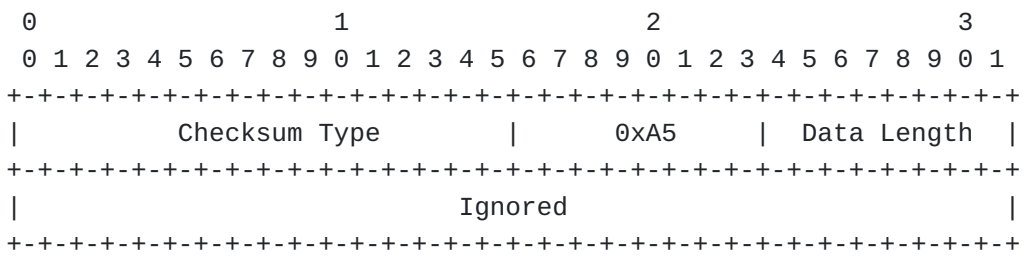


**Figure 1: Null Authentication Data**

---

The authentication data field in the standard OSPFv2 packet header is redefined as shown above, when null authentication is used. The new field definitions are as follows:

> **Checksum Type:** This field indicates the new checksum algorithm that the routers must use and is described in detail in the later sections.
>
> **Magic:** This field is set to 0xA5. This magic, in combination with the OSPF and IP packet lengths, signals the use of this extension.
>
> **Data Length:** The length in 4-octet words of the extended checksum data block appended to the OSPFv2 packet.

---

## 4. Stronger Checksum mechanism for OSPFv3

TOC

OSPFv3 uses IPSec for protection and does not carry any authentication information in its headers. Thus it is not possible to overload the Null Authentication type as was done in case of OSPFv2.

---

### 4.1. EC-Bit in Options Field

TOC

A new EC-bit (EC stands for Extended Checksum) is introduced into the OSPFv3 Options field. Routers MUST set the EC-bit in all OSPFv3 packets to indicate that the packet is carrying the new extended checksum data.

---

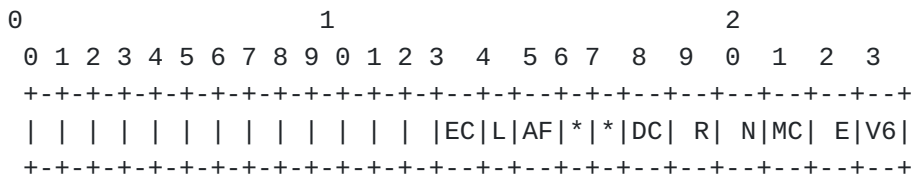


**Figure 2: OSPFv3 Options Field**

### 4.2. Extended Checksum Data Block

TOC

The data block for carrying extended checksum in OSPFv3 is formatted as described below.

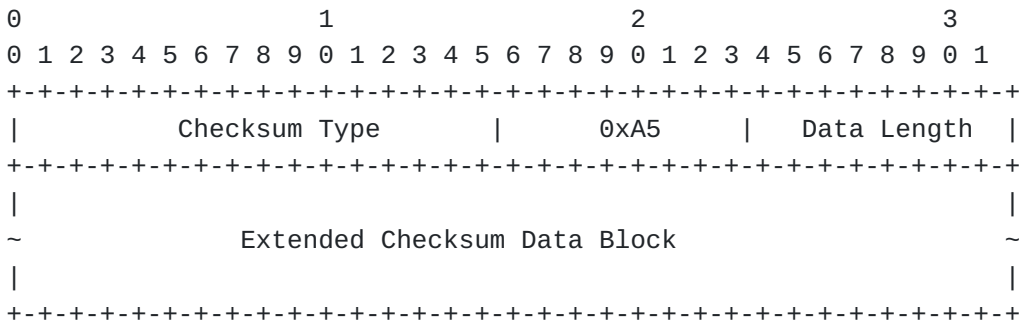


**Figure 3: OSPFv3 Options Field**

The Checksum Type is of two octets and indicates the new checksum algorithm that the routers must use. This is described in detail in the later sections. The next field is a reserved magic field set to 0xA5. The Data length field is of two octets and carries the size of the entire extended checksum data block that has been appended to the OSPFv3 payload, specified in units of 4-octet words. The Extended Checksum Data Block carries the checksum data that the recievers will use to verify the integrity of the OSPFv3 protocol payload.

TOC

## 5. Generation

The same steps are followed as for D.4.1 of [RFC2328] (Moy, J., "OSPF Version 2," April 1998.). Additionally, a 2nd integrity check algorithm is also computed over the packet data, with at least the same amount of zero padding, to produce an "extended checksum", which is appended to the OSPFv2 packet. Its is size accounted for in the Null Authentication Data "data length" field and in the IP length, but not in the OSPFv2 packet header, in a similar fashion to the standard OSPFv2 cryptographic authentication mechanism.
The "Checksum Type" and "Data Length" fields are set to the appropriate values for the 2nd integrity check algorithm.
In case of OSPFv3 the entire extended checksum block is appended to the OSPFv3 packet, with its size accounted for in the IPv6 payload length, but not in the OSPFv3 packet header.
Implementations MUST append the extended checksum data, that is carried as part of the OSPF protocol payload, before the link local signaling (LLS) [RFC5613] (Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling," August 2009.) block (if it exists).

---

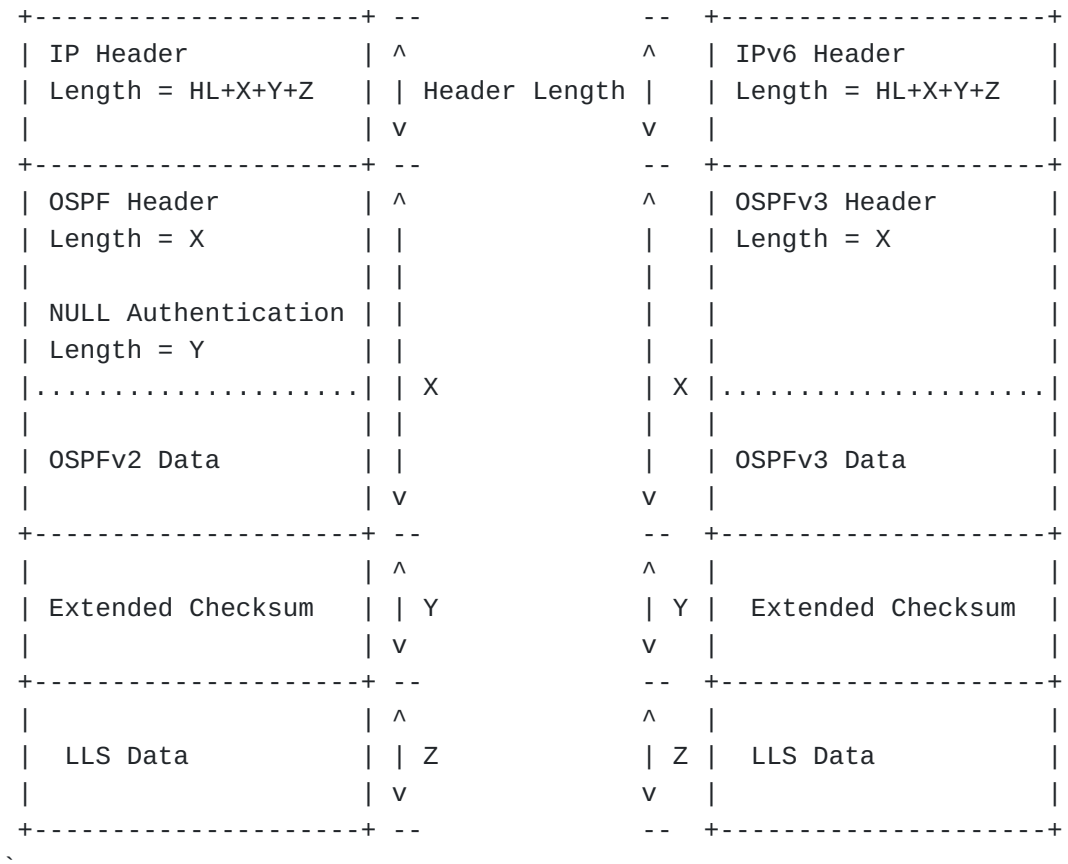

**Figure 4: Extended Checksum Block in OSPFv2 and OSPFv3**

## 6. Verification

TOC

The packet data is padded out, as required by [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.).
In case of OSPFv2, the Null Authentication Data "0xA5" magic field is examined. If it does not match, then verification proceeds as per D.5.1 of [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.). If it matches, then the IP length in the header MUST be verified. An incoming packet will only contain a valid extended checksum if the length in the IP header = length in OSPF header + "data length" in the NULL Authentication header + data length in the LLS [RFC5613] (Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, “OSPF Link-Local Signaling,” August 2009.) block (if it exists). Implementations can trivially determine if an LLS block is being carried by inspecting the "L" bit in the OSPF Options field in the HELLOs and DDs.
Implementations MUST proceed with regular checksum if these numbers dont match. If they do then the IP checksum field of the OSPF header MUST be ignored. Instead the stronger integrity algorithm specified by the "Checksum Type" field is used, and verified against the corresponding checksum. The packet MUST be discarded if the computed checksum does not match with what's carried in the OSPF packet.
In case of OSPFv3, the presence of the EC-bit in the OSPFv3 Options field will indicate that a new checksum algorithm is being used. Routers MUST parse the packet till the end of the OSPFv3 payload till it reaches the start of the extended checksum data block. The processing that follows next is similar to the way its done for OSPFv2 as explained earlier.

## 7. Stronger Integrity Algorithm Types

TOC

### 7.1. CRC32

TOC

The CRC32 algorithm, as used with IEEE 802.3 and defined by [hammond] (Hammond, J., Brown, J., and S. Lui, “Development of a Transmission Error Model and an Error Control Model,” May 1975.) is used to

calculate its 4-byte digest. The length set in the Null Authentication Data thus will be 1.

### 7.2. MD5-Digest

TOC

The MD5 algorithm, as per 5ref17 of [RFC2328] (Moy, J., "OSPF Version 2," April 1998.) is used in plain digest mode (i.e. solely over the data, unlike the HMAC mode used by cryptographic authentication) to calculate its 8-byte digest. The length set in the Null Authentication Data thus will be 2.

## 8. IANA Considerations

TOC

OSPFv2 Null Authentication Checksum Types are maintained by the IANA. Extensions to OSPFv2 that require a new Checksum Type must be reviewed by a designated expert from the routing area.
This document assigns OSPF Null Authentication Checksum Types 1 and 2, for CRC32 and MD5-Digest respectively.
IANA is also requested to allocate EC-bit in the OSPFv3 "Options Registry"

## 9. Security Considerations

TOC

This extension does not raise any new security concerns. It only is used where operators have chosen not to configure cryptographic security mechanisms.

## 10. References

TOC

### 10.1. Normative References

TOC


| | |
|---|---|
| [RFC2119] | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML). |
| [RFC2328] | Moy, J., "OSPF Version 2," STD 54, RFC 2328, April 1998 (TXT, HTML, XML). |

| | |
|---|---|
| [RFC5340] | Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6," RFC 5340, July 2008 (TXT). |
| [RFC5709] | Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication," RFC 5709, October 2009 (TXT). |
| [hammond] | Hammond, J., Brown, J., and S. Lui, "Development of a Transmission Error Model and an Error Control Model," Technical Report Georgia Institute of Technology, May 1975. |


### 10.2. Informative References

TOC


| | |
|---|---|
| [RFC5613] | Zinin, A., Roy, A., Nguyen, L., Friedman, B., and D. Yeung, "OSPF Link-Local Signaling," RFC 5613, August 2009 (TXT). |
| [partridge] | Stone, J., Greenwald, M., Partridge, C., and J. Hughes, "Performance of checksums and CRC's over real data," IEEE/ACM Trans. Netw. vol 6, num 5, pages 529-543, 1998. |


## Authors' Addresses

TOC


| | |
|---|---|
| | Paul Jakma |
| | School of Computing Science, University of Glasgow |
| | Lilybank Gardens |
| | Glasgow G12 8QQ |
| | Scotland |
| Email: | paulj@dcs.gla.ac.uk |
| | |
| | Manav Bhatia |
| | Alcatel-Lucent |
| | Bangalore, |
| | India |
| Phone: | |
| Email: | manav.bhatia@alcatel-lucent.com |