

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 29, 2007

B. Friedman
L. Nguyen
A. Roy
D. Yeung
Cisco Systems
A. Zinin
Alcatel
October 26, 2006

**OSPF Link-local Signaling
draft-nguyen-ospf-lls-06.txt**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 29, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

OSPF is a link-state intra-domain routing protocol used in IP networks. OSPF routers exchange information on a link using packets that follow a well-defined format. The format of OSPF packets is not flexible enough to enable applications exchange arbitrary data, which may be necessary in certain situations. This memo describes a vendor specific, backward-compatible technique to perform link-local signaling, i.e., exchange arbitrary data on a link.

Table of Contents

- [1. Introduction](#) [3](#)
- [1.1. Requirements notation](#) [3](#)
- [2. Proposed Solution](#) [4](#)
- [2.1. Options Field](#) [5](#)
- [2.2. LLS Data Block](#) [5](#)
- [2.3. LLS TLVs](#) [6](#)
- [2.4. Predefined TLV](#) [6](#)
- [2.4.1. Extended Options TLV](#) [6](#)
- [2.4.2. Cryptographic Authentication TLV](#) [7](#)
- [3. Backward Compatibility](#) [9](#)
- [4. Security Considerations](#) [10](#)
- [5. IANA Considerations](#) [11](#)
- [6. References](#) [12](#)
- [6.1. Normative References](#) [12](#)
- [6.2. Informative References](#) [12](#)
- [Appendix A. Acknowledgments](#) [13](#)
- [Authors' Addresses](#) [14](#)
- [Intellectual Property and Copyright Statements](#) [15](#)

1. Introduction

Formats of OSPF [[RFC2328](#)] packets are not very flexible to provide an acceptable mechanism for opaque data transfer. However, this appears to be very useful to allow OSPF routers to do so. An example where such a technique could be used is exchanging some capabilities on a link (standard OSPF utilizes Options field in Hello and Exchange packets, but there are not so many bits left in it).

One potential way of solving this task could be introducing a new packet type. However, that would mean introducing extra packets on the network which may not be desirable, so this document describes how to exchange data using existing, standard OSPF packet types.

1.1. Requirements notation

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](#) [[RFC2119](#)].

2. Proposed Solution

To perform link-local signaling (LLS), OSPF routers add a special data block at the end of OSPF packets or right after the authentication data block when cryptographic authentication is used. Like with OSPF cryptographic authentication, the length of the LLS-block is not included into the length of OSPF packet, but is included in the IP packet length. Figure 1 illustrates how the LLS data block is attached.

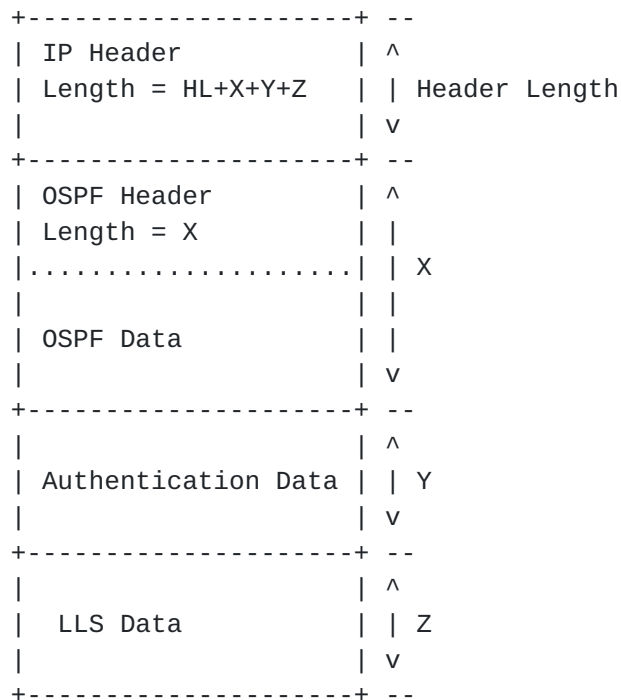


Figure 1: Attaching LLS Data Block

The LLS data block may be attached to OSPF packets of two types--- type 1 (OSPF Hello), and type-2 (OSPF DBD). The data included in LLS block attached to a Hello packet may be used for dynamic signaling, since Hello packets may be sent at any moment in time. However, delivery of LLS data in Hello packets is not guaranteed. The data sent with DBD packets is guaranteed to be delivered as part of the adjacency forming process.

This memo does not specify how the data transmitted by the LLS mechanism should be interpreted by OSPF routers. The interface between OSPF LLS component and its clients is implementation-specific.

2.1. Options Field

A new bit, called L (L stands for LLS) is introduced to OSPF Options field (see Figure 2). The value of the bit is 0x10. Routers set L bit in Hello and DBD packets to indicate that the packet contains LLS data block.

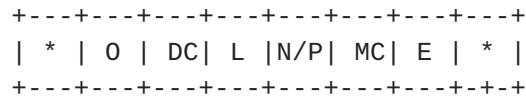


Figure 2: The Options field

L-bit

This bit is set only in Hello and DBD packets. It is not set in OSPF LSAs and may be used in them for different purposes.

2.2. LLS Data Block

The data block used for link-local signaling is formatted as described below (see Figure 3 for illustration).

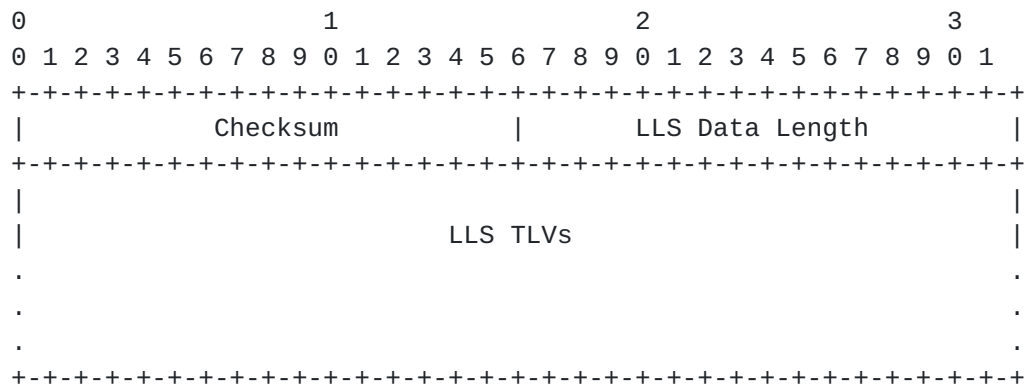


Figure 3: Format of LLS Data Block

Checksum

The Checksum field contains the standard IP checksum of the entire contents of the LLS block.

LLS Length

The 16-bit LLS Data Length field contains the length (in 32-bit words) of the LLS block including the header and payload.

Implementations should not use the Length field in the IP packet header to determine the length of the LLS data block.

Note that if the OSPF packet is cryptographically authenticated, the LLS data block must also be cryptographically authenticated. In this case the regular LLS checksum is not calculated and the LLS block will contain a cryptographic authentication TLV (see Section 2.4.2).

The rest of the block contains a set of Type/Length/Value (TLV) triplets as described in Section 2.3. All TLVs must be 32-bit aligned (with padding if necessary).

2.3. LLS TLVs

The contents of LLS data block is constructed using TLVs. See Figure 4 for the TLV format.

The type field contains the TLV ID which is unique for each type of TLVs. The Length field contains the length of the Value field (in bytes) that is variable and contains arbitrary data.

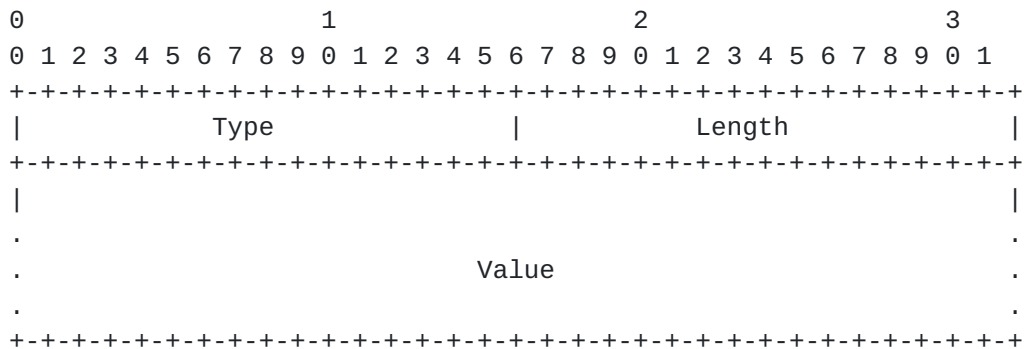


Figure 4: Format of LLS TLVs

Note that TLVs are always padded to 32-bit boundary, but padding bytes are not included in TLV Length field (though it is included in the LLS Data Length field of the LLS block header).

2.4. Predefined TLV

2.4.1. Extended Options TLV

This subsection describes a TLV called Extended Options (EO) TLV. The format of EO-TLV is shown in Figure 5.

Bits in the Value field do not have any semantics from the point of view of LLS mechanism. This field may be used to announce some OSPF capabilities that are link-specific. Also, other OSPF extensions may allocate bits in the bit vector to perform boolean link-local signaling.

The length of the Value field in E0-TLV is 4 bytes.

The value of the type field in E0-TLV is 1.

E0-TLV should only appear once in the LLS data block.

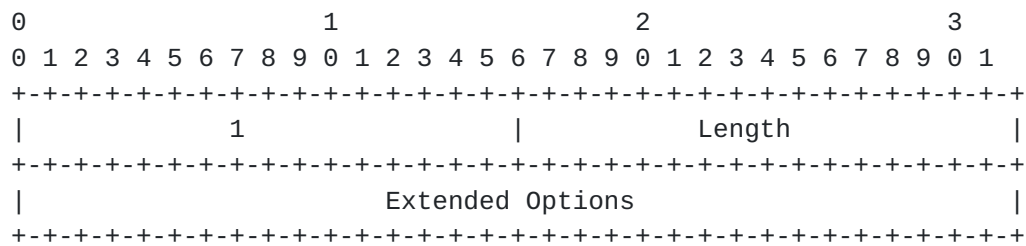


Figure 5: Format of E0 TLV

Currently, [OOB] and [RESTART] use bits in the Extended Options field of the E0-TLV. The Extended Options bits are also defined in Section 5.

2.4.2. Cryptographic Authentication TLV

This document defines a special TLV that is used for cryptographic authentication (CA-TLV) of the LLS data block. This TLV should be included in the LLS block when the cryptographic (MD5) authentication is enabled on the corresponding interface. The message digest of the LLS block should be calculated using the same key as that used for the main OSPF packet. The cryptographic sequence number is included in the TLV and must be the same as the one in the main OSPF packet for the LLS block to be considered authentic.

The TLV is constructed as shown Figure 6.

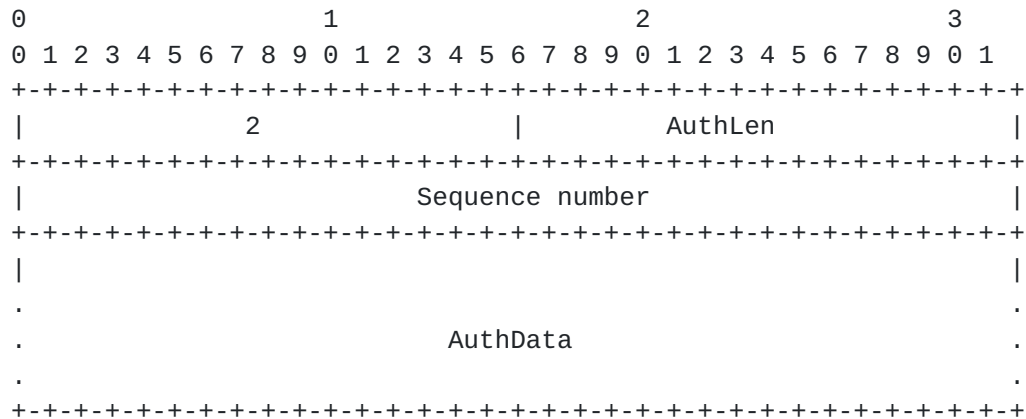


Figure 6: Format of Cryptographic Authentication TLV

The value of the Type field for CA-TLV is 2.

The Length field in the header contains the length of the data portion of the TLV that includes 4 bytes for the Sequence Number and the length of the message digest (MD5) block for the whole LLS block in bytes (this will always be 16 bytes for MD5). So AuthLen field will have value of 20.

The Sequence Number field contains the cryptographic sequence number that is used to prevent simple replay attacks. For the LLS block to be considered authentic, the Sequence Number in the CA-TLV must match the Sequence Number in the OSPF packet.

The AuthData contains the message digest calculated for the LLS data block.

The CA-TLV may appear in the LLS block only once. Also, when present, this TLV should be the last in the LLS block.

3. Backward Compatibility

The modifications to OSPF packet formats are compatible with standard OSPF because LLS-incapable routers will not consider the extra data after the packet; i.e., the LLS data block will be ignored by routers which do not support the LLS extension.

4. Security Considerations

The function described in this document does not create any new security issues for the OSPF protocol. The described technique provides the same level of security as OSPF protocol by allowing LLS data to be authenticated (see [Section 2.4.2](#) for more details).

5. IANA Considerations

LLS TLV types are maintained by the IANA. Extensions to OSPF which require a new LLS TLV type must be reviewed by an designated expert from the routing area.

Following the policies outlined in [[RFC2434](#)], LLS type values in the range of 0-32767 are allocated through an IETF Consensus action and LLS type values in the range of 32768-65536 are reserved for private and experimental use.

This document assigns LLS types 1 and 2, as follows:

LLS Type	Name	Reference
0	Reserved	
1	Extended Options	[RFCNNNN]*
2	Cryptographic Authentication	[RFCNNNN]*
3-32767	Reserved for assignment by the IANA	
32768-65535	Private Use	

*[RFCNNNN] refers to the RFC number-to-be for this document.

This document also assigns the following bits for the Extended Options bits field in the E0-TLV outlined in [Section 2.4.1](#):

Extended Options Bit	Name	Reference
0x00000001	LSDB Resynchronization (LR)	[OOB]
0x00000002	Restart Signal (RS-bit)	[RESTART]

Other Extended Options bits will be allocated through an IETF consensus action.

6. References

6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFC's to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [RFC2328] Moy, J., "OSPF Version 2", [RFC 2328](#), April 1998.
- [RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 2434](#), October 1998.

6.2. Informative References

- [OOB] Nguyen, L., Roy, A., and A. Zinin, "OSPF Out-of-band LSDB resynchronization", Work in progress , October 2006.
- [RESTART] Nguyen, L., Roy, A., and A. Zinin, "OSPF Restart Signaling", Work in progress , October 2006.

[Appendix A](#). Acknowledgments

The authors would like to acknowledge Russ White for his review of this document.

Authors' Addresses

Barry Friedman
Cisco Systems
225 West Tasman Drive
San Jose, CA 95134
USA

Email: friedman@cisco.com

Liem Nguyen
Cisco Systems
225 West Tasman Drive
San Jose, CA 95134
USA

Email: lhnguyen@cisco.com

Abhay Roy
Cisco Systems
225 West Tasman Drive
San Jose, CA 95134
USA

Email: akr@cisco.com

Derek Yeung
Cisco Systems
225 West Tasman Drive
San Jose, CA 95134
USA

Email: myeung@cisco.com

Alex Zinin
Alcatel
Sunnyvale, CA
USA

Email: zinin@psg.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

