Network Working Group
Internet Draft
Expiration Date: July 2001
File name: draft-ietf-ospf-lls-00.txt

Alex Zinin (Cisco Systems)
Barry Friedman (Cisco Systems)
Abhay Roy (Cisco Systems)
Liem Nguyen (Cisco Systems)
Derek Yeung (Procket)
November 2000

OSPF Link-local Signaling
draft-ietf-ospf-lls-00.txt

Status of this Memo

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 backward-compatible technique to perform link-local signaling, i.e., exchange arbitrary data on a link.

1 Motivation

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, in some situations it may not be desirable, so this document describes how to exchange data using standard OSPF packet types.

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.

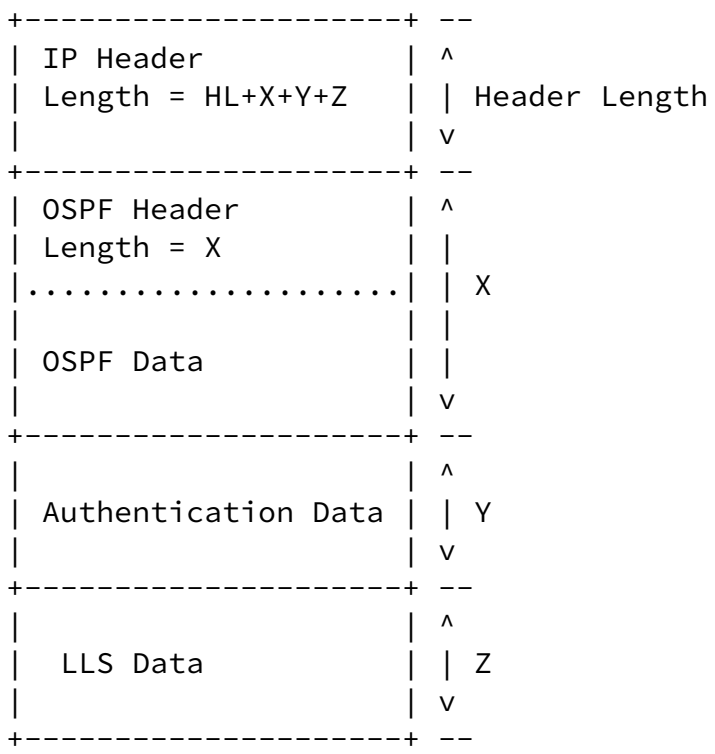


Figure 1: Attaching LLS Data Block

The LLS data block may be attached to OSPF packets of two types--- type 1 (OSPF Hello), and type-2 (OSPF DBD). Note that only the

initial DBD packet (with the I bit set) may carry the LLS block. 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 an initial DBD packets is guaranteed

to be delivered as soon as the adjacency proceeds from ExStart state, but this info may not change dynamically, since sending of an initial DBD packet will bring the adjacency to ExStart state.

This memo does not specify how the data transmitted by 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 Hellow and DBD packets to indicate that the packet contains LLS data block.

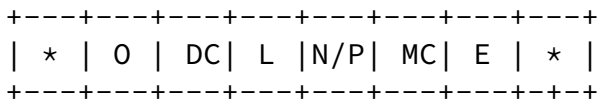
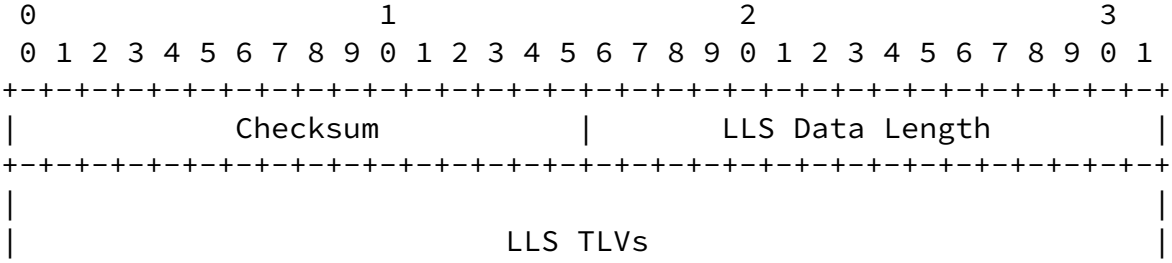


Figure 2: The Options field

The L-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).



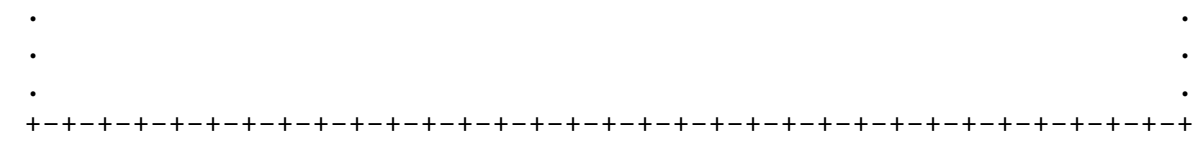


Figure 3: Format of LLS Data Block

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

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.

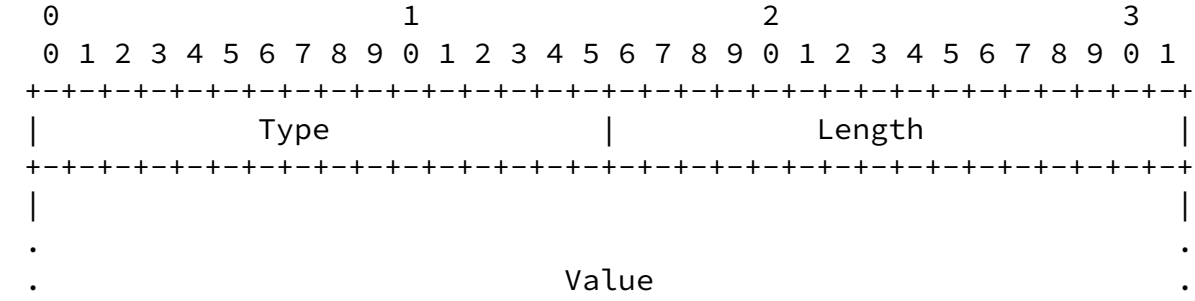
Note that if the OSPF packet is cryptographically authenticated, the LLS data block must also be cryptographically authenticated. In this case the regular checksum is not calculated and the LLS block will contain a cryptographic authentication TLV (see Section 2.4.2).

The rest of the block contains a set of Type/Length/Value (TLV) triplets as described in Section 2.2. 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 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.



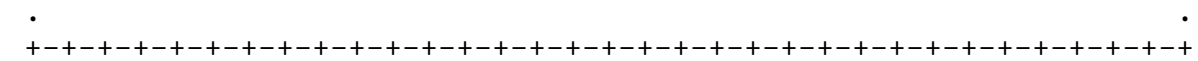


Figure 4: Format of LLS TLVs

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 EO-TLV is 4 bytes.

The value of the type field in EO-TLV is TBD (temporarily used value is 1).

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

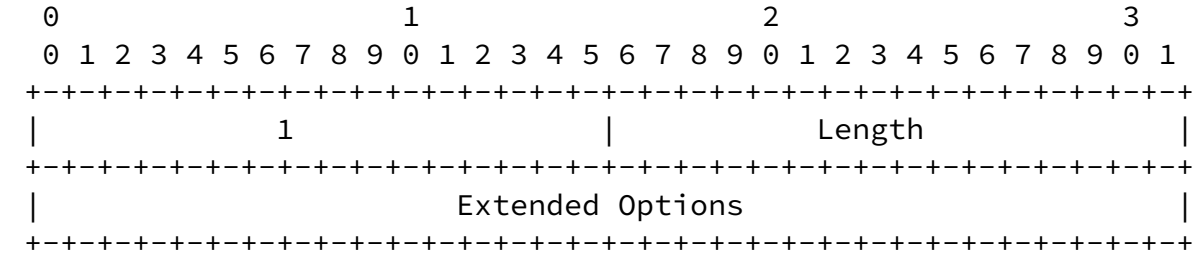


Figure 5: Format of EO TLV

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 inluded in the LLS block when the cryptographic (MD5) authentication is enabled on the corresponding inteface. 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.

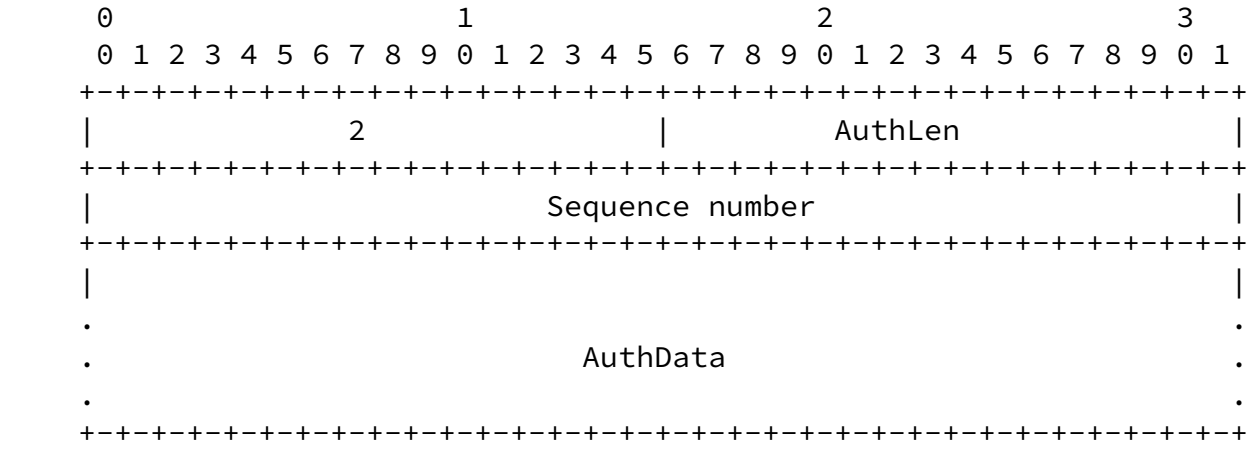


Figure 6: Format of Cryptographic Authentication TLV

The value of the Type field for CA-TLV is TBD. Temoprary used value

is 2.

The Length field in the header contains the length of the data portion of the TLV that includes 2 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 18.

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 IANA Considerations

LLS TLV types are maintained by the IANA. Extensions to OSPF which require a new LLS TLV type must be reviewed by the OSPF working group. In the event that the OSPF working group has disbanded the review shall be performed by a recommended Designated Expert.

Following the policies outlined in [IANA], 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.

4 Compatibility Issues

The modifications to OSPF packet formats are compatible with standard OSPF, because LLS-incapable routers will not consider the extra data after the packet.

5 Security considerations

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).

6 Acknowledgements

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

7 References

[RFC2328]
J. Moy. OSPF version 2. Technical Report RFC 2328, Internet Engineering Task Force, 1998. ftp://ftp.isi.edu/in-notes/rfc2328.txt.

[IANA]T. Narten, H. Alvestrand. Guidelines for Writing an IANA Considerations Section in RFCs. Best current practice RFC 2434. ftp://ftp.isi.edu/in-notes/rfc2434.txt

8 Authors' addresses

Alex Zinin
Cisco Systems
150 W. Tasman Dr.
San Jose,CA 95134
USA
E-mail: azinin@cisco.com

Barry Friedman
Cisco Systems
170 W. Tasman Dr.
San Jose,CA 95134
USA
E-mail: friedman@cisco.com

Liem Nguyen
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA
e-mail: lhnguyen@cisco.com

Abhay Roy
Cisco Systems
170 W. Tasman Dr.
San Jose,CA 95134
USA
E-mail: akr@cisco.com

Derek M. Yeung
Procket Networks
3850 N.First Street
San Jose, CA 95134
Phone: 408-954-7911
Fax: 408-987-6166
Email: myeung@procket.com