                      The OSPF Opaque LSA Option

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This document defines enhancements to the OSPF protocol to support a
   new class of link state advertisements (LSAs) called Opaque LSAs.
   Opaque LSAs provide a generalized mechanism to allow for the future
   extensibility of OSPF. Opaque LSAs consist of a standard LSA header
   followed by application-specific information. The information field
   may be used directly by OSPF or by other applications. Standard OSPF
   link-state database flooding mechanisms are used to distribute Opaque
   LSAs to all or some limited portion of the OSPF topology.

   This document replaces RFC 2370 and adds to it a mechanism to enable
   an OSPF router to validate Autonomous System (AS)-scope Opaque LSAs
   originated outside of the router's OSPF area.

Table of Contents

1. Introduction

   Over the last several years, the OSPF routing protocol [OSPF] has
   been widely deployed throughout the Internet. As a result of this
   deployment and the evolution of networking technology, OSPF has been
   extended to support many options; this evolution will obviously
   continue.

   This document defines enhancements to the OSPF protocol to support a
   new class of link state advertisements (LSAs) called Opaque LSAs.
   Opaque LSAs provide a generalized mechanism to allow for the future
   extensibility of OSPF. The information contained in Opaque LSAs may
   be used directly by OSPF or indirectly by some application wishing to
   distribute information throughout the OSPF domain. The exact use of
   Opaque LSAs is beyond the scope of this document.

   Opaque LSAs consist of a standard LSA header followed by a 32-bit
   aligned application-specific information field. Like any other LSA,
   the Opaque LSA uses the link-state database distribution mechanism
   for flooding this information throughout the topology. The link-
   state type field of the Opaque LSA identifies the LSA's range of
   topological distribution. This range is referred to as the flooding
   scope.

   It is envisioned that an implementation of the Opaque option provides
   an application interface for 1) encapsulating application-specific
   information in a specific Opaque type, 2) sending and receiving
   application-specific information, and 3) if required, informing the
   application of the change in validity of previously received
   information when topological changes are detected.

1.1. Organization of This Document

   This document first defines the three types of Opaque LSAs followed
   by a description of OSPF packet processing. The packet processing
   sections include modifications to the flooding procedure and to the
   neighbor state machine. Appendix A then gives the packet formats.

1.2. Acknowledgments

   We would like to thank Acee Lindem for his detailed review and useful
   feedback. The handling of AS-scope Opaque LSAs described in this
   document is taken from "Validation of OSPF AS-scope opaque LSAs"
   (April 2006).

2. Conventions Used in This Document

   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].

3. The Opaque LSA

   Opaque LSAs are types 9, 10, and 11 link state advertisements.
   Opaque LSAs consist of a standard LSA header followed by a 32-bit
   aligned application-specific information field. Standard link-state
   database flooding mechanisms are used for distribution of Opaque
   LSAs. The range of topological distribution (i.e., the flooding
   scope) of an Opaque LSA is identified by its link-state type. This
   section documents the flooding of Opaque LSAs.

   The flooding scope associated with each Opaque link-state type is
   defined as follows.

   o Link-state type-9 denotes a link-local scope. Type-9 Opaque LSAs
      are not flooded beyond the local (sub)network.

   o Link-state type-10 denotes an area-local scope. Type-10 Opaque
      LSAs are not flooded beyond the borders of their associated area.

   o Link-state type-11 denotes that the LSA is flooded throughout the
      Autonomous System (AS). The flooding scope of type-11 LSAs are
      equivalent to the flooding scope of AS-External (type-5) LSAs.
      Specifically, type-11 Opaque LSAs are 1) flooded throughout all
      transit areas, 2) not flooded into stub areas or Not-So-Stubby
      Areas (NSSAs), see [NSSA], from the backbone, and 3) not
      originated by routers into their connected stub areas or NSSAs.
      As with type-5 LSAs, if a type-11 Opaque LSA is received in a stub
      area or NSSA from a neighboring router within the stub area or
      NSSA, the LSA is rejected.

   The link-state ID of the Opaque LSA is divided into an Opaque type
   field (the first 8 bits) and a type-specific ID (the remaining 24
   bits). The packet format of the Opaque LSA is given in Appendix A.
   Section 7 describes Opaque type allocation and assignment.

   The responsibility for proper handling of the Opaque LSA's flooding
   scope is placed on both the sender and receiver of the LSA. The
   receiver must always store a valid received Opaque LSA in its link-
   state database. The receiver must not accept Opaque LSAs that
   violate the flooding scope (e.g., a type-11 (domain-wide) Opaque LSA

is not accepted in a stub area or NSSA). The flooding scope affects
both the synchronization of the link-state database and the flooding
procedure.

The following describes the modifications to these procedures that
are necessary to insure conformance to the Opaque LSA's Scoping
Rules.

3.1. Flooding Opaque LSAs

The flooding of Opaque LSAs MUST follow the rules of flooding scope
as specified in this section. Section 13 of [OSPF] describes the
OSPF flooding procedure. Those procedures MUST be followed as
defined except where modified in this section. The following
describes the Opaque LSA's type-specific flooding restrictions.

   o If the Opaque LSA is type-9 (the flooding scope is link-local) and
      the interface that the LSA was received on is not the same as the
      target interface (e.g., the interface associated with a particular
      target neighbor), the Opaque LSA MUST be discarded and not
      acknowledged. An implementation SHOULD keep track of the IP
      interface associated with each Opaque LSA having a link-local
      flooding scope.

   o If the Opaque LSA is type-10 (the flooding scope is area-local)
      and the area associated with the Opaque LSA (as identified during
      origination or from a received LSA's associated OSPF packet
      header) is not the same as the area associated with the target
      interface, the Opaque LSA MUST be discarded and not acknowledged.
      An implementation SHOULD keep track of the OSPF area associated
      with each Opaque LSA having an area-local flooding scope.

   o If the Opaque LSA is type-11 (the LSA is flooded throughout the
      AS) and the target interface is associated with a stub area or
      NSSA, the Opaque LSA MUST NOT be flooded out the interface. A
      type-11 Opaque LSA that is received on an interface associated
      with a stub area or NSSA MUST be discarded and not acknowledged
      (the neighboring router has flooded the LSA in error).

When opaque-capable routers and non-opaque-capable OSPF routers are
mixed together in a routing domain, the Opaque LSAs are typically not
flooded to the non-opaque-capable routers. As a general design
principle, optional OSPF advertisements are only flooded to those
routers that understand them.

An opaque-capable router learns of its neighbor's opaque capability
at the beginning of the "Database Exchange Process" (see Section 10.6
of [OSPF] regarding receiving Database Description packets from a

neighbor in state ExStart). A neighbor is opaque-capable if and only
if it sets the O-bit in the Options field of its Database Description
packets; the O-bit SHOULD NOT be set and MUST be ignored when
received in packets other than Database Description packets. Using
the O-bit in OSPF packets other than Database Description packets
will result in interoperability issues. The setting of the O-bit is
a "SHOULD NOT" rather than a "MUST NOT" to remain compatible with
earlier specifications.

In the next step of the Database Exchange process, Opaque LSAs are
included in the Database summary list that is sent to the neighbor
(see Sections 3.2 below and 10.3 of [OSPF]) when the neighbor is
opaque capable.

When flooding Opaque LSAs to adjacent neighbors, an opaque-capable
router looks at the neighbor's opaque capability. Opaque LSAs are
only flooded to opaque-capable neighbors. To be more precise, in
Section 13.3 of [OSPF], Opaque LSAs MUST be placed on the link-state
retransmission lists of opaque-capable neighbors and MUST NOT be
placed on the link-state retransmission lists of non-opaque-capable
neighbors. However, when sending Link State Update packets as
multicasts, a non-opaque-capable neighbor may (inadvertently) receive
Opaque LSAs. The non-opaque-capable router will then simply discard
the LSA (see Section 13 of [OSPF] regarding receiving LSAs having
unknown LS types).

Information contained in received Opaque LSAs SHOULD only be used
when the router originating the LSA is reachable. As mentioned in
[OSPFv3], reachability validation MAY be done less frequently than
every SPF calculation. Additionally, routers processing received
Opaque LSAs MAY choose to give priority to processing base OSPF LSA
types over Opaque LSA types.

3.2. Modifications to the Neighbor State Machine

The state machine as it exists in Section 10.3 of [OSPF] remains
unchanged except for the action associated with State: ExStart,
Event: NegotiationDone, which is where the Database summary list is
built. To incorporate the Opaque LSA in OSPF, this action is changed
to the following.

   State(s): ExStart

      Event: NegotiationDone

New state: Exchange

Action: The router MUST list the contents of its entire area
         link-state database in the neighbor Database summary
         list. The area link-state database consists of the
         Router LSAs, Network LSAs, Summary LSAs, type-9 Opaque
         LSAs, and type-10 Opaque LSAs contained in the area
         structure, along with AS External and type-11 Opaque LSAs
         contained in the global structure. AS External and
         type-11 Opaque LSAs MUST be omitted from a virtual
         neighbor's Database summary list. AS External LSAs and
         type-11 Opaque LSAs MUST be omitted from the Database
         summary list if the area has been configured as a stub
         area or NSSA (see Section 3.6 of [OSPF]).

         Type-9 Opaque LSAs MUST be omitted from the Database
         summary list if the interface associated with the
         neighbor is not the interface associated with the Opaque
         LSA (as noted upon reception).

         Any advertisement whose age is equal to MaxAge MUST be
         omitted from the Database summary list. It MUST instead
         be added to the neighbor's link-state retransmission
         list. A summary of the Database summary list will be
         sent to the neighbor in Database Description packets.
         Only one Database Description Packet is allowed to be
         outstanding at any one time. For more detail on the
         sending and receiving of Database Description packets,
         see Sections 10.6 and 10.8 of [OSPF].

4. Protocol Data Structures

   The Opaque option is described herein in terms of its operation on
   various protocol data structures. These data structures are included
   for explanatory uses only. They are not intended to constrain an
   implementation. In addition to the data structures listed below,
   this specification references the various data structures (e.g., OSPF
   neighbors) defined in [OSPF].

   In an OSPF router, the following item is added to the list of global
   OSPF data structures described in Section 5 of [OSPF]:

   o Opaque capability. Indicates whether the router is running the
      Opaque option (i.e., capable of storing Opaque LSAs). Such a
      router will continue to interoperate with non-opaque-capable OSPF
      routers.

4.1. Additions to the OSPF Neighbor Structure

   The OSPF neighbor structure is defined in Section 10 of [OSPF]. In
   an opaque-capable router, the following items are added to the OSPF
   neighbor structure:

   o Neighbor Options. This field was already defined in the OSPF
      specification. However, in opaque-capable routers, there is a new
      option that indicates the neighbor's Opaque capability. This new
      option is learned in the Database Exchange process through
      reception of the neighbor's Database Description packets and
      determines whether Opaque LSAs are flooded to the neighbor. For a
      more detailed explanation of the flooding of the Opaque LSA, see
      Section 3 of this document.

5. Inter-Area Considerations

   As defined above, link-state type-11 Opaque LSAs are flooded
   throughout the Autonomous System (AS). One issue related to such
   AS-scoped Opaque LSAs is that there must be a way for OSPF routers in
   remote areas to check availability of the LSA originator.
   Specifically, if an OSPF router originates a type-11 LSA and, after
   that, goes out of service, OSPF routers located outside of the
   originator's OSPF area have no way of detecting this fact and may use
   the stale information for a considerable period of time (up to 60
   minutes). This could prove to be suboptimal for some applications
   and may result in others not functioning.

   Type-9 Opaque LSAs and type-10 Opaque LSAs do not have this problem
   as a receiving router can detect if the advertising router is
   reachable within the LSA's respective flooding scope. In the case of
   type-9 LSAs, the originating router must be an OSPF neighbor in
   Exchange state or greater. In the case of type-10 Opaque LSAs, the
   intra-area SPF calculation will determine the advertising router's
   reachability.

   There is a parallel issue in OSPF for the AS-scoped AS External LSAs
   (type-5 LSAs). OSPF addresses this by using AS border information
   advertised in AS boundary router (ASBR) Summary LSAs (type-4 LSAs);
   see Section 16.4 of [OSPF]. This same mechanism is reused by this
   document for type-11 Opaque LSAs.

   To enable OSPF routers in remote areas to check availability of the
   originator of link-state type-11 Opaque LSAs, the originators
   advertise themselves as ASBRs. This will enable routers to track the
   reachability of the LSA originator either directly via the SPF
   calculation (for routers in the same area) or indirectly via type-4
   LSAs originated by ABRs (for routers in other areas). It is

important to note that per [OSPF], this solution does not apply to
OSPF stub areas or NSSAs as AS-scoped Opaque LSAs are not flooded
into these area types.

The procedures related to inter-area Opaque LSAs are as follows:

(1) An OSPF router that is configured to originate AS-scope opaque
    LSAs will advertise itself as an ASBR and MUST follow the
    requirements related to setting of the Options field E-bit in
    OSPF LSA headers as specified in [OSPF].

(2) When processing a received type-11 Opaque LSA, the router MUST
    look up the routing table entries (potentially one per attached
    area) for the ASBR that originated the LSA. If no entries exist
    for the ASBR (i.e., the ASBR is unreachable), the router MUST do
    nothing with this LSA. It also MUST discontinue using all Opaque
    LSAs injected into the network by the same originator whenever it
    is detected that the originator is unreachable.

6. Management Considerations

   The updated OSPF MIB, [RFC4750], provides explicit support for Opaque
   LSAs and SHOULD be used to support implementations of this document.
   See Section 12.3 of [RFC4750] for details. In addition to that
   section, implementations supporting [RFC4750] will also include
   Opaque LSAs in all appropriate generic LSA objects, e.g.,
   ospfOriginateNewLsas and ospfLsdbTable.

7. Backward Compatibility

   The solution proposed in this document introduces no interoperability
   issues. In the case that a non-opaque-capable neighbor receives
   Opaque LSAs, per [OSPF], the non-opaque-capable router will simply
   discard the LSA.

   Note that OSPF routers that implement [RFC2370] will continue using
   stale type-11 LSAs even when the LSA originator implements the
   inter-area procedures described in Section 6 of this document.

8. Security Considerations

   There are two types of issues that need be addressed when looking at
   protecting routing protocols from misconfigurations and malicious
   attacks. The first is authentication and certification of routing
   protocol information. The second is denial-of-service attacks
   resulting from repetitive origination of the same router
   advertisement or origination of a large number of distinct
   advertisements resulting in database overflow. Note that both of

these concerns exist independently of a router's support for the
Opaque option.

To address the authentication concerns, OSPF protocol exchanges are
authenticated. OSPF supports multiple types of authentication; the
type of authentication in use can be configured on a per-network-
segment basis. One of OSPF's authentication types, namely the
Cryptographic authentication option, is believed to be secure against
passive attacks and provide significant protection against active
attacks. When using the Cryptographic authentication option, each
router appends a "message digest" to its transmitted OSPF packets.
Receivers then use the shared secret key and received digest to
verify that each received OSPF packet is authentic.

The quality of the security provided by the Cryptographic
authentication option depends completely on the strength of the
message digest algorithm (MD5 is currently the only message digest
algorithm specified), the strength of the key being used, and the
correct implementation of the security mechanism in all communicating
OSPF implementations. It also requires that all parties maintain the
secrecy of the shared secret key. None of the standard OSPF
authentication types provide confidentiality. Nor do they protect
against traffic analysis. For more information on the standard OSPF
security mechanisms, see Sections 8.1, 8.2, and Appendix D of [OSPF].

Repetitive origination of advertisements is addressed by OSPF by
mandating a limit on the frequency that new instances of any
particular LSA can be originated and accepted during the flooding
procedure. The frequency at which new LSA instances may be
originated is set equal to once every MinLSInterval seconds, whose
value is 5 seconds (see Section 12.4 of [OSPF]). The frequency at
which new LSA instances are accepted during flooding is once every
MinLSArrival seconds, whose value is set to 1 (see Section 13,
Appendix B, and G.5 of [OSPF]).

Proper operation of the OSPF protocol requires that all OSPF routers
maintain an identical copy of the OSPF link-state database. However,
when the size of the link-state database becomes very large, some
routers may be unable to keep the entire database due to resource
shortages; we term this "database overflow". When database overflow
is anticipated, the routers with limited resources can be
accommodated by configuring OSPF stub areas and NSSAs. [OVERFLOW]
details a way of gracefully handling unanticipated database
overflows.

In the case of type-11 Opaque LSAs, this document reuses an ASBR
tracking mechanism that is already employed in basic OSPF for type-5
LSAs. Therefore, applying it to type-11 Opaque LSAs does not create
any threats that are not already known for type-5 LSAs.

9. IANA Considerations

   This document updates the requirements for the OSPF Opaque LSA type
   registry. Three following changes have been made:

   1. References to [RFC2370] have been replaced with references to this
      document.

   2. The Opaque type values in the range of 128-255 have been reserved
      for "Private Use" as defined in [RFC5226].

   3. The reference for Opaque type registry value 1, Traffic
      Engineering LSA, has been updated to [RFC3630].

   The registry now reads:

      Open Shortest Path First (OSPF) Opaque Link-State
      Advertisements (LSA) Option Types

      Registries included below:
      - Opaque Link-State Advertisements (LSA) Option Types

      Registry Name: Opaque Link-State Advertisements (LSA) Option Types
      Reference: [RFC5250]
      Range   Registration Procedures   Notes
      --------   --- --------
      0-127   IETF Consensus
      128-255   Private Use

      Registry:
      Value   Opaque Type   Reference
      -------   --- ---------
      1   Traffic Engineering LSA   [RFC3630]
      2   Sycamore Optical Topology Descriptions   [Moy]
      3   grace-LSA   [RFC3623]
      4   Router Information (RI)   [RFC4970]
      5-127   Unassigned
      128-255   Private Use

10. References

10.1. Normative References

   [DEMD]   Moy, J., "Extending OSPF to Support Demand Circuits", RFC
              1793, April 1995.

   [OSPF]   Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

   [RFC2119] Bradner, S., "Key words for use in RFCs to indicate
              requirements levels", BCP 14, RFC 2119, March 1997.

   [RFC4750] Joyal, D., Ed., Galecki, P., Ed., Giacalone, S., Ed.,
              Coltun, R., and F. Baker, "OSPF Version 2 Management
              Information Base", RFC 4750, December 2006.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              May 2008.

10.2. Informative References

   [MOSPF]   Moy, J., "Multicast Extensions to OSPF", RFC 1584, March
              1994.

   [NSSA]   Murphy P., "The OSPF Not-So-Stubby Area (NSSA) Option",
              RFC 3101, January 2003.

   [OSPF-MT] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P.
              Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC
              4915, June 2007.

   [OSPFv3]   Coltun, R., Ferguson, D., Moy, J., and A. Lindem, Ed.,
              "OSPF for IPv6", Work in Progress, May 2008.

   [OVERFLOW] Moy, J., "OSPF Database Overflow", RFC 1765, March 1995.

   [RFC2370] Coltun, R., "The OSPF Opaque LSA Option", RFC 2370, July
              1998.

   [RFC3630] Katz, D., Kompella, K., and D. Yeund, "Traffic Engineering
              (TE) Extensions to OSPF Version 2", RFC 3630, September
              2003.

   [RFC4576] Rosen, E., Psenak, P., and P. Pillay-Esnault, "Using a
              Link State Advertisement (LSA) Options Bit to Prevent
              Looping in BGP/MPLS IP Virtual Private Networks (VPNs)",
              RFC 4576, June 2006.

Appendix A. OSPF Data Formats

   This appendix describes the format of the Options Field followed by
   the packet format of the Opaque LSA.

A.1. The Options Field

   The OSPF Options field is present in OSPF Hello packets, Database
   Description packets, and all link state advertisements. The Options
   field enables OSPF routers to support (or not support) optional
   capabilities, and to communicate their capability level to other OSPF
   routers. Through this mechanism, routers of differing capabilities
   can be mixed within an OSPF routing domain.

   When used in Hello packets, the Options field allows a router to
   reject a neighbor because of a capability mismatch. Alternatively,
   when capabilities are exchanged in Database Description packets a
   router can choose not to flood certain link state advertisements to a
   neighbor because of its reduced functionality. Lastly, listing
   capabilities in link state advertisements allows routers to forward
   traffic around reduced functionality routers by excluding them from
   parts of the routing table calculation.

   All 8 bits of the OSPF Options field have been assigned, although
   only the O-bit is described completely by this document. Each bit is
   described briefly below. Routers SHOULD reset (i.e., clear)
   unrecognized bits in the Options field when sending Hello packets or
   Database Description packets and when originating link state
   advertisements. Conversely, routers encountering unrecognized Option
   bits in received Hello Packets, Database Description packets, or link
   state advertisements SHOULD ignore the capability and process the
   packet/advertisement normally.

```
             +--------------------------------------+
             | DN | O | DC | EA | N/P | MC | E | MT |
             +--------------------------------------+
```

                         The Options Field

   MT-bit
         This bit describes the router's multi-topology link-excluding
         capability, as described in [OSPF-MT].

   E-bit
         This bit describes the way AS-External LSAs are flooded, as
         described in Sections 3.6, 9.5, 10.8, and 12.1.2 of [OSPF].

MC-bit
     This bit describes whether IP multicast datagrams are forwarded
     according to the specifications in [MOSPF].

N/P-bit
     This bit describes the handling of Type-7 LSAs, as specified in
     [NSSA].

DC-bit
     This bit describes the router's handling of demand circuits, as
     specified in [DEMD].

EA-bit
     This bit describes the router's willingness to receive and
     forward External-Attributes-LSAs. While defined, the documents
     specifying this bit have all expired. The use of this bit may
     be deprecated in the future.

O-bit
     This bit describes the router's willingness to receive and
     forward Opaque LSAs as specified in this document.
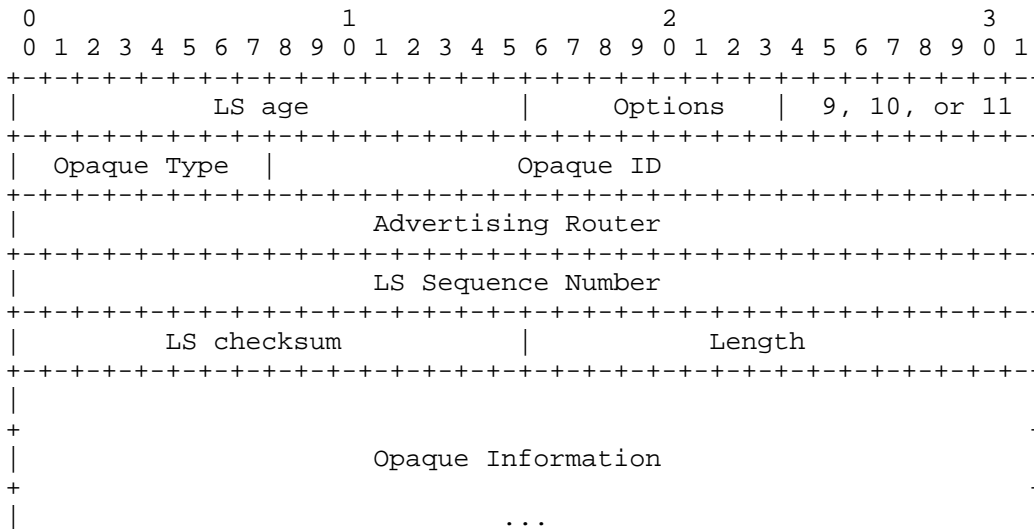
DN-bit
     This bit is used to prevent looping in BGP/MPLS IP VPNs, as
     specified in [RFC4576].

A.2. The Opaque LSA

   Opaque LSAs are Type 9, 10, and 11 link state advertisements. These
   advertisements MAY be used directly by OSPF or indirectly by some
   application wishing to distribute information throughout the OSPF
   domain. The function of the Opaque LSA option is to provide for
   future OSPF extensibility.

   Opaque LSAs contain some number of octets (of application-specific
   data) padded to 32-bit alignment. Like any other LSA, the Opaque LSA
   uses the link-state database distribution mechanism for flooding this
   information throughout the topology. However, the Opaque LSA has a
   flooding scope associated with it so that the scope of flooding may
   be link-local (type-9), area-local (type-10), or the entire OSPF
   routing domain (type-11). Section 3 of this document describes the
   flooding procedures for the Opaque LSA.

```
         0                   1                   2                   3
         0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |            LS age              |    Options    | 9, 10, or 11 |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |  Opaque Type  |               Opaque ID                       |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                      Advertising Router                       |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                      LS Sequence Number                       |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |         LS checksum           |           Length             |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |                                                               |
        +                                                               +
        |                      Opaque Information                       |
        +                                                               +
        |                              ...                              |
```

Link-State Type

   The link-state type of the Opaque LSA identifies the LSA's range
   of topological distribution. This range is referred to as the
   flooding scope. The following explains the flooding scope of each
   of the link-state types.

   o A value of 9 denotes a link-local scope. Opaque LSAs with a
      link-local scope MUST NOT be flooded beyond the local
      (sub)network.

   o A value of 10 denotes an area-local scope. Opaque LSAs with an
      area-local scope MUST NOT be flooded beyond their area of
      origin.

   o A value of 11 denotes that the LSA is flooded throughout the
      Autonomous System (e.g., has the same scope as type-5 LSAs).
      Opaque LSAs with AS-wide scope MUST NOT be flooded into stub
      areas or NSSAs.

Syntax of the Opaque LSA's Link-State ID

   The link-state ID of the Opaque LSA is divided into an Opaque Type
   field (the first 8 bits) and an Opaque ID (the remaining 24 bits).
   See section 7 of this document for a description of Opaque type
   allocation and assignment.

Authors' Addresses

   Lou Berger
   LabN Consulting, L.L.C.
   EMail: lberger@labn.net

   Igor Bryskin
   ADVA Optical Networking Inc
   7926 Jones Branch Drive
   Suite 615
   McLean, VA 22102
   EMail: ibryskin@advaoptical.com

   Alex Zinin
   Alcatel-Lucent
   750D Chai Chee Rd #06-06
   Technopark@ChaiChee
   Singapore, 469004
   EMail: alex.zinin@alcatel-lucent.com

   Rob Coltun
   Acoustra Productions
   3204 Brooklawn Terrace
   Chevy Chase, MD 20815
   USA