                   OSPF Link-Local Signaling (LLS) Extensions for
                       Local Interface ID Advertisement

Abstract

   Every OSPF interface is assigned an Interface ID that uniquely
   identifies the interface on the router. In some cases, it is useful
   to know the assigned Interface ID on the remote side of the adjacency
   (Remote Interface ID).

   This document describes the extensions to OSPF link-local signaling
   (LLS) to advertise the Local Interface ID.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8510.

Copyright Notice

Table of Contents

1. Introduction

   Every OSPF interface is assigned an Interface ID that uniquely
   identifies the interface on the router. [RFC2328] uses this
   Interface ID in the Router Link State Advertisement (Router-LSA) Link
   Data for unnumbered links and uses the value of the MIB-II ifIndex
   [RFC2863]. [RFC4203] refers to these Interface IDs as the Link
   Local/Remote Identifiers and defines a way to advertise and use them
   for GMPLS purposes. [RFC8379] defines a way to advertise Local/
   Remote Interface IDs in the OSPFv2 Extended Link Opaque LSA.

   There is a known OSPFv2 protocol problem in verifying the
   bidirectional connectivity with parallel unnumbered links. If there
   are two parallel unnumbered links between a pair of routers and each
   link is only advertised from a single direction, such two
   unidirectional parallel links could be considered as a valid single
   bidirectional link during the OSPF route computation on some other
   router. If each link is advertised with both its Local and Remote
   Interface IDs, the advertisement of each link from both sides of
   adjacency can be verified by cross-checking the Local and Remote
   Interface IDs of both advertisements.

   From the perspective of the advertising router, the Local Interface
   ID is a known value. However, the Remote Interface ID needs to be
   learned before it can be advertised. [RFC4203] suggests using the TE
   Link Local LSA [RFC3630] to communicate the Local Interface ID to
   neighbors on the link. Though such a mechanism works, it has some
   drawbacks.

   This document proposes an extension to OSPF link-local signaling
   (LLS) [RFC5613] to advertise the Local Interface ID.

1.1. Interface ID Exchange Using Link Local TE Opaque LSA

Usage of the Link Local TE Opaque LSA to propagate the Local
Interface ID to the neighbors on the link is described in [RFC4203].
This mechanism has the following problems:

o LSAs can only be flooded over an existing adjacency that is in
   Exchange state or greater. The adjacency state machine progresses
   independently on each side of the adjacency and, as such, may
   reach the Full state on one side before the Link Local TE Opaque
   LSA arrives. The consequence of this is that the link can be
   initially advertised without the Remote Interface ID. Later, when
   the Link Local TE Opaque LSA arrives, the link must be advertised
   again but this time with the valid Remote Interface ID.
   Implementations may choose to wait before advertising the link,
   but there is no guarantee that the neighbor will ever advertise
   the Link Local TE Opaque LSA with the Interface ID. In summary,
   the existing mechanism does not guarantee that the Remote
   Interface ID is known at the time the link is advertised.

o The Link Local TE Opaque LSA is defined for MPLS Traffic
   Engineering, but the knowledge of the Remote Interface ID is
   useful also for cases where MPLS TE is not used. One example is
   the mentioned lack of a valid 2-way connectivity check for
   parallel point-to-point links between OSPF routers.

1.2. 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.

2. Interface ID Exchange Using OSPF LLS

To address the problems described earlier and to allow the Interface
ID exchange to be part of the neighbor discovery process, we propose
to extend OSPF link-local signaling to advertise the Local Interface
ID in OSPF Hello and Database Description (DD) packets.

2.1. Local Interface ID TLV

   The Local Interface ID TLV is an LLS TLV. It has the following
   format:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Local Interface ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
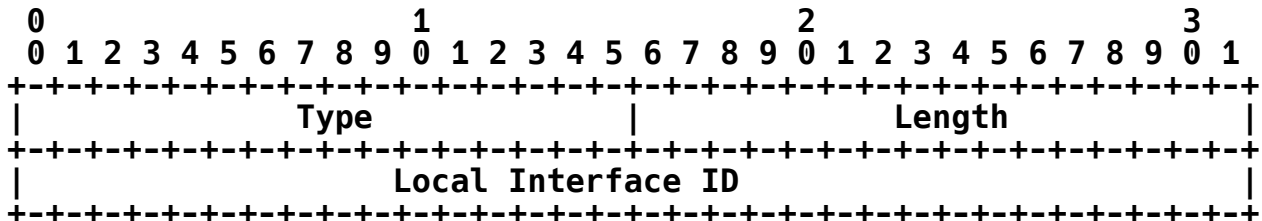
      Type: 18

      Length: 4 octets

      Local Interface ID: The value of the Local Interface ID.

   Local Interface ID TLV signaling using LLS is applicable to all OSPF
   interface types other than virtual links.

3. Backward Compatibility with RFC 4203

   If the Local Interface ID signaling via the Link Local TE Opaque LSA
   is supported in addition to the new LLS mechanism, implementations
   that support Local Interface ID signaling using LLS MUST prefer the
   Local Interface ID value received through LLS over the value received
   through the Link Local TE Opaque LSA if both are received from the
   same OSPF router.

   Implementations that support Local Interface ID signaling via the
   Link Local TE Opaque LSA MAY continue to do so to ensure backward
   compatibility. If they also support Local Interface ID signaling
   using LLS as described in the document, they MUST signal the same
   Local Interface ID via both mechanisms.

   During the rare conditions in which the Local Interface ID changes, a
   timing interval may exist where the received values of the Local
   Interface ID advertised through LLS and the Link Local TE Opaque LSA
   may differ. Such a situation is temporary, and received values via
   both mechanisms should become equal as soon as the next Hello and/or
   Link Local TE Opaque LSA is regenerated by the originator.

4. IANA Considerations

   IANA has allocated the following code point in the "Link Local
   Signalling TLV Identifiers (LLS Types)" subregistry of the "Open
   Shortest Path First (OSPF) Link Local Signalling (LLS) - Type/Length/
   Value Identifiers (TLV)" registry.

   18 - Local Interface ID TLV

5. Security Considerations

   The security considerations for "OSPF Link-Local Signaling" [RFC5613]
   also apply to the Local Interface ID TLV described in this document.
   The current usage of a neighbor's Local Interface ID is to
   disambiguate parallel links between OSPF routers. Hence,
   modification of the advertised Local Interface ID TLV may result in
   the wrong neighbor Interface ID being advertised in the OSPFv2
   Extended Link Opaque LSA [RFC7684] and could prevent the link from
   being used. If authentication is being used in the OSPF routing
   domain [RFC5709][RFC7474], then the Cryptographic Authentication TLV
   [RFC5613] SHOULD also be used to protect the contents of the LLS
   block.

   Receiving a malformed LLS Local Interface ID TLV MUST NOT result in a
   hard router or OSPF process failure. The reception of malformed LLS
   TLVs or sub-TLVs SHOULD be logged, but such logging MUST be rate-
   limited to prevent denial-of-service (DoS) attacks.

   The Interface ID is assigned by the advertising OSPF router as a
   locally unique identifier and need not be unique in any broader
   context; it is not expected to contain any information about the
   device owner or traffic transiting the device, so there are no
   privacy concerns associated with its advertisement.

6. References

6.1. Normative References

   [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>.

   [RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328,
              DOI 10.17487/RFC2328, April 1998,
              <https://www.rfc-editor.org/info/rfc2328>.

   [RFC3630] Katz, D., Kompella, K., and D. Yeung, "Traffic Engineering
              (TE) Extensions to OSPF Version 2", RFC 3630,
              DOI 10.17487/RFC3630, September 2003,
              <https://www.rfc-editor.org/info/rfc3630>.

   [RFC4203] Kompella, K., Ed. and Y. Rekhter, Ed., "OSPF Extensions in
              Support of Generalized Multi-Protocol Label Switching
              (GMPLS)", RFC 4203, DOI 10.17487/RFC4203, October 2005,
              <https://www.rfc-editor.org/info/rfc4203>.

   [RFC5613] Zinin, A., Roy, A., Nguyen, L., Friedman, B., and
              D. Yeung, "OSPF Link-Local Signaling", RFC 5613,
              DOI 10.17487/RFC5613, August 2009,
              <https://www.rfc-editor.org/info/rfc5613>.

   [RFC7684] Psenak, P., Gredler, H., Shakir, R., Henderickx, W.,
              Tantsura, J., and A. Lindem, "OSPFv2 Prefix/Link Attribute
              Advertisement", RFC 7684, DOI 10.17487/RFC7684, November
              2015, <https://www.rfc-editor.org/info/rfc7684>.

   [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>.

   [RFC8379] Hegde, S., Sarkar, P., Gredler, H., Nanduri, M., and
              L. Jalil, "OSPF Graceful Link Shutdown", RFC 8379,
              DOI 10.17487/RFC8379, May 2018,
              <https://www.rfc-editor.org/info/rfc8379>.

6.2. Informative References

   [RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group
              MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000,
              <https://www.rfc-editor.org/info/rfc2863>.

   [RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M.,
              Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic
              Authentication", RFC 5709, DOI 10.17487/RFC5709, October
              2009, <https://www.rfc-editor.org/info/rfc5709>.

   [RFC7474] Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, Ed.,
              "Security Extension for OSPFv2 When Using Manual Key
              Management", RFC 7474, DOI 10.17487/RFC7474, April 2015,
              <https://www.rfc-editor.org/info/rfc7474>.

Authors' Addresses

   Peter Psenak (editor)
   Cisco Systems, Inc.
   Apollo Business Center
   Mlynske nivy 43
   Bratislava 821 09
   Slovakia

   Email: ppsenak@cisco.com

   Ketan Talaulikar
   Cisco Systems, Inc.
   S.No. 154/6, Phase I, Hinjawadi
   Pune, Maharashtra 411 057
   India

   Email: ketant@cisco.com

   Wim Henderickx
   Nokia
   Copernicuslaan 50
   Antwerp 2018
   Belgium

   Email: wim.henderickx@nokia.com

   Padma Pillay-Esnault
   Huawei USA
   2330 Central Expressway
   Santa Clara, CA 95050
   United States of America

   Email: padma@huawei.com