                     Passive Interface Attribute
                draft-wang-lsr-passive-interface-attribute-03

Abstract

   This document describes the mechanism that can be used to
   differentiate the passive interfaces from the normal interfaces
   within ISIS or OSPF domain.

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 https://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 1, 2021.

Table of Contents

1. Introduction

   Passive interfaces are used commonly within an operators enterprise
   or service provider networks. One of the most common use cases for
   passive interface is in a data center Layer 2 and Layer 3 TOR(Top of
   Rack) switch where the inter connected link between the TOR switches
   and uplink to the Core switch are only a few links and a majority of
   the links are Layer 3 VLAN Switched Virtual Interface Default
   Gateways trunked betwen the TOR switches servicing Layer 2 broadcast
   domains. In this scenario all the VLANs are made passive as it is
   recommended to limit the number of network LSAs between routers and
   switches to avoid unnecessary hello processing overhead.

   Another common use case is an inter-as routing scenario where the
   same routing protocol but diffent IGP instance is running between the
   adjacent BGP domains. Using passive interface on the inter-as
   tiepoint connections can ensure that prefixes contained within a
   domain are only reachable within the domain itself and not allow the
   link state database to be merged between domain which could result in
   undesirable consequences.

   For operator which runs different IGP domains that interconnect with
   each other, there is desire to obtain the inter-as topology
   information as described in
   [I-D.ietf-idr-bgpls-inter-as-topology-ext]. If the router that runs
   BGP-LS is within one IGP domain and can distinguish passive
   interfaces from other interfaces with transit neighbor, it is then
   easy for the router to report these passive links using BGP-LS to
   centralized PCE controller.

But OSPF and ISIS have no capabilities to flag such passive
interface.

This document defines the protocol extension for OSPF and ISIS for
the prefix that comes from passive interface.

[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](). Scenario Description

Figure 1 illustrates the topology scenario when ISIS/OSPF is running
in different domain. B1, B3 are border routers within IGP domain A,
B2, B4 are border routers within domain B. S1-S4 are the internal
routers within domain A, T1-T4 are the internal routers within domain
B. The two domain are interconnected via the links between B1/B2 and
B3/B4.

Passive interfaces are enabled in the links between B1/B2 and B3/B4
respectively. For domain A and B, the S2/T1 router that runs ISIS/
OSPF can't extract the passives links from the normal links and
report it to PCE controller via the BGP-LS protocol. They can only
judge the passive interfaces from other characteristics, such as no
IGP neighbor on this link. Such judgement can extract these passive
links but it is not accurate, because it covers also the situation
when there are some issues to establish the ISIS adjacency/OSPF
neighbor but not the passive interface.

For passive interfaces that are used in the edge router or switches
which connects the server, for example in the router S1/S4 and T2/T4
in Figure 1, knowing these interfaces are correctly configured will
also benefit the management of them.

The method to label these passive interfaces explicitly is necessary
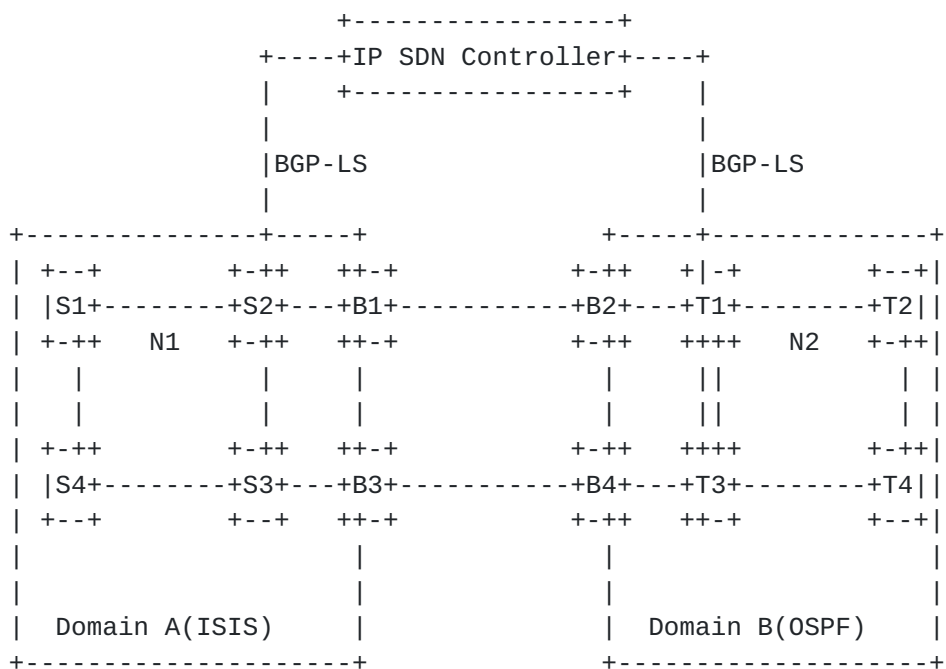then.

```
                        +----------------+
                  +----+IP SDN Controller+----+
                  |     +----------------+     |
                  |                            |
                  |BGP-LS                      |BGP-LS
                  |                            |
        +---------------+-----+        +-----+--------------+
        | +--+        +-++  ++-+       +-++  +|-+        +--+|
        | |S1+--------+S2+---+B1+-----------+B2+---+T1+--------+T2||
        | +-++   N1   +-++  ++-+       +-++  ++++   N2   +-++|
        | |  |         |     |          |    ||          | |
        | |  |         |     |          |    ||          | |
        | +-++        +-++  ++-+       +-++  ++++        +-++|
        | |S4+--------+S3+---+B3+-----------+B4+---+T3+--------+T4||
        | +--+        +--+  ++-+       +-++  ++-+        +--+|
        |               |              |               |
        |               |              |               |
        |   Domain A(ISIS)  |          |  Domain B(OSPF)   |
        +--------------------+         +--------------------+
```

                 Figure 1: Inter-AS Domain Scenarios

4. Passive Interface Attribute

4.1. ISIS Passive Interface Attribute

   [RFC7794] defines the "IPv4/IPv6 Extended Reachability Attribute
   Flags" sub-TLV to advertise the additional flags associated with a
   given prefix advertisement. We propose new bit(Bit 5 is desired) to
   be assigned by the IANA for the passive interface attribute, as
   illustrated in Figure2:

```
                 0 1 2 3 4 5 6 7
                 +-+-+-+-+-+-+-+-+
                 |X|R|N|E|A|U
                 +-+-+-+-+-+-+-+-+
            Figure 2: Prefix Attribute Flags
```

       U-flag: Unactive Flag(Bit 5)
               Set for local interface that is configured as passive
   interface.

   When the interfaces on one router be configured as the passive
   interface, the U-flag bit will be set in the "IPv4/IPv6 Extended
   Reachability Attribute Flags" sub-TLV. This sub-TLV will be included
   in the TLV 135, TLV 235, TLV 236 and TLV 237 as necessary and be
   flooded within the ISIS domain.

4.2. OSPF Passive Interface Attribute

   [RFC5340] defines the "Prefix Option field" in "Intra-Area-Prefix-
   LSAs" LSA to describe the prefix capabilities. The bits in this
   field can be defined to flag the prefix is coming from the passive
   interface. We propose new bit(Bit 1 is desired) to be assigned by
   the IANA for the passive interface, as illustrated in Figure 3:

```
                0  1  2  3  4  5  6  7
               +--+--+--+--+--+-+--+--+
               |  |  | U|DN| P|x|LA|NU|
               +--+--+--+--+--+-+--+--+
```

                 Figure 3: The PrefixOptions Field

        U-flag: Unactive Flag(Bit 2)
                 Set for local interface that is configured as passive
interface.

   When the interfaces on one router be configured as the passive
   interface, the U-flag bit will be set in the "Prefix Option field" of
   Intra-Area-Prefix-LSAs.

   The router receives such advertisement can then easily distinguish
   the passive interfaces from the normal interface, and reports them to
   the PCE controller if it run the BGP-LS protocol.

5. Security Considerations

   Security concerns for ISIS are addressed in [RFC5304] and[RFC5310]

   Advertisement of the additional information defined in this document
   introduces no new security concerns.

6. IANA Considerations

   IANA is requested to allocate the U-bit (bit position 5 is desired)
   from the "Bit Values for Prefix Attribute Flags Sub-TLV" registry of
   ISIS TLV codepoint.

   IANA is requested to allocate the U-bit(bit position 2 is desired)
   from the "OSPFv3 Prefix Options" registry of OSPFv3 Parameters
   codepoint.

7. Acknowledgement

   Thanks Shunwan Zhang, Tony Li, Les Ginsberg and Robert Raszuk for
   their suggestions and comments on this idea.

8. References

8.1. 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>.

   [RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic
              Authentication", RFC 5304, DOI 10.17487/RFC5304, October
              2008, <https://www.rfc-editor.org/info/rfc5304>.

   [RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R.,
              and M. Fanto, "IS-IS Generic Cryptographic
              Authentication", RFC 5310, DOI 10.17487/RFC5310, February
              2009, <https://www.rfc-editor.org/info/rfc5310>.

   [RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF
              for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008,
              <https://www.rfc-editor.org/info/rfc5340>.

   [RFC7794] Ginsberg, L., Ed., Decraene, B., Previdi, S., Xu, X., and
              U. Chunduri, "IS-IS Prefix Attributes for Extended IPv4
              and IPv6 Reachability", RFC 7794, DOI 10.17487/RFC7794,
              March 2016, <https://www.rfc-editor.org/info/rfc7794>.

8.2. Informative References

   [I-D.ietf-idr-bgpls-inter-as-topology-ext]
              Wang, A., Chen, H., Talaulikar, K., and S. Zhuang, "BGP-LS
              Extension for Inter-AS Topology Retrieval", draft-ietf-
              idr-bgpls-inter-as-topology-ext-08 (work in progress),
              April 2020.

Authors' Addresses

   Aijun Wang
   China Telecom
   Beiqijia Town, Changping District
   Beijing 102209
   China

   Email: wangaj3@chinatelecom.cn

   Zhibo Hu
   Huawei Technologies
   Huawei Bld., No.156 Beiqing Rd.
   Beijing 100095
   China

   Email: huzhibo@huawei.com

   Gyan S. Mishra
   Verizon Inc.
   13101 Columbia Pike
   Silver Spring MD 20904
   United States of America

   Email: gyan.s.mishra@verizon.com