Network Working Group
Request for Comment: 5523
Category: Experimental

L. Berger
LabN Consulting, LLC
April 2009

OSPFv3-Based Layer 1 VPN Auto-Discovery

Status of This Memo

Copyright Notice

Abstract

This document defines an OSPFv3-based (Open Shortest Path First version 3) Layer 1 Virtual Private Network (L1VPN) auto-discovery mechanism. This document parallels the existing OSPF version 2 L1VPN auto-discovery mechanism. The notable functional difference is the support of IPv6.

Table of Contents

1. Introduction

This document defines an OSPFv3-based (Open Shortest Path First version 3) Layer 1 Virtual Private Network (L1VPN) auto-discovery mechanism. This document parallels the existing OSPF version 2 L1VPN auto-discovery mechanism. The notable functional difference is the support of IPv6.

1.1. Terminology

The reader of this document should be familiar with the terms used in [RFC4847] and [RFC5251]. The reader of this document should also be familiar with [RFC5340], [RFC5329], and [RFC5252]. In particular, the following terms:

L1VPN Layer 1 Virtual Private Network

CE Customer (edge) network element directly connected to the Provider network (terminates one or more links to one or more PEs); it is also connected to one or more Cs and/or other CEs.

C Customer network element that is not connected to the Provider network but is connected to one or more other Cs and/or CEs.

PE Provider (edge) network element directly connected to one or more Customer networks (terminates one or more links to one or more CEs associated with the same or different L1VPNs); it is also connected to one or more Ps and/or other PEs.

P Provider (core) network element that is not directly connected to any of Customer networks; P is connected to one or more other Ps and/or PEs.

LSA OSPF Link State Advertisement.

LSDB Link State Database: a data structure supported by an IGP speaker.

PIT Port Information Table.

CPI Customer Port Identifier.

PPI Provider Port Identifier.

1.2. 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].

1.3. Overview

The framework for Layer 1 VPNs is described in [RFC4847]. Basic mode operation is further defined in [RFC5251]. [RFC5251] identifies the information that is necessary to map customer information (port identifiers) to provider information (identifiers). It also states that this mapping information may be provided via provisioning or via an auto-discovery mechanism. [RFC5252] provides such an auto-discovery mechanism using Open Shortest Path First (OSPF) version 2. This document provides the same functionality using OSPF version 3 and adds support for IPv6.

Figure 1 shows the L1VPN basic service being supported using OSPF-based L1VPN auto-discovery. This figure shows two PE routers interconnected over a GMPLS backbone. Each PE is attached to three CE devices belonging to three different Layer 1 VPNs. In this network, OSPF is used to provide the VPN membership, port mapping, and related information required to support basic mode operation.

```
                  PE                        PE
               +---------+             +--------------+
   +--------+  | +------+|             | +----------+ | +--------+
   |  VPN-A |  | |VPN-A ||             | |  VPN-A   | | |  VPN-A |
   |   CE1  |--| |PIT   ||  OSPF LSAs  | |  PIT     | |-|   CE2  |
   +--------+  | |      ||<----------->| |          | | +--------+
               | +------+| Distribution| +----------+ |
               |         |             |              |
   +--------+  | +------+|   -------   | +----------+ | +--------+
   | VPN-B  |  | |VPN-B ||             | |   VPN-B  | | |  VPN-B |
   |  CE1   |--| |PIT   ||--( GMPLS )--| |   PIT    | |-|   CE2  |
   +--------+  | |      ||  (Backbone) | |          | | +--------+
               | +------+|   --------  | +----------+ |
               |         |             |              |
   +--------+  | +-----+ |             | +----------+ | +--------+
   | VPN-C  |  | |VPN-C| |             | |   VPN-C  | | |  VPN-C |
   |  CE1   |--| |PIT  | |             | |   PIT    | |-|   CE2  |
   +--------+  | |     | |             | |          | | +--------+
               | +-----+ |             | +----------+ |
               +---------+             +--------------+
```

Figure 1: OSPF Auto-Discovery for L1VPNs

The approach used in this document to provide OSPFv3-based L1VPN auto-discovery uses a new type of Link State Advertisement (LSA), which is referred to as an OSPFv3 L1VPN LSA. The OSPFv3 L1VPN LSA carries information in TLV (type, length, value) structures. An L1VPN-specific TLV is defined below to propagate VPN membership and port information. This TLV is referred to as the L1VPN Info TLV.

The OSPFv3 L1VPN LSA may also carry Traffic Engineering (TE) TLVs; see [RFC3630], [RFC4203], and [RFC5329].

2. OSPFv3 L1VPN LSA and Its TLVs

This section defines the OSPFv3 L1VPN LSA and its TLVs.

2.1. OSPFv3 L1VPN LSA

The format of a OSPFv3 L1VPN LSA is as follows:

```
    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              |          LS type              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Link State ID                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Advertising Router                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    LS sequence number                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        LS checksum            |            length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           L1VPN Info TLV                      |
   |                             ...                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                            TE Link TLV                        |
   |                             ...                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

LS age

As defined in [RFC5340].

LS type

As defined in [RFC5340]. The U-bit MUST be set to 1, and the S1 and S2 bits MUST be set to indicate either area or Autonomous System (AS) scoping. The LSA Function Code portion of this field MUST be set to 14, i.e., the OSPFv3 L1VPN LSA.

Advertising Router

As defined in [RFC5340].

LS Sequence Number

As defined in [RFC5340].

LS checksum

As defined in [RFC5340].

Length

As defined in [RFC5340].

L1VPN Info TLV

A single L1VPN Info TLV, as defined in Section 2.2 of [RFC5252] or Section 2.2 of this document, MUST be present. If more than one L1VPN Info TLV is present, only the first TLV is processed and the others MUST be ignored on receipt. If no L1VPN Info TLV is present, the LSA is processed (and flooded) as normal, but the L1VPN PIT table MUST NOT be modified in any way.

TE Link TLV

A single TE Link TLV MAY be included in an OSPFv3 L1VPN LSA. When an L1VPN IPv4 Info TLV is present, a single TE Link TLV as defined in [RFC3630] and [RFC4203] MAY be included. When an L1VPN IPv6 Info TLV is present, a single TE Link TLV as defined in [RFC5329] MAY be included.

2.2. L1VPN IPv6 INFO TLV

The following TLV is introduced:

Name: L1VPN IPv6 Info
Type: 32768
Length: Variable

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           L1VPN TLV Type      |         L1VPN TLV Length      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 L1VPN Globally Unique Identifier              |
   |                              ...                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          PE TE Address                        |
   |                              ...                              |
   |                              ...                              |
   |                              ...                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Link-Local Identifier                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                              ...                              |
   |                 L1VPN Auto-Discovery Information              |
   +                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                              .|           Padding             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

L1VPN TLV Type

The type of the TLV (see above).

TLV Length

The length of the TLV in bytes, excluding the four (4) bytes of the TLV header and, if present, the length of the Padding field.

L1VPN Globally Unique Identifier

As defined in [RFC5251].

PE TE Address

This field MUST carry an address that has been advertised by the LSA originator per [RFC5329] and is either the Router IPv6 Address TLV or Local Interface IPv6 Address link sub-TLV. It will typically carry the TE Router Address.

Link-Local Identifier

This field is used to support unnumbered links. When an unnumbered PE TE link is represented, this field MUST contain a value advertised by the LSA originator per [RFC5340] in a Router LSA. When a numbered link is represented, this field MUST be set to zero (0).

L1VPN Auto-Discovery Information

As defined in [RFC5251].

Padding

A field of variable length and of sufficient size to ensure that the TLV is aligned on a 4-byte boundary. This field is only required when the L1VPN Auto-Discovery Information field is not 4-byte aligned. This field MUST be less than 4 bytes long, and MUST NOT be present when the size of L1VPN Auto-Discovery Information field is 4-byte aligned.

3. OSPFv3 L1VPN LSA Advertising and Processing

PEs advertise local <CPI, PPI> tuples in OSPFv3 L1VPN LSAs containing L1VPN Info TLVs. Each PE MUST originate a separate OSPFv3 L1VPN LSA with area or AS flooding scope, based on configuration, for each local CE-PE link. The LSA MUST be originated each time a PE restarts and every time there is a change in the PIT entry associated with a local CE-PE link. The LSA MUST include a single L1VPN Info TLV and MAY include a single TE Link TLV. The TE Link TLV carries TE attributes of the associated CE-PE link. Note that because CEs are outside of the provider TE domain, the attributes of CE-PE links are not advertised via normal OSPF-TE procedures as described in [RFC5329]. If more than one L1VPN Info TLVs and/or TE Link TLVs are found in the LSA, the subsequent TLVs SHOULD be ignored by the receiving PEs.

Every time a PE receives a new, removed, or modified OSPFv3 L1VPN LSA, the PE MUST check whether it maintains a PIT associated with the L1VPN specified in the L1VPN Globally Unique Identifier field. If this is the case (the appropriate PIT will be found if one or more local CE-PE links that belong to the L1VPN are configured), the PE SHOULD add, remove, or modify the PIT entry associated with each of the advertised CE-PE links accordingly. (An implementation MAY choose to not remove or modify the PIT according to local policy or management directives.) Thus, in the normal steady-state case, all PEs associated with a particular L1VPN will have identical local PITs for an L1VPN.

4. Backward Compatibility

Neither the TLV nor the LSA introduced in this document present any interoperability issues. Per [RFC5340], and due to the U-bit being set, OSPFv3 speakers that do not support the OSPFv3 L1VPN LSA (Ps for example) just participate in the LSA's flooding process but should ignore the LSA's contents.

5. Manageability Considerations

The principal concern in operating an auto-discovery mechanism for an L1VPN is that the PE needs to be configured with information about which VPNs it supports. This information can be discovered from the CEs using some form of membership negotiation, but is more likely to be directly configured by the operator as described in [RFC4847], [RFC5251], and [RFC5253]. No standardized mechanisms to configure this information have been defined, and it is a matter for individual implementations with input from operator policy how a PE is told which L1VPNs it supports. It is probable that configuration of this information is closely tied to the configuration of CE-facing ports on the PE, which in turn causes PITs to be established in the PE.

Additionally, it may be of value to an operator to view the L1VPN membership information that has been learned by a PE. An implementation may supply this information through a proprietary interface, or may allow it to be inspected through the OSPFv3 MIB module [OSPFv3-MIB] or the Traffic Engineering Database MIB [TED-MIB].

Note that the operation of the control plane has no impact on IP network traffic because all of the user data is in Layer 1, while the control plane is necessarily out of band in a Data Communications Network (DCN).

5.1. Coexistence with and Migration from OSPFv2

It is expected that only a single routing protocol instance will be used to operate auto-discovery within an L1VPN at any time. Thus, coexistence issues only apply to the migration from OSPFv2 to OSPFv3 and can be expected to be transient.

Migration from OSPFv2 to OSPFv3 would be a once-only event for any network and would probably depend on the migration of the routing protocol used within the network for normal GMPLS procedures. The migration process would not be any different from the process used to migrate the normal GMPLS routing protocol. The steps to follow are clearly a matter for the operator of the network and are not a matter for standardization, but the following sequence is provided to illustrate the potential actions:

1. Assign IPv6 addresses to all control plane and data plane resources.

2. Install and enable OSPFv3 on all controllers.

3. Use OSPFv3 to advertise IPv4 and IPv6 resource identifiers.

4. Manually verify the advertised membership and topology information from the OSPFv2 and OSPFv3 databases.

5. Start a maintenance window where data continues to flow, but no L1VPN connections can be changed.

6. Cut over to the OSPFv3 membership and topology information.

7. Close the maintenance window.

8. Turn off OSPFv2.

9. Remove/disable the IPv4 address for all control plane and data plane resources.

6. Security Considerations

The approach presented in this document describes how PEs dynamically learn L1VPN specific information. Mechanisms to deliver the VPN membership information to CEs are explicitly out of scope of this document. Therefore, the security issues raised in this document are limited to within the OSPF domain.

This defined approach reuses mechanisms defined in [RFC5340]. Therefore, the same security approaches and considerations apply to this approach. OSPF provides several security mechanisms that can be applied. Specifically, OSPF supports multiple types of authentication, limits the frequency of LSA origination and acceptance, and provides techniques to avoid and limit the impact of database overflow. In cases were end-to-end authentication is desired, OSPF's neighbor-to-neighbor authentication approach can be augmented with an approach similar to the experimental extension to OSPF, see [RFC2154], which supports the signing and authentication of LSAs.

7. IANA Considerations

IANA has assigned an OSPFv3 LSA Function Code as described in Section 2.1 of this document. IANA has made an assignment in the form:

Value	OSPFv3 LSA type function Type	Reference
14	OSPFv3 L1VPN LSA	[RFC5523]

8. Acknowledgment

This document was created at the request of Pasi Eronen. Adrian Farrel and Acee Lindem provided valuable reviews of this document. Adrian also provided the text for Section 5.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

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

[RFC4203] Kompella, K., Ed., and Y. Rekhter, Ed., "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, October 2005.

[RFC5251] Fedyk, D., Ed., Rekhter, Y., Ed., Papadimitriou, D., Rabbat, R., and L. Berger, "Layer 1 VPN Basic Mode", RFC 5251, July 2008.

[RFC5252] Bryskin, I. and L. Berger, "OSPF-Based Layer 1 VPN Auto-Discovery", RFC 5252, July 2008.

[RFC5329] Ishiguro, K., Manral, V., Davey, A., and A. Lindem, Ed., "Traffic Engineering Extensions to OSPF Version 3", RFC 5329, September 2008.

9.2. Informative References

[OSPFv3-MIB] Joyal, D., Ed. and V. Manral, Ed., "Management Information Base for OSPFv3", Work in Progress, November 2008.

[RFC2154] Murphy, S., Badger, M., and B. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.

[RFC4847] Takeda, T., Ed., "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

[RFC5253] Takeda, T., Ed., "Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode", RFC 5253, July 2008.

[TED-MIB] Miyazawa, M., Otani, T., Nadeau, T., and K. Kumaki, "Traffic Engineering Database Management Information Base in support of MPLS-TE/GMPLS", Work in Progress, January 2009.

Author's Address

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