

Network Work Group
Internet-Draft
Intended status: Standards Track
Expires: January 23, 2026

P. Bottorff
HPE Aruba Networking
P. Congdon
Congdon Consulting, LLC
July 22, 2025

Using IEEE Std 802.1AB (LLDP) for IETF LSVR neighbor discovery and
configuration
draft-bottorff-lsvr-lldp-01.txt

Abstract

IEEE Std 802.1AB, known as the Link Layer Discovery Protocol (LLDP), can be applied to LSVR neighbor discovery and configuration. This can be achieved by using a "nearest router group address" as the LLDP Scope MAC Address to target LSVR interfaces while advertising a set of LSVR-specific LLDP TLVs. These LSVR-specific TLVs are defined using LLDP Organizationally Specific TLVs, as specified by LLDP for use by individual organizations to allow them to define their own Type-Length-Value (TLV) objects for exchange over the LLDP protocol. The IETF Organizationally Specific TLVs for LSVR can be encoded using the IETF IANA OUI (RFC 9542). This document provides an overview of applying LLDP to LSVR neighbor discovery and configuration and specifies the IETF Organizationally Specific TLVs that support link discovery for LSVR routers. In addition, a brief discussion of the use of IEEE Connectivity Fault Management (CFM) as specified in IEEE Std 802.1Q-2022 cl 18-22 for link liveliness is included.

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 November 22, 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction.....	3
1.1. Requirements Notation.....	4
1.1.1. Requirements Language.....	4
2. Terminology.....	5
3. Abbreviations.....	5
4. LLDP Operation.....	6
4.1. Nearest Router Scope MAC Address for LLDP.....	7
4.2. Logical Link Endpoint Identification.....	8
4.3. Layer-2 Link Liveliness.....	8
4.4. LLDP Organizationally Specific TLVs.....	9
4.4.1. Type.....	10
4.4.2. Length.....	10
4.4.3. Organizationally Unique Identifier.....	10
4.4.4. Subtype.....	10
4.4.5. Information.....	10
4.5. LLDP IETF Organizationally Specific TLVs for LSVR.....	11
4.6. LSVR LLDP L3 data link application.....	12
5. Encapsulation TLVs for LSVR.....	12
5.1. Encaps Flags.....	13
5.1.1. Announce.....	13
5.1.2. Primary.....	13
5.1.3. Under/Over.....	13
5.1.4. Loopback.....	13
5.1.5. Reserved.....	14
5.2. IPv4 Announcement TLV.....	14
5.2.1. Encaps Flags.....	14
5.2.2. IPv4 Address.....	14
5.2.3. Prefix Length.....	14
5.2.4. IPv4 Announcement TLV usage rules.....	15

5.3. IPv6 Announcement TLV.....	15
5.3.1. Encaps Flags.....	15
5.3.2. Prefix Length.....	15
5.3.3. IPv6 Address.....	16
5.3.4. IPv6 Announcement TLV usage rules.....	16
5.4. MPLS IPv4 Announcement TLV.....	16
5.4.1. MPLS Label List.....	16
5.4.1.1. Label Count.....	17
5.4.1.2. Label.....	17
5.4.1.3. Exp.....	17
5.4.1.4. S.....	17
5.4.2. Encaps Flags.....	17
5.4.3. Prefix Length.....	17
5.4.4. IPv4 Address.....	17
5.4.5. IPv4 Announcement TLV usage rules.....	18
5.5. MPLS IPv6 Announcement TLV.....	18
5.5.1. MPLS Label List.....	18
5.5.2. Encaps Flags.....	18
5.5.3. IPv6 Address.....	19
5.5.4. Prefix Length.....	19
5.5.5. MPLS IPv6 Announcement TLV usage rules.....	19
6. Upper-Layer Protocol Configuration TLVs.....	19
6.1.1. AttrTypes.....	19
6.1.2. BGP ASN.....	20
6.1.3. BGP IPv4 Peering Address.....	20
6.1.4. BGP IPv6 Peering Address.....	20
6.1.5. BGP Authentication Data.....	20
6.1.6. BGP Flags.....	20
6.1.7. BGP Protocol Configuration TLVs usage rules.....	21
7. Security Considerations.....	21
8. IANA Considerations.....	21
9. Conclusions.....	21
10. References.....	21
10.1. Normative References.....	21
11. Acknowledgments.....	23

1. Introduction

The IEEE Std 802.1AB [802.1AB][802.1ABcu][802.1ABdh], commonly known as the Link Layer Discovery Protocol (LLDP), is an extremely simple L2 protocol used to advertise the identity and capabilities of router, switch, bridge, and end-station ports to network neighbors. It is supported by many vendors and is widely deployed in data centers and campus networks where it provides information used to identify neighbors, capabilities, and current state. The LLDP information is used in turn by management systems to map the network

topology and capabilities and by LLDP applications to perform protocol configuration.

The LLDP protocol operates over both point-to-point and multipoint networks. It can be used to advertise neighbors and capabilities both at the physical port level and at virtual interfaces within systems. LLDP provides three standardized advertisement scopes which identify the type of port being advertised. These standard types are identified by a multicast Scope MAC Addresses which is used as an LLDP destination address. The standard port types are nearest bridge, nearest non-TPMR bridge, and nearest customer bridge. In addition, the standard allows the use of an alternate group MAC address or individual MAC address for the Scope MAC Address. For LSVR an alternate Scope MAC Address can be used to identify router ports which are internal to a switch or to identify router ports that are behind a bridged network.

LLDP provides a means for individual organizations to define their own Type-Length-Value (TLV) objects for exchange over the protocol. TLVs that belong to an organization are identified by the inclusion of the organization's OUI and an organizationally defined subtype in the initial octets of the information field.

The IETF is a standards development organization with an IANA OUI. The usage and considerations for this OUI are discussed in [RFC9542]. The IANA OUI can be used to identify IETF specific LLDP Organizationally Specific TLVs.

The LSVR working group is specifying protocols that need to discover IP Layer 3 attributes of links, encapsulations and neighbors. This document specifies a set of IETF LLDP Organizationally Specific TLVs that carry the necessary discovery attributes for LSVR working group protocols.

1.1. Requirements Notation

1.1.1. 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. Terminology

Extended Link Layer Discovery Protocol: Refer to [8021.ABdh]

Extension LLDP PDU: Refer to [8021.ABdh]

Extension Request LLDP PDU: Refer to [8021.ABdh]

Link or Logical Link: A logical connection between two logical ports on two devices. E.g. two VLANs between the same two ports are two links.

Logical Link Endpoint: One end of a logical link.

Logical Link Endpoint Identifier: The unique identifier for a Logical Link Endpoint.

LLDP Protocol Data Unit: Refer to [802.1AB]

Manifest LLDP PDU: Refer to [8021.ABdh]

Normal LLDP PDU: Refer to [8021.ABdh]

Scope MAC Address: Refer to [8021.ABdh]

3. Abbreviations

LLDP - Link Layer Discovery Protocol

LLEI - Logical Link Identifier

TLV - Type-Length-Value

XLLDP - Extended Link Layer Discovery Protocol

XPDU - Extension LLDPDU

XREQ - Extension Request LLDPDU

4. LLDP Operation

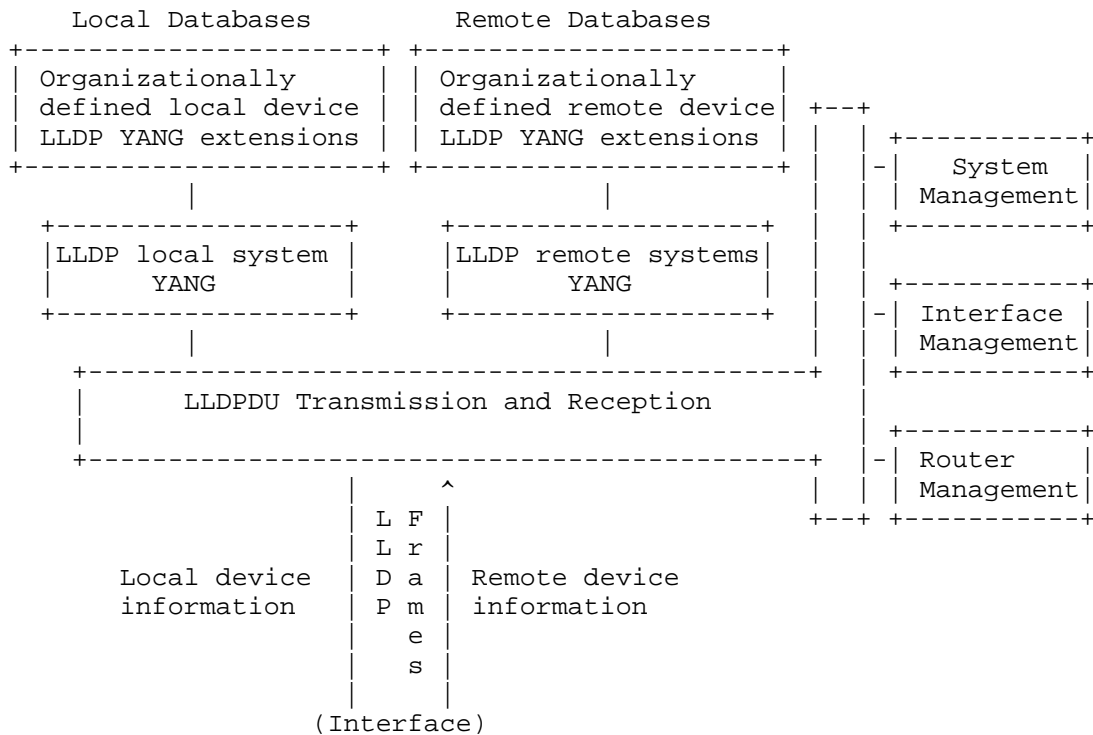


Figure 1 LLDP Agent and databases

Figure 1 is a simplified illustration of figure 6-1 from [802.1AB]. It illustrates an LLDP Agent and its relationship to the databases. For a more detailed description refer to clause 6 of [802.1AB].

LLDP is a link layer protocol that allows an Ethernet device to advertise the capabilities and status of a system interface. The local database (see figure 1) is loaded with the information to be advertised by the interface. The LLDP Agent at the interface periodically encodes the local database into LLDP PDUs and transmits a Normal LLDP PDU destined to the Scope MAC Address. The interfaces subscribed to the Scope MAC Address receive the incoming LLDP PDUs and direct them to the LLDP Agent based on the LLDP PDU destination address and the LLDP Ethertype 0x88CC. The information received in LLDP PDUs is stored by the LLDP Agent in the remote database. The local database contains the information advertised by LLDP for the interface, while the remote database contains the information received from each remote interface.

In the event the TLVs that encode the local database do not fit in a single LLDP PDU (which is a single frame), the LLDP Agent will encode additional TLVs in extension LLDP PDUs (XPDUs) and will add a Manifest TLV to the Normal LLDP PDU. The Manifest TLV contains a digest of each XPDUs. The receiver of a Normal TLV containing a Manifest TLV will decide if any of the XPDUs contains new information by comparing the digest for the XPDUs in its remote database with the digest contained in the Manifest. If new XPDUs are found the receiver will make explicit requests for the new XPDUs using the Extension Request LLDP PDU (XREQ). The transmitting LLDP Agent responds to XREQs by sending the requested XPDUs. The LLDP extended request response performed using the XREQ and XPDUs exchange is performed using unicast addressing. Since the receiver makes explicit requests for XPDUs it can determine the pacing rate based on its processing overhead and resources. The receiver is responsible for timing out and retrying failed XREQs.

4.1. Nearest Router Scope MAC Address for LLDP

There are two choices for how to address LLDP PDUs for application to LSVR discovery and configuration. These are to use the Nearest Bridge Address (01-80-C2-00-00-0E) [802.1AB] for the LLDP Scope MAC Address or to select an application specific Nearest Router Multicast Address for use as the LLDP Scope MAC Address.

If the IEEE standard Nearest Bridge Address is used, the LLDP Agent will be at the physical switch port. In this case, routers attached to subinterfaces or Switched Virtual Interfaces (SVIs) will need to support information for multiple Logical Link Endpoints within the local LLDP databases on each physical port. The LLDP local databases will require the Logical Link Endpoint Identifier (LLEI), VLAN IDs, and MAC addresses associated with each Logical Link Endpoint. In addition, if the nearest bridge address is used, router interfaces with bridges between them will not be discoverable because the LLDP PDUs will not travel through the bridges.

If an LSVR specific Nearest Router, Multicast Address which is not a member of the reserved bridge addresses, is selected for the LLDP Scope MAC Address, then the LLDP Agents can be associated directly with the router interfaces regardless of whether they are physical, subinterfaces, or Switched Virtual Interfaces (SVIs). In addition, such an address will allow LLDP to operate when a bridge intervenes between the router interfaces.

Within this document a Nearest Router Multicast will be assumed as the only LLDP Scope MAC Address used for the LSVR discovery application. We believe this approach is consistent with the current

intent of draft-ietf-lsvr-l3dl. The Nearest Router Multicast Address for the LSVR LLDP Scope MAC Address should be reserved for router interface discovery applications by IANA. IEEE may also reserve the nearest router multicast selected by IANA, however since the nearest router multicast would not have any special meaning to the IEEE 802 protocols reservation by IEEE is not required.

4.2. Logical Link Endpoint Identification

Every LLDP PDU begins with a ChassisID TLV and a PortID TLV [802.1AB]. These two TLVs identify the sending LLDP location which is the equivalent of the draft-ietf-lsvr-l2dl Logical Link Endpoint Identifier. The ChassisID provides a unique identifier for the system, in this case an LSVR router (i.e. a MAC address, any IANA address family identifier, see [8021.AB] for further details). The PortID provides a unique identifier for the interface within the system (i.e. port number, IfIndex, see [8021.AB] for further details).

Within this draft we assume the use of a Nearest Router Multicast Scope MAC Address for LLDP which places LLDP Agents at the Logical Link Endpoint. Provided the LLDP Agent is advertising information from each router interface (physical or virtual) the ChassisID and PortID can be used as the Logical Link Endpoint Identifier. This draft assumes the LLDP ChassisID and PortID are used to identify Logical Link Endpoints.

4.3. Layer-2 Link Liveliness

Two mechanisms are available to determine layer-2 link liveliness. These are the periodic LLDP PDU transmissions along with the LLDP time-to-live protocol and the IEEE Connectivity Fault Management (CFM) protocol as specified in IEEE Std 802.1Q cl 18-22 [802.1Q].

The LLDP mechanism is part of the basic LLDP protocol. Every Normal LLDP PDU contains a Time-To-Live TLV which specifies how long the information advertised for each Logical Link Endpoint is valid. LLDP retransmits the Normal LLDP PDU periodically to maintain the liveliness of the information in the remote LLDP databases. The default retransmit time for LLDP is once every 30 seconds and is settable in 1 second steps. The Time-To-Live is calculated based on the Normal LLDP PDU retransmit window to allow multiple LLDP PDU retransmits before expiring. The default is 4 transmission times. A time-to-live timeout is indicated to the coupled application layer, in this case the router, which can take action to disable the associated Logical Link(s).

The l3dl protocol specifies a hello timer of 10 seconds with a timeout of 3 transmission intervals. The LLDP transmissions and timeout can be set to match these values if desired.

The Connectivity Fault Management (CFM) mechanism provides a multi-level Operations, Administration and Maintenance facility that can be used to provide liveliness as well as L2 network diagnostics. For application to LSVR link liveless CFM Continuity Check Messages (CCMs) can be generated from each Logical Link Endpoint by implementing a CFM Management End Point (MEP) at each Logical Link Endpoint. These CCM messages travel over a Maintenance Domain (MD) within a Maintenance Association (MA).

The Maintenance Domain specifies the boundaries of the L2 communication such as Customer/Service Provider/Operator. The MD levels nest, however never intersect allowing support for network layering. The MD level are 0-7 where 7 is the broadest reach. Each MD level also is named. For the application of LLDP to LSVR LLE discovery there could be lower level domains. For instance, if the LSVR router interface was attached to a MEF E-LINE service, then there could be both service provider and operator MDs as part of the router link. In this case the LSVR interface MD should be in the upper level. Another possibility is that the LSVR router provides an L2 service interface to the data center (perhaps to the overlay). In this case there could be MDs of greater extent than the used for LSVR link discovery. To allow for these two cases the MD selected for LSVR link discovery could be MD level 5 which is the lowest customer level allowing 0-4 for provider networking and 6-7 for data center L2 services.

A Maintenance Association (MA) within a MD is defined by a set of Maintenance End Points (MEPs) at the edge of the MD to monitor connectivity of a particular service. In this case every LSVR LLE can be part of an MA.

The Connectivity Check Messages (CCMs) running over LSVR Management Associations can provide link continuity checking down to the 10 msec range.

Further support for rapid L2 link liveliness may also use the IEEE 802.3ah OAM procedures. Refer to IEEE 802.3 cl 57.

4.4. LLDP Organizationally Specific TLVs

IEEE Std 802.1AB defines the format of the Organizationally Specific TLVs. The format is redrawn here for convenience.

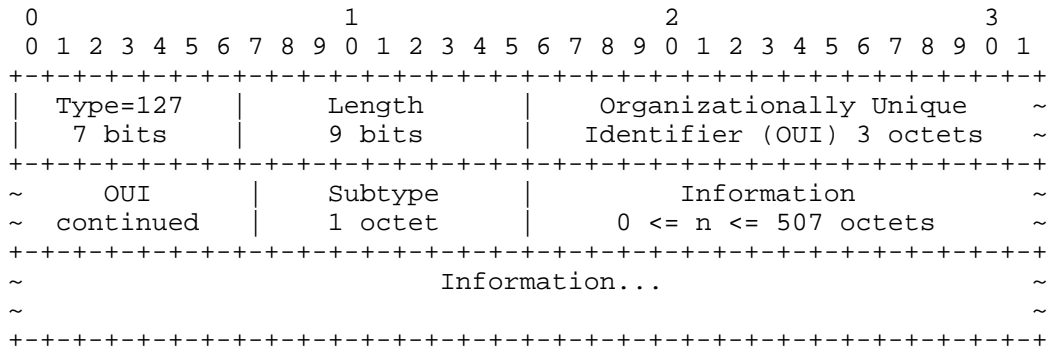


Figure 2 LLDP Organizationally Specific TLV Format

4.4.1. Type

The Type field is 7 bits in length and is set to the value of 127 indicating the TLV type is an Organizationally Specific TLV.

4.4.2. Length

The Length field contains the length of the TLV specific information, the OUI and subtype. The Length is from 4 to 511 octets.

4.4.3. Organizationally Unique Identifier

The Organizationally Unique Identifier indicates the organization specifying the TLV. For IETF use, this field is the IANA OUI as discussed in RFC 9542 and has the hex value of 00-00-5E.

4.4.4. Subtype

The Subtype field indicates the specific IETF Organizationally Specific TLV. The format of the information string is dependent upon the Subtype field.

4.4.5. Information

The Information field contains the octets that are specific to the Organizationally Specific TLV. The field length is between 0 and 507 octets.

4.5. LLDP IETF Organizationally Specific TLVs for LSVR

The IETF draft [I-D.acee-idr-lldp-peer-discovery] describes the use of LLDP by BGP for peer discovery. The IETF LLDP TLV format specified for BGP is used here as the basis for LSVR router discovery TLVs.

The format taken from draft-acee-idr-lldp-peer-discovery specifies using the LLDP Organizationally Specific TLV subtype (4.4.4.) to identify the IETF working group followed by a working group specific subtype.

The content of the TLVs specified here for the LSVR are modeled after the TLVs specified for the L3DL protocol in draft [I-D.ietf-lsvr-l3dl].

Each LLDP Organizationally Specific TLV starts with the same first four fields as shown in (4.4.). For LSVR the Type field SHALL be 127; the Length field SHALL be the length in octets of the LLDP TLV information string which starts immediately after the Length field; the OUI field SHALL be the IETF OUI 00-00-0E; the Subtype field SHALL be xx assigned by IANA to designate the LSVR group.

Following the LLDP Organizationally Specific TLV Subtype a LSVR specific one octet LsvrType SHALL be used to identify the TLV content. The values of the LsvrType are shown in the following table:

Subtype	Name
-----	-----
0	Reserved
1	IPv4 Announcement
2	IPv6 Announcement
3	MPLS IPv4 Announcement
4	MPLS IPv6 Announcement
5	Upper-Layer Protocol Configuration
6-255	Reserved

The specific TLV format for each LsvrType and remaining fields of each Organizationally Specific TLV for LSVR are specified in the following sections.

Since LLDP TLVs are limited in size the LLDP database may contain multiple copies of a single LSVR TLV type.

4.6. LSVR LLDP L3 data link application

LSVR LLDP Agents are associated with router Logical Link Endpoint. Each agent advertises the local database associated with the Logical Link Endpoint and updates its remote database to include the information advertised by other router Logical Link Endpoints.

An L3 data link application accesses the LLDP databases to determine the network configuration and operation. The application using the LLDP databases signals to the LLDP Agent whenever it changes something in the local database by using the LLDP SomethingChangedLocal() routine. The LLDP Agent signals the application whenever a change is detected in the remote database using the LLDP SomethingChangedRemote() routine.

The L3 data link application uses the information in the LLDP databases to determine active logical links and the operating configurations. The application informs the LSVR router of operational links and parameters. The interface between the L3 data link application and BGP-SPF can use the restricted profile of BGP-LS [RFC9552] API as specified in l3dl.

5. Encapsulation TLVs for LSVR

LLDP advertises the encapsulations available in the local database associated with its interface. The interface is uniquely identified by the ChassisID and PortID TLVs encoded as the first two TLVs within each LLDP PDU. The ChassisID and PortID TLVs together encode the Logical Link Endpoint Identifier for the router interface within the sending system associated with the LLDP Agent.

The encapsulation types the peers can exchange are IPv4, IPv6, MPLS IPv4, MPLS IPv6, and/or possibly others not defined here.

The sender of an encapsulation type MUST NOT assume the peer is capable of the same encapsulation type. Only if an interface has the encapsulation type in both the local and remote LLDP databases is it safe for L3 protocols to assume they are compatible for that type.

The LLDP L3 data link application might recognize an addressing conflict, such as both ends of the link trying to use the same address. Because alternative addresses or encapsulations may be available, this error might be logged to allow the upper-layer topology builder to determine a suitable option.

Furthermore, for an L3 data link of a given encapsulation type to be formally established and passed to upper-layer protocols, its addressing must be compatible(e.g., residing on the same IP subnet).

5.1. Encaps Flags

Each Encapsulation TLV specifies a set of flags for each address listed for the encapsulation. These flags are specified here and used in all the encapsulations.

The Encaps Flags specify attributes about the address being announced and are compatible with the Encapsulation Flags defined in [I-D.ietf-lsvr-l3dl]. The Encaps Flags have the following format:

0	1	2	3	4 ... 7
Announce	Primary	Under/Over	Loopback	Reserved

Figure 3 Encapsulation Flags

5.1.1. Announce

The Announce flag bit SHALL always be set to 1. [I-D.ietf-lsvr-l3dl] defines this bit as an Announce/Withdraw bit to allow encapsulations to be both announced and withdrawn by the L3DL protocol. Old encapsulations are withdrawn in LLDP by simply excluding them in the next transmission of an LLDP PDU.

5.1.2. Primary

The Primary flag bit indicates that the encapsulation interface is a primary interface. The value of 1 indicates the interface is primary and the value of 0 indicates it is not. If the LLEI has multiple addresses for an encapsulation type, one and only one address SHOULD be marked as primary.

5.1.3. Under/Over

The Under/Over flag bit indicates if the interface address is for an underlay interface or an overlay interface. The value of 1 indicates the interface is an underlay and the value of 0 indicates it is an overlay.

5.1.4. Loopback

The Loopback flag bit indicates if the interface address is a loopback address. Loopback addresses are generally not seen directly on an external interface. One or more loopback addresses MAY be announced. The value of 1 indicates that the interface

address is a loopback address and the value of 0 indicates it is not.

5.1.5. Reserved

MUST be transmitted as 0 and ignored on receive.

5.2. IPv4 Announcement TLV

The IPv4 Announcement TLV describes a device's ability to exchange IPv4 packets on one or more subnets. It does so by announcing the interface's addresses and the corresponding prefix lengths. Multiple tuples of IPv4 address information can be announced in a single TLV, each tuple with its own set of encapsulation flags, address and prefix length. The format of the IPv4 Announcement TLV is as follows:

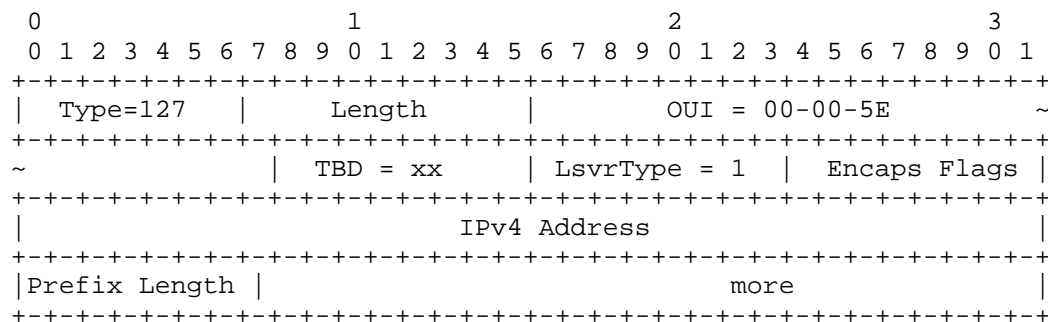


Figure 4 IPv4 Announcement TLV

5.2.1. Encaps Flags

The Encaps Flags are the same flags specified in section 5.1.

5.2.2. IPv4 Address

The IPv4 Address field holds the IPv4 address to be announced.

5.2.3. Prefix Length

The Prefix Length field indicates the number of bits in the IPv4 Address that represent the IPv4 prefix for the subnet (network portion of the address).

5.2.4. IPv4 Announcement TLV usage rules

An LLDP PDU MAY contain multiple IPv4 Announcement TLVs, however, the encapsulation flags, IPv4 address and prefix length tuple for a specific IPv4 address MUST only appear once in the LLDP PDU.

5.3. IPv6 Announcement TLV

The IPv6 Announcement TLV describes a device's ability to exchange IPv6 packets on one or more subnets. It does so by announcing the interface's addresses and the corresponding prefix lengths. Multiple tuples of IPv6 address information can be announced in a single TLV, each tuple with its own set of encapsulation flags, address and prefix length. The format of the IPv6 Announcement TLV is as follows:

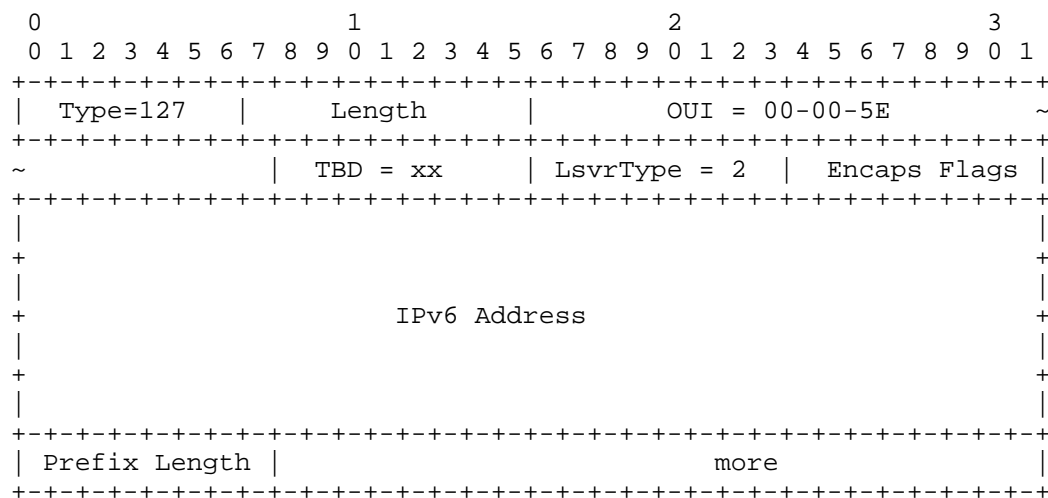


Figure 5 IPv6 Announcement TLV

5.3.1. Encaps Flags

The Encaps Flags are the same flags specified in section 5.1.

5.3.2. Prefix Length

The Prefix Length field indicates the number of bits in the IPv6 Address that represent the IPv6 prefix for the subnet (network portion of the address).

5.3.3. IPv6 Address

The IPv6 Address field holds the IPv6 address to be announced.

5.3.4. IPv6 Announcement TLV usage rules

An LLDP PDU MAY contain multiple IPv6 Announcement TLVs, however, the encapsulation flags, IPv6 address and prefix length tuple for a specific IPv6 address MUST only appear once in the LLDP PDU.

5.4. MPLS IPv4 Announcement TLV

The MPLS IPv4 Encapsulation describes a logical link's ability to exchange labeled IPv4 packets on one or more subnets. It does so by stating the interface's addresses the corresponding prefix lengths, and the corresponding labels which will be accepted for each address. The format of the MPLS IPv4 Announcement TLV is as follows:

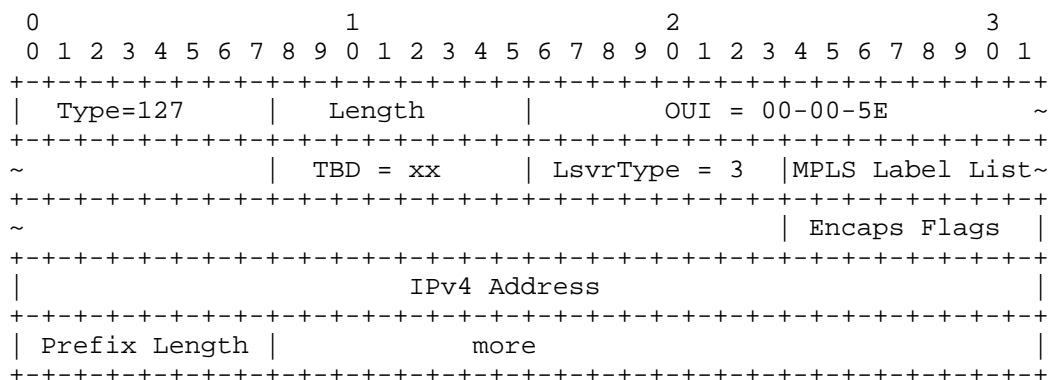


Figure 6 MPLS IPv4 Announcement TLV

5.4.1. MPLS Label List

The MPLS Label List is a variable length field that contains the label stack, see [RFC3032], that the sender will accept for the prefix to which the list is attached. The format of the MPLS Label List is as follows:

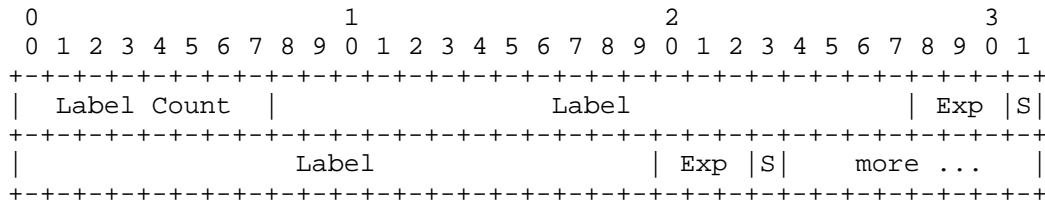


Figure 7 MPLS Label List

5.4.1.1. Label Count

The number of label stack entries that are included in the list. Each label stack entry has a label, experimental use bits and the bottom of stack indicator. The Label Count MUST NOT be 0.

<<Editor's note: We really don't need this count because the S bit indicates when the list ends>>

5.4.1.2. Label

The Label field is the 20-bit value of the label.

5.4.1.3. Exp

The Exp field is a 3-bit value reserved for experimental use.

5.4.1.4. S

The S field is a single bit that indicates the last entry in the label stack. The bit is set to 1 for the last entry and 0 for all other entries in the list.

5.4.2. Encaps Flags

The Encaps Flags are the same flags specified in section 5.1.

5.4.3. Prefix Length

The Prefix Length field indicates the number of bits in the IPv4 Address that represent the IPv4 prefix for the subnet (network portion of the address).

5.4.4. IPv4 Address

The IPv4 Address field holds the IPv4 address to be announced.

5.4.5. IPv4 Announcement TLV usage rules

An LLDP PDU MAY contain multiple MPLS IPv4 Announcement TLVs, however, the encapsulation flags, label list, IPv4 address and prefix length tuple for a specific IPv4 address MUST only appear once in the LLDP PDU.

5.5. MPLS IPv6 Announcement TLV

The MPLS IPv6 Encapsulation describes a logical link's ability to exchange labeled IPv6 packets on one or more subnets. It does so by stating the interface's addresses the corresponding prefix lengths, and the corresponding labels which will be accepted for each address. The format of the MPLS IPv6 Announcement TLV is as follows:

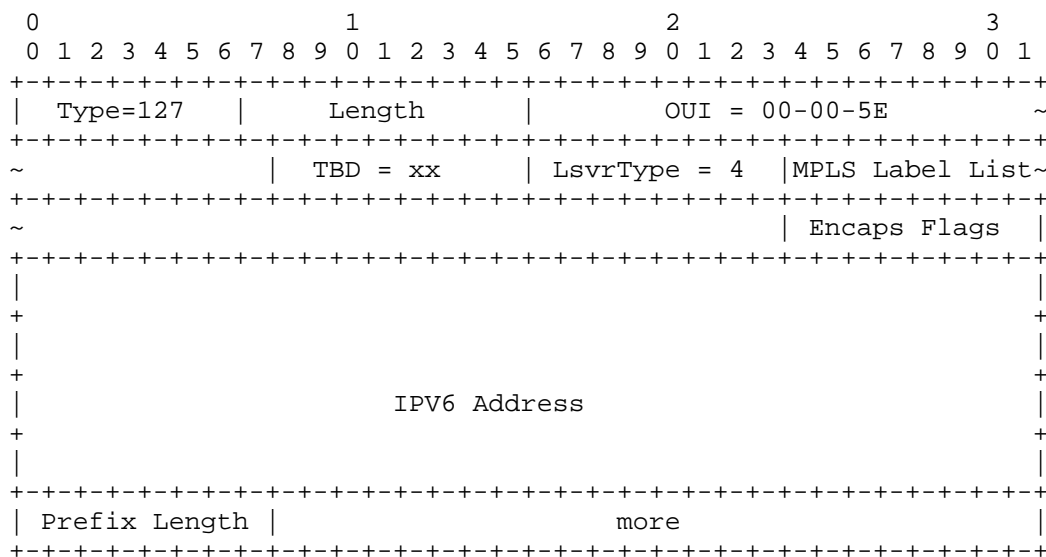


Figure 8 MPLS IPv6 Announcement TLV

5.5.1. MPLS Label List

The MPLS Label List is the same as specified in section 5.4.1.

5.5.2. Encaps Flags

The Encaps Flags are the same flags specified in section 5.1.

5.5.3. IPv6 Address

The IPv6 Address field holds the IPv6 address to be announced.

5.5.4. Prefix Length

The Prefix Length field indicates the number of bits in the IPv6 Address that represent the IPv6 prefix for the subnet (network portion of the address).

5.5.5. MPLS IPv6 Announcement TLV usage rules

An LLDP PDU MAY contain multiple MPLS IPv6 Announcement TLVs, however, the encapsulation flags, label list, IPv6 address and prefix length tuple for a specific IPv6 address MUST only appear once in the LLDP PDU.

6. Upper-Layer Protocol Configuration TLVs

A router or switch supporting LSVR protocols MAY include the following BGP Attribute TLV which is modeled after the l3dl ULPC TLV. Alternatively, the TLVs from [I-D.acee-idr-lldp-peer-discovery] could be used for BGP configuration. The format of the following TLV is compatible with the TLVs in I-D.acee-idr-lldp-peer-discovery, however don't use a length field in the sub-TLV.

The BGP Protocol Configuration TLV for LSVR is shown in Figure 2.

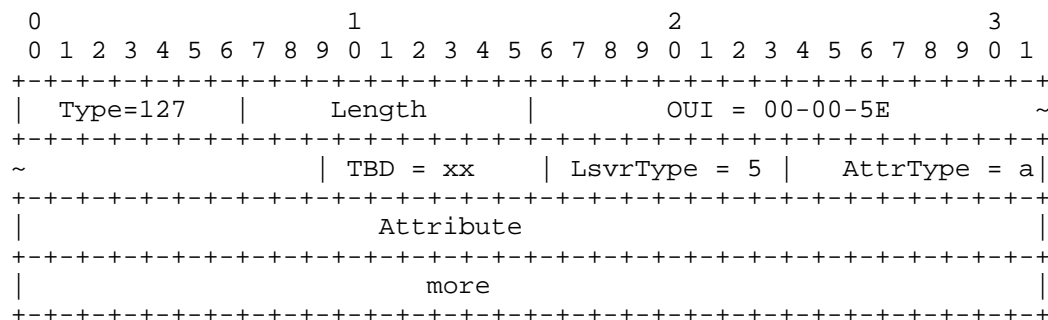


Figure 9 BGP Protocol Configuration TLV Format

6.1.1. AttrTypes

The AttrType identifies the BGP attribute type. The types are:

AttrType = 1: BGP ASN

AttrType = 2: BGP IPv4 Peering Address
AttrType = 3: BGP IPv6 Peering Address
AttrType = 4: BGP Authentication Data
AttrType = 5: BGP Flags, Bit 0: GTSM, Bit 1: BFD,
 Bit 2-15 reserved = 0

6.1.2. BGP ASN

The four octet Autonomous System number MUST be specified. If the AS Number is less than 32 bits, it is padded with high order zeros.

6.1.3. BGP IPv4 Peering Address

The five octet IPv4 Peering Address along with the Prefix Length.

6.1.4. BGP IPv6 Peering Address

The 17 octet IPv6 Peering Address along with the Prefix Length.

6.1.5. BGP Authentication Data

The BGP Authentication TLV provides any authentication data needed to OPEN the BGP session. Depending on operator configuration of the environment, it might be a simple MOS key (see [RFC2385]), the name of a key chain in a KARP database (see [RFC7210]), or one of multiple Authentication TLVs to support [RFC4808].

6.1.6. BGP Flags

The BGP session OPEN has extensive, and a bit complex, capability negotiation facilities. In case one or more extra attributes might be needed, the two octet BGP Flags TLV may be used. No flags are currently defined.

BGP Flags:

Bit 0: GTSM
Bit 1: BFD
Bit 2-15: Must be zero

The GTSM flag, when 1, indicates that the sender wishes to enable the [RFC5082] Generalized TTL Security Mechanism for the session.

The BFD flag, when 1, indicates that the sender wishes to enable the [RFC5880] Bidirectional Forwarding Detection for the session.

6.1.7. BGP Protocol Configuration TLVs usage rules

An LLDP PDU MUST contain only a single BGP Protocol Configuration TLV.

7. Security Considerations

<Add any security considerations>

8. IANA Considerations

The LSVR WG needs to use the IANA OUI to form the Organizationally Specific TLVs used for LSVR discovery and configuration.

The LSVR WG needs a group address for the purpose of LLDP Nearest Router discovery. This address should be recognized by IANA for this application.

9. Conclusions

<Add any conclusions>

10. References

10.1. Normative References

- [802.1AB] "IEEE Standard for Local and metropolitan area networks- Station and Media Access Control Connectivity Discovery", IEEE Std 802.1AB-2016, 29 January 2016, <https://ieeexplore.ieee.org/document/7433915>
- [802.1ABcu] "IEEE Standards for Local and metropolitan area networks- Station and Media Access Control Connectivity Discovery Amendment 1: YANG Data Model" IEEE Std 802.1ABcu-2021, December 2021, <https://ieeexplore.ieee.org/document/9756407>
- [802.1ABdh] "IEEE Standards for Local and metropolitan area networks- Station and Media Access Control Connectivity Discovery Amendment 2: Support for Multiframe Protocol Data Units", IEEE Std 802.1ABdh-2021, December 2021, <https://ieeexplore.ieee.org/document/9760302>
- [802.1Q] "IEEE Standards for Local and metropolitan area networks- Bridges and Bridged Networks", IEEE Std 802.1A-2022, September 2022, <https://ieeexplore.ieee.org/document/10004498>

- [802.1AE] "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security", IEEE Std 802.1AE-2018, September 2018,
<https://ieeexplore.ieee.org/document/8585421>
- [RFC2119] Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997,
<https://datatracker.ietf.org/doc/html/rfc2119>
- [RFC2385] Heffernan, A. "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998,
<https://datatracker.ietf.org/doc/html/rfc2385>
- [RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T. and Conta, A. "MPLS Label Stack Encoding", RFC 3032, January 2001,
<https://datatracker.ietf.org/doc/html/rfc3032>
- [RFC4808] Bellovin, S. "Key Change Strategies for TCP-MD5", RFC 4808, March 2007,
<https://datatracker.ietf.org/doc/html/rfc4808>
- [RFC5082] Gill, V., Heasley, J. Meyer, D. Savola, P. and Pignataro, C., "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007,
<https://datatracker.ietf.org/doc/html/rfc5082>
- [RFC5880] Katz, D. and Ward, D. "Bidirectional Forwarding Detection (BFD)", RFC 5880, June 2010,
<https://datatracker.ietf.org/doc/html/rfc5880>
- [RFC5925] Touch, J., Mankin, A. and Bonica, R. "The TCP Authentication Option", RFC 5925, June 2010,
<https://datatracker.ietf.org/doc/html/rfc5925>
- [RFC8174] Leiba, B. "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, May 2017,
<https://datatracker.ietf.org/doc/html/rfc8174>
- [RFC9542] Eastlake, D. and Abley, J. "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", RFC 9542, April 2024,
<https://datatracker.ietf.org/doc/html/rfc9542>

[RFC9552] Talaulikar, K., Ed., "Distribution of Link-State and Traffic Engineering Information Using BGP", RFC 9552, DOI 10.17487/RFC9552, December 2023, <https://www.rfc-editor.org/info/rfc9552>

[I-D.ietf-lsvr-l3dl] Bush, R., Austein, R. and Patel, K., "Layer 3 Discovery and Liveness", draft-ietf-lsvr-l3dl-15.txt (work in progress), July 2019, <https://datatracker.ietf.org/doc/draft-ietf-lsvr-l3dl/>

[I-D.acee-idr-lldp-peer-discovery] A. Lindem, K. Patel, S.Zandi, J.Haas, X. Xu2, "BGP Logical Link Discovery Protocol (LLDP) Peer Discovery", draft-acee-idr-lldp-peer-discovery-20.txt (work in progress), January 9, 2025, <https://datatracker.ietf.org/doc/draft-acee-idr-lldp-peer-discovery/>

11. Acknowledgments

<Add any acknowledgements>

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Paul Congdon
Congdon Consulting, LLC
5582 Carlile Ct
Granite Bay, CA 95746

Email: paul.congdon@outlook.com

Paul Bottorff
HPE Aruba Networking
8000 Foothill Blvd
Roseville, CA 95747

Email: paul.bottorff@hpe.com

