Auto-attach using LLDP with IEEE 802.1aq SPBM networks
draft-unbehagen-lldp-spb-00

Abstract

This informational document describes a compact method of using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) with IEEE 802.1aq Shortest Path Bridging (SPB) network to automatically attach network devices not supporting IEEE 802.1ah to individual services in a SPB network. These network devices typically do not support SPBM, MAC-in-MAC (802.1ah), nor I-SID usage and therefore cannot easily take advantage of the SPB infrastructure without manual configuration of attachment of VLANs to I-SIDs in multiple locations. A motivation for this draft is to suggest a useful means to simplify and automate connections to PBB L2VPN based service networks such as those defined in SPBM-EVPN.

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 http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months.
1. Terminology

802.1aq - defines a technology for providing a link state protocol for the control of a common Ethernet switching layer.
802.1ah - Provider Backbone Bridges (PBBs), MAC-IN-MAC encapsulation

AAC - Auto Attach Client agent that resides on a non-SPB/PBB capable element that uses LLDPDUs to request I-SID assignment for the VLANs which have been configured on its network port.

AAS - Auto Attach Server agent that processes VLAN to I-SID requests from AAC elements that are connected to a SPB BEB

BCB - Backbone Core Bridge

BEB - Backbone Edge Bridge

B-TAG - Backbone VLAN Tag

C-TAG - Customer VLAN Tag

Element - Any end device or network node that may implement the auto attach functionality

I-SID - Backbone Service Instance Identifier

IS-IS - Intermediate System to Intermediate System Protocol

LAN - Local Area Network

LLDP - IEEE 802.1AB Link Layer Discovery Protocol

SPB - IEEE 802.1aq Shortest Path Bridging

SPBM - Shortest Path Bridging, Mac mode

VLAN - Virtual Local Area Network

2. Requirements Language

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 RFC 2119 [RFC2119].

3. Applicability
This section provides an overview of the behavior of auto attachment functionality into a SPBM [802.1aq] environment and is not intended to be interpreted as normative text. IEEE 802.1aq SPB software is available from multiple vendors of Ethernet switches to connect end devices and non-SPB compliant switches to the SPB enabled backbone network. Edge switches in SPBM that utilize the 802.1ah PBB encapsulation are referred to as Backbone Edge Bridges (BEB). In support of SPBM, these bridges map a VLAN ID on the UNI to an I-SID (Individual Service ID), as defined in IEEE 802.1ah. In order to facilitate an automatic way in which a AAC can request individual service connectivity from an SPBM Backbone Edge Bridge BEB acting as an AAS, this method of using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) with IEEE 802.1aq Shortest Path Bridging network can be used. These widely deployed client devices typically do not support SPBM, IEEE 802.1ah and therefore cannot easily take advantage of the SPB infrastructure without manual configuration of attachment of VLANS to I-SIDs in multiple locations.

Elements that utilize this automated method for service assignment pass this data to attached SPBM capable BEB nodes where the mappings are processed and approved or rejected. Specific actions are taken on the non-SPBM devices, referred to as Auto Attach Clients (AAC), as well as the SPBM device, referred to as Auto-Attach Server (AAS), based on the outcome of the mapping request.

These devices pass this data to attached SPBM nodes where the mappings are processed and approved or rejected. Specific actions are taken on the non-SPBM devices, referred to as servers and clients, as well as the SPBM device, referred to as a Auto-Attach server, based on the outcome of the mapping request.

![Conceptual SPB Auto Attach Model](image)

Figure 1: LLDP exchanges trigger IS-IS SPBM announcements.

Figure 1 depicts a conceptual example of the process where a AAC can use LLDP to communicate the need to connect a VLAN to the appropriate I-SID on the SPB BEB it is attached to on its network uplink port.

4. Auto Attachment Architecture

4.1. Element Discovery
The first stage of establishing AA connectivity involves element
discovery. An Auto Attach agent resides on all capable elements.
Server agents control the Auto Attach (AA) of VLANs to I-SIDs on
themselves when enabled to accept and process such requests from AAC
elements. Typically this is done through a global service setting
and through per-port settings that control the transmission of
information in LLDPDUs on the appropriate links that interface AAC’s
and AAS’s.

Once the required AA settings are enabled on the elements (e.g., the
AA service and the per-port AA settings) the AA agent on each element
type, both AAC and AAS, advertises its capabilities (i.e., server/
client) through LLDPDU packets to each other.

Following discovery of AA capabilities by both the AAC and the AAS,
the AA agent on each element is aware of all AA services currently
provided by the network elements to which it is directly connected.
Based on this information, an AAC agent can determine whether Auto
Attach data, namely locally administered I-SID/VLAN assignments that
should be exported to the AAS, that is associated with an SPBM BEB to
which it is attached to on its network uplink ports.

Initial Auto Attach functionality, when enabled, can be used to
extract management VLAN data from the primary AA server
advertisements and can use this data to update the in-band management
VLAN and initiate IP address acquisition using techniques such as
DHCP

4.2. Service Requests

Service mappings can be established when these two criteria are met:

1. AA Server found during discovery

   Assuming that an administrator has defined one or more ports
   for auto attach mode a discover message is sent out each port
   defined using LLDP.

2. I-SID/VLAN bindings are defined locally

   Assuming that an administrator has defined one or more I-SID/
   VLAN assignments (or AAC bindings have been received for
   processing), an AAC sends the I-SID/VLAN assignment list to
   the discovered AAS. I-SID/VLAN data is exported using LLDP TLV
   extensions defined in section 5.2.

4.2.1. Element Inactivity Timeout
An AAC must handle primary AAS loss and this requires maintenance of a server’s inactivity timer. If primary AAS advertisements are not received for a pre-determined amount of time, the I-SID/VLAN assignments accepted by the server are considered rejected. I-SID/VLAN assignment data is then defaulted (reverts to the ‘pending’ state) and the AA agent, which resides on the AAC, removes related settings.

4.3. Server Mapping Request Processing

Each I-SID/VLAN assignment in an AA request received by the AAS is processed individually and can be accepted or rejected. An assignment may be rejected for a number of reasons, such as server resource limitations or, for example, restrictions related only to the source AAC. Rejected assignments are passed back to the originating AAC with a rejected state and, if appropriate, an indication as to why the rejection occurred. Limited state information may be maintained on the server related to rejected I-SID/VLAN assignments.

Each VLAN that is associated with an accepted I-SID/VLAN assignment must be created on the AAS bridge if it does not already exist. These VLANs are designated SPBM UNI VLANs on a BEB. The port through which the AA I-SID/VLAN assignment list was received (i.e., the AAS downlink) must be a member of the VLAN(s) in the I-SID/VLAN assignment list that are accepted by the AAS. Port membership is automatically updated when the UNI service (I-SID/VLAN/port) is created. To ensure that VLAN markings are maintained between switches, traffic on the downlink port MUST be tagged. The AA agent on the serving BEB handles all of these tasks automatically. No administrator intervention is required.

The AAS agent is responsible for tracking which, if any, of these actions are performed so that settings can be cleared when they are no longer needed. This can occur, for example, when configuration changes on an AAC updates the received I-SID/VLAN assignment list when an AAC associated with a downlink port changes or an AAC connection disappears entirely. Specifically, when an SPBM switched UNI-based VLAN and a switched UNI have been created on a downlink port because of an accepted AA I-SID/VLAN assignment (and not because of an explicit administrator port action), then the UNI and
associated VLAN SHOULD be deleted when the related I-SID/VLAN assignment is cleared by the AAS.

4.4. Server Mapping Response Processing

Each VLAN that is associated with an AAC I-SID/VLAN assignment must be defined on the client’s device. The port associated with the uplink connecting the AAC to the AAS must be a member of the VLAN(s) in the I-SID/VLAN assignment list that are sent to and accepted by the AAS. This allows traffic on these VLANs to pass through the switch into the SPB fabric when required. To ensure that VLAN markings are maintained between devices, traffic on the uplink port MUST be tagged. If a VLAN has not been created before the I-SID/VLAN assignment itself, it is automatically created by the AAS agent when a proposed assignment is accepted. Port tagging and the port VLAN membership update are also performed by the AAS automatically based on assignment acceptance. To ensure consistency, VLANs SHOULD NOT be deleted while they are referenced in any I-SID/VLAN assignments on the device.

4.5. Service Mapping Timeout

A "last updated" timestamp is associated with all active assignments on the AAS. When this value is not updated for a pre-determined amount of time, the I-SID/VLAN assignment is considered obsolete. Obsolete assignment data and related settings are removed by the AAS, subject to the constraints imposed by section 4.3.

The current I-SID/VLAN assignment list is advertised by an AAC at regular intervals (dictated by LLDP operation). During processing of this data, an AAS must handle list updates and delete assignments from previous advertisements that are no longer present. Though these entries would be processed appropriately when they timeout, the AAS attempts to update the data in real-time and SHOULD initiate deletion immediately upon detection of this condition.

5. Auto Attach LLDP Extensions

The Auto Attach TLVs are implemented as extensions to the LLPD standard, using its flexible extension mechanism. They SHOULD be implemented as vendor-specific TLVs using TLV type 127 as described in the 802.1ab (LLDP) standard. TLVs supporting the exchange of AA element data and I-SID/VLAN assignment data have been defined.

5.1. AA Element TLV

The Element TLV is used by an AA device to announce its capabilities to its LLDP peer on a given interface. Use of the Auto Attach functionality is encoded in to the 802.1AB LLDP Custom Element TLV as follows:

AA Element TLV
Subtype = 8 for AA Element TLV

Supported Auto Attach Element Type values:

- Element Type Unknown (1)
- Server (2)
- Untagged Client (4)
- Tagged Client (5)

The element type identifies the capability of the advertising AA node. The AA Server describes an AAS capable device that can map incoming VLAN to I-SID and announce I-SID connectivity to the SPB network. AA Clients may operate in either tagged or untagged modes. If an AA client announces untagged, then the entire port MUST be mapped to the I-SID on the BEB.

The AA Element TLV can only exist once in a LLDPDU. It is included in all LLDPDUs when the Auto Attach service is enabled and when the port transmission flags associated with this TLV, as required by the 802.1ab standard, are enabled.

5.2. I-SID/VLAN Assignment TLV

The AA I-SID/VLAN Assignment TLV is used by the AAC to announce I-SID/VLAN assignments that it would like supported by a directly connected AAS. It is also used by the AAS to announce that it is active.
The AA I-SID/VLAN Assignment TLV can only exist once in a LLDPDU. It is only included in a LLDPDU when complementary AA element (i.e., AA server/ client) devices are directly connected. Data integrity and source validation is supported through the use of the HMAC-SHA256 message authentication algorithm. The HMAC-SHA256 generated digest size is 32 octets and the FA I-SID/VLAN Assignment TLV includes a field to support the digest exchange between source and destination parties.

Per-port TLV transmission flags must be enabled on the communicating devices as well. The AA Element TLV must also be present in the LLDPDU for the AA I-SID/VLAN Assignment TLV to be processed. The TLV cannot exceed the LLDP 512 byte TLV size limit, which implies a maximum of 94 I-SID/VLAN assignments in a LLDPDU.

TLV as follows:

<table>
<thead>
<tr>
<th>Type: 127 (7 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length: 41-506 octets</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>OUI: 3 octets</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Subtype: 9 (1 octet)</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>HMAC-SHA256 Digest: 32 octets</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Assignment Status: 4 bits</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>VLAN: 12 bits</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>I-SID: 3 octets</td>
</tr>
</tbody>
</table>

The HMAC-SHA256 digest is computed for the series (1-94) of I-SID/VLAN assignments (i.e. data for the digest computation starts at [0-based] byte 38 of the TLV). The digest is then placed in the HMAC-SHA256 Digest field in the TLV prior to transmission. Upon receipt, the digest is again computed for the series (1-94) of I-SID/VLAN assignments in the received TLV and the resulting digest is compared against the received digest. If the received digest is the same as the newly computed digest, the TLV is considered valid and processing can commence. If the comparison fails, the TLV is discarded and processing is terminated. Additionally the value for the I-SID in the incoming LLDP exchanges SHOULD trigger an IS-IS SPBM announcement using normal IEEE 802.1aq mechanisms if not already being announced by the BEB.

6. Security Considerations
It is important to provide an option to ensure that the aforementioned Auto Attach communication is secure in terms of data integrity (i.e., the data has not been altered in transit) and authenticity (i.e., the data source is valid).

If communication is occurring between non-secure systems, the HMAC-SHA256 Digest data should always be zero and the digest data, regardless of the value, is ignored. A misconfiguration can occur with one system operating in secure mode and the other operating in non-secure mode. In this scenario, the I-SID/VLAN Assignment TLV will always be discarded prior to processing by the system operating in secure mode.

These security requirements are satisfied by using an optional keyed-hash message authentication code (HMAC) to protect the AAC/AAS I-SID/VLAN assignment exchanges. This type of message authentication allows communicating parties to verify that the contents of the message have not been altered and that the source is authentic. Use of this mechanism is optional and is controlled through a user-configurable attribute.

6.1. Element TLV Security Considerations

A HMAC-SHA256 digest is computed for the series of I-SID/VLAN assignments, where the digest computation starts [0 based] at byte 38 of the TLV. The resulting digest is then placed in the TLV prior to sending. Where upon receipt of the digest, the contents are again computed in the same manner and the digests are compared, if the comparison fails then the TLV is discarded, otherwise if both digests are the same the TLV is considered valid and processed appropriately.

7. Acknowledgements

We would like to thank the following people (in no particular order) for their contributions:

1. Zenon Kuc
2. Cristian Mema
3. Roger Lapuh
4. Craig Griffin
5. Chris Buerger

8. IANA Considerations

This memo includes no request to IANA.
All drafts are required to have an IANA considerations section (see the update of RFC 2434 [I-D.narten-iana-considerations-rfc2434bis] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

9. References

9.1. Normative References


9.2. Informative References


Authors’ Addresses

Paul Unbehagen Jr, editor
Avaya
1300 W. 120th Avenue
Westminster, CO 80234
US

Email: unbehagen@avaya.com
Dan Romascanu
Avaya
Atidim Technology Park, Bldg. #3
Tel Aviv, 61131
Israel

Phone: +972-3-645-8414
Email: dromasca@avaya.com

John Seligson
Avaya
4655 Great America Parkway
Santa Clara, CA 95054
US

Email: jseligso@avaya.com

Carl Keene
Avaya
600 Technology Park Dr
Boston, MA 01821
US

Email: ckeene@avaya.com

Nigel Bragg
Ciena
Ciena House
43-51 Worship Street
London, EC2A 2DX
UK

Email: nbragg@ciena.com

Ludovic Beliveau
Wind River

Email: Ludovic.Beliveau@windriver.com