To: IETF Internet Area WG
Juan-Carlos Zúñiga, Co-Chair, Internet Area Working Group
j.c.zuniga@ieee.org
Wassim Haddad, Co-Chair, Internet Area Working Group
Wassim.Haddad@ericsson.com
Suresh Krishnan, Area Director, Internet Area
suresh.krishnan@ericsson.com

From: Glenn Parsons, Chair, IEEE 802.1
Date: March 2017

Colleagues,

The following Internet draft has come to our attention as under consideration to become an IETF Internet Area Working Group Draft: draft-nordmark-intarea-ippl-05.

We infer that the intent of section 3 of this draft is to be more a "profile" than a standard. In a profile, MUST and MUST NOT (or some similar terms) are constraints on the network administrator to configure a device to exhibit the desired behavior. But, in a standard, MUST and MUST NOT are constraints on a conformant implementation. Any SDO should be free to write the former document for any device; the latter is the exclusive province of the SDO defining the device.

The draft talks about IEEE Std 802.1Q bridges, and lists MUST and MUST NOT statements to which an 802.1Q bridge is to conform. This can easily be taken as a constraint on bridge implementations, and as such, is inappropriate

“Private VLANs” is an implementation of asymmetric VLANs and Rooted-Multipoint connectivity. "Private VLANs" were an integral part of 802.1Q-1998. The MUST and MUST NOT statements are aligned with the way an 802.1Q bridge can be configured to work.

“Private VLANs” as described in the draft are a combination of the “Multi-Netted Server” and the “Rooted-Multipoint” use cases described in 802.1Q annex F.1.3 “Asymmetric VLANs and Rooted-Multipoint Connectivity”. The “Multi-Netted Server” example describes how a bridged network allows a server to communicate with multiple mutually-isolated groups of clients by allocating a VLAN ID per group. The “Rooted-Multipoint” example describes an optimization that allows all groups containing a single client to share a single VLAN ID while still remaining isolated from each other. Note that 802.1Q annex F as a whole describes the use of “Shared and Independent VLAN Learning (IVL and SVL).” Configuring Shared VLAN Learning for the VLAN IDs by Asymmetric (Private) VLANs prevents the learning issues alluded to in section 14 of draft-nordmark-intarea-ippl-05. Section 14 appears to provide a very useful recommendation for protecting the network from mis-configurations of Shared VLAN Learning.

We would suggest:

1. The tone of the draft should be, "how a router can take advantage of the Asymmetric (Private) VLAN feature offered by 802.1Q bridges."
2. Modifying the section in question to describe how it works, without any conformance language on bridge behavior but explaining 802.1Q standard bridge configuration instead.
3. Make a normative reference to 802.1Q.

Ideally, the document should reference managed objects in 802.1Q clause 12. Attached is a description of how that can be accomplished.

Best regards,
Glenn Parsons, Chair IEEE 802.1 Working Group
(glenn.parsons@ericsson.com)

In the details for basic private VLANs below, all clause numbers are IEEE Std 802.1Q-2014. Clause 12 is used as a reference for management. The MIBs in clause 17 are constructed as an implementation of the management model in clause 12, as are the YANG models currently being developed.

- Select a set of VLAN IDs (VIDs) – let's call them the Branch VID (communication from Leaf ports [hosts] to Root ports [routers]), the Trunk VID (from Root ports to each other and to Leaf ports), and zero or more Party VIDs (from Community ports to Root ports and other Community ports in the same community).
- Assign all VIDs to the same FID (12.10.3.4) – this activates Shared VLAN Learning and needs to be done in all bridges.
- For all Leaf ports:
    - Configure the Branch VID as the PVID (the default input VID, 12.10.1.2.2:a).
    - Configure the port to accept only untagged or priority tagged frames (12.10.1.3.2:a:2).
    - Configure the port to disable ingress filtering (12.10.1.4.2:a:2).
    - Create a permanent VLAN registration entry (12.7.7.1) specifying a fixed registration (8.8.2:b:1:i), frames to be output untagged (8.8.2:b:2) for the Trunk VID.
- For all Community ports:
    - Configure the Party VID for this port’s community as the PVID (the default input VID, 12.10.1.2.2:a).
    - Configure the port to accept only untagged or priority tagged frames (12.10.1.3.2:a:2).
    - Configure the port to disable ingress filtering (12.10.1.4.2:a:2).
    - Create a permanent VLAN registration entry (12.7.7.1) specifying a fixed registration (8.8.2:b:1:i), frames to be output untagged (8.8.2:b:2) for the Trunk VID and the Party VID.

- For all Root ports:
    - Configure the Trunk VID as the PVID (the default input VID, 12.10.1.2.2:a).
    - Configure the port to accept only untagged or priority tagged frames (12.10.1.3.2:a:2).
    - Configure the port to disable ingress filtering (12.10.1.4.2:a:2).
    - Create a permanent VLAN registration entry (12.7.7.1) specifying a fixed registration (8.8.2:b:1:i), frames to be output untagged (8.8.2:b:2) for the Trunk, Branch, and all Party VIDs. Alternatively, they can use the MVRP protocol (11.2) to configure the VIDs dynamically.

The above configuration assumes the router attached to a Root port is transmitting untagged frames and is participating only in this set of VIDs. If the router is participating in other VLANs as well, then it transmits all frames for this Private VLAN using the Trunk VID, and the Root port configuration consists simply of creating the permanent VLAN registration entries for all VIDs specifying a fixed registration and frames to be output tagged.

Note that the set of Trunk, Branch, and all Party VIDs, together, implement a single VLAN with special connectivity properties – not separate VLANs.

The connectivity of that VLAN is:

- Frames transmitted from Root ports can be received by all ports on the VLAN.
- Frames transmitted from Leaf ports can only be received by Root ports on the VLAN.
- Frames transmitted from Community ports can only be received by Root ports and other Community ports (in the same community) on the VLAN.