Network Working Group
INTERNET-DRAFT
Intended status: Informational

Expires: February 27, 2012

Donald Eastlake
Susan Hares
Huawei
Jon Hudson
Brocade

August 28, 2011

RBridge and Switching Device Layering and Compatibility
<draft-eastlake-rbridge-compatibility-02.txt>

Abstract

This document describes a layering and peering model for network switches and end stations. It also discusses, using this model, the compatibility of RBridges (Routing Bridges) with Layer 3 routers and various types of bridges including Shortest Path Bridges. RBridges are devices that implement the IETF TRILL (TRansparent Interconnection of Lots of Links) standard.

Status of This Memo

Distribution of this document is unlimited. Comments should be sent to the TRILL working group mailing list.

Table of Contents

1. Introduction

RBridges (Routing Bridges) provide transparent least-cost forwarding in networks with arbitrary topology using the IETF TRILL (TRansparent Interconnection of Lots of Links) standard [RFC6325] that builds on IS-IS (Intermediate System to Intermediate System) routing [IS-IS] [RFC1195] [RFC6326].

This document describes a model of the layered relationship between types of switching devices and how this correlates with peering for some protocols. It also discusses the compatibility of RBridges with end stations, Layer 3 routers, Layer 2 Customer Bridges, general Layer 2 Provider Bridges, and Shortest Path Bridges.

1.1 Simplifying Assumptions

There tend to be many twists and turns in the real world so, to keep this document to a reasonable size, the following assumptions are made:

1. All physical links between devices are point-to-point Ethernet connections [802] [802.3].

2. Although there are a variety of Layer 3 routers, we will assume pure IPv4/IPv6 [IS-IS] [RFC1195] routers.

3. It is assumed that the reader has some general understanding of what Layer 3 routing and Layer 2 bridging [ITU-X.200] are, how Ethernet works, and is familiar with [RFC6325].

1.2 Terminology

The terminology and acronyms of [RFC6325] are used in this document supplemented by the following definitions:

Bridge - as used in this document, a device that transparently forwards frames using some version of the Spanning Tree Protocol.

RBridge - Routing Bridge - a device generally conformant to the TRILL base protocol standard [RFC6325] that transparently routes frames.

SPB - Shortest Path Bridge - a device that is not only a Bridge as defined above but that can also forward frames using bridging mechanisms that are configured using the IS-IS protocol.

2. Layers and Peering

This section discusses a model of the layered relationship between switching devices and how it affects peering for some protocols.

2.1 Basic Layers

Relative layering is essential to a clear understanding of the model used by this document. While "Layer 2" and "Layer 3," in approximately the OSI (Open System Interconnect) sense [ITU-X.200], are commonly used terms, finer gradations are needed. For the most part, only relative layer between two technologies matters, i.e., which is at a "higher" or "lower" layer, not whether they are precisely Layer 2 or Layer 3 or Layer 2.718281828459045 or Layer (2 + 7i).

To a general approximation, a device at Layer X sees all lower layer devices, that is devices at Layer Y where X > Y, as transparent. In other words, with the possible exception of some minor implementation details, "layer violating" optimizations, or odd corner cases, two devices at layer X don't particularly care if there are devices at layer Y (or lower) between them.

On the other hand, to devices at Layer Y, all higher layer devices, that is devices at Layer X where X > Y, act as boundaries. That is, Layer X (or higher) devices bound a cloud of such Layer Y devices.

In the past, when things were simpler, one could generally understand networks by distinguishing three layers as shown below:

```
+------------------+
| User End Station |
+---+-------+------+
    |       |
    |  +----+------+
    |  | L3 Router |
    |  +-----+-----+
    |        |
 +--+--------+--+
 |    Bridge    |
 +--------------+
```

Figure 1. Simple Layers

The above diagram is meant to indicate that user end stations are at the highest relative layer, Layer 3 routers are at an intermediate layer, and bridges are at the lowest layer. The vertical lines mean that you can have bridges and routers between and directly connected to user end stations and bridges between and directly connected to routers.

The two types of devices above bridges act as boundaries for a bridging area. That is, user end stations and Layer 3 routers bound a bridged LAN (Local Area Network). To Layer 3 routers, bridges are approximately transparent but user end stations bound a routed area. And, finally, both bridges and Layer 3 routers are pretty much transparent to communications between user end stations.

2.2 Basic Peering

In the cases we are discussing, if two devices are at the same layer, there is a significant protocol related to the device type in which (1) they peer with each other, (2) devices at lower layers are generally transparent to and do not interfere with such peering, and (3) devices at a higher layer block the protocol and do not permit peering through such higher layer devices.

For example, consider the diagram below

```
        +----------+                                  +----------+
        | User End |                 peer             | User End |
        |  Station |..................................|  Station |
        +--+----+--+                                  +--+---+---+
          /      \                                       |   |
         |        |                                     /     \
  +------+-+not +-+------+     peer    +---------+     |       |
  | Router |peer| Router |.............| Router  |     |       |
  +--+-----+    +----+---+             +--+---+--+    /         \
     |               |                   /     \     |           |
     |               |                  /       \    |           |
+----+---+        +--+-----+peer+------+-+     +-+---+--+     +--+-----+
| Bridge |  not   | Bridge |....| Bridge | not | Bridge | not | Bridge |
|        |  peer  |        +----+        | peer|        | peer|        |
+--------+        +--------+    +--------+     +--------+     +--------+
```

Figure 2. Simple Layered Peering

As shown in this diagram, for the model in this document, devices at the same level peer if and only if there are no higher layer devices intervening.

How does this simple peering and layering work? It is generally implemented, as described below, by the discarding or propagation of frames based on their destination MAC address or their protocol type (typically represented by an Ethertype). (There are additional details not covered here for the sake of brevity such as registration protocols, OAM, link level protocols, and IEEE 802.1 Two-Port MAC Relays.)

2.2.1 Bridges

At the bridging and link layers there are reserved MAC multicast addresses that are used, particularly the block from 01-80-C2-00-00-00 to 01-80-C2-00-00-0F [802.1Q]. From the beginning, the specifications for bridges included a requirement to discard any frame sent to an address in this block if the bridge did not understand a protocol that used that address.

2.2.2 Layer 3 Routers

Layer 3 routers normally only recognize or forward frames in the specific Layer 3 protocol(s) they are routing and those related to the routing protocol itself. For example, an IPv4/IPv6 router will recognize or forward only IPv4/IPv6 packets (including IPv4/IPv6 multicast if it handles such traffic) and Layer 3 routing control frames such as those for Layer 3 IS-IS.

(IPv4/IPv6 multicast uses MAC multicast addresses 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF (IPv4) and 33-33-00-00-00-00 to 33-33-FF-FF-FF-FF (IPv6) [RFC5342] and Layer 3 IS-IS routing uses MAC multicast addresses 01-80-C2-00-00-14 and 01-80-C2-00-00-15 [IS-IS].)

Layer 3 routers normally do not route frames sent to any of the bridging and link layer multicast addresses thus blocking bridge peering and properly limiting the scope of link protocols. But bridges forward IS-IS routing frames, IPv4 and IPv6 multicast frames and, of course, unicast frames addressed to a router or end station. Thus, of the devices we are discussing in this section, bridges can transparently connect Layer 3 routers but Layer 3 routers block bridging protocols and bound bridged LANs.

2.2.3 User End Stations

A pure user end station does not normally forward any frames received. Thus it clearly meets the layering criterion of blocking the peering of devices at all lower layers. Devices cannot peer if they cannot exchange frames. (Of course, it is possible to have what is thought of as a user end station also act like a bridge or router or whatever, but then it isn't a pure user end station any more, is it?) An example of a protocol by which end stations peer is TCP/IP.

But wait, you say, it is common for an end station to speak TCP/IP with a bridge or a router, for SNMP or SSH or the like. Actually, the best way to look at such interactions, and the way they are commonly implemented, is that the TCP/IP interactions with a bridge or router are with a virtual end station inside that bridge or router. To have included this in Figure 2, we could draw an end station box at the top for each bridge or router box and draw a link from the end station down to the corresponding bridge or router. Thus the model of end stations peering with each other using TCP/IP is pretty much correct.

2.3 More Layers

The world is now more complex than that described above. There can be quite a number of layers but, for the purposes of this document, the five layers shown in the diagram below are adequate.

```
                   +--------------------------------+
                   |        User End Station        |
                   +-+---+----+-------------------+-+
                     |   |    |                   |
                     |   | +--+---------------+   |
                     |   | |    L3 Router     |   |
                     |   | +----+--------+--+-+  /
                     |   |      |        |  |   /
                     | +-+------+------+ |   \ /
                     | |    RBridge    | |    X
                     | +--+-------+----+ |   /  \
                     |    |       |      |  |    \
                     |    | +-----+------+--+-+   \
                     |    | | Customer Bridge |   |
                     |    | +-------+---------+   |
                     |    |         |             |
                   +-+----+---------+-------------+-+
                   |        Provider Bridge         |
                   +--------------------------------+
```

Figure 3. More Layers

As in Figure 1, the position of a box in this diagram corresponds to the relative layer of the device type. And the more or less vertical connections, which exist between every pair of types indicate that it is workable to have devices of any type shown between and directly connected to instances of any higher layer device shown.

The additions are a layer for RBridges (Routing Bridges), devices that implement the IETF TRILL standard [RFC6325] [RFC6326], and the splitting of the bridge layer into Customer Bridges and Provider

Bridges. RBridges are discussed in Section 2.3.1, Customer Bridges and VLANs are discussed in Section 2.3.2, and Provider Bridges and Provider VLANs are discussed in Section 2.3.3.

The transparency and bounding properties of layers, depending on their relative position, are as before. Any of the four types of devices shown layered above provider bridges will bound a provider bridged LAN. To customer bridges, provider bridges are approximately transparent, while RBridges, Layer 3 routers, and user end stations will bound a customer bridged LAN. To RBridges, customer and provider bridges are approximately transparent while Layer 3 routers and user end stations bound an RBridge campus. To Layer 3 routers, bridging and RBridges are all approximately transparent while user end stations bound a routed area. And user end stations see all four types of devices layered below user end stations as approximately transparent.

2.3.1 RBridges (Routing Bridges)

RBridges are devices that implement the IETF TRILL standard. (Approval of the TRILL base protocol [RFC6325] as an IETF standard was announced 15 March 2010. Approval of the TRILL base protocol specific IS-IS code points and formats [RFC6326] used as an IETF standard was announced 9 February 2011.)

There have been endless arguments about whether RBridges are routers or bridges. They are neither. They are a new type of device that is demonstrably higher layer than a Layer 2 bridge, because they bound bridging protocols such as spanning tree and stop bridges from peering with each other, and demonstrably lower layer than Layer 3 routing because they are transparent to Layer 3 routing such as IS-IS. So Layer 3 routers can peer through RBridges.

Nevertheless, when looked at in one way, RBridges are a type of router because they implement a Hop Count, can do equal cost multi-path, swap the outer link header on each RBridge hop, etc. But, looked at another way, they appear to be a type of bridge because they transparently deliver frames unmodified, can provide useful plug and play service with zero configuration, honor frame customer VLANs and priorities, and the like.

Arguing about what an RBridge "really" is like arguing about whether a proton is really a wave or a particle. The fact that you can perform experiments that provide very strong evidence that a proton is a wave and other experiments that provide the same for it being a particle does not make it a wave or just a particle. A proton is really just a proton and has wave/particle duality. Just so, the fact that you can present strong arguments that an RBridge is a router or that an RBridge is a bridge does not make RBridges be one of those types. RBridges are just RBridges, a new type of device at a new layer.

Looking downward in our layering and peering model from RBridges, RBridges as currently standardized do not forward frames sent to any of the addresses in the basic 01-80-C2-00-00-00 to 01-80-C2-00-00-0F bridging and link protocols block. Thus they bound and are layered above bridging protocols and they appropriately scope link protocols. In particular, this means they bound the various versions of the spanning tree protocol. It was always a goal of TRILL to bound the spanning tree protocol due to its poor performance in large networks [RFC5556]. RBridge ports may still interact with bridging and/or link protocols but those bridging and/or link protocols cannot communicate through an RBridge between ports of that RBridge.

The TRILL protocol itself, including IS-IS control frames supporting TRILL, uses unicast frames addressed to RBridge ports and multicast frames sent to MAC addresses in the block from 01-80-C2-00-00-40 to 01-80-C2-00-00-4F. That block has been reserved exclusively for TRILL use by the IEEE Registration Authority [RegAuth]. Since these addresses have no special meaning to bridges, bridges forward them normally and thus bridges are transparent to TRILL.

On the other hand, looking up our layering and peering model from RBridges, because this block of TRILL multicast addresses has no special meaning to Layer 3 routers, frames addressed to them are discarded by Layer 3 routers, bounding the RBridge campus. Thus RBridges are layered below Layer 3 routers. User end stations also bound an RBridge campus, even if they are multi-port, because the don't normally forward anything.

The default for a bridge is to forward frames it doesn't know anything about. The default for a Layer 3 router is to discard frames it doesn't know anything about. The default for a user end station is to forward no frames.

2.3.2 Customer Bridges and VLANs

(The discussion of bridge types and VLANs in this and the immediately following section may seem a bit tedious but stick with it, they are of some relevance to the topic of this document.)

Bridging worked well enough that there was a desire to share bridged LANs across multiple Layer 2 communities. To differentiate these communities, a "tag" was specified to indicate the particular "VLAN" (Virtual LAN) a frame was in. It consisted of the Ethertype 0x8100 followed by 2 bytes that include a 12-bit VLAN identifier. (For brevity, the use of the remaining four bits in these two bytes will be ignored.) This tag goes after the MAC destination and source addresses and before the payload in Ethernet frames. It labels the frame as being in the VLAN indicated. Use of other than a default VLAN requires configuration.

Devices at different layers commonly treat VLANs differently but VLAN treatment is a characteristic that can vary for different devices at the same layer:

Bridges: Typically data frames sent between VLAN-aware bridges are VLAN tagged but, since most end stations are not VLAN-aware, those sent to/from end stations are usually not. The VLAN of an untagged frame received by a VLAN aware bridge is typically determined by the port on which it arrives but may be determined by the frame's protocol or other factors. Unless a VLAN group or the like is configured, bridges keep data in different VLANs isolated. Bridge ports can be configured to filter on VLAN.

RBridges: Customer VLANs are treated by RBridges in a manner similar to bridges. There are differences but they are not relevant to this document.

Layer 3 Routers: Some Layer 3 routers are VLAN aware and some are not. They typically treat data in different VLANs arriving at a port as arriving on different virtual ports. In this case, the data internal to the Layer 3 router has typically lost its VLAN tagging and the router may not consider VLAN identity in deciding which port or ports to output the packet on or whether to drop a packet. If VLAN unaware, a Layer 3 router treats the VLAN tag as part of the data; however, that data might not be routed because, if the VLAN tag Ethertype was visible to the router, it would not be recognized as a type of Layer 3 traffic to route.

User End Stations: User end stations are generally VLAN unaware and also might treat a VLAN tag as part of the data; however, in that case the data would not typically be processed because the VLAN tag Ethertype would not be recognized as a type of traffic a VLAN unaware end station is interested in.

When provider bridges and VLANs, discussed in Section 2.3.3, were added to IEEE 802.1, the previously standardized bridges and VLANs, discussed above, were retroactively called "customer" bridges and "customer" VLANs to distinguish them from provider bridges and VLANs.

2.3.3 Provider Bridges and VLANs

"Provider" facilities derive from the concept of a carrier providing Ethernet connectivity to customers. As a first approximation, they would like to be transparent to the customer devices and traffic. So, naturally, Provider Bridges are at a lower layer than customer bridges. As a result, customer bridges and all higher layer devices block peering between provider bridges and bound provider bridged LANs. This is primarily accomplished by (1) provider bridges being transparent to multicast address 01-80-C2-00-00-00, the address used for Customer Bridge spanning tree peering and the like and (2) provider facilities using the multicast address 01-80-C2-00-00-08, a destination address customer bridges discard, for provider bridge peering.

Of course, the bits don't know anything about business relationships so "provider" facilities can be used inside the network of what a carrier would consider a "customer".

Provider Bridges use VLANs but they use a different tag. The VLAN ID field is the same size, 12 bits, but the Ethertype is different (0x88A8) and they are called S-tags, for service tags, and customer VLAN tags are now commonly called C-tags.

The first type of Provider Bridge specified use of S-tags and S-VLANs to separate the traffic from different customers or services. If there are already C-tags in place, this results in two nested VLAN tags, an S-tag and then a C-tag relative to that S-tag. This is colloquially known as "Q-in-Q".

To the extent that provider bridged LANs are supplying a service to multiple different customers, provider facilities want to protect themselves from customer behavior. They are typically more configuration dependent than customer bridges. If customer facing "edge" ports and internally connected ports are rigorously configured, then the provider bridging should be relatively immune to customers forging provider control frames or the like. In fact, such frames need not have been "forged". It can easily be the case that what is desired is a second order provider or the like, connecting "customer" LANs that are already using the provider bridging protocols.

"Q-in-Q", or nested VLAN tags, do not isolate provider bridges from having to learn customer MAC addresses for transit traffic and use of S-tags in the obvious way to isolate services limits the number of services to 4K. Provider Backbone Bridges (PBBs) overcame these limitations. PBBs use a "MAC-in-MAC" encapsulation so that customer MAC addresses are nested inside PBB MAC addresses and those customer

MAC addresses need only be learned by edge PBBs. PBBs also use an expanded tag, called an I-tag, that provides a 24-bit Service

Instance Identifier that can be used, in effect, as a VLAN. PBB can make use of an outer VLAN tag that uses the same Ethertype as the S-VLAN tag but is called a "B-VLAN tag" (backbone VLAN) and is used for different purposes than the S-VLAN, purposes such as traffic engineering.

Customer and provider bridging are both standardized by IEEE 802.1 and they are more entangled than one might expect for two different layers. For example, there are "provider aware" customer bridges that use S-tags on frames they submit to provider bridges to indicate the service desired for the frame. However, generally, all layers above customer bridging are S-tag ignorant; they treat an S-tag as just part of the data

What happens when an RBridge gets a frame with an S-tag? This is a trick question. At first glance, it seems pretty ugly. RBridges as currently specified don't recognize S-tags and treat them as part of the payload. An RBridge campus could ingress such a frame and egress it, still S-tagged, from another port or ports of the same or some other RBridge, perhaps causing some confusion.

But, wait a minute, how is this any different from what any provider-ignorant customer bridge would do if it got a frame starting with an S-tag? Or what a Layer 3 router might do? In fact, it is pretty much the same.

Asking this trick question is like asking what happens if you divide 1 by 0. If you have gotten to a place where you are trying to divide 1 by 0, you've already made a mistake. Just so, if you have gotten to the point where a frame intended for a provider device, as denoted by an S-tag, is being sent to a customer device that does not understand S-tags, particularly one that will likely forward it, such as a customer bridge or an RBridge, your network is already misconfigured.

3. A Prevalent Confusion

When the TRILL Working Group was starting up in the IETF, IEEE 802.1 was working on its Provider Backbone Bridging (PBB) project. It happens that both protocols do what is called "MAC-in-MAC", although they do it for different but overlapping sets of reasons. These reasons include, in the TRILL protocol, providing a place for a Hop Count and options, and in the PBB amendment to the 802.1Q protocol, providing a place for a 24-bit Service Instance Identifier and a new priority field. (There are other differences.) In both cases original destination and source MAC addresses are nested inside new destination and source MAC address fields that are used inside the RBridge campus (TRILL) or Provider Backbone Bridging region (PBB) and these new address fields are discarded and the original addresses are restored on exit from that campus or region.

The coincidence of TRILL and PBB both doing "MAC-in-MAC" has been a source of endless confusion. For years, at essentially every TRILL Working Group meeting someone would ask a question that made it clear that, perhaps because TRILL and PBB both did "MAC-in-MAC", the questioner believed that TRILL *must* be a provider protocol appropriate for use by carriers connecting parts of customer networks. But encapsulation, or a "MAC-in-MAC tag", or whatever you want to call it, has nothing to do with the relative layer of a protocol in the model discussed in this document. Based on that model, RBridges, as currently standardized, are customer devices above the customer bridge layer, while PBBs are provider devices at the Provider Bridging layer.

For example, there is no problem connecting different parts of an RBridge campus together through provider bridging. If you used Provider Backbone Bridges for such provider bridging, as shown below, you would have two nested levels of "MAC-in-MAC" inside the provider bridged LAN for the RBridge campus TRILL Data frames. The provider bridged LAN would look to TRILL like just a transparent part of a TRILL level link between RBridges.

```
       +---------+     +-----+       +-----+     +---------+
   ----| RBridge |-----| PBB |-------| PBB |-----| RBridge |----
    ^  +---------+  ^  +-----+   ^   +-----+  ^  +---------+  ^
    |               |            |            |               |
   Note 1         Note 2       Note 3       Note 2        Note 1
```

Figure 4

Note 1: Zero or one level of MAC-in-MAC depending on the extent of
   the RBridge campus.
Note 2: Inside an RBridge campus. One level of MAC-in-MAC.

Note 3: Inside Provider Back Bridged region that is in turn inside an RBridge campus. Two levels of MAC-in-MAC.

The RBridges in the above diagram peer with each other through the PBBs, becoming part of one RBridge campus that encompasses the entirety of the provider bridge LAN that includes the PBBs shown. The RBridges are part of the bounds of that provider bridged LAN. If there are any other RBridges connected elsewhere to that provider bridged LAN or to customer bridges connected to the that provider bridged LAN, those RBridges will also be part of that RBridge campus.

On the other hand, if the nesting is reversed, the Provider Backbone Bridges will, of course, be unable to peer through the higher layer RBridges and the RBridges will bound any adjacent provider bridged LAN(s). As a result, for traffic between end stations that are off the left and right edges of the page in Figure 5 and assuming no additional RBridges between the RBridges shown and those end stations, there will be no more than one level of "MAC-in-MAC" nesting as shown below.

```
       +-----+     +---------+       +---------+     +-----+
   ----| PBB |-----| RBridge |-------| RBridge |-----| PBB |----
    ^  +-----+  ^  +---------+   ^   +---------+  ^  +-----+  ^
    |           |                |                |           |
   Note 4     Note 5           Note 6           Note 5    Note 4
```

Figure 5

Note 4: Zero or one level of MAC-in-MAC depending on the extent of the PBB region.
Note 5: Native frames with zero levels of MAC-in-MAC.
Note 6: Inside an RBridge campus. One level of MAC-in-MAC.

In Figure 5, because the PBBs cannot peer through the RBridges, they are each part of a separate PBB region unless there is a path, not shown, uniting them into a single PBB region.

You can shuffle the boxes around in the above diagrams in other ways, but this does not reveal anything particularly interesting. For example:

```
           |           |   |           |           |   |
        +-----+     +---------+     +-----+     +---------+
    ----| PBB |-----| RBridge |-----| PBB |-----| RBridge |----
        +-----+     +---------+     +-----+     +---------+
           |           |   |           |           |   |
```

Figure 6

Looking at Figure 6, it is certainly possible to confuse yourself, perhaps if you try to think about the RBridges as simultaneously being bridges and routers and apply some particular ideas about how bridge and routers are "supposed" to work. But, if you apply the simple principles given in this document, it is easy to see what happens. From the RBridges' point of view, the PBBs are approximately transparent, so all of the above diagram is part of a single RBridge campus. From the PBBs' point of view, PBBs cannot peer through RBridges so the RBridge facing PBB ports are PBB edge ports and the PBBs shown are parts of one or two PBB regions depending on whether there is a PBB path between them. (No such path is shown in Figure 6.)

For Figures 4 through 6 you could replace "PBB" and "RBridge" with any relatively lower layer and relatively higher layer devices with the same results as to regions and bounds. (The "MAC-in-MAC" comments above would only apply to the extent that one or both of the devices types were RBridges or the PBB type of Provider Bridge, the only devices discussed that do "MAC-in-MAC".) The names of the regions involved would change as follows, based on the vocabulary used in this document:

Device	Region Name in this document
End Station	network
Layer 3 router	routed area
RBridge	campus
Customer Bridge	bridged LAN
Provider Bridge	provider bridged LAN

4. Shortest Path Bridges

Shortest Path Bridges (SPBs) are being specified by IEEE 802.1 through their [802.1aq] drafts (and in the applicable parts of the IEEE virtual LAN bridging standard [802.1Q] that is to be amended by 802.1aq). ([802.1aq] is anticipated to become an IEEE Standard sometime in 2012.)

Shortest Path Bridges have been somewhat of a moving target. They started as a variety of Provider Bridge operating within the Provider Bridging layer. Later, a type of SPB based on Provider Backbone Bridging (PBB) was added. We will refer to these as PBB SPB and non-PBB SPB. (The IEEE 802.1 abbreviation for PBB SPB is SPBM (where M stands for MAC Mode) and for non-PBB SPB, it is SPBV (where V stands for VID (VLAN ID) Mode.) Like previous Provider Backbone Bridges, PBB SPBs only peer with each other over point-to-point links.

SPBs of either type can forward frames using bridging mechanisms that are configured to provide least-cost paths. In the earliest versions of SPB, this was done with many instances of spanning tree protocol but later SPB drafts specify the use of the IS-IS protocol to configure bridge-forwarding mechanisms. All versions of SPB so far have also retained the ability to forward using variations of the spanning tree protocol. Which method is used for a particular frame is determined by that frame's VLAN and the SPB's configuration.

Earlier SPB drafts specified only the use of the standard multicast addresses used for Layer 3 routing for SPB IS-IS. While it might seem this would interfere with Layer 3 routing, as long as the ports for PBB SPB are properly configured as to which are edge ports and which are internal ports, then any Layer 3 IS-IS control frames transiting a SPB region using the PBB type of SPB will be encapsulated and not falsely recognized as SPB IS-IS control frames. However, this does not help the non-PBB version of SPB; so more recent SPB drafts include the proposed allocation of provider bridging layer multicast addresses, presumably from within the bridging and link protocols multicast address block (01-80-C2-00-00-00 to 01-80-C2-00-00-0F), for use in non-PBB SPB IS-IS.

In addition, recent versions of the SPB draft have suggested that customer bridging layer multicast addresses be assigned for optional use in sending SPB IS-IS control frames, presumably also from the bridging and link multicast address block, and suggest that there should be a way to have what would appear to be customer bridging layer SPBs.

(As discussed in Section 2.3.1, for TRILL IS-IS, RBridges as currently standardized use multicast addresses dedicated to the TRILL protocol. These addresses do not overlap with the Layer 3 IS-IS multicast addresses or with any of the bridging and link protocols multicast addresses.)

5. Conclusions

This document describes a model of switching device layers and peering that the authors believe corresponds to common ideas of layers for such devices. Based on this model, RBridges implementing the IETF TRILL standard are compatible, well behaved devices that cleanly fit into a specific relative layer of their own.

Also based on this device layer and peering model, the current IEEE 802.1 Shortest Path Bridging (SPB) draft appears to specify similarly compatible and well behaved devices. SPBs were originally at the Provider Bridging layer but their specification appears to be undergoing extension so they may also optionally operate at the Customer Bridging layer.

As required by the original TRILL WG Charter, a review by the IEEE 802.1 Working Group of the TRILL base protocol specification was requested before its approval as an IETF standard. This resulted in the IEEE 802.1 Liaison of 1 March 2009 to the IETF [Liaison] which states in part:

> "By inserting RBridges into a C-VLAN network a network structure is created that is incompatible with current 802.1Q S-VLAN and B-VLAN network architecture."

The IEEE 802.1 "S-VLAN and B-VLAN network architecture" is, as far as the authors can tell, the layer at which Provider Bridges and Provider Backbone Bridges operate. RBridges work just fine with provider bridging in accordance with their relative layer (see Figure 3). Thus the authors believe that the IEEE 802.1 Working Group's assertion of "incompatibility" is incorrect. And the IEEE 802.1 Working Group liaison's subsequent intimation that such mixed RBridge and bridge networks would be, to use the word chosen by 802.1, "broken", is equally incorrect.

RBridges as currently standardized and the latest Shortest Path Bridging draft have similar goals when viewed at a high level of abstraction. It is true that they achieve these goals through different mechanisms and can be considered to be in competition; however, the authors are unable to find any way in which they currently conflict in a technical sense. Given that SPB is not yet an IEEE standard and continues to evolve, whether this will be true when 802.1aq is finally approved as an IEEE standard (anticipated to occur in 2012) cannot, unfortunately, be determined at this time.

6. IANA Considerations

This document requires no IANA actions. RFC Editor: Please delete this section before publication.

7. Security Considerations

This is an informational document that does not consider security questions or threats.

8. Informative References

[802] - IEEE 802, "IEEE Standard for Local and Metropolitan Area Networks / Overview and Architecture", 802-2001, 6 December 2001.

[802.1aq] - IEEE 802.1, "Local and Metropolitan Area Networks / Virtual Bridged Local Area Networks / Amendment 9: Shortest Path Bridging", Draft P802.1aq/D4.0, 14 June 2011.

[802.1Q] - IEEE 802.1, "IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks", IEEE Std 802.1Q-2011, May 2011.

[IS-IS] - ISO/IEC 10589:2002, Second Edition, "Intermediate System to Intermediate System Intra-Domain Routeing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)", 2002.

[ITU-X.200] - ITU-T, "X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model", July 1994.

[Liaison] - IEEE 802.1, <https://datatracker.ietf.org/documents/LIAISON/file710.pdf> or <http://www.ieee802.org/1/files/public/docs2009/liaison-to-trill-wg-0309.pdf>, 1 March 2009.

[RegAuth] - IEEE Registration Authority, http://standards.ieee.org/develop/regauth/index.html

[RFC1195] - Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.

[RFC5342] - Eastlake 3rd, D., "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters", BCP 141, RFC 5342, September 2008.

[RFC5556] - Touch, J. and R. Perlman, "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement", RFC 5556, May 2009.

[RFC6325] - Perlman, R., D. Eastlake, D. Dutt, S. Gai, and A. Ghanwani, "RBridges: Base Protocol Specification", RFC 6325, July 2011.

[RFC6326] - Eastlake, D., A. Banerjee, D. Dutt, R. Perlman, and A. Ghanwani, "TRILL Use of IS-IS", RFC 6326, July 2011.

9. Normative References

This is an empty normative references section to make the nits checker happy. As an informational document, there are no normative references. RFC Editor: please delete this section before publication.

Authors' Addresses

Donald Eastlake, 3rd
Huawei Technologies (USA)
155 Beaver Street
Milford, MA 01757 USA

Tel: +1-508-333-2270
EMail: d3e3e3@gmail.com

Susan Hares
Huawei Technologies (USA)
2330 Central Expressway,
Santa Clara, CA 95050, USA

EMail: shares@huawei.com

Jon Hudson
Brocade
130 Holger Way
San Jose, CA 95134 USA

EMail: jon.hudson@gmail.com

Copyright, Disclaimer, and Additional IPR Provisions