INTAREA
Internet-Draft
Intended status: Standards Track
Expires: October 1, 2017
E. Nordmark
March 30, 2017

IP over Intentionally Partially Partitioned Links
draft-ietf-intarea-ippl-00

Abstract

IP makes certain assumptions about the L2 forwarding behavior of a multi-access IP link. However, there are several forms of intentional partitioning of links ranging from split-horizon to Private VLANs that violate some of those assumptions. This document specifies that link behavior and how IP handles links with those properties.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IPv4 and IPv6 can in general handle two forms of links; point-to-point links when only have two IP nodes (self and remote), and multi-access links with one or more nodes attached to the link. For the multi-access links IP in general, and particular protocols like ARP and IPv6 Neighbor Discovery, makes a few assumptions about transitive and reflexive connectivity i.e., that all nodes attached to the link can send packets to all other nodes.

There are cases where for various reasons and deployments one wants what looks like one link from the perspective of IP and routing, yet the L2 connectivity is restrictive. A key property is that an IP subnet prefix is assigned to the link, and IP routing sees it as a regular multi-access link with link-local unicast and multicast addresses functioning as expected. But a host attached to the link might not be able to send packets to all other hosts attached to the link. The motivation for this is outside the scope of this document, but in summary the motivation to preserve the single link view as seen by IP routing is to conserve IP(v4) address space, and the motivation to restrict communication on the link could be due to (security) policy or to wireless connectivity approaches.

This intentional and partial partition appears in a few different forms. For DSL [TR-101] and Cable [DOCSIS-MULPI] the pattern is to have a single access router on the link, and all the hosts can send and receive from the access router, but host-to-host communication is blocked. A richer set of restrictions are possible for Private VLANs (PVLAN) [RFC5517], which has a notion of three different ports i.e. attachment points: isolated, community, and promiscuous. Note that other techniques operate at L2/L3 boundary like [RFC4562] but those are out of scope for this document.

The possible connectivity patterns for Private VLANs appears to be a super-set of the DSL and Cable use of split horizon, thus this document specifies the PVLAN behavior, shows the impact on IP/ARP/ND, and specifies how IP/ARP/ND must operate to work with PVLAN.

If private VLANs, or the split horizon subset, has been configured at layer 2 for the purposes of IPv4 address conservation, then that layer 2 configuration will affect IPv6 even though IPv6 might not have the same need for address conservation.

The cases covered in this document are where the link has been intentionally partitioned, which is different from the cases where a collection of links are joined to have a common IP subnet prefix. An example of the differences is the expected behavior for packets sent to link-local IP addresses. The issues for such multi-link subnets are described in [RFC4903].

2. Keywords and Terminology

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

a The following terms from [RFC4861] are used without modifications:

node	a device that implements IP.
router	a node that forwards IP packets not explicitly addressed to itself.
host	any node that is not a router.
link	a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IP. Examples are Ethernets (simple or bridged), PPP links, X.25, Frame Relay, or ATM networks as well as Internet-layer (or higher-layer) "tunnels", such as tunnels over IPv4 or IPv6 itself.
interface	a node's attachment to a link.
neighbors	nodes attached to the same link.

This document defines the following set of terms:

bridge a layer-2 device which implements 802.1Q
port a bridge's attachment to another bridge or to a node.

3. Private VLAN

A private VLAN is a structure which uses two or more 802.1Q (VLAN) values to separate what would otherwise be a single VLAN, viewed by IP as a single broadcast domain, into different types of ports with different L2 forwarding behavior between the different ports. A private VLAN consists of a single primary VLAN and multiple secondary VLANs.

From the perspective of both a single bridge and a collection of interconnected bridges there are three different types of ports use to attach nodes plus an inter-bridge port:

- o Promiscuous: A promiscuous port can send packets to all ports that are part of the private VLAN. Such packets are sent using the primary VLAN ID.
- o Isolated: Isolated VLAN ports can only send packets to promiscuous ports. Such packets are sent using an isolated VLAN ID.
- o Community: A community port is associated with a per-community VLAN ID, and can send packets to both ports in the same community VLAN and promiscuous ports.
- o Inter-bridge: A port used to connect a bridge to another bridge.

Private VLANs is an implementation of asymmetric VLANs and Rooted-Multipoint connectivity. Private VLANs were an integral part of [IEEE802.1Q-1998]. The mapping between the mechanisms in that standard plus the above Private VLAN notion of different types of ports to the L2 forwarding behavior are somewhat complex and described in the following sections.

3.1. Bridge Configuration for Private VLANs

This text is reproduced from [IEEE802.1-LIAISON] to ensure this specification together with [IEEE802.1Q-1998] provide a complete standard on which we can describe the IP implications. Note that this section uses slightly different terminology than above e.g., "root port" instead of "promiscuous port".

"Private VLANs" as described in this document 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.

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:

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

3.2. Resulting Bridge Behavior

Once a bridge or a set of interconnected bridges have been configured with both the primary and isolated VLAN ID, and zero or more community VLAN IDs associated with the private VLAN, it results in the following L2 forwarding behaviors for the bridge:

- o A packet received on an isolated port will not be L2 forwarded out an isolated or community port; it will (subject to bandwidth/ resource issues) be L2 forwarded out promiscuous and inter-bridge ports.
- o A packet received on a community port will not be L2 forwarded out an isolated port or a community port with a different VLAN ID; it will be L2 forwarded out promiscuous and inter-bridge ports as well as community ports that have the same community VLAN ID.
- o A packet received on a promiscuous port will be L2 forwarded out all types of ports in the private VLAN.
- o A packet received on an inter-bridge port with an isolated VLAN ID will be L2 forwarded as a packet received on an isolated port.

- o A packet received on an inter-bridge port with a community VLAN ID will be L2 forwarded as a packet received on a community port associated with that VLAN ID.
- o A packet received on an inter-bridge port with a promiscuous VLAN ID will be L2 forwarded as a packet received on a promiscuous port.

In addition to the above VLAN filtering and implied MAC address learning rules, the L2 packet forwarding is also subject to the normal 802.1Q rules with blocking ports due to spanning-tree protocol etc.

4. IP over IPPL

When IP is used over Intentionally Partially Partitioned links like private VLANs the normal usage is to attached routers (and potentially other shared resources like servers) to promiscuous ports, while attaching other hosts to either community or isolated ports. If there is a single host for a given tenant or other domain of separation, then it is most efficient to attach that host to an isolated port. If there are multiple hosts in the private VLAN that should be able to communicate at layer 2, then they should be assigned a common community VLAN ID and attached to ports with that VLAN ID.

The above configuration means that hosts will not be able to communicate with each other unless they are in the same community. However, mechanisms outside of the scope of this document can be used to allow IP communication between such hosts e.g., by having firewall or gateway in or beyond the routers connected to the promiscuous ports. When such a policy is in place it is important that all packets which cross communities are sent to a router, which can have access-control lists or deeper firewall rules to decide which packets to IP forward.

5. IPv6 over IPPL

IPv6 Neighbor Discovery [RFC4861] can be used to get all the hosts on the link to send all unicast packets except those send to link-local destination addresses to the routers. That is done by setting the L-flag (on-link) to zero for all of the Prefix Information options. Note that this is orthogonal to whether SLAAC (Stateless Address Auto-Configuration) [RFC4862] or DHCPv6 [RFC3315] is used for address auto-configuration. Setting the L-flag to zero is RECOMMENDED configuration for private VLANs.

If the policy includes allowing some packets that are sent to link-local destinations to cross between different tenants, then some for

of NS/NA proxy is needed in the routers, and the routers need to IP forward packets addressed to link-local destinations out the same interface as REQUIRED in [RFC2460]. If the policy allows for some packets sent to global IPv6 address to cross between tenants then the routers would IP forward such packets out the same interface. However, with the L=0 setting those global packets will be sent to the default router, while the link-local destinations would result in a Neighbor Solicitation to resolve the IPv6 to link-layer address binding. Handling such a NS when there are multiple promiscuous ports hence multiple routers risks creating loops. If the router already has a neighbor cache entry for the destination it can respond with an NA on behalf of the destination. However, if it does not it MUST NOT send a NS on the link, since the NA will be received by the other router(s) on the link which can cause an unbounded flood of multicast NS packets (all with hoplimit 255), in particular of the host IPv6 address does not respond. Note that such an NS/NA proxy is defined in [RFC4389] under some topological assumptions such as there being a distinct upstream and downstream direction, which is not the case of two or more peer routers on the same IPPL. For that reason NS/NA packet proxies as in [RFC4389] MUST NOT be used with IPPL.

IPv6 includes Duplicate Address Detection [RFC4862], which assumes that a link-local IPv6 multicast can be received by all hosts which are attached to the same link. That is not the case in a private VLAN, hence there could potentially be undetected duplicate IPv6 addresses. However, the DAD proxy approach [RFC6957] defined for split-horizon behavior can safely be used even when there are multiple promiscuous ports hence multiple routers attached to the link, since it does not rely on sending Neighbor Solicitations instead merely gathers state from received packets. The use of [RFC6957] with private VLAN is RECOMMENDED.

The Router Advertisements in a private VLAN MUST be sent out on a promiscuous VLAN ID so that all nodes on the link receive them.

6. IPv4 over IPPL

IPv4 [RFC0791] and ARP [RFC0826] do not have a counterpart to the Neighbor Discovery On-link flag. Hence nodes attached to isolated or community ports will always ARP for any destination which is part of its configured subnet prefix, and those ARP request packets will not be L2 forwarded by the bridges to the target nodes. Thus the routers attached to the promiscuous ports MUST provide a robust proxy ARP mechanism if they are to allow any (firewalled) communication between nodes from different tenants or separation domains.

For the ARP proxy to be robust it MUST avoid loops where router1 attached to the link sends an ARP request which is received by

router2 (also attached to the link), resulting in an ARP request from router2 to be received by router1. Likewise, it MUST avoids a similar loop involving IP packets, where the reception of an IP packet results in sending a ARP request from router1 which is proxied by router2. At a minimum, the reception of an ARP request MUST NOT result in sending an ARP request, and the routers MUST either be configured to know each others MAC addresses, or receive the VLAN tagged packets so they can avoid proxying when the packet is received with the promiscuous VLAN ID. Note that should there be an IP forwarding loop due to proxying back and forth, the IP TTL will expire avoiding unlimited loops.

Any proxy ARP approach MUST work correctly with Address Conflict Detection [RFC5227]. ACD depends on ARP probes only receiving responses if there is a duplicate IP address, thus the ARP probes MUST NOT be proxied. These ARP probes have a Sender Protocol Address of zero, hence they are easy to identify.

When proxying an ARP request (with a non-zero Sender Protocol Address) the router needs to respond by placing its own MAC address in the Sender Hardware Address field. When there are multiple routers attached to the private VLAN this will not only result in multiple ARP replies for each ARP request, those replies would have a different Sender Hardware Address. That might seem surprising to the requesting node, but does not cause an issue with ARP implementations that follow the pseudo-code in [RFC0826].

If the two or more routers attached to the private VLAN implement VRRP [RFC5798] the routers MAY use their VRRP MAC address as the Sender Hardware Address in the proxied ARP replies, since this reduces the risk nodes that do not follow the pseudo-code in [RFC0826]. However, if they do so it can cause flapping of the MAC tables in the bridges between the routers and the ARPing node. Thus such use is NOT RECOMMENDED in general topologies of bridges but can be used when there are no intervening bridges.

7. Multiple routers

In addition to the above issues when multiple routers are attached to the same PVLAN, the routers need to avoid potential routing loops for packets entering the subnet. When such a packet arrives the router might need to send a ARP request (or Neighbor Solicitation) for the host, which can trigger the other router to send a proxy ARP (or Neighbor Advertisement). The host, if present, will also respond to the ARP/NS. This issue is described in [PVLAN-HOSTING] in the particular case of HSRP.

When multiple routers are attached to the same PVLAN, whether they are using VRRP, HSRP, or neither, they SHOULD NOT proxy ARP/ND respond to a request from another router. At a minimum a router MUST be configurable with a list of IP addresses to which it should not proxy respond. Thus the user can configure that list with the IP address(es) of the other router(s) attached to the PVLAN.

8. Multicast over IPPL

Layer 2 multicast or broadcast is used by protocols like ARP [RFC0826], IPv6 Neighbor Discovery [RFC4861] and Multicast DNS [RFC6762] with link-local scope. The first two have been discussed above.

Multicast DNS can be handled by implementing using some proxy such as [I-D.ietf-dnssd-hybrid] but that is outside of the scope of this document.

IP Multicast which spans across multiple IP links and that have senders that are on community or isolated ports require additional IP forwarding mechanisms in the routers that are attached to the promiscuous ports, since the routers need to IP forward such packets out to any allowed receivers in the private VLAN without resulting in packet duplication. For multicast senders on isolated ports such IP forwarding would result in the sender receiving the packet it transmitted. For multicast senders on community ports, any receivers in the same community VLAN are subject to receiving duplicate packets; one copy directly from layer 2 from the sender and a second copy IP forwarded by the multicast router.

```
                      +------+--------+
                      |     Eth2      |
                      |    Router     | #4 route to other subnets
                      |     Eth1      | Members on Eth1 interface
                      +-------+-------+
             ^                |
             | #3 to VID 10   | | #5 to promisc VID
                              | v
                              |
                      +-------+-------+
                      |               | #6 bridge in promisc VID
                      |    Bridge     |
                      |               | #2 bridge in VID 10
                      +--+--+--+--+---+
                         |  |  |  |
        +----------------+  |  |  +-----------------+
        |             +-----+  +-----+              |
        |             |              |             | | #3 to VID 10
        | ^ #1 to     |              |             | v
        | | VID 10    |              |             |
        |             | | # 7 to     | | # 7 to    | | #7 to promisc VID
        |             | v promisc    | v promisc   | v
        |             |   VID        |   VID       |
        |             |              |             |
        |             |              |             |
        |             |              |             |
        |             |              |             |
   +----+-----+ +-----+----+    +----+-----+ +-----+----+
   | Community| | Community|    | Isolated | | Community|
   |   VID 10 | |   VID 20 |    |   VID 99 | |  VID 10  |
   |   Host 1 | |   Host 2 |    |   Host 3 | |  Host 4  |
   +----------+ +-----+----+    +----------+ +----------+
```

Figure 1: Example upstream multicast duplication

The example in the figure shows where the router has been configured to route multicast packets out the ingress PVLAN interface so that receivers on isolated ports and in other communities will receive packets sent by Host 1. But that has the side effect of Host 4, which is in the same community as Host 1 will receive both a bridged and a routed packet. Alternatively, if the router is configured to not route multicast out the ingress PVLAN interface, then Host 2 and Host 3 would not receive the packet.

For that reason it is NOT RECOMMENDED to configure outbound multicast IP forwarding from private VLANs.

9. DHCP Implications

With IPv4 both a static configuration and a DHCPv4 configuration will assign a subnet prefix to any hosts including those attached to the isolated or community ports. Hence the above robust proxy ARP is needed even in the case of DHCPv4.

With IPv6 static configuration, or SLAAC (Stateless Address Auto-Configuration) [RFC4862] or DHCPv6 [RFC3315] can be used to configure the IPv6 addresses on the interfaces. However, when DHCPv6 is used to configure the IPv6 addresses it does not configure any notion of an on-link prefix length. Thus in that case the on-link determination comes from the Router Advertisement. Hence the above approach of setting L=0 in the Prefix Information Option will result in packets being sent to the default router(s).

Hence no special considerations are needed for DHCPv4 or DHCPv6.

10. Redirect Implications

ICMP redirects can be used for both IPv4 and IPv6 to indicate a better first-hop router to hosts, and in addition for IPv6 can be used to indicate the direct link-layer address to use to send to a node which is on the link. ICMP redirects to another router which attached to a promiscuous port would work since the host can reach it. However, communication will fail if that port is not promiscuous. In addition, the IPv6 redirect to an on-link host is likely to be problematic since a host is likely to be attached to an isolated or community port.

For those reasons it is RECOMMENDED that the sending of IPv4 and IPv6 redirects is disabled on the routers attached to the IPPL.

11. Security Considerations

In general DAD is subject to a Denial of Service attack since a malicious host can claim all the IPv6 addresses [RFC3756]. Same issue applies to IPv4/ARP when Address Conflict Detection [RFC5227] is implemented.

12. IANA Considerations

There are no IANA actions needed for this document.

13. Acknowledgements

The author is grateful for the comments from Mikael Abrahamsson, Fred Baker, Wes Beebee, Hemant Singh, Dave Thaler, Pascal Thubert, and Sowmini Varadhan, and also the IEEE 802.1 Working Group in general and Norm Finn and Steve Haddock in particular for their careful review and providing the text in [IEEE802.1-LIAISON].

14. Appendix: Layer 2 Learning Implications

While not in scope for this document, there are some observations relating to the interaction of IPPL (and private VLANs in particular) and layer 2 learning which are worth mentioning. Depending on the details of how the deployed Ethernet bridges perform learning, a side effect of using a different .1Q tag for packets sent from the routers than for packets sent towards the routers mean that the 802.1Q learning and aging process in intermediate bridges might age out the MAC address entry for the routers MAC address. If that happens packets sent towards the router will be flooded at layer two. The observed behavior is that an ARP request for the router's IP address will result in re-learning the MAC address. Thus some operators work around this issue by configuring the ARP aging time to be shorter than the MAC aging time.

15. References

15.1. Normative References

[IEEE802.1Q-1998]
IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", IEEE Std 802.1Q-1998, 1998, <https://standards.ieee.org/findstds/standard/802.1Q-1998.html>.

(Access Controlled link within page)

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, DOI 10.17487/RFC0826, November 1982, <http://www.rfc-editor.org/info/rfc826>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC6957] Costa, F., Combes, J-M., Ed., Pougnard, X., and H. Li, "Duplicate Address Detection Proxy", RFC 6957, DOI 10.17487/RFC6957, June 2013, <http://www.rfc-editor.org/info/rfc6957>.

15.2. Informative References

[DOCSIS-MULPI] "DOCSIS 3.0: MAC and Upper Layer Protocols Interface Specification", August 2015, <http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-MULPIv3.0-I28-150827.pdf>.

[I-D.ietf-dnssd-hybrid] Cheshire, S., "Discovery Proxy for Multicast DNS-Based Service Discovery", draft-ietf-dnssd-hybrid-06 (work in progress), March 2017.

[IEEE802.1-LIAISON] "Asymmetric (private) VLANs - comments on draft-nordmark-intarea-ippl", March 2017, <https://datatracker.ietf.org/liaison/1510/>.

[PVLAN-HOSTING] "PVLANs in a Hosting Environment", March 2010, <https://puck.nether.net/pipermail/cisco-nsp/2010-March/068469.html>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, DOI 10.17487/RFC3756, May 2004, <http://www.rfc-editor.org/info/rfc3756>.

[RFC4389] Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, DOI 10.17487/RFC4389, April 2006, <http://www.rfc-editor.org/info/rfc4389>.

[RFC4562] Melsen, T. and S. Blake, "MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network", RFC 4562, DOI 10.17487/RFC4562, June 2006, <http://www.rfc-editor.org/info/rfc4562>.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <http://www.rfc-editor.org/info/rfc4903>.

[RFC5227] Cheshire, S., "IPv4 Address Conflict Detection", RFC 5227, DOI 10.17487/RFC5227, July 2008, <http://www.rfc-editor.org/info/rfc5227>.

[RFC5517] HomChaudhuri, S. and M. Foschiano, "Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment", RFC 5517, DOI 10.17487/RFC5517, February 2010, <http://www.rfc-editor.org/info/rfc5517>.

[RFC5798] Nadas, S., Ed., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, DOI 10.17487/RFC5798, March 2010, <http://www.rfc-editor.org/info/rfc5798>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <http://www.rfc-editor.org/info/rfc6762>.

[TR-101] "Migration to Ethernet-Based DSL Aggregation", The Broadband Forum Technical Report TR-101, July 2011, <http://www.broadband-forum.org/technical/download/TR-101_Issue-2.pdf>.

Author's Address

Erik Nordmark
Santa Clara, CA
USA

Email: nordmark@sonic.net