Network Working Group
Internet-Draft
Intended status: Informational
Expires: 9 April 2021

O. Troan
cisco

6 October 2020

IP Point to Point Ethernet subnet model
draft-troan-6man-p2p-ethernet-00

Abstract

Ethernet topology is no longer a shared medium. It is a long time since Ethernet has been a thick yellow cable snaking its way from station to station. Ethernet is now effectively deployed in a hub and spoke topology. With a point to point link between a host and the network device. This memo describes a set of simplications for how to run IP over such links, where the physical topology is exposed in the network layer topology.

Table of Contents

1. Introduction

This memo describes a way of connecting network layer devices across Ethernet, where the physical topology is exposed to the network layer. With 10BASE-T [IEEE.802-3.1990], Ethernet is a hub and spoke network topology with the Ethernet switch as the hub and stations as spokes. While the techniques described in this document in part applies to a bridged or switched network, for the sake of simplicty of explanation only a network where all devices are IP nodes is considered. Most modern Ethernet switches are also IP routers, and of course all Ethernet stations are IP hosts.

> | Suspension of disbelief. This note assumes the reader accepts
> | that Ethernet switches can do IP routing, and for the purpose
> | of this memo the reader should think of anything that is a
> | "hub" in an Ethernet network as an IP router.

This mechanism delivers complete host isolation at the network layer. A host only shares the same network layer link with the default router, and the shared subnet is only the link-local prefix.

The simplest example of this topology is an IP router with a set of Ethernet interfaces (i.e. an Ethernet L3 switch) with one port connecting one IP host. Lets call this network device an "Ethernet Router".

While there are many ways P2P Ethernet could be implemented, the simplest to explain is one where there the router has a (virtual) interface per station.

If an address prefix is configured on a router's typical network layer Ethernet interface, it results in the prefix in the FIB pointing to a glean adjacency. Packets being forwarded against the glean adjacency will undergo address resolution. If address resolution is successful a host route is installed in the FIB with an adjacency containing the required encap-string (known as a complete adjacency). The encap string contains the full Ethernet header with the source and destination MAC addresses. An IP multicast packet forwarded out the interface would undergo address multicast address mapping as described in [RFC2464]. With this technique no broadcast or multicast Ethernet packet will be sent out an P2P Ethernet interface from the network side. A legacy host might of course.

A P2P Ethernet interface connects to a single host and skips the above address resolution step. Each (virtual) P2P Ethernet interface will have the associated complete adjacency with a full encap-string. I.e. the full Ethernet header, including the destination MAC address. This encap string is also used for multicast packets. That is, no address mapping is required for multicast packets and no address resolution is required for unicast packets.

Now, the avid reader might wonder how this virtual interface is spawned in the first place? It clearly has to be dynamic as hosts connect to the network. Well, the answer is that it depends. In the simple topology of hosts directly connected to an Ethernet router, the physical interface is configured in p2p mode and the host's MAC address can be learnt with a simple mechanism like first sign of life (FSOL). If 802.1x is used, then successful 802.1x authentication can be used to spawn the creation of the P2P Ethernet interface. On wireless networks, a tight integration between access point and router would allow the AP to signal station attachment to the router for interface spawning. Otherwise the same could be done in a wireless LAN controller setup.

The changes described here can be deployed purely on the network side. Although it could also be extended with host support, with a marginal saving in the number of packets sent on the link. A legacy host will behave as if it was connected to a normal multi-access link, and would do address resolution to it's router, perform DAD etc.

Is a wireless network a hub and spoke network? You can make that assertion. All traffic from station to access point goes to the AP, and with different encryption keys per station, it's essentially behaving like a set of point to point link between station and AP.

This provides an alternative (and a much simpler solution) to the proposal in [I-D.thubert-6man-ipv6-over-wireless].

1.1. Conventions and Terminology

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].

Additionally, the key words "*MIGHT*", "*COULD*", "*MAY WISH TO*", "*WOULD PROBABLY*", "*SHOULD CONSIDER*", and "*MUST (BUT WE KNOW YOU WON'T)*" in this document are to interpreted as described in RFC 6919 [RFC6919].

2. Terminology

ethernet router: An Ethernet switch with IP routing enabled.

3. Addressing

P2P Ethernet simplifies addressing. A node at one end of the point to point link does not need to share a subnet with the other end.

If DHCP address assignment is used, then a host route can be installed in the FIB pointing out the given virtual P2P Ethernet interface.

2001:db8::1/128 -> Virtual-P2PEthernet0

For SLAAC a /64 route can be pointed at the interface and a PIO configured to be sent in RA. Note that in the case of SLAAC, regardless of how many addresses a host would use, no more state is required on the router. Which in contrast with the classical Ethernet deployment, where each address uses a slot in the neighbour cache.

4. Implications for Neighbor Discovery

Neighbor Discovery [RFC4861] solves a set of problems related to the interaction between nodes attached to the same link. The following details of these functions apply, do not apply or can be simplified on a point to point link.

Router Discovery: On a point to point link it is still useful to discover an attached router. Although in theory the host can just send the packet on the link. The RA is required if SLAAC is used. The RA could also be extended to convey to the host that it's connected to a point to point link.

Prefix Discovery: Prefix discovery for the purposes of address assignment [RFC4862] is done like on a multi-access link. If SLAAC is not used prefix discovery is not strictly required. The link-model assumes that only the link-local prefix is shared among the two nodes on the link. On-link discovery is not performed on a p2p link.

Parameter Discovery:

Unchanged.

Address Autoconfiguration: SLAAC can be simplified, e.g. DAD is not necessary.

Address resolution:

Address resolution is not needed on a point to point link. A> Discuss consequences for detection of bidirectional connectivity**

Next-hop determination: On a point to point link next-hop determination is not required. There is only one choice.

Neighbor Unreachability Detection:

NUD might still provide some usefulness in cases where data-link layer notifications are masked.

Duplicate Address Detection: Duplicate Address Detection is only required for the link-local address.

Redirect: Redirects are not needed. There is no-one to redirect to on a point to point link.

5. TODO/Open issues

* The consequences of random MAC addresses Appear as a completely new host?

* Tethering

* Mobility

* Describe that the mDNS domain is restricted to a single host / require homenet solution / mDNS proxy

* New P2P bit in Router Advertisement

* IPv4 support. A legacy IPv4 host would typically require that the default gateway is in the same subnet as the host's IPv4 address.

6. Security Considerations

A shared network using ND, without SEND assumes that all other nodes on the link are trust-worthy. The mechanism proposed here isolates all hosts, so that most of the ND functions are no longer needed. The host still needs to trust it's connected router.

7. IANA Considerations

8. Normative References

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

[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, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <https://www.rfc-editor.org/info/rfc6919>.

9. Informative References

[I-D.thubert-6man-ipv6-over-wireless] Thubert, P., "IPv6 Neighbor Discovery on Wireless Networks", Work in Progress, Internet-Draft, draft-

thubert-6man-ipv6-over-wireless-06, 1 June 2020,
<https://tools.ietf.org/html/draft-thubert-6man-ipv6-over-wireless-06>.

[IEEE.802-3.1990]
"Information Processing Systems - Local Area Networks - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 2nd edition", September 1990.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

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

Appendix A. Acknowledgements

Thanks to lots of people.

Author's Address

O. Troan
cisco

Email: ot@cisco.com