NDProxy Issues
draft-ietf-ipv6-ndproxy-01.txt

Dave Thaler
dthaler@microsoft.com

Problem Statement

Share subnet prefix(es) on upstream link to one or more downstream links, where a L2 bridge would be desirable but either:

a) no promiscuous support exists

Scenario 1: 802.11 upstream

b) heterogeneous L2 addresses exist

Scenario 2: PPP upstream

Be transparent to upstream routers (as a bridge is):

- Indistinguishable from a host with many addresses
- Don't require any coordination with upstream ISP, completely plug-and-play

Example use scenarios:

- Existing L2 bridge -> add PPP and/or 802.11 support
- Existing IPv4 ARP Proxy -> dual v4/v6 proxy

Recap

- Accepted as WG doc in 2003
- Recently went through WG Last Call
- 7 issues raised & discussed on list
- draft-ietf-ipv6-ndproxy-01.txt contains latest apparent consensus as of I-D cutoff date

Issues List

- http://www.icir.org/dthaler/NDProxyIssues.htm

16	Loop prevention, revisited	Erik Nordmark
17	SEND	Erik Nordmark
18	Dynamic removal of proxy	Erik Nordmark
19	Make Experimental not Informational	Brian Carpenter
20	DHCPv4	Ralph Droms
21	Editorial nits in ipv6-00	Ralph Droms
22	Unclear text about ICMP	Dave Thaler

19: Make Experimental not Informational

- Draft was made Informational to resolve Issue #8
  - Primary point was non-standards track
- New consensus is to be Experimental
- Issue is considered closed

16: Loop prevention, revisited (1/3)

- Draft -01 specified that loop prevention was optional, stated how to do it (STP), and an example of when optional (cell phone)
- Issue was to clarify to say MUST prevent loops, and allow two ways to do it (STP, physical constraints)
  - Text proposed on list
- Erik Nordmark then suggested a simple alternative to avoid loops

16: Loop prevention, revisited (2/3)

- New P-bit in RA
  - If clear and on upstream link, a proxy would set and forward on downstream links
  - If set or on downstream link, a proxy would disable proxy functionality on that interface for some time
- Accepted in draft-01, with holddown of 60 minutes (2 * maximum RA interval).

```
+-+-+-+-+-+-+-+-+
|M|O|H|Prf|P|Rsv|
+-+-+-+-+-+-+-+-+
```

16: Loop prevention, revisited (3/3)

Draft-01 text (excerpt):

An implementation MUST ensure that loops are prevented, via either:

a) by using the P bit in RA's as described below, or

b) by running the Spanning Tree Algorithm and Protocol defined in [BRIDGE] on all proxy interfaces as described below, or

c) by being physically deployable only in an environment where physical loops cannot occur. For example, in a cell phone which proxies between a PPP dialup link and a local Ethernet interface, it is typically safe to assume that physical loops are not possible and hence there is no need to support the Spanning Tree Protocol (STP).

Bob Hinden suggested removing C now, authors agree.

17: SEND (1/4)

The issue:

- Draft ietf-00 said working with SEND was a requirement
- SEND today doesn’t work with MITM changing ND packets
- NDproxy modifies ND packets

Since pkts must be modified whenever L2 address formats differ or no promiscuous mode, securing *any* solution in this space requires hosts to have a relationship with the proxy

Not unique to this document:

- RFC 2461 defines the ability to proxy NAs
- MIPv6 also modifies ND packets

17: SEND (2/4)

- Requirements and trust models are asymmetric for NDProxy
  - On downstream links, okay for hosts to have knowledge of trusted proxy, same as for a router
  - On upstream link, requirement is that it's indistinguishable from a host

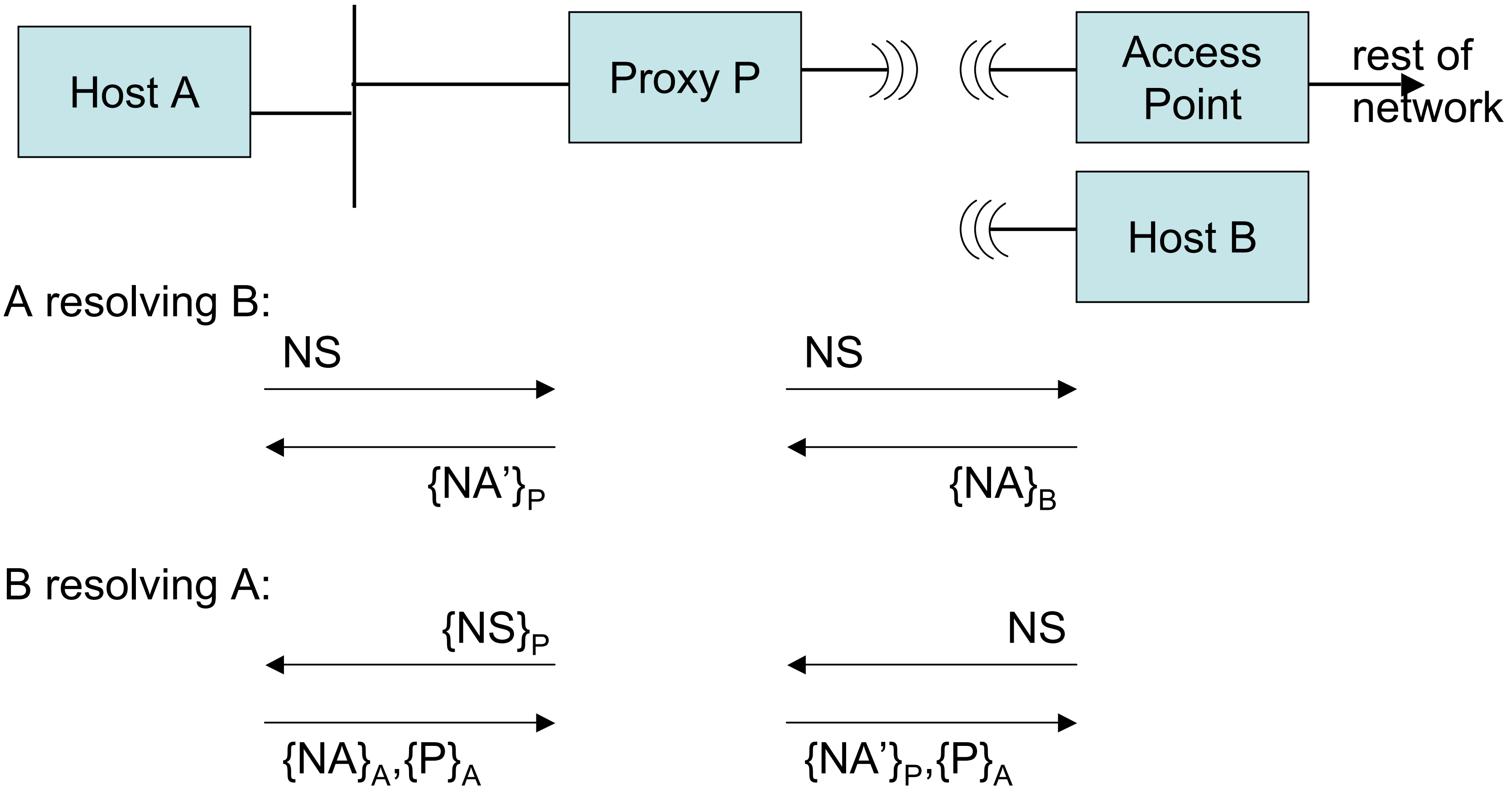
For nodes on a *downstream* subnet:

- Accept NA if from owner OR trusted proxy
- Securing NA from trusted proxy similar to securing RAs, but left for future work since not limited to use by this spec

For nodes on an *upstream* subnet:

- Allow owner to delegate permission to the trusted proxy
- (If p2p, SEND may not even be needed on that link)

17: SEND (3/4)



A resolving B:

B resolving A:

17: SEND (4/4)

Rough consensus on list was that it is not a technical blocker for this Experimental protocol, as long as draft is consistent

Draft -01 removes the explicit requirement but adds additional discussion of future work in Security Considerations

Securing Proxy ND work is being done in draft-daley-send-spnd-prob-01.txt

18: Dynamic removal of proxy

- Draft-00 said there was a requirement to allow dynamic removal of a proxy without adversely disrupting the network
- But any time you remove a router, bridge, switch, whatever, it adversely affects the network (e.g., convergence time, possible partition, etc)
- Proposed removing bad “requirement”
- No objections from list
- Done in -01

20: DHCPv4

- Ralph Droms raised “two small issues”
  - Incompatible with DHCPv4 AUTH
  - Add warning that client may detect the change by the proxy
- Point of IPv4 text is to document existing practice by ARP Proxies
  - Added both of Ralph’s points to the DHCPv4 section.
- Ralph responded saying new text is fine.
- Issue is considered closed.

21: Editorial nits in ipv6-00

- Various editorial-only issues from Ralph Droms
- Proposed changes posted to list
- No objections
- Accepted in draft-01

22: Unclear text about ICMP errors

- Two seemingly contradictory statements about whether proxy can send ICMP errors (never vs PacketTooBigs)
- Clarified in -01 that only sends PacketTooBigs
- No objections on list
- Erik asked about source address of ICMP, but this is no different from sourcing any other locally originated packet.