Host Joins the Network

- Host
- Router

Router Solicitation

Router NC:
Host LLA <> Host MAC STALE

Host configures GUA (m.b. Optimistic)

Host NC: Router LLA <> Router MAC STALE
Host Starts Sending Traffic

Host NC: Router LLA <-> Router MAC

Router NC: Host LLA <-> Host MAC

Host GUA -> d1
Host GUA -> d2
Host GUA -> d3
And Here Comes the Return Traffic

Host

Host NIC: Router LLÅ <-> Router MAC

Router

ref
1 packet buffer

Host GWÅ <-> INCOMPLETE

Host GWÅ -> INCOMPLETE

MS to Solicited Node MCast Address

packets are dropped as there is no MCast entry for Host GWÅ

Neighbor Advertisement

Host GWÅ <-> REACHABLE

buffered packets delivered

packet to Host GWÅ

Host

Router

packet to Host GWÅ

Server
In the Ideal World...

Host MC: Router LLA <> Router MAC

Host GUA -> Server

Neighbor Cache is prepopulated somehow:
Host GUA <> Host MAC STALE

Server -> Host GUA

Server -> Host GUA

Server -> Host GUA

Host

Router

Server
Dual-Stack Network

- Hosts sends Gratuitous ARP
- Routers get their cache updated
- Happy Eyeballs
IPv6 and RFC4861

7.2.5. Receipt of Neighbor Advertisements

When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target's entry. If no entry exists, the advertisement SHOULD be silently discarded. There is no need to create an entry if none exists, since the recipient has apparently not initiated any communication with the target.

Not a case for host2router communication.
Impact

- Almost Inevitable packet loss
- Noticeable delay in using the network
- Negative perception of IPv6-Only networks
What Can We Do?

- Nothing
- Modernize Neighbor Discovery
- Make hosts advertise their addresses
  - Might require tweaking Neighbor Discovery on routers
- Fix hosts
- Make routers buffer more packets
Requirements

MUST:

● Creating a new STALE entry if one does not exist
● MUST NOT override the existing entry
● Work for Optimistic addresses too

Nice to Have:

● Work for asymmetric traffic flows
Do Nothing aka “Working as Intended”

“It’s a cosmetic issue, just a few packets, transport/applications shall deal with it”

Pros:
- Easy

Cons:
- Unhappy Eyeballs
- Unhappy support
- More resistance to deploy IPv6
Use Registration-Based ND/RFC8505

As proposed by Pascal Thubert

Pros:

- Would solve the problem

Cons:

- Might introduce other issues (e.g. state recovery)
- Migration Strategy is unclear
Host Sends Unsolicited NAs + Routers Glean

“Gratuitous ARP” for Neighbor Discovery

7.2.5. Receipt of Neighbor Advertisements

When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target's entry. If no entry exists, the advertisement SHOULD be silently discarded. There is no need to create an entry if none exists, since the recipient has apparently not initiated any communication with the target.

...unless the receiving device is a router....
Pros:
- RFC4861-Compliant
  - It says ‘SHOULD’
- Already implemented in some platforms
- Updates all routers

Cons:
- Changes to hosts required
- Needs to be configurable (to prevent attacks)
- “Smart” WiFi devices
Host Sends NS from GUA to Router

- **Source:**
  - Host GUA

- **Destination:**
  - Host default router link-local address

- **Options:**
  - SLLA set to the host MAC
Pros:
- RFC6583-compliant routers might prioritize those packets

Cons:
- Changes to hosts required
- Prohibited for Optimistic addresses
- “Smart” WiFi devices
Host Sends RS from GUA to its Router

- **Source:**
  - Host GUA

- **Destination:**
  - ff02::2

- **Options:**
  - SLLA set to the host MAC - ONLY if the GUA is not optimistic
Pros:

- RFC6583-compliant routers might prioritize those packets
- Cache updated on all routers

Cons:

- Changes to hosts required
- Prohibited for Optimistic addresses(*)
- “Smart” WiFi devices

(*)Would work w/o SLLA if routers respond with unicast solicited RAs
Host Pings the Router

Pros:
- Works even with “smart” WiFi middleboxes

Cons:
- Packets could be blocked
- Load on routers
- Only active router is updated
Proposed Tactical Solution

Hosts send unsolicited NAs when:

- If optimistic DAD is used: new optimistic address assigned
- Else: tentative -> preferred state change

Routes glean from unsolicited NAs (configurable)
Security Considerations

No changes proposed re: existing entries

All solutions discussed only creates an entry

Threat model: malicious host trying to exhaust the router NC:

Malicious hosts can do it today
QUESTIONS?
COMMENTS?