Zero valid lifetimes on point-to-point links

Lorenzo Colitti, Erik Kline

IETF 102

Current situation

- An RA cannot reduce the valid lifetimes of a PIO below two hours
  - Unless the RA “has been authenticated (e.g., via ... SEND)”
  - RFC 4862 §5.5.3

- Intended to address a DoS attack where a malicious node causes all hosts on link to expire their IPv6 addresses prematurely

- On some link types, this DoS vector does not exist
  - e.g., links that are point-to-point at layer 2
    - Cellular networks (see RFC 6459)
    - PPP links
    - IPsec tunnels
    - ...

Use cases for zero valid lifetime RAs

- Addresses from one prefix are no longer routed to host, but host has addresses from other prefixes

- Multihomed network that experiences an outage on one upstream

- Graceful handover in 5G networks with Session/Service Continuity Mode 3
    - “For a PDU Session of IPv6 type, the new IP prefix anchored on the new PDU Session Anchor may be allocated within the same PDU Session (relying on IPv6 multi-homing specified in clause 5.6.4.3)”
    - “After the new IP address/prefix has been allocated, the old IP address/prefix is maintained during some time indicated to the UE via … or via Router Advertisement ... and then released.”
    - 3GPP TS 23.501 - http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-f20.zip

Proposal

- Accept zero valid lifetimes if:
  - The link-layer guarantees that there is only one node on the link from which the host can receive Router Advertiesements, and
  - The link has another prefix of the same scope with sufficient Valid Lifetime
- The host needs to know that it’s on such a link
  - A link with RA guard enabled does not qualify since the host does not know if it’s enabled
  - Note: when IPv4 goes away, RA guard becomes an absolute must, and this document (and the DoS scenario in §5.5.3) will become obsolete

List discussion

- How does the host know it’s on such a link?
  - ND implementations tightly coupled to link-layer. For example, must know MAC address, link type, whether link is multicast, …
- What about P2P links over non-P2P networks (e.g., IPv6-in-IP tunnels)?
  - Not covered: no guarantee that only one node can send RAs.
- Why not make “this link is point-to-point” a negotiated flag in SLAAC?
  - Still the potential for abuse by rogue router
  - What if multiple routers disagree? See discussion on draft-ietf-6man-ipv6only-flag
- Clarify that RA guard is not sufficient, and this cannot be used on Ethernet.
  - Agreed

Next steps

- Call for adoption?