Security Assessment of Neighbor Discovery (ND) for IPv6

(draft-ietf-opsec-ipv6-nd-security)

Fernando Gont
Ron Bonica
Will Liu

IETF 88
November 3-8, 2013. Vancouver, BC, Canada

Goal of this presentation

- Discuss validation checks
- Post result to the mailing-list
- And continue making progress piecemeal
- Any volunteers to review the entire document or sections of it?

Router Solicitations

- Message length >= 8 bytes
- Source Address should not be:
  - multicast address
  - what about loopback?
- Destination Address:
  - Must be all-routers multicast, or,
  - if unicast, require it to be link-local?

Router Solicitations (II)

- Source link-layer address option:
  - Must not be multicast or broadcast
  - If one is included, IPv6 Source address should not be the unspecified (::) address

Router Advertisements

- Message length >= 16
- Source Address
  - Must be link-local
- Destination Address:
  - all-nodes multicast
  - if unicast, require it to be link-local?
- Cur Hop Limit, if non-zero,

  SanitizedCH = max(Cur Hop Limit, MIN_HOP_LIMIT)

  where MIN_HOP_LIMIT == 64, and is configurable by the admin

Router Advertisements (II)

- Router Lifetime, if non-zero:

  SanitizedRL = min(max(Router Lifetime, MIN_ROUTER_LIFETIME),MAX_ROUTER_LIFETIME)

  - Where:

    MIN_ROUTER_LIFETIME==1800 secs (AdvDefaultLifetime)

    MAX_ROUTER_LIFETIME==9000 secs (upper limit for AdvDefaultLifetime)

- When RA with RL==0
  - May keep the router in the default router list?

Router Advertisements (III)

- Rechable Time. If non-zero,

  SanitizedRT = max(min(Reachable Time, MAX_REACHABLE_TIME), MIN_REACHABLE_TIME)

  - Where:

    MIN_REACHABLE_TIME==20,000

    - (such that MIN_RANDOM_FACTOR * SanitizedRT >= 10 seconds)

    MAX_REACHABLE_TIME==3,600,000 (one hour) (AdvReachableTime)

Router Advertisements (IV)

- Retrans Timer. If non-zero,

  SanitizedRXT = max(min(Retrans Timer, MAX_RETRANS_TIME), MIN_RETRANS_TIME)

  - Where:

    MIN_RETRANS_TIME==1,000

    MAX_RETRANS_TIME==60,000

Neighbor Solicitations

- Message length >= 24
- Source Address must be
  - Unspecified address, or,
  - Unicast address
  - What about loopback?
- Destination Address must be:
  - Solicited-node multicast address
  - Target address
  - Restrict others?

Neighbor Solicitations (II)

- Target Address must not be (per RFC4861):
  - Unspecified, loopback, or multicast
- And must be:
  - Unicast or anycast address of receiving interface
  - Unicast or anycast address for which node is offering proxy service
  - Tentative address (while performing DAD)

Neighbor Solicitations (III)

- Source link-layer address:
  - Drop packet if it contains SLLA and SOurce Address is the unspecified address (::)
  - Drop packet if Destination Address is multicast, Source Address is != ::, and there's not SLLA

Neighbor Advertisements

- Message length >= 24
- Source Address:
  - Must be link-local unicast
- Destination Address
  - All-nodes multicast
  - Unicast address

Neighbor Advertisements (II)

- R flag
  - Do not drop router if not set for an address of default router?
- S flag
  - Drop packet if S flag set and Destination Address is multicast
  - Drop packet if S flag is set and there was no pending Neighbor Solicitation
- O flag
  - Drop packet if set in unsolicited NA

Neighbor Advertisements (III)

- Target Address
  - Must not be multicast, unspecified, or loopback
- Target Link-Layer Address option
  - Drop packet if it does not contain a TLLA and NS destination was a multicast address

Please send feedback :-)