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 $\geq 8$ 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 $\geq 16$
- 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,

  $$\text{SanitizedCH} = \max(\text{Cur Hop Limit}, \text{MIN\_HOP\_LIMIT})$$

  where $\text{MIN\_HOP\_LIMIT} = 64$, and is configurable by the admin
Router Advertisements (II)

- Router Lifetime, if non-zero:
  
  \[ \text{SanitizedRL} = \min(\max(\text{Router Lifetime}, \text{MIN\_ROUTER\_LIFETIME}),\text{MAX\_ROUTER\_LIFETIME}) \]

  - Where:
    
    \[ \text{MIN\_ROUTER\_LIFETIME} = 1800 \text{ secs} \] (AdvDefaultLifetime)
    
    \[ \text{MAX\_ROUTER\_LIFETIME} = 9000 \text{ secs} \] (upper limit for AdvDefaultLifetime)

- When RA with RL==0
  
  - May keep the router in the default router list?
Router Advertisements (III)

• Reachable Time. If non-zero,

\[
\text{SanitizedRT} = \max(\ \min(\ \text{Reachable Time}, \\
\text{MAX\_REACHABLE\_TIME}), \ \text{MIN\_REACHABLE\_TIME})
\]

– Where:

\[
\text{MIN\_REACHABLE\_TIME} = 20,000
\]

– (such that \(\text{MIN\_RANDOM\_FACTOR} \times \text{SanitizedRT} \geq 10\) seconds)

\[
\text{MAX\_REACHABLE\_TIME} = 3,600,000 \text{ (one hour)}
\]
(AdvReachableTime)
Router Advertisements (IV)

• Retrans Timer. If non-zero,

\[
\text{SanitizedRXT} = \max(\min(\text{Retrans Timer, MAX\_RETRANS\_TIME}), \text{MIN\_RETRANS\_TIME})
\]

- Where:

\[
\begin{align*}
\text{MIN\_RETRANS\_TIME} &= 1,000 \\
\text{MAX\_RETRANS\_TIME} &= 60,000
\end{align*}
\]
Neighbor Solicitations

- Message length $\geq 24$
- 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 $\geq 24$
• 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 :-}