IPv6 Secure ND implementation report on Cisco IOS

Eric Levy-Abegnoli

IETF 70th, vancouver

Implementation status

- Implements RFC3971 & RFC3972
- Includes CGA support and Authorization Discovery
- Supports Certificate profile, with X.509 IP extensions but initial release won't.
- Router mode (send CPA) and host mode (send CPS)
- Leverage PKI tooling already available on routers
- Leverage router crypto engine (for RSA operations acceleration)
- Supports transition mode with preference of SEND over ND
- Availability: interop (now), trials (early 2008), commercial (TBD)
- Very few implementation issues identified against the spec.

Implementation issue #1

- Validating Non-CGA addresses is needed for routers which like to have hand-crafted addresses but ...
- Inconsistencies between “CGA MUST” and section “5.2.3 Configuration”, when authorization method = trust anchor
- Furthermore, mixture of “this is how this would work to certify non-CGA addresses” and “non-CGA addresses is future work, beyond the scope of this specification” is confusing.
  - What is missing to support non-CGA addresses through trust-anchor method?
- → suggestion : we specify the complete behaviour for non-CGA addresses (using trust-anchor)

Implementation issue #2

- A timestamp cache seems to be a must for preventing replay attacks, but …
- Such cache is very sensitive to DoS attacks:
  - ND packets sourced with a large range of CGA sources can easily fill the cache
  - Old entries could be protected, but new comers will be denied services
  - Removing entries with lower security level does not help: single modifier with high sec-level could be used to generate many different source addresses (FE80:1::x, FE80:2::y, etc).
- → suggestion: use the neighbor cache to give precedence to reachable peers, others?

Implementation issue #3

- A router can send an unsolicited RA in response to one *or many RS*.
- Section 5.3.3 a bit unclear on how to cope with such unsolicited RA:
  - Can a router include multiple NONCE options in the case mentioned?
  - If such unsolicited advertisement contains one (out of many) NONCE of interest to the host, should this advertisement falls into the “solicited advertisement” category and be processed according to section 5.3.4.1?
- → suggestion: state that an unsolicited RA can carry many NONCE option instances, and should be processed according to section 5.3.4.1 if the receiver recognize one of the nonce values as one of his.

Implementation issue #4

- RFC3971, section 6.3.1 calls for “provisional acceptance” of the certificate, to allow for CRL check via a possibly compromise router.
- In case the router is indeed compromised (certificate revoked), what do we do? It sounds bogus to keep a state for compromised routers, and if we don’t, the same router will be “provisionally accepted” quickly after the certificate verification failure.
- → suggestion: remove the MUST

Implementation concern

Everywhere SEND modifies ND behaviour per 4861 is a potential concern (extending is fine). Few examples:

#1 Address resolution:

- ND (RFC4861): could send NA with source=LL, and target=global, in response to NS sourced with LL
- SEND behaviour: NA MUST have source=target.

#2 Cache update:

- ND : existing state machine fully described in RFC4861
- SEND: Conditional update of neighbor cache based on various trust level, and sometimes on previous states transitions (section 8 of 3971).

- → suggestion: avoid modifying ND *whenever* possible. For instance for #1, why not make the CGA address the target (instead of the source) in NA?
- → When it's unavoidable, make it clear by referencing the original ND section. For instance, taking decision on previous state transition means new state. Provide the new state diagram.