SEND / ND Proxy
Problem Statement
IETF 71 – CSI WG
Jean-Michel Combes, Greg Daley
Contents

• SEND overview
• Identified scenarios
• SEND and ND Proxy
• Potential approaches
• Generalization
• Open issues/Next steps
SEND overview (1/3)

• Two parts (in fact 3)
  – RS/RA security
  – NS/NA security

• Two mechanisms
  – Certificates based
  – Cryptographically based (i.e. CGA [RFC3972])
SEND overview (2/3)

• **NS/NA Security**
  – Public/private key pair linked to a CGA
  – CGA option
  – RSA Signature option
SEND overview (3/3)

- **RS/RA Security**
  - Public/private key pair linked to a certificate
  - Trust Anchor option
  - Certificate option
  - RSA Signature option
  - CGA option
Identified scenarios (1/3)

- IPv6 Mobile Nodes
  - Two nodes need to be able to "advertise" a same address (i.e. DAD, Neighbor Resolution)
  - Impact on NS/NA messages
  - E.g. in Mobile IPv6 [RFC3775], a MN and a HA with the MN's HoA
Identified scenarios (2/3)

- IPv6 Fixed Nodes
  - One node needs to "advertise" a address but owned by another node
    - Impact on NS/NA messages
    - E.g. address assignment in IKEv2 [RFC4306] with the Security Gateway
  - Sub-case of the previous scenario
    - But with a larger solution space
Identified scenarios (3/3)

• Bridge-like ND Proxies [RFC4389]
  – A Bridge needs to rewrite information in forwarded packets
  – A Bridge needs to "advertise" a address but owned by another node
    • Impact on NS/NA messages
  – A Bridge needs to "advertise" a prefix but owned by another router
    • Impact on RS/RA messages
SEND and ND Proxy

• No appropriate keys/authorizations
  – To generate messages and to sign them instead of another node
  – To modify messages and to keep valid the signatures
Potential approaches

- Trusted ND Proxy
  - Do nothing
- Relax SEND policy
  - To accept unsecured ND/RD messages
- Authorization delegation
  - Generation of certificates for the ND Proxy
- Crypto based
  - Ring/Group signatures
Generalization

• Case where N nodes "advertise" a same address (with N ≥ 2)
  – Anycast addresses
  – PMIPv6 case (i.e. ingress MAG's LLA)
Open issues/Next steps

• Others proposals about SEND-NDP PS?
  – Merge of the proposals?
• To keep "Potential approaches" section?
  – To add "Solution Space analysis" in the title?
  – To add references to potential solutions?
• Integration of the "Generalization" Appendix in the core of this draft?
Comments/Questions?