Secure EVPN MAC Signaling

draft-thubert-bess-secure-evpn-mac-signaling

Pascal Thubert, Tony Przygienda, and Jeff Tantsura

IETF 113

Remote
IPv6 IS Different

• DHCP is observable and stateful

=> DHCP addresses have a deterministic beginning and a lifetime

=> Corporate Network admins trust that state

=> A solid foundation for EVPN
The Hassle is the “SL” in SLAAC

• SLAAC stands for IPv6 Stateless Address Autoconfiguration

=> SLAAC address lifecycle is insecure and not deterministically observable

=> There is no protocol to sync SLAAC state with the network (just snooping)

=> Non-deterministic state in EVPN leads to stale state and BUM
Issues with IPv6 ND SLAAC (Non-Deterministic snooping)

- SLAAC lacks mobility signaling
- SLAAC prone to attacks (DDoS, address theft, SAVI)
- Snooping SLAAC is unreliable, causes silent nodes and stale state
- NS Lookup for Silent node causes broadcast ND in overlay (BUM)

L2 broadcast Domain (segment)

IP Links

L3 Subnet (in overlay)
Till we made IPv6 ND stateful

- RFC 8505 / RFC 8928 Stateful Address Autoconfiguration
  => Synchronizes addressing state with network
  => Carries address control semantics (lifetime negotiation, redistribution...)
  => Secures address ownership, enables Source Address Validation
Secure EVPN
MAC signaling

- Redistributing RFC 8505 / RFC 8928 in EVPN
  ⇒ Sorts duplication vs. anycast; can support multicast, too
  ⇒ Handles mobility with sequencing
  ⇒ protects address ownership
Stateful IPv6 ND: Creates a deterministic state for routing

1) Node autoconfigures an IPv6 address
2) Node Registers the IPv6 address NS(EARO) unicast
3) Router checks ownership, policy, mobility sequence, duplicate and acks NA(EARO, ok/~ok)
4) Routers redistributes SFAAC in routing
5) Routing (eVPN) distributes state in all Routers
RFC 8928 flow

Direct L2 connection, IP Link == P2P

RFC 8505 / RFC 8928

NS (EARO(ROVR=Crypto-ID, "R" set))

NA (EARO(status=Validation Requested), Nonce)

NS (ROVR, EARO("R" set)), CIPO*, Nonce and NDPSO**)

NA (EARO(status=0, "R" set))

* Crypto-ID Parameters Option
** NDP Signature Option

Check eVPN state:
- Is address already known?
- If so, was it signed with RFC 8928?
- Same vs. Different ROVR?
- If diff: duplicate address
- If same force challenge

Inject in BGP

Add new NLRI:
- TID, Lifetime
- Signed with RFC 8928

Host

6LBR / EVPN Router

Routed Subnet

BGP Route Reflector
Stable

⇒ Inherits from RFC 8929 (ND proxy), RFC 9010 (RPL), and RIFT
⇒ Published 03, with Jorge’s comments using ARP/ND Extended Community
⇒ Calling for adoption