RFC8273

Unique IPv6 Prefix per Host

RIPE 76 - Marseille
May 2018

Jordi Palet (jordi.palet@theipv6company.com)
RFC8273

• RFC8273: “Unique IPv6 Prefix per Host”

• Not a “new” protocol, so already widely supported
  – Use “existing IPv6 protocols” to allow a unique IPv6 prefix
    (instead of a unique IPv6 address from a shared IPv6 prefix)
    to be assigned to a host interface

• Allows improved host isolation and enhances subscriber
  management on shared network segments, such as
  Wireless networks, data centres, among others

• Provides a very simple mechanism for a single host or
  interface, to be able to run $2^{64}$ virtual machines, with their
  own global IPv6 address, not requiring to share a single one
“How To”

1. First-hop router is a L3 edge router
2. UE connects to the shared-access network and starts IP configuration with SLAAC RS
3. First-hop router sends solicited RA response ONLY to the requesting UE
   - Instead of using the link-layer multicast address (all-nodes group), using the link-layer unicast address of the requesting UE
   - The solicited RA contains the unique prefix (/64) and flags (to indicate if SLAAC and/or DHCPv6 should be used, etc.)
   - Prefix from locally/centrally managed pool, aggregate IPv6 block, …
   - Flags, best practices:
     - M-flag = 0 (address not managed with DHCPv6, 1 for DHCPv6 prefix delegation)
     - O-flag = 1 (DHCPv6 used for other configuration information)
     - A-flag = 1 (UE can configure itself using SLAAC)
     - L-flag = 0 (prefix is not an on-link prefix, everything sent to the gateway)
4. Periodically unsolicited RAs follow same approach
Usage Scenarios

• We are already doing in cellular:
  – /64 per PDP context
  – Prefix sharing with other devices (tethering)
  – Facilitate IPv6-only access (and IPv4-as-a-service)

• Allows extending same concept to other scenarios:
  – Hot-Spot
    • WiFi Calling: Secured Voice over WiFi over “untrusted” connection
      – IPv4 or IPv6 IPsec tunnels to the ePDG (evolved Packet Data Gateway)
  – Corporate networks
  – Data Center

• Allows also IPv6-only access and IPv4-as-a-service
  – Same concept as above for WiFi Calling
    • VPN “on demand” in “own” network for IPv4 services
    • No need for NAT44 (lowers logging costs and fragmentation issues)
Hot-Spot Usage

• WiFi shared-access L2 network

• Provide isolation between user devices either due to legal requirements or to avoid potential abuse

• By using “unique IPv6 prefix per host”, devices only can communicate thru the first-hop router

• Automatically avoids attacks based on link-local ICMPv6:
  – DAD reply spoofing
  – ND cache exhaustion
  – Malicious redirects
  – Rogue RAs

• Better scalability and robustness than DAD proxy, forced forwarding, ND snooping, etc.
Hot-Spot Example
Hot-Spot Example

ISP
IPv6 /48

Hot-Spot Provider Router

IPv6 /56

AP 1

IPv6 /56

AP n

IPv6 /56

---

The IPv6 Company
Hot-Spot Example
Hot-Spot Example

ISP

Hot-Spot Provider Router

IPv6 /48

IPv6 /56

IPv6 /56

IPv6 /56

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64
Hot-Spot Example

ISP

IPv6 /48

IPv6 /56

IPv6 /56

IPv6 /56

IPv6 /56

Hot-Spot Provider Router
Data Centre Usage

• “How to” same as for the Hot-Spot case

• The UE “server” may need multiple addresses from the same unique IPv6 prefix (VMs, containers), so just need to configure them

• The first-hop router must be able to handle the presence and use of those
Data Center Example

ISP
IPv6 /48
Data Center Router
Data Center Example

IPv6 /56

Rack 1

IPv6 /56

... IPv6 /56...

Data Center Router

IPv6 /48

ISP

Rack n
Data Center Example

Server 1

IPv6 /64

Rack 1

IPv6 /56

ISP

IPv6 /48

Data Center Router

IPv6 /56

Rack n

IPv6 /56
Data Center Example

ISP

Data Center Router

Server 1

IPv6 /64

Rack 1

IPv6 /56

... IPv6 /56...

Rack n

IPv6 /56

Server 1

IPv6 /64

IPv6 /64

IPv6 /64

... IPv6 /64...

IPv6 /64
Data Center Example

ISP
IPv6 /48

Data Center Router
IPv6 /56

Rack 1
IPv6 /56

Server 1
IPv6 /64

Server 2
IPv6 /64

Server n
IPv6 /64

Rack 1
IPv6 /64

... IPv6 /64

Rack n
IPv6 /64

... IPv6 /64

The IPv6 Company
Enterprise Example

ISP

IPv6 /48

Enterprise Router
Enterprise Example

Switch 1

IPv6 /56

Switch n

Enterprise Router

ISP

IPv6 /48
Enterprise Example

IPv6-only VLAN /64

Switch 1

IPv6 /56

Switch n

IPv6 /56

Enterprise Router

IPv6 /48

ISP
Enterprise Example

- Switch 1
  - IPv6 /56
  - IPv6 /56
  - IPv6 /56
  - IPv6 /56

- Switch n
  - IPv6 /56
  - IPv6 /56
  - IPv6 /56
  - IPv6 /56

- ISP
  - IPv6 /48

- Enterprise Router
  - IPv6 /48

- IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
  - IPv6-only VLAN /64
Enterprise Example

- IPv6 /48
- IPv6 /56

Switch 1

Switch n

Enterprise Router

IPv6-only VLAN /64
Enterprise Example

On-Demand VPN IPv4

IPv6-only VLAN /64

Switch 1

IPv6 /56

Switch n

IPv6 /56

Enterprise Router

IPv6 /48

ISP
Conclusions RFC8273

• Stable and secure IPv6-only experience

• No performance impact

• Secure host-to-host communication managed by first-hop router

• Each unique IPv6 prefix can function as a control-plane anchor point to ensure that each device receives expected subscriber policy and service levels
  – Throughput
  – QoS
  – Security
  – Parental control
  – Other value-added-services …
Thanks!

Contact:

– Jordi Palet:
  jordi.palet@theipv6company.com