IPv6 New RFCs

LACNIC 29 - Panamá
May 2018

Jordi Palet (jordi.palet@theipv6company.com)

Happy Eyeballs v2

RFC8305

(see previous LACNOG LT)
http://slides.lacnic.net/wp-content/uploads/2017/09/deteccion-fallos-ipv6-v1.pdf
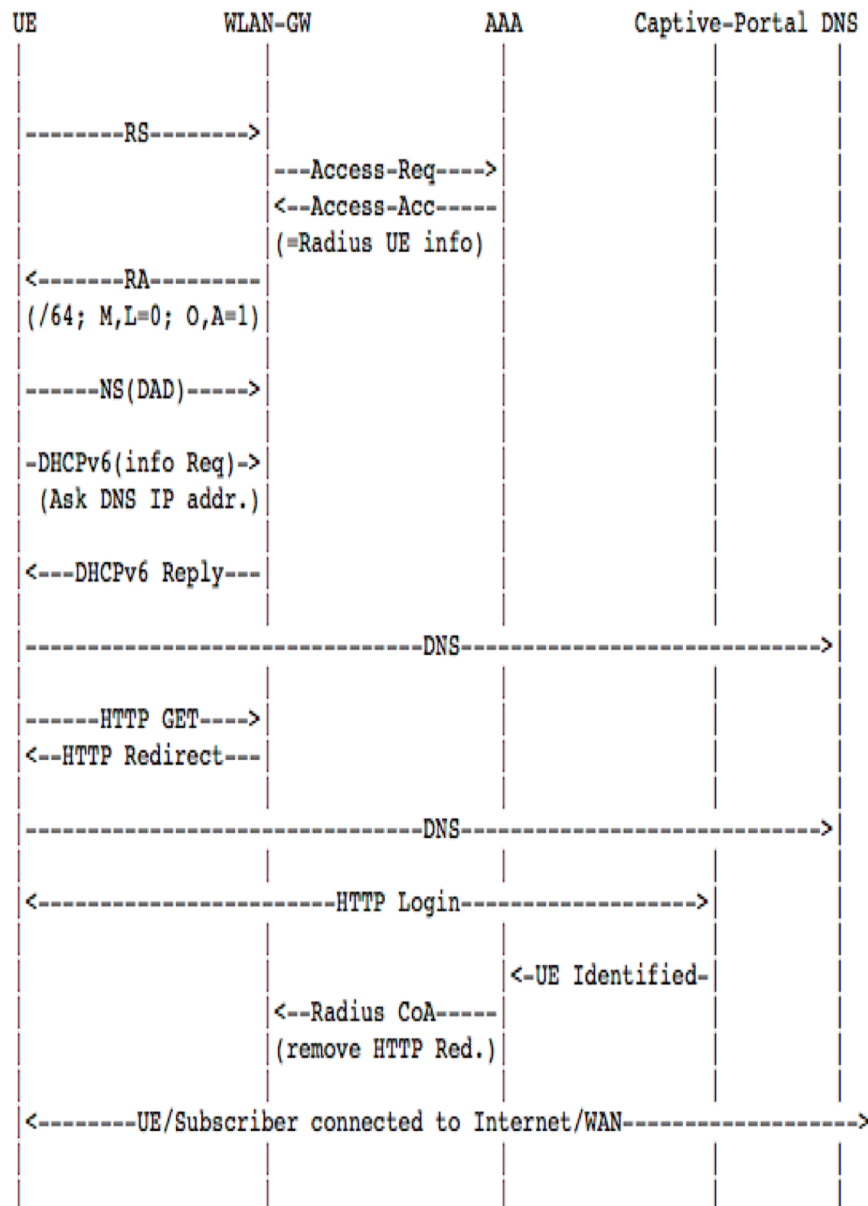
Unique IPv6 Prefix per Host

RFC8273

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"

```
UE          WLAN-GW        AAA      Captive-Portal DNS
|              |             |             |
|              |             |             |
|------RS------>|            |             |
|              |             |             |
|              |---Access-Req---->|        |
|              |<--Access-Acc-----|        |
|              |(=Radius UE info) |        |
|<-------RA--------|             |         |
|(/64; M,L=0; O,A=1)|            |         |
|              |             |             |
|------NS(DAD)----->|          |           |
|              |             |             |
|-DHCPv6(info Req)->|         |            |
| (Ask DNS IP addr.)|         |            |
|              |             |             |
|<---DHCPv6 Reply---|         |            |
|              |             |             |
|----------------------DNS-------------------------->|
|              |             |             |
|------HTTP GET---->|         |            |
|<--HTTP Redirect---|         |            |
|----------------------DNS-------------------------->|
|              |             |             |
|<---------------------HTTP Login------------------->|
|              |             |             |
|              |             |<-UE Identified-|
|              |<--Radius CoA-----|         |
|              |(remove HTTP Red.)|         |
|<---------UE/Subscriber connected to Internet/WAN-->|
|              |             |             |
```

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
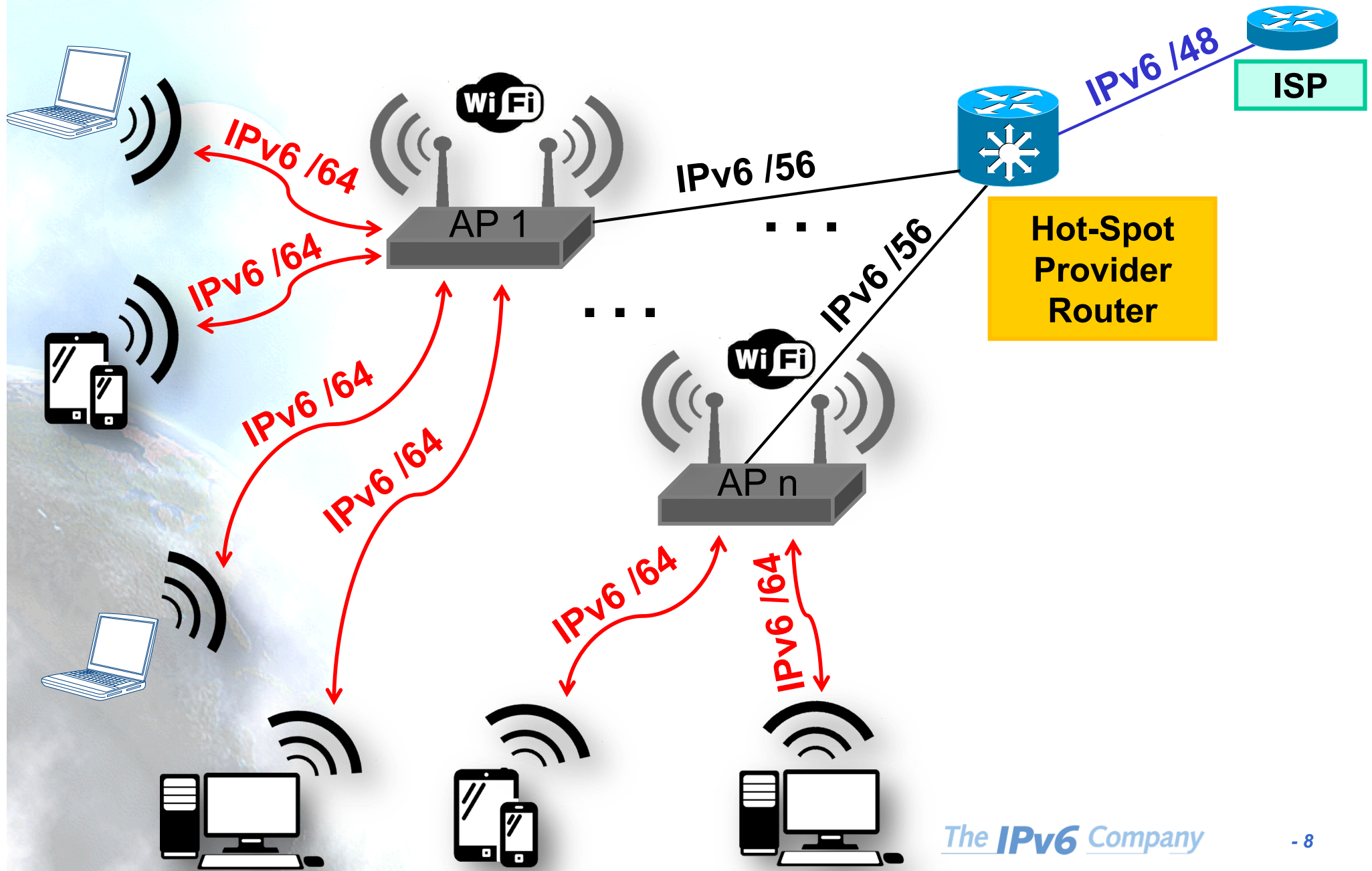
The **IPv6** Company   - 5

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.
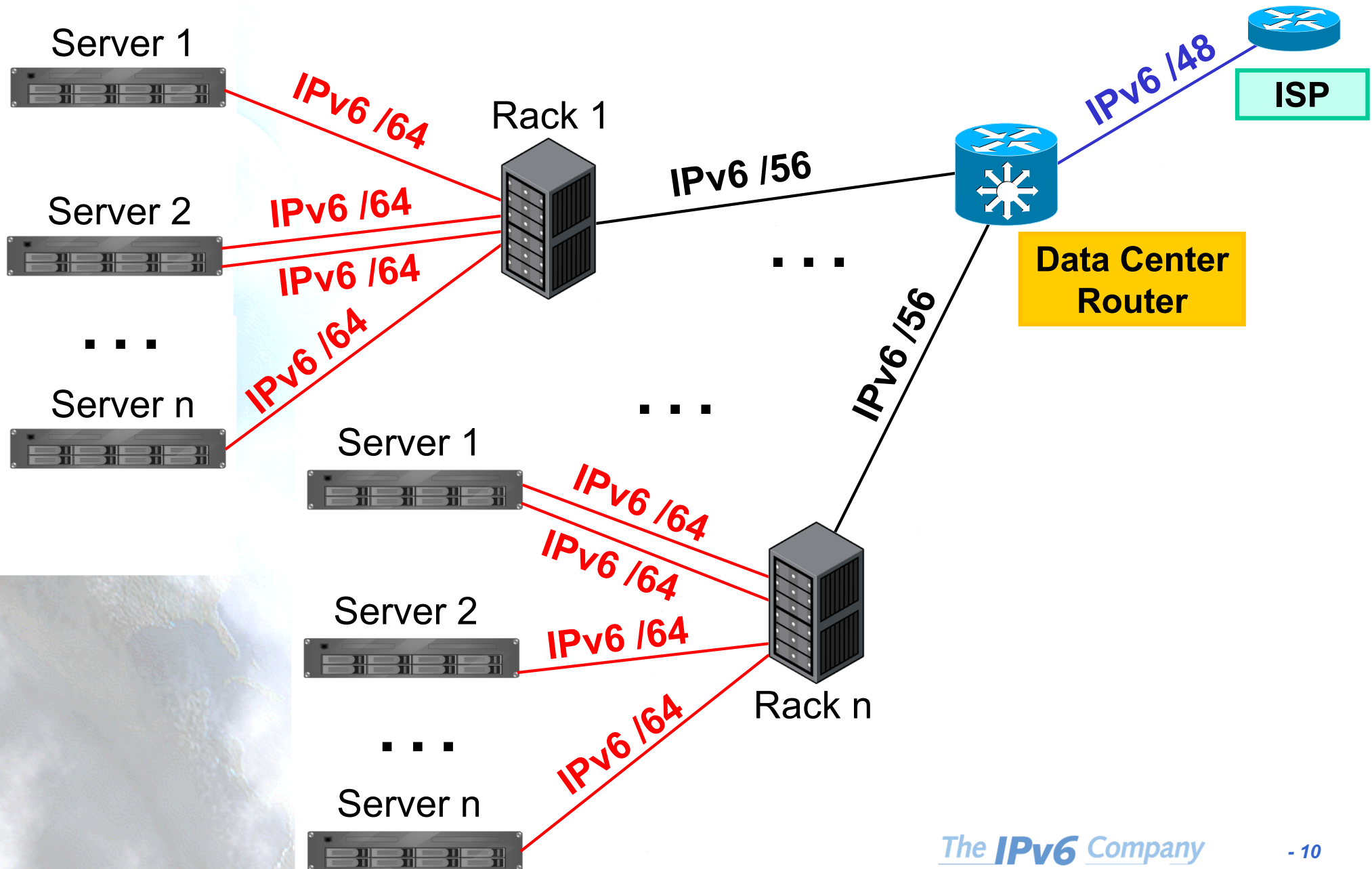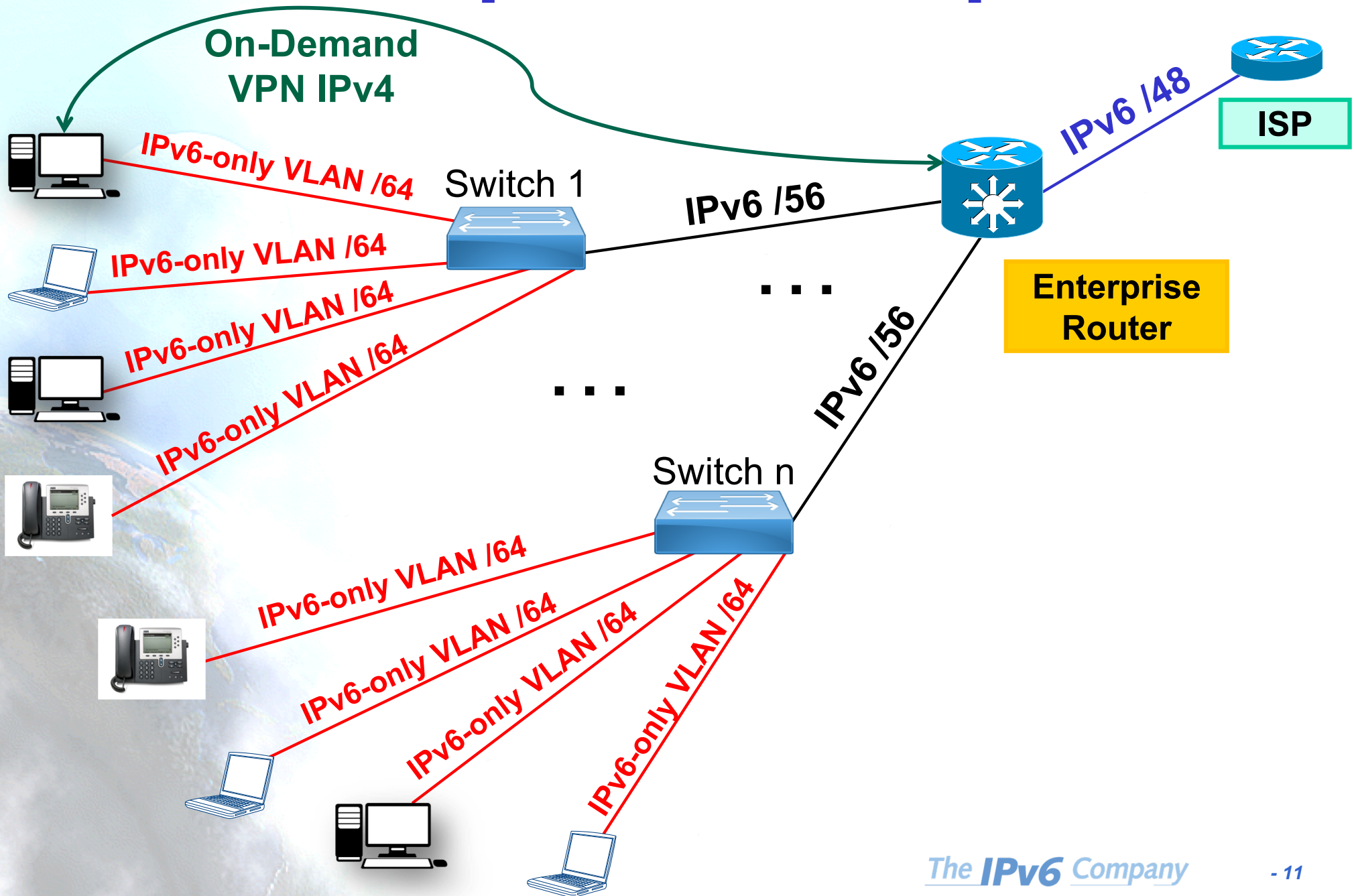
Hot-Spot Example

ISP

IPv6 /48

IPv6 /56

Hot-Spot
Provider
Router

IPv6 /64

AP 1

AP n

WiFi

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /64

IPv6 /56

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

Server 1

IPv6 /64

Server 2

IPv6 /64

IPv6 /64

. . .

Server n

IPv6 /64

Rack 1

IPv6 /56

. . .

. . .

IPv6 /56

IPv6 /48

ISP

Data Center Router

Server 1

IPv6 /64

IPv6 /64

Server 2

IPv6 /64

. . .

Server n

IPv6 /64

Rack n

Enterprise Example

On-Demand
VPN IPv4

IPv6 /48

ISP

IPv6-only VLAN /64

Switch 1

IPv6 /56

IPv6-only VLAN /64

Enterprise Router

IPv6-only VLAN /64

IPv6-only VLAN /64

. . .

. . .

IPv6 /56

Switch n

IPv6-only VLAN /64

IPv6-only VLAN /64

IPv6-only VLAN /64

IPv6-only VLAN /64

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

IPv4 addresses needed for your transition?

Contact   iP.BROKER

info@ipbroker.es - www.ipbroker.es
(reference "The IPv6 Company")