Microsoft IT: Journey to IPv6

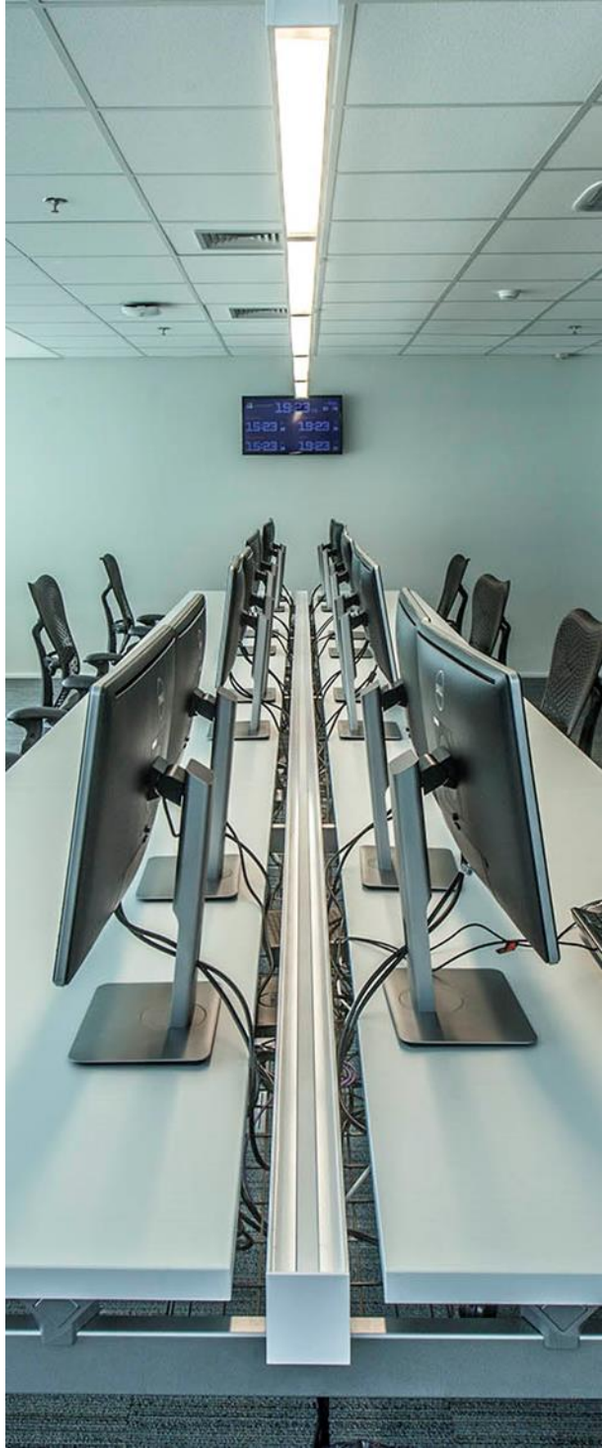
Veronika McKillop
Network Architect
Microsoft CSE&O

Agenda

- Network Overview
- Dual-Stack Status
- Moving to IPv6-Only

Network Overview

- Four regions with smaller campuses and tail sites
  - Puget Sound (Redmond, WA) – the main campus
  - North America, Europe/Middle East/Africa, and Asia Pacific
  - 790+ locations in total
- On-premise DCs and services in Azure
- Tail sites WAN connectivity as MPLS
- Internet peering enabled in US and regions
  - Mostly with AS8075
  - AS that supports online services in Microsoft (Azure, Microsoft.com, Bing, Office 365, etc.)
- ~ 113K+ employees (~220K end users)
- ~ 1900 LOB applications managed by Microsoft IT
- ~ 1.2M devices hitting the network



Dual-Stack Story

IPv6 is always a story of *perseverance*…

Dual Stack Story

- IPv6 since 2001, Microsoft Research investigating and deploying it
  - ISATAP – first on Windows servers, then on a HW platform
- IPv6 more broadly deployed in 2006 using mixture of ISATAP and native
  - In large development centres (India, China, Redmond, WA, etc.)
- 2011 – IPv6 became a strategic goal
  - Remember the Nortel IPv4 address space acquisition? All public space moved to Azure
  - Backbone network – Dual Stack rolled out, converted to Single Topology IS-IS
- One /32 prefix per RIR region (ARIN, RIPE, APNIC)
- During 2016 retrofit IPv6 native pushed to all corporate networks
  - All managed labs dual stacked since 2011
  - Unmanaged labs and some other environments are a bit harder
- There are still many networks which are IPv4-Only… ☹

Moving to IPv6-Only

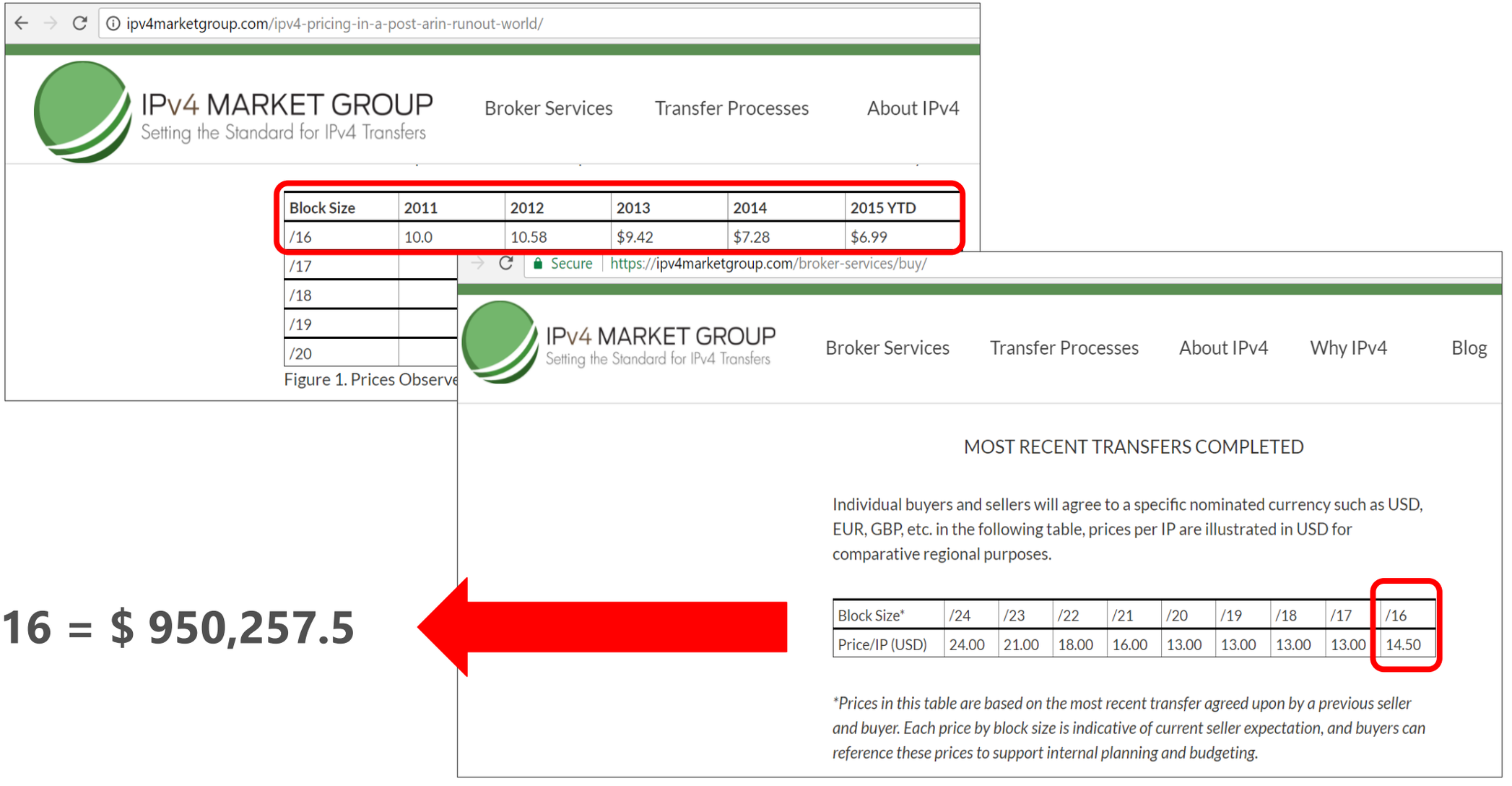
Motives

Why is Microsoft IT moving to IPv6-Only?

- Industry pressure = Microsoft Product Group requirements
  - June 2015 Apple WWDC announced IPv6-Only
  - MS Apps in App Store?
  - >89 apps in Apple App Store


- Exhaustion of RFC1918 space
  - Countless items consume our IP addressing space
  - No large contiguous blocks available
  - IoT is not just a buzz word - Smart parking signs, Micro-herb greenhouses, Security cameras, Door access systems, anything that requires connectivity
- Overlapping RFC1918 space
  - Azure, Acquisitions
- Operational complexity of dual stack
- Strategic goal with management support

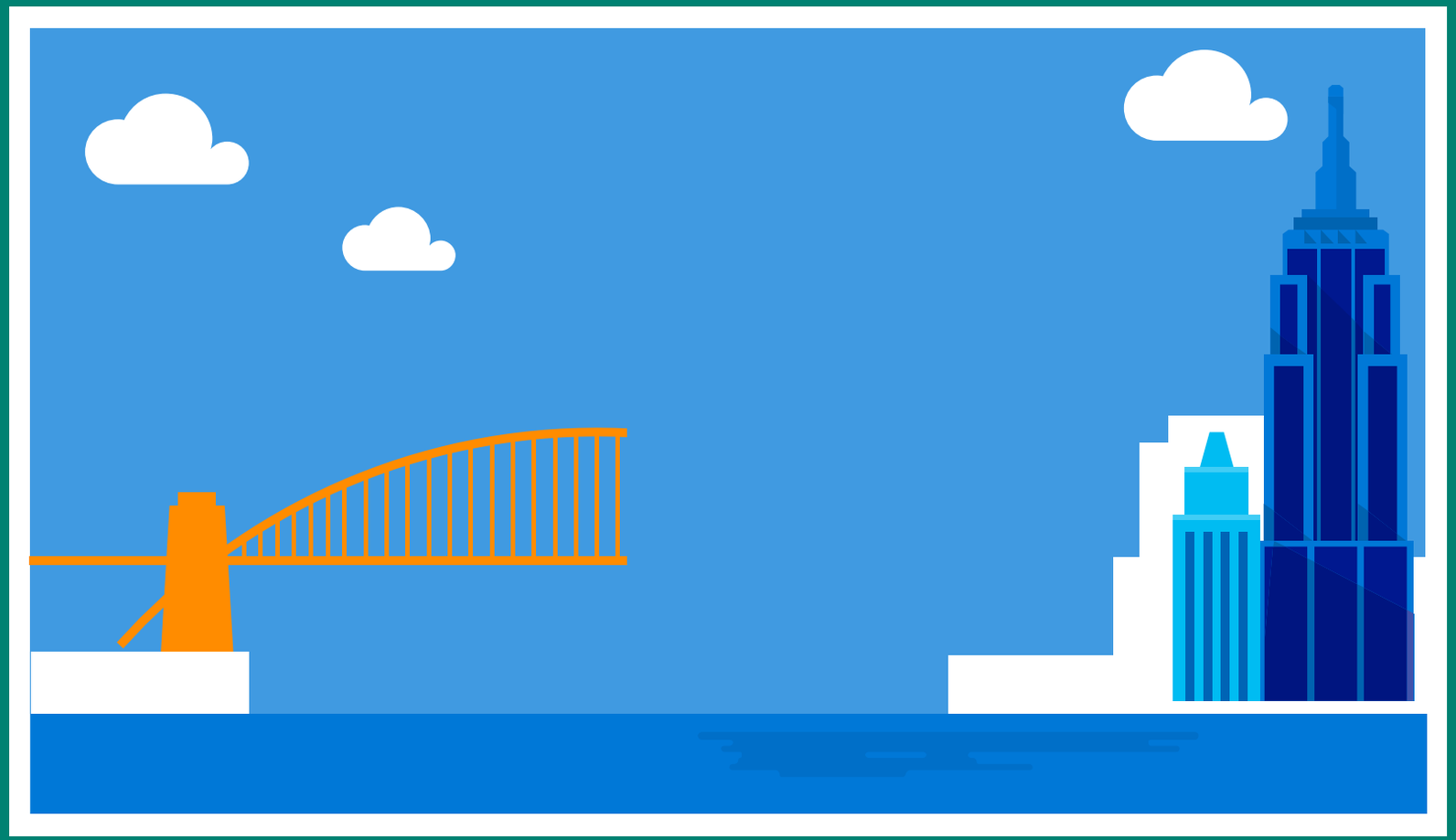
Why IPv6-Only? Because IPv4 is costing $$



/16 = $ 950,257.5

Source: [IPv4 Market Group]

Dual stack is IPv6 only half done…



Moving to IPv6-Only

Past & Present

Wireless Guest IPv6-Only

- We needed to test what IPv6-Only looks like
  - What was going to break?
- We thought the application profile was much simpler
  - Web, email, etc.
- Could be used by internal development
- We assumed fewer Service Level Agreement issues expected versus the corporate network
- We wanted to get the exposure, move faster

This WAS the plan…

IPv6-Only on Wireless Guest cancelled ☹

- IPv6-Only leverages NAT64 & DNS64 to access IPv4-Only resources
- Majority of VPN clients doesn't work through NAT64
  - RFC 7269 notes IPSec issues – a VPN needs NAT Traversal support in IKE and must use IPSec ESP over UDP
- Lesson learned: When your VPN concentrator is dual-stacked, IPv6 gets you out ☺

The result: roll out of Dual-stack in our Wireless Guest globally

"Scream tests" of IPv6-Only in the next 12 months when vendors deliver IPv6-Only Features

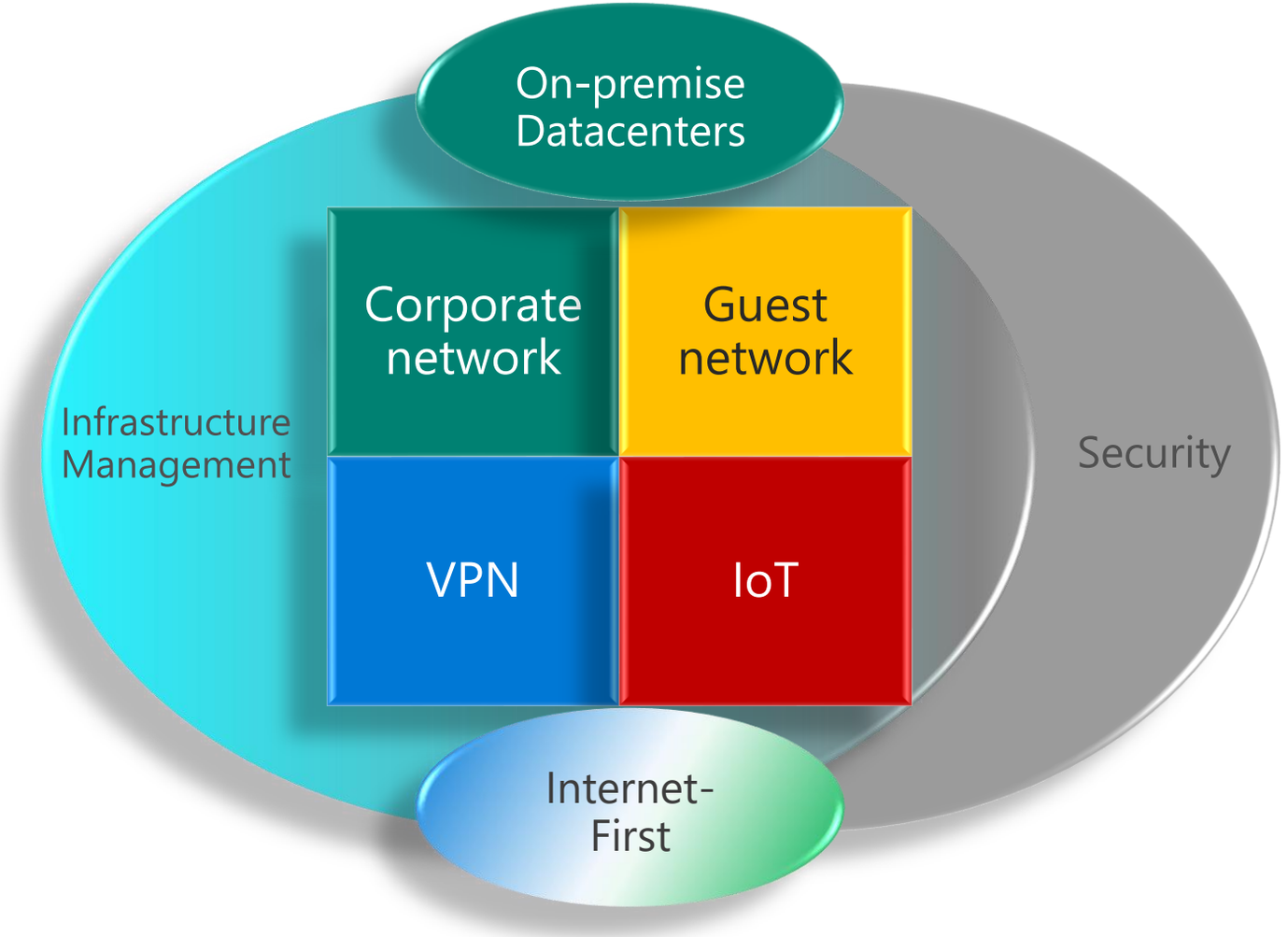
IPv6-Only SSID for Product Groups

- Production IPv6-Only network for Product Groups
- Helps to meet the industry and regulatory requirements for Microsoft products
  - Apple AppStore, US Federal Government
- Pure Internet connectivity with NAT64/DNS64
  - Test cases focused on consumers, services living on the Internet and in the Cloud
- Challenge with Android platform
  - Doesn't support DHCPv6
  - RDNSS needed on our building routers (upgrades in progress)
- Deployed in 11 locations
  - 6 more coming, 1 to be decommissioned already
  - Demand driven

Moving to IPv6-Only

aka *"The Future is Forever"* (©ISOC)

When I look at the Microsoft networks…



Everything needs IPv6, not everything will be IPv6-Only

Remote Access VPN

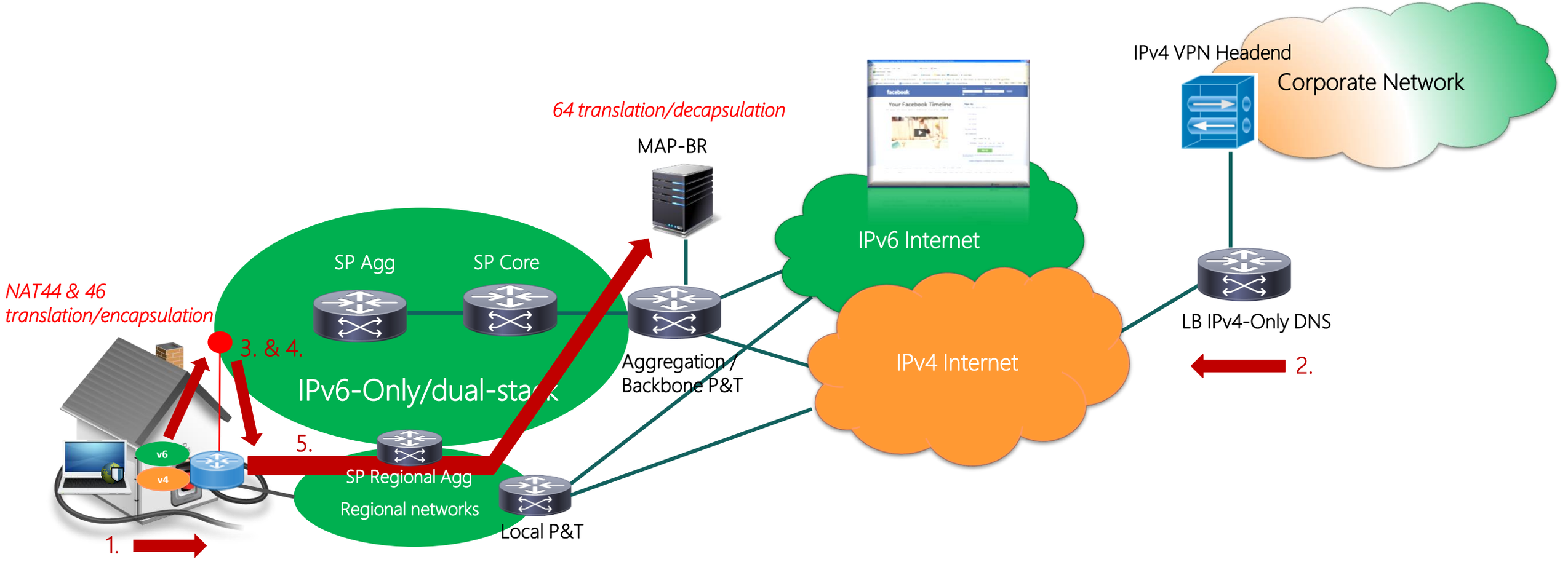
- NG-VPN dual-stacked on the inside
  - Rollout during H2 CY2017
  - Currently ~50,000 users
- NG-VPN concentrators IPv4-Only on the outside
  - Need to be dual stacked
  - Dependency on our load balancing solution

Let's look into the (not-so-distant) future…

…where IPv4-as-a-Service is reality

IPv4 NG-VPN behavior in SP IPv4-as-a-Service network

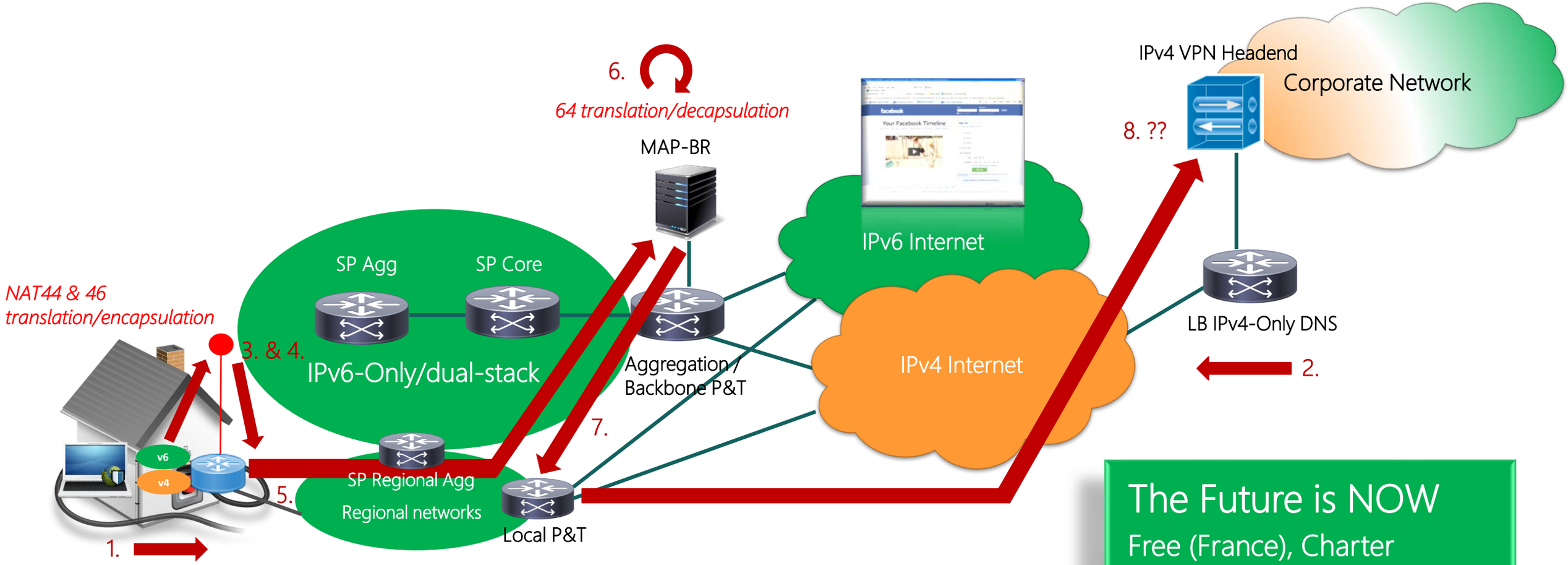
(MAP-T/E Example & IPv4-Only LB and VPN Headend)



1. VPN client does VPN concentrator address resolution
2. Load-Balancer provides DNS A record
3. VPN session establishment over IPv4 is NAT44 translated on the home CPE
4. Then 4->6 header translation/encapsulation is performed on the home CPE
5. This traffic is forwarded over IPv6-Only/Dual-stack network to MAP Border Relay

IPv4 NG-VPN behavior in SP IPv4-as-a-Service network

(MAP-T/E Example & IPv4-Only LB and VPN Headend)



6. At MAP-BR the traffic is IPv6 traffic has header replaced with IPv4/decapsulated
7. The traffic is forwarded over IPv4 to the VPN headend
8. Will the VPN Headend accept this traffic?

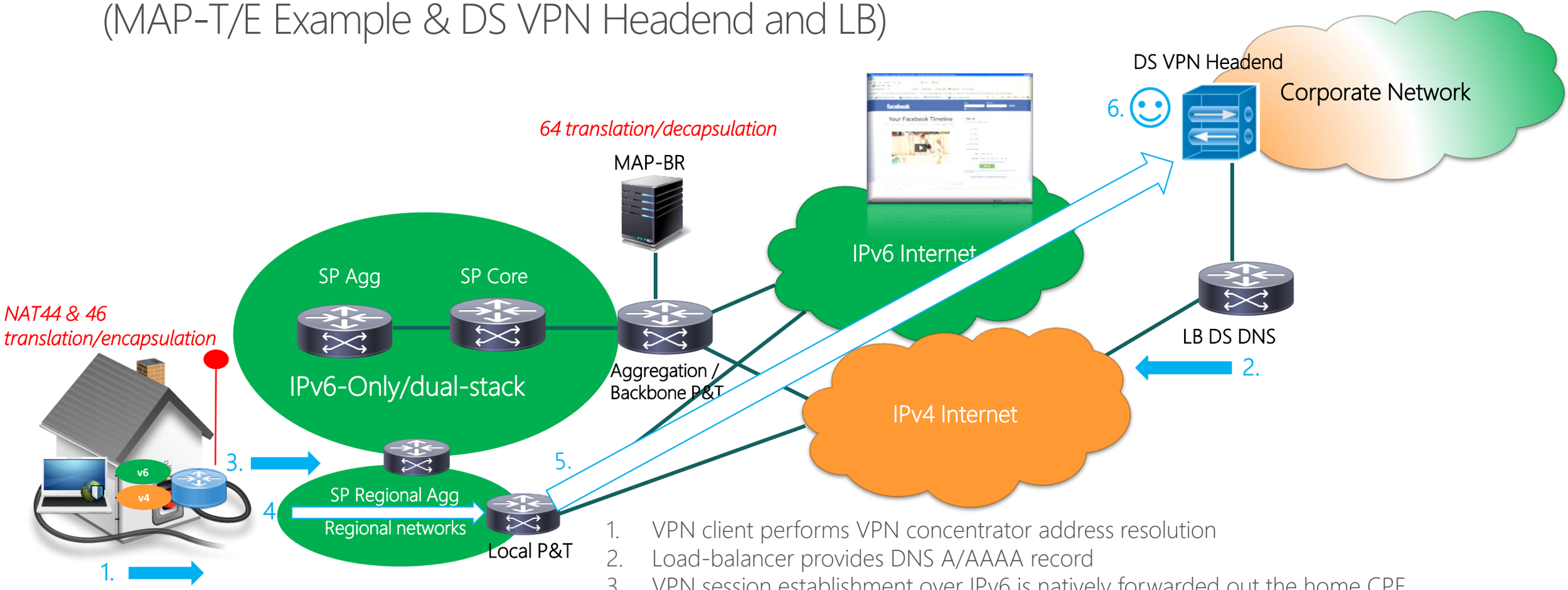
- The header has been tampered with (MAP-T)
- What about Jumbo frames (in MAP-E), fragmentation (it is SW processed on the MAP-BR)??

The Future is NOW

Free (France), Charter Communications, Comcast (tests), your any given mobile ISP (BT/EE, T-Mobile US, Reliance JIO)…

DS NG-VPN behavior in SP IPv4-as-a-Service network

(MAP-T/E Example & DS VPN Headend and LB)



1. VPN client performs VPN concentrator address resolution
2. Load-balancer provides DNS A/AAAA record
3. VPN session establishment over IPv6 is natively forwarded out the home CPE
4. This traffic is forwarded over IPv6-Only network to the nearest exit point (local P&T etc.)
5. At the local exit point the traffic is natively forwarded to the IPv6 address of the VPN Headend.
6. VPN session is established and both IPv6 and IPv4 traffic from the user device for the Corpnet is sent through the VPN tunnel

It doesn't matter what IPv4-as-a-Service technology is used by the ISP, native IPv6 gets around it.

Remote Access VPN

- NG-VPN dual-stacked on the inside
  - Rollout during H2 CY2017
  - Currently ~50,000 users
- NG-VPN concentrators IPv4-Only on the outside
  - Need to be dual stacked
  - Dependency on our load balancing solution
- VPN is a big consumer of IPv4 address space
- IPv6-Only* (on the inside) Proof of Concept
  - NAT64/DNS64 for IPv4-Only corporate resources
  - OS & VPN integration is causing different user experience

“Hitting the Walls” with IPv6-Only

- IPv6-Only VPN PoC
  - Our security vendor doesn’t support IPv6-Only Client profile
- WLAN Infrastructure Management over IPv6
  - One of our wireless vendors doesn’t support AP dynamically discovering WCL over IPv6…
- Internet-First
  - Cloud Security providers have not heard of IPv6 yet. They do indeed live in clouds…
- Network/Infrastructure Management
  - Back to “Square 1” with IPv6-Only, aka Dual-Stack “Déjà vu”?
- The Story of a Docking station
  - Switch off IPv6 RAs in the network, please… ??? ☺

We keep going

- Corpnet Wireless IPv6-Only PoC
  - The biggest consumer of IPv4 space
  - Segments of corporate network to be converted to IPv6-Only and tested on
- Measuring IPv6 traffic vs IPv4 to gain visibility
- Internet-First – enabling IPv6
  - Dual-stacked pilot in our IT building
  - Moving forward we'll have to do IPv6-Only in the offices
  - Challenge with multiple IPv6 prefixes (from the ISP and from the Corporate network) – source address selection?
  - Provisioning Domains IETF draft
    - https://datatracker.ietf.org/doc/html/draft-bruneau-intarea-provisioning-domains
- "No more IPv4" date – bad luck, do IPv6!

Internal communication is **crucial**

- IPv6 Newsletter
- IPv6 Position Paper
- IPv6 Strategy (work in progress)

Recognition matters

- Microsoft IT recognized as IPv6 World Leader 2017

The “Microsoft effect”

- At least 85% of global laptop/desktop market is Microsoft Windows-based
- 100s millions of devices (i.e. servers, Xbox, tablets, HoloLens)
- How long will it make sense to support IPv4 and IPv6 in Windows?

- How would YOU support your customers’ transition to IPv6-Only?

IPv6 Conclusion

IPv6 – No good or bad, there are just News…

- IPv6 is a long story of constant set backs and sudden victories
  - Luckily we are in 2018
- It is easy to get disheartened, but NEVER give up
  - You MUST REMEMBER to look back, consider what you have achieved and appreciate it.
  - It will carry you going forward
- Speaking publicly about the efforts also helps
  - Engage with the UK IPv6 Council
- In medium to long term, only IPv6-Only makes sense