Overview of IPv6 Transition Technologies

Veronika McKillop

UK IPv6 Council workshop

September 2018

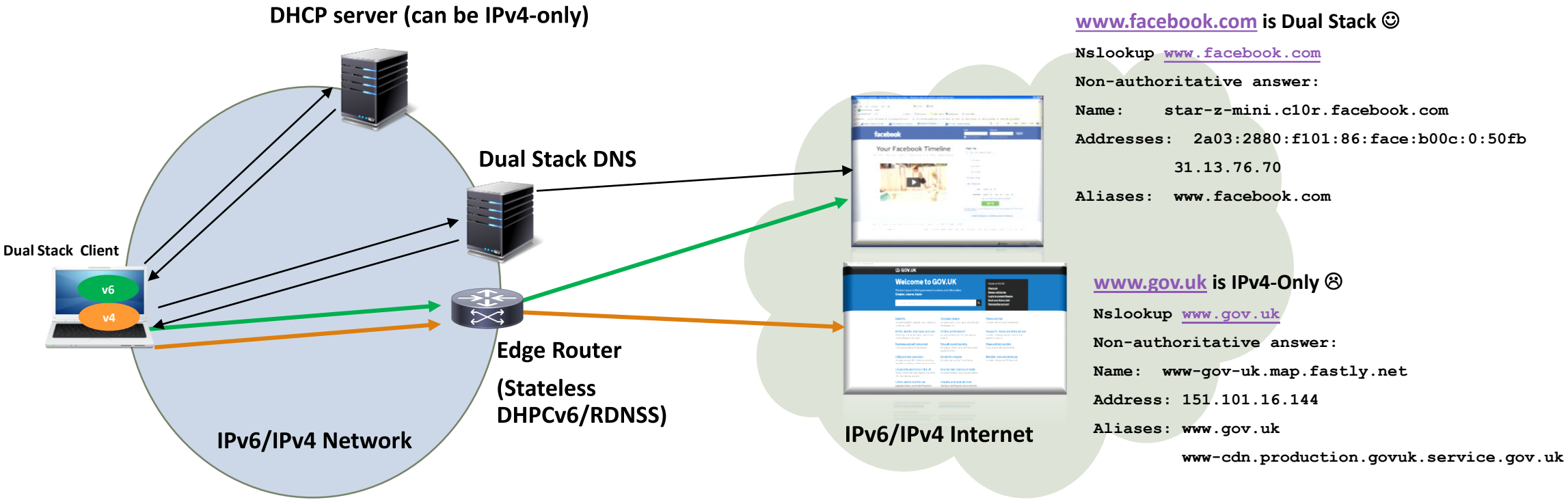
Agenda

- Dual Stack
- 6rd
- DS-Lite
- LW4o6
- MAP-T/E
- NAT64/DNS64
- 464XLAT

Dual stack = Dual IP Layer Operation

- Dual stack (IPv6/IPv4) implies providing complete implementations of both versions of the Internet Protocol (IPv4 and IPv6)
  - Run IPv4 and IPv6 alongside, both configured on interfaces, in routing, security and QoS policies, ACLs
  - Host has both capabilities enabled, IP addresses are assigned for both protocols, DNS has mapping for both IPv4 (A record) and IPv6 (AAAA record), DNS resolver on the host is capable of handling both A and AAAA record => **the whole works is running IPv6 and IPv4**
- RFCs covering the technology
  - RFC 4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service
  - RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
  - RFC 3596 DNS extension to support IP version 6 (IPv6)
  - RFC 3493 Basic socket extension for IPv6
  - RFC 4477 DHCP: IPv4 and IPv6 Dual-stack issues
  - Many more…
- IPv6 Address assignment – static, dynamic (SLAAC + stateless DHCPv6/RDNSS; stateful DHCPv6)
- Operational experience – dual security measures, dual QoS policies, dual protocol troubleshooting (IPv6 always gets the blame)
- IPv6 Routing Protocols Update – Cisco Live Online (session BRKRST-2022)

Operation of Dual Stack



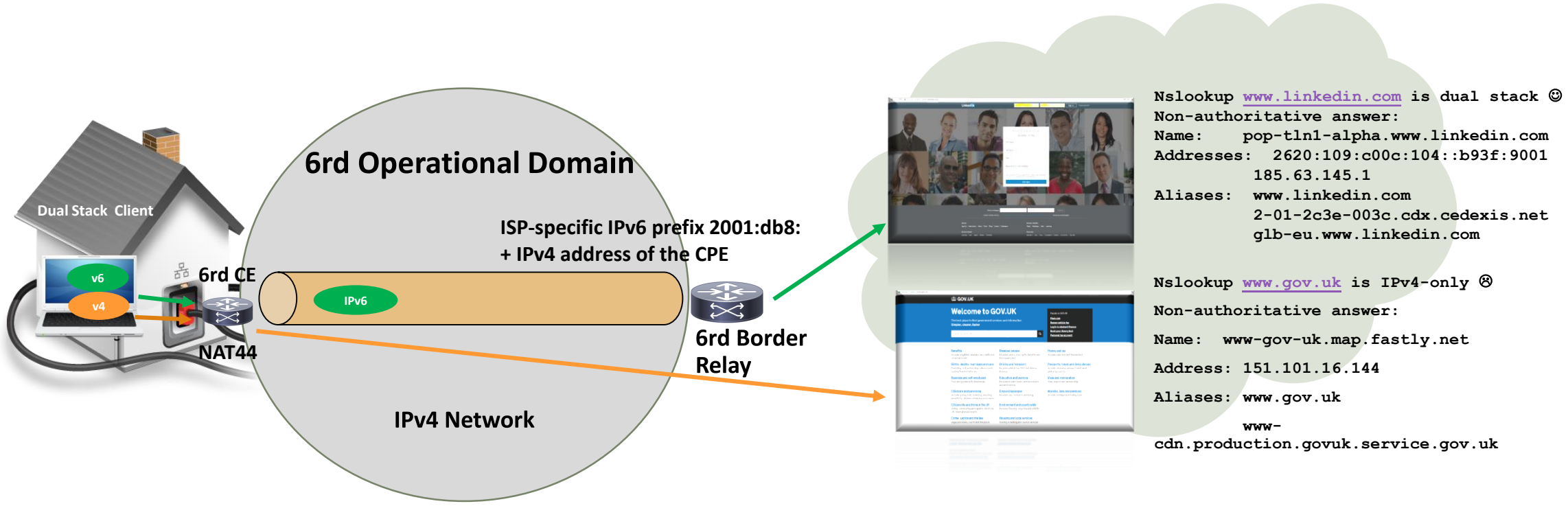
Address acquisition: IPv4 – DHCPv4; IPv6 – SLAAC w/stateless DHCPv6 or RDNSS, or stateful DHCPv6

Native routing of both IPv4 and IPv6 (OSPFv2/OSFPv3; IS-IS; EIGRP; BGP; static)

6rd = IPv6 Rapid Deployment

- An automatic tunneling mechanism enabling deployment of IPv6 to end users via a service provider's IPv4 network infrastructure
  - Automatic IPv6 prefix delegation to sites, stateless operation, simple provisioning, and service, which is equivalent to native IPv6 at the sites that are served by the mechanism.
- History – Free of Ilyad group (FR) deployed within 5 weeks IPv6 for its 1.5M residential customers in 2007.
- Adjusted 6to4 tunneling mechanism with SP specific prefix
  - Operational domain is limited to the SP network
  - IPv6 address is derived from ISP IPv6 prefix and CPE IPv4 address; RG and 6rd BR perform automatic IPv6/IPv4 encap/decap
  - Relies on algorithmic mapping between the IPv6 and IPv4 addresses assigned for use within the SP network, which allows for automatic determination of IPv4 tunnel endpoints form IPv6 prefixes => stateless operation of 6rd
- RFCs covering the technology (first in 2010)
  - RFC 5569 IPv6 Rapid Deployments on IPv4 Infrastructures (6rd)
  - RFC 5969 IPv6 rapid deployment in IPv4 infrastructure (6rd) – Protocol specification
  - RFC 6930 RADIUS Attribute for IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)
  - RFC 7084 Basic requirements for Customer Edge routers (6rd and DS-Lite)

Operation of 6rd



Reuses IPv4 infrastructure in SP

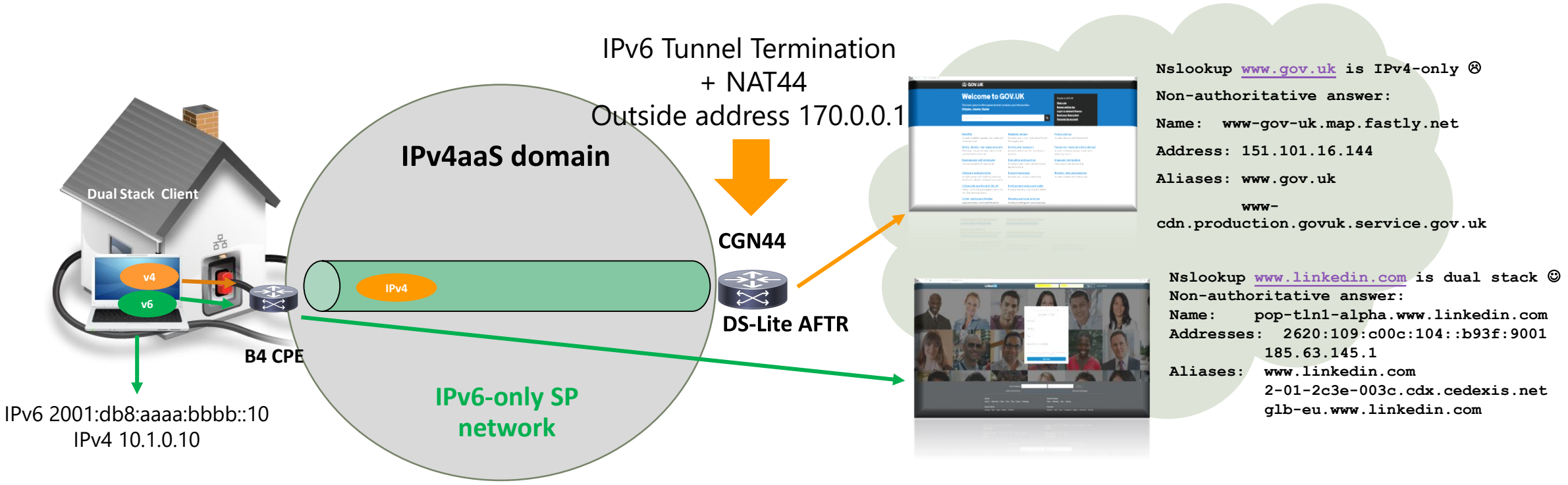
- No IPv6 support in Access and Aggregation
- No DHCP server

(!) 6rd support on residential gateway/CPE necessary

Dual-Stack Lite (DS-Lite)

- Enables a broadband SP to share IPv4 addresses among customer by combining two technologies: IP(v4) in IP(v6) and NAT
  - Carrier's network is IP6-only
  - Provides IPv4 connectivity over IPv6
  - A DS-Lite architecture consists of 2 endpoints:
    - Basic Bridging Broadband Elemet (B4): Encapsulation at CPE
    - Address Family Translation Router (AFTR): Decapsulation at Carrier + NAT (CGN)
  - NAT44 moves from CPE to the AFTR
- RFCs covering the technology
  - RFC 6333 Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
  - RFC 6908 Deployment Considerations for Dual-Stack Lite

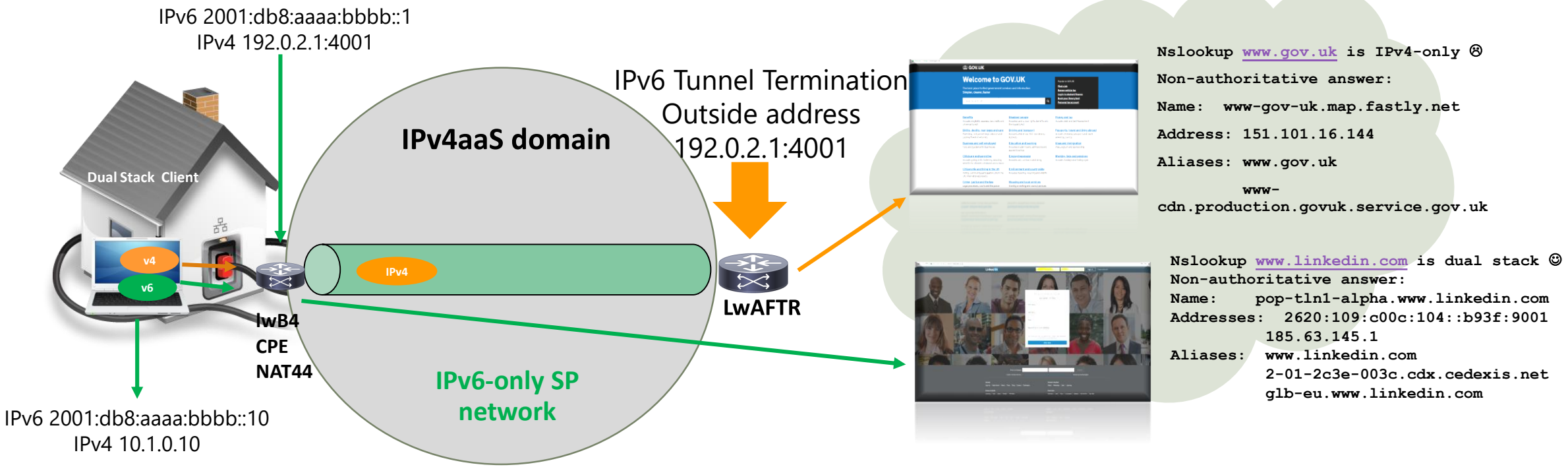
Operation of DS-Lite



Lightweight 4over6 (Lw4o6)

- Extension to DS-Lite which moves NAT from AFTR to the tunnel client in the CPE
- Reduces the amount of centralized state to be held on a per-subscriber level
- Completely stateless and thus scalable
- Access network IPv6-Only
- It consists of 2 network functions:
  - lwB4: NAT + Encapsulation
  - lwAFTR: Softwire lookup + Decapsulation
  - Relies on a A+P (Address + Port) softwires
  - A+P: Split the port space into ranges of fixed size
- RFCs covering the technology
  - RFC 7596 Lightweight 4over6: an extension to Dual-stack Lite Architecture

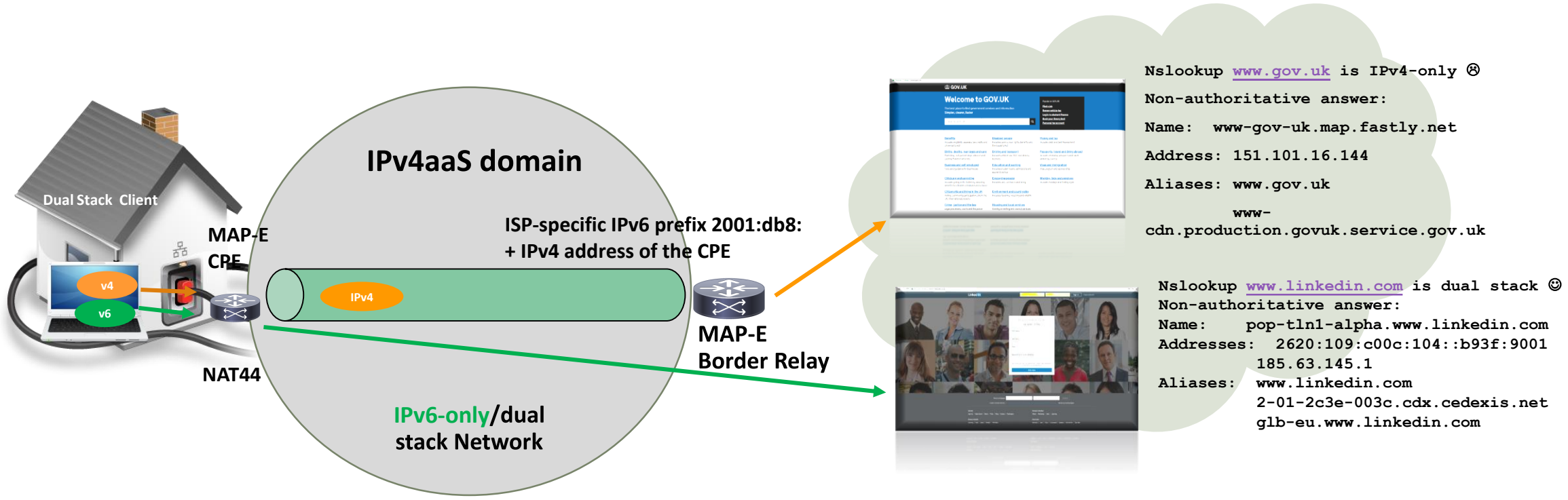
Operation of Lw4o6



MAP-T/E = Mapping Address Port
Translation/Encapsulation

- A solution that allows a service provider to enable IPv4 services at IPv6 (customer) sites to which it provides Customer Premise Equipment (CPE) IPv4aaS
- It utilizes stateless IPv4-in-IPv6 translation/encapsulation to transit IPv6-enabled network infrastructure (**often IPv6-only**)
- The encapsulation/translation must be supported by the CPE and MAP-T/E Gateway/Border Relay, which handles the IPv6 translation/encapsulation from IPv4 packets while forwarding them to the legacy Internet.
- RFCs covering the technology
  - RFC 7599 Mapping of Address and Port using Translation (MAP-T)
  - RFC 7597 Mapping of Address and Port using Encapsulation (MAP-E)

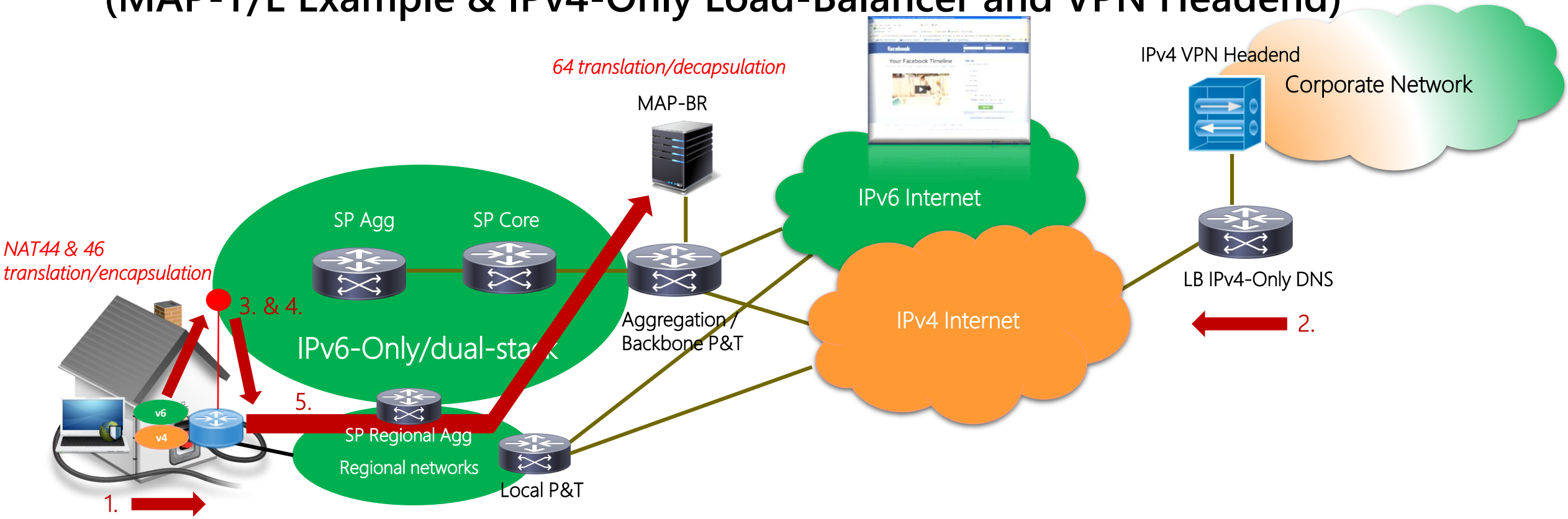
Operation of MAP-E



- It can break things for external enterprise services – you better IPv6-enable them ☺

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

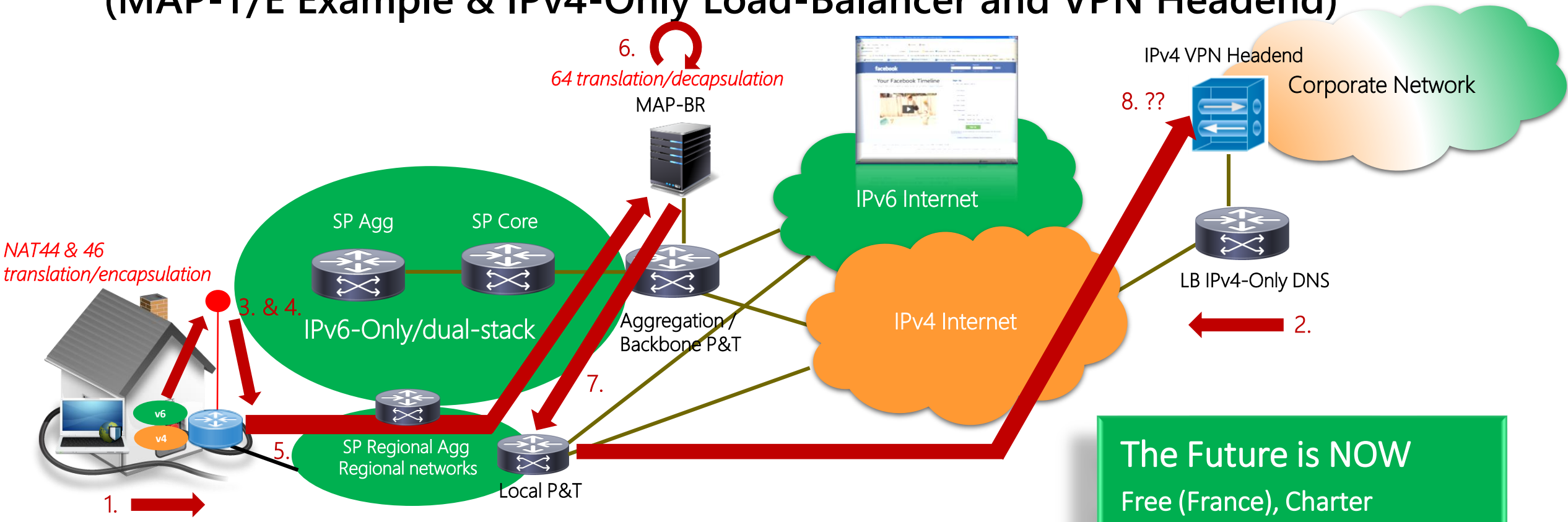
(MAP-T/E Example & IPv4-Only Load-Balancer and VPN Headend)



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 a MAP Border Relay

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

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



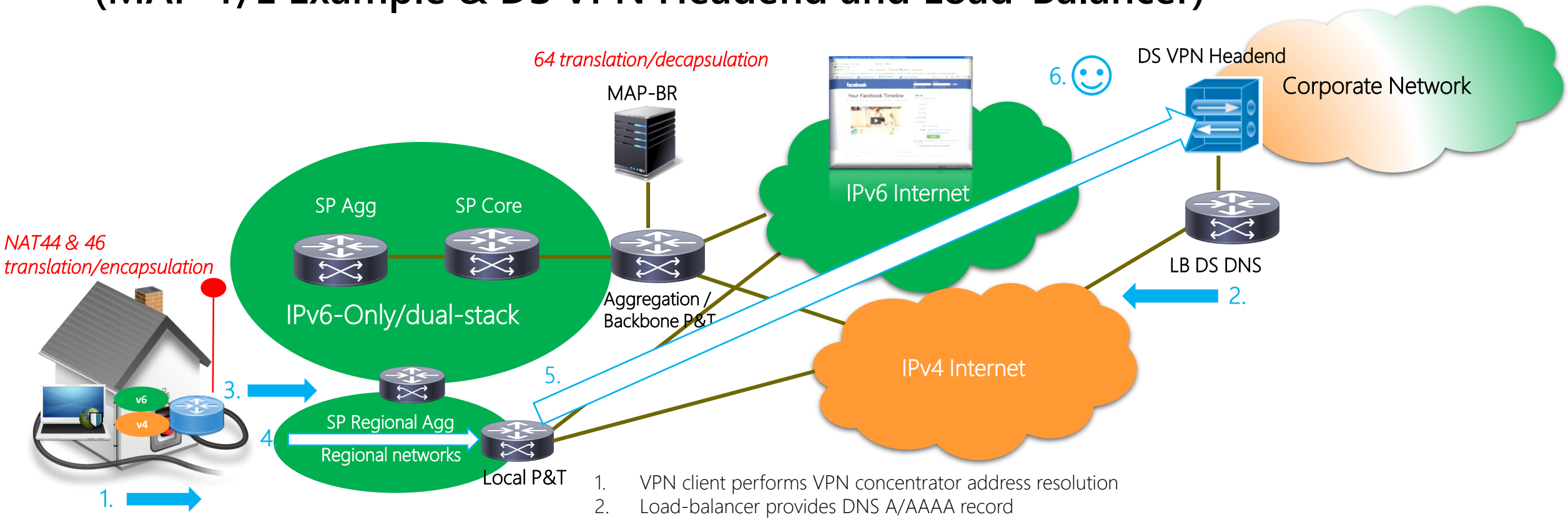
6. At MAP-BR the traffic is IPv6 traffic has header replaced with IPv4/decapsulated
7. The traffic is forwarded over IPv4 to the VPN headend
8. Will the VPN Headend accept this traffic?

- 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 VPN behavior in SP IPv4-as-a-Service network
(MAP-T/E Example & DS VPN Headend and Load-Balancer)



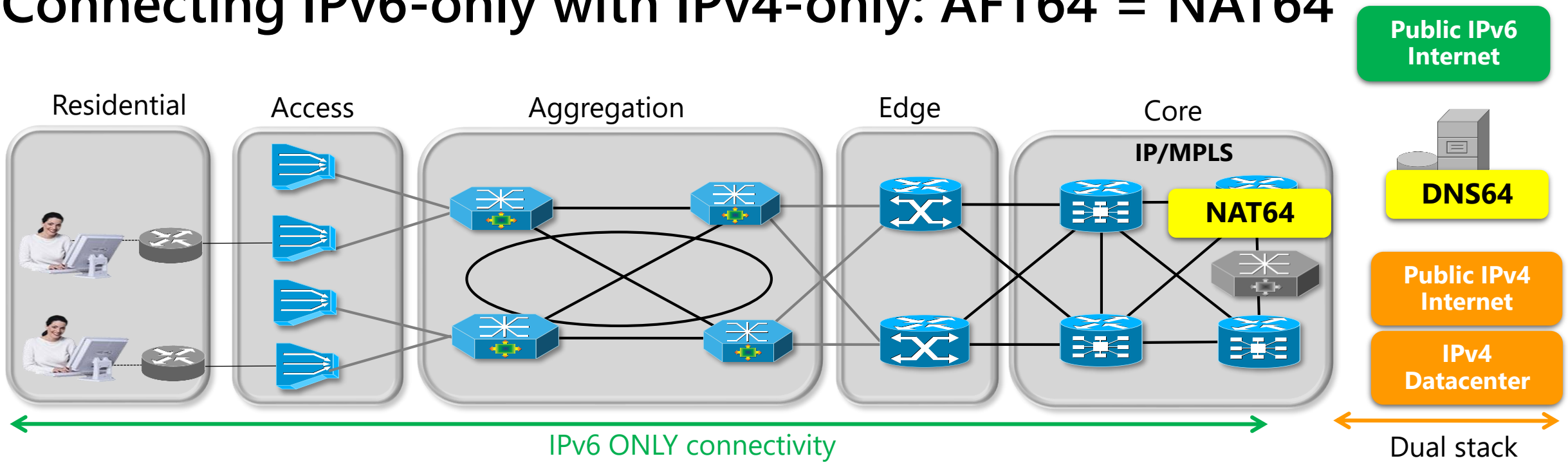
1. VPN client performs VPN concentrator address resolution
2. Load-balancer provides DNS A/AAAA record
3. VPN session establishment over IPv6 is natively forwarded out the home CPE
4. This traffic is forwarded over IPv6-Only network to the nearest exit point (local P&T etc.)
5. At the local exit point 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.

NAT64/DNS64

- NAT64/DNS64 network functions enable connectivity of IPv6-only clients to IPv4-only Internet/networks
  - You can't deploy scalable NAT64 without DNS64
    - DNS64 does the "magic" = IPv4 to IPv6 prefix synthetisation
  - IPv6 routing takes the traffic to NAT64 device
  - The session set up matters: IPv6-only ➡ IPv4-only (not the other way around!)
  - In Enterprise environment – typically deployed in Edge locations
  - In SP networks – typically in P&T locations
- RFCs covering the technology
  - RFC 6144 Framework for IPv4/IPv6 Translation
  - RFC 6145 IP/ICMP Translation Algorithm
  - RFC 6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
  - RFC 6147 DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
  - RFC 6052 IPv6 Addressing of IPv4/IPv6 Translators

Connecting IPv6-only with IPv4-only: AFT64 = NAT64

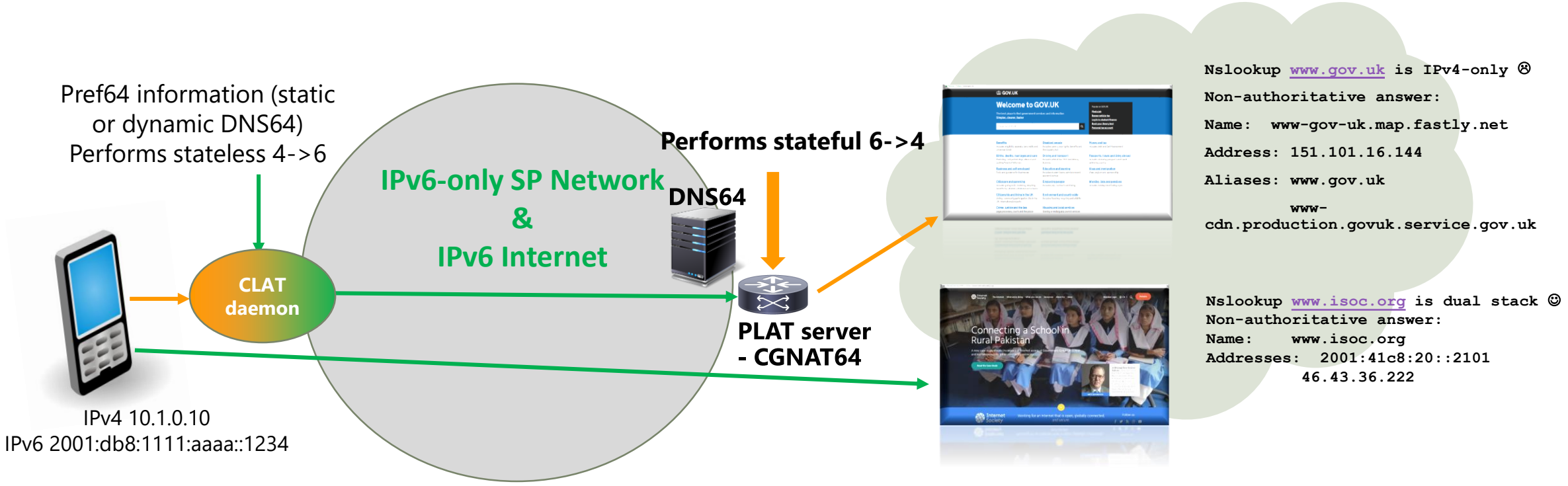


- NAT64 technology is only applicable in case where there are IPv6 only end-points that need to talk to IPv4 only end-points (NAT64 for going from IPv6 to IPv4)
- NAT64:= “stateful v6 to v4 translation” or “stateless translation”, ALG still required
- Key components include NAT64 and DNS64 (synthetic AAAA records)
- Assumption: Network infrastructure and services have fully transitioned to IPv6 and IPv4 has been phased out

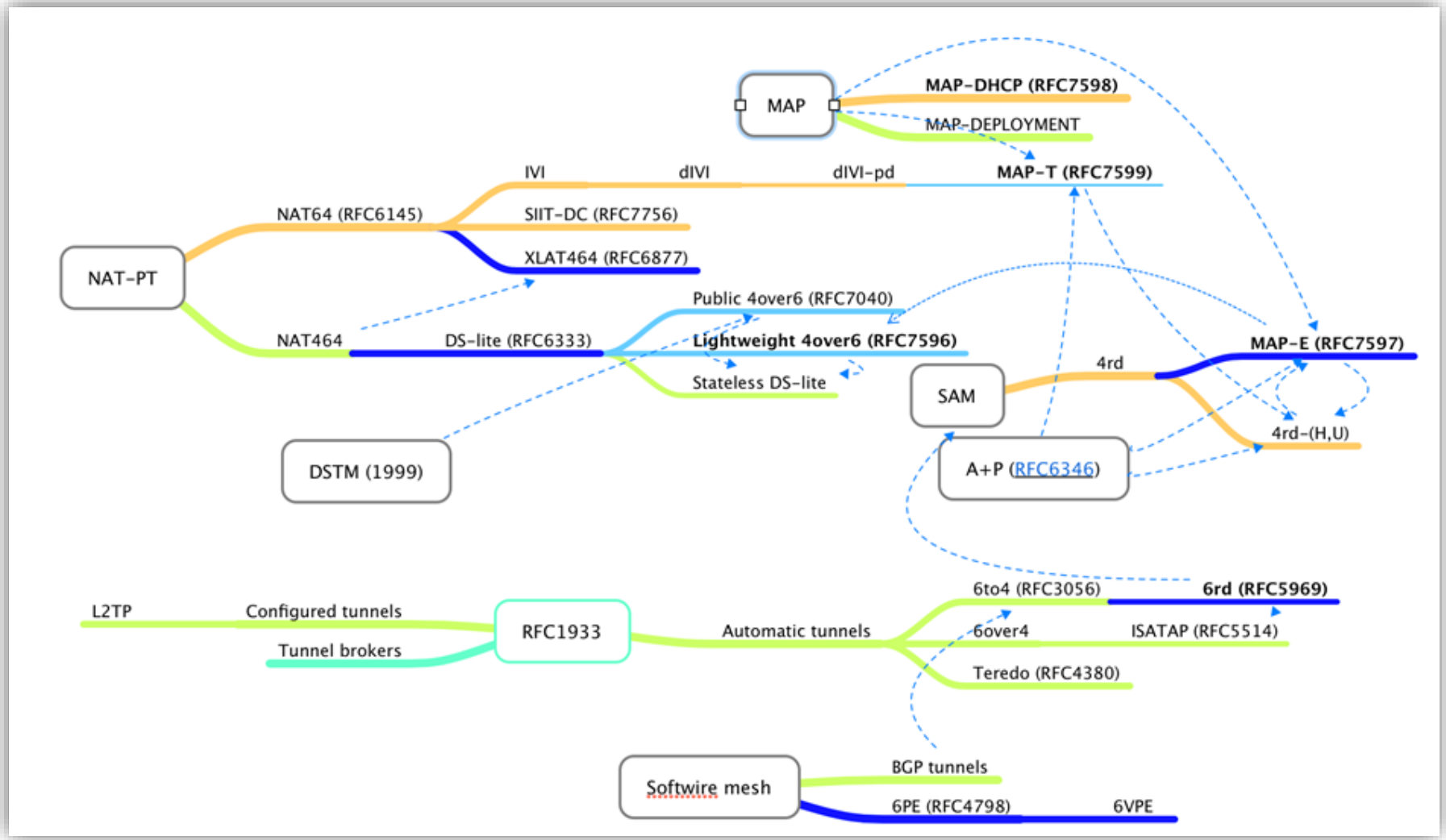
464XLAT

- 464XLAT is a simple and scalable technique to quickly deploy limited IPv4 access service to IPv6-only edge networks without encapsulation
- Components
  - CLAT – Customer side translator – a small component on your handset that exposes IPv4 to it while on IPv6-only network. It performs NAT64/DNS64-like action, it knows the DNS64 prefix, appends it to IPv4 address, creates an IPv6 packet which is transported over IPv6-only to NAT64 GW
  - PLAT – Provider side translator – strips the IPv6 prefix of the destination address and forwards the packet to the IPv4 website
- Works with applications that use Socket APIs and IPv4 literals
- RFCs covering the technology
  - RFC 6877 464XLAT: Combination of Stateful and Stateless Translation
    - RFC 6145 IP/ICMP Translation Mechanism
    - RFC 6146 NAT64
    - RFC 6147 DNS64
  - RFC 7050 Discovery of IPv6 prefix – alternative to hardcoded pref64, sends DNS query IPV4ONLY.ARPA AAAA and extracts the pref64
- Tutorial RIPE 75: https://ripe75.ripe.net/wp-content/uploads/presentations/44-ipv6-cellular_v6.pdf

Operation of 464XLAT



State of IPv6 Transition Technologies
(September 2018)



IPv6 Transition Technologies Evolution mind-map courtesy of Ole Troan, Cisco