



IPv6 in Cellular Networks

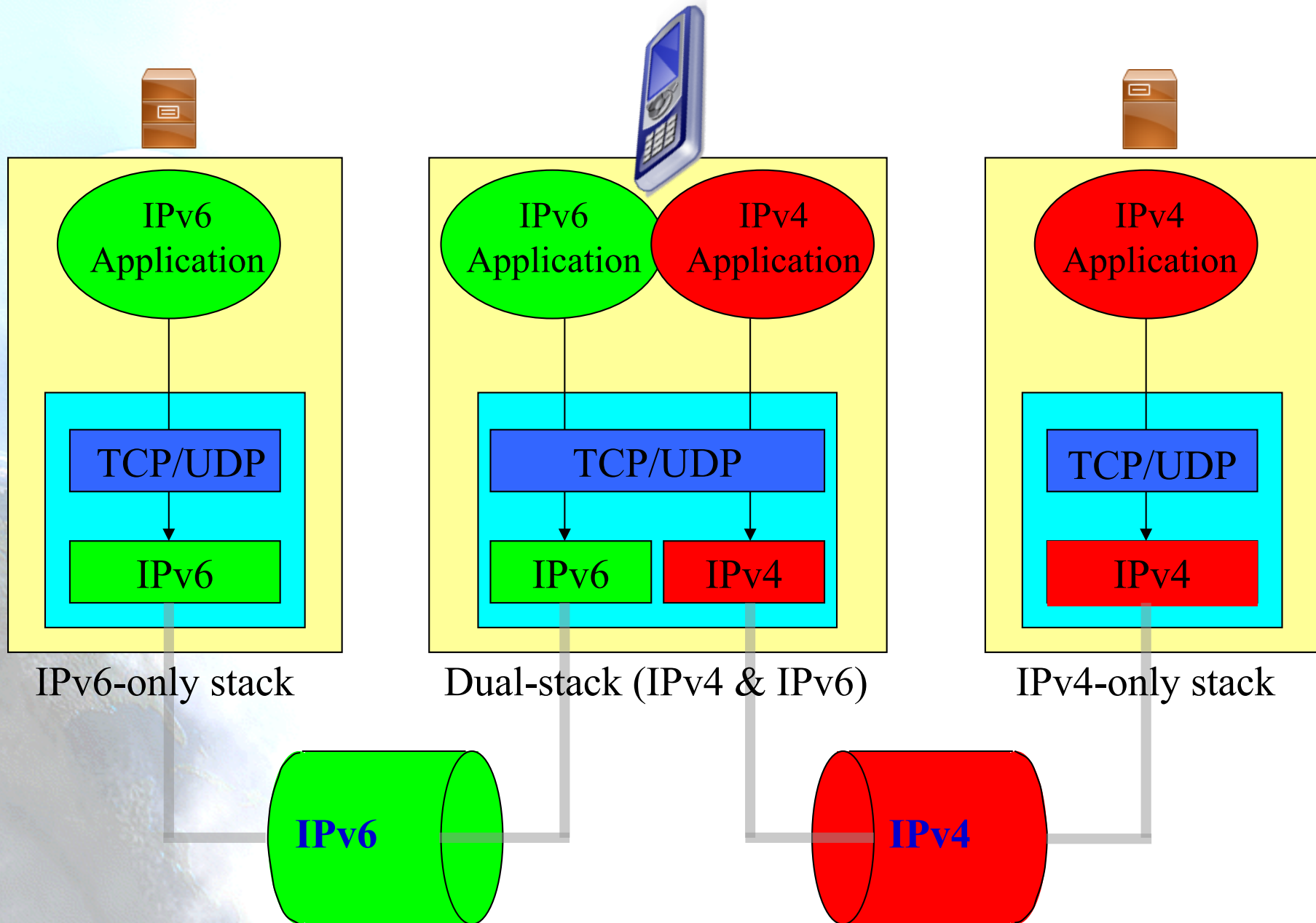
LACNIC 28
Montevideo, Uruguay
September 2017

Jordi Palet (jordi.palet@theipv6company.com)

Need to support IPv6

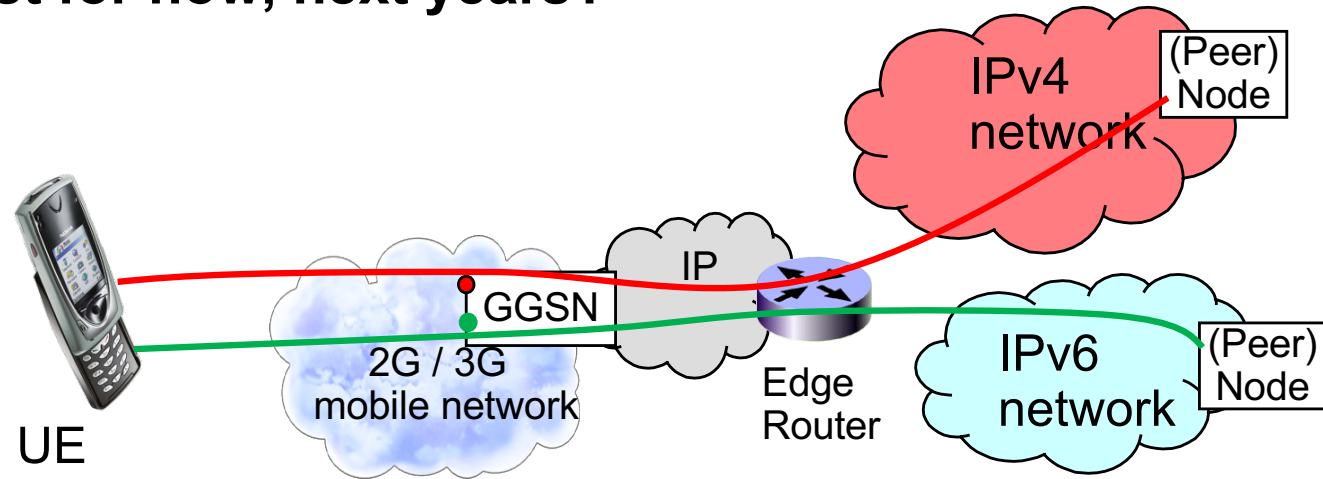
- IPv4 exhaustion
 - Sharing IPv4 (CGN) is not enough and is problematic
- Increase in number of users
- Increase in number of devices per user (and also tethering)
- Increase in number of addresses per device (VMs, other reasons)
- VoLTE/IMS
- IoT
- **LONG TERM STRATEGY**

The best solution: Dual-Stack!



Sure ?

- Do you have enough IPv4 addresses?
 - Not just for now, next years?



- O&M cost?
- Call-center impact?
- Performance?
- Licenses?
- Issues authenticating 2 addresses?

Alternatives to Dual-Stack

- **IPv6-only**
- **IPv6-only with NAT64**
- **IPv6-only with NAT64 and DNS64**
- **464XLAT**
- **Other transition technologies**

So ... IPv6-only?

- **Many examples in content providers**
- **FaceBook is one of them**
- **Datacenters are IPv6-only**
 - Started in 2014, internal traffic was 90% IPv6
 - +100 Terabits per second
 - 100% IPv6 in June 2015
 - Allows using FaceBook in IPv6-only networks and clients
 - IPv4 (from Internet) terminated in the IPv6-only clusters
 - RFC1918 space for IPv4 BGP sessions
 - Later on use RFC5549
 - Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop
 - IPv4 in IPv6 tunneling, for IPVS (IP Virtual Server)
 - IPv4 link-local (169.254.0.0/16) for Linux and switches

IPv6-only in the cellular net

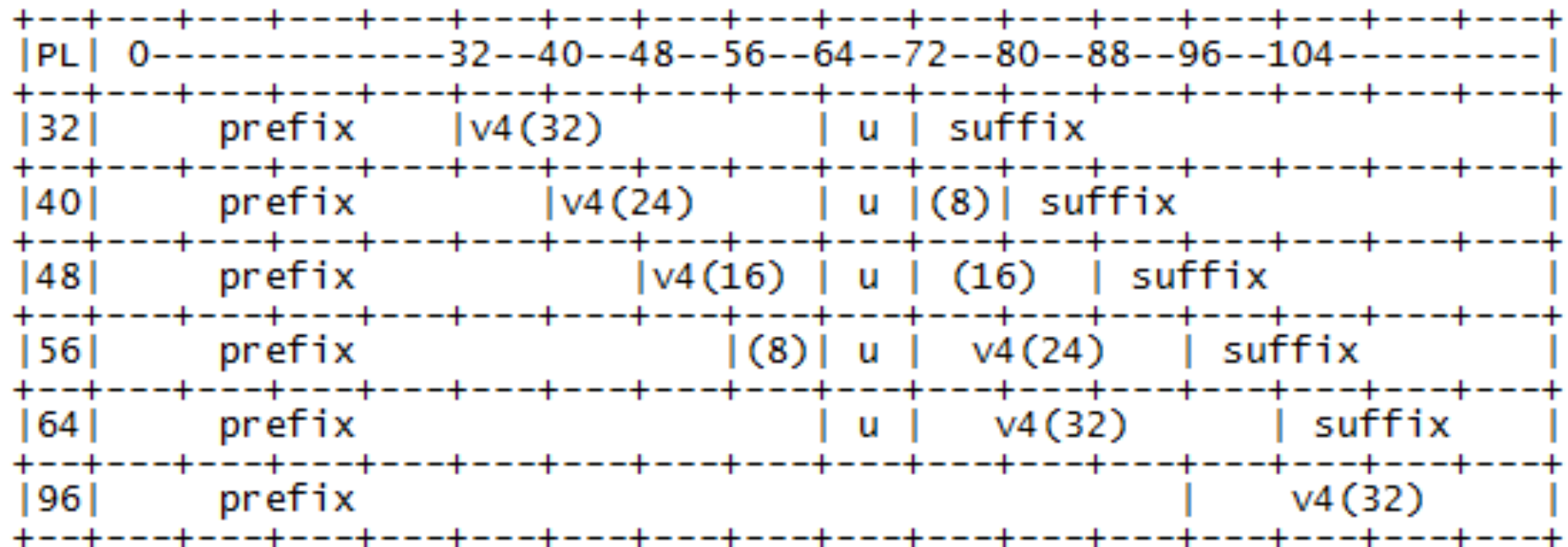
- Not an option today
- Users will be able to access IPv6-only contents and apps
 - However no access to IPv4-only ones
 - IPv4-only tethered devices will not work

NAT64 (1)

- Problem: When ISPs only provide IPv6 connectivity or devices are IPv6-only (cellular)
 - but there are still IPv4-only contents/apps in Internet
- Similar idea as NAT-PT, but working better
- Several **IPv6-only** nodes share a public IPv4 address to access IPv4 Internet
- NAT64 is a mechanism to translate IPv6 packets to IPv4 and vice versa
- Translation is carried out in packet headers following the IP/ICMP Translation Algorithm [RFC7915][RFC6146]
- Current specification only defines how NAT64 translates unicast TCP, UDP, and ICMP packets

NAT64 (2)

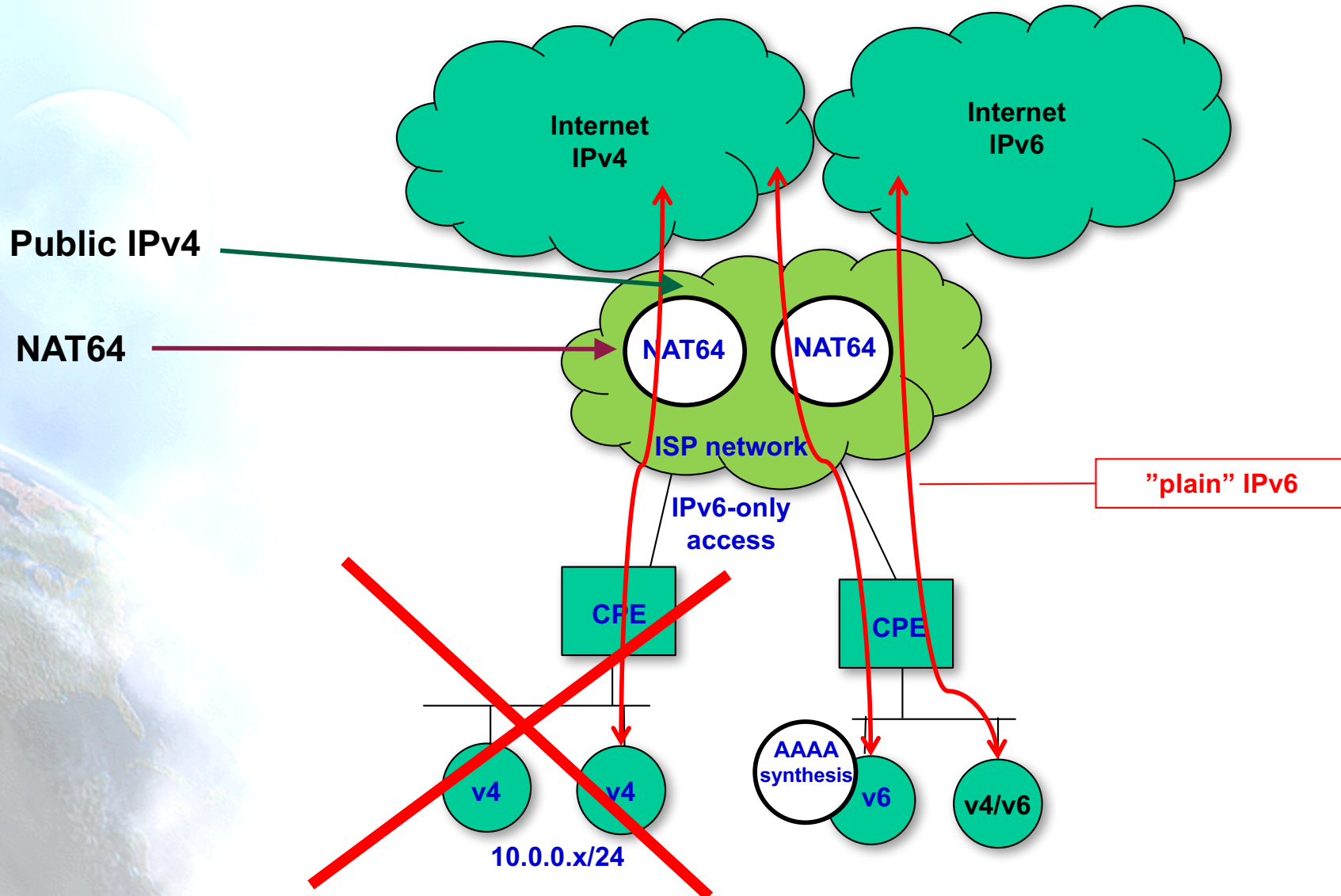
- IPv4 addresses of hosts is algorithmically translated to/from IPv6 addresses using a specific algorithm [RFC6052]
- It's based on statically configured information, including a well known prefix
- A well-known prefix is defined (64:ff9b::/96), another could be used



NAT64 (3)

- It's known that there are things that doesn't work:
 - Everything out of TCP,UDP, or ICMP: Multicast, Stream Control Transmission Protocol (SCTP), the Datagram Congestion Control Protocol (DCCP), and IPSEC
 - Applications that carry layer 3 information in the application layer: FTP [RFC6384], SIP/H323
 - Some apps: online gaming, skype, etc.
 - Peer-to-peer using IPv4 “references”
 - Literal addresses
 - Socket APIs

NAT64



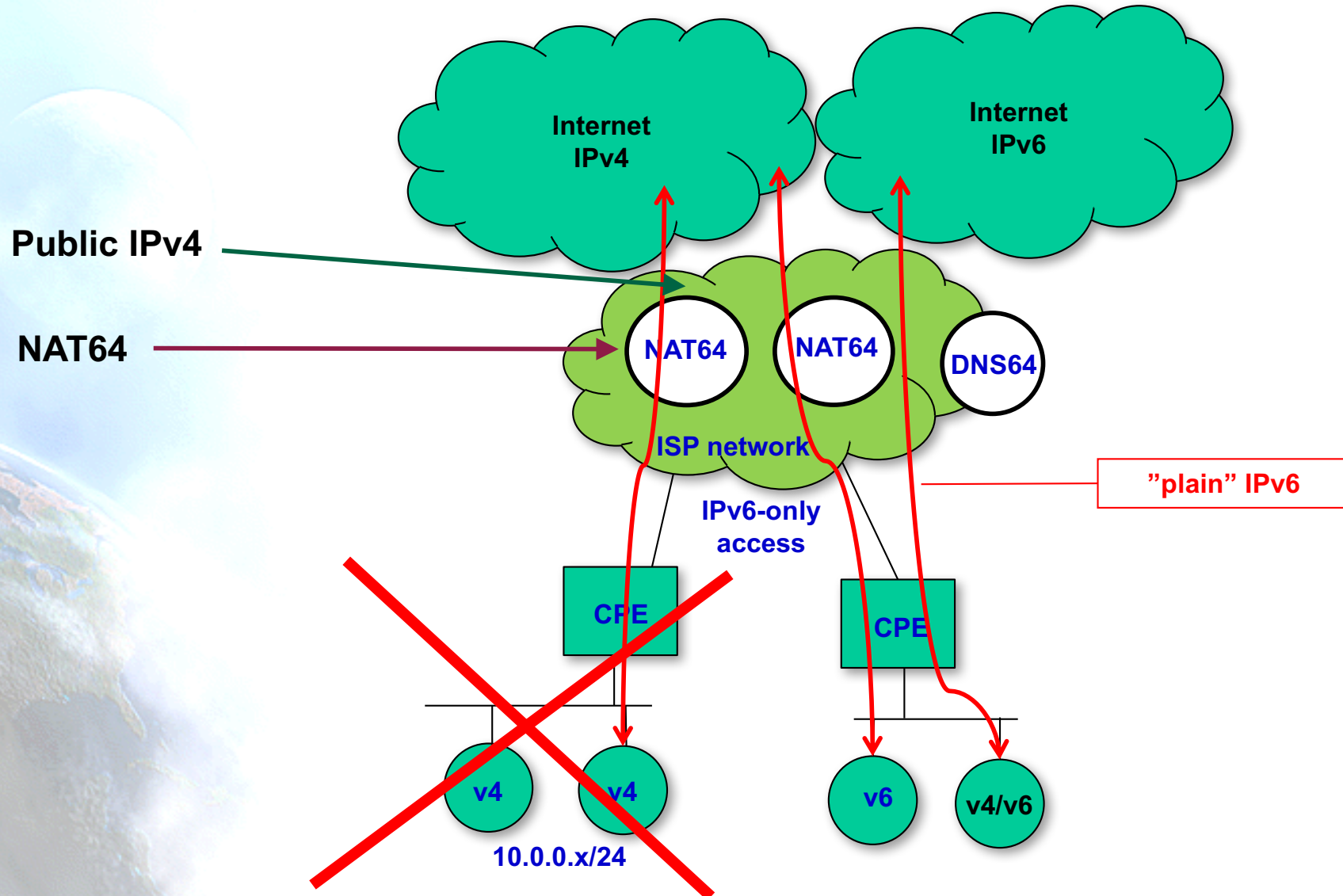
IPv6-only with NAT64

- Only valid if UE supports it
 - By means of “built-in” AAAA synthesis
 - RFC7050 (Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis) + RFC6052 (IPv6 Addressing of IPv4/IPv6 Translators)
 - Happy Eyeballs v2 includes it
- For the rest of the cases
 - Users will be able to access IPv6-only contents and apps
 - However no access to IPv4-only ones
 - IPv4-only tethered devices will not work

DNS64

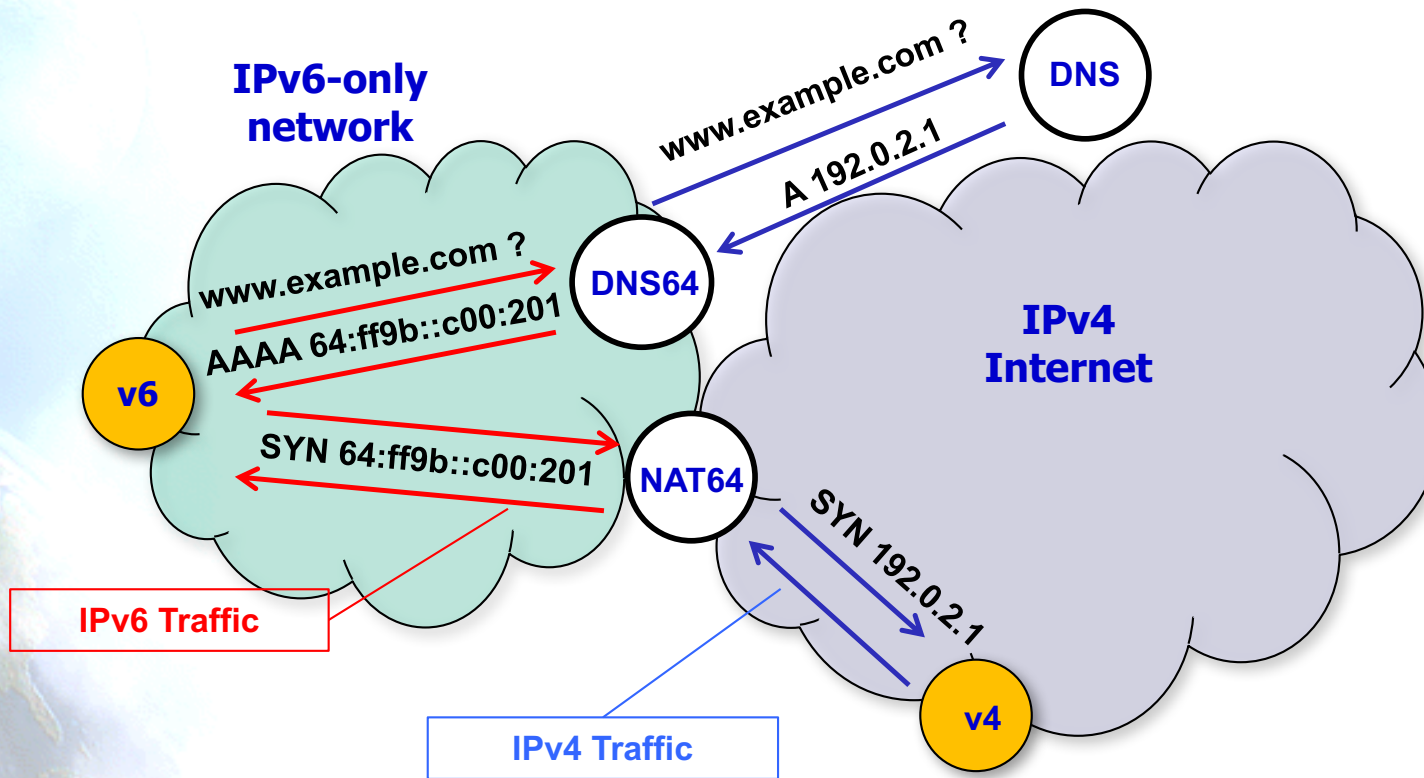
- DNS64 is a mechanism to synthesize RRs of type AAAA from A RRs [RFC6147]
- IPv6 addresses in synthesized AAAA is generated from IPv4 address and the IPv6 prefix assigned to the NAT64 device [RFC6052]
- When there is an AAAA query, it asks outside for A and AAAA RRs. If only receives an A, converts it into an AAAA
- Hosts see the host as IPv6 reachable, with the synthesized IPv6 address

NAT64+DNS64



Stateful NAT64

- Allow an IPv6-only network to connect to IPv4 Internet



IPv6-only with NAT64+DNS64

- All good ?
- NOT really ...
 - Will break if apps use:
 - Literal addresses
 - Socket APIs
 - IPv4-only tethered devices will not work

NAT64 breaks ...

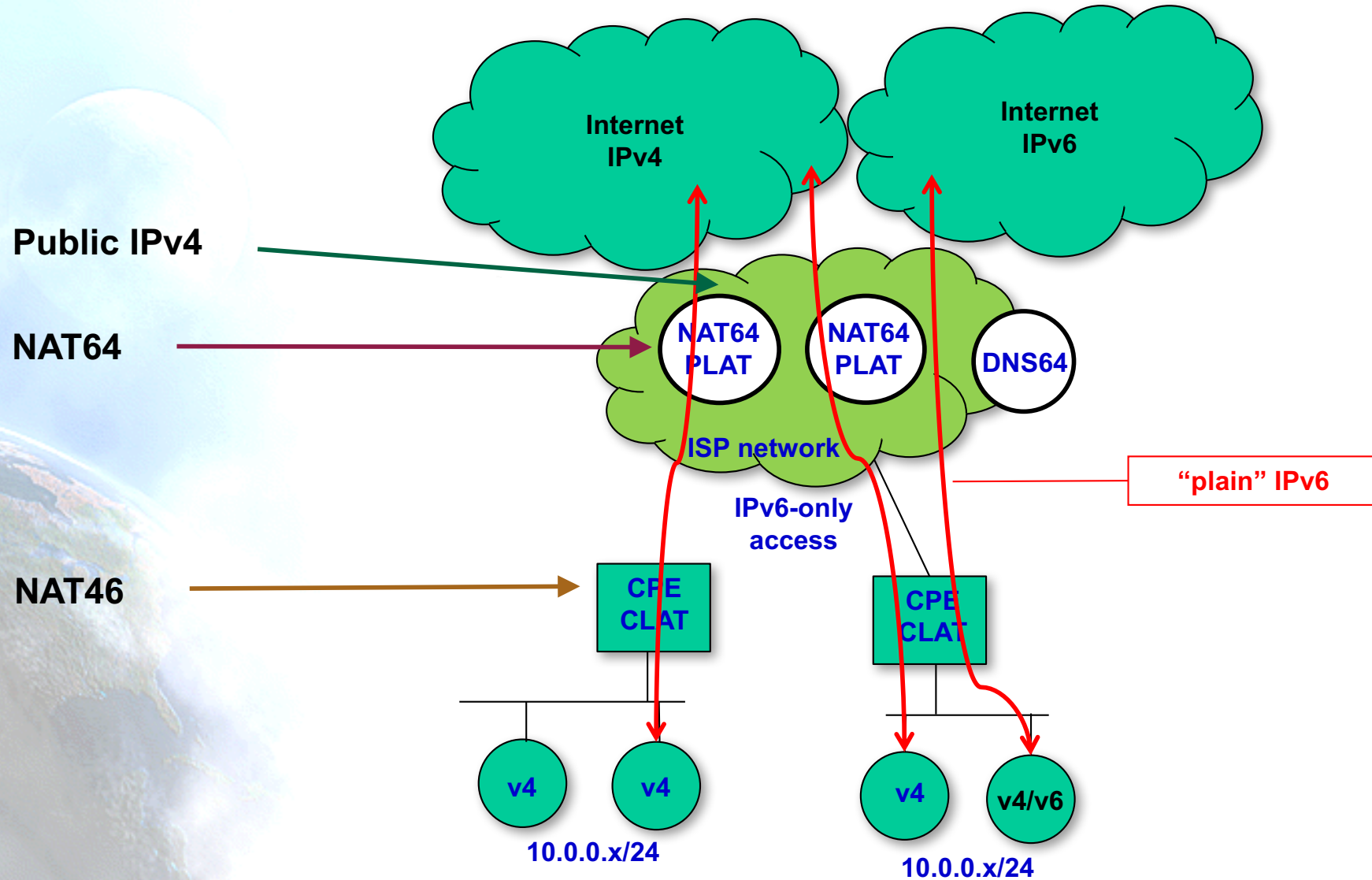
App Name	Functionality	Version	464XLAT Fixed
connection tracker	Broken	NA	NA
DoubleTwist	Broken	1.6.3	YES
Go SMS Pro	Broken	NA	YES
Google Talk	Broken	4.1.2	YES
Google+	Broken	3.3.1	YES
IP Track	Broken	NA	NA
Last.fm	Broken	NA	YES
Netflix	Broken	NA	YES
ooVoo	Broken	NA	YES
Pirates of the Caribbean	Broken	NA	YES
Scrabble Free	Broken	1.12.57	YES
Skype	Broken	3.2.0.6673	YES
Spotify	Broken	NA	YES
Tango	Broken	NA	YES
Texas Poker	Broken	NA	YES
TiKL	Broken	2.7	YES
Tiny Towers	Broken	NA	YES
Trillian	Broken	NA	YES
TurboxTax Taxcaster	Broken	NA	
Voxer Walkie Talkie	Broken	NA	YES
Watch ESPN	Broken	1.3.1	
Zynga Poker	Broken	NA	YES
Xabber XMPP	Broken	NA	

***T-Mobile**

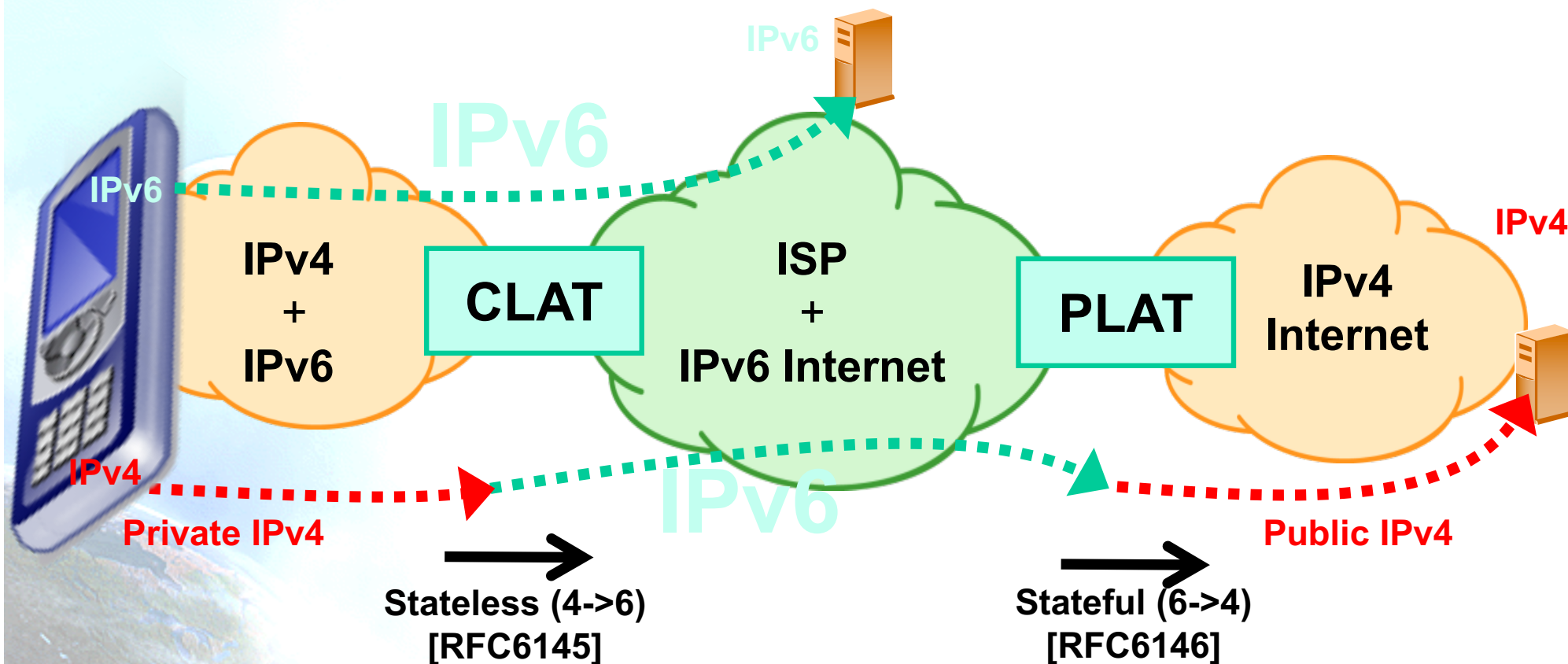
464XLAT

- 464XLAT (RFC6877): RFC6145 + RFC6146
- Very efficient use of scarce IPv4 resources
 - N*65.535 flows per each IPv4 address
 - Network growth not tied to IPv4 availability
- IPv4 basic service to customers over an-IPv6 only infrastructure
 - **WORKS** with applications that use socket APIs and literal IPv4 addresses (Skype, etc.)
- Allows traffic engineering
 - Without deep packet inspection
- Easy to deploy and available
 - Commercial solutions and open source

464XLAT

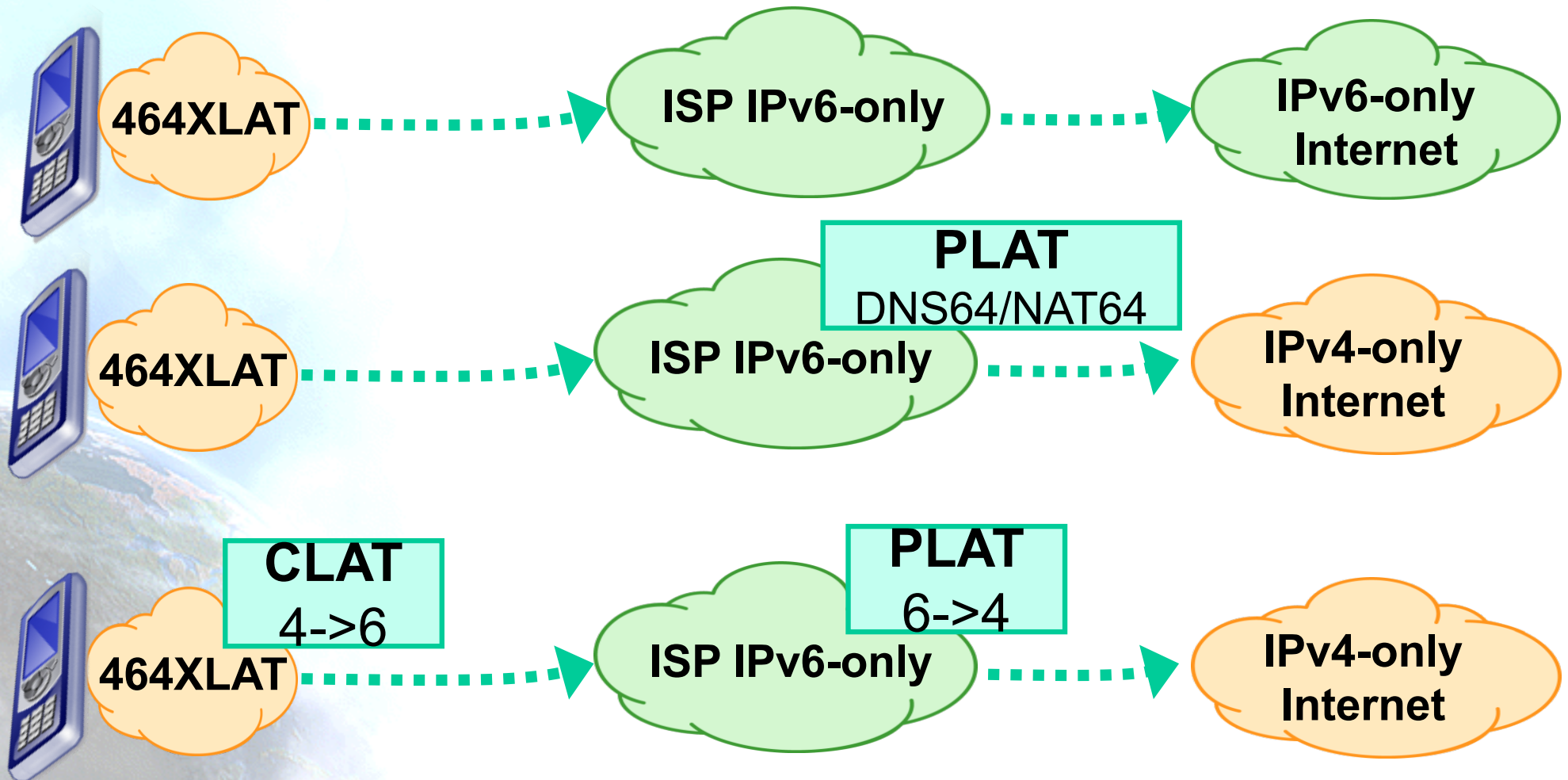


How it works 464XLAT?

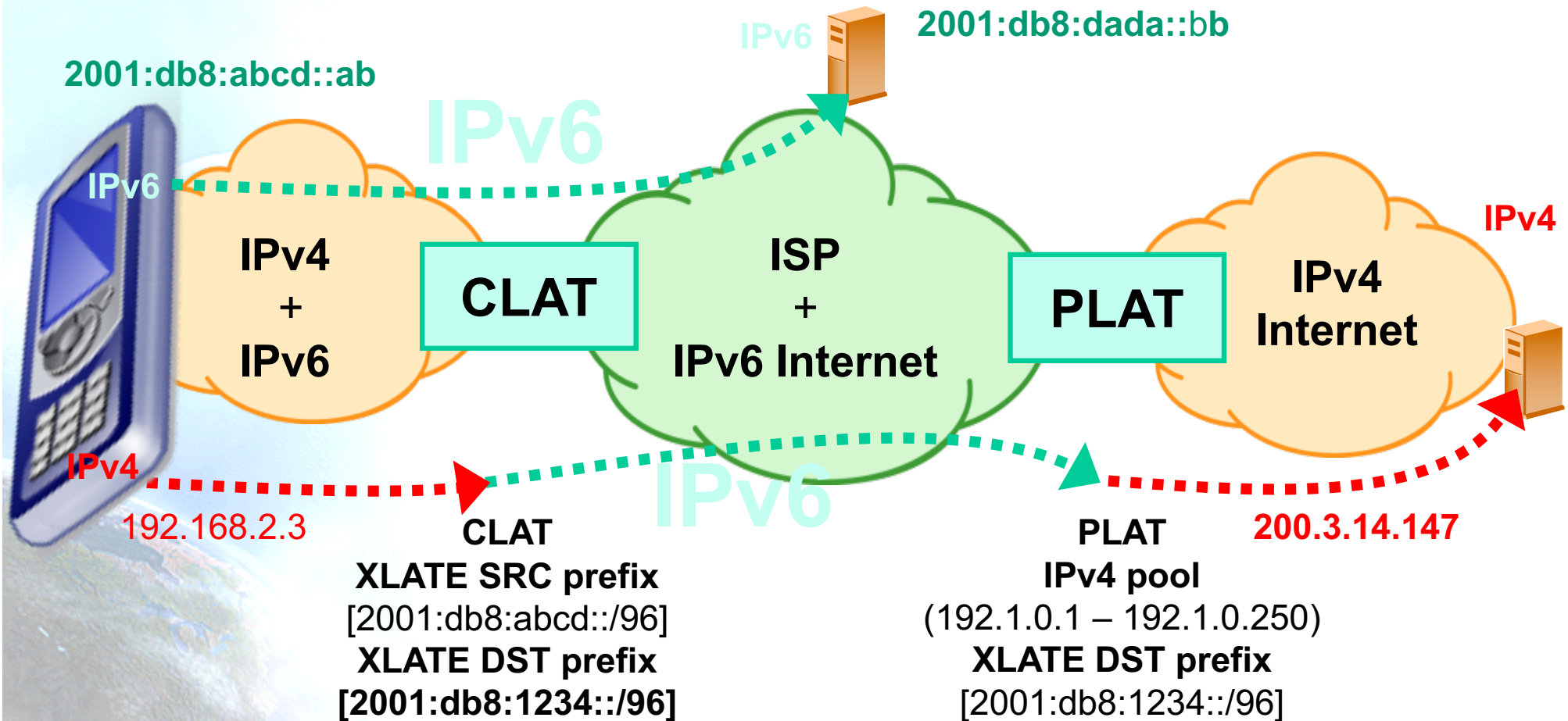


CLAT: Customer side translator (XLAT)
PLAT: Provider side translator (XLAT)

Possible “app” cases



464XLAT Addressing



IPv4 SRC
192.168.2.3
IPv4 DST
200.3.14.147

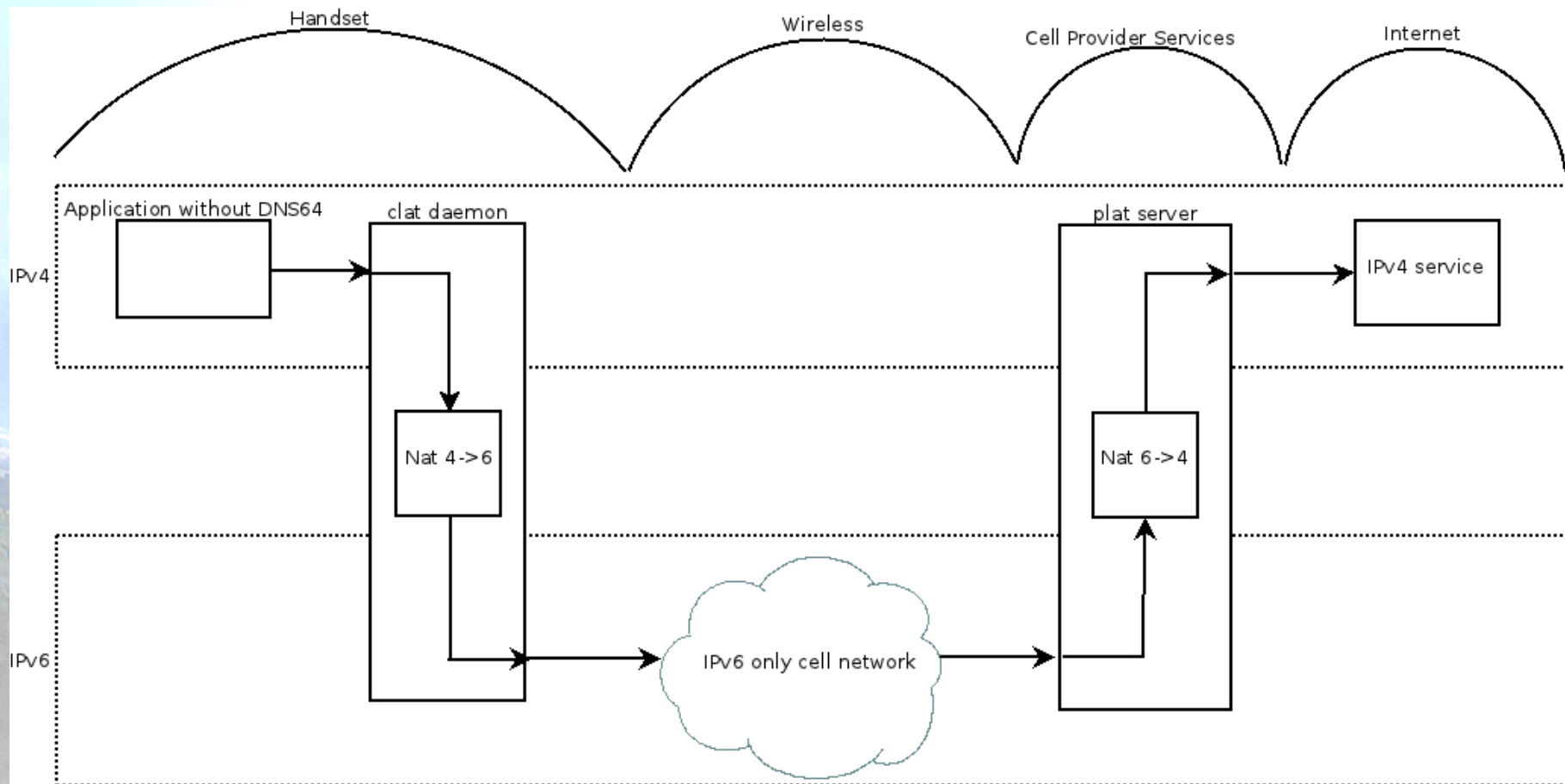
→
Stateless
XLATE
[RFC6145]

IPv6 SRC
2001:db8:abcd::192.168.2.3
IPv6 DST
2001:db8:1234::200.3.14.147

→
Stateful
XLATE
[RFC6146]

IPv4 SRC
192.1.0.1
IPv4 DST
200.3.14.147

Simplicity



* Dan Drown

Availability and Deployment

- NAT64:
 - A10
 - Cisco
 - F5
 - Juniper
 - NEC
 - Huawei
 - Jool, Tayga, Ecdsys, Linux, OpenBSD, ...
- CLAT
 - Android (since 4.3)
 - Nokia
 - Windows
 - NEC
 - Linux
 - Jool
 - OpenWRT
 - Apple (sort-of, is Bump-in-the-Host [RFC6535] implemented in Happy Eyeballs v2) - IPv6-only since iOS 10.2
- Commercial deployments:
 - T-Mobile US: +68 Millions of users
 - Orange
 - Telstra
 - SK Telecom
 - ...
 - Big trials in several ISPs

DNSSEC Considerations

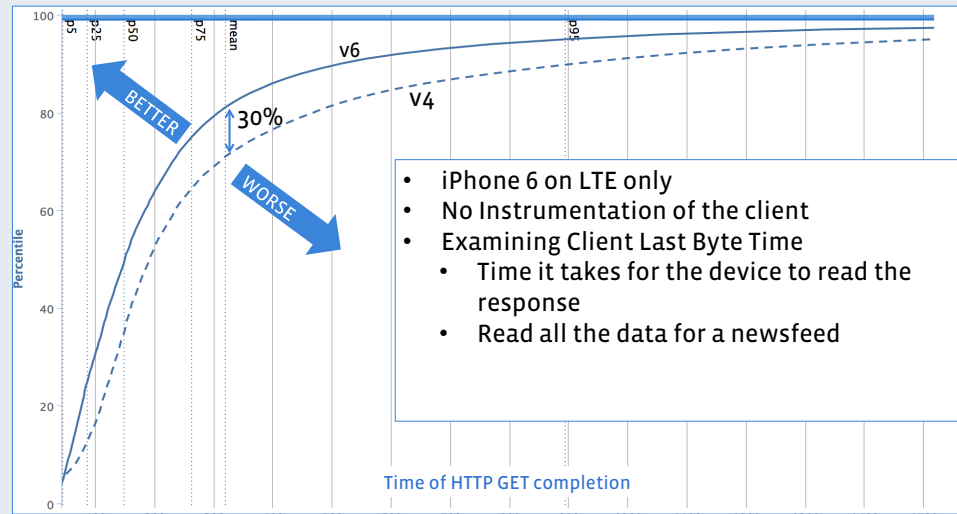
- DNS64 modifies DNS answers and DNSSEC is designed to detect such modifications, DNS64 can break DNSSEC
- In general, DNS servers with DNS64 function, by default, will not synthesize AAAA responses if the DNSSEC OK (DO) flag was set in the query. In this case, as only an A record is available, it means that the CLAT will take the responsibility, as in the case of literal IPv4 addresses, to keep that traffic flow end-to-end as IPv4, so DNSSEC is not broken
- Today no apps in cellular that use DNSSEC, but you should be ready for that
 - Consider apps used by means of tethering
 - Very relevant for non-cellular networks

Other Transition Technologies

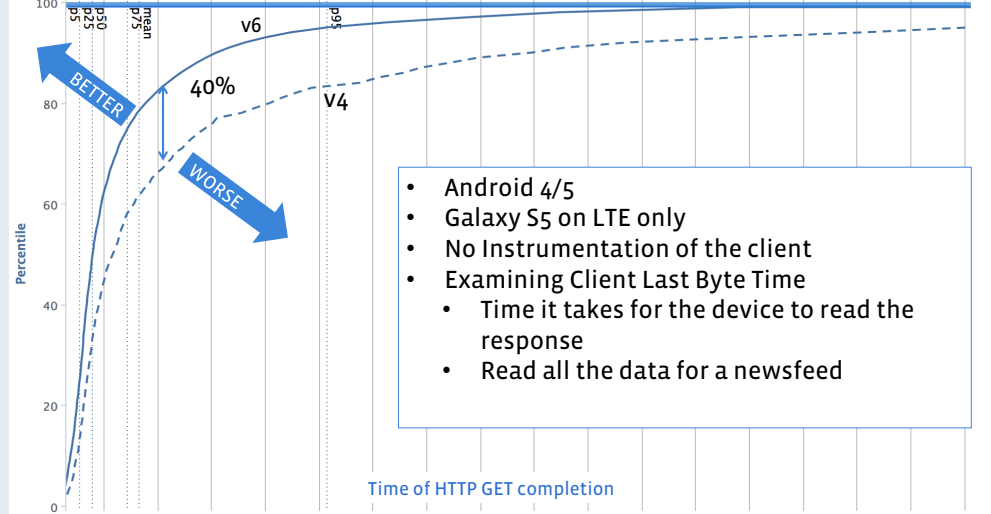
- 6RD
- DS-Lite
- MAP-E or MAP-T
- ...
- No way!
 - Not implemented in smartphones
 - Require using lots of IPv4 addresses
 - Heavy setup and network overhead, require DHCP
 - Take less advantage of “multiplexing” IPv4 addresses & ports, than stateful NAT64

Performance

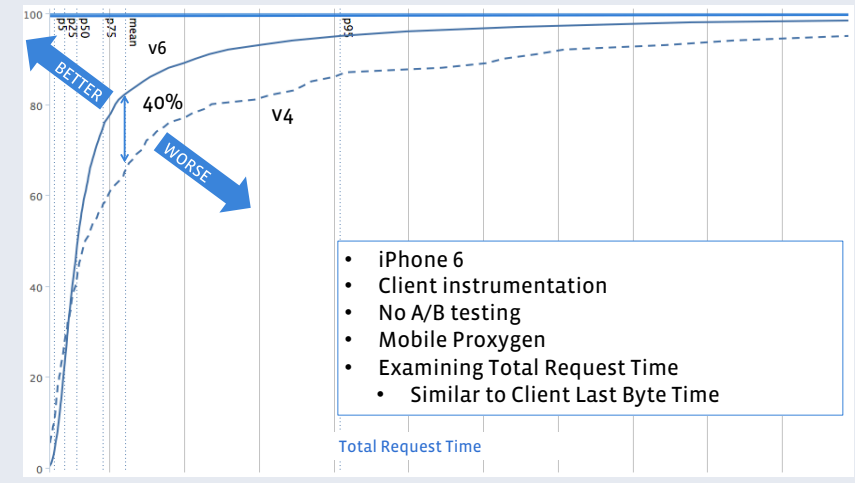
US Mobile Performance – Dual Stack Provider iOS



US Mobile Performance – Dual Stack Provider Android



US Mobile Performance – Dual Stack Provider iOS



***Facebook data**
(17/3/2015)

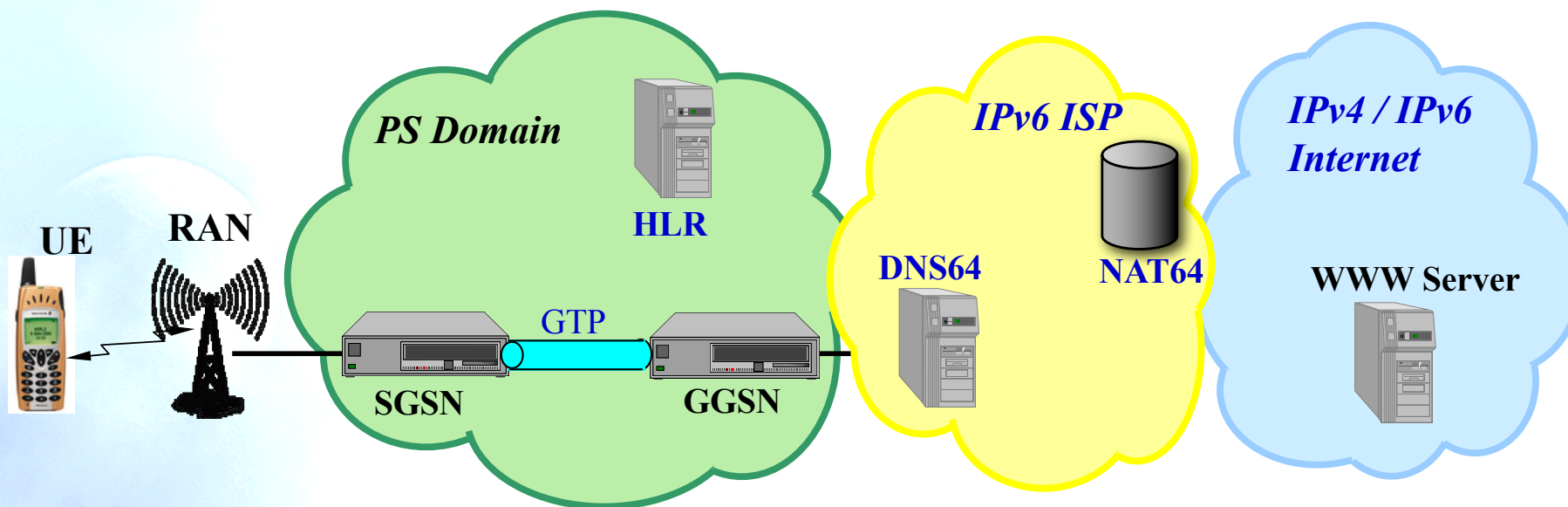
Cost ?

- No CapEx/OpEx
 - No need to buy CGN
 - NAT64 scales better, you have open source solutions, lower cost
 - No need to buy IPv4
- Progressive deployment:
 - New phones
 - Not impacting existing users
 - Naturally increase your IPv6 traffic
 - Decrease IPv4 one
- Billing
 - Trunking IPv6 addresses in CDRs
 - Hash IPv6 addresses in IPv4 records

Roaming

- Use PCRF (Policy and Charging Control Function) to selectively enable IPv6 in roaming customers sessions
 - Depending on “roaming partner”
- RFC7445
 - Analysis of Failure Cases in IPv6 Roaming Scenarios

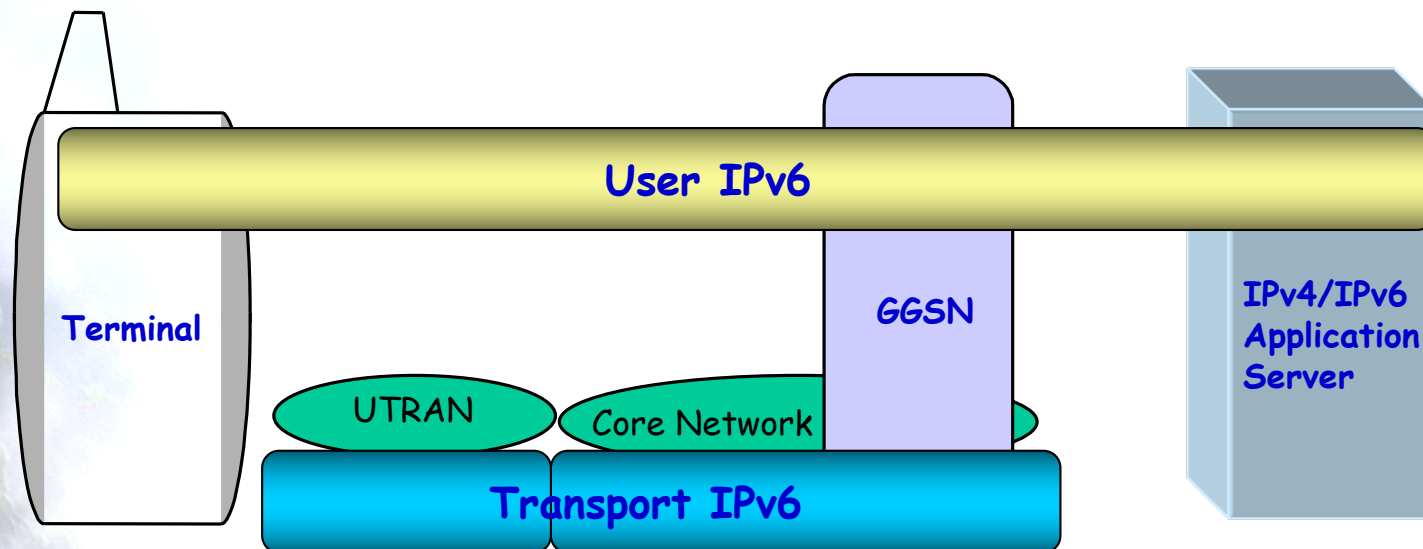
Overall IPv6 3G/4G Architecture



- RFC6459: IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)
- UE: User Equipment
- RAN: Radio Access Network (UTRAN, LTE, ...)
- SGSN/MME: Serving GPRS Support Node/Mobility Management Entity
 - Acts as a “switch”
- GTP: GPRS Tunneling Protocol
- HLR: Home Location Register
- GGSN/EPG: Gateway GPRS Support Node/Evolved Packet Gateway
 - Acts as a “router”

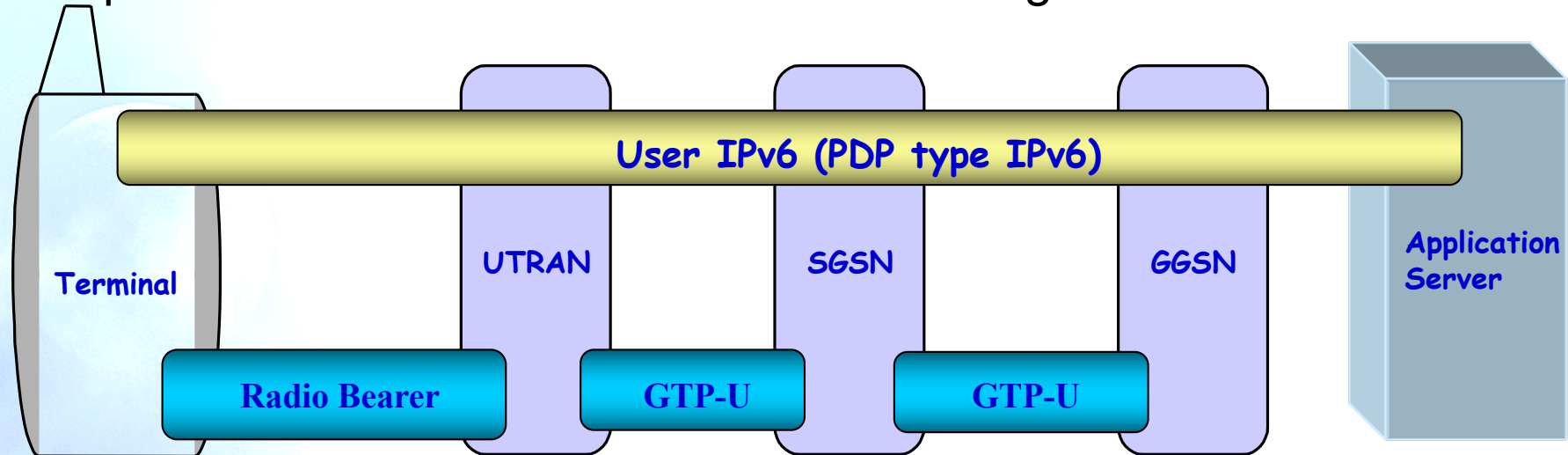
User plane vs. transport plane

- User and transport planes are completely independent:
 - The transport plane can run on a different IP version than the user plane
- RAN and Core Network transport can also run on different IP versions



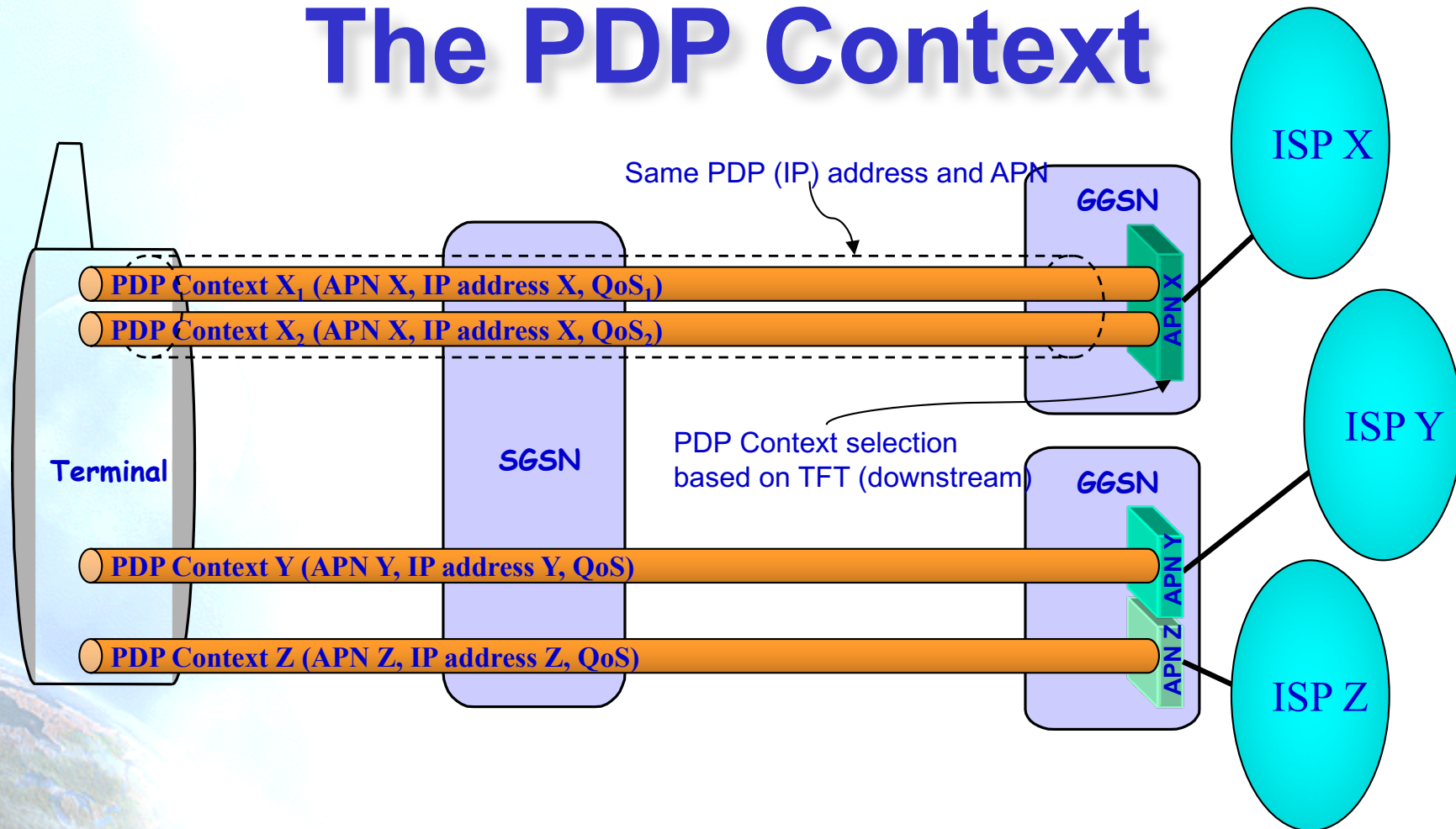
Transport of user IP packets

- IP packets to/from the UE are tunneled through the cellular network.



- When an UE attaches to the Network, the SGSN creates a Mobility Management context containing information pertaining to e.g., mobility and security for the MS.
- At PDP Context Activation (PDP - Packet Data Protocol), the SGSN and GGSN create a PDP context, containing information about the session (e.g. IP address, QoS, routing information , etc.).
- Each Subscriber may activate several PDP Contexts towards the same or different GGSNs.
- When activated towards the same GGSN, they can use the same or different IP addresses.

The PDP Context

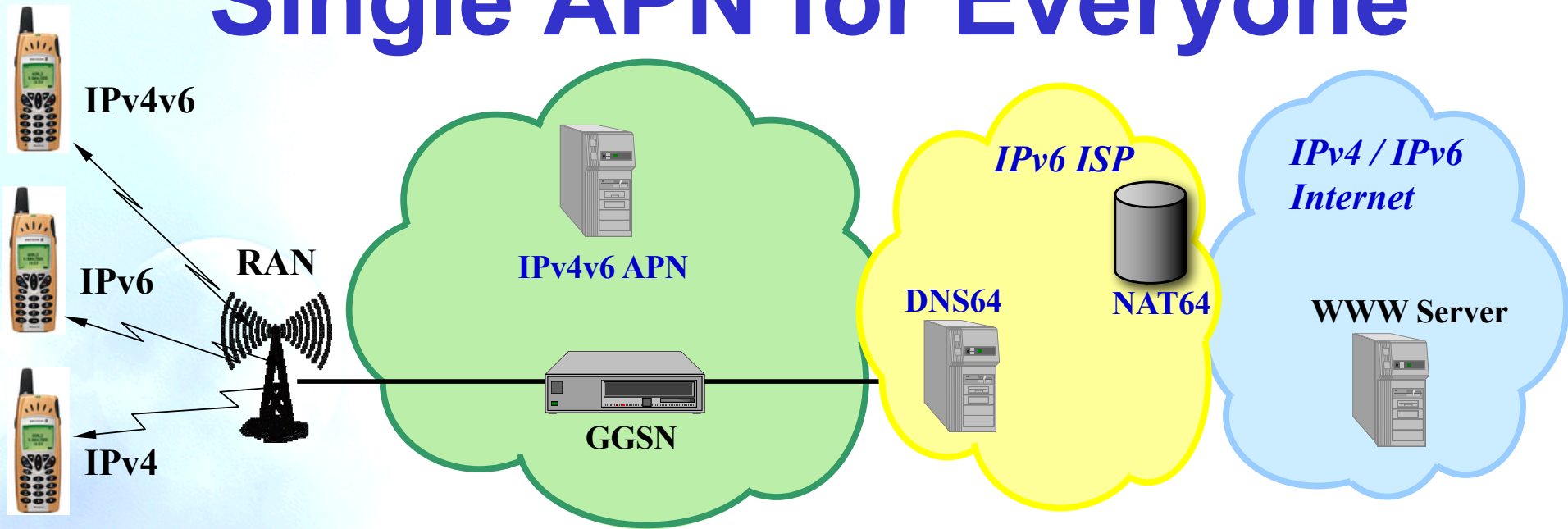


- PDP context can be IPv4-only (IPv4), IPv6-only (IPv6) or dual-stack (IPv4v6)
- Dual-stack could also be provided with two PDP contexts (one each protocol, however it means 2 PDP context licenses)
- 4G/LTE works with IPv6-only PDP context (long-term strategy)

The Access Point Name - APN

- The APN is a logical name referring to a GGSN. The APN also identifies an external network.
- The syntax of the APN corresponds to a fully qualified name.
- At PDP context activation, the SGSN performs a DNS query to find out the GGSN(s) serving the APN requested by the terminal.
- The DNS response contains a list of GGSN addresses from which the SGSN selects one address in a round-robin fashion (for this APN).

Single APN for Everyone

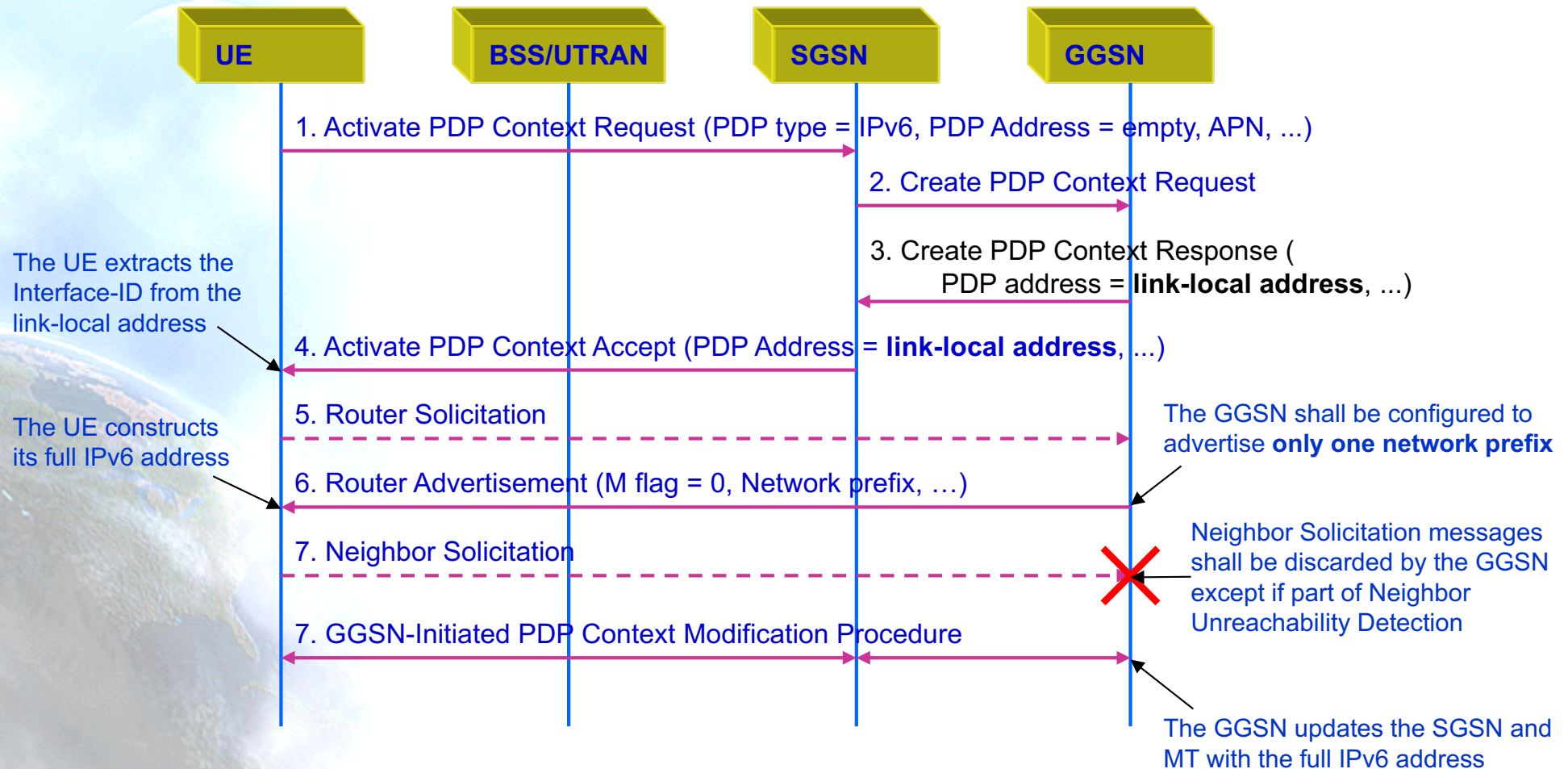


- Single APN
 - Supporting Dual-Stack and Single-Stack
 - Cellular IPv6 deployment is easy because the network supports whatever the UE ask.
 - Progressive deployment, as slow or fast as you want
 - One new phone, all new phones, then OTA old ones
- DNS supporting RFC7050
 - Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis

IPv6 Address Allocation Methods

- Stateless Address Autoconfiguration
 - Default, /64 for each PDP context
 - Introduced in GPRS R'99
- Stateful Address Autoconfiguration
 - DHCPv6 client in the terminal
 - Requires DHCPv6 relay agent in the GGSN
- GPRS-specific Address Configuration
 - Static Address Configuration
 - The UE provides its statically configured IPv6 address at PDP context activation
 - Dynamic Address Allocation
 - The IPv6 address is provided by the GGSN at PDP context activation

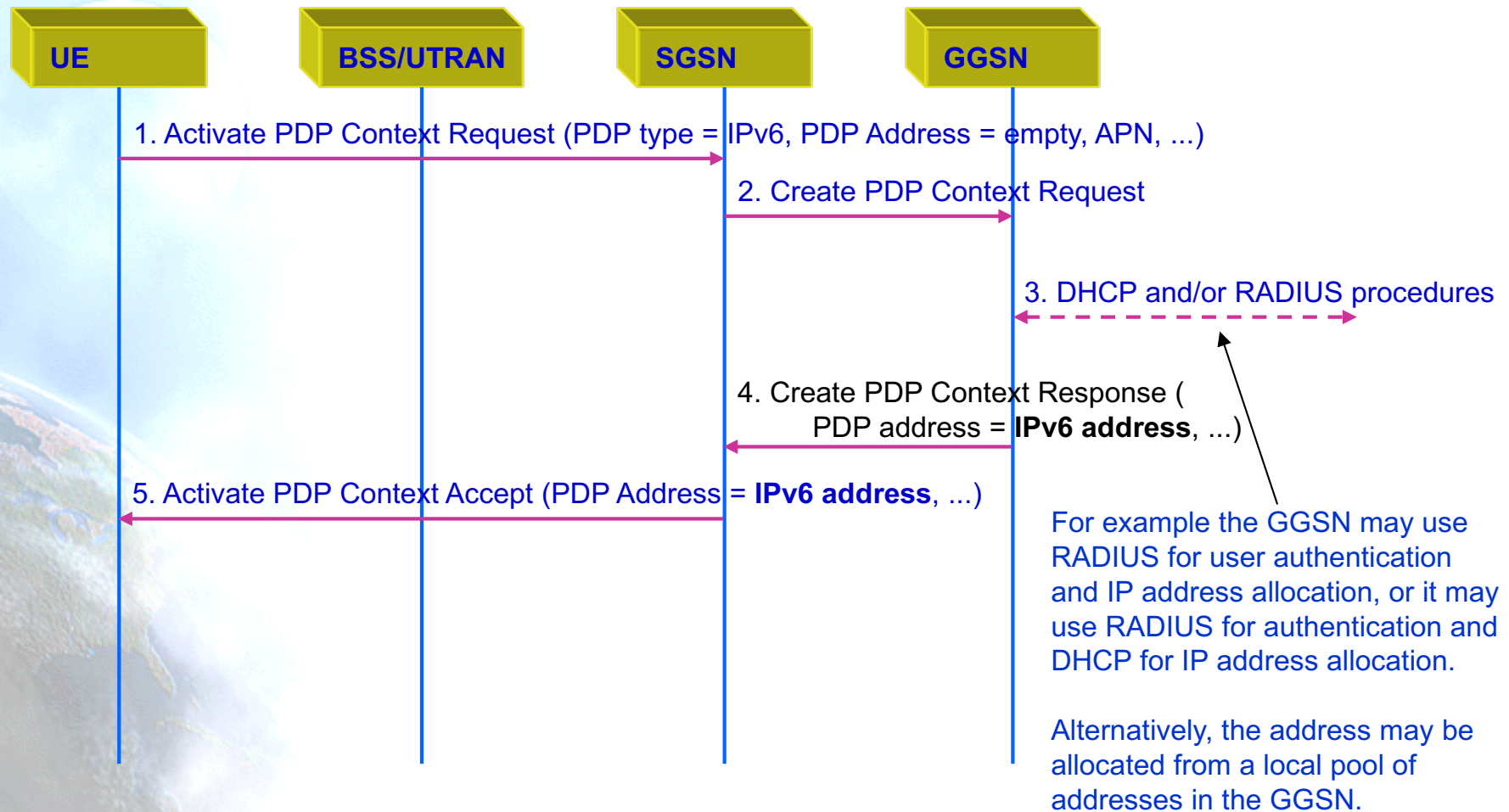
Stateless Address Auto-configuration



Tethering

- RFC7278
 - Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link
 - The UE is switched from an IPv6 host mode to an IPv6 router-and-host mode
- If the UE is also a CLAT, it provides IPv4 service with private addresses to the “tethered” devices

Dynamic Address Allocation



Prefix Exclude Option

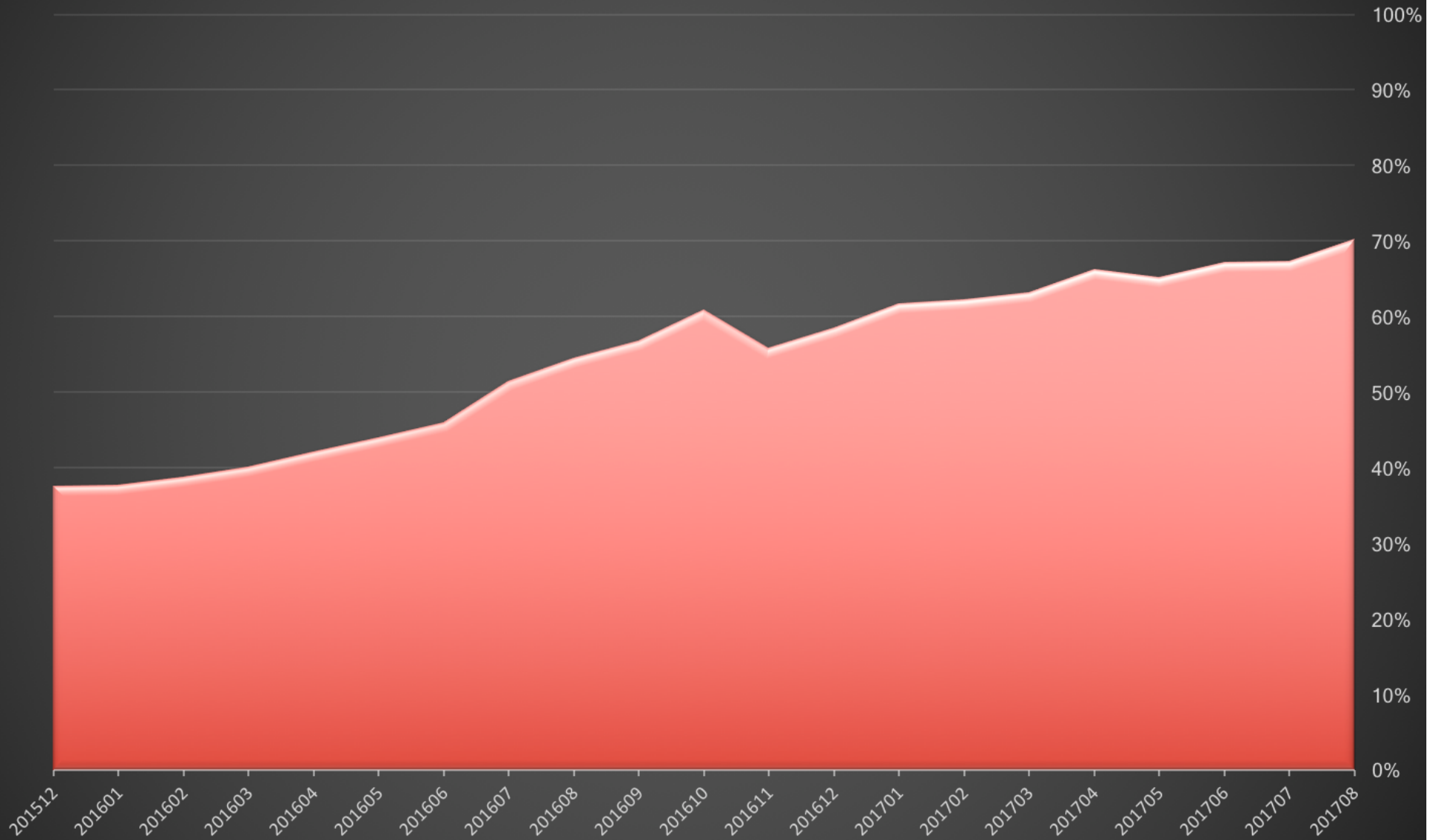
- If DHCPv6 is used, it may be interesting a single aggregated route/prefix for each customer, instead of using one prefix for the link between the delegating router and the requesting router and another prefix for the customer network.
- RFC6603
 - Prefix Exclude Option for DHCPv6-based Prefix Delegation

Declare Success

- Traffic moves from IPv4 to IPv6
- Customers never notice anything changed

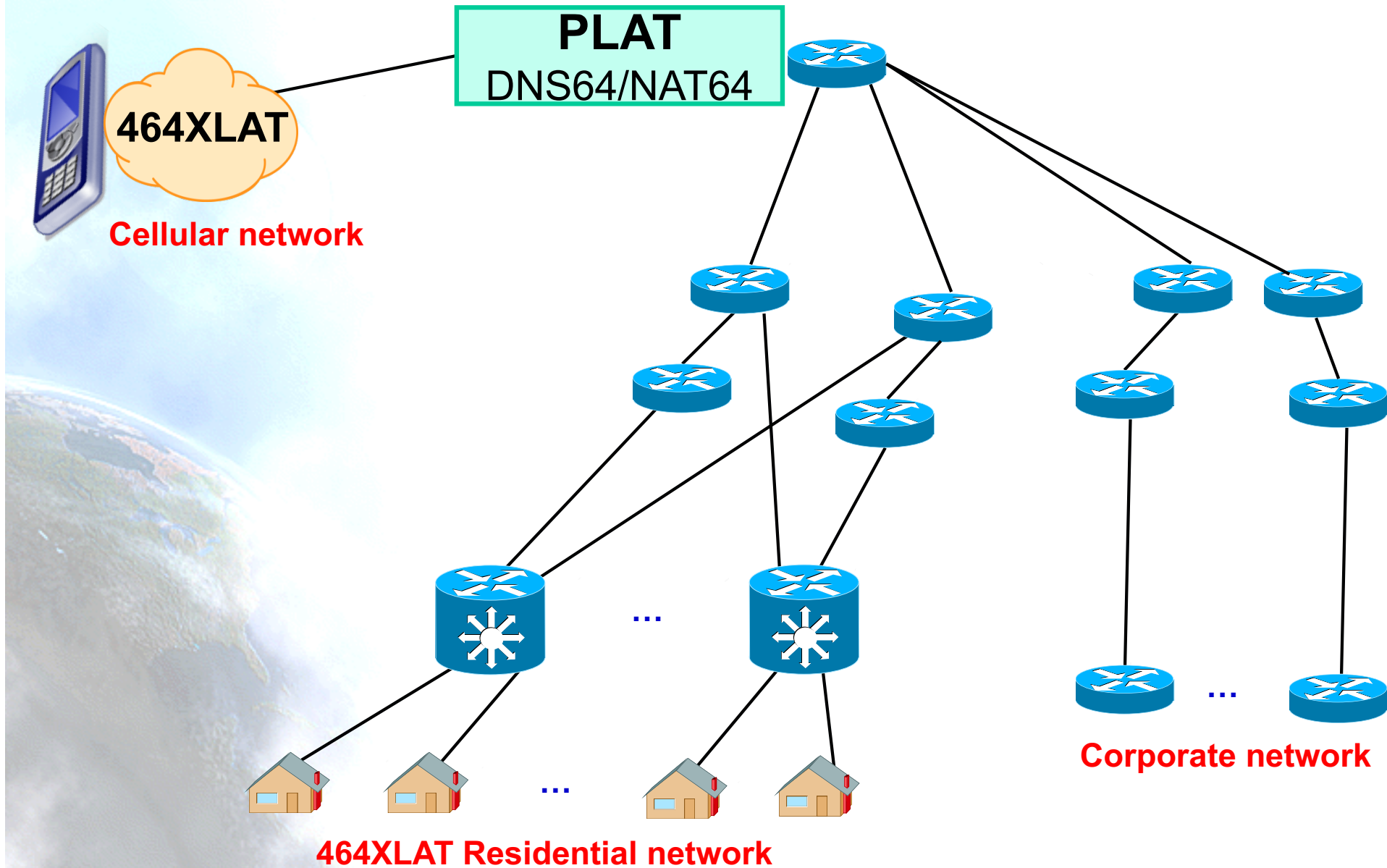
IPv6 in Cellular/US

Major USA Mobile Networks IPv6 Deployment

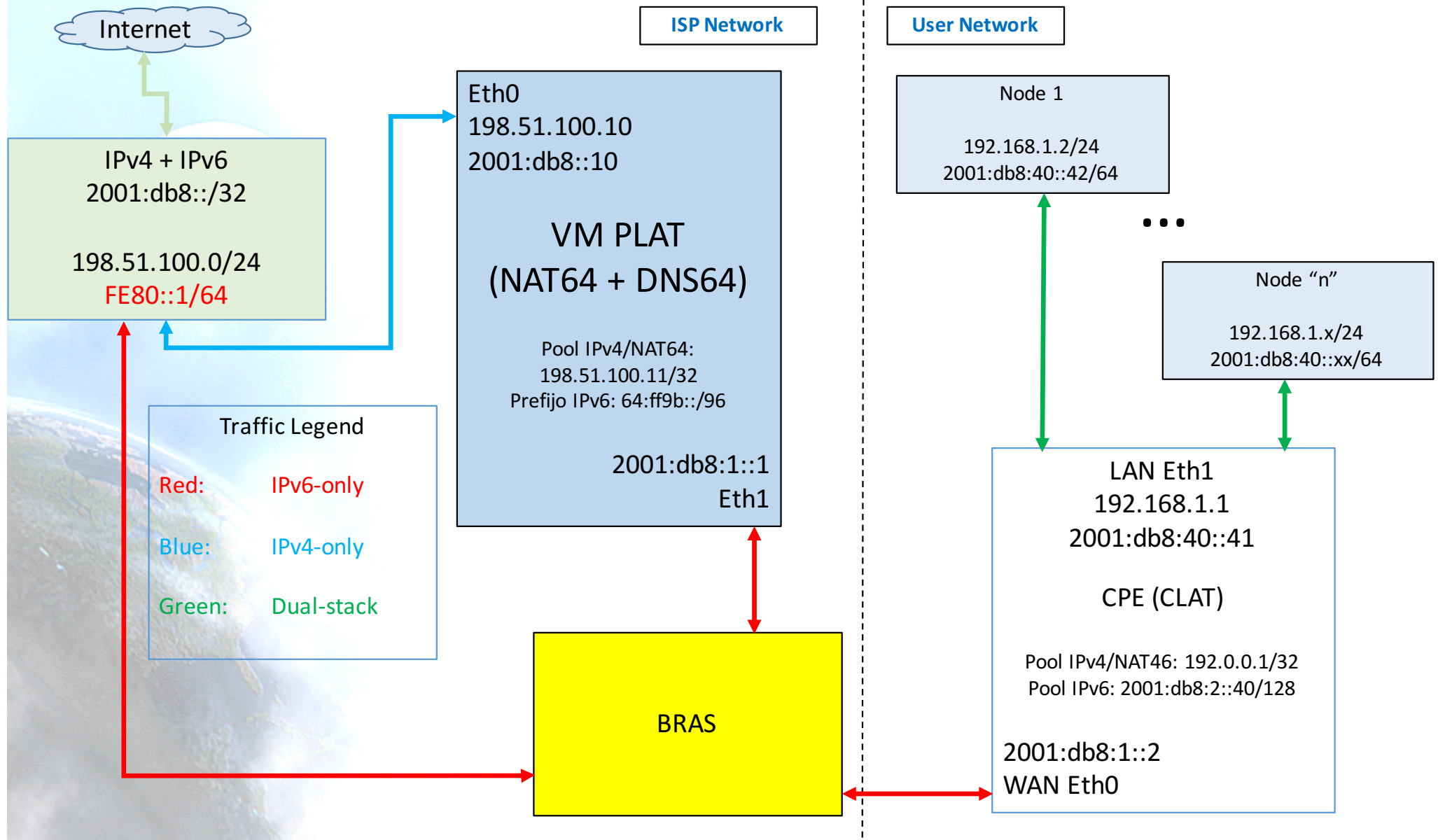


*ISOC/World IPv6 Launch data

Multiservice Network



Example Residential Customer



Thanks!

Contact:

– Jordi Palet:

jordi.palet@theipv6company.com