IPv6 Transition Mechanism and CPE panel

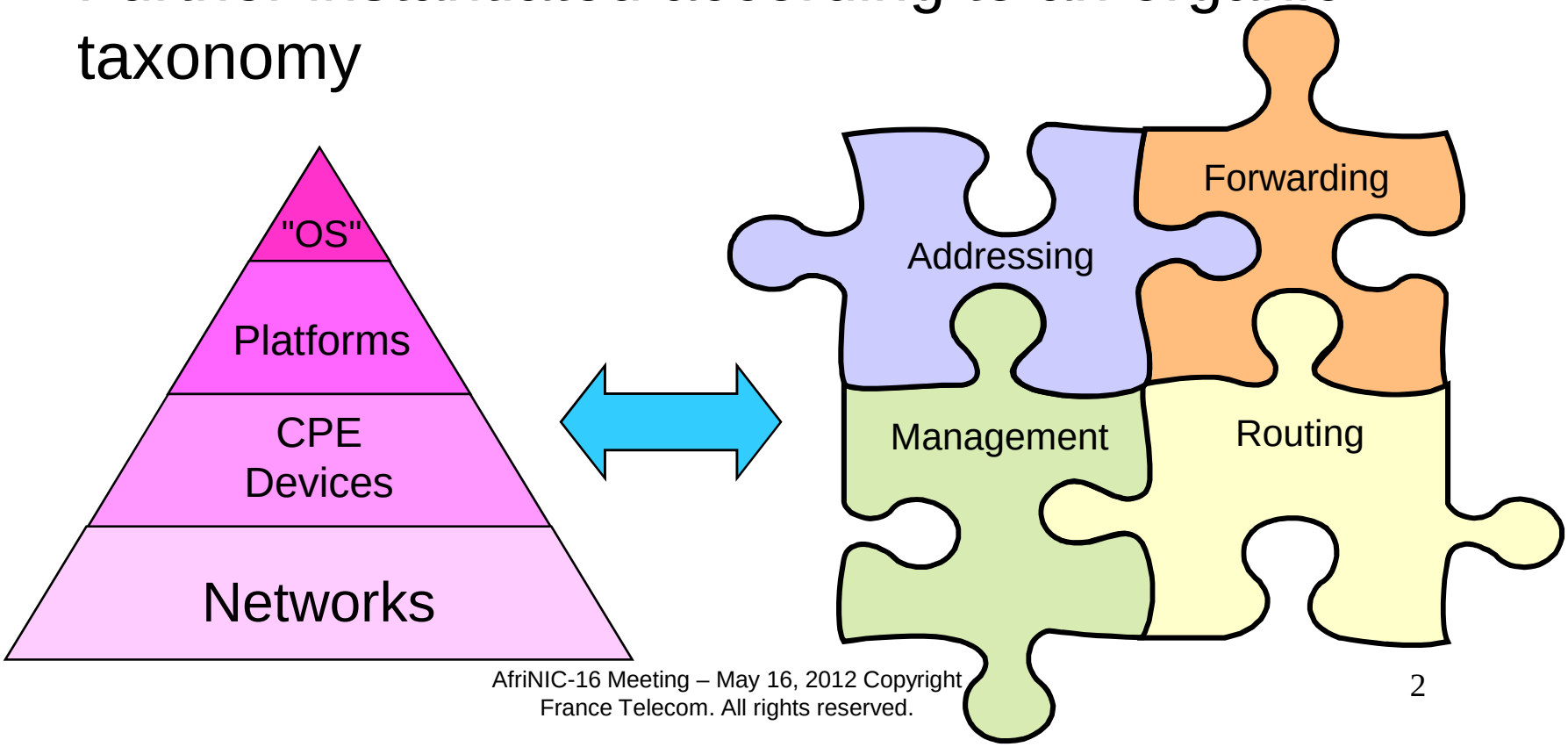
AfriNIC-16, Meeting May 16-Serekunda

M. Sall

modou.sall@orange-sonatel.com

A Function-Derived Organization

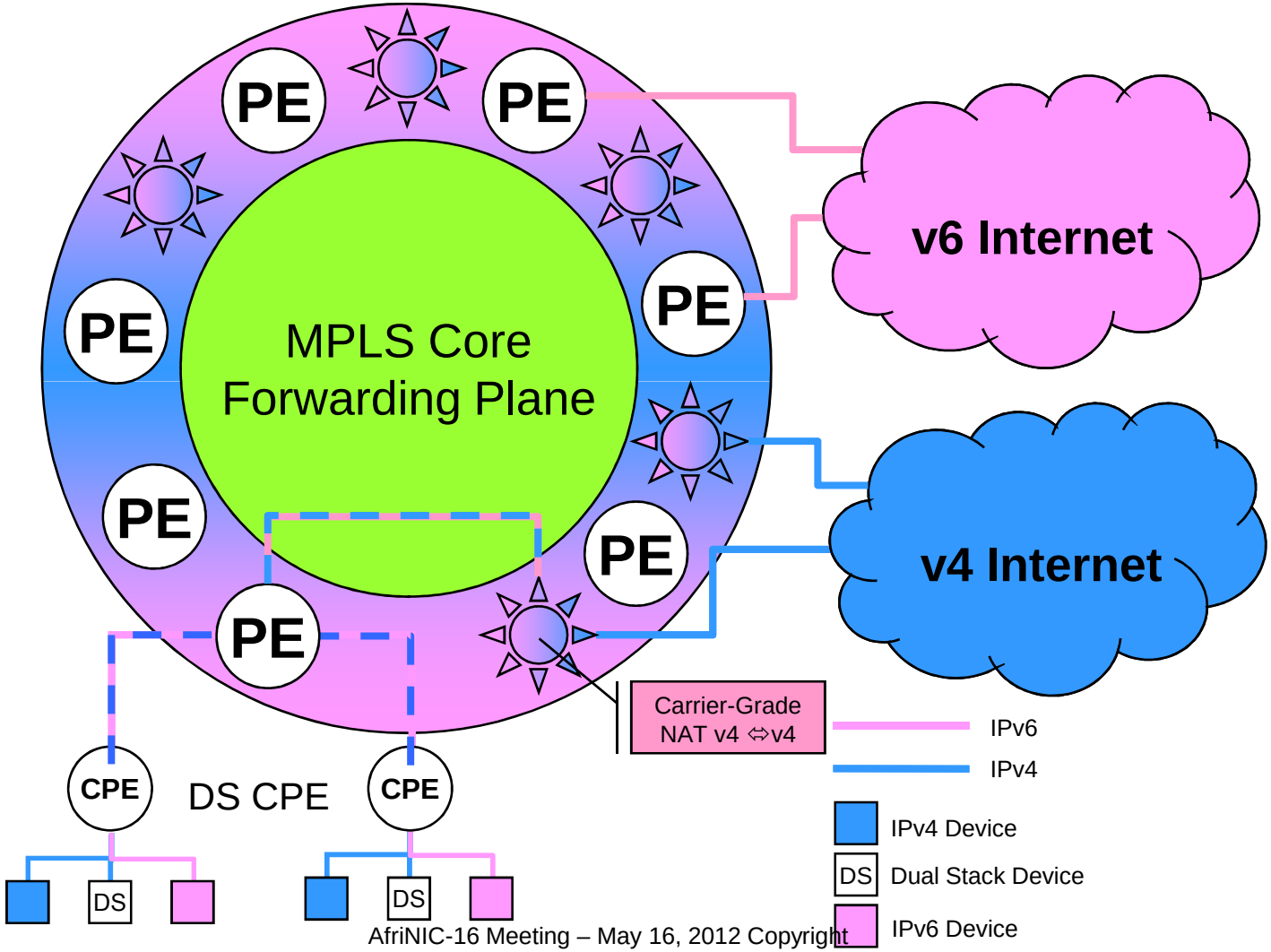
- To make sure the design approach remains network/service-wise, global and systemic
- Further instantiated according to an organic taxonomy



Introducing FT Approach

- Dual Stack architecture
  - CPE and devices of the access layer are DS-enabled
- IPv6 prefixes are dynamically assigned to CPE by means of DHCP
  - Prefix Delegation context where the DR is the DHCP server itself
    - Need to centralize {Prefix; Customer information} bindings
  - Hosts connected to CPE devices dynamically form their addresses by means of SLAAC
    - Privacy is encouraged by adequate extensions (RFC 4941) and walled garden design for some services (IPTV, VoIP)
- Privately-addressed v4 traffic is encapsulated in v6 datagrams by the CPE
  - By means of DS-Lite design where CGN is as close to the CPE as possible
  - CGN reachability information is provided to the CPE by means of DHCPv6

Global Picture



Key Features

- CPE and PE devices are Dual Stack routers
  - According to so-called 6PE design
  - IPv6 traffic is conveyed over MPLS LSP paths computed by the v4 IGP
- MPLS forwarding plane is preserved in the core
  - No need for an IPv6 IGP
  - Reduces OPEX costs
  - Encourages MPLS-based P2MP tree structures for multicast-based services (such as Orange TV)

IPv6 CPE…

Hardware and software used for our MPLS VPNv6 customers

Ethernet access.

- Router Cisco1841 or Cisco 28xx with FE or GigE interface

IOS to use

- The minimum IOS release to run IPv6 service option is: 12.4(15)T8, 12.4(20)T1 12.4(22)T

Please use the last validated release that is later to these minimum releases.
The minimum IOS feature pack to run IPv6 is "ADVANCED IP SERVICES"

Hardware and software used for our ADSL customers

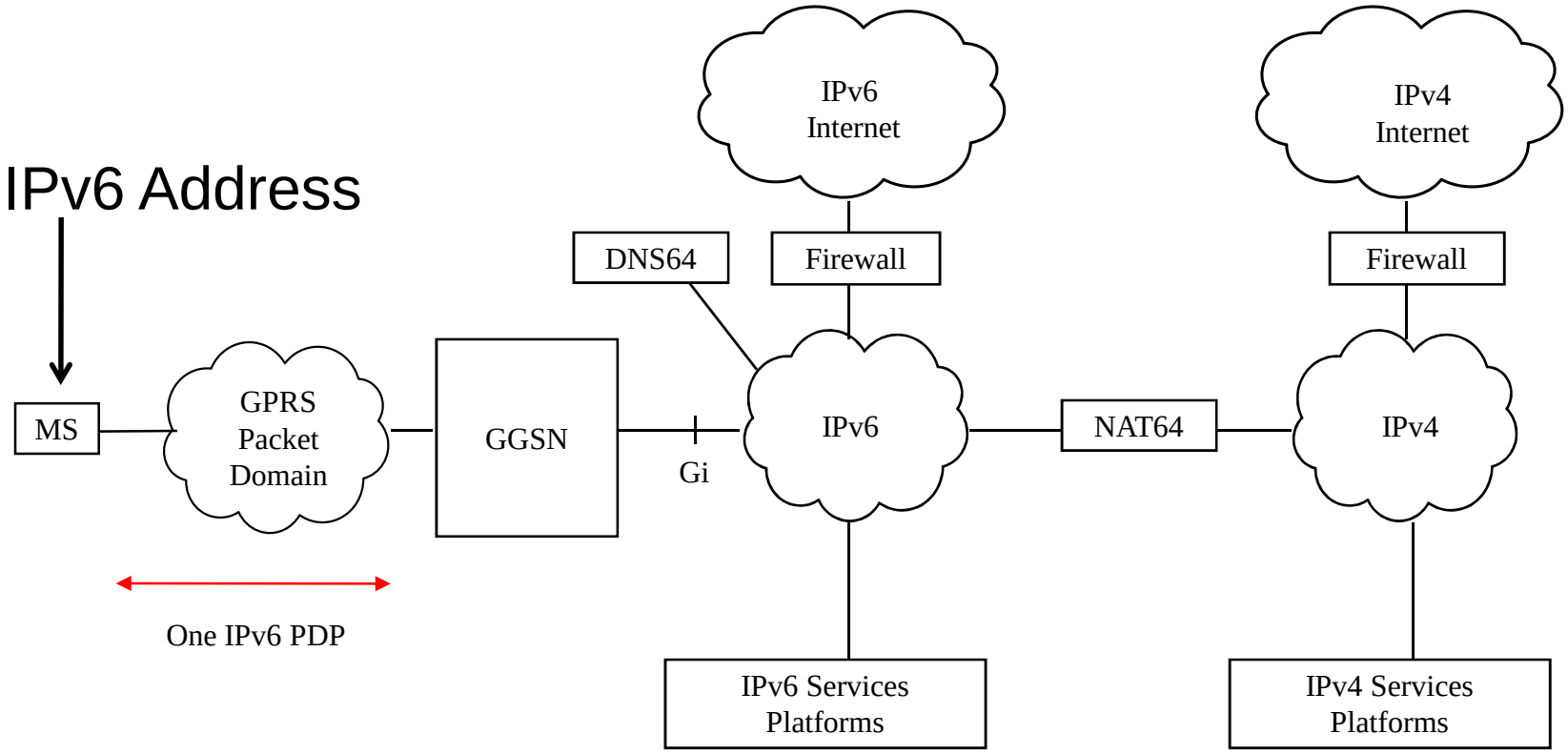
Device	Vendor/Type	Release	CPU Details
CPE	Cisco 877	12.4(15)T IP/FW/PLUS 3DES	64 M DRAM, 12 M Flash

IPv6 CPE..

- Device management (including CPE routers) remains IPv4-based, i.e. devices will be managed by means of SNMP (Simple Network Management Protocol). The introduction of IPv6 capabilities (DHCPv6, 6(V)PE forwarding scheme) assumes the compilation of additional Management Information base (MIB) modules ([RFC-4292], [RFC-4293], in particular).

- Customer management also remains IPv4, but the provisioning of IPv6 connectivity may encourage an update of the Information System from both a service production and customer identification standpoint (e.g. to include the IPv6 prefix that has been allocated to a given customer in the customer-specific information that is maintained by an accounting or a billing system).

Description of target architecture: IPv6-only connectivity + NAT64 + DNS64 solution



IPv6 only connectivity: Advantages and Drawbacks

- **Advantages:**
  - No IPv4 addresses are needed for customer addressing
  - Reduce public IPv4 address usage (address sharing in NAT64 for IPv4-only applications use)
  - Allow services based on incoming flows based on IPv6 always-on connectivity
  - Standardized solution (IETF).
- **Drawbacks:**
  - All applications on UEs must be IPv6 compatible;
  - If application server is IPv4 only, the application should be able to traverse the NAT 64
  - Inherent limitations of NATs with shared public addresses for remaining IPv4 services and applications
- Impact on roaming: Visited network shall support IPv6 connectivity (else IPv4 fallback may be required in case no IPv6 connectivity is supported on visited mobile network => application should still be compatible with IPv4).
- Target solution must be deployed before IPv4 addresses are exhausted

Why IPv6-only + NAT64 design could not be introduced from start ?

- Some softwares are developed exclusively over IPv4 sockets. These softwares cannot run over an IPv6 only connectivity
  - **Only software using an AF independent API or capable of using an IPv6 connection through an IPv6 capable API (in addition to IPv4 one) will work with IPv6 only connectivity. In case applications (on server side) are IPv4-only, some NAT64 (+DNS 64) is recommended**
  - On-going evaluation of NAT64 application support is performed in lab test using a PC and DNS64/NAT64 server.

- Migration strategy towards NAT64
  - NAT64 can be deployed for selected APNs (distinct APN from DS solution is required)
  - NAT64 could apply for new or also for legacy customers (assuming APN can be changed)
  - Migration strategy has to be elaborated separately for Mass Market and for Business Market

Introducing IPv6 in dual-stack mode is necessary

- DS mode will be necessary because IPv6 compliant applications embedded within the devices will not be largely available when migration towards IPv6 will begin.
- To allow services based on incoming flows, at least thanks to IPv6 connectivity
- To start introducing IPv6, to train people on IPv6, to learn and prepare services migration to be IPv6 compatible
- To set up some progressive introduction of IPv6 in mobile networks and evaluate side effects
- To maintain QoE for customers before IPv6 connectivity is provided
- To experiment NAT64 + DNS64 (+ proxies) before large scale deployment
- To validate IPv6-only support in IS

Dual Stack mode and PDP contexts

- **Two possibilities:**

– two PDP contexts (IPv4 and IPv6)
– one PDP context (IPv4v6, from Release 9 in 3G networks)

- **PDP IPv4v6 advantages :**

– GGSN : licences per max number of simultaneous PDP (at this time)
– GGSN : limited numbers of PDP per server (performance)
– load balancing issues with 2 PDP (the two PDP may not be anchored at the same GGSN nor Data Content Billing systems aka CSG)
– billing : easier to manage only one PDP (CSG)

- => The Orange choice is IPv4v6 PDP context

Impact of IPv6 scenario on APN configuration

- Applications should generally be independent of APN choice (apart from specific cases, such as MMS). IPv6 should be introduced on general APN first.
- APNs must be configured to be dual stack in the terminal. The choice of connectivity type must kept under network control.
- a legacy APN can be used also for the Dual Stack solution.
- a specific APN is needed for the IPv6 only connectivity case
- APN redirection/modification may be needed in roaming cases:
  - solutions are under investigation
- a migration strategy must be defined:
  - when to introduce new IPv6 only APN?
  - IPv6 can be only configured for new compatible devices => impact to be analyzed

Thank you