France Telecom's IPv6 Strategy

Christian JACQUENET

christian.jacquenet@orange-ftgroup.com

Outline

- Rationale
- FT Group-wise IPv6 program
  - Objectives
  - Phased approach
- Design principles
- Current status
  - Program-derived, affiliate-specific projects and pilot deployments
- Lessons learnt
- Next steps

Rationale

- Make sure France Telecom's ready to face the depletion
- Make sure depletion does not negatively affect business growth nor customers' QoE
  - Regardless of IPv4 address availability
- Therefore:
  - Networks must convey both IPv4 and IPv6 traffic
  - Networks and services must cope with address translation design and operation during transition

Program's Objectives

- *Federate* IPv6 initiatives
  - For the sake of consistency and sync, covering both residential and corporate markets
- *Specify* and consolidate a set of design and operational guidelines documents
  - To serve as the cornerstone of the IPv6 strategy
  - To be further derived into DNF-specific engineering rules and operating procedures
- *Validate* by driving and monitoring IPv6 field trials, meant to:
  - Validate design principles
  - Assess (service-driven) performance and scalability aspects
- *Communicate* on IPv6 program-driven activities
  - Both internally (*e.g.* newsletter, "IPv6 days", *etc*.) and externally (contribution to the standardization effort, PR, *etc*.)

A Phased Approach

- Phase 1 (2008-2009): IPv6 Introduction
  - Publish a reference architectural framework
  - Conduct a scope-restricted pilot deployment
    - Validate design guidelines with basic Internet service
    - Assumes Group's affiliate involvement from Day 1
- Phase 2 (2009-2010): IPv6 Migration
  - Refine reference architectural framework with further (VoIP, IPTV-inferred) design recommendations
    - Including IPv6-inferred Multicast, VPN, SIP capabilities
  - Conduct service-wise experiment accordingly
- Phase 3 (2010-): IPv6 Production
  - Publish consolidated IPv6 service production procedures
  - Towards IPv6-only backbone and customer environmental infrastructures, gracefully coping with IPv4 address depletion

Introducing FT Design

- Dual Stack architecture
  - CPE and devices of the access layer are DS-enabled
- IPv6 prefixes are dynamically assigned to CPE/UE by means of DHCPv6
  - Prefix Delegation context where the DR is the DHCPv6 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)
  - CPE IPv6 reachability information is acquired by first hop router by means of DHCPv6 RAAN (Relay Agent Assignment Notification) option

A Necessary Evil

- Make sure IPv4-to-IPv4 communications can still be established during transition period is a MUST
- But global IPv4 addresses become scarce resource
  - Hence the need to share them between several customers
- Inevitably yielding the deployment of NAT capabilities in the network
  - Because of current SoA

Two CGN Flavors

- "Double NAT" approach
  - Addresses are translated at the CPE level then at the CGN level
  - Assumes forwarding scheme is based on non-routable addresses within a domain
  - Overlapping private addressing schemes and subsequent operational complexity are likely to become the rule, not the exception
- "DS-Lite" approach
  - Privately-addressed IPv4 traffic is encapsulated in IPv6 datagrams (by the CPE or the UE)
  - CGN IPv6 reachability information can be provided to the CPE/UE by means of DHCPv6

The Choice of DS-Lite

- A **catalyst** of IPv6 deployment
  - CPE and UE devices need to be provided with IPv6 connectivity and IPv4-in-IPv6 encapsulation capabilities
  - Unlike “double NAT” and 6to4(-like) solutions which still mandate (global) IPv4 addresses
- Maintains only one level of NAT
  - CPE-embedded NAT capabilities are de-activated and “outsourced” in the network
- Technology is commercially available
  - While standardization is straightforward and underway
- DS-Lite extensions also facilitate IPv4-to-IPv6 stateless communication as well as graceful migration towards A+P
  - See http://tools.ietf.org/html/draft-boucadair-dslite-interco-v4v6-01 and http://tools.ietf.org/html/draft-boucadair-behave-ipv6-portrange-02, respectively

Connecting

- DS CPE embeds DHCPv6 client
  - DHCPv6 **server** uses IA_PD identity association to assign /56 global prefixes (in RIPE-dependent countries)
    - Because of the need for centralizing customer/prefix bindings
  - DS and IPv6 hosts automatically form their own IPv6 address by means of SLAAC
- DS CPE still embeds a DHCPv4 server
  - To provide IPv4 private addresses to DS and IPv4 hosts

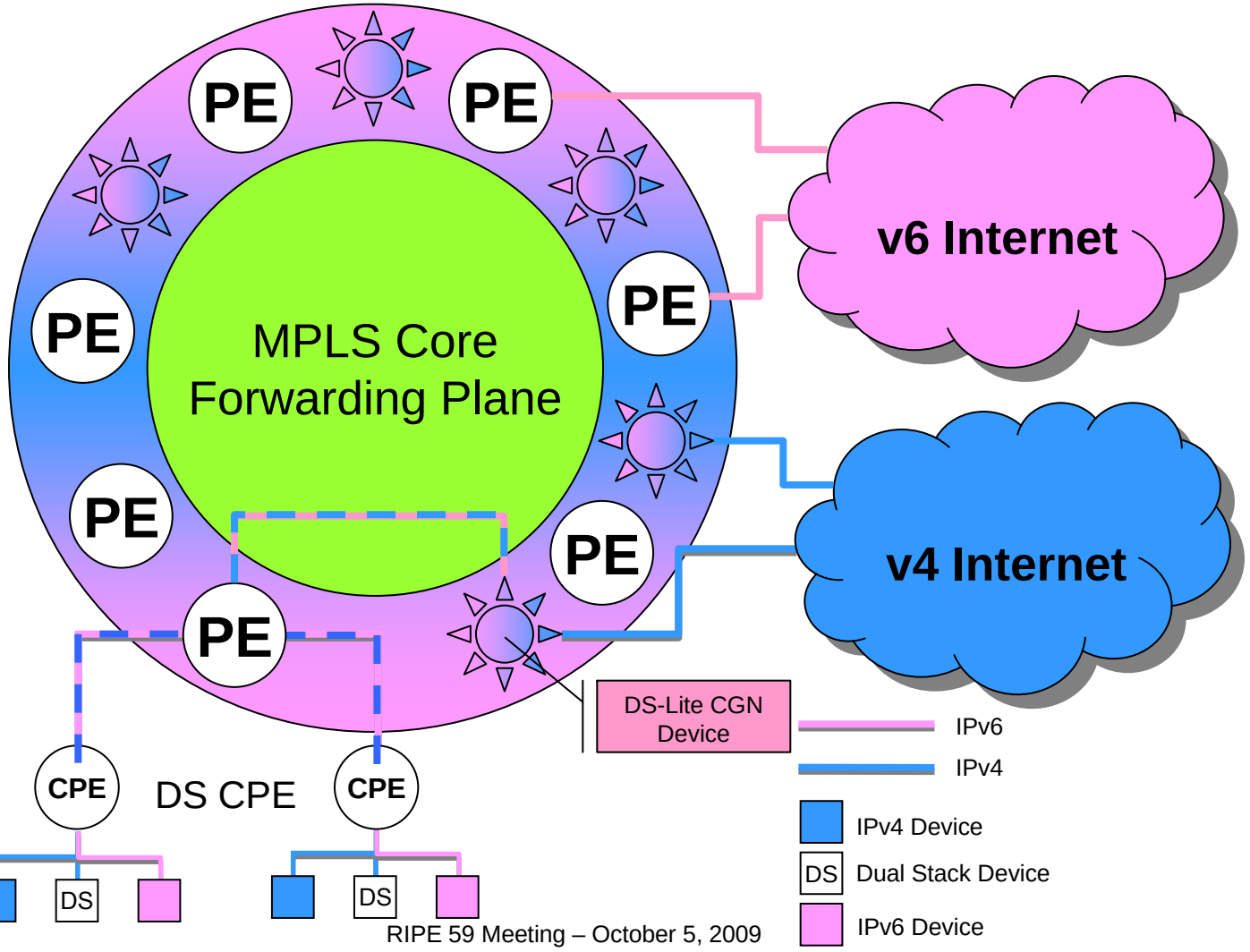
Forwarding

- CPE is a DS router
  - Default route is acquired by means of RS/RA exchange between CPE and first hop DS router
- IPv6 traffic is natively forwarded
  - Based upon 6PE design
    - No need for an IPv6 IGP
    - Reduces OPEX costs
    - Encourages QoS-guaranteed MPLS-based P2MP tree structures for multicast-based services such as live TV broadcasting
- Privately-addressed IPv4 traffic is:
  - Forwarded to and translated by DS-Lite CGN devices
  - Encapsulated in IPv6 datagrams *a la* RFC 2473

Operating

- Device management remains v4-based by default
  - Because of DS routers and preserved IPv4 core
  - But DS-Lite design assumes CPE is IPv6-managed
- Customer management relies upon DHCPv6 information
  - Including use of Options #18 and #37 (equivalent of sub-options #1 “Circuit-ID” and #2 “Remote-ID” of RFC 3046, respectively)

Global Networking Picture

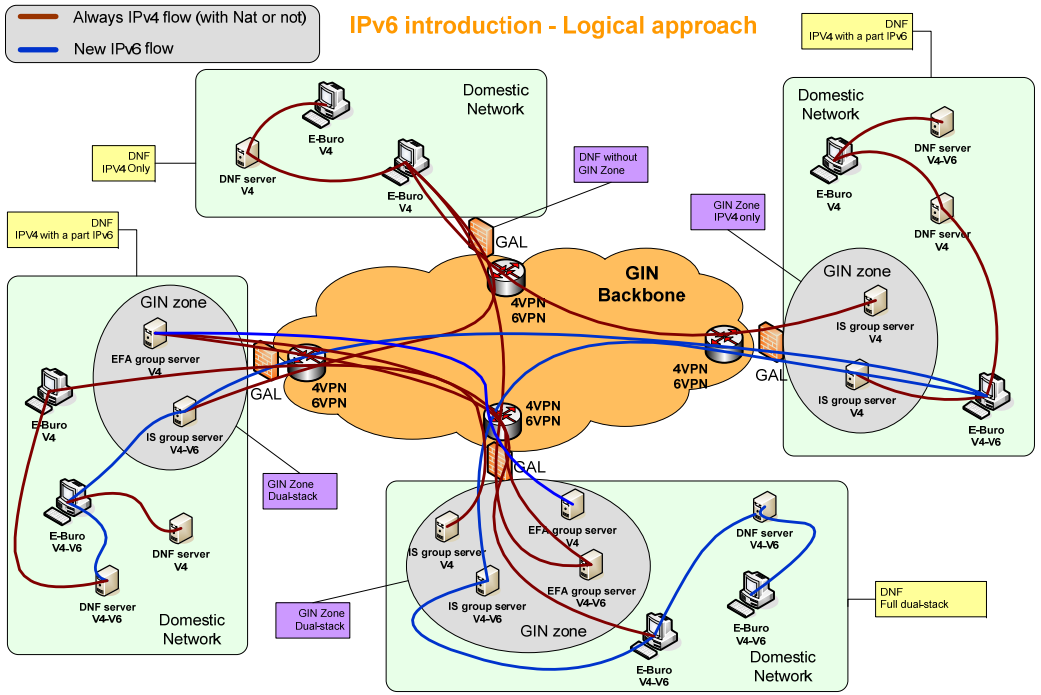


Pilot Deployments are Underway

- Program-derived affiliate-specific projects
  - Meant to enforce group's strategy according to environmental and technological contexts
  - Primarily focused on residential (fixed) market
  - But 6VPE-based IPv6 VPN service offering has been launched in May for corporate customers
    - See http://www.orange-business.com/mnc/press/press_releases/2009/IPv6.html
- France, Poland, Senegal and Switzerland projects have kicked off
  - First (Internet service-restricted) phase starts on Q4 2009/H1 2010 with several hundreds of (internal) customers
  - Generalization to follow as per program's milestones

FT Group's Internal Network

- Any FT group employee must access affiliate's corporate intranet wherever he/she's connected to the GIN network
  - Based upon Microsoft's Active Directory
- But AD does not work in NAT environments
  - Hence the use of IPv6
- First phase involves France, Poland, UK and Romania affiliates
  - Core network will be IPv6 ready by November
- Global IPv6 deployment to be completed by the end of 2010



(Some) Lessons Learnt…

- Information systems (OSS/BSS) should be upgraded first
- Some vendors are not IPv6-minded yet
  - This sometimes mandates in-house workarounds (*e.g.* outsourcing of DHCPv6 Relay-Agent capabilities) that may delay generalized deployment
  - Encourages service providers' community to unite and consolidate (functional) requirements in light of possible design options
    - Standardization can surely help

…And Still Learning

- Early pilot deployments are meant to assess functional design in-the-field
  - Hundreds of customers are not sufficient to discuss performance and scalability
- Access to the IPv4 Internet will change
  - DS-Lite CGN introduction encourages customer education
- IPv6 introduction is isotropous
  - Keeping a global, systemic view of the problem is key
    - But who can claim everything's under control ☺?

Next Steps

- Specification
  - Specification of IPv6 flavors of the whole range of service offerings to be completed by December
- Standardization
  - Promote the adoption of IETF-, 3GPP-, and BBF-targeted contributions by the end of 2009 (CGN-, A+P-, sensor- and DHCPv6-related matters)
- Support
  - Generalize IPv6 training (Q4 2009/Q1 2010)
  - Drive forthcoming pilot deployments