Transition to IPv6 in Service Providers

Jean-Marc Uzé
Director Product & Technology, EMEA
juze@juniper.net

UKNOF14 Workshop
Imperial college, London, Sept 11th, 2009

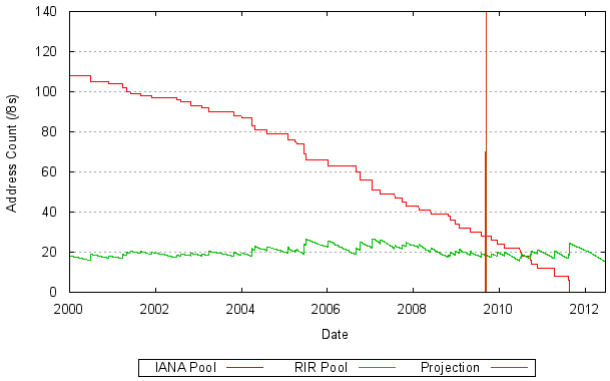
Agenda

- **Planning Transition**
- **Transition trends in Service Providers**
  - **In the core**
  - **In the access**

The End of the Road Comes into View

Only 11% of IPv4 space remains available in IANA pool

Depletion projected mid-2011

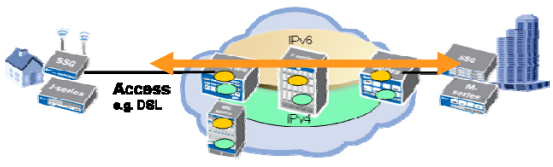


Projected RIR and IANA Consumption (nb /8s)

http://www.potaroo.net/tools/ipv4/index.html

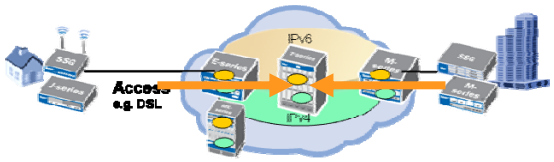
Methodologies: Core to Edge

- **IPv6 implemented in core network first**
  - **Incrementally migrated outward toward edge**
- **Application and advantages:**
  - **Core devices usually the easiest/safest to add IPv6 to**
  - **Gains time for addressing more difficult issues**
    - **Security**
    - **Management**
  - **Gives time for operations to gain experience before IPv6 reaches users at the edge**
  - **Best approach for "holistic" IPv6 deployment**



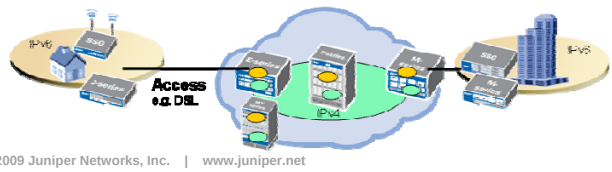
Methodologies: Edge to Core

- IPv6 implemented at edge first
  - Might or might not be incrementally migrated inwards to core
- Application and advantages:
  - Best approach when IPv6 must be quickly deployed to users
  - Best approach when a network must demonstrate early IPv6 capability
  - Best approach when older devices in core cannot support IPv6
  - Allows a plan to spare IPv4 addresses



Methodologies: IPv6 “Islands”

- IPv6 distributed over areas of devices in network
  - Appearance of IPv6 less topologically deterministic
  - IPv6 added where it is needed most, then expanded
  - In later phases, IPv4 islands in an IPv6 network
  - Manual or automatic tunnelling
- Application and advantages:
  - Best when IPv6 must be focused
  - Useful when IPv6 is needed for limited applications, devices, or areas



Implementation mechanisms
A (maybe too?) rich IPv6 Transition Toolkit…

- Dual stacks
  - Co-existence, no intersection
- Manually configured or signalled tunnels
  - GRE, IPSec
  - MPLS L2VPN, VPLS, L3VPN, P2MP LSPs
  - Manual tunnels are ideal for interconnecting IPv6 sites or edges over an IPv4 network
- Automatic tunnels
  - Tunnel brokers, Teredo, 6to4, ISATAP
- Translators
  - NAT-PT: same as IPv4 but with IPv6 pool
  - But now deprecated by IETF to historical status…

=> other under development (IVI, softwires, Dual-Stack Lite, Carrier Grade NAT…)

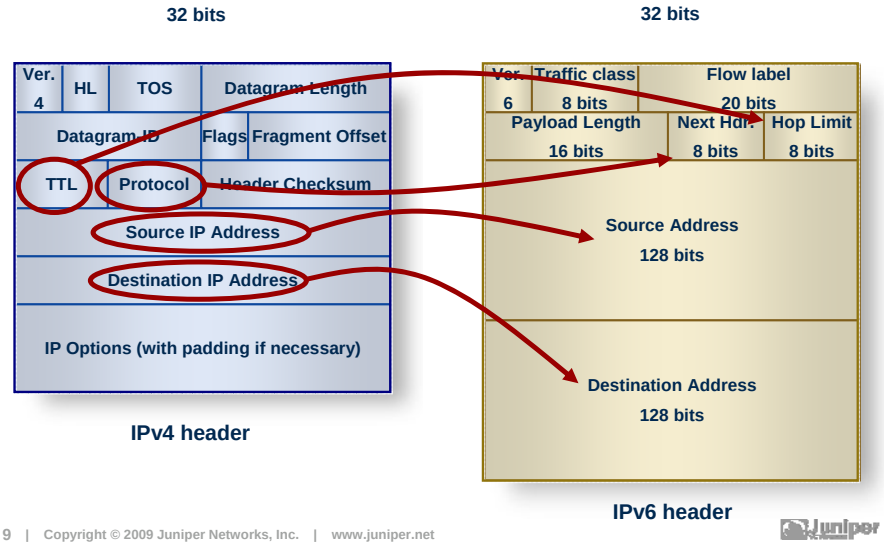
Elements of a Practical IPv6 Deployment Plan

- IPv6 has specific implementation mechanisms
- Relative lack of extensive experience
- New technologies increase project risk
- Careful planning can bring those risks back to an acceptable level

IPv6 Plan

- ✓ Design
- ✓ Inventory
- ✓ Methodology
- ✓ Milestones
- ✓ Vendor Evaluation and Selection
- ✓ Design and Interoperability Testing
- ✓ Training
- ✓ Cost and Risk Analysis
- ✓ Project Executables

A Comparison of IPv4 and IPv6 Headers



Factors to Consider

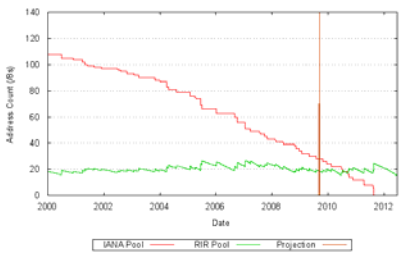
- IPv4 and IPv6 are not interoperable
  - Means must be established for interconnecting
  - Means must be established for coexistence
- Incremental deployment requires interim mechanisms
  - Multiple mechanisms might be required
  - Choices driven by methodology
- A well-equipped toolbox is essential
- Planning is all about controlling cost and risk
  - Balance timelines against projected demands
  - Apply principle of least surprises
  - Do not forget Training

Agenda

- Planning Transition
- **Transition trends in Service Providers**
  - **In the core**
  - **In the access**

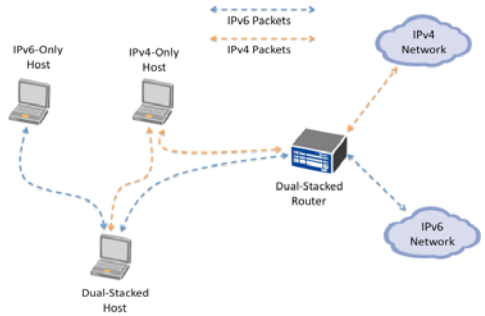
The End of the Road Comes into View

- **Smooth transition plan is not sufficient**
  - **Dual stack approach**
  - **From IPv6 islands to IPv4 islands**
- **Window time has changed: from a decade to 2-3 years**
- **Moving to a forced scenario where NAT is unavoidable**
  - **IPv4 will remain for a long time**
  - **“NAT at the edge”, “NAT in the middle”, Carrier-Grade NAT (CGN), Large Scale NAT (LSN), …**



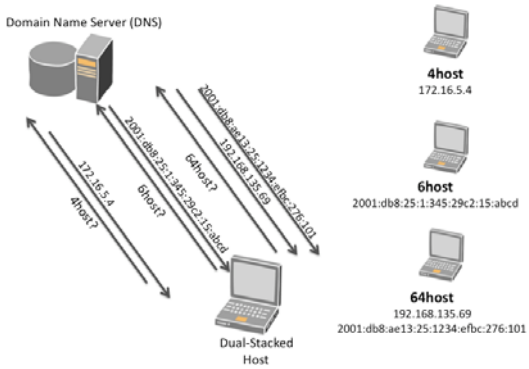
Dual Stacks

- Device supports IPv4 and IPv6 on the same interface
- All routers are configured with IPv6 on the interfaces and IPv6 routing protocols)
- Preferred method for deploying intra-site, full network, or core to edge



Dual Stacks

- Device is “bilingual”
  - If DNS returns IPv4 address, device speaks IPv4
  - If DNS returns IPv6 address, device speaks IPv6



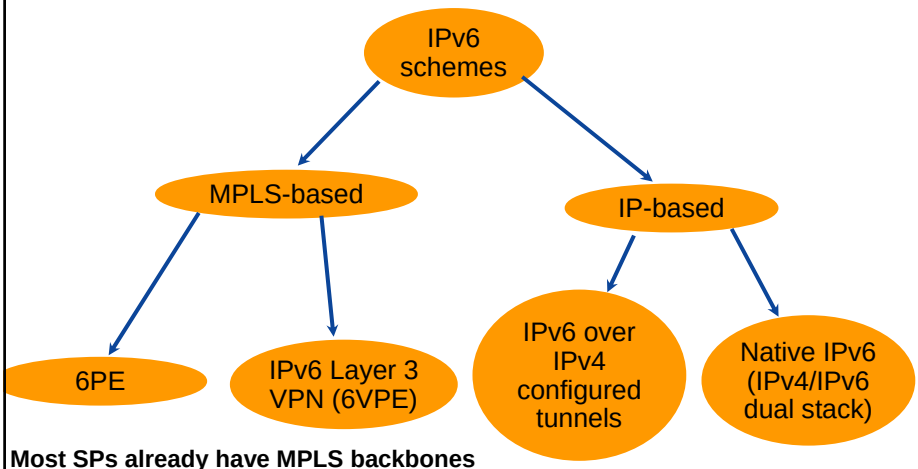
Dual Stacks

- **Pros:**
  - **Implementation driven by DNS**
  - **Simplest of the implementation mechanisms**
- **Cons:**
  - **Requires both IPv4 and IPv6 addresses on all interfaces**
  - **Potential for conflicts when DNS returns *both* and IPv4 and IPv6 address**

Agenda

- **Planning Transition**
- **Transition trends in Service Providers**
  - **In the core**
  - **In the access**

IPv6 core transport schemes



Most SPs already have MPLS backbones

Schemes for IPv6 over MPLS

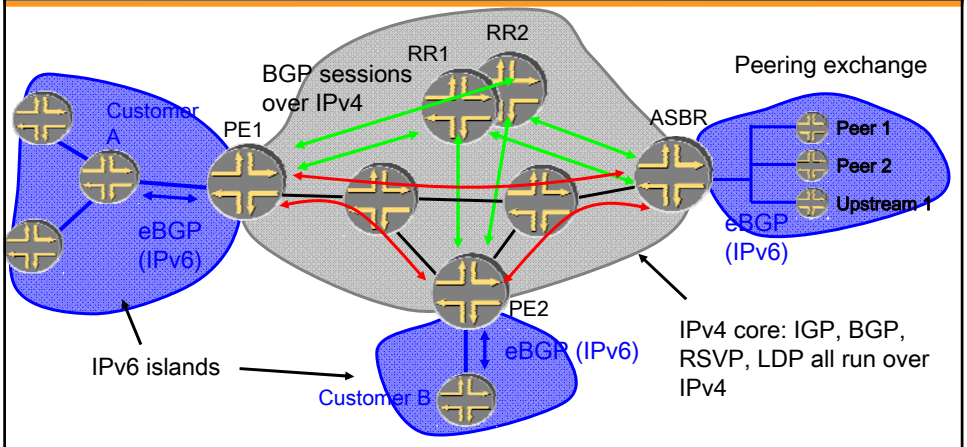
Two main schemes exist:

- **IPv6 islands over MPLS IPv4 core (sometimes known as "6PE")**
  - **RFC 4798, "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)"**
- **IPv6 VPN (sometimes known as "6VPE")**
  - **RFC 4659, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN"**
- **Both schemes avoid need to turn on IPv6 in the core of the network**
  - **Existing IPv4-signalled transport LSP infrastructure can be used**

Applicability of 6PE and IPv6 VPN

- **Both are mature technologies, IPv6 VPN has been available in Junos production code for 4-5 years now and 6PE for even longer..**
- **In 6PE, routes reside within the main routing context on each PE, so is *not* a VPN scheme**
  - **Useful for transporting "Internet IPv6" across a service provider's IPv4 MPLS network.**
- **IPv6 VPN is very similar to the IPv4 VPN model**
  - **Routes reside in VRFs on each PE**
  - **Gives separation between client networks and allows for overlapping addresses**
  - **Also used for "Internet IPv6", e.g. by having a VRF containing the internet routes**

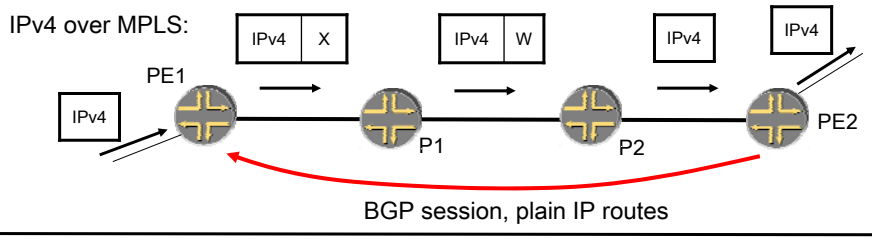
Infrastructure for 6PE

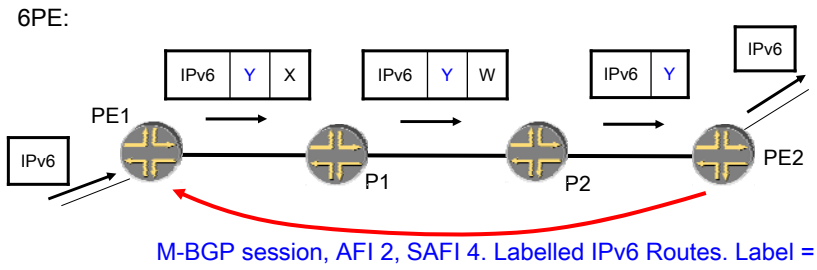


6PE mechanisms

- When transporting IPv4 packets over MPLS, one simply places IPv4 packet directly into transport LSP
- If we did the same with IPv6 packets, could cause problems
  - If PHP is being used, bare IPv6 packet would be exposed on penultimate router, and penultimate router typically is P router that does not run IPv6
  - If explicit-null label is being used on last hop, explicit null label value is different for IPv4 and IPv6, so same LSP could not be used for both IPv4 and IPv6 traffic
- Hence use an "inner label". M-BGP is used to enable PEs to exchange the inner label values.

IPv4 over MPLS and *IPv6 over MPLS (6PE)* compared

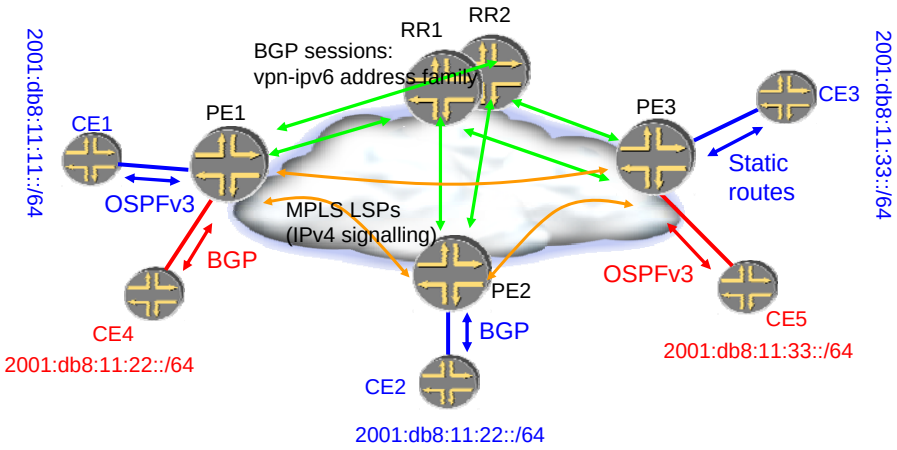




IPv6 VPN mechanisms

- Described in RFC 4659, “BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN”
- The MPLS tunnels can be existing IPv4-signalled LSPs
- Uses very similar machinery as IPv4 VPNs:
  - Use of M-BGP to exchange labelled routes between PEs (“inner label”, aka “VPN label”)
  - Route Distinguishers to disambiguate routes
  - Extended Community Route Targets to identify the VPN
  - Label stacking in data plane: ingress PE pushes VPN label and then pushes outer transport label(s)

IPv6 VPN case

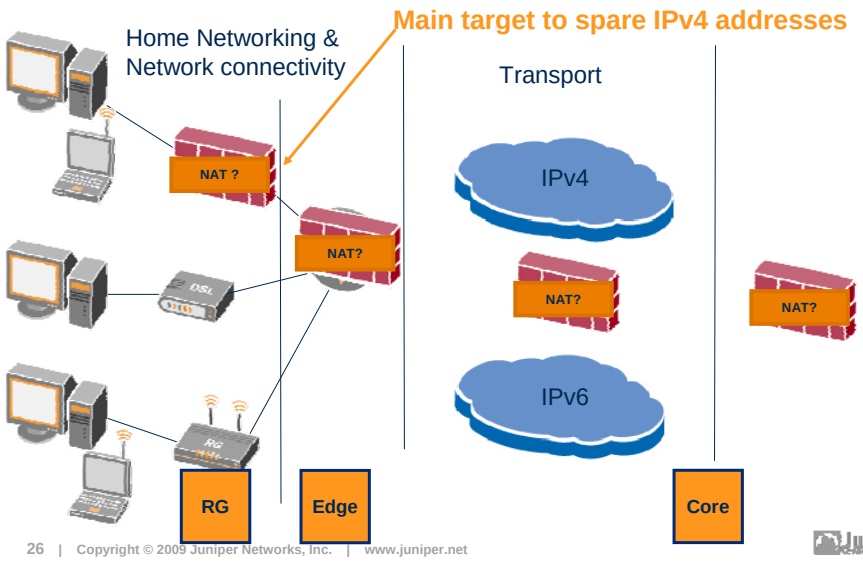


N.B. IPv6 VPN could instead run over an IPv6 core in principle, but current implementations/deployments/trials are over an IPv4 core (IPv4 IGP, BGP sessions over IPv4, MPLS LSPs signalled by IPv4)

Agenda

- Planning Transition
- **Transition trends in Service Providers**
  - In the core
  - **In the access**

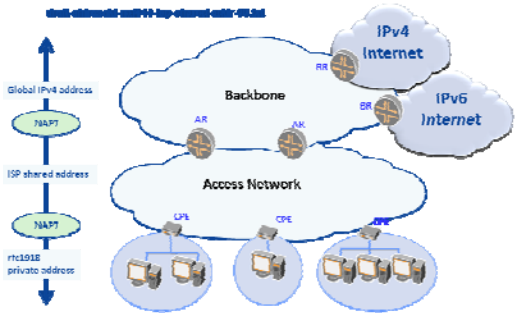
Possible Locations for NAT/CGN



1. NAT444 -- pros/cons

Pros :
- No need for change the current CPE spec.
- All consists of existing technologies. Easier to implement.

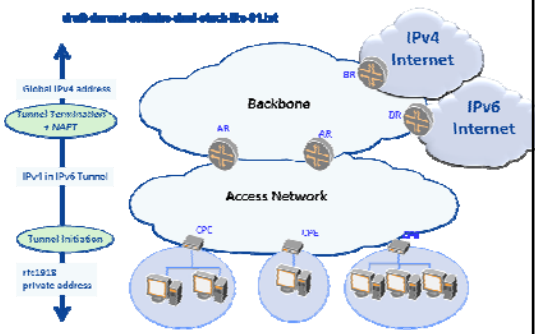
Cons :
- Session states at Core
- Scalability Concern (LSN to support massive number of sessions).
- Applications are restricted
- Fullcone/BEHAVE compliance is new to high-end NAT/firewall.



2. DS-lite -- pros/cons

Pros :
- only one layer of NAT (no dual NAT like NAT444)
- Access Network could be IPv6-only

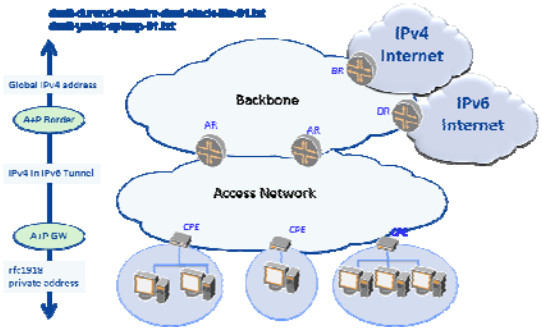
Cons :
- Requires CPE change
- Same concerns as NAT444 applies in terms of CGN/LSN



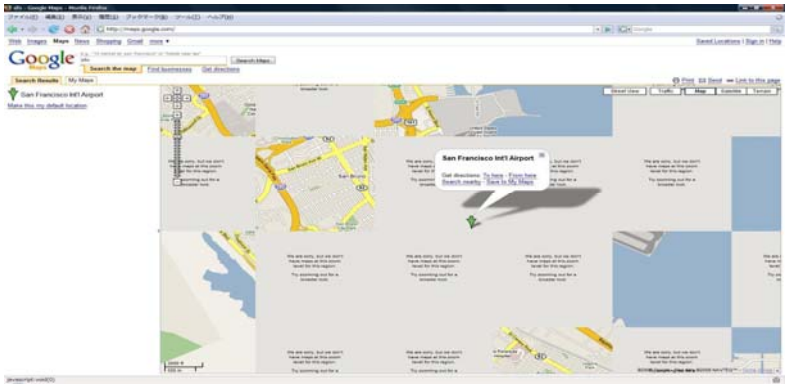
3. DS-lite + A+P -- pros/cons

Pros :
- No session states at Core (Translation&States only at the Edge)
- Scalable
- Less harmful to the end-to-end principle of the Internet
- Access Network could be IPv6-only

Cons :
- Requires considerable CPE change
- New CPE management scheme is also needed (i.e. address+port assignment via DHCP)
- Brand-new technology



NAT Scaling (example with 10 TCP Sessions) http://www.nttv6.jp/~miyakawa/IETF72/



- Port Usage and Scaling are additional concern if NAT or NAT-PT is performed by Service Provider in the Edge or in the Core

Juniper Networks
The Preferred IPv6 Supplier

- Juniper included IPv6 in hardware from the beginning
  - First support in 2001 on JUNOS routers !
  - JUNOS: Core, Edge, Access
  - JUNOSe: Broadband Access
  - ScreenOS: Security and Translation
- Juniper has long been the preferred vendor for high-performance, next-generation IPv6 networks
  - Dual-Stack IPv4/IPv6, IPv6 over MPLS

Conclusions

- IPv6 is inevitable
- IPv4 exhaustion is pushing IPv6 deployment up the agenda
- IPv6 is an infrastructure issue, not an application issue
- IPv6 deployment is happening worldwide
- Planning now is essential
- Juniper Networks has a long experience in deploying and supporting IPv6 in production infrastructures

THANK YOU

Jean-Marc Uzé
Director Product & Technology, EMEA
juze@juniper.net