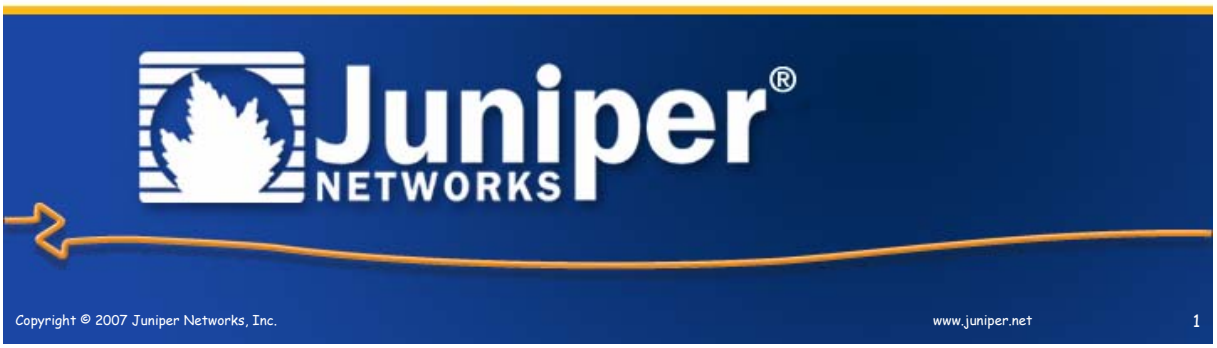
Practical Experiences with IPv6 – VPNs, Transition, and more

Umesh Krishnaswamy
Juniper Networks

November 20, 2007



Agenda

- Background
- Dual stack mechanism
  - SINET3 deployment
- 6PE mechanism
  - Telefonica deployment of 6PE
- IPv6 VPN mechanisms
  - Pacific Northwest Gigapop deployment of IPv6 VPN
  - BT 21CN trial of IPv6 VPN

Service Provider Drivers for IPv6

- IPv4 address depletion
  - Affects service providers differently in different geographies based on addresses available from RIR
  - Different estimates of when this will be an issue. Range is 2010-2011
  - New services that accelerate the pace of address consumption (mobile, cable)
- Regulation and standards
  - US Federal Networks
  - 3GPP Release 5 for IMS

IPv6 in mobile communications networks

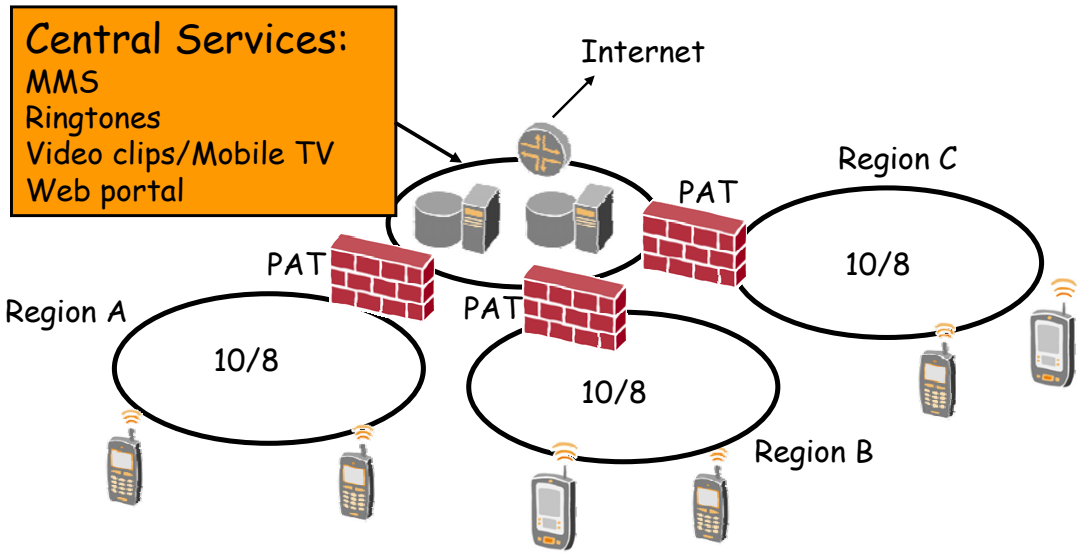
- Many mobile backbones are now MPLS-based
- There are strong drivers for IPv6 in mobile networks, hence interest in IPv6 over MPLS schemes
- IMS in 3GPP Release 5 was specified to be exclusively IPv6-based
- Although 3GPP Release 6 softened this slightly…
  - "3GPP specifications design the IM CN subsystem elements and interfaces to exclusively support IPv6. However, early IMS implementations and deployments may use IPv4."
- …there is still impetus for deploying IPv6

Mobile Communications Networks

Use of IPv4 addressing can be problematic

- All new handsets are IP-enabled. Increasing tendency for handsets to need an IP address all the time they are switched on, because of services that push data to the handset (e.g. email etc)
- Not feasible to have sufficient public IP addresses to allow a public IP address for each handset that is active and using IP services
- Hence usually use private addresses. When mobile networks are merged (due to company mergers/acquisitions), often end up with overlapping addresses
  - PAT is used between the network islands and central services (e.g. internet access, MMS, ringtones etc). But PAT can make it difficult to roll out new services.
- Also only ~17M IPv4 private addresses, which could be a limitation

Problem with overlapping private addresses in mobile networks



United States Federal Networks

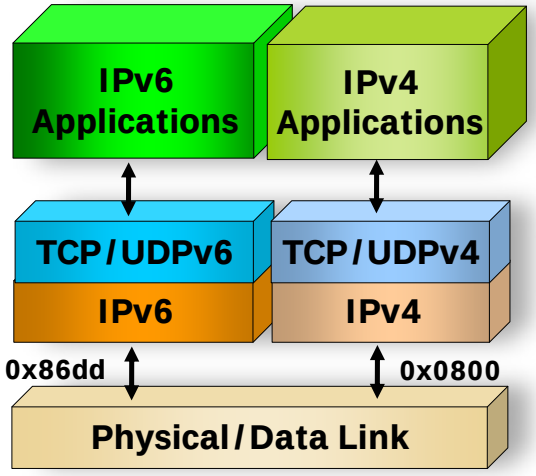
- US Dept of Defense in 2003 specified network equipment to be IPv6 capable by 2008
- US Government's *Office of Management and Budget (OMB)* issued a memorandum in 2005 covering all US Federal agencies saying *"…we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure."*
  - http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf

United States Federal Networks (cont'd)

- Many of these Federal agencies use MPLS VPN services supplied by carriers, hence the need to support IPv6 over MPLS VPNs on those carriers' networks

Dual Stack

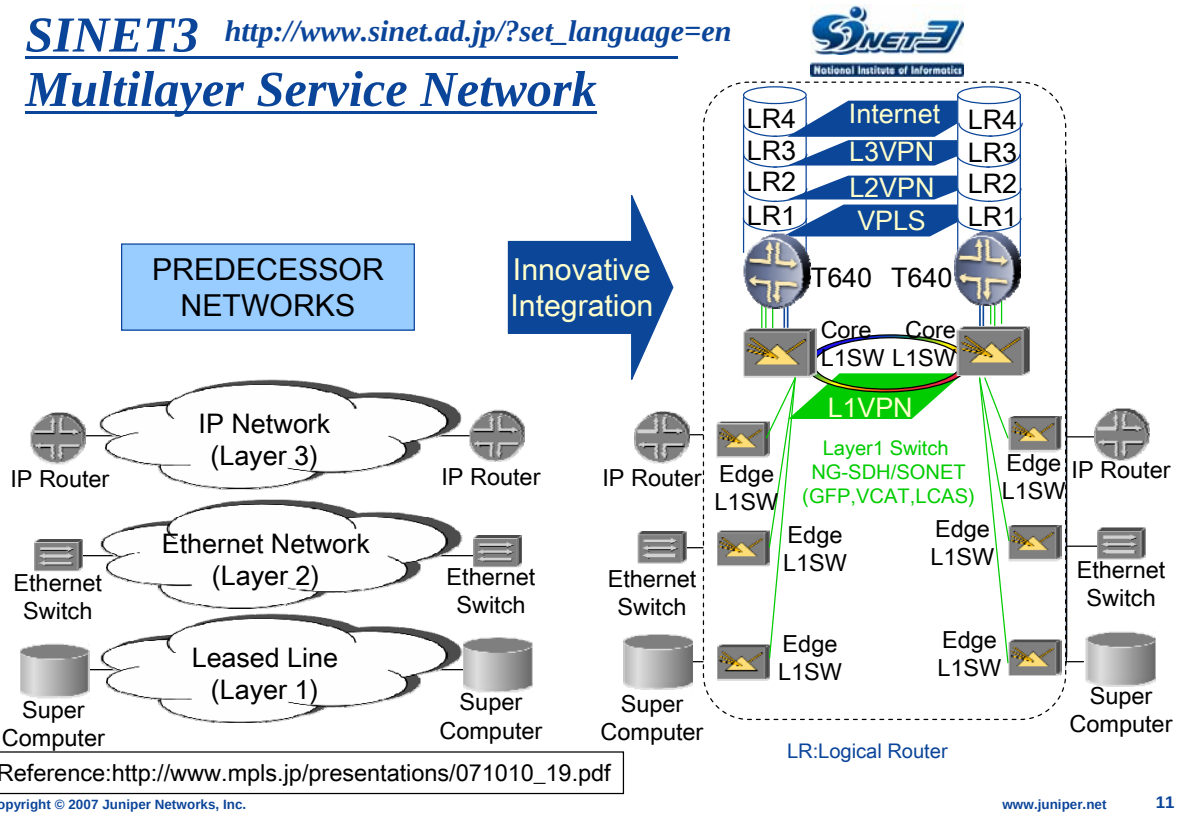
- IPv4 and IPv6 coexisting on same device
- Use IPv6 variants of IGP (RIPng, OSPFv3, ISIS)



SINET3 Deployment

- The next two slides describe the deployment of dual stack in SINET3.

SINET3 http://www.sinet.ad.jp/?set_language=en
Multilayer Service Network



Reference:http://www.mpls.jp/presentations/071010_19.pdf

SINET3 IPv6 Service

SINET3 assigns IPv6 addresses(2001:2F8::/32) to universities and research institutions

- **Predecessor NETWORKS**
  - IPv6 over IPv4 Tunnel Service
- **SINET3**
  - IPv6 Native Service(IPv4/IPv6 Dual Stack)
  - Service deployment over Logical Router
  - QoS
  - Multicast

Schemes for IPv6 over MPLS

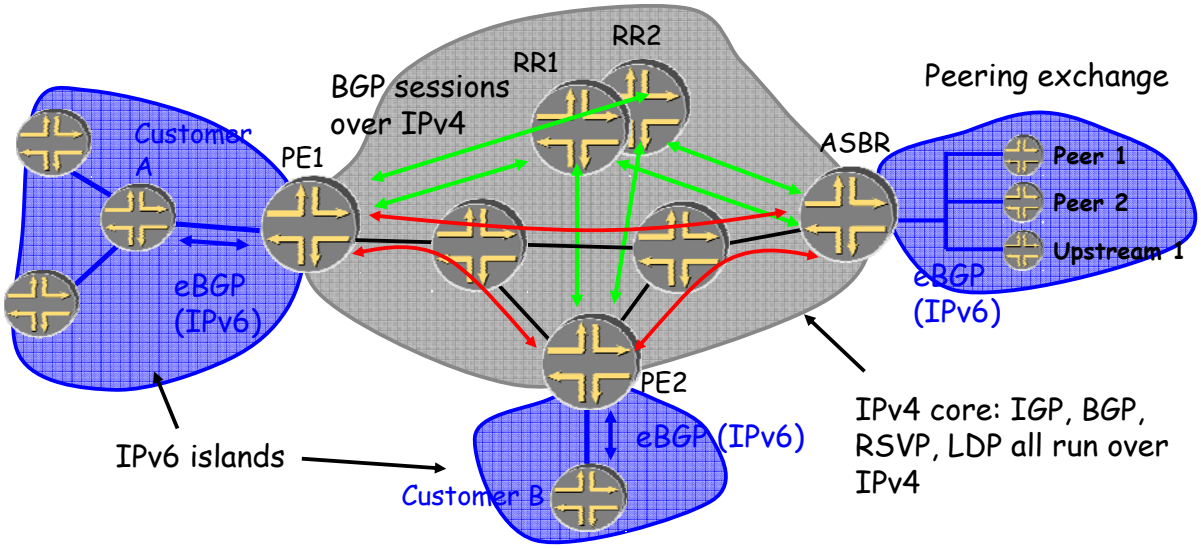
Two main schemes exist:

- 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
  - 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 production code for three 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



MPLS LSPs, signalled using IPv4

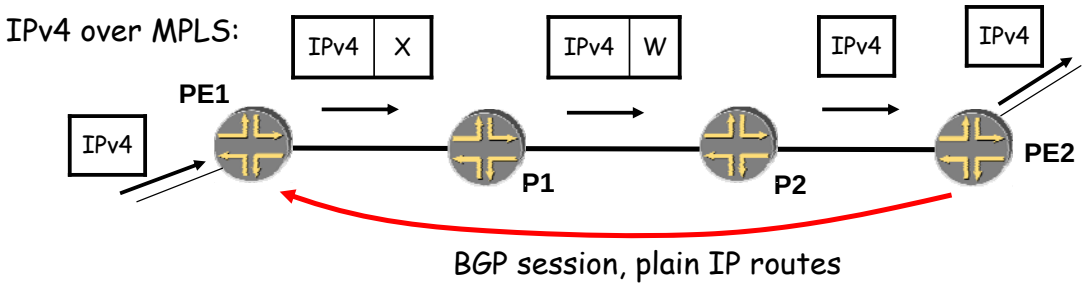
Links in black have IPv4 addresses, and use an IPv4 IGP

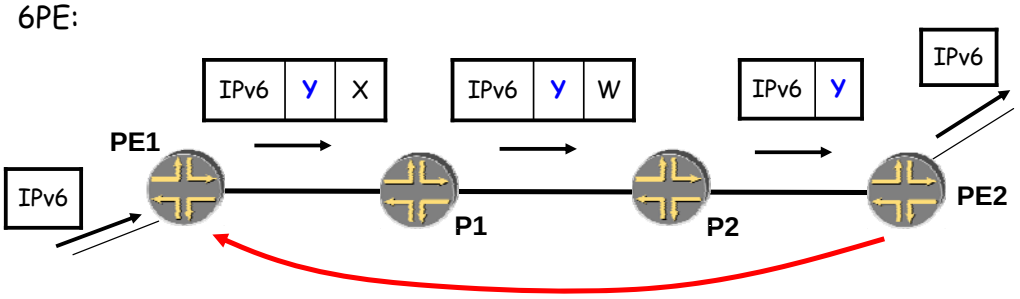
Links in blue have IPv6 addresses, and use an IPv6 protocol

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





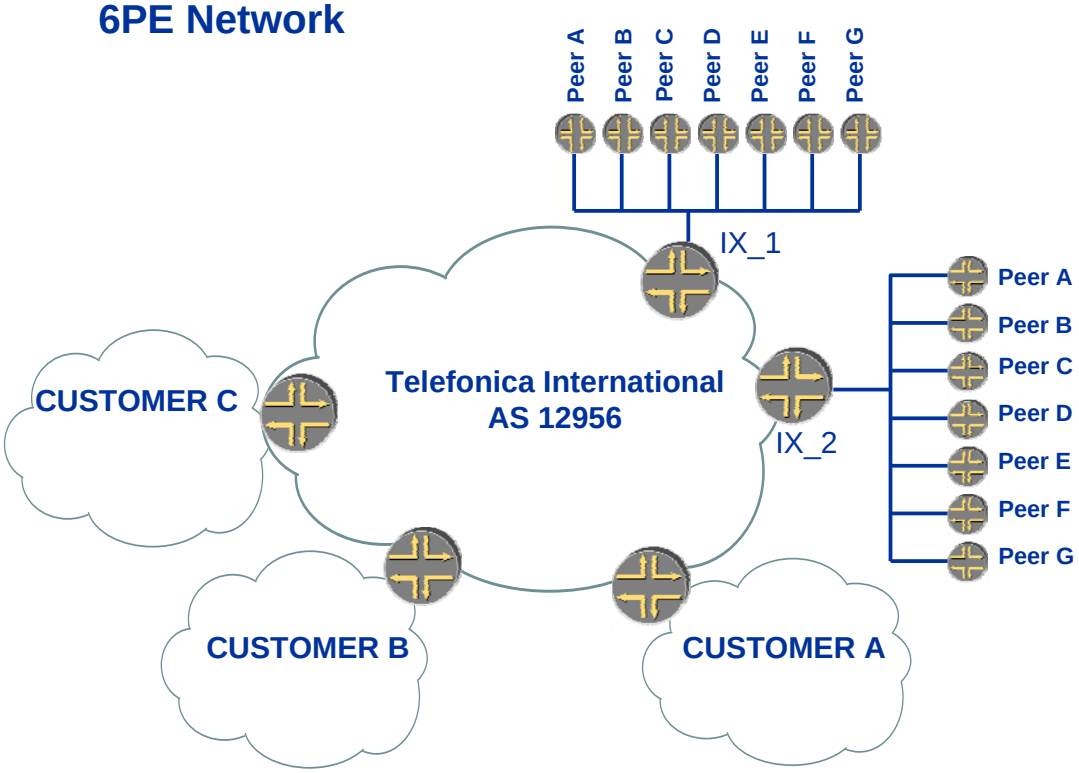
Telefonica deployment

- The next two slides describe the deployment of 6PE in Telefonica

Telefonica 6PE Deployment

- Traffic carried on Telefonica International Worldwide Service backbone using 6PE scheme, providing IPv6 connectivity to other Telefonica ASes
- Network spans Europe and South America:
- IPv6 peerings to outside world at AMSIX and LINX
- Full-mesh of BGP sessions between the 6PE PE routers
- LDP LSPs for transport

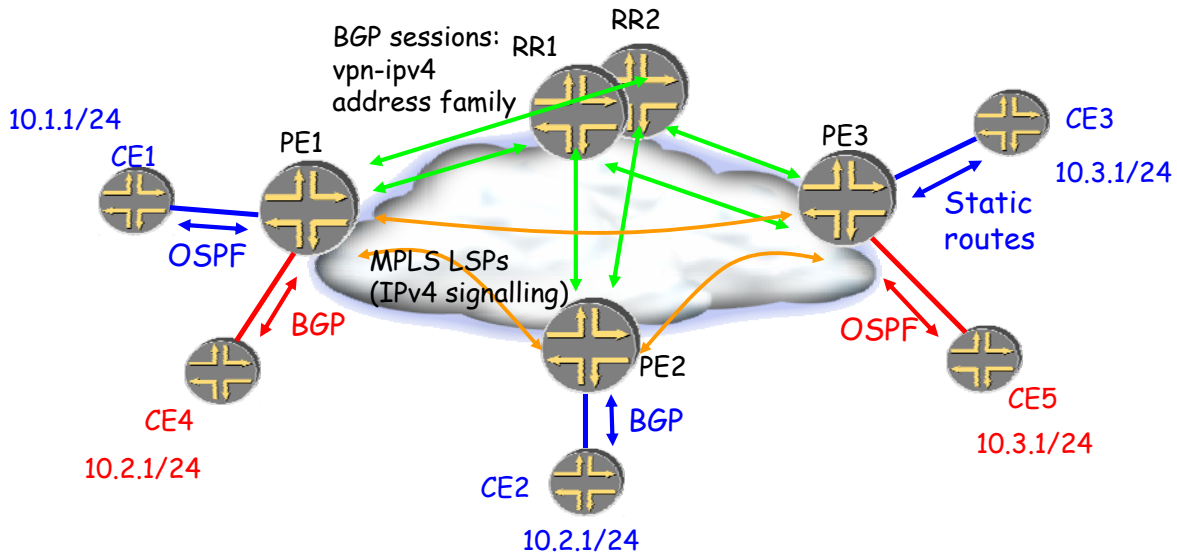
6PE Network



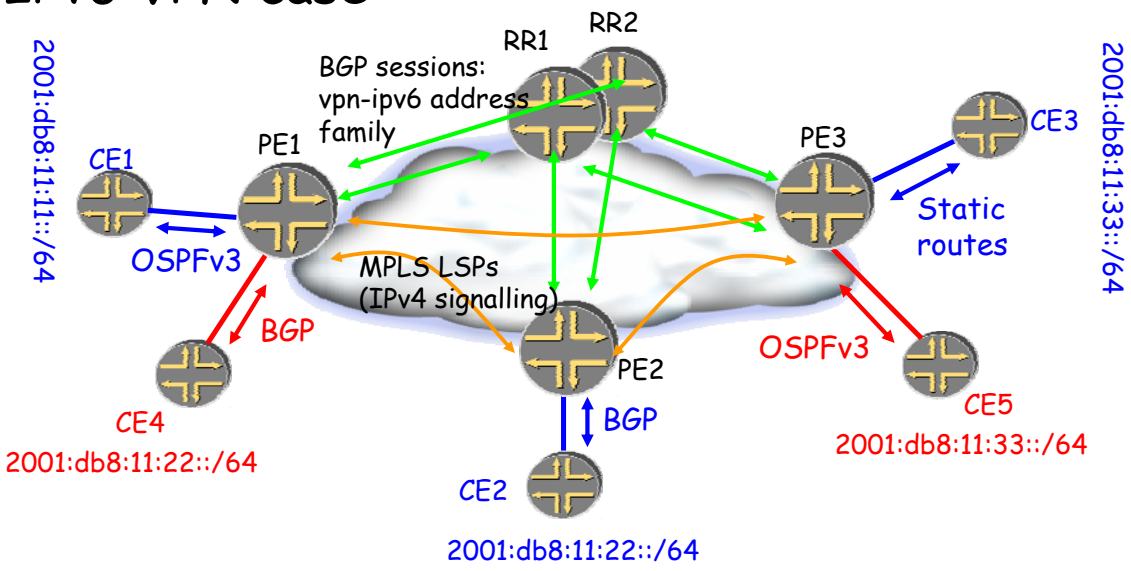
IPv6 VPN mechanisms

- Described in RFC 4659, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN"
- The MPLS tunnels could be IPv6 LSPs or IPv4 LSPs
  - Or other tunnel types can be used (GRE, IPSec etc)
  - IPv4 LSPs are the most commonly used today
- 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)

IPv4 VPN case



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)

BGP Update: schematic comparison

IPv4 VPN case:

AFI = 1, SAFI = 128
Route Target: Blue VPN
Next-hop = 192.168.0.4
NLRI:
Length
Route Distinguisher:PE1
10.1.1/24
Label = 100000

VPN-IPv4 address family

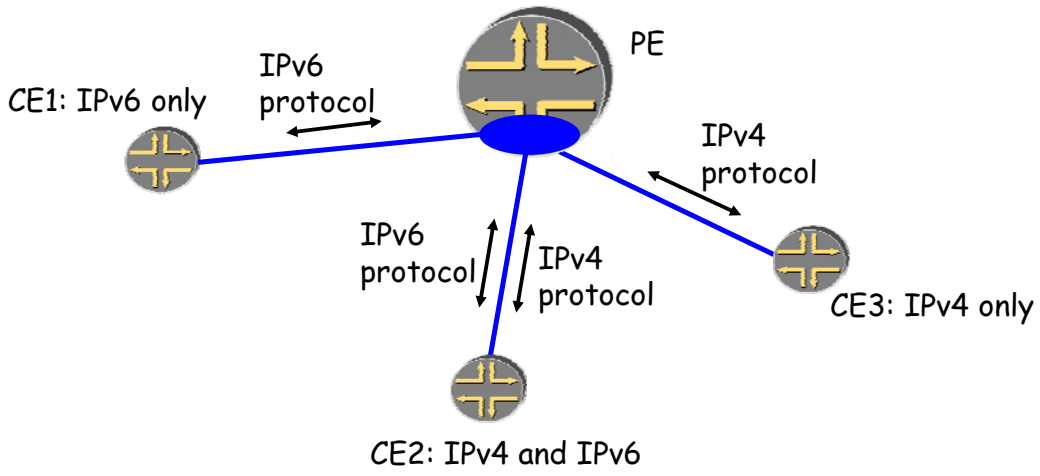
IPv6 VPN case:

AFI = 2, SAFI = 128
Route Target: Blue VPN
Next-hop = ::ffff:192.168.0.4
NLRI:
Length
Route Distinguisher:PE1
2001:db8:11:11::/64
Label = 100000

VPN-IPv6 address family

IPv4-mapped IPv6 address

IPv4 and IPv6 in same VRF



Introducing IPv6 VPN into existing VPN infrastructure

- In principle can be relatively straight-forward as operational model and configuration are very similar to IPv4 VPN
- Can use same LSPs and same BGP sessions as for existing IPv4 VPNs, BGP-L2VPN and BGP-VPLS that may have already been deployed
  - Simply turn on VPN-IPv6 address family on the BGP sessions
- Same features as for IPv4 VPN can be used:
  - Packet processing features on ingress and egress PE
  - Route Target Filtering
  - Accounting features
  - Interprovider VPN: same options (a), (b), (c) apply as for IPv4 VPN

VRF configuration comparison

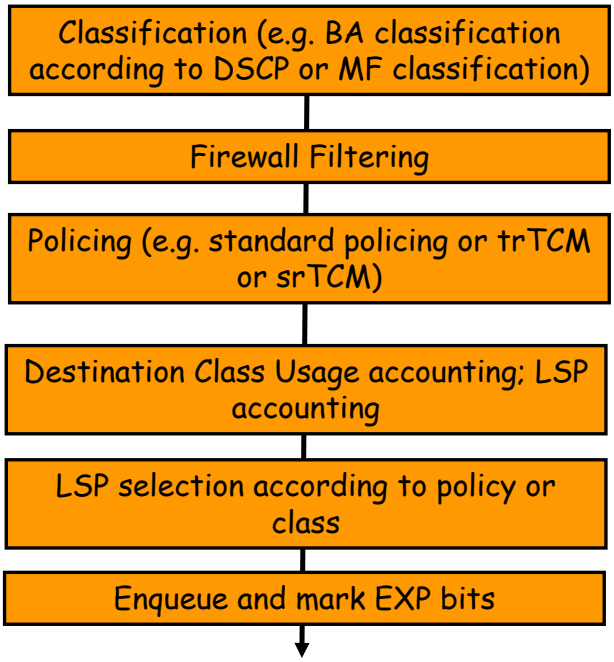
IPv4 case:

```
routing-instances {
   test1 {
      instance-type vrf;
      interface so-0/2/2.0;
      vrf-target target:1:1;
      vrf-table-label;
      protocols {
         ospf  {
            export bgp2ospf;
            area 0.0.0.0 {
               interface so-0/2/2.0;
            }
         }
```

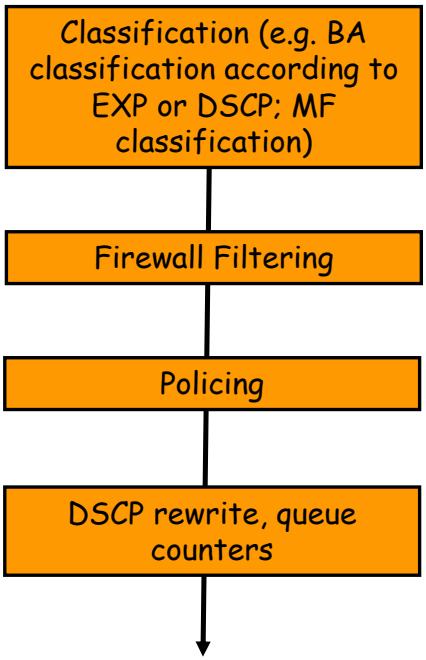
IPv6 case:

```
routing-instances {
   test1 {
      instance-type vrf;
      interface so-0/2/2.0;
      vrf-target target:1:1;
      vrf-table-label;
      protocols {
         ospf3 {
            export bgp2ospf;
            area 0.0.0.0 {
               interface so-0/2/2.0;
            }
         }
```


Packet processing in IPv6 VPN: ingress PE



Packet processing in IPv6 VPN: egress PE



Pacific Northwest Gigapop

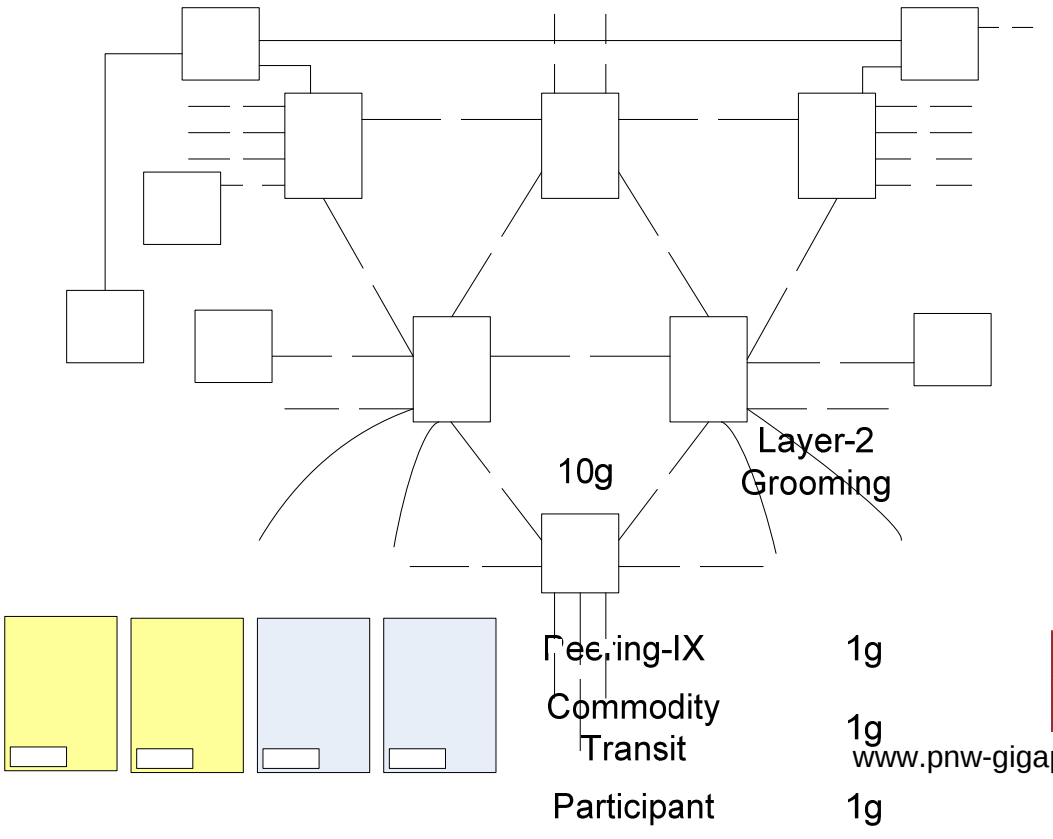
- The next two slides describe the Pacific Northwest Gigapop deployment of IPv6 VPNs

Pacific Northwest Gigapop

- Not-for-profit Research and Education Network Services Provider
  - Layer 1, 2, and 3 services
  - Layer 3 supports IPv4 uni- & multicast, IPv6 unicast
  - Currently 15 IPv6 peer/participant connections
- Next generation network will use an MPLS-based VPN deployment supporting multiple route views. Initial route views will be:
  - Commodity Internet (Peers and Transit)
  - Research & Education Peers
  - National LambdaRail
  - Internet2
- Participants will receive access to three or four of the VPN's
  - Multiple service offerings will be created via route filtering within each VPN
  - Physical interface will be virtualized based on access technology (.1q, Frame, etc.)
- All routers in the network will have access to the VPN's and will potentially be PE's
- Lab testing complete Nov 2006
- In production since September 2007

www.pnw-gigapop.net

Network Topology Overview

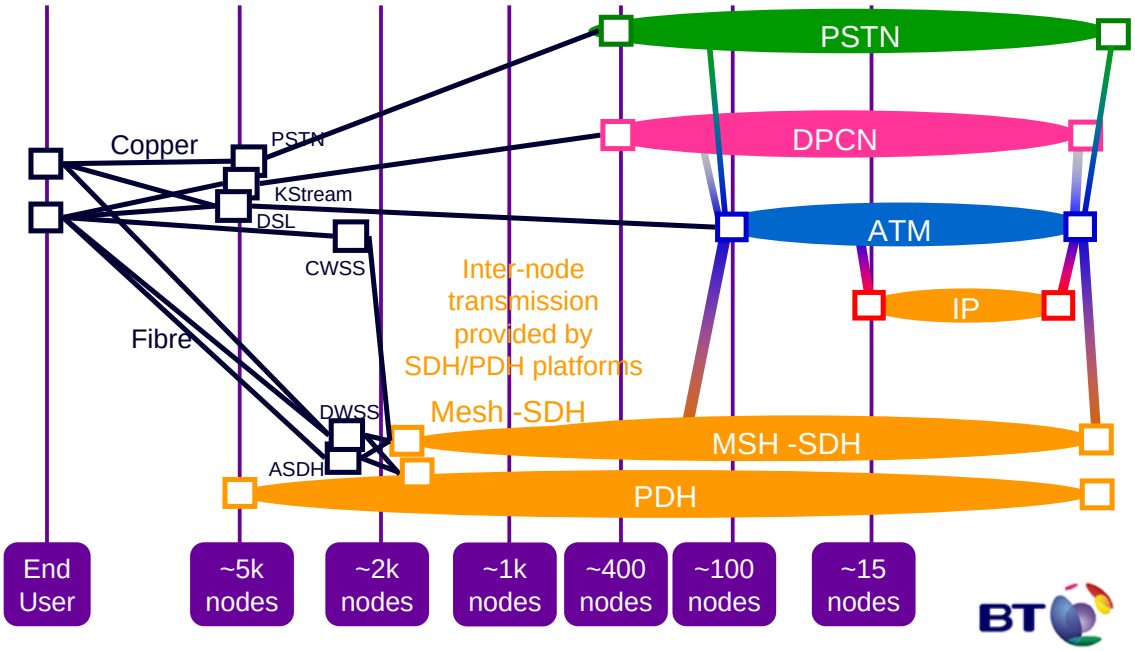


BT 21CN IPv6 proof of concept

- The next five slides describe BT's use of IPv6 VPNs within the 21CN IPv6 proof of concept

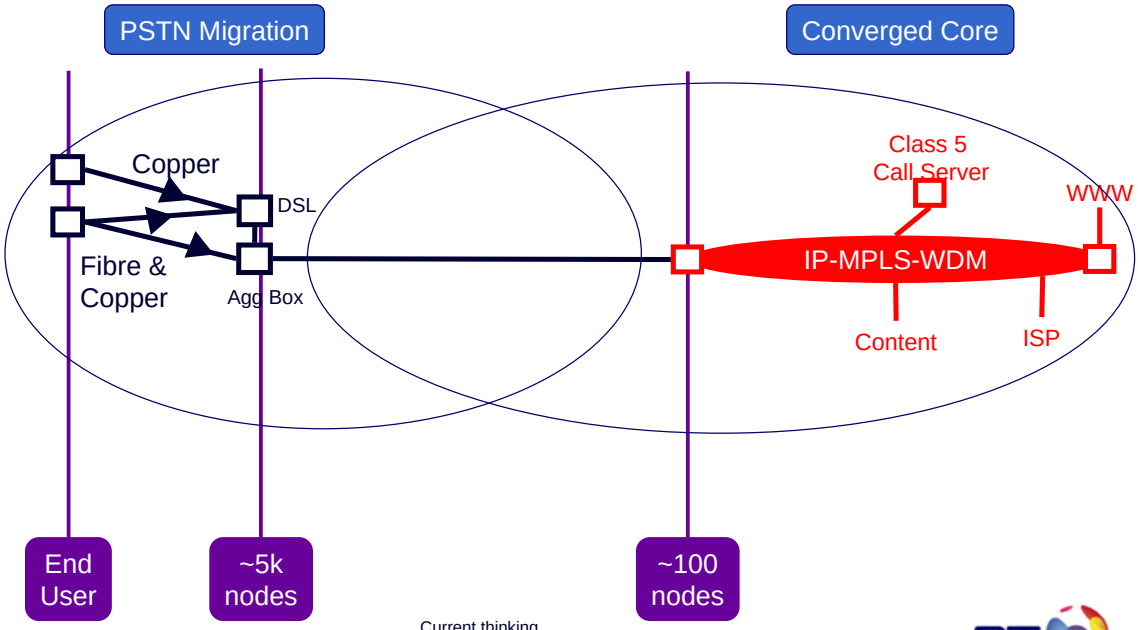
BT's 21st Century Network

Current network



BT's 21st Century Network

Proposed Network

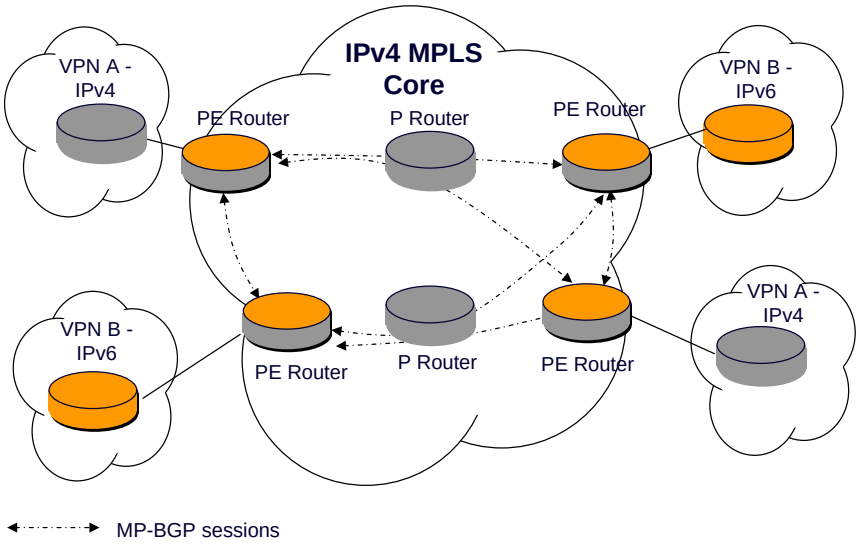


Current thinking.
No implementation assurances

IPv6 in the 21CN

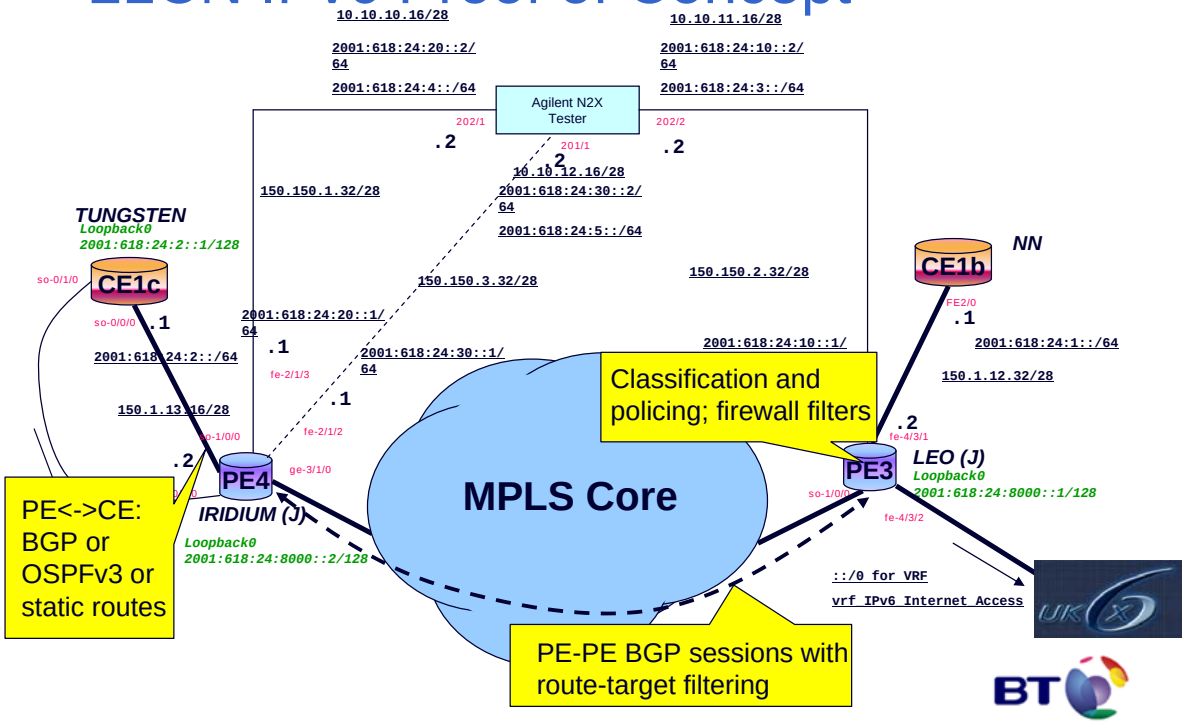
- 21CN will be IPv6 ready when demand arises
- BT needs to be ready to react swiftly to any change in the market or to use IPv6 to cost-effectively grow our business.
- BT selected vendors that were IPv6 compatible
- Primary focus for deployment on the services necessary to support IPv6 products
  - IP VPN's to support core transport of IPv6
    - Enterprise connectivity
    - Internet Access

Proposed IPv6 Migration



Current thinking.
No implementation assurances

21CN IPv6 Proof of Concept



A word about IPv6 multicast over MPLS

- IPv6 multicast packets can be placed into P2MP LSPs, by pushing an IPv6 explicit-null label followed by the label corresponding to the P2MP LSP
- Also, the Next-Generation MVPN schemes are applicable to IPv6 MVPN

Summary

- IPv6 over MPLS attracting large amount of attention from network operators
- 6PE allows "Internet IPv6" to be carried across an MPLS-IPv4 backbone in a non-disruptive way
- IPv6 VPNs allow customer's private IPv6 traffic to be catered for using the same mechanisms as in IPv4 2547 VPNs
- Mature implementation of both 6PE and IPv6 VPNs exists in production code

Acknowledgements

- Many thanks to..
  - NII for SINET3 (Dr. Urushidani)
  - Telefonica (Ignacio Vazquez)
  - Pacific Northwest Gigapop (David Sinn and Dave McGaugh)
  - BT (John King)
  - Juniper (Julian Lucek)
- …for providing material for this presentation