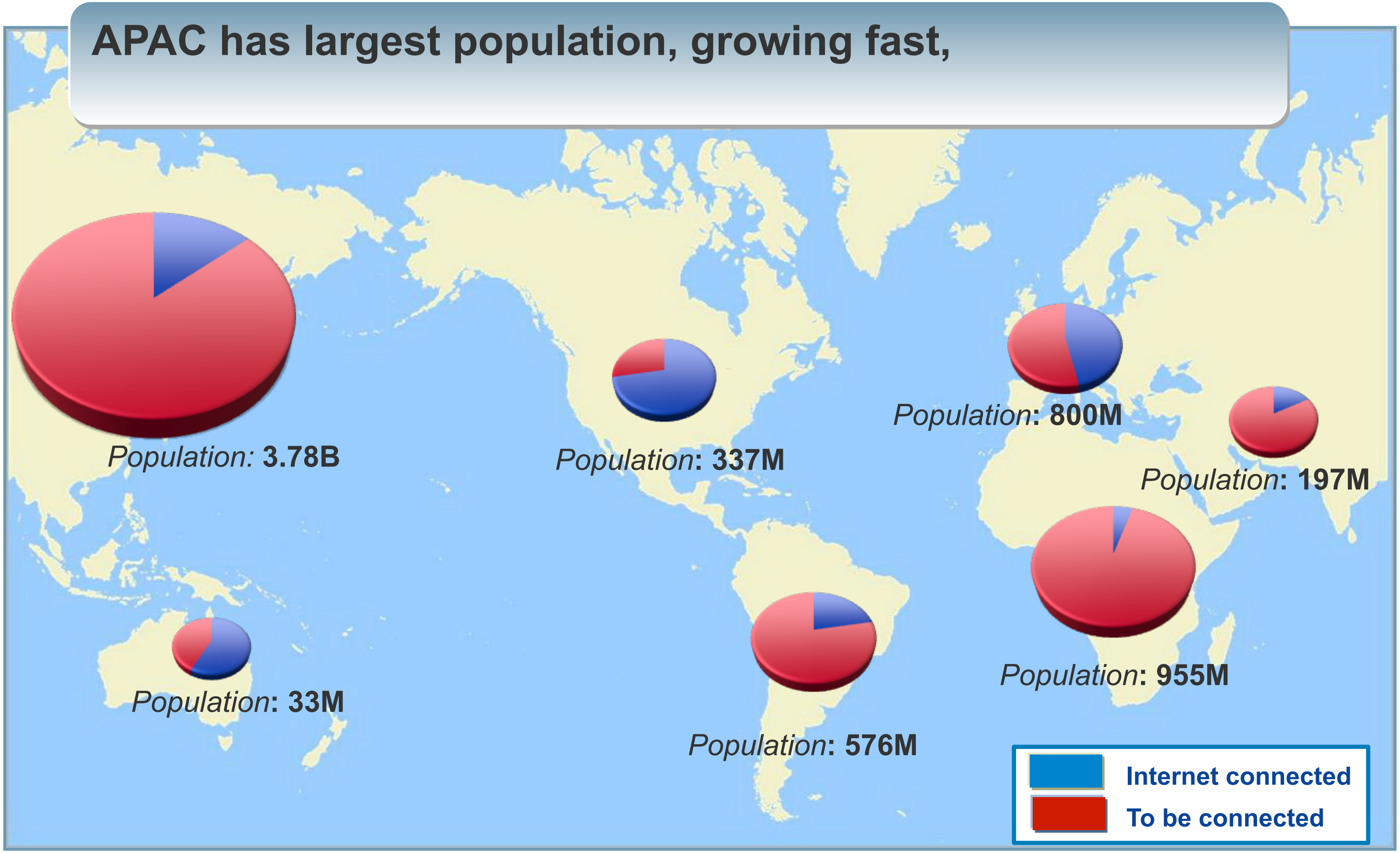
Deploying IPv6 in Service Providers

Markku Rantanen
markku@juniper.net

TREX Tampere
Feb 19th, 2010

EMERGING ECONOMIES & THE INTERNET

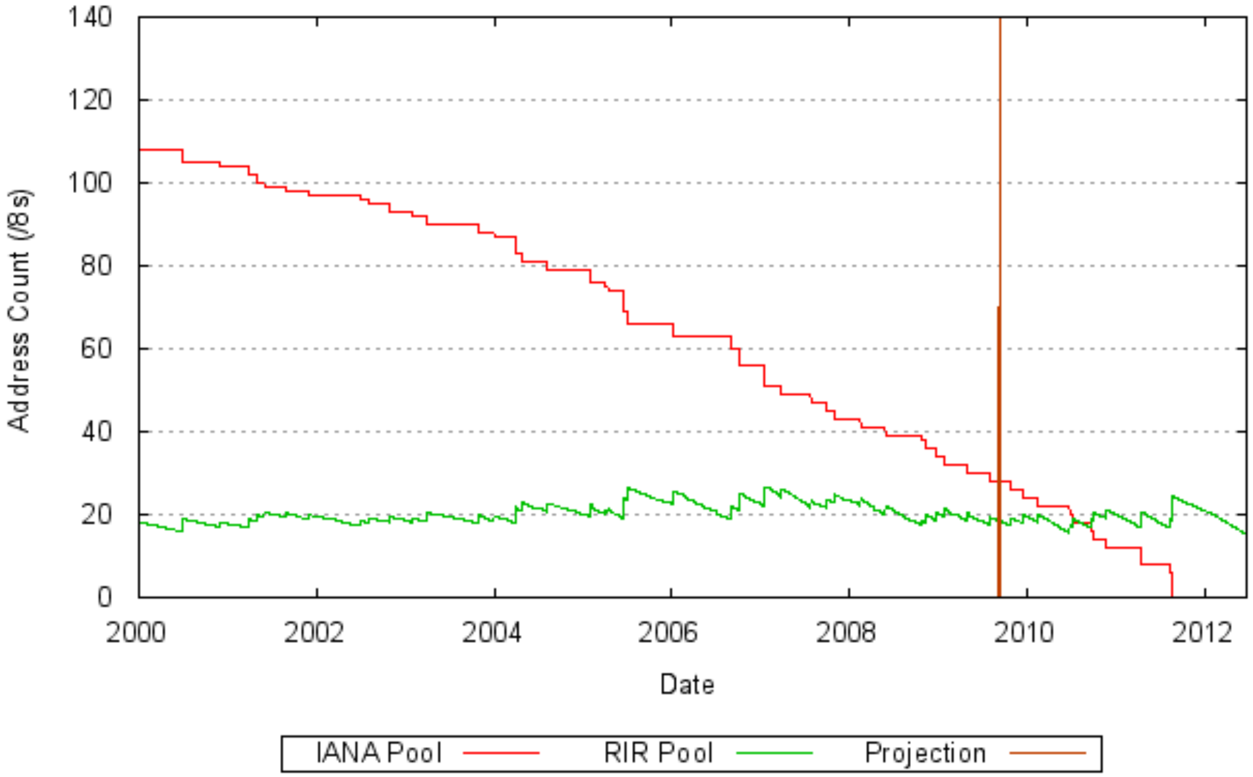
APAC has largest population, growing fast,



THE END OF THE ROW COMES INTO VIEW

Only 11% of IPv4 space remains available in IANA pool

Depletion projected mid-2011



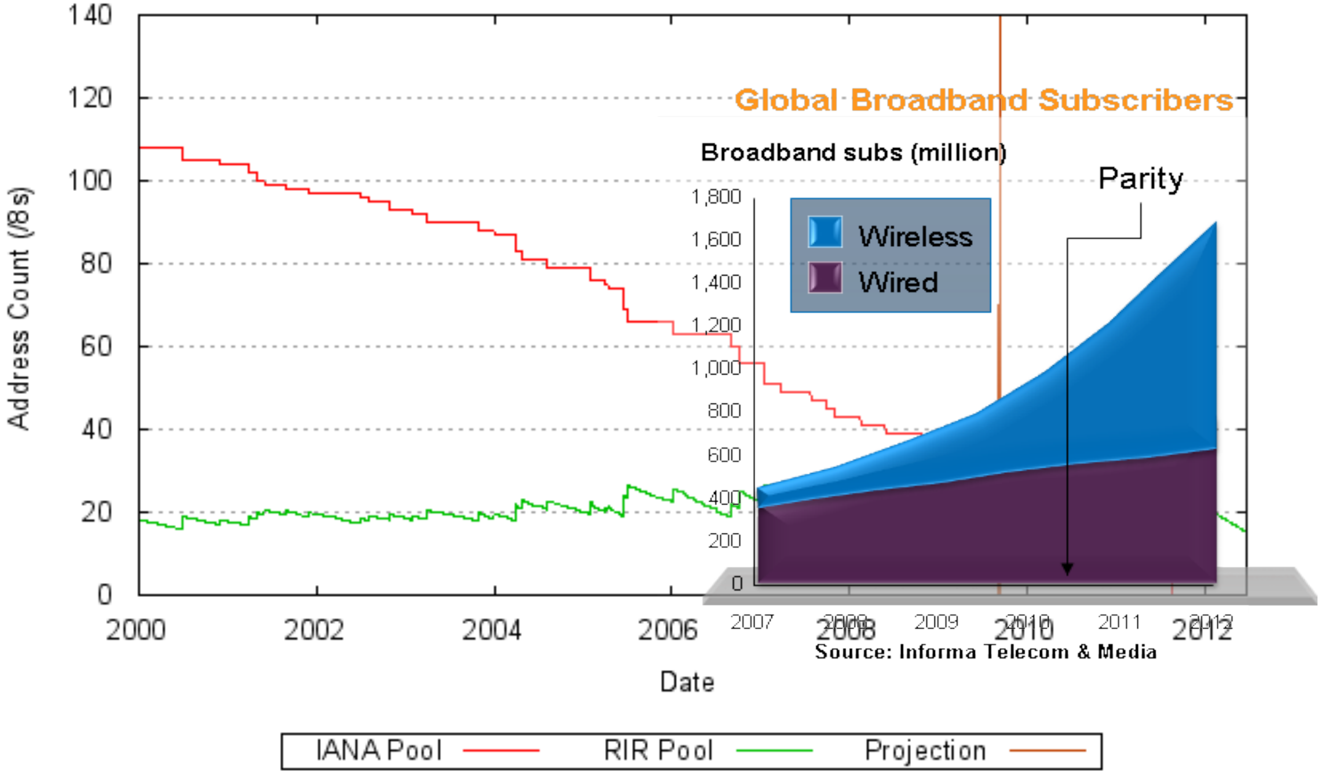
Projected RIR and IANA Consumption (nb /8s)

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

THE END OF THE ROW COMES INTO VIEW

Only 11% of IPv4 space remains available in IANA pool

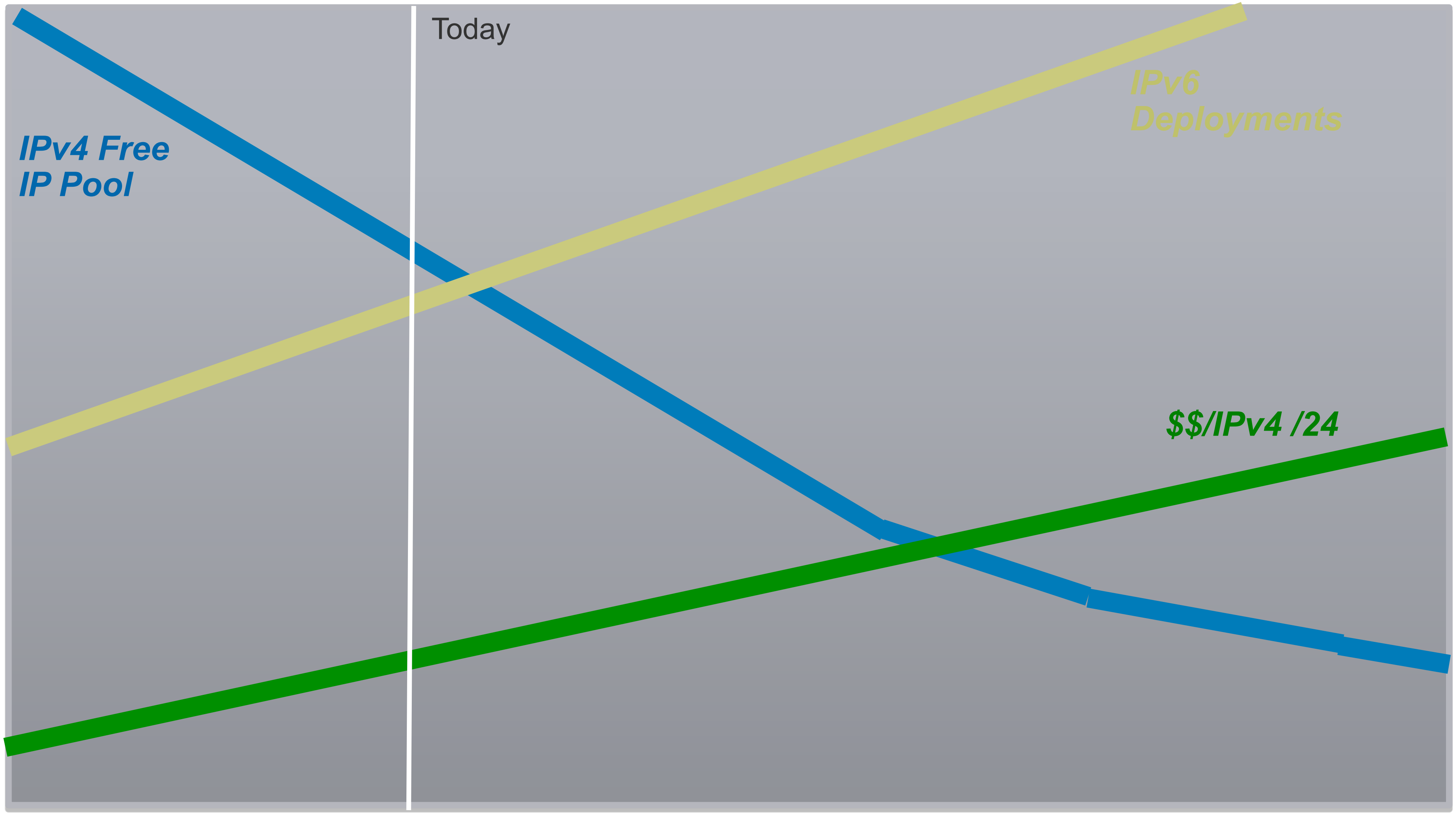
Depletion projected mid-2011



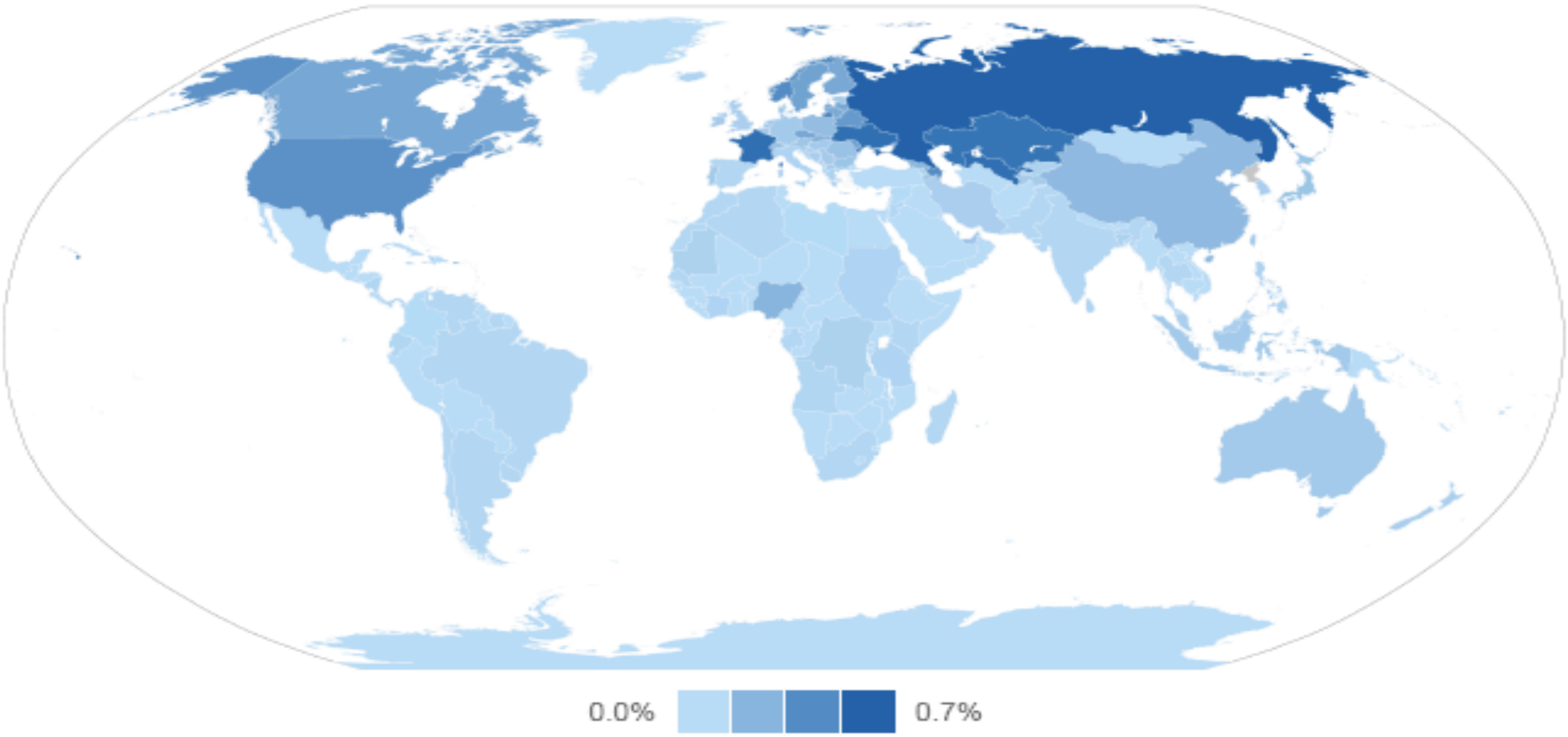
Projected RIR and IANA Consumption (nb /8s)

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

WHAT SHOULD HAVE HAPPENED



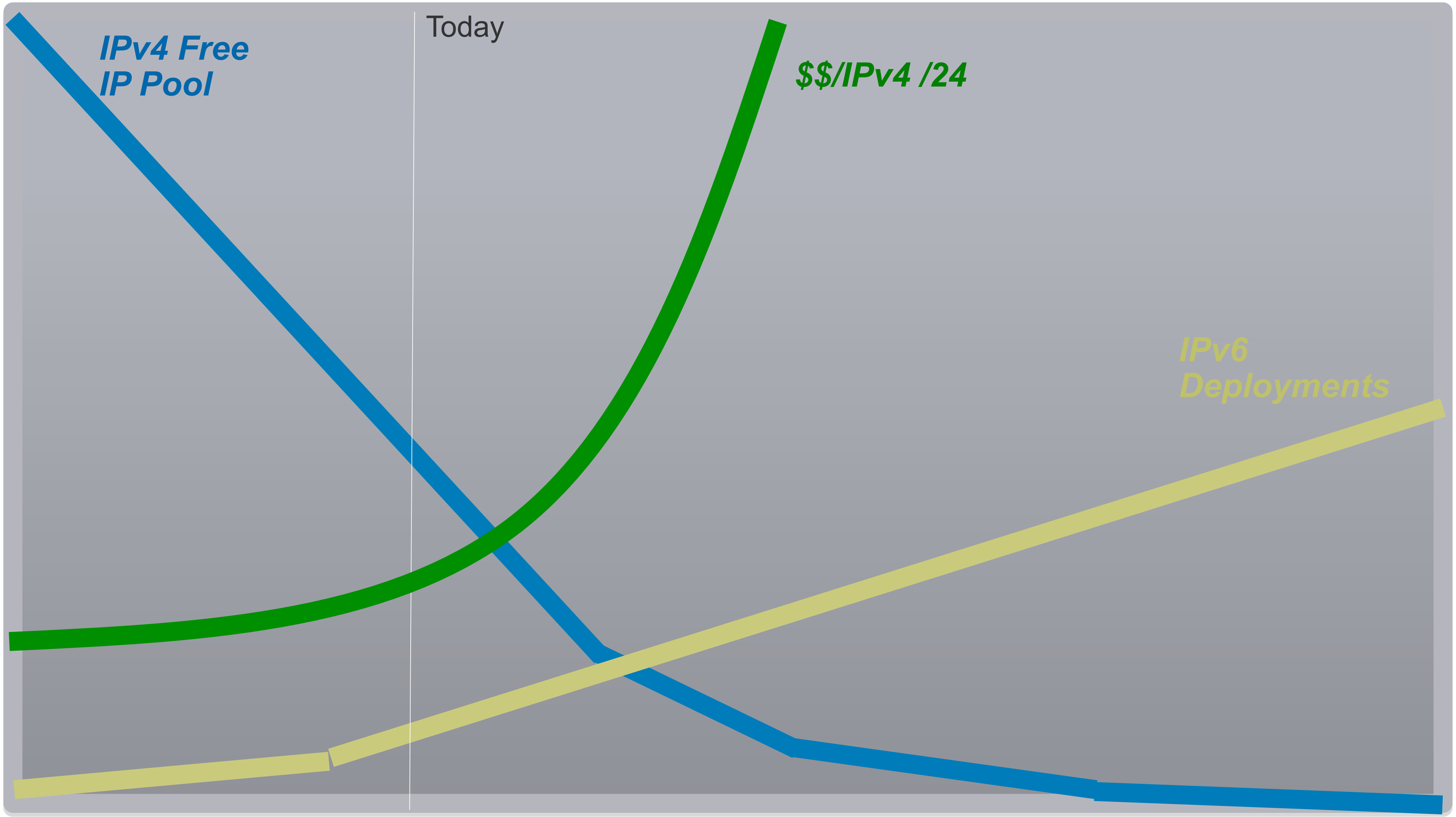
CURRENT STATE OF IPV6 DEPLOYMENT



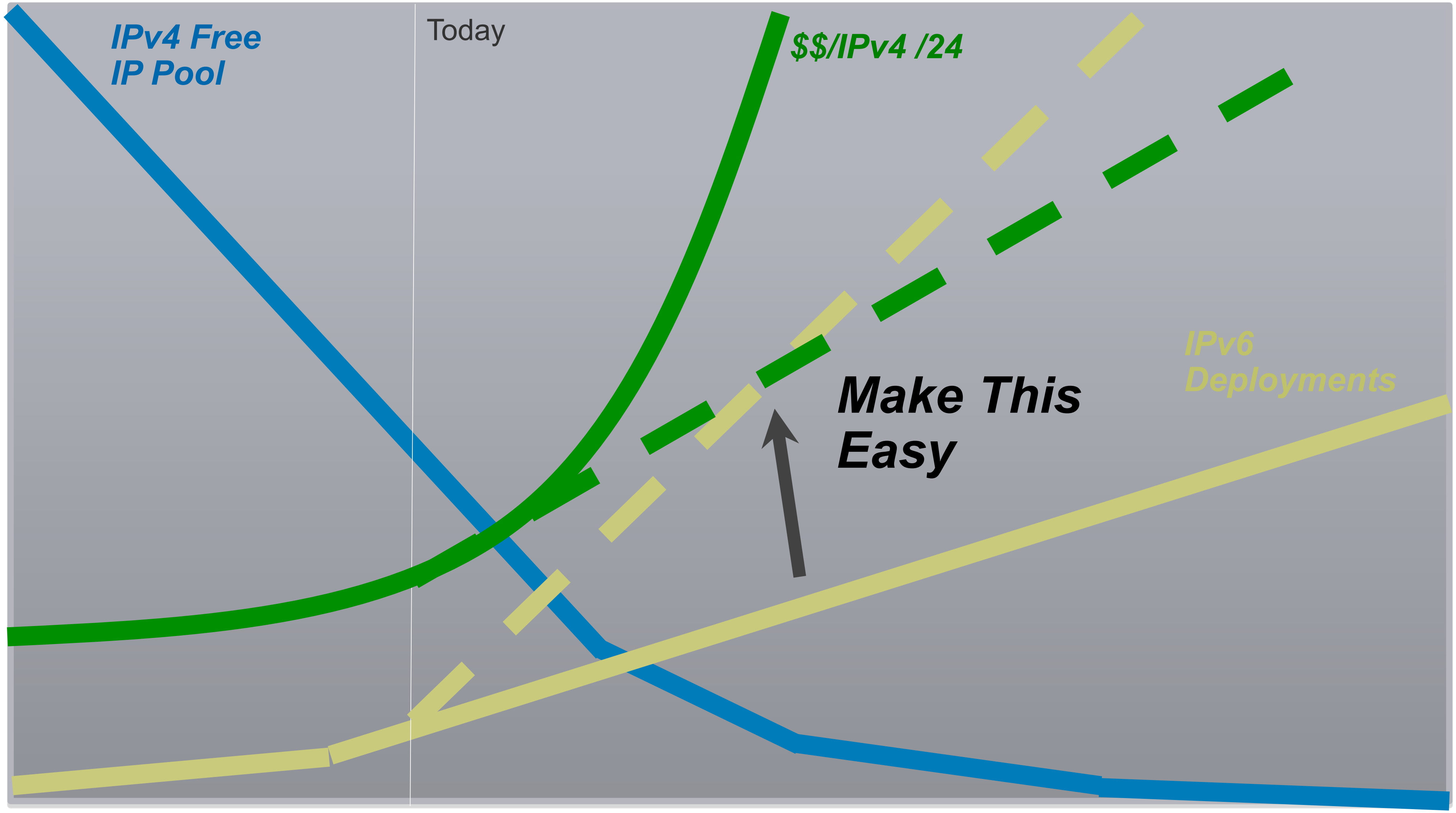
IPv6 connectivity by country — combined data, Aug-Oct 2008, lower bound of 68% confidence interval. *Source: Google Inc.*

Source: Google

WHAT IS HAPPENING



WHAT WE NEED TO DO



Service and Content Providers

Business case unclear - it’s still cheaper and easier to hook up a IPv4 site

ISCPs need to play along - no real content on IPv6-only sites today

Need a good solution for IPv4 only hosts to communicate with IPv6 only hosts

And other details to make it work

What Do We Think Will Happen?

- IPv4 address exhaustion is approaching in the next few years
    - Consumption of IPv4 addresses is accelerating
    - Current trends predict that IANA will run out of addresses to assign soon
- This may create problems for the internet
    - If we do nothing
        - Internet will keep working
        - Will be very challenging to grow

IPv6 Deployment

IPv6 in ISP networks

- Some backbones/core networks of ISPs have already made a move to IPv6
  - Either native IPv6 (dual stack)
  - Or using some kind of tunnels (including MPLS)
- Some have concrete plans for supporting IPv6….matter of appropriate time
- Why haven't all ISPs deployed IPv6
  - It does not imply new business/more revenue
  - Deploying dual stack increases short term cost (managing two protocols)

IPv6 Deployment…….

IPv6 in the end user platforms

- Many Operating Systems have supported ipv6 for years…..fair to say that all OS’s marketed today support IPv6
- Some IPv6 applications, such as peer-to-peer, may be cheaper to develop then IPv4 apps because of NAT implications

IPv6 Deployment….

Majority of Access/Edge networks (last-mile) don't yet support IPv6

- no economic incentive to update access networks
- No new services to help pay for the upgrade cost
  - Most of the low cost residential routers are not ipv6 ready

No real content available on ipv6-only sites today

- No real incentive for Content Providers to move to IPv6
  - No new revenues are foreseen….not at least till new applications can be offered that take advantage of IPv6
  - No benefit of ipv6 when it comes to applications such as internet browsing, email, client-to-server apps
    - These work fine with NAT

IPv6 Deployment…..

What will/can make ISPs deploy IPv6

- Create customer awareness so that they request their ISPs for IPv6 service
  - But then again why when most of their apps work fine with ipv4?
- Till customers' demand IPv6 service, ISPs have little incentive to move full fledge to IPv6
  - Demand from customers expected to grow in the next 24 months

IPv6 in Research and Education Networks

IPv6 deployment an exception in NREN

- No business case required
- Benefits research
- GEANT (PAN European Research Network)
  - Connects 18 NRENs natively
  - Dual stack IPv6
- Academic Deployments in general:
  - Validates production deployment for commercial ISPs
  - Leads technology awareness

IPv6 Deployment around the globe…..

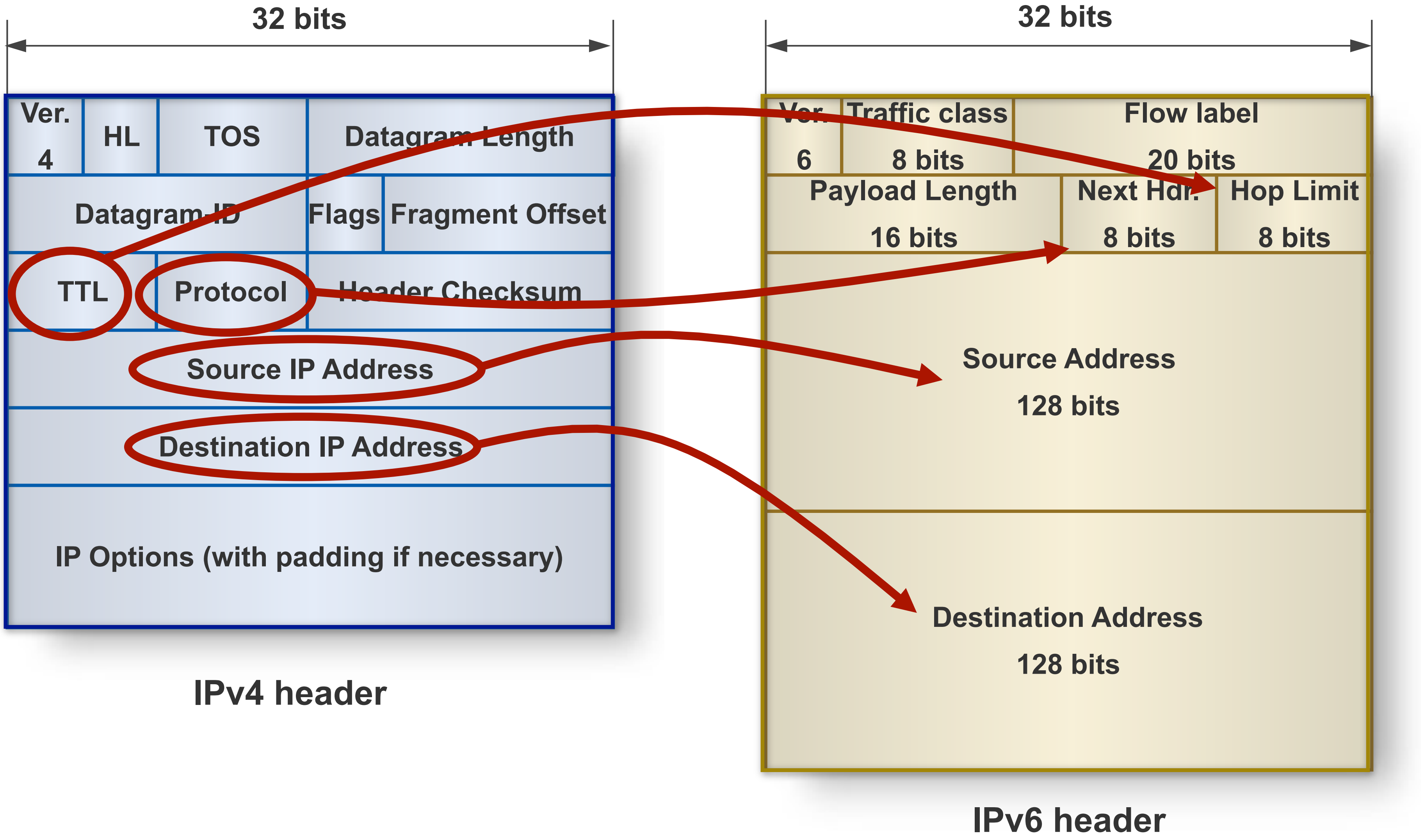
In North America networks are generally less IPv6 Ready as compared to Asia & Europe

In Japan, some ISPs provide IPv6 up to the edge for residential customers….has not yet happened in North America

Much larger percentage of ISPs in Asia and Europe support IPv6 in the core of their networks than in North America

Most of the Research and Education networks and universities in Japan and Europe support IPv6

IPv4 AND IPv6 ARE NOT INTEROPERABLE ISSUES: COEXISTENCE AND INTERCONNECTION



IPV6 TRANSITION TOOL KIT

IPv6 Transport Solution

- Core Backbone
  - Dual Stack
    - 2 routing protocols
  - 6PE
    - IPv6 over MPLS
  - 6VPE
    - IPv6 over MPLS VPN
- Access Network
  - Dual Stack
  - Enabling IPv6 Access on a IPv4 Network:
    - 6to4, Teredo, ISATAP
    - 6rd
    - IP6 over IPv4 (IPoIP)
  - Enabling IPv6 Access via agnostic network:
    - L2TP LNS IPv6
    - PPPoE Bridged CPE
    - Layer 2 Backhaul

IPv4 Depletion Mitigation

- NAT444
  - End point independent NAT
- DS-Lite
- A+P

IPv6 to IPv4 NAT

- NAT-PT
  - ICMP, Tracert ALG
  - DNS ALG
- NAT64
  - DNS64
- NAT66
  - ALG

Potential Mitigations for IPv4 exhaustion

Temporary Mitigations

- Return experimental blocks to the pool of regular addresses
  - Challenges there……
    - Requires standardization effort
    - Hw/sw upgrades will be required
    - Cost will be huge for a small gain
- Reclaim unused addresses
  - May require renumbering due to fragmented address space
  - Requires changes in policies
  - Will take years….not cheap

Potential Mitigations for IPv4 exhaustion……

Temporary Mitigations…..

- Increased use of NAT (NAT: A Tool to Prevent IPv4 Exhaustion)
  - Has its own issues and challenges…scaling issues, expensive etc.
  - We'll see more networks with few global IPv4 addresses
  - They will still use private IP and NAT

Is NAT-PT a Must?

Yes: must be supported for IPv4-only sites to communicate with IPv6-only sites

No: Everything will be dual homed or IPv4-only

- This is fine as long as v4 addresses are available
- But if they are not, this does not make sense

Permanent Mitigation for IPv4 exhaustion

Transition to IPv6

- Transition technologies include:
  - dual stack
  - tunneling mechanisms
  - Not cheap either but a permanent solution for ipv4 exhaustion issue

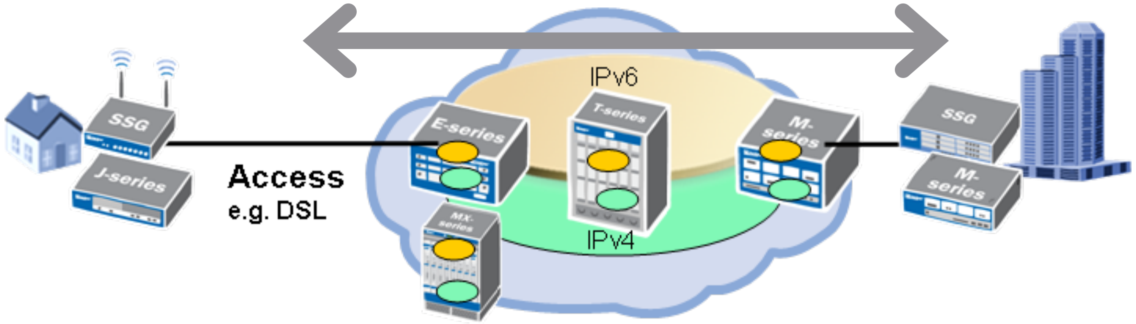
METHODOLOGIES: Core to Edge

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



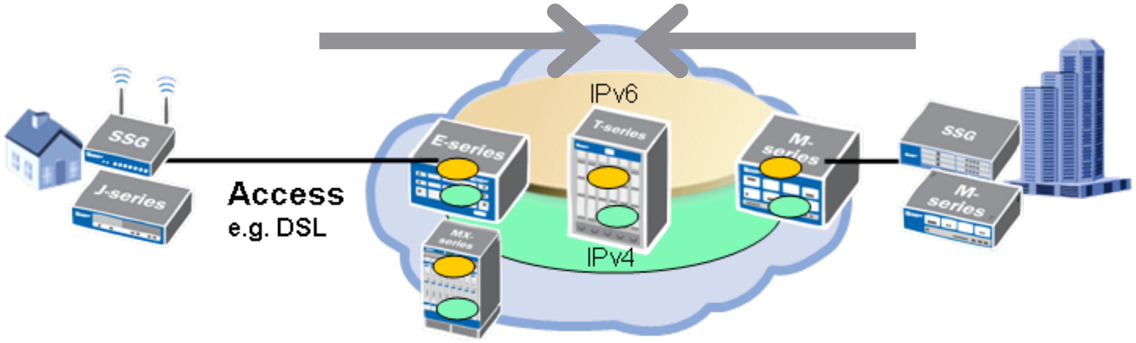
METHODOLOGIES: Edge to Core

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



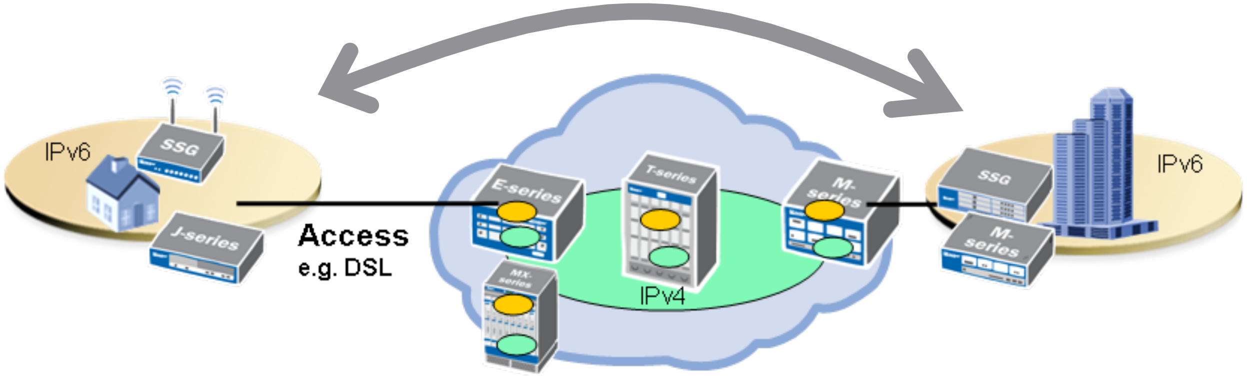
METHODOLOGIES: IPv6 ISLANDS

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



Elements of a Practical IPv6 Deployment Plan

IPv6 has specific implementation mechanisms

Relative lack of extensive experience

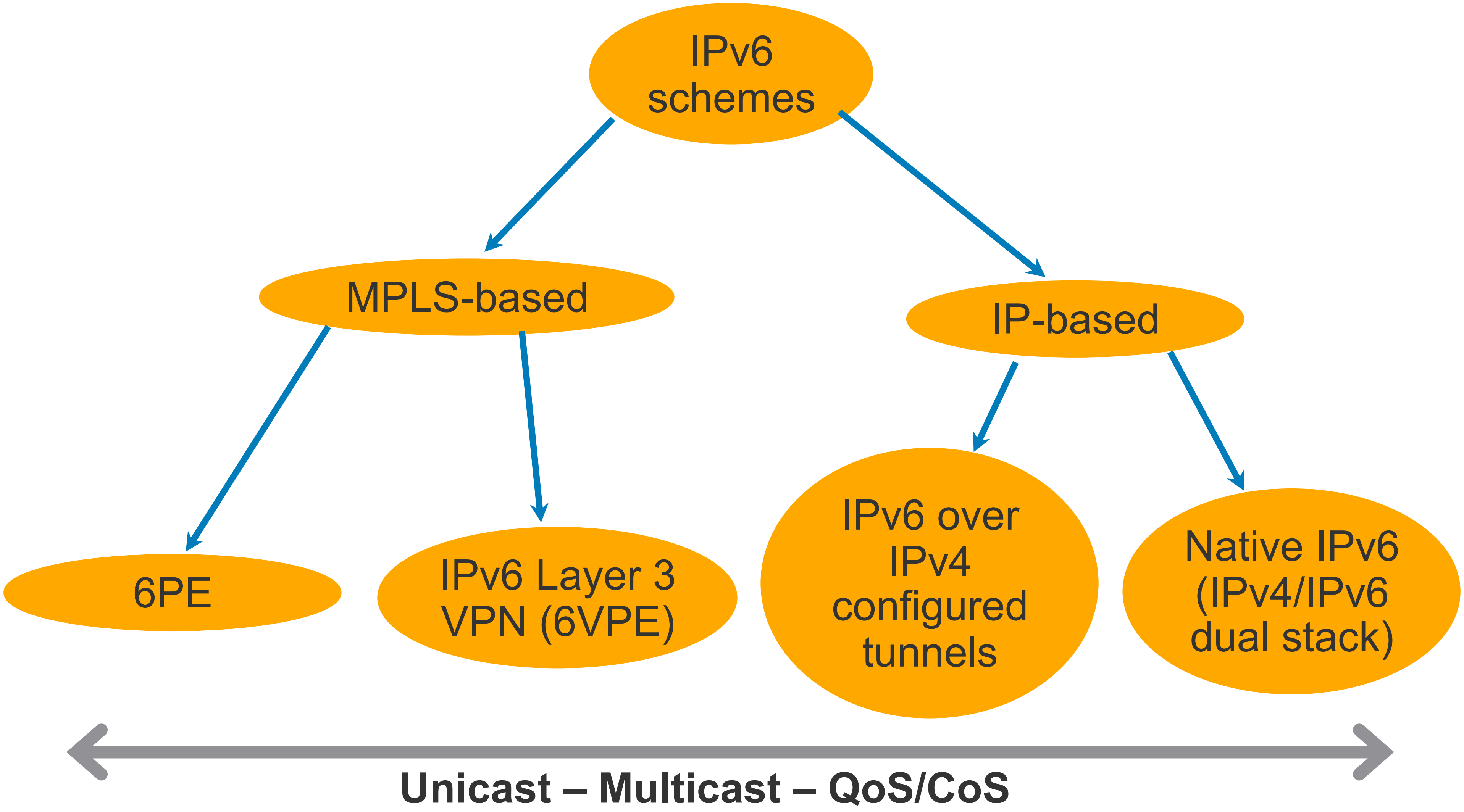
New technologies increase project risk

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

Deploying IPv6 in the Core
Various Transport Schemes

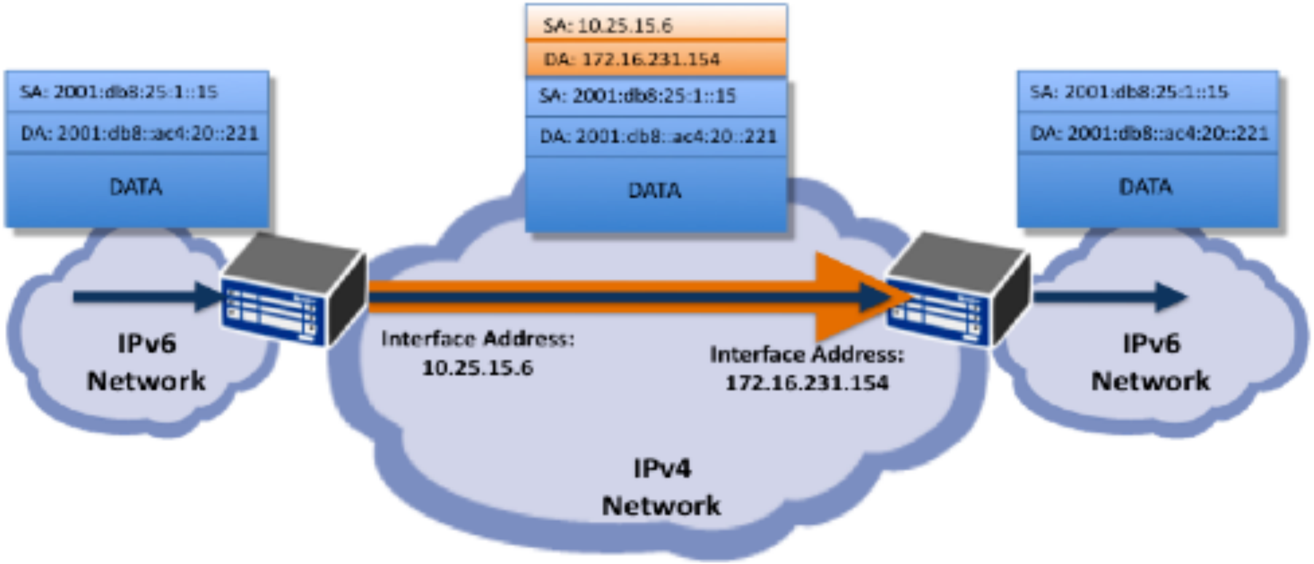

IPv6 schemes
MPLS-based
IP-based
6PE
IPv6 Layer 3 VPN (6VPE)
IPv6 over IPv4 configured tunnels
Native IPv6 (IPv4/IPv6 dual stack)

Unicast – Multicast – QoS/CoS

Manually Configured Tunnels

- Packet of one version is encapsulated in packet of other version

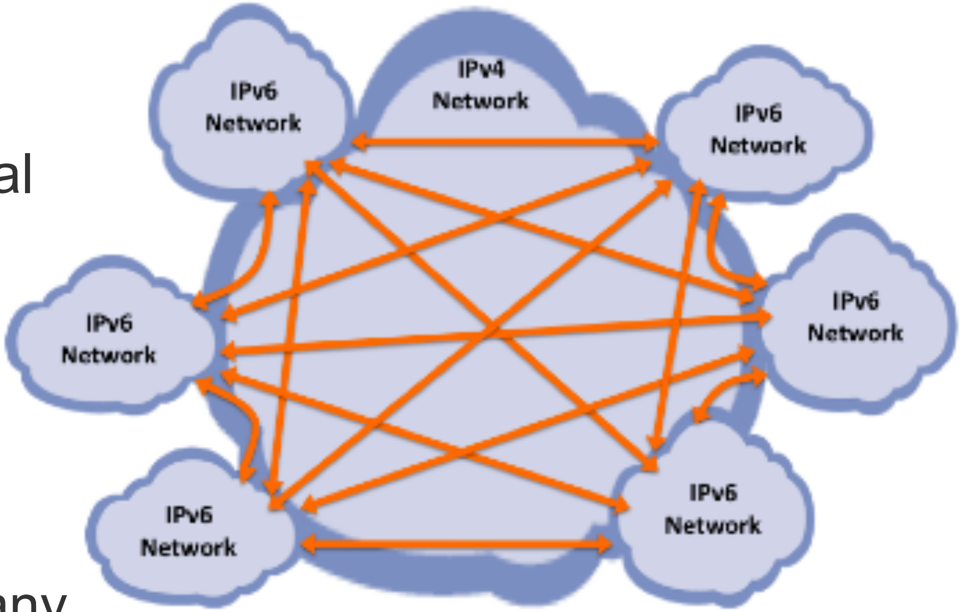
- Preferred method for interconnecting sites
  - Edge to core or interconnection through service provider networks



Manually Configured Tunnels

Pros:

- Easy to configure
- Multiple tunneling technologies available
- Most routers support most manual tunneling technologies



Cons:

- Potential scaling issues when many sites of dynamic topologies are involved

Automatic Tunnels

- **Server-based automatic tunnels:**
    - Tunnel brokers:
        - Well-known examples: Freenet6, Hurricane Electric
        - Useful for site-to-site or individual devices
        - Usually secure, can tunnel through IPv4 NATs
    - Teredo
        - Useful for individual devices
        - Can tunnel through IPv4 NATs
- **Automatic tunnels using embedded IPv4 addresses:**
        - 6to4
            - Useful for site to site
        - ISATAP
            - Useful for individual devices

MPLS and IPv6

- A type of manually configured tunnel, with auto- provisioning and signaling

- Ideal implementation mechanism for service providers
  - Most SPs already have MPLS backbones

- Provides a portfolio of IPv6 site-to-site solutions
  - Native IPv6 over MPLS tunnels (6PE - RFC 4798)
  - Layer 3 IPv6 VPNs (6VPE - RFC 4659)
  - Layer 2 point-to-point VPNs (Layer 3 agnostic)
  - Virtual Private LAN Service (VPLS)

Schemes for IPv6 over MPLS

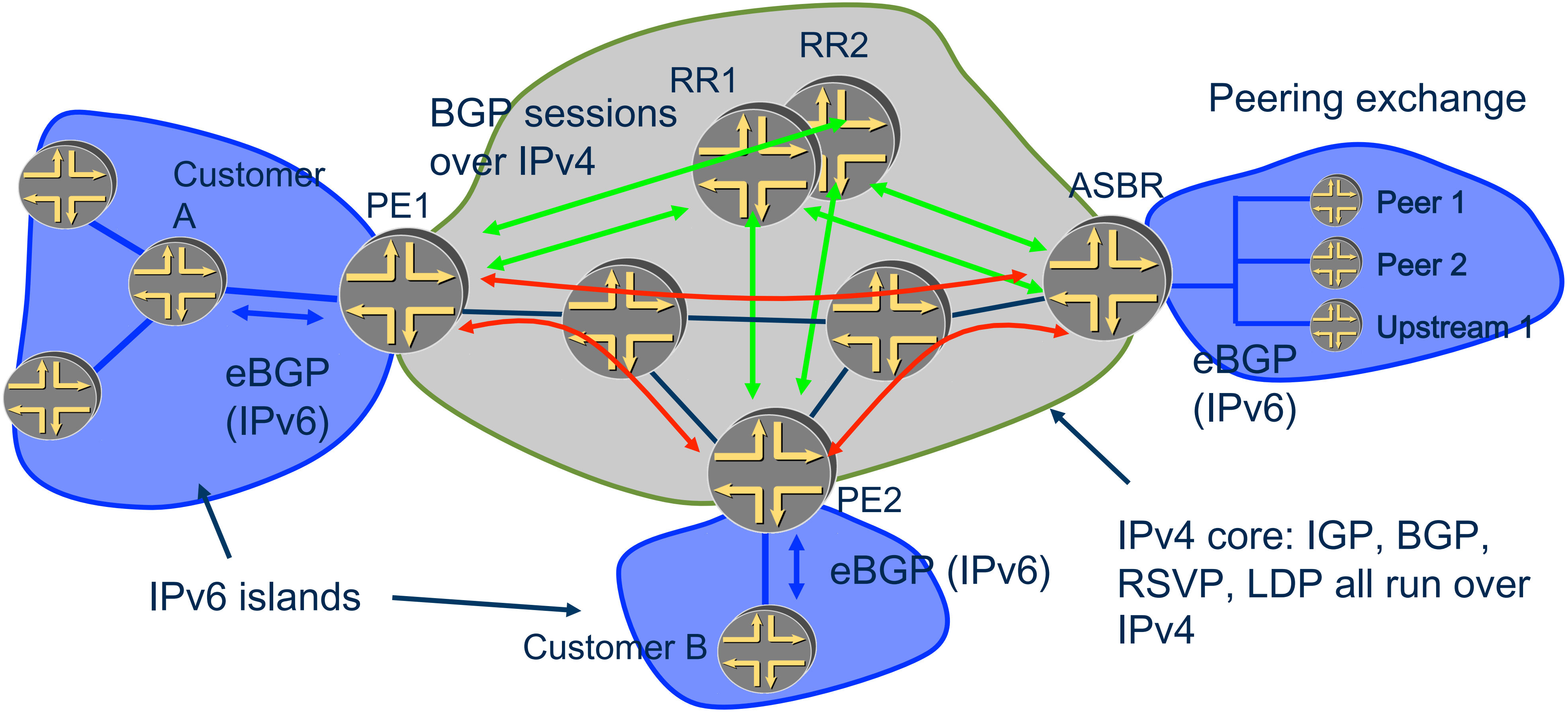
Two main schemes exist:

- 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



IPv6 islands

IPv4 core: IGP, BGP, RSVP, LDP all run over IPv4

⟷ MPLS LSPs, signalled using IPv4

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

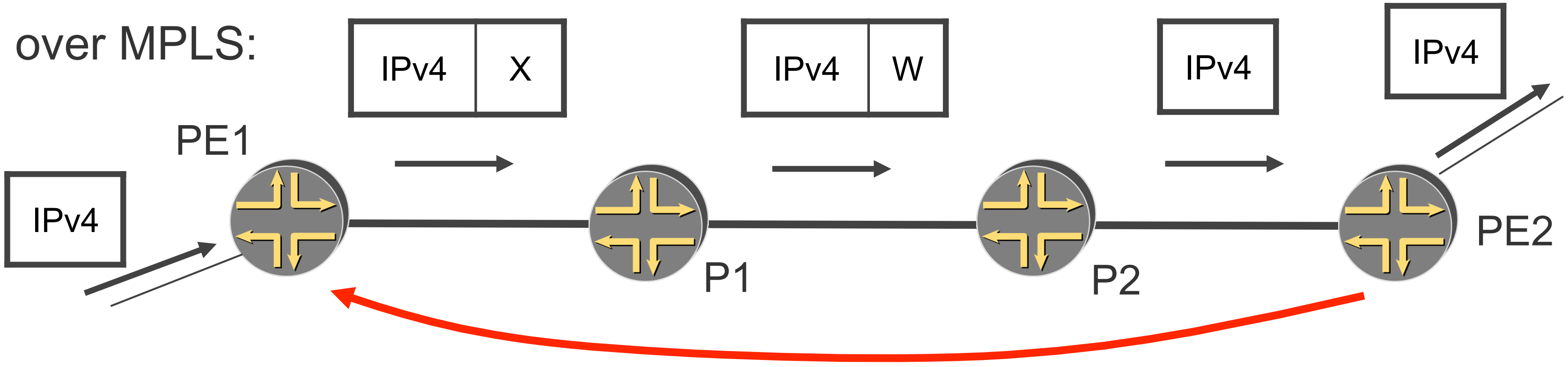
━ Links in blue have IPv6 addresses, and use an IPv6 protocol

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.

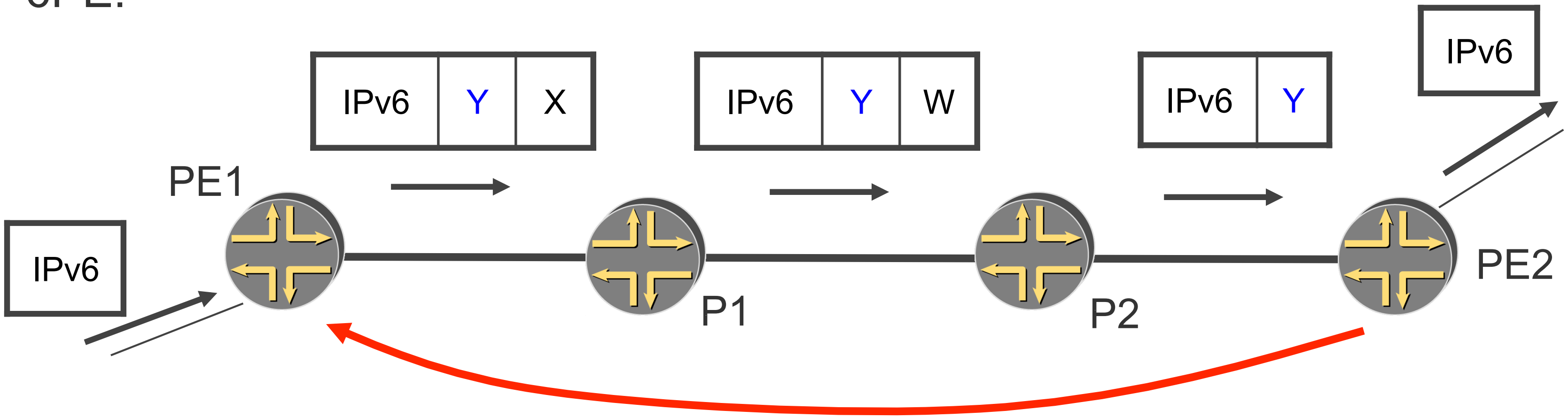
IPv4 over MPLS and IPv6 over MPLS (6PE) compared

IPv4 over MPLS:



BGP session, plain IP routes

6PE:



M-BGP session, AFI 2, SAFI 4. Labelled IPv6 Routes. Label = Y

IPv6 VPN mechanisms

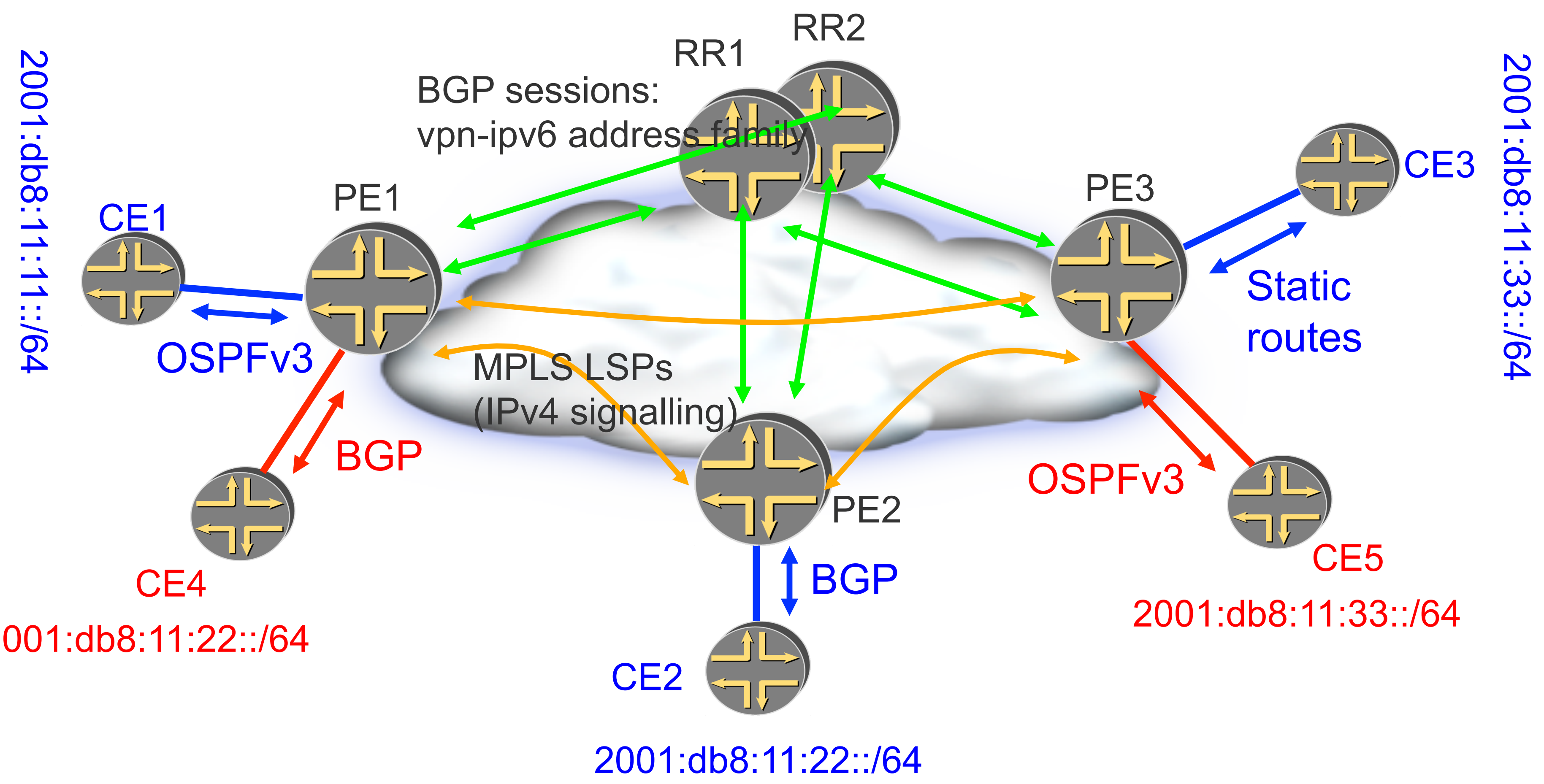
Described in RFC 4659, “BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN”

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)

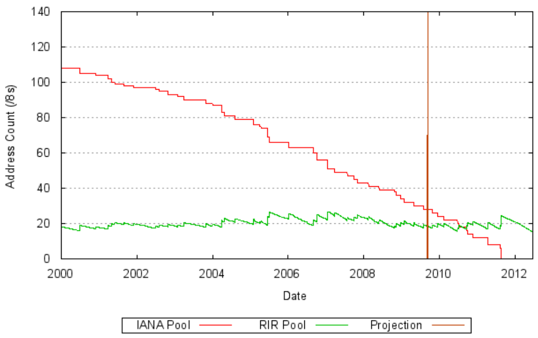
IPv6 VPN case



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)

38 Copyright © 2009 Juniper Networks, Inc. www.juniper.net

Deploying IPv6 in the Broadband Edge
Two Main Approaches



1

Maintain IPv4 paradigm as much as possible

- CPE NAT alone can not face IPv4 depletion anymore
- Solution is to add another layer of NAT: NAT444 with Carrier Grade NAT

In parallel, the recommendation is to start IPv6 implementation, and think about transition

- Translation techniques are not stabilized
- Dual stack end user service recommended

or

2

IPv6 deployment, with as a first application to spare IPv4 addresses

Translation techniques are not stabilized.

- Dual stack end user service recommended
- But DS requires same number of IPv4 and IPv6 addresses

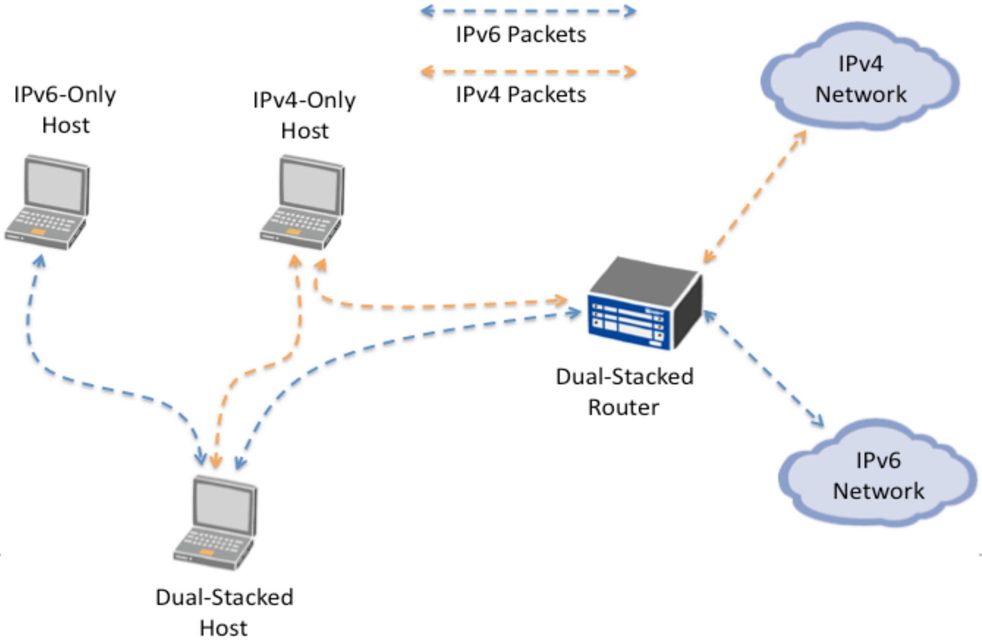
DSLite and Carrier Grade NAT offers dual stack while improving IPv4 public addresses sharing

Dual Stacks for End Users

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 Approach

Device is “bilingual”

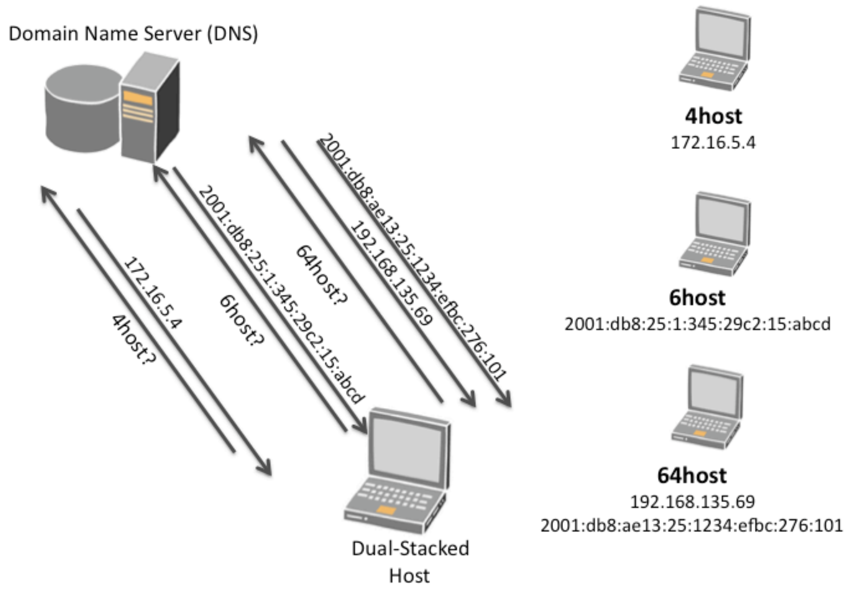
- If DNS returns IPv4 address, device speaks IPv4
- If DNS returns IPv6 address, device speaks IPv6

Pros:

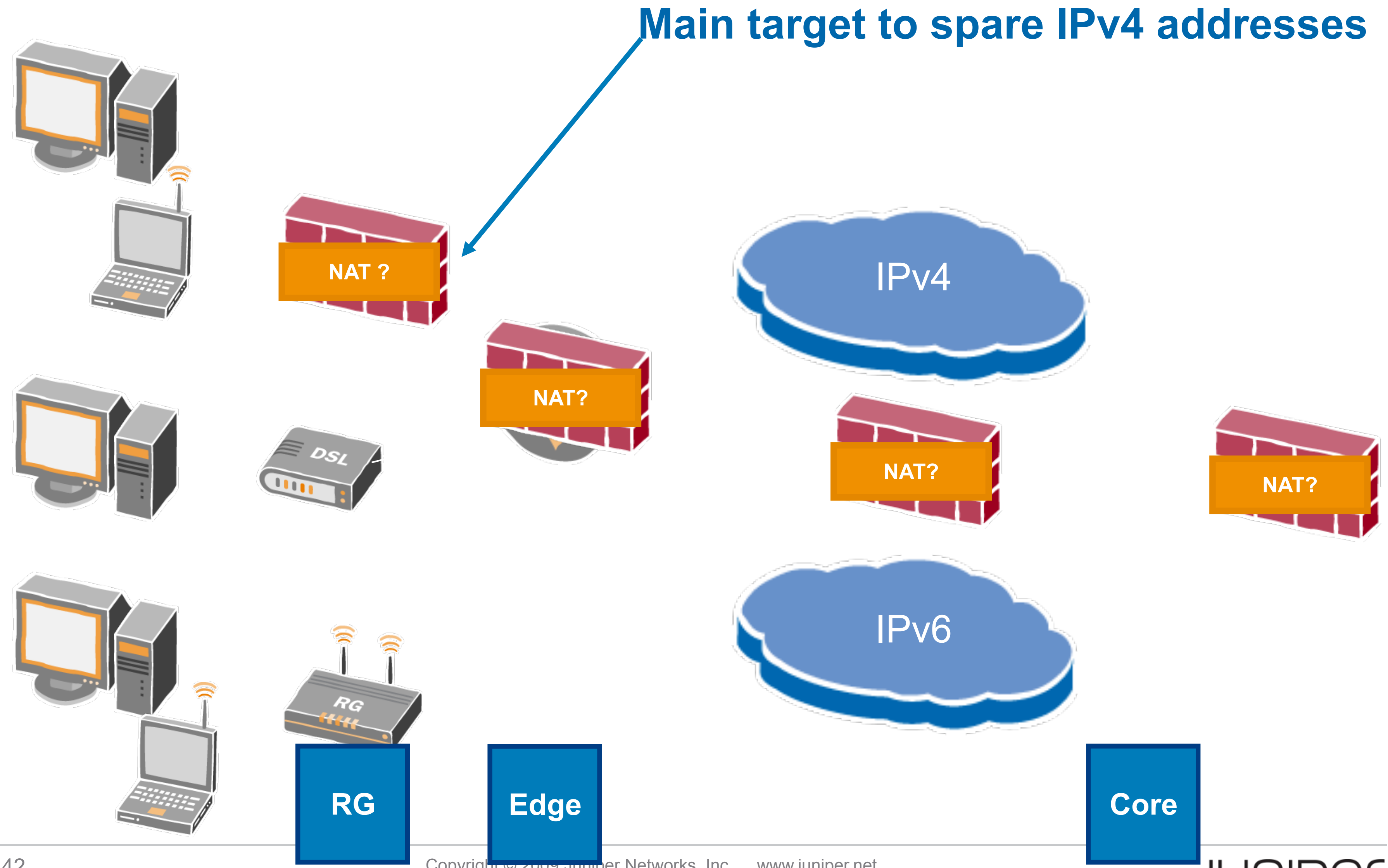
- Implementation driven by DNS
- Simplest of the implementation mechanisms

Cons:

- Requires both IPv4 and IPv6 addresses on all interfaces
- Potential for conflicts when DNS returns *both* and IPv4 and IPv6 address


Domain Name Server (DNS)
4host?
172.16.5.4
6host?
2001:db8:25:1:345:29c2:15:abcd
64host?
192.168.135.69
2001:db8:ae13:25:1234:efbc:276:101
Dual-Stacked Host
4host
172.16.5.4
6host
2001:db8:25:1:345:29c2:15:abcd
64host
192.168.135.69
2001:db8:ae13:25:1234:efbc:276:101

Possible Locations for NAT/CGN/LSN



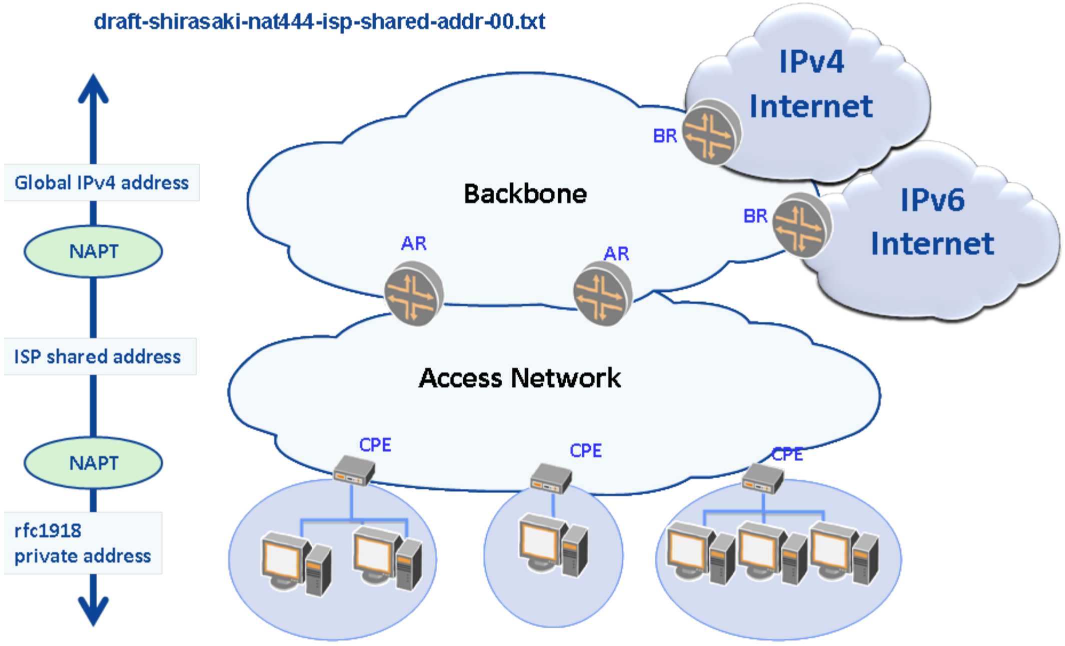
1. NAT444 - PROS/CONS

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)

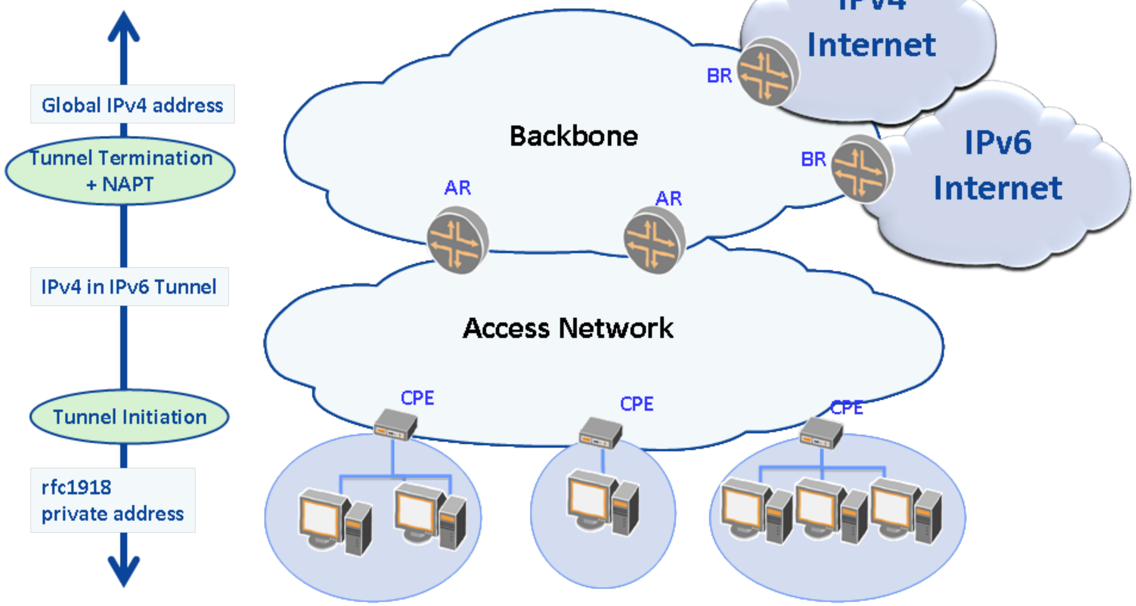
- Access Network could be IPv6-only

Cons :

- Requires CPE change

- Same concerns as NAT444 applies in terms of CGN/LSN

draft-durand-softwire-dual-stack-lite-01.txt



3. DS-LITE + A+P - PROS/CONS

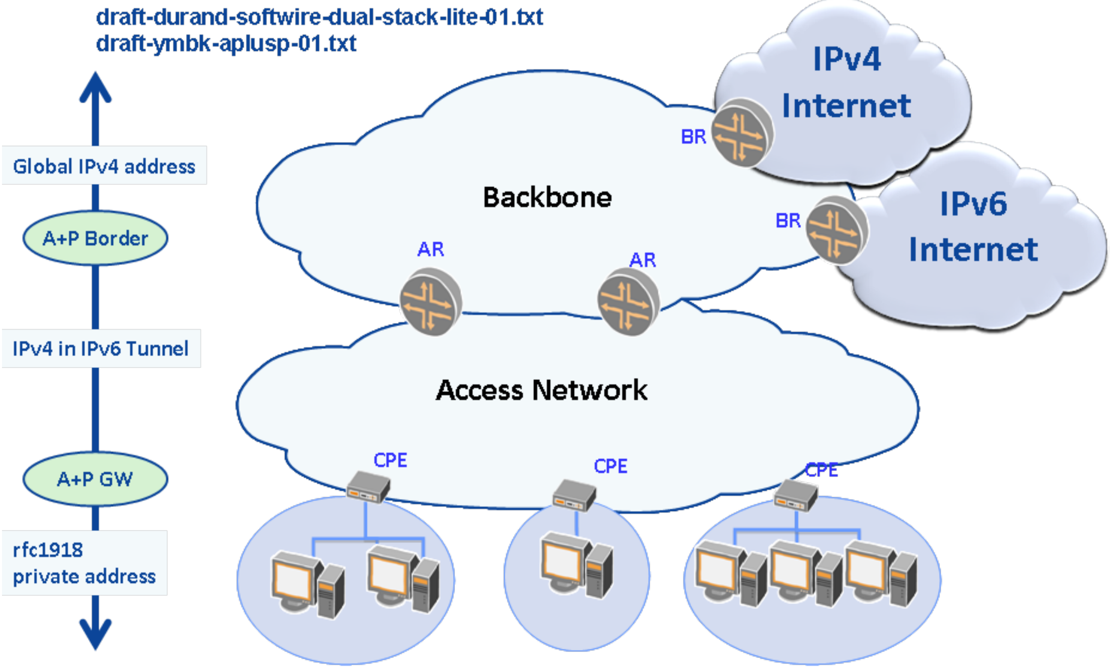
Pros :

- 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 :

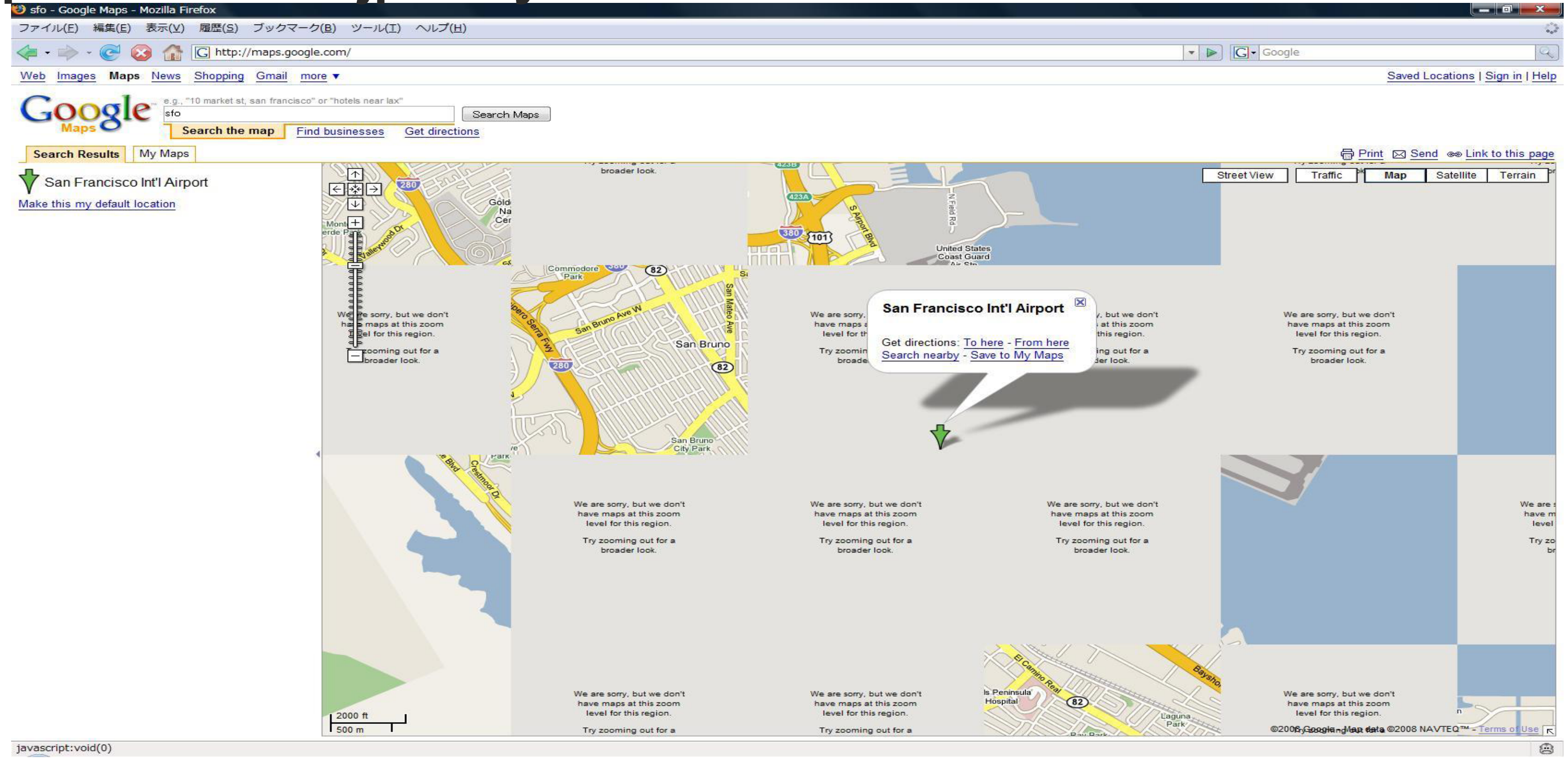
- Requires considerable CPE change
- New CPE management scheme is also needed
  (i.e. address+port assignment via DHCP)
- Brand-new technology

draft-durand-softwire-dual-stack-lite-01.txt
draft-ymbk-aplusp-01.txt



NAT SCALING (EXAMPLE WITH MAX 10 TCP SESSIONS)

http://www.nttv6.jp/~miyakawa/IETF72/


sfo - Google Maps - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
http://maps.google.com/
Google
Web Images Maps News Shopping Gmail more ▾
Saved Locations | Sign in | Help
Google Maps
e.g., "10 market st, san francisco" or "hotels near lax"
sfo
Search Maps
Search the map
Find businesses
Get directions
Search Results
My Maps
Print
Send
Link to this page
San Francisco Int'l Airport
Make this my default location
Street View
Traffic
Map
Satellite
Terrain
San Francisco Int'l Airport
Get directions: To here - From here
Search nearby - Save to My Maps
San Bruno
San Bruno Ave W
San Mateo Ave
Commodore Park
San Bruno City Park
United States Coast Guard
El Camino Real
Bayshore
Peninsula Hospital
Laguna Park
2000 ft
500 m
©2008 Google - Map data ©2008 NAVTEQ™ - Terms of Use
javascript:void(0)

We are sorry, but we don't have maps at this zoom level for this region.

Try zooming out for a broader look.

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

STANDARDS AND FORUMS

IETF:

- Significant Juniper Presence & Contributions
- For IPv6 & Transition: IPv6, IPv6 Ops, IPv4/IPv6 Translation, Behave (NAT)
- For IPv6 Routing Protocols: OSPF, BGP, Multicast, MPLS, ...
- Internet Architecture Board

BB Forum:

- Significant Juniper Presence & Contributions
- Focus on Architecture and Transport (BNG):
  - Closer to Broadband Home (RG) for IPv6 protocol and addressing development

IPv6 Forum:

- Juniper Presence & Contributions e.g. IPv6 Israel 2-3.3.09
- Many Regional Organisations

Certifications:

- IPv6 Ready (JUNOS M & T Series)
- US Federal Certification (JUNOS, Security Products)
- BB Forum does not have a certification program for BNG or RG
- Isocore Dual Stack and Migration (NAT-PT) Verification Report (Initial JUNOS Focus)
- Also see that Service Providers perform own testing, just as for IPv4

JUNIPER NETWORKS
THE PREFERRED IPv6 SUPPLIER

Juniper included IPv6 in hardware from the beginning

- First support in 2001 on JUNOS !
- 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

中国电信 CHINA TELECOM

ESnet

CNC 中国网通

KDDI

CONCLUSIONS

IPv4 exhaustion is pushing IPv6 deployment up the agenda

IPv4 depletion and IPv6 deployment can be decoupled, but a synergy seems to be the preferred approach

Carrier Grade NAT performance with feature richness is the key technology building block for the next 5+ years

IPv6 deployment is happening worldwide

Planning now is essential

everywhere