IPv6 Deployment

Issues and Examples of IPv6 Deployment

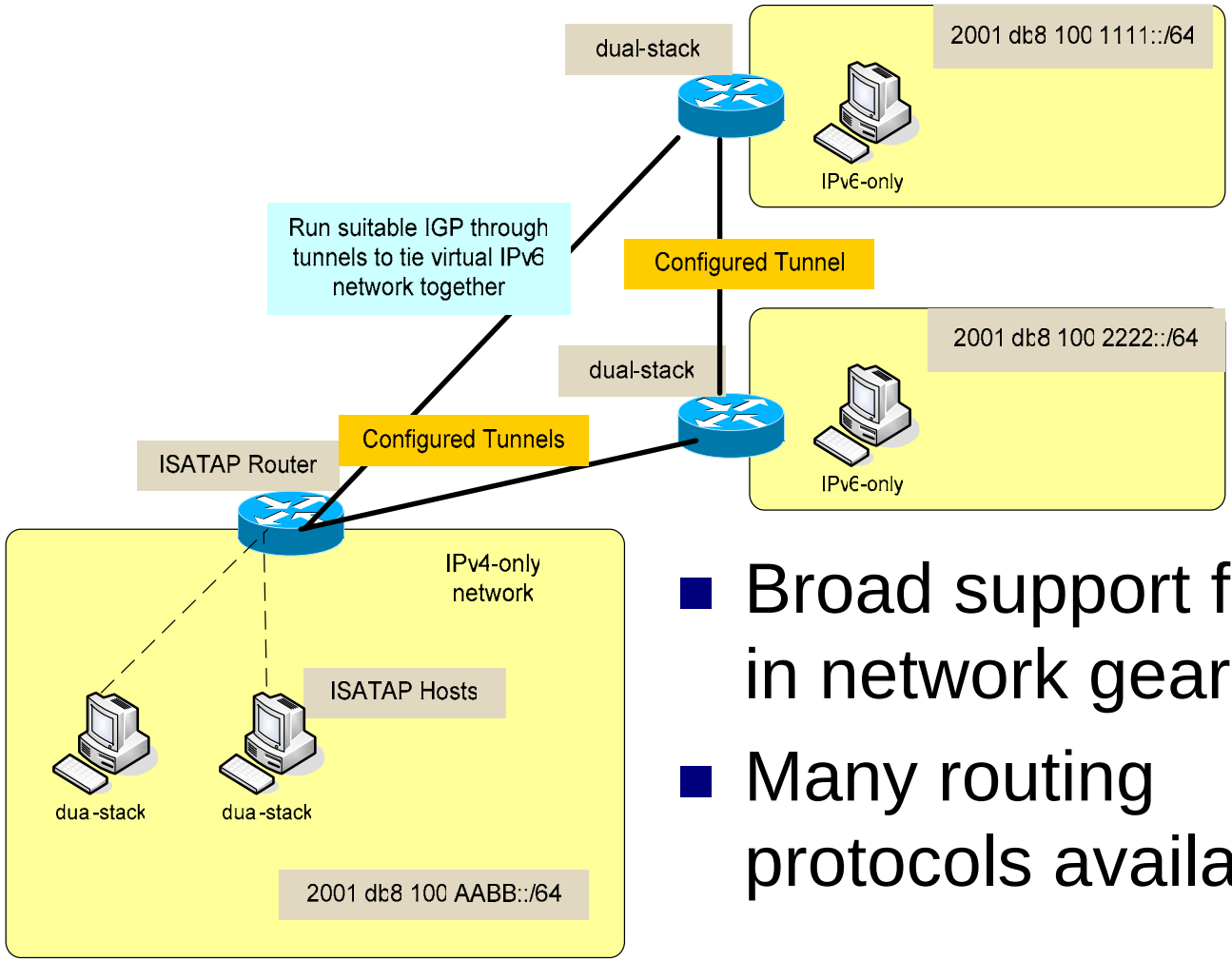
by Yurie Rich
Business Director, NAv6TF
President, Native6, Inc.

Presentation Agenda

- Who am I?
- Network Infrastructure
- DNS/DHCP
- Services
- Custom Applications
- Connecting to the IPv6 Internet
- Address Allocation
- Security
- Examples

Native6 Inc.

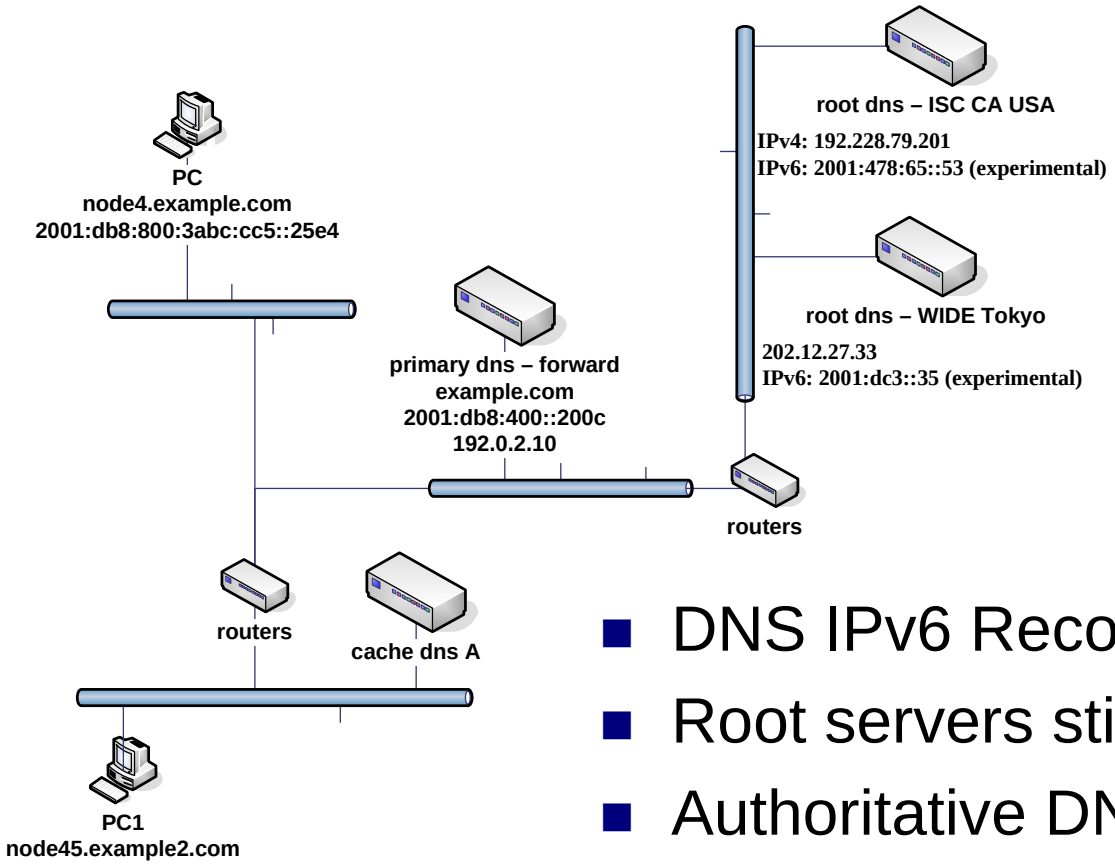
Network Infrastructure



- Broad support for IPv6 in network gear
- Many routing protocols available

Native6 Inc.

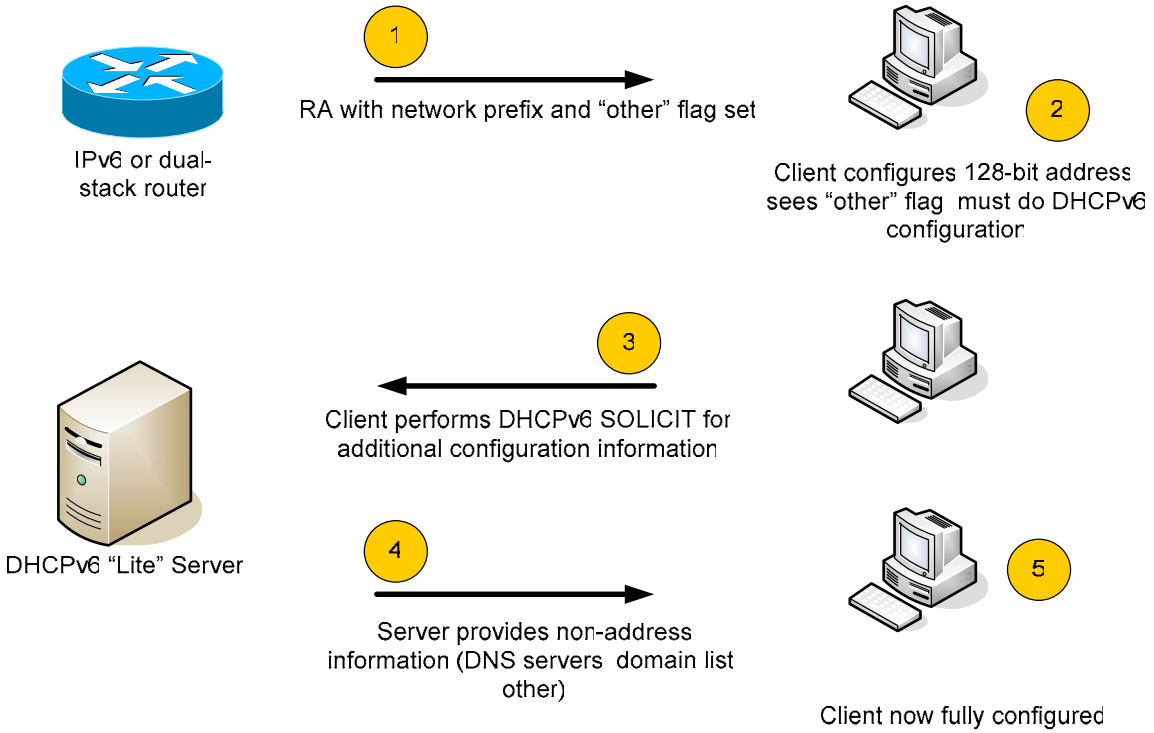
DNS



- DNS IPv6 Records well-supported
- Root servers still IPv4-only
- Authoritative DNS almost all IPv4
- Peer-to-peer will drive DDNS

Native6 Inc.

DHCPv6

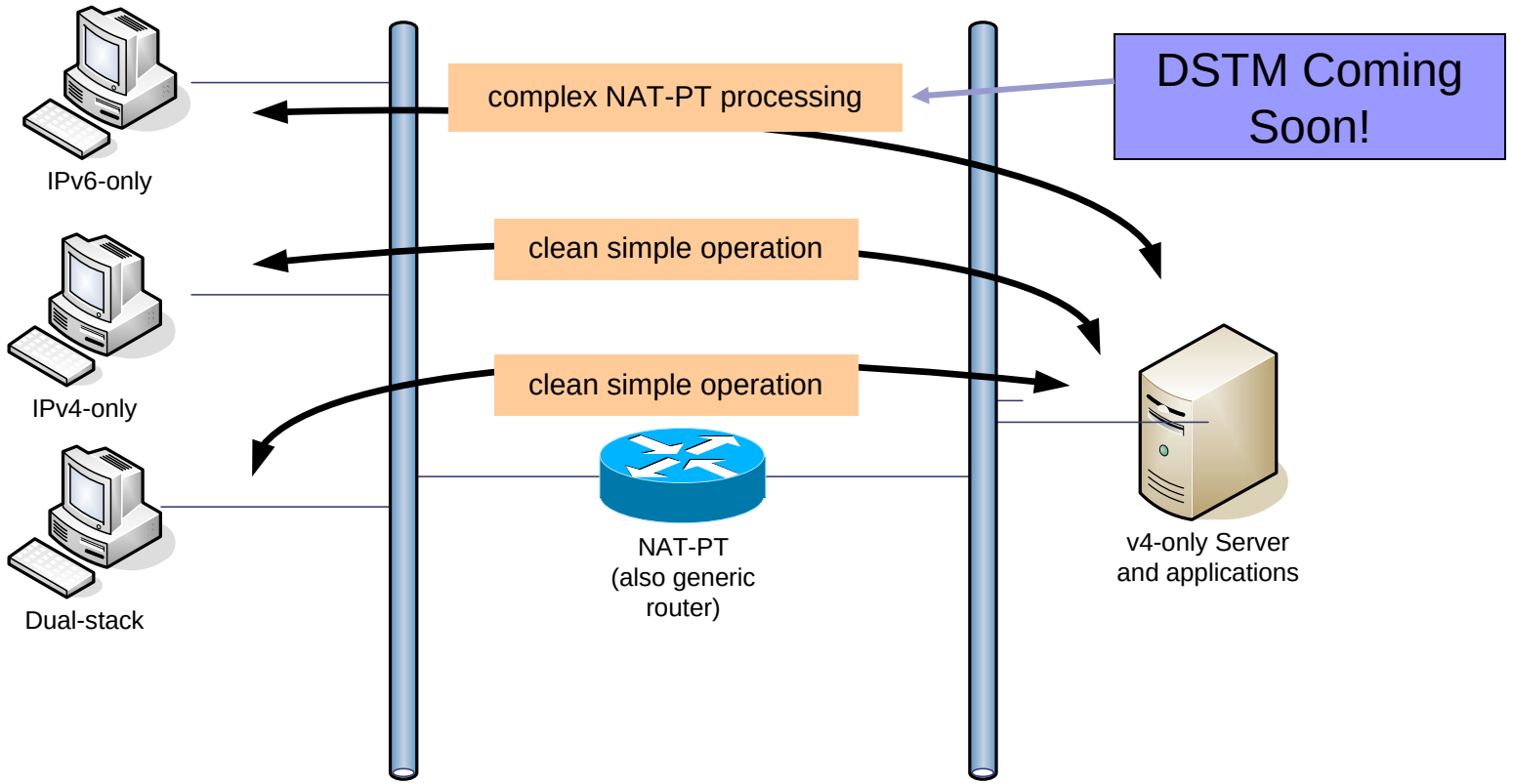


- DHCPv6 solutions still new
- "stateless" DHCPv6 useful in combination with stateless autoconfiguration
- Enterprises may gravitate to DHCPv6 due to comfort factor

Services

- Few services ready today
- Apache on Unix “poster child” for mature solution
- Microsoft IISv6 IPv6-capable
- Support for “complementary tools” patchy
- Many things that can be done (fetch IMAP mail over IPv6 with non-Microsoft clients) are more technology demonstration than products ready for deployment

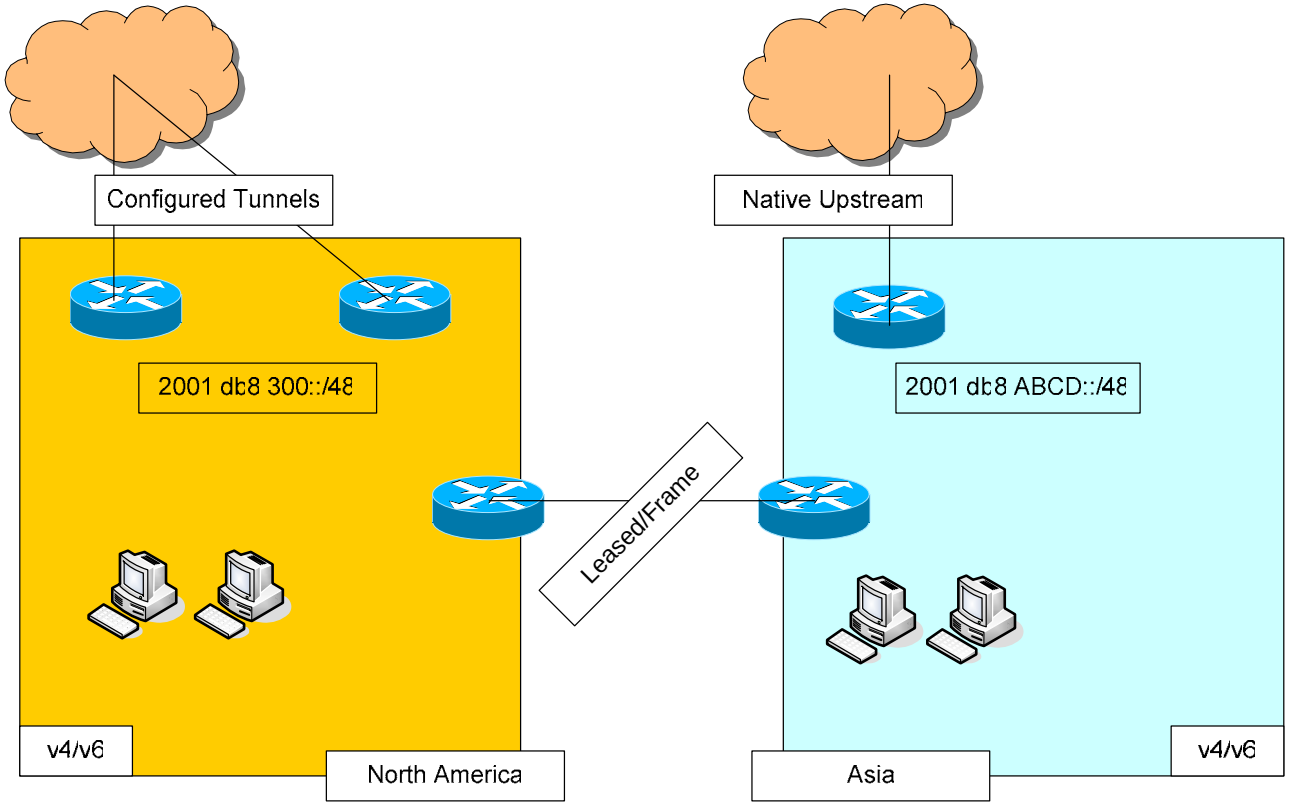
Custom Applications



- Most cases dual-stack clients will be better than NAT-PT
- Some applications will port to IPv6/IPv4 easily

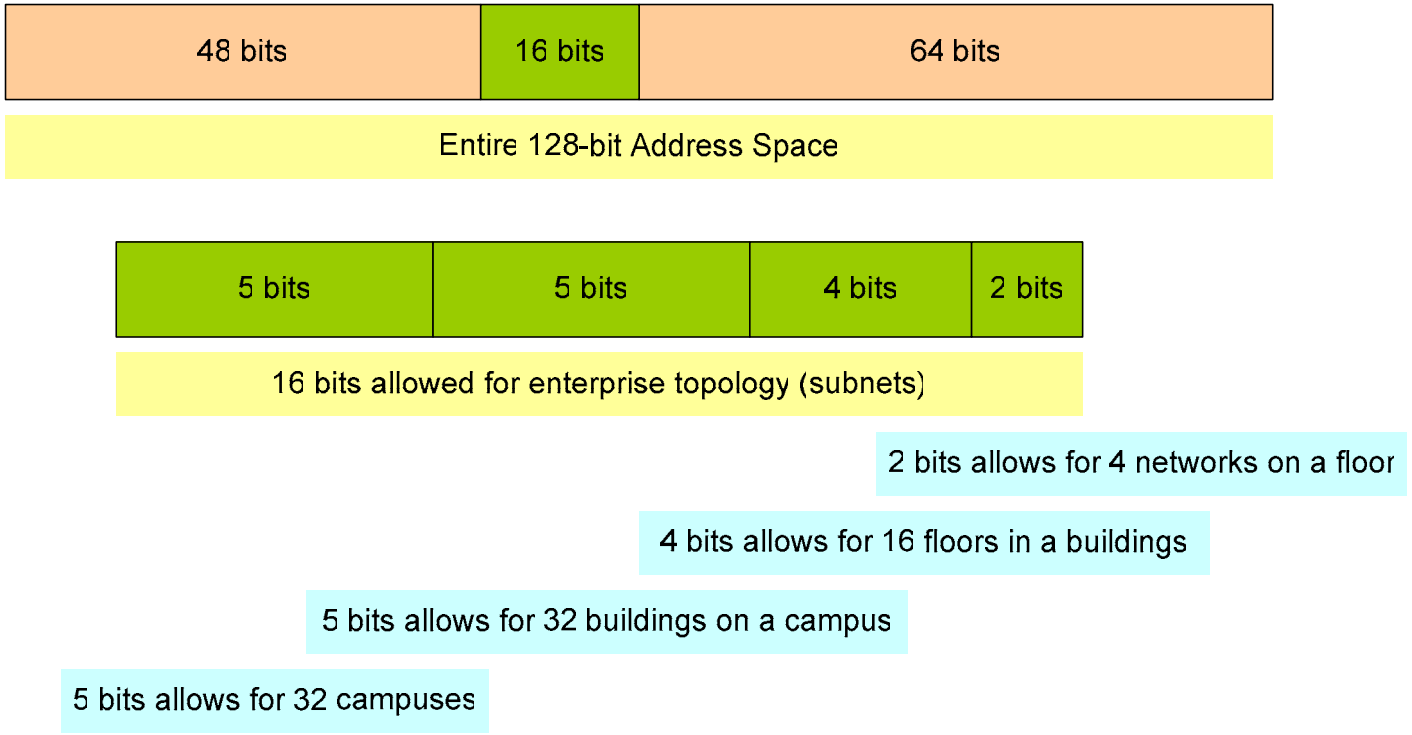
Native6 Inc.

Connectivity to the Internet



- Many choices for connectivity today
- Early deployments can use tunnel to gain experience
- Multihoming still an important issue to be resolved

/48 allocations

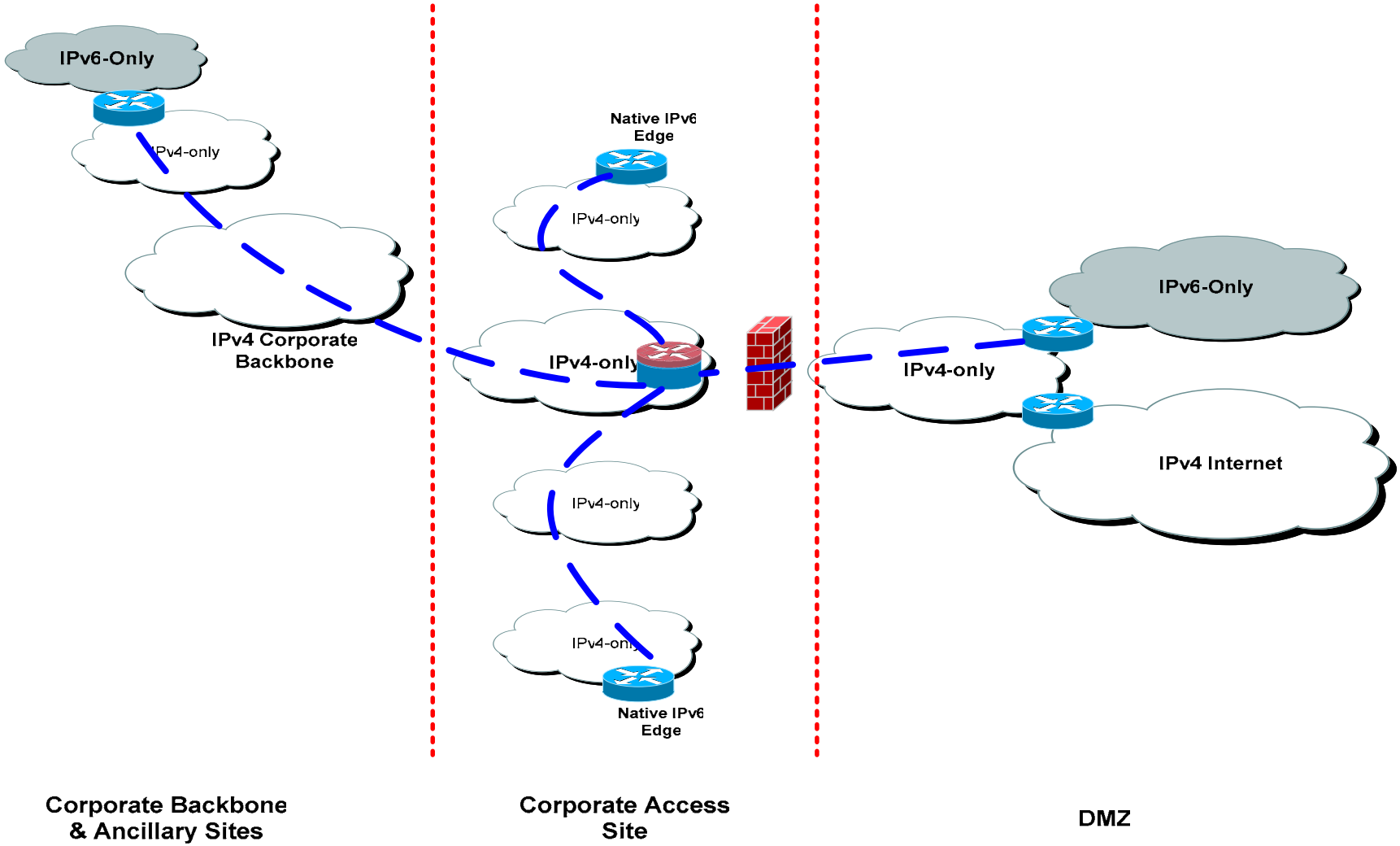


- 16 bit topology goes fast for a large growing organization
- Poor deployment planning will lead to renumbering
- Multiple /48 allocations will be common for large enterprise

Security

- Tunneled traffic difficult to inspect and control
- IPsec tunnels are completely opaque to edge-based firewalls
  - use distributed firewalls for IPsec peers talking to un-trusted external peers
- Teredo is based on defeat of (weak) NAT protections – understand how this mechanism works
- IPsec deployment will still lack without PKI and widespread alternatives to manual keying
- ICMP rate-limiting should replace ICMP-packet dropping at network edge

IPv6 Enterprise Deployment



IPv6 Enterprise Deployment

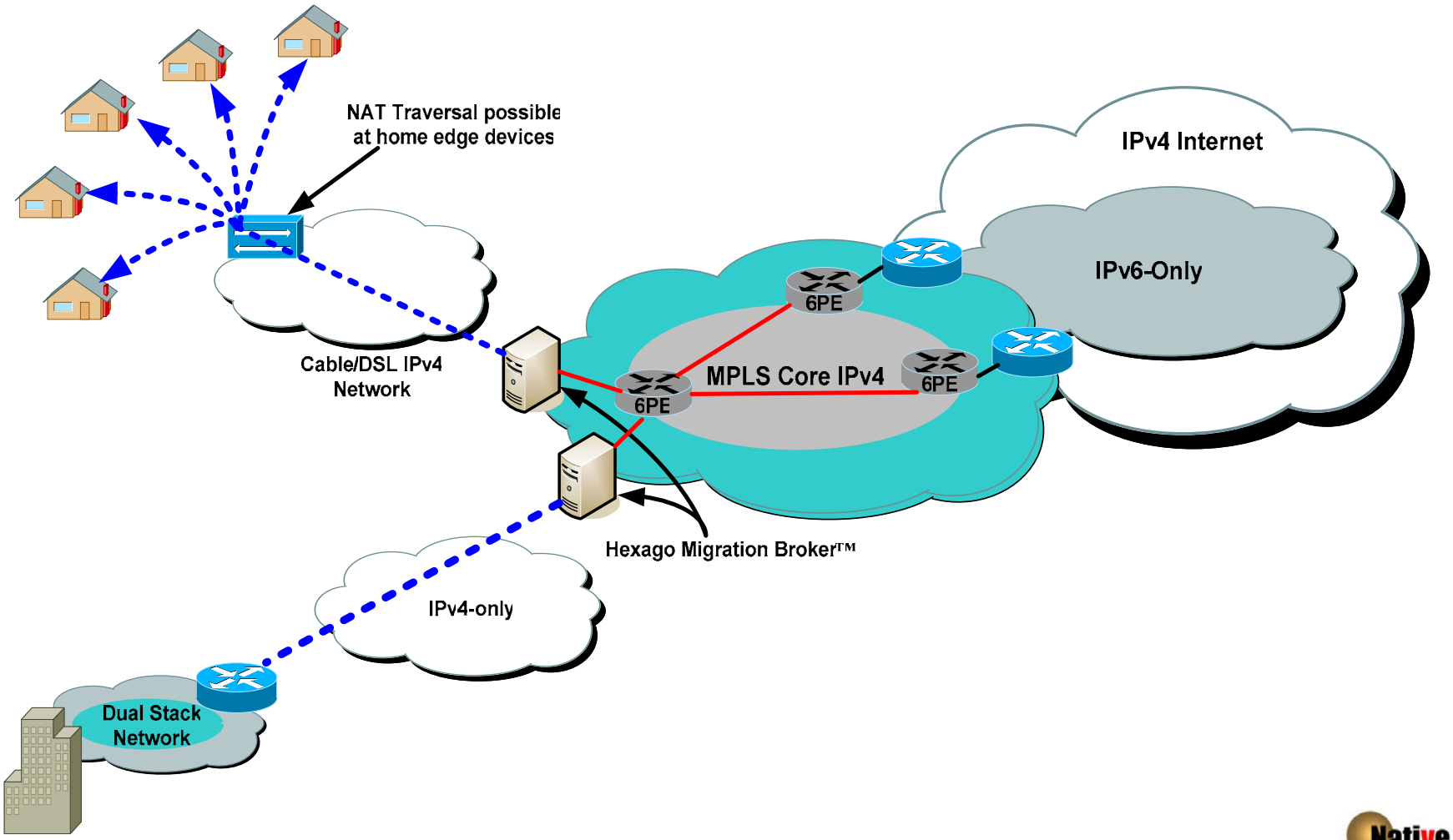
- Addressing
  - Secured a /32 block for global deployment
  - Proposing to break up and work with upstream to advertise smaller allocations
  - Looking for multihoming solution
- DNS
  - manually supporting IPv6 records but over v4 transport
- Routing
  - use EIGRP for v4 network and wishes to do so with IPv6
  - in interim, using RIPng since size of IPv6 network is small, its easy to configure, and minimal route convergence issues

IPv6 Enterprise Deployment

- Connectivity & Transition
  - Native IPv6 upstream provider(s)
  - Use mainly manually configured tunnels internally
  - May utilize ISATAP in some locations with centralized ISATAP servers.
- Security
  - Stateless ACL for traffic filtering
  - Force v6 traffic through major v6 ingress/egress points – through DMZ
  - Strict guidelines regarding IP protocol 41, UDP traffic at remote sites with Internet access
- Host Implementation
  - Dual Stack hosts. Widespread deployment will be incumbent on applications w/ v6 support, OS with robust stack

Native6 Inc.

Service Provider IPv6 Deployment



Service Provider IPv6 Deployment

- Addressing
  - Service provider has a /32 allocation from the their RIR
  - Migration Broker (MB) has a /38 or /39 from which is allocates /48 to enterprises
  - Individual nodes (mobile nodes) can maintain a static IPv6 address
- DNS
  - Service provider supports IPv6 records over v4 transport
  - Enterprises deploying are responsible for internal IPv6 DNS support, if needed.
  - MB can update the DNS servers
- Routing
  - No routing occurs between the MB and the Enterprise gateway, nor between the MB and the 6PE router.
  - Default routes established via static routes
  - 6PE routes on MPLS network via MP-iBGP

Native6 Inc.

Service Provider IPv6 Deployment

- Connectivity & Transition
  - “Native” connection to IPv6 Internet at exchange point
  - MPLS network ignorant of IPv6, use 6PE to make v6 connection across MPLS core
  - Migration broker establishes IPv6-in-IPv4 tunnel over v4 infrastructure
- Security
  - Migration broker will not forward packets that are not from allocations it is servicing, will not forward spoofed packets
- Host Implementation
  - Enterprise end users can connect natively using a dual stacked host, or via some TM like ISATAP.
  - Mobile users must have a dual stacked client in addition to the TSP client software installed.

Native6 Inc.

Questions

Thank you for your time

yrich@native6.com

www.native6.com