Qwest
Spirit of Service

IPv6 Meeting the Looming Transition Deadline and related issues

Dr. Wesley K. Kaplow
Chief Technology Officer
Qwest Government Services

wesley.kaplow@qwest.com
703-293-6936

December 12, 2007

About Qwest Government Services

- Serving the federal government for over 100 years through our telecommunications heritage in the Bell System
- Over 400 employees located across the country
- Broad employee experience base: AT&T, Bell Atlantic, Broadwing, MCI, Sprint, US WEST, Verizon, military, government
- Headquarters at 4250 N. Fairfax Drive in Arlington, Virginia
  - Other key locations:
    - Atlanta, Denver, Los Alamos, Northern Virginia, Maryland, Oak Ridge, Seattle
- Provides innovative solutions for Civilian agencies and the DoD
- Self-sufficient business unit with sales, engineering, and operations functions
- #41 on 2006 Washington Technology Top 100 Federal Prime Contractors

Qwest
Spirit of Service

And you think IPv6 is a problem…

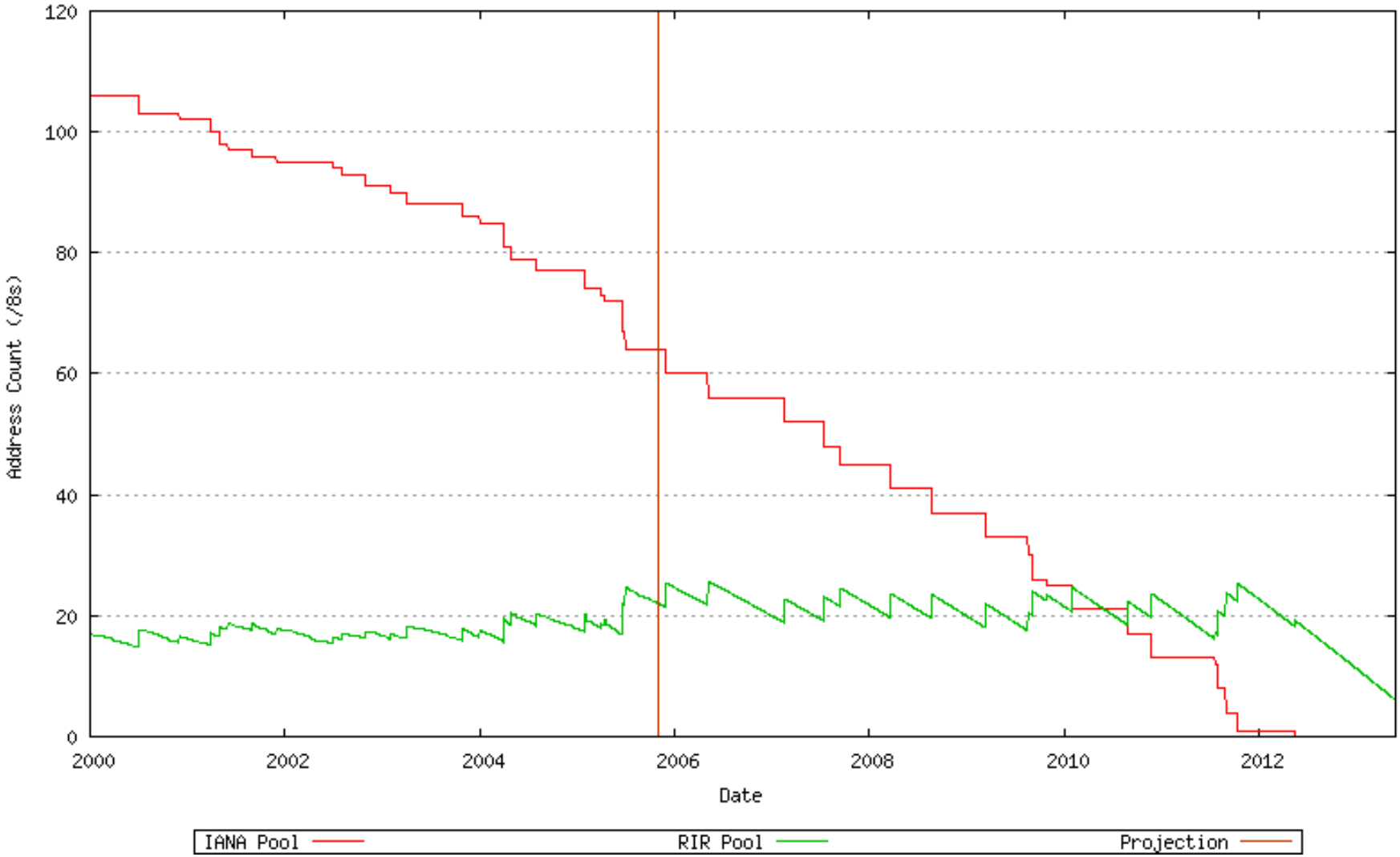
Qwest
Spirit of Service

So what do we hear about IPv6?

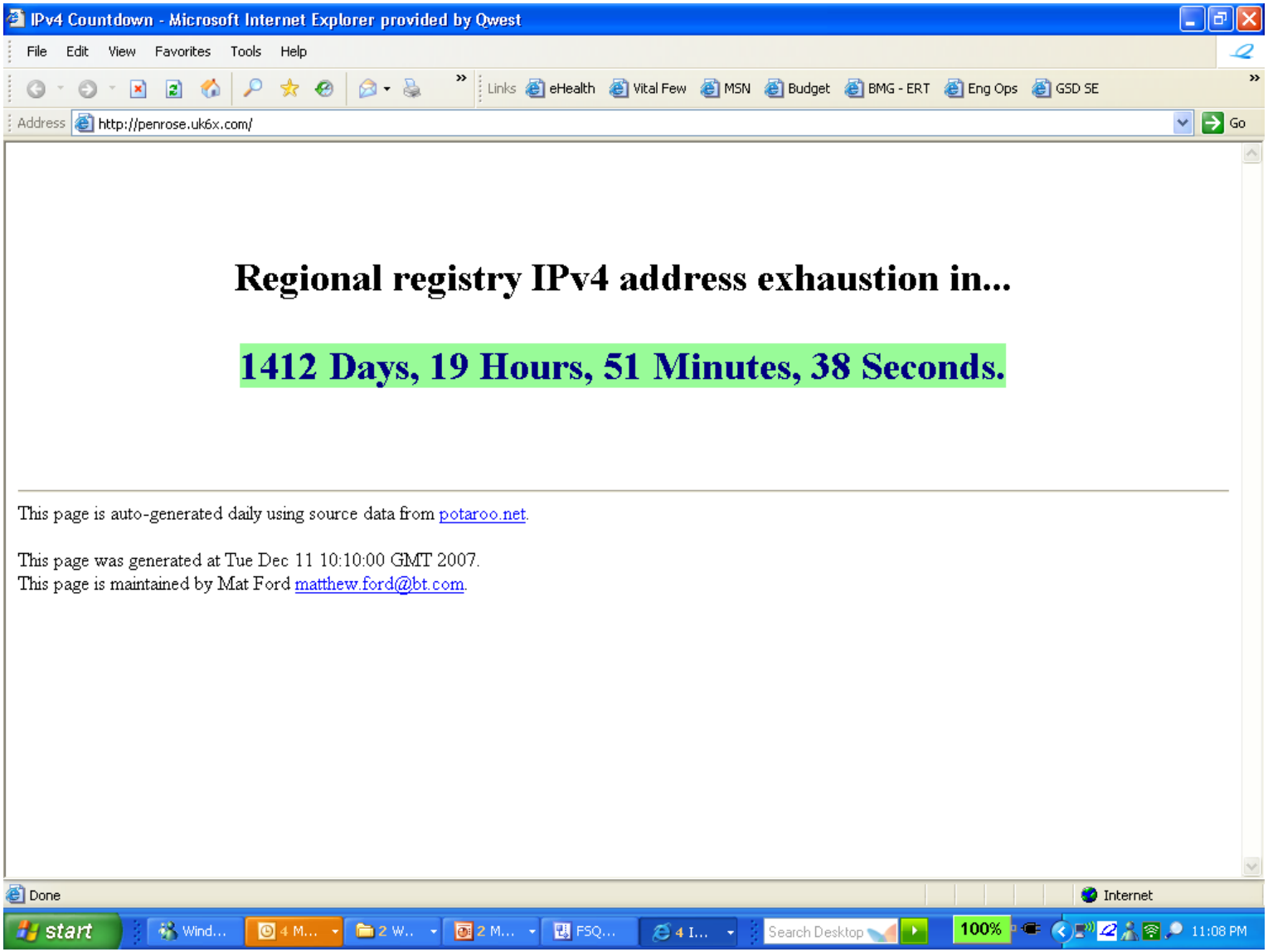
- We're running out of IPv4 address space
- It's got Class of Service
- It's easier to configure
- Improves security
- OMB has you in their sights

It's got you nervous about what to do…

We are running out of unassigned address space!



There's even an BLEEPING countdown clock…



Resolution from ARIN

- **WHEREAS**, community access to Internet Protocol (IP) numbering Resources has proved essential to the successful growth of the Internet; and,
- **WHEREAS**, ongoing community access to Internet Protocol version 4 (IPv4) numbering resources can not be assured indefinitely; and,
- **WHEREAS**, Internet Protocol version 6 (IPv6) numbering resources are available and suitable for many Internet applications,
- **BE IT RESOLVED**, that this Board of Trustees hereby advises the Internet community that migration to IPv6 numbering resources is necessary for any applications which require ongoing availability from ARIN of contiguous IP numbering resources; and,
- **BE IT ORDERED**, that this Board of Trustees hereby directs ARIN staff to take any and all measures necessary to assure veracity of applications to ARIN for IPv4 numbering resources; and,
- **BE IT RESOLVED, that this Board of Trustees hereby requests the ARIN Advisory Council to consider Internet Numbering Resource Policy changes advisable to encourage migration to IPv6 numbering resources where possible**.

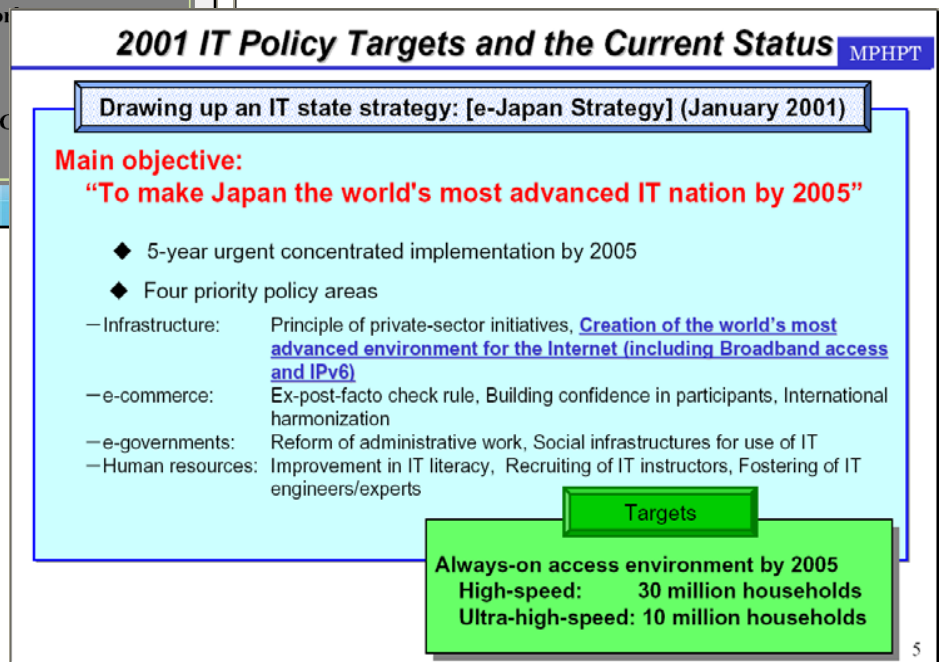
Unanimously passed by the ARIN Board of Trustees May 7, 2007

It's a national strategic direction in Asia

The Stand of IPv6 in China

- The push to national manufacturing's development, realize informationlization induct industrialization
- Own kernel technique and intellectual property
- Supervision and regulation of telecom network, so it can serve nation, society and people better.
- NGN and NGI together

China Academy of Telecommunication Research



Qwest
Spirit of Service

In case you are confused, IPv6 is really all about the address space…

- Driving force is IPv4 address space exhaustion
  - Based on recent ARIN announcement – IPv4 addresses will be exhausted by 2012-2013
  - (http://www.arin.net/announcements/20070521.html)
- End-to-end communication
  - All hosts 'can' be globally reachable – Everything reachable
    - Cell phones, PDA's, Home Area Networks (HANs), Automobiles, vending machines, more
- IPv4 addresses are 32-bit; 2^{32} = 4,294,967,296 (4.2 billion) addresses.
  - Not even one address per person on Earth!
- IPv6 is 128-bit; 2^{128} = 340,282,366,920,938,000,000,000,000,000,000,000, 000 (340 undecillion) addresses
  - To put in perspective, a 128 bit address provides for:

Approximately 50 octillion addresses for each of the roughly 6.5 billion people alive on Earth today!

Qwest
Spirit of Service

But, in the immortal words of the Hitch Hiker's Guide to the Galaxy

DON'T PANIC

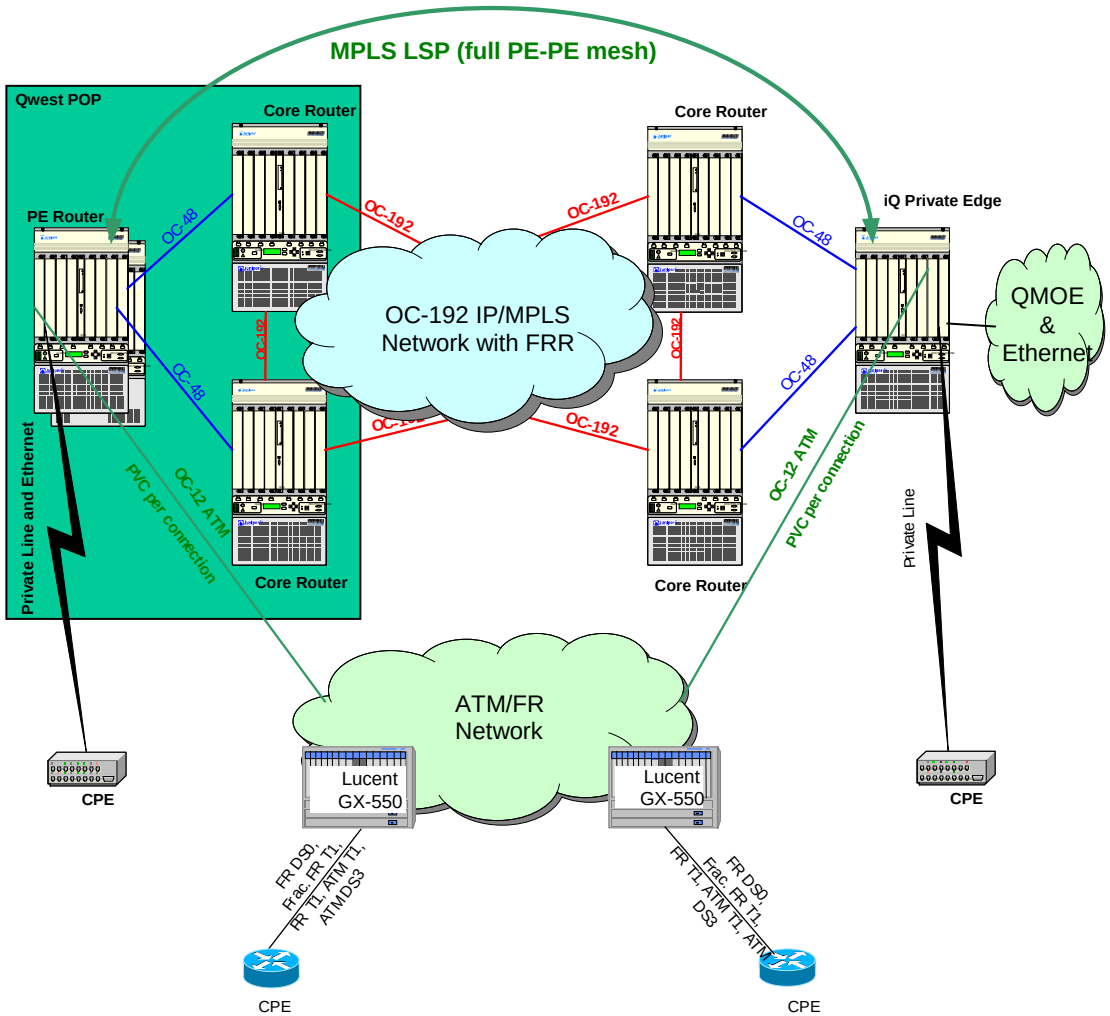
Qwest
Spirit of Service

Why should you not panic?

- Carriers are preparing
  - And have or will have IPv6 capable MPLS and Internet services by 1Q2008
- Operating Systems are preparing
  - Vista is IPv6 capable now
  - Linux-based IPv6 available as well
- Router and appliance vendors are preparing
  - The likely candidates have IPv6 versions of their routers

But, still be very concerned

A brief technical view of a carrier's IP network

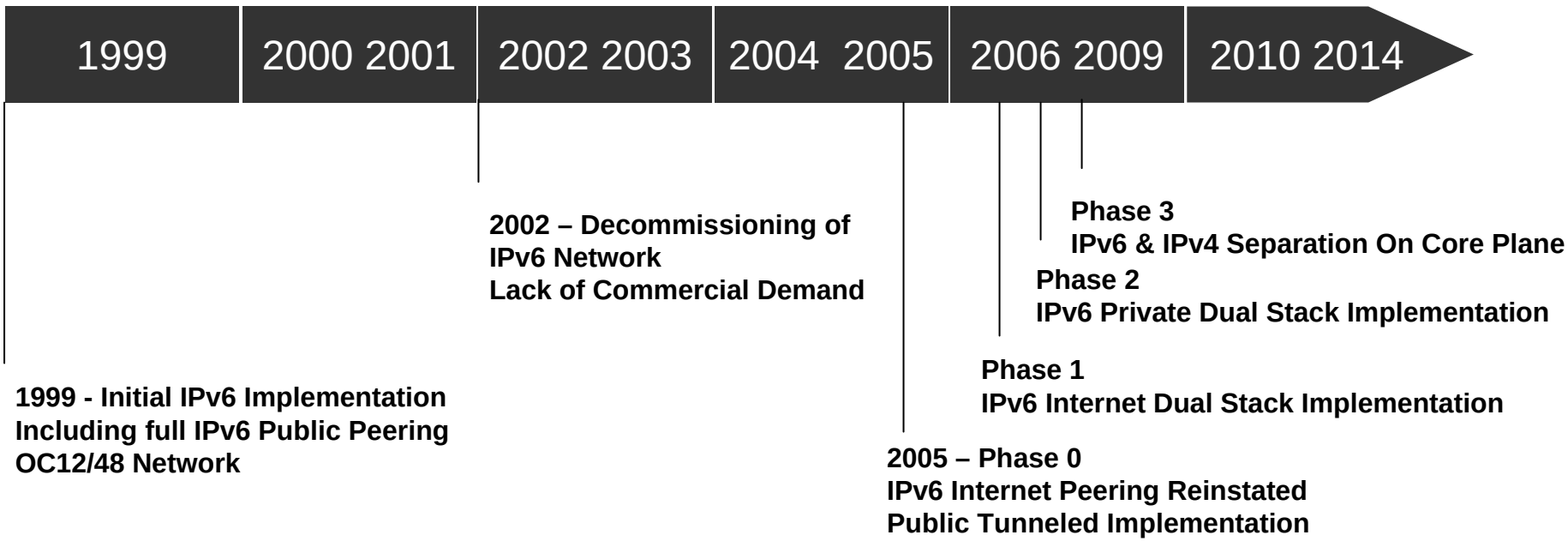


- Layer 3 ports are provisioned to private edge routers and utilize the RFC 4364 (was RFC 2547bis) MPLS based Layer 3 virtual private network (VPN) functionality.
- Layer 2 ports are provisioned to private routers and use H-VPLS for learned Ethernet Bridging and Ethernet Multicast
- Private edge routers are completely isolated from the Internet and do not carry Internet routes.
- Private edge routers are capable of terminating both FR/ATM, Ethernet, and Private Line access.
- Complete isolation between customer route instances via use of virtual route forwarding (VRF).
- Implementation of RSVP-TE to ensure MPLS VPN traffic has higher priority than other traffic
- Strict capacity planning ensures that all traffic failure modes do not impact 100% packet delivery performance

Qwest IPv6 Development & Implementation Timelines

Qwest IPv6 Implementation Timelines – A Phased Approach

- Phase 0 – Addition of Internet Peering Routers
- Phase 1 – Internet Network Dual-Stack Implementation
- Phase 2 – Implementation of IPv6 within Private IP Environment
- Phase 3 – Implementation of IPv6 & IPv4 Separation on Core Plane



What to do…

- Get your inventory together
  - Leverage your Networx transition inventory
  - Private and public IP address spaces
  - Router hardware and software versions
  - Ethernet hardware and software
  - Desktop machines
  - Printers and other IP-enabled devices on the network
  - Firewalls and other security devices
  - Network and security management software
- Determine the upgrade approach for each component
- Determine the criticality of the service being performed by the component
  - Need to understand the severity of the impact if something goes wrong

Qwest
Spirit of Service

and more…

- Develop an Internet Strategy
  - Maintain both an IPv4 and IPv6 presence on the Web
  - Remote access and business partner access over the Internet
  - Common or split firewall and security devices
  - Dual homing is an issue with IPv6
- Develop an Intranet Strategy
  - IPv6 addressing scheme
  - Define IPv4 routing scheme
    - Still need to get to the Internet
    - Still need to address other devices
- New Security Policy Development
  - NAT does not necessarily go away, but it changes
  - Lots more addresses
  - Changes in Access Control Lists
- Network and Security Management Upgrade
  - And an IPv4 and IPv6 address management tool
- Training for network manager, engineers, and help desks
- Development of new help desk documentation and procedures

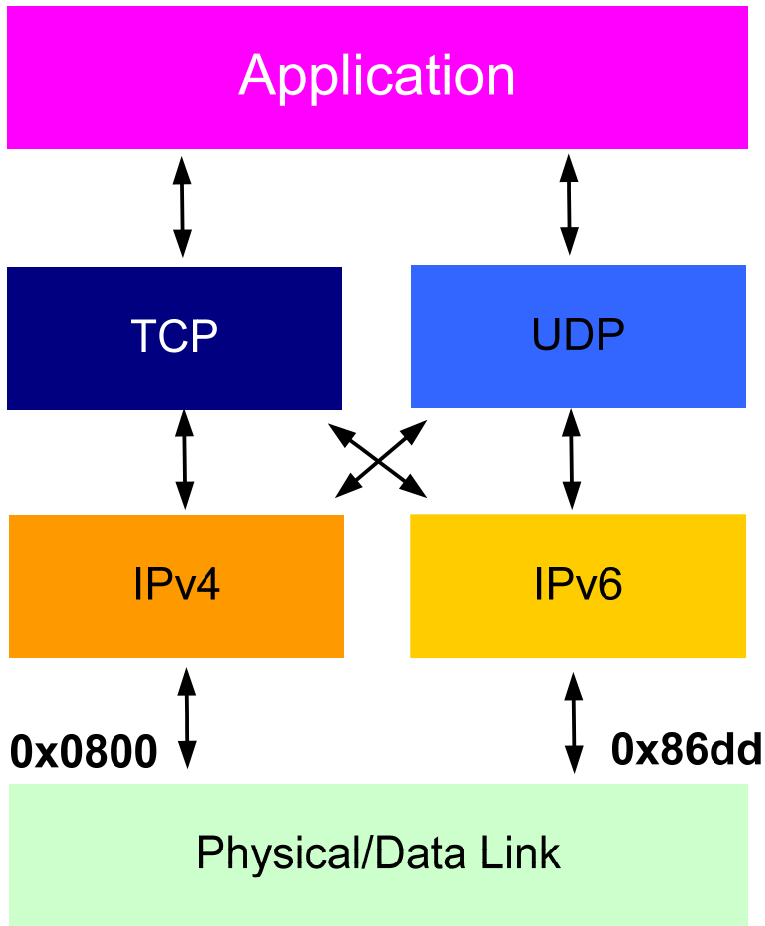
Transition Mechanisms

- Dual Stacks
  - IPv6/IPv4 coexistence
- Tunnels
  - IPv6 over IPv4 clouds - earlier
  - IPv4 over IPv6 clouds - later
  - ISATAP
    - Intra-Site Automatic Tunnel Addressing Protocol to enable IPv6 over existing IPv4 networks without multicast
  - Teredo
    - Getting IPv6 through IPv4 NAT devices
- Translators
  - IPv6 <-> IPv4

Which is the best method? It depends on your network, one size does not fit all

Dual Stacks

- **Both IPv4 and IPv6 stacks are enabled**
- **Applications can talk to both**
- **Choice of IP version is based on DNS lookup and application preference for IPv4 or IPv6**



Translator

- Proxy Mechanisms
- When an IPv6-only host needs to access an IPv4-only service (for example a web server), some form of translation is necessary. The most widely supported form of translation is the use of a dual-stack application-layer proxy, for example a web proxy.

We're all used to these types of gateway devices, such as proxy firewalls and Session Boarder Controllers

The infrastructure stuff that is lurking…

- Upgrade all layer 2/3 components: Routers, RAS, switches
  - Performance with dual stack or pure IPv6 may be limited, especially with ACLs
- Upgrade services: DHCP, DNS, NTP, SMTP, etc.
  - Issues related to security of SMTP and may need to stay IPv4
- Security components: Firewalls, IDS, VPN, etc.
  - Again, performance issues and hardware replacement
- Network Management: SNMP, syslog
- Authentication: TACAS, RADIUS, Windows Active Directory, LDAP
- Other Services: Web, Load Balancers, FTP, File servers, print servers, E-mail systems, Application servers, etc.
- Other devices: Printers, Scanners, VoIP, Video Conferencing
- Clients: Various operating systems
- Servers
  - Issues related to application performance

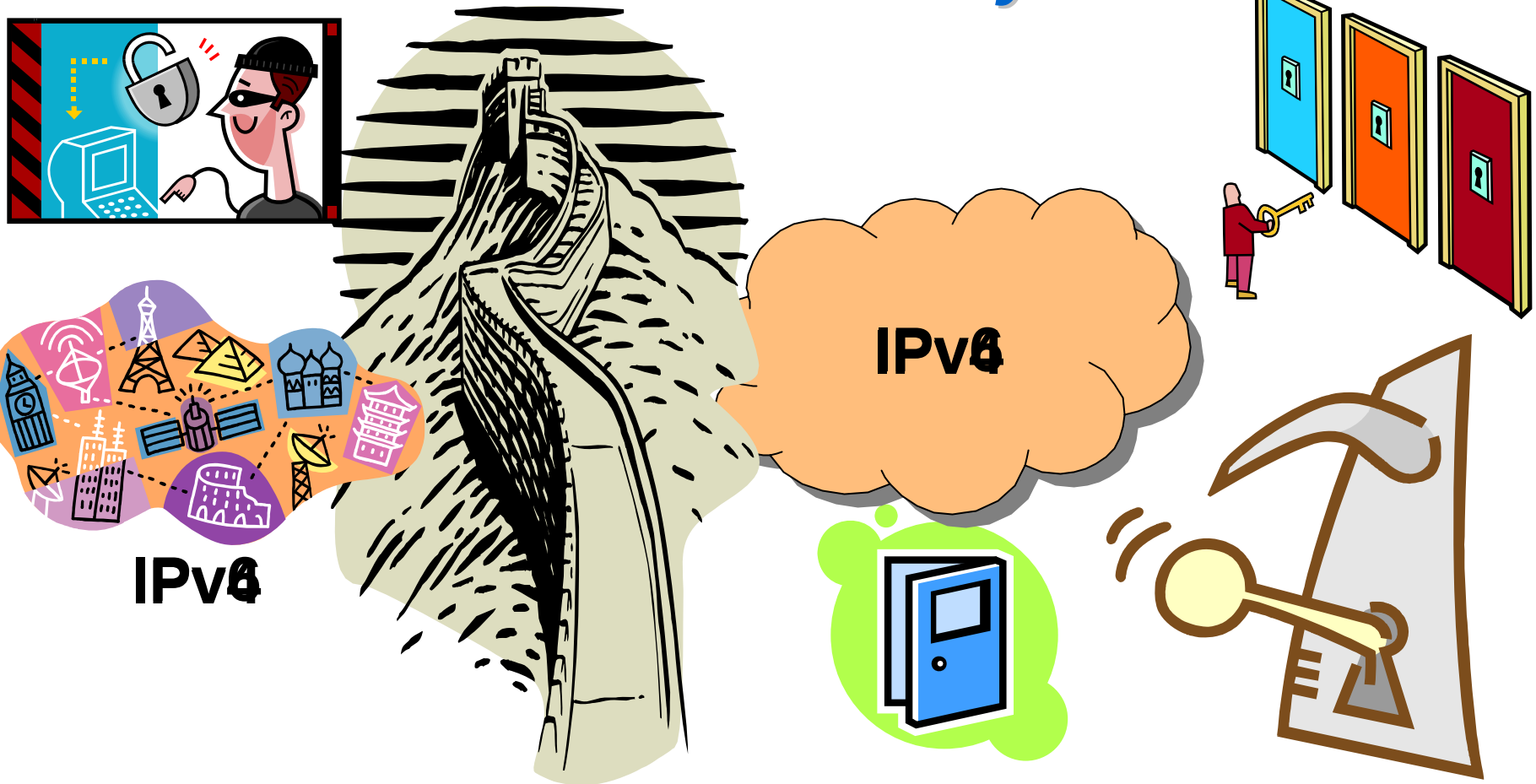
What not to do…

- Trying to solve transition to IPv6 world hunger
  - Don’t try to replace every printer with an IPv6 upgrade
- Try to make a pure transition
  - Need to cohabitate with IPv4 devices and subnets internal and external
- Fight an impossible battle to upgrade all applications that are currently hardwired for IPv4 or operating systems that cannot be upgraded

Execution

- Get IPv6 address space
  - Provided by ARIN or an ISP
- Develop an addressing plan
- Develop a device upgrade or replacement plan
- Create a testbed
  - Analyze traffic for ports and protocols
  - Upgrade hardware
    - Components (memory or flash)
    - Entire device
  - Training for support personnel
  - Application inventory and test in the lab
  - DNS entries – Naming convention
  - Pilot sites – Have few of the sites on a production pilot network – dual stack
- Plan for final implementation
  - phased approach – Run parallel systems

Brief comments on security



Currently, perimeter protection requires that each application and resource have its own lock…if anything is open security is breached

Qwest
Spirit of Service

We need a new security model

- Objects need certificates
  - People
  - Routers
  - Workstations
- How do we leverage the IPv6 address space?
  - Why not have dozens, hundreds, even thousands of IP address for a server?
  - Segregate reachability with certificates for each address to ensure end-to-end security
- Keep our network clean
  - Why not have IPv6 intermediaries also understand object reachability just like applications do?

We need an end-to-end security model that does not allow every IPv6 endpoint to test the security of all the other endpoints it can reach

Networx Related Support

- IPv6 Enabled Services
  - Both Internet and MPLS VPN
- IPv6 Enabled Equipment
  - Service Enabling Devices
- Testbed Support
  - Get a test connection now
- Professional Services
  - Program management and transition support
  - Engineering support
  - Security support including architecture and Certification and Accreditation

Qwest

Spirit of Service

Thank you