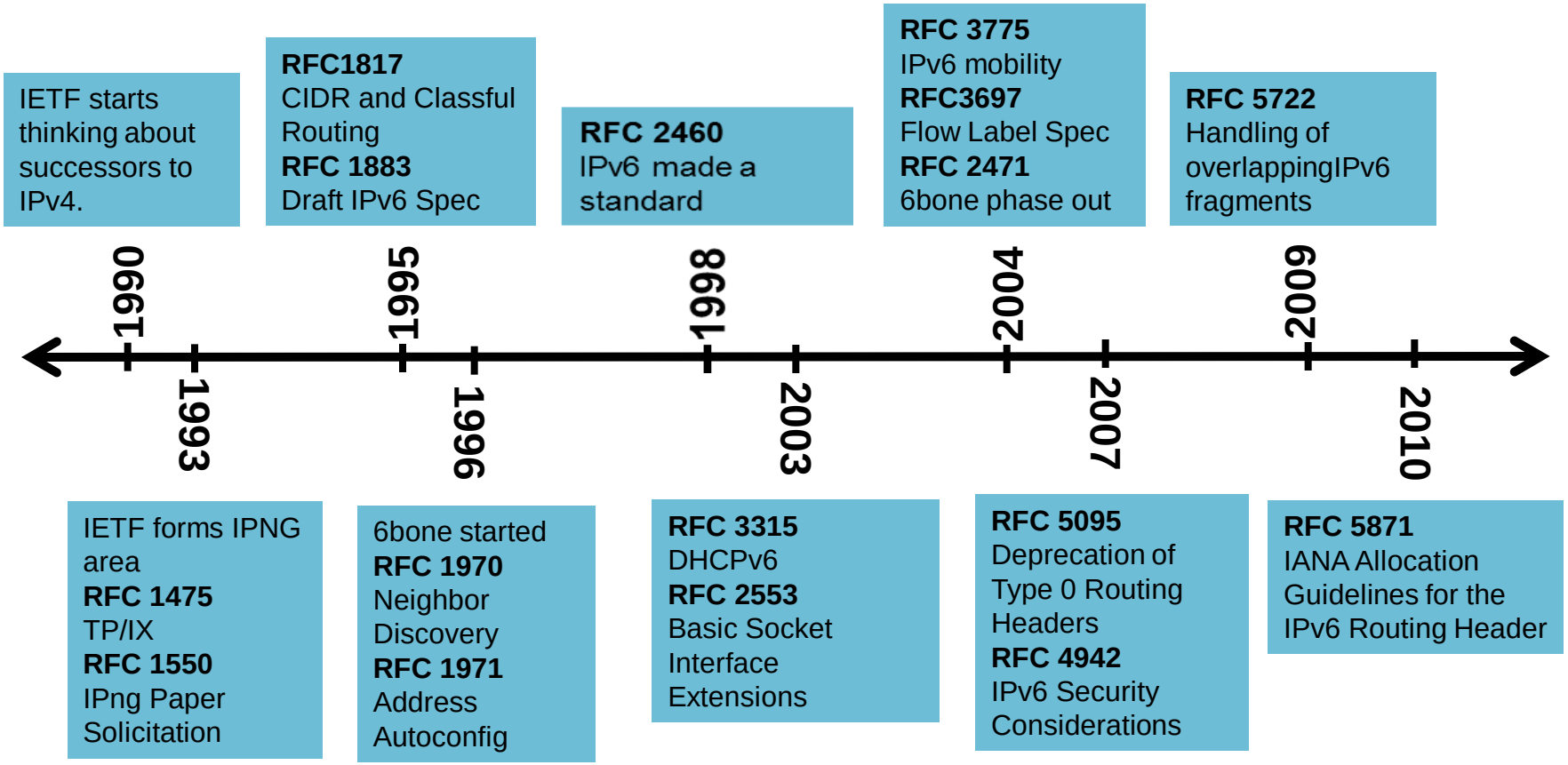
IPv6@ARIN

Matt Ryanczak
Network Operations Manager

IPv6 Timeline



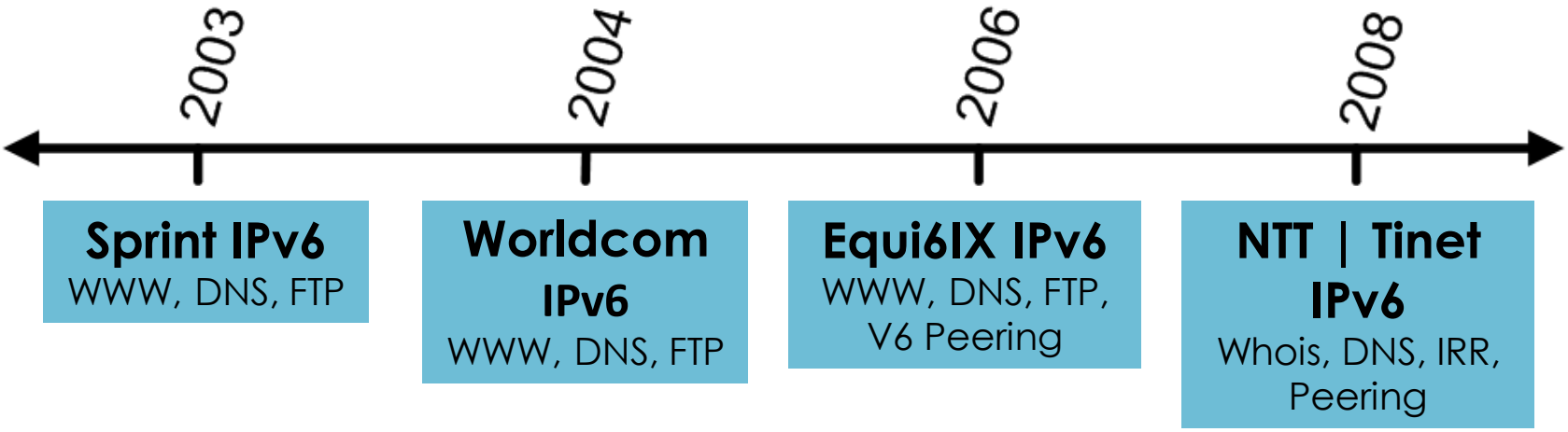
What happened to IPv5?

The Internet Stream Protocol (ST, ST2, ST+)

- First developed in the late 1970s (Internet Engineering Note 119, 1979)
- Designed to transmit voice and other real time applications
- Guaranteed bandwidth, QOS
- Set the version field in IP header to 5
- ST2 and ST+ saw interest from IBM, Sun and others in to the 1990s

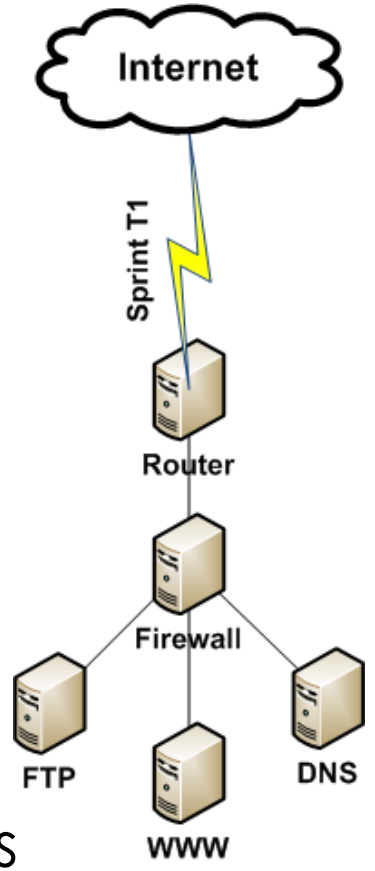
There were a lot of potential replacements for IPv4:
RFC 1752 Recommendation for the IP Next Generation Protocol (Pv6)
RFC 1475: TP/IX: The Next Internet (IPv7)
RFC 1621: PIP - The P Internet Protocol (IPv8)
RFC 1374: TUBA - TCP and UDP with Bigger Addresses (IPv9)
RFC 1606: A Historical Perspective On The Usage Of IP Version 9

ARIN IPv6 Timeline



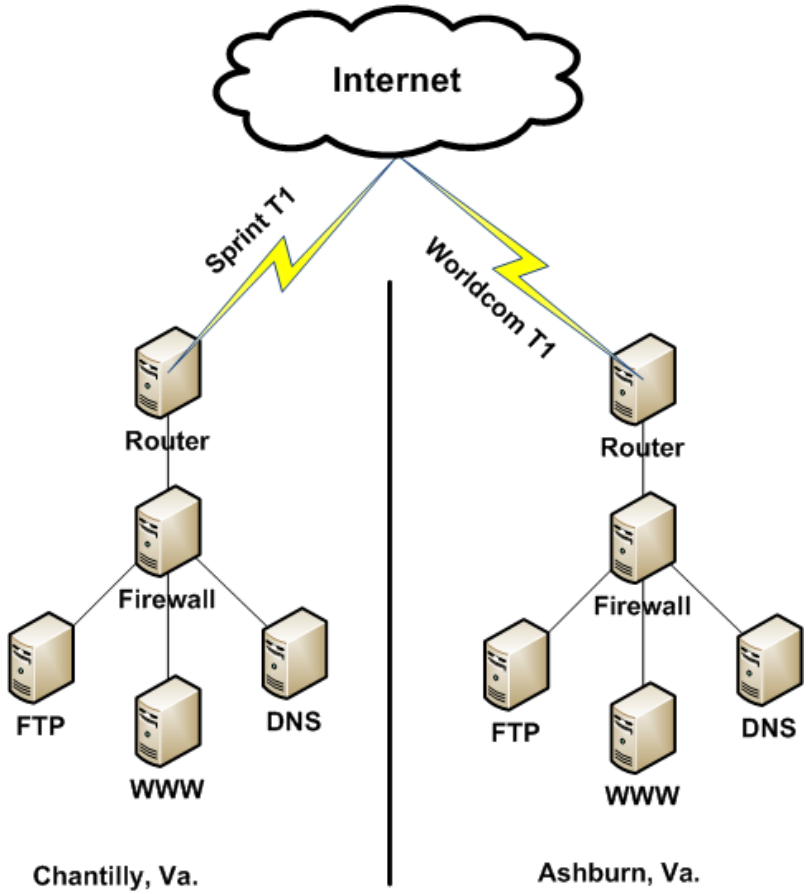
2003: Sprint

- T1 via Sprint
- Linux Router with Sangoma T1 Card
- OpenBSD firewall
- Linux-based WWW, DNS, FTP servers
- Segregated network no dual stack (security concerns)
- A lot of PMTU issues
- A lot of routing issues
- Service has gotten better over the years



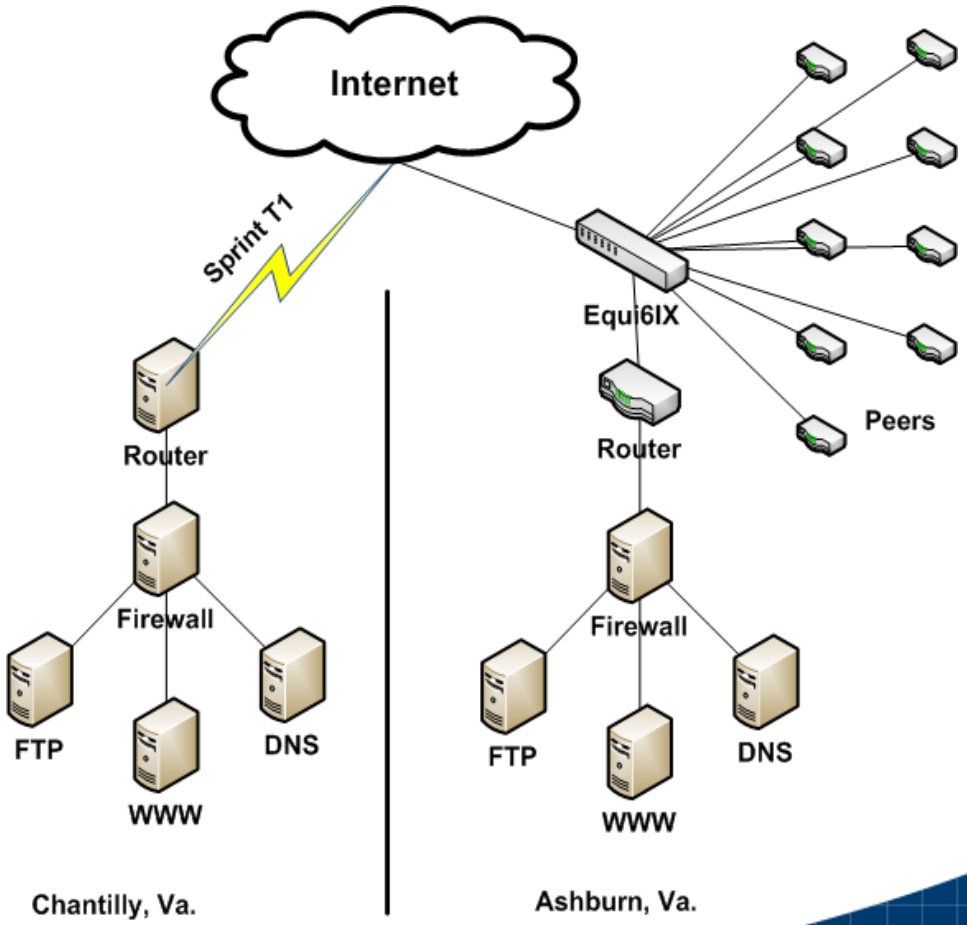
2004: Worldcom

- T1 via Worldcom to Equinix
- Cisco 2800 router
- OpenBSD firewall
- Linux-based WWW, DNS, FTP servers
- Segregated network no dual stack (security concerns)
- A lot of PMTU Issues
- A lot of routing issues



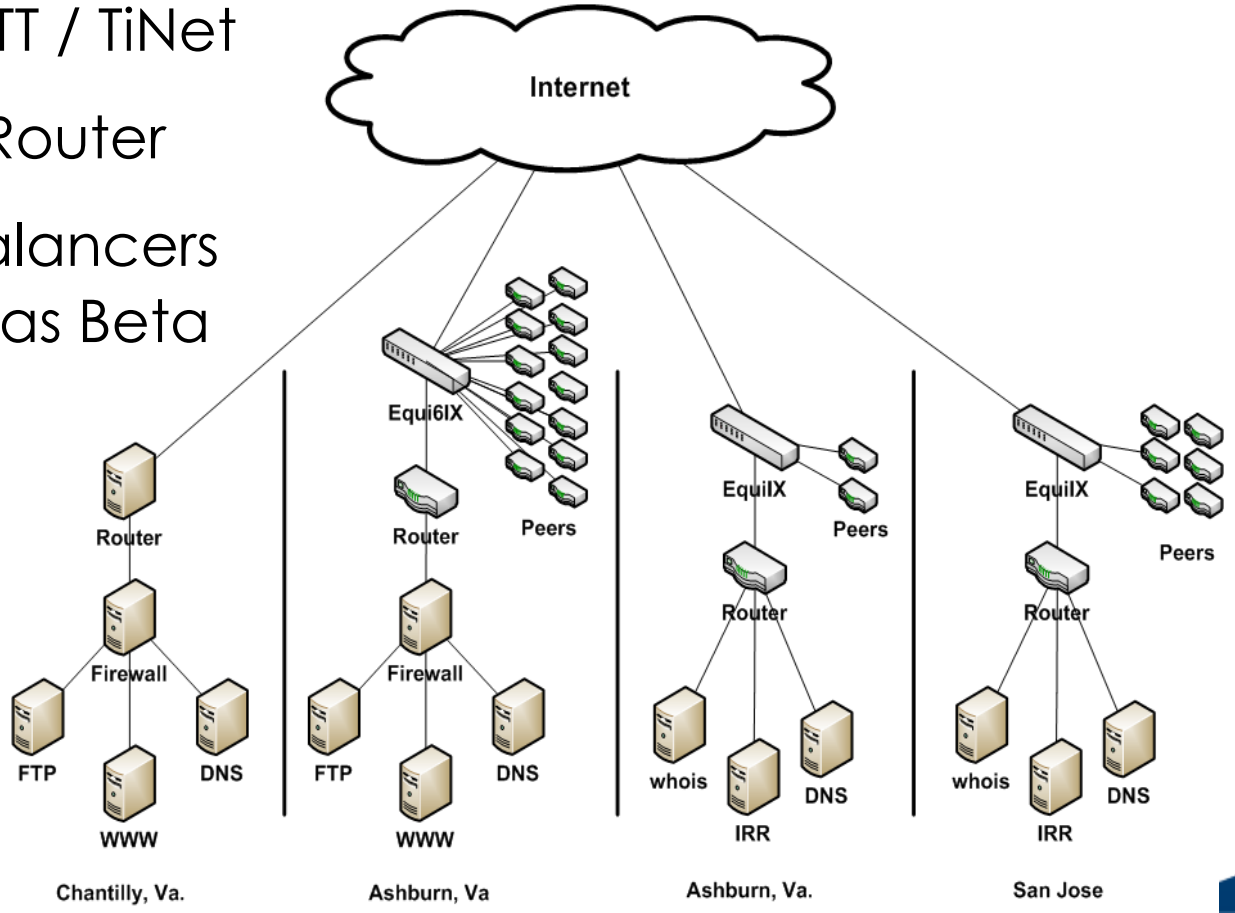
2006: Equi6IX

- 100 Mbit/s Ethernet to Equi6IX
- Transit via OCCAID
- Cisco router
- OpenBSD firewall
- WWW, DNS, FTP, SMTP
- Segregated -> dual stack



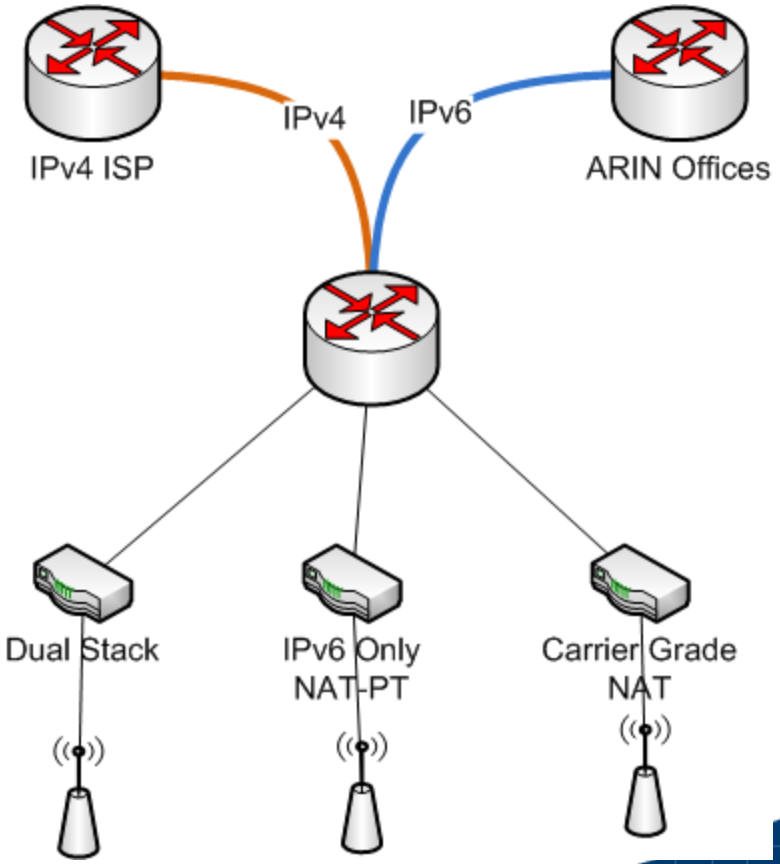
2008: NTT / TiNet IPv6

- 1000 Mbit/s to NTT / TiNet
- Cisco ASR 1000 Router
- Foundry Load Balancers
  - IPv6 support was Beta
- DNS, Whois, IRR, more later
- Dual stack
- Stand Alone Network

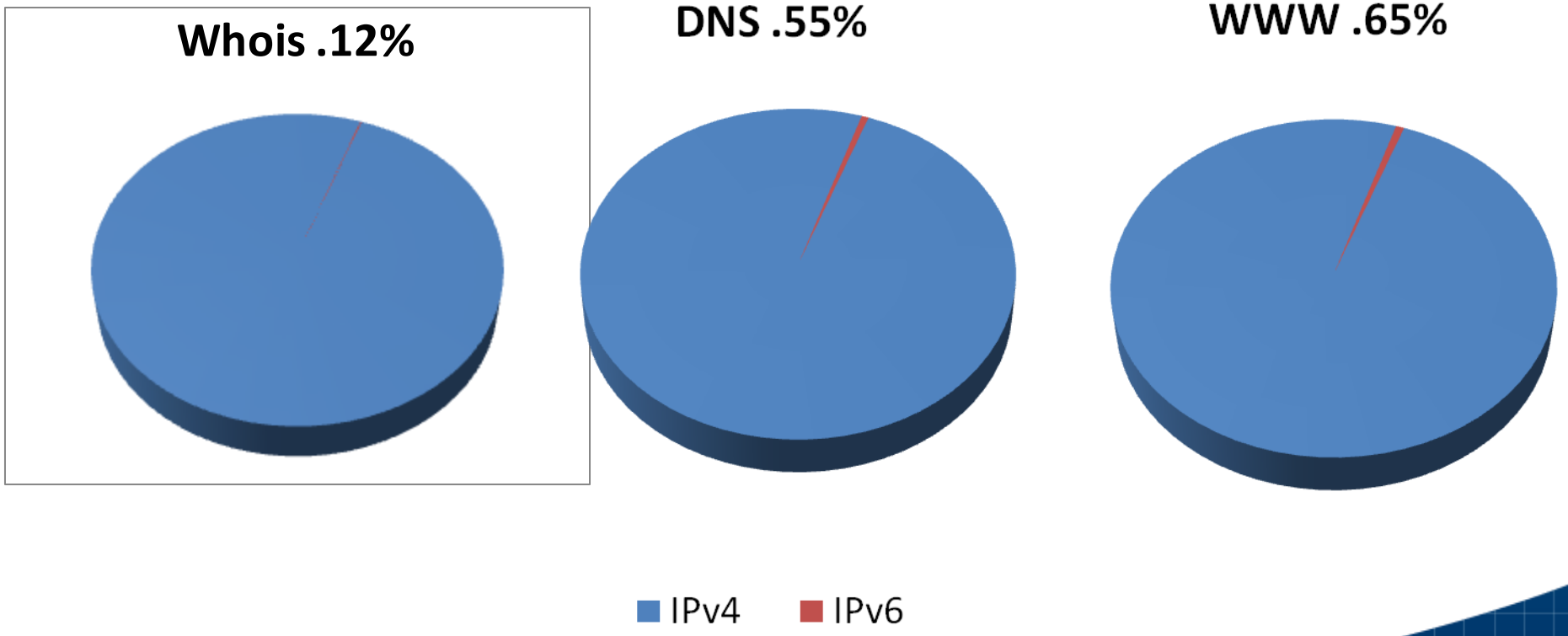


Meeting Networks

- IPv6 enabled since 2005
  - Tunnels to ARIN, others
- Testbed for transition tech
  - NAT-PT (Cisco, OSS)
  - CGN / NAT-lite
- Training opportunity
  - For staff & members



How much IPv6 Traffic?



So what about Security?

- Many things are the same, but different
- There are many unknowns, new territory!
- Built in (in)security features
- Multiple protocol == multiple policies

More Protocols, More Problems

IPv4 and IPv6 are not the same

- IPv4 features != IPv6 features
- IPv6 does not have ARP. It uses ICMPv6
- ICMPv6 is critical to IPv6 functionality
- DHCPv6 / router advertisement

More Protocols, More Problems

Hardware / Software support is less than ideal

- Application and OS behavior inconsistent
- Firewalls, IDS, etc. have weak IPv6 support
- Switches, load balancers also lack support

Security Through Obscurity

- IPv6 has been in many OSes for 10+ years
- Stacks are not battle tested
- Applications are not well tested
- Stack smashing? Buffer overflows?
- Many unknowns in IPv6 implementations

Security Through Obscurity

- Exploits are not well known either
- Difficult to scan IPv6 networks with current tools
- Hard to guess addresses
- Black & White hats starting over (again)

Built(in)Security Features

- IPsec ESP is built-in
- IPSec AH is built-in
- Easy VPNs
- Enhanced routing security
- Application layer security

Built-in (in)Security Features

- ESP can make DPI difficult
- AH hard to configure / maintain
- IPv6 enabled backdoor, trojans, etc.
- No NAT? How to hide those networks?
- IPv6 address types complex and confusing

Cross Contamination

- Multiple stacks, multiple targets
- Maintaining policy parity is difficult
- Applications lack feature parity
- Appliances lack feature parity

Lessons Learned: Implementation

- Tunnels are less desirable than native
- Not all transit is equal
- Routing is not as reliable
- Dual stack is not so bad
- Proxies are good for transition

Lessons Learned: Implementation

- Native support is better
- DHCPv6 is not well supported
- Reverse DNS is a pain
- Windows XP is broken but usable
- Bugging vendors does work!

Lessons Learned: Security

- Dual stack makes policy more complex
- IPv6 security features double-edged sword
- Security vendors behind on IPv6
- IPv6 stacks are relatively untested
- A whole new world for hackers to explore

Lessons Learned: Security

- Understanding ICMPv6 is a must
- Fragmentation is very different in IPv6
- Multicast is an attack and discovery vector
- Read RFC 4942!

Thank You