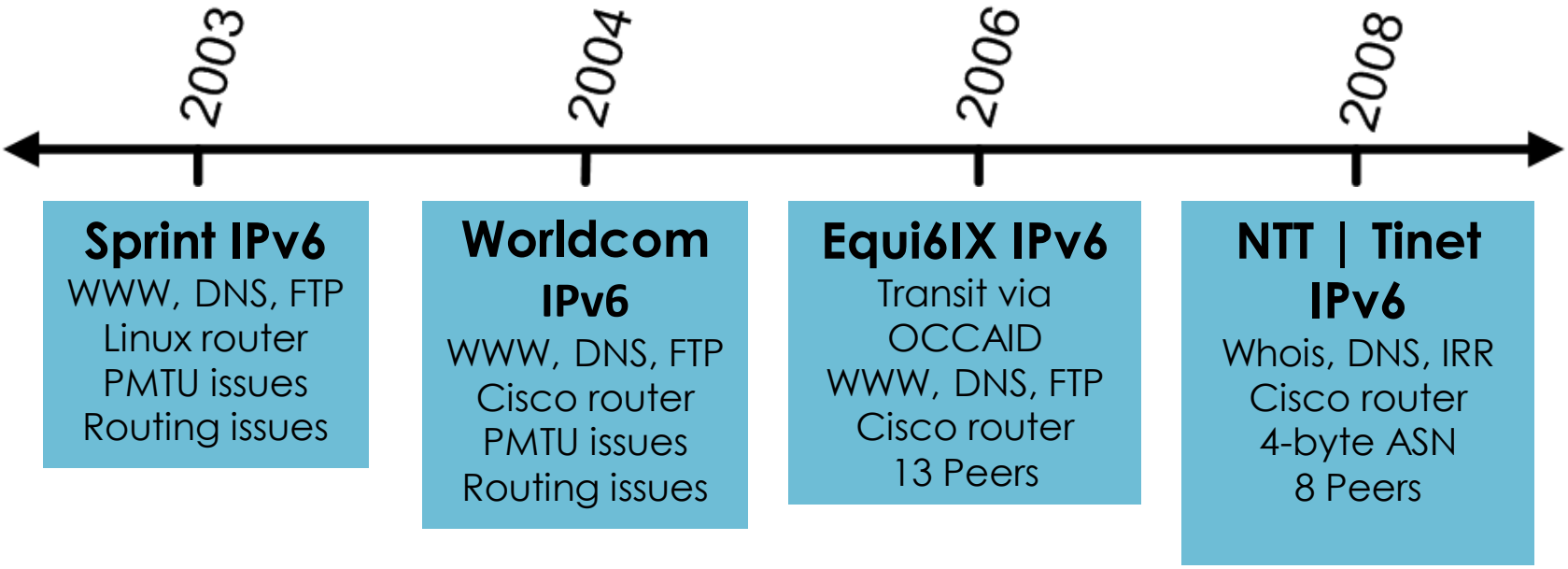
IPv6@ARIN

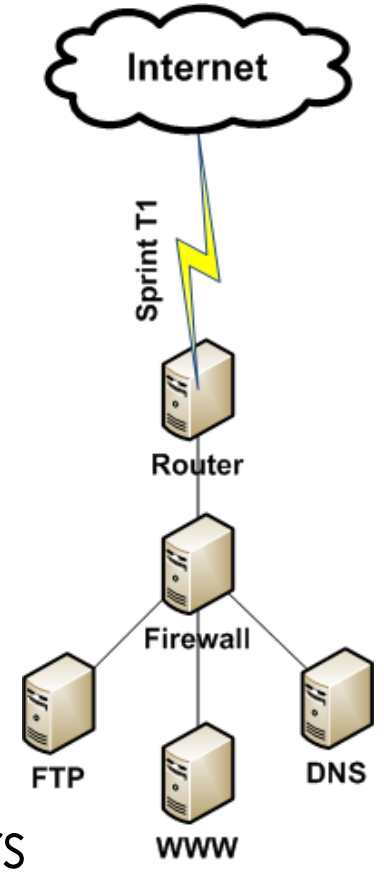
Matt Ryanczak
Network Operations Manager

Timeline


2003
2004
2006
2008
Sprint IPv6
WWW, DNS, FTP
Linux router
PMTU issues
Routing issues
Worldcom IPv6
WWW, DNS, FTP
Cisco router
PMTU issues
Routing issues
Equi6IX IPv6
Transit via OCCAID
WWW, DNS, FTP
Cisco router
13 Peers
NTT | Tinet IPv6
Whois, DNS, IRR
Cisco router
4-byte ASN
8 Peers

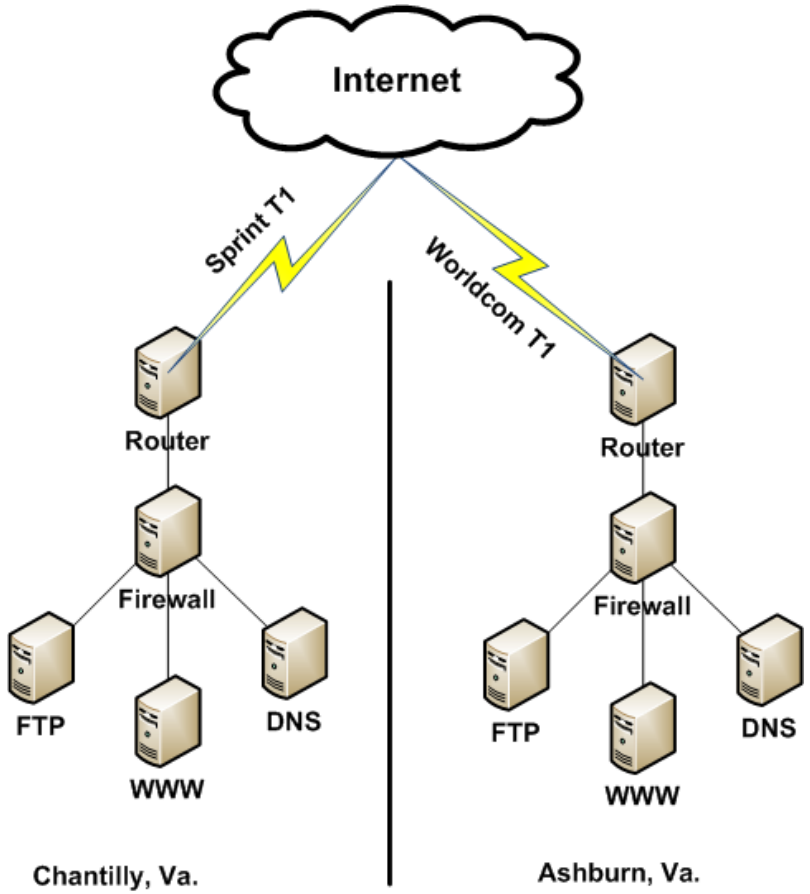
2003: Sprint

- 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



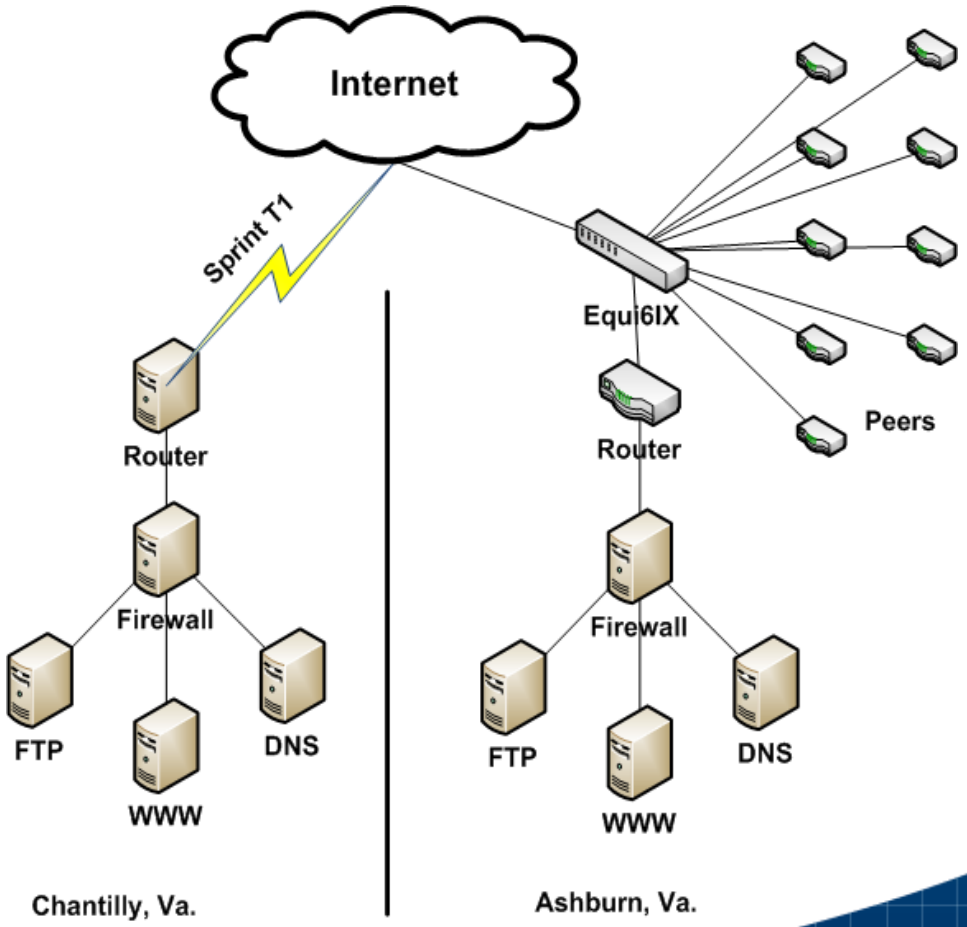
2004: Worldcom

- 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



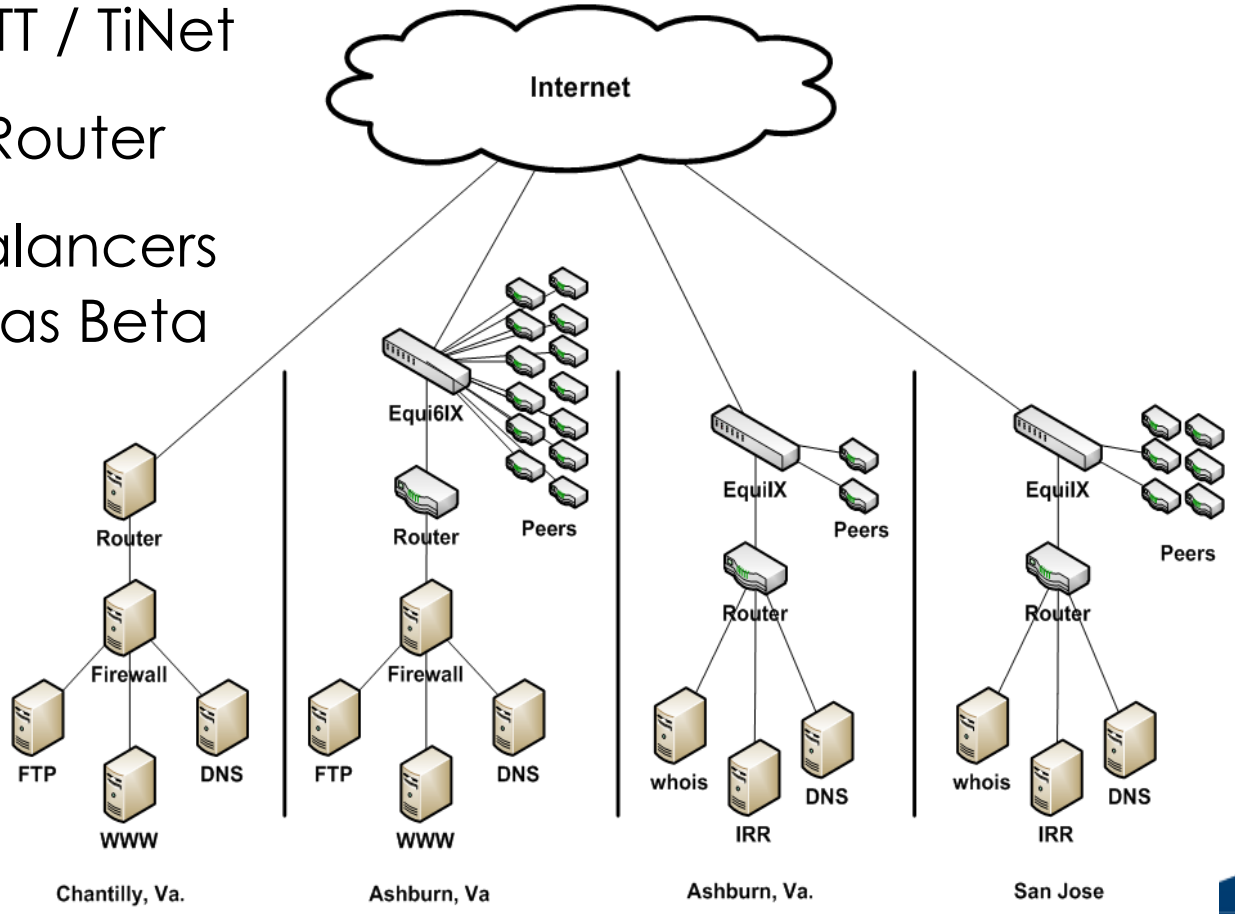
2006: Equi6IX

- 100 Mbit/s Ethernet to Equi6IX
- Transit via OCCAID
- Cisco 2800 router
- OpenBSD firewall
- WWW, DNS, FTP servers
- Segregated Network
- Some dual stack



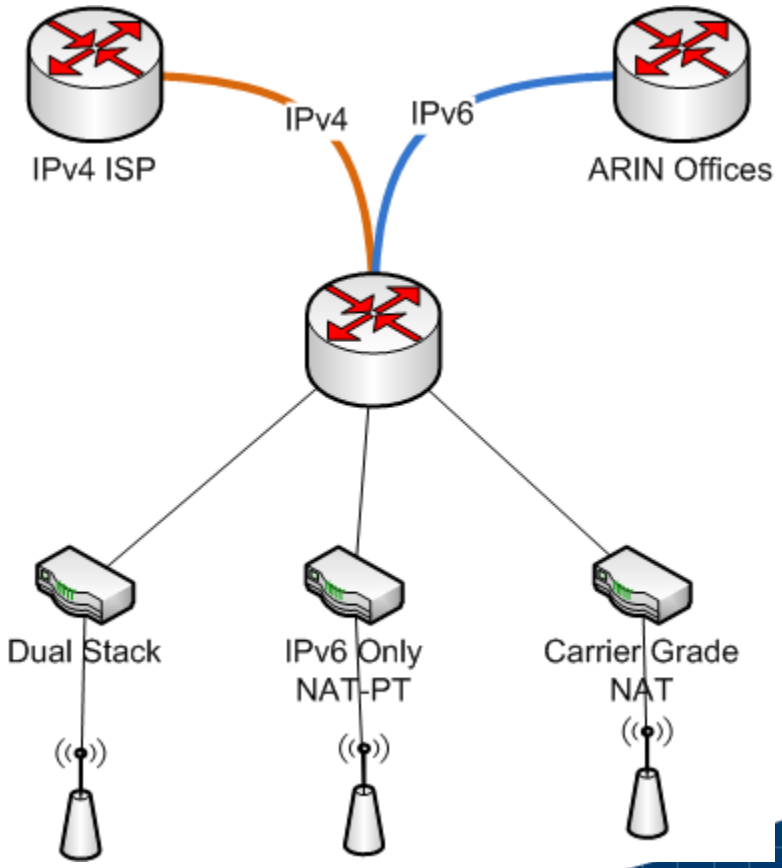
2008: NTT / TiNet IPv6

- 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

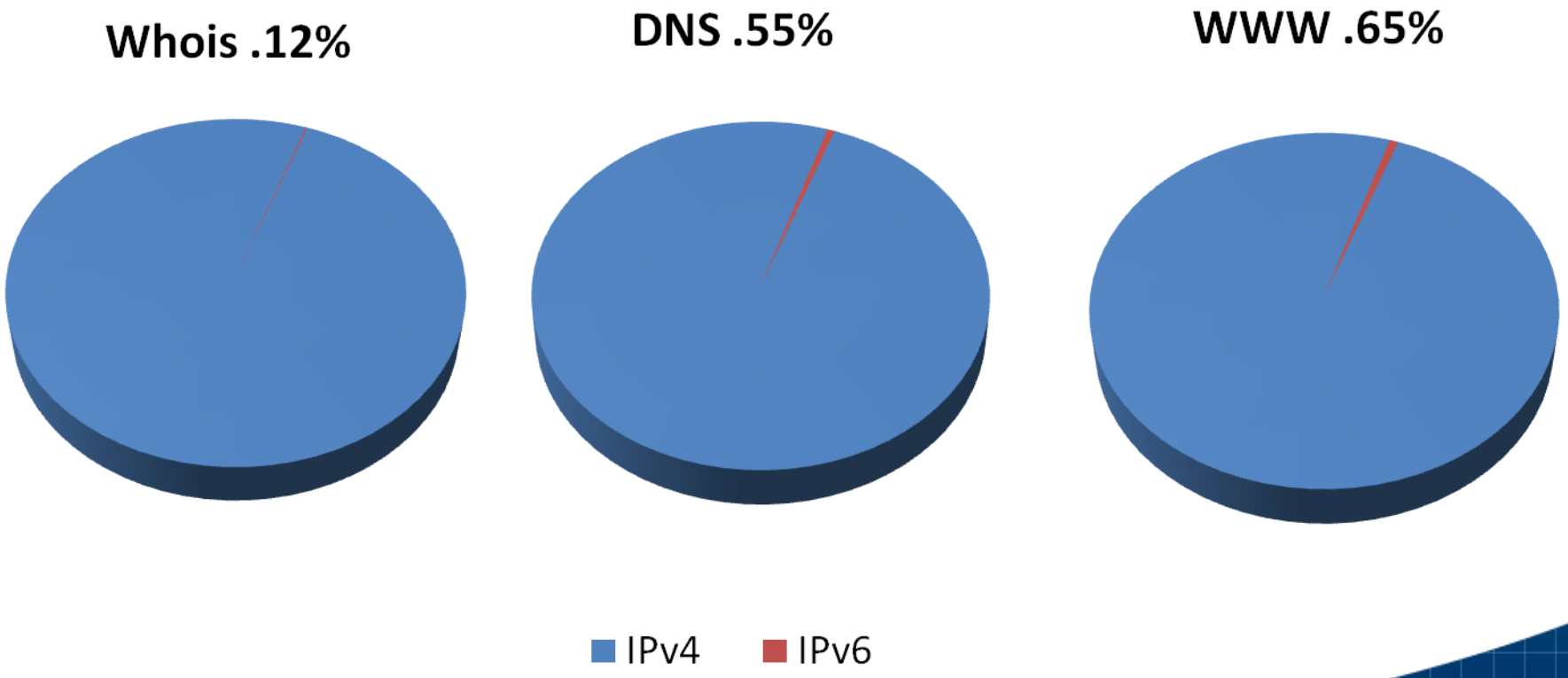


Meeting Networks

- 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?

- More protocols. More problems
- Security through obscurity
- Built in (in)security features
- Cross contamination

More Protocols, More Problems

IPv4 and IPv6 are like oil and water

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

More Protocols, More Problems

Access control is more complex

- IPv4 and IPv6 have separate ACLs
- Crafting consistent policies difficult
- Application and OS behavior inconsistent
- Firewalls, IDS, etc. have weak IPv6 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? Application 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
- More security out of the box
- Black hats & White hats starting over (again)

Built-in (in)Security Features

- IPsec ESP is built-in
- IPSec AH is built-in
- Virtual private networks without tunnels
- Enhanced routing security
- Application layer security

Built-in (in)Security Features

- IPsec ESP can make DPI difficult
- IPsec 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
- People fear 4-byte ASN

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
- Lack of NAT is a good thing (Really!)
- A whole new world for hackers to explore

Thank You