IPv6 at Monash University

John Mann

Summary

- **IPv6 research at CTIE, Advanced Technologies CRC**
- **Production IPv6 dual-stack network**
- **Problems**
- **Future Plans**

The Centre for Telecommunications and Information Engineering, and Advanced Technologies CRC
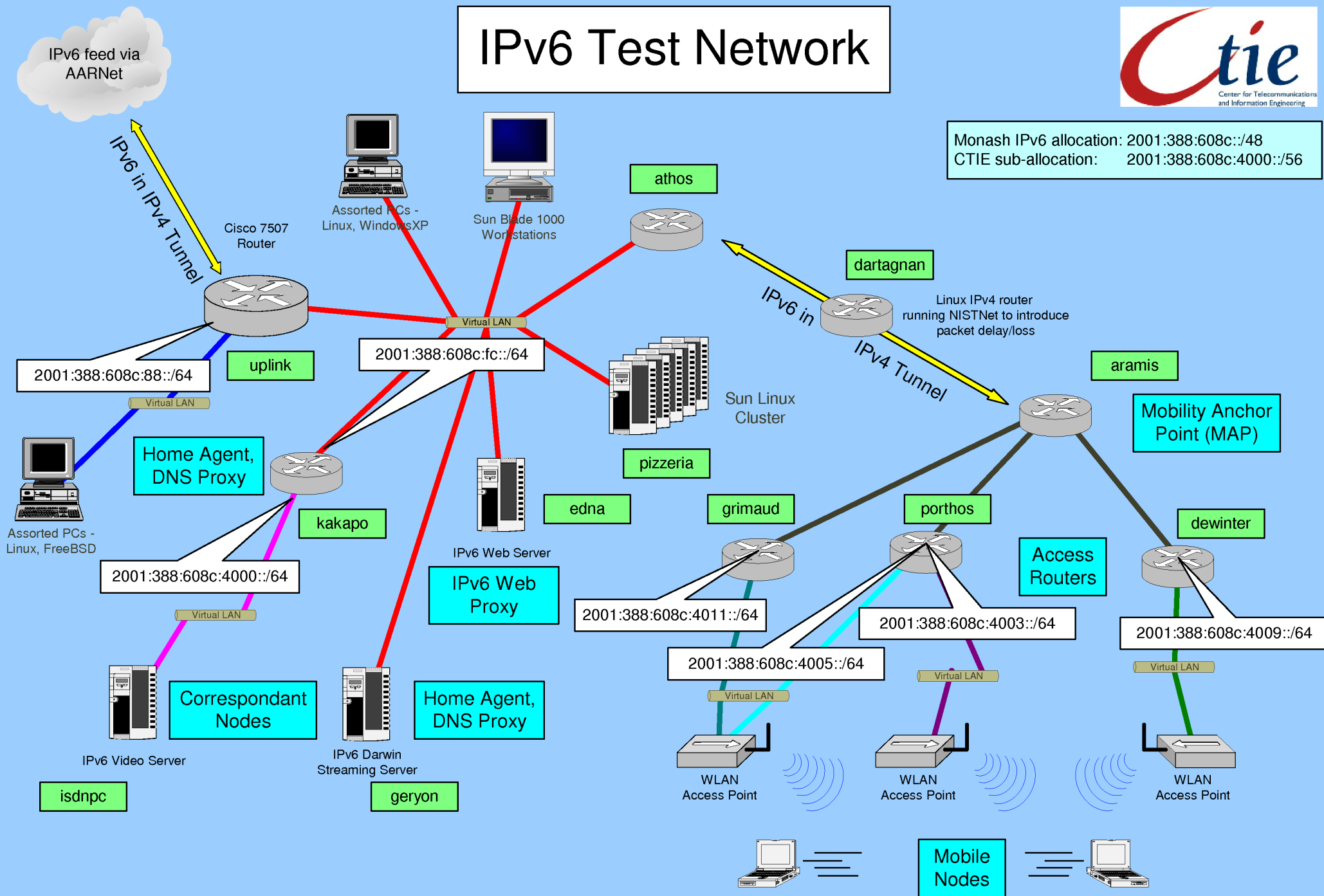
Did leading-edge research into

- **Mobile IPv6**

- **Protocols for Detecting Network Attachment**

- **Fast handovers and fast address configuration for Mobile IPv6**

- **Streaming Video over IPv6**

IPv6 Test Network

CTIE
Center for Telecommunications
and Information Engineering

IPv6 feed via AARNet

IPv6 in IPv4 Tunnel

Monash IPv6 allocation: 2001:388:608c::/48
CTIE sub-allocation: 2001:388:608c:4000::/56

Cisco 7507 Router

Assorted PCs - Linux, WindowsXP

Sun Blade 1000 Workstations

athos

dartagnan

Linux IPv4 router running NISTNet to introduce packet delay/loss

Virtual LAN

2001:388:608c:fc::/64

IPv6 in IPv4 Tunnel

aramis

uplink

2001:388:608c:88::/64

Virtual LAN

Home Agent, DNS Proxy

Assorted PCs - Linux, FreeBSD

Sun Linux Cluster

pizzeria

Mobility Anchor Point (MAP)

kakapo

2001:388:608c:4000::/64

Virtual LAN

edna

grimaud

porthos

dewinter

IPv6 Web Server

IPv6 Web Proxy

Access Routers

Correspondant Nodes

Home Agent, DNS Proxy

2001:388:608c:4011::/64

2001:388:608c:4003::/64

2001:388:608c:4009::/64

2001:388:608c:4005::/64

Virtual LAN

Virtual LAN

Virtual LAN

IPv6 Video Server

IPv6 Darwin Streaming Server

WLAN Access Point

WLAN Access Point

WLAN Access Point

isdnpc

geryon

Mobile Nodes

Advanced Technologies CRC

Involved

- **14 staff from Monash and RMIT**
- **50+ students**

And resulted in

- **30+ Internet Drafts**
- **RFC 4135 and RFC 4429**
- **Optimistic DAD now in Linux kernel**
- **125k lines of IPv6Suite simulation code**
- **7 PhDs**

Production Monash IPv6 dual-stack Network

- **Why Now?**
- **Addressing Plan**
- **Upgrading the Infrastructure**
- **Configuring Routers and ACLs**
- **DNS and DHCP Services**
- **Servers**
- **IPv6 Usage**

Why Now?

- Monash is a large organisation, it will take a long time to embrace a change

- Needed to break the chick-and-egg problem by providing the IPv6 infrastructure

- End-systems and servers now come with IPv6 enabled

- Dual-stacking the infrastructure is a 50-device problem, v. dual-stacking edge devices which is a 30,000-device problem

- Cost of failure, or having to do things over, is low now, compared to having to do things in a rush later

- Be seen to be a leader

IPv6 is already here.
It's just not evenly distributed.

- Apologies to William Gibson

- **First IPv6 RFCs in 1996**

- **Monash has had native IPv6 since 2003**

- **Windows Vista, Mac OS X, Linux already come with IPv6 enabled**

- **Some Web sites are now IPv6 enabled**
  - On 23-Jan-2009, Google enable AAAA DNS replies for uses on AARNet
    - http://www.google.com.au
    - http://mail.google.com
    - http://docs.google.com ...
  - This provided a **HUGE** amount of support for IPv6

IPv4 address plan

- **Originally used 130.194/16 for everything**
- **When that became full, added**
  - 172.16/16 (private nets)
  - 172.17/16 (wireless)
  - 172.18/16 (students)
  - 172.19/16 (staff)
  - 172.20/16 (management)
  - ...
  - with Internet access via Proxies
- **Renumbered half the network**

IPv6 Address Plan

- **No easy way to map IPv4 addresses <=> IPv6 addresses**
- **IPv4 address plan a bit disorganised anyway**
- **So, new logical IPv6 address plan**

Use (2 bits)	Org Unit (4 .. 12 bits)	Location (8 .. 0 bits)
Server Research Staff Student	ITS Admin Arts …	North East West …

- **/64 for p-p router backbone links**
- **/64 for router loopbacks, DNS anycasts**

IPv4 Address Plan 2

- In 2008, replaced Web and SOCKS proxies with Cisco Service Control Engine (SCE)
- All hosts that want Internet access needed to move to Public IPv4 addresses
- Obtained extra IPv4 addresses, and renumbered half the network again
- IPv4 network plan is now less messy – so less justification for a different IPv6 network plan

Upgrading the Infrastructure

- **IPv6 is just another infrastructure upgrade**
  - There is no IPv6 "killer app", just more addresses and simpler protocol
- **Monash has done infrastructure upgrades before**
  - Terminals → Ethernet → Thinwire → UTP
  - Point-to-point → bus → hub → router → switch
  - Copper wires → multimode fibre → singlemode fibre → CWDM → DWDM
  - DECnet, AppleTalk, Banyan, IPX/SPX → IPv4

Cisco Routers

- **Catalyst 6500 routers**
  - IPv6 availability varies with releases/feature sets
  - From 12.2(33)SXI, released 13th Nov 2008,
    IPv6 is in IP SERVICES,
    previously ADVANCED IP SERVICES
- **Catalyst 3750 routers**
  - IPv6 features with ADVANCED IP SERVICES license, about A$4k list price
  - IPv6 ~halves TCAM available for IPv4 functions
  - Has severely restricted IPv6 for small campuses that use 3750's as their routers
  - I hope Cisco will put IPv6 in IP SERVICES

Router Configuration

- **We enter all subnet information into a database: subnet name, address ranges, Vlan number, on which routers, access rules, …**

- **The database is then used to generate router configurations**

- **We extended the database to manage IPv6 addresses and generate IPv6 router configs**

ACL Management

- **Old scheme creates IPv4 ACLs using a Perl script and a flat-file list of exceptions**
- **ACL heuristics in script evolved over time**
- **Now we need to generate IPv6 ACLs as well**
- **New ACL creation scheme uses ACL templates and macro expansion for both IPv4 and IPv6 ACLs**
- **More-transparent scheme, but lower level**

IPv6 out ACL Template Example

permit tcp any any established

%special-top-out6

permit ipv6 %fromgroup6 any ! normal out traffic

deny udp any any range 135 139 log ! block window virus

deny udp any any eq 445 log ! block window virus

permit udp %net-monash-au6 any ! NACP

permit udp any any gt 1024 ! NACP2

permit icmp any any ! NACP

permit ipv6 any ff00::/8 ! multicast out

%special-bottom-out6

deny ipv6 any any log-input

DNS

- **Addhost, our network host registration scheme, was extended to cater for**
    - Fixed IPv6 addresses; and also
    - "auto" IPv6 addresses generated from

        IPv4 address => IPv4 subnet => IPv6 subnet table,

        and Ethernet address => EUI-64 host address
- **No need for normal users to enter long hex addresses**
- **Forward and reverse DNS**
    - But not fe80::/64 reverse yet
- **DNS servers have Ipv4 and IPv6 Anycast addresses, tied to /dev/tun0 and advertised using Quagga**

nsla.its.monash.edu DNS queries: Last 48 Hours
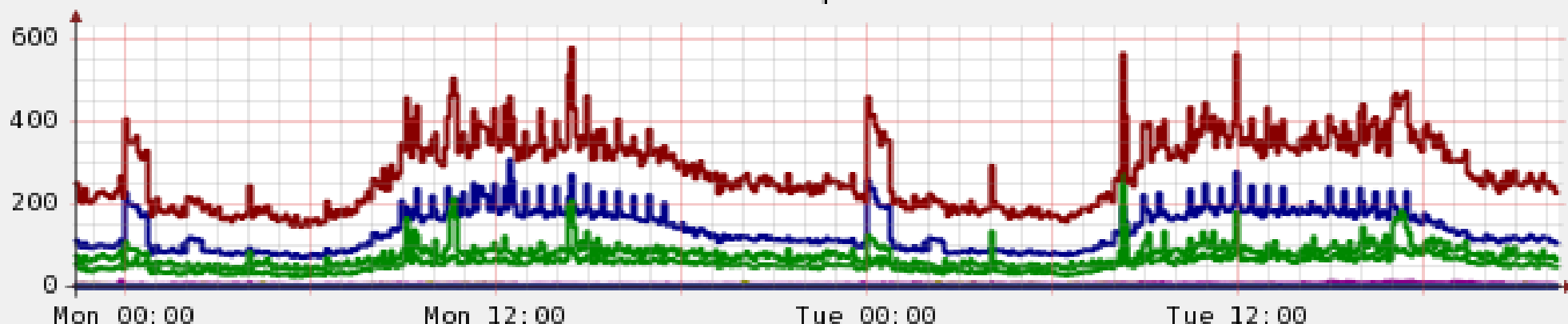
		Current	Min	Average	Max
■ A	queries/sec	Current: 106.15	Min: 71.41	Average: 138.54	Max: 306.85
■ PTR	queries/sec	Current: 48.78	Min: 24.87	Average: 55.50	Max: 132.33
■ ANY	queries/sec	Current: 40.24m	Min: 17.05m	Average: 161.86m	Max: 874.54m
■ MX	queries/sec	Current: 4.82	Min: 3.45	Average: 5.73	Max: 12.82
■ NS	queries/sec	Current: 2.83	Min: 990.01m	Average: 2.83	Max: 9.60
■ CNAME	queries/sec	Current: 3.31m	Min: 0.00	Average: 9.96m	Max: 76.19m
■ SOA	queries/sec	Current: 50.14m	Min: 20.07m	Average: 351.61m	Max: 2.97
■ SRV	queries/sec	Current: 80.11m	Min: 40.29m	Average: 189.58m	Max: 1.48
■ AAAA	queries/sec	Current: 65.75	Min: 41.59	Average: 76.26	Max: 275.51
■ TOTAL	queries/sec	Current: 228.50	Min: 146.50	Average: 279.56	Max: 577.55

Tue Nov 11 22:23:05 2008

IPv6 DNS Usage

- **About 25% of DNS queries are for AAAA records**
- **Unfortunately, most of these are for non-existent domains, or hosts without AAAA records**
- **For example: 4 AAAA queries before A query**

15:00:04.106 query: directory.monash.edu.au IN AAAA +

15:00:04.109 query: directory.monash.edu.au.its.monash.edu.au IN AAAA +

15:00:04.110 query: directory.monash.edu.au.monash.edu IN AAAA +

15:00:04.111 query: directory.monash.edu.au.monash.edu.au IN AAAA +

15:00:04.111 query: directory.monash.edu.au IN A +

- **Also occasional storms of requests for "ISATAP"**
  - 600 queries per second, per PC !!

Off-site Web and DNS Hosting IPv6 FAIL

.EDU Parent DNS Glue Records

MONASH University

.EDU.AU Parent DNS Glue Records

- **The web site for managing .edu.au DNS registrations does not allow entering IPv6 addresses for nameservers**

- **But, the Registrar education.au can manually add IPv6 glue records into AusRegistry's DNS and Whois database**

```
[whois.aunic.net]
Domain Name:                    monash.edu.au
Last Modified:                  11-Jun-2008 02:54:03 UTC
Registrar ID:                   EducationAU
...
Name Server:                    ns1.its.monash.edu.au
Name Server IP:                 2001:388:608c:281::1
Name Server:                    ns2.its.monash.edu.au
Name Server IP:                 2001:388:608c:282::1
Name Server:                    ns3.its.monash.edu
```

DHCP and network auto-discovery

- **Since we are planning to run a dual-stack network, there isn't a pressing need for IPv6 DHCP**

- **Hosts get (IPv4) DNS server addresses from IPv4 DHCP, or statically configured**

- **Network router auto-discovery has worked very well so far – have only rebooted routers once in last 1.5 years**

- **Haven't done IPv6 HSRP**

- **Beware of rogue IPv6 routers**

Enabling IPv6 Applications

- **Everywhere that IPv4 addresses are entered, compared, computed or displayed will need to handle IPv6 addresses as well**

Steps in Enabling IPv6 Applications

- **Determine the IPv6 capability of the application**
- **Enable IPv6 networking on subnet, host, and host firewall**
- **Configure application to listen on IPv4 and IPv6**
- **Configure application access controls to allow IPv6 users**
- **Test service using hex IPv6 address, or a test DNS name**
- **Check via logs and/or network packet capture**
  - Up to this point, changes are invisible to users
- **Add AAAA record to DNS for service name**
- **Test service via DNS name**
- **Check via logs and/or network packet capture**
  - Beware of users who have IPv6 connectivity that doesn't work

Servers

- **Many servers auto-configure IPv6 by default**
- **May need to tweak**
  - /etc/hosts
  - /etc/hosts.allow
  - /etc/security/access.conf
  - Ifcfg-eth0
    - > Preference to use auto-discovery IPv6 address rather than fixed IPv6 address for outgoing connections

Web Servers

- **A customised Apache 1.3 is used on our main Web serving farm**
    - Too hard to add IPv6 support
- **Apache 2.0 does support IPv6**
    - Need to update .htaccess files
        - > Permissions based on IPv4 addresses aren't relevant any more

Web Reverse Proxy

- **Use Apache in Reverse-proxy mode as IPv6 => IPv4 gateway**

```
Listen [2001:388:608c:88b::123]:80
<VirtualHost *:80>
    ProxyPreserveHost On
    ProxyPass / http://130.194.11.123:80/
    ProxyPassReverse / http://130.194.11.123:80/
</VirtualHost>
```

Diagram of IPv6 -> IPv4 Web proxy
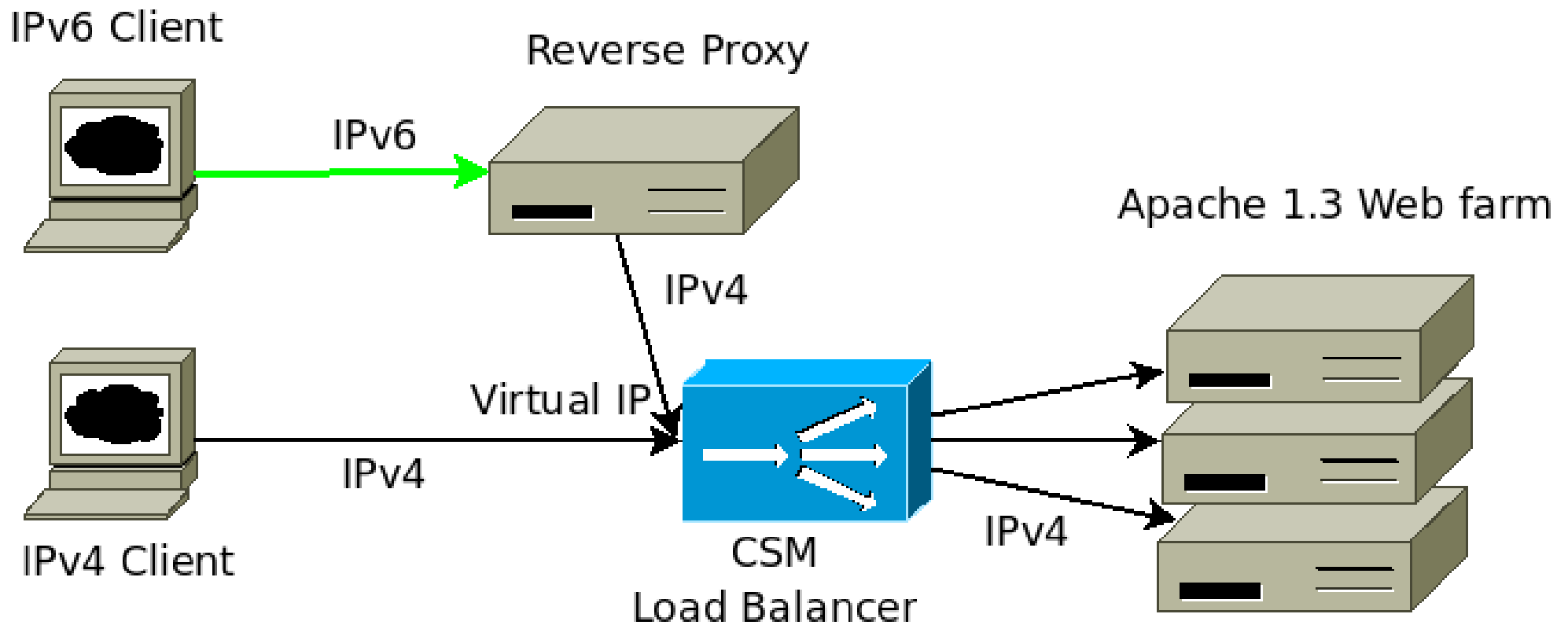
IPv6 Usage

- **Most server subnets are IPv6 enabled, but many IPv6-speaking hosts don't have AAAA DNS entries**
- **Currently, end-user IPV6 subnets are in**
    - Electrical Engineering
    - eResearch
    - Information Technology Services
- **Three Vista laptops with ICS wanted to be IPv6 routers, advertising 2002:... 6to4 tunnel networks**
- **5% of requests to Monash Web Farm are IPv6**
- **1.5% of Monash's Internet traffic is IPv6**

Problems

- **Perception: IPv6 is Boring**
- **Monitoring the Network**
- **IPv6 Capability of Middle-boxes**
- **Lessons Learnt**

Problem: Perception - IPv6 is Boring

- **IPv6 _IS_ Boring to End Users**
  - Users don't care about bits on the wire
  - IPv4 addresses haven't run out yet
  - They just want Web / E-mail / YouTube to keep working
- **IPv6 _IS_ an Infrastructure Upgrade**
  - That makes it a task for technical people
  - Our job to make infrastructure upgrades as invisible and non-disruptive to end-users as possible
  - Strategic upgrade project
    - > Many network problems have messy IPv4 solutions or cleaner IPv6 solutions

Problem: Monitoring IPv6 Network

- **Statseeker V3**
  - Can monitor interface usage and up/down status
  - Can't ping IPv6 addresses
- **flow-tools**
  - Handles Cisco NetFlow V5 – IPv4 only
  - Need NetFlow V9 for IPv6
- **Fluke NetFlow Tracker 3.0.7**
  - Can accept NetFlow V9
  - Can show 6to4 IPv6 traffic
- **Snort 2.8**
  - IPv6 support is incomplete
  - Needs addresses like 2001:0:0:0:0:0:0:0/16
- **No IPv6 usage statistics collection !!!**

Problem: IPv6 Capability of Middle-boxes

- **CSM - Content Switch Module**
  - Load-balances and routes IPv4 only
  - Could add extra IPv6-only router interface to provide IPv6 service to real server Vlan
- **FWSM - Firewall Services Module**
  - L2 mode - Pass IPv6 without inspection
  - L3 mode - IPv6 inspected, but no Multicast
- **SSL Services Module**
  - IPv4 only
- **WISM - Wireless Services Module**
  - IPv6 multicast feature clashes with dynamic Vlan feature
- **SCE 2000 - Service Control Engine**
  - Pass IPv6 without inspection
- **VPN 3000 Concentrators**
  - VPN over IPv4 only, IPv4 inside (could do v6-in-v4 in VPN)

Lessons Learnt

- **IPv4 not broken yet. Users see little need to migrate to IPv6, or dual-stack**

- **IPv4 address exhaustion like Y2K, or Global Warming, or Urban Sprawl, or …**
  - But no definite deadline date
  - IPv4 will continue to work after exhaustion
  - "Will effect others, not us"

- **Enabling IPv6 (over a relaxed timescale) has created opportunities for improving many IPv4 practices**
  - Address plan
  - ACLs
  - Router configuration management
  - Network monitoring

To Do

- **IPv6 E-mail and LDAP services**
- **IPv6 for South Africa and Malaysia campuses**
- **IPv6 usage statistics**
- **More**
  - IPv6 servers
  - IPv6 user subnets
  - IPv6 education

Monash will be part of VIC6 TestNet

Questions?