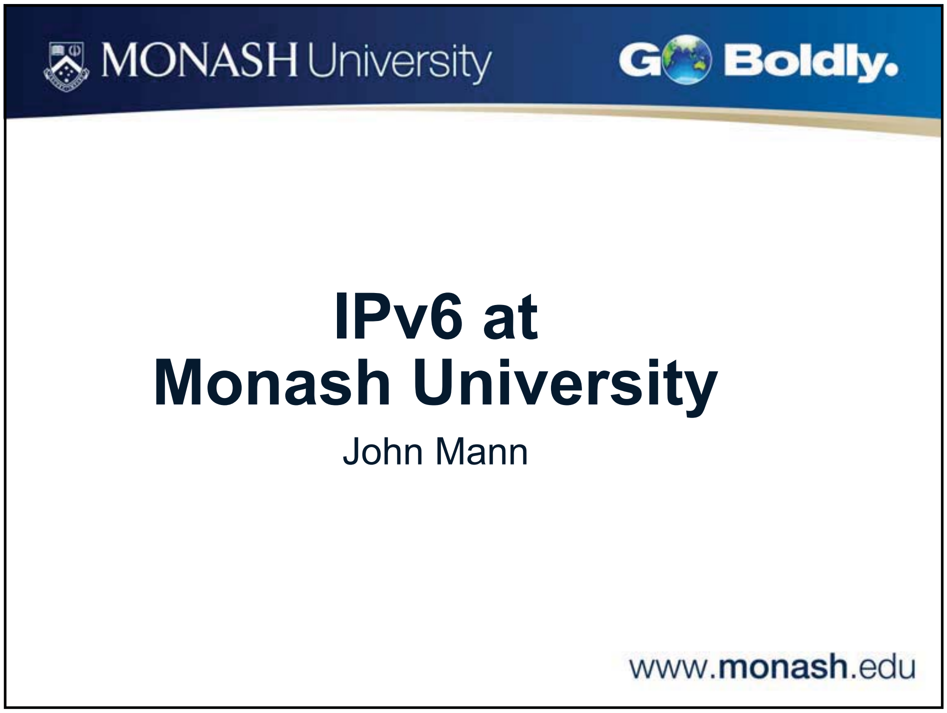


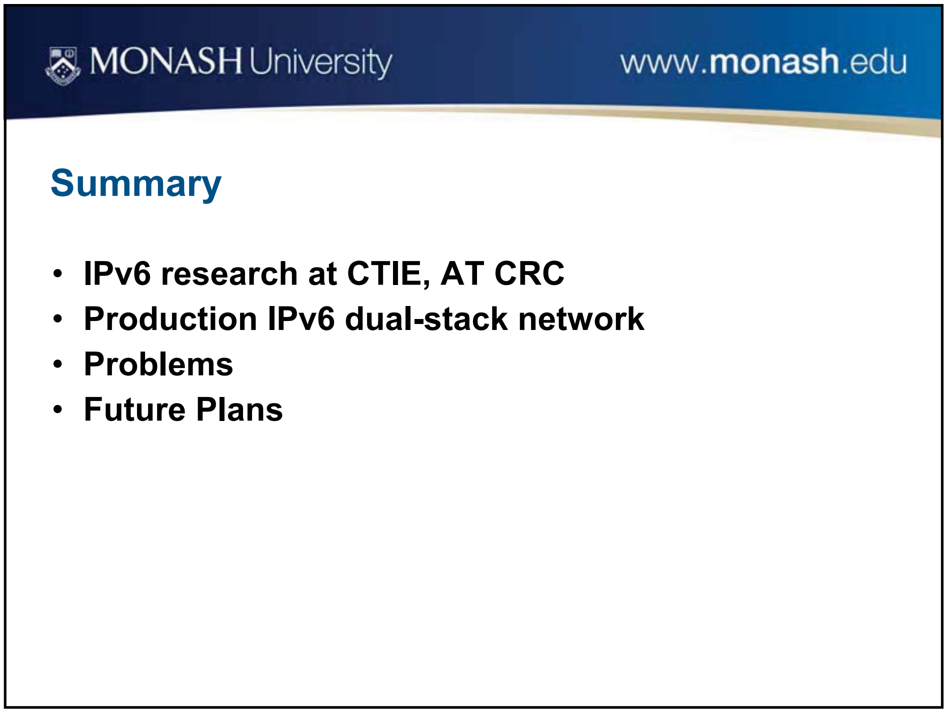
MONASH University

GO Boldly.

IPv6 at Monash University

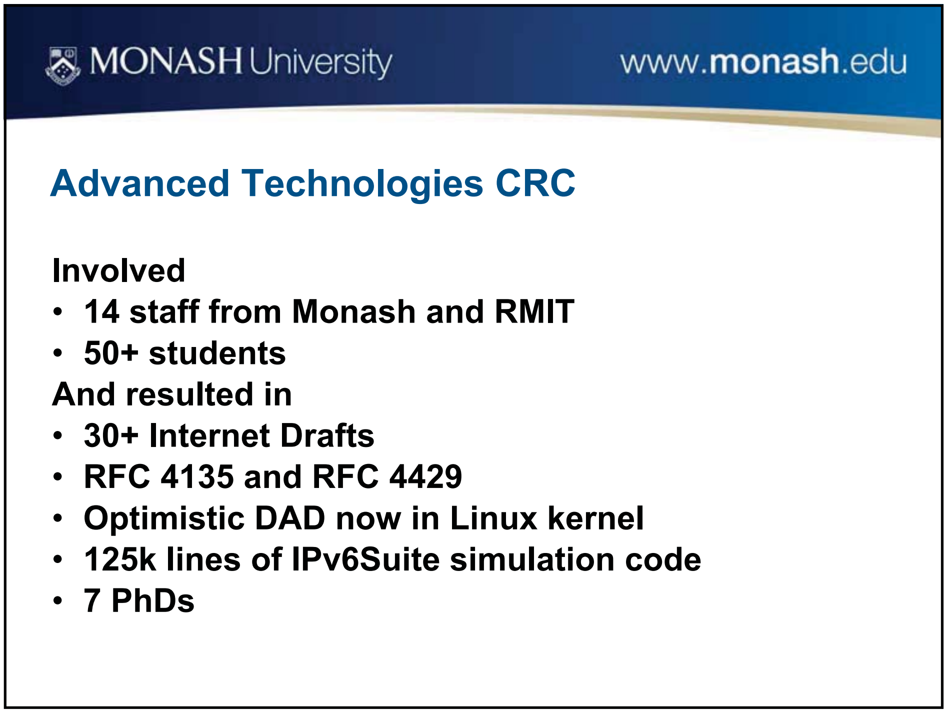
John Mann

www.monash.edu



Summary

- IPv6 research at CTIE, AT CRC
- Production IPv6 dual-stack network
- Problems
- Future Plans



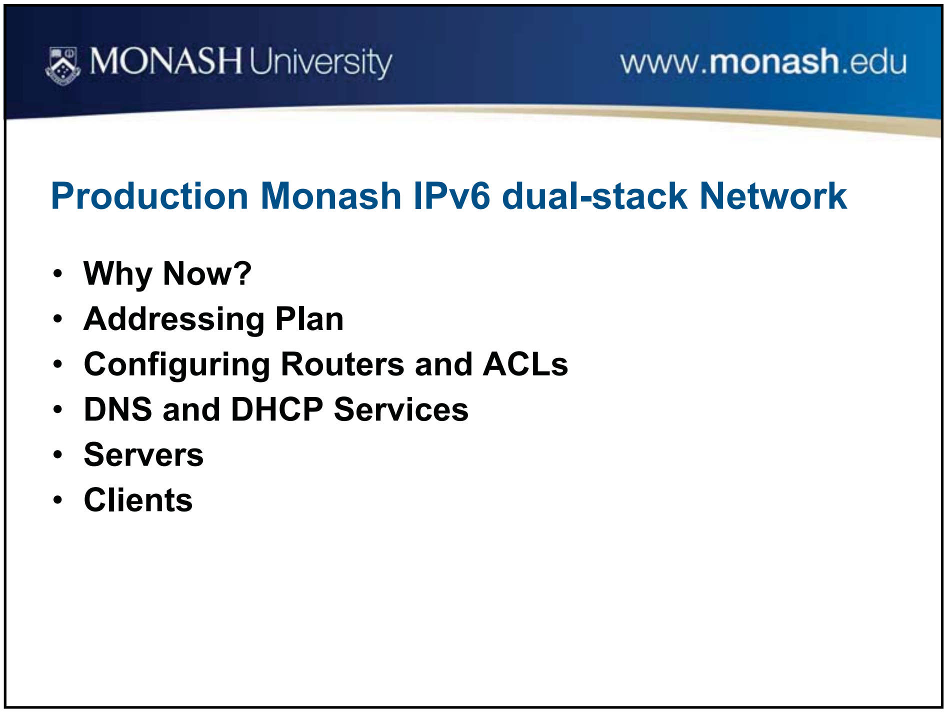
Advanced Technologies CRC

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

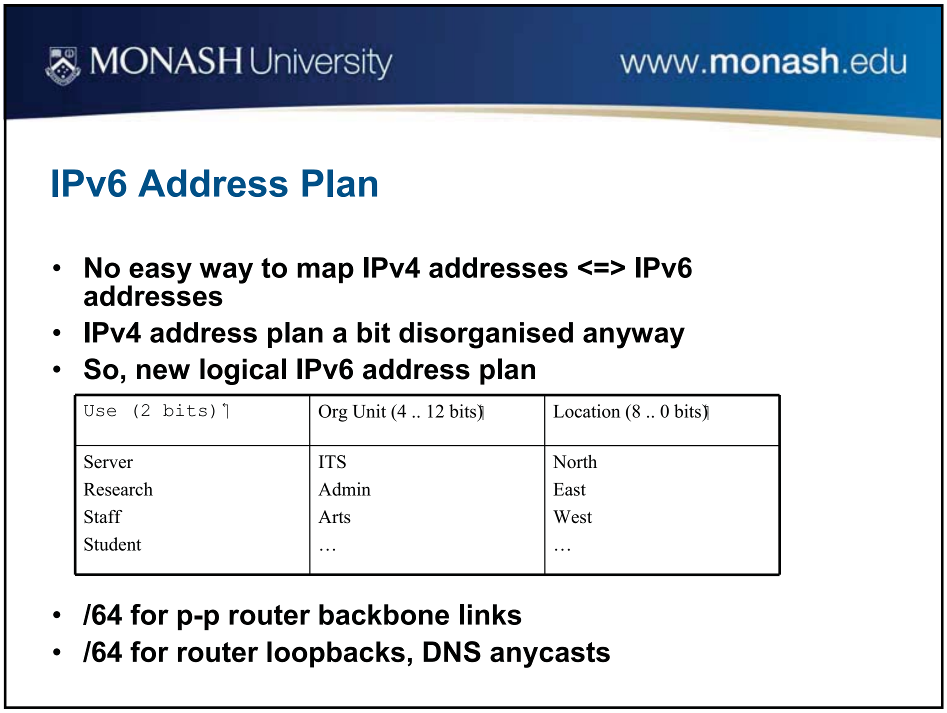
- Why Now?
- Addressing Plan
- Configuring Routers and ACLs
- DNS and DHCP Services
- Servers
- Clients

Why Now?

- Monash is like a battleship, it will take a long time to change direction
- Need to break the chick-and-egg problem by providing the IPv6 infrastructure
- Need to raise IPv6's profile, and show that it does actually work
- Need to find out what we don't know
- 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

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**

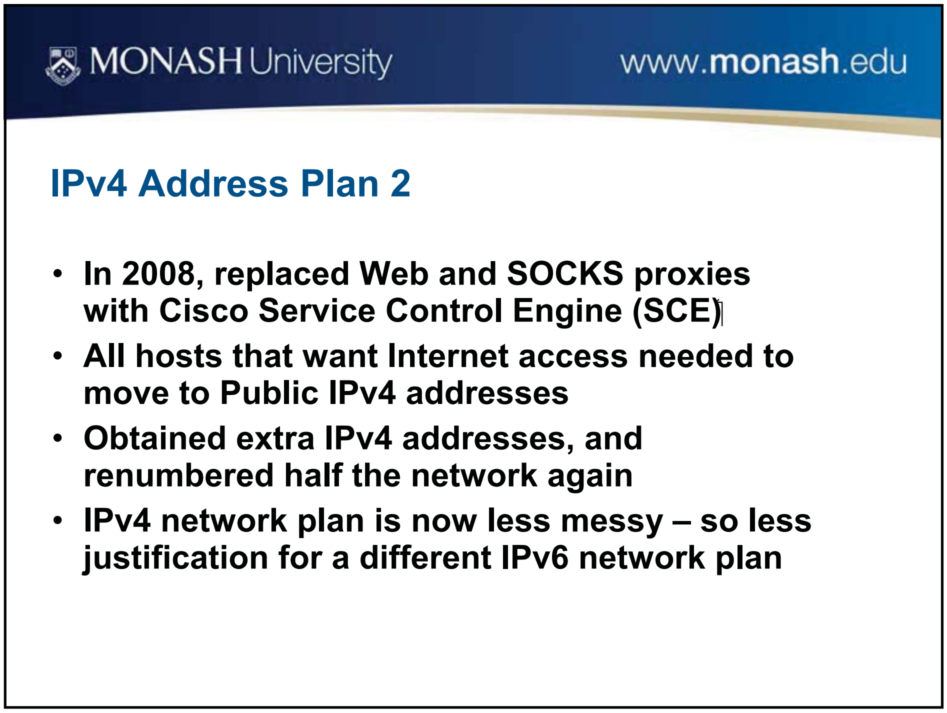


IPv6 Address Plan

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

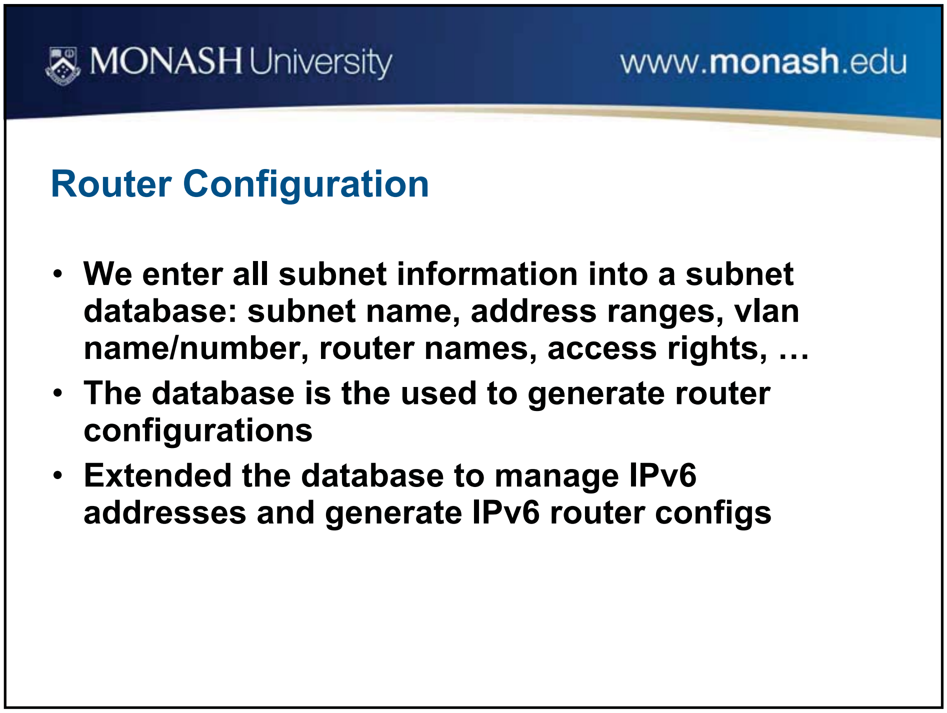
Use (2 bits)	Org Unit (4 .. 12 bits)	Location (8 .. 0 bits)
Server	ITS	North
Research	Admin	East
Staff	Arts	West
Student	…	…

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



IPv4 Address Plan 2

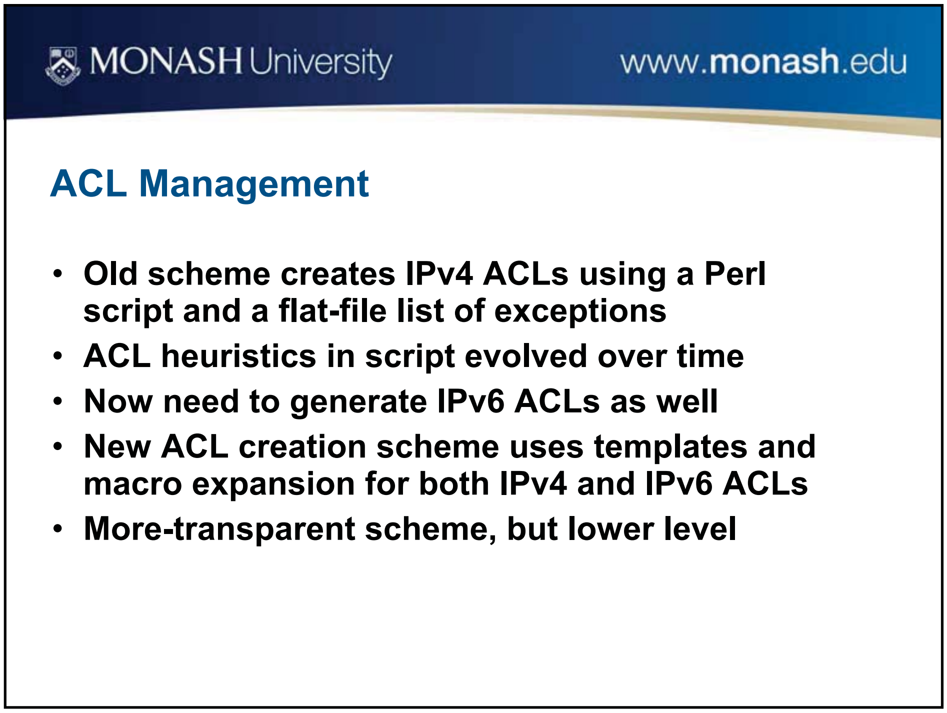
- In 2008, replaced Web and SOCKS proxies with Cisco Service Control Engine (SCE)
- All hosts that want Internet access needed to move to Public IPv4 addresses
- Obtained extra IPv4 addresses, and renumbered half the network again
- IPv4 network plan is now less messy – so less justification for a different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



MONASH University www.monash.edu

Router Configuration

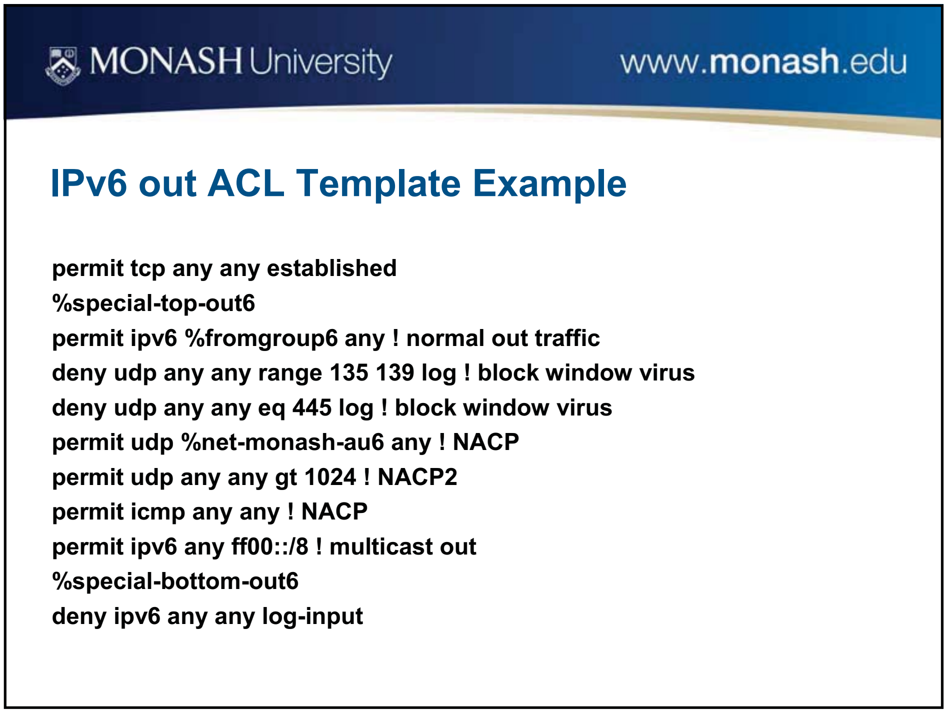
- We enter all subnet information into a subnet database: subnet name, address ranges, vlan name/number, router names, access rights, …
- The database is the used to generate router configurations
- Extended the database to manage IPv6 addresses and generate IPv6 router configs



MONASH University www.monash.edu

ACL Management

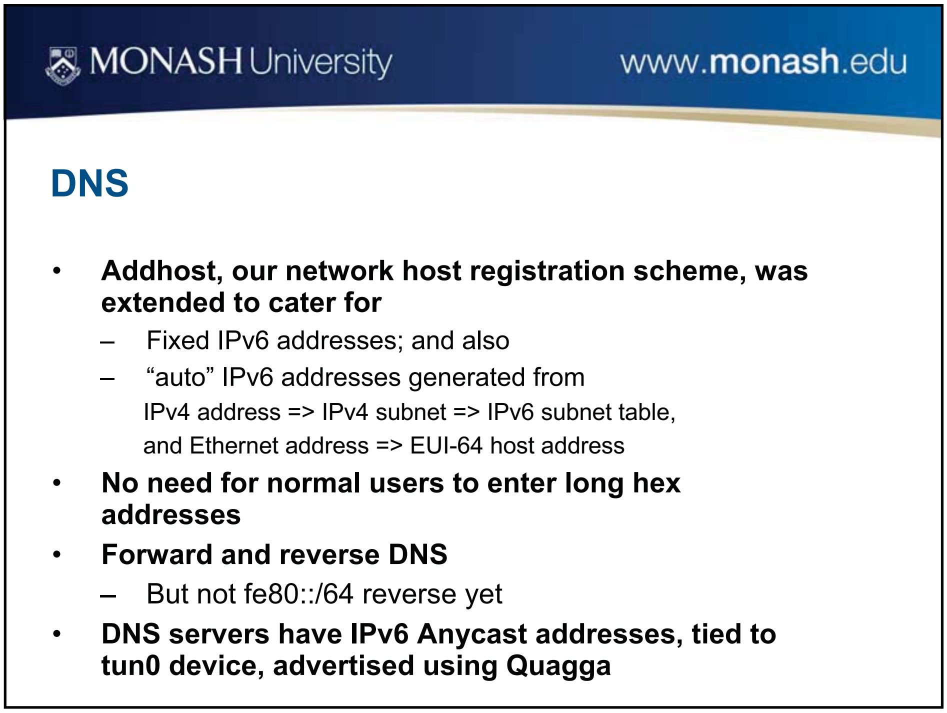
- Old scheme creates IPv4 ACLs using a Perl script and a flat-file list of exceptions
- ACL heuristics in script evolved over time
- Now need to generate IPv6 ACLs as well
- New ACL creation scheme uses templates and macro expansion for both IPv4 and IPv6 ACLs
- More-transparent scheme, but lower level



MONASH University www.monash.edu

IPv6 out ACL Template Example

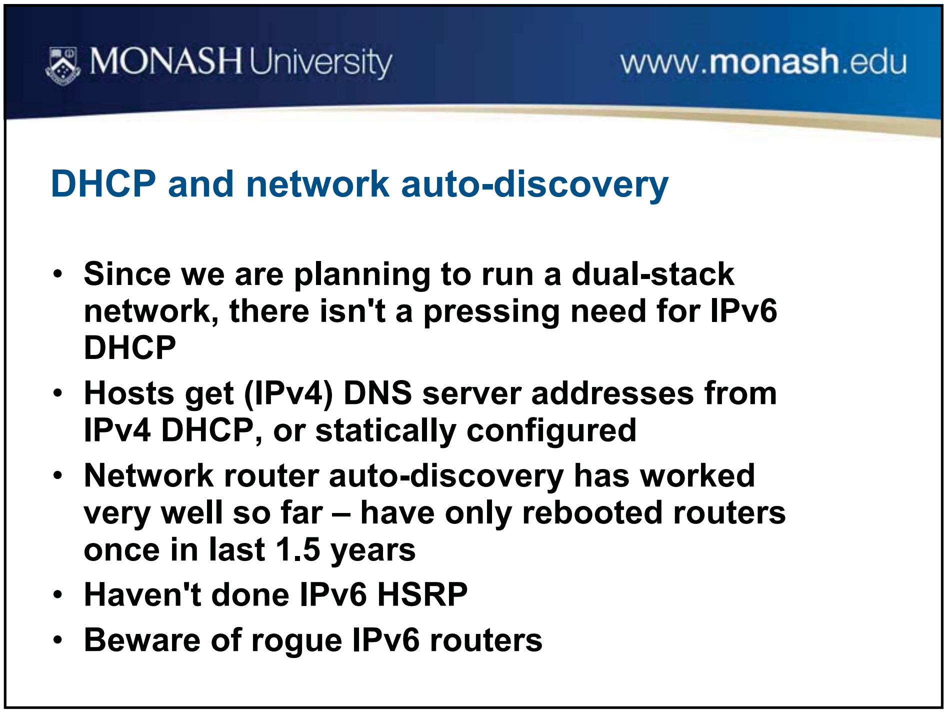
```
permit tcp any any established
%special-top-out6
permit ipv6 %fromgroup6 any ! normal out traffic
deny udp any any range 135 139 log ! block window virus
deny udp any any eq 445 log ! block window virus
permit udp %net-monash-au6 any ! NACP
permit udp any any gt 1024 ! NACP2
permit icmp any any ! NACP
permit ipv6 any ff00::/8 ! multicast out
%special-bottom-out6
deny ipv6 any any log-input
```



MONASH University www.monash.edu

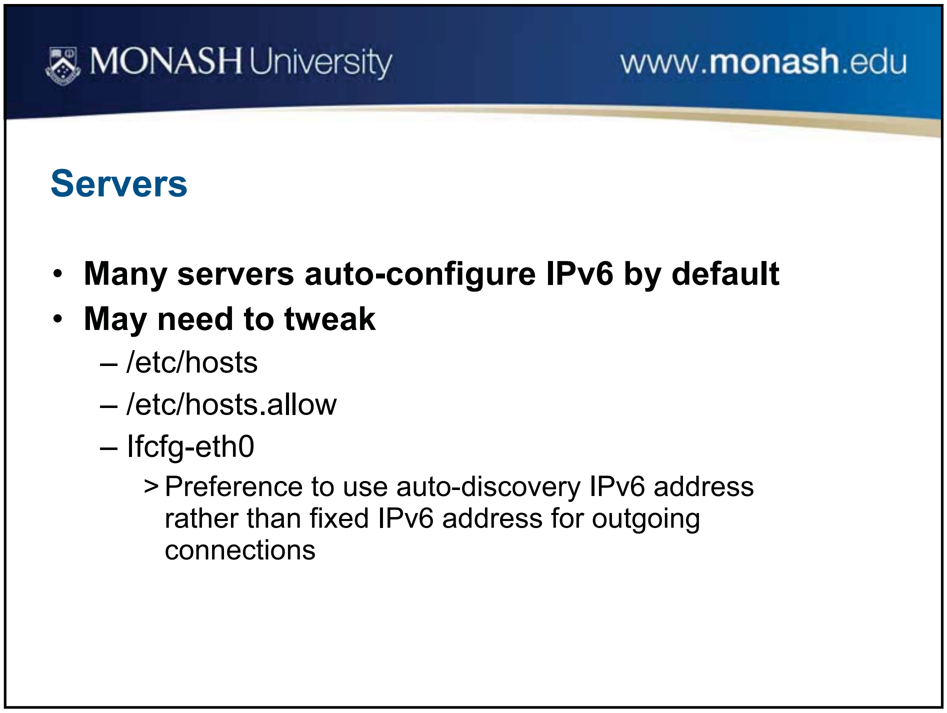
DNS

- **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 IPv6 Anycast addresses, tied to tun0 device, advertised using Quagga**



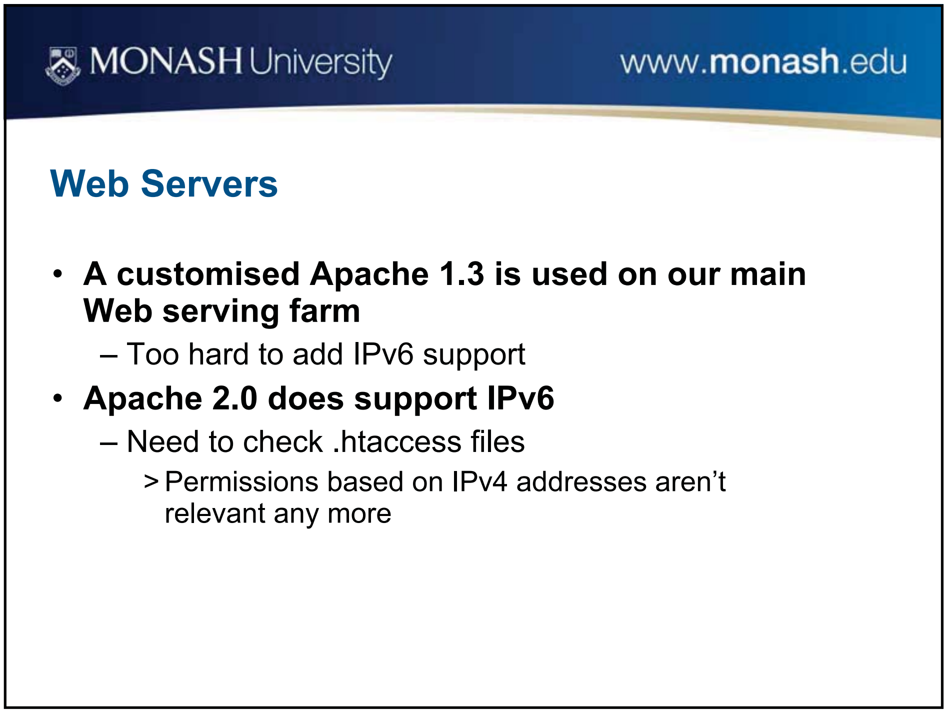
DHCP and network auto-discovery

- 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



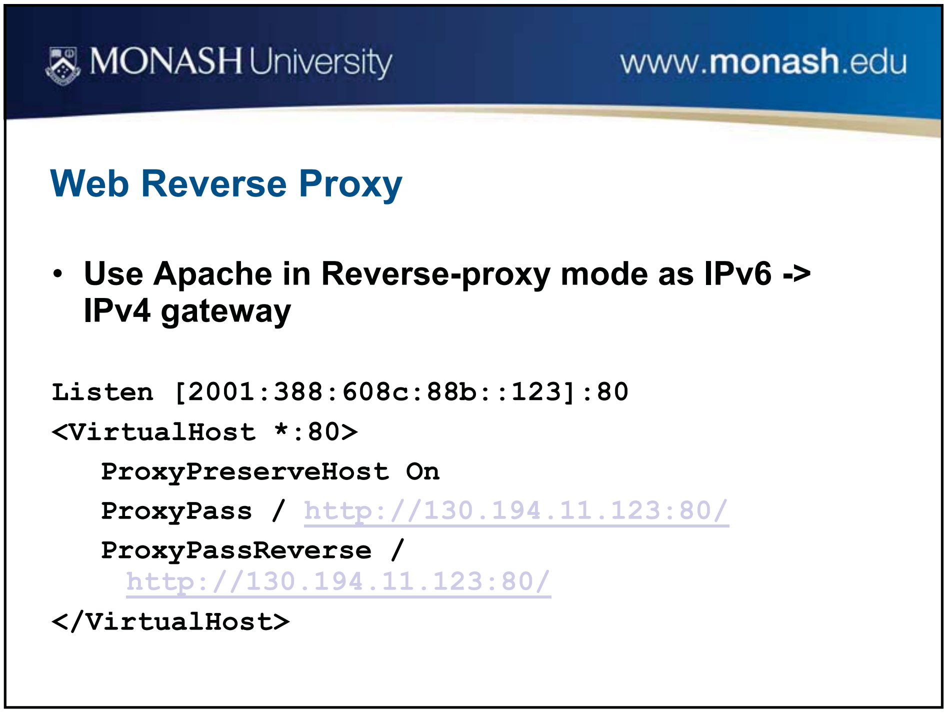
Servers

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



Web Servers

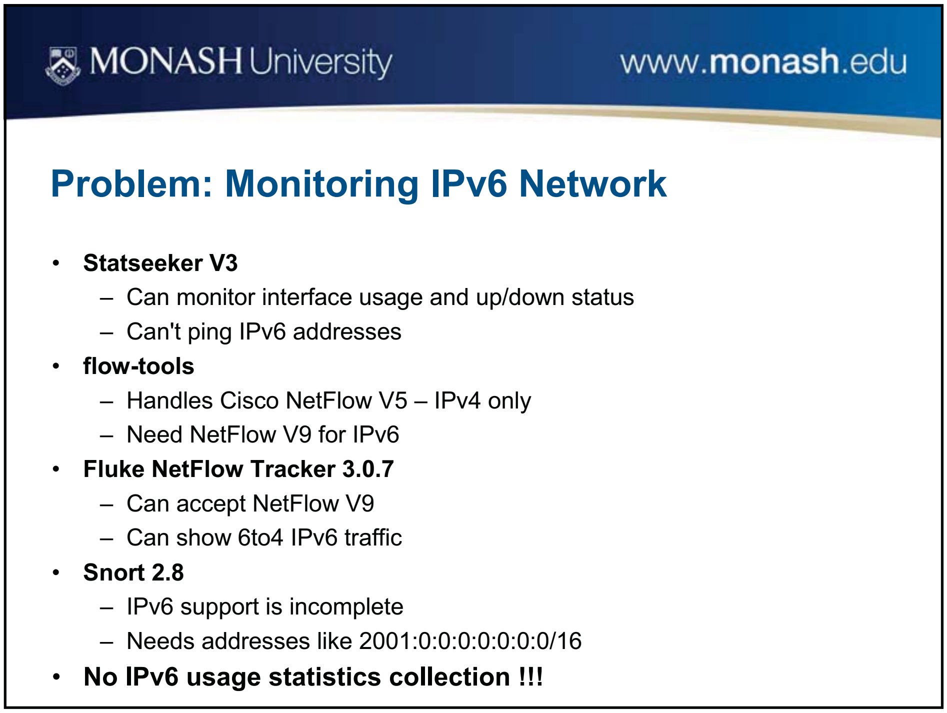
- **A customised Apache 1.3 is used on our main Web serving farm**
  - Too hard to add IPv6 support
- **Apache 2.0 does support IPv6**
  - Need to check .htaccess files
    - > Permissions based on IPv4 addresses aren’t relevant any more



Web Reverse Proxy

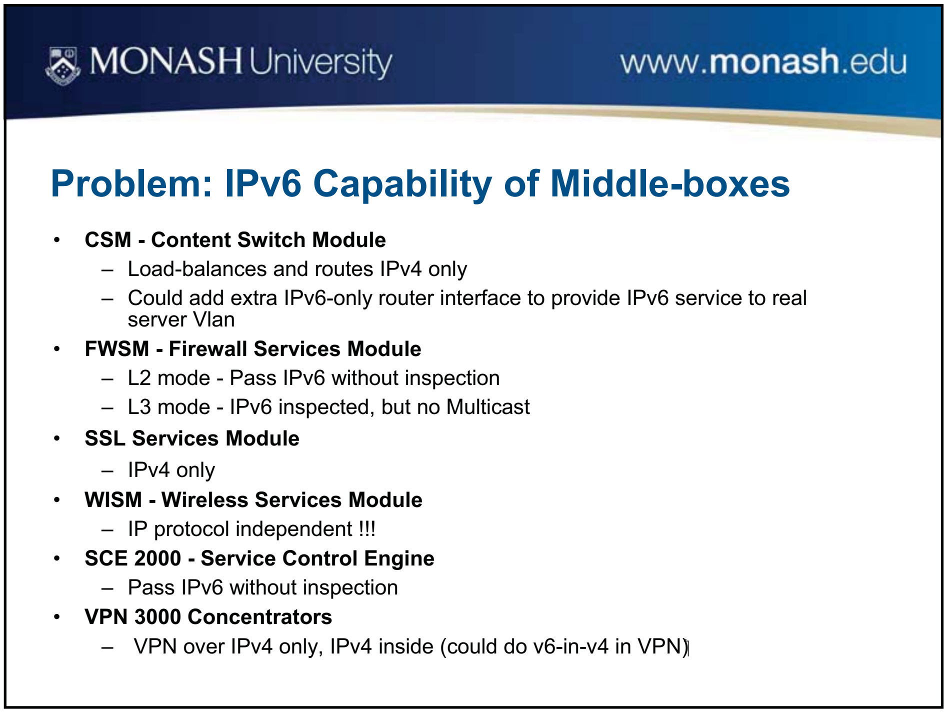
- **Use Apache in Reverse-proxy mode as IPv6 -> IPv4 gateway**

```
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>
```



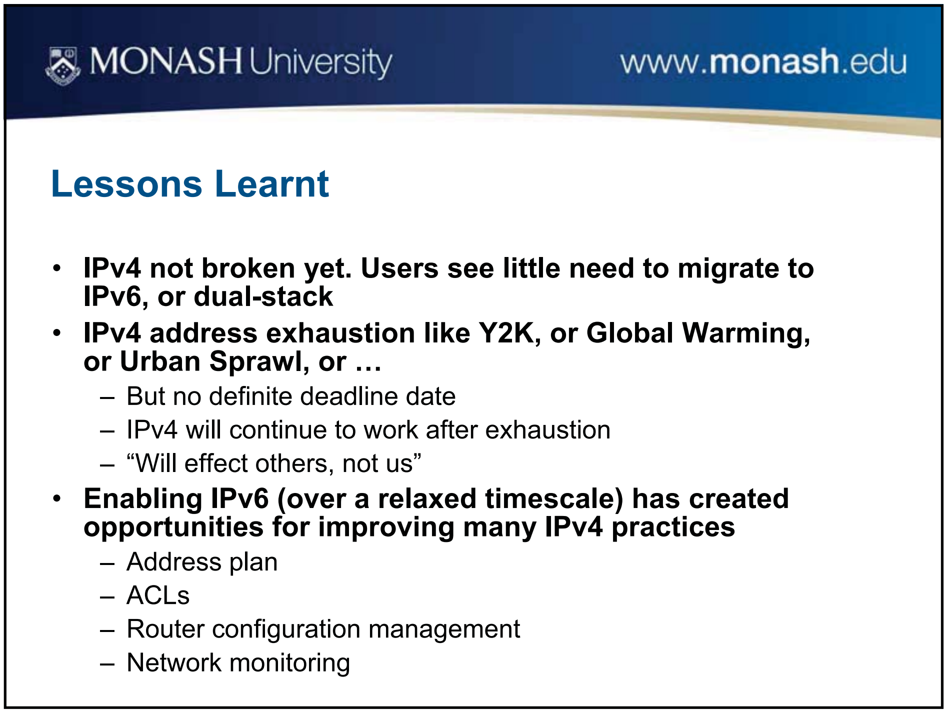
Problem: Monitoring IPv6 Network

- **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 !!!**



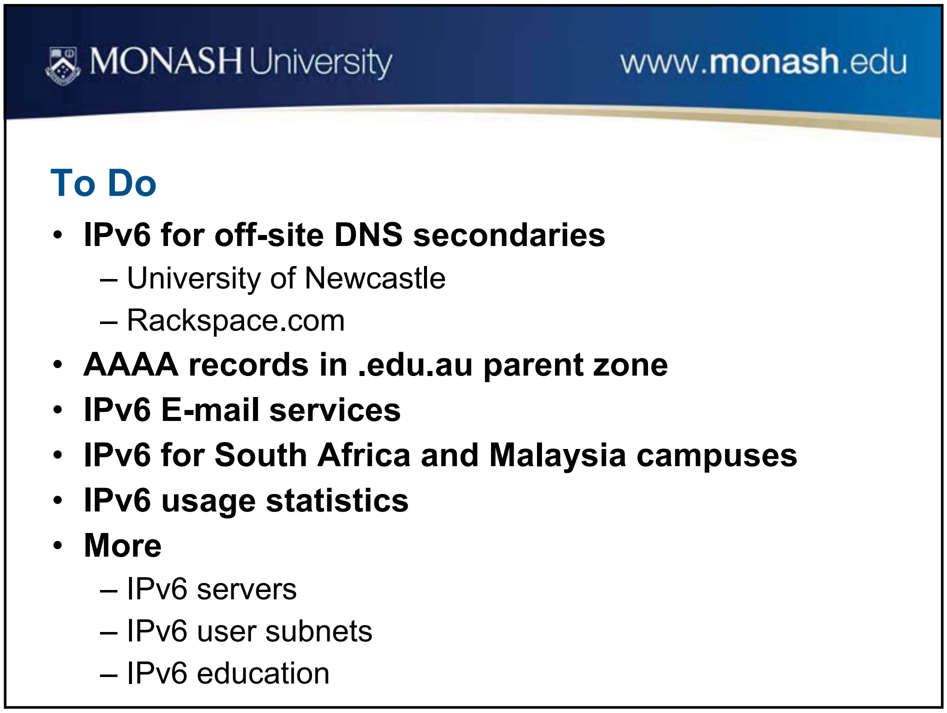
Problem: IPv6 Capability of Middle-boxes

- **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**
  - IP protocol independent !!!
- **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 for off-site DNS secondaries**
  - University of Newcastle
  - Rackspace.com
- **AAAA records in .edu.au parent zone**
- **IPv6 E-mail services**
- **IPv6 for South Africa and Malaysia campuses**
- **IPv6 usage statistics**
- **More**
  - IPv6 servers
  - IPv6 user subnets
  - IPv6 education