MONASH University

Information Technology Services

Network Registration using "addhost"

- John Mann

Network Infrastructure Services

Monash University

Agenda

- **Background**
- **“addhost” database**
- **Problems encountered**
- **Uses for network registration database**
- **Lessons learnt**
- **Future**

Monash data network

- **Campuses**
  - 6 main campuses in Victoria
  - ~10 smaller campuses in Victoria
  - South Africa
  - Malaysia
- **Edge**
  - 40,000 Gigabit Ethernet-capable ports
  - 420 Wireless Access Points
  - 47,000 registered IP addresses

Network Registration in 1994

- **Old process to add new computer:**
  - Manual edit bootptab
  - Manual edit dept.monash.edu.au forward DNS
  - Manual edit 130.194.NNN reverse DNS
- **Averaged 40..45 new machines per week**
- **Required skill and care to do properly**
- **"John can't go on holiday" problem**

Essential Network Services Project

- **Need for always-on "Network Dial-Tone"**
- **Provide DHCP, DNS, NTP, TFTP**
- **For a reliable network, we claimed a mandate that everything on network be (pre-)registered**
- **Committee with wide representation**
- **Wish-list bloat**
  - Inventory of installed programs on each PC
  - Hard disk size, etc
- **Search of Usenet lead to “addhost”**
  - Acceptable to committee

“addhost”

"addhost is a ncurses(3) front-end to a Berkley DB database.

Also "rmhost", "baddhost", "brmhost", "dumphost" and "addhostd"

Primary key: hostname and aliases

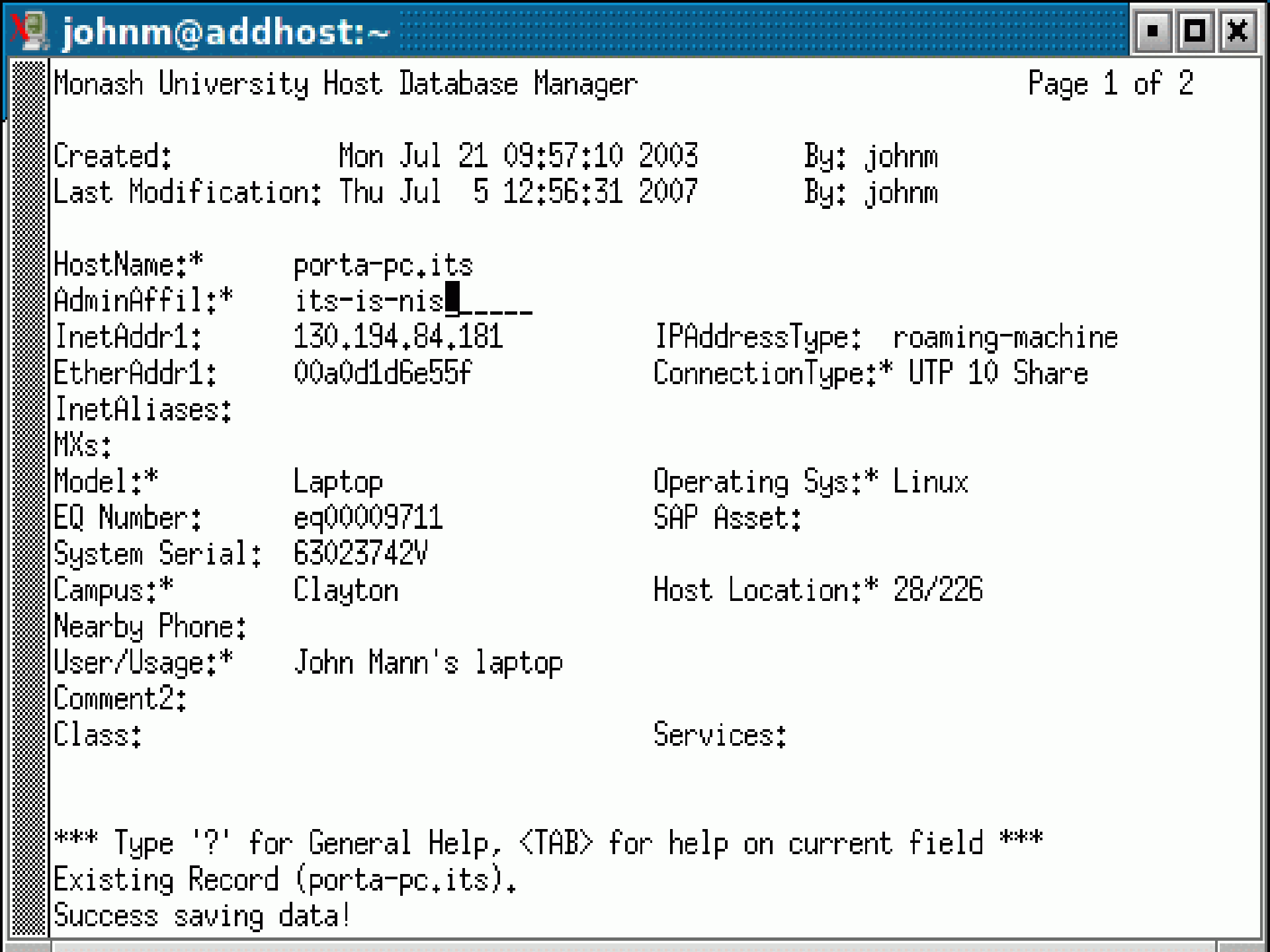
Secondary keys: IP address, Ethernet address, EQ and Serial numbers

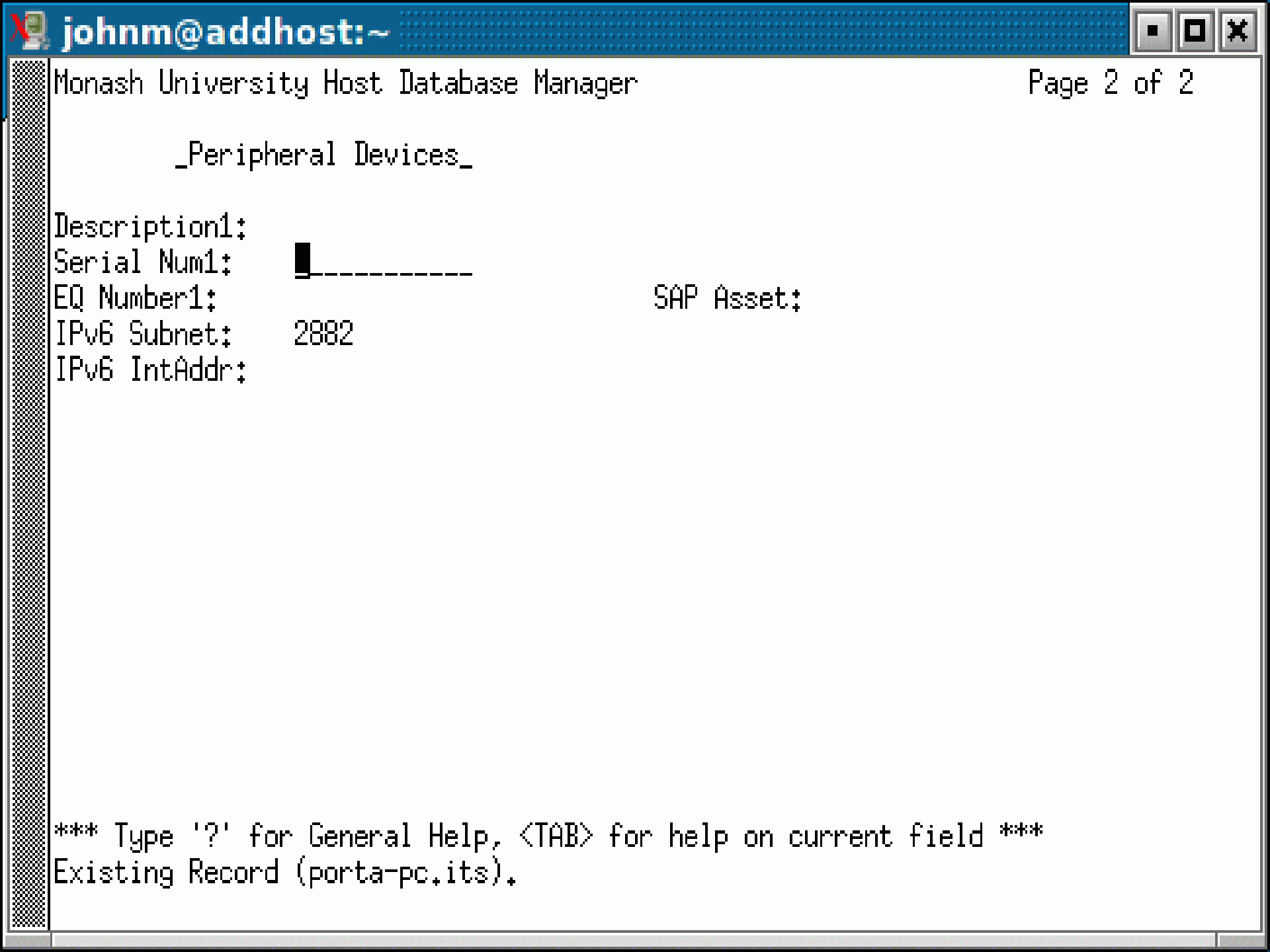
Database entries being viewed are locked from access by others

Low bit-rate UI, usable from anywhere, even Nokia 9000 phone.

From John C. Hardt of University of Colorado, Feb 1994

Still in use: http://www.colorado.edu/its/networking/terminology.html


johnm@addhost:~
Monash University Host Database Manager Page 1 of 2
Created: Mon Jul 21 09:57:10 2003 By: johnm
Last Modification: Thu Jul 5 12:56:31 2007 By: johnm
HostName:* porta-pc.its
AdminAffil:* its-is-nis
InetAddr1: 130.194.84.181 IPAddressType: roaming-machine
EtherAddr1: 00a0d1d6e55f ConnectionType:* UTP 10 Share
InetAliases:
MXs:
Model:* Laptop Operating Sys:* Linux
EQ Number: eq00009711 SAP Asset:
System Serial: 63023742V
Campus:* Clayton Host Location:* 28/226
Nearby Phone:
User/Usage:* John Mann's laptop
Comment2:
Class: Services:
*** Type '?' for General Help, <TAB> for help on current field ***
Existing Record (porta-pc.its).
Success saving data!


johnm@addhost:~
Monash University Host Database Manager
Page 2 of 2
Peripheral Devices
Description1:
Serial Num1:
EQ Number1:
SAP Asset:
IPv6 Subnet: 2882
IPv6 IntAddr:
*** Type '?' for General Help, <TAB> for help on current field ***
Existing Record (porta-pc.its).

“addhost” fields

- **HostName**
  - Just “host.subdomain”
  - Exactly 1 level of subdomain
  - Post-processing adds parent domain names
- **AdminAfil**
  - Hierachical name space
    - > Subdomain-part-subpart
  - Used to control who can add/modify records
  - 338 different AdminAfills
  - 396 authorized administrators
    - > Training courses run regularly

“addhost” fields

- **InetAddr1**
  - Stores the (single) IP address of a host
  - Has a “Presto” feature to choose the next available address on a subnet
- **IPAddressType**
  - Controls types of DNS and DHCP records generated
  - Network behaviour expectations
- **Computer identification and location / use fields**
- **Extra fields to track peripheral, e.g. display screen**

Generated files

- **DNS Zone files**
  - Builds multiple country domains
    - > Australian IP => .edu and .edu.au
    - > South Africa IP => .edu and .ac.za
    - > Other IP => .edu
  - If IPv6 Subnet field, then generate AAAA records
    - > Use registered IPv6 Interface address, or generate from Ethernet address
  - Also generates MX entries, reverse zone files
  - No CNAME records
  - No invalid syntax or missing “.” 's

Generated files

- **DHCP config files**
  - Creates static IP entries, known and unknown client pools
  - Uses a per-subnet template from Subnet Database
  - TODO: dhcpv6 config files
- **other**
  - Feed to Webnet network monitoring and billing system
  - Feed to monIP, monDHCP tools
  - RADIUS wireless Ethernet Address authentication
  - Ethers files for sniffers (88,700 entries)
- **Files generated every 15 minutes during business hours**

One Computer = 1 IP = 1 Ether address?

- **Servers can have multiple NICs**
  - IP failover or Ethernet teaming
  - Extra addhost records for each interface
- **Computers can have multiple names**
  - Use InetAliases: field if <6 extras
  - Or “master.extra” file for e.g. Central Web farm vhosts
- **Routers have many Interfaces**
  - A script adds/removes per-interface addhost records
  - Also extra *router-all* name giving all IPs of router.
- **Laptops have wired and wireless interfaces**
  - Treat as 2 separate devices (YUK)

Dynamic DNS?

- **WINS was a disaster**
  - Showed that end-users couldn't be trusted to name their own machines. Many called “SERVER”, “WWW” ...
- **Administrator knows best**
  - Central management, not end-user
  - Tracking and accountability for billing
- **Microsoft Active Directory**
  - Tolerated, but not part of the official DNS tree
- **Missing:**
  - Would be nice to find IP of roaming clients, without churning the addhost database et al too much

Student-owned computers in Residences?

- **1000 network ports were installed in student residences**
  - Students want to add computers out-of-hours
  - Students move rooms, change/swap computers frequently
  - Huge influx at beginning of each semester
  - Need to de-register computers when students move out
- **Assign static IP to each room ?**
  - Required too much skill from each resident
  - Address collisions were frequent and very hard to resolve
- **Created Self-Registration Web page**

Student Wireless laptops?

- **Problem:**
  - Didn't want to burden ITS or Faculty helpdesks with registering student laptops
  - Need to bill correct Faculty for student's wireless access
    - > But Faculty want to limit potential costs
  - Student wireless devices change a lot
  - Need to track when student leaves, and de-register computers
- **Allowed all students to use the Network Self-Registration system to register 1 device**

Self registration (ITS) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://addhost.its.monash.edu.au/cgi-bin/register

Go

Skip to content | Change text size

MONASH University

Monash home | About Monash | Faculties | Campuses | Contact Monash

Staff directory | A-Z index | Site map SEARCH SEARCH ITS website Go

Monash University > ITS > Students > Wireless

Network self registrations for usercode "johnm", AdminAffil "its-is-nis", MRS Affil "mannix-stud"

The self-registration scheme has been changed from the beginning of 2006.

Students enrolled in a course can self-register one Ethernet card for wireless use.

Also, residents in MRS accomodation can self-register one Ethernet card for wired use.

Staff can not create new self-registrations

For extra self-registrations, contact your l presentative.

Enter two fields

Simple controls

Your Network Self Registrations

Hostname	Ethernet addres	Contact infor tion	Connection	
johnm-wired-self.mannix	none	none	none	Register
johnm-wlan-self.its	000423506e90	Machine owned by johnm	Wireless	Modify Deregister

Note: The Ethernet address must be 12 hexadecimal (0..9 or a..f) characters long (if necessary, insert leading 0's to make 6 pairs of digits).

Note: It takes 30 minutes before any new or changed registration will work on the network.

The Contact information may be used to contact you if some problem is found with your network registration, or with your computer's use of the network.

Done

Adblock

Network Self-Registration

- **Registration is billed to student's current Faculty or Residence**
  - Script checks every night, and changes AdminAfil when necessary
- **A registration is deleted**
  - When a student stops being a resident, or stops studying
  - If a new registration is not used within 30 days
  - If a old registration is no used for 180 days
  - An e-mail is sent to the user explaining what happened and why

Use - Everything is Registered

- **No name or address collisions when adding something**
  - Users can't grab a router's or a reserved IP addresses
  - Can't double-register the same name, MAC, serial or EQ number
- **Network sniffing**
  - Ethernet address -> Name
  - IP address -> Name
  - One Spanning-tree packet tells you which port you are plugged into, and if the network is partitioned
  - Useful Ethernet addresses have been registered, e.g. HSRP, IP Multicast, spanning-tree, CDP, Windows PPP

Example “where am I” packet sniffs

```
# tcpdump -e -X -vv ether dst spantree.net
10:20:52.494367 clay-28-202-rk2-fes1.net:3/0/4 > spantree.net, <...>
        0x0000:  4242 0300 0002 023c 0054 0015 c77b 4400  BB.....<.T...{D.
        0x0010:  0000 0007 8054 000e 8464 6600 806c 0300  .....T...df..l..
        0x0020:  1400 0200 0f00 0000 0000 0000 0000       ..............
```

Looking up Ethernet addresses inside packets gives:

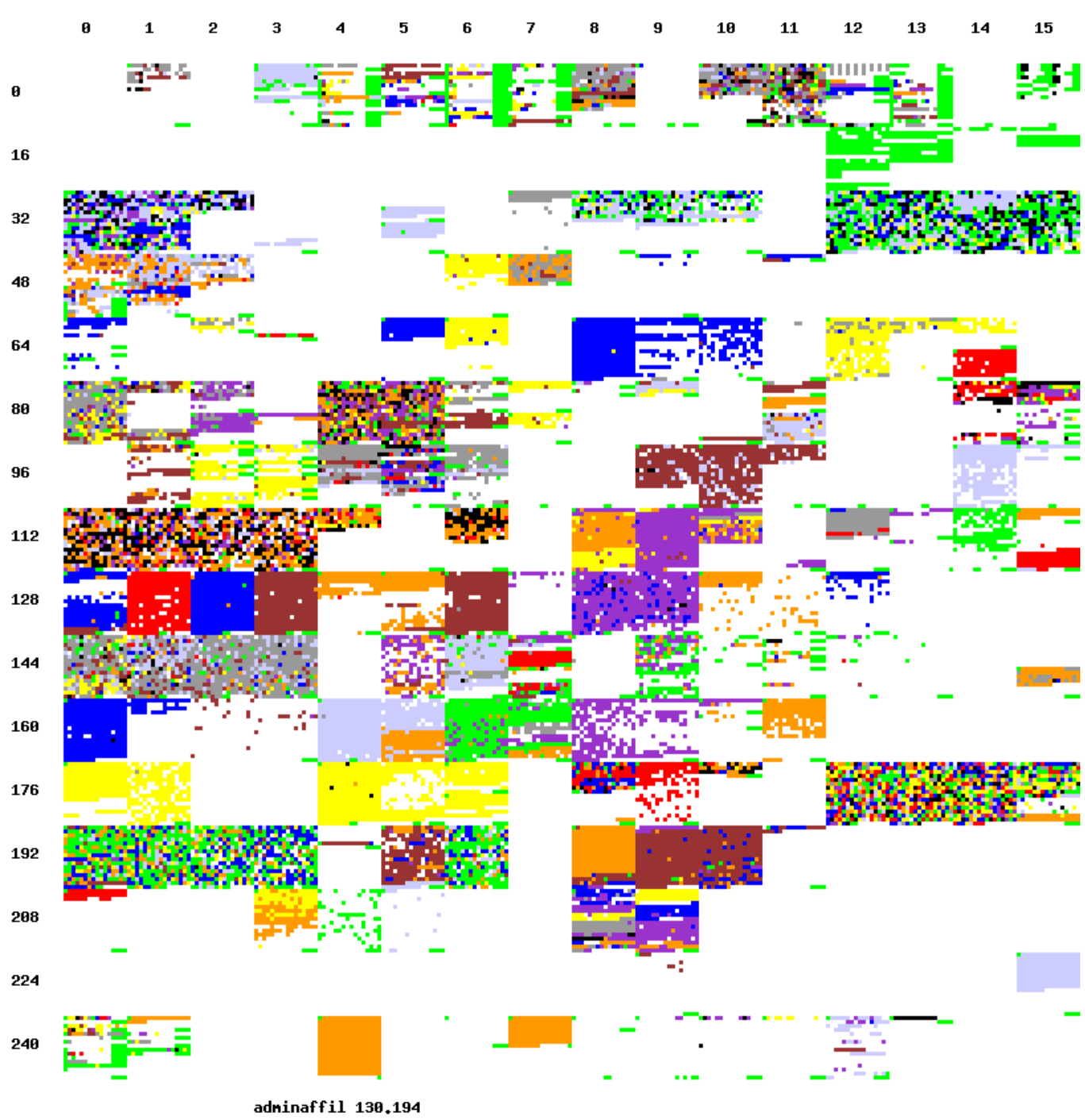
```
# snoop.pl -i eth1
BPDU from 000ab8fd1684(clay-28-202-rk2-fes1.net:3/0/4) bridge 000e84646600
(clay-28-202-rk2-fes1.net) port 108 root 0015c77b4400(west1-gw.net)
"""""""""""""""""""""""""
CDP from 000ab8fd1684(clay-28-202-rk2-fes1.net:3/0/4) dev clay-28-202-rk2-
fes1.net.monash.edu.au port GigabitEthernet3/0/4 VLAN 84
```

Use – Fault finding

- **When something is going wrong**
  - Computer has a virus
  - Someone is downloading things they shouldn't
- **It is incredibly useful to know**
  - Which computer is sending the bad traffic
  - Who added that machine to the network
  - What the machine's purpose is
  - Where is is
  - Possibly a nearby phone number

Use – Managing Address Plan

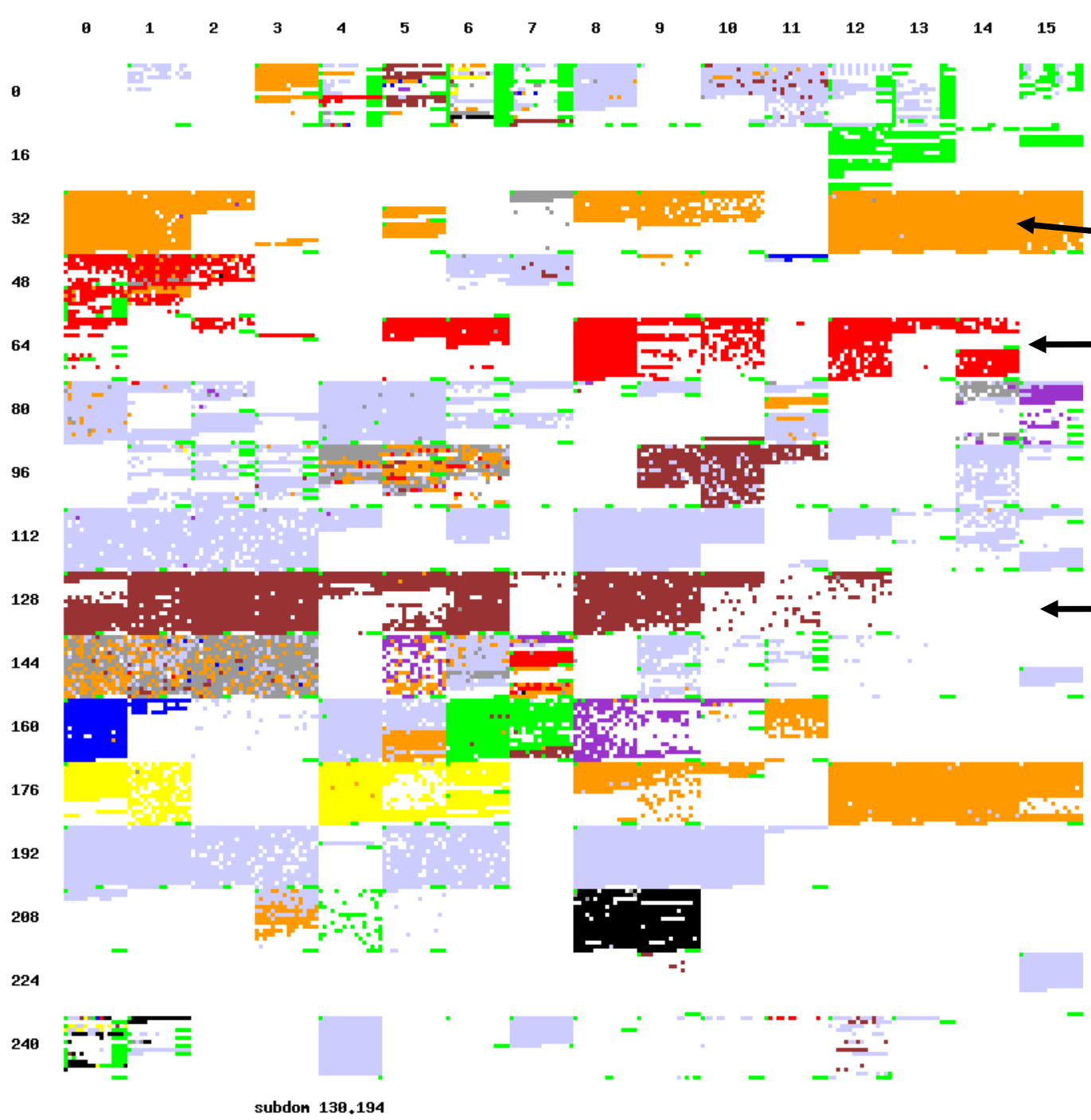
- **Can create reports of subnet utilization**
- **Can create pictures of IP address space coloured by**
  - AdminAffil (who manages / pays for the IP)
  - Subdomain name
  - IP address type (static / DHCP / roaming)
  - How recently seen on network



Coloured by AdminAffil

Each square is 256 addresses.
Whole picture is a /16

Web page can drill in to /24, and then to individual addresses

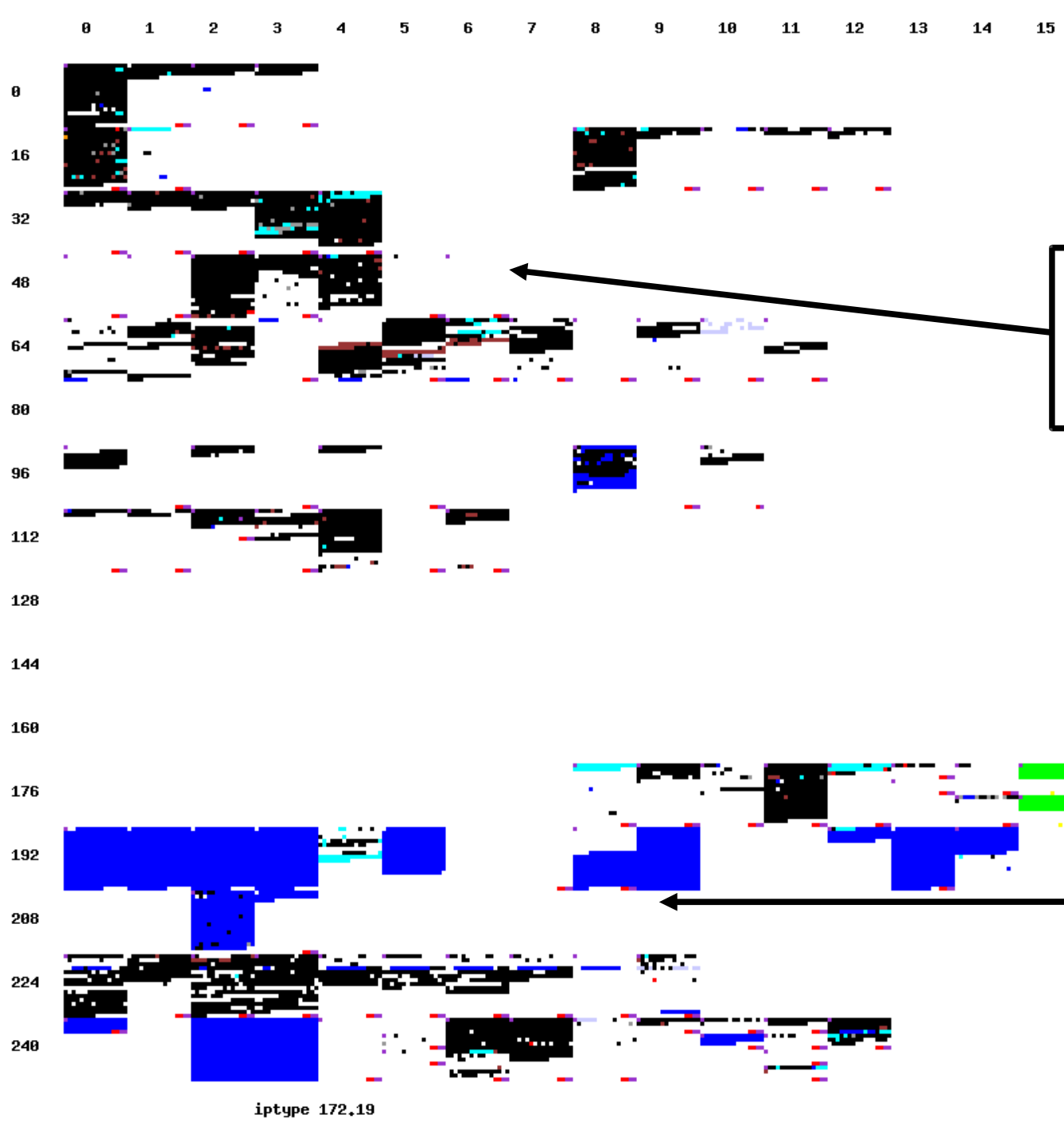


Coloured by subdomain

BusEco

InfoTech

Engineering

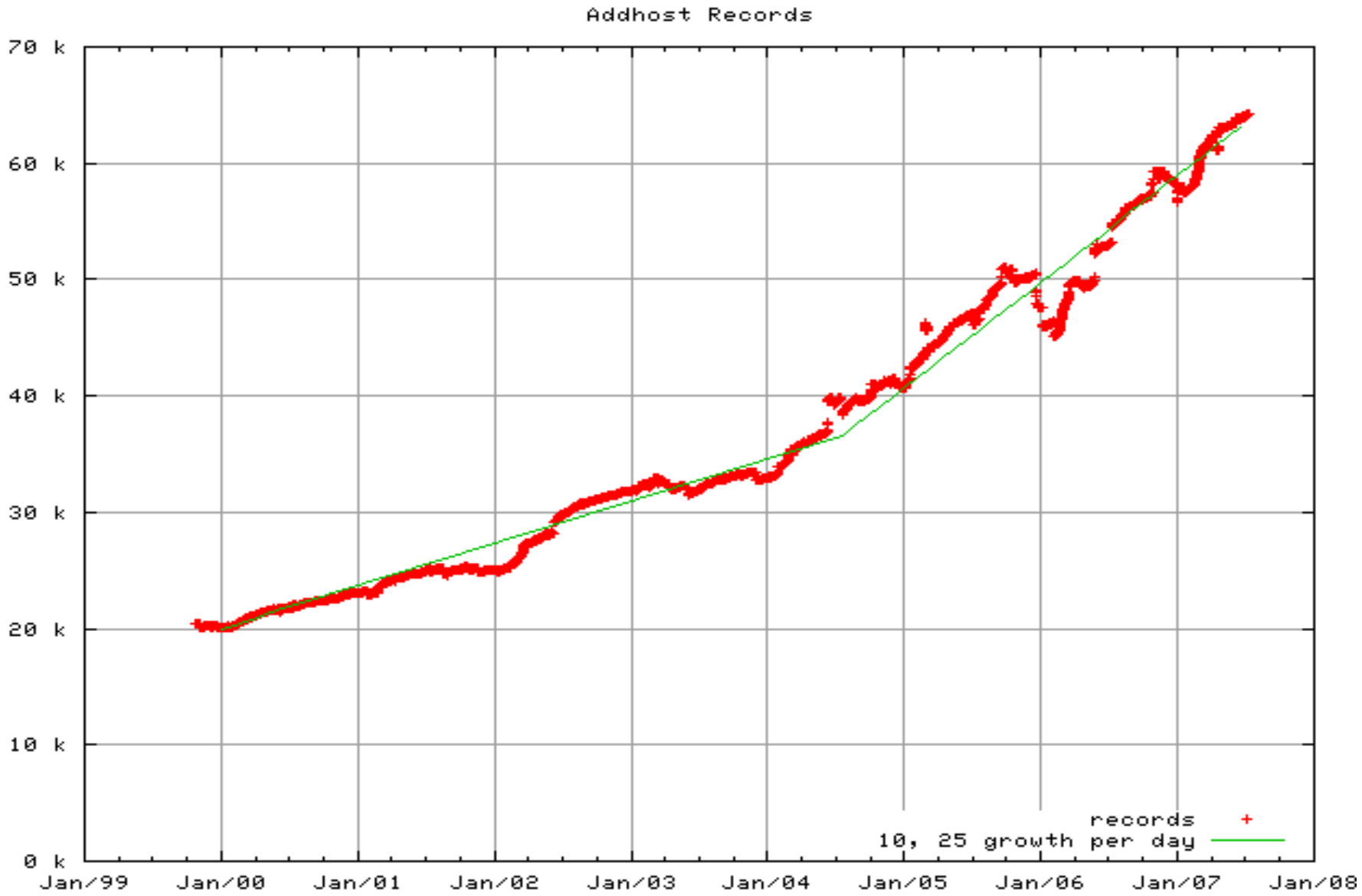


Coloured by IP Type

Student Labs
Mostly Static DHCP

Student
Residences
Dynamic DHCP

Use – Planning for Growth



Use - Billing

- **At Monash, we have a "Network Access Charge" for a**
  - Registered IP address, and/or
  - Registered Ethernet address, and/or
  - Wall outlet switch port
- **We take the largest count of these numbers per AdminAffil and multiply by the monthly charge**

Billing Services 2.0 - Mozilla Firefox <2>

File Edit View Go Bookmarks Tools Help

http://webnet.its.monash.edu.au/Billing/billingsummary

Billing Services 2.1

Network Infrastructure Services

Data Network Services Summary Report: **Monthly Service Charges by Admin Affil**

To ***change details*** or ***cancel ports*** you need to click on the Admin Affiliation link on Today's Report. *(Changes and cancellations can not be made on historical information)* logout.

Logged in: johnm

List Adminaffils

Note: printed

Admin Affiliation	Addhost Records	Addost IP's	Addhost MAC's	Machines Seen	Standard Ports	Server Ports	Seen Ports	Total Ports	Walloutlet	Billable Services
its-is	68	56	45	27	29	0	19	29	27	56
its-is-ews	228	181	203	108	73	1	60	74	47	203
its-is-ims	47	40	43	31	26	1	21	27	26	43
its-is-mgmt	8	5	8	8	14	0	13	14	14	14
its-is-micros	0	0	0	0	23	0	5	23	20	-22
its-is-nis	241	126	220	109	205	7	101	212	120	220
its-is-prod	78	71	74	40	49	4	39	53	33	74
its-is-security	24	17	24	13	5	0	5	5	4	24
its-is-ss	123	112	102	63	92	9	65	101	80	112
Total	817	608	719	399	516	22	328	538	371	724

Done Adblock

Lessons - Databases

"A Database is only a reflection of reality, it isn't reality" - Keith Lewis

- **Some changes to database can effect real world**
  - Change DHCP-assigned IP address
- **But users can change reality to be different from database**
  - Student sells wireless card to friend
  - PC is hard-coded to new IP address ***or*** server is given a secondary IP address
- *Can be difficult to find and fix discrepancies*

Lessons - Databases

"Any database that doesn't have some system to keep it updated will rot and become useless" - Stephen Dart

- **Mechanisms:**
  - Monitor reality and feed back updates – closed loop
  - Monitor reality and raise alarms – open loop
  - If entry bad or not in database, your PC won't work
  - Encourage cleanups by charging for entries, even if computer has gone.
- **Real-time database update syntax checking**
- **Periodic consistency checking**
  - Feedback from file generation, ARP and DHCP logs
  - Nag e-mails every 30 mins up to daily

Lessons - Databases

- **Some fields were created, but not used**
  - Insufficient effort was put in to entering data, keeping it up to date, ***using*** the data – lack of business drivers
  - Avoid replicating data that is/should be in a different database, such as installed software or lease tracking.

    > Link to other databases using common key
- **Fully-specified unique keys are best**
  - A “WallOutlet” field failed partly because it only specified a port relative to a wiring rack, not globally across all of Monash. (There were 3 “C1” ports on my floor)
- **Start with only a few fields, add more when *necessary***

Lessons - Databases

- **A database can be useful even if it can't hold 100% of all possible records**
  - A small number of exceptions, or classes of exceptions, can be handled by some “extras” glued on around the database
  - “addhost” only holds 98% of DNS
  - “addhost” doesn't have Ethernet addresses of individual switch ports

Future

- **Web-based front end**
  - Am to use AJAX for verifying uniqueness of entered data and for enforcing required syntax
  - Still prevent multiple concurrent updates to same record
- **PostgreSQL back end**
  - Move onto same database as other network management and monitoring tools
- **IPv6 enhancements**
  - IPv6=YES will lookup IPv6 subnet based on IPv4 address
  - DHCPv6

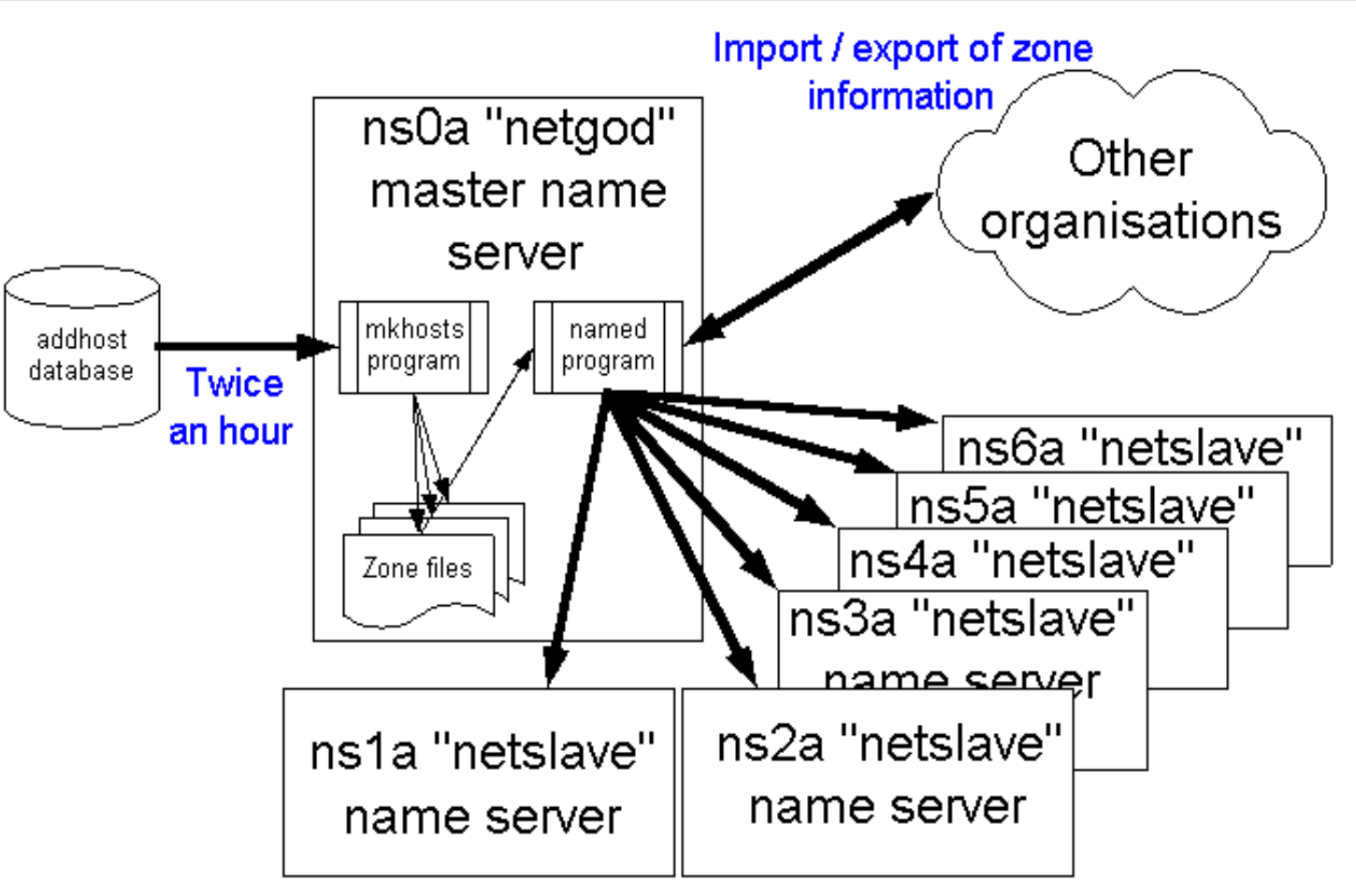
Hardware

- **addhost**
  - Hosts the database
  - All department admins have access
- **ns0a**
  - Network management and control master
  - Only ITS network staff
- **ns1a ... ns6a, ns3, ns8, ns9**
  - Slave machines
  - No user logons
- **nsaa, ns7a**
  - Development, research slave machines

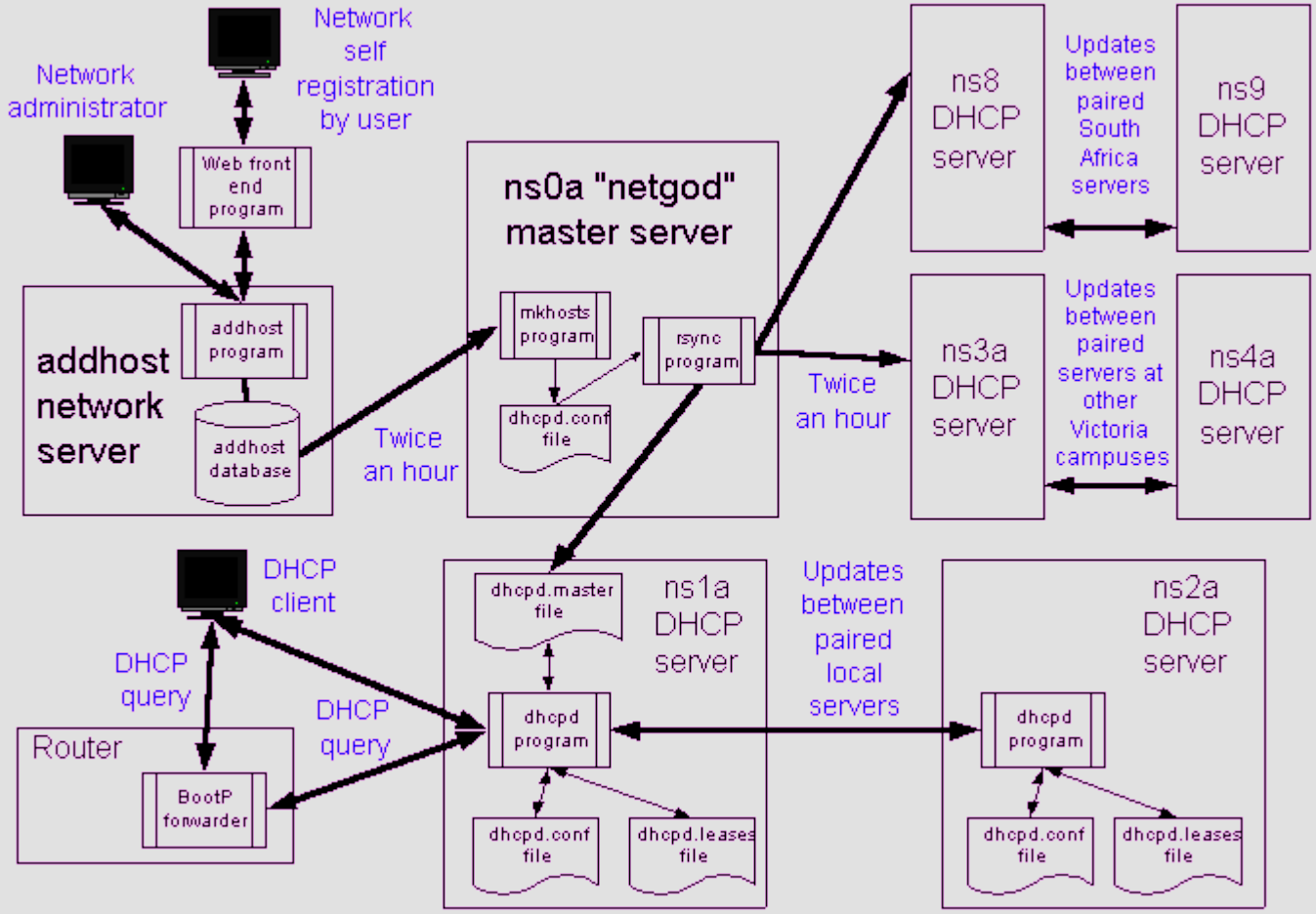
Resilience model

- **Pairs of DHCP servers**
  - Clayton – one per data centre
  - Other Australia – Gippsland + Caulfield
  - Research – one + development box
  - South Africa – 2 blade servers
- **Farms of anycast DNS servers**
  - 130.194.1.99 – 4 machines
  - 130.194.7.99 – 2 machines
- **Servers are dual-power with RAID disks**
  - Common software, config and data files for consistency and to ease administration
  - But, susceptible to common-mode failures

DNS server architecture



DHCP server architecture



Coping with disasters

- **Network catastrophe**
  - Monash falls off network or AARNet breaks
  - ns3 is on a Rackspace.com server along with top few levels of Monash's staic Web tree.
  - ssh to there, update DNS manually, push to secondaries