UQnet: a simple portal for combining & comparing silos of network information & configuration

Danny Thomas

Specialist Systems Programmer

ITS, University of Queensland

Background

- Many network devices and applications are configured individually. Services usually involve several components and I believe too little effort goes into checking between the various configurations involved, e.g. for a web-site does it:
  - have a DNS name resolving to the web-server (site)
    and is that name properly delegated so it is seen on the Internet ?
  - exist in the web-server configuration ?
  - have an ip-address associated with that name that is routed ?
- One approach would be to try an HTTP connection to each `www` . DNS record, but that is more a monitoring function

Background

- The advantage of cross-checking configurations compared to trying HTTP connections is that it identifies web-sites that should be removed.
- There will be complaints when a new web-site is not working, but there's much less care about cleaning up old configuration items. The degree this happens is a reflection of the quality of processes.
- Of course the alternative to cross-checking configurations is a provisioning system which can generate consistent configuration fragments for the various sub-systems.

Outline

- Some History about UQ Network Records
- UQnet: Basic Functionality
- UQnet: Enriching Network Records
- UQnet: Cross-checks between Configurations
  NB the title of this talk mainly refers to this section
- UQnet: Other Reports

NB the UQnet portal should be accessible from the conference network for the next 2 days as

`http://uqnet.cc.uq.edu.au`

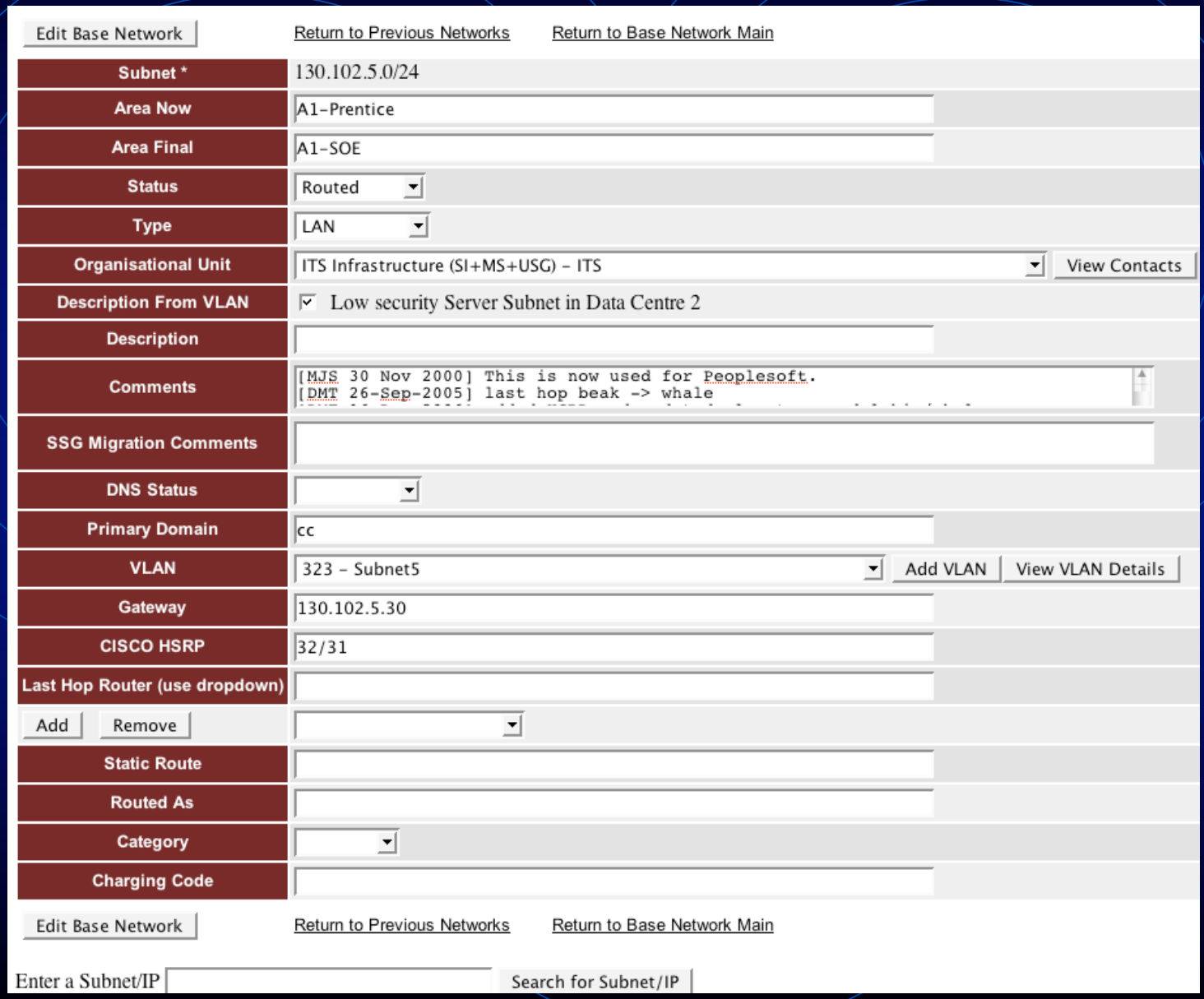
Some History about UQ Network Records

- UQ hostmaster responsible for maintaining subnet spreadsheet used for assigning bills to subnet owners
  (assumption: being informed of network changes)
- Many columns were added to spreadsheet to make it useful as a repository of network information: items like VLAN, router(s), HSRP, gateway, …
- Spreadsheet replaced by the locally developed "Pizza" database system in 2003. While the focus was on traffic billing, the BaseNetworks table shows how our address-space is broken up, with comprehensive network information for each subnet.

Pizza: Portion of BaseNetworks Display

Copy	Parent		Merge	130.102.1.200/30	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	--ENET-AMON-OSPREY	amon <-> osprey
Copy	Parent	Split	Merge	130.102.1.204/30	Spare					A4-Links	A4-Links			
Copy	Parent		Merge	130.102.1.208/29	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	--ENET-AMON-BACS	amon <-> bacs
Copy	Parent		Merge	130.102.1.216/30	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	--ENET-BACS-ZEUS	bacs <-> zeus
Copy	Parent	Split	Merge	130.102.1.220/30	Spare					A4-Links	A4-Links			
Copy	Parent		Merge	130.102.1.224/30	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	--ENET-KITE-ZEUS	kite <-> zeus
Copy	Parent	Split	Merge	130.102.1.228/30	Spare					A4-Links	A4-Links			
Copy	Parent		Merge	130.102.1.232/30	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	--ENET-OSPREY-ZEUS	osprey <-> zeus
Copy	Parent	Split	Merge	130.102.1.236/30	Spare					A4-Links	A4-Links			
Copy	Parent		Merge	130.102.1.240/29	Routed	Links	its-dn		router	A4-Links	A4-Links	Y	388	feather <-> psychology FW
Copy	Parent		Merge	130.102.1.248/29	Routed	Links	hs		router	A4-Links	A4-Links	Y	133	bacs/kite <-> earfw
Copy	Parent		Merge	130.102.2.0/24	Routed	LAN	its-infrastructure		cc	A1-SOE	A1-SOE	Y	271	St Lucia Net2
Copy	Parent		Merge	130.102.3.0/24	Routed	LAN	its-infrastructure		cc	A1-SOE	A1-SOE	Y	480	Server Farm DMZ 1 2
Copy	Parent		Merge	130.102.4.0/24	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	479	Server Farm DMZ 1 1
Copy	Parent		Merge	130.102.5.0/24	Routed	LAN	its-infrastructure		cc	A1-Prentice	A1-SOE	Y	323	Low security Server Subnet in Data Centre 2
Copy	Parent		Merge	130.102.6.0/27	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	289	Exchange server subnet: client side of SLB
Copy	Parent		Merge	130.102.6.32/27	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE		296	
Copy	Parent		Merge	130.102.6.64/27	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	294	SLB radius-client
Copy	Parent		Merge	130.102.6.96/27	Routed	LAN	its			A1-SOE	A1-SOE			suit SSGnew testing
Copy	Parent		Merge	130.102.6.128/25	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	49	Client network side of WSA
Copy	Parent		Merge	130.102.7.0/26	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	473	Load Balancing LAN
Copy	Parent		Merge	130.102.7.64/26	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	490	DMZ 2 2 - Servers
Copy	Parent		Merge	130.102.7.128/26	Routed	LAN	its-infrastructure		soe	A1-SOE	A1-SOE	Y	489	DMZ 2-1 Server Farm
Copy	Parent		Merge	130.102.7.192/27	Routed	LAN	its-irt		cc	A1-SOE	A1-SOE	Y	493	monitoring
Copy	Parent	Split	Merge	130.102.7.224/28	Spare					A1-SOE	A1-SOE			
Copy	Parent		Merge	130.102.7.240/28	Routed	LAN	its-infrastructure		router	A1-SOE	A1-SOE	Y	485	dolphin/whale FWSM/SSL admin

Pizza: Information for a Subnet



UQnet: Basic Functionality

- Initial impetus for UQnet portal was to provide more convenient grouping of information from Pizza
  NB Pizza currently has little in the way of data entry validation which reduces the quality of the information and causes problems with UQnet scripts
- Implemented with the perl-based mason templating system, using various previously written perl modules to parse `named.conf`, `dhcpd.conf`, etc
- An advantage over Pizza is user-friendly URLs
  - http://uqnet.cc.uq.edu.au/display/ip/130.102.152.7
  - http://uqnet.cc.uq.edu.au/display/vlan/270
  - http://uqnet.cc.uq.edu.au/display/org-units
  - http://uqnet.cc.uq.edu.au/reports/networks-by-subnets

UQnet: Pizza Information about an ip

130.102.152.7 has the reverse DNS entry 'im-ntp.its.uq.edu.au'

status: ROUTED

VLAN 270

VLAN: ITS desktop network
VLAN type: network
VLAN site: St Lucia

routed by claw

CIDR	gateway	Q	ou
130.102.152.0/23	130.102.152.30	Y	its
192.168.152.0/22	192.168.152.30	Y	its-uqg

the Q column represents whether the CIDR is handled by *the Quotient Traffic Charging system*

Enriching Network Records

- Basic network information from Pizza augmented from
  - Daily dump of all DNS records, e.g. to find all names resolving to an ip
  - DHCP configuration (but not yet lease activity)
  - Router netflows identifying active (source) ip-addresses
  - Quotient configuration

UQnet: Enriched with non-Pizza Info

130.102.152.7 has the reverse DNS entry 'im-ntp.its.uq.edu.au'

The following 5 DNS names resolve to 130.102.152.7 (CNAMEs in upper-case):
im-ntp.its.uq.edu.au, CUPS-1.ITS.UQ.EDU.AU, A.STRATUM1.NTP.UQ.EDU.AU, ntp-1a.uq.edu.au, NTP0.UQ.EDU.AU

status: ROUTED

Active on 01-Aug-2006 .. 03-Jul-2007 (334 days)
based on netflows during 01-Aug-2006 thru 03-Jul-2007 (336 days)

VLAN 270

VLAN: ITS desktop network
VLAN type: network
VLAN site: St Lucia

621 hosts (76 not registered in DNS), 40.6% of 1,530 usable-addresses
244 hosts, 47.9% of 509 usable-public-addresses; 377 hosts, 36.9% of 1021 usable-private-addresses

this VLAN is handled by the central DHCP server
with a dynamic pool of 61 addresses: 192.168.155.194-192.168.155.254
NB in practice, the pool is half this size

routed by claw

CIDR	gateway	#	?	x	Q	ou
130.102.152.0/23	130.102.152.30	244	33	51	Y	its
192.168.152.0/22	192.168.152.30	377	43	126	Y	its-uqg

the # column has the total number of hosts seen from flows during 01-Aug-2006 thru 03-Jul-2007 (336 days)
the ? column has the number of such hosts *not registered in the central DNS*
the x column has the number of hosts registered in the central DNS *not seen in flows*
the Q column represents whether the CIDR is handled by *the Quotient Traffic Charging system*

UQnet: Cross-checks between Configurations

- One of the most basic cross-checks is to ensure Pizza information is correct by comparing listed VLANs, subnets, gateways, HSRP, static-routes, routers, etc against router configurations
  - in general we don't have ready access to routing firewall configurations
  - In the past we could use the RIP routing table which would include entries published by some of the firewalls
  - some subnet attributes in Pizza don't relate to routers:
    VLAN description, domain-name, type of network (LINKS/NETMAN/LAN)

UQnet: Cross-check Pizza vs Routers

NB script not yet complete leading to some extraneous messages

- 130.102.11.64/28: Pizza has VLAN LIB-MAYNEVIEW, but is VLAN 1 in libwarehouse
- 130.102.16.0/26: Pizza has VLAN MBRS-WIRED, but is VLAN 1 in mbrs-adsl
- 130.102.17.192/27: Pizza has VLAN BLUECARE-TOOWONG, but is VLAN 1 in bluecare-adsl
- 130.102.18.0/26 not found in any router; Pizza router 'silver', vlan 'JKMRC', gway '130.102.18.30'
- 130.102.18.64/26 not found in any router; Pizza router 'silver', vlan 'JKMRC', gway '130.102.18.94'
- 130.102.18.128/25 not found in any router; Pizza router 'silver', vlan 'JKMRC', gway '130.102.18.158'
- 130.102.18.128/25 not found in any router; Pizza router 'silver', vlan 'JKMRC', gway '130.102.18.158'
- 130.102.19.140/30 not found in any router; Pizza router 'goondiwindi', vlan '666', gway '130.102.19.141'
- 130.102.19.160/28 not found in any router; Pizza router '', vlan '', gway '130.102.19.161'
- 130.102.19.192/26: Pizza has VLAN HYSHOT-PINJARRA.1, but is VLAN 1 in hyshot
- 130.102.20.0/24 not found in any router; Pizza router 'silver', vlan 'JKMRC', gway '130.102.20.30'
- 130.102.27.128/27: Pizza has VLAN 729, but is VLAN 675 in mater
- 130.102.64.0/22 not found in any router; Pizza router '', vlan '', gway ''
- 130.102.71.32/30 not found in any router; Pizza router '', vlan '', gway ''
- 130.102.71.48/28 not found in any router; Pizza router '', vlan '', gway ''
- 130.102.71.128/30 not found in any router; Pizza router '', vlan '', gway ''
- 130.102.71.152/29 not found in any router; Pizza router 'iteefw', vlan '380', gway ''
- 130.102.71.184/29 not found in any router; Pizza router 'iteefw', vlan '383', gway ''
- 130.102.71.192/27 not found in any router; Pizza router 'iteefw', vlan '386', gway ''
- 130.102.72.0/23 not found in any router; Pizza router 'iteefw', vlan '373', gway ''
- 130.102.74.0/23 not found in any router; Pizza router 'iteefw', vlan '373', gway '130.102.74.253'
- 130.102.78.128/25 not found in any router; Pizza router 'iteefw', vlan '382', gway ''
- 130.102.79.0/24 not found in any router; Pizza router 'iteefw', vlan '372', gway ''
- 130.102.95.0/24 not found in any router; Pizza router '', vlan '', gway ''
- 130.102.116.0/24 not found in any router; Pizza router 'qbp', vlan 'IMB2', gway '130.102.116.30'
- 130.102.117.0/24 not found in any router; Pizza router 'qbp', vlan 'IMB3', gway '130.102.117.30'
- 130.102.118.0/24 not found in any router; Pizza router 'qbp', vlan 'IMB4', gway '130.102.118.30'
- 130.102.119.0/24 not found in any router; Pizza router 'qbp', vlan 'IMB5', gway '130.102.119.30'
- 130.102.139.32/29 not found in any router; Pizza router '', vlan '', gway '130.102.139.33'
- 130.102.170.0/26 not found in any router; Pizza router 'hades', vlan '84', gway '130.102.170.1'
- 130.102.170.64/26 not found in any router; Pizza router 'hades', vlan '84', gway '130.102.170.65'
- 130.102.172.0/23: Pizza says static-routed to VLAN 431, but seen in hawk
- 130.102.192.64/26 not found in any router; Pizza router 'bacs/kite', vlan '151', gway '130.102.192.65'
- 130.102.195.0/24: Pizza says static-routed to VLAN 358, but seen in kite
- 130.102.197.0/24: Pizza says static-routed to VLAN 335, but seen in kite

UQnet: Cross-check Pizza vs Router HSRP

NB script not yet complete leading to some extraneous messages

Comparison of HSRP between Pizza and routers (66 messages)

- Pizza CIDR 130.102.1.160/28 (VLAN 363) has HSRP of '130.102.1.168/130.102.1.167', but not found in any router config
- Pizza CIDR 130.102.1.248/29 (VLAN 133) has HSRP of '130.102.1.250/130.102.1.251', but should be '130.102.1.251/130.102.1.250'
- Pizza CIDR 130.102.2.0/24 (VLAN 271) has blank HSRP, but should be '130.102.2.31/130.102.2.32'
- Pizza CIDR 130.102.5.0/24 (VLAN 323) has HSRP of '130.102.5.32/130.102.5.31', but not found in any router config
- Pizza CIDR 130.102.6.32/27 (VLAN 296) has HSRP of '130.102.6.35/130.102.6.34', but not found in any router config
- Pizza CIDR 130.102.6.64/27 (VLAN 294) has HSRP of '130.102.6.67/130.102.6.66', but not found in any router config
- Pizza CIDR 130.102.6.128/25 (VLAN 49) has HSRP of '130.102.6.130/130.102.6.131', but not found in any router config
- Pizza CIDR 130.102.11.80/28 (VLAN 99) has blank HSRP, but should be '130.102.11.82/130.102.11.83'
- Pizza CIDR 130.102.11.96/27 (VLAN 109) has HSRP of '130.102.11.124/130.102.11.125', but not found in any router config
- Pizza CIDR 130.102.28.128/25 (VLAN 278) has blank HSRP, but should be '130.102.28.159/130.102.28.160'
- Pizza CIDR 130.102.33.0/25 (VLAN 451) has blank HSRP, but should be '130.102.33.31/130.102.33.32'
- Pizza CIDR 130.102.39.64/27 (VLAN 147) has blank HSRP, but should be '130.102.39.66/130.102.39.67'
- Pizza CIDR 130.102.92.32/27 (VLAN 495) has HSRP of '130.102.92.35/130.102.92.34', but not found in any router config
- Pizza CIDR 130.102.102.72/29 (VLAN 21) has HSRP of '130.102.102.77/76,74,75', but should be '130.102.102.77/130.102.102.76'
- Pizza CIDR 130.102.111.0/27 (VLAN 77) has blank HSRP, but should be '130.102.111.3/130.102.111.2'
- Pizza CIDR 130.102.130.128/26 (VLAN 65) has blank HSRP, but should be '130.102.130.160/130.102.130.159'
- Pizza CIDR 130.102.137.0/26 (VLAN 302) has HSRP of '130.102.137.2/130.102.137.3', but not found in any router config
- Pizza CIDR 130.102.139.32/29 (VLAN) has HSRP of '130.102.139.34/130.102.139.35', but not found in any router config
- Pizza CIDR 130.102.147.0/24 (VLAN 322) has HSRP of '130.102.147.32/130.102.147.31', but not found in any router config
- Pizza CIDR 130.102.192.64/26 (VLAN 151) has HSRP of '130.102.192.66/130.102.192.67', but not found in any router config
- Pizza CIDR 130.102.215.128/27 (VLAN 78) has HSRP of '130.102.215.130,131', but not found in any router config
- Pizza CIDR 130.102.247.32/27 (VLAN 538) has HSRP of '130.102.247.34,35', but should be '130.102.247.35/130.102.247.34'
- Pizza CIDR 130.102.247.32/27 (VLAN 538) has Routers of 'letron,synot', but should be 'letron/synot'
- Pizza CIDR 152.98.220.0/24 (VLAN 15) has blank HSRP, but should be '152.98.220.2/152.98.220.3'
- Pizza CIDR 152.98.240.0/27 (VLAN 768) has blank HSRP, but should be '152.98.240.28/152.98.240.29'
- Pizza CIDR 152.98.240.104/29 (VLAN 786) has HSRP of '152.98.240.107/106,108', but should be '152.98.240.107/152.98.240.106'
- Pizza CIDR 172.19.248.0/22 (VLAN 26) has HSRP of '172.19.248.no', but not found in any router config
- Pizza CIDR 172.23.36.0/24 (VLAN 278) has blank HSRP, but should be '172.23.36.2/172.23.36.3'
- Pizza CIDR 172.23.37.0/26 (VLAN 275) has blank HSRP, but should be '172.23.37.31/172.23.37.32'
- Pizza CIDR 172.23.40.8/29 (VLAN 703) has blank HSRP, but should be '172.23.40.11/172.23.40.10'
- Pizza CIDR 172.23.79.0/27 (VLAN 122) has HSRP of '172.23.79.2 172.23.79.3', but not found in any router config
- Pizza CIDR 172.23.128.0/24 (VLAN 1) has Routers of 'shark', but should be 'claw/dolphin/falcon/hawk/kite/whale/wing'
- Pizza CIDR 172.23.132.0/22 (VLAN 1-feather) has HSRP of '172.23.132.31/172.23.132.32', but not found in any router config
- Pizza CIDR 172.23.154.0/24 (VLAN 256) has HSRP of '172.23.154.2, 172.23.154.3', but not found in any router config
- Pizza CIDR 172.23.155.0/25 (VLAN 318) has HSRP of '172.23.155.2/172.23.155.3', but should be '172.23.155.3/172.23.155.2'
- Pizza CIDR 172.23.211.0/24 (VLAN 451) has blank HSRP, but should be '172.23.211.30/172.23.211.32'
- Pizza CIDR 172.23.228.0/22 (VLAN 128) has HSRP of '172.23.228.2/3/4', but should be '172.23.228.2/172.23.228.3/172.23.228.4'

UQnet: Cross-checks other Configs vs Pizza

- Once there is reasonably confidence in the list of subnets in Pizza, we can check against other configs:
  - the list of subnets can be compared against those in the Pizza Network table which associates a subset of subnets against an OrgUnit to be billed
  - the list of subnets can be compared against the list of reverse-zones in `named.conf`, remembering that reverse zones correspond to /8, /16 & /24 blocks of address-space
    NB our policy is to have reverse DNS only for all routed address-space
  - the list of subnets can be compared against `webdns.conf` to identify any which are no longer routed or which have changed size
    NB WebDNS is our local delegated DNS admin tool
  - the VLAN structure can be compared against those configured in `dhcpd.conf`, either to identify VLANs no longer being used or situations when the list of subnets in a VLAN differs
    NB only a subset of VLANs is configured for DHCP, and these can be determined from whether the router VLAN config includes DHCP relaying

UQnet: Identifying Inactive Servers

The following server ip-addresses have been identified from netflow records as being inactive. I'm asking USG & MS groups to look at their entries and remove ones which have gone. USG might want to consult with SI about certain entries.

A separate page exists for inactive network devices

NB those marked with a '*' are dns entries not created through the WebDNS interface.

Produced in 2.0 secs at 13:06 PM on 05-Jul-2007 by make-inactive-ip-pages.pl (script)
The following domains were inspected:

- cc.uq.edu.au
- mgmt.cc.uq.edu.au
- soe.uq.edu.au
- sinet.uq.edu.au
- ldap.uq.edu.au

These 77 have been inactive for past 4 weeks:

IP	last-seen	hostname
10.0.0.10	2007-05-25	uqweb1-lb.soe.uq.edu.au (MS)
10.0.0.12	2007-04-13	uqwebdev-lb.soe.uq.edu.au (MS)
130.102.2.131	2007-02-09 *	ausc-netmon-db.cc.uq.edu.au
130.102.4.6	2007-03-15	uqapsc-test.soe.uq.edu.au (MS)
130.102.4.18	2007-04-16	ps02.soe.uq.edu.au (MS) + 1 other name
130.102.4.19	2007-03-27	uqapsph19.soe.uq.edu.au (MS)
130.102.4.20	2007-03-27	uqapsph20.soe.uq.edu.au (MS)
130.102.4.89	2007-05-05	legend.soe.uq.edu.au (USG)
130.102.4.90	2007-03-30	myth.soe.uq.edu.au (USG)
130.102.4.91	2007-05-18	x-testshamrock.soe.uq.edu.au (USG)
130.102.4.92	2007-05-18	x-testshamrockx.soe.uq.edu.au (USG)
130.102.4.97	2007-05-18	x-shamrock.soe.uq.edu.au (USG)
130.102.4.166	2006-09-01	limeb.soe.uq.edu.au (USG)
130.102.4.181	2007-05-22	uqbkcv4.soe.uq.edu.au (MS)
130.102.4.208	2006-11-18	uqnecsip.soe.uq.edu.au (MS)
130.102.4.239	2007-04-12	its-r2std-tmplt.soe.uq.edu.au (MS)

UQnet: Identifying Inactive Network Devices

The following router/netman ip-addresses have been identified from netflow records as being inactive.

A separate page exists for inactive server devices

NB those marked with a '*' are dns entries not created through the WebDNS interface.

Produced in 6.0 secs at 13:06 PM on 05-Jul-2007 by make-inactive-ip-pages.pl (script)
The following domains were inspected:

- router.uq.edu.au
- mcast.router.uq.edu.au
- router.uqi.uq.edu.au
- router.uq.net.au
- netman.uq.edu.au
- netman.uq.net.au
- netman.uqg.uq.edu.au
- netman.uqi.uq.edu.au
- wlan.netman.uq.edu.au

These 132 have been inactive for past 4 weeks:

IP	last-seen	hostname
10.0.1.128	2007-05-28 *	net-d0.1-128.router.uq.edu.au
130.102.0.48	2007-02-15	net-a0-48.router.uq.edu.au (uqacroom)
130.102.0.51	2007-02-15	broadcast-a0-48.router.uq.edu.au (uqacroom)
130.102.0.88	2007-02-15	net-a0-88.router.uq.edu.au (uqacroom)
130.102.0.91	2007-02-15	broadcast-a0-88.router.uq.edu.au (uqacroom)
130.102.0.92	2007-02-15	net-a0-92.router.uq.edu.au (uqacroom)
130.102.0.95	2007-02-15	broadcast-a0-92.router.uq.edu.au (uqacroom)
130.102.1.128	2007-01-23	net-a1-128.router.uq.edu.au (uqacroom)
130.102.1.129	2007-02-07	hawk-zeus.router.uq.edu.au (uqacroom)
130.102.1.130	2007-02-07	zeus-hawk.router.uq.edu.au (uqtodono)

UQnet: Checking all DNS records

Generated by dnswalk2. one of the DNS checking scripts, at Fri Jul 6 13:10:06 2007

Zone error messages (233 msgs in 57 zones)

zone '2.102.130.in-addr.arpa' (1 msgs; serial 2007062201 from ns1.uq.edu.au)

- WARNING xcheck_5 '51/PTR' missing fwd entry for 'something-for-rodney.test.uq.edu.au' (NXDOMAIN)

zone '19.102.130.in-addr.arpa' (3 msgs; serial 2007041802 from ns1.uq.edu.au)

- WARNING xcheck_5 '192/PTR' missing fwd entry for 'net-a19-192.hyshot.eng.uq.edu.au' (NXDOMAIN)
- WARNING xcheck_5 '193/PTR' missing fwd entry for 'hyshot-a19-192.hyshot.eng.uq.edu.au' (NXDOMAIN)
- WARNING xcheck_5 '255/PTR' missing fwd entry for 'broadcast-a19-192.hyshot.eng.uq.edu.au' (NXDOMAIN)

zone '97.102.130.in-addr.arpa' (2 msgs; serial 2007062801 from ns1.uq.edu.au)

- WARNING xcheck_8 '127/PTR' has fwd entry for 'net-a97-0.epsa.uq.edu.au', but 'A' points to '130.102.97.0'
- WARNING xcheck_5 '255/PTR' missing fwd entry for 'broadcast-a97.epsa.uq.edu.au' (NXDOMAIN)

zone '113.102.130.in-addr.arpa' (2 msgs; serial 2007070506 from ns1.uq.edu.au)

- WARNING rfc2317_5 '141/CNAME' has fwd entry for '141.128-191.113.102.130.in-addr.arpa/PTR', but 'www2.imb.uq.edu.au/A' points to '130.102.113.158'
- WARNING rfc2317_3 '169/CNAME' has resolves to '169.128-191.113.102.130.in-addr.arpa/PTR', but lookup of 'qbi.imb.uq.edu.au' failed (NXDOMAIN)

zone '128.102.130.in-addr.arpa' (1 msgs; serial 2007070403 from ns1.uq.edu.au)

- WARNING xcheck_8 '95/PTR' has fwd entry for 'uhs-server.uhs.hs.uq.edu.au', but 'A' points to '130.102.39.10'

zone '236.102.130.in-addr.arpa' (1 msgs; serial 2007062501 from ns1.uq.edu.au)

- WARNING xcheck_5 '235/PTR' missing fwd entry for 'ipswich2.uqwireless.uq.edu.au' (NXDOMAIN)

zone '0.19.172.in-addr.arpa' (2 msgs; serial 2007070203 from ns1.uq.edu.au)

- WARNING xcheck_5 '0/PTR' missing fwd entry for 'net-u19.wlan.netman.uq.edu.au' (NXDOMAIN)
- WARNING xcheck_5 '1/PTR' missing fwd entry for 'gateway-u19.wlan.netman.uq.edu.au' (NXDOMAIN)

zone '1.19.172.in-addr.arpa' (1 msgs; serial 2007070203 from ns1.uq.edu.au)

- WARNING xcheck_5 '255/PTR' missing fwd entry for 'broadcast-u19.wlan.netman.uq.edu.au' (NXDOMAIN)

UQnet: Checking DNS Delegations

- One cross-check not currently in UQnet is done between zones that should be delegated to us and their parent name-servers

```
# ./check-delegations.pl -q > /dev/null
found 1,466 zones in named.conf (includes not inspected)
found 1,224 commented-out zones in named.conf & named.conf.oldzones

total of 62 parents to DELEGATED/NOT_DELEGATED apical zones

not testing 3 LOCALCOPY zones
    .
    arpa
    in-addr.arpa

ignoring the following 1 zones:
    bpe.ipv1.info

testing 538 DELEGATED apical zones (882 non-apical)
  banjomad.com.au: is ours; no UQ ns in parent
  dirtcomp.com.au: is ours; no UQ ns in parent
  fingerstyle.com.au: is ours; no UQ ns in parent
  trinitycollege.qld.edu.au: is ours; no UQ ns in parent
total of 538 zones tested (4 problems)

testing 999 NOT_DELEGATED apical zones (268 non-apical)
  71.155.in-addr.arpa: not ours; has UQ ns in parent
  bjaonline.com: not ours; has UQ ns in parent
total of 999 zones tested (2 problems)
```

UQnet: Identifying Inactive Websites

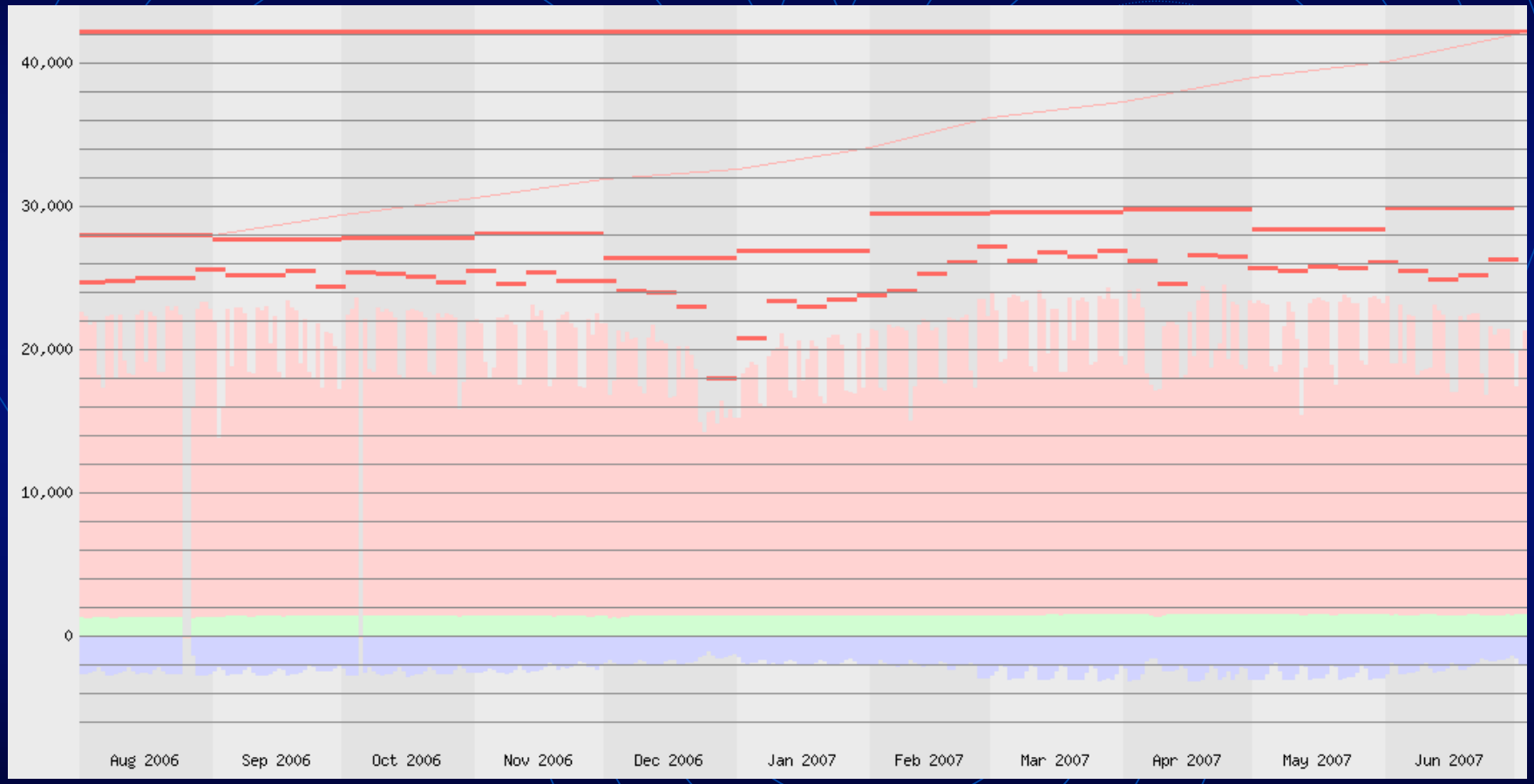
- Another cross-check not currently in UQnet regards UQ's commercial web-hosting.
  The cross-check is between 3 information silos
  - the list of sites from the commercial web-server is gathered, particularly the domain-name & username for each
  - the domain-name is checked against `named.conf`
  - the username is checked against those active in the billing system
    complicated because billing system does not record each user's domains
- The first cross-check revealed nearly 200 sites that should be removed from the web-server
  - Either because the domain had expired from the DNS (NXDOMAIN)
  - or because the domain was now delegated elsewhere
  - or because the client was no longer active
    in some cases the domain was still delegated to the UQ name-servers and the zone was replaced by an empty one if the client could not get the delegation removed/changed

UQnet: Other Reports

- Several other reports are generated providing statistical breakdowns. It was convenient to publish these through the UQnet portal

UQnet: Other Reports

- Active ip-addresses seen on UQ network



UQnet: Other Reports

- Analysis of DNS queries

26,123,948 queries analysed from 3 log-files in 681.9 secs
19,151,837 internal (UQ), 6,972,111 external
covering 04-Jul-2007 00:00:00.001 .. 04-Jul-2007 23:59:59.992

Breadown of QTYPE from all queries, UQ and external

17,605,051	A
4,894,158	PTR
1,548,897	MX
661,282	TXT
449,867	AAAA
362,446	SOA
214,371	ANY
206,439	NS
109,442	SRV
62,579	A6
6,033	AXFR
1,327	CNAME
1,275	NAPTR
753	SPF
17	RESERVED0
8	HINFO
3	TYPExx

UQ addresses making most queries (top 50 or so)

4,539,490	130.102.148.150 (air.soe.uq.edu.au)
4,219,528	130.102.149.128 (mailhub2.uq.edu.au)
3,031,067	130.102.149.150 (sea.soe.uq.edu.au)
1,331,797	130.102.152.39 (mollari.its.uq.edu.au)
417,516	130.102.7.209 (maya.cc.uq.edu.au)
376,341	130.102.7.208 (inca.cc.uq.edu.au)
260,694	130.102.7.27 (gold.soe.uq.edu.au)
255,434	130.102.7.36 (tin.soe.uq.edu.au)

UQnet: Other Reports

- Breakdown of DNS zones

Breakdown of all zones into classes and types:

class	total	master	slave	forward	hint
.	1	1	-	-	-
wpad	1	1	-	-	-
test	2	2	-	-	-
dummy	0	-	-	-	-
rbl/sorbs	0	-	-	-	-
UQ-oz	4	1	3	-	-
UQ-fwd	274	228	46	-	-
UQ-AD	176	176	-	-	-
UQ-rev	205	165	40	-	-
UQ-priv	390	379	11	-	-
UQ-ipv6	1	1	-	-	-
for-UQ-units	165	126	39	-	-
AARNet	1	-	1	-	-
QRNO	26	3	23	-	-
QTAC	22	22	-	-	-
ISP-fwd	7	7	-	-	-
ISP-rev	98	94	4	-	-
ISP-clients	232	177	55	-	-
ISP-ex-clients	0	-	-	-	-
total	1605	1383	222	0	0

Source for zones of type master (excluding UQ-AD):

source	zones
AD	176

Some UQ units are running their own name-server:

unit	zones
business	10
cmr	8
imb	7
itee	29
jkmrc	13
maths	14
minmet	9
physics	4
psychology	4
total	98

UQnet: Other Reports

- DNS delegation glue for AARNet members

In the following table, the first domain listed for an organization is that used for the link on the AARNet member page. I've added a second domain when I happen to be aware of it.

script took 1.7 secs at 13:50 PM on 06-Jul-2007

23 out of 41 domains for 38 AARNet members had at least one delegation NS not requiring edu.au glue
NS records not needing glue are listed in **bold**
so vulnerable domains are those without any bold name-server entries

AARNet	aarnet.edu.au	tiny-teddy.aarnet.edu.au **ns1.aarnet.net.au** **ns2.aarnet.net.au** **ns3.aarnet.net.au**
Bond University	bond.edu.au	kirk.bond.edu.au spock.bond.edu.au
Central Queensland University	cqu.edu.au	ns1.cqu.edu.au ns2.cqu.edu.au **ns1.uq.edu.au** **ns2.uq.edu.au**
Charles Darwin University	cdu.edu.au	ns1.cdu.edu.au ns2.cdu.edu.au **ns2.aarnet.net.au** **ns3.aarnet.net.au**
	ntu.edu.au	**ns1.cdu.edu.au** **ns2.cdu.edu.au** **ns2.aarnet.net.au** **ns3.aarnet.net.au**
Charles Sturt University	csu.edu.au	csuna.csu.edu.au csunb.csu.edu.au csunw.csu.edu.au
Curtin University of Technology	curtin.edu.au	dns.curtin.edu.au dns2.curtin.edu.au dnsp1.curtin.edu.au networks.curtin.edu.au
Deakin University	deakin.edu.au	midas.its.deakin.edu.au rana.its.deakin.edu.au sol.its.deakin.edu.au wasat.its.deakin.edu.au