THE AUSTRALIAN NATIONAL UNIVERSITY

Network Monitoring Workshop

Ben Carbery
Networks & Communications
September 2009

Network Overview

Snapshot

- Typical campus network
- Few routers, many switches
- 200+ buildings

- Remote campuses connected usually connected at L2 via ethernet or microwave
  (Siding Springs, Mount Stromlo..)

Network Overview

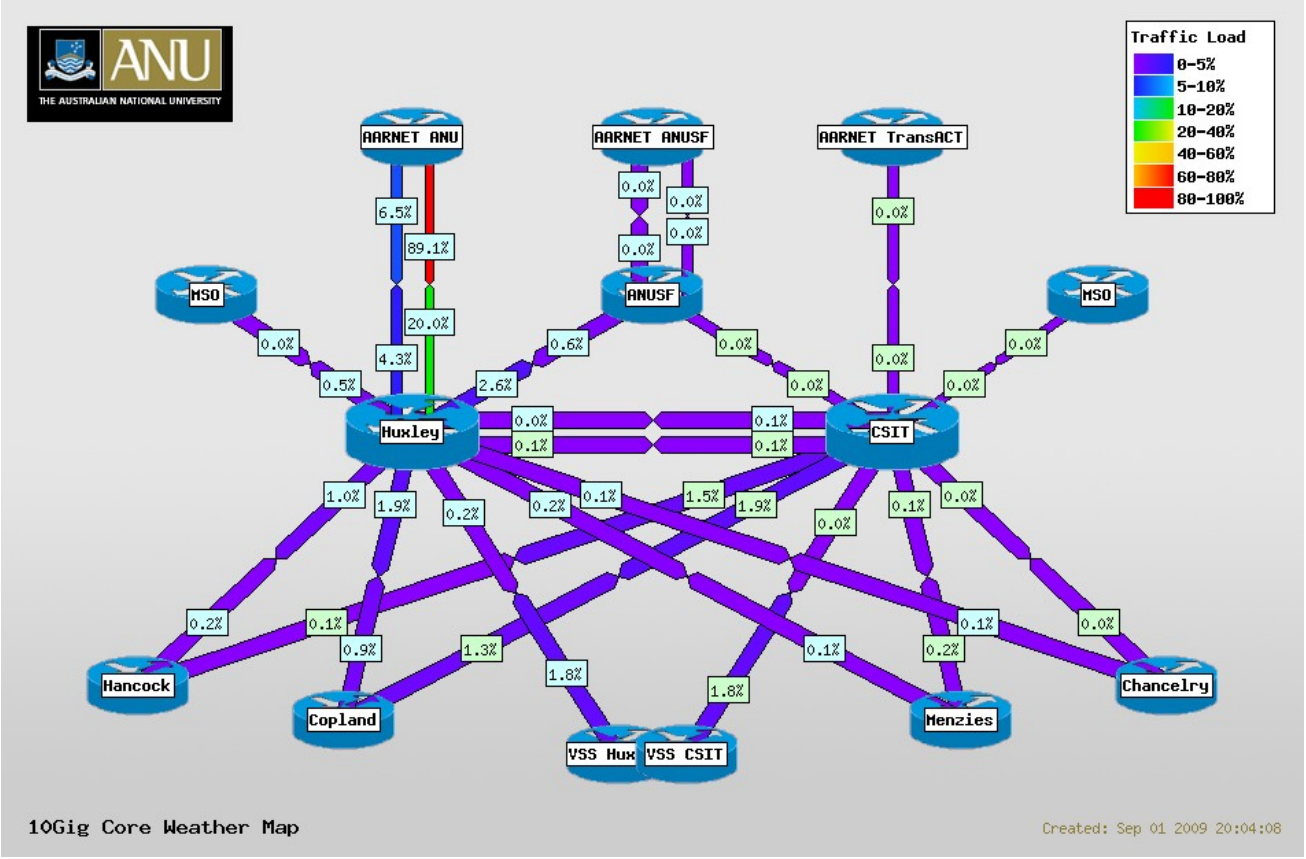
Core Network

- 10 x Cisco 6500 Switches (Sup 720)
- Dual-star routed core (OSPF)
- 10 Gig backbone

- Technically 'collapsed core' - all routers host user networks

THE AUSTRALIAN NATIONAL UNIVERSITY

Network Overview



Network Overview

Internet

- Dual-homed to AARNET at 1Gbps
- Dedicated 10Gbps to ANUSF
- Port-based Service for Wireless and InfoCommons (60 Mbps)

Network Overview

Distribution + Edge

- 1000+ Enterasys Switches (replacing HP4000)
- 600 'stacks'
- 30,000 ports
- N-Series selectively used for distribution layer
- C-Series stackable switches
- POE
- L2-L4 policy per-port

Network Overview

Server Farm Environment

- Cisco Virtual Switching System (VSS)
  (pair of 6500s acting as a virtual router)
- Provides geographical deversity for a single L3 network
  (irrelevant for switched core)
- Servers connect via Enterasys N7 / Cisco 4510
  (10Gig connectivity available)
- Legacy Cisco Content Switches

Network Services

Data

- Virtual Firewalling via Cisco FWSM
- 8 modules, 70+ virtual firewalls
- Still many unfirewalled subnets

- Satellite TV Reticulation + Mbone
- Various video conferencing

Network Services

VPN

- Cisco VPN 3000s (ASA on order)

Voice

- VOIP since 2002
- Avaya-based solution
- 6000 IP phones
- 2000 analogue phones
- SIP trials

Network Services

Wireless

- Aruba solution since Jan 09 (500 APs)
- 802.11abgn
- Cisco wireless maintained for residences / bridging

- Legacy captive-portal service (ANU-Access)
- WPA2 802.1x service (ANU-Secure)

- Eduroam (unresolved issues with outbound auth)

Network Monitoring & Mgmt

3 years ago flashback..

- Many disparate disconnected systems
- All out of date to some degree

NetDisco

Statseeker 2.x

SNIPS (ICMP)

MRTG

Flow-tools

Network Monitoring & Mgmt

NMS Issues

- No systematic logging / config mgmt
- Network changes not propogated to NMS
- Multiple systems maintained manually
- No 'definitive' view of network 'assets'
- NMS not accessible / used by support staff
- Patching not performed
- Some 'essential' needs not met (config backups)

Network Monitoring & Mgmt

Today

Many problems solved or WIP..

- Standard hardware and software platform (HP + RHEL5)
- Repeatable kickstart build process + documented
- Comprehensive logging (syslog-ng <10GB per day)
- Network devices are audited for correct snmp/syslog config
- TACACS administration + command logging
- csv + expect inventory system
- Cacti replaced MRTG / offered a 'portal' view of all web-based NMS

Network Monitoring & Mgmt

Today – Systems

Web-based NMS..

- Airwave - multi-vendor wireless mgmt (+WLSE)
- Logging servers
- Netflow servers
- Statseeker 3.x
- Cacti - RRDtool front-end
  - discovery
  - weathermap

Network Monitoring & Mgmt

Today - Systems

Application-based NMS..

- NetSite - Enterasys suite
- Prognosis - Voice services
- Packetlogic - Shaper and Stats server
- SiteProtector - ISS IPS

Network Monitoring & Mgmt

NMS Issues

The usual suspects..

- ~~No systematic logging / config mgmt~~
- Network changes not propogated to NMS
- Multiple systems maintained manually
- No 'definitive' view of network 'assets'
- ~~NMS not accessible / used by support staff~~
- ~~Patching not performed~~
- ~~Some 'essential' needs not met (config backups)~~

Network Monitoring & Mgmt

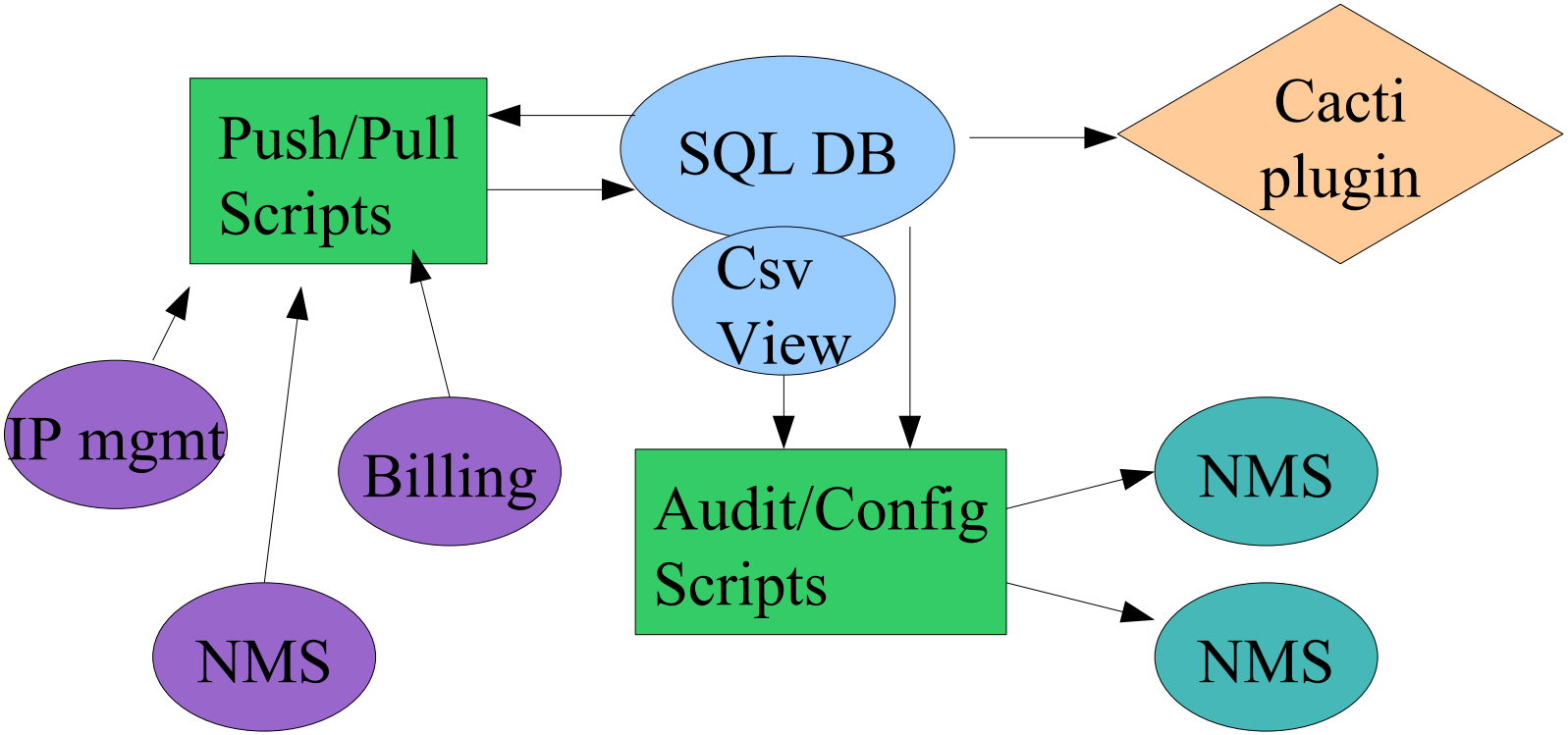
Our Approach

- NIMS – network inventory management system
- Solves need for an authoritative source of information about the network
- Central definitive view of network assets
- Audits NMS against the definitive view (or what is in other NMS)
- Provide graphical (user) & command-line (machine) interface

- Essentially a bunch of scripts, a DB, and a cacti plugin

Network Monitoring & Mgmt

NIMS Components



Network Monitoring & Mgmt

NIMS Components

- Essentially a DB, a BOS (bunch of scripts) & a cacti plugin
- Scripts push/pull data from the 'authority' for each asset
- Relational DB obvious choice to link asset data:

VLAN->Subnet->Billing Code->College

Room->Switch->Set of VLANs->Set of Depts

- Front-end utilises Cacti plugin architecture for displaying & manipulating SQL tables