NOC Tools and Techniques

Joel Jaeggli

The problem...

- Customers place demands on the resources you provide.
- Management and financial considerations place limits on the resources you provide.
- Hardware and software fail.
- The human capital you have available to you is finite.

The solution...

- We're technocrats here, so obviously we're inclined towards a technical solution.
- Deploy instrumentation, management, and collaboration tools to:
  - Measure, and respond to resource demands.
  - Identify failures before they affect the users.
  - Increase the productivity of your workforce.
  - Help provide guidance to management on demand and costs.

Instrumentation

- Nagios, Big Brother, Big Sister.
  - Monitor hosts for outages.
  - Monitor network or hosts resource utilization, do historical trending, monitor service performance, collect and report on snmp traps.
- Smokeping
  - Perform latency monitoring on network links and services
- Flow export and processing tools.
  - ip accounting, understanding what traffic is actually on your network.

Instrumentation – Part 2

- IP inspection tools – Snort, Bro
  - intrustion detection tools can take a deper look at traffic on your network.
- Accounting tools, the third A in AAA (free radius, open ldap)

Management Tools

- Track changes in router configuration (rancid)
- Do revision control on configuration files for routers and host services (subversion, cvs)

Collaboration

- Maintain your documentation, public web presence, in wikis and content management systems. (plone)
- Support systems, ticket tracking. (RT, Trac, Buzilla).
- Calendering and project management.