

Network Operations and Network Management

APRICOT 2008
Network Management
Taipei, Taiwan
February 20-24, 2008



Overview

- What is network operations and management ?
- Why network management ?
- The Network Operation Center
- Network monitoring systems and tools
- Statistics and accounting tools
- Fault/problem management
- Ticket systems
- Configuration management & monitoring
- The big picture...

What is network management ?

- System & Service monitoring
 - Reachability, availability
- Resource measurement/monitoring
 - Capacity planning, availability
- Perf. monitoring (RTT, throughput)
- Statistics & Accounting/Metering
- Fault Management
 - Fault detection, troubleshooting, and tracking
 - Ticketing systems, helpdesk
- Change management & configuration monitoring

What we don't cover...

- Provisioning
 - (processes associated with allocation and configuration of resources)
- Security aspects
 - Basic security is proper administration and management!

Why network management ?

- Make sure the network is up and running. Need to monitor it.
 - Deliver projected SLAs (Service Level Agreements)
 - Depends on policy
 - What does your management expect ?
 - What do your users expect ?
 - What do your customers expect ?
 - What does the rest of the Internet expect ?
 - Is 24x7 good enough ?
 - There's no such thing as 100% uptime

Why network management ? - 2

- What does it take to deliver 99.9 % ?
 - $30,5 \times 24 = 762$ hours a month
 - $(762 - (762 \times .999)) \times 60 = 45$ minutes max of downtime a month!
- Need to shutdown 1 hour / week ?
 - $(762 - 4) / 762 \times 100 = 99.4$ %
 - Remember to take planned maintenance into account in your calculations, and inform your users/customers if they are included/excluded in the SLA
- How is availability measured ?
 - In the core ? End-to-end ? From the Internet ?)

Why network management ? - 3

- Know when to upgrade
 - Is your bandwidth usage too high ?
 - Where is your traffic going ?
 - Do you need to get a faster line, or more providers ?
 - Is the equipment too old ?
- Keep an audit trace of changes
 - Record all changes
 - Makes it easier to find cause of problems due to upgrades and configuration changes
- Where to consolidate all these functions ?
 - In the Network Operation Center (NOC)

The Network Operations Center (NOC)

- Where it all happens
 - Coordination of tasks
 - Status on network and services
 - Fielding of network-related incidents and complaints
 - Where the tools reside ("NOC server")
- One of the goals of this workshop...
 - Build a NOC box
 - It will be the most important machine on your network
 - We will do this during the week, by installing, and configuring, various tools to help in network monitoring and management.

Network monitoring systems and tools

- Two kinds of tools
 - Diagnostic tools - used to test connectivity, ascertain that a location is reachable, or a device is up - usually active tools
 - Monitoring tools - tools running in the background ("daemons" or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.

Network monitoring systems and tools - 2

- Active tools
 - Ping – test connectivity to a host
 - Traceroute – show path to a host
 - MTR – combination of ping + traceroute
 - SNMP collectors (polling)
- Passive tools
 - log monitoring, SNMP trap receivers
- Automated tools
 - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
 - MRTG – record and graph bandwidth usage on a switch port or network link, at regular intervals

Network monitoring systems and tools - 3

- Network & Service Monitoring tools
 - Nagios – server and service monitor
 - Can monitor pretty much anything
 - HTTP, SMTP, DNS, Disk space, CPU usage, ...
 - Easy to write new plugins (extensions)
 - Basic scripting skills are required to develop simple monitoring jobs – Perl, Shellscript...
 - Many good Open Source tools
 - Zabbix, ZenOSS, Hyperic, ...
- Use them to monitor reachability and latency in your network
 - Parent-child dependency mechanisms are very useful!

Network monitoring systems and tools - 4

- Monitor your critical Network Services
 - DNS
 - Radius/LDAP/SQL
 - SSH to routers
- How will you be notified ?
- Don't forget log collection!
 - Every network device (and UNIX and Windows servers as well) can report system events using syslog
 - You **MUST** collect and monitor your logs!
 - Not doing so is one of the most common mistakes when doing network monitoring

Network Management Protocols

- SNMP – Simple Network Management Protocol
 - Industry standard, hundreds of tools exist to exploit it
 - Present on any decent network equipment
 - Network throughput, errors, CPU load, temperature, ...
 - UNIX and Windows implement this as well
 - Disk space, running processes, ...
- SSH and telnet
 - It's also possible to use scripting to automate monitoring of hosts and services

Statistics & accounting tools

- Traffic accounting
 - what is your network used for, and how much
 - Useful for Quality of Service, detecting abuses, and billing (metering)
 - Dedicated protocol: NetFlow
 - Identify traffic "flows": protocol, source, destination, bytes
 - Different tools exist to process the information
 - Flowtools, flowc
 - NFSen
 - ...

Fault & problem management

- Is the problem transient ?
 - Overload, temporary resource shortage
- Is the problem permanent ?
 - Equipment failure, link down
- How do you detect an error ?
 - Monitoring!
 - Customer complaints
- A ticket system is essential
 - Open ticket to track an event (planned or failure)
 - Define dispatch/escalation rules
 - Who handles the problem ?
 - Who gets it next if no one is available ?

Ticketing systems

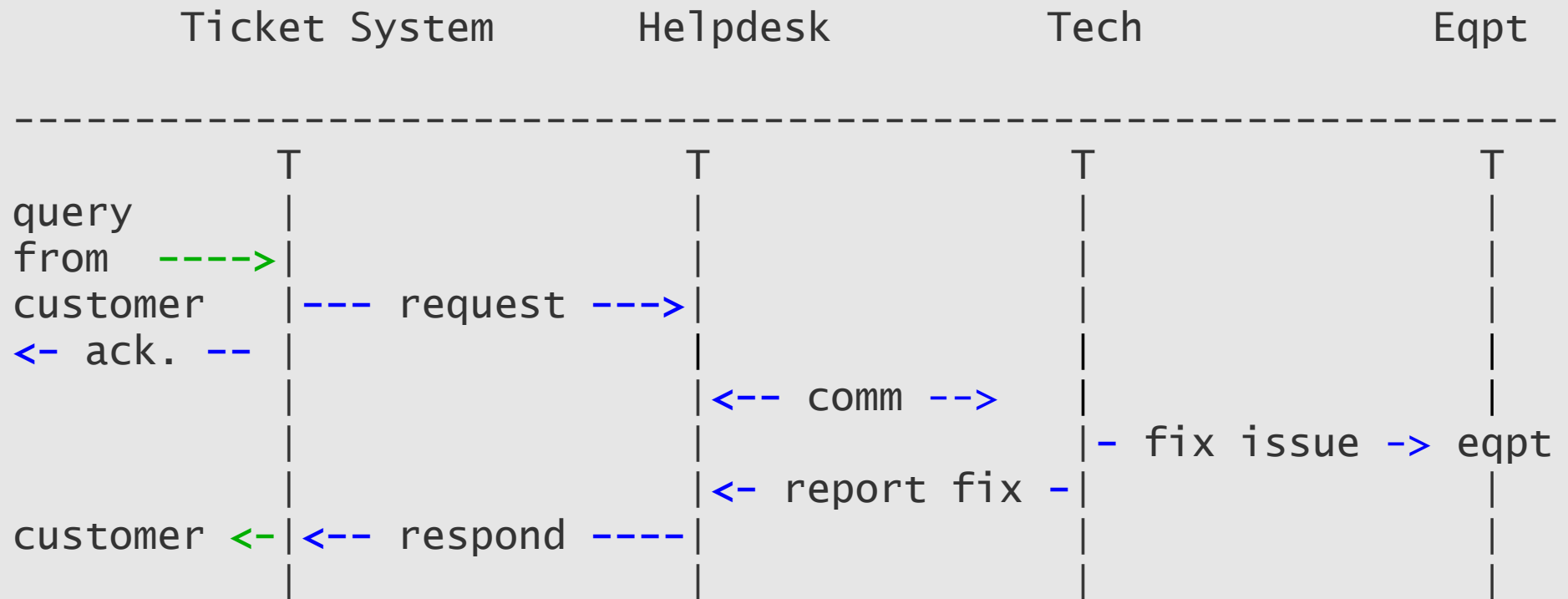
- Why are they important ?
 - Track all events, failures and issues
- Focal point for helpdesk communication
- Use it to track all communications
 - Both internal and external
- Events originating from the outside:
 - customer complaints
- Events originating from the inside:
 - System outages (direct or indirect)
 - Planned maintenance / upgrade – Remember to notify your customers!

Ticketing systems - 2

- Use ticket system to follow each case, including internal communication between technicians
- Each case is assigned a case number
- Each case goes through a similar life cycle:
 - New
 - Open
 - ...
 - Resolved
 - Closed

Ticketing systems - 3

- Workflow:



Ticketing systems - 4

- Some ticketing software systems:
 - Trac
 - RT
- We'll be looking at using Trac later in the workshop

Configuration management & monitoring

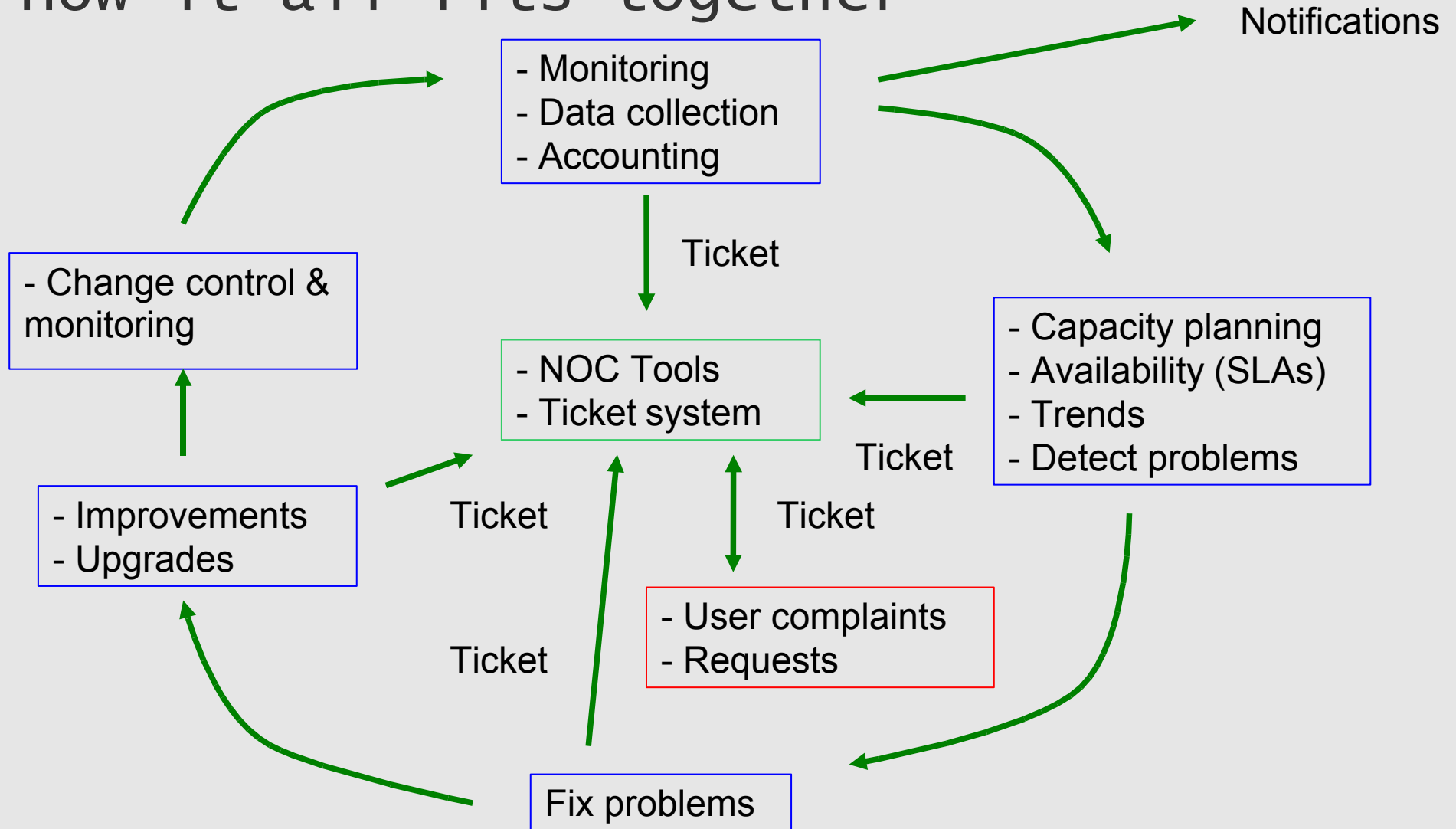
- Record changes to equipment configuration, using *revision control* (also for configuration files)
- Inventory management (equipment, IPs, interfaces, ...)
- Use version control!
 - As simple as:
"cp named.conf named.conf.20070827-01"
- For plain configuration files:
 - CVS, Subversion
 - Mercurial

Configuration management & monitoring - 2

- Traditionnally, used for source code (programs)
- Works well for any text-based configuration files
 - Also for binary files, but less easy to see differences
- For network equipment:
 - RANCID (Automatic Cisco configuration retrieval and archiving, also for other equipment types)

Big picture

- How it all fits together



Questions ?

