Network monitoring systems & tools

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, Shell scripts, php, etc...
- Many good Open Source tools
  - Zabbix, ZenOSS, Hyperic, OpenNMS ...

Use them to monitor reachability and latency in your network

- Parent-child dependency mechanisms are very useful!

Network monitoring systems & tools

Monitor your critical Network Services

- DNS/Web/Email
- 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 is also possible to use scripting to automate monitoring of hosts and services

SNMP tools

Net SNMP tool set

- http://net-snmp.sourceforge.net/

Very simple to build simple tools

- One that builds snapshots of which IP is used by which Ethernet address
- Another that builds shapshots of which Ethernet addresses exist on which port on which switch.
- Query remote RAID array for state.
- Query server, switches and routers for temperatures.
- Etc…

Statistics and accounting tools

Traffic accounting and analysis

- 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
  - Many more: http://www.networkuptime.com/tools/netflow/

Fault and 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:

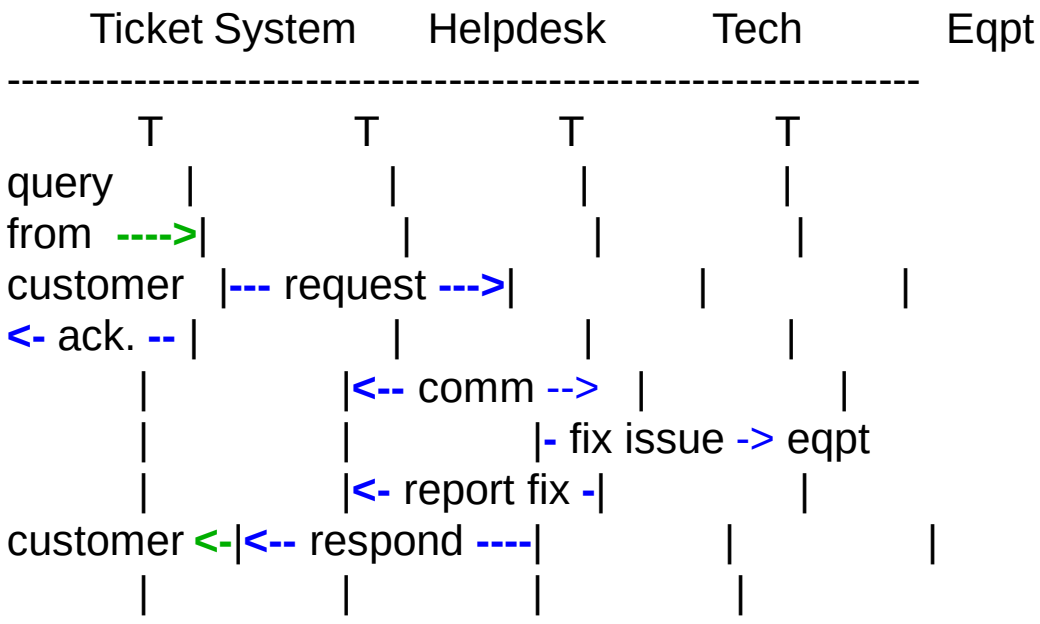
- System outages (direct or indirect)
- Planned maintenances or upgrades – Remember to notify your customers!

Ticketing systems

- 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

Workflow:



Ticketing systems: examples

rt (request tracker)

- Heavily used worldwide.
- A classic ticketing system that can be customized to your location.
- Somewhat difficult to install and configure.
- Handles large-scale operations.

trac

- A hybrid system that includes a wiki and project management features.
- Ticketing system is not as robust as rt, but works well.
- Often used for ”trac”king group projects.

redmine

- Like trac, but more robust. Harder to install

Network Intrusion Detection Systems (NIDS)

These are systems that observe all of your network traffic and report when it sees specific kinds of problems, such as:

- hosts that are infected or are acting as spamming sources.

A few tools:

- **SNORT** - a commonly used open source tool: http://www.snort.org/
- **Prelude –** Security Information Management System https://dev.prelude-technologies.com/
- **Samhain –** Centralized HIDS http://la-samhna.de/samhain/
- **Nessus** - scan for vulnerabilities: http://www.nessus.org/download/

Configuration mgmt & monitoring

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

Configuration mgmt & monitoring

- Traditionally, 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)
- Built-in to Project Management Software like:
  - **Trac**
  - **Redmine**
  - And, many other wiki products. Excellent for documenting your network.

The big picture revisited