Network Management & Monitoring Overview

Advanced ccTLD Workshop

September, 2008
Amsterdam, Holland
What is network management?

- System & Service monitoring
  - Reachability, availability
- Resource measurement/monitoring
  - Capacity planning, availability
- Performance monitoring (RTT, throughput)
- Statistics & Accounting/Metering
- Fault Management (Intrusion Detection)
  - Fault detection, troubleshooting, and tracking
  - Ticketing systems, help desk
- Change management & configuration monitoring
Big picture – First View

• How it all fits together

- Monitoring
- Data collection
- Accounting

- NOC Tools
- Ticket system

- Capacity planning
- Availability (SLAs)
- Trends
- Detect problems

- Change control & monitoring

- Improvements
- Upgrades

- User complaints
- Requests

Fix problems

Notifications
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 administration/government 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 for a server
    - Can we get 100% uptime for DNS? What are people's experience?
Why network management?

- What does it take to deliver 99.9% uptime?
  - 30.5 x 24 = 762 hours a month
  - (762 - (762 x .999)) x 60 = 45 minutes maximum of downtime a month!

- Need to shutdown 1 hour / week?
  - (762 - 4) / 762 x 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?
Documentation: Diagramming Software

Windows Diagramming Software

• Visio:

• Ezdraw:
  http://www.edrawsoft.com/

Open Source Diagramming Software

• Dia:
  http://live.gnome.org/Dia

• Cisco reference icons
  http://www.cisco.com/web/about/ac50/ac47/2.html

• Nagios Exchange:
  http://www.nagiosexchange.org/
Network monitoring systems and tools

• Three kinds of tools (imho)

  - **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.

  - **Performance tools** – tell us how our network is handling traffic flow and how much flow (traffic) there is.
Performance Tools

- Key is to look at each router interface (probably don’t need to look at switch ports).
- Some common tools:
  - http://cricket.sourceforge.net/
  - http://www.mrtg.com/
  - http://nfsen.sourceforge.net/
Network monitoring systems and tools - 3

• 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, NetFlow

• Automated tools
  - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
  - MRTG/RRD – record and graph bandwidth usage on a switch port or network link, at regular intervals
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 - 5

- 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
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:

<table>
<thead>
<tr>
<th>Ticket System</th>
<th>Helpdesk</th>
<th>Tech</th>
<th>Eqpt</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>query from</td>
<td>request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>comm</td>
<td></td>
<td></td>
<td>eqpt</td>
</tr>
<tr>
<td>report fix</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>respond</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

nsrc@ccTLD-advanced
Amsterdam
Some ticketing software systems:

rt
- 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.
Configuration management & monitoring

- Record changes to equipment configuration, using *revision control* (also for configuration files)
- Inventory management (equipment, IPs, interfaces, etc.)
- Use versioning control
  - As simple as:
    "cp named.conf named.conf.20070827-01"
- For plain configuration files:
  - CVS, Subversion
  - Mercurial
Configuration management & monitoring - 2

- 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)
Big picture – Again

- How it all fits together

- Monitoring
  - Data collection
  - Accounting

- Change control & monitoring

- NOC Tools
  - Ticket system

- Improvements
  - Upgrades

- Capacity planning
  - Availability (SLAs)
  - Trends
  - Detect problems

- User complaints
  - Requests

- Fix problems

- Ticket

Notifications
# Summary of Some Open Source Solutions

## Performance
- Cricket
- IFPFM
- flowc
- mrtg
- dsc
- dnsmon
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

## SNMP/Perl/ping Net Management
- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios
- Netdisco
- OpenNMS
- Sysmon
- Zabbix
- ZenOSS

## Change Mgmt
- Mercurial
- Rancid (routers)
- RCS
- Subversion

## Security/NIDS
- Nessus
- SNORT
- ACID (base/lab)

## Ticketing
- rt
- trac
Questions ?