INTRODUCTION TO NETWORK MANAGEMENT AND MONITORING

HEZRON MWANGI
Systems Administrator
hmwangi@kenet.or.ke

14th August 2013

kenet
Kenya Education Network

INTRODUCTION TO NETWORK MANAGEMENT

HEZRON MWANGI
Systems Administrator
hmwangi@kenet.or.ke

14th August 2013

kenet
Kenya Education Network

Introduction To Network Management

- Network management refers to the activities, methods, procedures and tools of networked systems that pertain to the:
  - Operation - keeping the network up and running smoothly.
  - Administration - keeping track of resources in the network and how they are assigned.
  - Maintenance - performing repairs and upgrades .
  - Provisioning - configuring resources in the network to support services.

Introduction To Network Management Cont'd

- Network management is generally carried out in a network operations center (NOC).
- A common way of characterizing network management functions is FCAPS:
  - Fault.
  - Configuration.
  - Accounting.
  - Performance.
  - Security.

Network Management Functions

- controlling, planning, allocating, deploying, coordinating, and monitoring network resources.
- network planning.
- predetermined traffic routing to support load balancing.
- configuration management.
- fault management.
- security management.
- performance management.
- bandwidth management.
- Route analytics.
- accounting management.

Why Manage your Network

- 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.
- Keep a history of your network operations..
  - Using a ticket system lets you keep a history of events.
  - Allows you to defend yourself and verify what happened.

Why Manage your Network Cont'd

- Accounting
  - Track usage of resources
  - Bill customers according to usage
- Know when you have problems
  - Stay ahead of your users! Makes you look good.
  - Monitoring software can generate tickets and automatically notify staff of issues.
- Trends
  - All of this information can be used to view trends across your network.
  - This is part of baselining, capacity planning and attack detection.

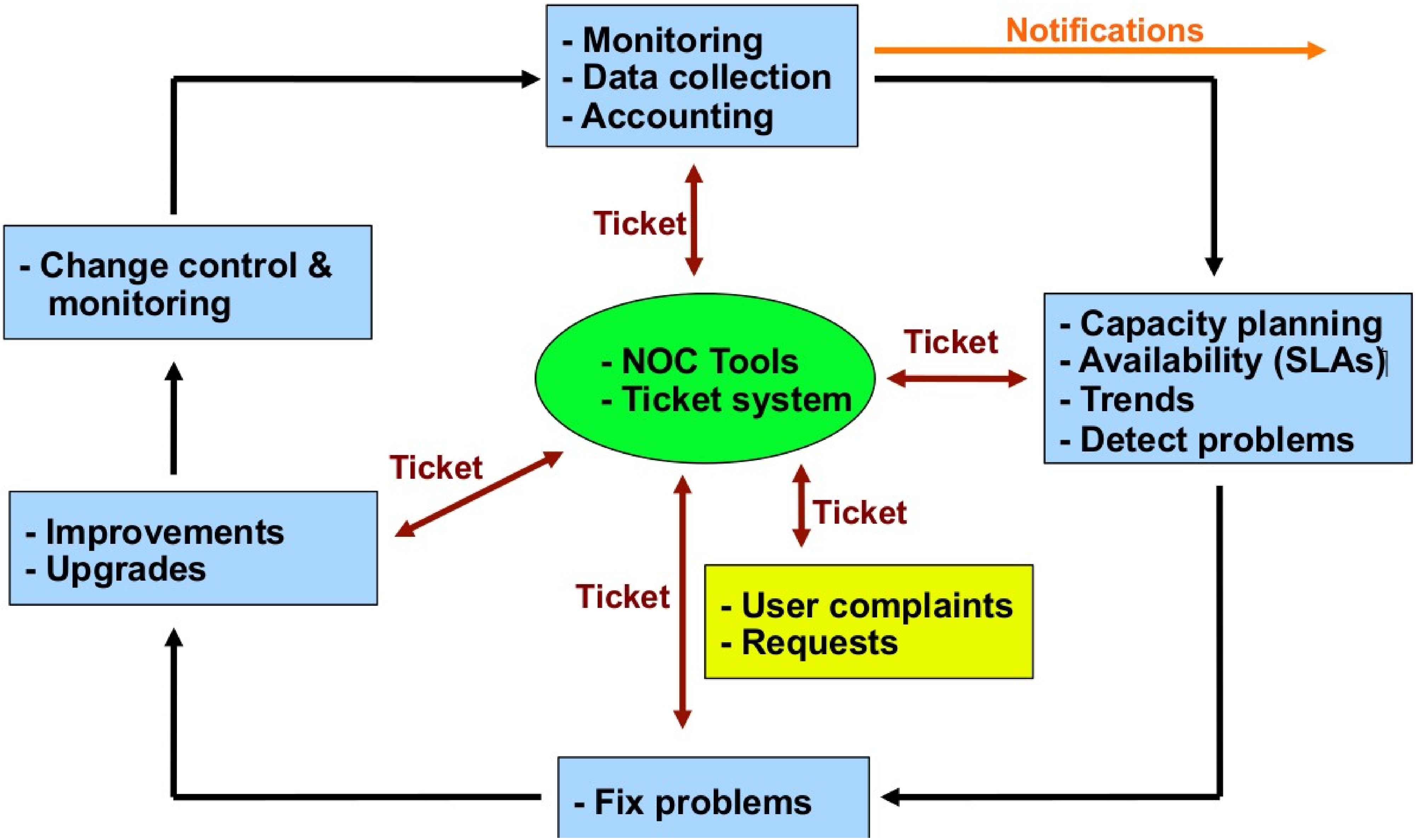
What is Constantly Tracked

- Statistics
  - for purposes of accounting and metering.
- Faults
  - Detection of issues.
  - Troubleshooting issues and tracking their history.
- Ticketing systems are useful for this.
- Help Desks are also useful and a critical component.

Attack Detection

- Trends and automation allow you to know when you are under attack.
- The tools in use can help you to mitigate attacks:
- Flows across network interfaces
- Load on specific servers and/or services
- Multiple service failures

Putting It All Together



- Monitoring
- Data collection
- Accounting

Notifications

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

- NOC Tools
- Ticket system

- Change control & monitoring

- Improvements
- Upgrades

- User complaints
- Requests

- Fix problems

A few Open Source NOC Tools...

Performance

Cricket
IFPFM
Flowc
graphite
mrtg*
NetFlow*
NfSen*
ntop
perfSONAR
pmacct
RRDtool*
SmokePing*

Ticketing

RT*
Trac*
Redmine

Change Mgmt

Mercurial
Rancid* (routers)
CVS*
Subversion*
git*

Security/NIDS

Nessus
OSSEC
Prelude
Samhain
SNORT
Untangle

Logging

swatch*
syslog-ng/rsyslog*
tenshi*

Net Management

Big Brother
Cacti*
Hyperic
Munin
Nagios*
OpenNMS*
Observium*
Sysmon
Zabbix

Documentation

IPplan
Netdisco
Netdot*
Rack Table

Protocols/Utilities

SNMP*, Perl, ping

INTRODUCTION TO NETWORK MONITORING

HEZRON MWANGI
Systems Administrator
hmwangi@kenet.or.ke

14th August 2013

kenet
Kenya Education Network

Introduction To Network Monitoring

- To monitor or monitoring generally means to be aware of the state of a system.
- To observe a situation for any changes which may occur over time, using a monitor or measuring device of some sort.
- The term network monitoring describes the use of a system that constantly monitors a computer network for faults and notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

Monitoring Types

- Application Performance Monitoring.
- Environmental Monitoring.
- Network Monitoring.
- System Monitoring.
- Website Monitoring.

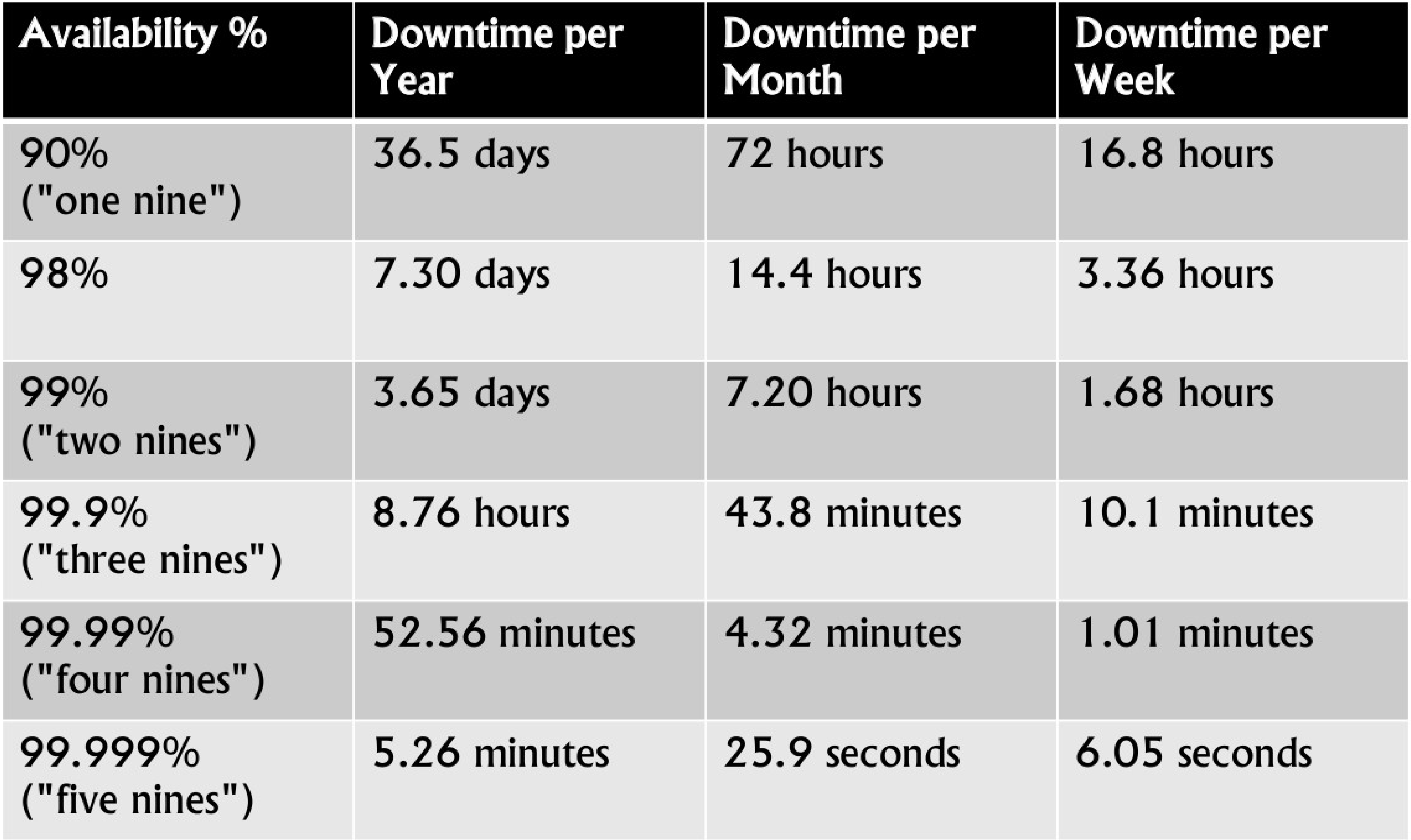
What is Monitored

- Systems/Service for Availability and Reliability.
- Resource Utilization for expansion planning and maintaining availability.
- Reliability & Performance (RTT & Throughput).
- Configuration changes for documentation, revision control and logging.

Why Monitor

- Deliver on targets i.e. key performance Indicators (KPIs) and Service Level Agreements (SLAs).
- Early detection and fault resolution Mean time to repair (MTTR).
- Accurately report on the state of the systems being managed.

Availability



Availability %	Downtime per Year	Downtime per Month	Downtime per Week
90% ("one nine")	36.5 days	72 hours	16.8 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds

Monitoring Tools

- Availability
  - Nagios - Services, servers, routers, switches.
- Reliability
  - Smokeping - Connection health, rtt, service response time, latency.
- Performance
  - Cacti - Total traffic, port usage, CPU RAM, Disk, processes.
- *Functional overlap exists between these programs!*

Nagios

- Nagios actively monitors the availability of devices and services.
- Availability of services, servers and network devices.
- Possibly the most used open source network monitoring software.
- Sends alerts and/or triggers alerts.
- Logs history and generates SLA reports.
- Can support up to thousands of devices and services.

Nagios - Installation

- Dependencies:
  - Apache 2
  - PHP
  - GCC compiler and development libraries
  - GD development libraries
- Install nagios using the apt package manager.
- Key directories:

  /etc/nagios3

  /etc/nagios3/objects

  /lib/libexec/nagios

  /var/www/nagios
- Nagios web interface sample is here:

  http://ipaddress/nagios

Nagios - Architecture

- Plugins are used to verify the state of devices & services.
  - Small, self-contained applications which make a single connection to test a service then quit.
  - Return OK, Warning, Critical or Unknown..
  - Many plugins supplied, even more available
    - http://exchange.nagios.org
    - http://nagiosplugins.org
- Data storage: plain text files.
- Data visualisation: CGI web interface.
- Configuration: plain text files.

Nagios - Configuration Files

- Located in /etc/nagios3:
  - cgi.cfg
    - Controls the web interface and security options.
  - nagios.cfg
    - Main configuration file.
  - resource.cfg
    - Used to specify an optional resource file that can contain $USERn$ macro definitions.
  - objects/
    - All other configuration files go here.

Nagios - Configuration Files Cont'd

- The /etc/nagios3/objects directory:
  - commands.cfg
    - The commands that nagios uses for notifications.
  - contacts.cfg
    - Users and groups.
  - localhost.cfg
    - Definition of the nagios host.
  - printer.cfg, switch.cfg
    - Definition of printers and switches.
  - templates.cfg
    - Sample object templates.
  - timeperiods.cfg
    - Defines when to check the state of objects.

Nagios - Features

- Allows you to acknowledge an event.
    - A user can add comments via the GUI.
- You can define maintenance periods.
    - By device or a group of devices.
- Maintains availability statistics.
    - Can detect flapping and suppress additional notifications.
- Allows for multiple notification methods:
    - e-mail, pager, SMS, win-popup, audio, etc...
- Allows you to define notification levels for escalation.

Smokeping

- Based on RRDTool (the same author).
- Measures latency and can measure performance and status of services such as HTTP, DNS, SMTP, SSH, LDAP, etc.
- Define ranges on statistics and generate alarms.
- Written in Perl for portability.
- Easy to install harder to configure.

Smokeping Features

- SmokePing keeps track of your network latency:
- Best of breed latency visualization.
- Interactive graph explorer.
- Wide range of latency measurement plugins.
- Master/Slave System for distributed measurement.
- Highly configurable alerting system.
- Live Latency Charts with the most 'interesting' graphs.
- Free and Open Source Software written in Perl.
- written by Tobi Oetiker, the creator of MRTG and RRDtool.

Reading Smokeping Graphs

- Smokeping sends multiples tests (pings), makes note of RTT, orders these and selects the median.
- The different values of RTT are shown graphically as lighter and darker shades of grey (the “smoke”).
- This conveys the idea of variable round trip times or jitter.
- The number of lost packets (if any) changes the color of the horizontal line across the graph.

Smokeping Dependencies

- RRDtool http://oss.oetiker.ch/rrdtool/
- Fping http://www.fping.com/
- Echoping http://echoping.sourceforge.net/
- Apache http://httpd.apache.org/
- Perl http://www.perl.org/
- FCGI http://www.fastcgi.com/drupal/
- SpeedyCGI http://www.daemoninc.com/SpeedyCGI/

Smokeping Installation

- Install using the apt package manager.
- Configuration file:

  /etc/smokeping/config
- Change Smokeping’s appearance:

  /etc/smokeping/basepage.html
- Restart the service:

  /etc/init.d/smokeping restart

  /etc/init.d/smokeping reload

Smokeping Config File

- Config file is set out in the following sections:
  - General
  - Database
  - Presentation
  - Probes
  - Slaves
  - Targets
- Generally most time is spent configuring Targets, Probes and Alerts.

Smokeping Summary

- Simple but powerful network monitoring.
- Monitor machines, services and link health.
- Distributed instances for external views often a paid-for service.
- Easy to configure and customize, but very extensible.
- Can be used with Ticketing Systems to automate alerts.
- Very small disk and CPU footprint.

Cacti

- Cacti is a complete network graphing solution designed to harness the power of SNMP, RRDTool's data storage and graphing functionality.
- Cacti is presented in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices.

Cacti Features

- Cacti features include:
  - a fast poller,
  - advanced graph templating,
  - multiple data acquisition methods
  - unlimited graph items
  - auto-padding support for graphs
  - graph data manipulation
  - flexible data sources

Cacti Features Cont'd

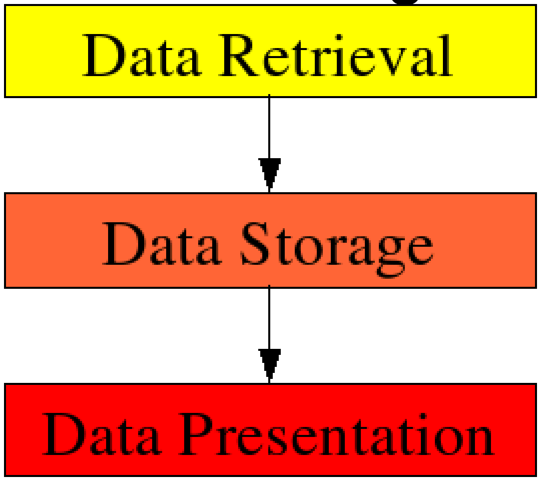
- data gathering on a non-standard timespan
- custom data-gathering scripts
- built-in SNMP support
- graph templates
- data source templates
- host templates
- tree, list, and preview views of graph data
- user-based management and security
- Supplied with many plugins.

Cacti Installation

- Dependencies
  - RRDTool
  - MySQL
  - PHP
  - A Web Server e.g. Apache or IIS
- Install Cacti using the apt package manager.

Cacti Principle of Operation

- Cacti operation may be divided into three different tasks:
  - Data Retrieval through it's Poller either cmd.php or spine.
  - Data Storage uses RRDTool to store data.
  - Data Presentation through web based graphs.



Q/A

THANK YOU!

kenet

Kenya Education Network