Introduction to Network Monitoring

Introduction

- Welcome to the Advanced Campus Network Monitoring and Management course. This course is designed to give you as the campus Network/Systems administrator the necessary skills and tools to implement a campus network operations center.

- A campus network comprises of different components: Switches, routers, access points, ip telephones, servers offering different services among others. As a network/systems administrator it is vital you monitor these devices and services for reasons such as ensuring uptime, statistics collection , detecting intrusions and availability of resources.

This course has been developed by KENET with some reference to materials created by the NSRC team

www.nsrc.org

Objectives

The Campus Network Monitoring Course will cover the following topics:

- What is network Monitoring and Management?

- Why you need to monitor and manage your network

Why Network Monitoring & Management?

As a system/network administrator you need to monitor the following:

System & Services

The systems and services offered on campus need to be monitored for availability.

Resources

You need to ensure that the services you are offering have enough resources to run. Eg is there enough RAM and Hardisk Space on your server?

Performance

This involves checking on issues like throughput and the round-trip-time eg what is the optimal throughput between the Core switch and the switch at the School of engineering.

Changes and Configurations

As you make changes to your network you need to keep track of the changes and also backup all the configurations. Eg you need to track the switch configurations.

Statistics

You need to have records of your campus network for accounting purposes.

Faults (Intrusion Detection)

You need to be able to detect issues on your network and keep track of the issues as they arise. It is recommended that you have an ICT Help Desk with a ticketing system.

Baselining

What is normal on your Campus Network?

You need to measure the following on your campus network:

- Typical load on links: eg the vlan to computer lab, what is the load on that link?

- Level of jitter between end points eg between the switch in Administration block and the switch

- Percentage use of resources: you need to monitor the resources on your servers. This includes RAM, Hard-disk space etc

- Typical amounts of noise:
    - Network Scans
    - Dropped data
    - Reported errors or failures

Why do you do this?

Know when to upgrade

- Is the bandwidth you are getting from your NREN sufficient to meet the campus demands?
- Which VLAN or users are consuming the most bandwidth on campus?

Keep an audit trace of changes

- All changes made to the campus network need to be tracked.
- When a configuration change is made on the server or switch, this needs to be recorded.

Maintain history of network operations

- You need to have a ticketing system to keep track of events

Accounting

- You need to track usage of resources on the campus network. This includes server resources, etc

Know when you have problems

- Stay ahead of the network users. Monitoring tools can generate tickets and automatically notify staff of any issues.

Trends

- Monitoring your network enables you to know the norm on your network.

The "Big Three"

The following are the main open-source tools that you already have!!

Availability

Nagios- This tool can be used to check on the availability of Services, Servers, Routers, Switches etc
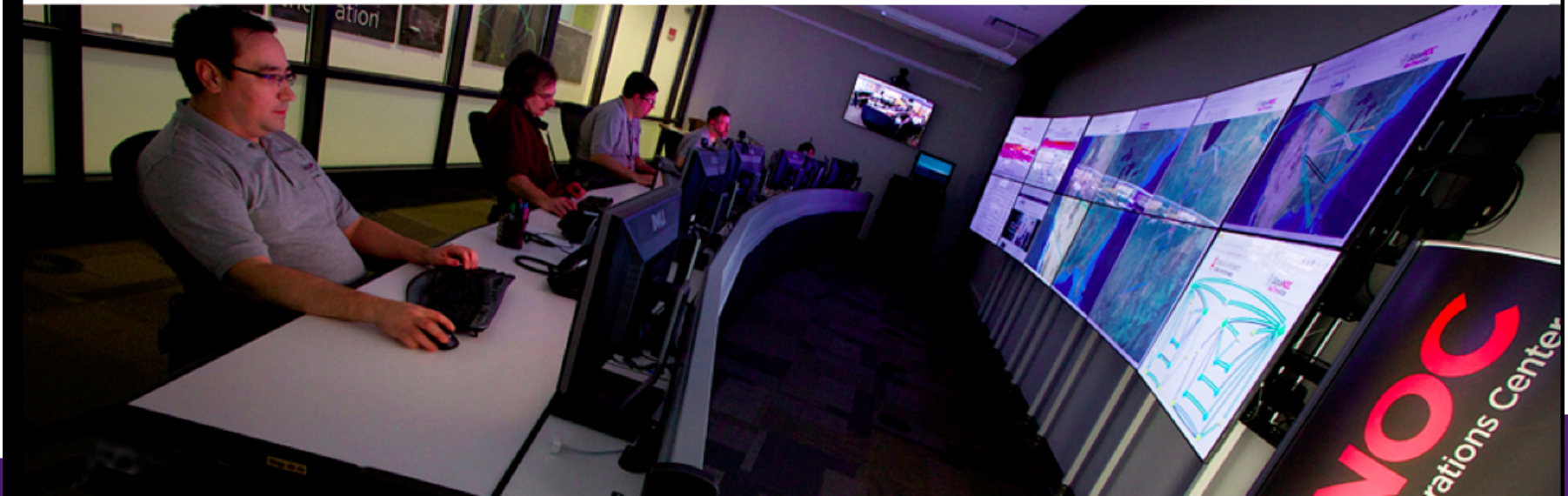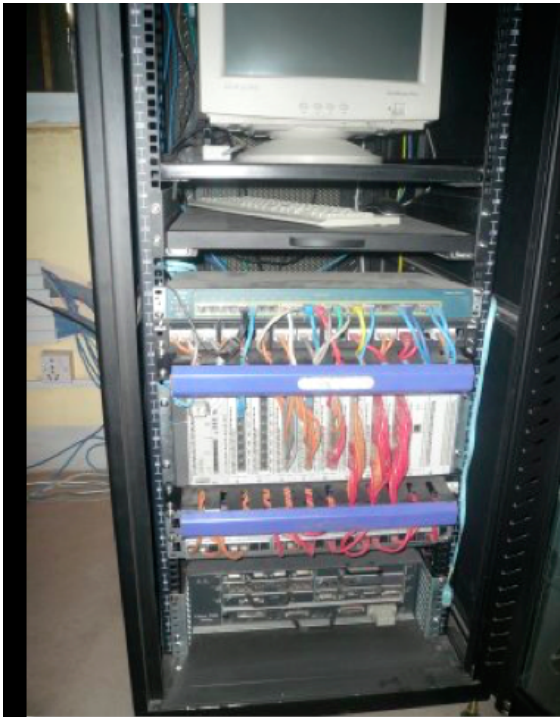
Reliability

Smokeping- This tool can be used to check on the reliability of connections; rtt, service response time,latency.

Performance

Cacti- This tool can be used to check on the performance of links, total traffic, port usage, CPU RAM, Disk, processes etc

Network Operation Center (NOC)

Network Operation Center (NOC)

The NOC is a location on your campus where network monitoring and management is done from.

The following roles are performed in the NOC:

- Coordination of tasks

- Monitoring and management of the network and services

- Fielding of network-related incidents and complaints

- Documentation including:
    - ✓ Network Diagrams
    - ✓ Database/flat file of each port on each switch
    - ✓ Network description
    - ✓ etc

Network Monitoring & Management Center

Monitoring

Check the status of a network

Management

Processes for successfully operating a network

Monitoring Systems & Services

Systems

– Routers

– Switches

– Servers

Services

– DNS

– HTTP

– SMTP

– SNMP

What do we Manage?

- Asset mangement: What equipment have we deployed?

  What software is it running

  What's its configuration (hardware & software)

  Where is it installed

  Do we have spares?

- Incident management: fault tracking and resolution

- Change management: Are we satisfying user requests?

  Installing, moving, adding, or changing things

- Staff management

Why do we Manage?

- To ensure we meet business requirements for service level, incident response times etc

- To make efficient use of our resources (including staff)

- To learn from problems and make improvements to reduce future problems

- To plan for upgrades, and make purchasing decisions with sufficient lead time

Network Management Tools

Ticket Systems: RT

Manage provisioning & support

Configuration Management: RANCID

Track router configurations

Network Documentation: Netdot

Inventory, Location, Ownership of Network Assets

Integration & overlap exists between these programs!

Transforming *education* through *ICT*

Thank You

www.kenet.or.ke

Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500