kenet
Kenya Education Network

Introduction to Network Monitoring and Management

KENET TRAINING

Transforming education through ICT

Objectives

Introduce Core Concepts & Terminology

- ❖ Network Monitoring & Management
- ❖ What & Why we Monitor
- ❖ Uptime Expectations & Calculations
- ❖ Baseline Performance & Attack Detection
- ❖ What & Why we Manage
- ❖ Network Monitoring & Management Tools
- ❖ The NOC: Consolidating Systems

NOC: Consolidating NMM Systems

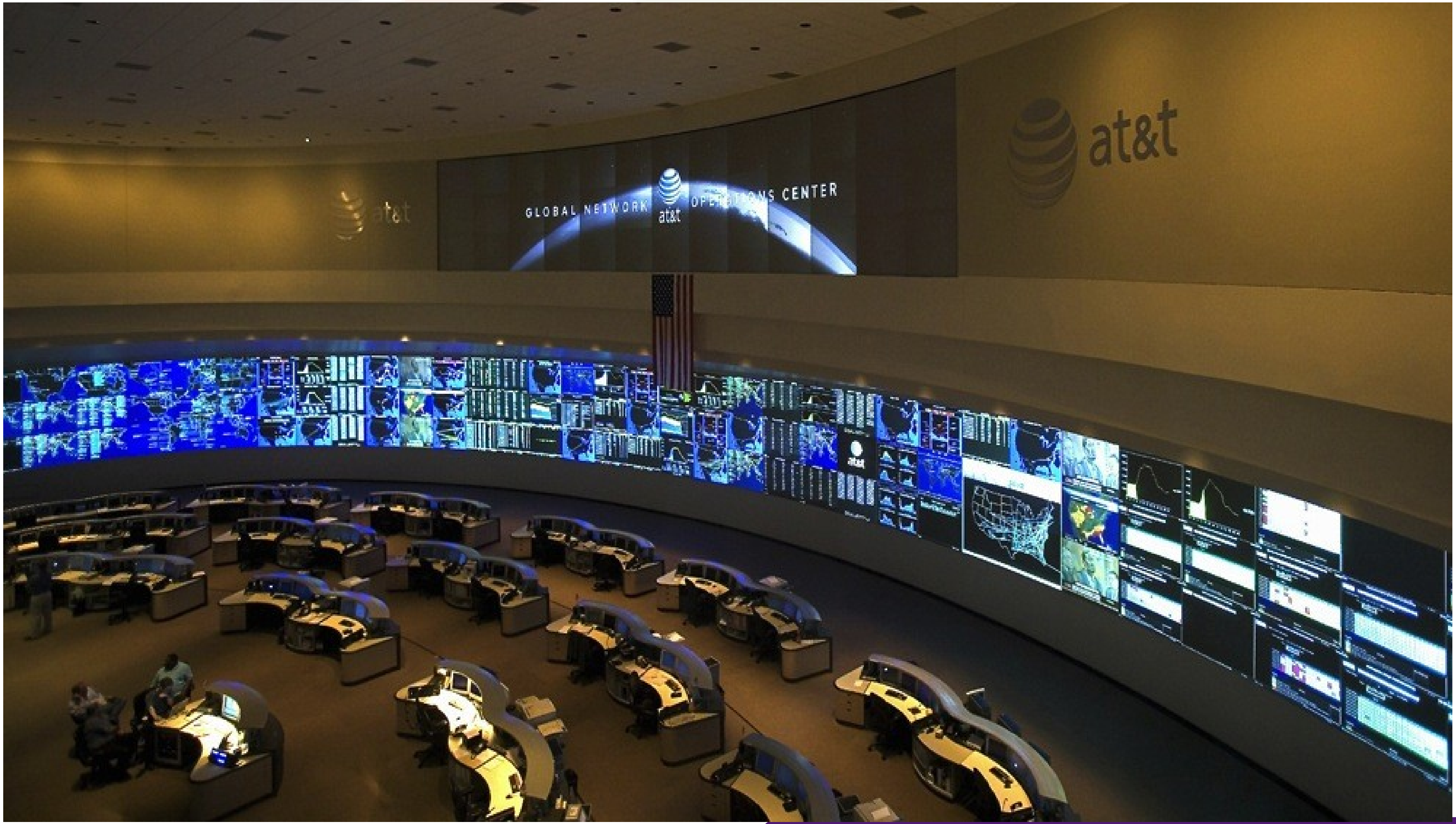
NOC = Network Operations Center

- Coordination of tasks
- Status of network and services
- Handling of network related incidents
- Where the tools are accessed
- Store of Documentation

NOC Location

- NOC is a business construct
- Does not need to be a place, or even a single server
- Remote / Distributed NOC is valid with OOB Management

A BIG NOC



A small NOC

In the same room there is a desk with a phone, another computer and a monitor. This acted as the group's Help Desk.

Many network problems could be detected and solved on the spot!

Network Monitoring & Management

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

Why do we Monitor?

- Are Systems and Services Reachable?
- Are they Available?
- What's their Utilisation?
- What's their Performance
  - Round-trip times, throughout
  - Faults and Outages
- Have they been Configured or Changed?
- Are they under Attack?

Why do we Monitor?

- Know when there are problems - before our customers!
- Track resource utilisation, and bill our customers
- To Deliver on Service Level Agreements (SLAs)
  - What does management expect?
  - What do customers expect?
  - What does the rest of the Internet expect?
- To prove we're delivering
  - Have we achieved Five Nines? 99.999%
- To ensure we meet SLAs in the future
  - Is our network about to fail? Become congested?

Uptime Expectations

- What does it take to deliver 99.9% uptime?
  - Only 44 minutes of downtime a month!
- Need to shut down one hour a week?
  - That's only 99.4% uptime
- Maintenance should be negotiated in SLAs
- What does it mean that the network is up?
  - Does it work at every location? Every host?
  - Is the network up if it works at the Boss's desk?
  - Should the network be reachable from the Internet?

Establishing a Baseline

- Monitoring can be used to Establish a Baseline
- Baseline = What's normal for your network?
  - Typical latency across paths
  - Jitter across paths
  - Load on links
  - Percent Resource Utilisation
  - Typical amounts of noise
    - Network scans & random attacks from the Internet
    - Dropped packets
    - Reported errors or failures

Detecting Attacks

- Deviation from baseline can mean an attack
- Are there more flows than usual?
- Is the load higher on some servers or services?
- Have there been multiple service failures?
- These things could mean an attack

What do we Manage?

- What equipment have we deployed?
  - What software is it running
  - What's its configuration (hardware & software)
  - Where is it installed
  - Do we have spares?
- Are we satisfying user requests?
  - Installing, moving, adding, or changing things
  - Fault tracking and resolution

Why do we Manage?

- Know when there are problems - before our customers!
- Track resource utilisation, and bill our customers
- To Deliver on Service Level Agreements (SLAs)
  - What does management expect?
  - What do customers expect?
  - What does the rest of the Internet expect?
- To prove we're delivering
  - Have we achieved Five Nines? 99.999%
- To ensure we meet SLAs in the future
  - Is our network about to fail? Become congested?

Network Monitoring Tools

- **Availability: Nagios**
  - for servers, services, routers, switches, environment
- **Reliability: Smokeping**
  - connection health, rtt, service response time, jitter
- **Performance: Cacti**
  - traffic, port utilisation, cpu, RAM, disk, processes

- ***Integration & overlap exists between these programs!***

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!***

A Few Open Source NMM Tools

Performance	**Change Management**	**Net Management**
Cricket	Mercurial	Big Brother
flowc	RANCID	Cacti
mrtg	CVS	Hyperic
NetFlow	Subversion	LibreNMS
NfSen	git	Nagios
ntop	Security/NIDS	OpenNMS
perfSONAR	Nessus	Sysmon
pmacct	OSSEC	Zabbix
RRDTool	Prelude	Documentation
SmokePing	Samhain	IPplan
Ticketing	SNORT	Netdisco
RT	Untangle	Netdot
Trac		**Utilities**
Redmine		SNMP, Perl, Ping

NOC: Consolidating NMM Systems

- NOC = Network Operations Center
  - Coordination of tasks
  - Status of network and services
  - Handling of network related incidents
  - Where the tools are accessed
  - Store of Documentation
- NOC Location
  - NOC is a business construct
  - Does not need to be a place, or even a single server
  - Remote / Distributed NOC is valid with OOB Management

NMM Review

- Network Monitoring & Management
- What & Why we Monitor
- Uptime Expectations & Calculations
- Baseline Performance & Attack Detection
- What & Why we Manage
- Network Monitoring & Management Tools
- The NOC: Consolidating Systems

Questions

kenet
Kenya Education Network

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