

Campus Network Design Workshop

Introduction to Network Management & Monitoring



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(<http://creativecommons.org/licenses/by-nc/4.0/>)



UNIVERSITY OF OREGON

Last updated 18th October 2016



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

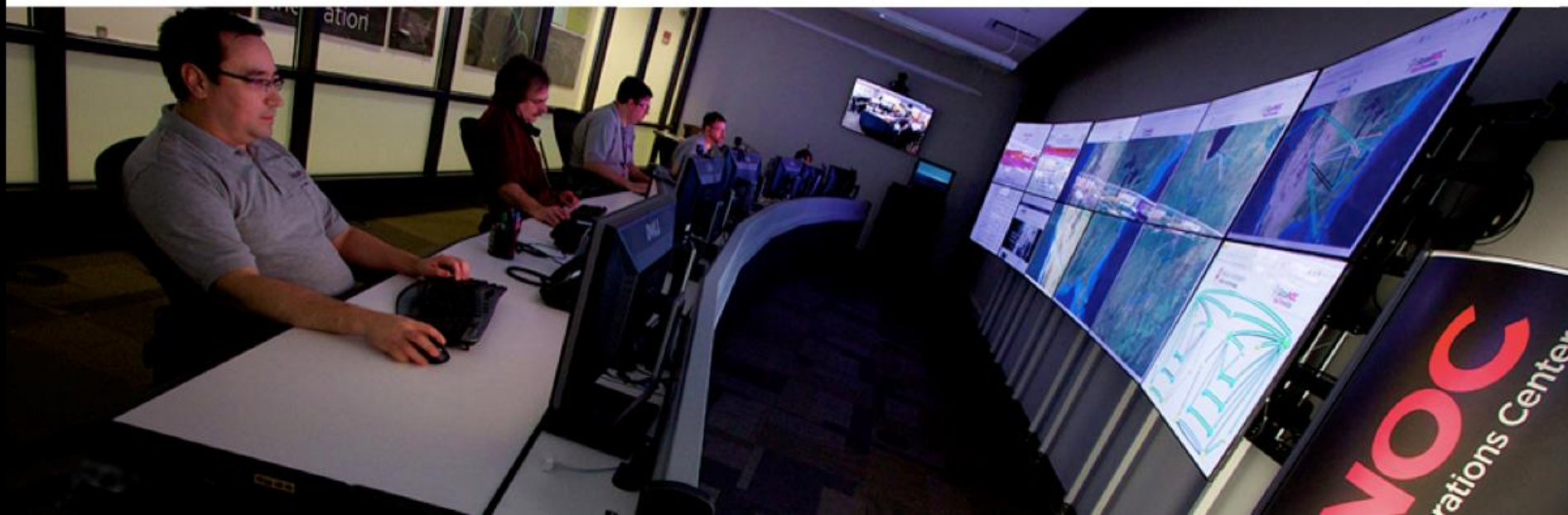
NOC = Network Operations Center

- Coordination of tasks, handling of network related incidents (ticketing system)
- Status of network and services (monitoring tools)
- Where the tools are accessed
- Store of Documentation (wiki, database, repository ==> network documentation tool(s))

NOC Location

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





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



UNIVERSITY OF OREGON



Why do we Monitor?

- Are Systems and Services Reachable?
- Are they Available?
- What's their Utilisation?
- What's their Performance
 - Round-trip times, throughput
 - 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?



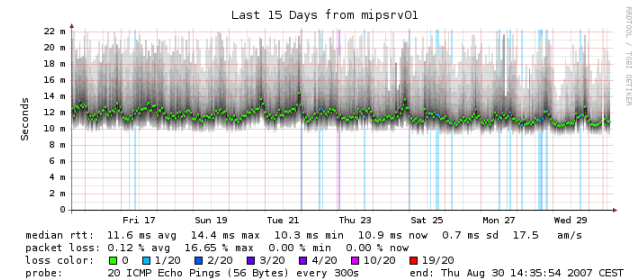
Uptime Expectations

- 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 $((732-4)/732 = .9945355\dots)$
- Maintenance might 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

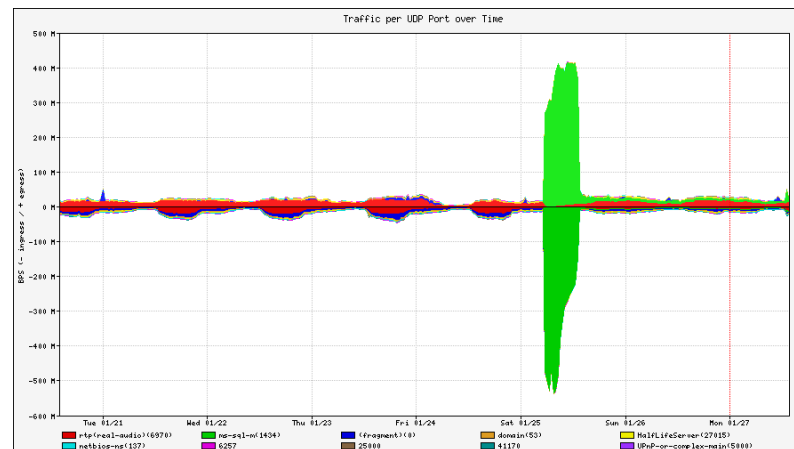
- Monitoring can be used to Establish a Baseline
- Baseline = What's normal for your network?
 - Typical latency across paths
 - **Jitter across paths**
 - Load on links
 - Percent Resource Utilisation
 - Typical amounts of noise
 - Network scans & random attacks from the Internet
 - Dropped packets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

- Asset management: 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 Monitoring Tools

- Availability: [Nagios](#)
 - for servers, services, routers, switches, environment
- Reliability: [Smokeping](#)
 - connection health, rtt, service response time, jitter
- Performance: [LibreNMS](#)
 - 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

NMM Review

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



Questions?



UNIVERSITY OF OREGON

