SI5 – Administration des Réseaux

Monitoring, Managing, and Troubleshooting Computer Networks

Dr. Quentin Jacquemart
quentin.jacquemart@unice.fr

http://www.qj.be/teaching/

Plan du module

1. 09 octobre 2018
    1. Introduction générale
    2. Méthodes pour diagnostiquer/déboguer le réseau
    3. TD
2. 16 octobre 2018
    1. Management et Monitoring des réseaux et services
    2. TP

The Need for Network Management [K&R]

- Complex systems:
  - Jet airplanes
  - Nuclear power plants
  - ...
- Autonomous System $\Leftrightarrow$ hundreds/thousands of connected devices
  - Software *and* hardware
- Goals:
  - Fault detection (e.g. links/interfaces failures)
  - Monitoring of hosts, traffic, ...
  - Route flapping detection
  - Monitoring service level agreement (SLA)

Functional Areas I

[K&R; NSRC]

We monitor

- **systems** and **services**

  ⇒ *availability*, *accessibility*

- **resources**

  ⇒ *replacement*, *addition*, *fail-over*

- **performances**

  ⇒ *bandwidth*, *RTT*, *bottlenecks*

  — requires real-time changes to maintain/improve (network) conditions

- **configurations** (and their changes)

  ⇒ *documentation*, *versioning*, *logs*

Functional Areas II

[GSRI; K&R; NSRC]

We record:

- **statistics**
  - ⇒ *accounting/billing*
  - ⇒ network *modeling*
- **faults**
  - — faults = *any* **abnormal** operation (detection, isolation; ≠ error)
  - — keep historical traces
- ideally: **ticketing system**
  - ⇒ create, update, debug, and resolve issues
  - — between network operators and network users

Network Management: a Definition

[K&R]

Network management
includes

the **deployment**, **integration**, and **coordination**
of the *hardware*, *software*, and *human elements*

to

monitor, **test**, **poll**, **configure**, **analyze**, **evaluate**, and **control**
the *network* and *element resources*

to meet the *real-time* **operational performance** and **Quality of Service**
requirements at a *reasonable cost*.

Monitoring vs. Management

- **Monitoring**
  - Check the status of a network/service
- **Management**
  - Processes for successfully operating a network

Meet Service Level Agreements (SLAs) I

[NSRC]

- **Service Level Agreements** = *SLAs* (accords niveau de service)
  - *Quality of Service* (**QoS**) expected/required *from* a provider
- SLAs depend on many factors. For example:
  - management criteria
  - end-user criteria
  - customer criteria
  - external factors
- Is it enough to require a 99.999% uptime?

Meet Service Level Agreements (SLAs) II

- A 99.999% *uptime* (SLA), corresponds to a weekly acceptable downtime d, such that

$$\frac{7 \times 24 \times 60 - d}{7 \times 24 \times 60} \geq \frac{99.999}{100}$$

  i.e. a downtime of **6.048 seconds per week**, *at most*.

$\Rightarrow$ on average (approximately), this means, at most

  — a downtime of **24 secondes** per month;

  — a downtime of **5 minutes** per year.

- Q1: is it enough a guarantee?
- Q2: what about (planned) updates, maintenance, . . . ?
- Q3: how to measure downtime?

  From the Internet? From the network itself? Between network services/hosts?

Network Baseline

- What is **normal**/*typical* for *your* network?
- Need to know:
  - the usual **load** on links (⇒ MRTG/Cacti)
  - the **jitter** across paths (⇒ SmokePing)
  - the usual **usage** of resources (e.g. CPU/RAM percentages, requests/min, . . .)
  - the amount of **noise** on the network
    - random network scans & attacks from the Internet
    - rates of dropped packets
    - rates of failures and/or errors
    - . . .

Why a Network Baseline? I

⇒ Know when to **upgrade** the infrastructure

- need for more providers, internal links, ...
- migrate to a newer/better/more appropriate underlying technology

⇒ Detect (potential) **problems**

- preventive detection of a failing network card/wire

⇒ Detect global **trends**

- capacity planning

⊕ Audit and logging/attribution

⊕ Billing

Why a Network Baseline? II

[NSRC]

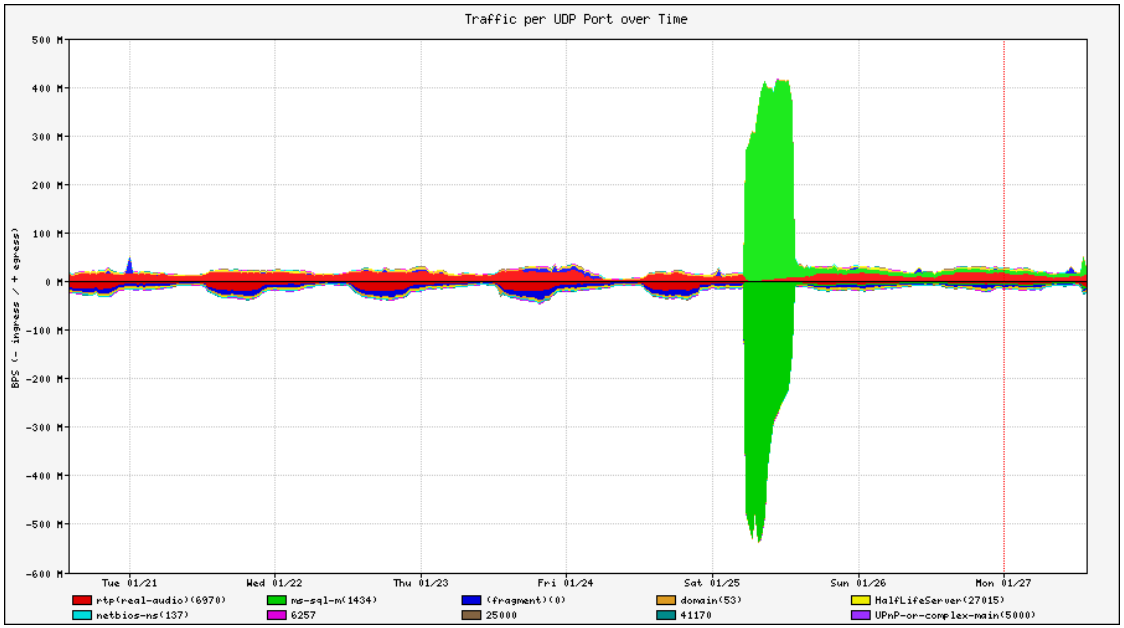


Figure source: [NSRC]

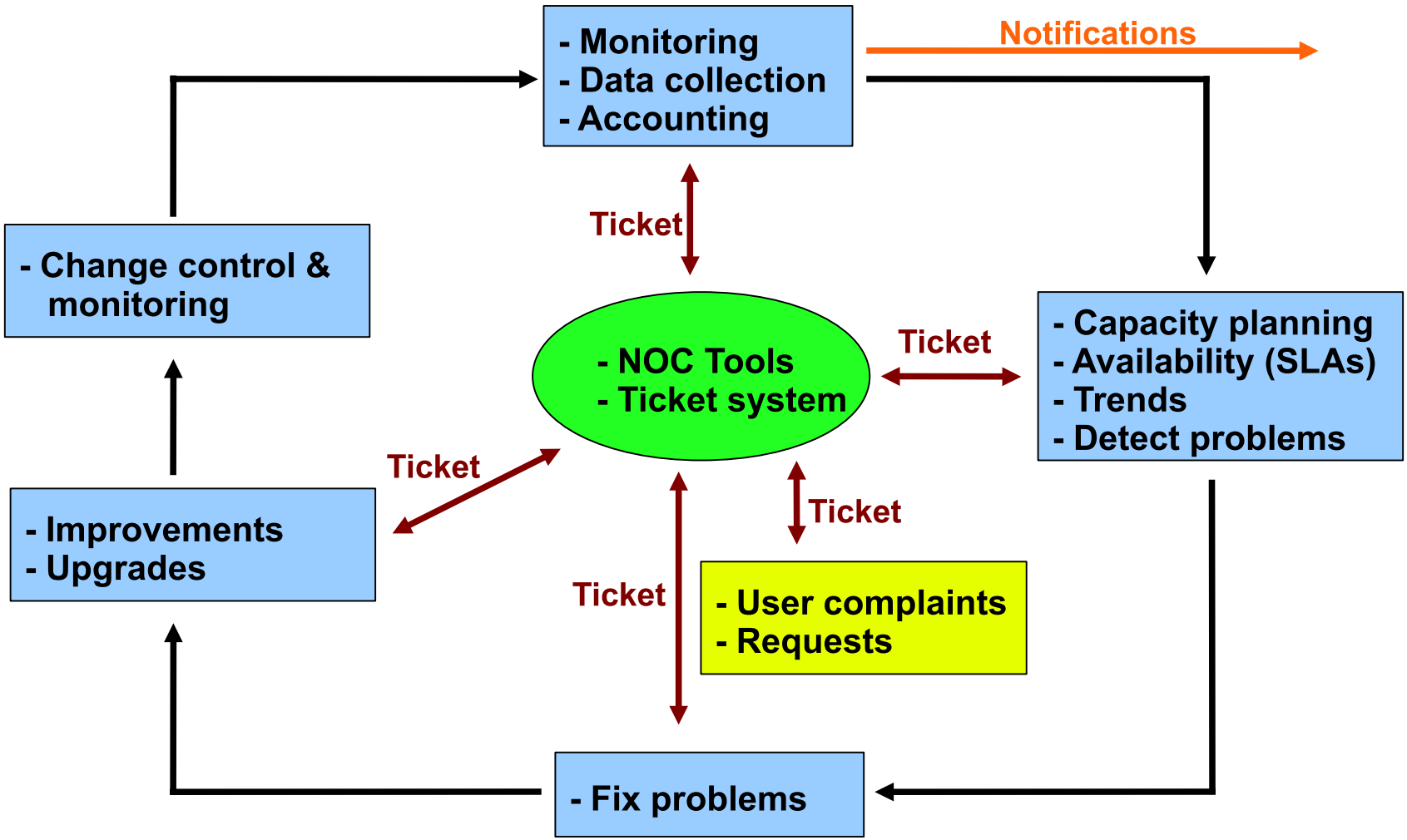
- Deviation from baseline can mean an attack
  - Are there more flows than usual?
  - Is the load higher on specific servers/services?
  - Have there been multiple (cascaded) service failutres?

Network Operations Center I

[NSRC]

- *NOC* = **Network Operations Center**
- *Coordination* of tasks of network-related incidents
- *Monitoring* the status of network and services
- Responsible for handling **tickets** (faults, incidents, complaints)
- Responsible for **documenting** the network:
  - diagrams/schematics
  - technical description
  - information database about devices (e.g. port status of each router/switches)
  - etc.
- Responsible for hosting/handling ad-hoc tools (i.e. *NOC server*)
- NOC is an *organizational concept*, not necessarily a single/physical location

Network Operations Center II



A few open-source tools...

Performance

- Cricket
- IFPFM
- flowc
- mrtg
- NetFlow
- NfSen
- ntop
- perfSONAR
- pmacct
- RRDtool
- SmokePing

Tickets

- RT
- Trac
- Redmine

Version control

- Mercurial
- Rancid
- CVS
- Subversion
- git

Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Logging

- swatch
- syslog-ng/rsyslog
- tenshi

Management

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

Documentation

- IPplan
- Netdisco
- Netdot
- Rack Table

Protocols/Tools

- SNMP
- bash/perl/python
- ping/traceroute

Bibliography I

[GSRI]
G. Leduc, *Gestion et securite des reseaux informatiques (info-056), chapitre 1*, http://www.montefiore.ulg.ac.be/~leduc/cours/GSRI.html, 2010.

[K&R]
J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th. Addison-Wesley, 2012.

[NSRC]
Network Startup Resource Center, *Introduction to network monitoring and management*, https://nsrc.org/activities/agendas/en/nmm-3-days/netmgmt/en/welcome-intro/network-management.pdf.