Network Monitoring and Management

Introduction to Networking Monitoring and Management

Part I: Overview

Core concepts presented:

- What is network monitoring
- What is network management
- Getting started
- Why network management
- The big three
- Attack detection
- Documentation
- Consolidating the data
- The big picture

Network Management Details

We Monitor

- **System & Services**
  - Available, reachable
- **Resources**
  - Expansion planning, maintain availability
- **Performance**
  - Round-trip-time, throughput
- **Changes and configurations**
  - Documentation, revision control, logging

Network Management Details

We Keep Track Of

- **Statistics**
  - For purposes of accounting and metering
- **Faults (Intrusion Detection)**
  - Detection of issues,
  - Troubleshooting issues and tracking their history

- Ticketing systems are good at this
- Help Desks are a useful to critical component

Expectations

A network in operation needs to be monitored in order to:

- Deliver projected SLAs (Service Level Agreements)
- SLAs depend on policy
  - What does your management expect?
  - What do your users expect?
  - What do your customers expect?
  - What does the rest of the Internet expect?
- What's good enough? 99.999% Uptime?
  - There's no such thing as 100% uptime (as we'll see) →

“Uptime” Expectations

What does it take to deliver 99.9 % uptime?

30.5 days x 24 hours = 732 hours a month

(732– (732 x .999)) x 60 = 44 minutes

only 44 minutes of downtime a month!

Need to shutdown 1 hour / week?

(732 – 4) / 732x 100 = 99.4 %

Remember to take planned maintenance into account in your calculations, and inform your users/customers if they are included/excluded in the SLA

How is availability measured?

In the core? End-to-end? From the Internet?

Baselining

What is normal for your network?

If you've never measured or monitored your network you will need to know things like:

- Typical load on links (➔ Cacti)
- Level of jitter between endpoints (➔ Smokeping)
- Typical percent usage of resources
- Typical amounts of "noise":
  - Network scans
  - Dropped data
  - Reported errors or failures

Why do all this?

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 network management?

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.

The “Big Three”?

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!

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

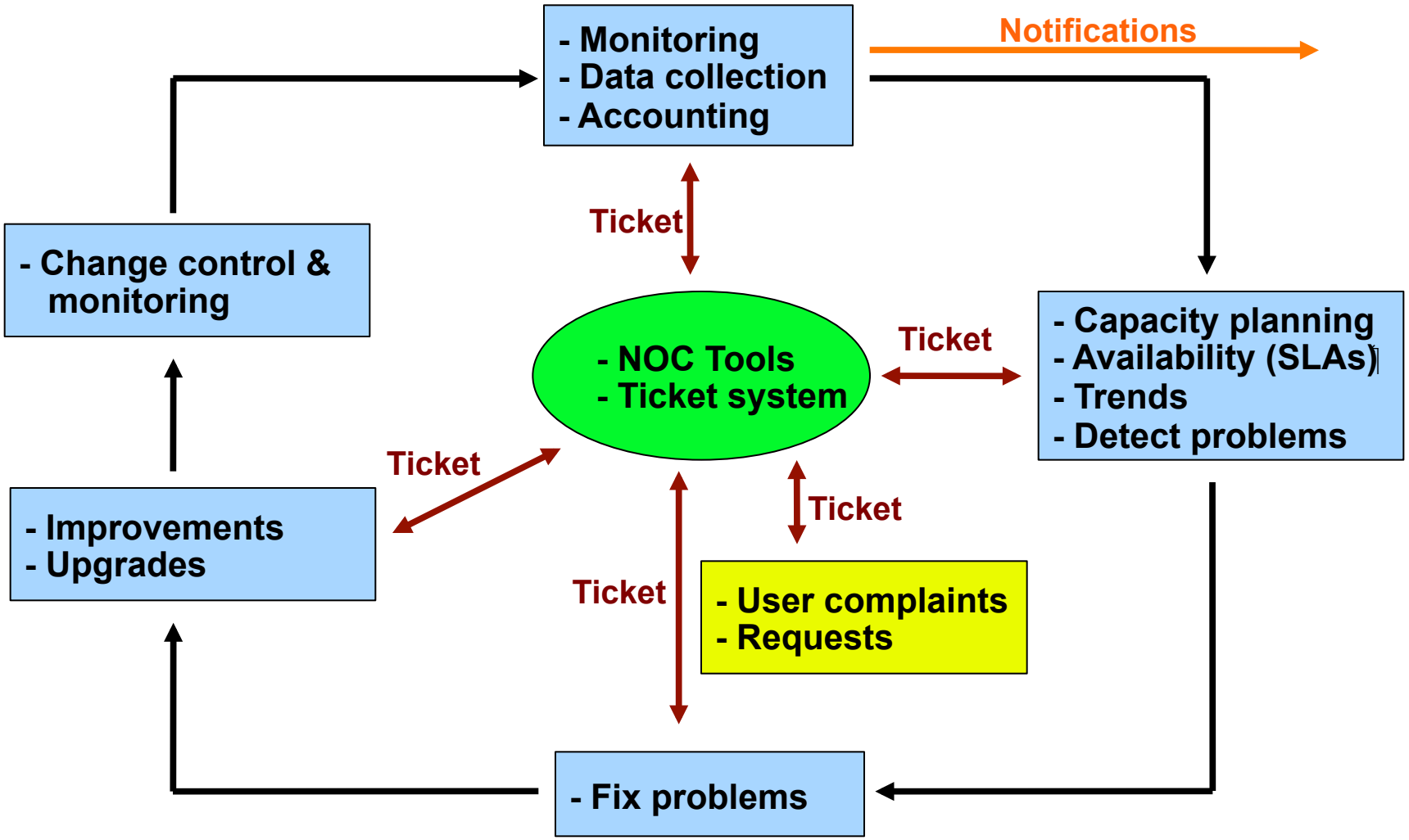
Consolidating the data

The Network Operations Center (NOC)

“Where it all happens”

- Coordination of tasks
- Status of network and services
- Fielding of network-related incidents and complaints
- Where the tools reside (”NOC server”)
- Documentation including:
  - Network diagrams
  - database/flat file of each port on each switch
  - Network description
  - Much more as you'll see.

The big picture



A *few* Open Source solutions…

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

Questions?

?