INASP: Effective Network Management Workshops

Unit 4: Network Management

About these workshops

Authors:

- Dick Elleray, AfriConnect
    - delleray@africonnect.com
- Chris Wilson, Aptivate
    - chris + inaspbmo2013@aptivate.org

Date: 2013-04-29

Objectives

On completion of this session, we hope you will know about:

- Good practice in network management
- Identifying and solving problems
- Detecting and predicting problems
- Preparing for disasters
- The role of policy in guiding/changing behaviour

What is network management?

ISO network management model:

- Faults
- Configurations
- Performance
- Security
- Accounting

See Cisco's Network Management System: Best Practices White Paper.

What is Fault Management?

> Detect, isolate, notify, and correct faults encountered in the network.

Why does ISO think this is important?

Cisco says:

> The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

The first task of a network administrator is to *keep the network running*.

Some network admins never get beyond that part. Too busy fighting fires. Our aim is to get beyond there, but how?

- Reduce incidences of faults
- Reduce effects of faults (redundant systems) - reduces pressure
- Detect and correct faults before users do - reduces pressure
- Keep users informed - reduces pressure

Let's be Aikido network admins: we deflect (resolve) problems and maintain our calm and happiness.

There is a unit on detecting and isolating faults.

What problems must we solve?

Users report faults all the time.

What faults do you NOT want to fix?

We need boundaries to be relaxed. Otherwise, the amount of work you might be asked to do is infinite:

- "Fix my printer!"
- "Fix my light switch!"
- "Fix my telephone!"

Please spend a few minutes making a list of common problems that you're expected to solve. In a group, try brainstorming out a list of 10-15 problems. Include some which you consider to be your job, and some which you'd like to refuse.

To be a relaxed sysadmin, we must spend less time solving urgent problems like these. We can do that by:

- Limiting our domain (job description), e.g. "no electrics". This makes it someone else's problem.
- Understanding user problems and solving them before they occur

Limiting our domain is a policy issue, needs management support:

- Decide what you want to support
- Negotiate with management to get it in writing (policy)
- Post it on the door and walls of the IT centre and online helpdesk

For example, you might be able to:

- Make it someone else's job to fill up the printer?
- Shut down the internal phone system and use mobiles instead?

We can also help users to help each other, by setting up a forum for self-help within the organisation, and helping people to use online resources to solve problems themselves (for example ServerFault.com). Could you allow users to sign for and collect more toner themselves?

Look at your list of faults, and cross off the ones that can realistically be made someone else's problem, or where users could help themselves.

How do we diagnose faults?

Users report faults all the time.

We need an objective standard to verify and understand them, quickly.

Users aren't usually lying, but they often don't understand the problem:

- "The internet is slow" could mean "Internet Explorer is running slowly" or "I have too many programs open" or "I stepped on my network cable and now it's broken".
- "The printer is broken" could mean "the cable is broken" or "my nephew uninstalled the printer driver from my computer".

We have a lot of practice at diagnosing problems, but often by hand, and there can be better ways to do it.

Whenever you solve a problem, take five minutes at the end to think how you could have solved it more quickly, or prevented it from happening next time:

- How would you check the printer status? Remotely?
- How would you tell if the user's computer is running slowly? Remotely?
- How would you tell if the user's computer is connected to the network? Remotely?
- How would you tell if the Internet connection is OK? Remotely?

Faster diagnosis of faults means a higher level of user satisfaction and quality of service. The whole university network runs better.

Doing things remotely saves you the time of leaving your desk to visit the other person. It also allows you to check many potential causes quickly.

There are many useful command-line and graphical tools that can help you:

- Most printers have a web server that tells you their status, if you connect them to the network.
- You can use Windows Remote Desktop or VNC to log into a computer and Task Manager to check its performance.
- You can enable Windows' Performance Counters and access these remotely over the network. (Memory, swap, disk and CPU usage would be particularly useful).
- You can use the `ping` command to check the network connection of a computer or the Internet.
- You can use the `traceroute` command to identify routing hops between you and a target computer, locally or on the Internet.
- You can use Netdot to automatically draw network diagrams at layer two, to help you diagnose layer two faults (between switches).

Look at your list of faults, and identify which tools you could use to diagnose them. Use the Internet or brainstorm in a group to generate ideas.

What faults can we predict?

Users report faults all the time.

If we can detect the fault early, we have more time to fix it, which means less stress and more flexibility.

Sometimes you can fix the fault before the users can notice it.

Fewer noticed faults means a higher level of user satisfaction and quality of service. The whole university network runs better.

We can often detect and solve problems before they occur:

Printer running out of toner.

> We can monitor the printer automatically with Nagios, which will send us email when the toner is running low.

Or before users notice and complain about them:

Internet connection slowing down.

> If causes by one individual's excessive traffic, we can identify them, talk to them or take other measures to reduce their impact before other users complain.

We can often solve problems before they occur. This requires reflection. At least you can make a list of problems. Analyse your day and see what you spend time on. Ideally, track problems through a ticketing system, including how long it took to resolve them.

It also requires that you know how to diagnose the problem automatically. If you have a tool that gives you a *yes or no* answer, *is there a problem or not*, then you can automate the use of that tool to generate alerts automatically as soon as a problem occurs.

Most of advanced network and systems administration is about automated fault detection. *That means it is difficult - but not impossible!* Tools already exist to detect most faults in an automated way, if you can work out how to use them.

Look at your list of faults, and identify how you could get a *yes/no answer* about whether the fault exists. Use the Internet or brainstorm in a group to generate ideas.

How do we mitigate faults?

Users report faults all the time.

By planning, we can reduce the impact of faults, and have more time (less pressure) to resolve them.

Reducing severity of faults means a higher level of user satisfaction and quality of service. The whole university network runs better.

To do that, you must make faults:

- less likely
    - redundant systems
    - automatic failover
    - more reliable technology
    - failure prediction and prevention
- less severe/urgent
    - how can users continue to work without this system?
    - a computer lab they could use instead of their desktop?
    - a spare computer they could borrow?
    - a wireless network they could use instead?
    - some way to send mail even if the main mail server is down?
    - a backup (slower) internet connection/provider?

Look at your list of faults, and identify how you could mitigate each one, making it less likely or less severe. Use the Internet or brainstorm in a group to generate ideas.

How do we keep users informed?

- Why does it matter to users?
- When do you notify them?
- What do you tell them?
- How do you tell them?

By notifying users when a fault has occurred, we allow them to plan their time, to avoid frustration and wasting time. This results in a higher level of user satisfaction and quality of service.

The network does not run better, but people are happier if their time is not being wasted.

We can notify users in advance, as soon as we know that a fault or reduced service will occur.

If we did not notify them in advance, we can notify them as soon as possible when a fault has occurred.

In both cases, we can tell them when it will be fixed by. If we can't do that, we should make it clear why we don't know, what we are doing to find out, and when we expect to have more information by.

We can keep users informed of current and future status, for example by having a network status and planned outages web page. We can encourage users to check this page before contacting IT support or submitting fault reports. We can make the page easy to find and to update.

How do we get better?

- Desire to improve
- Reflect on what we did
- Inquire into other possibilities
- Share knowledge with peers

From Reflective Practice on Wikipedia:

> Reflective practice is “the capacity to reflect on action so as to engage in a process of continuous learning”, which, according to the originator of the term, is “one of the defining characteristics of professional practice”.
>
> It involves “paying critical attention to the practical values and theories which inform everyday actions, by examining practice reflectively and reflexively. This leads to developmental insight”.
>
> Reflective practice can be an important tool in … individuals learning from their own professional experiences, rather than from formal teaching or knowledge transfer. It may be the most important source of personal professional development and improvement. As such the notion has achieved wide take-up, particularly in professional development for practitioners in the areas of education and healthcare.
>
> The question of how best to learn from experience has wider relevance however, to any organizational learning environment. In particular, people in leadership positions have a tremendous development opportunity if they engage in reflective practice.

One great value of a support ticket system is in examining closed tickets. Regularly take a sample and ask yourself:

- How do you know it was resolved?
- Has it happened again since?
- How many times has this happened?
- How much frustration or difficulty does it cause?
- Could you reduce the risk or severity of it happening?
- How long did it take to resolve? Could it be faster?
- Could you add monitoring to detect if it happens again?

Also, look at the users of the system. How many people will come back next time they have a problem? If not, why not? Does the system reward or discourage them?

What fraction of support tickets are duplicates? How much extra work do they create? Can the system do anything to reduce them, such as searching for similar tickets and offering them to the user? Can you provide self-help information, such as instructions on resolving common problems?

How long does it take to resolve a support request/ticket? Is the time reasonable? Could it be reduced?

If some requests are denied, because they fall outside the scope of the IT department’s responsibility or contradict policy:

- How many requests are successfully resolved and how many denied?
- Do successful and denied requests fall into categories?
- Could you help users to know in advance whether their request is likely to be accepted or denied?

It’s a good idea to schedule time regularly to work on these issues. Preferably, leave a minimal support staff at the office, and work from a quiet place with phones off, where you can think clearly without distraction.

Personally I like to reflect, immediately after a problem is resolved, to find two sensible ways to prevent that problem from happening again, and implement both of them.

If you don’t have time to implement them immediately:

- Make a list of things to do.
- Schedule a reasonable amount of time each month to work on them.

Recognise and reward staff who provide excellent service to users.

Tell people about what you do. Write an organisational blog about the changes you've made to improve service. If users believe that you can change, they are likely to try to change you. *This is an excellent thing.*

Your users know what the biggest problems are. Who are your most important users? Do you talk to them?

What is Configuration Management?

Recording changes to configuration of network devices such as:

- configuration file management,
- inventory management,
- software management.

Why use Configuration Management?

- What changed?
- When did it change?
- Why did it change?
- Can we put it back?
- Can we solve the problem a better way?

Configuration management helps us to solve two important problems:

- We often need to understand what caused a problem in terms of changes to a system, in order to reverse them or find a better solution.
- We often want to repeat the changes, for example setting up a new router or server in minimal time, or reconfiguring all routers at the same time.

Configuration management is a form of *version control*, applied to system configurations: configuration files, installed packages and updates, registry changes, connection maps and diagrams.

Benefits include:

- Always having an up-to-date network map for troubleshooting.
- Fast replacement of hardware with the latest configuration files.
- Faster testing of new configurations, with quick reversion.
- Easier and more reliable creation of labs for testing new configurations.
- Hardware inventory for insurance, updates, patching and advisory impact assessment.
- Diagnosing and repairing a fault caused by a configuration change.
- Better communication in a network management team.
- Better license compliance, reduces the risk of prosecution.

Configuration management is hard

How would you do it?

Configuration management's scope includes the entire state of every device:

- The partition layout, entire filesystem and registry of servers;
- The physical connections between machines and network devices;
- The configuration files of devices.

Some problems with this scope:

- Do you have space to back up your entire servers?
- Do you have the software and time to run those backups?
- How quickly can you identify a one-file change in a 400GB full-system backup?
- How do you monitor or backup physical connections between devices?

- How do you backup devices that don't have an automated interface?
- How do you cope with encrypted, binary or unreadable configuration files?
- How do you deal with dynamic configuration, such as IP addresses?
- What happens if you forget to document a change, or don't have time?

Some possible solutions:

- Can automatically monitor some switches and routers configurations with RANCID: Cisco routers, Juniper routers, Catalyst switches, Foundry switches, Alteon switches, and HP Procurve switches among others.
- Netdot can automatically generate network maps for you.
- Can configure Linux and FreeBSD servers using Puppet or Chef to make initial configuration easier.
- Can standardise and automate installation of servers.
- Can use full-system backups that support listing the changes between two abitrary increments, and restoring just those files (e.g. `rdiff-backup` or `duplicity` plus shell scripting).
- Can reduce the number of people allowed to make configuration changes.
- Can set policy to require documentation for changes.
- Can monitor servers and routers for unexpected or unauthorised changes, for example using `tripwire` or backup systems.

What is Performance Management?

Monitor and measure various aspects of performance so that overall performance can be maintained at an acceptable level.

How would you do it?

Some software tools return numerical information about services, or even archive and graph it:

Smokeping

collect and graph low-level packet loss and latency data from wireless and modulated Layer 2 links (quality of service/QoS).

Munin

collect and graphing information from Unix servers, such as disk, memory and CPU usage, mail queue size, etc.

Windows Performance Counters

collect and graphing information from multiple (newer) Windows servers across a network.

Nagios

collect performance metrics as well as up/down decision data and from each service, can derive service uptime, can be graphed using add-ons.

Zenoss and Cacti

collect performance metrics from devices with SNMP support and graph them.

pmacct, pmgraph, argus and nfsen

collect network traffic information broken down by flow for analysis.

squid cache manager, webalizer and Google Analytics

collect web traffic logs for analysis.

Diagnosis using baseline data

Useful questions for diagnosing performance-related problems:

- What is "normal"?

- Are we within a “normal” range?
- When did it change?
- What happened at the same time?

All of these require collecting and storing historical data (a baseline).

Why use Performance Management?

- Forensic analysis of failures
- Predicting future failures

We most often use these graphs when a failure has occurred, or a problem is detected by a monitoring system, such as:

- a server crashed
- a network connection is slow/congested/lossy
- Nagios detected a server running out of disk space or memory
- a server is/was running slowly (out of spec)

Nagios checks (yes/no answers) are our most important performance spec. We set thresholds for things like:

- “too slow” page loading
- “too slow” email delivery
- “too much” packet loss
- “too little” disk space free

All these thresholds are arbitrary, *but* they often detect problems before they occur. They also often create noise. Sometimes we have to change the thresholds to reduce noise and keep the system useful.

By looking at the performance graphs we can establish correlations:

- The disk filled up suddenly, overnight: someone left a job running?
- The network connection has been getting more congested for a while,
- Available bandwidth suddenly dropped two weeks ago when the ISP sent an engineer out to resolve another issue.
- The server’s memory is nearly full every night: a scheduled cron job?

Usually these correlations either help us to create new hypotheses, or rule out some hypotheses, to help us identify the cause. They rarely answer the question by themselves.

Graphs are really useful for quickly analysing large quantities of performance data that would otherwise be useless, to pick out correlations and trends by engaging the brain’s visual circuitry.

Careful with Performance Management!

- It’s possible to measure everything;
- Everything has a cost;
- The benefits are limited:
    - post-mortem analysis,
    - early warning of problems.

Performance data can require:

- a lot of CPU time and bandwidth to collect and aggregate;
- a lot of disk space to store;
- a lot of CPU to produce graphs.

For example, our monitoring system with 55 hosts, 650 services in Nagios and 31 hosts, 1085 services in Munin, uses:

- 93% of one virtual CPU
- 5.7 GB disk space
- 1.8 GB per day bandwidth

What is Security Management?

Provide access to network devices and corporate resources to authorized individuals.

Why use Security Management?

- detect intrusions
- identify culprits
- ease account/password management
- prevent access by untrusted individuals

Security stops people from doing things they want to do:

- plugging their computer into the network
- downloading large files, videos and pornography
- installing unauthorised software on your computers
- accessing the network without authorization

Therefore it's important to sensibly balance security and ease of use, and to be flexible (willing to change if necessary).

Sometimes good security makes life hard for legitimate users:

- having to remember many user accounts and passwords
- having to use long passwords which are hard to remember
- having to change their passwords regularly or if compromised
- not being able to access the network from the Internet
- not being able to access the network using any socket they want
- requiring the use of antivirus software that slows their computer down
- blocking legitimate traffic based on keywords
- installing security updates regularly creates downtime

These can be balanced by improved security technology:

having to remember many user accounts and passwords:

provide a directory service integrated with most or all services, such as RADIUS, LDAP, Active Directory, Kerberos, FreeIPA, Samba4 or GoSa.

having to use long passwords which are hard to remember:

Provide two-factor authentication such as hardware tokens to reduce password strength and change requirements while maintaining security.

having to change their passwords regularly or if compromised:

provide a directory service as above.

not being able to access the network from the Internet:

provide a VPN service such as OpenVPN, Cisco IPsec or IPsec/L2TP.

not being able to access the network using any socket they want:

use 802.1x and RADIUS for network authentication instead of MAC address locking, to maintain identity and access control.

requiring the use of antivirus software that slows their computer down:

choose antivirus software with lower performance impact, or use systems which are less vulnerable, such as tablets, phones and Linux machines.

blocking legitimate traffic based on keywords:

slow down traffic, or monitor and investigate, instead of blocking traffic outright if it appears to breach acceptable use policy.

installing security updates regularly creates downtime:

schedule and automate installation of security updates at quiet times such as during the night. Test security updates on some canary servers before applying to others, or using one of a redundant group.

What are good security practices?

Too many to list! Some examples are:

- strong passwords, regularly changed, or two-factor authentication
- single sign on
- every password has an expiry date
- monitor attempts to log in using expired accounts
- run an intrusion detection system and tune it
- practise penetration testing, security bypass and intrusion response at least annually
- monitor web access for unusual/banned sites and protocols
- encrypt where possible: passwords, disks, emails, backups
- restrict access to certain IP addresses where possible
- use VPNs to provide additional protection on public services where possible
- install security updates regularly, on a schedule
- monitor security and antivirus status and alert if not updated
- lock down computers and user accounts to prevent unauthorised software installation
- ensure that computers use is always associated with a user account
- ensure that security protocols are written down and staff trained in them
- protect yourselves against social engineering and dumpster diving
- monitor blacklists to alert you if your IP addresses appear on them
- store system logs, especially security logs, on a write-only server
- physically secure network equipment, servers, desktops and laptops
- keep backups of servers and configurations to restore quickly after an intrusion

What is Accounting Management?

Usage information of network resources, for:

- detecting and tracing excessive use
- predicting future capacity needs
- auditing and forensics
- billing for usage or enforcing quotas (in some cases)

Detecting, tracing, billing and quotas are covered in the Bandwidth Management unit.

Disaster Response

- What disasters might happen to your network?
- How would you cope with them?

Plan for destruction of all your equipment by fire or theft:

- How long would it take you to recover?
- What does your insurance cover you for?
- How much would it cost?
- How would you respond?
- Can you have a backup/alternate system in place quickly?

Keep backups of all servers and practise restoring a server every year.

From the e-book How to Accelerate your Internet:

Make regular backups

Over time your network configuration will grow and expand to suit your particular network. Remembering the intricate details will become impossible making it very difficult to reproduce the same configuration if it is lost.

Making regular backups ensures that you can rebuild your configuration from scratch if required. Having multiple backups means you can roll back to a previous known working state if a configuration change goes awry.

Disaster plan

Technology is not always as reliable as we hope, and it is a certainty that at some point major problems will strike your network. By planning for these, and having a procedure in place for dealing with them, you will be in a far better situation when the lights go off!

Fallback network mode

It is useful to prepare a basic network configuration state, which only allows a minimum set of services on a network. When a problem occurs which stops the network from functioning effectively you can implement this fallback mode, allowing others to use essential services whilst you are troubleshooting the problem.

Policy and Behaviour

Technical measures alone fail to change behaviour. Why?

“5% of users use 50% of the traffic, so 95% should be on your side.” Discuss.

A hint:

- Who has authority to create policy?
- Who has authority to implement technical measures?
- Who do users fear more?
- Whose side are the users on? What do they want?

Consider your Acceptable Use Policy (AUP). That means you have to find a copy of it. How easy or hard is it? Ask the next person you see to find your policy. Or even better, to explain it to you!

We have a whole session on policies, as well as a separate Policy Development workshop (TODO link to it).

For now, consider how well your users understand your policy. Test them. Test the next person you see: is action X allowed by the policy or not?

How is your policy enforced, by who, and how well? Who follows the policy, who fights against it? How could you get them on side?

It’s been said that “5% of users use 50% of the traffic, so 95% should be on your side.” Do you agree? How many people abuse your network or cause problems for you? Do the others understand the problem and the benefits of reasonable, fair use? If not, how would you show them?

Who is responsible?

Who needs to be involved in network management, and why?

- Executive management
- Senior IT management
- Technical staff involved in the day-to-day implementation
- Academics, librarians and other legitimate Internet users

What roles do they play in managing a network?

Executive management

have the power to create or change policy and budgets.

Senior IT management

bridge the gap between staff on the ground, executives and the rest of the university.

Technical staff

have the skills to understand the problem, implement changes, and identify policy violations.

Legitimate Internet users

are the reason why the University pays so much for its Internet connection and the IT department. They are your customers!

Summary

Hopefully you now feel confident with:

- Good practice in network management
- Identifying and solving problems
- Detecting and predicting problems
- Preparing for disasters
- The role of policy in guiding/changing behaviour

Please take a moment to reflect, review and share your learnings and plans for action with the group.