Network Management Report



James Phillips

October 2015

Introduction 3

Functions of Network Management 4

Configuration 5

Fault Management 6

Account Management 7

Performance Variables 8

Security 9

Data Logging 11

Checking Performance and Traffic 11

Reporting 12

Why Fault Management Should be Included 13

Why Fault Management is Necessary 13

Aims of Fault Management 14

Consequences of Failing at Fault Management 15

Why Routine Performance Management is Required 16

Conclusion 18

Bibliography and Sources 19

# Introduction

This document describes Network Management including details on the functions of network management. Also included are specific details of Fault Management and Routing Performance Management.

The functions of network management will include all phases of the process from initial design through to operating then network. This section will introduce the various functions and explain each.

When looking at fault management, the section will explain why fault management should be included when dealing with network management. In this section we will examine the aims and any consequences of failing.

Finally, we will look at performance management, examining why these activities should be carried out and looking at aspects relating to efficiency and quality standards.

# Functions of Network Management

The functions of network management allow administrator and operators to effectively configure and manage networks. In this section we will look at 8 functions

Configuration

Fault Management

Account Management

Performance Variables

Security

Data Logging

Checking Performance and Traffic

Reporting

The following sections cover each of these points.

## Configuration

Configuration is the process of setting up or changing settings on devices and services that form the network such that they operate together correctly and meet the requirements of the organisation.

During configuration devices such as routers or switches will need to be configured to allow them to work together to correctly and effectively move data around the network.

User accounts will need to be configured, allowing access to specific services, resources (applications, data folders and printers would be examples of resources).

Application software will need to be configured so that users have access to the program and associated items (templates, databases and so on).

Security Software such as virus checking, spam filtering and any software to restrict usage of facilities (for example some organisations block USB access to prevent copying of data to portable devices) or reporting agents for software discovery tools, will need to be installed.

Configuration may also involve installation and setup of a network monitoring tool, checking that the tool correctly communicates with devices (switches etc.) so that the network’s performance can be monitored.

Network configuration is done both when setting up a network and throughout the lifetime of a network to improve performance and respond to problems.

## Fault Management

Any problem with the network is likely to prevent an organisation from working effectively and will possibly have a financial impact. Being able to detect, diagnose and respond to issues with the performance or availability of the network and associated services is therefore an important consideration.

Fault management is the techniques and technology used by a network administrator or operator to keep the network operating, to reduce the chances of failure and to minimise the impact of any failure.

Network fault management can be monitored though programs that send an alarm to the administrator if the network starts to deteriorates in any monitored areas, either by a warning on a central console or by email/SMS text message. This is useful as it can reduce the impact of a fault as the problem can be found and dealt with potentially before any users have been affected.

Effective fault management requires that devices can be remotely controlled (the SNMPv3 protocol – Simple Network Management Protocol, is designed to allow this). A fault management system showing the whole network (including devices from different vendors) in a single console is the most effective tool in fault management.

## Account Management

Users of the network will have an account used to access resources (typically in the fashion of a username and password for login). This account will be used by the network operating system (NOS) to allocate access rights to data folders, applications and other resources such as printers.

These accounts will typically require a tool to allow the administrator(s) of the network to create and maintain accounts.

Account details may include security considerations such as password complexity (length of the password, policy for re-use of passwords, composition of the password – such as must contain at least one capital, one number and one special/non-alpha character, and the length of time a password is valid for). These all help to make user accounts more secure.

In a large organisation there will be a greater number of user accounts. These will typically be managed by making each a member of a group, with the group controlling the access rights. This will make management easier as all members of the group can be provided with access to resources (such as a new application) by amending the definition of the group rather than for each account individually.

An example of a group would be in an educational environment, each year a significant number of new students will require accounts to be provisioned and access to resources on the network allowed. Equally a large number of accounts will need to be deactivated as students leave the organisation. Both activities will benefit from a network management tool that allows group based administration.

## Performance Variables

To maintain performance and reliability of the network requires an understanding of the metrics that are important to the performance and reliability (up-time). These metrics can be referred to as performance variables.

A network management tool will report as to how different parts of the network are performing and allow access to historical data, allowing current performance to be compared to previous periods and the corresponding performance (for example there may appear to be a problem, but it may be a specific periodic or seasonal activity that temporarily increases load on one part of the system).

Any detrimental performance will be of concern, requiring investigation and potentially changes to configuration to restore performance to the required level. Using the same performance variables that identified a problem will allow the network administrator(s) to confirm that any changes or corrective actions have worked.

Typical performance variables are:

* Network Throughput – the amount of data passing through the network. This may be affected by bandwidth issues (if a link between two networks over an external connection is not performing as expected) or by a component such as a network switch not working effectively.
* User Response Times – the time taken for resources (typically applications or services on the network) to respond to user requests. For example users may be using a web-application and seeing responses to store data taking a long time, this could be due to problems in the network (bandwidth issues) or that the server is not performing or is under an unanticipated load (higher than expected number of users).
* Line utilisation – the amount of data that is being put onto the cabling/connections of the network at any one time. Being able to view this in a form that is easy to understand (e.g. a graph) assists in identifying over and under used routes. This may then influence a decision for upgrade or downgrade of the cabling (or other connections) in use.
* Packet Loss – as data is transmitted over the network, the number or percentage of packets not reaching their destination provides an indicator of the networks health. Greater than expected packet loss indicates a problem.

## Security

Network security is the process and techniques of protecting the network from threats to the data stored within and the configurations which keep the network running effectively.

Security covers a range of areas including the threats from internal users, external users and unplanned events such as fire, theft, flood and hardware failures. Each threat type requires a different type of defense.

* Internal Users – can pose a threat through errors (accidental deletion of data or files), inaccurate or incorrect entry of data or by inadvertently introducing a virus or other malware to the network by visiting a compromised or rouge website or by using media (such as a USB memory stick) already infected.

An internal user may also deliberately attempt to cause malicious damage in the event of them having a grievance with the organisation.

To counter threats from internal users, it is vital to have regular backups of data and configurations and to structure account permissions to provide only the resources and access required for a specific job role. Appropriate security software for virus, Trojans and other malware should be used.

User Account details may include security considerations such as password complexity (length of the password, policy for re-use of passwords, composition of the password – such as must contain at least one capital, one number and one special/non-alpha character, and the length of time a password is valid for). These all help to make user accounts more secure.

All staff should be trained in the importance of keeping any access credentials confidential.

* External Users – a network may allow internal users to remotely access the network. Any network that has a connection to the outside (via the internet or dial-in access) is vulnerable to attack by hackers. This may be by impersonating an authorised user or by exploiting a flaw in part of the network security (e.g. in a Network Operating System, Application or hardware device). Firewalls and stringent controls along with good threat management (anti-virus) software are key to minimising this threat.

Security of the software and other assets needs to be considered – especially ensuring that any security related patches are promptly deployed.

* Fire, Flood and Theft – unexpected events such as a fire, flood (including risk from burst pipes, or response to a fire as opposed to a river overflowing) and theft of equipment all pose a threat to the running of a network.

To counter the threat, a comprehensive backup policy is required, ensuring that all data and configuration information is backed up and stored appropriately. By appropriately, we mean in a secure environment – this could be in a fire and waterproof safe, or by transmitting the information (either on physical media or over a connection as data) to another site.

* Hardware Failure – various hardware items may fail, compromising the network. With some components of the network it is feasible to run two of the device in a fail-over mode (when one breaks down the other item will continue to run keeping the network running) or to keep a spare for that device. Other components will not be able to be run in this way and will represent a single point of failure, which should be noted as a risk.

An organisation will typically have a Business Continuity Plan which covers the processes in the event of a major problem with the infrastructure (this will include unavailability of the network or various critical parts of the network). Such as plan may require that resources are made available to a separate site, which may impact on the remaining network infrastructure.

## Data Logging

Data logging provides a record of the interactions passing through a particular point in the system or from a specific device (such as a keyboard and display). By using the results of logging the data it is possible to reconstruct the actions that lead to a system failure and therefore this can help identify and correct the cause of problems.

Logging all traffic/data would create an unmanageable amount of data, so such logs are usually very temporary or activated in response to certain situations.

## Checking Performance and Traffic

When managing a network it is necessary to be aware of the traffic that is passing through the system, this can be achieved by using network monitoring software that allows the user to visually see in real time what the statistics of the networks usage are. Tools such as Microsoft Network Monitor and Paessler Traffic Grapher show current and historic bandwidth usage.

Routine checking of performance and traffic allows the administrator(s) of a network:

* Assess normal performance
* Assess the impact of changes (such as new devices or configuration changes)
* Recognise when performance is degraded
* Recognise when there are device faults
* Understand periodic or seasonal performance issues, to gain and understanding of the requirement, cause and to determine an appropriate resolution strategy.

## Reporting

Being able to access reports detailing network performance (including uptime, throughput and other measures) allows the network administrator(s) to share this information with the appropriate other people within the organisation. This may be to highlight successes or areas that require improvement.

In larger organisations there may be SLAs (Service Level Agreements) that the network management team are working to and are measured against.

Reports can be obtained from the NOS (Network Operating System), such as Windows Server or from devices themselves. The benefit of a tool which covers the whole network would be that the information would be presented from a single tool and in a consistent manner. NetQoS Performance Centre (a CA Technologies product) is one such example, which provides reporting for:

* Application Response Times
* Traffic Analysis
* Packet Analysis
* Device Performance

# Why Fault Management Should be Included

In this section we look in more detail at Fault Management and why it is necessary, it’s aims and the consequence of failing.

## Why Fault Management is Necessary

In a modern organisation, computers are invariably connected to the network in order to allow users to work with shared resources and complete their work.

Any problem with the network involving a degradation of performance or a period of total or partial unavailability (downtime) is likely to prevent an organisation from working effectively and will almost certainly have a financial impact. Being able to detect, diagnose and respond to issues with the performance or availability of the network and associated services is therefore a necessary part of network management.

Including fault management in the overall network management approach allows for the organisation to be alerted to and then to react to problems with the network and avoid or minimise the disruption and costs of a fault.

## Aims of Fault Management

In summary the aims of fault management are to reduce the occurrence and impact of issues and to keep the network running at optimal conditions by preventing as many faults as possible, and quickly isolating and resolving any that occur.

The aims of fault management can be broken down as:

* Reduction in the frequency and impact of network faults
* Early detection of network issues
* Prevention of issues through proactive network management

When faults occur, whether because of hardware failure or poor configuration, there are five elements of network fault management:

* Detecting the fault – this could be by setting thresholds and alarms relating to usage statistics or other performance variables.
* Recognising the cause of the fault – identifying any usage patterns or problems that have led to the fault.
* Correcting the fault – fixing the issue, perhaps by replacing a component, changing configuration or upgrading infrastructure such as cabling.
* Logging the fault and its solution – recording issues and the solutions may assist the organisation respond quickly to future issues of the same type. This is especially valuable if the root cause of a fault is not immediately obvious.
* Trend analysis – recognising patterns of faults, perhaps the network is put under intense load at certain peak times or following a certain event.

## Consequences of Failing at Fault Management

Failing at fault management could result in periods of network downtime or degraded performance. In this eventuality, network users within an organisation could experience difficultly in getting tasks completed and the result of this could be that external deliverables (the provision of goods or services) is affected. For example, the failure of a network in a large supermarket chain may prevent orders being placed, therefore produce would not be in the stores to be sold – the effect being a loss of revenue and a negative customer experience.

# Why Routine Performance Management is Required

Routine performance management will include a number of activities that will collectively benefit the performance (speed and availability) of the network. By ensuring that the network is operating correctly the network administrator(s) are providing the best possible service to the users in the organisation.

Regular measurement of the relevant performance variables and checking of traffic and performance will assess the overall health of the network, when combined with alerting to show changes in status (low-disk space, high line utilisation etc.) this routine management allows for early intervention. This can then be further combined with regular housekeeping activities such as:

* Ensuring user accounts are appropriately cleared for ex-users this could affect performance of the network in respect to storage but also in relation to security.
* Checking storage growth (the rate at which free space is being consumed is a more valid metric than the amount of free space).
* Checking the growth in traffic over network “lines” including internal and external connections and adjusting plans accordingly (if traffic is increasing due to a greater number of users, then understanding the cause of the growth e.g. company expanding, can be used to identify a point where performance will start to degrade and to put in place preventative measures.

By carrying out routine performance management and acting on the information made available from fault resolution and network management tools. It is possible to foresee and therefore plan around upcoming issues relating to demand for network resources.

This in turn will ensure that the efficiency of the network (and the staff administering the network – scheduled preventative activities are easier to manage the reactive activities needed when a problem occurs) and the quality of the service is maintained.

Therefore, to ensure that a network provides an efficient, high quality service to its user’s routine performance management is essential. Without performing routine performance management it is likely that the quality of service will be reduced leaving an organisation with a non-performing or under-performing network. This is turn could have effects on the ability of the organisation to continue its work, which in a commercial venture would have an impact on financial performance and also reputation.

By carrying out routine performance management activities, a network manager will have a suitable baseline to measure against, allowing for growth to be monitored and additional resources to be requested or deployed ahead of a situation occurring.

Quality standards can be incorporated into the role of the network manager. By utilising a standard such as the ISO framework for network management FCAPS (Fault, Configuration, Administration, Performance and Security) sometimes referred to as the ISO or OSI network management model, the organisation can rely on a proven standard. Within this model the SNMP standard protocol is used to collect data, which can be logged and monitored to review for issues relating to capacity or reliability before they affect services.

# Conclusion

In this report we have examined the functions of network management:

Configuration

Fault Management

Account Management

Performance Variables

Security

Data Logging

Checking Performance and Traffic

Reporting

And looked at the detail behind each.

We have also examined the why Fault Management and Routine Performance Management are critical to the successful operation of a network.

# Bibliography and Sources

|  |  |
| --- | --- |
| Source | Information |
| http://www.opsview.com/network-monitoring-software | Background Info |
| https://en.wikipedia.org/wiki/Network\_management | Background Info |
| http://docwiki.cisco.com/wiki/Network\_Management\_Basics | Background Info |
| BTEC Level 3 Information Technology Book 1 - Anderson, Jarvis, Kaye, Lawson, McGill, Phillips, Smith | Background Info |
| <https://en.wikipedia.org/wiki/FCAPS> | FCAPS Info |