Simon Light

Unit 5

Assignment 1

P4.

# The functions of network management.

## Configuration

Configuration is essentially the setting up of the network so that it fits the requirements of the user. This is done mainly at the beginning of the life of the device/network however it should be maintained throughout the lifespan to make minor tweaks. Configuration will also improve performance by removing services that are not needed on the device (such as Bluetooth; Wi-Fi, if on a wired network; graphics drivers etc.

Network devices such as routers and switches need to be configured so that they can communicate to each other. This could be done on a closed loop or on the existing network.

User accounts need to be set up so that the specific users can access their hardware (drives/personal hardware like home printers) and also access the printers and internet or public drives. They also need to be configured with the correct access rights such as administrator/root settings.

Application software needs to be configured in a way so that when it is distributed it can access the necessary files and folders it needs to run correctly. It also may need access to the internet to do updates and to run these configurations remotely.

Virus checking software needs to be configured so that it can correctly identify what is and isn’t a virus. It also needs to be told when to run scans, of which folders, what to do if it finds a threat and where reports of the scan are to be sent. This is especially important if the firm is using monitoring tools such as Impero as these can be seen as a virus if scanned with an anti-virus software.

## Fault management

Fault management is needed to maintain the usage of the network to a high standard. There are a few different methods of fault management that include their own advantages and disadvantages.

Fault management systems continuously monitor the state of individual parts of the network to see if their condition deteriorates. If they do then the system will alert an operator who can resolve the problem quickly without creating a long downtime for the network.

The operator may need to run tests on certain parts of the network to identify the problem more specifically. This can be done with a management system but it can be a lot more expensive for the company.

It is greatly beneficial if the network devices can be remotely controlled as this allows an operator to remotely reboot/reconfigure parts of the network when the company isn’t running which is a prime time to do it as no one will be using the network so won’t lose any of their work

## Account management

Network accounts are the network wide accounts that mean at any computer an employee can sign in and access all of their folders, preferences and rights. This means that any changes a person makes on one computer it effects all computers that you then log into. Network administrators will often use tools to help manage the accounts and the changes to them.

Large network obviously have a large amount of users. The easiest way to manage this is by grouping them (e.g. administrators, HR, accounting, business etc.). This means configuration can be applied to the whole group rather than individually. This allows a lot more efficient configuration of users and also with less errors.

Changes can also be made to individuals without effecting the whole group. This includes things such as rights to software, access bans, added/less firewalls. In addition to this users can be placed into multiple groups/subgroups that can apply changes that don’t take effect as that isn’t their main group.

Using this type of software also means that changes made can also be made temporary e.g. week long internet bans. This avoids errors of forgetting to remove the ban after a week and other such mistakes.

## Performance variables

Performance variables are figures that are sent to the network manager about how well important parts of the network are performing.

This is used to quickly identify the areas of fault in a network. When the data is reported to the manager it will also be sent with a history of performance data for comparison. Once the manager has determined if a certain device in the network needs to be replaced then he may need to do some investigation into exactly what part of the device and if it can be repaired.

The report may also show an improvement in performance. This may be down to reconfiguration in the device or in other parts of the network.

Some performance variables include:

Network throughput is the speed at which data can travel through the entire network. A test for this is moving a large file from one side of the network to the other and timing delivery. This will however show an over optimistic speed as the test is being done in controlled conditions. A better test for throughput is using a tool such as Iperf or Bwiping.

User response times is pretty much what it says on the tin. How quick does the network seem for the user? As the user will not be able to supply very accurate feedback it is good practise to use a tool such as Nimsoft’s Monitoring Solution (NMS).

NMS allows the organisation to read the actual response times the user will be receiving. This can be done in two ways:

* Active monitoring: uses remote computers and software probes to access the network and report response times.
* Passive monitoring: Intercepts packets to and from a specific user and reads time delay between the requests and responses.

Both active and passive monitoring can be used at the same time as they do not interfere with each other.

Line utilisation is data showing how much data is loaded onto the cabling in the network. This is usually shown as a graph. The perfect amount of line load is the maximum capability of the cabling. This is because if it is more, then data may be lost of the network will be slowed down drastically. If it is less then it isn’t as much of a problem, however you know that your network could be running at higher speeds but it isn’t.

This is useful as it can identify areas in the network that need to be given better cabling. IBM offer a NetView Performance Monitor (NPM) network tool. This tool contains a feature that can produce line utilisation graphs for review of a network manager. An important point for configuring this tool is correctly identifying the maximum capability of each cable. That way you can clearly see if data is being overloaded in specific points.

## Security

Security is obviously a massive factor for any network and attacks can come in many forms. Some include: Internet, Staff, Fires, Thefts, Floods and Hardware failures. Network defences are tailored to the types of threat they are used to protect against.

The internet is used a lot by an organisation for communication and promoting their business. The internet is also filled with viruses and hackers. This means that firewalls and anti-virus software needs to be in place to stop these things.

Staff can also be dangerous to the network. They can corrupt data accidently, by making typos or formatting mistakes, or on purpose, if they dislike the company or are planning to leave. This is why you need security measures in place such as regular backups and correct configuration of accounts so that people can only access the parts of the network that they need.

Staff can also introduce viruses into the network form places such as USB drives, the internet, emails etc. This is why good practices should be carried out like staff following safe computing practices, firewalls to prevent email and internet shared viruses entering the network, and virus checkers to remove any viruses that are already on the network.

Fire, theft, floods and hardware failures all provide a threat to the actual hardware that stores this data, the drives. It is a good idea to keep backups in a secure location which means you will lose the minimum amount of information. Keeping the backups in the same place as the original copies is pointless as both will be destroy if there is a fire in the room, instead you should store the backups separately to the originals, perhaps in a fire-proof safe or in an entirely different building. This will provide maximum protection.

## Data logging

Data logging software such as Advanced TCP/IP Logger records data travelling between devices, e.g. keyboard to PC. This data can then be used to decide if and how someone has caused an incident in the network.

Data logs are temporary files which are deleted if not needed. This means that it is good practise to link your data logger software with your fault management software. That way if there is a fault in the network you record inputs to that device to see what caused the error. This is useful as fault management cannot track human input.

## Checking performance and traffic

Constant checking of what your network is actually being used for is a vital tool that needs to be carried out to ensure proper use of the network and therefore proper efficiency. Checking the traffic in your network helps:

* Understand the normal use of your network to identify misuse/errors when they occur.
* See what changes when you connect new devices to your network (you can use this to prevent non administrated access to the network)
* Recognise when performance is reduced.
* Recognise devices that are causing trouble on the network.
* Recognise peak time that your network is struggling and how to prevent this.

Using all of this data you should be able to have a full understanding on what should and should not be popping up on your network and how to prevent or remove these,

M2.

# Fault management

Fault management should always be included in a network. This can be done with either software or by personal manually checking the network. Fault management means that you both try to avoid faults and try to fix them quickly. This means that the users of the network will never have to wait very long for the network to be useable again.

Pre-empting faults is also massively important. It means that you can prevent/fix faults at times which are appropriate for the network. This could be done at time where your network is least in use (at night or early in the morning) or when the network managers have planned a down period, this means that anything users may need off of the network they can get before this time.

It should be included in network management as signs of faults in the network can come from network management tools. If for example you find that your network performance (throughput/line load is low) then you know that you may have a fault. This means that you can identify specific areas of faults. It then means that you can send an engineer to check/solve problems.

If you do not correctly manage faults then it could result in a large unexpected down time on the network. This could mean a company cannot access their data and possibly may lose some data. This makes you (the network manager) liable for any loss to the company. It may also take a long time to fix. This is because you may have to order a new device for the network. This may take weeks to arrive and again will cause a long down time.

Some fault management could include having spare parts laying around the company so that if there is an unexpected fault in the network you can handle it.

D1.

Performance management is the main part of running a network. It is important to carry out as it can identify many things. This can include faults, areas of the network that need to be improved, it can improve efficiency of the network and it allows the pre-emption of performance low spots.

Some of these things can include the growth of storage. This may mean that in the future you have to add more drive space to your network. It may also include the identification of growing traffic through the network. This can affect the speed and performance of your network. This may lead to the network being upgraded due to lack of these factors.

Keeping the network properly configured and optimised means that efficiency is kept to a good standard. This is because staff at the organisation you are working for can always access the network to upload and download data and files. It means this will also be done at a good speed so that they do not have to wait a long time for this to happen, therefore, increasing productivity and efficiency.

This is also down to fixes/upgrades being done at the correct times. This means that the network is only down when very few people need to use it. It also requires pre warning of this s that people can get the information from the network that they need.

Quality standards can be met by using some of the network protocols. The ISO framework for network management FCAPS (Fault, Configuration, Administration, Performance and Security) sometimes referred to as the ISO or OSI network management model. This means that the company (and you) are relying on standards that are proven to work.

Bibliography

http://www.opsview.com/network-monitoring-software

https://en.wikipedia.org/wiki/Network\_management

http://docwiki.cisco.com/wiki/Network\_Management\_Basics

BTEC Level 3 Information Technology Book 1 - Anderson, Jarvis, Kaye, Lawson, McGill, Phillips, Smith

<https://en.wikipedia.org/wiki/FCAPS>