Network operating systems

A network operating system is the same as any other operating system however it has more network oriented application and features built into as standard. It is designed to be run on server machines and is configured to take advantage of hardware that normal operating systems aren’t such as ECC RAM or a massive amount of storage space. Network operating systems are also designed to make it easier to run server side applications and setup servers easier than on normal operating systems. A few main things that network operating systems have that normal operating systems don’t Is the already mentioned hardware support, protocol support such as ICMP, better security as standard with more user access control, management features that have more configurability for administrative actions and finally server functions built in as standard such as email, DNS, file sharing (Samba).

# Linux Server Operating System

The Linux Operating System was a system designed by Linus Torvalds. It was originally designed only as an operating system to be run on x86 architecture however it was adopted by the open source community which resulted in a multitude of version of the operating system. Today there are many versions of the network operating system all based on the same design however all have different implementations of applications and different ideas and designs for the GUI. The main advantages of Linux over the other networking operating systems that are available are the fact that it is free and incredibly highly configurable compared to every other NOS available today. It allows you to run things like Apache web servers, FTP servers, MYSQL Server and many more server applications with ease. Linux is also incredibly fast an efficient compared to most other NOS’s, this is normally because it doesn’t have or need any form of GUI to use it because the majority of the NOS is command line based. One downside to Linux however is the fact it’s a rather big learning curve for a lot of people today, most people are used to using fancy GUI’s to configure and setup pretty much everything while Linux operating systems tend to be require you to type a lot of commands and learn a lot of syntax to be able to use it effectively.

# Windows Server

Windows server is a network operating system designed and sold by Microsoft; it is essentially the same as their normal windows operating system as it has much of the same GUI and application feature aspects. The way in which the server version of windows distinguishes itself from their normal operating system is the features and the industry leading management software implementations it has. Windows server uses something called active directory management to configure and manage all of the access and user rights of all server features on the operating system. It dynamically alters and adapts to different implementations while allowing for a massive amount of configurability in the form of security and application management. It also allows you to configure and manage all of the server applications on the operating system via an easy to use GUI which makes it incredibly easy to both setup and administrate. It allows you to do all of the same things as Linux in the form of DNS Servers, Proxy server, Web Servers, FTP Servers. More than that though it allows you to easily adapt different server aspects to work with their standard operating system interface such as networked file shares that are easily interfaced with via a feature called hard drive mapping.

Network Protocols

Network protocols are designed and needed to fix the problem that occurs when one computer can’t understand another. A protocol is designed to make it so that every computer that is using a specific format of communication can understand and know how to process that information. A good way to explain a protocol is to imagine two different networked computers 1 & 2. Computer 1 can only transmit in French and computer 2 can only understand German. What a protocol allows you to do is have a standard way which we will call English to communicate, so a protocol is an agreement between all application developers and hardware designers to make sure they all use the same language to communicate and process information over a network.

# SNMPv3

SNMPv3 is otherwise known as Simple Network management protocol version 3. This protocol is an application layer protocol that is used in the communication of network management between networked devices for example two networked computers.

SNMPv3 consist of:

* SNMP Manager
* Managed devices
* SNMP agent
* Management Information Database Otherwise called as Management Information Base (MIB)

## SNMP Manager:

The SNMP manager is the management system that is normally a single computer that runs management software across multiple or a single network. The key functions of this management system are:

* Queries agents
* Gets responses from agents
* Sets variables in agents
* Acknowledges asynchronous events from agents

## Managed Devices:

These are the devices on the network that are going to be managed by the manager. Examples of these devices could be, routers, switches, UPS’s, workstations, servers, computers and network printers.

## SNMP Agent:

The agent is what allows the whole of the network management system work. It normally runs on the devices that have management systems on them to collect the information locally and to send it the manager when it requested.

Functions:

* Collects management information about its local environment
* Stores and retrieves management information as defined in the MIB.
* Signals an event to the manager.
* Acts as a proxy for some non–SNMP manageable network node.

## MIB:

MIB or Management Information Base, this is pretty much a database of all the monitored device information that is stored so it can be provided upon request. The MIB is commonly shared between the Agent and the management system so the data is the same and can be updated quickly.

# ICMP:

ICMP is otherwise known as Internet Control Management Protocol. This is one of the main protocols in the internet protocol suite. It is used in many networked devices such as routers or hubs to communicate errors. An example of something this might communicate may be services that are or aren’t currently available, this protocol is commonly seen on desktop computers in the form of the network status icon in the bottom right corner of the computer screen. It’s the ICMP that is in charge of making sure the status of the internet service is reported correctly. Works with routers

Cabling

All networks need some form of connection to be able to communicate information between each other. While there are wireless options available to connect and communicate data over a network. These are normally slow and highly restricted in terms of speed, interference and distance. As such there are cables that you can use the connect networks together, the most common of these are:

# STP

A shielded twisted pair is a way of wiring network cables in such a way so the cable itself is shielded from any outside interference. This is especially good for cabling where you are running it through areas of a building that would have a lot of electrical interference from power cables or even just areas where there is a lot of other network cables running which could also cause a lot of interference. The downsides to this type of cable are that it’s more expensive and is normally harder to run through areas where lots of turns and angles are needed for it to run correctly. This is because the cable shielding adds an element of resistance when trying to run it in areas that are hard to get to or areas that require you two do lots of turns with the cable.

# UTP

An unshielded twisted pair is much like the cabling mentioned above however it has no shielding or very little shielding around the cable. The reason this cable is used a lot is that it’s easier to run and cheaper to buy. You can do much sharper turns with this type of cable due to the lack of resistance on the cable. The downside to this type of cable is that it’s a lot more susceptible to outside interference.

# Fibre Optic

Fibre Optic cables are a much newer cabling medium and allow for much faster transfer speeds than that of Ethernet (STP and UPT). This cable using glass fibre to transfer data and the data is sent in beams of light. This theoretically allows you to transfer data at the speed of light which you can imagine is a lot faster than any other cabling medium. This type of cable is also completely unsusceptible to electromagnetic interference.

Topologies

There are many ways to setup networks, these are all known as topologies. Below are descriptions of all the main Topologies.

Star Topology  
The star topology is commonly used in homes, and features a central hub that can be a hub, switch or router. This hub then connects to the computers, printers and anything else that may be needed, and are normally connected by unshielded twisted pair cables.

Ring Topology  
In a ring topology, every device has two other devices that it connects to. All messages travel through a ring in the same direction, which is either clockwise or counter clockwise. Any failure in the cables can cause the entire network to fail.

Bus Topology  
Bus networks use a common thing that connects all the devices, usually a single cable. A device that wants to communicate with another device on the network sends a message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

Tree Topology  
Tree topologies implement more than one star topology onto a bus. This makes it so that only hub devices connect directly to the tree bus.

Mesh Topology  
Mesh topologies regularly use routes to get something such as a message to its destination, which basically means that something sent on a mesh topology can take any of a number of different paths to the intended destination.

Hybrid Topology  
The basic description of a hybrid topology is that it is a combination of two or more different topologies. Hybrid topologies can be extremely effective and flexible, as the most useful advantages of two or more topologies can be combined into one topology, making it much better than a regular one.

Wireless Facilities

Wireless facilities have blown up in the last few years with the emergence of Wi-Fi as a main source to access networks and the internet overall. Its ease of access factor and the fact that’s it’s literally plug and play due to the industry standards set across all wireless devices today make it possibly one of the most well used facilities for accessing networks in the world (second to only Ethernet). These wireless facilities come in all shapes and forms today so I will cover the most commonly used ones below.

# Wi-Fi

Wireless technology comes in many shapes and forms, the most basic would be Radio or RF. A wireless radio signal was one of the first wireless mediums to be used on a wide scale and allowed people to communicate over vast distances in real time. Since then there has been many different mediums of wireless communication such as satellite and Wi-Fi. Wi-Fi is however the most widely used wireless communication technology in use today. Wireless allows you to send data over moderately large distances depending on the technology you’re using. It’s good for communicating data in areas where having a wired connection just isn’t feasible.

# Wireless Access Points

A wireless access point works exactly like you might think, it allows you to put a point of access for your wireless network somewhere in your home or building. You can use wireless access points in several ways: the first is you can position the access points so that you are in essence boosting your signal distance, you do this by placing the access point where it is in distance of your standard wireless hub however far enough away to extend the overall coverage. The second way you could use an access point is to gain wireless coverage in an area where you may not have coverage from a standard wireless hub and where range extension would be ineffective. To do this you may have a wired connection into the area where you are placing your range extender which would allow you to have wireless coverage in that area too. You could also use wireless access points to create wireless hotspots for your network that would allow others to take advantage of your network.

# Mobile Data (3g/4g)

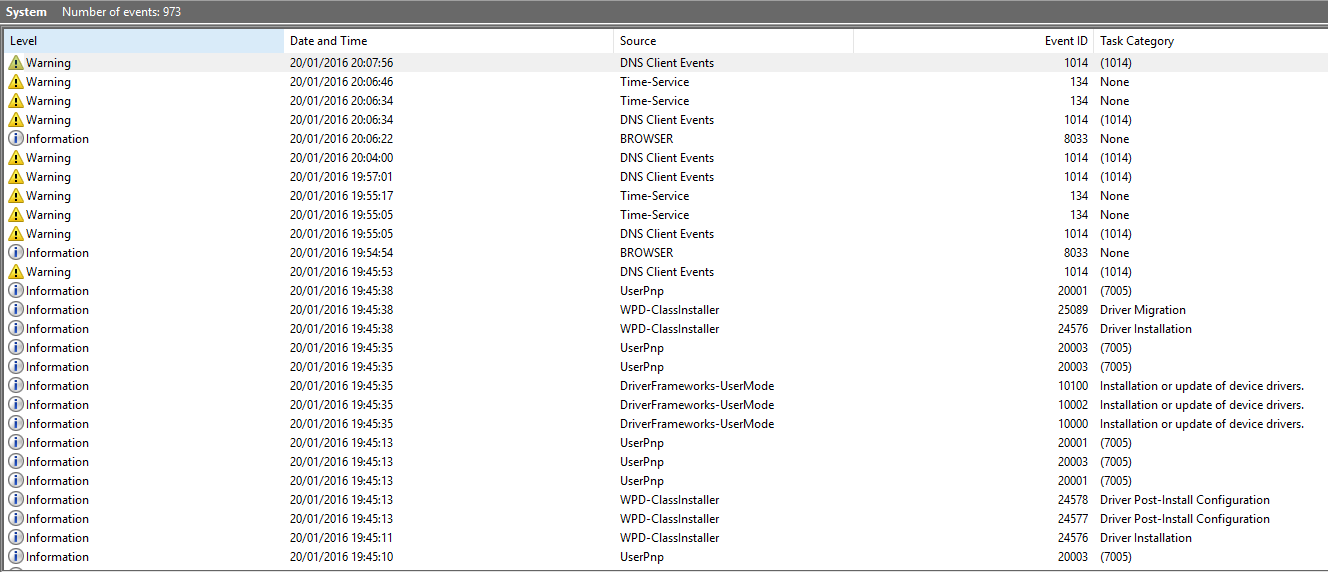
Mobile technology is a lot newer than most other wireless technologies out there and is simply the way of sending and receiving data over the same network your phone calls go through (your mobile service provider). Since then there has been several new implementations of mobile wireless technology with the newest being 4G. 4G allows you to communicate over amazingly vast distances at speeds of up to 50mbit/s.

Server Maintenance Tools

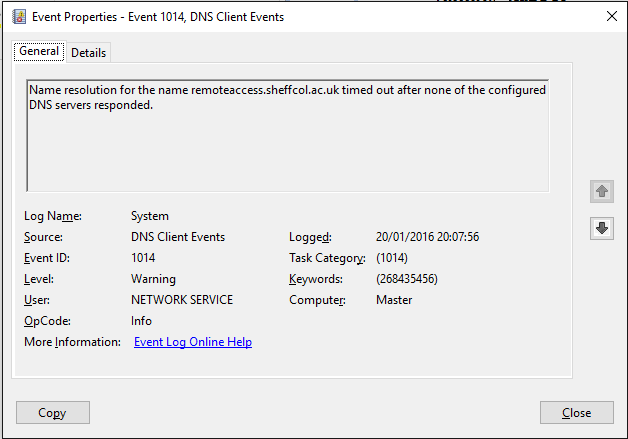
Server maintenance tools are the tools that either come with the server operating system or are third party tools that you can install and use upon your server to monitor just about everything. You would these tools to do a variety of tasks such as the following: Manage Faults, track server performance and track network assets. Some of the tools available to you are the following.

# Event Viewer (Built In)

Event viewer is a tool that is built into all Microsoft windows operating systems (both server and none server). It allows you to monitor the events that occur on your server and will report weather an event was successful, had a problem (warning) or failed all together. This tools is very useful because it allows you to make sure that any events on your server are tracked and useful information is reported back. Here below you can see an example of the event viewer on a Windows Server monitoring and reporting feedback on all events that occur upon the server.

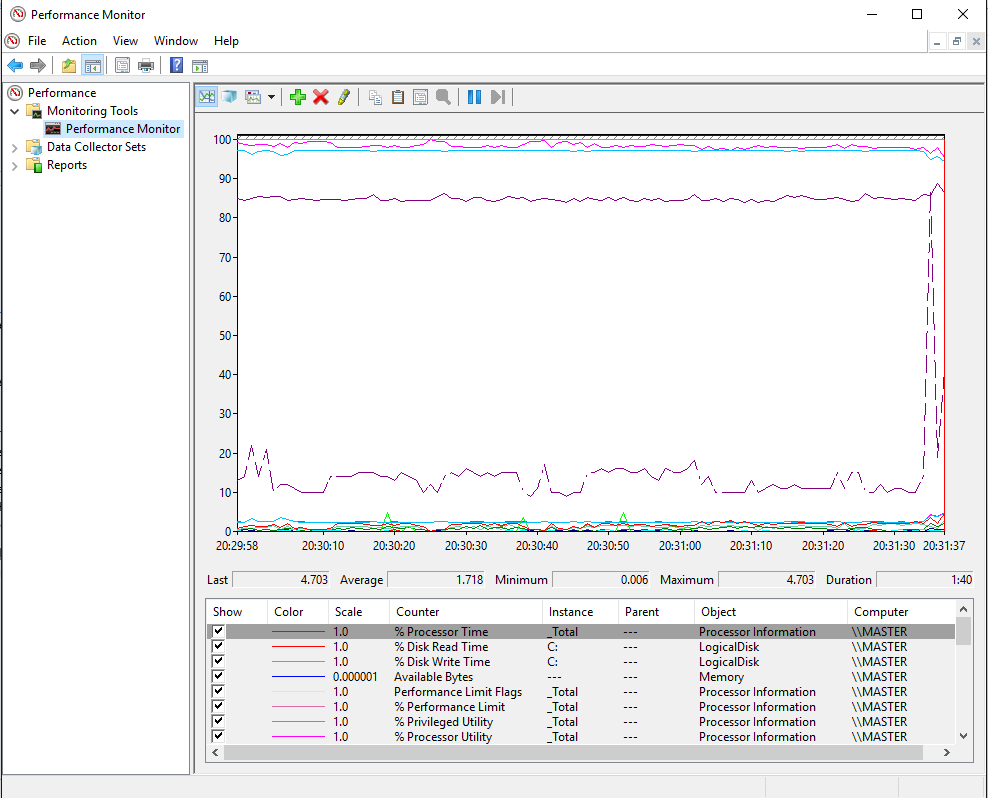


You can also check the feedback of individual events for example, here below I am checking what error (warning) was reported back from a DNS event upon my server.



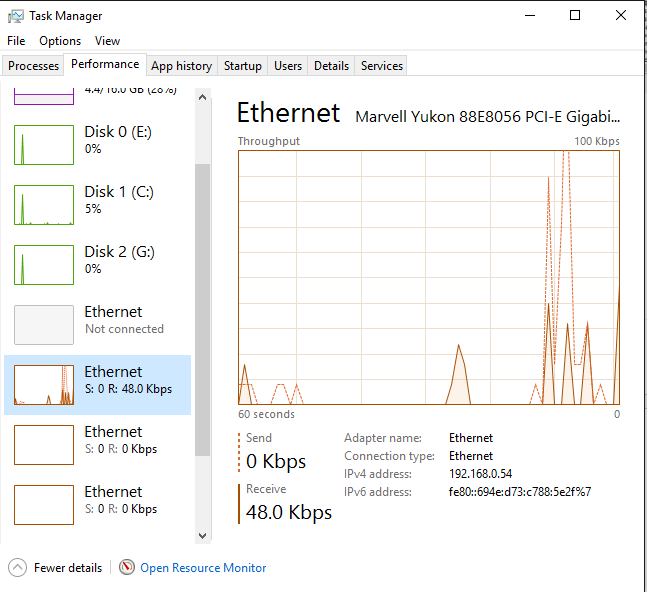
# Performance Monitor (Built In)

Performance monitor is an inbuilt tool that allows you to keep an eye on and track the overall performance and current state as a percentage of the component you are tracking. For example, in the below image you can see that I have several counters set up to track various things on my server that might be important to me to keep an eye on. This is useful because it allows you to see how your hardware is being utilized and you can also use this tool to check for bottlenecks within your system. This tool is also used by just about every third party windows application as they link into the counters and use them within the program itself to setup logic based on factors they want to monitor within the third party application.



# Network Monitor (Built In)

The network monitor on a windows server operating system is a tool that is now built into the task manager software of the operating system. The Network monitoring tool allows you to monitor the network or networks incoming and outgoing traffic. In most cases these tools are limited to monitoring the incoming and outgoing traffic of the devices on that single server and no more. However a lot of third party network monitoring tools are able to monitor and link in with several different servers/client machines to monitor the network on a larger scale. Here below is an image of the network monitor that is built into windows as standard. As you can seem it is clearly displaying all the relevant incoming and outgoing information for the network.



# Redundancy – Fault Management (Built In)

Redundancy and fault management on a server is a combination of all the tools and features I have already mentioned all put together to help ensure that you can keep your server up and running without problem. The main 3 goals of fault management are as follows:

1. Reduced frequency and severity of network and server faults.
2. Early Detection of network issues for the ability to fix quickly without much downtime.
3. Timely prevention through proactive network management.

These goals go towards ensuring that the elements that make up fault detection (listed below) can be achieved effectively.

* Fault Detection.
* Recognising the cause of the fault.
* Correcting the fault.
* Logging the fault and its solution to help create knowledge for when or if the fault occurs again and for trend analysis.

# Backups

Part of the redundancy features of a network for the server itself is to have a backup of the whole sever system when needed. This helps ensure that you always have a fall-back for the server system in the event that the system becomes corrupt.

# Backup Hardware

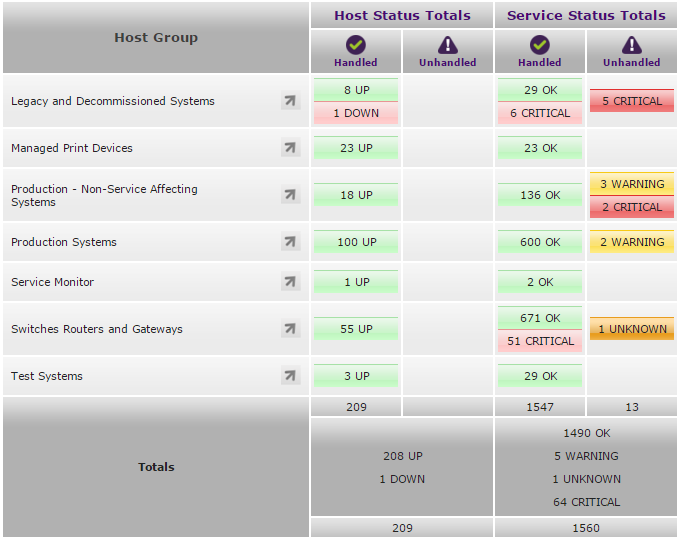
Backup hardware is much like having a backup of the server system however instead you have backups of physical equipment such as routers/switches and other things that are integral parts of your network infrastructure. This helps ensure that your network is kept up and running in the event that a piece of hardware fails and that down time is kept to a minimum.

# Network Fall-Back

Network fall-backs are simply separate networks that aren’t anywhere near as powerful or as big as the main network however offer enough connectivity so you can ensure that network communications continues to work to a good enough extent while the main network is down. For example you may have a system in place that would start up in the event that the main network is reported as completely down. This sub network would act as a life line for the company while the main network is fixed.

# 3rd Party Tools

A third party tool is a piece of software that allows you to connect multiple server to it to monitor them all at the same time. A good example of this working would be something like what the college network uses for monitoring all the hard drives of the college and the systems overall within the college. It allows you to set a bunch of variables and logic settings that report warnings upon the logic being triggered. Here below you can see a third party application called OPSView that the college uses to monitor the many servers and systems they have running on the Sheffield city college network and even for other colleges. You can see it reports various information and gives warnings as-well as critical (Higher level) warnings for various systems that it is setup to monitor.



These tools are much like the inbuilt tools in windows however they allow you to get a lot more specific with the type of things you monitor and how you monitor them. They often allow for much better ways of monitoring too such as online monitoring (more information on that below).

Management Functions

# Fault Management

Fault management is the act of managing any faults that occur on your network. This usually equates to several different types of management variables that you have to take into consideration and think about before you do any work on faults that occur on your network. The following variables should be considered:

* Importance of fault (level of severity)
* Type of fault
* Where fault is located
* Possible solutions (whether it is easy to fix or not)
* Impact to company EG: Costs, Time, Downtime

The function of fault management is to be able to properly assess a situation using the above variables to define in which order you choose to fix a fault and how you go about fixing it. This is a necessary part of the role as a network manager of sports4u to maintain network operations because you need to be able to define how and when faults are dealt with to ensure as little downtime and as little costs are incurred as possible. As a network manager your main job is to ensure that the company and its assets are running in a clean and efficient manor, this means that your job is to make sure that sports4u’s network continues to work in a correct manor and faults are kept to a minimum. However in the event of fault occurring you also need to ensure that network faults are dealt with in such a way that ensures the company can continue to function without any downtime or loss of income as a result of the issue/fault.

# Account management

Account management on a network is the act of ensuring that every user account on the network as a whole has the correct access levels pertaining to the job rolls of the user that is using the account. Account management on a network is important as you need to be able to ensure that each and every user on the network that you are managing has the correct access level in order to do their jobs as-well as to be able to access only things that are relevant to their rolls within the sports4u company.

# Performance Variables (Network throughput and user response time)

Performance variables on a network relates to how the server and network as a whole is working and how easy it is able to deal with the amount of throughput and users upon it. This is impoirant because you need to ensure that the network you have built for the company is able to deal with the everyday workings of the users (staff) that are on the network. For example you would need to ensure that each and every user that needs to have access to the company database which would be stored on a server and accessed via the network has the ability to do so all at the same time if needed. This may be something that doesn’t occur all the time however in times where the company is very busy and taking more orders than normal (example Christmas) there would be a massive influx of network traffic from the staff. Performance variables help ensure that your network can handle these events without a problem.

# Planning

There are several things to take into consideration when you are planning to create network infrastructure for your company. These are the following:

* How long it’s going to take
* Costs
* Implementation
* Type of network
* Impact to the company

These factors all need to be taken into consideration when you are considering creating a network within a company and when you are planning to do and maintenance or updates/upgrades to the network as to ensure you keep the impact to the business as low as possible.

# Designing

Designing the network before you implement it is an important thing to ensure you do as it allows you to get an overall layout and ensure your overall plan you have created is going to work before you start spending money on the network implementation.

This is a very important step to undertake as in most cases, installing a network within your company is going to effect many mission critical parts of your business such as Purchasing, Sales and payrolls. Designing the network before implementation ensures you keep the impact the those mission critical areas as low as possible.

# Security

having a secure network is a must in this day and age because of the amount of malicious attacks that can be done over the internet onto networks. Having an insecure network can lead to data being stolen, things being edited or changed, resources being tampered with and in extreme circumstances can equate to your network going down all together which would (in most cases) grind you company to a halt. Ensuring the network is secure can be as simple as making sure passwords are set to a good standard such as ensuring no 'one is using 123456789 as their password. You could also ensure your network is secure by encrypting the data that is transferred on the network and ensuring you have adequate security firewalls and anti virus/malware software installed.

# Performance Monitoring

Performance monitoring is the act of using software to monitor the current state of the hardware upon your network to ensure it is running correctly and no problems can be seen arising. As a network manager you will have to ensure that the network can continue to perform correctly when it's being used a lot by all the staff within the company.

Justification of Routine Performance Management Activities

# Fault Management

Fault management is the act of managing any faults that occur on your network. This usually equates to several different types of management variables that you have to take into consideration and think about before you do any work on faults that occur on your network. The following variables should be considered:

* Importance of fault (level of severity)
* Type of fault
* Where fault is located
* Possible solutions (whether it is easy to fix or not)
* Impact to company EG: Costs, Time, Downtime

This is a needed thing to do as a network manager because it helps prevent any faults occurring on a regular basis that could impact the company in a bad way and ensures that the network continues to function for the company in an adequate manor. Without this you are simply allowing for many points of failure within the company that could have very well been overcome if you did this task as a network manager.

# Account Management

Account management on a network is the act of ensuring that every user account on the network as a whole has the correct access levels pertaining to the job rolls of the user that is using the account. Account management on a network is important as you need to be able to ensure that each and every user on the network that you are managing has the correct access level in order to do their jobs as-well as to be able to access only things that are relevant to their rolls within the sports4u company.

# Performance Variables

Performance variables on a network relates to how the server and network as a whole is working and how easy it is able to deal with the amount of throughput and users upon it. This is impoirant because you need to ensure that the network you have built for the company is able to deal with the everyday workings of the users (staff) that are on the network. For example you would need to ensure that each and every user that needs to have access to the company database which would be stored on a server and accessed via the network has the ability to do so all at the same time if needed. This may be something that doesn’t occur all the time however in times where the company is very busy and taking more orders than normal (example Christmas) there would be a massive influx of network traffic from the staff. Performance variables help ensure that your network can handle these events without a problem.

# Planning

There are several things to take into consideration when you are planning to create network infrastructure for your company. These are the following:

* How long it’s going to take
* Costs
* Implementation
* Type of network
* Impact to the company

These factors all need to be taken into consideration when you are considering creating a network within a company and when you are planning to do and maintenance or updates/upgrades to the network as to ensure you keep the impact to the business as low as possible.

# Designing

Designing the network before you implement it is an important thing to ensure you do as it allows you to get an overall layout and ensure your overall plan you have created is going to work before you start spending money on the network implementation.

This is a very important step to undertake as in most cases, installing a network within your company is going to effect many mission critical parts of your business such as Purchasing, Sales and payrolls. Designing the network before implementation ensures you keep the impact the those mission critical areas as low as possible.

# Security

having a secure network is a must in this day and age because of the amount of malicious attacks that can be done over the internet onto networks. Having an insecure network can lead to data being stolen, things being edited or changed, resources being tampered with and in extreme circumstances can equate to your network going down all together which would (in most cases) grind you company to a halt. Ensuring the network is secure can be as simple as making sure passwords are set to a good standard such as ensuring no 'one is using "123456789" as their password. You could also ensure your network is secure by encrypting the data that is transferred on the network and ensuring you have adequate security firewalls and anti virus/malware software installed.

Without having adequate and constantly updated security procedures in place you are opening your network up to the following attacks. (This is just a few and not all the threats)

* Data Theft
* Hacking
* DOS & DDOS Attacks
* Viruses
* Malware
* Data Corruptions

# Performance Monitoring

Performance monitoring is the act of using software to monitor the current state of the hardware upon your network to ensure it is running correctly and no problems can be seen arising. As a network manager you will have to ensure that the network can continue to perform correctly when it's being used a lot by all the staff within the company.

One of the biggest things that effect most networks that are setup is a lack of foresight when it comes to network utilization. In a lot of cases performance monitoring can help prevent this becoming an issue because you are able to analyse and detect trends related to network utilization and update or upgrade the network to assist in the event that the network becomes very heavily utilized (such as in a very busy period of time like Christmas where sales are high and the network will be needed to be accessed a lot more to handle the sales of items more often).