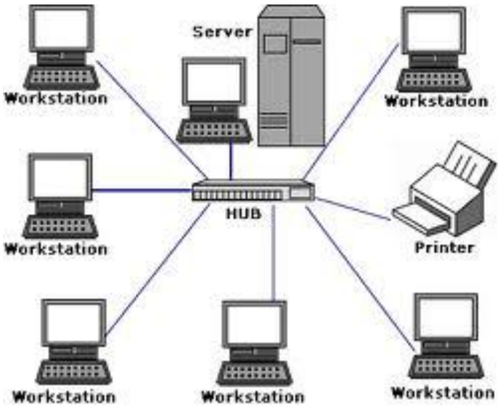
Candidates should be able to:

OCR 2.1.6 (a) explain the advantages of networking stand-alone computers into a local area network

AQA 3.1.13 understand what a computer network is and be able to discuss the advantages and disadvantages of using a computer network

A network is defined as a collection of computers and peripheral devices (such as printers) connected together.

A local area network (LAN) is a network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.



The connections can be cable, fibre-optic, or wireless (infra-red, microwave or radio).

Advantages of networks

- Sharing resources:
  - Sharing folders and files so you can access them anywhere on the network from any computer
  - Sharing peripheral devices such as printers and scanners
  - Sharing an internet connection

- Communication:
  - Using email to communicate with colleagues
  - Using messaging systems to chat while you are working on other things
  - Transferring files between computers

- Centralised management:
  - User profiles and security can all be managed centrally
  - Software can be distributed across the network rather than having to install it on
  - each individual computer
  - Users can use any PC on the network but still see their own files
  - Data can easily be backed up centrally.

Some Networking Fantasy

Read Terry Pratchett's book 'Going Postal' for a fun fantasy about inventing and making money from networking technology on DiscWorld. Loads of computer scientists who've read any Terry Pratchett's books like them instantly even if they don't read much else.

OCR 2.1.6 (b) describe the hardware needed to connect stand-alone computers into a local area network, including hub/switches, wireless access points

- A **network interface card** (NIC) is needed in each computer and peripheral connected in a LAN. This interface allows the devices to communicate over the network either by using cables or wirelessly.

- **Cabling** is needed in a non-wireless network to connect the computers and peripherals together, either directly or through a hub/switch. The amount of cabling needed depends on the network topology (the way computers and peripherals are physically connected together).

- A **hub** is used to link computers and peripherals together in a cabled network that uses a star network topology. A hub is a sort of junction box but does not manage any of the traffic that comes through it, any data packet entering any port is broadcast out to all the other ports resulting in data packet collisions which slow the network considerably as the amount of data traffic rises.

- A **switch** is used in the same way as a hub but the data entering the device is switched to the port it is meant to go to, rather than being broadcast to all the ports. This greatly reduces data packet collisions resulting in a faster network than the equivalent one using a hub.

- A **wireless access point** is a device that allows computers and printers etc. to connect to a wired network using radio waves rather than cabling, provided they are equipped with a wireless NIC. This allows a network to be built with few or no cables and makes it simple to add further wireless devices.

Student Activity

If possible it is best to get the students to make construct a simple wired network. You need 2 computers (some decommissioned ones are ideal) a switch or hub, network cards and patch cables. If the students ask questions such as “What is CAT 5?” or “What is the difference between ISA and PCI?” you can write all these down and set them a task to research. You do not have to connect this to your school network so it should not present a security threat to your administration staff.
http://windows.microsoft.com/en-GB/windows-vista/What-you-need-to-set-up-a-home-network

How to make a patch cable
http://www.youtube.com/watch?v=482VtesZwZ8

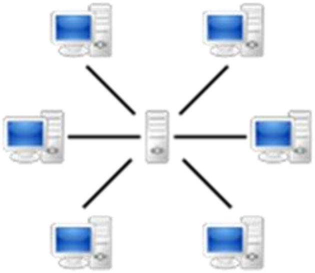
OCR 2.1.6 (c) explain the different roles of computers in a client-server and a peer-to-peer network
AQA 3.1.13 understand the client-server model

Client-server networks
On a client-server network there are two types of computers with two distinct roles. One or more server computers have the role of controlling access to shared resources like files and printers. Multiple client computers are then connected to the server computers and these are where the user actually works.

The user logs onto a client computer which then connects to the server, verifies the user and then allows them access to the files stored on the server that they have permission to access.

All the data is stored on the servers, which generally have far greater security controls than the client computers. Since data storage is centralised, security is easier to manage, updates to the data are far easier to administer and it is far easier to backup the data centrally in comparison to a peer-to-peer network.

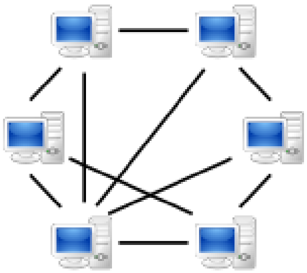
Other servers may have a more specialised role such as a print server, dedicated to controlling access to shared printers and queuing print jobs.



Peer-to-peer networks
In a peer-to-peer network computers are simply linked together, either using cables and a hub or wirelessly.

Such networks do not have computers with particular roles; instead, each computer has equivalent responsibilities and status. This means that any computer on the network can load information from the hard disk of any other computer and a computer on the network can use any printer connected to any other computer.

Peer-to-peer networks are cheaper to set up and easier to manage than server based networks but they are less secure than a client-server network.



OCR 2.1.6 (d) describe, using diagrams or otherwise, the ring, bus and star network topologies

AQA 3.1.13 be able to describe and explain the bus, ring and star networking topologies and be able to discuss the advantages and disadvantages of each of these topologies

Computers can be connected together in different layouts, or topologies. There are three main topologies but these may be combined in a large network.

Ring network

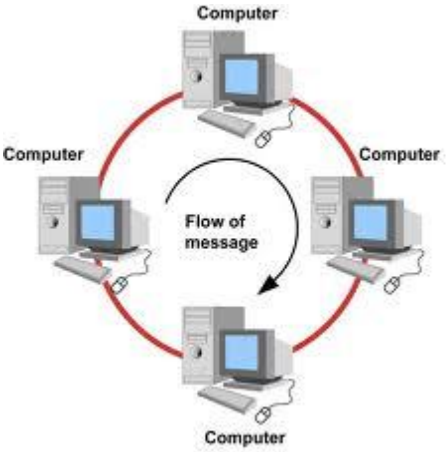
This is typically a peer-to-peer network. The nodes are connected in a ring and data travels in one direction using a control signal called a 'token'.

Advantages:

- Consistent performance when adding further nodes or heavy network traffic as only the node with the 'token' can transmit data so there are no data collisions.
- Relatively cheap to install and expand.
- Token passing protocol is simple and reliable.
- Not dependent on a central computer

Disadvantages:

- Slower than a star topology under normal load.
- If the cable fails anywhere in the ring then the whole network will fail because if any node fails then the token cannot be passed around the ring. The hardest topology to troubleshoot because of the difficulty of tracking down where in the ring the failure has occurred.
- Inconvenient to modify or expand because to add or remove a node you must shut down the network temporarily. In order for the nodes to communicate with each other they must all be switched on.



Are ring networks still in use?

http://www.techrepublic.com/blog/classic-tech/does-anyone-actually-still-use-token-ring/115

Bus network

Nodes are connected to a main (bus) cable.
Computers are connected to a single backbone (bus) cable. The computers all share this cable to transmit to each other but only one computer can transmit at any one time. This is fine most of the

time if the network is not too busy but if there is a lot of traffic then transmissions interfere with each other.

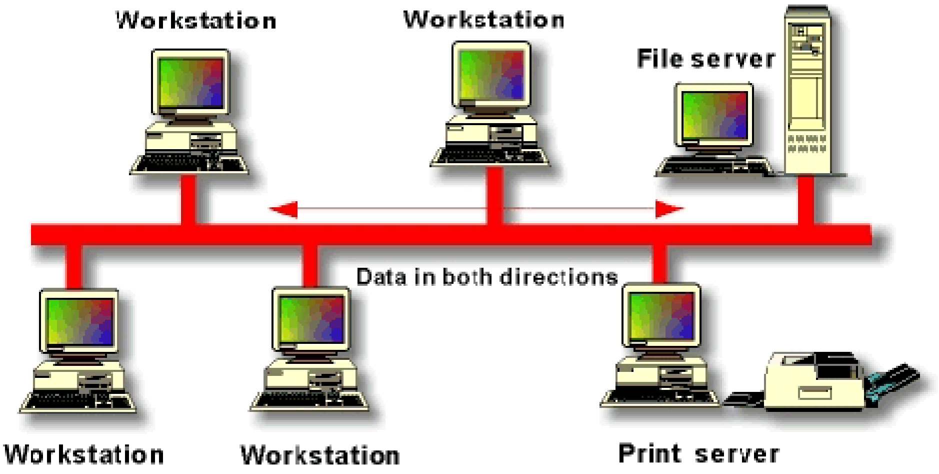
In an Ethernet network if data is being sent between nodes then the other nodes cannot transmit. If too many nodes are connected then the transfer of data slows dramatically as the nodes have to wait longer for the bus to be clear.

Advantages:

- The simplest and cheapest to install and extend.
- Well suited for temporary networks with not many nodes.
- Very flexible as computers can be added or taken away without disturbing the rest of the network.
- Failure of one node does not affect the rest of the bus network.
- Simpler than a ring topology to troubleshoot if there is a cable failure because sections can be isolated and tested independently.

Disadvantages:

- If the bus cable fails then the whole network will fail.
- Performance of the network slows down rapidly with more computers or heavy network traffic.
- Slower than a ring network as data cannot be transmitted while the bus is in use by other computers.



Star network

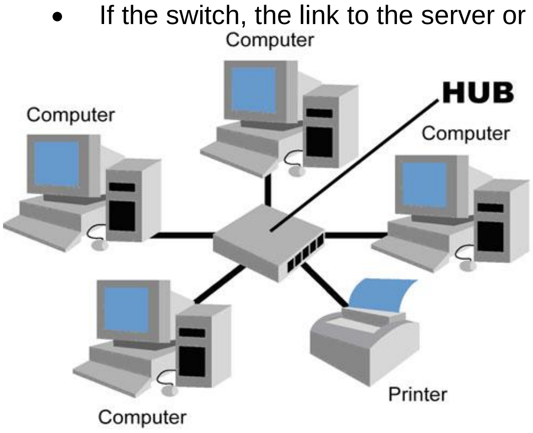
A central computer (server) and the subsidiary computer are connected to each other through a switch or hub.

Advantages:

- The most reliable because the failure of a computer or a cable does not affect other computers.
- Simple to troubleshoot because only one computer is affected by a broken cable.
- Adding further computers does not greatly affect performance because the data does not pass through unnecessary nodes.
- Easily upgraded by replacing a hub with a switch.
- Easy to expand with extra computers.

Disadvantages:

- Uses the most cable which makes it more expensive to install than the other two topologies. The extra hardware required such as hubs or switches further increases the cost.
- As the central computer controls the whole system, the whole system will be affected if it breaks down or if the cable link between it and the switch fails.
- If the switch, the link to the server or the server itself fails then the whole network fails

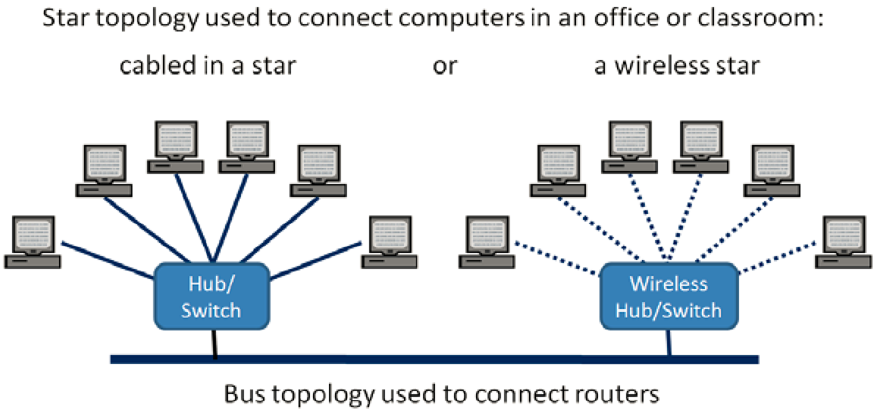


Network topologies presentation

Get students to produce an animated presentation showing how data packets are transmitted around a ring, bus network and a star network with a hub or a switch.

Find out which layout is used in your school

Get students to talk to the network technicians to find out what network layouts are used in your school. This is usually some sort of combined setup:


Star topology used to connect computers in an office or classroom:
cabled in a star
or
a wireless star
Hub/
Switch
Wireless
Hub/Switch
Bus topology used to connect routers

Computer science for fun

www.cs4fn.org/fundamentals/networks.php

Solve a networking problem: fix the pipes. One of the major issues in networking is finding the best way for data to travel round the network. With old-style telephone calls, when you made a call to a friend there was a physical link made so that everything you said travelled along the same path from start to finish. With digital networks, your data (whether your voice, emails, a movie or the contents of a web page) doesn't have to all go the same way. It is broken into parts known as data packets. Each part can go whichever way is best for the network or the person. One issue is finding ways to send data between two points so that as many data packets can travel at once as possible. What is needed is an algorithm that computers controlling the network can follow that guarantees to solve this problem. Pinky's Pipes Pickle is a game to maximise the flow in a pipe network.

Comparison Grid

Topology	Performance with few computers	Performance with many computers	Ease of troubleshooting	Cost of installation	Ease of setting up and modifying	Problems caused by cable or computer failure
LINE (BUS)	Medium	Most affected	Fairly easy	Low	Easy to set up and modify	Failure of the bus cable causes total failure. Failure of a computer has no affect.
RING	Slow	Least affected	Hard	High	Easy to set up but harder to modify	Cable or computer failure causes total network failure.
STAR	Fast	Some affect but the switch/hub can be upgraded easily	Easy	High	Easy to set up and modify	Cable or computer failure only affects that node. Failure of the hub/switch or the server causes total network failure.

OCR 2.1.6 (e) describe the differences between a local area network and a wide area network such as the Internet

A Wide Area Network, or WAN, is a collection of computers and networks over a geographically wide area. The Internet is the largest WAN. . Smaller examples of a WAN would include a national ATM network used by a bank to allow customers to access cash. Many supermarkets and other large companies operate their own national WANs.

WANs use hired infrastructure to connect the LANs together. A business with offices in London and Manchester will lease connections from a network service provider to connect the office LANs together.

OCR 2.1.6 (f) explain the terms IP addressing, MAC addressing, packet and protocols
AQA 3.1.13 be able to explain, in simple terms, the handshake process used in most modern networking protocols

IP Addressing

An Internet Protocol (IP) address is a unique 32-bit reference number that is allocated to devices on a computer network that uses the Internet Protocol.

Although IP addresses are stored as 32-bit numbers, for our convenience they are usually displayed as a series of 4 decimal numbers, each one representing 8 bits of the original binary address.

32-bit binary version: 110010011010000001011011011111111

decimal version: 201.64.182.255

Some IP addresses are reserved for private network ranges e.g.

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

MAC Addressing

In computer networking, a Media Access Control address (MAC address) is a unique 48-bit number assigned to a network interface card (NIC) to identify it on a LAN. Because they are so long, MAC addresses are usually displayed in hexadecimal.

48-bit binary version: 000000000000100101111100111100011111011110000101

hexadecimal version: 00-09-7C-F1-F7-85

MAC addresses are limited to being used on a LAN while IP addresses can be used on multiple types of networks including the Internet.

On a LAN, data packets that use a protocol such as TCP/IP will be packaged inside data packets that use the MAC address to deliver them correctly.

Another use for the MAC address is as a security feature on cabled and wireless systems, only allowing computers with authorised MAC addresses to have access to the network. This works by inspecting the data packet that is sent from a computer to see if its MAC address matches one of the approved ones in a pre-defined table.

Packets

Modern computer networks, including the Internet, carry data by breaking it down into a series of distinct units called packets, rather than sending it as a continuous stream of data. A typical packet might contain 1,000 to 1,500 bytes and has two parts:

Control information - this provides the data that the network needs to deliver the payload, for example the source and destination addresses. It will also have error checking data and the number of the packet so they can be reassembled in the correct order. The control information is found in the packet headers and footers

Data - this is the user data that is to be delivered and is located between the packet headers and footers.

In complex networks such as the Internet, a series of packets sent from one computer to another may follow different routes to reach the same destination. This technology is called packet switching and makes the network more efficient because the network can balance the load across various pieces of equipment and if there is a problem with one piece of equipment in the network then packets can be routed around it.

Protocols

A protocol is the set of rules that define how devices communicate. As long as the computers on a network are using the same protocol then they will be able to exchange data correctly. A protocol will cover:

- how the communication will start
- the transmission speed
- the significance of the bits being transmitted
- how the bits will be delivered (one at a time or in groups of 16 for example)
- error checking procedures used

The Internet Protocol is known as TCP/IP, named from two of the most important protocols in it:

- the Transmission Control Protocol (TCP)
- the Internet Protocol (IP).

The TCP provides the service of exchanging data directly between two networked computers while the IP is used to route data packets between networks and over the Internet.

Accessing Websites on the Internet

Websites are stored on web servers connected to the internet. The site will have an IP address so people can access the pages using their browser software.

However, when you want to access a site you don’t type the IP address, you type in a domain name such as www.bbc.co.uk. This is because humans are quite bad at remembering numbers and typing them in correctly so the domain name is a text reference to a site that can be translated into the numerical IP address.

When you type the domain name, “www.microsoft.com” into the browser the web page request is sent to a Domain Name System (DNS) server in the internet. The DNS server has a database of domain names and IP addresses so it can translate the domain name into an IP address.

Student Research

What Is the IP Address of your school website?

What Is the IP Address of Facebook?

Handshaking

When a computer communicates with another device like a modem, printer, or network server, it needs to handshake with it to establish a connection.

A simple handshaking protocol might only involve the receiver sending a message meaning "I received your last message and I am ready for you to send me another one."

A more complex handshaking protocol might allow the sender to ask the receiver if he is ready to receive or for the receiver to reply e.g. "I did not receive your last message correctly, please resend it" (if the data was corrupted en route).

Establishing a normal TCP connection requires three separate steps:

1. The first computer (Alice) sends the second computer (Bob) a "synchronize" (SYN) message, which Bob receives.
2. Bob replies with a synchronize-acknowledgment (SYN-ACK) message, which Alice receives.
3. Alice replies with an acknowledgment message, which Bob receives, and doesn't need to reply to.

OCR 2.1.6 (g) explain the need for security measures in networks, such as user access levels, suitable passwords and encryption techniques

Usernames/Passwords

The file server must ensure that people can only access files that they are permitted to. Most file servers do this by making each user log on with a user name and password before they can access any files. The user name that a user logs on with will determine which files the user can access and change.

Passwords are the most common way of securing a network. A user will have a public username and a private password. Anyone can know, or guess, a username, but only the user will know the password. The password should be something that that the user will remember, but very difficult for anyone else to guess (or crack).

A username is sometimes likened to the address of a house and the password as the front-door key – anyone can find the address, but very few will have the front-door key.

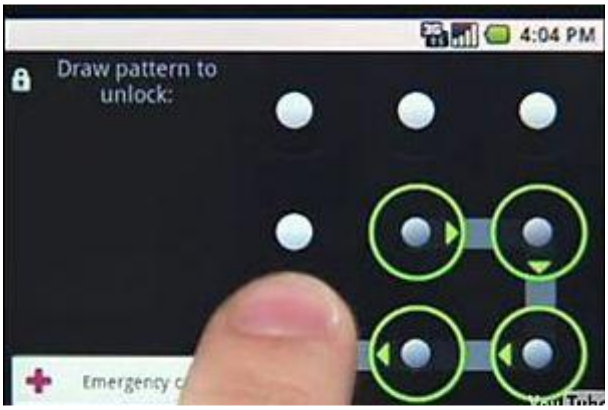
A password and username are a set of characters that need to be typed in. The stronger the password, the harder it is for someone else to find the password. Passwords should be a mixture of upper case, lower case, digits and punctuation marks (e.g. Hello79_?!).

The numerous ways in which permanent or semi-permanent passwords can be compromised has prompted the development of other techniques.

Some alternatives to passwords:

- Single-use passwords. Most users find single use passwords extremely inconvenient. They have, however, been widely implemented in personal online banking, where they are known as Transaction Authentication Numbers (TANs).
- Access controls based on public key cryptography. The necessary keys are usually too large to memorize and must be stored on a local computer, security token or portable memory device, such as a USB flash drive or even floppy disk.
- Biometric methods promise authentication based on unalterable personal characteristics, but currently have high error rates and require additional hardware to scan, for example, fingerprints, irises, etc.
- Non-text-based passwords, such as graphical passwords or mouse-movement based passwords. Graphical passwords are an alternative means of authentication for log-in intended to be used in place of conventional password; they use images, graphics or colours instead of letters, digits or special characters. One system

requires users to select a series of faces as a password, utilizing the human brain's ability to recall faces easily.



- Cognitive passwords use question and answer cue/response pairs to verify identity.

Research

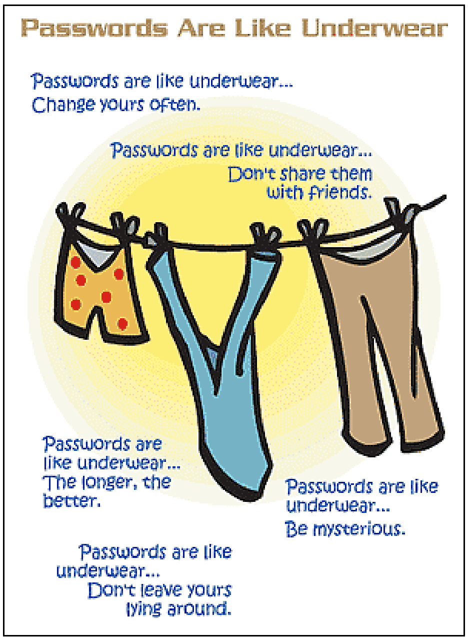
There are lots of opportunities for research.

Spoof fingerprints:
http://www2.washjeff.edu/users/ahollandminkley/Biometric/index.html

Poster

Create a poster on creating strong passwords.

http://www.microsoft.com/en-gb/security/online-privacy/passwords-create.aspx


Passwords Are Like Underwear
Passwords are like underwear... Change yours often.
Passwords are like underwear... Don't share them with friends.
Passwords are like underwear... The longer, the better.
Passwords are like underwear... Be mysterious.
Passwords are like underwear... Don't leave yours lying around.

Access levels

Network managers can set up groups of users with different levels of access to the network.

At the highest level, the network manager can install and remove software, access all user areas and change permissions. At lower levels, a group of users may only be able to access particular pieces of software and their files stored in their own areas.

Different levels of access help to ensure that the network remains secure and that only licenced software is used on it.

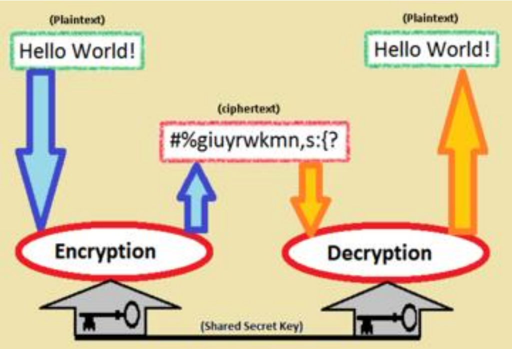
Your level of access is linked to your User ID

What levels of access are there in your school?

Network Managers, The Headmaster, Teachers, Students

Encryption

This is the process of converting data to be sent over a network into something that is unreadable by a human. Data is first encrypted by software then sent over the network. The receiver will know how to decrypt the message into something that is recognisable.

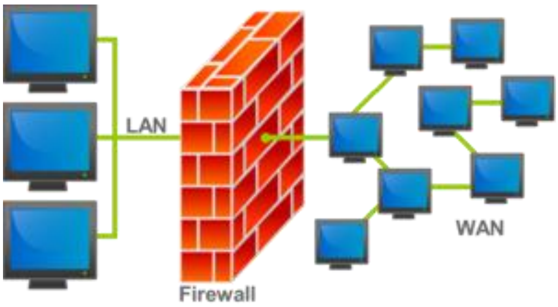


Encryption uses very advanced mathematical techniques, commonly relying on properties of prime numbers. The best encryption (harder to crack) uses a lot of bits to store the key (a number that is used to decipher the encrypted data). Typically 128 or 256 bits are used.

When you buy something on the internet or use internet banking you may have noticed that instead of HTTP in front of the domain name it changes to HTTPS.It works in the same way as HTTP but is encrypted so your payment details are kept secure.

Firewalls

A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.



Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

OCR 2.1.6 (h) describe and justify network policies such as acceptable use, disaster recovery, failover, back up, archiving.

Acceptable Use Policy (AUP)

An acceptable use policy (AUP; also sometimes acceptable usage policy or Fair Use Policy) is a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used. AUP documents are written for corporations, businesses, universities, schools, internet service providers, and website owners often to reduce the potential for legal action that may be taken by a user, and often with little prospect of enforcement.

Acceptable Use Policies are an integral part of the framework of information security policies; it is often common practice to ask new members of an organization to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of an organization. It should also define what sanctions will be applied if a user breaks the AUP.

What is the AUP in your school?

When do you have to comply with the rules?

Do you think all the rules are reasonable ?

Should some rules be added?

Is it clear and concise?

What sanctions are applied if you break the rules?

Disaster Recovery

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

It is estimated that most large companies spend between 2% and 4% of their IT budget on disaster recovery planning, with the aim of avoiding larger losses in the event that the business cannot continue to function due to loss of IT infrastructure and data. Of companies that had a major loss of business data, 43% never reopen, 51% close within two years, and only 6% will survive long-term.

Disasters can be classified in two broad categories. The first is natural disasters such as floods, hurricanes, tornadoes or earthquakes. While preventing a natural disaster is very difficult, measures such as good planning which includes mitigation measures can help reduce or avoid losses. The second category is man made disasters. These include hazardous material spills, infrastructure failure, or bio-terrorism. In these instances surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events.

Failover

In computing, failover is the capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active application, server, system, or network. Failover happens without human intervention and generally without warning, unlike switchover.

Systems designers usually provide failover capability in servers, systems or networks requiring continuous availability and a high degree of reliability.

At server-level, failover automation takes place using a "heartbeat" cable that connects two servers. As long as a regular "pulse" or "heartbeat" continues between the main server and the second server, the second server will not initiate its systems. There may also be a third "spare parts" server that has running spare components for "hot" switching to prevent down time.

The second server will immediately take over the work of the first as soon as it detects an alteration in the "heartbeat" of the first machine. Some systems have the ability to page or send a message to a pre-assigned technician or center.

Some systems, intentionally, do not failover entirely automatically, but require human intervention. This "automated with manual approval" configuration runs automatically once a human has approved the failover.

Failback, conversely, involves the process of restoring a system/ component/ service in a state of failover back to its original state (before failure).

Back up

In Computing, a backup refers to making copies of data so that the copy may be used to restore the original after a data loss event.

The primary purpose is to recover data as a reaction to data loss. Data loss is a very common experience of computer users. 67% of internet users have suffered serious data loss. Though backups represent a simple form of disaster recovery, and should be part of a disaster recovery plan, by themselves, backups should not be considered disaster recovery. Not all backup systems and/or backup applications are able to reconstitute a computer system.

Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. Organizing this storage space and managing the backup process is a complicated undertaking. In the modern era of computing there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.

Archiving

Archiving means to move files to a long-term storage medium.

Backup and archiving are two different processes.

The storage media used within an archive should be stable and long lasting. To comply with corporate and government regulations on data, companies will archive data not in used but may be needed.

Archiving can result in two major benefits:

- It lets you reclaim disk space on the primary storage. Saving disk space, along with other factors, can lower storage costs. This also means a significant reduction in costs of backup media.
- It can improve performance. By separating inactive data from active data, database scans and other data access operations become faster.