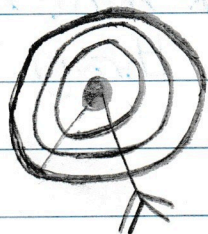


Chapter Four $\Rightarrow$ Networks and the effects of using them

Objectives:-



* Networks:-

Routers, common network devices, Wi-Fi & Bluetooth, cloud computing, intranets, extranets & the internet, LANs, WANs & WLANs

* Network issues & communication:-

security, anti-malware & electronic conferencing.



Common Network Devices & Terms:-

1. **Network Interface Card (NIC)** $\Rightarrow$ needed to allow a device to connect to a network. It turns binary data into electrical signals. Each NIC is given a unique **MAC** address.

There are Wireless NIC to connect to the internet or other networks.

• **Media Access Control Address (MAC)** $\Rightarrow$

OR Physical Address

NN - NN - NN - DD - DD - DD
manufacturer's code device serial number

A number which uniquely identifies a device when it is connected to a network. It is made up of 48 bits shown as six groups of hexadecimal digits.

• Internet Protocol Address (IP) $\Rightarrow$ 254.25.28.77

It is given to a device when it is connected to the internet. Identifies the location of a device on a network. Assigned by the internet service provider. Define the rules that must be agreed by senders & receivers of data communicating through the internet.

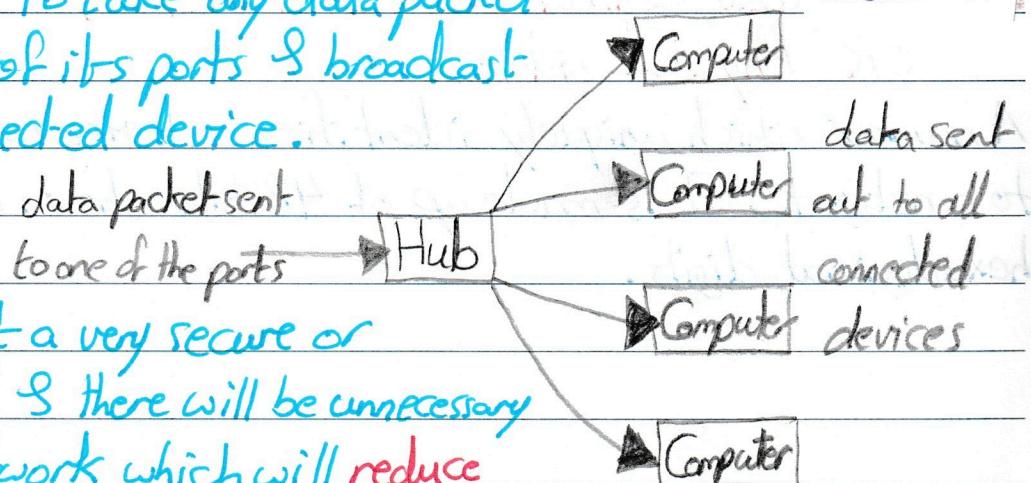
• **Data packets** $\rightarrow$ Data is moved around networks in the form of data packets.

Packets usually contain the following information:-

1. The sender's IP address
2. The receiver's IP address
3. The sequence / identify number of the packet
4. The packet size
5. How many data packets make up the whole message

2. **Hubs** $\Rightarrow$ devices that can have a number of devices or computers connected to them. They are often used to connect devices to form a LAN.

The main task is to take any data packet received at one of its ports & broadcast it to **every** connected device.



Using a hub is not a very secure or efficient method & there will be unnecessary traffic on the network which will **reduce** the bandwidth.

3. **Switches** $\Rightarrow$ Intelligent versions of hubs and more secure than hubs because the data packets will be sent **only** to the specific device.

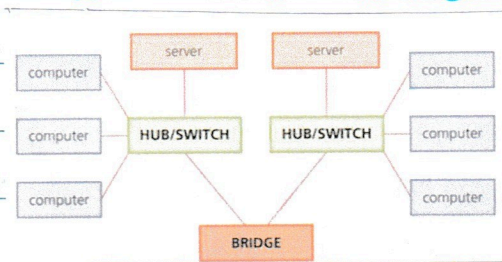


How does it work?

- The switch stores the MAC addresses of all devices on the network.
- Each port on the switch connected to a device will have a matching MAC address (called a lookup table)
- A switch matches the MAC address of an incoming data packet arriving at one of its ports & directs it to the correct device.

Both hubs & switches are used to connect devices in a LAN, both use data packets and both exchange data within their own LAN networks.

4. **Bridge** $\Rightarrow$ Device that connect one LAN to another LAN that uses the same protocol so that they can function as a single LAN. Bridges **cannot** communicate with other external networks such as the internet.

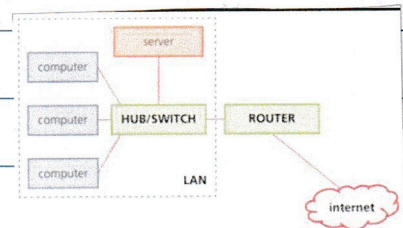


5. Router $\Rightarrow$ used to route data packets from one network to another network based on IP addresses.

Routers are used to join a LAN to the internet.

Router inspects the IP address & determines whether the data packet is meant for its own network or for another.

Routers know where to send data packets by consulting a routing table which contains information about the computer addresses & about other routers.



Router	Bridge
• It connects various types of network together • Scan a device's IP address • Data is sent out using data packets • Connected networks will use different protocols • A routing table is used to direct data packets to the correct device • Routers have more than two ports	• It connects LANs together • Scan a device's MAC address • Data is sent out using data packets • Connects networks together that use the same protocol • Bridges do not make use of routing tables • Bridge has only two ports

• Wi-Fi & Bluetooth :-

Similar points $\Rightarrow$

- Both offer wireless communication between devices
- Both use electromagnetic radiation as the carrier of data transmission

$\rightarrow$ Bluetooth $\Rightarrow$

- sends & receives radio waves in a band of 79 different frequencies
- Automatically detect & connect to each other
- To communicate it picks one of the 79 channels at random to pair with another device
- If the channel is already used, it randomly picks another channel
- Uses key encryption to create a secure wireless personal area network.

Why Bluetooth is useful?

- Transfer data between two or more devices which are very close
- The speed of data transmission is not critical
- Used for low-bandwidth applications (such as sending music files from mobile phone to a headset)

$\rightarrow$ Wi-Fi $\Rightarrow$

- Sends & receives radio waves in a several frequency band.
- Each band is also further split into channels
- Offers much faster data transfer rates
- Better range & better security than Bluetooth
- Device can access internet wirelessly at any access point or hot spot up to 100 meters.

• **Cloud Storage** $\Rightarrow$ Is a method of data storage where data is stored on offsite servers. The same data is stored on more than one server in case of maintenance or repair, allowing clients to access data at any time. This is known **data redundancy**.

There are three common systems:-

[1] **Public cloud** $\rightarrow$ storage environment where the customer and cloud storage provider are different companies.

[2] **Private cloud** $\rightarrow$ storage provided by a dedicated environment behind a company firewall, customer & cloud storage provider are integrated and operate as a single entity.

[3] **Hybrid cloud** $\rightarrow$ combination of the two previous environments, some data resides in the private cloud while less sensitive data can be accessed from a public cloud storage provider.

Advantages (storage) $\Rightarrow$

- Customer files stored in the cloud can be accessed at any time from any device
- There is no need for a customer to carry an external storage or use the same computer to store & retrieve information
- The cloud provides the user with remote backup of data
- If a customer has a failure of their hard disk or backup device, cloud storage will allow a recovery
- The cloud system offers almost unlimited storage capacity.

Disadvantages (storage) ⇒

- Security aspects
- If the customer has a slow or unstable internet connection, they could have problems accessing or downloading their data.
- Costs can be high
- The potential failure of the cloud storage company is always possible

Advantages of using cloud storage rather than other storage devices

- No need to carry memory sticks
- No need to pay for large storage capacity on your device
- Companies will ensure that your files are backup and reduce the possibility of losing them
- The ability to synchronize files ensures they are automatically updated across all devices
- Cloud storage is ideal for collaboration purposes. It allows several users to edit & collaborate on a single file or document.

Data Security / Data Loss using cloud storage ⇒

Data Security → Companies that transfer vast amounts of confidential data from their own systems to a cloud service provider are effectively relinquishing control of their data security

Data Loss →

- There is a risk that important data could be lost from cloud storage facilities
- Actions from hackers could lead to loss or corruption of data
- Users need to be certain sufficient safeguards exist to overcome these potentially very harmful risks

Local Area Networks (LANs) and Wide Area Networks (WANs)

→ Local area networks (10m to 1000m)
networks are usually within one building or not very far away from each other geographically.

Consist of a number of computers & devices that are connected to hubs or switches.

One of the hubs or switches will usually be connected to a router and a modem to allow the LAN to connect to the internet so it then becomes part of WAN

Advantages	Disadvantages
• The sharing of resources	• Easier spread of viruses
• Ease of communication between users	• Printer queues developing
• Network admin to control and monitor all aspects of the network	• Slower access to external networks
	• Increased security risk
	• If the main server breaks down the network will no longer function

Wireless LANs (WLANs)

similar to LANs but there are no wires or cables. They provide wireless network communications over fairly short distance using radio or infrared signals.

Devices known as access points or wireless nodes are connected into the wired network.

End-users access the WLAN through wireless LAN adapters that are built into the devices or are a plug-in module.

Wide Area Networks (WANs) (100 km to over 1000 km) used where computers or networks are situated a long distance from each other geographically. If a number of LANs are joined together using a router or modem, then they can form a WAN. The most common examples of WAN include the **internet** and the networks of **ATMs**

Wireless Networking	Wired Networking
• easier to expand the networks • gives devices increased mobility • there is a safety improvement and increased flexibility • there is an increased chance of interference from external sources • data is less secure than with wired systems • data transmission rate is still slower than for cabled networks • it is possible for signals to be stopped by thick walls	• wireless connectivity is often subject to interference • data transfer rates tend to be faster • setting up cabled networks tend to be cheaper • cabled networks lose the ability for devices to be mobile, they must be close enough • having lots of wires can lead to a number of hazards

Network Issues & Communication:

* Passwords $\Rightarrow$ passwords are used:

- When accessing your email account
- When carrying out online banking
- Accessing social networking sites

* Passwords should be protected by:

- Running anti-spyware software to make sure that your password is not being relayed back to whoever put the spyware on your computer.

- Change passwords on regular basis

- Passwords should not be easy to crack:

- At least one capital letter
- At least one numerical value
- At least one other keyboard character such as @ & *

* Zero Login & Biometrics $\Rightarrow$

.Zero Login:- new technology standard that allows users to login to computer systems without the need to type in a password

Advantages

- Fairly clear
- Enhanced security
- Easier & much quicker way to login to a system

Disadvantages

- Users don't know when they are being monitored
- Users don't know if they have been logged out
- How well protected is it in reality.

* **Biometrics** $\Rightarrow$ used on many smart-phones as a way of logging into the phone by placing your finger on the screen or using face recognition to unlock it.

* **Behavioral patterns** $\Rightarrow$ include how you walk, your typing speed, your normal location and how you swipe your screen.

* **Magnetic Stripe Cards:**

Cards that have a magnetic stripe on the reverse side which contains data such as name, ID number, gender, ---

- The stripe is read by swiping it through a card reader.
- Some ID cards use a holographic image - hologram (images that change color or appear to have a moving object as the image is viewed from different angles) to make it difficult to prevent photocopying the card & using it illegally.
- Other cards have photographic image of the card user to prevent stolen card from being used.

Advantages

- Easy to use
- not an expensive technology
- can be remotely deactivated
- cards may be multi-purpose

Disadvantages

- Less secured
- The cards wear out with a lot of use
- Magnetic readers often fail to read the cards on first attempt

* **Smart Cards** $\Rightarrow$ act like a contactless card which can be read from a distance by using a chip and antenna

* **Physical tokens** $\Rightarrow$ is a form of authentication in the form of a physical, solid object. They contain internal clocks & when a PIN & other authentication details are entered, then a one-time password (OTP) is generated.

Example - Customer logged on to the bank's website:

- Customer inserts their debit card into the top of the token device & the device either recognizes the card or rejects it.
- The device then asks the customer to press 'IDENTIFY' and then enter their PIN.
- A one-time password is then shown on the device screen.
- The customer now goes back to their bank web page & enters the eight-digit code.
- They are now given access to their account.

There are two types of physical tokens:

$\rightarrow$ **disconnected physical token**

separate device is used requiring the user to key in data

$\rightarrow$ **connected physical token**

transmits the generated one time password directly to a computer through a USB connection.

* **Electronic tokens** $\Rightarrow$ are software installed on a user's device such as a smartphone.

When the website requests the user to authenticate who they are, the user opens the app. The app generates a one-time password. The user enters this OTP with some other form of authentication such as PIN, touch ID or face ID.

Electronic Conferencing

Very Important

* Video Conferencing $\Rightarrow$ communication method that uses both video & sound. It is a face-to-face conference between a number of people who may be in a different part of the country or live overseas. It is carried out in real time.

The basic hardware includes:

Webcams

Large monitors / television screens

Microphones

Speakers

There are a few items to consider when a conference begins:

- Agree a time & date for the conference
- The delegates must log in to the video conference system
- The set-up needs to be checked before the meeting goes live
- Webcams need to be placed in the correct position & mics need to be placed centrally.
- One person must be the main contact in each conference room to make sure each delegate is able to be heard.

The basic software includes:

Webcam & microphone software drivers

CODEC coder-decoder or compression-decompression

Echo cancellation software

• Potential issues with video conferencing:-

- Time lag in responses / delays when talking
- Jerking images due to poor internet
- Can be expensive to set up in the first place
- There can be problems if the delegates live in different countries where the time zone differences are large
- Training people can be both costly and time consuming
- It can be demotivating for staff if they believe that one of the perks of their job is travelling
- If the internet connection breaks down, the video conference can be almost unusable

• Advantages of video conferencing:-

- As people are in their own building, it is much easier to access important documents
- It is possible to hold conference at short notice
- Not travelling physically to meetings reduce costs
 - Reduce travelling costs
 - No need to pay for hotel or venue hire
 - Reduces the cost of taking people away from their work
- It may be better to use video conferencing than have delegates travel to potentially unsafe places around the world

* Audio Conferencing $\Rightarrow$ Meetings held between people using audio equipment. It can be telephone, a computer (with built-in microphones and speakers) this makes use of VoIP which allow communication.

The procedure of audio conferencing:

1. The conference organizer is given two PINs by the phone company. One is the personal PIN & the other one is the participant's PIN.
2. The organizer contacts all the participants & inform them of their PIN and the conference date & time.
3. When the conference is about to start, the organizer dials the conference phone number & once he/she is connected, keys in his/her personal PIN.
4. The participants then call the same conference number to join in.

The only drawback is the quality of the sound connection - otherwise 'drop out', echoing or a very noisy line making it difficult to understand.

* Web Conferencing $\Rightarrow$ uses the internet to permit conferencing to take place.

Allows the following types of meeting to take place:-

- Business meetings to discuss new idea

- Presentation

- Online education or training

The only requirement is a computer & a high-speed, stable internet connection.

To carry out web conferencing:-

- each user either downloads an application or logs on to a website from a link.
- delegates can leave or join the conference as they wish.
- the organizer can decide on who can speak at any time using the control panel on their computer.
- If a delegate wishes to speak, they raise a flag next to their name, delegates can post comments using instant messaging for all delegates to see at any time.

Some of the main features include:-

- Slide presentation using presentation software.
- It is possible for any delegate to draw or write on a 'whiteboard' using their own keyboard or mouse
- It is possible to transmit images or videos using the webcam throughout the conference.
- Documents can be shared by uploading them to the website before the conference begins
- It is possible to chat verbally or by using instant messaging throughout the conference.

Advantages:-

- Reduce cost as less extra hardware is needed.
- Fewer issues with video lag
- Can be used on more devices
- Increased privacy as there is no camera

Disadvantages :-

- Requires stable internet connection
- Cannot see the body language
- Cannot tell if the employees are paying attention
- Fewer features than video-conferencing.

-- ~ -- ~ -- ~ --