Cambridge

OL

ICT

CODE: (0417)

Section 4

Networks and the effects of using them

4.1 Networks

4.1.1 Common network devices and terms

We will begin this section by defining four important terms you will often come across in this chapter:
» Network interface card (NIC)
» Media access control (MAC) address
» Internet protocol (IP) address
» Data packet.

Network interface card (NIC)

A **network interface card (NIC)** is a crucial component in a network, converting binary data into an electrical signal for access. Typically integrated into the motherboard, NICs have a unique hardwired MAC address, identifying the device. Wireless NICs, on the other hand, use wireless connectivity via an antenna.

Media access control (MAC) address

The media access control (MAC) address is a number which uniquely identifies a device when it is connected to a network. The MAC address is made up of 48 bits which are shown as six groups of hexadecimal digits with the general format:

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

The MAC address is sometimes referred to as the **physical address** because it uniquely identifies a device.

Internet protocol (IP) addresses

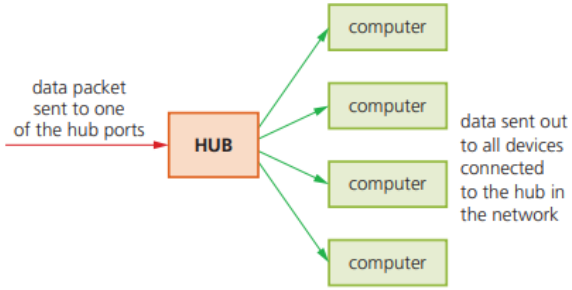
Whenever a computer connects to the internet it is given an **internet protocol (IP) address**. An IP address is assigned to a computer by an ISP and is necessary for internet protocol operation. It identifies a device's location on a network, changing each time a device logs in at different locations. This is different from the constant MAC address.

Data packets

Data is moved around networks in the form of data packets. Whenever a user sends some data, it is split up into a number of packets and each packet is transmitted separately. Packets of data will usually have a header which contains:
» The sender's IP address » the receiver's IP address
» The sequence/identity number of the packet (this is to ensure that all the packets can be reassembled into the correct order once they reach the destination)
» The packet size (this is to ensure the receiving station can check if all of the packets have arrived intact)
» How many data packets make up the whole message.

Hubs

Hubs are hardware devices that can have a number of other devices connected to them. They are used primarily to connect devices together to form a **local area network (LAN)**, often in the same building. A hub will take a data packet received at one of its ports and broadcast it to **every** device connected to it.



▲ **Figure 4.2** Hub network connections

Because data packets are delivered to every device on the network:
» Hubs are not very secure because every device will receive every data packet
» There will be unnecessary traffic on the network, which results in reduced bandwidth.

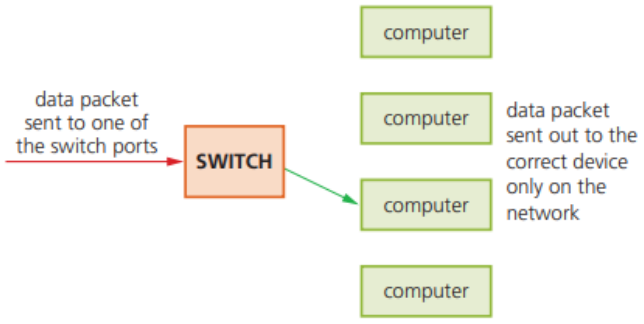
Switches

Switches are 'intelligent' versions of hubs. As with hubs, they connect a number of devices together to form a LAN.

A switch uses a look-up table to match the MAC address of an incoming data packet, directing it to the correct device, ensuring that no other devices see the packet.

▼ **Table 4.1** Switch MAC address table

Port number	MAC address
1	a4-00-22-a4-fe-d1
2	00-1c-b3-4f-25-ff
3	33-11-ad-6f-f1-00
4	a4-00-22-b2-24-11
5	00-1c-b3-44-ff-02
6	0d-3e-4f-1a-22-00



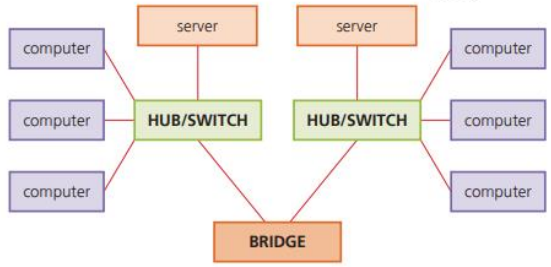
▲ **Figure 4.4** Switch network connections

Hubs and switches are used to exchange data **within** their own local area networks. They are unable to exchange data with outside networks (such as the internet). To exchange data outside their own LAN, a device needs to be able to read an IP address.

Bridges

Bridges are devices that connect one LAN to another LAN that uses the same protocol (communication rules). They are often used to connect together different parts of a LAN so that they can function as a single LAN.

▲ **Figure 4.5** Bridge

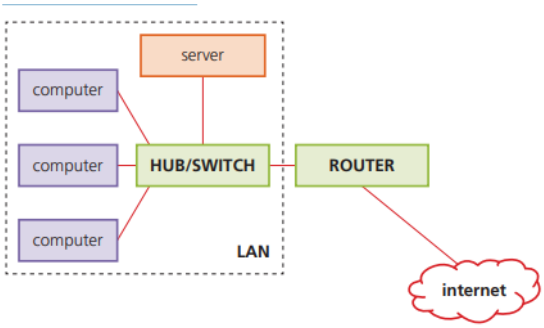


▲ **Figure 4.6** Use of a bridge to connect two LANs together

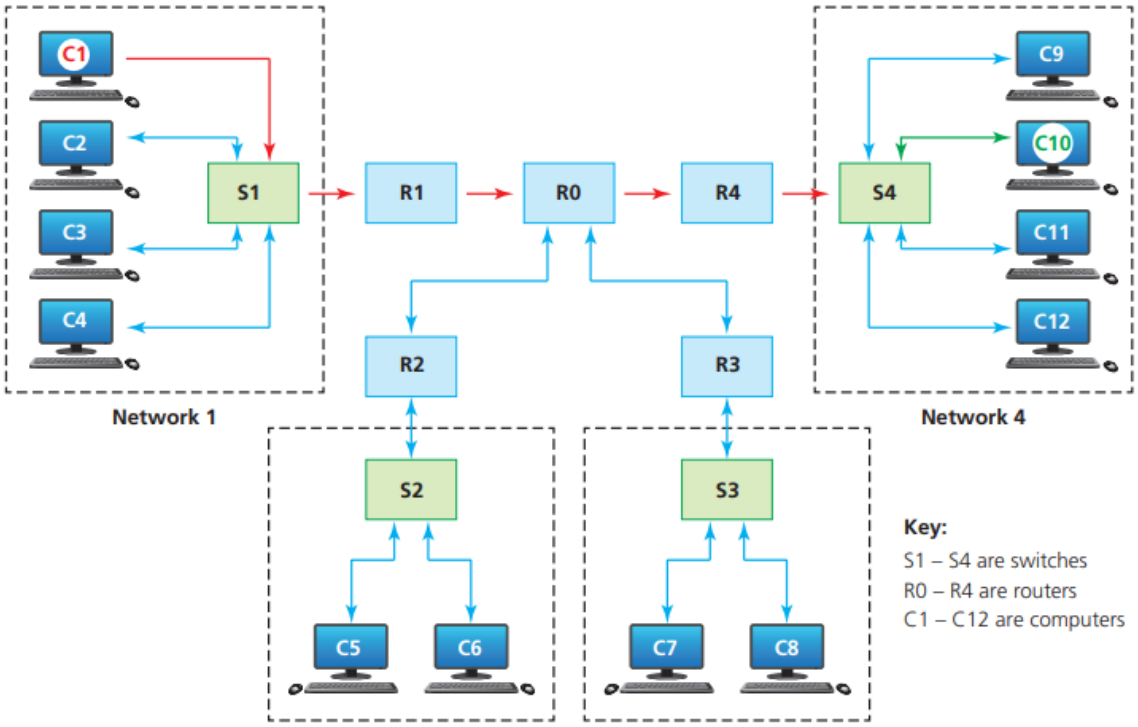
4.1.2 Routers

Routers are used to route data packets from one network to another network, based on IP addresses. It can do this because each router has its own IP address. Routers are used to join a LAN to the internet.

A router receives a data packet and checks its IP address to determine if it's meant for its network or an external one. If it's meant for its network, it's routed to a local switch or hub, otherwise, it's sent to an external router. Routers use a routing table on their RAM to determine the sender's location. The router doesn't store MAC addresses, as the packet is sent to a local switch using its look-up table.



▲ **Figure 4.8** Router used to connect a LAN to the internet



▲ **Figure 4.9** Routing of data from **C1** to **C10**

Suppose in Figure 4.9, computer C1 wishes to send data to computer C10:

» Data packets are sent from C1 to R1.

» R1 checks the IP addresses and notes the data packets are not intended for any devices on Network 1.

» The data packets are then forwarded onto the internet (R0).

» The IP address (in the header of the data packet) matches that of R4; this ensures that each data packet is eventually forwarded to R4.

» R4 recognises that the IP address of each data packet refers to Network 4 and forwards them to S4 which then directs each data packet to C10.

▼ **Table 4.2** Comparison of routers and bridges

Router	Bridge
The main objective of a router is to connect various types of network together	The main objective of a bridge is to connect LANs together
Routers scan a device's IP address	Bridges scan a device's MAC address
Data is sent out using data packets	Data is sent out using data packets
Connected networks will use different protocols	Connects networks together that use the same protocols
A routing table is used to direct data packets to the correct device	Bridges do not make use of routing tables
A router has more than two ports	A bridge has only two ports

4.1.3 Wi-Fi and Bluetooth

Both **Wi-Fi** and **Bluetooth** offer wireless communication between devices. They both use electromagnetic radiation as the carrier of data transmission

Devices randomly select one of 79 channels to pair with another, if already used, and constantly change channels to minimize interference risks, changing channels several times a second to ensure efficient communication. This is known as **spread-spectrum frequency hopping**. Bluetooth uses key encryption to create a secure **wireless personal area network (WPAN).**

Bluetooth is useful:

» When transferring data between two or more devices which are very close together (less than 30 metres distance)

» When the speed of data transmission is not critical

» For low-bandwidth applications

The internet wirelessly at any **access point** (**AP**) or '**hot spot'** up to 100 metres away. Table 4.3 summarises some of the differences between Wi-Fi and Bluetooth.

▼ **Table 4.3** Comparison of Wi-Fi and Bluetooth connectivity

Feature	Bluetooth	Wi-Fi
Transmission frequency used	2.4 GHz	2.4, 3.6, 5.0 GHz
Data transfer rate (maximum)	25 Mbits/second (~3.1 Mbytes/second)	250 Mbits/second (~31 Mbytes/second)
Maximum effective range (metres)	30 metres	100 metres (but can be obstructed by walls, etc. reducing effective range to only a few metres)
Maximum number of devices connected	Up to 7	Depends on the router used (can be one device or many devices)
Type of data transmission security	Key matching encryption	WEP (wireless equivalent privacy) and WPA (Wi-Fi protected access) are the most common security systems)

4.1.4 Cloud computing (storage)

Cloud computing involves data storage on remote servers, allowing clients to access data at any time, even during maintenance or repair. This is known as **data redundancy**.

» Public cloud – this is a storage environment where the customer/client and cloud storage provider are different companies.
» Private cloud – this is storage provided by a dedicated environment behind a company firewall; customer/client and cloud storage provider are integrated and operate as a single entity.
» Hybrid cloud – this is a combination of the two previous environments; some data resides in the private cloud and less-sensitive/less-commercial data can be accessed from a public cloud storage provider.

Advantages of cloud computing (storage)
» Customer/client files stored in the cloud can be accessed at any time, from any device, anywhere in the world, as long as internet access is available.
» There is no need for a customer/client to carry an external storage device with them, or even use the same computer, to store and retrieve information.
» The cloud provides the user with remote backup of data, with obvious advantages in the event of data loss/disaster recovery on their own computer.
» If a customer/client has a failure of their hard disk or backup device, cloud storage will allow recovery of their data.
» The cloud system offers almost unlimited storage capacity (at a price!)

Disadvantages of cloud computing (storage)
» Security aspects of storing data in the cloud (see comments later on).
» If the customer/client has a slow or unstable internet connection, they could have many problems accessing or downloading their data/files
» Costs can be high if a large storage capacity or high download/upload data transfer is required.
» The potential failure of the cloud storage company is always possible – this poses a risk of loss of all backup data.

Data security using cloud storage/computing

Companies that transfer vast amounts of confidential data from their own systems to a cloud service provider are potentially relinquishing control of their own data security. This raises a number of questions:
» What physical security exists regarding the building where the data is housed?
» How good is the cloud service provider's resistance to natural disasters or power cuts?
» What safeguards exist regarding personnel who work for the cloud service company? Can they use their authorisation codes to access confidential data for monetary purposes?

Data loss

There is a risk that important and irreplaceable data could be lost from cloud storage facilities. In 2019, there were a number of breaches of cloud security. We will briefly mention two of these breaches:

» On 2 April, a Mexican digital media company (called Cultura Colectiva) exposed 540 million Facebook accounts stored on one of their cloud servers; the data included user profiles, user IDs, account names, likes and comments.

» On 29 July, Capital One Bank (in the USA) had some of their cloud-based data hacked exposing 80,000 bank account numbers, 140,000 social security numbers and over one million government ID numbers.

4.1.5 Common network environments

Extranets, intranets and the internet

Extranets, intranets and the internet are all common types of network environment.

4.1.6 Network types

This section will cover the following types of networks:
» Local area network (LAN)
» Wireless local area network (WLAN)
» Wide area network (WAN).

Local area network (LAN)

Local area networks (LANs) are usually within one building or geographically near each other. A typical LAN will consist of a number of computers and devices (for example, printers) which will be connected to hubs or switches.

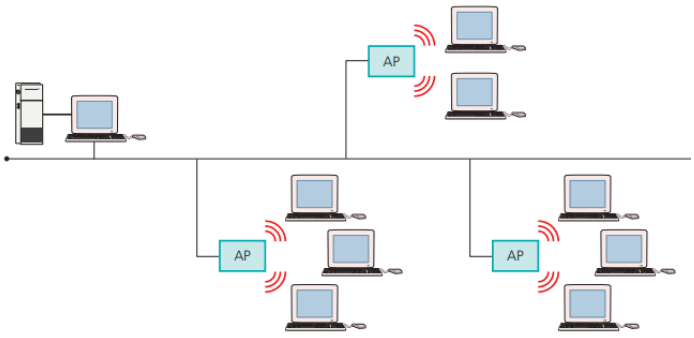
There are advantages of networking computers together using LANs:
» They allow the sharing of resources such as hardware (e.g. printers and scanners) and software (e.g. word processors and photo editing software)
» They permit easy communication between users of the LAN (e.g. by using simple text messaging between computers on the network)
» They use a network administrator that ensures security and use of the LAN is constantly monitored (e.g. the administrator can maintain passwords and also monitor data traffic within the network).

There are also disadvantages of networking computers using LANs:
» Easier spread of viruses throughout the whole network » queues for shared resources (such as a printer) which can be frustrating
» Slower access to external networks
» Increased security risk when compared to stand-alone computers
» If the main server breaks down, in many types of network structures, the network will no longer function properly.

Wireless local area network (WLAN)

Wireless LANs (WLANs) are similar to LANs, but there are no wires or cables. In other words, they provide wireless network communications over fairly short distances using radio or infrared signals instead of using cables.

Devices, known as **access points (APs),** are connected into a wired network at fixed locations. The APs use either **spread-spectrum technology (**which is a wideband radio frequency with a range of about 30 to 50 metres) or **infrared**, but this has a very short range (about 1–2 metres) and is easily blocked, and therefore infrared has limited use.



▲ **Figure 4.10** Wireless LAN set-up

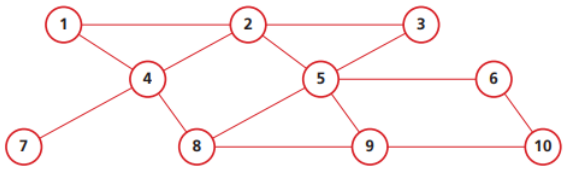
Wired versus wireless

▼ **Table 4.4** Wired versus wired LAN

Wireless networking	Wired networking
It is easier to expand the networks and it is not necessary to connect the devices using cables	Using cables produces a more reliable and stable network; wireless connectivity is often subject to interference
This gives devices increased mobility, as long as they are within range of the APs	Data transfer rates tend to be faster and there will not be any 'dead spots'
No cabling, so there is a safety improvement and increased flexibility	
There is an increased chance of interference from external sources	Setting up cabled networks tends to be cheaper overall in spite of the need to buy and install cable
Data is less secure than with wired systems; it is easier to intercept radio waves and microwaves than cables; it is essential to protect data transmissions using encryption	However, cabled networks lose the ability for devices to be mobile; they must be close enough to allow for cable connections
Data transmission rate is still slower than for cabled networks although it continues to improve	Having lots of wires can lead to a number of hazards, such as tripping hazards, overheating of connections (leading to potential fire risk) and disconnection of cables during routine office cleaning
It is possible for signals to be stopped by thick walls (for example, in old houses) and there may be areas of variable signal strength leading to 'drop out'	

Wide area networks (WANs)

Wide area networks (WANs) are used for long-distance connections between computers or networks, such as ATMs in banks. They can be formed using a router and can use public or dedicated communication lines, depending on the distance between devices. A typical WAN consists of end and intermediate systems.



▲ **Figure 4.11** WAN end systems and intermediate systems

The following is used as a guide for deciding the 'size' of a network:
» WAN: 100 km to over 1000 km
» MAN: 1 km to 100 km
» LAN: 10 m to 1000 m (1 km)

4.2 Network issues and communication

4.2.1 Security issues regarding data transfer

This section covers some of the more general aspects of internet security, together with how we use networks to communicate.

4.2.2 Passwords

Passwords are used in many instances when accessing the internet.

There are many more instances when you might need to type in a password and, in many cases, a user ID. It is important that passwords are protected. Some ways of doing this are described below:
» Run anti-spyware software to make sure that your passwords are not being relayed back to whoever put the spyware on your computer

» Change passwords on a regular basis in case it has come into the possession of another user illegally or accidentally.
» Passwords should not be easy to crack (e.g. your favourite colour, name of a pet or favourite rock group); passwords are grouped as either strong (hard to crack or guess) or weak (relatively easy to crack or guess).
» Strong passwords should contain:
– at least one capital letter
– at least one numerical value
– at least one other keyboard character (such as @, *, & etc.)

4.2.3 Other authentication methods

Passwords are one of the most common types of authentications (that is, a way of proving your identity). This section will look at a number of other types of authentications:
» Zero login
» Biometrics
» Magnetic stripes
» Smart cards
» Physical tokens
» Electronic tokens.

Zero login and biometrics

The Fast ID online (FIDO) Alliance and WWW Consortium (W3C) announced a new technology standard that allows users to login to computer systems without the need to type in a password.

Zero login essentially relies on devices being smart and secure enough to instantly recognise a user by a number of features based on:
» Biometrics
» Behavioural patterns

Magnetic stripe cards

Chapters 2 and 6 discuss magnetic stripe cards, which have a reverse magnetic stripe made up of magnetic particles. These cards can contain sensitive information like name, ID number, sex, and date of birth, and only allow access if scanned data matches database data.

Some ID cards also use a **holographic image (hologram**). These are designed to make forgery of the card more difficult.

Advantages of magnetic stripe cards
» They are easy to use.
» It is not an expensive technology.
» Magnetic cards can be remotely deactivated (if lost or stolen).
» The cards can be multi-purpose

Disadvantages of magnetic stripe cards
» Less secure than, for example, biometric methods (no encryption is used and the stripe contents can be copied fairly easily).
» The cards wear out with a lot of use.
» Magnetic readers often fail to read the cards on first attempt

Smart cards

By inserting a tag (chip and antenna) into a security card, it can act as a smart **contactless card** (that is, it can be read from a distance and does not have to be swiped through a card reader).

Physical tokens

Physical tokens are solid objects used for authentication, containing internal clocks and generating a one-time password (OTP) when a PIN and other details are entered. These tokens are valid for less than a minute and are commonly used in banking, where customers need to prove their identity.

To do this, they need to use a physical token supplied by the bank:
» The customer inserts their debit card into the top of the token device (first authentication step) and the device either recognises the card as genuine or rejects it.
» The device then asks the customer to press 'IDENTIFY' and then enter their PIN (second authentication step).
» A one-time password is then shown on the device screen – this is usually an eight-digit code.
» The customer now goes back to their bank web page and enters the eightdigit code.
» They are now given access to their account

There are two types of physical tokens:
1. A **disconnected physical token** – this is the type described above, where a separate device is used, requiring the user to key in data manually using a keypad
2. A **connected physical token** – this type of token transmits the generated one-time password directly to a computer through a USB connection; the user does not need to manually enter data

Electronic tokens

Electronic tokens are software installed on a user's device, such as a smartphone, to authenticate a user to a website. The user installs an app on their smartphone, which generates a one-time password (OTP) and other authentication methods. The website server runs the same software, and the user is allowed access once the OTP and other authentication methods are verified.

4.2.4 Anti-malware software

Running **anti-virus software** in the background on a computer will constantly check for virus attacks. Although various types of anti-virus software work in different ways they all have the following common features.

» They check software or files before they are run or loaded on a computer.
» Anti-virus software compares a possible virus against a database of known viruses.
» They carry out **heuristic checking** – this is the checking of software for types of behaviour that could indicate a possible virus; this is useful if software is infected by a virus not yet on the database.

» Any possible files or programs which are infected are put into **quarantine** which:
– allows the virus to be automatically deleted, or
– allows the user to make the decision about deletion (it is possible that the user knows that the file or program is not infected by a virus – this is known as a **false positive** and is one of the drawbacks of anti-virus software)

» Anti-virus software needs to be kept up to date because new viruses are constantly being discovered.

» Full system checks need to be carried out once a week, for example, because some viruses lie dormant and would only be picked up by this full system scan.

4.2.5 Electronic conferencing

This section will consider three types of electronic conferencing:
» Video conferencing
» Audio conferencing
» Web conferencing

Video conferencing

Video conferencing is a communication method that uses both video and sound. It is a substitute for face-to-face conferences between a number of people, who may be in a different part of the country or live overseas.

The basic hardware includes:
» Webcams
» Large monitors/television screens
» Microphones
» Speakers.

There are a few items to consider when a conference is about to begin:
» It is essential to agree a time and date for the conference to take place.
» The delegates in each conference room must log into the video-conference system.
» The video-conference set-up needs to be checked before the meeting goes live
» Webcams need to be placed in the correct position so that all the delegates in the room are within visual contact
» Microphones need to be placed centrally so that all of the delegates can speak – the sound is picked up by the microphones and is transmitted to the other delegates
» It is important for one person to be the main contact in each conference room to make sure each delegate is able to be heard; this is particularly important if more than two video-conference rooms are linked up at the same time.

▼ **Table 4.5** Software used in video conferencing

Software	Description
Webcam and microphone software drivers	It is vital that the correct software is used to ensure that the webcam and microphone transmit their images and sound to the other delegates (these are sometimes referred to as hardware drivers).
CODEC	**CODEC** can stand for **CO**der-**DEC**oder or **CO**mpression-**DEC**ompression. The first is used to encode or decode the digital data stream to allow data to be transmitted (encoded) and played back (decoded). The second is used to compress the data before it is transmitted and then decompress it again at the receiving conference room.
Echo cancellation software	**Echo cancellation software** allows talking to take place in real time and permits the synchronisation of communication. Microphones can pick up sound from the speakers (creating an echo); this software copies received signals and checks for parts of the signal that reappear but are delayed slightly. The reappearing parts are removed from the signal (the echo is removed).

Advantages of using video conferencing
» As people are in their own building, it is much easier to access important documents or bring in 'experts' at key parts of the conference – this would be difficult if they were a long way away from their office.
» It is possible to hold conferences at short notice (a conference date can be set up within a few hours as no person needs to travel very far).
» Not travelling physically to meetings reduces costs:
– reduced travelling costs
– no need to pay for hotel accommodation or venue hire
– it also reduces the cost of taking people away from their work for two or three days to travel
» It may be better to use video conferencing than have delegates travel to potentially unsafe places around the world.
» It is better for the environment – less travel means less pollution.
» It connects people in an organisation who might be otherwise left out,

Disadvantages of using video conferencing

» There is potential time lag in responses/delays when talking.
» Images can jerk – usually due to poor internet/network performance or poor bandwidth.
» It can be very expensive to set up in the first place (both the hardware and the software are expensive to purchase and get set up correctly).
» There can be problems if the delegates live in different countries where the time zone differences are large.
» Training people to use the system correctly 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 international travel.
» The whole system relies on a good network connection – if it breaks down or the signal strength is diminished in any way, then the video conference can be almost unusable

Audio conferencing

Audio conferencing refers to meetings held between people using audio (sound) equipment. Audio conferencing can be done over the standard telephone network (often referred to as a **phone conference)**

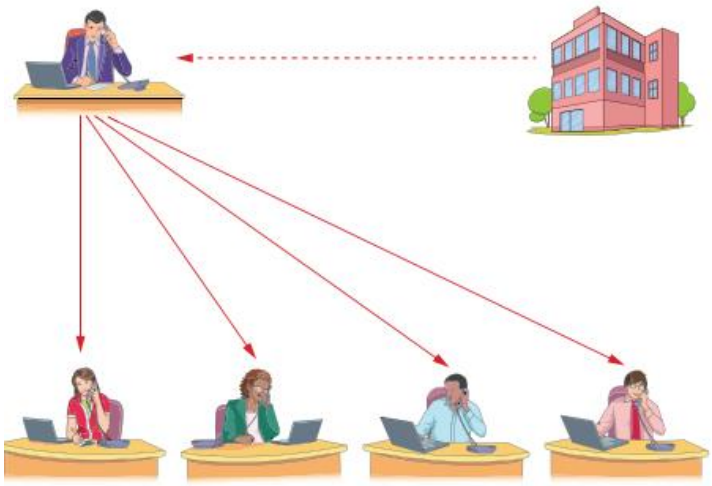


Figure 4.16 Audio conferencing

The equipment required for an audio conference over a standard telephone network normally just includes a standard telephone. It is also possible to hold an audio conference using a computer, as long as a microphone and speakers are connected. This makes use of Voice over Internet Protocol (VoIP).

It is also possible to connect an internet telephone, which usually plugs into the router or other internet device.

In this case equipment can include:
» A computer (with built-in microphones and speakers)
» External microphone and/or speakers » an internet phone
» A standard phone.

Web conferencing

Web conferencing (often referred to as a **webinar** or **webcasts**) uses the internet to permit conferencing to take place.

Multiple computers are used with this system, all connected over the internet. As with video conferencing, it is carried out in real time and allows the following types of meeting to take place:
» Business meetings to discuss new ideas
» Presentations
» Online education or training.

Delegates can post comments using instant messaging for all delegates to see at any time. Some of the main features include:
» Slide presentations using presentation software can be posted on the conference website in advance of the meeting. » The host's computer screen can be shared for live presentations, or other live demonstrations.
» 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 first uploading them to the website before the conference begins.
» As described earlier, it is possible to chat verbally or by using instant messaging throughout the conference

Revision questions

(2022 June)
1).Network devices are used in computer systems.
Complete each sentence by identifying the most appropriate network device.
(a) The network device that is used to transmit the data along an analogue telephone line is a
(b) The network device that connects a LAN to a WAN is a
(c) The network device that allows data to be directed to a specific computer on a LAN is a
(d) The internal network device that allows a computer to connect to a LAN is a

(2022 June)
2).The Internet of Things (IoT) allows devices as well as computers to connect to the internet using a router. Each device uses an IP address.
(a) Explain what is meant by an IP address.
(b) Explain how a router sends data packets to another network.
(c) The network has a firewall.
Explain why a firewall is needed.

3). (2022 June)
Both the internet and the intranet are used for communication.
(a) Define the terms internet and intranet.
(i) Internet
(ii) Intranet

4). (2023 Nov)
A bridge and a router are examples of networking devices. (a) Explain the differences between a bridge and a router.

5). (2023 Nov)
Explain the purpose of a routing table.

6). (2023 Nov)
(a) Explain what is meant by cloud storage and how it is used.
(b) Describe two issues related to the security of data in the cloud.

(2022 june)
7).Tawara Hotel uses magnetic stripe cards to allow guests access to their bedrooms. The hotel is changing the electronic lock it uses on its bedroom doors so the lock can work with RFID cards.
Compare the use of magnetic stripe cards and RFID cards for key entry. Your answer must include similarities and differences.

8). (2022 june)
Many bank cards now use contactless technology.
Describe the advantages and disadvantages of using these cards rather than cards that use chip and PIN.
2021 Nov

9).Employees in the organisation are allowed to access the intranet using their smartphones.
The employees are required to secure their smartphones using either facial recognition, passwords or voice recognition.
Tick (✓) whether the following statements refer to facial recognition, password or voice recognition.

	Facial recognition (✓)	Password (✓)	Voice recognition (✓)
This method cannot access the smartphone unintentionally			
The accuracy of this method can be affected by noise			
This method requires the use of the smartphone's camera			
This method could be compromised by shoulder surfing			

10). 2021 Nov
Write down the most appropriate network device to match the following statements. Your answers should be different in each part.
(a) This network device checks the data packet arriving from one computer and sends the data to a specific computer.
(b) This network device sends the data packet from a computer to all devices connected to it.
(c) This network device connects a LAN to the internet.
(d) This network device connects one LAN to another with the same protocol.

11). 2021 Nov
A family has purchased a wireless router for use in their home to allow their devices to be connected via WiFi to form a wireless local area network (WLAN).
(a) When the family purchased the wireless router they were advised to change the default password.
Explain why they should change the default password.

Explain why they should change the default password.
(b) Describe the process of using WiFi to connect to a WLAN.