CAMBRIDGE
UNIVERSITY PRESS

Computer Science

for Cambridge International AS & A Level

COURSEBOOK

Sylvia Langfield & Dave Duddell

Second edition

Cambridge Assessment International Education

Endorsed for full syllabus coverage

CAMBRIDGE
UNIVERSITY PRESS

Computer Science

for Cambridge International AS & A Level

COURSEBOOK

Sylvia Langfield & Dave Duddell

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06 -04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/ 9781108733755

First published 2015
Second edition 2019

20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Printed in the United Kingdom by Latimer Trend

A catalogue record for this publication is available from the British Library

ISBN 978-1-108-73375-5 Paperback
ISBN 978-1-108-56832-6 Paperback with Cambridge Elevate edition (2 years)
ISBN 978-1-108-70041-2 Cambridge Elevate edition (2 years)
ISBN 978-1-108-70039-9 Digital edition

All exam-style questions and sample answers in this title were written by the authors. In examinations, the way marks are awarded may be different.

Past exam paper questions throughout reproduced by permission of Cambridge Assessment International Education.

Contents

Part 1: Theory fundamentals

Part 2: Fundamental problem-solving and programming skills

Part 3: Advanced theory

Part 4: Further problem-solving and programming skills

Introduction

This full-colour, illustrated textbook has been written by experienced authors specifically for the Cambridge International AS & A Level Computer Science syllabus (9618) for examination from 2021. It is based on the first edition by the same authors for the previous Cambridge International AS & A Level Computer Science syllabus (9608). There are substantial changes, the most important being the inclusion of the topic of Artificial Intelligence (See Chapter 22) and the replacement of the Pascal programming language by the Java programming language.

The presentation of the chapters in this book reflects the content of the syllabus:

- The book is divided into four parts, each of which is closely matched to the corresponding part of the syllabus.
- Each chapter defines a set of learning objectives which closely match the learning objectives set out in the syllabus.
- The chapters in Parts 1 and 3 have been written with emphasis on the promotion of knowledge and understanding. The chapters in Parts 2 and 4 have been written with an emphasis on problem solving and programming.

The key concepts for Cambridge International AS & A Level Computer Science are:

Computational thinking

Computational thinking is a set of skills such as abstraction, decomposition and algorithmic thinking. Chapter 12 (Algorithm design and problem-solving), Chapter 15 (Software development) and Chapter 23 (Algorithms) concentrate on this key concept.

Programming paradigms

A programming paradigm is a way of thinking about or approaching problems. Most of the programming in this book follows the imperative (procedural) paradigm. Chapter 25 (Programming paradigms) gives an overview of other paradigms, while Chapter 6 (Assembly language programming), Chapter 28 (Low-level programming), Chapter 27 (Object Oriented Programming) and Chapter 29 (Declarative programming) give an insight into these paradigms.

Communication

Communication in this context ranges from the internal transfer of data within a computer system to the transfer of data across the internet. See Chapter 2 (Communication and networking technologies) and Chapter 17 (Communication and internet technologies).

Computer architecture and hardware

Computer architecture is the design of the internal operation of a computer system. Computer systems consist of hardware (internal components and peripherals) and software that makes the hardware functional. See Chapter 3 (Hardware), Chapter 4 (Logic gates and logic circuits), Chapter 8 (System software), Chapter 18 (Hardware and virtual machines), Chapter 19 (Logic circuits and Boolean algebra) and Chapter 20 (System software).

Data representation and structures

An understanding of binary numbers and how they can be interpreted in different ways is covered in Chapter 1 (Information representation) and Chapter 16 (Data representation). Chapter 11 covers databases. Chapter 13 (Data types and structures) and Chapter 14 (Programming and data representation) show how data can be organised for efficient use and storage.

The chapters in Parts 1 and 3 have a narrative which involve a number of interdependent topics. We would encourage learners to read the whole chapter first before going back to revisit the individual sections.

The chapters in Parts 2 and 4 contain many more tasks. We would encourage learners to approach these chapters step-by-step. Whenever a task is presented, this should be carried out before progressing further.

In particular, Chapter 12 (Algorithm design and problem-solving) may be worked through in parallel with Chapter 14 (Programming and data representation). For example, Task 14.03 is based on Worked Example 12.03. After studying this worked example, learners may wish to cover the first part of Chapter 14 and write the program for Task 14.03. This will give the learner the opportunity to test their understanding of an algorithm by implementing it in their chosen programming language. Then further study of Chapter 12 is recommended before attempting further tasks in Chapter 14.

How to use this book

This book contains a number of features to help you in your study.

Learning objectives

By the end of this chapter you should be able to:

- show an understanding of monitoring and control systems
- show understanding of how bit manipulation can be used to monitor/control a device.

Learning objectives – each chapter begins with a short list of the learning objectives and concepts that are explained in it.

Key Terms – clear and straightforward explanations of the most important terms in each chapter.

KEY TERM

Bit: a digit in the binary number system written using either of the symbols 0 and 1

Task – exercises for you to test your skills.

TASK 1.01

Convert each of the denary numbers 96, 215 and 374 into hexadecimal numbers.
Convert each of the hexadecimal numbers B4, FF and 3A2C to denary numbers.

Question – questions for you to test your knowledge and understanding.

Question 1.01

Does a computer ever use hexadecimal numbers?

Discussion Point:

What is the two's complement of the binary value 1000? Are you surprised by this?

Discussion Point – discussion points intended for class discussion.

Reflection Point – opportunities for you to check your understanding of the topic that has just been covered.

Reflection Point:

Can you recall the different possibilities for what one byte might be coded to represent?

Extension Question – extended questions for consideration of more advanced aspects or topics beyond the immediate scope of the Cambridge International AS & A Level syllabus.

Extension Question 1.01

Graphic files can be stored in a number of formats. For example, JPEG, GIF, PNG and TIFF are just a few of the possibilities. What compression techniques, if any, do these use?

WORKED EXAMPLE 1.01

To carry out the conversion you start at the most significant bit and successively multiply by two and add the result to the next digit. The following shows the method being used to convert the binary number 11001 to the denary number 25:

	1	×	2	=	2
add 2 to 1, then	2	×	3	=	6
add 6 to 0, then	2	×	6	=	12
add 12 to 0, then	2	×	12	=	24
add 24 to 1 to give 25.					

Worked Example – step-by-step examples of solving problems or implementing specific techniques.

Tip – quick notes to highlight key facts and important points.

TIP

To check that an answer with eight bits is sensible, remember that the maximum denary value possible in seven bits is $2^7 - 1$ which is 127 whereas eight bits can hold values up to $2^8 - 1$ which is 255.

Summary

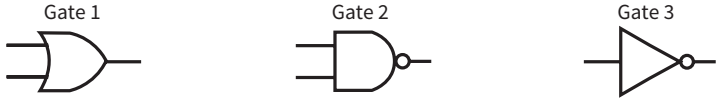
- A logic scenario can be described by a problem statement or a logic expression.
- A logic expression comprises logic propositions and Boolean operators.
- Logic circuits are constructed from logic gates.
- The operation of a logic gate matches that of a Boolean operator.
- The outcome of a logic expression or a logic circuit can be expressed as a truth table.
- A logic expression can be created from a truth table using the rows that provide a 1 output.

Summary – these appear at the end of each chapter to help you review what you have learned

Exam-style Questions

Exam-style Questions – these aim to test your skills, knowledge and understanding using exam-style questioning.

1 a The following are the symbols for three different logic gates.



i Identify each of the logic gates. [3]

ii Sketch the truth table for either Gate 1 or Gate 2. [2]

Chapter 2: Communication and networking technologies

Learning objectives

By the end of this chapter you should be able to:

- show understanding of the purpose and benefits of networking devices
- show understanding of the characteristics of a LAN (local area network) and a WAN (wide area network)
- explain the client-server and peer-to-peer models of networked computers
- show understanding of thin-client and thick-client and the differences between them
- show understanding of the bus, star, mesh and hybrid topologies
- show understanding of cloud computing
- show understanding of the differences between and implications of the use of wireless and wired networks
- describe the hardware that is used to support a LAN
- describe the role and function of a router in a network
- show understanding of Ethernet and how collisions are detected and avoided
- show understanding of bit streaming
- show understanding of the differences between the World Wide Web (WWW) and the Internet
- describe the hardware that is used to support the Internet
- explain the use of IP addresses in the transmission of data over the Internet
- explain how a Uniform Resource Locator (URL) is used to locate a resource on the World Wide Web (WWW) and the role of the Domain Name Service (DNS).

2.01 The evolution of the purpose and benefits of networking

Wide area network (WAN)

During the 1970s it would be normal for a large organisation to have a computer. This computer would be a mainframe or minicomputer. The computer could have been running a time-sharing operating system with individual users accessing the computer using a terminal connected to the computer with a cable. Technology was developed that allowed computers in different organisations to be networked using what would now be described as a **wide area network (WAN)**. In a WAN, the networked computers could be thousands of kilometres apart.

The benefits of having the computers connected by a WAN were:

- a 'job' could be run on a remote computer that had the required application software
- a data archive that was stored on a remote computer could be accessed
- a message could be transmitted electronically to a user on a remote computer.

Today, a typical WAN is characterised by the following.

- It will be used by an organisation or a company to connect sites or branches.
- It will not be owned by the organisation or company.
- It will be leased from a public switched telephone network company (PSTN).
- A dedicated communication link will be provided by the PSTN.
- The transmission medium will be fibre-optic cable.
- Transmission within the WAN will be from switch to switch.
- A switch will connect the WAN to each site.
- There will not be any end-systems connected directly to the WAN.

Local area network (LAN)

In the 1980s the arrival of the microcomputer or personal computer (PC) changed computing. In an organisation, a user could have their own computer on their desk. The computer could be a stand-alone system or some organisations chose to have more than one computer connected using a **local area network (LAN)**. It was called a local area network because it typically connected PCs that were in one room or in one building or on one site.

KEY TERMS

Wide area network (WAN): a network connecting computers on different sites, possibly thousands of kilometres apart

Local area network (LAN): a network connecting computers in a single room, in a single building or on a single site

The benefits of connecting PCs in a LAN included the following.

- The expense of installing application software on each individual PC could be saved by installing the software on an application server attached to the LAN instead.
- A file server could be attached to the LAN that allowed users to store larger files and also allowed files to be shared between users.
- Instead of supplying individual printers to be connected to a user's PC, one or more printers could be attached to a print server that was connected to the LAN; these could be higher quality printers.

- Managers in organisations could use electronic mail to communicate with staff rather than sending round memos on paper.
- The 'paper-less office' became a possibility, where files were to be stored in digital form on a file server rather than as paper copies in a filing cabinet.

Today, a typical LAN is characterised by the following.

- It will be used by an organisation or a company within a site or branch.
- It will be owned by the organisation or company.
- It will be one of many individual LANS at one site.
- The transmission medium will be twisted pair cable or WiFi.
- The LAN will contain a device that allows connection to other networks.
- There will be end-systems connected which will be user systems or servers.

Discussion Point:

If a print server was attached to a network, what functionality could it provide?

Internet working

The 1990s can be said to be when the modern era of computing and network use started, with the beginning of widespread use of the Internet. The word Internet is a shortened form of the term 'internetwork', which describes a number of networks all connected together. LANs are connected to WANs which are in turn connected to the Internet to allow access to resources world-wide. The other technologies defining the modern era, namely mobile devices and wireless networking, started to become commonly used in the 2000s.

The purpose and benefits of networking have not changed but their scale and scope has increased enormously. In particular, people now have full access to networks from their personal devices.

The client-server model

The **client-server** model (or architecture) was first used in large organisations when they had installed internal networks. Typically, the organisation would have individual LANs connected via an organisation-wide WAN. An individual LAN might have had an application server attached. The organisation was likely to need a powerful central computer. The central computer could be connected to the WAN as a server. It would probably not have individual users connected to it directly. A PC, attached to a LAN, could access the server as a client.

The client-server mode of operation nowadays is different. The client is a web browser connected to the Internet. The server is a web server hosted on the Internet.

The server provides an application and the client uses the application. There are two options for how the client functions.

A **thin-client** is one which:

- chooses an application to run on the server
- sends input data to the server when requested by the application
- receives output from the application.

KEY TERMS

Client-server: an architecture where a client runs an application provided by a server on a network

Thin-client: a client that only provides input and receives output from the application

A **thick-client** is one which:

- chooses an application provided by the server
- possibly carries out some processing before running the application on the server and also after receiving output from the application
- alternatively, possibly downloads the application from the server and runs the application itself.

TIP

In thick-client mode the processing on the client can be controlled by the use of a scripting language. You do not need to know any details of this.

KEY TERM

Thick-client: a client that carries out at least some of the processing itself

The client-server approach is the choice in the following circumstances.

- The server stores a database which is accessed from the client system.
- The server stores a web application which allows the client system to find or, sometimes, supply information.
- The server stores a web application which allows the client system to carry out an e-commerce or financial transaction.

File sharing

If a user uploads files to a file server then the client-server operation can be used by another user to download these from the server.

An alternative mode of operation for sharing files is peer-to-peer networking. Instead of having one server that many clients access, a peer-to-peer network operates with each peer (networked computer) storing some of the files. Each peer can therefore act as a client and request a file from another peer or it can act as a server when another peer requests the download of a file.

The peer-to-peer model has several advantages compared to client-server file downloading:

- it avoids the possibility of congestion on the network when many clients are simultaneously attempting to download files
- parts of a file can be downloaded separately
- the parts are available from more than one host.

The client-server model has the following advantages.

- It allows an organisation to control the downloading and use of files.
- The files can be better protected from malware attacks because the files are stored on one server which will be regularly scanned using appropriate anti-virus software.

2.02 Network topologies

There are five requirements for a data communications system: a sender, a receiver, a transmission medium, a message and a protocol (see Chapter 17 for details about protocols). A transmission medium can be air (e.g. for WiFi) or cables (e.g. for Ethernet). Data can be sent through the medium in different modes:

- simplex mode where data flow is one-way only
- half duplex where data can flow either way but not simultaneously
- full duplex where simultaneous both-ways data flow is possible.

A 'message' is any type of data, which can be sent as either:

- a broadcast, which is a one-to-all communication (as used traditionally for radio and television)
- a multicast, which is from one source to many destinations
- a unicast, which is a one-to-one communication.

A data communications system may consist of a single isolated network. There are several possibilities for the **topology** of an isolated network. The simplest of these is where two systems are connected by a network link as shown in Figure 2.01. This is an example of a point-to-point connection, which is a dedicated link. Transmission might be simplex or duplex and a message can only be unicast.

Figure 2.01 A point-to-point network

Early LAN topologies used either a ring or a **bus topology**. We don't need to cover the ring topology as it is not used very often now. A bus topology has only one link but it is shared by a number of end-systems and is therefore described as a multi-point connection. The configuration is shown in Figure 2.02. There is no direct connection between any pair of end-systems. A message must therefore be broadcast even though it might only be intended for one **end-system**. The topology is resilient because a fault in an end-system or in the link to it does not affect the use of the network by the other end-systems.

Figure 2.02 A bus network

An example of a fully-connected **mesh topology** is shown in Figure 2.03. In this configuration, each end-system has a point-to-point connection to each of the other end-systems. Transmission is duplex; messages might be unicast, multicast or broadcast.

KEY TERMS

Topology: the configuration of a network that defines how the various devices on the network are connected

Bus topology: contains one shared link to which all devices are attached

End-system: a computer or server connected to a network

Mesh topology: contains direct links between devices

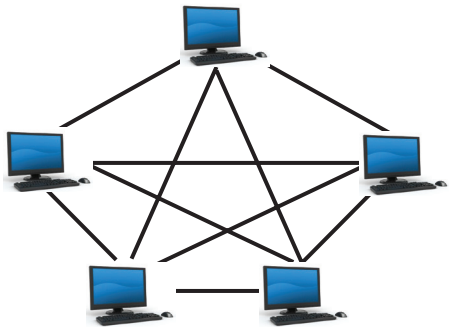


Figure 2.03 A mesh network.

Figure 2.03 shows end-systems connected in a mesh topology but this is unrealistic because of the amount of cabling required. A mesh topology can be used when individual LAN switches are connected in a network. The topology is essential for the connection of routers within the infrastructure of the Internet.

The final possibility is a **star topology** which is shown in Figure 2.04.

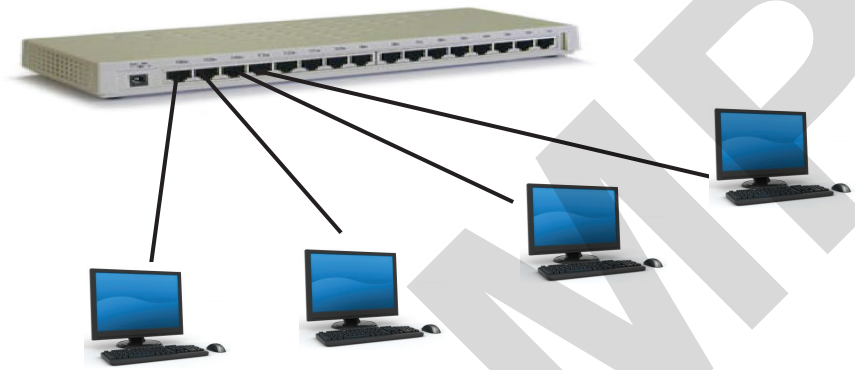


Figure 2.04 A star topology

KEY TERM

Star topology: each end-system is linked to a central device

Figure 2.04 could have been drawn so that it looked like a star but has been drawn to show the physical configuration that is used in a real life installation. In a star topology, each end-system has a point-to-point connection to the central device. Transmission is duplex and messages from the central device might be unicast, multicast or broadcast. As with the bus topology, the failure of an end-system, or its link, leaves the other end-systems unaffected. However, the central device must not fail.

In the bus topology most of the end-systems might be user workstations and the others are servers. However, in the star topology, the end-systems might be user workstations or servers but the central device is different. It is a specialised device with the purpose of connecting other devices in the network. Currently, the star topology is the usual way to configure a network. There are several reasons for this. The most important is that the central device can be used to connect the network to other networks and, in particular, to the Internet.

Discussion Point:

Which network topologies have you used? You might wish to defer this discussion until you have read about network devices later in this chapter.

In a situation where several LANs are connected, they can have different topologies or supporting technologies. This collection of LANs then becomes a **hybrid network**. A special connecting device is needed to ensure that the hybrid network is fully functional. It is often an advantage to be able to connect a new topology LAN to existing LANs where it is not sensible or not possible to use the existing topology for the new LAN. An example is when a wired LAN is already installed but a new wireless LAN is to be connected to it.

KEY TERMS

Hybrid network: a collection of connected LANs where some of them have different topologies or supporting technologies

Cable: a transmission using copper wire or fibre-optic

Bandwidth: a measure of the amount of data that can be transmitted per second

2.03 Transmission media

Cable

A network **cable** can be twisted pair, coaxial or fibre-optic. The twisted pair and coaxial cables both use copper for the transmission medium. In discussing suitability for a given application there are a number of factors to consider. One of these is the cost of the cable and connecting devices. Another is the best **bandwidth** that can be achieved. The bandwidth governs the possible data transmission rate. There are then two factors that can cause poor performance: the likelihood of interference affecting transmitted signals and the extent of attenuation (deterioration of the signal) when high frequencies are transmitted. These factors will dictate whether repeaters or amplifiers are needed in transmission lines and how many will be needed. Table 2.01 shows some comparisons of the different cable types.

	Twisted pair	Coaxial	Fibre-optic
Cost	Lowest	Higher	Highest
Bandwidth or data rate	Lowest	Higher	Much higher
Attenuation at high frequency	Affected	Most affected	Least affected
Interference	Worst affected	Less affected	Least affected
Need for repeaters	More often	More often	Less often

Table 2.01 Comparisons between cable types

You need to understand that for each of the three types of cabling there are defined standards for different grades of cable which must be considered when you decide which type of cable to use. Fibre-optic cable performs best but costs more than the other kinds. For a new installation the improved performance of fibre-optic cable is likely to be the factor that governs your choice. However, where copper cable is already installed the cost of replacement by fibre-optic cable may not be justified.

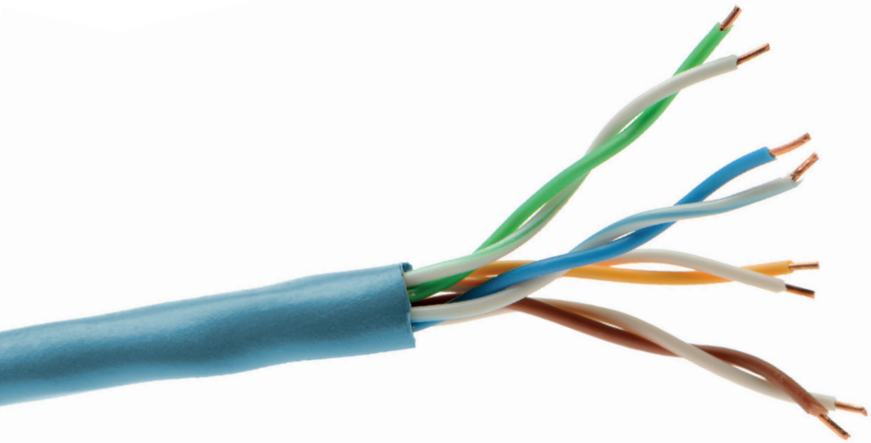


Figure 2.05 One cable with four twisted pairs with differing twist rates to reduce interference

Currently, twisted pair cable is normally used to connect telephone handsets to telephone lines. This type of cable is illustrated in Figure 2.05. It is also the technology of choice for high-speed local area networks.

Question 2.01

Twisted pair cable can be shielded or unshielded. What are the options for this? How does shielding affect the use of the cable?

Coaxial cable is used extensively by cable television companies and in metropolitan area networks. It is not usually used for long-distance telephone cabling. Fibre-optic cable is the technology of choice for long-distance cabling. As shown in Figure 2.06, coaxial cable is not bundled but a fibre-optic cable contains many individual fibres.

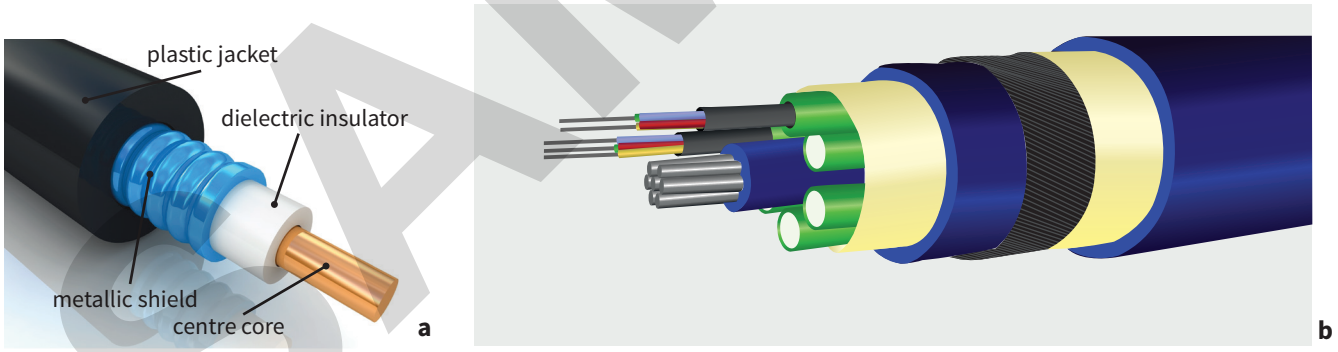


Figure 2.06 (a) Coaxial cable and (b) a bundled fibre-optic cable

Wireless

The alternative to cable is **wireless** transmission. The three options here are radio, microwave or infrared. These are all examples of electromagnetic radiation; the only intrinsic difference between the three types is the frequency of the waves.

KEY TERM

Wireless: a transmission using radio, microwave or infrared

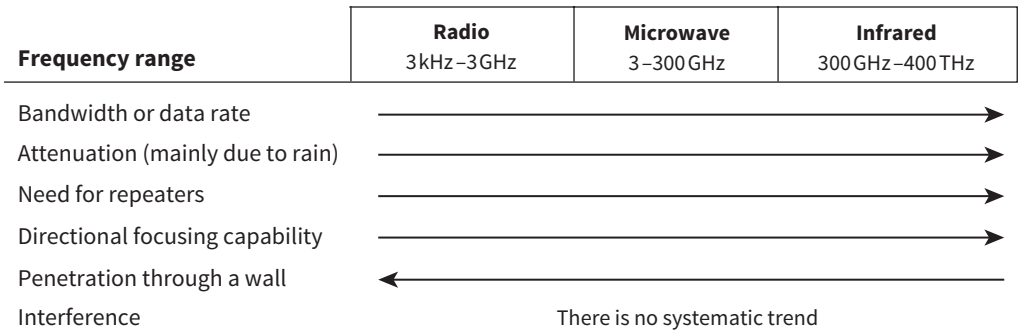


Figure 2.07 Frequency ranges and frequency dependency of factors affecting wireless transmission

When making a choice of which wireless option to use you need to consider all of the same factors that were discussed when comparing different kinds of cable. In addition, the ability of the radiation to transmit through a solid barrier is an important factor. Also, the extent to which the transmission can be focused in a specific direction needs to be considered. Figure 2.07 shows the approximate frequency ranges for the three types of radiation. The factors listed on the left increase in the direction of the arrows. The bandwidth increases through radio and microwave to infrared but the ability of the waves to penetrate solid objects is greatest for radio waves. Interference is not consistently affected by the frequency.

The increased attenuation for infrared transmission, which has the highest frequency, means that it is only suitable for indoor applications. The fact that it will not penetrate through a wall is then of benefit because the transmission cannot escape and cause unwanted interference elsewhere. For most applications, microwave transmission is the best option because it has a better bandwidth compared to that available using radio waves.

Comparing cable and wireless transmission

It is worth noting that cables are often referred to as 'guided media' and wireless as 'unguided media'. This is slightly misleading because only radio wave transmission fits the description of unguided. It is possible with microwaves or infrared to direct a transmission towards a particular receiver (as suggested in Figure 2.07).

There are other points to consider when we compare the relative advantages of transmission through a cable or wireless transmission.

- The use of certain wireless transmission frequencies is regulated by government agencies and so permission has to be obtained before wireless transmission is used.
- Outside these frequencies, no permission is needed to use the air for transmission but cables can only be laid in the ground with the permission of landowners.
- For global communications, the two competing technologies are: transmission through fibre-optic cables laid underground (or on the sea bed) and satellite transmission (discussed later in this section).
- Interference is much more significant for wireless transmission and its extent is dependent on which frequencies are being used for different applications.
- Repeaters are needed less often for wireless transmission.
- Mobile (cell) phones now dominate Internet use and for these, only wireless transmission is possible.
- For home or small office use, wired or wireless transmission is equally efficient; often, not having to install cables favours wireless connections for a small network.

Satellites are components of modern communication systems. Figure 2.08 shows the altitudes (distances above Earth) of three different types of satellite. The Van Allen belts are areas containing high levels of electrically charged particles, which interfere with satellites.

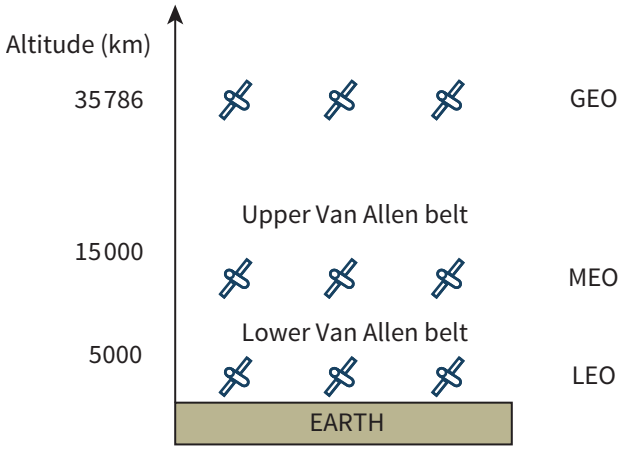


Figure 2.08 Satellite altitudes

The highest altitude satellites are in geostationary Earth orbit (GEO) over the equator and these are used to provide long-distance telephone and computer network communication. 'Geostationary' means that the satellite orbits at the same speed as the Earth spins, so from a point on the Earth the satellite always appears to be at the same point in the sky. Only three GEO satellites are needed for full global coverage. Closer to Earth are a group of medium-Earth-orbit (MEO) satellites some of which provide the global positioning system (GPS). Ten MEO satellites are needed for global coverage. Finally, low-Earth-orbit (LEO) satellites work in 'constellations' to supplement the mobile phone networks. Fifty LEO satellites are needed for full global coverage but currently there are several hundred LEO satellites in orbit.

A satellite can act as a component in a network and can directly connect with ground-based components. These ground-based components can be much further apart than in a network with no satellites. The disadvantage of satellites is that the greater transmission distance causes transmission delays, which can cause technical problems for the network.

TASK 2.01

Calculate the approximate time taken for a transmission from the surface of the Earth to a medium-Earth-orbit satellite. (Take the speed of light to be 300 000 km per second.)

The use of satellites in networks tends to be for specialised applications such as the Global Positioning System (GPS) or for Internet use in remote locations. At one stage, a lot of Internet communication was expected to make use of satellites, but the development of high-speed fibre-optic cabling at relatively low cost has reduced the need for satellites.

2.04 LAN hardware

Wired LANs

In the early years, coaxial cable was used for LANs. Nowadays, twisted pair cables are probably the most widely used networking connections, and fibre-optic cables are becoming more common. In a bus configuration the bus will consist of a series of sockets linked by cables. The ends of the bus have terminators attached that prevent signals from reflecting

back down the bus. Each end-system (which is either a user workstation or a **server**), has a short length of cable with an RJ-45 connector at each end. One end is plugged into a bus socket and the other end is plugged into the LAN port of the end-system.

In a star configuration each end-system has the same type of cable with the same connectors but the cable tends to be much longer because it has to plug into a socket on the central device.

A bus can be extended by linking two bus cables using a **repeater**. A repeater is needed because over long distances, signals become attenuated (reduced in strength), making communication unreliable. A repeater receives an input signal and generates a new full-strength signal. Sometimes a bus network is constructed in what are called segments. Two segments are connected using a **bridge**. The bridge stores the network addresses for the end-systems in the two segments it connects.

The LAN port on an end-system is connected to a **Network Interface Card (NIC)**. The NIC is manufactured with a unique network address that is used to identify the end-system in which it has been installed. The addressing system is discussed in Chapter 17 (Section 17.05). For a star network, the central device might be a hub, a **switch** or a router. The switch is by far the most likely. A switch is a connecting device that can direct a communication to a specific end-system. There is discussion of how it functions in Section 2.05. The router is discussed later in this chapter and also in Chapter 17.

Wireless LANs

WiFi (WLAN in some countries) is a term used to describe wireless Ethernet. Its formal description is IEEE 802.11. This is a wireless LAN standard that uses radio frequency transmission. The central device in a WiFi LAN is a **Wireless Access Point (WAP)**. This can be an end-system in a wired network. The WAP can communicate with an end-system in the WiFi LAN provided that the end-system has a **Wireless Network Interface Card (WNIC)** installed.

KEY TERMS

Server: a system providing a service to end-systems
Repeater: a device that connects two cables and provides a full-strength signal to the second cable
Bridge: a device that connects two segments of a LAN
Network Interface Card (NIC): a component used to identify the end-system
Switch: a connecting device that can send a unicast message
Wireless Access Point (WAP): the connecting device in a WiFi LAN
Wireless Network Interface Card (WNIC): provides the NIC function in a WiFi LAN

2.05 Ethernet

Ethernet is one of the two dominant technologies in the modern networked world. It is primarily focused on LANs. Although Ethernet was first devised in the 1970s independently of any organisation, it was later adopted for standardisation by the Institute of Electrical and Electronics Engineers (IEEE). In particular it was their 802 committee that took responsibility for the development of the protocol. The standard for a wired network is denoted as IEEE 802.3 which is sometimes used as an alternative name for Ethernet. The standard has so far evolved through five generations: standard or traditional, fast, gigabit, 10 gigabit and 100 gigabit. The gigabit part of the name indicates its data transfer speed capability.

Original (or 'legacy') Ethernet was implemented on a LAN configured either as a bus or as a star with a hub as the central device. In either topology, a transmission was broadcast type. Any message would be made available to all of the end-systems without any controlled

communication exchange between any pair of end-systems. For each message received an end-system had to check the destination address defined in the message to see if it was the intended recipient.

The use of a shared medium for message transmission has the potential for messages to be corrupted during transmission. If two end-systems were to transmit messages at the same time there would be what is described as a 'collision'. This is when the voltages associated with the transmission interfere with each other causing corruption of the individual messages. The method adopted for dealing with this was CSMA/CD (carrier sense multiple access with collision detection). This relied on the fact that if a message was being transmitted there was a voltage level on the Ethernet cable which could be detected by an end-system.

The transmitter uses the following procedure.

1. Check the voltage on the transmission medium.
2. If this indicates activity, wait a random time before checking again.
3. If no activity is detected, start transmission.
4. Continuously check for a collision.
5. If no collision is detected, continue transmission.
6. If a collision is detected, stop transmission of the message and transmit a jamming signal to warn all end-stations; after a random time, try again.

Although there might be some legacy Ethernet LANs still operating, modern Ethernet is switched. The star configuration has a switch as the central device. The switch controls transmission to specific end-systems. Each end-system is connected to the switch by a full-duplex link, so no collision is possible along that link. Because there might be high levels of activity the switch needs to be able to store an incoming message in a buffer until the cable is free for the transmission to take place. Since collisions are now impossible, CSMA/CD is no longer needed. Some further details concerning Ethernet are provided in Chapter 17 (Section 17.04).

Discussion Point:

Carry out some research about the different versions of Ethernet. Which version is implemented for the systems you use? For how long will it give sufficient performance?

2.06 The Internet infrastructure

To describe the Internet as a WAN pays little attention to its size and complexity. The Internet is the biggest internetwork in existence. Furthermore, it has never been designed as a single 'whole'; it has just evolved to reach its current form and is still evolving towards whatever future form it will take.

Internet Service Provider (ISP)

One of the consequences of the Internet not having been designed is that there is no agreed definition of its structure. However, there is a hierarchical aspect to the structure (meaning that there are several distinct 'levels' within the structure). For example, the initial function of an Internet Service Provider (ISP) was to give Internet access to an individual or company. This function is now performed by what we can call an 'access ISP'. These access ISPs then connect to what we can call 'middle tier' or regional ISPs, which in turn are connected to tier 1 (or 'backbone') ISPs. An ISP is a network and connections between ISPs are handled by Internet Exchange Points (IXPs). The tier 1 ISPs are at the top of the hierarchy, along with major Internet content providers.

Discussion Point:

How many ISPs or major Internet content providers are you familiar with?

Router

We can also think of the Internet in terms of the connections that carry the most traffic, which consist of a set of fibre-optic cables laid under the sea and across land, which can be described as a 'mesh' structure. This mesh of cables contains many points where the cables connect together, which we call nodes. At every node is a device called the **router**. Routers are found not only in the general 'mesh' of the Internet but also within the ISP networks. Each router is connected to several other routers and its function is to choose the best route for a transmission. The details of how a router works are discussed in Chapter 17 (Section 17.05).

KEY TERM

Router: a device that acts as a node on the Internet

Question 2.02

How near are you to an under-the-sea Internet fibre-optic cable?

Public switched telephone network (PSTN)

Communication systems that were not originally designed for computer networking provide significant infrastructure support for the Internet. The longest standing example is what is often referred to as POTS (plain old telephone service) but is more formally described as a PSTN (public switched telephone network). There is some discussion about how PSTNs provide that support in Chapter 17. During the early years of networking the telephone network carried analogue voice data. However, digital data could be transmitted provided that a modem was used to convert the digital data to analogue signals. Another modem was used to reverse the process at the receiving end. Such so-called 'dial-up' connections provided modest-speed, shared access when required. However, an organisation could instead pay for a leased line service that provided a dedicated, permanently connected link with guaranteed transmission speed. Typically, organisations made use of leased lines to establish WANs (or possibly MANs (metropolitan area networks)).

More recently, the PSTNs have upgraded their main communication lines to fibre-optic cable employing digital technology. This has allowed them to offer improved leased line services to ISPs but has also given them the opportunity to provide their own ISP services. In this role they provide two types of service. The first is a broadband network connection for traditional network access. The second is WiFi hotspot technology, where an access point as described in Section 2.04 has a connection to a wired network providing Internet access.

Cell phone network

For users of devices with mobile (cell) phone capability there is an alternative method for gaining Internet access. This is provided by mobile phone companies acting as ISPs. The mobile phone, equipped with the appropriate software, communicates with a standard cell tower to access the wireless telephone network, which in turn provides a connection to the Internet.

2.07 Applications that make use of the Internet

The World Wide Web (WWW)

It is common practice to talk about 'using the web' or 'using the Internet' as though these were just two different ways of saying the same thing. This is not true. The Internet is, as has been described above, an Internetwork. By contrast, the World Wide Web (WWW) is a distributed application which is available on the Internet.

Specifically, the web consists of an enormous collection of websites each having one or more web pages. The special feature of a web page is that it can contain hyperlinks which, when clicked, give direct and essentially immediate access to other web pages.

Cloud computing

Cloud computing is the provision of computing services usually via the Internet. An organisation may choose to establish its own **private cloud**. In this case there are three possible approaches:

- The organisation takes full responsibility for creating and managing the cloud installed on-site and connected to a private network
- The organisation outsources to a third-party the creation and management of an on-site installation connected to a private network
- The organisation outsources the creation and management of an Internet accessible system by a third-party.

The alternative is a **public cloud**. This is created, managed and owned by a third-party cloud service provider.

The services provided by a cloud are familiar ones provided by file servers and application servers. They are accessible via a browser and therefore accessible from any suitable device in any location. A public cloud can be accessed by an individual user or by an organisation. One major difference is the scale of the systems. The provision is established using large mainframe computers or server farms. The services provided can be characterised as being one of:

- infrastructure provision
- platform provision
- software provision

Many of the advantages to a cloud user arise from the fact that the cloud does not have the limitations that the systems already available have. For the infrastructure provision, the advantages include the better performance when running software and the increased storage capacity. For the platform provision, the cloud can offer facilities for software development and testing. For the software provision, the cloud will be able to run applications that require high performance systems. Alternatively, it could be that the costs to a company of buying and installing a software package themselves would be far too high. The other advantage is the familiar one with regard to outsourcing. The cloud user no longer needs technical expertise.

The disadvantages to a cloud user relate to the use of a public cloud. The cloud service provider has complete access to all of the data stored on the cloud. The cloud user cannot be sure that their data is not being shared with third-parties. This is a concern with regard to data privacy. The security of the data stored is an issue; the cloud service provider is being relied on to ensure data cannot be lost.

KEY TERMS

Private cloud: owned by and only accessed by an organisation

Public cloud: owned by a cloud service provider for general access

Bit streaming

Streaming media make use of the Internet for leisure activities like listening to music or watching a video. But what is a 'bit stream'? In general, before data is transmitted it is stored in bytes which can be transmitted one after the other as a 'byte stream'. Because of the file sizes involved, streamed media is always compressed to a sequence of bits - a 'bit stream'. Generic compression techniques mentioned in Chapter 1 (Section 1.07) can convert the byte stream to a bit stream with fewer bits overall. For the decoding process at the receiver end to work properly, the data must be transferred as a bit stream.

For one category of streaming media, the source is a website that has the media already stored. One option in this case is for the user to download a file then listen to it or watch it at some future convenient time. However, when the user does not wish to wait that long there is the streaming option. This option is described as viewing or listening **on demand**. In this case the delivery of the media and the playing of the media are two separate processes. The incoming media data are received into a buffer created on the user's computer. The user's machine has media player software that takes the media data from the buffer and plays it.

The other category of streaming media is **real-time** or live transmission. In this case the content is being generated as it is being delivered such as when viewing a sporting event. At the receiver end the technology is the same as before. The major problem is at the delivery end because a very large number of users may be watching simultaneously. The way this is managed now is to transmit the media initially to a large number of content provider servers which then transmit onwards to individual users.

A crucial point with media streaming is whether the technology has sufficient power to provide a satisfactory user experience. When the media is created it is the intention that the media is to be delivered to the user at precisely the same speed as used for its creation; a song that lasted four minutes when sung for the recording would sound very peculiar if, when it is received by a user, it lasts six minutes. The process of delivering the content is determined by the **bit rate**. For example, a relatively poor-quality video can be delivered at a bit rate of 300 kbps but a reasonably good-quality audio file only requires delivery at 128 kbps. Figure 2.09 shows a simple schematic diagram of the components involved in the streaming.

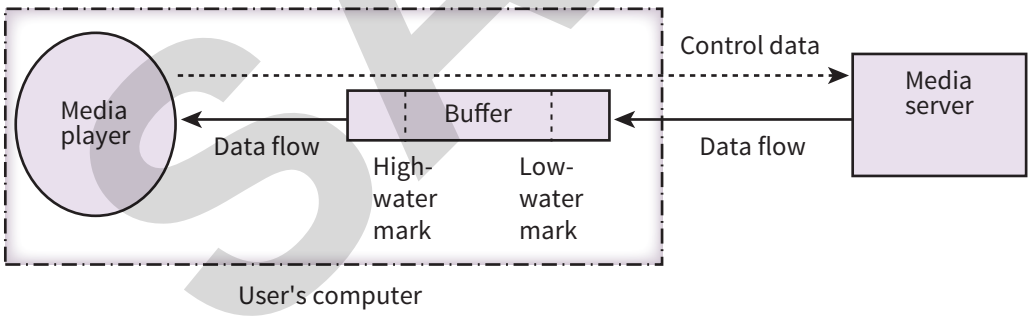


Figure 2.09 Schematic diagram of bit streaming

KEY TERMS

On-demand: when the bit stream content is transmitted at a time chosen by the user

Real-time: when the bit stream content is transmitted as it is produced

Bit rate: the number of bits transmitted per second

The buffer must deliver the data to the user, at the correct bit rate for the media being used. Data which is sent into the buffer should be sent at a higher rate to allow for unexpected delays. The media player continuously monitors how full the buffer is and controls the bit rate in relation to the defined high- and low-water marks. It is essential to have a buffer size that is sufficiently large for it never to get filled.

The rate of transmission to the buffer is limited by the bandwidth of the network connection. For a connection via a PSTN, a broadband link is essential. For good-quality movie presentation the broadband requirement is about 2.5 Mbps. Because this will not be available for all users it is often the practice that an individual video is made available at different levels of compression. The most highly compressed version will be the poorest quality but the bit rate may be sufficiently low for a reasonable presentation with a relatively low bandwidth Internet connection.

TASK 2.02

Consider a bit-streaming scenario for a video where the following values apply:

- the buffer size is 1 MiB
- the low-water mark is set at 100 KiB
- the high-water mark is set at 900 KiB
- the incoming data rate is 1 Mbps
- the video display rate is 300 Kbps.

Assume that the video is playing and that the buffer content has dropped to the low-water mark. The media player sets the controls for data input to begin again.

Calculate the amount of data that will be input to the buffer in two seconds and the amount of data that will be removed from the buffer in the same time period.

Repeat the calculation for 4, 6, 8, 10 and 12 seconds.

From this data, estimate when the buffer will have filled up to the high-water mark.

Assuming that the incoming transmission is halted at this time, calculate how long it will be before the buffer content has again fallen to the low-water mark level.

2.08 IP addressing

The Internet requires technical protocols to function. A protocol suite called TCP/IP is used as a standard (see Chapter 17). One aspect of this is IP addressing, which is used to define from where and to where data is being transmitted.

IPv4 addressing

Currently the Internet uses Internet Protocol version 4 (IPv4) addressing. IPv4 was devised in the late 1970s, before the invention of the PC and the mobile phone. IPv4 provides for a large but limited number of addresses for devices, which is no longer enough to cover all the devices expected to use the Internet in future.

The IPv4 addressing scheme is based on 32 bits (four bytes) being used to define an **IPv4 address**. It is worth putting this into context. The 32 bits allow 2^{32} different addresses. For big numbers like this it is worth remembering that 2^{10} is approximately 1000 in denary so the

KEY TERM

IPv4 address: a 32-bit long, hierarchical address of a device on the Internet

32 bits provide for approximately four billion addresses. The population of the world is about seven billion and it is estimated that approaching half of the world's population has Internet access. From this we can see that if there was a need to supply one IP address per Internet user the scheme would just about be adequate. However, things are not that simple.

The original addressing scheme was designed on the basis of a hierarchical address with a group of bits defining a network (a netID) and another group of bits defining a host on that network (a hostID). The aim was to assign a unique, universally recognised address for each device on the Internet. The separation into two parts allows the initial transmission to be routed according to the netID. The hostID only needs to be examined on arrival at the identified network. Before proceeding, it is important to note that the term 'host' is a little misleading because some devices, particularly routers, have more than one network interface and each interface requires a different IP address.

The other feature of the original scheme was that allocated addresses were based on the concept of different classes of networks. There were five classes; we are going to look at the first three classes. The structures used for the addresses are shown in Table 2.02.

Class	Class identifier	Number of bits for netID	Number of bits for hostID
Class A	0	7	24
Class B	10	14	16
Class C	110	21	8

Table 2.02 Address structure for three classes of IPv4 address

It can be seen from Table 2.02 that the most significant bit or bits identify the class. A group of the next most significant bits define the netID and the remaining, least significant, bits define the hostID. The reasoning behind this was straightforward. The largest organisations would be allocated to Class A. There could only be 2^7 i.e. 128 of these but there could be 2^{24} distinct hosts for each of them. This compared with 2^{21} (approximately two million) organisations that could be allocated to Class C but each of these could only support 2^8 i.e. 256 hosts.

The problems with this scheme arose once LANs supporting PCs became commonplace. The number of Class B netIDs available was insufficient but if organisations were allocated to Class C the number of hostIDs available was too small. There have been a number of different modifications made available to solve this problem.

Before considering some of these, the representation used for an IP address needs to be introduced. During transmission, the technology is based on the 32-bit binary code for the address; to make it simpler for users, we write the address using decimal numbers separated by dots. Each byte is written as the denary equivalent of the binary number represented by the binary code. For example, the 32 bit code:

```
10000000 00001100 00000010 00011110
```

is written in dotted decimal notation as:

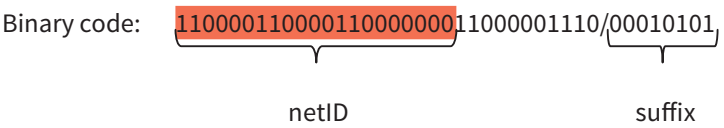
```
128.12.2.30
```

Discussion Point:

There were options available when the dotted decimal notation was chosen. Can you identify these?

Classless inter-domain routing (CIDR)

The first approach developed for improving the addressing scheme is called 'classless inter-domain routing' (CIDR). This retains the concept of a netID and a hostID but removes the rigid structure and allows the split between the netID and the hostID to be varied to suit individual need. The simple method used to achieve this is to add an 8-bit suffix to the address that specifies the number of bits for the netID. If, for instance, we define the suffix as 21, that means that 21 bits are used for the netID and there are 11 bits remaining (of a 32-bit address) to specify hostIDs allowing 2^{11} (i.e. 2048) hosts. One example of an IP address using this scheme is shown in Figure 2.10. The 21 bits representing the netID have been highlighted. The remaining 11 bits represent the hostID which would therefore have the binary value 11000001110.



Dotted decimal notation: 195.12.6.14/21

Figure 2.10 A CIDR IPv4 address

Note that with this scheme there is no longer any need to use the most significant bit or bits to define the class. However, it does allow already existing Class A, B or C addresses to be used with suffixes 8, 16 or 24, respectively.

TASK 2.03

Create an example of the binary code for a Class C address expressed in CIDR format. Give the corresponding dotted decimal representation.

Sub-netting

Sub-netting is a different approach. It allows a more efficient use of a hostID by applying a structure to it.

To illustrate an example of this we can consider a medium-sized organisation with about 150 employees each with their own computer workstation. Let's assume that there are six individual department LANs and one head-office LAN. Figure 2.11 shows a schematic diagram of how the LANs would be connected to the Internet if the original scheme were used. Note that the diagram has been simplified by showing the LANs connected to a gateway. This is a device that connects networks with different protocols. For the connection to the Internet the gateway would either first connect to a router or have the capability to act as a router itself.

The organisation would need seven individual Class C netIDs; one for each LAN. Each of these would point to one of the LAN gateways. The netID for each LAN would be identified by the first 24 bits of the IPv4 address, leaving 8 bits for the hostID. This would mean 256 individual codes for identifying different workstations on just one LAN. For the seven LANs the total number of workstations that could be identified would be:

$$256 \times 7 = 1792$$

Since the organisation only has 150 workstations in total, there are 1642 unused addresses. Not only would these be unused they would be unavailable for use by any other organisation.

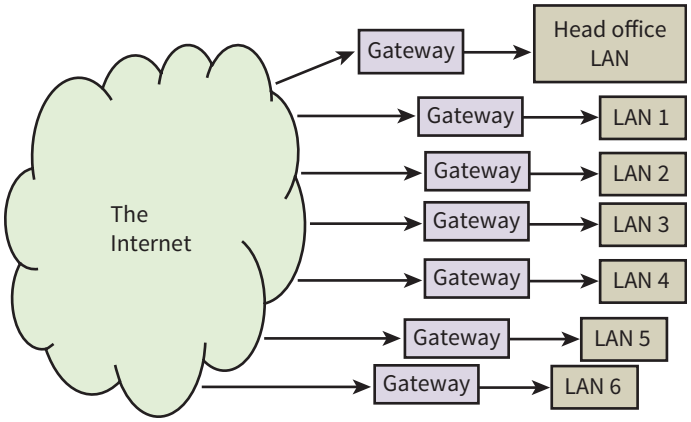


Figure 2.11 Connecting LANs using the original classful IPv4 scheme

The sub-netting solution for this organisation would require allocating just one Class C netID. For example, the IP addresses allocated might be 194.10.9.0 to 194.10.9.255 where the netID comprises the first three bytes, represented by the decimal values 194, 10 and 9.

The sub-netting now works by having a defined structure for the 256 codes constituting the hostID. A sensible solution for this organisation is to use the top three bits as a code for the individual LANs and the remaining five bits as codes for the individual workstations. Figure 2.12 shows a schematic diagram of this arrangement.

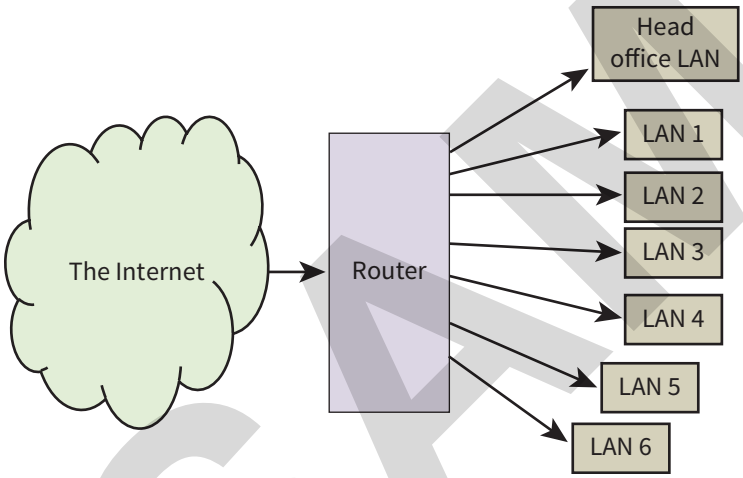


Figure 2.12 Connecting LANs using sub-netting

On the Internet, all of the allocated IP addresses have a netID pointing to the router. The router then has to interpret the hostID to direct the transmission to the appropriate workstations on one of the LANS via a gateway. Examples of workstation identification:

- hostID code 00001110 would be the address for workstation 14 on the head office LAN 0 (LAN 000)
- hostID code 01110000 would be the address for workstation 16 on LAN 3 (LAN 011).

With 150 workstations the organisation hasn't used all of the 256 allocated IP addresses. However, there are only 106 unused which is a reasonable number to have available in case of future expansion. Only one netID has been used leaving the other six that might have been used still available for other organisations to use.

Network address translation (NAT)

The final scheme to be considered is different in that it deviates from the principle that every IP address should be unique. In this scheme, provision has been made for large organisations to have private networks (intranets) which use the same protocols as those used for the Internet. One justification for using a private network has always been that this provides extra security because of the isolation from the Internet. However, this is no longer normal practice. Organisations want private networks but they also want Internet connectivity.

The solution for dealing with the addressing is to use network address translation (NAT). Figure 2.13 shows a schematic diagram of how this can be used.

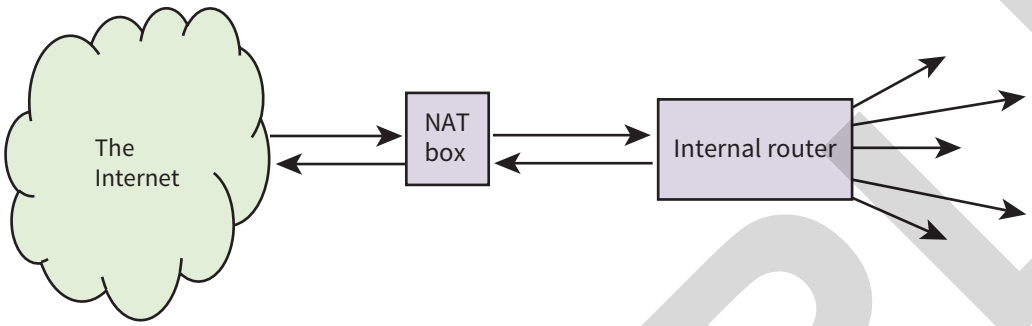


Figure 2.13 An intranet connected to the Internet using a NAT box

The NAT box has one IP address which is visible over the Internet and so can be used as a sending address or as a receiving address. Internally the IP addresses have to be chosen from one of the three ranges of IP addresses shown in Table 2.03 that have been allocated for such networks. (You do not need to remember these numbers!)

Lower bound	Upper bound
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Table 2.03 IPv4 addresses to be used in private networks

The important point is that each address can be simultaneously used by any number of different private networks. There is no knowledge of such use on the Internet itself or in any other private network. The interface in the NAT box has software installed to examine each incoming or outgoing transmission. There can be a security check before an incoming transmission is directed to the correct internal address. The diagram shows undefined arrows from the router connected to the NAT box. These indicate that the network structure within the organisation could take many different forms.

Static and dynamic IP addresses

As discussed in Section 2.06, when a user wishes to have a connection to the Internet the connection is handled by an Internet Service Provider. The ISP will have available a large number of hostIDs. However, the number of users that the ISP is supporting could very likely be larger than the total number of addresses available. Fortunately for the ISP and for an individual user many of these potential users will not be engaged in Internet interaction.

The normal practice is for the ISP to create a 'dynamic address' for a user. This is one that the ISP is free to change if it suits but more importantly the address is available for re-allocation once a user disconnects from the Internet. The alternative is a 'static address' which never changes and can be provided if a user is prepared to pay an extra charge.

Discussion Point:

Can you find out which IP addressing scheme is being used when you are connected to the Internet?

IPv6 addressing

Today there are combinations of IPv4 approaches in use and these allow the Internet to continue to function. Respected sources argue that this cannot continue beyond the current decade. There must soon be a migration to IP version 6 (IPv6), which uses a 128-bit addressing scheme allowing 2^{128} different addresses, a huge number! In practice, this will allow more complex structuring of addresses. Documenting these addresses is going to be difficult. The addresses are written in a colon hexadecimal notation. The code is broken into 16-bit parts, with each part represented by four hexadecimal characters. Fortunately, some abbreviations are allowed. A few examples are given in Table 2.04.

IPv6 address	Comment
68E6:7C48:FFFE:FFFF:3D20:1180:695A:FF01	A full address
72E6::CFFE:3D20:1180:295A:FF01	:0000:0000: has been replaced by ::
6C48:23:FFFE:FFFF:3D20:1180:95A:FF01	Leading zeros omitted
::192.31.20.46	An IPv4 address used in IPv6

Table 2.04 Some examples of IPv6 addresses

Extension Question 2.01

If IPv6 addressing is used, how many addresses would be available per square metre of the Earth's surface? Do you think there will be enough to go round?

2.09 Domain names

In everyday use of the Internet, a user needs to identify a particular web page or email box. As users, we would much prefer not to identify each IP address using its dotted decimal value! To get round this problem the **domain name service (DNS, also known as domain name system)** was invented in 1983. The DNS service allocates readable domain names for Internet hosts and provides a system for finding the IP address for an individual domain name.

KEY TERM

Domain name service (DNS): a hierarchical distributed database installed on domain name servers that is responsible for mapping a domain name to an IP address. Also known as domain name system.

The system is set up as a hierarchical distributed database which is installed on a large number of domain name servers covering the whole of the Internet. The domain name servers are connected in a hierarchy, with powerful root servers at the top of the hierarchy supporting the whole Internet. The root servers are replicated, meaning that multiple copies of all their data are kept at all times. DNS name space is then divided into non-overlapping zones. Each zone has a primary name server with the database stored on it. Secondary servers get information from this primary server.

As a result, the naming system is hierarchical. There are more than 250 top-level domains which are either generic (e.g. .com, .edu, and .gov) or represent countries (e.g. .uk and .nl).

The domain name is included in a universal resource locator (URL), which identifies a web page, or an email address. A domain is named by the path upward from it. For example, .eng.cisco.com. refers to the .eng subdomain in the .cisco domain of the .com top-level domain.

Looking up a domain name to find an IP address is called 'name resolution'. For such a query there are three possible outcomes.

- If the domain is under the control of the server to which the query is sent then an authoritative and correct IP address is returned.
- If the domain is not under the control of the server, an IP address can still be returned if it is stored in a cache of recently requested addresses but it might be out of date.
- If the domain in the query is remote then the query is sent to a root server which can provide an address for the name server of the appropriate top-level domain. This in turn can provide the address for the name server in the next lower domain. This continues until the query reaches a name server that can provide an authoritative IP address.

Reflection Point:

In several places you have been asked to carry out some research. Are you using the most efficient search methods? Specifically, how could they be improved?

Summary

- Client-server and peer-to-peer networking are options for file sharing.
- The star topology is the one most commonly used for a LAN.
- The main transmission media are copper (twisted pair, coaxial) cables, fibre-optic cables and wireless (radio, microwave, infrared).
- Factors to consider when choosing a medium are bandwidth, attenuation, interference and the need for repeaters.
- CSMA/CD (carrier sense multiple access with collision detection) has been used to detect and avoid message collisions in shared media.
- The Internet is the largest internetwork in existence.
- ISPs provide access to the Internet.
- Internet infrastructure is supported by PSTNs and cell phone companies.
- The World Wide Web is a distributed application accessible on the Internet.
- The current Internet addressing scheme is IPv4, with IPv6 a future contender.
- The DNS resolves a domain name to an IP address.

Exam-style Questions

1 A new company has been established. It has bought some new premises which consist of a number of buildings on a single site. It has decided that all of the computer workstations in the different buildings need to be networked. They are considering ways in which the network might be set up.

a One option they are considering is to use cabling for the network and to install it themselves.

i Name the **three** types of cabling that they might consider. [2]

ii Explain **two** factors, other than cost, that they need to consider when choosing suitable cabling. [4]

b Another option they are considering is to use wireless technology for at least part of the network.

i Explain **one** option that might be suitable for wireless networking. [2]

ii Identify **one** advantage, other than cost, of using wireless rather than cable networking. [1]

iii Identify **one** disadvantage (other than cost) of using wireless rather than cable networking. [1]

c The final option they are considering is to use the services of a PSTN.

i Define what a PSTN is or does. [1]

ii Explain how a PSTN could provide a network for the company. [3]

2 **a** The Domain Name System is vitally important for Internet users.

i Name the type of software used by the system and the type of hardware on which the software is installed. [2]

ii Name **two** types of application that use the Domain Name System and for each give a brief description of how it is used. [4]

b In the classful IPv4 addressing scheme, the 32-bit binary code for the address has the top (most significant) bit set to 0 if it is of class A, the top two bits set to 10 if class B or the top three bits set to 110 if class C. In a document an IPv4 address has been written as 205.124.16.152.

i Give the name for this notation for an IP address and explain how it relates to the 32-bit binary code. [2]

ii Identify the class of the address and explain your reason. [2]

iii Explain why an IPv4 address defines a netID and a hostID. [3]

c If the CIDR scheme for an IPv4 address is used the IP address 205.124.16.152 would be written as:

205.124.16.152/24

State the binary code for the hostID in this address, with a reason. [2]

3 A user watches a video provided by a website that uses on-demand bit streaming.

Describe the measures needed to ensure that the video does not periodically pause when it is being watched. [6]

4 **a** Describe where private IP addresses can be used. [2]

b Explain how it can be ensured that private and public IP addresses are not used in the wrong context. [4]

5 **a** An IP address has the following value:

11.64.255.90

i Write the above IP address in hexadecimal. [4]

ii Explain the format of an IP address. [2]

b Study the following sentence:

"When a user enters a URL into their web browser, the DNS service locates the required resource."

Explain how a URL and DNS are used to locate a resource. [4]

Cambridge International AS & A level Computer Science 9608 paper 12 Q9 June 2015

6 Access to World Wide Web content uses IP addressing.

a State what IP stands for. [1]

b The following table shows four possible IP addresses.

Indicate for each IP address whether it is valid or invalid and give a reason.

Address	Denary/Hexadecimal	Valid or Invalid	Reason
`3.2A.6AA.BBBB`	Hexadecimal		
`2.0.255.1`	Denary		
`6.0.257.6`	Denary		
`A.78.F4.J8`	Hexadecimal		

[4]

c Describe **two** differences between public and private IP addresses. [2]

Cambridge International AS & A level Computer Science 9608 paper 11 Q7 June 2016