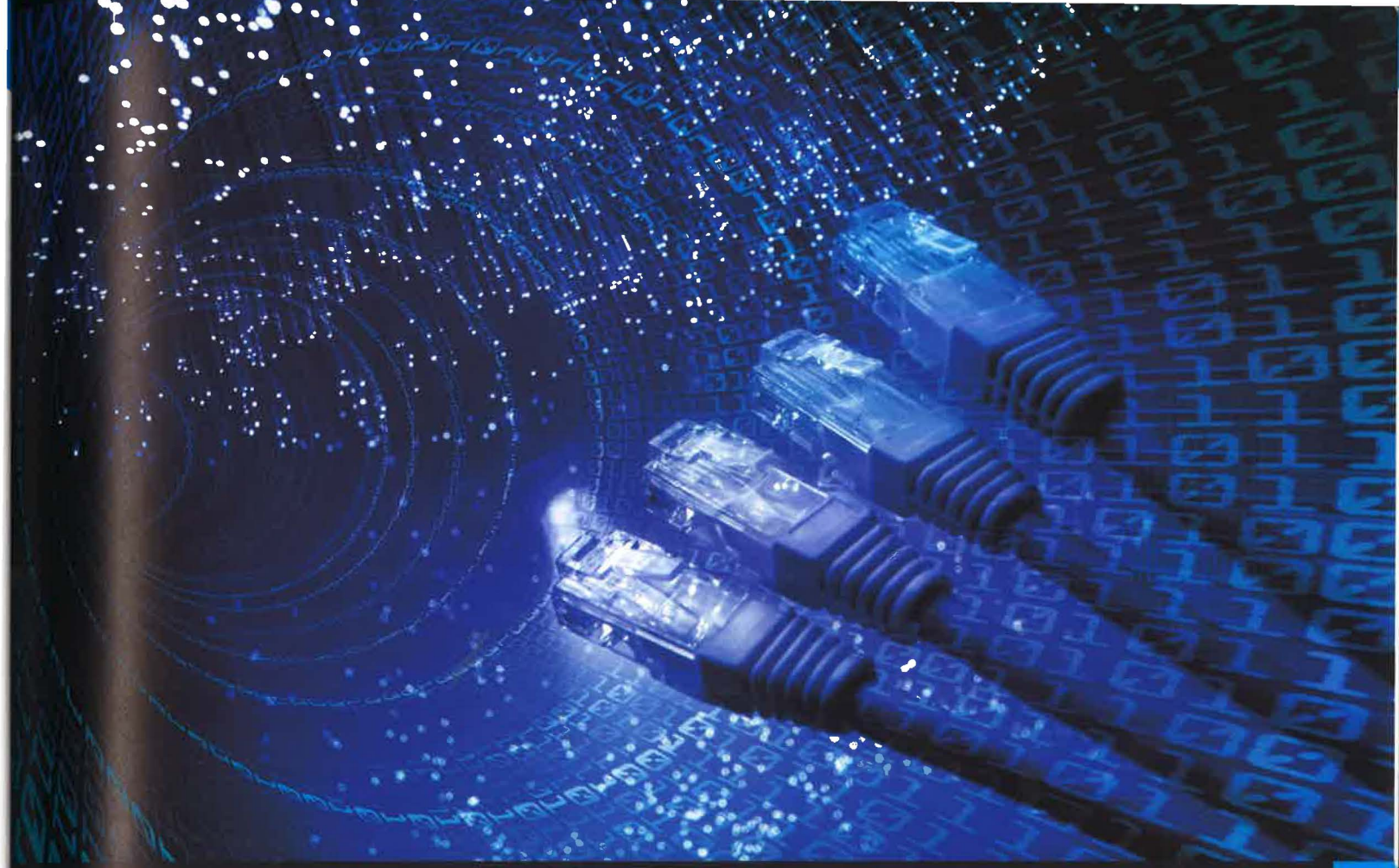


Chapter 2:
Communication and Internet Technologies

Learning objectives

By the end of this chapter you will:

- understand what is meant by transmitting data and be able to distinguish between serial and parallel transmission, as well as simplex, duplex and half-duplex transmission
- understand and be able to describe different methods of error checking and error detection
- understand the security risks that can arise when using the internet and how they can be minimised
- be able to explain how antivirus and protection software help to protect a user from security risks
- understand the role of the internet browser and internet service provider (ISP)
- understand HTML structure and presentation and what is meant by HTML and hypertext transfer protocol
- understand the concepts of MAC addresses, internet protocol address, uniform resource locator and cookies.

Byte Nibble bit

2.01 Data transmission

SYLLABUS CHECK

Show understanding of what is meant by transmission of data.

B = Byte b = bit

KEY TERM

Bit – short for binary digit, it is the smallest unit of data in a computer.

Bit rate – the rate at which data is transferred.

The transfer of data occurs either wirelessly by radio waves or over a cable, for example by fibre optic cable or copper twisted wire. The data is transmitted as a stream of **bits**. There are a number of differing methods that can be used to transfer the data.

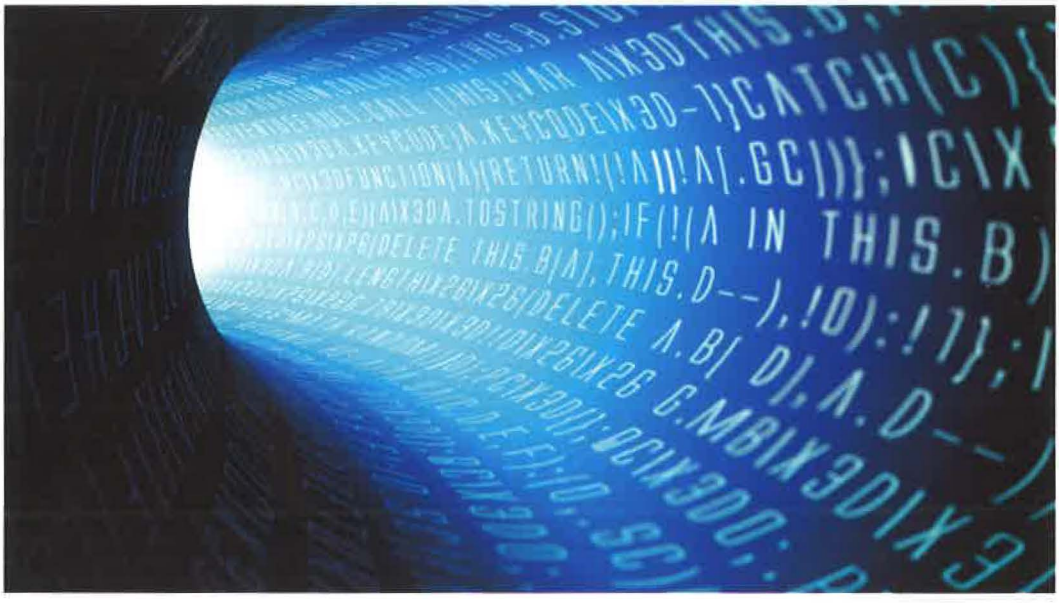


Figure 2.01 Transfer of data

The rate at which the transfer of data occurs is called the **bit rate**. This is the number of bits that can be transmitted in a given period of time. Bit rate is measured in bits per second (bps) or now more commonly in megabits per second (Mbps). The more megabits per second a data transfer connection is capable of, the quicker the data can be transferred. For example, a broadband connection that has a bit rate of 50Mbps will allow data to be transferred quicker than a broadband connection of 25Mbps.

number of bits sent per second * (bps)

broadband fast internet connection

SYLLABUS CHECK

Distinguish between serial and parallel data transmission.

KEY TERM

Serial transmission – uses a single wire to transfer bits of data.

Parallel transmission – uses multiple wires to transfer bits of data.

Interference – disturbances that can occur in the signals when sending data that may corrupt it.

Serial vs parallel which is better?

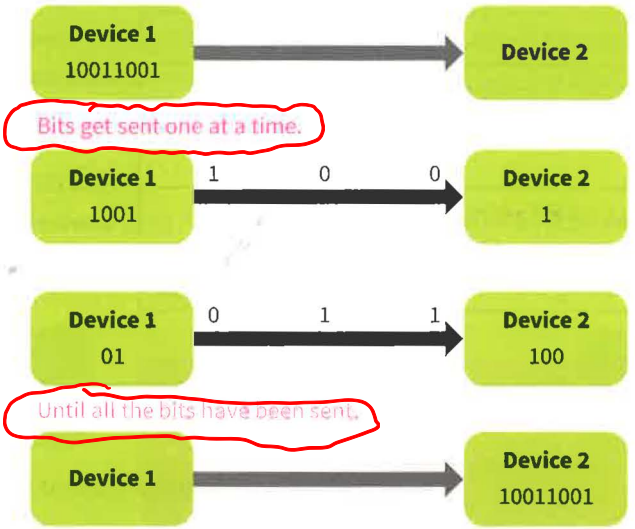
Serial data transmission

Serial transmission uses a single wire to transfer the data bits. A single wire is cheap to build and can transmit data over long distances. The bits are transmitted sequentially, one bit at a time. There is a set time interval between sending each bit. The time interval depends on the speed of the transmitting and receiving devices. For example, a 56K modem can transmit 57 600 bits per second.

Sequential - one bit at a time

Modem - used to send data
modulator-demodulator

If we consider the 8-bit byte of data 10011001, using serial data transmission the byte would be transferred as shown in Figure 2.02.



longer distance

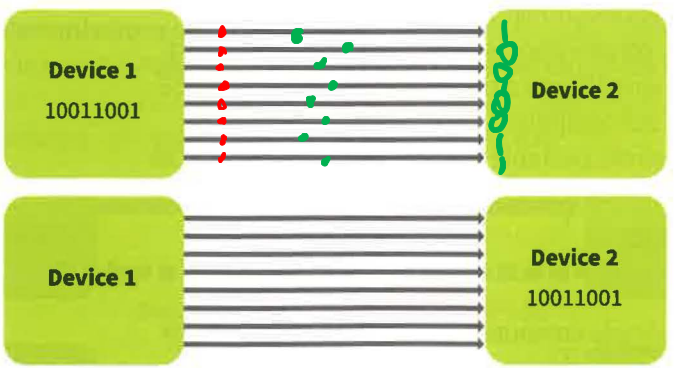
Figure 2.02 8-bit byte of data using serial data transmission

Parallel data transmission

Parallel transmission uses several wires to transfer the data bits simultaneously. For example, with eight wires, 1 byte (8 bits) could be transmitted all at once. Parallel transmission transfers data quicker than serial transmission. However, because there are more cables, parallel transmission is more expensive and is therefore limited to shorter distances.

Simultaneous
All at the same time

If we consider the same 8-bit byte of data 10011001, using parallel data transmission it would be transferred as shown in Figure 2.03.



Quicker ✱
short distances
expensive

Figure 2.03 8-bit byte of data using parallel data transmission

The byte is sent over multiple wires simultaneously. All bits of the byte are received at the same time.

We can compare the use of serial transmission to parallel transmission:

Table 2.01

Serial transmission	Parallel transmission
Used over long distances	Used over short distances
Uses a single wire	Uses multiple wires
Reduced costs as only single wire needed	Increased costs as multiple wires needed
Slower transmission as data is only transmitted one bit at a time over a single wire	Quicker transmission as data is sent simultaneously over multiple wires
Safer transmission as it is easier to accurately collate the bits together as they are sent one at a time	Less safe transmission as bits are sent simultaneously and errors can occur in collating them together at the receiver's side

SYLLABUS CHECK

Show understanding of the reasons for choosing serial or parallel data transmission.

Identify current uses of serial and parallel data transmission, such as Integrated Circuits (IC) and Universal Serial Bus (USB).

Parallel transmission is quite simple to implement but, because it has multiple wires, **interference** can occur between them. It is because of the level of interference between wires that it is generally limited to short distances of around 5 metres. The same level of interference does not occur with serial transmission as it is only one wire and so the distance of serial transmission can be much further, up to 100 metres.

Interference is an issue
5 metres
100 metres

For many years, parallel transmission was used for data transfer between computers and printers. This is because printers needed data quickly and were generally placed next to computers. Today, parallel transmission has largely been replaced by high-speed serial transmission methods such as the Universal Serial Bus (USB), which transmits data much quicker than parallel transmission. However, this speed comes at a much higher cost and greater level of complexity. We use USB to connect electronic devices to a computer, for example our mobile phones and tablet devices. We can also use it to connect our keyboard and mouse to our computer. To do this we will normally use a USB cable that will have a USB plug. This USB plug will plug into a USB port on our computer. USB is also used in storage devices, for example a USB flash drive. This is a small, portable storage device that has a USB plug to plug the device into the computer. USB can then be used to transfer the data from the computer to the storage device and vice versa.

USB widely used
flash drive
phones
Keyboard
Screen X
printer

To learn more about storage devices see Chapter 8.

Parallel transmission is still sometimes used in simple computers such as integrated circuits (IC) where low costs, simplicity and speed are important factors. We often refer to an IC as a microchip. They are used to create microprocessors, which are the small computers that are built into many of the devices we have in our homes, for example a washing machine or a microwave. As ICs are generally built into devices there is little chance for interference to

IC = micro chip = integrated circuit

occur and the device can be controlled very quickly through the use of parallel transmission. The internal components of a computer use parallel data transmission to operate.

In order for any data to be sent by serial transmission it needs to be converted. Data is converted from parallel to serial at the sender's side, to be transmitted over a single wire. It is then converted back from serial data to parallel to be processed by the receiver's device. The direction in which the data is transmitted can also vary.

stop here

KEY TERM

Simplex transmission – sending data in one direction only at a time.

Duplex transmission – sending data in both direction at the same time.

Half-duplex transmission – sending data in both directions but only one direction at a time.

Simplex transmission

In **simplex transmissions** data is sent in one direction only. Think of it as a one-way street where traffic can only drive in one direction down it. An example is a television broadcast, where data is transmitted to receiving televisions.

Simplex - television broadcast

Figure 2.04 Simplex transmission

Full duplex transmission

In full **duplex transmissions** data is sent in both directions at the same time. An example is a telephone conversation where both people can speak to each other at the same time.

telephone conversation

Figure 2.05 Duplex transmission

Half-duplex transmission

In **half-duplex transmissions** data is sent in both directions but only one direction at a time. An example is a walkie-talkie (two-way radio): both people can speak to each other but only one person can speak at a time. Each person needs to hold down the talk button to speak and then needs to release it to hear the other person speak.

walkie talkie (two-way radio)

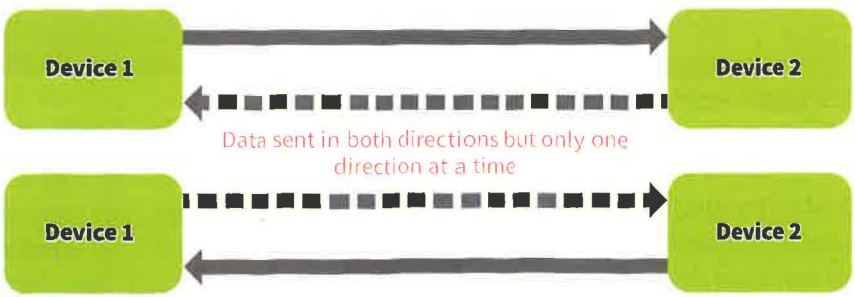


Figure 2.06 Half-duplex transmission

occur and the device can be controlled very quickly through the use of parallel transmission. The internal components of a computer use parallel data transmission to operate.

In order for any data to be sent by serial transmission it needs to be converted. Data is converted from parallel to serial at the sender's side, to be transmitted over a single wire. It is then converted back from serial data to parallel to be processed by the receiver's device. The direction in which the data is transmitted can also vary.

KEY TERM

Simplex transmission – sending data in one direction only at a time.

Duplex transmission – sending data in both direction at the same time.

Half-duplex transmission – sending data in both directions but only one direction at a time.

Simplex transmission

In **simplex transmissions** data is sent in one direction only. Think of it as a one-way street where traffic can only drive in one direction down it. An example is a television broadcast, where data is transmitted to receiving televisions.

Figure 2.04 Simplex transmission

Full duplex transmission

In full **duplex transmissions** data is sent in both directions at the same time. An example is a telephone conversation where both people can speak to each other at the same time.

Figure 2.05 Duplex transmission

Half-duplex transmission

In **half-duplex transmissions** data is sent in both directions but only one direction at a time. An example is a walkie-talkie (two-way radio): both people can speak to each other but only one person can speak at a time. Each person needs to hold down the talk button to speak and then needs to release it to hear the other person speak.

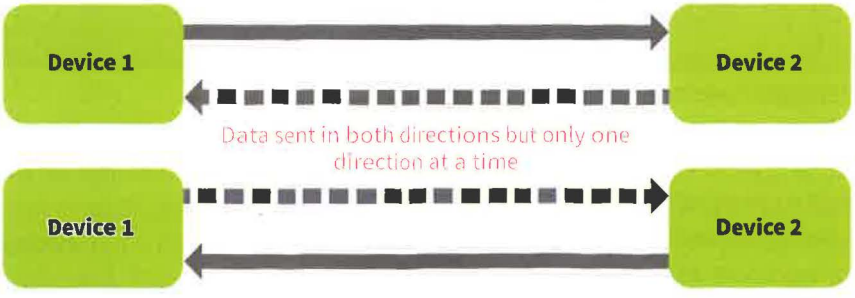


Figure 2.06 Half-duplex transmission

Different methods of data transmission can be combined. For example, a modern network uses serial duplex transmission whereas a walkie-talkie uses serial half-duplex transmission. A mouse uses serial simplex transmission. You can also get parallel simplex, parallel duplex and parallel half-duplex transmissions too.

choose transmission technique based on the device's needs.

SYLLABUS CHECK

Identify and describe methods of error detection and correction, such as parity checks, check digit, checksums and Automatic Repeat reQuests (ARQ)

Show understanding of the need to check for errors.

Explain how parity bits are used for error detection.

Error detection and correction

Errors can occur when transmitting and storing data. This is because the channels that are used to transmit the data can be subjected to disturbance. These errors can lead to inaccuracies in the data and make the data unreliable. This is something that we want to avoid, so we use methods of error detection and error correction to increase the accuracy and reliability of the data.

Ensure data is reliable
Avoid errors

10100100

Checksum

A checksum is a simple method of error detection. The number of bits being transmitted is counted up and this numeric count is transmitted with the data. The receiver can then see if the same number of bits has arrived. If the counts match then the receiver knows a full transmission of the data has been received.

count bits and transmit number
count at Rx if matches OK

Parity check

A parity check uses a parity bit to make sure that that the data has been sent accurately. Data is sent in bytes, normally made up of 8 bits. In a parity check, the first 7 bits of the byte are the data itself, the last bit is the parity bit. A parity check can use odd parity or even parity. All the bits are added together in the byte and depending on whether odd or even parity is being used a 1 or a 0 will be added as the finally parity bit.

If we use the example 1001100, using an even parity check, the parity bit would be a 1:

$$1 + 0 + 0 + 1 + 1 + 0 + 0 = 3$$

As 3 is an odd number we need to add 1 to it to make it even. This is why, when using even parity, the parity bit for this byte will be a 1.

Using the example 1001100 and an odd parity check, the parity bit would be a 0:

$$1 + 0 + 0 + 1 + 1 + 0 + 0 = 3$$

As 3 is an odd number we need to add 0 to it to keep it odd. This is why, when using odd parity, the parity bit for this byte will be a 0.

The devices that the data is being transferred between will be set to check for even parity or odd parity before the data is sent. Parity check is a simple and effective method of error checking. It cannot detect though if disturbance has affected a byte that would still have the same odd or even calculation, but the bits themselves have changed. For example, even parity is being used, the byte 1001100 is being sent with parity bit of 1. If the byte arrived as 110100 with the parity bit of 1, no error would be detected by a parity check as the

what if it receives data and parity is correct but the data is still wrong

calculation of the bits is still even. Parity checking is also used on data that is stored as well as data that is transmitted.

Check digits

A check digit is a method of error detection that is used on identification numbers such as barcodes, ISBNs and bank account numbers. It is used to detect human error when entering these numbers. A calculation is performed using the digits in the identification number and a check digit added to the end of the number as a result. The computer will perform the same calculation and compare the result to the check digit. If the two match, it knows the number is correct.

ISBN
Bank account No
Bar code

ISBN-13 : 978-1108733755

error
7→9

check digit

Automatic repeat request

Automatic repeat request (ARQ) is a set of rules for error control when transmitting data. When the device receiving the data detects there is an error with a packet, it automatically sends a request to the device transmitting the data to resend the packet. This resend request will be sent repeatedly until the packet is received error free or a limited amount of resend requests is reached.

TEST YOURSELF

1 Explain the difference between serial and parallel data transmission.
2 Using an example, describe half-duplex data transmission.
3 Explain why parallel transmission is mainly only used over short distances.
4 Explain how a parity check detects errors.

2.02 Security aspects

SYLLABUS CHECK

Show understanding of the security aspects of using the internet and understand what methods are available to help minimise the risks.

There are various security issues that can be encountered when using the internet. The internet itself is a fairly insecure way of transferring data, so security has become a top priority for the everyday user as well as businesses and governments. Security issues can arise for many reasons; it could be when downloading a file, entering data through a web form or sending data via email.

*fishing
*Phishing

TEST YOURSELF

These are a few of the reasons, can you think of any others?

Hackers steal personal data

Good internet security is necessary to protect your personal details, financial details and transactions, as well as downloading and transferring lots of other data. If good internet security is not in place, not only would people's personal computers be attacked, by people such as **hackers**, but it could potentially bring a whole country's economy to a halt if business is affected. This section explains some of the risks you can encounter and how you can avoid them through the use of some good internet security methods.

Figure 2.07 Internet security

SYLLABUS CHECK

Show understanding of the internet risks associated with malware, including viruses, spyware and hacking.

KEY TERM

Hacker – a person who tries to gain unauthorised access to a computer or network.
Malware – a software program that is designed to damage or disrupt a computer.
Virus – a software program that is designed to corrupt a computer and the files on it.
Spyware – a software program that collects user's information through their internet connection.
Hacking – gaining unauthorised access to a computer or network.

French for bad
Mal Software

Malware

There are risks associated with using the internet that can be harmful to your computer such as **malware**. There are a number of different types of malware that you could encounter, for example viruses and spyware.

Programs that attack computers
Malware
Virus Spyware

Figure 2.08 Internet risks

Viruses

A **virus** is a program that is downloaded on to a computer without the user's knowledge or permission. It is designed to harm a computer and the files that are on it. The most common type of virus will replicate itself over and over until it bring your computer system to a halt. A virus is often spread through sharing files and attachments on emails.

The first known computer virus was called the Creeper virus. It was written by Bob Thomas at a technology company called BBN. The Creeper virus was a test program. It replicated itself and it displayed the message 'I'm the creeper, catch me if you can!' on every system it infected. It was not designed to harm any computers, just to be a demonstration of a computer application. Prior to this, self-replicating programs had not been demonstrated and it was the ability to self-replicate that gained it the name of the first computer virus. A correction program was written called Reaper that deleted the Creeper virus. No damage was left to a computer when the Reaper program was run.

virus happens through sharing files and clicking onto links in email attachments

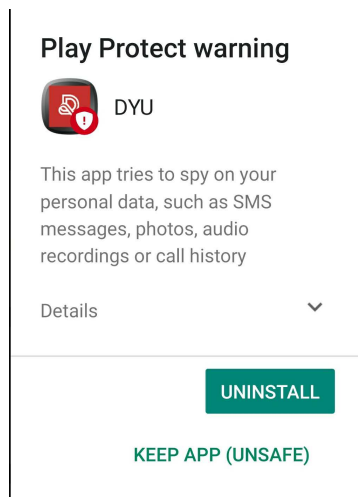
First known virus creeper virus

REPLICATES

Spyware

Spyware is software that is created to collect information on a user's computer use through their internet connection. The collection of the data is done without the user's knowledge or permission and it is collected normally to be sold on for marketing purposes. It can also gather information such as passwords, bank details and credit card details. These details can then be used to steal the user's identity. Spyware is created by people who want to obtain this data to use it unlawfully. It is often downloaded from untrustworthy websites without the user's knowledge. The spyware hides inside the data downloaded and infects the computer without the user being aware of the action.

As well as collecting information on the user without permission, spyware will also take up some of the bandwidth available for a user's internet connection as it passes back collected information. As a result it can reduce the bandwidth available to the user.



Hacking

As well as the risks above users can also be exposed to **hacking** when using the internet. A hacker is someone who tries to gain unlawful access to a computer or a network by writing a program that will do this. Hackers normally look for a weakness in the setup of a network or computer system and use this as a way to enter. They do this for a number of reasons, such as they may be trying to gain access to money, create a challenge for themselves or it could possibly be out of protest for an issue they want to see highlighted.

A hacker is usually classified as a 'white hat hacker' or a 'black hat hacker'. A white hat hacker exposes security issues in a network or system, but not for unlawful reasons. A white hat hacker can be hired by an organisation to test its own systems to discover any weaknesses that exist. This way those weaknesses can be fixed. White hat hackers are sometimes also known as ethical hackers. A black hat hacker is a hacker that gains access unlawfully.

To learn more about the security issues that can be encountered when using a computer and the internet see Chapter 9.

Hacker- creates a program that will unlawfully gain access to your computer

Protecting against the risks

SYLLABUS CHECK

Explain how anti-virus and other protection software helps to protect the user from security risks.

KEY TERM

Firewall – a system that protects unauthorised access to or from a computer or network.

Norton

It is possible to protect your computer from attacks that can arise from various issues encountered when using the internet. Anti-virus software can be used to detect a virus attack on a computer system. The anti-virus software will scan the computer's hard disk for any virus attacks and it will remove any that it finds. New viruses are constantly being developed so most anti-virus software will have an update function built into them. This means that when a new virus is discovered, the anti-virus software developers can release an update for computers to detect it

Anti virus detects an attack Does not prevent

As well as detecting viruses, anti-virus software can be used to detect and remove further malware and spyware. Anti-virus software cannot prevent an attack happening to a computer system, but they can detect it as it is happening and remove the harmful programs. To detect an attack normally a scanning process has to take place. The software scans the computer's hard drive for any viruses. If detected, a virus is removed from the system.

Firewalls are used to monitor transmissions coming into and transmissions going out of a computer or network. Firewalls can be hardware based or software based. Hardware based firewalls are more difficult to compromise but are expensive, whereas software firewalls are cheap, can be easily updated, but can be disabled by a virus.

Firewalls monitor incoming and outgoing traffic to a network

A firewall uses rules to determine whether an inbound or outbound transmission should be allowed. Some rules, for example those governing email transmission, are determined by the system. Others, such as transmissions for online multiplayer games, can be determined by the user. The firewall allows authorised transmissions to take place, but blocks any transmission that does not conform to the set rules.

Set rules to prevent unwanted traffic

Spyware sends outbound transmissions containing stolen data to scammers. Hackers use inbound transmissions to gain access to computers via the internet. Firewalls block these transmissions, thereby protecting the computer.

You can learn more about how to protect against security risks when using the internet in Chapter 9.

TEST YOURSELF

1 Describe how a firewall protects a computer or a network.
2 Explain the difference between a virus and spyware.
3 What is hacking?

2.03 Internet principles of operation

SYLLABUS CHECK

Show understanding of the role of the browser and internet server.

Modem – Modulator – demodulator

KEY TERM

Modem – a hardware device that converts data so that it can be transmitted from computer to computer over telephone wires.

Browser – a program used to access the World Wide Web that displays HTML files.

Packet – a unit of data that can be sent across a network.

Protocol – an agreed format or set of rules to transmit data.

- Firefox
- Edge
- Internet Explorer
- Chrome
- Apple's browser

http:// ← protocol hyper text transfer protocol

Internet service provider ISP

The internet is a global wide area network (WAN) of interconnected computers and devices. To access the internet we normally need an internet service provider (ISP). An ISP is a company that provides us with access to the internet, normally for a fee. We then use a **modem** to connect our computer to the internet, using the connection provided by the ISP. An older style of connection to the internet that can be used is called a dial-up connection. Dial-up connections use only telephone lines to connect to the internet. They are a cheaper way to connect to the internet, but they are very slow. People or businesses in very remote areas often use dial-up connections as they may not have the cabling in place to use broadband. An alternative way to access the internet is broadband. Broadband connections use different cabling to telephone wires, such as fibre-optic cables. They allow a much quicker speed of access to the internet than dial-up connections.

WAN

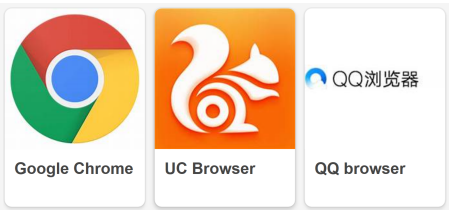
56 Kbps
5mbps
100mbps

ISPs will have terms of service that a customer will need to adhere to when using the internet. Terms of service are the rules that a customer must follow when using the service from the ISP. They will normally detail any limitations of the service, such as the amount of data a customer can download. It will also cover any legal issues such as using the service for hacking. An ISP will often allow a customer to personalise access to the internet, such as setting a filter that will prevent access to any underage websites.

Internet browser

A website consists of one or more pages of information that can be accessed by other computers on the internet. These pages are known as webpages. A **browser** is a program that allows the computer user to visit, retrieve and display the information that a webpage contains. Content is presented to the user in the form in which it is provided, such as text, images, video and sound. Some forms of content, such as animation, cannot be presented without the use of additional software known as a plugin. Not all plugins work with all browsers.

What we use to access the Internet
Browser able to handle most content



Animations and some programming languages need additional software
Plugins

Figure 2.09 Accessing information across computers on the internet

Figure 2.10 Accessing information across computers on the internet

Earl- English name

URL

Input into the browser address space

URL = uniform resource locator

To access a website, the user inputs the website's web address into the browser. This address is known as the site's uniform resource locator (URL). The URL is translated into the unique internet address of the web server that hosts the website. The browser accesses the website determined by the URL and downloads the content. Browsers also allow the user to navigate to different webpages on the website and to other websites via the use of hyperlinks.

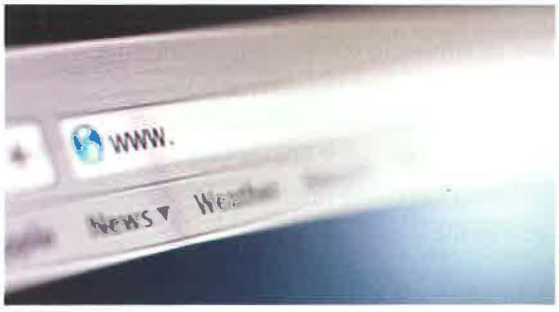


Figure 2.11 Web address bar

URL is a simplified form of an IP address

uploading server downloading

Web server

A computer that hosts a website is known as a web server. A web server may host many websites. The webserver stores each page of the website and its related content. Retrieving information from a web server is known as downloading. Sending information to a website is known as uploading. A computer that accesses information from a webserver is referred to as a client.

Storage of Web sites and Webpages

Accessing a website is known as a request. Web servers are designed to handle many requests from many clients simultaneously. Requested information is downloaded from a web server in **packets**. Since each packet consists of only a few bytes, many packets can be sent to many computers in a very short space of time. This means the more bandwidth a web server has access to, the more requests it can handle simultaneously.

Web server

store data
streaming
Gaming
Websites
email

As well as hosting websites, web servers are also used to manage facilities such as data storage, online multiplayer gaming and email. Many organisations use web servers on their local area networks to handle email and access to data. Such web servers can only be accessed by a computer on the local area network, making them private.

Although extremely powerful web servers are used to host popular and heavily visited websites, a computer of comparatively limited performance, such as the Raspberry Pi or Arduino, can act as a website host. However, the more limited the web server, the fewer the number of requests it can handle over a given period of time.

TIP

The Raspberry Pi and Arduino are very small computers that can do most of the tasks performed by a desktop computer. They are not as powerful as a desktop computer, but are great for use in projects such as creating a basic web server.

Even powerful web servers are limited in the number of requests that can be handled, leading to website crashes when too many people try to access the website at once. A good example of this is when tickets are released online for music festivals or sporting events. In these instances the web servers are often unable to handle the number of requests being made.

Furthermore, web servers can be forced offline through what are known as distributed denial of service (DDOS) attacks. With this type of attack, hackers flood the web server with millions of requests. The web server comes to a halt trying to satisfy so many requests simultaneously.

Internet protocols

SYLLABUS CHECK

Show understanding of what is meant by hypertext transfer protocol (http and https) and HTML. Distinguish between HTML structure and presentation.

Hypertext transfer protocol (http) is the core **protocol** that governs transmission of data via the internet. It is an access protocol. Http works as a request–response action. This means that a client (a computer or other device) makes a request that a web server responds to. For example, when visiting a website the client requests, via http, that the information on the website be made available to it. The web server responds by transmitting the website data via http to the client computer.

The actual transfer of the information is governed by another protocol. This is known as the transmission control protocol (TCP). TCP handles the transfer of the data and also checks to ensure the transmission is error free.

Although http is widely used for internet communication, the messages it sends are not particularly secure, making it unsuitable for applications such as banking or internet shopping, where private customer and financial data may be intercepted. Instead, a secure version of http known as https is used. Https encrypts the messages making them extremely difficult to understand by anyone other than the intended recipient that might intercept them.

Figure 2.12 Start of a https address

Mark-up language

The transmission a client computer receives from a web server is often in the form of a hypertext mark-up language (HTML) document. An HTML document consists of two parts: the content to be displayed and instructions on how to interpret that content. The language used to convey these instructions consists of mark-ups. Mark-ups are instructions on how content is to be formatted, structured and displayed by the browser. The term originates from the publishing industry where editors would mark-up paper documents from authors with corrections or suggestions. The mark-ups are read and interpreted by the browser, but not displayed.

Mark-ups in HTML take the form of tags. Content that requires formatting in some way is tagged. Tags enclose the content, with an opening tag <> at the beginning of the content and a closing tag </> at the end. Example formatting tags are shown in Table 2.02.

Table 2.02

Opening tag	Tag contents	Closing tag	Output
	emboldens the text		**emboldens the text**
<h1>	sets the text as a heading in a large font	</h1>	sets the text as a heading in a large font
<a>	defines a hyperlink		defines a hyperlink
	sets a new paragraph		sets a new paragraph

Hypertext is text that conveys information and also contains a link to other information, such as another webpage, website, picture, video or sound file. Contained within the hypertext is a hyperlink that is the URL of the additional content. Hyperlinks are named as such because they allow the user to go directly to the linked resource, simply by clicking on the hypertext.

Cascading style sheets

When creating websites, it is usually preferable to separate content and structure from presentation. This is because of the dynamic nature of the internet where many organisations refresh the look and style of their websites on a regular basis to maintain audience interest. However, in many cases the actual content remains the same. By separating the style from the content, the style can easily be changed without having to also change the content and vice versa. Styling mark-up instructions are placed in a separate document known as a cascading style sheet (CSS). Once created, the style sheet can be applied to any HTML document and the document will have its contents presented in the format stated by the style sheet's mark-up instructions.

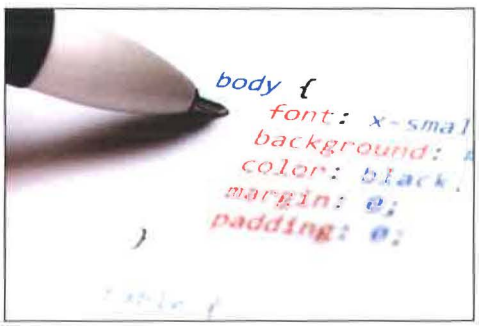


Figure 2.13 Cascading style sheet (CSS) sample

Cascading style sheets have huge benefits for website designers, as all the pages of a site can be quickly and uniformly updated simply by changing the mark-up instructions in the style sheet. Each HTML page provides the content and structure and the CSS specifies the presentation.

An HTML document is structured into two elements, the header and the body (see Figure 2.14). The header declares the document type (HTML), the page title, and any special instructions for the page, such as plugins to be used or scripts to be run. Additionally, the header includes any CSS that are to be used on the page and where to locate them.

The body contains the content to be displayed, hyperlinks to other pages and if a CSS is not used, any formatting instructions for the content.

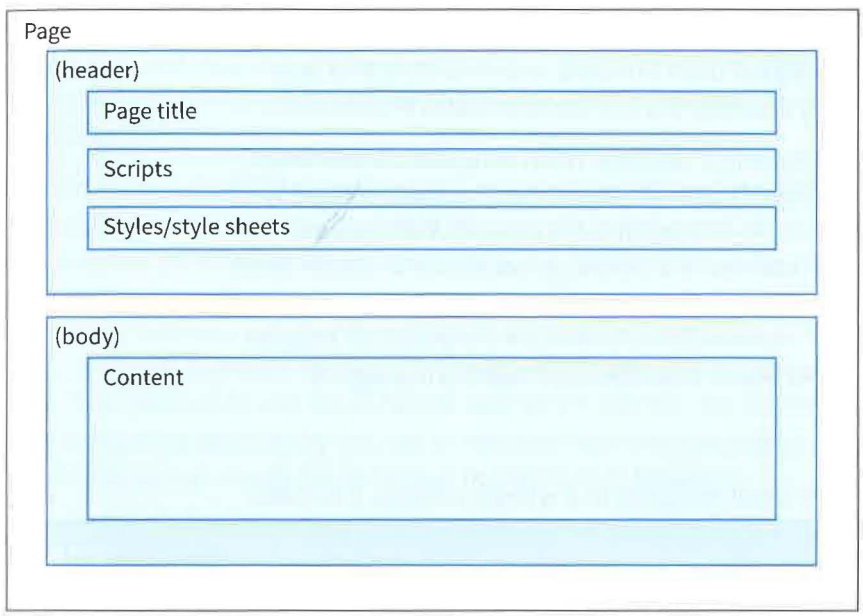


Figure 2.14 HTML document structure

Internet addresses

SYLLABUS CHECK

Show understanding of the concepts of MAC address, Internet Protocol (IP) address and cookies.

IP address

Networks and the internet use the transmission control protocol (TCP) for communication. Each device on a network has an address. Just like a house has an address, each device needs an address so that other devices know how to reach it. Without an address other devices would not be able to communicate with the device, as the TCP would not know where to send the communication. The device's network address is known as its internet protocol address (IP address).

Each IP address consists of a 32-bit code. For ease of use, this code is broken down into four groups of three digits, each group being in the range 0 to 255. For example, the IP address of a router on a network could be 192.168.001.255.

In binary, this code would be represented in 32 bits: 11000000101010000000000111111111.

Table 2.03

Denary	Binary
192	11000000
168	10101000
1	00000001
255	11111111

This version of IP addressing is known as IPv4.

Every device connected to the internet has an IP address. As the number of devices connected to the internet has grown, the number of available IP addresses has dramatically decreased. To overcome this a newer version of IP addressing has been launched, known as IPv6. IPv6 uses 128 bits to assign addresses. This has greatly extended the number of available IP addresses.

A device can be assigned either a static or a dynamic IP address. When using static IP addresses, each device is assigned a fixed (static) IP address. The device retains that IP address unless it is changed, even if the device is disconnected and re-connected to the network. With dynamic addresses, the device retains the assigned IP address for a limited period, known as a lease. When the lease period is up, the device is either re-assigned the same address, or assigned another. Additionally, when a device disconnects then reconnects to the network the previously assigned address may have now been taken by another device, so a different IP address is assigned.

Uniform resource locator

A uniform resource locator (URL) is what we could recognise as a website address. It is made up of the access protocol (http or https) and a domain name, for example amazon.com. This URL would be https://www.amazon.com. When visiting a website on the internet, we usually type the website's URL into our browser. The URL is translated by a special type of web server, known as a domain name server, into the 32-bit binary IP address. A URL is far easier for a user to remember than a 32-bit binary number. It also allows an organisation to personalise its web address with the organisation's name.

Figure 2.15 Web address bar

MAC address

Each device on the network also has another address, which is known as its media access control address (MAC address). The MAC address uniquely identifies each device. This address is assigned by the device's manufacturer, unlike an IP address which is assigned by the network. Additionally, the MAC address cannot be changed, unlike a device's IP address. This means a device can be identified, even if its IP address has changed. A MAC address consists of six pairs of two-digit hexadecimal numbers, which are translated into a 48-bit binary code for use by the computer. For example the MAC address 1a2f08a1234c would be 000110100010111100001000101000010010001101001100 in binary (see Table 2.04).

Table 2.04

Hexadecimal	Binary
1a	00011010
2f	00101111
08	00001000
a1	10100001
23	00100011
4c	01001100

Cookies

Cookies are tiny pieces of data that are downloaded by a computer when it visits a website. Cookies are stored by the computer's browser and are accessed by the website whenever it is visited by the client.

Cookies perform various essential tasks. Some are designed to help keep track of whether or not a user has logged in to secure websites, whilst others store dynamic data such as the items the user has added to an online store's shopping basket. Without cookies these facilities would not be available. However some cookies are used for purposes that can raise concern. Some websites use cookies to track a user's internet surfing activities and then tailor online adverts to match the user's interests. Others are used to store sensitive information such as passwords and credit card details, which can then be accessed at a later date. Cookies can be declined by the user or removed from the computer if the user has concerns. Both actions can usually be performed by the device's browser.

Summary

- Data can be transmitted in different ways, along a single wire as serial transmission or multiple wires as parallel transmission. Data can also be transmitted in different directions, in one direction at a time as simplex transmission, both directions at a time as duplex transmission, or in both directions but only one direction at a time as half-duplex transmission.
- Errors can occur when transmitting data so there are methods for error detection and correction, such as parity checks, check digit, checksums and Automatic Repeat reQuests (ARQ)
- Security risks such as malware, including viruses, spyware and hacking can arise when using the internet. These risks can be minimised through the use of software and hardware such as anti-virus software and firewalls.
- An ISP is a company that provides a connection to use the internet, normally for a fee.
- A browser is a program that allows a user to visit, retrieve and display the information that a webpage contains. A computer that hosts a website is called a web server. https is a more secure version of http used for banks, shopping and other sites that need added security in transmitting personal information.
- HTML is the language that webpages are written in. An HTML document consists of two parts, the content to be displayed and instructions on how to interpret that content. The instructions on how to display the content is done through the use tags known as mark-ups.
- Each computer or device has a unique address called a MAC address. This is an address that is fixed to that device and cannot be changed. When using the internet, each computer or device is assigned an IP address, which can be static or dynamic.
- We use a URL to access a website. It is normally typed into the address bar of a computer and is made up of the access protocol and the website domain name.
- Cookies are tiny pieces of data that are downloaded by a computer when it visits a website. Cookies are stored by the computer's browser and are accessed by the website whenever it is visited by the client.

Exam-style questions

1 Explain what is meant by bit rate. (3 marks)

2 Describe two advantages of serial data transmission. (2 marks)

3 Draw a line to match the error detection and correction terms to the correct definitions: (4 marks)

Check digit	The number of bits transmitted are added up and this calculation is transmitted with the data
Parity check	A 1 or a 0 is added as an extra bit to make the sum of the bits in a byte odd or even
Checksum	A digit added when transmitting data from a calculation performed on the digits in the data
Automatic repeat request	A request that is sent by the receiving device to tell a sender that there is an error in the data being received

4 Explain how anti-virus software protects a computer. (2 marks)

5 Sami wants to access a website that sells his favourite records. Explain how Sami will do this. (2 marks)

6 The Rock Factory uses a CSS to store the formatting instructions for their website. Explain what the advantages are for doing this. (2 marks)

7 Describe the difference between a static IP and a dynamic IP. (4 marks)

8 Why can the use of cookies raise concern for an internet user? (6 marks)