Chapter 17
Communication and Internet Technologies

Learning objectives

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

- show understanding of a bus or star topology network
- show understanding of circuit switching and where it is applicable
- show understanding of packet switching and explain how it is used to pass messages across a network
- explain how hardware is used to support a LAN
- show understanding of why a protocol is essential for communication between computers
- show understanding of how protocol implementation can be viewed as a stack
- show understanding of the function of each layer of the TCP/IP protocol suite and the application of the suite when a message is sent from one host to another on the internet
- show understanding of the function of a router in packet switching
- show awareness of other protocols (HTTP, FTP, POP3, SMTP) and their purposes
- show understanding of Ethernet and how collision detection and avoidance works
- show understanding of how the BitTorrent protocol provides peer-to-peer file sharing
- show understanding of a wireless network.

17.01 Isolated network topologies

There are five requirements for a data communications system: a sender, a receiver, a transmission medium, a message and a protocol. Here, a 'message' is a general term to describe any type of transmitted data. A message can only be transmitted if there is an agreed protocol. Protocols are discussed in later sections of this chapter.

A data communications system may consist of an isolated network. There are several possible topologies for an isolated network. The simplest possible network is where two end-systems are connected by a network link as shown in Figure 17.01. This is an example of a point-to-point connection for which there is a dedicated link.

Figure 17.01 A point-to-point network

A bus topology also 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 17.02. This configuration has a major difference in that there is no direct connection between any pair of end-systems.

Figure 17.02 A bus network

A ring topology is shown in Figure 17.03(a). In this configuration, each end-system has a point-to-point connection to the two adjacent end-systems.

An example of a fully-connected mesh topology is shown in Figure 17.03(b). In this configuration, each end-system has a point-to-point connection to each of the other end-systems.

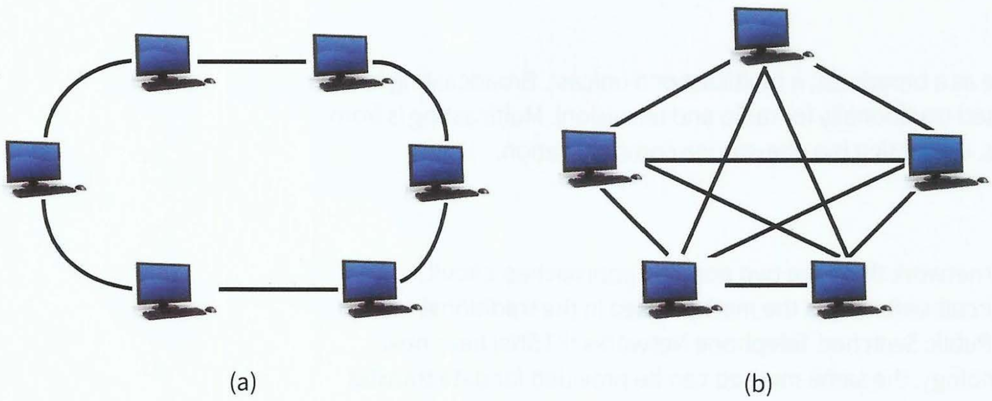

Figure 17.03 (a) A ring network and (b) a mesh network

The final possibility is a star topology which is shown in Figure 17.04. This could have been drawn so that it looked like a star but it is better drawn to represent the physical configuration that is used in an actual installation. In a star topology, each end-system has a point-to-point connection to the 'central' device.

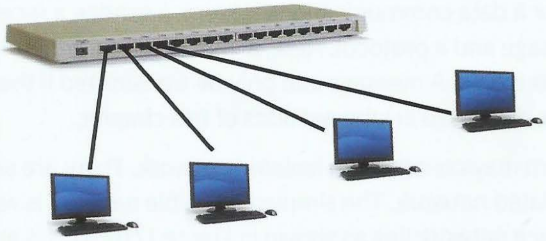

Figure 17.04 A star topology

The ring and bus topologies were used in early networks. Most of the end-systems would have been user workstations; the others would have been servers. With regard to the end-systems the same applies to a fully-connected mesh network but this was never a realistic configuration because of the amount of cabling required.

In the star topology, the end-systems may again be user workstations or servers but the central device is different. The star topology is nowadays the dominant configuration for an individual 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. A specialised application is to use the star topology to function logically as a ring. With the appropriate software installed, each end-system can function as though it has just two directly connected neighbours.

Discussion Point:

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

17.02 Communication and transmission concepts

There are several concepts relating to the use of a network for communication and data transmission.

Data flow modes

The data flow along an individual link is simplex, half duplex or full duplex. In simplex mode the flow is one-way. In a duplex mode flow is both ways but only occurs simultaneously in full-duplex mode.

Message types

When a message is sent it can be as a broadcast, a multicast or a unicast. Broadcasting is a one-to-all communication (as used traditionally for radio and television). Multicasting is from one source to many destinations. Unicasting is a one-to-one communication.

Transmission modes

For communication over an internetwork there are two possible approaches: circuit switching or packet switching. Circuit switching is the method used in the traditional telephone system. Because the Public Switched Telephone Networks (PTSNs) have now largely converted to digital technology, the same method can be provided for data transfer rather than voice communication. Typically this is provided in a leased line service. The concept is illustrated in Figure 17.05, which shows end-systems connected to local exchanges which have a switching function and which are connected via a number of intermediate nodes with a switching function.

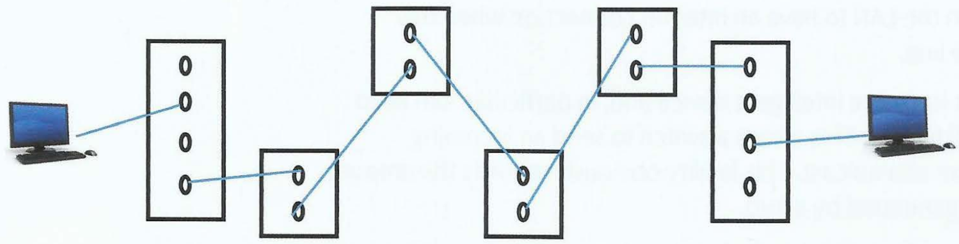

Figure 17.05 Circuit-switched data transmission

For data transfer to take place, the following has to happen:

1 The sender provides the identity of the intended receiver.
2 The system checks whether or not the receiver is ready to accept data.
3 If the receiver is available, a sequence of links is established across the network.
4 The data is transferred.
5 The links are removed.

It is not necessary for this discussion to define what could constitute a node in a circuit-switched network. The links that are provided between the nodes are dedicated channels in shared transmission media that guarantee unimpeded transmission. When a telephone call is made there is a definite end of the call with removal of the links. However, for a leased-line data connection there might be a permanent circuit established.

The packet-switching method allows data transmission without a circuit being established. Data cannot be sent in a continuous stream. Instead data is packaged in portions inside packets. A packet consists of a header which contains instructions for delivery plus the data body. The method is similar to that used by the postal service but rather more complex! The network schematic shown in Figure 17.05 is still appropriate to describe packet switching except that the links used are not defined at the time a packet is transmitted by the sender.

Packet-switching services

When packet switching is used there are two ways that the network can provide a service: connectionless service or connection-oriented service.

If a connectionless service is provided, a packet is dispatched with no knowledge of whether or not the receiver is ready to accept it. In a connection-oriented service the first packet sent includes a request for an acknowledgement. If this is received, the sender transmits further packets. If no acknowledgement is received the sender tries again with the first packet.

17.03 Hardware connection devices

An end-system on an Ethernet LAN needs a network interface card (NIC). Each NIC has a unique 'physical' address. This is sometimes referred to as the MAC address as explained in Section 17.06. The end-system itself has no identification on the network. If the NIC is removed and inserted into a different end-system, it takes the address with it.

The simplest device that can be used at the 'centre' of a star topology LAN is a hub. A hub ensures that any incoming communication is broadcast to all connected end-systems. However, the use of a hub is not restricted to supporting an isolated network. One possibility is to have a hierarchical configuration with one hub connected to other hubs, which support individual LANs. Another possibility is for a hub to have a built-in broadband modem. This allows all of the end-user systems on the LAN to have an Internet connection when this modem is connected to a telephone line.

A switch can function as a hub but it is a more intelligent device and, in particular, can keep track of the addresses of connected devices. This allows a switch to send an incoming transmission to a specific end-system as a unicast. This facility obviously reduces the amount of network traffic compared to that generated by a hub.

A router is the most intelligent of the connecting devices. It is in effect a small computer. It can function as a switch but the router can make a decision about which device it will transmit a received transmission to. As was mentioned in Chapter 2 (Section 2.04), the main use of routers is in the backbone fabric of the Internet. Nearer to the end-systems, a router may function as a gateway, as a network address translation box (described in Chapter 2 (Section 2.07)) or be combined with a firewall. There is further discussion of routers in Section 17.04.

17.04 The TCP/IP protocol suite

Protocols are essential for successful transmission of data over a network. Each **protocol** defines a set of rules that must be agreed between sender and receiver. At the simplest level, a protocol could define that a positive voltage represents a bit with value 1. At the other extreme, a protocol could define the format of the first 40 bytes in a packet.

> **KEY TERMS**
>
> **Protocol:** a set of rules for data transmission which are agreed by sender and receiver

The complexity of networking requires a very large number of protocols. A protocol suite is a collection of related protocols. TCP/IP is the dominant protocol suite for Internet usage. TCP/IP can be explained on the basis of the network model shown in Figure 17.06.

Figure 17.06 shows a stack of layers for the protocols where:

- Each layer except the physical layer represents software installed on an end-system or on a router.
- The software for each layer must provide the capability to receive and to transmit data in full-duplex mode to an adjacent layer.
- A protocol in an upper layer is serviced by the protocols in lower layers.

As a result, an application run on one end-system can behave as though there was a direct connection with an application running on a different end-system. To achieve this, the application layer protocol on the sender end-system sends a 'message' to the transport layer protocol on the same system. The transport layer protocol then initiates a process which results in the identical 'message' being delivered to the receiver end-system. Finally, on the receiver end-system, the transport layer protocol delivers the 'message' to the application layer protocol.

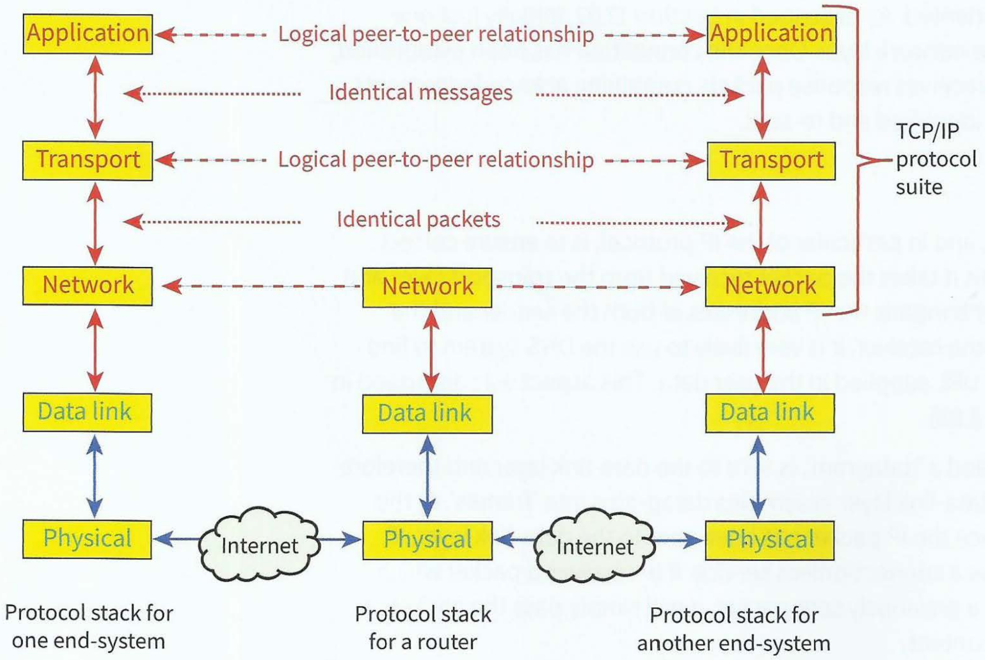

Figure 17.06 A network model relating to the TCP/IP protocol suite

The TCP/IP protocol suite only operates at the top three layers. The lower layers operate with a different protocol suite, such as Ethernet. A router has no awareness of the two highest layers.

The TCP/IP suite comprises a number of protocols, including the following:

- Application layer: HTTP, SMTP, DNS, FTP, POP3
- Transport layer: TCP, UDP, SCTP
- Network layer: IP, IGMP, ICMP, ARP

The selection has been chosen to illustrate that the TCP/IP suite encompasses a very wide range of protocols which is still evolving. Some of the listed protocols will not be considered further.

TCP (Transmission Control Protocol)

If an application is running on an end-system where a 'message' is to be sent to a different end-system the application will be controlled by an application layer protocol (see Section 17.05). The protocol will transmit the user data to the transport layer. The TCP protocol operating in the transport layer now has to take responsibility for ensuring the safe delivery of the 'message' to the receiver. To do this it creates sufficient packets to hold all of the data. Each packet consists of a header plus the user data.

As well as needing to ensure safe delivery, TCP also has to ensure that any response is directed back to the application protocol. Thus one item in the header is the port number which identifies the application layer protocol. For example, for HTTP the port number is 80. The packet must also include the port number for the application layer protocol at the receiving end-system. However, TCP is not concerned with the address of the receiving end-system. If the packet is one of a sequence, a sequence number is included to ensure eventual correct reassembly of the user data.

The TCP protocol is connection-oriented. As described in Section 17.02, initially just one packet of a sequence is sent to the network layer. Once the connection has been established, TCP sends the other packets and receives response packets containing acknowledgements. This allows missing packets to be identified and re-sent.

IP (Internet Protocol)

The function of the network layer, and in particular of the IP protocol, is to ensure correct routing over the Internet. To do this it takes the packet received from the transport layer and adds a further header. This header contains the IP addresses of both the sender and the receiver. To find the IP address of the receiver, it is very likely to use the DNS system to find the address corresponding to the URL supplied in the user data. This aspect was discussed in some detail in Chapter 2 (Section 2.08).

The IP packet, which is usually called a 'datagram', is sent to the data-link layer and therefore to a different protocol suite. The data-link layer assembles datagrams into 'frames'. At this stage, transmission can begin. Once the IP packet has been sent to the data-link layer, IP has no further duty. IP functions as a connectionless service. If IP receives a packet which contains an acknowledgement of a previously sent packet, it will simply pass the packet on to TCP with no awareness of the content.

The router

As Figure 17.06 shows, the frame sent by the data-link layer will arrive at a router during transmission (more likely at several routers!). At this stage, the datagram content of the frame is given back to IP. It is now the function of the router software to choose the next target host in the transmission. The software has access to a routing table appropriate to that router. The size and complexity of the Internet prohibits a router from having a global routing table. IP then passes the datagram back to the data-link layer at the router.

The distinction between a switch and a router was discussed earlier. A further point to note here is that when a frame arrives at a switch, it is transmitted on without any routing decision. A switch operates in the data-link layer, not in the network layer.

17.05 Application-layer protocols associated with TCP/IP

There are very many application-layer protocols. This discussion will consider only a few of the protocols that were introduced early in the use of TCP/IP.

HTTP (HyperText Transfer Protocol)

Because HTTP (HyperText Transfer Protocol) underpins the World Wide Web it has to be considered to be the most important application-layer protocol. Every time a user accesses a website using a browser, HTTP is used but its functionality is hidden from view.

HTTP is a transaction-oriented, client–server protocol. The transaction involves the client sending a 'request' message and the server sending back a 'response' message. The HTTP protocol defines the format of the message. The first line of a request message is the 'request line'. Optionally this can be followed by header lines. All of this uses ASCII coding. The format of the request line is:

```
<Method> <URL> <Version>CRLF
```

where CR and LF are the ASCII carriage return and line feed characters. The request line usually has GET as the method. However, there are several alternatives to the GET method which makes HTTP potentially a more widely applicable protocol than just being used for webpage access. The version has to be specified because HTTP has evolved so there is more than one version in use.

In Chapter 2 (Section 2.09), a sequence of events was described for when a browser accesses a webpage. This can now be presented as a sequence of protocol actions. The following is an abbreviated version:

1. HTTP transmits a request message to TCP.
2. TCP creates one or more packets and sends the first one to IP using port 80 for the destination port and a temporary port number for the sending port.
3. IP uses the URL in the message to get an IP address using DNS and sends a datagram.
4. At the server, IP forwards the datagram to TCP.
5. The server TCP sends an acknowledgement.
6. When a connection has been established, TCP sends the remaining packets, if any, to IP which then forwards them through the server IP and TCP to the server application layer.
7. HTTP transmits a response message which is transmitted via TCP, IP, IP and TCP to the client browser application.

All of this can happen with just one click on a bookmark item in a browser!

Email protocols

The traditional method of sending and receiving emails is schematically illustrated in Figure 17.07. It can be seen that three individual client–server interactions are involved. The client has a connection to a mail server which then has to function as a client in the transmission to the mail server used by the receiver.

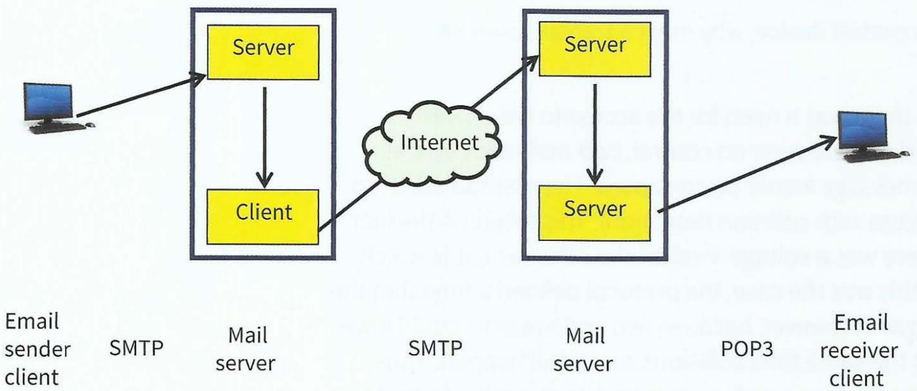

Figure 17.07 An email message being transmitted from a sender to a receiver

SMTP (Simple Mail Transfer Protocol) is a 'push' protocol. POP3 (Post Office Protocol version 3) is a 'pull' protocol. There is a more recent alternative to POP3, which is IMAP (Internet Message Access Protocol). IMAP offers the same facilities as POP3 but also a lot more.

This approach has been largely superseded by the use of web-based mail. A browser is used to access the email application, so HTTP is now the protocol used. However, SMTP remains in use for transfer between the mail servers.

FTP (File Transfer Protocol)

For routine transfers of files from one user to another the most likely method is to attach the file to an email. However, this is not always a suitable method. FTP (File Transfer Protocol) is the application-layer protocol that can handle any file transfer between two end-systems. File transfer can be less than straightforward if the end-systems have different operating systems with different file systems. FTP handles this by separating the control process from the data-transfer process.

17.06 Ethernet protocol

Ethernet is the other dominant protocol 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 (obviously one of many!) that took responsibility for the development of the protocol. The standard for a wired network is denoted as IEEE 802.3 which can be considered to be a synonym for Ethernet. The standard has evolved through five generations: standard or traditional, fast, gigabit, 10 gigabit and 100 gigabit. The gigabit part of the name indicates the transfer speed capability.

Ethernet transmits data in frames. Each frame contains a source address and a destination address. The address is the physical or MAC address, which uniquely defines one NIC, as described in Section 17.03. The reason that a unique address can be guaranteed is that 48 bits are used for the definition. The address is usually written in hexadecimal notation, for example:

4A:30:12:24:1A:10

Standard 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 in a connectionless service.

Extension Question 17.01

In a star topology LAN with a hub as the central device, why must a transmission be broadcast?

Because of the broadcast transmission, there was a need for the access to the shared medium by end-systems to be controlled. If there were no control, two messages sent at the same time would 'collide' and each message would be corrupted. The method adopted was CSMA/CD (carrier sense multiple access with collision detection). This relied on the fact that if a frame was being transmitted there was a voltage level on the Ethernet cable which could be detected by an end-system. If this was the case, the protocol defined a time that the end-system had to wait before it tried again. However, because two end-systems could have waited then both decided to transmit at the same time collisions could still happen. Thus there was also a need to incorporate a means for an end-system to detect a collision and to discontinue transmission if a collision occurred.

Although there might be some legacy standard Ethernet LANs still operating, the modern implementation of 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. Since collisions are now impossible, CSMA/CD is no longer needed.

Ethernet is the most likely protocol to be operating in the data-link layer defined in the TCP/IP protocol stack. Referring back to Figure 17.06, the diagram shows IP in the network layer sending a datagram to the data-link layer. When the data-link layer uses Ethernet, the protocol defines two sub-layers. The upper of these is the logical link-control layer, which handles flow control, error control and part of the framing process. The lower is the media access control (MAC) sublayer which completes the framing process and defines the access method. The MAC layer transmits the frames that contain the physical addresses for sender and receiver. This is the reason that these addresses are often referred to as MAC addresses.

17.07 Peer-to-peer (P2P) file sharing

The network traffic generated by peer-to-peer (P2P) file sharing has come to be a dominant feature of Internet usage. It is an architecture that has no structure and no controlling mechanism. Peers act as both clients and servers and each peer is just one end-system.

The BitTorrent protocol is the most used protocol because it allows fast sharing of files. There are three basic problems to solve if end-systems are to be confident in using BitTorrent:

- How does a peer find others that have the wanted content?
- How do peers replicate content to provide high-speed downloads for everyone?
- How do peers encourage other peers to provide content rather just using the protocol to download for themselves?

The answer provided by BitTorrent to the first question is to get every content provider to provide a content description, called a torrent, which is a file that contains the name of the tracker (a server that leads peers to the content) and a list of the chunks that make up the content. The torrent file is at least three orders of magnitude smaller than the content so can be transferred quickly. The tracker is a server that maintains a list of all the other peers (the 'swarm') actively downloading and uploading the content.

The answer to the second question involves peers simultaneously downloading and uploading chunks but peers have to exchange lists of chunks and aim to download rare chunks for preference. Each time a rare chunk is downloaded it automatically becomes less rare!

The answer to the third question requires dealing with the free-riders or 'leechers' who only download. The solution is for a peer to initially randomly try other peers but then to only continue to upload to those peers that provide regular downloads. If a peer is not downloading or only downloading slowly, it will eventually be isolated or 'choked'.

It is worth noting that the language of BitTorrent is somewhat esoteric and there are other terms used which have not been mentioned. Fortunately the principles are straightforward.

17.08 Wireless networks

All of the previous discussion in this chapter has related to transmission using a cable medium. In today's world, this is no longer the dominant technology. The following brief discussion considers four important examples of wireless technology discussed in order of increasing scale of operation.

Bluetooth

Bluetooth has been standardised as IEEE 802.15. Communication is by short-range radio transmission in a confined area. A Bluetooth LAN is an ad hoc network. This means that there is no defined infrastructure and network connections are created spontaneously. There is an almost limitless range of applications that use Bluetooth; some are very simple, such as using a wireless keyboard or mouse.

WiFi

WiFi (WLAN in some countries) is a term used by the public to describe what is sometimes called wireless Ethernet but is formally IEEE 802.11. This is a wireless LAN protocol which uses radio frequency transmission. Most often a WiFi LAN is centred on a wireless access point in an 'infrastructure' network (i.e. not an ad hoc network). The wireless access point communicates wirelessly with any end-systems that have connected to the device. It also has a wired connection to the Internet.

WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) or IEEE 802.16 is a protocol for a MAN or WAN. It is designed for use by PSTNs to provide broadband access to the Internet without having to lay underground cables. Local subscribers connect to the antenna of a local base station using a microwave signal.

Cellular networks

A mobile phone is often called a 'cell phone' because of the fundamental infrastructure provided for mobile phone users. This is illustrated in Figure 17.08.

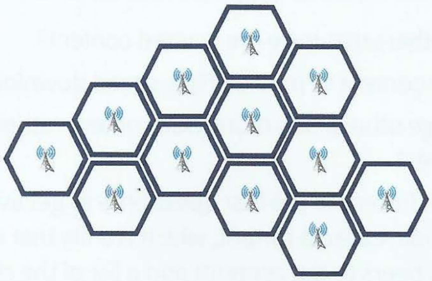

Figure 17.08 A collection of mobile phone cells

Each cell has at its centre a base station. The system works because each cell has a defined frequency for transmission which is different from the frequencies used in adjacent cells.

The technology available in a mobile phone has progressed dramatically through what are described as generations:

- 1G was designed for voice communication using analogue technology.
- 2G went digital.
- 3G introduced multimedia and serious Internet connection capability.
- 4G introduced smartphones with high-bandwidth broadband connectivity.

Summary

- Possible topologies for an isolated network are: single link, bus, ring, star or mesh.
- Circuit switching requires a dedicated circuit to be established between sender and receiver before transmission can start.
- In packet switching, packets can be transmitted without any circuit being created.
- Hardware network-connecting devices include network interface cards, hubs, switches and routers.
- The TCP/IP protocol suite is implemented as a layered stack.
- Examples of application-layer protocols are HTTP, SMTP, POP3 and FTP.
- The dominant LAN protocol is Ethernet.
- Peer-to-peer file sharing on the Internet uses the BitTorrent protocol.
- The four major wireless technologies are Bluetooth, WiFi, WiMAX and cellular networks.

Exam-style Questions

1 a There are five requirements for a data communication system. State the five requirements. [3]

b An isolated wired network is to be used as a data communication system.

i Draw two possible topologies. [2]

ii For each topology, explain why there is or is not direct point-to-point connections between the end-systems. [4]

c Each end-system is fitted with a network interface card (NIC).

i Explain why the NIC is needed. [3]

ii Explain what would happen if the NIC in an end-system was replaced by a newer version. [2]

2 One end-system with an Internet connection has a file. A user on another end-system connected to the Internet needs a copy of the file. There are different methods that might be used to enable the user to obtain a copy of the file.

a Identify three possible methods with a brief explanation for each. [6]

b Identify the application-layer protocols that each method will use with a brief explanation for each one. [8]

3 a Standard Ethernet is a term used to describe the original version of Ethernet.
CSMA/CD was a feature of standard Ethernet.

i Describe, with the aid of a diagram, a network topology that could be used with standard Ethernet. [3]

ii Describe the CSMA/CD method and explain its use. [4]

b Ethernet can be used in conjunction with the TCP/IP protocol suite.

i Draw a diagram to illustrate how the combination of Ethernet and the TCP/IP suite provides support for data communication. [5]

ii Explain the meaning of the term 'MAC address'. [3]