CHAPTER 4

Computer networks

In this chapter you will learn about:

- types of networks:
  - ring, bus, star and tree
  - local area networks (LANs), wide area networks (WANs) and wireless LANs (WLANs)
- network devices – modems, hubs and switches, routers and bridges
- the internet – web browsers and internet services providers (ISPs)
- intranets
- network security – user IDs, passwords, encryption and authentication techniques
- communications – fax, email, video conferencing and voice over internet protocol (VOIP).

4.1 Introduction

Most computer systems are now connected together in some way to form what is known as a **network**. This ranges from the basic school/home network of only a few computers (often set up to share resources such as printers or software) to large networks such as the **internet** which effectively allows any computer connected to it to communicate with any other computer similarly connected.

This chapter considers the types of networks that exist and the many features that are available because of networking.

4.2 Common types of network

Most networks are controlled by the use of **servers**. There are different types of servers, for example:

- **file servers**, which allow users to save and load data/files
- **applications servers**, which deal with the distribution of applications software to each computer
- **printer servers**, which ensure printing from devices on the network is done in a queue, for example
- **proxy servers**, which are used as a buffer between WANs (discussed at the end of this section) and LANs (discussed in Section 4.3).

This section will now describe a number of different types of networks.

Local area networks

A **local area network (LAN)** is usually within one building or certainly not over a large geographical area. A typical LAN will consist of a number of computers and devices (e.g. printers) which will be connected to **hubs** or **switches**. One of the hubs or switches will usually be connected to a **router** and **modem** (usually **broadband**) to allow the LAN to connect to the internet; in doing so it then becomes part of a **wide area network (WAN)**.

There are advantages of networking computers together using LANs:

- the sharing of resources (such as expensive peripherals and applications software)
- communication between users
- a network administrator to control and monitor all aspects of the network (e.g. changing passwords, monitoring internet use and so on).

However, there are also disadvantages:

- easier spread of viruses throughout the whole network
- the development of printer queues, which can be frustrating
- slower access to external networks, such as the internet
- increased security risk when compared to stand-alone computers
- the fact that if the main server breaks down, in most cases the network will no longer function.

There are four common types of LAN network **topologies**: ring, bus, star and tree networks.

Ring networks

Ring networks, shown in Figure 4.1, are becoming less popular. Every computer in the network is connected in a ring, including the server. Data is transmitted around the ring and each computer only removes the data which is relevant to it. This allows each computer to send and receive data since they all have a unique identification/address.

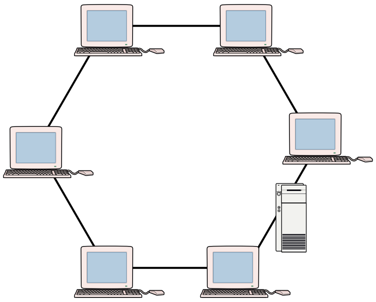

Figure 4.1 A ring network

Advantages

- Ring networks work well under heavy loading.
- It is possible to create very large networks using this topology.

Disadvantages

- If there is a fault in the wiring between two computers then the whole network will fail.
- Adding a new device or computer to the network can be difficult since it has to be placed between two existing devices.

Bus networks

In a **bus network**, illustrated in Figure 4.2, each computer or device is connected to a common central line. Data travels along this central line until it reaches the computer or device that requires it. The ends of the line have terminators to prevent, for example, signal bounce, which would cause data interference.

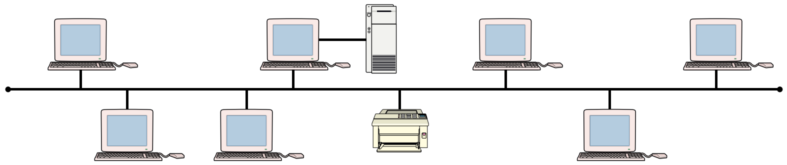

Figure 4.2 A bus network

Advantages

- It is easy to add a new computer or device to the network.
- If one device or computer fails, it does not affect the rest of the network.
- This type of network doesn't need a hub or a switch and also requires less cabling than, for example, a star network. It therefore also saves on costs.

Disadvantages

- It is difficult to isolate any fault on the network.
- If the central line has a fault then the whole network fails.
- This is becoming an increasingly outdated topology for network design.
- Its performance worsens noticeably as more and more devices/ computers are added.

Star networks

With a **star network**, shown in Figure 4.3, each computer or device is connected via a central hub or switch. Data is sent to the hub which then sends out data along *every* cable to every computer or device (no checking is done to see where the data should be sent).

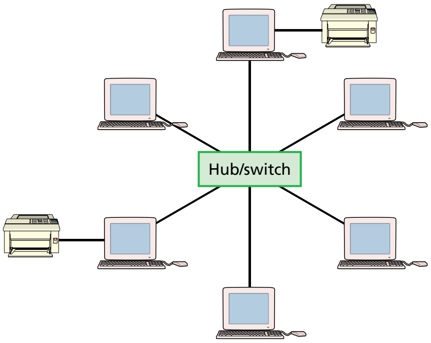

Figure 4.3 A star network

Advantages

- If one computer or device fails, then the rest of the network is unaffected.
- Problems on the network are easy to identify and work can be carried out on a faulty device without affecting the rest of the network.
- It is easy to expand the network.

Disadvantages

- If the central hub breaks down, the whole network crashes.

Tree network

A **tree network** has a central line (just like a bus network) connecting together a series of star networks, as shown in Figure 4.4. The server is also connected to this central line. Because of its flexibility, and the fact that it has the advantages of both bus and star networks, this topology is becoming increasingly popular.

The advantages and disadvantages are the same as for bus and star networks.

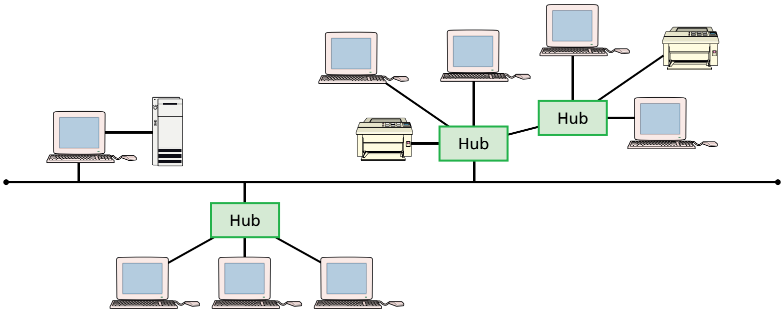

Figure 4.4 A tree network

Wireless LANs (WLANs)

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

Devices, known as **access points (APs)**, are connected into the wired network at fixed locations (see Figure 4.5). Because of the limited range, most commercial WLANs (e.g. on a college campus or at an airport) need several APs to permit uninterrupted wireless communications. The APs use either **spread spectrum technology** (which is a wideband radio frequency with a range of about 30 to 50 metres) or **infrared** but this has a very short range (i.e. about 1 to 2 metres) and is easily blocked, so is of limited use.

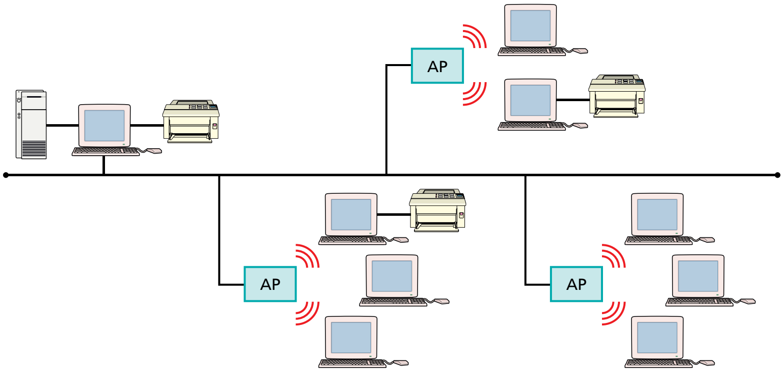

Figure 4.5 A network connecting WLANs

The AP receives and transmits data between the WLAN and the wired network structure. End users access the WLAN through WLAN adapters, which are built into the devices or are plug-in modules.

Advantages

- All computers can access the same services and resources (e.g. printers, scanners, internet access from anywhere within range of the APs).
- There is no cabling to individual computers and devices so safety is improved.
- The system is more flexible, since users can move their laptops from their desks.
- Adding new computers and devices is very easy (all that is required is a WLAN adapter, provided the device is within range of an AP) and costs are reduced since no extra cabling is needed.

Disadvantages

- Security is a big issue since anyone with a WLAN-enabled laptop computer can access a network if it can pick up a signal. It is therefore necessary to adopt complex data encryption techniques.
- There may be problems of interference which can affect the signal.
- The data transfer rate is slower than in a wired LAN.

WiFi

WiFi refers to any system where it is possible to connect to a network or to a single computer through wireless communications, for example:

- on the WLAN described above
- PDAs and other handheld devices

- laptop computers which are WiFi enabled
- peripheral devices such as printers, keyboards and mouse which can interface with the single computer when fitted with WiFi adapters.

WiFi systems rely on some form of AP, which uses radio frequency technology to enable the device to receive and send signals.

Note that WiFi is *not* short for wireless fidelity (a common misconception!). Rather, it is the trademark name for any product which is based on the **IEEE 802.11** standard.

WiFi **hotspots** are places where you can access WiFi (free or paid). They exist in public places such as airports, hotels and internet cafés. It is possible to logon to free WiFi hotspots unless they are protected by passwords. Software exists which can be loaded onto a laptop computer which then searches for non-protected WiFi systems. The practice of driving around in a car looking for these unsecured WiFi hotspots is known as **war driving** and poses a security risk to any unsecured WiFi system.

Bluetooth

Bluetooth is an example of **wireless personal area networking (WPAN)** technology. Spread spectrum transmission (radio waves) is used to provide wireless links between mobile phones, computers and other handheld devices and allow connection to the internet.

With this system, it is possible to create a small home network, for example, to allow communication between any PDA, mobile phone, computer, media player and printer. The range is, however, quite small (about 10 metres). Examples of its use include the transfer of photographs from a digital camera to a mobile phone or the transfer of phone details to a computer. It behaves like a mini-LAN.

Wide area networks

A wide area network (WAN) is basically formed by a number of LANs being connected together through either a router or a modem. Some companies will set up private WANs (usually by way of fibre optic cabling or telephone wires restricted to company use only). This is expensive but comes with the advantage of much enhanced security. It is more common to use an **internet service provider (ISP)** for connections to the internet and communicate via this network system.

The following additional hardware is needed for a WAN: routers, modems and **proxy servers** (described in Section 4.3).

4.3 Network devices

Modems

Modem means *mo*dulator *dem*odulator and is a device which converts a computer's digital signal (i.e. modulates it) into an analogue signal for transmission over an existing telephone line. It also does the reverse process, in that it converts analogue signals from a telephone line into digital signals (demodulates) to enable the computer to process the data. (Section 5.5 discusses digital and analogue data in more detail.)

Modems are used to allow computers to connect to networks (e.g the internet) over long distances using existing telephone networks.

Dial-up modems operate at transmission speeds of about 60 kilobits per second, which is quite slow by today's standards. (These are discussed in more detail in Section 4.4.) However, modern broadband or **asymmetric digital subscriber line (ADSL)** modems operate at 11,000 kilobits per second (or higher). The term 'asymmetric' means that the modem is faster at **downloading** (getting) data than it is **uploading** (sending) data.

Although the ADSL modems still use the existing telephone network, unlike dial-up modems they do not tie up the line while accessing the internet, so the land-line telephone can still be used at the same time. Furthermore, they can always be 'on' so internet access can be available 24 hours a day. ADSL modems can allow telephone conversations and internet traffic to occur at the same time because of the wide bandwidth signal used: the higher frequencies are used to carry the internet signals, so they do not interfere with normal telephone traffic. Cable modems also exist which allow cable television providers to offer internet access as well as receiving television signals.

Network hubs

Network hubs are hardware devices that can have a number of devices/computers connected to them. Its main task is to take any data received via one of the ports and then send out this data from all of the ports. Each computer/device will receive the data, whether it is relevant or not.

Switches

Switches are similar to hubs but are more efficient in the way they distribute data. A hub learns which devices are connected to which ports. Each device has a **media access control (MAC) address** which identifies it uniquely. **Data packets** sent to the switch will have a mac address giving the source and receiving device. If a device X is always sending the switch data via port 4 then it learns that X must be connected to that port; any data packet which is intended for X only is then sent through port 4 and not through any of the others. This means that the network traffic only goes to where it is needed and so a switch is more efficient than a hub, especially when the network is very busy.

Bridges

Bridges are devices that connect one LAN to another LAN that uses the same **protocol** (the rules that determine the format and transmission of data). They decide whether a message from a user is going to another user on the same LAN or to a user on a different LAN. The bridge examines each message and passes on those known to be on the same LAN and forwards messages meant for a user on a different LAN.

In networks that use bridges, workstation addresses are not specific to their location and therefore messages are actually sent out to every workstation on the network. However, only the target workstation accepts this message. Networks using bridges are interconnected LANs since sending out every message to every workstation would flood a large network with unnecessary traffic.

Routers

Since large companies often have more than one network there are occasions when the computers in one network want to communicate with the computers in one of the other networks. Routers are often used to connect the LANs together and also connect them to the internet.