

CHAPTER

3

NETWORKS

Key knowledge

After completing this chapter, you will be able to demonstrate knowledge of:

Digital systems

- applications and capabilities of local area networks (LANs) and wide area networks (WANs)
- functions and characteristics of key hardware and software components of networks required for communicating and storing data and information
- purposes of network protocols
- strengths and limitations of wireless communications technology
- types, capabilities and limitations of mobile devices connected to networks
- security threats to data and information communicated and stored within networks
- technical underpinnings of malware that intentionally threaten the security of networks

Implications and impact

- how people, processes, digital systems and data combine to form networked information systems
- legal requirements and ethical responsibilities of network professionals and users of networks with respect to social protocols and the ownership of data and information
- risks and benefits of using networks in a global environment.

For the student

This chapter provides an overview of communications, with an emphasis on the communication of data and information locally and within a global environment. The chapter explains some of the terminology, equipment, procedures and applications that are required to connect and maintain computers so that files, programs and resources can be shared. It also discusses the advantages and disadvantages of using wireless networks, and the role of portable devices. The ways that the security of data and information can be compromised by accidental or deliberate acts are also explored.

In the Outcome at the end of this chapter, you will propose a wireless networked information system that meets a particular need, explain its configuration and predict outcomes for intended users.

For the teacher

This chapter focuses on networks used in a global environment. The capabilities of local area networks (LANs) and wide area networks (WANs) are discussed. An overview of hardware, operating systems and wireless network protocols is provided. A range of wireless transmission media is considered, and several factors that influence the design of a networked information system are identified. The roles and responsibilities of network professionals in terms of their legal requirements and ethical responsibilities are considered. At the completion of this chapter, students will have examined the roles and functions of the components of wireless networks and will be able to recommend a networked information system for a specific use. They will have also considered security threats to data and information communicated via networks. The contents of this chapter will help students to demonstrate key knowledge required to complete Unit 1, Outcome 2.

Students must use a graphics software tool to depict the components of a network.

Networks

A **network** is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with one another. Examples of resources are data, information, hardware and software. Networks can be internal to an organisation or cover the whole world by connecting to the internet.

Networks exist for sharing information, such as spreadsheet files, database records, email – indeed anything that helps someone get their job done. The ability to share resources, such as servers, printers and software, also makes a network valuable.

As shown in Figure 3.1, for successful communications, a network needs:

- a **sending device**, such as a notebook computer, which initiates an instruction to transmit data, instructions or information
- a communications device, such as a wireless adaptor inside a notebook computer, to forward packets of data, instructions or information from a sending device via signals carried by a communications channel
- a communications channel or transmission media, such as a cable or radio waves, through which the digital signals travel
- a communications device, such as a wireless router, which receives the signals from the communications channel and forwards the packets to the receiving device
- a **receiving device**, such as a printer, which accepts the data, instructions or information.

Notebook computers, tablets, smartphones and other sending devices usually have a built-in communications device.

The primary function of a communications device, such as a broadband router, is to transmit data, instructions and information between a sending and a receiving device. Data, instructions and information travel along a communications channel in digital form.

A **digital signal** consists of individual electrical pulses that represent the bits grouped together into bytes. Early networks used analog signals that consist of a continuous electrical wave. Computers process data as digital signals, so a modem was used to convert between analog and digital signals.

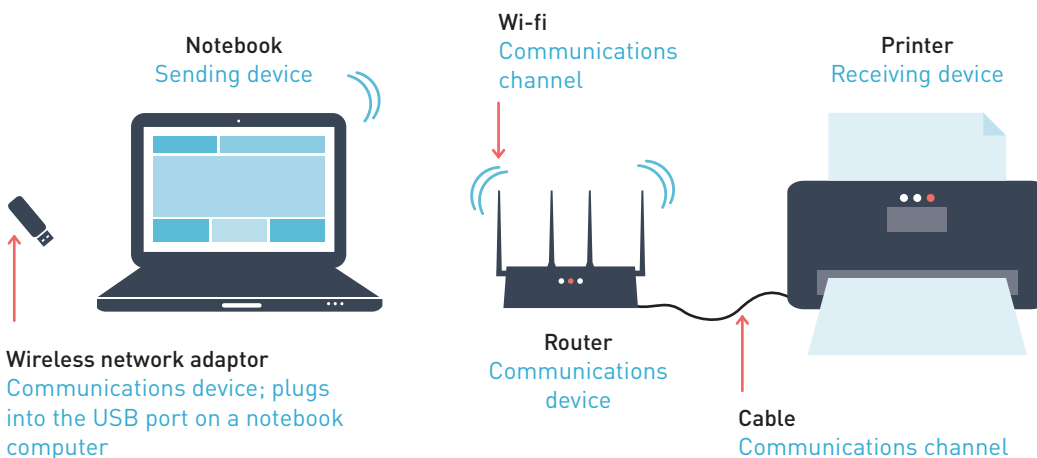


FIGURE 3.1 The notebook sends an instruction to the wireless adaptor (communications device), which sends a signal over radio waves (communications channel). The router (communications device) receives the signal and sends an instruction to print via cable (communications channel) to the printer (receiving device).



To check the download speed of your home internet connection, visit the speed test weblink and run the speed test.

Sending devices can usually also serve as receiving devices. Examples include notebook computers, personal computers and mobile phones.

Types of networks

Local area networks and wide area networks are types of networks that are in common use. The type of network refers to the area over which the network provides connectivity.

Local area networks

A **local area network** (LAN) connects computers and devices in a limited geographical area, such as a home, school, office building (Figure 3.2) or closely positioned group of buildings. Each computer or device on the network is a **node**. In many networks, the nodes are connected to the LAN via cables. Many new networks use wireless transmission media. A wireless LAN (WLAN) uses no physical wires; instead it uses wireless media, such as radio waves. Computers and devices that access a WLAN must have built-in wireless capability. Usually a WLAN communicates with a wired LAN for access to its resources, such as software, hardware and the internet.

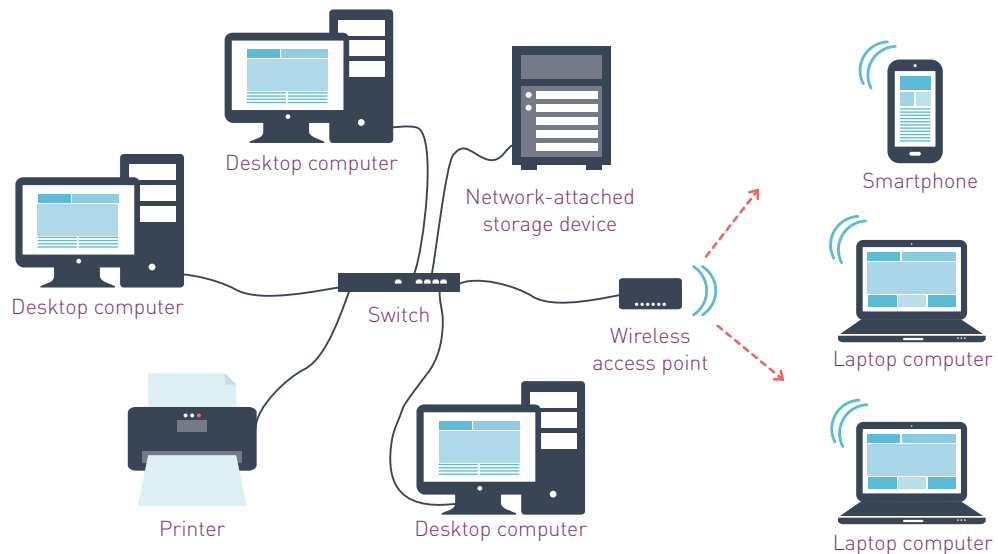


FIGURE 3.2 A local area network operating within a confined geographical area.

The logical design of the components of the network, including the number and types of servers, workstations and network resources, is known as the **network architecture**. It includes the communications devices and the types of physical and wireless transmission media used to connect components.

Intranets

Organisations typically use an **intranet** to publish their event calendars, policies, procedure manuals and technical support files, and to allow access to documents required for group work. An intranet will often include a connection to the internet, allowing employees access to information from the Web. Intranet pages will often include links to internet sites, with information relevant to the organisation.

An intranet uses a **web server**, supports multimedia webpages coded in **HTML** and is accessible via a **web browser**, such as Google Chrome, Mozilla Firefox, Microsoft Edge and Internet Explorer.

An intranet provides the following efficiencies.

- It facilitates communication by allowing employees to work in groups.
- Users can access information faster since data does not need to pass through a router, and loading graphics and images becomes much quicker than on the internet.
- An intranet reduces paper waste because companies are able to move their documents and processes onto the intranet. This can greatly reduce the need for centralised printing



and distribution. If a hard-copy version of a document is needed, on-demand printing at the end-user level is all that is required.

- An intranet improves ease of use. Point-and-click technology allows easy access to hyperlinked company documents.

The effectiveness benefits of an intranet include the following.

- An intranet allows restricted access to company information.
- An intranet provides dynamic information. Company documents stored on an intranet can be updated more easily and quickly than hard-copy versions. The documents can be kept up to date, providing more accurate and timely information to decision makers.
- An intranet allows connection across different network platforms. Users of complex networks that employ a number of different operating systems – such as Microsoft Windows, Macintosh and UNIX – are able to communicate easily within an intranet using their browser software. The HTML code used by the webpages is universal across all platforms.
- An intranet makes data more accessible. Information stored on an intranet can be accessed from anywhere in the world via the internet, if the user is authorised to connect to the internal network. An employee travelling overseas can use the internet to access files that otherwise would have been locked away in a filing cabinet back in the office.
- An intranet supports the ability to communicate using audio and video files rather than just traditional text and graphic images.

Home networks

If you have multiple computers in your home or home office, you can connect all of them together with a home network (see Figure 3.3). The advantages of a home network include the following.

- Desktop computers, notebooks, tablets and smartphones can all communicate with each other.
- All the computers can be connected to the internet at the same time.
- All computers can share peripherals, such as a scanner, printer or a network-attached storage device.

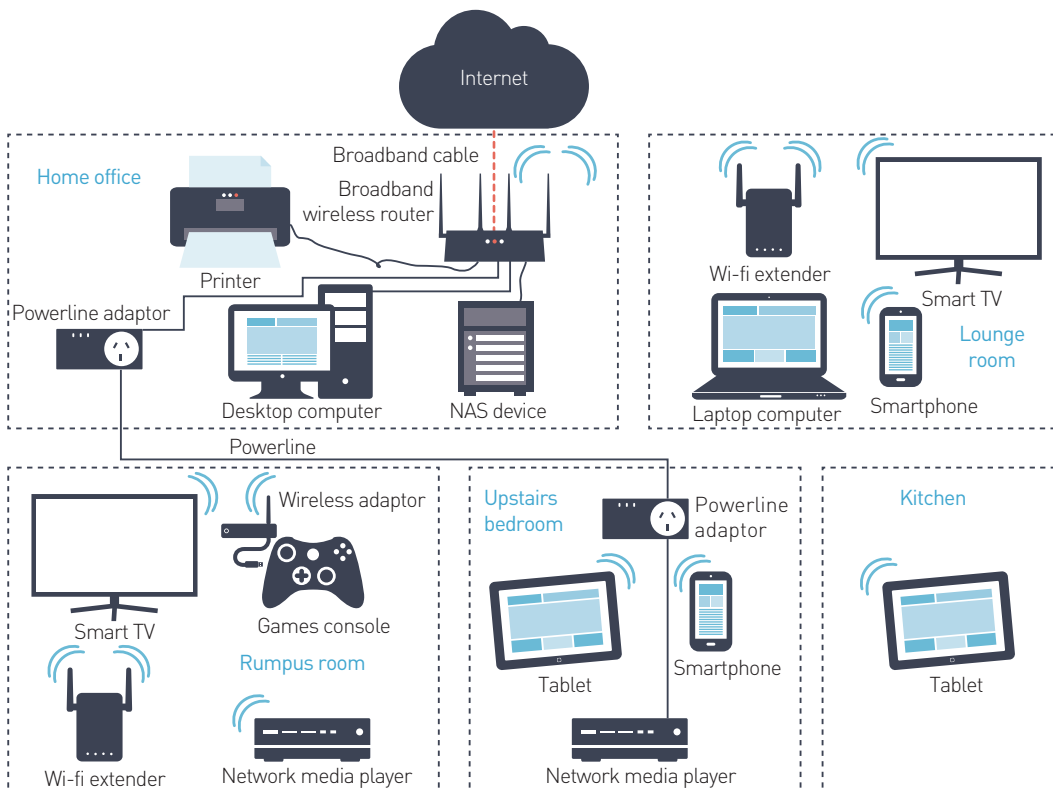


FIGURE 3.3 A home network.

- Each networked computer is able to play multiplayer games with players on other computers in the house.
- Smart TVs can connect to the internet.

Wide area networks

A **wide area network (WAN)** covers a large geographical area – for example, a city, a country or the world – using a communications channel that combines many types of media, such as telephone lines, cables and radio waves. A WAN can be one large network, or it can consist of two or more LANs connected together. The internet is the world's largest WAN. Mobile phones could be considered to be operating in their own WAN.

Network architecture

Each type of network can be further categorised by its architecture. Network architecture refers to the layout or design of the network. In this section we will consider client–server, peer-to-peer and virtual private network (VPN) layouts.

Client–server networks

In a **client–server network**, a server, sometimes called the host computer, controls access to the hardware and software on the network and provides a centralised storage area for programs, data and information. Besides storage capacity, a server allows for file sharing, website hosting, email management and access to shared printers. The other computers on the network, called clients, rely on the server for these resources (Figure 3.4). For example, a server in a school's administration might store a database of student details. Every client on the network can access this database on the server.

The costs associated with a server-based network are significantly higher than those for a peer-to-peer network. Not only is the start-up equipment more expensive, but a client–server network also requires ongoing technical support to maintain the sophisticated hardware and software. On the positive side, however, there are clear economies of scale, as the cost of adding clients that share the server's resources becomes relatively less.

The major difference between the server computer and the client computers is that the server has more storage space and power. Some servers, called **dedicated servers**, perform

THINK ABOUT COMPUTING 3.1

Suggest reasons why a peer-to-peer network would not be used in organisations with more than 10 computers.

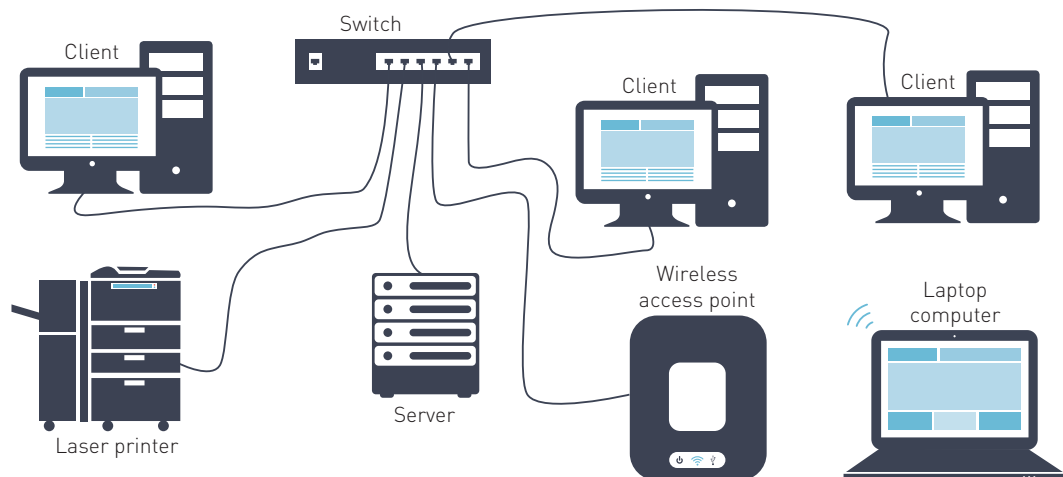


FIGURE 3.4 On a client–server LAN, one or more computers acts as a server and the other computers on the network are called clients.

a specific task. For instance, a file server stores and manages files. Each user on the LAN can share files or programs stored on the file server. A print server manages printers and print jobs. Print jobs received from users on the LAN are queued on the print server in order of their arrival and fed to the various network printers one document at a time. A database server stores and provides access to a database. A network server manages network traffic. A number of servers are often configured in a type of rack, which makes it easier to manage the cables and power supplies. The server rack is often located in a specialised room where the temperature is kept cool to offset the amount of heat generated by the power-hungry servers.

In the past, network administrators used to dedicate each server to a particular task. One application per server made it easier to track down any problems that arose. This approach, however, does not take advantage of the processing power of modern servers. Also, a larger storage room is required as the number of servers is increased. Many servers in networks are now virtual rather than physical. Specially designed software is used to convert one physical server into multiple virtual machines.

Although it can connect a smaller number of computers, it is typically most efficient for a client–server LAN to connect 10 or more computers. Most client–server LANs have a network administrator because of their larger size. The **network administrator** is the operations person in charge of the network.

Peer-to-peer networks

A **peer-to-peer network (P2P)** is a simple, inexpensive network that typically connects fewer than 10 computers. Each computer on a peer-to-peer network can share the hardware (such as a printer), data or information located on any other computer in the network (Figure 3.5).

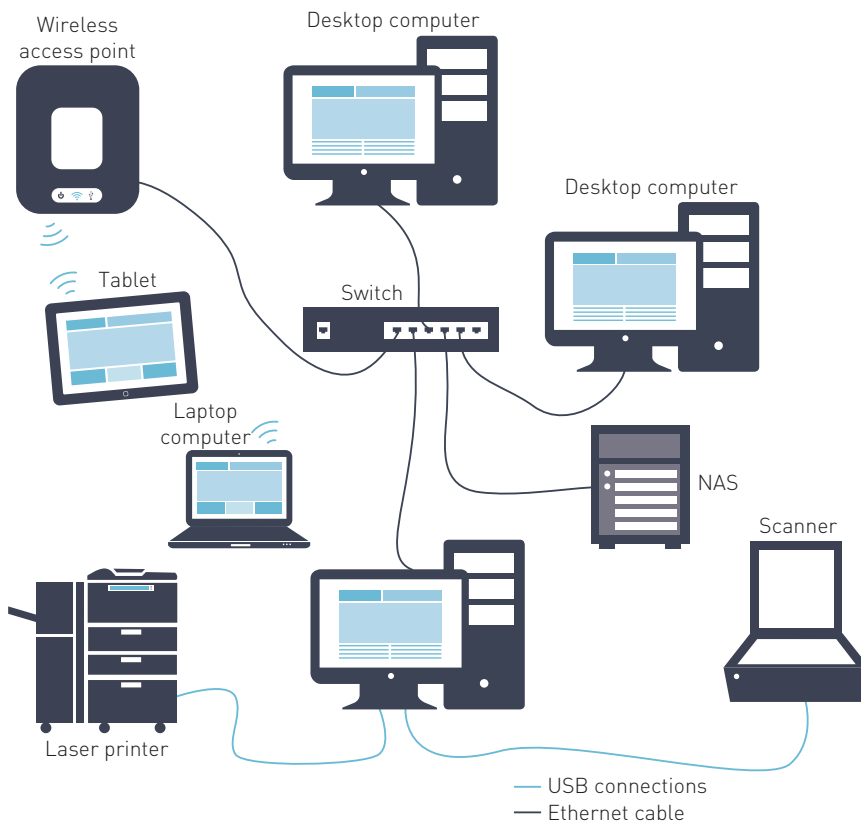


FIGURE 3.5 Each computer on a peer-to-peer network can access data from other users and share resources such as printers. A peer-to-peer network differs from a client–server network in that files can be directly transmitted between nodes rather than from a server.

A client–server network provides better security than other configurations, because user access can be managed and logged.

Each node in a peer-to-peer network shares hardware and data with all other computers on the network.

Network-attached storage devices (NAS) are discussed later in this chapter.

THINK ABOUT COMPUTING 3.2

Kazaa was a popular Internet P2P application for finding, downloading, playing and sharing files with millions of other users. The Kazaa client could be downloaded free of charge, but it came bundled with adware. After numerous legal proceedings against Kazaa by the recording industry, resulting in damages payments in excess of \$100 million, it now operates as a music subscription service. Users pay around \$25 per month for unlimited downloads of songs.

The P2P acronym has been adapted by some to mean people-to-people. The development of social media software that allows individuals on the internet to meet each other and share ideas is an example of people-to-people technology.

Each computer can store files on its own storage device or on another computer. Each computer in the network contains both a client operating system (like the 'Home' versions of Windows) with basic networking capability, and application software. All computers on the network share any peripheral device attached to any computer. For example, one computer may have a laser printer and a scanner, whereas another may have an ink-jet printer. They may also share a network-attached storage device (NAS) with a movie and music repository. Peer-to-peer networks are popular in homes where a login server is neither necessary nor practical.

Internet peer-to-peer

Another use of peer-to-peer (called **P2P**) involves an **internet peer-to-peer network**, which enables users with the same **networking software** to connect to one another's hard disk drives and exchange files directly (Figure 3.6).

Early P2P programs, such as Kazaa and Limewire, stirred up much controversy about the copyright infringement of music because they allowed users to copy MP3 music files easily from one computer to another. To help reduce copyright infringement, music-sharing services, like iMesh, typically are fee-based, and music files are often encrypted as they travel across the internet.

Many businesses see an advantage to using P2P – that is, companies and employees can exchange files using P2P, freeing the company from maintaining a network for this purpose.

Allowing internet peer-to-peer file sharing exposes your computer to possible security violations. For files to be shared within a P2P network, a specific TCP port must be opened through the firewall on the computer. Once the port is opened, the computer is no longer protected from malicious software, such as viruses and Trojans, capable of causing computers to malfunction or seize. Recognised sites, such as BitTorrent, often have built-in security measures, but their dependability is open to question, and using them can be risky at best.

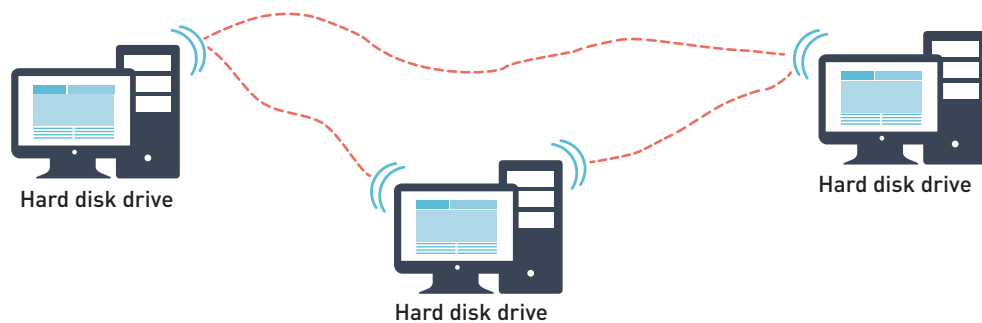


FIGURE 3.6 P2P describes an internet peer-to-peer network that enables users with the same networking software to connect to one another's hard disks and exchange files directly.

Virtual private networks (VPN)

Businesses with offices and branches across Australia or around the world need a fast, secure and reliable way to share data and information across networks. A **virtual private network (VPN)** allows businesses to use a public WAN, (the internet) to create a private network that links remote sites and users to the business's head office. The VPN uses encryption (we discuss encryption later in this chapter) to ensure files and messages are secure.

A VPN provides secure connections over the internet that allow businesses to extend their private network, which in turn allows communication and information sharing with remote branches and travelling salespeople.

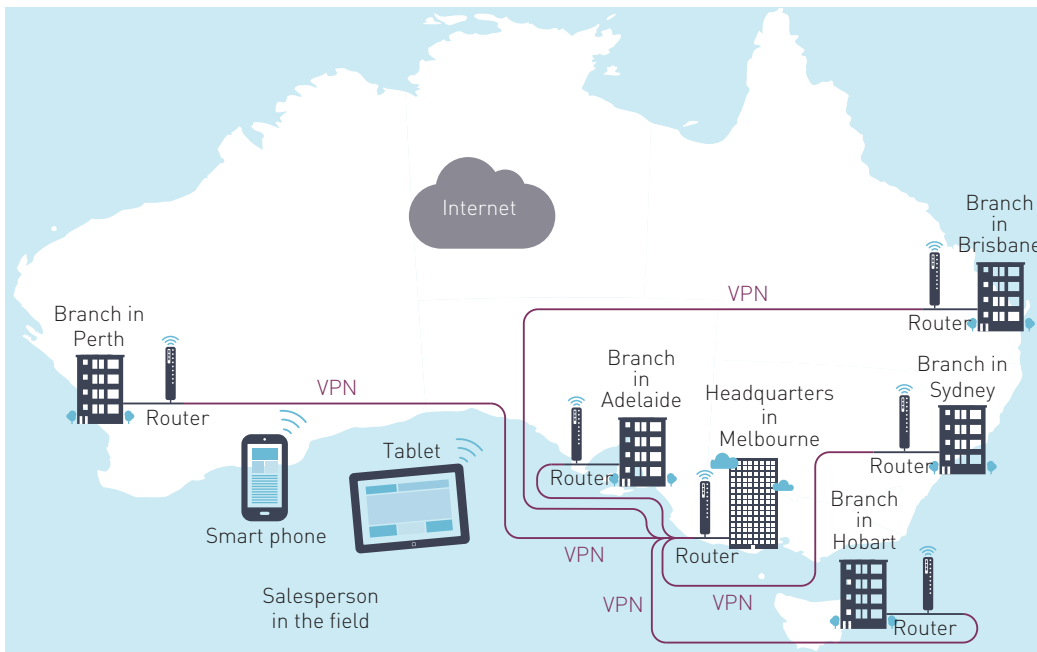


FIGURE 3.7 An example of a wide area network in Australia. The business is using a virtual private network (VPN) to communicate over the internet with branches around the country.

Prior to businesses using VPNs over the internet, the common way to connect computers between remote offices was to use a leased telephone line. Leased lines provided organisations with a means to expand their private network beyond its immediate geographic area. These connections formed a wide area network for the organisation. The telephone lines were leased from telecommunications companies such as Telstra. While the leased lines proved to be reliable and secure, they were expensive to operate, particularly the further the WAN had to reach.

P2P DOWNLOADS: TORRENTS

Internet P2P networks provide a popular means of downloading music, TV, video and software files. Downloading a file from a single site like iTunes typically involves a stream of sequential fragments of the file being sent to the requesting computer. Since the fragments are sequential, the user can play the file as it is being downloaded. If multiple people want to download the same file then that single source can become overworked and possibly crash. The more users on the network, the slower downloads become.

An alternative to single source file downloads is to use a torrent **protocol**. With torrents, there are multiple users who download a particular file at the same time, or who have previously downloaded the whole file. These users act as a source for each other. Together the downloaders become a network of multiple sources all providing pieces of the file to each other.

Here is how it works (Figure 3.8).

A user, for example Jack, installs a torrent client application on his computer. Jack searches the web to find a torrent provider. A **torrent** is a small file that holds information

Data sent or received over the internet is sent to the IP address of the remote computer and a specific Transmission Control Protocol (TCP) port on that computer. We discuss TCP/IP further on page 102. A firewall is hardware and/or software that restricts access to data and information on a network. We discuss firewalls on page 120.

about, say, a video file. It includes metadata (for example, the name and size) about the file to be shared and identifies the tracker. The tracker is a specific computer that coordinates the file distribution by making links to **peers** who have pieces of the required file. On the torrent provider's website, Jack locates the file he is after and downloads the torrent to his computer. The torrent is read by the torrent application which uses the specified tracker to locate other computers that are downloading the requested video file (peers) or already have the whole file (**seeds**). The tracker makes links between Jack's computer and the identified peers and seeds. With the connections in place, Jack's computer starts to receive the pieces of file he has requested. Since the file is being sent in non-sequential pieces from multiple sources, the video cannot be watched until all pieces are received and the video assembled.

Jack's computer also can start to send pieces of the file to other peers who are downloading the same video even while his computer is still receiving pieces. The torrent application therefore turns downloaders into sources. The more downloaders means the more sources and hence the faster the downloads. Using torrents to download files means that home computers, rather than servers, can act as sources, and a lower bandwidth connection to the internet is not the problem it would be with single source downloading.

If Jack does not allow his computer to pass pieces of the file to peers (that is, he only downloads) he is referred to as a **leecher**.

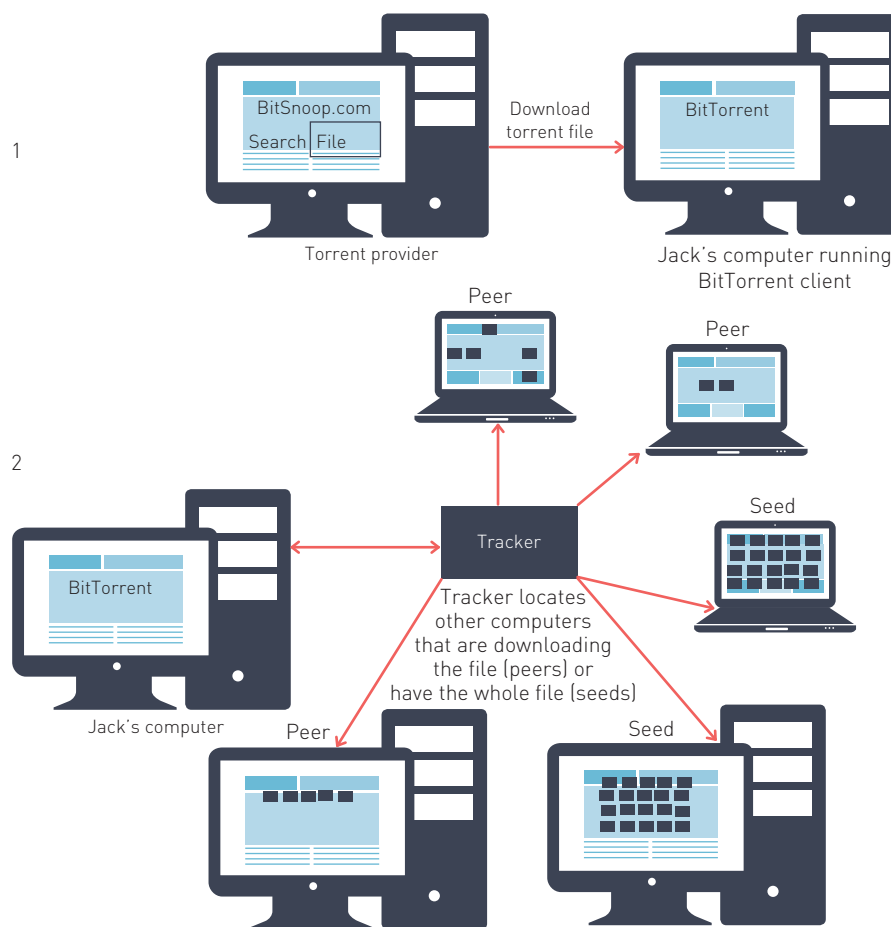
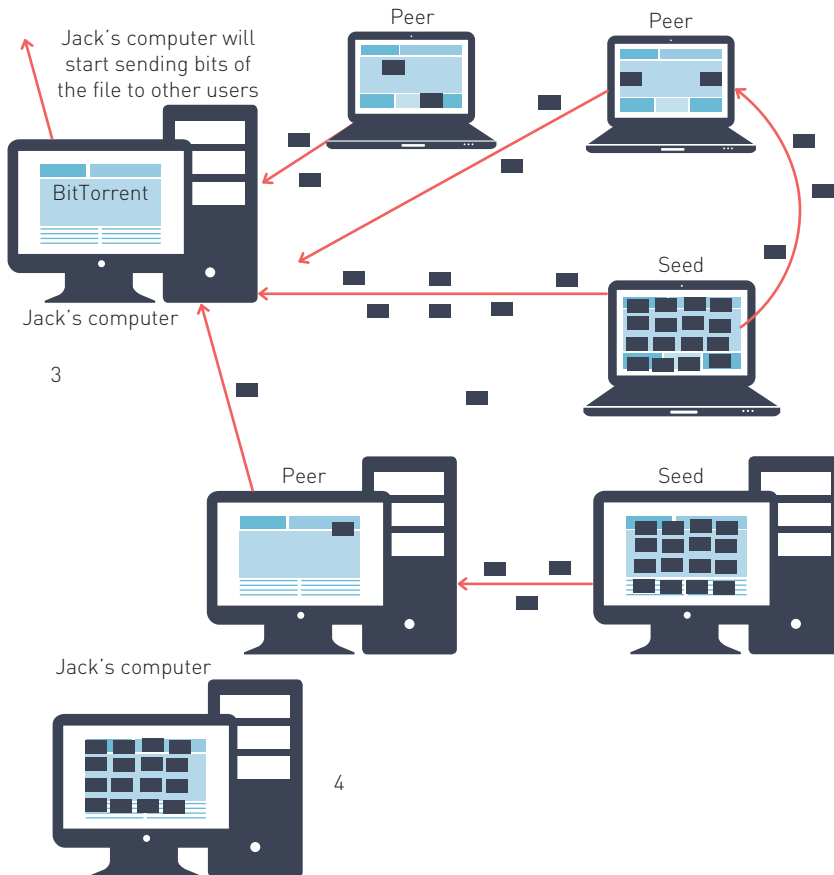


FIGURE 3.8

- 1 Jack's computer downloads a torrent from a provider and loads it into BitTorrent on his computer.
- 2 BitTorrent uses the torrent to locate a tracker that makes links with peers and seeds who have part or all of the requested file.



- 3 The peers and seeds transfer pieces of the requested file to Jack's computer. Meanwhile, Jack can also act as a peer by allowing some of the pieces he has downloaded to be sent to someone else requesting the same file. The more downloaders of the file, the more sources and the faster the downloads become.
- 4 The requested file has been downloaded to Jack's computer.

ISSUE

Is it legal to download music and video files?

The *Copyright Act 1968* allows users to download music and video files from the internet via peer-to-peer transfers only if they have the permission of the copyright holder. Downloading a TV show, a film or a music file is in breach of the law unless the owner has approved the transfer, usually for the payment of a fee. If you pay to download a file, or even if you are not required to pay a fee, you often have to agree to certain conditions before you can download it. Any such conditions override the default provisions in the *Copyright Act* that allow private copying of the file. Sites like The Pirate Bay allow torrents to be downloaded, which can then be used with an application like BitTorrent or uTorrent to collect pieces of the original file from a number of peer sites and put them together. If the user plays the assembled file without permission they have broken the law.

THINK ABOUT COMPUTING 3.3

- 1 For each file-sharing Internet site that has been forced to shut down because of copyright violations, many more have been launched in their place. How can the rights of artists, film makers and TV producers be properly protected?
- 2 Should governments be doing more? Or is it the responsibility of society to do the right thing?
- 3 Look for recent examples of attempts to regulate or control torrent sites. How successful have these measures been?

The Pirate Bay website operates from Sweden, where the copyright laws are possibly less strongly enforced than other countries like the United States. Nevertheless, in 2009 the founders of the site were found guilty of making copyright content available to others. The site was shut down for a short period in 2010, but has since reappeared. In 2012 the High Court of the United Kingdom ruled that British-based internet service providers must block The Pirate Bay. The British Phonographic Industry stated that sites like The Pirate Bay destroy jobs in the UK and undermine investment in new artists.

Critics of site blocking argue that such measures are ineffective as they can be circumvented using proxy servers and other techniques.

Pirate Bay must be blocked, High Court tells ISPs, by Matt Warman, Consumer Technology Editor, The Telegraph, 30 April 2012

Communications devices

Communications devices enable computer users to communicate and exchange items such as data, instructions and information with another computer. For example, a broadband router is a communications device that enables computers to communicate via telephone or cable. At the receiving end, the communications device receives the signals from the communications channel.

Today, thousands of networked digital systems exist, ranging from small wireless networks operated by home users to global networks operated by numerous telecommunications firms. To interconnect these networks, various communications devices exist. Some of the more common types of communications devices are switches, basic routers, broadband routers, network interface cards and wireless access points.

Switches

A **switch** is a device that provides a connecting point for cables in a LAN.

Network traffic in a LAN typically follows specific paths that connect members of a work group, such as the accounts department of a business. A switch stores the address of every device down each cable connected to it. When a packet enters the switch, it uses simple logic to detect the destination of the packet and sends the packet only down the cable that contains the addressed device. The result is that the packet reaches its destination quickly and without colliding with packets being sent to other nodes.

As packets are sent straight to the destination device through a switch, the two devices act as if they are directly connected. On a 100 **Mbps** switch, data can be sent simultaneously to all nodes at 100 Mbps uninterrupted.

Encryption of data packets enhances the security of wireless transmissions. Setting up complex passwords for file sharing, routers and access points, as well as using encryption keys that are not obvious, greatly improves security.

Routers

A **router** is a device used to connect multiple networks – several LANs or a LAN and a WAN, such as the internet. A router will connect LANs and WANs irrespective of the hardware and network communications protocol used in each segment. On the internet or a large corporate network, for example, routers receive TCP/IP packets, look inside each packet to identify the source and target IP addresses, and then forward these packets as needed to ensure the data reaches its final destination. Figure 3.9 looks at how a router can be used to communicate between two LANs operating within one organisation.

While a switch uses a node's MAC (Media Access Control) address to identify which path to send the packet, a router uses the IP, IPX or Appletalk address. The algorithm that switches use

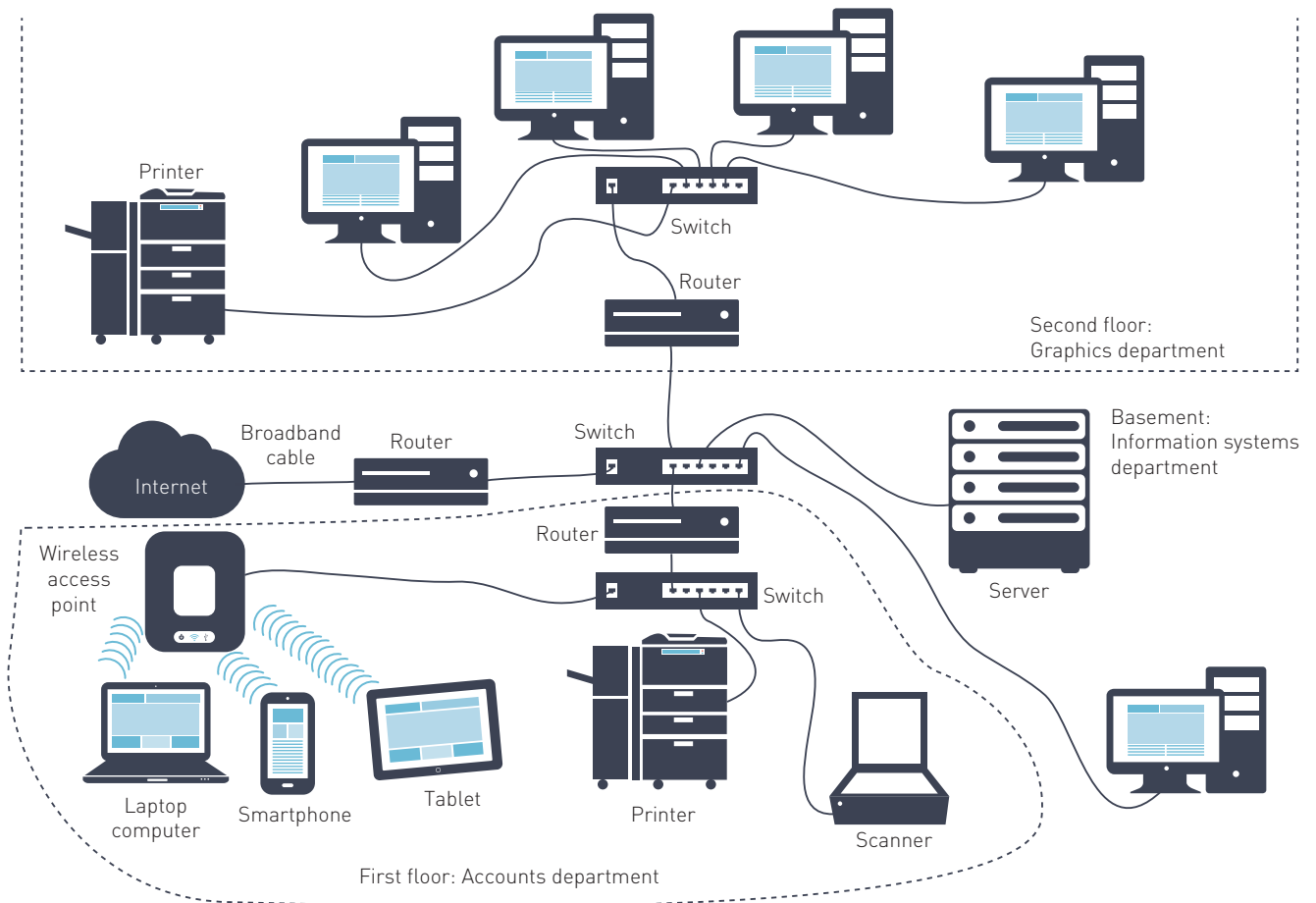


FIGURE 3.9 How a router can connect two LANs and provide internet access to both networks.

to decide how to forward packets is different from the one used by routers. Most carriers, such as Vodafone, offer a 4G USB modem stick. The small size makes it ideal to use with a mobile device, such as a laptop computer, to connect to the internet using the 4G phone network.

In Figure 3.9, a file sent from one member of a graphics department to another member of the same group stays on the graphics LAN and does not affect network traffic on the accounts LAN. The router detects if a file needs to move from one LAN to another and allows its passage. For example, the graphics department may need to send large animation files between members. The size of these files means that allowing all members of the two work groups to have unlimited communication on the one cable through a single LAN can consume the available resources of the cable. The network will become sluggish and frustrating for users. To overcome this, each work group is given its own LAN and a switch with a router used to link the work group LANs. In this way, large files that are needed only by the graphics department stay on the one LAN, while files that need to be shared between departments can move from one LAN to the other.

Broadband routers

Routers for home networks (often called **broadband routers**) also can join multiple networks. These routers are designed specifically to join the home (LAN) to the internet (WAN) to share internet connections.

Wireless broadband routers combine the functions of a basic router (connecting the LAN to the internet), a switch (for devices, such as a desktop computer, connected by cable), a firewall (security measure) and a wireless access point (to allow wireless connectivity). Figure 3.10 shows a broadband router with an antenna for wireless connections, LAN ports for wired connections and a WAN port for connection to the internet.

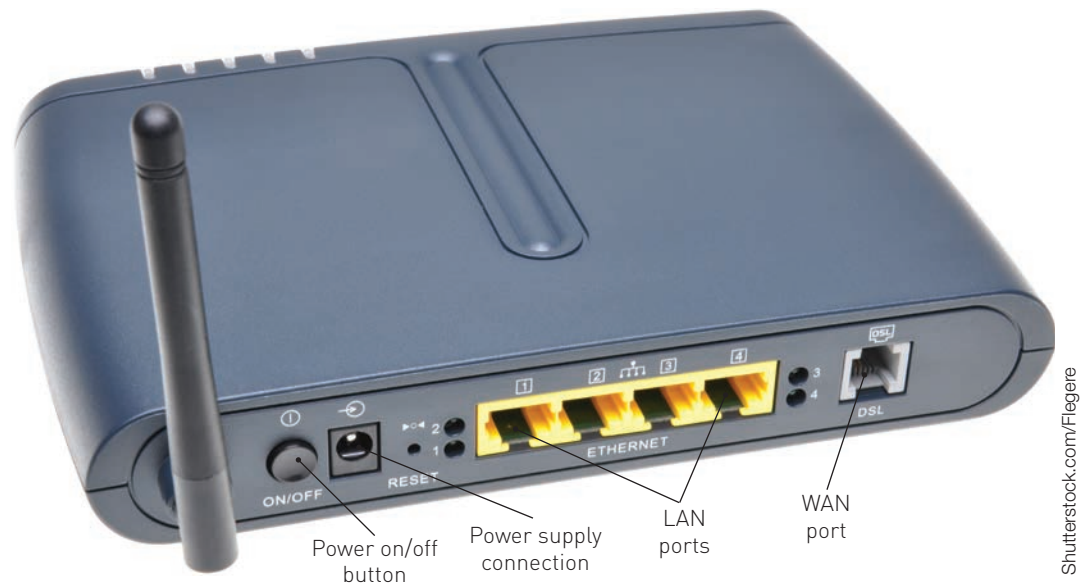


FIGURE 3.10 Wireless broadband router

The type of broadband router used to act as a bridge between a LAN and the internet depends on the type of connection provided by the Internet Service Provider (ISP). A cable connection uses the high bandwidth available through the same broadband connection that delivers information to a television via a provider such as Foxtel. An **asymmetric digital subscriber line (ADSL)** connection provides internet access using copper wiring in telephone lines. The cost of an ADSL broadband router is around \$100. A cable broadband router is usually sourced from an ISP, since it has to be registered on the ISP's network before it will work.

NBN devices

The National Broadband Network (NBN) is a national network of communication infrastructure that uses lightning-fast fibre-optic, fixed wireless and satellite technology. The original NBN plans were to reach 93 per cent of Australian homes with download speeds up to 100 megabits per second. Revised plans by the federal government, whereby connections are made to a local node rather than directly to a home or business, will result in a speed of 25 megabits per second. Current ADSL 2+ connections are 24 megabits per second depending on line quality and capability of components in local telephone exchanges.

Homes connected to the National Broadband Network (NBN) will require a router that is capable of supporting the faster download speeds that are available.

The NBN utility box (also known as the Premises Connection Device, or PCD) is installed to the outside of a house during the street roll-out of NBN cable. Fibre-optic cable from the roll-out is connected to the utility box (see Figure 3.11). The home-owner's ISP then arranges for the NBN connection box (also known as a Network Termination Device, or NTD) to be installed in the home (see Figure 3.12). A fibre-optic cable is used to connect the PCD to the NTD.

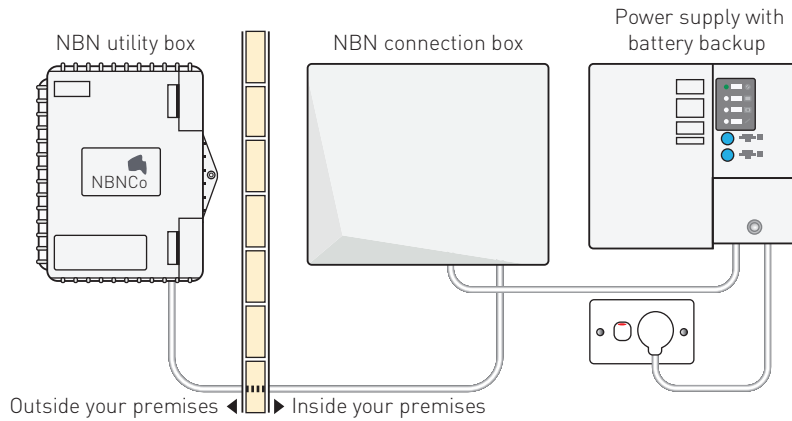


FIGURE 3.11 The NBN utility box

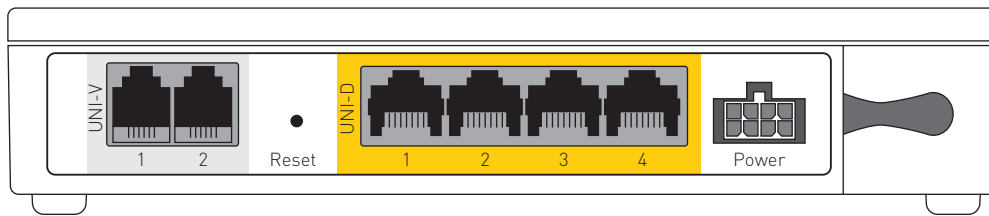
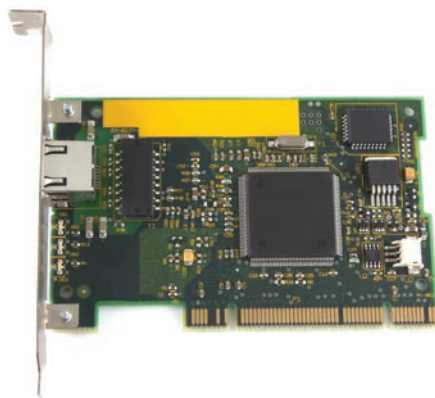


FIGURE 3.12 NBN connection box

On the left-hand side of the NBN connection box are two voice ports. When copper-based telephone connections are phased out, one of these ports will be used for phone connection over the fibre-optic NBN network. The other voice port can be used for other services such as a personal alarm service (for the elderly or disabled). One of the four data ports is used to join the connection box to the home network's router. The other ports allow a home-owner to connect to other service providers.

Network interface cards and wireless adaptors

A **network interface card (NIC)** is a card inserted into an expansion slot of a personal computer, or it may be built in to the computer's motherboard. A **wireless adaptor** performs the function of a NIC for notebook and other mobile computers (Figure 3.13).



Shutterstock.com/louke van Keulen



iStockphoto/connect11

FIGURE 3.13 **a** A network interface card slots into the motherboard on a desktop computer. **b** A wireless adaptor can plug into the USB port on a desktop computer or notebook that does not have wireless capability.

Wireless adaptors and NICs work with a particular network technology, such as Ethernet. An Ethernet card is the most common type of NIC for hard-wired networks. Depending on the type of wiring used, the transfer rate on an Ethernet network can be up to 1000Mbps.

A NIC performs three functions: it increases the strength of the signal from the computer, packages the data for transmission and controls access to and from the network cable or the wireless channel. An external USB wireless adaptor is available for a desktop computer or portable device that does not have built-in wireless connectivity.

Mobile devices, such as tablets and mobile phones, can connect to a LAN using a built-in **wi-fi** adaptor.

Wireless access point

A **wireless access point** is a communications device used on wireless local area networks. It acts as a central transmitter and receiver of wireless radio signals. A wireless access point is often connected to a wired network backbone for faster transmission of data back to the network server.

Wireless access points are mostly used in business networks where larger buildings and spaces need wireless coverage. Home networks are small enough that a wireless router can provide sufficient coverage without the need for an access point.

If an area is too large to be covered by a single wireless access point, multiple access points can be used. There can be a momentary loss of connectivity when a user moves from the vicinity of one access point to another. Figure 3.14 shows a wireless network with overlapping access points. Overlapping access points provide a seamless area for users to move around in, using a feature known as 'roaming'. When a user moves from one area to another, the wireless networking hardware automatically jumps to the access point that gives the strongest signal.

To guard against hackers stealing valuable files from your wireless network, consider using a protocol other than TCP/IP, such as Ethernet, for file sharing. Access points are usually installed on a LAN behind the firewall. If a hacker successfully connects to your access point, they will have open access to your LAN. Since the hacker will be using TCP/IP to connect to your LAN, you can deny them file-sharing access by using a protocol other than TCP/IP for that service. The hacker may still be able to use your Internet connection, but they will not be able to access your files.

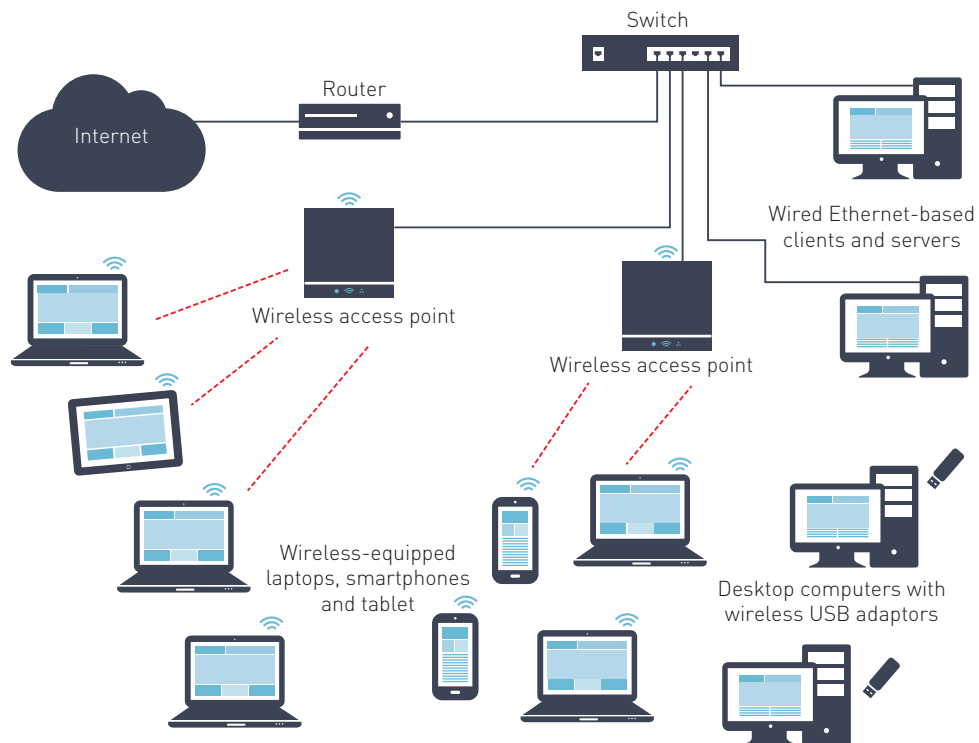


FIGURE 3.14 A business network using multiple wireless access points.

Wireless extender

Wireless extenders (wireless repeaters) increase the area covered by a wireless network (Figure 3.15). They allow users to keep mobile devices, media players and computers connected to a wi-fi network with expanded coverage throughout the home or office. Wireless extenders pick up a wireless signal in the same way as a tablet or notebook computer, then re-broadcast that signal, effectively giving the network a second access point to connect to. This allows users to overcome obstacles that normally would block radio signals and to enhance the signal quality. Extenders typically increase the range of a wireless network by 20 metres (depending on the physical layout and construction materials of the home or office), allowing users to roam anywhere in the home or office and remain connected to the internet.

The location of the extender is critical – too close to the wireless source can cause interference while too far from the source there may not be enough signal to enhance.



FIGURE 3.15 A wireless extender, such as the 5GHz NETGEAR WN2500RP, increases the coverage of a wireless network to all parts of the home. The extender also has four ports for hard-wired devices such as a smart TV, Blu-ray player or game console.

Summary of wireless network technologies

Components used in wireless networks have strengths and limitations in terms of data transfer rates, cost, security and reliability. Refer to Table 3.1.

Networks in homes and organisations often use hard-wired technologies to support the wireless connectivity of end users. For example, Ethernet cables may be required to connect a wireless access point to a router, or fibre-optic cable may be used to connect a broadband router to the internet. Storage options in a wireless network can include a hard-wired or wireless connection to a network-attached storage device (NAS), a file server or cloud storage.

THINK ABOUT COMPUTING 3.4

A concern with a single frequency wireless extender is that they can cause a throughput loss of about 50% of the radio signal, since the extender must receive then re-transmit each packet using the same radio signal on the same channel as the router. An alternative to using a wireless extender is to increase the network's range by using Ethernet-over-power (EOP). Investigate the advantages and disadvantages of EOP over wireless extenders.

Wireless network security options, including WPA2 and WPS, are discussed later in this chapter.

TABLE 3.1 A summary of the strengths and limitations of wireless communications technology; the transfer rates and price data were current in 2015.

Device	Cost estimate	Data transfer rate	Security	Reliability
Wireless broadband router	\$150	802.11ac standard, 867–1300 Mbps, dual band (2.4 GHz and 5 GHz frequencies).	High provided <ul style="list-style-type: none"> the router identifier is kept secret encryption is used for broadcasts (WPA2) Wi-fi Protection Setup (WPS) is used to attach devices to the wireless network 	<ul style="list-style-type: none"> Throughput on the 5 GHz band can drop quickly as the range increases. In the early years of 5 GHz connectivity, there is little congestion. The 2.4 GHz band can be affected by interference from household devices such as automatic garage doors, or from other nearby networks operating on the same band.
Access point	\$120			
Wi-fi extender	\$140			
Wireless adaptor	\$80			

Communications software

Communications software is an application or program designed to pass or support the movement of information over a network. Some communications devices are pre-programmed to accomplish communications tasks; others require a separate communications software program to ensure proper data transmission. Communications software consists of programs that help you establish a connection to another computer or network and manage the transmission of data, instructions and information. For two computers to communicate, they must have compatible communications software.

THINK ABOUT COMPUTING 3.5

Check out the software installed on the network in your school. Find out from the network manager how many users are covered by a site licence for one of the software packages. Compare the cost of the site licence with that of the equivalent number of single-user versions (check the price of a single-user version, such as in the newspaper or online). What is the cost saving for the school by purchasing the network version over the single-user version? What disadvantage is there in purchasing site licence software compared with single-user packages?

Network operating system

A server operating on a client–server network requires operating system and application software that differs from those of a desktop or portable computer. A server is able to share data with multiple users in a secure environment and reduce bottlenecks. A server often is assigned a particular role in a network, with associated software to facilitate that task. A server can be set up to provide email services, internet connectivity, file backup functionality and to manage print requirements.

A server uses specialised software to support its function. For example, an email server may use Windows Mail Server Software. A print server is responsible for sending jobs from multiple clients to a printer in the right order and at the right time. Appropriate software is needed to manage these tasks.

A **network operating system** (also called a **network OS** or **NOS**) is the system software that organises, controls and coordinates the activities on a local area network. A NOS controls the attached computer systems, any peripherals and the communication between them. Some of the tasks performed by a NOS include:

- administration – adding, deleting and organising users and performing maintenance tasks, such as backup
- file management – locating and transferring files

- device management – coordinating print jobs and reports sent to specific printers on the network, ensuring resources are used correctly and efficiently
- security – monitoring and, when necessary, restricting access to network resources.

Network analysis tools

Network administrators use a variety of software packages designed to monitor devices on a network, check the use of different protocols, identify which ports have been accessed on a web server, view event logs and analyse network traffic (Figure 3.16). A **network analysis tool**, or network utility, is software designed to analyse and configure various aspects of computer networks.

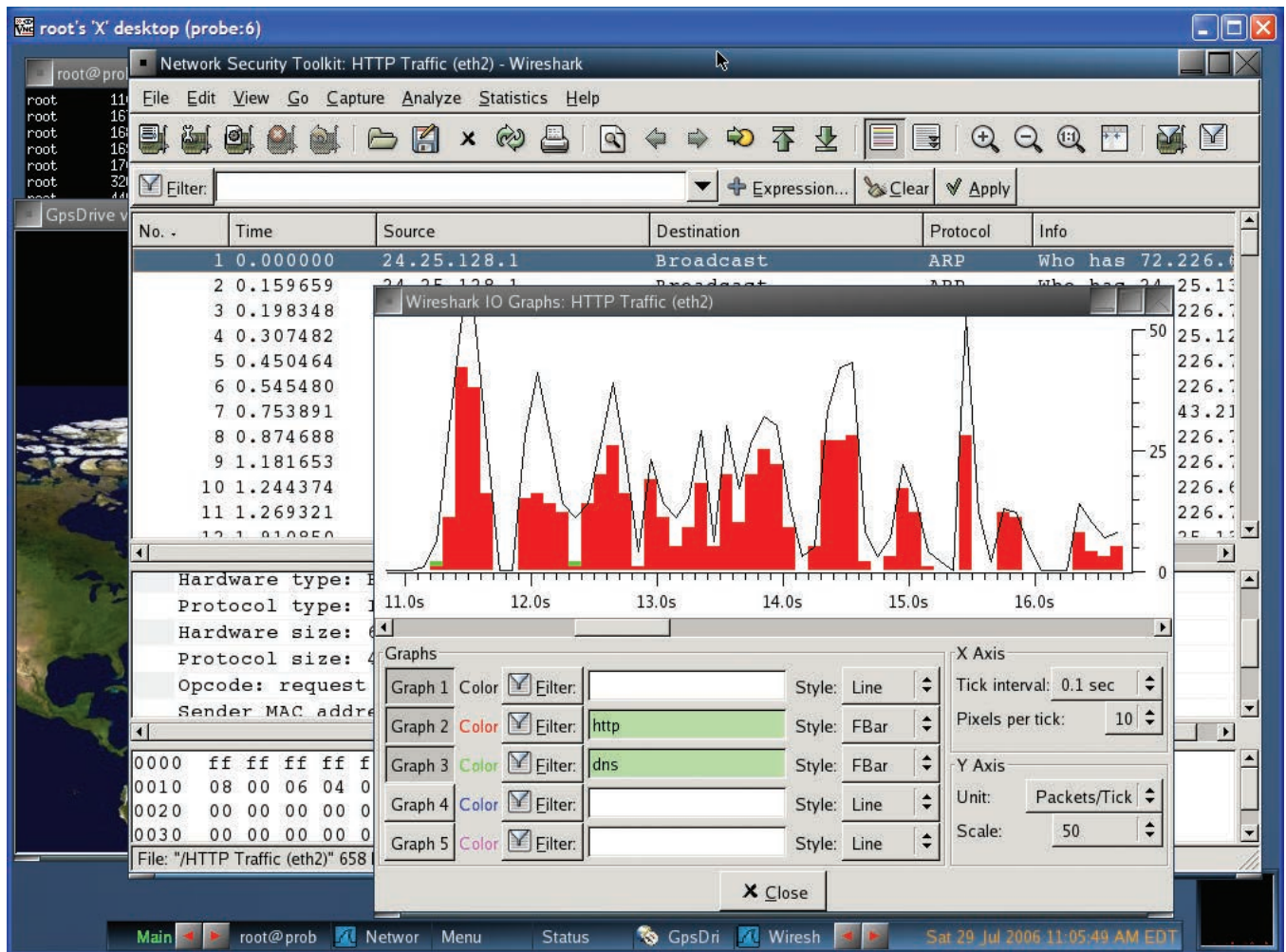


FIGURE 3.16 Analysis of network traffic using Wireshark analysis software.

TABLE 3.2 Popular analysis tools

Angry IP Scanner	Scans a network's open and closed ports. For each IP address found it identifies the hostname, computer name, group name, username and MAC address.
Wireshark	Network protocol analyser and packet sniffer that allows administrators to see what is happening on their network. Used for network troubleshooting and analysis.
Snort	A network intrusion prevention system capable of real-time traffic analysis and packet logging.
NetStumbler	Allows administrators to identify locations that suffer from a weak signal within a WLAN, detect issues of wireless interference and rogue access points. Within a business, it can be used to identify unauthorised wireless LANs that provide access to outside users and thus run the risk of imminent infiltration.
Cain and Abel	Decrypts or recovers lost or forgotten passwords.

Internet services

A significant reason why individuals and organisations purchase computers is to access the internet. The internet is a worldwide collection of networks that links millions of businesses, educational institutions, government departments and individuals. A number of services are available through the internet, with different types of software to support them. **Internet service software** includes web browsers, email, **Voice over Internet Protocol (VoIP)** software and cloud storage.

Web browsers

A **web browser** is an application software package that allows users to access and view webpages. Popular browsers include Internet Explorer, Chrome, Firefox and Safari. When the URL (Uniform Resource Locator) of a site has been entered into the address bar of a browser (Figure 3.17), a webpage from that site is downloaded. The web address consists of a protocol, the domain name, the path to a specific page and the name of the page to be downloaded. A **domain name server (DNS)** identifies the requested site and ensures that data and information are routed to the correct computer.

Search engines such as Google and Yahoo are helpful in locating webpages that contain information of interest. Many search engines maintain a list of words found on the internet. The search engine scans the list for words that have been entered in the search request. The sequence of the list displayed prioritises sites where the search text appears in the page title or descriptor.

Hypertext transfer protocol

Hypertext transfer protocol, better known as **http**, is a set of rules that defines how pages are transferred on the internet. Many browsers and websites do not require the user to enter the 'http://' and 'www' portions of the address.

Hypertext transfer protocol secured

Hypertext transfer protocol secured, or **https**, is a communications protocol for secure transmissions over the internet. The https system provides authentication and encryption communication and is widely used for security-sensitive processing, such as payment transactions and connections to banks. When a secure connection is made, 'https://' is displayed at the start of the URL and a lock symbol appears in the browser window (see Figure 3.18).

When the https protocol is used in an address the computer uses a different TCP port (443) to standard http transfers (TCP port 80). https uses a protocol called Transport Layer Security (TLS) to transport data safely over the Internet. The predecessor to TLS was called Secure Socket Layer (SSL).

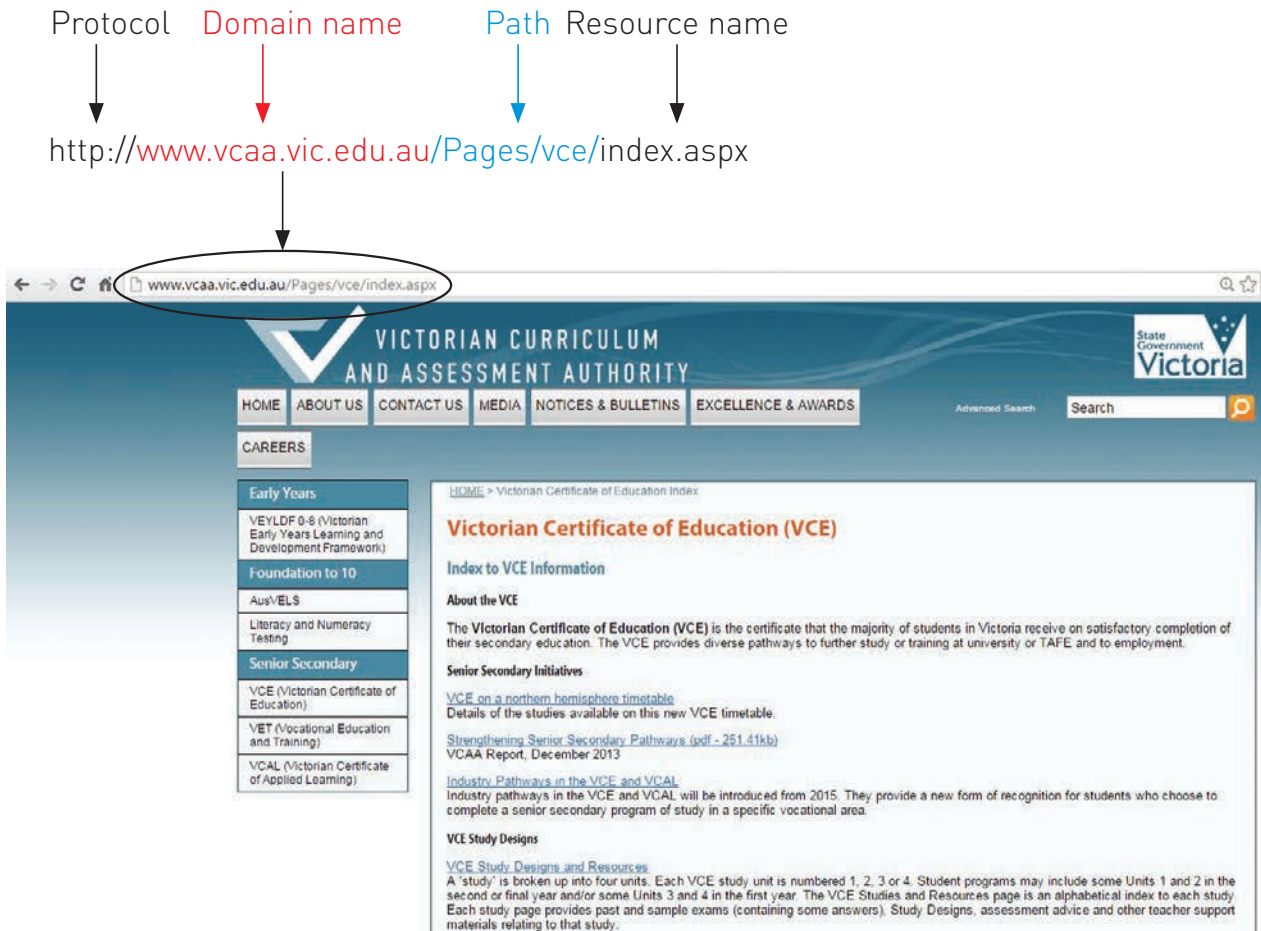


FIGURE 3.17 A URL contains a protocol, domain name, path and resource name



FIGURE 3.18 A secure connection is indicated by 'https://' appearing in the URL and the lock symbol, in this case to the left of the address bar.

Email

Email is the transmission of messages and files via a computer network. Email can be sent over the internet or within a LAN. Email software is used to create, send, read, forward, reply and print emails. A client-server network will have a mail server established to handle the receipt and delivery of mail to and from the LAN over the internet.

File transfer protocol

File transfer protocol (FTP) is an internet standard that allows computers to upload and download files. Uploading is the process of transferring a document, graphic or video from the user's computer to a server on the internet. When someone creates a webpage they need to upload it and associated resources to their ISP's web server using FTP. Files can be downloaded from an internet server to a user's computer also using FTP.



A list of Australian VoIP providers together with plan prices and call rates can be found at VoIP Choice.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) allows users to speak to other users over the internet. Users need a high-speed internet connection (broadband cable, NBN cable or ADSL 2+), a microphone or alternative audio input device such as existing phones, VoIP adaptor and subscription to a VoIP provider. A VoIP app needs to be installed on a mobile device such as a smartphone.

If calls are mostly within Australia, then a local provider will make billing easier and likely will provide better quality service. If international calls are important, then an overseas provider may offer the best value. There is no reason why users need to limit themselves to just one provider. A local provider for calls within Australia and an overseas provider for international destinations may prove to be the best strategy.

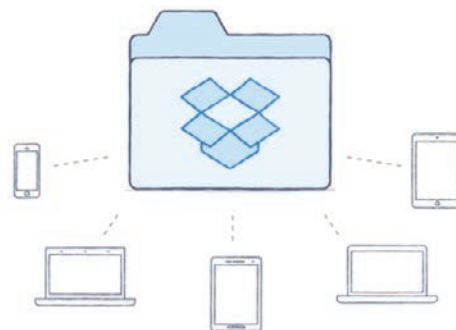
International VoIP providers can allocate users an indial number for use in many countries. This is particularly useful in situations where contacts do not have internet access, such as in some developing countries. An indial number is allocated to the city of the user’s choice so that overseas friends and family can call that local indial number to connect with the user. The call is treated as a local call, which saves money.

Cloud storage

Cloud storage refers to saving data to an off-site storage system maintained by a third party. Data is saved to a remote database using the internet rather than on a computer’s hard drive (see Figure 3.19). The advantages of cloud storage are that data can be accessed from any location in the world that has internet access and there is no need to carry a storage device or use the same computer to access data that was used to create it. Cloud storage encourages collaborative work practices since members of a project team can be given read and write access rights to the data held in the cloud.

THINK ABOUT COMPUTING 3.6

What are some potential drawbacks of cloud storage?



Why upgrade to Dropbox for Business?

It's the power of Dropbox, built to help your team work together and get even more done. Just create a folder, share it, and start collaborating instantly. Dropbox for Business works with all the apps your team already uses to be productive – everything from Word and Excel to Photoshop and Acrobat. Plus support for Windows, Android, iOS, Mac, and Linux mean no one's left out in the cold.



Any app, any format



Desktop, mobile, web



Simplified sharing

FIGURE 3.19 Dropbox is a file-hosting service that allows users to store and share files over the Internet.

Network communications standards

Today's networks connect terminals, devices and computers from many different manufacturers across many types of networks. These include wide area and local area networks, which use both wireless and wired communication channels. For the different devices on several types of networks to be able to communicate, the networks must use similar techniques for moving data from one application to another.

To avoid problems associated with incompatibility between hardware and software components, organisations such as the Institute of Electrical and Electronics Engineers (IEEE) develop network standards. A **network standard** defines guidelines that specify the way computers access the medium to which they are attached, the type of medium used, the speed at which data flows and the physical technology used. A standard that defines how two network devices communicate is called a **protocol**. The manufacturers of hardware and software must design their products in accordance with the appropriate standard to ensure that their devices can communicate with the network.

Standards are important in the computer industry because they allow the combination of products from different manufacturers to create a customised system. Without standards, only hardware and software from the same company could be used together. In addition, standard user interfaces make it much easier to learn how to use new applications.

As data flows through a network from one application to another, it may use one or more standards. Some of the widely used network communications standards and protocols for use in both wired and wireless networks are Ethernet and TCP/IP.

Ethernet

Ethernet is a popular network standard that allows personal computers to contend for access to the network.

Ethernet is a popular LAN standard because it is relatively inexpensive and easy to install and maintain. Ethernet networks use cables to transmit data.

The speed at which data is transmitted is usually expressed as bits per second (bps). The original Ethernet standard is not very fast by today's standards – standard Ethernet transfer rate is 10 Mbps. A second Ethernet standard, called Fast Ethernet, transmits data and information at speeds of 100 Mbps, up to 10 times faster than the original standard. Gigabit Ethernet is now in use in many graphic-design studios, and provides an even higher speed of transmission, with speeds up to 10 times faster than Fast Ethernet.

Fast Ethernet uses the same twisted pair cabling as standard Ethernet with upgraded switches and adapters. Signals with Fast Ethernet travel up to 100 Mbps. Gigabit Ethernet (1 Gbps or higher) requires cables capable of handling this faster speed (see Figure 3.32).

When a workstation on an Ethernet network wishes to transmit, it checks the network to see if it is not busy and then broadcasts a **packet**. A switch ensures that if the packet is addressed to workstation #15, only workstation #15 will read it. If two workstations simultaneously check the network, find it is not busy and send packets at the same time, a collision occurs. When a collision occurs, a special signal travels over the network to indicate that it is 'jammed'. The workstations that sent the messages wait a random amount of time before resending their packets.

An analogy for a **network protocol** would be to consider a computer on a network as a person. The language that person speaks is the network protocol. Only two people who speak the same language can communicate with each other. Similarly, only computers that have the same network protocol can communicate on the network. Just as some people are able to speak several languages, computers on a network may have several different protocols installed and running.

The IEEE is a leading authority in technical areas, ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace engineering and consumer electronics. The American National Standards Institute (ANSI) is another organisation that has developed globally accepted network standards.

Twisted pair cabling is discussed on page 110.

TCP/IP

TCP/IP (transmission control protocol/internet protocol) is a network standard that manages the transmission of data by breaking it up into packets and transmitting the packets over the internet. An important part of the IP protocol is the IP address. The IP addressing standard – four numbers between 0 and 255 separated by full stops – defines a mechanism to provide a unique address for each computer on the network.

A typical TCP/IP packet contains less data than other network protocols. On a WAN, such as the internet, the smaller size allows the packets to travel in multiple paths to the destination. On a LAN there is often only one viable path to the destination, so larger packets are more sensible (less space is allocated to addresses and communications information). Nevertheless, most LANs are now running the TCP/IP protocol because intranets require files to be communicated in this medium.

When a computer sends data over a network, the data is divided into packets. Each packet contains the data, the recipient (destination) information, the sender (origin) information, and the sequence information used to reassemble the data at the destination (Figure 3.20). These packets travel along the fastest available path, avoiding congestion and broken links to the recipient's computer via routers (routers were discussed on page 90). This technique of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data is called **packet switching**.

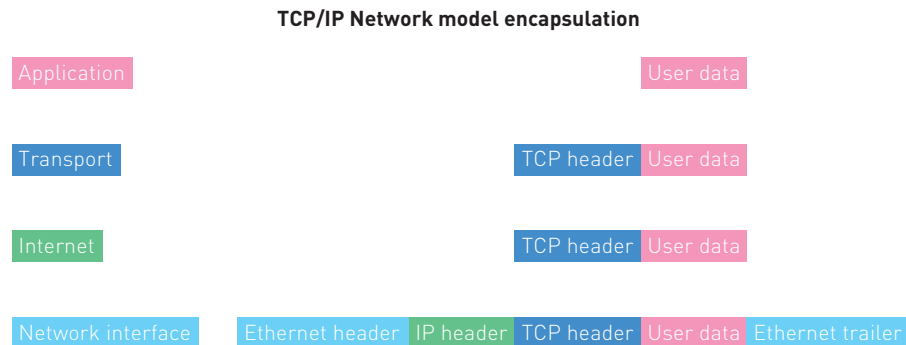


FIGURE 3.20 TCP/IP Network model encapsulation. At each network layer another piece is added to the data packet. The Ethernet frame at the network interface level, consists of a header containing the destination and source address, the middle section, which includes the data and headers for IP and TCP protocols, and a final section that checks for correct transmission.

Some blocks of IP addresses are set aside for internal private use by computers not directly connected to the internet. They are used by business or home networks that need to use TCP/IP but do not want to be directly visible on the internet. The block 10.0.0.0 to 10.255.255.255 is commonly used by school networks and other large organisations with many nodes. Home networks often use the block 192.168.0.0 to 192.168.255.255 to assign addresses to connected devices while IP addresses from 172.16.0.0 to 172.31.255.255 are also for private use. Home network routers often have 192.168.0.1 as their default IP address.

ISSUE**Are we running out of IP addresses?**

Currently you should not have any trouble connecting your computer to the internet using the Internet Protocol (IP). The version of IP address in common use for many years was Internet Protocol Version 4 (IPv4). An IPv4 address has four groups of numbers that range from 0 to 256 separated by a decimal point (the system is called a dotted decimal number). Each group of numbers is called an octet. The first octet identifies the network on which a computer resides, and the remaining three octets together identify the specific computer or host within that network. The four octets in an IPv4 address allows 2 to the power of 32, or a little over 4 trillion (4×10^9), unique values. Some of these are reserved for special use, leaving more than 3 trillion available addresses.

Three trillion addresses may sound like a lot; however, because so many computers and other devices connected to the internet need a unique address, there is a shortage of IP addresses. To overcome this shortage, a new version of IP addressing was developed. Internet Protocol Version 6 (IPv6) lengthens IP addresses from 32 bits (the octet size) to 128 bits, and increase the available IP addresses to 340×10^{38} .

IPv6 uses eight hexadecimal strings to specify the address. The problem is that adopting the new IP version requires organisations to reconfigure their networks and possibly update their switches to accommodate the new standard.

Home networks and smaller corporate networks do not have enough devices attached to warrant the implementation of IPv6. For the time being, home networks will remain within the 192.168.0.0 to 192.168.255.255 private address block provided by IPv4.

A tablet connected to the Internet on a home wi-fi network can use IPv4. If the tablet is used on a 4G mobile network it will need IPv6.

The 802.11 standard

The **802.11 standard** was developed to specify how two wireless computers or devices communicate with each other via radio waves. This standard uses techniques similar to those of the Ethernet standard and is therefore easy to integrate into existing wired Ethernet networks. The range of wireless communications is up to 300 metres in open areas outside, and about 50 metres inside buildings. Wireless networks are popular in locations where there is no existing wired system, or where the construction of the building makes it difficult to add a wired network. For example, it can be difficult to place wires inside the brick or solid plaster walls that are common in older buildings.

The term wi-fi (wireless fidelity) identifies any network based on the 802.11 series of standards.

The older 802.11b and 802.11g standards use frequencies in the 2.4 GHz band and employ direct sequence spread spectrum technology to avoid interference from microwave ovens, Bluetooth devices and cordless phones. The 802.11n standard uses 2.4 GHz and/or the 5 GHz band. The higher frequency allows the signal to carry more data. The 802.11n standard transmits data at up to 150 Mbps. The newest standard, 802.11ac, operates in the 5 GHz band with data transmission of 1300 Mbps.

THINK ABOUT COMPUTING 3.7

The new IPv6 standard is needed because we are about to run out of IPv4 addresses. Do you think all organisations should be forced to adopt the IPv6 standard to increase the number of addresses available? Do you think the demand for IP addresses will increase over the next few years in the same way that it has over the last 10 years, or will there be an escalation? If an escalation were to occur, what might be the trigger?

The 5 GHz band is not populated by many devices, hence it tends to be quieter, meaning there is less interference from neighbourhood networks or other devices. The 802.11ac standard also makes use of **beamforming**, which means it detects where devices are and intensifies the signal in their direction, rather than using the scattergun approach of earlier standards. The result is the 802.11ac standard allows fibre optic broadband speeds throughout a house, with multiple streams of full high-definition content.

Sending and receiving devices

Sending and receiving devices initiate or accept the transmission of data, instructions and information. Notebook computers, desktop computers, tablets, midrange servers and mainframe computers can all serve as sending and receiving devices. These computers can communicate directly with another computer, with hundreds of computers on a company network or with millions of other computers on the internet.

Web-enabled hand-held computers and devices also serve as sending and receiving devices. A **web-enabled device** provides access to the internet and email from any location. Examples are smartphones and GPS receivers.

Earlier in this chapter we noted that communication over a global network requires:

- a sending device, such as a computer
- a communications device attached to the sending device, such as a cable modem
- a communications channel – either cable, radio, microwave or satellite
- a communications device at the receiving end
- a receiving device that accepts the data or information.

Mobile devices connected to networks

Mobile devices are usually small enough to fit in a pocket. These devices store programs and data permanently on special memory inside the system unit or on a flash memory card. They can usually be connected to personal computers to exchange information or to install applications.

Most mobile devices can be connected wirelessly to the internet. This allows users to chat, send messages, email and access websites. Internet-enabled mobile devices in common use include smartphones, hand-held computers, navigation systems, games consoles and digital cameras. A convergence of technologies has resulted in some devices including functions and features from two or more different types of devices, while other devices like personal digital assistants (PDAs) have become redundant.

Tablets

A **tablet** is a special type of notebook or laptop computer that resembles a letter-sized slate, which allows a user to write on the screen using a digital pen. Tablets are able to connect to wi-fi networks to gain access to the internet and other network resources. Tablets are designed to be held rather than sat on a desk or in the user's lap. Tablet computers have a number of capabilities and some limitations.

TABLE 3.3 Capabilities and limitations of tablet computers

Capabilities of tablets	Limitations of tablets
Allows users to: <ul style="list-style-type: none"> • surf the internet • send and receive emails • operate a calendar of events • play music • take pictures • store images • use GPS to identify location • run apps. 	<ul style="list-style-type: none"> • No physical keyboard • Difficult to print from • Applications are limited to running on iOS, Android or Windows devices. Some Windows-based software used by businesses is not available on either platform

Smartphones

Besides acting as a phone for voice-based communications, a **smartphone** allows users to send emails and access the web (Figure 3.21). For many businesspeople, smartphones are replacing notebook computers, especially if their work involves frequent travel. A smartphone and its charger weigh about 200 grams, compared with a laptop computer and its related accessories that weigh 2–3 kilograms.

Smartphones communicate wirelessly with other devices or computers. They also function as a portable media player and a digital camera. Smartphones have a number of capabilities and some limitations.

TABLE 3.4 Capabilities and limitations of smartphones

Capabilities of smartphones	Limitations of smartphones
Allows users to: <ul style="list-style-type: none"> • make and receive phone calls • surf the internet • send and receive emails • operate a calendar of events • play music • take pictures • store images • use GPS to identify location • run apps. 	<ul style="list-style-type: none"> • Screens are smaller than a desktop or tablet, so only a few lines of a document can be displayed • Many webpages are not designed for a small screen • The keyboard is usually a touch screen and smaller than a standard keyboard, so correct data entry can be difficult • Difficult to print from

Most smartphones can connect directly to Bluetooth-enabled devices, such as keyboards and printers. Bluetooth connections are discussed later in this chapter.

Mini-applications software, also called **apps**, are a significant component of smartphones. Smartphones come pre-loaded with apps for social networking, photography, travel and more. Additional apps can be downloaded from Apple's App Store (for iPhone clients), Google's Play Store (for Android devices) or the Microsoft Store (for Windows phones).

The increasing popularity of internet-connected mobile applications among businesspeople, teenagers and students is producing a strain on carrier networks. Applications on portable devices that require continuous connection to a website can place a huge load on wireless networks. As these devices become more popular, the traffic on networks is only going to increase, putting further pressure on the ability of carriers to cope.

**FIGURE 3.21** The Samsung Galaxy S6 is a web-enabled smartphone.

Shutterstock.com/Zeynep Demir

THINK ABOUT COMPUTING 3.8

Describe how the limitations of smartphones may in part be overcome or addressed.

Australia's digital economy grew strongly during 2012–13 with increases in internet usage and mobile phone access to the internet, according to the ACMA Communications report tabled in Parliament. The report stated that 7.5 million Australians were accessing the internet via their mobile phones during June 2013, an increase of 33 per cent compared to June 2012. There were 11.19 million smartphone users in Australia in May 2013.

Shutterstock.com/Voznikovich Konstantin



Getty Images/Arno Masse

Handheld data-collection devices

As the name implies, a hand-held data collection device is small enough to fit into your hand. Hand-held devices communicate wirelessly with other computers and devices, and many have miniature or specialised keyboards. Some hand-held devices use a stylus for data entry, including recording a client signature to acknowledge receipt of goods.

Hand-held computers (Figure 3.22) are often used by people who need to record information as they travel; for example, electricity and water meter readers, scientists collecting natural resource data in the field and couriers who deliver parcels. Table 3.5 lists the capabilities and limitations of hand-held data collection devices.

FIGURE 3.22 A handheld data-collection device is used for high-volume data collection, and features a touch screen, keyboard and number pad.

There is concern that drivers relying on GPS are performing illegal or dangerous acts. For example, the rural village of Wedmore, in England, has seen its share of truck drivers wedged between buildings because they blindly followed the route their GPS planned out – regardless of the fact that trucks are prohibited from the village because of their size. There have also been cases in which GPS units have directed drivers onto train tracks or the wrong way down a one-way street.

TABLE 3.5 Capabilities and limitations of hand-held data collection devices

Capabilities of handheld devices	Limitations of handheld devices
<ul style="list-style-type: none"> • Designed to operate outdoors in variable weather conditions • Shockproof • High visibility screens even in sunlight • Runs apps of spreadsheets, word-processors, presentation software, calendar and email • Allows users to reach a specified location using GPS • Allows the collection, storage and management of large amounts of data • Data collection can be tagged to location using GPS coordinates • Data can be transferred to larger computers or networks using Bluetooth or wi-fi 	<ul style="list-style-type: none"> • Screens are smaller than a desktop or tablet, so only a few lines of a document can be displayed. • The keyboard is smaller than a standard keyboard, so correct data entry can be difficult. • Text written with a stylus may not be easy to read.

Navigation systems

The **global positioning system (GPS)** is a navigation system made up of a group of at least twenty-four satellites that communicate with a fixed or portable device mounted in, for example, a car. The GPS navigation device is able to pinpoint the car's location to within 15 metres (see Figure 3.23). It receives three-dimensional data – latitude, longitude and altitude – as well as precise time. The car's position is then overlaid with digital mapping, and navigation information is stored within the GPS receiver. From this the device is able to give the driver directions, suggest a route around congested traffic or locate a petrol station. The text-to-speech function allows the GPS device to read street addresses rather than simply provide left and right turn directions. This allows drivers to keep their eyes on the road.

Smartphones have GPS technology built in to them. Parents can locate a child's whereabouts through a smartphone with a GPS receiver (Figure 3.24).

Shutterstock.com/3d brained

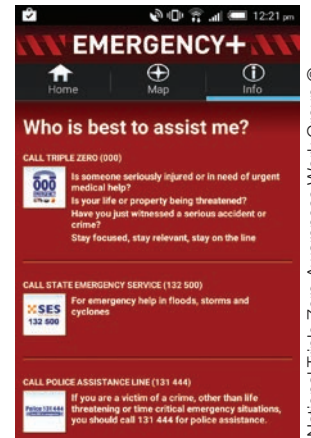


FIGURE 3.23 The GPS navigation device receives three-dimensional data from a satellite network, which enables the receiver to pinpoint the car's location and give travel directions to the driver.



Getty Images/Patrick T. Fallon/Bloomberg

FIGURE 3.24 Life360 is an app for a smartphone that allows parents to set up a circle of family members and follow their movements on a map, communicate with them, and receive alerts when members arrive at home, school or work.



National Triple Zero Awareness Work Group © Fire Rescue New South Wales

FIGURE 3.25 Emergency + is an app developed by the NSW Fire Rescue Service.

TABLE 3.6 Capabilities and limitations of GPS devices

Capabilities of GPS devices	Limitations of GPS devices
<ul style="list-style-type: none"> Receives latitude, longitude and altitude data from satellites Plots accurate location on a map Can be used to plan a route Provides audio directions Can provide traffic information and speed limit alerts Locate places of interest such as petrol stations 	<ul style="list-style-type: none"> Accuracy may be variable due to triangulation issues and atmospheric conditions GPS receivers are accurate to within 15 metres on average, though some systems might improve accuracy to 3 metres Devices do not connect to satellites in thick tree covering or in a gorge The device may provide a direct route rather than the safest route

The NSW Fire Rescue Service has released an app for mobile phones (see Figure 3.25) that uses a smartphone's GPS function to locate exactly where a person is. Users in an emergency can provide the 000 operator with their precise location – either the address or map coordinates.

THINK ABOUT COMPUTING 3.9

Suna is an automated traffic congestion notification system used by VicRoads. Investigate what information is provided by the system and how the data is collected.

Wearable technology

AFL coaches are keen to know how fast a player runs, track exactly where they go and collect data on the movements of groups of players, such as defenders or the on-ballers. Players wear a wireless position locating system (Figure 3.26) developed by CSIRO in a pouch on their backs. These devices use wireless signals and hence work in areas that GPS satellites do not reach, such as in Etihad Stadium when the roof is closed.

This is a wireless ad-hoc system for positioning (WASP) technology and it monitors player movements on the field. The device is called ClearSky and is used by international sports associations, including the US National Football League (NFL). Rather than using satellites, the WASP system uses fixed reference nodes usually located inside the stadium. The mobile device measures the time it takes signals to travel to each of the fixed nodes and uses triangulation to work out the player's position. The WASP system has accuracy down to 20 cm (compared to 3 metres for GPS systems).

A combination of heart rate measurements and position tracking allows clubs to monitor player fatigue and improve training.

Wearable technology falls into three broad areas – notifiers, trackers and glasses. The notifiers are devices that show off the world around you. Pebble Steel is a smartwatch that can load iPhone and Android apps. Trackers use sensors to record data and include cameras, audio recorders, fitness-tracking devices (see Figure 3.27) and pedometers. Glasses include virtual displays worn on the head. The website www.bluetooth.com/Pages/wearables.aspx describes some uses of wearable technology.



Getty Images/Adam Trafford/AFL Media

FIGURE 3.26 AFL players wear a wireless position locator on their backs so that their movement around the ground can be analysed.



Shutterstock.com/BsWei

FIGURE 3.27 Wearable devices are being used to improve our daily lives, health care and safety; such devices include fitness trackers, health care monitors, smartwatches, heads-up displays and smart clothing.

TABLE 3.7 Capabilities and limitations of wearable technologies

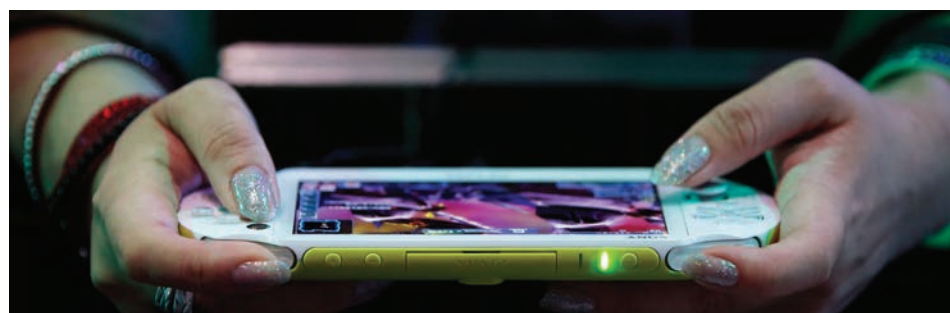
Capabilities of wearable technologies	Limitations of wearable technologies
<ul style="list-style-type: none"> • Body sensors that track information relating to health and fitness • Synchronise with the user’s smartphone using Bluetooth • Smart watches run apps and identify incoming calls on smartphones 	<ul style="list-style-type: none"> • Some of the wearables can be uncomfortable • Contacts can degrade if they get worn or dirty leading to incorrect readings or none at all • Power requirements require regular replacement of batteries (if not rechargeable) • Static electricity (from sports uniform) and electric fields from other devices can cause erroneous results • Most wearables lack a screen so immediate feedback from a tracking app is not possible • Some wearables are limited to connection with a particular smartphone • Devices may have limits to the number of apps they can hold at a time • Portability and size means the devices can be lost or misplaced

Games consoles

A **game console** is a computing device designed for single-player and multi-player video games. A standard game console uses a handheld controller for input, a television screen for output and a hard disk or memory disk for storage. Popular models include Microsoft’s Xbox One, Sony’s PlayStation 4 and Nintendo’s Wii U.

A smaller handheld game console fits in the users hands and includes the controls, screen and speakers in the one portable device (Figure 3.28).

 The first home video game was called Magnavox Odyssey and was released in 1972. The console lacked a CPU so cartridges were used for each separate game – tennis, volleyball and chase. The home game industry struggled until the Atari game Pong became popular in the early 1970s.



Getty Images/Kiyoshi Ota/Bloomberg

FIGURE 3.28 A portable game console MP5 player

TABLE 3.8 Capabilities and limitations of game consoles

Capabilities of game consoles	Limitations of game consoles
<ul style="list-style-type: none"> • Play games using Blu-ray disks or digital downloads • Wi-fi connection to internet • Upload saved data to a cloud server • 3D graphics • Stream videos from an online source • Stream gameplay to an online service, such as Ustream • Record videos and images for posting online • Social connectivity – voice chat with online players or group chat with friends 	<ul style="list-style-type: none"> • Tend not to be upgradeable – technological advances require a new model • Old consoles do not play media designed for a newer model • The manufacturer’s monopoly over a particular console market forces developers to certify games for that platform. This in turn can force limits on the functionality that can be built into games.

Network-attached storage device

A **network-attached storage (NAS)** device acts as a centralised repository for data. NAS devices (Figure 3.29) share files across a network. In a home environment, the files are often videos, photos or audio files. Most NAS devices can be used as a multimedia server which can share and stream multimedia files to network clients such as computers, tablets, game consoles and phones. A NAS used on a home network is likely to have storage capacity of about 16TB. Most NAS devices require a cable connection to a switch that has Gigabit Ethernet connectivity.



Shutterstock.com/ShawnWilkinson

One terabyte (1 TB) is the same as one thousand gigabytes (1000 GB) or one million megabytes (1 000 000 MB).

FIGURE 3.29 A network-attached storage (NAS) device

Communications channel

An important aspect of communications is the **channel**, which is the communications path between two devices. **Bandwidth** is the width of the communications channel. The higher the bandwidth, the more data and information the channel can transmit.

For transmission of text-based documents, a lower bandwidth delivers acceptable performance. If you transmit music, graphics and photographs, or work with virtual-reality or 3-D games, you need a higher bandwidth. When the bandwidth is too low for the application, you will notice a considerable slowdown in system performance. For example, movies may ‘stutter’ or pause while buffering more data.

A communications channel consists of one or more **transmission media**. When you send data from your computer to another device, the signal carrying that data most likely travels over a variety of transmission media.

Transmission media are either physical or wireless. **Physical transmission media** use wire, cable or fibre-optics to send communications signals. **Wireless transmission media** send communications signals through the air or space using radio, microwave and infra-red signals.

Physical transmission media

Physical transmission media used in communications include **twisted-pair cables** and fibre-optic cables. These are typically used within buildings or underground. Ethernet LANs often use physical transmission media. Many wireless LANs rely on physical cables to transmit data between a switch or router and a wi-fi device such as a wireless access point. Table 3.9 lists the transfer rates of LANs using various physical transmission media.

TABLE 3.9 The speeds of various physical transmission media when they are used in LANs

Type of cable	Transfer rates
Twisted-pair cable	
10Base-T (Ethernet)	10 Mbps
100Base-TX (Fast Ethernet)	100 Mbps
1000Base-T (Gigabit Ethernet)	1 Gbps
Fibre-optic cable	
10Base-FL (Ethernet)	10 Mbps
100Base-FX (Fast Ethernet)	100 Mbps
Gigabit Ethernet	1 Gbps
10-Gigabit Ethernet	10 Gbps

Noise in a cable can be caused by cross-talk (electric currents between pairs of wires in the same cable) and outside electrical fields, such as power lines, motors and radio transmitters. The greater the cable's ability to resist internal and external noise, the longer the cable that can be used to connect workstations and resources.

Twisted-pair cables

One of the more commonly used transmission media for network cabling and telephone systems is the **twisted-pair cable**. This cable contains one or more twisted-pair wires bundled together (see Figure 3.30). Each **twisted-pair wire** consists of two separate insulated copper wires that are twisted together. The wires are twisted together to reduce noise. Noise is an electrical disturbance that can degrade communications.

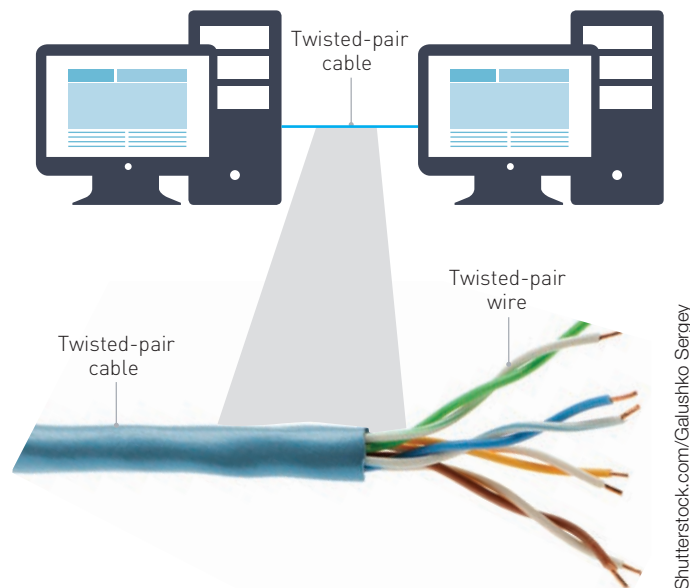


FIGURE 3.30 A twisted-pair cable consists of one or more twisted-pair wires; each twisted pair wire is usually colour-coded for identification. Telephone networks and LANs often use twisted-pair cables.

Fibre-optic cable

The core of a **fibre-optic cable** consists of dozens or hundreds of thin strands of glass or plastic that use light to transmit signals. Each strand, called an **optical fibre**, is as thin as a human hair. Inside the fibre-optic cable, an insulating glass cladding and a protective coating surround each optical fibre (Figure 3.31).

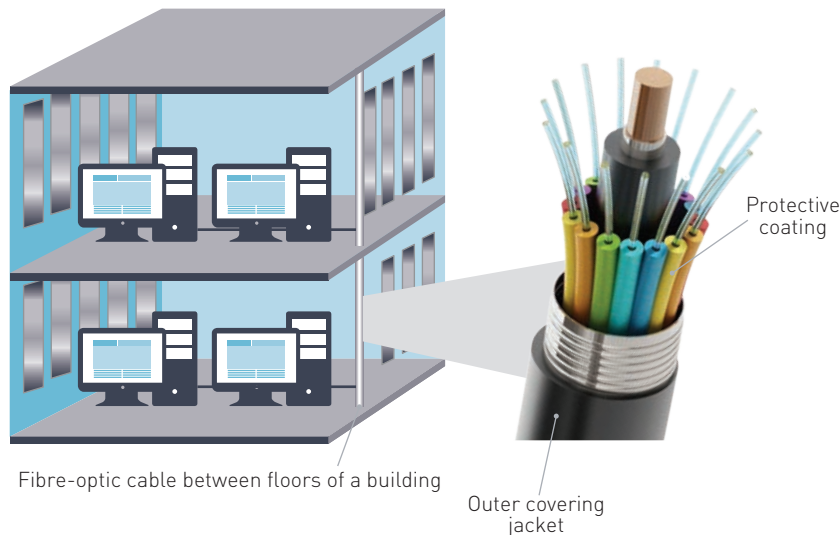


FIGURE 3.31 A fibre-optic cable consists of hair-thin strands of glass or plastic that carry data as pulses of light.

Fibre-optic cables have several advantages over twisted-pair cables. These advantages include:

- the ability to carry significantly more signals than wire cables
- faster data transmission
- less susceptibility to noise (interference) from other devices, such as a copy machine
- better security for signals during transmission as they are less susceptible to noise
- their smaller size (much thinner and lighter).

The material used for fibre-optic cable has optical properties that cause light in the cable to totally internally reflect from the outer surface. This allows all the light to progress down the cable rather than escape to the surrounding air. As fibre-optic cables use pulses of light, they have total immunity from electrical noise. Signals can therefore be sent over much larger distances than with twisted-pair cables.

The disadvantages of fibre-optic cable are that it costs much more than twisted-pair and it can be difficult to install and modify. Despite these limitations, many local and long-distance telephone companies and cable television operators are replacing existing telephone and coaxial cables with fibre-optic cables. Many businesses are also using fibre-optic cables in high-traffic networks or as the main cable in a network.

National Broadband Network (NBN)

The National Broadband Network (NBN) is designed to provide infrastructure for affordable and reliable high speed internet and telephone access to all Australians. The nature and size of Australia means that a variety of technologies are required to deliver the NBN. The original NBN proposal was for communications of 100 Mbps, with fibre-optic cable connecting the internet directly to homes. The scheme has been modified with a change of government, so that the plan

At a connection speed of 25 Mbps the NBN will have a similar maximum speed to ADSL 2+ connections (24 Mbps).



View the progress of the NBN rollout at the NBN website.

THINK ABOUT COMPUTING 3.10

Some future speculators believe that by 2023 households will have more than 100 devices connected to the internet. Devices such as lights, air conditioners, heating systems, door locks, irrigation systems, motion detectors, smoke detectors, home entertainment systems and connections that monitor family members, pets and vehicles all will require bandwidth. Online video chatting will become common practice and requires fast download and upload speeds. Do you think that 25 Mbps provide adequate bandwidth in five to 10 years' time? What devices do you expect to be connected in your home in 10 years' time?



AAP Image/NENCO

FIGURE 3.32 The roll-out of the NBN

is for fibre-optic cable to reach a node in the street (called the 'street cabinet') from where it will be split and hybrid cables or existing copper telephone networks used to carry signals to homes and businesses. The revised specifications indicate connection speeds of about 25 Mbps. The government argues that this is more than adequate for domestic connections. The estimate for the revised NBN network is A\$29.5 billion (the original estimate was A\$37.4 billion) with a completion date of 2019 (Figure 3.32).

Households where it is impractical to use fibre cable will connect to the NBN via fixed wireless and satellite technologies. It is estimated that up to 10 per cent of homes will need wireless or satellite connections.

Wireless transmission media

Wireless transmission media are used when it is inconvenient, impractical or impossible to install cables. With the faster speeds afforded by the 802.11ac standard, wireless connections are on a par with wired networks. Wireless transmission media used in communications include broadcast radio, cellular radio, microwaves, communications satellites and infra-red.

TABLE 3.10 Transfer rates of various wireless transmission media

Transmission medium	Transfer rates (maximum)
Bluetooth	1–2 Mbps
HomeRF	1.6–10 Mbps
802.11a	54 Mbps
802.11b	11 Mbps
802.11g	54 Mbps
802.11n	108–600 Mbps
802.11ac	867–1300 Mbps
Cellular radio	
2G	9.6–19.2 Kbps
3G	200 Kbps–2 Mbps
4G	2–12Mbps
Microwave radio	150 Mbps
Communications satellite	1 Gbps
Infra-red	115 Kbps–4 Mbps

An 802.11ac wireless router operates on the 5 GHz bandwidth but can still run on the 2.4 GHz network simultaneously. Some vendors may quote a wireless 802.11ac router as a single speed device operating at 1.75 Gbps. This figure is an amalgamation of the 5 GHz and 2.4 GHz capabilities of the router. That is, it is the addition of 1.3 Gbps from the 5 GHz connection with 450 Mbps from the 2.4 GHz network.

Wi-fi communications

For **wi-fi communication** transmissions, you need a transmitter to send the radio signal and a receiver to accept it. To receive the signal, the receiver has an antenna that is located in the range of the signal. Some networks use a transceiver, which both sends and receives signals from wireless devices. Wi-fi communication is slower and more susceptible to noise than physical transmission media, but it provides flexibility and portability.

Wireless computer network components typically use radio signals in either a 2.4 GHz range or a 5 GHz range. A 5 GHz network can carry more data than a 2.4 GHz network; however, the higher the frequency of a radio signal, the shorter its range. So a 2.4 GHz network covers a much larger range than a 5 GHz network. The higher frequency is not as good at penetrating solid obstacles such as walls. On the other hand, there are a number of household devices, such as cordless phones, that operate on the 2.4 GHz band that could interfere with the broadcast transmissions. The 5 GHz band does not compete with other common household devices. A number of components now come with dual band capacity to get the best of both worlds.

Bluetooth

Bluetooth uses short-range radio waves to transmit data among Bluetooth-enabled devices. These devices contain a small chip that allows them to communicate with other Bluetooth-enabled devices. Examples of these devices can include desktop personal computers, notebook computers, hand-held computers, mobile telephones, fax machines and printers. To communicate with one another, they must be within a specified range (about 10 metres, but the range can be extended to 100 metres with additional equipment). A popular use of Bluetooth is to enable hands-free chatting on mobile phones. Most cars are now sold with a built in Bluetooth station that the user can synchronise with their mobile phone. Bluetooth and wi-fi communications technologies use radio signals.

Bluetooth gets its name from a legendary Viking king (one of the main developers was the Norwegian communications company Ericsson). One advantage of Bluetooth is that it can be used to set up a network on the spur of the moment. A group at a meeting can all network their computers to share files, access data from mobile telephones, and send documents to printers and fax machines, all without cables or additional network interface cards. Of course, all of the devices must be Bluetooth-enabled. Data transmission using Bluetooth is fairly slow compared with other wireless transmission media.

Near field communication



AAP/AP Photo/Manu Fernandez

FIGURE 3.33 An example of a near field communication use for short-range contactless communication.



FIGURE 3.34 The myki public transportation ticketing system uses near field communication to read a commuter's details from their smart card.

THINK ABOUT COMPUTING 3.11

Use the Internet to explore creative ways in which people are using NFC tags.

There are four types of NFC tags. Type 1 tags store 96 bytes and operate at 106 Kbps. The biggest and fastest tag is Type 4 which can store up to 32 KB and transmit at 424 Kbps. Type 1 and 2 tags can be written to multiple times, or can use encryption, which permanently locks them so the data cannot be manipulated. Type 3 and 4 tags can be written to once only.

Near field communication (NFC) is a form of contactless communication between devices like smartphones or tablets. A user is able to wave their smartphone over a NFC compatible receiver to send information without needing to touch the devices together or set up a formal connection. A customer can simply wave their smartphone near a NFC device to pay for goods purchased in stores or pay for a parking meter (the parking meter can even send messages to the smartphone indicating how much time is left).

An unpowered chip, called a tag, can be used with an NFC device, such as a smartphone with NFC capability. The tag draws its power from the device that reads it using electromagnetic induction. A smartphone can be paired with an NFC tag which can be programmed by apps on the phone to automate tasks. For example, tapping on a smart tag on a poster will transfer information from an embedded chip in the poster onto the smartphone. So a user tapping a movie

advertising poster will receive comprehensive details about the film, such as session times, biographies of leading actors, reviews and more, on their smartphone. Tapping on a menu in a restaurant could load the menu into the phone with nutritional information and cooking notes.

NFC tags are small and cheap to produce, so are suited for a range of uses involving mobile payments and creative marketing. More interesting uses will appear as people get more aware of the capabilities of NFC (Figure 3.33).

Pay-wave transactions and Victoria's myki transportation system (Figure 3.34) are examples of cards that use NFC technology. Waving the card near a card reader allows data to pass from the card to the reader and hence the transaction is completed with little effort or time taken.

Cellular radio

A **mobile phone** is a telephone device that uses radio signals to transmit voice and digital data messages.

Cellular radio is a form of **broadcast radio** that is used widely for mobile communications, specifically mobile phones (Figure 3.35). A smartphone can be used to communicate with other

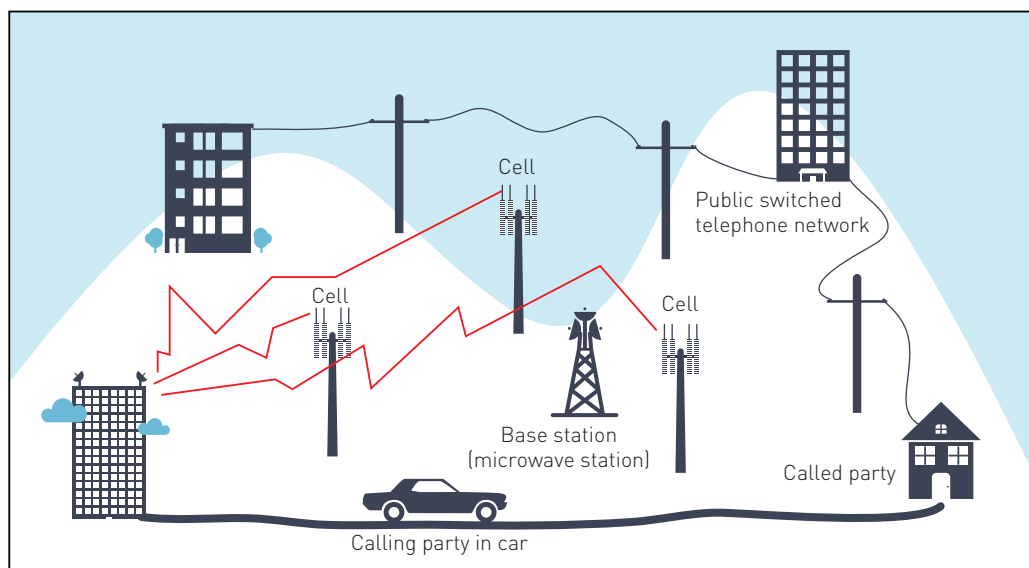


FIGURE 3.35 As a passenger in a car with a mobile telephone travels from one 'cell' to another, the radio signals transfer from the base station (microwave station) in one cell to a base station in another cell.

phones, access the Web, send and receive email, enter a chat room or connect to an office or school network while away from a standard telephone line, such as from a car or a park bench.

Several categories of cellular transmission exist.

- 1G (first generation) – transmitted analog data only
- 2G (second generation) – transmitted digital data at speeds of 9.6–19.2 Kbps
- 3G (third generation) – transmitted digital data at speeds from 200 Kbps to 2 Mbps
- 4G (fourth generation) – transmitted digital data at speeds from 2 Mbps to 12 Mbps

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave transmission involves sending signals from one **microwave station** to another (Figure 3.36).

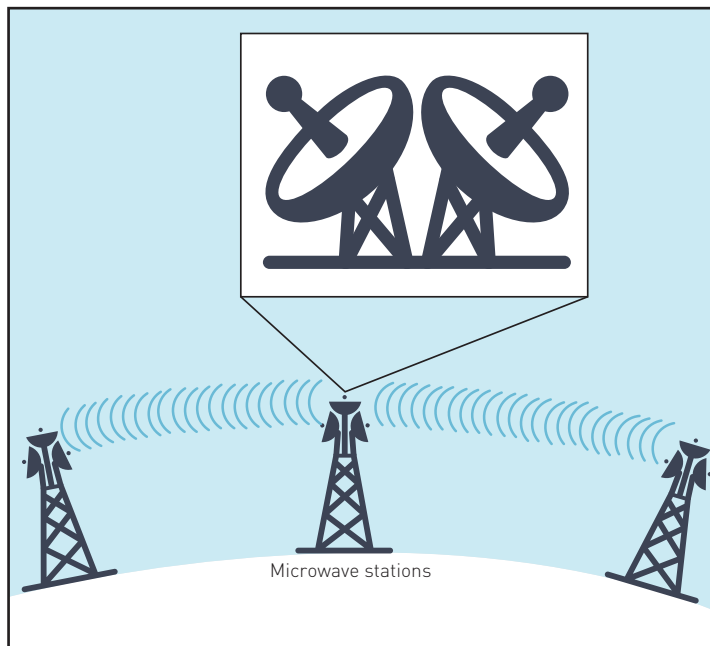


FIGURE 3.36 A microwave station is an Earth-based reflective dish that contains the antenna and other equipment necessary for microwave communications; the dish collects the signals and redirects them to the central collector.

Microwaves use line-of-sight transmission, which means that microwaves must transmit in a straight line with no obstructions between microwave antennas. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers or mountains.

Electromagnetic radiation, such as light and radio waves, travels almost as fast through the air as it does through a vacuum (about 300 000 km per second). This means that microwave communication is significantly faster than fibre optic transmissions which send laser light pulses down glass strands. The glass slows the light beam by 30 to 40 per cent. Microwave transmission is used in environments where installing physical transmission media is difficult or impossible, where the organisation occupies a large site and where line-of-sight transmission is available.

Communications satellite

A **communications satellite** is a space station that receives microwave signals from an **Earth-based station**, amplifies (strengthens) the signals and broadcasts the signals back over a wide area to any number of Earth-based stations (Figure 3.37). These Earth-based stations are often

Microwave transmissions are often a viable alternative to cabling where an organisation has premises on different sides of a major road. The cost of digging a tunnel under the road can be expensive and repairs are difficult if there is a break.

A licenced microwave link (operating at frequencies between 7 GHz and 42 GHz) would be used by organisations if the data being transferred is 'mission critical', the connection is long distance or they operate in a high density area where interference is a problem at the lower frequencies.

Although satellite internet connections are more expensive than cable internet, they are still the only high-speed option in remote areas.

microwave stations. Other devices, such as hand-held computers and GPS receivers, can also function as Earth-based stations. Transmission from an Earth-based station to a satellite is an **uplink**. Transmission from a satellite to an Earth-based station is a **downlink**.

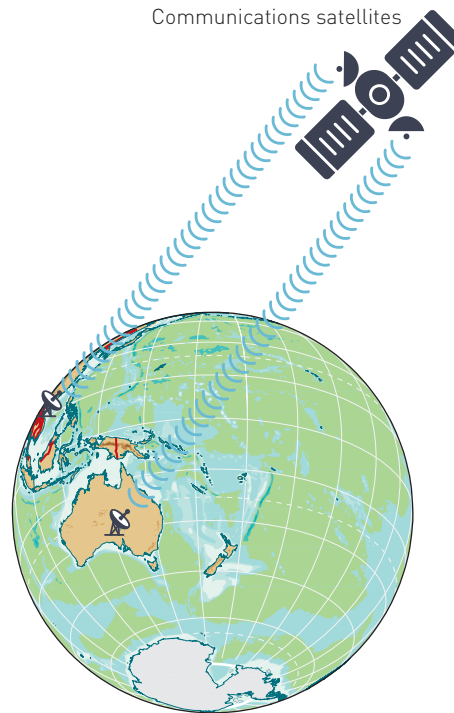


FIGURE 3.37 Communications satellites are placed approximately 37 000 kilometres above Earth's equator.

Network security

Information transmitted over networks has a higher degree of security risk than information kept on a company's premises. Many security techniques – such as usernames, passwords, biometrics and firewalls – are used by network administrators to protect a network. On a vast network with no central administrator, such as the internet, the risk is even greater. Every computer along the path of your data can see what you send and receive.

Security threats

The integrity and security of data and information stored within, and communicated between, information systems can be threatened by a number of actions, devices and events. The threats can be accidental, such as losing a portable storage device containing files; deliberate, such as denial of service and worms; or as a result of an event, such as a power surge.

Accidental threats

Some accidental threats are hard to guard against. For example, people can accidentally delete files or send attachments via email to the wrong person.

Portable memory devices are handy for storing files that you can take anywhere with you, but they can easily be lost. For example, losing a memory stick that contains important files would be inconvenient if those files were needed for a meeting or to continue working at a different location. Provided the original files were still available on a computer or network,

however, the situation is retrievable, albeit with time lost and opportunities missed. If the memory stick contained files that were irreplaceable, however, the situation could be dire. Losing a memory stick that contained strategic business information or confidential data could be critical if it fell into the wrong hands.

Deliberate threats

Deliberate threats to data and information occur when someone tries to damage or manipulate the system. This can be through a **hacker** finding a way into a network that bypasses security measures, or an employee sabotaging files or altering data for their own benefit.

A hacker tries to gain access to a network from a remote location using the internet. An authorised client using a password that is predictable or in some way compromised poses a threat to the network. Regardless of the method used, an unauthorised user can seek to damage files stored on the computer or network, steal secret information for their own advantage, or cause mischief in some way.

Networks should also be protected from deliberate attacks from **malware**, such as viruses, worms, Trojans, adware, **spyware**, keyloggers and logic bombs.

Malware is software that is created and used to disrupt computer operation, gather sensitive information or damage the system.

A **virus** is a computer program that can destroy files and alter the performance of the operating system. Once a virus is in a computer, it can spread over a network to other connected computers. The amount of damage caused by a virus depends on the maliciousness of the author. A number of viruses simply spread from file to file without causing any real damage, other than taking up storage space and perhaps the embarrassment of an email attachment being rejected by a colleague's antivirus program. There are many viruses; however, with sinister payloads: some actively destroy files, some overwrite the boot sectors on hard drives to render computers unbootable (unable to load the operating system), alter the directory information so that files cannot be accessed and an increasing number install backdoor programs that allow virus writers to take control of computers remotely. Computers with backdoor software installed are called 'zombies' and are often used for computer crime. Virus-infected files are often transmitted through peer-to-peer network connections.

Spyware is any software that covertly gathers information about a user through an internet connection without the user's knowledge or approval. Spyware is often bundled as a hidden component of free software, but can also be transferred with some software updates. Spyware monitors the user's activity on the internet and transmits that information to a third-party. The intention of spyware is to gather information about email addresses, banking details and credit card numbers.

A number of software developers offer their products as freeware (or adware) until you pay to register. Prior to registering, you may be swamped with reminders and upgrade offers. Other adware products can be embedded in browser software as an 'Add-on Extension'. Cleaning out the 'Add-on' manager regularly will reduce these annoying messages.

A **worm** copies itself repeatedly in memory or over a network, using up system resources and possibly shutting the system down. A computer virus embeds itself in some other executable software, including the operating system, on the target system. When this program is run the virus spreads to other executable files. A worm, on the other hand, actively transmits itself over the network to infect other computers. This suggests that a virus needs the operating system or user to initiate the infection, while a worm will spread by itself.

Trojans are programs that pretend to be one thing, but in reality are performing a quite different and malicious function. For example, a Trojan can pretend to be a game, while in the background it is collecting email addresses stored on your computer and sending them to spammers. Worms and Trojans most commonly use vulnerabilities in email programs to distribute themselves widely and quickly. **Logic bombs** are programs written to do something unexpected, such as deleting all your files, at a triggered event such as a date.

Keylogger software is a type of Trojan that is designed to secretly monitor and log all keystrokes. A number of keylogger programs are used for legitimate purposes, such as parental control that allows parents to track the websites accessed by their children, organisations tracking the use of computers for non-work related activities or businesses tracking keywords and phrases associated with critical commercial information that would be damaging in the wrong hands. While these uses may be legitimate, the majority of keylogger activities are related to stealing people's online payment system data.

Phishing involves sending an email to a user falsely claiming to be an established enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing emails typically purport to come from organisations such as banks. Normally, the phishing email will request the user to access a website that will closely resemble a legitimate site. The user will be asked to provide their login details or update their personal information. These are details already recorded by the legitimate organisation, but can be used by fraudsters to plunder the user's bank accounts.

Anti-virus and anti-spyware programs can be installed on computers to guard against malicious attacks. These programs need to be updated regularly to ensure they can recognise the profile of the latest threats.

Event-based threats

Event-based threats do not involve accidental or deliberate actions of a human. One example of an event-based threat would be a power surge, which occurs when the incoming electrical power increases more than 5 per cent above the normal system voltage (240 volts). A momentary surge, called a spike, can be caused by a lightning bolt striking power lines. It can result in immediate and permanent damage to a computer or network. Networks can be protected against a power surge with the use of a surge protector. A surge protector limits the voltage supplied to the computer by shorting any excess caused by a spike to ground.

A hard drive crash occurs when the hard drive malfunctions and stored data cannot be retrieved using normal procedures. The cause of a crash can be an impact that forces the read-write head of the device to scratch the disk surface, a magnetic field causing interference or some contamination such as dust or water. Special software can be used to try and retrieve lost files, but success is not guaranteed.

Measures to secure networks

An unprotected network is vulnerable to attack and this can result in serious consequences, such as corruption of files and loss of data. A number of measures can be used to minimise the chances of a security breach, such as usernames and passwords, firewalls, use of wireless security protocols and UPS devices.

THINK ABOUT COMPUTING 3.12

Adware, spyware and keyloggers are all considered to be malware. Are they all malicious?

Username and passwords

Most network operating systems require that you correctly enter a **username** and a **password** before you can access the data, information and programs stored on a computer or network. Some systems assign your username, or user identification (ID). For example, a school may use your student identification number as your user ID. With other systems, you select your own. Many users select a mixture of their first and last names. For instance, a user named Michael Roland might choose 'mroland' as his username.

For passwords, most systems require you to select your own. Users typically choose an easy-to-remember word or series of characters for passwords. If your password is too obvious, however, such as your initials or birthday, others can guess it easily. Easy passwords make it simple for hackers to break into a system, so you should select a password carefully.

Longer passwords provide greater security than shorter ones. Each character you add to a password significantly increases the number of possible combinations and the length of time it might take for someone to guess the password. Simply speaking, the more creative you are when selecting a password, the more difficult it is for someone to figure out. Table 3.11 shows the effect of increasing the length of a password that consists of letters and numbers. The longer the password, the more effort required to discover it. Long passwords are more difficult for users to remember, however.

Many software programs have guidelines that you must follow when you create your password. Many systems require your password to be at least eight characters long and use a mixture of numbers, upper and lower case letters and special characters.

TABLE 3.11 Password protection

Password		Average time to discover ^b	
Number of characters ^a	Possible combinations ^b	Human ^c	Computer ^d
1	36	3 minutes	0.000 018 second
2	1 300	2 hours	0.000 65 second
3	47 000	3 days	0.02 second
4	1 000 000	3 months	1 second
5	60 000 000	10 years	30 seconds
10	3 700 000 000 000 000	580 million years	59 years

^a Possible characters include the letters A–Z and numbers 0–9.

^b Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations.

^c Human discovery assumes one try every 10 seconds.

^d Computer discovery assumes 1 million tries per second.

Banks and other financial institutions concerned about unauthorised transfers of money from online accounts are now using a secure SMS system to validate the transfer. Users are still required to log in to the institution using their login and password; however, if they wish to transfer money to an account at another bank or to an organisation, the institution sends them a randomly generated six-digit code via SMS to their previously registered mobile phone number. The code is completely unique to that transaction and expires within a set time limit, usually five minutes. The user must read the code on their mobile phone and then enter that code on the website to validate the transfer.

A two-phase process to control access to a network involves 'identification' to verify that you are a valid user, and 'authentication' to verify you are who you claim to be. A username and password are two methods used to identify and authenticate a user's access rights.

The most common word used as a password is the word 'password'. Some networks require users to change their password each month. A log of the user's previous passwords can be checked to ensure that the password selected has not been used before. This can be an inconvenience to the user, but the increased security can be worthwhile.

THINK ABOUT COMPUTING 3.13

Many websites require passwords. Can a website be secure? Why or why not? Should a website limit the number of password entry attempts to three?

The purpose of a firewall is to securely separate the internet and other external networks from the internal LAN. The firewall examines the content of incoming packets and determines whether they should be allowed to pass through to the LAN. The firewall is usually configured so that the internet connection enters on a separate network interface card, giving total control over the routing of external packets.

THINK ABOUT COMPUTING 3.14

There are many ways that hackers and others with misguided intent may try to access or abuse a network. Use the internet to find out about email bombs, denial of service (website) and spam. What are they? Can they be avoided? How?

Firewalls

As the internet is a public network, anyone with the proper connection can access it. In contrast, a private corporate intranet restricts access to specific authorised users, usually employees, suppliers, vendors and customers. To prevent unauthorised access to data and information, companies protect their intranet with a **firewall** (Figure 3.38). One use of firewalls is to deny network access to outsiders.

To implement a firewall, many companies route all communications through a proxy server. A proxy server is a server outside the company's network that controls which communications pass into the company's network. That is, the firewall carefully screens all incoming and outgoing messages.

A server on a LAN can use one of the 1024 ports available to allow its services to be accessed by external users over the internet. Typical port numbers assigned to network services include:

- 21 – file transfer protocol used for uploading and downloading files (FTP)
- 25 – email (SMTP)
- 80 – web server (http)
- 443 – web server (https).

A firewall can be set to block any or all of these ports to restrict access to outsiders. By blocking the incoming ports, external users cannot use that port to hack into the local network. Holes are opened through the firewall by unblocking a port. This is done to allow legitimate access to the LAN, such as permitting external users to access the web server.

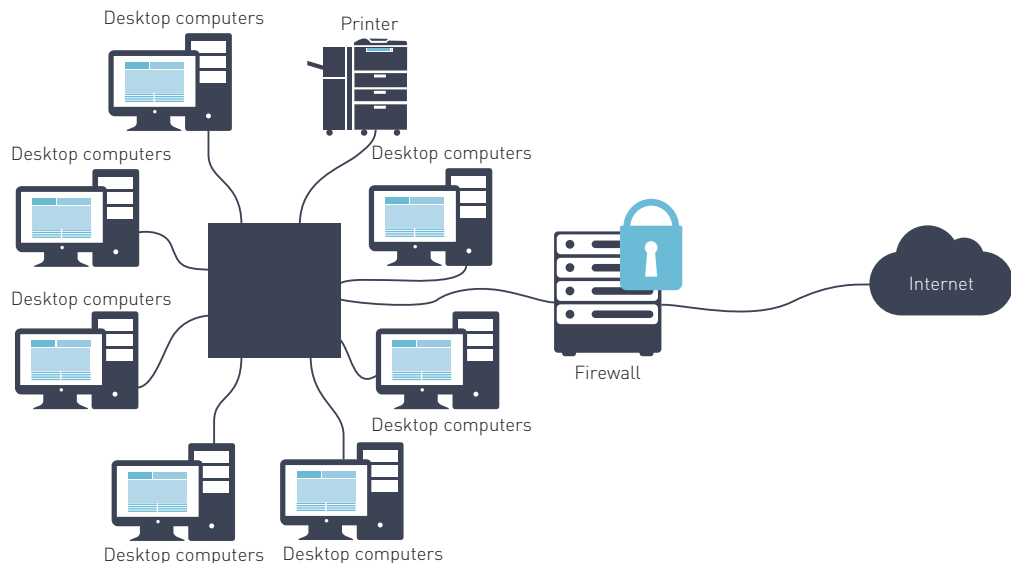


FIGURE 3.38 One use of a firewall is to restrict outsiders from accessing data and information on a network.

Uninterruptible power supplies

Power loss can be caused by storm damage, restricted supply imposed by the power company or heavy demand in the area. An uninterruptible power supply (UPS) provides about 10 minutes of reserve power, which provides sufficient time for the network administrator to shut down the network in an orderly way so that there is no resulting loss of data. To provide the backup power source, the UPS converts its 12-volt DC stored battery charge to a 240-volt AC supply. Most power blackouts last for less than one minute so the UPS can keep the system operating without the need to shut down. Most UPS devices also protect against power surges.

UPS devices come in a range of capacities, with those targeting the home network market operating at 1200 VA or 2200 VA. A volt-ampere (VA) is the unit used for the power in an electronic circuit (the root mean square voltage times the root mean square current).

As a rough guide, a desktop computer requires 200 VA, a 15-inch monitor requires 50 VA, a 21-inch monitor requires 200 VA, a router needs 50 VA and an external hard drive needs 100 VA. So a typical home network might need protection for, say, 550 VA. A UPS rated at 2200 VA will give longer back-up time and extra capacity if more devices are added to the network in the future.

Wireless security

Wireless communications technology has enabled billions of homes and businesses that use notebook computers, tablets and other mobile devices to communicate within a LAN or globally with relative ease. Although wireless provides many conveniences to users, it also poses additional security risks.

A common technique to locate a vulnerable wi-fi network is called ‘wardriving’. In this technique, a perpetrator attempts to connect to wireless networks through their notebook computer while driving through areas they suspect might provide easy access.

To avoid unauthorised network access, the wi-fi network should include a firewall and ensure equipment uses one or more wireless security standards. Recommended security strategies include the following.

- The wireless access point should be configured so that it does not broadcast its network name (the service set identifier, or SSID, which is a 32-bit alphanumeric password for the wireless LAN). It should also allow access only to specified devices.
- Use **wi-fi protected access (WPA or WPA2)**, which is a standard that defines how to encrypt data as it travels across wireless networks. Encryption technology scrambles messages sent over the wireless network so that they cannot be easily read. All devices on the wireless network must use the same encryption settings. WPA and WPA2 establish a passphrase that is used to check the identity of all devices on the wireless network.
- Use wi-fi protected setup (WPS) with a push-button connection to attach devices to the wireless network.

The alternative to a push-button WPS is to use a PIN. This is less secure, since many routers do not time-out after an incorrect WPS PIN is used. This leaves the router vulnerable to attack.

Network physical designs

The **physical design** of a network takes into account the hardware and software needed to provide the solution. One way to represent the physical design of a network is to draw a network diagram.

Network diagrams

Networks in medium-to-large organisations can become very complex, with servers, workstations, printers and wireless access points spread widely throughout the premises. Technical support staff need a method of representing both the network and all of its different pathways to provide an overview of the connections and to allow them to identify and locate equipment.

Network diagrams use lines to represent cables, and icons to represent communications devices. Figure 3.39 shows a network diagram for OzDVD, an internet-based DVD sales business. You should be able to identify a number of servers, desktop computers, printers, routers and switches.

The firewall restricts the traffic coming over the internet from directly accessing the internal servers. The web server would be used to hold the static items of the OzDVD webpage.

THINK ABOUT COMPUTING 3.15

To increase the security of a wireless network a number of other options, other than turning on WPA2, should be considered. Investigate the strategies that follow.

- MAC address filtering
- Assignment of static (rather than dynamic) IP addresses to devices on the network

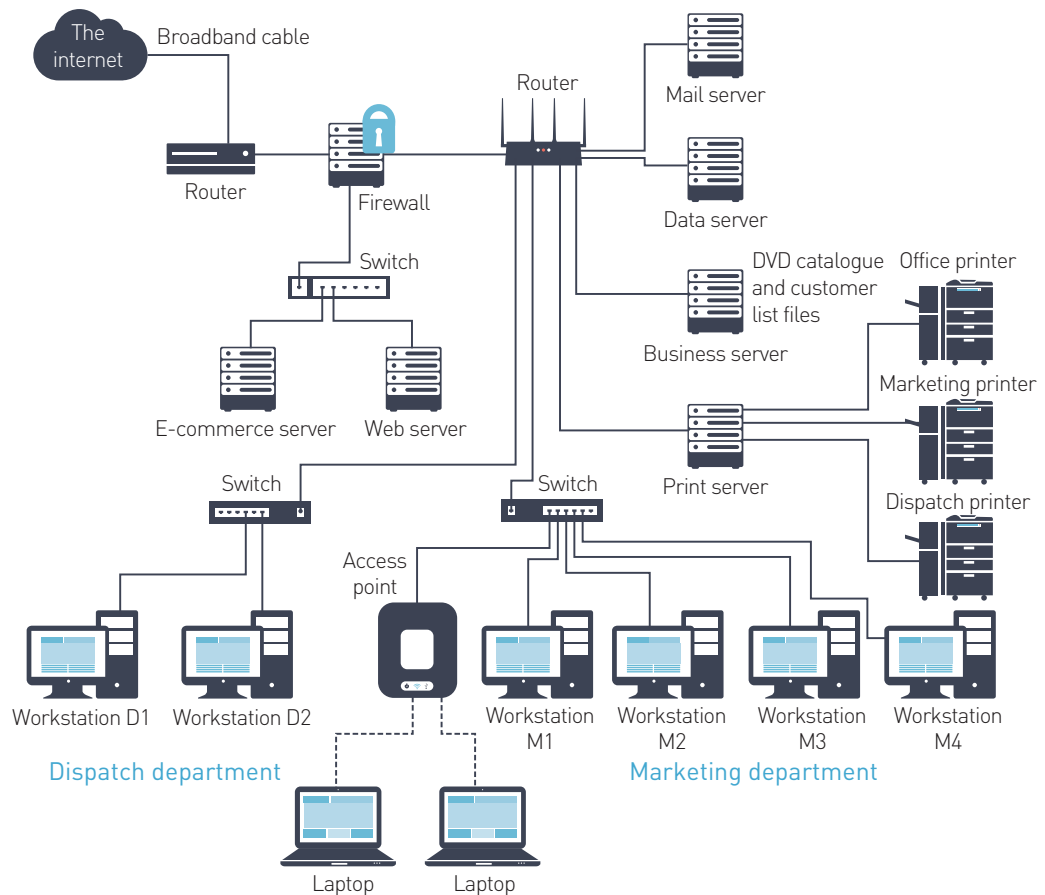


FIGURE 3.39 A network diagram for OzDVD's sales system, showing the communications devices and transmission media used in the network.

The e-commerce server provides the interaction with a customer. It would house the dynamic webpage elements, such as the shopping trolley, checkout facility, DVD-cover graphics and so on. The internal business server contains the catalogue and customer database files. Rules within the firewall allow the business server and the e-commerce server to communicate with each other.

Note that Figure 3.39 is not based on the plans of the building. This would make the diagram cumbersome and difficult to read. The physical buildings are not important in a network diagram, but it is necessary to identify work areas. The network diagram identifies the marketing department and the dispatch department work areas.

The VCE Unit 1 Computing course does not require the students to know the specifics of the laws that cover the legal obligations of network administrators and users with respect to the communication and storage of data and information. The relevant acts are listed below:
The Copyright Act 1968
The Privacy Act 1988
The Information Privacy Act 2000
Health Records Act 2001.

Legal and ethical responsibilities

Network professionals and users of networks have legal and ethical responsibilities with respect to social protocols and the ownership of data and information. Social protocols are a set of rules or behaviours that apply when people use online environments. The protocols cover appropriate behaviour when communicating online, the ownership of intellectual property, the application of digital information security practices and the use of personal security strategies.

Legal responsibilities

Legal responsibilities include those actions to which a person can be held accountable under law. Breaching a legal responsibility has the implication of litigation or facing charges in a court of law. The first legal area to consider relating to the communication and storage of information is ensuring that copyright laws are not infringed. For example, software used on the network should be legally purchased. Text, video and image files loaded on websites, or in files available on the network, should be original works or permission should have been given by the legal owner.

Another legal requirement is to ensure that privacy laws have been complied with. This involves obtaining permission from people for their photos to be used on a website or in documents stored on the network, checking that personal details are not disclosed and information is not available that allows a third party to identify individuals.

Information systems professionals also have a legal responsibility to ensure that data stored on a network or communicated between nodes cannot be accessed by unauthorised users.

Ethical responsibilities

Ethical responsibilities relate to following the correct moral path. Not adhering to ethical standards in an online environment has the consequences of a loss of respect, loss of customers and criticism from aggrieved users. Examples are ensuring that sexually explicit material is not stored or accessible; defamatory comments are not posted in email, in messages or on websites; that communications between users cannot be intercepted; and that metadata from tweets and other social media should not allow individuals to be identified.

Resolving legal, ethical and social tensions

Tensions can arise in a workplace if acceptable work practices are not clearly defined. Usually an organisation will adopt a series of policies that outline what workers should or should not do, and how to respond to particular events. If the policies lack clarity, or do not exist, issues can develop that need to be resolved.

There are six steps that an organisation can use to solve a legal, ethical or social tension.

- 1 Identify the problem: What decision has to be made and what facts are required?
- 2 Identify the stakeholders: Who are they? What interests do they have? Who is the key player?
- 3 Identify possible alternatives: What options are available? What are the likely consequences?
- 4 Identify ethical standards: Are there any applicable laws? Are there any morals or standards that could be applied? Is there a precedent?
- 5 Evaluate options: Identify strengths and weaknesses. Identify the option that causes least harm. Can the decision be reversed?
- 6 Make a decision: Select the preferred option. Justify the option. Notify all stakeholders of the decision.

Security practices

Applying appropriate security practices to protect information, particularly sensitive data such as personal details, forms part of the social protocols that users of networks should follow. Network professionals should ensure that networks are safe from accidental, deliberate and event-based threats, as discussed earlier in this chapter. This should include measures to protect the communication and storage of data and information, such as the use of firewalls

The use of cloud computing presents issues for many network managers and users. Moving data into the cloud means the data will move out of the direct control of an organisation or user. That data may be processed and stored outside of Australia. Users need to be aware of their privacy and data security obligations when transferring personal information into any cloud environment.

and security protocols that apply encryption techniques. Users of networks and members of online sites should be required to use logins and passwords to access a network. Websites that require users to input data online should incorporate a test to establish that the respondent is human rather than a machine.

Personal security strategies

Users of networked information systems should apply safe practices while participating in online environments. This includes users checking their default privacy settings to ensure maximum protection of personal details. Using online filtering techniques to restrict the content that can be communicated over a network is another form of personal security. Filtering can be applied by an employer to personnel within the organisation, by a school to its students and by parents to their children.

Users of social media should activate privacy settings in their accounts to avoid divulging personal data such as photographs, addresses and names.

Responsibilities of network users

Networks reach across societies that have different values and traditions. People using networks have capacities that allow them to do things they could not do before – and do so with anonymity. The norms of society and values can be challenged by the character of human interaction in electronic networks.

Users of networks, including those using social networking sites, must comply with copyright laws and behave ethically. Internet etiquette, also known as netiquette, is a set of guidelines on how users should behave when communicating online. These guidelines provide a set of social online protocols and include:

- avoiding the use of bad language and not saying things to make other people feel bad
- not typing emails in upper case (since it looks like you are shouting)
- not using emoticons in formal emails
- when forwarding an email, removing all personal information relating to the original sender, including their email address
- obeying the rules of online discussion forums
- deciding whether to use your real name or not (using a handle can protect your personal information)
- avoiding running malicious code on a network by not opening emails from unknown sources or opening files that may contain malware
- not making defamatory or discriminatory comments on social media
- not posting text, images, videos or files which infringe on intellectual property rights
- ensuring any sources used or quoted are reliable and authentic
- not uploading or downloading sexually explicit content
- respecting other people's privacy.

Rather than loading material that may be subject to copyright, it is better practice to include links to the website that contains the original source. Any material used should be appropriately cited.

Remember that it is often not possible to remove a comment made on a social media site. Think of the consequences before you post.

Benefits and risks associated with using a network

The use of networks has become widespread as the technology has become more widely available and the use of the internet and social media has become a seamless part of our lives. There are many clear benefits in using a network, from the sharing of hardware and software to accessing the internet. There are also a number of risks associated with the use of networks, particularly within the context of a global environment. In this section, we look at the benefits to individuals and organisations in using a network, then the risks that may be encountered.

Benefits of using a network

Establishing a network has a number of benefits over running standalone computers and resources, including access to peripherals (for example, printers), lower set-up costs (terminals are cheaper than standalone computers) and the speed of communications. Further advantages of using a network are provided below.

Facilitating communications

Using a network, people can communicate efficiently and easily via email, Facebook, instant messaging, chat rooms, VoIP, wireless messaging services and videoconferencing. Sometimes these communications occur within a business's network; at other times they occur globally through the internet.

Sharing hardware

Each networked computer can access and use hardware on the network. Suppose several personal computers on a network each require the use of a laser printer. If the personal computers and a laser printer are connected to a network, the personal computer users can each access the laser printer on the network when they need it. Businesses and home users network their hardware for one main reason – it may be too costly to provide each user with the same piece of hardware, such as a printer.

Sharing data and information

In a networked environment, any authorised computer user can access data and information stored on other computers in the network. For example, a large company might have a database of customer information. Any authorised person, including a mobile user using a smartphone to connect to the network, can access this database. The capability of providing access to and storage of data and information on shared storage devices is an important feature of many networks. Project teams can share data, even if they are geographically remote, by using an organisation's virtual private network (VPN), which uses the internet to make global connections. Networks support collaborative work practices through services such as cloud computing, email and file transfer.

Sharing software

Users connected to a network can access software (programs) on the network. To support multiple-user access of software, most software vendors sell network versions of their software. In this case, software vendors issue a site licence. A network licence is a legal agreement that allows multiple users to run the software package simultaneously. The site licence fee is usually based on the number of users or the number of computers attached to the network. Sharing software via a network usually costs less than buying individual copies of the software package for each computer.

Transferring funds

Electronic funds transfer (EFT) allows users connected to the internet (an example of a wide area network) to transfer money from one bank account to another via transmission media. Consumers can use credit cards or an online payment system like PayPal to make purchases over the internet. Businesses can use the internet to deposit their employees' salaries directly into their bank accounts. Both businesses and consumers pay bills online, which involves instructing their bank to use EFT payment to pay creditors. Global networks are a boon to online retailers, who can effectively trade 24/7.

THINK ABOUT COMPUTING 3.16

List the hardware that is shared on your school's network.

Facebook is an online social network established in 2004. It was originally available only to college students in the United States.

Virtual private networks were discussed on page 86.

THINK ABOUT COMPUTING 3.17

What are the advantages and disadvantages of using online programs such as Google Docs and Office 365?

Risks associated with using a network

The risks associated with using a network relate to inconvenience caused by any fault in the network devices and damage or loss of sensitive data caused by breaches of security.

Breaches of security

Networks with inadequate security systems are liable to be attacked by malware or hackers. These threats can result in valuable information being accessed, stolen, damaged or deliberately altered for fraudulent purposes. Hackers have been able to access customer credit card details by finding an opening in a commercial corporation's network. Viruses and other malware can deliberately sabotage the operation of computers and software.

Wireless networks without suitable encryption security run the risk of outsiders eavesdropping on messages or accessing important files transmitted between users.

User dependence

Network users rely on a network to operate correctly to be able to access files, applications and resources. If a component, such as a file server, develops a fault, users will not be able to run applications or access shared data. This would limit the effectiveness of a worker and impact on the productivity of the business.

Social networks

The popularity of social networking sites such as Facebook and Twitter has increased rapidly in recent years. There are a number of negative effects that overuse of social networking can have on users. These include:

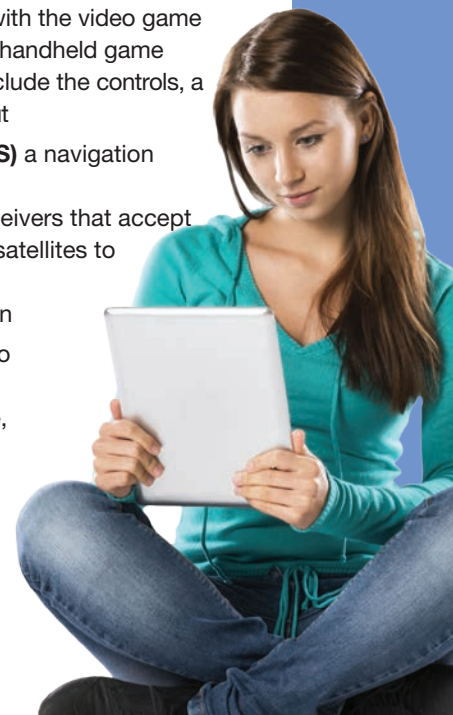
- distracting users from more purposeful tasks such as studying
- reduced learning and research capability as students rely on information easily accessible from social network sites but often unverified
- reduction in traditional communication between people, such as face-to-face conversations
- adoption of poor language skills and underdevelopment of creative writing skills
- negative impact on health due to skipping meals and not participating in physical activity
- reliance on virtual world experience rather than from the real world.

Social media are now important tools for businesses to market their services and keep in touch with their customer base. Customers expect organisations they do business with will be contactable via sites such as Twitter, Facebook and LinkedIn. Social media risks faced by organisations come under three areas: operational, regulatory and reputational.

- Operational risk relates to employees posting material in breach of copyright; the monitoring of employees on social media; ownership of material posted.
- Regulatory risk involves company disclosures – market sensitive data revealed on social media before a public announcement.
- Reputational risk includes what the business or employees say online, or what customers may say about the company.

ESSENTIAL TERMS

- 802.11 standard** the standard that specifies how two wireless computers or devices communicate via radio waves with each other
- app** a self-contained program installed on a mobile device that is designed to fulfil a particular purpose; some apps are provided as a standard feature on the mobile device while others can be downloaded from commercial providers
- asymmetric digital subscriber line (ADSL)** a digital line alternative for the small business or home user. ADSL transmits on existing standard copper telephone wiring. The ADSL2+ technology allows a faster transfer rate than the older ADSL rate – 20 Mbps compared with 8 Mbps.
- bandwidth** the width of the communications channel measured in bits per second
- Bluetooth** a protocol that uses short-range radio waves to transmit data along enabled devices, such as notebook computers, mobile telephones and printers
- broadband router** a basic router that connects a LAN to the internet, also functioning as a switch, a firewall and a wireless access point
- broadcast radio** a wireless transmission medium that distributes radio signals through the air over long distances (such as between cities, regions and countries) and short distances (such as within an office or home)
- cellular radio** a form of broadcast radio that is used widely for mobile communications
- channel** the communications path between two devices
- client-server network** a network in which one or more computers act as a server (host computer) and the other computers on the network (clients) can request services from the server. A server controls access to the hardware and software on the network, and provides a centralised storage area for programs, data and information.
- cloud storage** an off-site storage system maintained by a third party and accessed through the internet
- communications device** any type of hardware capable of transmitting data, instructions or information between a sending device and a receiving device
- communications satellites** communications facilities that receive microwave signals from Earth, amplify the signals, and retransmit them back to Earth
- communications software** an application or program designed to pass or support the movement of information over a network
- dedicated server** a server that performs a specific task, such as file servers, print servers, database servers and network servers
- digital signals** individual electrical pulses that represent the bits that are grouped together to form characters
- domain name server (DNS)** residing with the ISP used by the client, the DNS is used by the internet to store domain names and their corresponding IP addresses; when a browser requests that a page be downloaded, the DNS translates the domain name into its associated IP address
- downlink** a transmission from the satellite to a receiving Earth station
- Earth-based stations** communications facilities that use large, dish-shaped antennas to transmit and receive data from satellites
- Ethernet** a standard communications protocol embedded in software and hardware devices that allows computers to operate a LAN; it was developed in 1973 by American electrical engineer Bob Metcalfe, and has become the standard model for LANs worldwide
- fibre-optic cable** smooth, hair-thin strands of glass or plastic (**optical fibres**) that conduct light with high efficiency; fibre optics are frequently used in new voice and data installations
- firewall** hardware and software that restrict access to data and information on a network
- game console** an input device with the video game screened on a television set; handheld game consoles are portable and include the controls, a small screen and sound output
- global positioning system (GPS)** a navigation system that consists of one or more Earth-based receivers that accept and analyse signals sent by satellites to determine the receiver's geographic location
- hacker** a person who breaks into a computer for profit, from the motivation of a challenge, or to view restricted data
- hypertext mark-up language (HTML)** a set of special codes that format a file for



use as a webpage; these codes, or tags, specify how the text and other elements display in a browser and where the links lead

- hypertext transfer protocol (http)** a set of rules that defines how pages are transferred on the internet
- hypertext transfer protocol secured (https)** a communications protocol for secure transmissions over the internet; the https system provides authentication and encryption communication and is widely used for security-sensitive processing, such as payment transactions and connections to banks
- internet peer-to-peer network** an internet network which enables users with the same networking software to connect to one another's hard disk drives and exchange files directly
- internet service software** web browsers, electronic mail, Voice over internet Protocol (VoIP) software and cloud storage
- intranet** an internal network within an organisation that uses internet and web technologies
- keylogger** a type of Trojan designed to secretly monitor and record all keystrokes entered on a keyboard; some are legitimate (such as parental-control programs to allow parents to track their children's internet usage), but others may be used for spying or stealing data
- leecher** a person downloading a file using a torrent protocol during a P2P session who does not allow their computer to pass pieces of the file to other users
- local area network (LAN)** a group of neighbouring computers that can share information and resources using a network (such a network is usually within a building or several neighbouring dwellings, but can be up to a few kilometres); an organisation owns the infrastructure used by the network, including the cabling
- logic bomb** a program that lies dormant until a specific piece of program logic is activated. In this way, it is very analogous to a real-world land mine. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code.
- malware** programs designed to infiltrate and cause harm to a computer or network without the owner's knowledge or consent, such as viruses, worms, Trojans, adware, spyware, logic bombs and keyloggers; the term is short for 'malicious software'.

Mbps short for megabits per second

- microwaves** radio waves that can be used to provide high-speed transmission of both voice and data; data is transmitted through the air from one microwave station to another in a manner similar to the way radio signals are transmitted
- microwave station** an Earth-based reflective dish that contains the antenna, transceivers and other equipment necessary for microwave communications
- mobile devices** compact, lightweight, easily carried and often high-speed wireless broadband enabled devices, such as games consoles
- mobile phone** a telephone device that uses radio signals to transmit voice and digital data messages
- near field communication (NFC)** contactless communication between portable devices; a smartphone can be configured to read an NFC tag on a poster or menu to download relevant information (for example, Paywave transactions and the myki transportation system use NFC technology)
- network** collection of computers and devices connected together via communications devices and wired or wireless transmission media, allowing computers to share resources
- network administrator** the person who oversees the operations of a client-server network
- network analysis tools** allow network administrators to monitor devices, check protocols and port activity, view event logs and analyse traffic
- network architecture** the design of the network; for example, include client-server and peer-to-peer networks
- network-attached storage (NAS)** a storage device often used to hold video, photo and audio files on a network; a typical NAS has capacity to store 8 TB of data and can be configured as an FTP, web, email and print server
- network diagram** a schematic method of showing the physical devices and communications lines present in a network
- network interface card (NIC)** a communications devices that fits in an expansion slot of a computer and enables a computer that does not have in-built network capability to communicate with a network
- network operating system (network OS, NOS)** software that organises, controls and coordinates the administration, file management, printer management and security activities on a LAN

- network protocol** rules and conventions for communication between network devices; protocols for networks generally use packet-switching techniques to send and receive messages in the form of packets
- network standard** guidelines that specify the way computers access the medium to which they are attached, the types of media used, the speed at which data flows and the physical technology used. Examples of network standards are Ethernet, TCP/IP and 802.11
- networking software** computer programs that establish a connection to another computer or network, and manage the transmission of data, instructions and information
- node** a network connection point, including desktop or mobile computer, peripheral such as printer or scanner, or portable device such as a smartphone. A node normally is assigned its own IP address.
- optical fibre** a strand of glass or plastic, as thin as a human hair, that uses light to transmit signals
- packet switching** breaking a message into packets, sending the packets over a network pathway, and then reassembling the data
- packets** the small pieces into which data is broken before being transmitted over a network; they will be transmitted independently over the transmission media and, once all the packets have arrived at the receiving computer, are put back together to produce the original, complete message
- password** a secret combination of characters associated with the username that allows access to certain computer resources
- peer** someone with equal communication access rights in a network. In relation to torrent downloads, peers are computers on the internet that are downloading a particular file at the same time.
- peer-to-peer network (P2P)** an internet network that enables users to connect to each other's hard disks and exchange files directly, such as BitTorrent
- physical design** the communications devices, transmission media and software of a network
- physical transmission media** media that use wire, cable or fibre-optics to send communications signals
- phishing** sending an email to a user falsely, claiming to be an established enterprise of some kind, in an attempt to scam the user into giving up private information that will be used for identity theft
- protocol** a set of rules and procedures for exchanging information between two computers, such as the network transmission control protocol/internet protocol (TCP/IP)
- receiving device** accepts the data, instructions or information
- router** an intelligent network-connecting device that can route communications traffic directly to the appropriate network
- seed** a computer on the internet that has a complete file available for downloading using the torrent protocol
- sending device** initiates the transmission of data, instructions or information
- smartphone** an internet-enabled mobile phone that typically includes an address book, calendar and a calculator; a businessperson would require a smartphone that is capable of sending and receiving emails from the company's mail server, as well as opening and editing business applications, such as word processing, spreadsheets, presentations and PDF files, and a web browser.
- spyware** any software that covertly gathers information about a user through an internet connection without the user's knowledge or approval
- switch** a device that provides a common connection point for nodes on a network; it enables a packet to reach its destination faster by storing addresses in memory and using logic to direct the transmission
- tablet** a special type of notebook or laptop computer that resembles a letter-sized slate, which allows a user to write on the screen using a digital pen
- TCP/IP (transmission control protocol/internet protocol)** a network standard that manages the transmission of data by breaking it up into packets and transmitting the packets over the internet
- torrent** a small file that holds metadata relating to a file that can be shared on a P2P network; the metadata includes the file's name, size and its location
- transmission media** the materials or technologies that are used to establish the communications channel; two types of transmission media are physical transmission media, which use some type of physical cabling (twisted-pair wire, coaxial cable and fibre-optic cable); and wireless transmission media, which use wireless technology (microwaves, radio waves or light waves)

Trojan programs that pretend to be one thing, but that are actually performing another, malicious background function; for example, a Trojan that appears to be a game that is actually collecting email addresses stored on your computer and sending them back to spammers

twisted-pair cable a cable made up of **twisted-pair wires**; twisted-pair cable systems are graded according to categories that describe the quality of the components and the installation technique. The most common twisted-pair cable is graded as category 5, CAT 5e or CAT 6.

twisted-pair wire pairs of copper wires that are twisted together, commonly used for telephone lines and to connect personal computers with one another

uplink a transmission to the satellite

username a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user

virtual private network (VPN) a network in an organisation or business that uses the internet to link remote sites and users

virus a computer program that can destroy files and alter the performance of the operating system; once a virus is in a computer, it can spread over a network to other connected computers

Voice over Internet Protocol (VoIP) a high-speed internet connection that allows users to communicate as if they were on a conventional telephone

wearable technology devices that use wireless signals and can be worn by the user, either as clothing or an accessory, such as smart watches and devices that track information relating to health and fitness

web browser an application software package that allows users to access and view webpages

web-enabled device a digital device that provides access to the internet for hand-held devices, such as smartphones

web server a computer that delivers requested webpages to another computer

wide area network (WAN) a network that is geographic in scope (as opposed to local) and uses telephone lines, microwaves, satellites or a combination of communications channels

wi-fi any network based on the 802.11 standard

wi-fi communications a wireless transmission medium that distributes radio signals through the air over long distances

wi-fi protected access (WPA or WPA2) a standard that defines how to encrypt data as it travels across wireless networks

wireless access point a central communications device that allows computers and other mobile devices to transmit data among themselves wirelessly using radio waves

wireless adaptor a device used to connect computers and mobile devices to a wireless network; the adaptor maybe in-built or connected via a USB port on the computer

wireless broadband router a device that combines the functions of a basic router (connecting the LAN to the internet), a switch (for devices, such as a desktop computer, connected by cable), a firewall (security measure) and a wireless access point (to allow wireless connectivity)

wireless extender a device that increases the range of a wireless access point by re-broadcasting the signal it receives, which allows home networks to avoid obstacles and reach further than normal; a dual-band uses both the 2.4 GHz and 5 GHz radio frequencies, so one frequency can be used to communicate with a router while the other frequency can be used to communicate with clients. The device must provide simultaneous transmissions rather than the option of 2.4 GHz or 5 GHz.

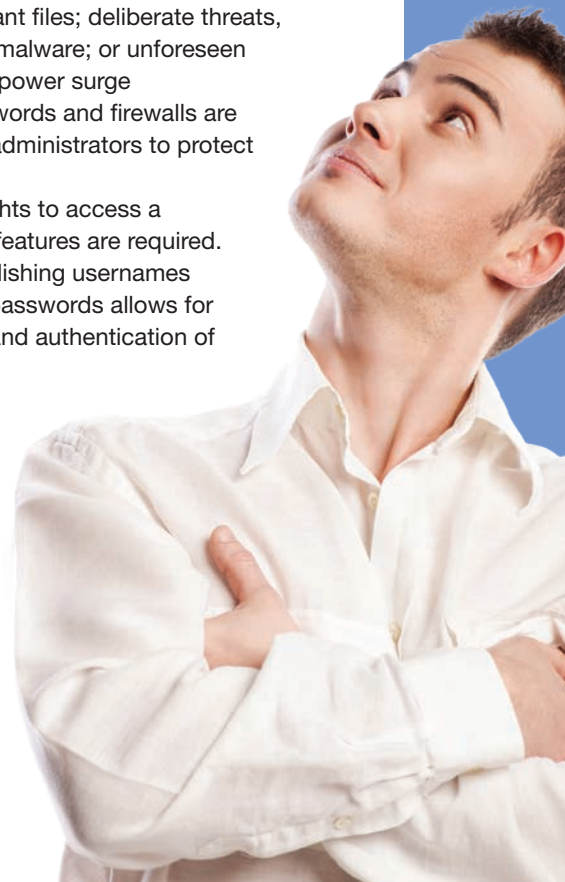
wireless transmission media media that send communications signals through the air or space using radio, microwave and infra-red signals

worm a virus that copies itself repeatedly in memory or over a network, using up a system's resources and possibly shutting it down; while a virus will embed in executable software on a computer, a worm will actively transmit over a network to infect other computers

IMPORTANT FACTS

- 1 Networks allow users to share resources such as data, information, hardware and software, and to transfer money via electronic funds transfer.
- 2 To protect wireless networks, security measures are recommended, such as configuring the wireless access point so that it does not broadcast a network name and only allowing access to specified devices. Data should also be encrypted before it travels across a wireless network.
- 3 Network professionals and users have legal and ethical responsibilities with respect to social protocols and the ownership of data and information. These responsibilities relate to copyright, privacy, socially appropriate material, malware, backup strategies and network access restrictions.
- 4 Networks allow users to share hardware, software, data and information, to transfer funds globally, attract new customers, entertain and acquire knowledge.
- 5 The risks associated with using a network in a global environment include breaches in security that allow malware or a hacker to access, steal or damage files and information, users' dependence, and the negative effects of overuse of social media.
- 6 Businesses need to be aware of the risks associated with communicating on social media. The risks include employees posting information in breach of copyright, issues relating to the monitoring of employee communications, sensitive market information being leaked before public announcements and employees or customers posting negative comments.
- 7 Software installed on servers, referred to as server software, allows them to provide email services, internet connectivity, file management and print services.
- 8 The National Broadband Network (NBN) requires a utility box to connect to the fibre-optic cable being rolled out across Australia and a connection box to be installed in the home. The connection box is used for phone connection and to link with the home's network router.
- 9 The range for a wi-fi network is about 50 metres inside a building.
- 10 A smart TV can function as a conventional television set as well as link to the internet to screen interactive media.
- 11 Mobile devices that can be connected to a network include:
 - smartphones
 - hand-held computers
 - netbooks
 - navigation systems
 - digital cameras.

A convergence of technologies has resulted in one type of device also performing the functions of a different type of device. For example, a smartphone may be capable of running applications software, accessing the internet, playing media and taking digital images beside its main function of voice communications.
- 12 Video games use a console to input commands, a screen for output and a hard-drive for storage. Popular consoles include XBox One, PlayStation 4 and Wii U.
- 13 The transmission rate of a communications channel is determined by its bandwidth and its speed. The bandwidth is the range of frequencies that a channel can carry. The speed at which data is transmitted is usually expressed as bits per second (bps), the number of bits that can be transmitted in one second.
- 14 The National Broadband Network (NBN) uses fibre-optic cable to connect homes and businesses to the internet using connection speeds of 25 Mbps. Fixed wireless and satellite connections are used where cable is impractical.
- 15 Security threats to networks include accidental loss, such as losing a portable storage device containing important files; deliberate threats, such as installing malware; or unforeseen events, such as a power surge
- 16 Usernames, passwords and firewalls are used by network administrators to protect networks.
- 17 To verify users' rights to access a network, security features are required. A system of establishing usernames (or user IDs) and passwords allows for the identification and authentication of each user.



TEST YOUR KNOWLEDGE



Review quiz

COMMUNICATIONS

- 1 What does the term 'data communications' mean?
- 2 Identify the devices you use on a day-to-day basis that connect to a network.

NETWORKS

- 3 Provide an example of a sending device and a receiving device.
- 4 What is a network? How is a local area network (LAN) different from a wide area network (WAN)?
- 5 How does a peer-to-peer network differ from a client-server network?
- 6 Identify the dedicated servers that are used on networks in your school.
- 7 Describe the type of network a business might use if they have a head office in one city and wish to enable other branches and travelling salespeople to maintain regular contact and access data and files stored on their central servers?
- 8 What security risks can occur if a user shares files on an internet P2P network?
- 9 Describe the benefits in downloading a file from a P2P network using torrents rather than from a single source.
- 10 What do the terms 'peer', 'seed' and 'leech' refer to when referring to torrent downloads?
- 11 What is an intranet? What benefits to organisations are there in setting up an intranet?
- 12 Describe the advantages of setting up a home network.
- 13 There are four types of home network in common use. Which type would you choose to set up a network in your home? Why would you choose that type?

COMMUNICATIONS DEVICES

- 14 Routers and switches are used to connect separate networks. Explain the circumstances in which each of these would be used.
- 15 What is the function of a wireless broadband router in a home network?
- 16 Identify the components that need to be installed in a home or business to enable a LAN to connect to the NBN.
- 17 What is the intended purpose of the two voice ports on the NBN connection box?
- 18 What is the purpose of a network interface card? What do mobile computers use in place of a network interface card?
- 19 A wireless access point can be wired to the fibre-optic backbone of a bus network. What is the purpose of the wireless access point?
- 20 It may be difficult to pick up a consistent wireless signal in a large home with solid brick walls. Where should the access point be located to provide the strongest signal throughout the house? What solution would you recommend to ensure that some of the more distant parts of the house, such as the back patio, receive a signal?
- 21 Many home networks include a smart TV and a network-attached storage device. Describe the functions of these devices.
- 22 A particular network-attached storage device has a capacity of 8 Terabytes. How many megabytes is this equivalent to?

COMMUNICATIONS SOFTWARE

- 23 Describe four important tasks of a network operating system.
- 24 Identify the four components of a URL address.
- 25 When should a website use the https:// protocol rather than the standard http:// protocol?
- 26 List some benefits for an organisation in using a cloud storage system such as Dropbox.

NETWORK COMMUNICATIONS STANDARDS

- 27 Why do manufacturers of network hardware and software follow established standards?
- 28 Briefly describe how an Ethernet network transmits data.
- 29 In what situations would the TCP/IP protocol be most useful?
- 30 Explain the term packet switching.
- 31 What network transmission standard would be useful in a situation where an old, heritage-listed building with solid stone walls needs to be networked?
- 32 What advantages are there for users if a network moves from the 802.11n standard to 802.11ac?

SENDING AND RECEIVING DEVICES

- 33 A mobile telephone is an example of a wireless device that can be web-enabled. What does the term web-enabled mean?
- 34 What functions are likely to be available on a smartphone?
- 35 What does the expression 'convergence of technologies' mean? Give an example in which convergence of technologies is apparent in portable network devices.
- 36 Provide three examples of wearable technology.

COMMUNICATIONS CHANNEL AND TRANSMISSION MEDIA

- 37 What advantage do fibre optics have over wire cables?
- 38 In what circumstances would a network designer consider using wireless transmission media?
- 39 Briefly describe the broadcast radio and cellular radio wireless transmission media.
- 40 Describe how near field communication technology allows a user with a smartphone to read information at a museum exhibit.
- 41 What is the main limitation of microwave transmission?
- 42 Many companies use satellite transmission to access the internet. Web satellites, however, will provide faster downlink transmissions than uplink transmissions. Why is the difference in speed not of major concern to these companies?

NETWORK SECURITY

- 43 Describe how a virus, worm, Trojan and keylogger may threaten a computer network.
- 44 Describe how verifying the identity of a user can protect a network.
- 45 What is a firewall?
- 46 Describe three measures that should be incorporated into a wireless network to restrict access by unauthorised users and to secure the transmission of data.

LEGAL AND ETHICAL RESPONSIBILITIES

- 47** The manager of a website in an organisation has legal responsibilities related to the ownership of material used on the site. Describe these responsibilities.
- 48** Use the internet to find an example of how researchers and analysts use Twitter or Facebook entries to study human behaviour.
- 49** What steps should a network user follow in order to behave ethically when using social media?

BENEFITS AND RISKS ASSOCIATED WITH USING NETWORKS

- 50** Describe the five main benefits of using a network.
- 51** Why is user dependence considered a possible disadvantage of networks?
- 52** What problems could eventuate if a network is not well managed?
- 53** How might the use of social media be considered as a possible risk for businesses?

APPLY YOUR KNOWLEDGE

XYZ ENGINEERING

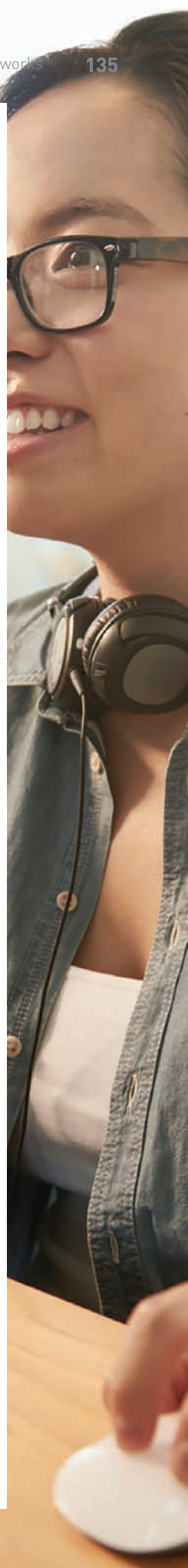
XYZ Engineering has its head office in the northern suburbs of Melbourne. The company designs and develops water systems including channels, culverts and bridges for municipal councils, government authorities and private owners. The head office contains several departments including the civil engineers who design systems for clients, a project team that sub-contracts building works to third parties, an accounts department that bills clients, pays sub-contractors and staff wages, and a small information systems department responsible for establishing and maintaining systems. The company has branch offices in Bendigo, Warrnambool and Bairnsdale. Engineers often need to visit sites to take measurements and make observations. They need to be able to access files stored on the LAN at head office and record their findings.


A number of requirements for a network have been identified.

- Desktop computers are used by those staff who work mainly from head office.
- Engineers and project team members who visit sites use notebook computers rather than desktops.
- All departments need access to files including work plans, schedules, job logs, costings and other documents relating to projects.
- Staff need access to printers.
- The company will require a website to promote their business.
- Files that include engineering plans and video clips of existing terrain or proposed developments can be very large and need to be stored centrally.
- Email is the primary means of communication.
- All staff have a company issued smartphone.
- Presentations to clients (involving plans, video clips and costings) need to be made from time-to-time at head office.
- A broadband cable connection to the internet is provided at head office.

Questions

- 1 What network device is needed to connect to the broadband cable at head office?
- 2 Employees with portable computers need to be able to use them throughout the head office. What communications technology will these notebooks require? What hardware is necessary to support this technology? What security measures are needed to protect data being communicated using this technology?
- 3 The desktop computers, printers and other network devices will use wired technology. What type of cabling would be suitable? What devices are needed to link the networks operating in each department?
- 4 What device would be suitable to store the large media files that the business uses for presentations to clients?
- 5 The company will operate a client-server network. What servers need to be installed?
- 6 The rural branches and on-site staff will need to access files from the network. What type of network will link remote sites to a central network via the internet?
- 7 Describe the legal requirements and ethical responsibilities of the information systems manager with respect to the company's website and files stored on network devices.



- 
- 8 What risks associated with use of the network does the information systems manager need to guard against? Identify some strategies that will negate these risks.
 - 9 Draw a network diagram of the system at head office. Label all devices and work areas.
 - 10 The company intends to set up a stand at the annual Water Treatment Exhibition. It is hoping that visitors to the exhibition will be able to access information about XYZ Engineering and the services they offer. Rather than providing information in paper form, the company hopes that visitors can download information onto their smartphones. Identify the technology that will be used and describe how it operates.

PREPARING FOR

UNIT 1 OUTCOME 2

Design a network with wireless capability that meets an identified need or opportunity, explain its configuration and predict risks and benefits for intended users

For Unit 1, Outcome 2, you are required to design a network for a specific use. The network must have wireless capability, though it may also have some wired components. You must explain its configuration, including identifying network devices and transmission media. You must also predict the risks and benefits for intended users.

OUTCOME MILESTONES

You will be required to:

- 1 Consider how the information needs of individuals or an organisation could be achieved through the use of a networked information system.
- 2 Identify the data and information that typically would flow through the information system.
- 3 Consider how data is to be stored within the network and where it is processed.
- 4 The network must have wireless capability. Determine whether wired transmissions are also required and identify the communications standard to be used.
- 5 Determine which network devices are needed.
- 6 Draw a physical representation of the network.
- 7 Consider the risks and benefits of using the network for intended users.

STEPS TO FOLLOW

Your teacher may provide a written scenario of a situation in which the implementation of a networked information system would provide benefits to an organisation. Alternatively, you may be asked to identify a system that you have observed and prepare a recommendation for the design of a small network.

- 1 Identify the information needs of individuals, such as a family, or organisation from the scenario provided or your own observations.
- 2 Describe the purpose of the proposed networked information system. In most cases, a local area network with wireless connectivity will be required, but users may also need access to the internet. If you are creating a simple network with a small number of users, will you opt for a peer-to-peer network or a client-server network? Why?
- 3 Identify the data and information that would flow within the information system and the location in which the data would be stored.

- 4 Identify which portable computers or devices are required to use the network. Determine if a wired connection to some devices is required, or whether a wireless environment on its own is sufficient to meet user's needs?
- 5 Identify the number of work groups that will operate and determine the number of switches (if any) required. Consider whether a router is needed.
- 6 Determine whether communications devices are necessary. If there is to be internet access, will you recommend cable, ADSL 2+ or some other form of transmission?
- 7 Use a software tool to depict the components of the network and its interactions.
- 8 Explain the function of components and how data and information are transmitted.
- 9 Predict the risks and benefits for intended users. Risks might include security threats to data and information or user dependence on the network. Benefits might include shared resources, access to the internet and reliable communications via email.

DOCUMENTS REQUIRED FOR ASSESSMENT

- 1 A brief report that identifies the information needs of the organisation, the purpose of the network and the type of network needed to support the information system
- 2 A written, oral or visual presentation that outlines your recommendation in terms of the network configuration and a rationale for the decisions made; points to discuss are:
 - LAN, WAN or a combination of both
 - peer-to-peer or client-server LAN
 - number and nature of servers if a client-server network is recommended
 - communications standard(s) to be used
 - communications devices (wireless access points, switches and routers)
 - transmission media (physical and wireless or just wireless)
 - inclusion of a firewall if internet access is recommended
- 3 A network diagram
- 4 A report that predicts the risks and benefits for intended users

ASSESSMENT

A set of assessment criteria will be prepared and distributed by your teacher before the start of the task.