Chapter 3 Networks

Test your knowledge

COMMUNICATIONS

1 The process by which a computer transfers data, instructions or information to another computer

2 Responses will vary. Students are likely to identify a smartphone, laptop or desktop computer, a smart TV and so on. They should tailor the responses to their own situation.

NETWORKS

3 Sending devices include desktop computers, notebook computers, tablets and smart phones.

Receiving devices include scanners, printers and smart TVs.

4 A network is a collection of computers and devices connected by communications channels (cabling, wireless, infrared, satellite). A local area network is confined to a limited geographic area such as a school or small business. A wide area network covers a large geographic area.

5 A computer on a peer-to-peer network stores files on its own storage device and can share printers, data or information located on any other computer on the network. A client–server network uses one computer (or more) to act as a server and other computers on the network can request services from that server.

6 Responses will vary, but may include file, print, proxy, internet and/or CD servers.

7 A VPN uses secure connections over the internet to link remote workers to a central network. The VPN usually consists of a LAN at the central location connected to a private WAN that is accessed using the internet. Encryption is used to ensure data transfers are secure.

8 Internet P2P requires a TCP port on the router to be open, which potentially means it is prone to attack by malicious software such as viruses and Trojans.

9 Downloading a file using torrents means that multiple sources can provide bits of the file at the same time. This results in a much faster download than if a single source was used.

10 A peer is a client who is downloading a file from the internet. The peer can also provide parts of the file (torrents) to other clients who are downloading at the same time. A seed is a peer who has the complete file and makes it available to others. A leech is a user who downloads a file but does not make it available to others.

11 An intranet is an internal network in an organisation that uses internet and web protocols to share information and policies with employees securely. Intranets restrict access to company information and facilities to employees.

12 A home network allows all computers in the house to be connected to the internet at the same time. All computers can also access files on any computer and share resources such as printers or DVD drives.

13 Responses will vary.

COMMUNICATIONS DEVICES

14 A router can connect networks running different network communications protocols. A switch stores the address of each device down every cable connected to it, so it is able to use logic to send packets directly to the destination device rather than broadcasting to all devices.

15 A wireless broadband router functions as a router by connecting a LAN to the internet, as a switch by connecting to network devices, as a firewall and a wireless access point.

16 An NBN utility box (to receive the signal from the NBN cable) and an NBN connection box are needed. A router is also required for connection to devices within the home.

17 One port is for digital telephone connection and the other is available for a personal alarm signal.

18 A network interface card packages data for transmission and controls access to and from the network cable. Mobile computers use a wireless network adaptor, which usually plugs into a USB port.

19 A wireless access point allows computers and devices to transmit data wirelessly among themselves. The transmission of data from a wireless access point back to a server is made faster if it is connected to a wired backbone.

20 The wireless access point would preferably be located in the centre of the house. A wireless extender could be used to allow distant nodes to receive a signal.

21 A smart TV can connect to the internet and thus provide interactive media, internet TV and streaming of movies. A network-attached storage device can store videos, photos and audio files for sharing on a network.

22 8 terabytes = 8 million MB

COMMUNICATIONS SOFTWARE

23 A network operating system is required to:

- administer the network by adding and deleting users and maintenance tasks such as backing up the system
- manage files by keeping track of locations and transferring them when required
- manage printing by prioritising jobs and sending documents to the appropriate printer
- keep the network secure by controlling the access of users.

24 Protocol, domain name, path and resource name

25 The https:// protocol is used for secure transactions, such as any connection where the transfer of money is involved.

26 Cloud storage encourages collaborative work practices. You can access files from anywhere that has an internet connection. You do not have to use the same computer to access the file that was used to create it.

NETWORK COMMUNICATIONS STANDARDS

27 Network standards are established to define the rules by which devices can communicate with each other. It ensures that devices produced by different manufacturers can be connected.

28 A workstation on an Ethernet network broadcasts a packet of data when the network is not busy. The packet is received by all workstations on the network, but only the workstation that the packet is addressed to will read it. If two workstations send a message at precisely the same time a collision occurs. Each workstation waits a random amount of time before resending the packet.

29 The TCP/IP protocol breaks data down into very small packets. This allows the packets to travel in multiple routes to the destination. This makes it ideal for use on a WAN such as the internet where there are numerous different paths a packet can take. The protocol is also being used on LANs, however, these usually have only one path to the destination and the advantage of small size is lost.

30 Packet switching is the process of breaking a message into individual packets, sending the packets along the best route available, and then reassembling the data at the destination.

31 The 802.11 standard would be best in an environment where penetrating walls with cable would be a problem. The 802.11 standard uses wireless transmission.

32 The 802.11ac standard operates in the 5 GHz band rather than the 2.4 GHz band where most 802.11n devices function. The 2.4 GHz band is getting crowded, not only with wireless connections, but also other household devices. The transfer rate for 802.11ac is 1300 Mbps (at 5 GHz) compared to the 802.11n standard which is 150 Mbps. So the 802.11ac standard is faster and has less interference than the 802.11n standard.

SENDING AND RECEIVING DEVICES

33 A web-enabled device is one that provides access to the internet and email from any location. It can be held in one hand.

34 A smartphone can access the internet and email, as well as send and receive voice-based communications. It can have a range of web-based apps and can operate as a media player and digital camera.

35 Convergence of technologies refers to devices that perform more than one function, where previously separate devices would have performed each of those tasks singularly. For example, a smartphone is a phone, but also sends email, takes photos and plays media files. In the past, a separate device would be required to perform each of these tasks.

36 Smart wristwatch, fitness tracking devices and virtual display glasses.

COMMUNICATIONS CHANNEL AND TRANSMISSION MEDIA

37 Fibre-optic cable uses light to transmit data. It is, therefore, unaffected by electrical interference and can be used over large distances with negligible loss of signal.

38 Wireless transmission is used when it is cheaper to install than wired cables, if portability is a major requirement, or when it is impractical or impossible to install cables.

39 Cellular radio is a form of broadcast radio that is used widely for mobile communications, specifically wireless modems and cellular telephones.

40 Provided the smartphone has near field communication (NFC) capability, the phone can read a tag on the exhibition. The tag contains an embedded chip that transfers information to the smartphone.

41 Microwave transmission requires line-of-sight communication. If there are any buildings, trees or other objects between the transmitter and the receiver then transmission will be blocked. This can become a problem if a new building is constructed in the current line of sight of an existing microwave network.

42 The slower speed of a dial-up modem for an uplink to a satellite is not of concern because users tend to uplink only small amounts of data compared with the amount they downlink.

NETWORK SECURITY

43 A virus can destroy files, overwrite boot sectors on hard drives (stops computers from loading the operating system) and alter directory information.

A worm uses up system resources by repeatedly copying itself.
A Trojan pretends to be doing one thing while secretly collecting data, such as email addresses or bank account details, which are then sent to others.
A keylogger secretly monitors keystrokes, which can lead to passwords being compromised.

44 Verifying the identity of a user through a username and password system restricts access to authorised people only. This stops people who are not recognised by the system from accessing or changing data or files on the network.

45 A firewall is hardware and/or software that restricts access to data and information on a network. It is placed between the network’s servers and the outside communication channel.

46 A firewall should be used to block server ports, thus restricting access to outsiders to the network. Wireless access points should be configured so that they do not broadcast a network name. Data transmitted over the wireless network should be encrypted so that if unauthorised access does occur, the data will be meaningless.

LEGAL AND ETHICAL RESPONSIBILITIES

47
- To ensure that copyright laws are not infringed and privacy laws are complied with
- To ensure that that sexually explicit material is neither stored nor accessible
- To prevent the posting of defamatory comments (or delete defamatory content if it is posted)
- To ensure that user communications are secure

48 Responses will vary. Students should include the URL in their answer, a screenshot and describe how the researchers or analysts are using the entries.

49
- Avoiding the use of bad language.
- Not typing emails in upper case (since it looks like you are shouting).
- When forwarding an email remove all personal information relating to the original sender, including their email address.
- Obeying the rules of online discussion forums.
- Avoid 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.

BENEFITS AND RISKS ASSOCIATED WITH USING NETWORKS

50 Any five of the following are acceptable.

- To facilitate communications, as well as make communicating easier; for example social media, email or VOIP
- To share hardware between multiple users
- To share data and information, because files can be stored on a server or on the internet so that any authorised user can access the data and make changes
- To share software; network administrators can control who has access to what software and multi-user licences are often are cheaper than stand-alone
- To transfer funds
- To raise business profiles
- For entertainment such as video streaming and multi-player gaming
- For knowledge acquisition

51 Users of networks rely on program and document files to be available whenever needed, for resources such as printers to produce their output when required and for communications channels such as email to be readily available. If a fault occurs in a component of the network then some or all of the functions will become unavailable. Users may get to the point where they are so dependent on the network that if it fails they have no reasonable alternative to complete their job, so they become idle and the organisation is unable to meet its goals.

52 The network’s performance may not be at optimal levels if components are not fully compatible or do not use available capacity. Viruses and other malware can infiltrate the network and cause problems. The network may become susceptible to accidental, deliberate or technical threats to the security of data and information.

53
- Employees may post material that breaches copyright.
- Employees may resent being monitored on social media.
- Market-sensitive data may be revealed on social media before a public announcement.
- Comments on social media posted by employees or customers relating to the company may be derogatory or unduly negative.
- Employee opinions and views may not reflect that of the company.

Apply your knowledge

1 A wireless broadband router

2
- A wi-fi network is needed, preferably operating with the 802.11ac standard. It should use WPA2 security, which will encrypt all data transfers over the LAN.
- A wireless broadband router is needed to receive the internet connection. It should include a firewall to block unauthorised access to the network.
- A switch will be needed to connect each device on the LAN.
- Wireless access points may be needed if the site is physically large. Both this and the router should be configured so the network identifier is not broadcast.
- A network-attached storage device is required to store large media files.
- Network printers and scanners will be needed.
- Hackers can sniff the SSID from a packet being transmitted over the network and use it to gain unauthorised access, so use wi-fi protected setup (WPS) to attach new devices to the wireless network.
- Assign static IP addresses internal network devices.

3 Ethernet cabling is most likely needed, either CAT5e or CAT6 twisted pair. Each LAN will need a switch to connect devices within that LAN. A router is needed to pass files from one LAN to another.

4 A network-attached storage (NAS) device, NAS, is the best solution for storing large media files on the network.

5 File server, email server, web server, proxy server and print server

6 A VPN is required. A VPN is a network that uses a public telecommunication network, such as the internet, to provide remote offices or individual users who are away from the office with secure access to their organisations LAN.

7 An information systems manager needs to ensure that:

- To ensure that copyright laws are not infringed: software on the network has been purchased legally; and text, video and images loaded on websites or in files available on the network are original works or permissions have been granted by the copyright owner
- To uphold privacy laws: to verify that permission has been granted from people for their photos to be used on a website or in documents stored on the network; personal details are not disclosed and information is not available that allows a third party to identify an individual; and to ensure that the organisation website provides a privacy policy
- To ensure that that sexually explicit material is neither stored nor accessible
- To prevent the posting of defamatory comments (or delete defamatory content if it is posted)

- To ensure that user communications are secure: the network system guards against messages being illegally intercepted, including suitable security protocols and encryption

8
- Security breaches, such as potential attacks by hackers or malware
- Inappropriate use of social media by employees, which may include content that infringes on copyright laws, privacy requirements or is defamatory
- The revealing of market-sensitive data to the public

Strategies to reduce the risk include the following.

- Use firewalls and wireless security using WPA2.
- Do not publish the wireless network name.
- Regularly update the login and password details including a minimum 8-digit password that requires alphanumeric characters and special digits.
- Create a procedures manual that clearly outlines how material to be published online is to be authenticated and checked for breaches of copyright and privacy laws.
- Conduct regular compliance checks.
- Publish a privacy policy that all employees must follow.

9 Responses will vary.

10 A chip containing the information about XYZ Engineering is embedded into a tag on a poster or exhibit. A user can touch the tag with their smartphone, which triggers a data transfer from the tags to the smartphone. An smartphone app then displays the data.