CHAPTER TEST ANSWERS

Chapter 3 Networks

Section A

Multiple-choice questions

1 LAN stands for:

C local area network.

2 The network device that allows multiple cables to connect together is a:

B switch.

3 Wireless networks communicate using:

A radio waves.

4 The defining characteristic of a LAN is that:

C it does not spread very far.

5 A node in a network is:

D any device that can receive or transmit data.

6 An intranet is:

B a closed, local form of the internet.

7 A web server:

C delivers webpages.

8 A wide area network (WAN) covers:

D a larger area than a LAN.

9 What is the difference between client–server and peer-to-peer networks?

A Client–server networks have a central controlling authority.

10 A virtual private network (VPN):

A allows external users to gain secure access to a LAN.

11 What is a firewall used for?

C Protecting a LAN against outside intrusion

12 A network interface card (NIC):

D allows a node to connect to a LAN.

13 A major potential problem associated with using wireless networking is:

B security.

14 A Melbourne business has 20 workers, many of whom are constantly roaming around the offices and factory with mobile computers and connecting to the company's database from different locations. Their LAN would be best to focus on using:

B wireless networking.

15 A network operating system is needed for:

A a file server.

Section B

Short-answer questions

1 Refer to the following URL to answer the question.

http://www.vcaa.vic.edu.au/Pages/vce/Index.aspx

a Identify the domain name.

Answer: www.vcaa.vic.edu.au

b Identify the resource name.

Answer: Index.aspx

c What does 'URL' stand for?

Answer: Uniform resource locater

d Identify the path.

Answer: /Pages/vce/

e Identify the protocol.

Answer: http://

2 **a** Explain how the DNS is related to domain names and IP addresses.

Answer: The DNS looks up a domain name (1 mark) to find its registered IP address (1 mark), so the web server that hosts the domain can be found (1 mark).

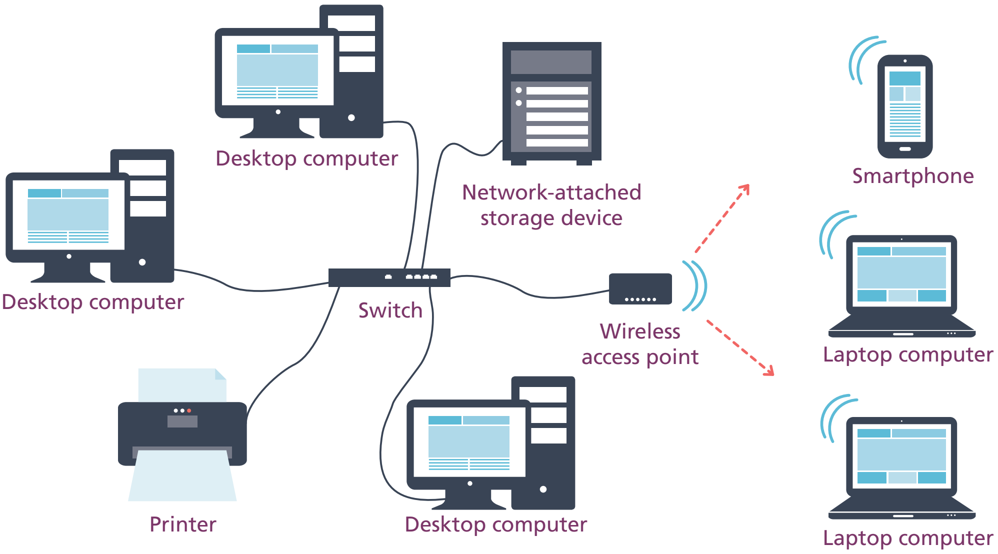
b Explain what HTTPS, TLS and SSL have in common.

Answer: All relate to encryption of web traffic (1 mark). HTTPS, a communications protocol for secure transmission, uses TLS to transmit data safely over the internet, while SSL was the predecessor to TLS (1 mark).

3 A small office has three workstations, laptops for the manager and assistant manager, a smartphone for the manager, a shared printer and internet access for all users.

Create a network diagram suitable for this office. Label all components.

Answer: Responses will vary. However, you should expect something similar to the diagram below.



4 **a** Define ‘network protocol’.

Answer: Network protocols are rules and conventions for communication between network devices (1 mark). Protocols for networks generally use packet-switching techniques to send and receive messages in the form of packets (1 mark).

b Why is it important to use standard networking protocols?

Answer: Standards are important in the computer industry because they allow the combination of products from different manufacturers to communicate meaningfully. Without standards, only hardware and software from the same company could be used together. (1 mark). In addition, standards make it easier to learn how to use new applications (1 mark).

c Identify the protocol used to request and send webpages.

Answer: HTTP (½ mark), hypertext transfer protocol (½ mark)

5 A networking consultant is hired to advise the manager of a small business how to protect his network. The network has an ADSL internet connection so staff can use email. They have a file server, and staff need to login to the network before they can use it. They use wireless networking to connect their laptops, phones and tablets to the internet.

Write a report identifying the five main accidental and deliberate threats to the company’s data, and recommendations to protect against them.

Answer: Responses will vary. Some of the many potential ways to protect against threats are listed below. Reports that list any of these should also clearly identify a potential threat, or multiple threats.

- Use strong passwords.
- Securely lock up the file server in a cool and dry environment with filtered, uninterruptible power supply.
- Train staff about detecting and handling phishing, unexpected email attachments and social engineering.

- Encrypt the WAP.
- Shred all paper waste.
- Lock doors, bar the windows.
- Keep visitors and non-staff away from company computers.
- Keep antivirus definitions up-to-date.
- Create and practise a DRP.
- Regularly back up data.