Unit 4—Networks...

HCCS STEM—Computer Science, IT, Engineering, Food/Nutrition, Business Studies

What do I need to be able to do?

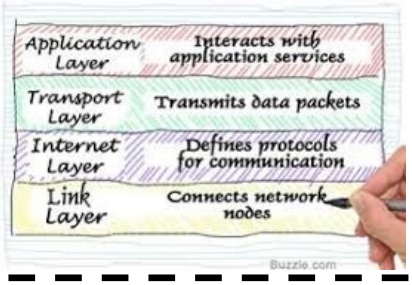
1. You must be able to **explain the purpose of computer networks**, differentiate between **Local Area Networks (LANs)** and **Wide Area Networks (WANs)**, and identify the key hardware on a network, including **routers**, **switches**, and **Network Interface Cards (NICs)**

2. You must be able to explain how the **Internet** works, including the concepts of **IP addressing**, the **Domain Name System (DNS)**, and **packet switching**, and describe the roles of common **communication protocols** like HTTP, HTTPS, FTP, POP3, IMAP, SMTP, and the **TCP/IP model**

3. You must be able to understand the characteristics and features of **network topologies** such as Star, Bus, and Mesh, and describe important methods for **network security**, including identifying vulnerabilities through penetration testing and ethical hacking, and protecting networks using access control, physical security, and firewalls.

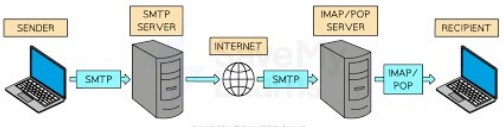
Keywords

1. **Network:** Computers can be connected to a network to share resources, enable communication (like email and social media), and provide services (like web servers and downloads)
2. **LAN (Local Area Network):** A network operating on a single site using its own cabling systems, connectin g nearby computers such as in a school, hotel, or business
3. **WAN (Wide Area Network):** A network connecting two or more networks together across a large geographical area, often using leased lines, with the Internet being the biggest and best known example
4. **Router:** A device that routes packets of data towards their destination by directing individual IP packets from one IP address to another
5. **IP Address (Internet Protocol address):** A unique address assigned to every computer or resource on the Internet, like a front door, which is where packets of data are sent to or received from
6. **Protocol:** A family of standard rules or instructions that devices use to format data and enable communication on a network
7. **Network Security:** The methods used to protect networks from threats and vulnerabilities, including access control, physical security, firewalls, and identifying weaknesses through penetration testing and ethical hacking.



Network Interface Cards are hardware in a device that allow it to connect to a network. **Switches and hubs** are used to connect multiple devices ***within*** a local network, with switches directing data specifically to the destination device while hubs send data to all connected devices; **routers**, however, connect ***different*** networks together, (e.g. home to the Internet, and route data packets.

TCP/IP model has **four-layers** (**Application, Transport, Internet, Link**) where each layer is responsible for a small part of the process. Data starts at the **Application layer** where applications use protocols such as **SMTP, FTP,** and **HTTP**. The **Transport layer**, uses the **TCP** protocol to divide the data into packets. The packets at the **Internet layer**, use the **IP** protocol for routing based on their destination **IP address**. At the **Link layer**, protocols like **MAC, Ethernet,** and **Wi-Fi** handle the physical transmission of data over the network hardware and cables. The self-contained nature of these layers allows different hardware and software to operate at particular layers, providing interoperability.



Network topologies describe the way in which parts of a system are connected; the three main types: Star, where computers and other devices are all connected to a central switch or hub; Bus, where devices are all connected to a central cable; and Mesh, where computers or devices are able to communicate directly with other devices.

Identifying weaknesses can be **penetration testing**, or deliberately trying to find security holes via White box (with system knowledge) and black box (without inside knowledge) testing. Networks can be protected using **access control** (usernames and passwords), **physical security** (CCTV, alarms, and locks), and **firewalls** which separate a trusted network from an untrusted one (check data packets against filtering rules).

10 Test your understanding questions

Here are 10 multiple-choice questions summarising the whole unit:

1. Which of the following best describes a **LAN (Local Area Network)**?

a) A network connecting multiple networks across a large geographical area. b) A network operating on a single site using its own cabling systems. c) The largest collection of interconnected networks in the world. d) A network that uses radio waves for communication.

2. Which network device is primarily responsible for directing data packets between different networks, such as connecting your home network to the Internet?

a) Switch b) Hub c) NIC d) Router

3. What is the purpose of an **IP address (Internet Protocol address)**?

a) To translate domain names into numerical addresses. b) To uniquely identify a computer or resource on the Internet for sending or receiving data. c) To manage the physical connection of a device to the network. d) To break data into small packets for transmission.

4. Which standard set of rules defines how data is formatted and transmitted on a network?

a) Packet switching b) Topology c) Bandwidth d) Protocol

5. In the **TCP/IP protocol stack**, which layer is responsible for breaking up messages into packets and reassembling them at the destination, as well as detecting errors?

a) Application layer b) Transport layer c) Internet layer d) Link layer

6. Which protocol is commonly used for accessing and receiving web pages via the Internet?

a) FTP b) SMTP c) HTTP d) IMAP

7. What term is used to describe the physical or logical layout of how computers and other devices are connected in a network?

a) Protocol b) Network topology c) Bandwidth d) Penetration testing

8. In which network topology are all devices connected to a single central cable, often requiring terminators at each end? a) Star b) Bus c) Mesh d) Ring

9. Which network security method involves physically protecting network hardware and access points using techniques like locks, alarms, and CCTV?

a) Access control b) Firewalls c) Ethical hacking d) Physical security

10. What is **Packet Switching**?

a) Setting up a dedicated connection between two devices for the duration of communication. b) Sending data over a single cable to all connected devices. c) Breaking data into small units that are routed individually across the network. d) Using usernames and passwords to restrict network access.

10 Test your understanding answers

1. b, 2.d, 3.b, 4.d, 5.b, 6.c, 7.b, 8.b, 9.d, 10.c