UNIT 1 COMPUTING 2016

AOS 2: NETWORKS

OVERVIEW

- In this area of study students investigate how networks with wireless capability allow data and information to be exchanged locally and within the global environment. Students examine the hardware and software components and procedures required to connect and maintain a wireless network. They focus on ways in which the security of exchanged and stored data and information can be compromised in wireless networks, in order to understand ways of controlling the networked devices they use.

- Students apply this technical knowledge to create the design for a network with wireless capability that meets a need or opportunity, identifying its components and how data and information are transmitted. Students use a software tool to depict the components of their network and its interactions.

- When designing network solutions, students apply systems thinking by considering how users will interact with the network and the potential effects of the network on users and their data and information.

Key Knowledge

Digital systems

- Applications and capabilities of Local Area Networks (LANs) &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, measured in terms of data transfer rate, data storage options, cost, security and reliability
- 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

Interactions and impact

- ways in which 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.

Key Skills

- describe the capabilities of different networks and wireless communications technology
- compare the capabilities of a range of network components to support the communication and storage of data and information
- apply design thinking skills when configuring a network solution with wireless capability, taking into account how data and information are transmitted and secured
- apply systems thinking skills to predict risks and benefits of the implementation of a new or modified network solution with wireless capability for the users.

Key Knowledge

On completion of this unit the student should be able to design a network with wireless capability that meets an identified need or opportunity, explain its configuration and predict risks and benefits for intended users.

What is a network?

- ***A network is a collection of computers and devices connected by communication channels that facilitates communication between users and allows user to share resources with one another.***

- Resources include data, information, hardware and software.
- The ability to share resources such as servers, printers and software also makes a network valuable.

Network needs…

For successful communication a network needs:

1. **A sending device** which initiates an instruction to transmit (e.g. A notebook or phone)
2. **A communication device** to forward packets of data (e.g. a wireless adapter inside a notebook)
3. **A communication channel or transmission media** through which the signal travels (e.g. cable or radio waves)
4. **A communication device** to receive the signal from the channel. This forwards the packets to the receiving device (e.g. a router)
5. **A receiving device** which accepts the data (e.g. a printer)

Note: Sending devices are also usually receiving devices and often have built in communication devices.

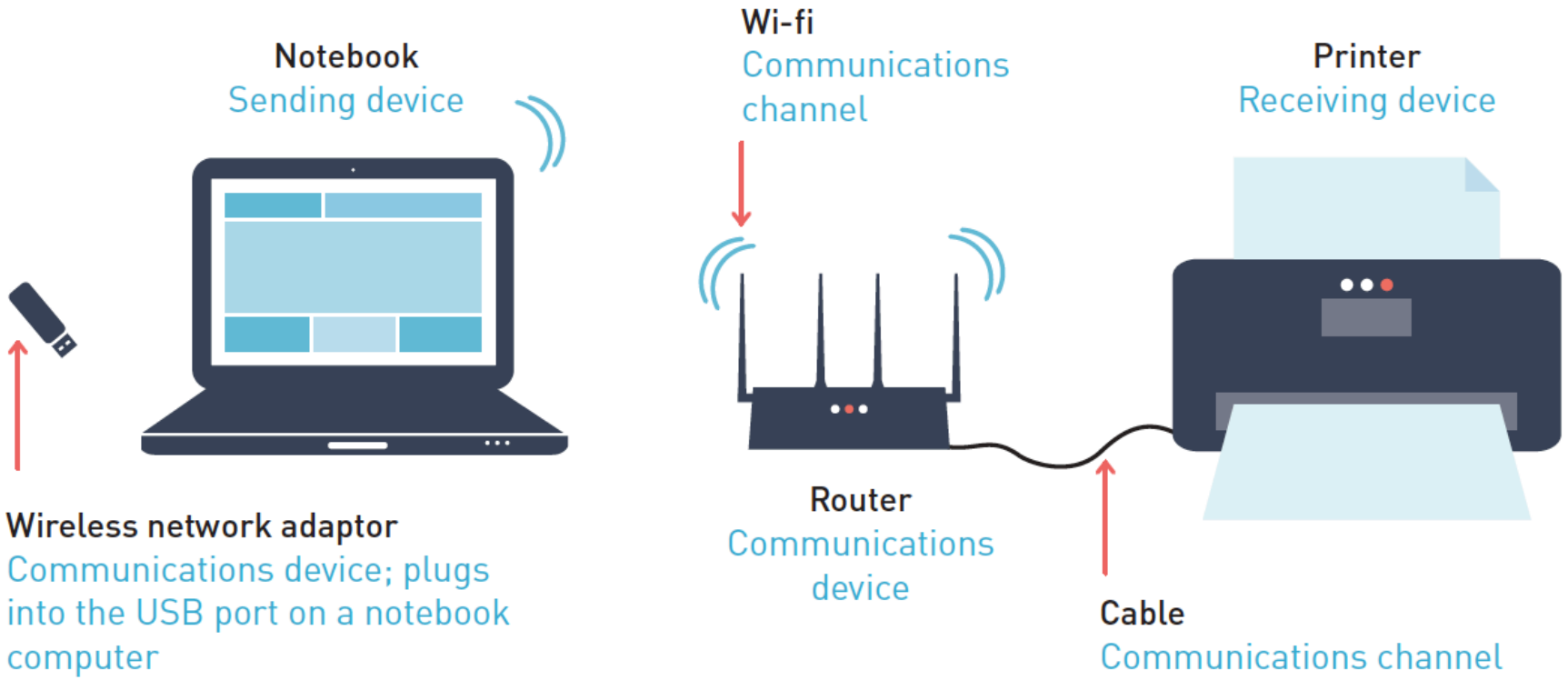


FIGURE 3.1 The notebook sends an instruction to the wireless adapter (communications device), which sends a signal over radio waves (communications channel). The router (communications device) receives the signal and sends an instruction to print via cable (communications channel) to the printer (receiving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

Test Your Knowledge

In my InTray there are the first few pages of the textbook, key terms and test your knowledge.

Write up the definitions for:

- Network
- Communication device
- LAN, WAN, Intranet, VPN

Test Your Knowledge Questions 1-5

Types of Networks

- In groups of 2 or 3 (max), you will be allocated one type of network or network architecture to investigate and report back to the class on.
- You will need to create a visually appealing **POSTER**, that will be displayed in class that includes:
  - The network / architecture name (full name)
  - Key characteristics and features
  - Network requirements
  - Examples of where this network might be found
  - A network diagram

Networks

NETWORK TYPE	NETWORK ARCHITECTURE
Local Area Network (LAN)	Client -Server
Intranet / Home Network	Peer-to-peer
Wide Area Network (WAN)	Internet peer-to-peer
	Virtual Private Network (VPN)

1024 bytes	=	**1 KB**
1024 KB	=	**1 MB**
1024 MB	=	**1 GB**
1024 GB	=	**1 TB**
1024 TB	=	**1 PB**

KB	=	**Kilobyte**
MB	=	**Megabyte**
GB	=	**Gigabyte**
TB	=	**Terabyte**
PB	=	**Petabyte**

Communication Devices

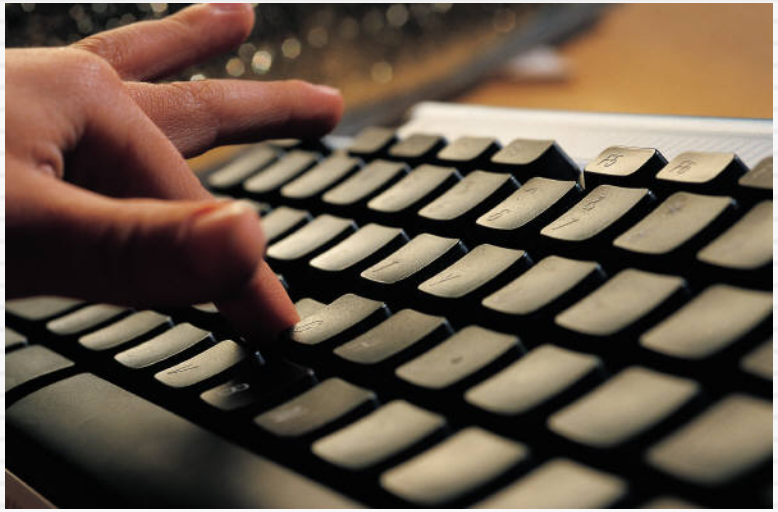
Communication Devices

- Communication devices enable computers users to communicate and exchange information with other devices. They send and receive the data/ information transmitted from one device to another.
  - Switches
  - Routers, Broadband routers, Wireless broadband routers
  - NBN Devices
  - Network interface cards (NIC)
  - Wireless adapters
  - Wireless access points
  - Wireless extenders

Communication Devices

Communication Device	
Switch	A device that provides a connecting point for cables in a **LAN**. Packets are sent from one node (device / computer) on a LAN to the switch, which, then forwards the packets to the desired receiving node (device / computer) by identifying the correct MAC address (Media Access Control).
Router (Broadband and Wireless Broadband)	A router is used to connect multiple networks – Several LANS or a LAN and a WAN, such as the internet. Routers use IP address to identify the destination of packets.
NBN Devices	The proposed NBN uses a "Utility Box" known as a Premises Connection Device, which is installed outside the house and then connected via Fibre-optic cable to a NBN connection box inside the house.
NIC / Wireless Adapters	A NIC is installed in a PC or built in to the motherboard. A wireless adapter performs the function of a NIC for laptops and mobile devices. It strengthens computer signal, packages data and controls access to and from the network. Most mobile devices now have built in wi-fi adapters.
Wireless Access Point	A communication device used on wireless LANS. It acts as a central transmitter and receiver of wireless radio signals. Often used in larger buildings and businesses were wireless coverage needs boosting.
Wireless Extender	Increase the area covered by a wireless network. Wireless extenders pick up a wireless signal and re-broadcast the signal to create additional connections.

Communication Software



Communications Software

- Communications software is an application or program designed to pass or support the movement of information over a network.
- Communications software consists of programs that help to establish a connection to another computer or network and manage the transmission of data, instructions and information.
- For two computers to communication, they must have compatible communications software.

Communications Software

- **Network Operating System (NOS):** The system software that organises, controls and coordinates the activities on a LAN. A NOS controls the devices on network (computers, printers etc.) and the communication between them.

- **Network analysis tools:** Software designed to to analyse and configure various aspects of computer networks. E.G. measure the traffic on a network or identify IP's and computer names.

File Servers / NOS

- File servers run the Network operating system (NOS) which handles:
  - authenticating users during login
  - controlling users' access to resources based on their rights
  - managing print queues
  - doing backups
  - running centralised software such as virus scanners
  - running services like DHCP to give out IP addresses to workstations
  - controlling internet services

Internet Services

Internet Services

- **Web browsers:** Software packages that allow users to access and view webpages (Chrome, Firefox, Safari)
- **Uniform Resource Locater (URL):** Think of like a street address – www.google.com
- **Domain Name Server (DNS):** Identifies the requested site and ensure that the data and information is routed to the correct device.
- **Hypertext Transfer Protocol (http):** A set of rules that defines how pages are transferred on the internet.
- **Hypertext Transfer Protocol Secured (https):** A communication protocol for secure transmissions over the internet. Provides authenticated and encrypted communication.

Internet Services

- **Email:** The transmission of messages and files via a computer network.
- **File Transfer Protocol (FTP):** An internet standard that allows computers to upload and download files
- **Voice of Internet Protocol (VoIP):** Allows users to speak to one another over the internet
- **Cloud storage:** 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 computers hard drive.

Internet Services

- **What do you think are the positives and negatives to cloud storage?**

Network Communication Standards

Network Standards

- To avoid problems associated with incompatibility between hardware and software components, we use 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 (cable, wireless), the speed at which data flows and the physical technology used.
- The most common in wired and wireless networks are Ethernet and TCP/IP

Protocols

- Communication protocols are agreed sets of rules and procedures for computers to exchange information.
- Like humans agreeing to speak the same language during a conversation.
- For two computers to exchange data, they must be using the *same or compatible* protocols.

Network Communication Standards

- **Ethernet:** ***A popular network standard that allows personal computers to contend for access to the network.***
- Used in most LAN setups
- Inexpensive
- Ethernet cables are used to transmit data
- Measured in bits per second (bps): standard = 10 Mbps
- Relatively slow in todays standard
- Twisted pair cabling

Network Protocols

- There is a standard protocol for each network communication task, such as:
  - - how to send data over the Internet (TCP/IP)
  - - how to send and receive email (POP, IMAP)
  - - how to request and deliver web pages (HTTP)
  - - how to request and deliver files (FTP)

- The internet only works because TCP/IP, POP, FTP and HTTP are universal standards, used by *all* shapes and sizes of computers.

Protocols – TCP

- **TCP (Transport Communication Protocol)**
- Breaks files into *packets* to be sent across the internet or a network.
- Each packet contains:
  - the address of the sender
  - the destination address
  - error-detecting checksum
  - a chunk of data (e.g. 1K)

Protocols – TCP/IP

- **IP (Internet Protocol)…**
- Once a file has been chopped into packets, the IP protocol delivers each packet to its destination.
- each packet can take a different route from A to B, bouncing from router to router getting more precise with each hop.
- the route is dynamically chosen for each packet, based on internet conditions at that time.

Protocols – TCP/IP

- **TCP again…**
- At the packets' destination the receiving computer's TCP re-assembles packets back into the original file.
- Recalculates checksum to see if packet is OK
- If packets are damaged, lost or delayed in transit, TCP will request the server to send the packet again.

Packet transmission

- https://www.youtube.com/watch?v=xIuBmOufbIs&nohtml5=False

Network Communication Standards

- **802.11:** Developed to specify how wireless computers or devices communicate with each other via radio waves.
- Range is up to 300 meters in open / outside areas and approximately 50 meters inside buildings.
- The term Wi-Fi (wireless fidelity) identifies any network based on the 802.11 standard.

Mobile Devices Connected to Networks

Mobile Devices

- Store programs / apps
- Small / Portable
- Connect wirelessly to the internet
- Can be connected to a computer to exchange information
  - Smart Phones
  - Hand held computers
  - Navigation systems
  - Gaming consoles
  - Digital cameras

Activity

- Read through pages 104-109.
- Create a summary of each Mobile device
  - 1. Outline what the device is used for
  - 2. Document three key capabilities and and two limitations of each device

Communication Channel

Communication Channel

- **Channel:** The path between two devices.
- **Bandwidth:** The width of the communication channel. The higher the bandwidth, the more data and information the channel can transmit
- **Transition Media:** The physical (wire, cables / fibre-optics) or wireless (radio waves, microwaves, infra-red) method carrying the data from one device to another

Physical Transmission Media

- Read through page 110 – 111,
- Make a comparison between Twisted-pair and Fibre-Optic cabling. (Speed, material, bandwidth, pros / cons)

NBN

- https://www.youtube.com/watch?v=dMAA4XCmaNk

Wireless transmission media

- Used when its inconvenient, impractical or impossible to install cables.
- Broadcast radio, cellular radio, microwaves, communication satellites and infra-red.

Wi-Fi Communication

- Slower and more susceptible to noise than wired physical transmission media, but it provides flexibility and portability.

- Read 113 – Summarise the pro's and con's to the different ranges (GHz) available for Wi-Fi networks.

Bluetooth

- Short-range radio waves to transmit data.
- Generally a 10 meter range, can be boosted with additional equipment

Cellular radio

- Broadcast radio that is used widely for mobile communications, specifically mobile phones.
- Different generations of cellular transmissions exist, with significant speed improvements since its inception.

Microwaves

- Radio waves that provide a high-speed signal transmission.
- Involves sending signals from one microwave station to another.
- Signals need to travel in straight lines (and therefore avoid obstacles like buildings and mountains)

Communication Satellite

- A space station that receives microwave signals from an Earth based station, amplifies (strengthens) the signal and broadcasts the signal back over a wide area.

Network Design

- https://www.draw.io/

Create a network diagram for the following

- Office building with 4 desktop computers
- 2 laptops with wireless connection
- 1 x Central server
- 1 x Router
- 1 x Switch
- Internet
- 1 x Printer / photocopier
- 6 mobile phones (wireless)

NETWORK SECURITY

Network Security

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

Security Threats

- Threats can come from actions, devices and events.

- Accidental (losing a USB)
- Deliberate (Denial of service)
- Result of an event (power outage)

Accidental Threats

- Hard to guard against
- Vigilance required

E.G.

- Sending an email to the wrong person
- Accidently deleting a file
- Losing a USB

Deliberate Threats

- When someone tries to intentionally damage or manipulate the system.
- Hacker – bypassing network security to sabotage files or alter data
- Malware – Intrusive software that causes damage.
  - Viruses
  - Worms
  - Trojan
  - Adware
  - Spy Ware
  - Keyloggers
  - Logic bombs
  - Phishing

ACTIVITY

- Create a power point presentation outlining each type of Malware. Include:
- How the Software works, the damage is causes and examples.
  - Viruses
  - Worms
  - Trojan
  - Adware
  - Spy Ware
  - Keyloggers
  - Logic bombs
  - Phishing

Event based threats

- Do not involve accidental or deliberate actions of a human.
- E.g. A power surge or a hard drive crashing.

PRACTISE SAC CONTINUED

- 5. Outline one advantage and one disadvantage for tutors who will utilise the wireless communication technology on the network.
  2 marks
- 6. When tutoring students in one of the tutoring areas tutors have the choice of using either a laptop or tablet in the room to access the resources needed during a session. List which of the two devices would be more appropriate for tutors to use during a session – a laptop or a tablet. Justify your answer. 3 marks
- 7. Sam has also talked to Benita about the potential of malware threating the security of the network. Other than malware, discuss one security threat to the data stored centrally on the network.
  2 marks
- 8. Define the term 'malware'. Give an example to support your answer.
  2 marks

Measures to secure networks

- Usernames and passwords
- Firewalls
- Uninterruptible power supplies
- Wireless securities

Usernames and passwords

- Used by most networks
- Access rights are assigned to the user profile by network administration (preferences / power)
- Unique credentials are used login to the network

Firewalls

- Firewalls are used to prevent unauthorised access to data and information on a private network.
- This can include denying access
- Firewalls are used in conjunction with Proxy Servers to monitor / screen all incoming and outgoing messages.
- A firewall can be set to block all or some ports available on a network.

Uninterruptable Power Supplies (UPS)

- As power loss can cause significant damage to a network, a UPS allows around 10 minutes of reserve power, which provides sufficient time for the network administrator to shut down the network in a safe and orderly way to avoid loss of data.
- UPS also often protect against power surges

Wireless Security

- Wireless access point should be configured to not broadcast the network name.
- Wi-Fi protected access (WPA or WPA2) – a standard that defines how to encrypt data as it travels across a wireless network.
- Wi-Fi protected setup (WPS) – push and connect (less secure)
- Firewall
- MAC Address filtering

Ethics & Legal Responsibilities

- Network professionals and users have responsibilities with respect to social protocols and ownership of data and information.
  - Conduct when online
  - Ownership of intellectual property
  - Application of digital information security practices
  - Use of personal security strategies

- Not adhering to ethical responsibilities can lead to a loss of respect, customers and serious public criticism. E.G. Defamatory comments posted online or emailed, private communication between users is intercepted and publicised.

Ethics & Legal Responsibilities

- Tensions can arise in a workplace if acceptable work practices are not clearly defined.
- User policies and agreements should outline the expected behaviour for network users.

- Read through “Resolving legal, ethical and social tensions”.
- Write out the six steps to resolving tensions.
- Do you think this is an appropriate way to solve ethical issues? Why? Why not?

Benefits and Risks of using a network

- Read page 125-126
- Create an infographic summarising the benefits and risks of using a network
- Post to your Weebly.

Network physical design

- Physical design: takes into account the hardware and software needed to provide the solution.

- Network diagram: Method to represent both the network and all of its different pathways to provide an overview of the connections and to allow IT Staff to identify and locate equipment

Network Diagrams

- Use lines to represent cables
- Icons to represent communication devices
- Physical building not important in a network diagram
- You can identify departments or areas (see Figure 3.39, page 122)

Homework and SAC Preparation

- SAC – FRIDAY 6TH MAY
- Case Study with written responses + draw.io network diagram

- Homework: Complete all chapter summary questions

Next week:

- SAC Preparation: APPLY YOUR KNOWLEDGE (Page 135)
- Practise SAC: Benita / Smarty Pants Tutoring
- Review all network notes and read textbook chapter