# Unit 3: Networks

## 1. The OSI model

Network Stacks and the Internet - Computerphile (7:10)
https://www.youtube.com/watch?v=PG9oKZdFb7w

Computer networks require a complex interplay between application software, the operating system, and hardware systems in order to function. The Open Systems Interconnection (OSI) model was developed to provide an abstraction to identify and separate the roles and responsibilities of each component within the network. It is an official standard with the International Standard Organisation, ISO/IEC 7498.

The OSI identifies seven layers within a network.

1. The Physical layer. The physical layer is responsible for the physical transmission of bits over a physical medium. Examples: Copper wire, fibre optic or wireless spectrum.

2. The Data link layer. The data link layer describes how your networking equipment accesses the physical transmission. The physical MAC address (Media Access Control) of your networking interface cards forms part of the data link layer. Globally every NIC is supposed to have a unique MAC address. The Ethernet protocol operates across the Physical and Data link layers.

3. The Network layer. The network layer adds a logical level of abstraction to the connection between two network nodes. The logical address, such as an IP address, is used to differentiate nodes and determine a path between them.

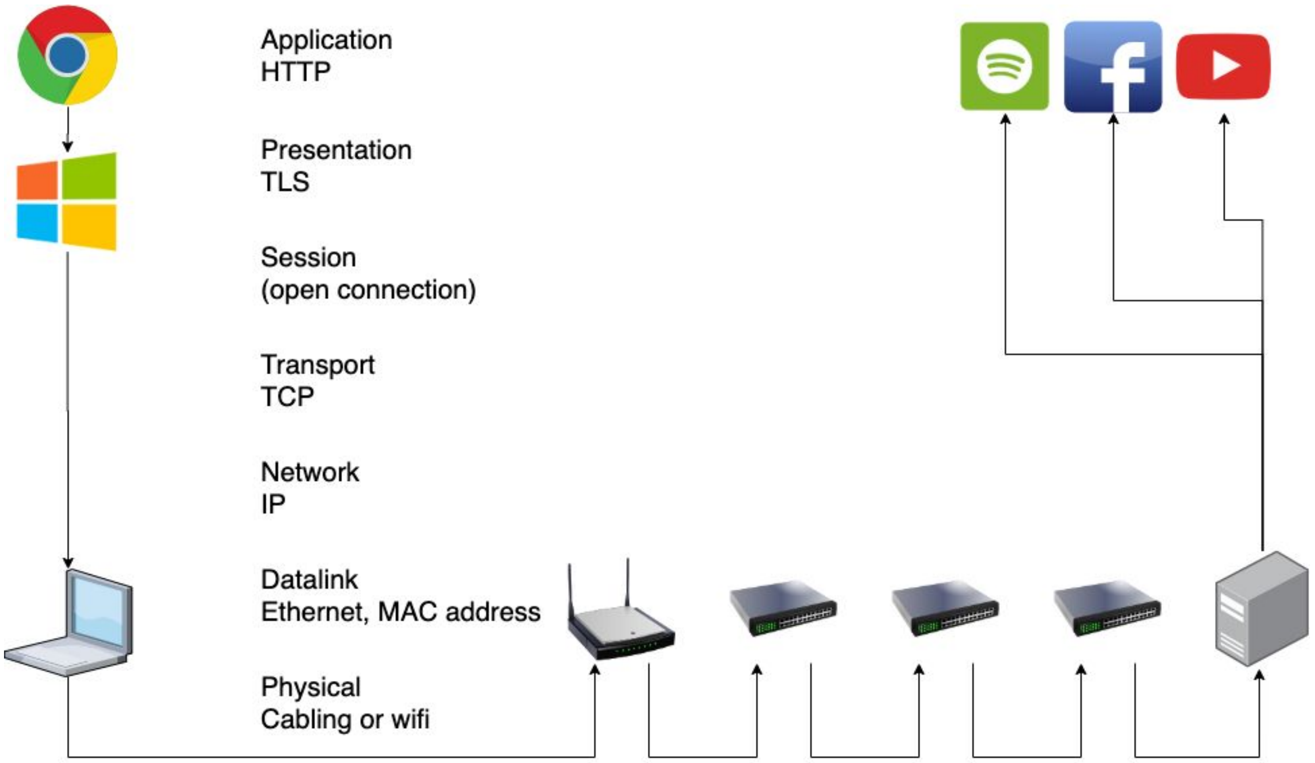
4. The Transport layer. The transport layer will take the information sent by the application and break it into transportable sized packets and transmit them through the network layer. Protocols such as TCP and UDP are used here. TCP (Transport Control Protocol) is used where receipt of transmission must be guaranteed, whereas UDP (User Datagram Protocol) is used where some parts of the message may be lost without significant consequence (think streaming services).

5. The Session layer. This layer establishes an open connection (session) between two network nodes for the transmission and receipt of data.

6. The Presentation layer. This layer is responsible for converting the data from something the application understands, to something that can be transmitted over the network (and then back again). Examples include binary blobs such as JPG images. Encryption and compression of data also occur at this layer (the "S" in HTTPS).

7. The Application layer. The application layer is the communications protocol your individual application is using. The most common example you are likely familiar with is HTTP.

A visual depiction of the different layers working together may look like



# 2. Types of networks

There are different types of networks, often defined by the size of the network, which use different network devices.

| Network type | | Features, size, typical devices |
|---|---|---|
| PAN | Personal area network | |
| LAN | Local area network | |
| WLAN | Wireless local area network | |
| VLAN | Virtual local area network | |
| VPN | Virtual private network | |
| SAN | Storage area network | |
| WAN | Wide area network | |
| P2P | Peer to peer network | |

# 3. Network standards

The glue that allows the different lays of the OSI model to work is the presence of internationally agreed standards that operate at each layer.

These standards are a technical specification that developers use to ensure one system is compatible with other systems at that layer.

Standards provide a technical specification and guidelines for specific network systems used to design and build different types of networks.

Students must be able to demonstrate an understanding of the role of standards to ensure network hardware interoperability, and discuss the similarities and differences between common network standards including wireless (802.11), Bluetooth (802.15.1) and ethernet (802.3).

## 3.1 Wireless (802.11)

- Medium range typically 100m
- Depending on the variant, usually 2.4GHz or 5.0GHz

## 3.2 Bluetooth (802.15.1)

- Short range typically 10m
- For peripheral devices
- 2.4 GHZ

## 3.3 Ethernet (802.3)

"Grandaddy" of the 802 specifications. Provides asynchronous networking using "carrier sense, multiple access with collision detect" (CSMA/CD) over coax, twisted-pair copper and optical fiber media. Current speeds range from 10 Mbps to 10 Gbps. (quoted)

# 4. Network protocols

Protocols are a system of rules that standardise how senders and receivers communicate over a network.

Protocols in networking are recorded in documents known as RFCs (request for comment). For example RFC 791 describes the Internet Protocol (IP), RFC 761 describes Transport Control Protocol (TCP) and RFC 2616 describes the Hypertext Transfer Protocol (HTTP). The RFC documents can be found at https://www.rfc-editor.org/rfc-index.html

As a set of rules to govern the conversation between two nodes on a network, a protocol needs to describe how to manage a range of foreseeable situations.

- Data integrity
- Flow control
- Deadlock
- Congestion
- Error checking

*Students must be able to demonstrate an understanding of the role of common protocols (TCP and IP) to ensure network hardware and software interoperability, how they are implemented (by hardware, software or a combination of both), and outline their role in the management of data integrity, flow control, deadlock, congestion and error checking.*

## 4.1 Internet protocol (IP)

- ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

| | |
|---|---|
| OSI layer | |
| Function | |
| Implementation at hw/sw | |
| Management of integrity, flow, deadlock, congestion or errors | |

## 4.2 Transport control protocol (TCP)

- ftp://ftp.rfc-editor.org/in-notes/rfc761.txt

| | |
|---|---|
| OSI layer | |
| Function | |
| Implementation at hw/sw | |
| Management of integrity, flow, deadlock, congestion or errors | |

## 4.3 User datagram protocol (UDP)

| | |
|---|---|
| OSI layer | |
| Function | |
| Implementation at hw/sw | |
| Management of integrity, flow, deadlock, congestion or errors | |

## 4.4 Hyper-text transfer protocol (HTTP)

- ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt

| | |
|---|---|
| OSI layer | |
| Function | |
| Implementation at hw/sw | |
| Management of integrity, flow, deadlock, congestion or errors | |

## 4.5 Secure sockets layer (SSL) and Transport layer security (TLS)

| | |
|---|---|
| OSI layer | |
| Function | |
| Implementation at hw/sw | |
| Management of integrity, flow, deadlock, congestion or errors | |

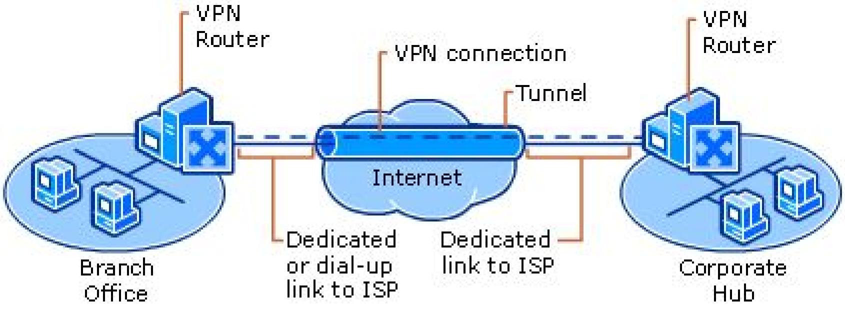
## Network packets & routing

Digital networks encapsulate and de-encapsulate communication into packets to route packets from a source to a destination.

Students must be able to explain how and why digital networks encapsulate and de-encapsulate packets routed through ethernet, wireless, and Bluetooth communication standards.

Watch the animation: https://pbaumgarten.com/ib-compsci/unit-3/img/packet_switching.gif

# 5. Virtual private networks (VPNs)



A VPN (virtual private network), is a software tool that provides an encrypted "tunnel" over the open internet for you to connect and interact with a remote network as if you were physically and presently connected to it.

An extranet is a range of services a network makes available for clients to access externally. They are not treated (granted the privileges) as if they were physically present on the LAN.

What is a VPN? We'll let Linus explain,

- Linus' Techquickie, 2015, VPNs or Virtual Private Networks as Fast As Possible
  https://www.youtube.com/watch?v=DhYeqgufYss
- Text: p145-148

While VPN's have their use, they are not a magic cure all for privacy and security online.

- VPN Companies Are Lying To You
  https://www.youtube.com/watch?v=CNRdHQJ9AMk
- Check
  https://amiunique.org/

VPN properties

- VPN authenticates the sender before (establishing the tunnel)
- VPN access is always encrypted, whereas an extranet may have limited encryption
- VPN transmission is always encrypted
- VPN users have access to everything whereas extranet users only have access to (enabled) specific services

VPN security features:

- Authentication
- Encryption
- Tunneling
- Multiple exit nodes

# 6. Compression

Discuss:

- What is compression?
- Why do we still need to worry about compression given we now have high speed broadband connections and fast processor computers?

## 6.1 Lossy compression

Examples: JPG, M4V

Tom Scott (Why Snow and Confetti Ruin YouTube Video Quality) 4m
https://www.youtube.com/watch?v=r6Rp-uo6HmI

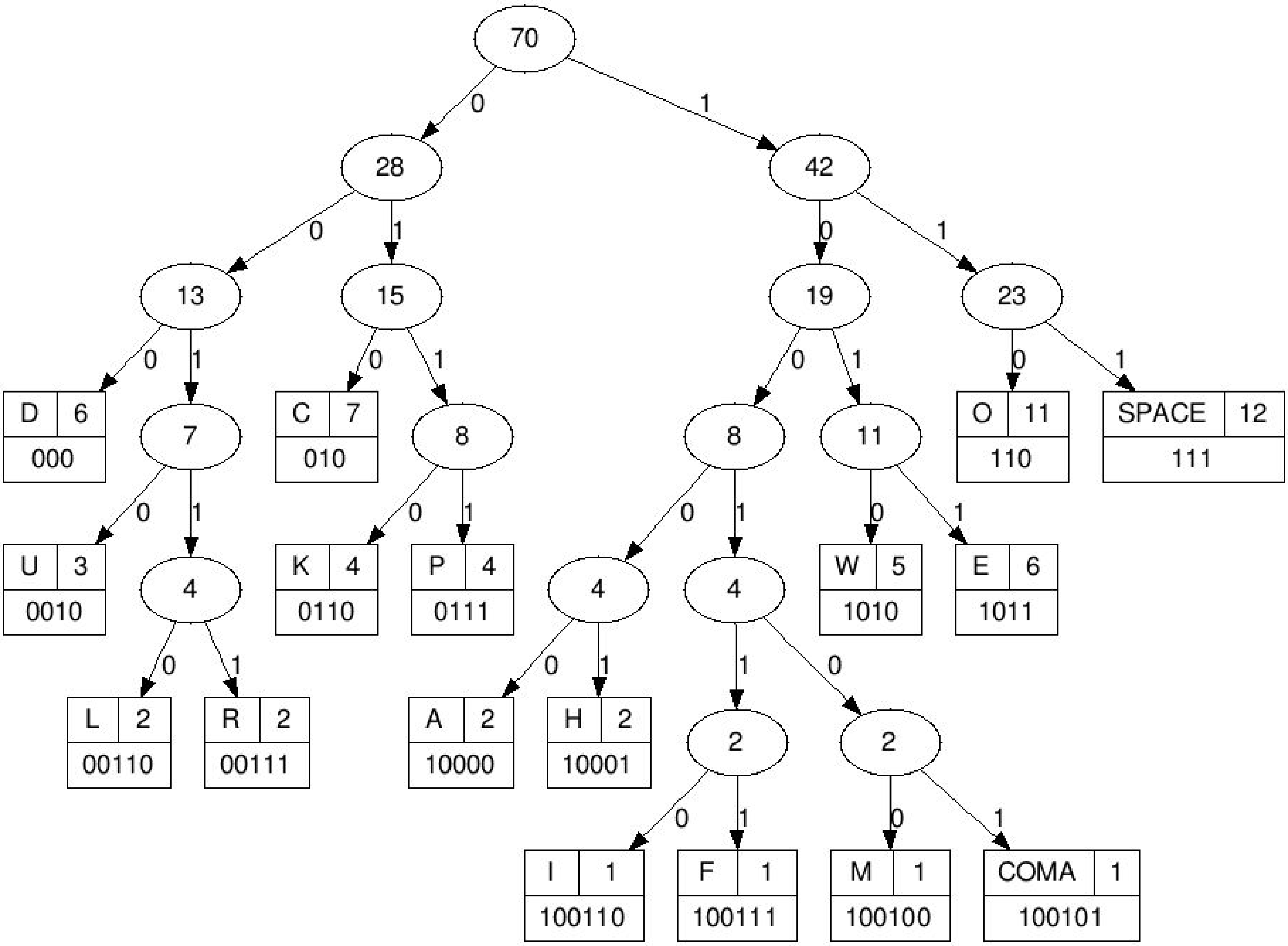
## 6.2 Lossless compression

Examples: Text

Tom Scott Basics: Huffman coding and huffman trees
https://www.youtube.com/watch?v=JsTptu56GM8

Demonstration:

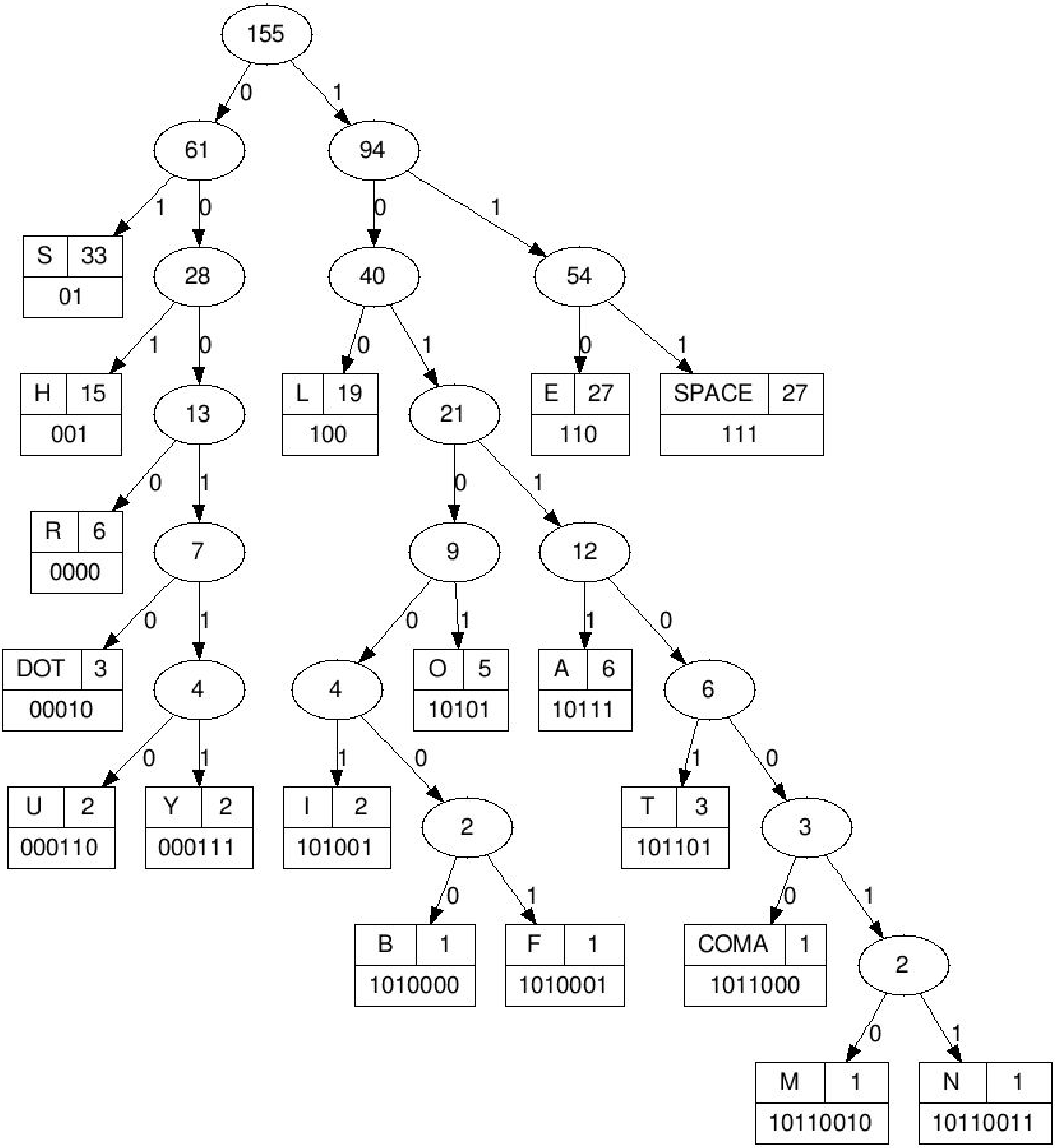
```
how much wood could a woodpecker peck, if a woodpecker could peck wood!
```



http://huffman.ooz.ie/

Example 2

she sells seashells by the sea shore. the shells she sells are surely seashells. so if she sells shells on the seashore, i'm sure she sells seashore shells.



# 7. Transmission factors

Briefly discuss factors affecting transmission rates:

- bandwidth,
- transfer rates of storage devices,
- interference,
- number of devices,
- malware,
- packet loss,
- security processes,
- transmission media
- denial of service attacks

Transmission media:

- Coaxial cabling – Speeds of up to 10Mbps over 300m
- Twisted pair cabling – Speeds of up to 1000Mbps over 100m though is typically running at speeds of 100Mbps in most installations.
- Optical cabling – Speeds of up to 40,000Mbps over many kilometres (speeds of up to 1Tbps are under development!)
- Wireless – Currently offering speeds of up to 50Mbps over 90m (Also known as 802.11)
- HSDPA – The 3G mobile phone broadband network offering speeds of 3Mbps over about a kilometre (ie: to the phone tower)
- Satellite – Speeds ranging from 1 to 40Mbps shared over all users in the region. Weather (especially rain) will slow the signal significantly. Latency becomes a significant issue – 500 to 900 milliseconds. Geostationary satellites are 35,000Kms high in orbit! That's a lot of distance for the signal to travel. What uses would be affected by this kind of latency?

The Internet: Wires, Cables & Wifi (code.org)
https://www.youtube.com/watch?v=ZhEf7e4kopM

Compare Coax, Twisted pair & Fibre (4:30m)
https://www.youtube.com/watch?v=EOCme3sNqws

# 8. Wireless networks

## 8.1 Advantages & disadvantages of wireless networks

Discuss in relation to:

- Changes in work patterns
- Social activities
- Health issues, concerns

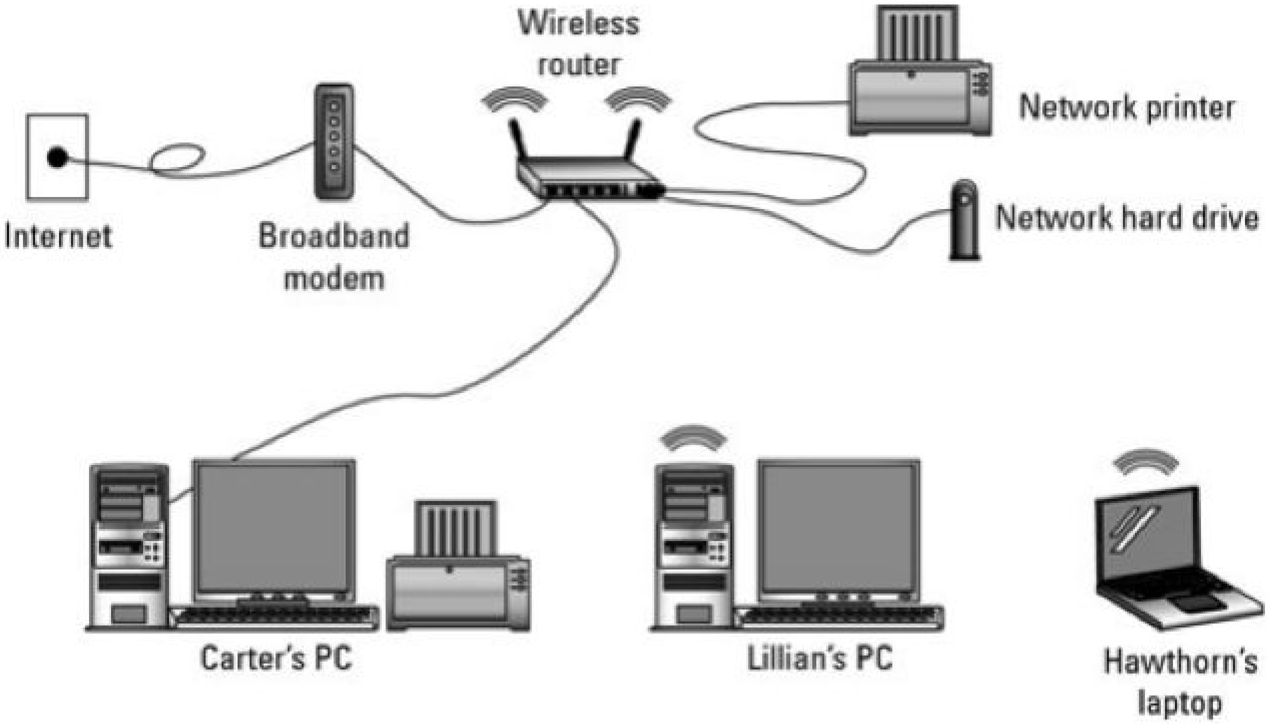
Some positives

- Freedom of movement
- Less infrastructure (no expensive cable runs)
- (Usually) easier to setup
- More devices per uplink

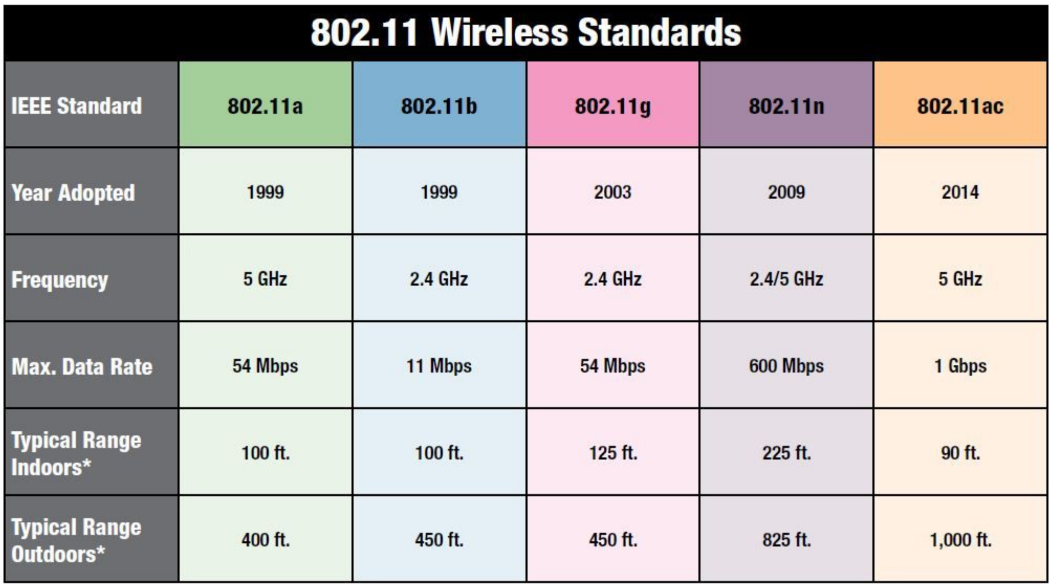
Some negatives

- Slower (shared bandwidth)
- Range
- Susceptible to interference and jamming
- Vulnerable to eavesdropping
- An increasing number of devices are wireless only

## 8.2 Components of wireless networks

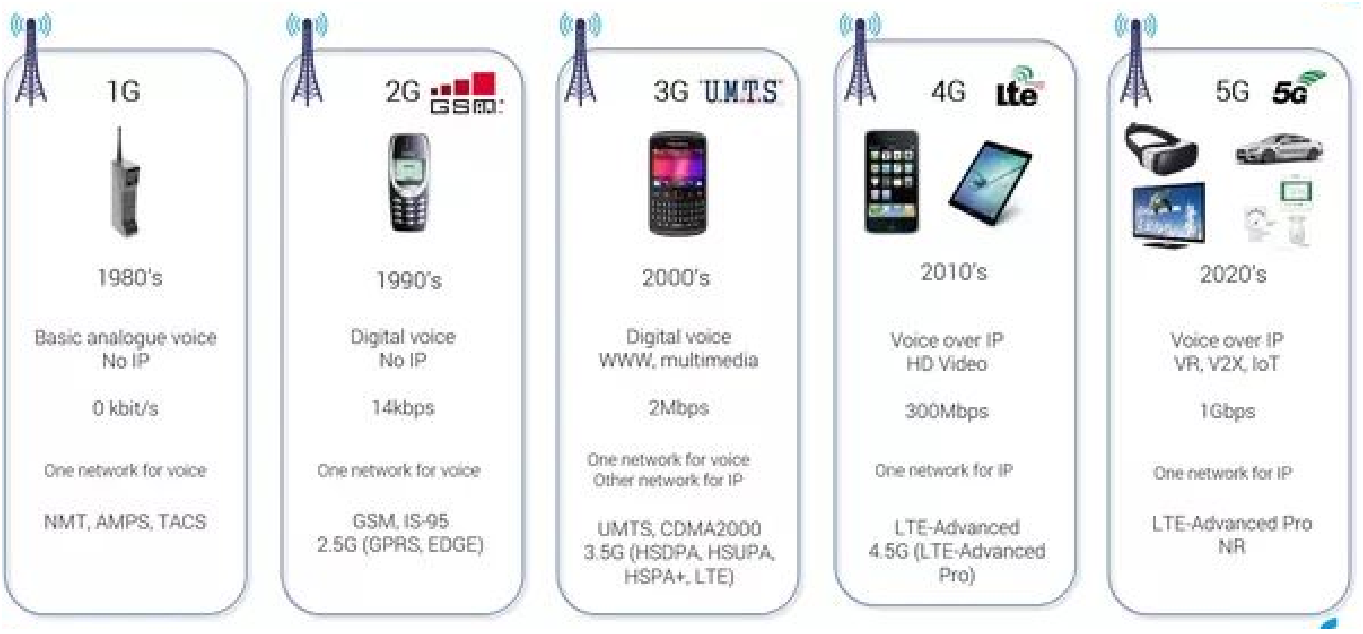


## 8.3 Evolution of wireless networks



802.11 Wireless Standards

| IEEE Standard | 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac |
|---|---|---|---|---|---|
| Year Adopted | 1999 | 1999 | 2003 | 2009 | 2014 |
| Frequency | 5 GHz | 2.4 GHz | 2.4 GHz | 2.4/5 GHz | 5 GHz |
| Max. Data Rate | 54 Mbps | 11 Mbps | 54 Mbps | 600 Mbps | 1 Gbps |
| Typical Range Indoors* | 100 ft. | 100 ft. | 125 ft. | 225 ft. | 90 ft. |
| Typical Range Outdoors* | 400 ft. | 450 ft. | 450 ft. | 825 ft. | 1,000 ft. |



## 8.4 Security of wireless networks

Briefly discuss:

- Firewalls
    - What traffic will you allow in/out?
- Passwords on wifi access points, routers
    - Change the default!
- Enable/disable SSID broadcast
    - Is security by obscurity a valid technique?
- Enable/disable access by MAC address
    - MAC addresses can be changed
- Choosing a wireless encryption protocol
    - WEP, WPA, WPA2, WPA3 - is WPA2 "broken"?
- WPS (wireless protected setup)
    - What is it?
- Controlling physical access
    - Maxim: If you can physically access the device, you can compromise it.

Computer Science Core (p161-170)

# Past paper questions for review

(refer to separate document)

---

**A TCP joke:**

Hello, would you like to hear a TCP joke?
Yes, I'd like to hear a TCP joke.
OK, I'll tell you a TCP joke.
OK, I'll hear a TCP joke.
Are you ready to hear a TCP joke?
Yes, I am ready to hear a TCP joke.
OK, I'm about to send the TCP joke. It will last 10 seconds, it has two characters, it does not have a setting, it ends with a punchline.
OK, I'm ready to hear the TCP joke that will last 10 seconds, has two characters, does not have a setting and will end with a punchline.
I'm sorry, your connection has timed out... ...Hello, would you like to hear a TCP joke?

**A UDP joke:**

I know a UDP joke, but you might not get it.