

CO1507: Introduction to networking

Jonathan Edwards 2023

Summary of module so far

- Binary and hexadecimal numbers
- Network devices and topology
- OSI model
- IP addressing
- ARP
- Custom subnetting
- DHCP
- DNS
- Routing
- CISCO IOS
- IP address depletion and NAT
- IP v6 introduction

Assessment reminder

- Week commenting 18th March (next week)
- Your practical assessment will take place within the normal lab time
- This means your assessment is either on Tuesday 19th or Thursday 21st
 - Attend YOUR normal class- not somebody else's!
- Failure to attend without MCs may result in a grade of 0
- Therefore, if you think you cannot attend apply for MCs ASAP!
- You may NOT access module materials or the internet during the assessment
- You may use **plain paper** to work out, use of a pocket calculator is also permitted
- You may **NOT** bring in any written notes

Wireless Networking (Wi-Fi)

1. What is Wi-Fi?
2. How does it work?
3. Limitations
4. Wireless security

Wireless Networking (Wi-Fi)

- Wi-Fi is a family of wireless networking technologies, using radio waves (RF) to provide connectivity to a wired network or the Internet
- A common misconception is that the term Wi-Fi is short for "*wireless fidelity*"
- However this is not the case, Wi-Fi is simply the wi-fi alliances trademarked phrase based on the IEEE 802.11 standards.
- The first wireless network was created in 1971, known as the "alohonet" and was the precursor to the modern wireless
- IEEE 802.11 standards evolved in the 1990's.

IEEE 802.11 standards

Generation / IEEE Standard	Maximum Link rate	Year Adopted	Frequency
802.11ax (Wi-Fi 6)	600 - 9608 Mbps	2019	2.4 / 5GHz
802.11ac (Wi-Fi 5)	433 – 6933 Mbps	2014	5GHz
802.11n (Wi-Fi 4)	72 – 600 Mbps	2009	2.4 / 5GHz
802.11g	3 – 54 Mbps	2003	2.4 GHz
802.11a	1.5 – 54 Mbps	1999	5 GHz
802.11b	1 – 11 Mbps	1999	2.4 GHz

Wi-Fi

- A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
- A wireless Access point receives the signal and decodes it, then sends the information to the wired network
- Instead of using wired connections like Ethernet, Wi-Fi uses radio waves to transmit information at specific frequencies.
- Wi-Fi most commonly uses the 2.4 gigahertz (120 mm) UHF and 5 gigahertz (60 mm) SHF radio bands

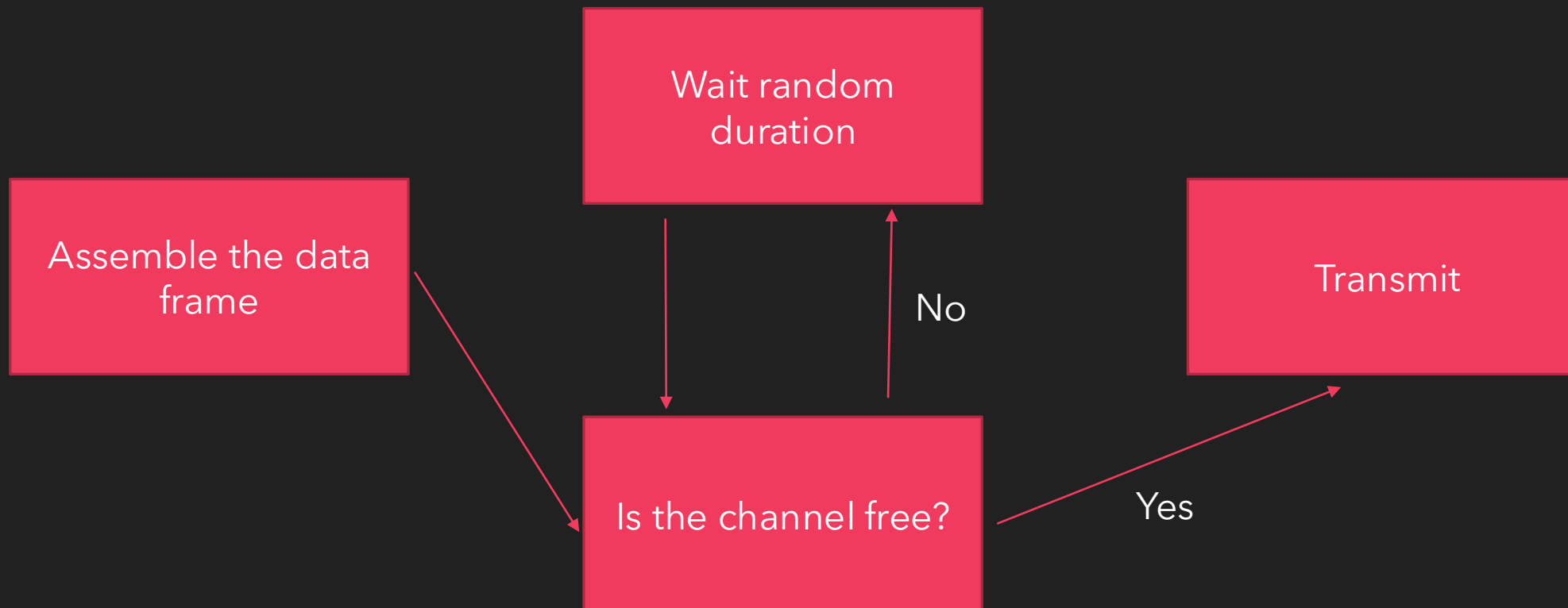
Wi-Fi

- Wi-fi originally operated on the 2.4 GHz spectrum (14 channels) and initially WI-FI wasn't in huge demand,
- Soon cracks began to show when more wireless networks began to emerge.
- A 5GHz spectrum was introduced to reduce this but this to has limitations.
- 2.4 GHz has a longer wavelength than 5 GHz. Longer wavelengths penetrate walls and physical objects better but can't carry as much bandwidth.
- Shorter wavelengths are more affected by the environment around them but suffer from less outside interference and can have higher bandwidth.

Wi-Fi

- All devices within range receive all data frames
 - Similar to devices connected to an old fashioned ethernet hub
- Privacy of data within the network therefore of greater concern
 - Important to encrypt data
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used
- This is in contrast to CSMA/CD (Carrier Sense Multiple Access with Collision Detection) used in wired ethernet

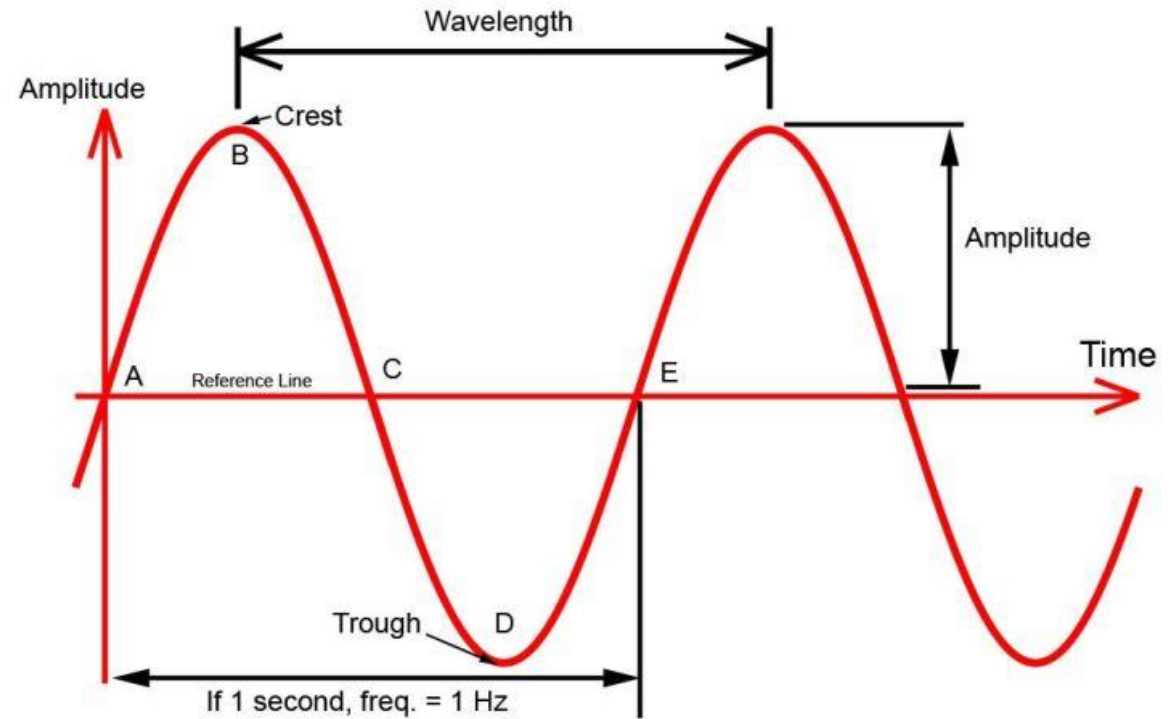
CSMA/CA



Obstacles

- Wireless communication is subject to regulation of the airwaves by national and international bodies
- Signal range can be affected in many ways including the following factors
 - Absorbtion
 - Reflection
 - Refraction
 - Diffraction
 - Scattering
- Interference from other nearby signals is also a concern

RF: Radio Frequency 30Hz - 300GHz (approx)



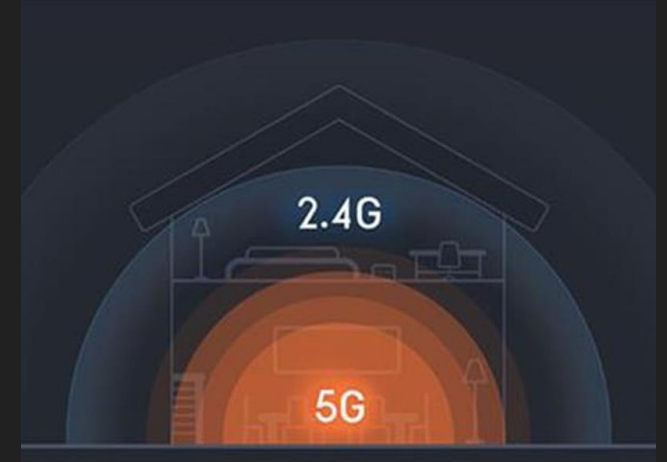
2.4 GHz Vs. 5 GHz

2.4 GHz

- Generally better range than **5 GHz**.
- More interference with other networks (which can lower range).
- Lower speeds.

5 GHz

- This is essentially a higher bandwidth version of **2.4 GHz** Wi-Fi.
- It has shorter range and can have more interference with walls and physical objects.
- However, in most cases, it is faster and has less interference with other wireless signals and electronic devices.



Channels

For example, when we refer to 2.4 GHz we don't literally mean transmission is at *EXACTLY* 2,400,000,000,000 Hz

In reality multiple channels exist within the approx. range of 2.4 GHz

Channel	(MHz)	Frequency range (MHz)
1	2412	2401-2423
2	2417	2406-2428
3	2422	2411-2433
4	2427	2416-2438
5	2432	2421-2443
6	2437	2426-2448
7	2442	2431-2453
8	2447	2436-2458
9	2452	2441-2463
10	2457	2446-2468
11	2462	2451-2473
12	2467	2456-2478
13	2472	2461-2483
14	2484	2473-2495

The channels are 22Mhz wide

The channels overlap so cannot ALL be used in overlapping geographical ranges

Not all channels are used in all countries

limitations of wireless networking

- The typical range of a standard Wi-Fi network can reach up to 100m in the open air
- However it is very susceptible to interference (other devices or thick walls etc.) therefore offers a connection radius of around 20-30m
- Security can still be an issue with Wi-Fi especially for users that just leave their equipment on default settings. (WPA or WPA2 should be used if available).
- It's not ideal for transferring lots of large data over the network as Wi-Fi is usually slower than a wired connection.
- Wi-Fi is inherently more vulnerable to attack than wired networks because anyone within range of a network with a wireless network interface controller can attempt access

Service Set Identifier (SSID)

- SSID is the name of a wireless network
- SSIDs are used to distinguish one WLAN from another
- SSIDs are needed for a PC to connect to a WLAN
- Changing the SSID changes the WLAN and any connected device would need to re-connect
- SSIDs are case sensitive
- Access points broadcast their presence regularly (100ms)

Security

- A user typically needs the network name (SSID) and an encrypted password.
- Wireless Equivalent Privacy (WEP) and Wi-fi protected access (WPA) is a family of technologies created to protect information
- SSID stands for **S**ervice **S**et **ID**entifier and is a case sensitive 32-character string used to identify any given network
- WEP was ratified in 1997 but deprecated in 2004 due to security limitations.
- Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) and soon WPA3 are used due to stronger encryption and mitigates security issues posed by weak passwords.

WiFi 6

- The new standard was announced in April 2018,
- Wi-Fi 6's headline feature that it will support transfer speeds of up to **10Gbps**
- This is almost **10 times** faster than previous mainstream standards.
- The new standard is designated **IEEE 802.11AX**
- Adopts a new **6GHz** band in addition to previous **2.4GHz** and **5GHz** bands
- Will itself be superseded by the **Wi-Fi 7** or **IEEE 802.11BE** standard which is expected by early 2024 and will feature speeds up to **46Gbps**

Other wireless standards

- Bluetooth
 - 2.4 GHz
 - Originally IEEE 802.15.1 (IEEE no longer maintains the standard)
 - Short range personal area networks (PAN)
 - Connect portable devices
 - Robust, low power, low cost
 - Cannot handle high bandwidth (1-3 mbps)
- Zigbee
 - Used in IOT
 - IEEE 802.15.4 standard
 - Ultra-low power
 - Not free
 - Slow speeds (250 kbps)