Lesson 8: Wireless Networks/WLAN

Van-Linh Nguyen

Fall 2024

國立中正大學
Cybersecurity Lab

Ask me a question without revealing your name

urity Lab

Outline

- Wireless Networks
  1. WiFi
  2. Cellular networks

Shannon formula

- How much bit per second we get from every Hz?

$$C = W * n * Log_2\left(1 + \frac{S}{N}\right)$$

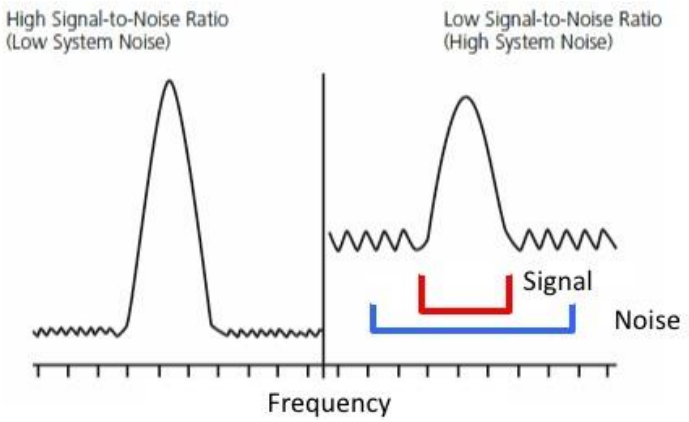
Signal power

Channel Capacity or Data rate (bits/sec)

Channel bandwidth (Hz)

Number of antennas

Signal to noise ratio (SNR) in dB



* Signal power S is decreased by path loss = $\left(\frac{4\pi d c}{f}\right)^2$

Distance

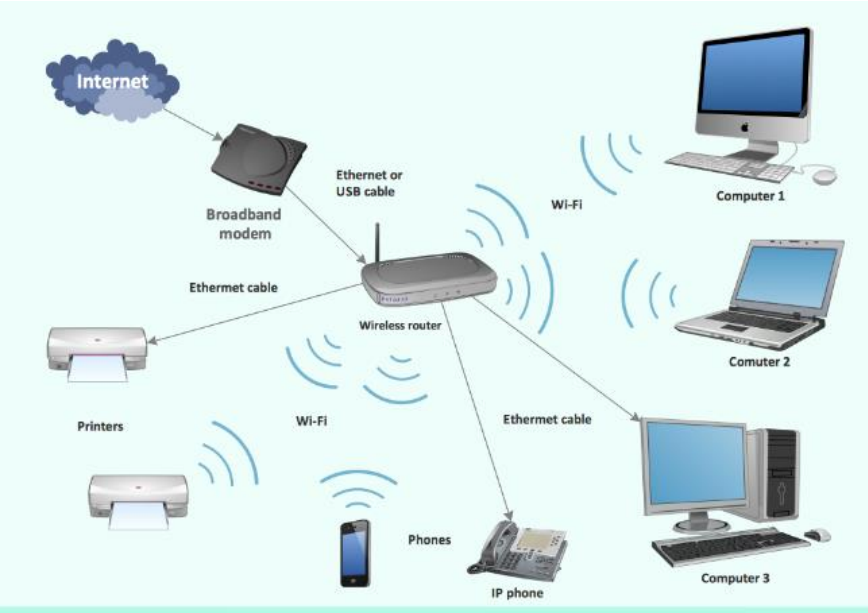
Speed of light

Frequency

Ask a question

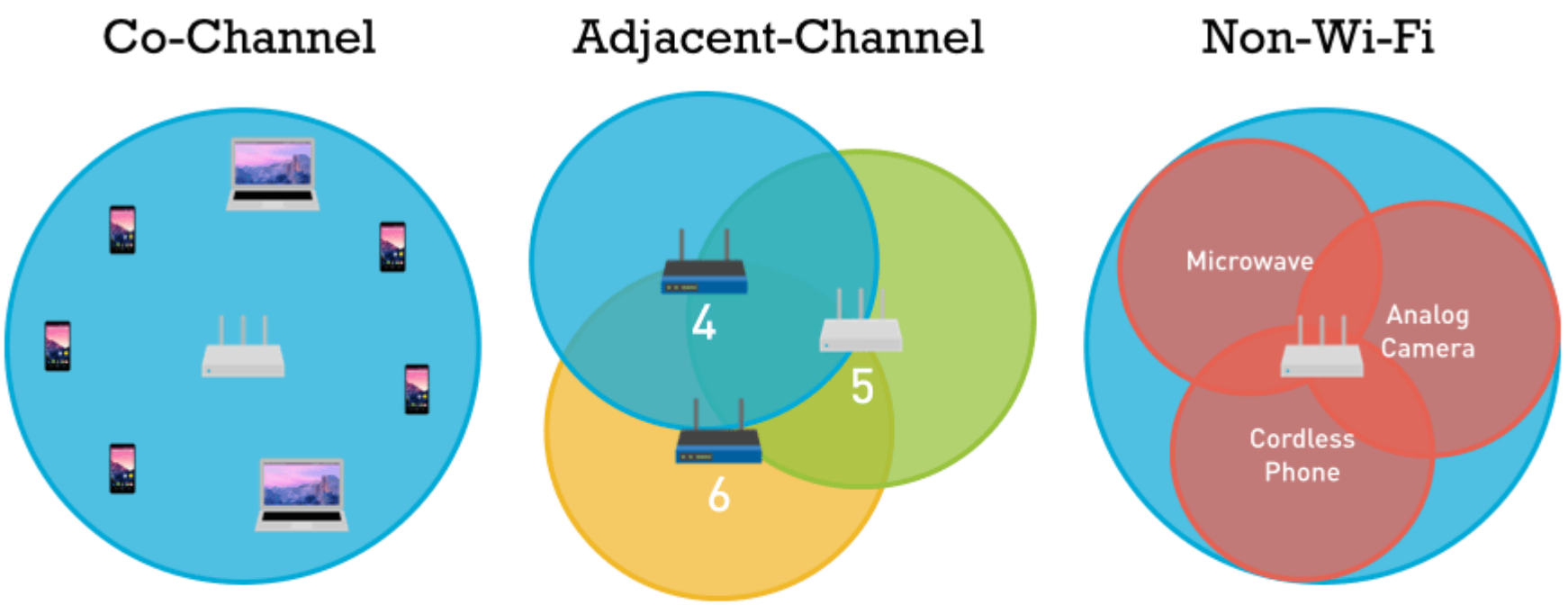
Wireless Links

- Wireless links transmit electromagnetic signals
  - Radio, microwave, infrared
- Wireless links all share the same channel
  - The challenge is to share it efficiently without unduly interfering with each other
  - Most of this sharing is accomplished by dividing the “link” along the dimensions of frequency and space



Ask a question

The shared wireless link



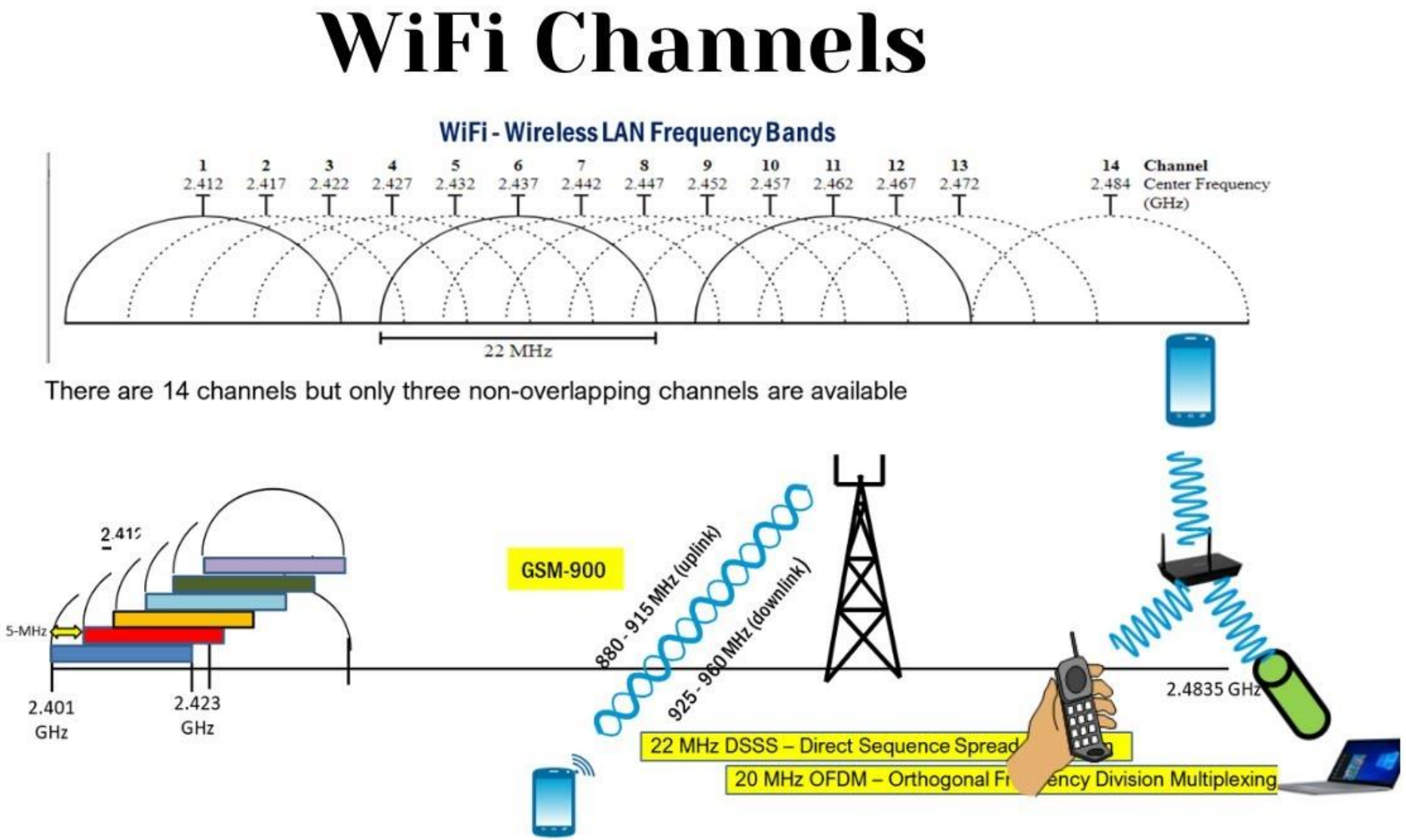
Every client and access point on the same channel competes for time to talk.

Every client and access point on overlapping channels talk over each other.

Non-802.11 devices compete for medium access.

Credit to MetaGeek

Dividing the channel along with frequency and space

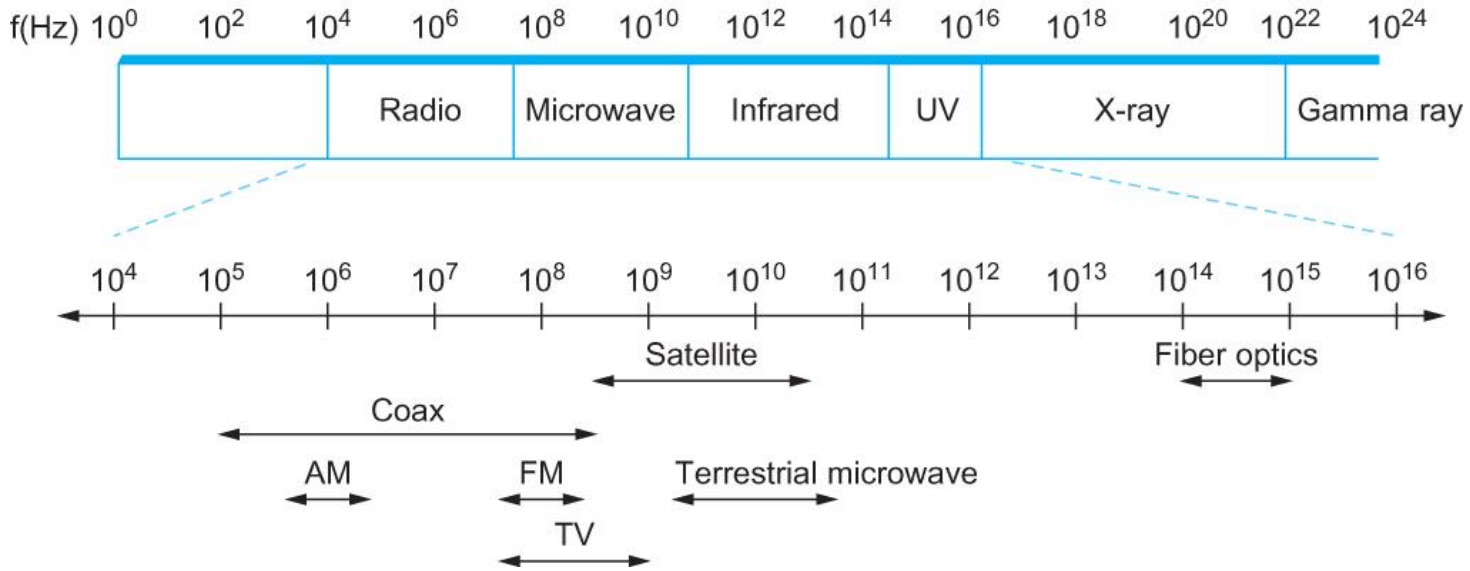


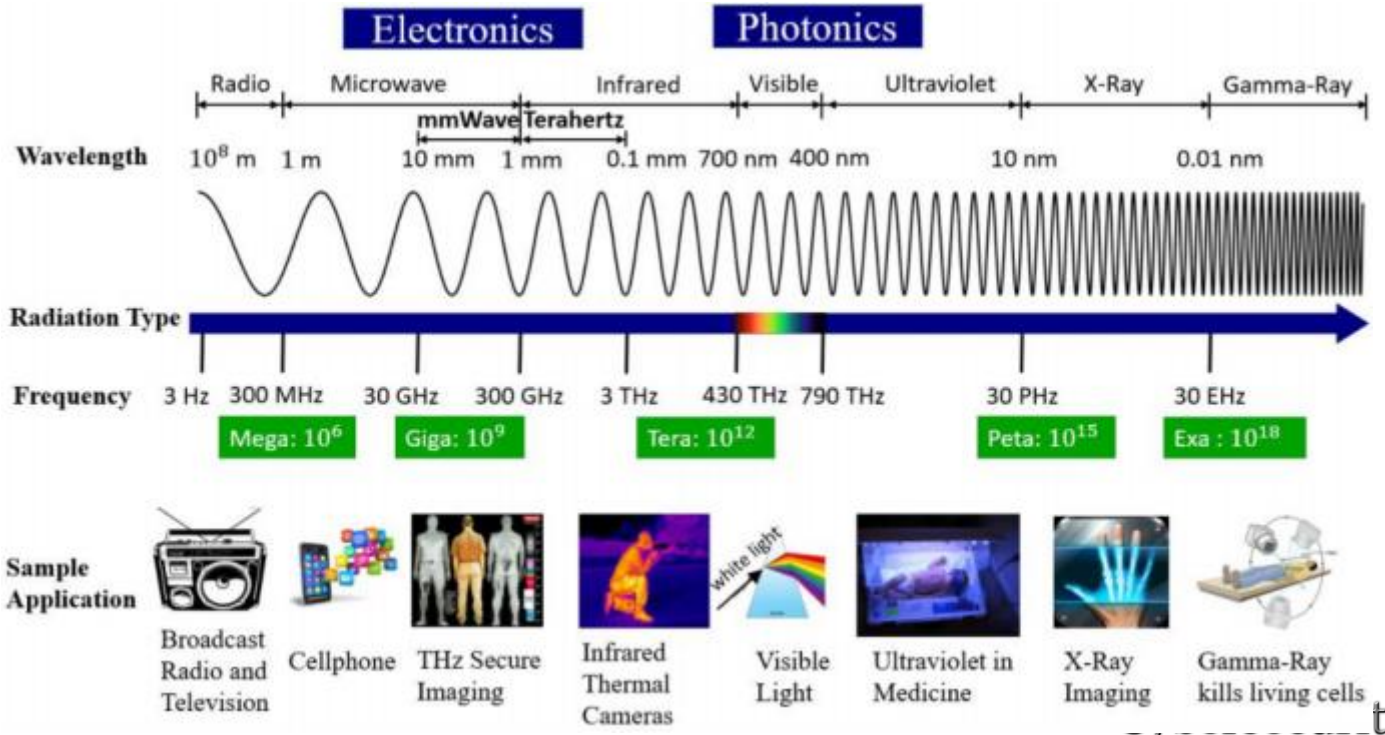
Ask a question

Wireless Links

- These allocations are determined by government agencies such as FCC (Federal Communications Commission) in USA
- Specific bands (frequency) ranges are allocated to certain uses.
  - Some bands are reserved for government use
  - Other bands are reserved for uses such as AM radio, FM radio, televisions, satellite communications, and cell phones
  - Specific frequencies within these bands are then allocated to individual organizations for use within certain geographical areas.
  - Finally, there are several frequency bands set aside for “license exempt” usage
    - Bands in which a license is not needed

Wireless frequency band

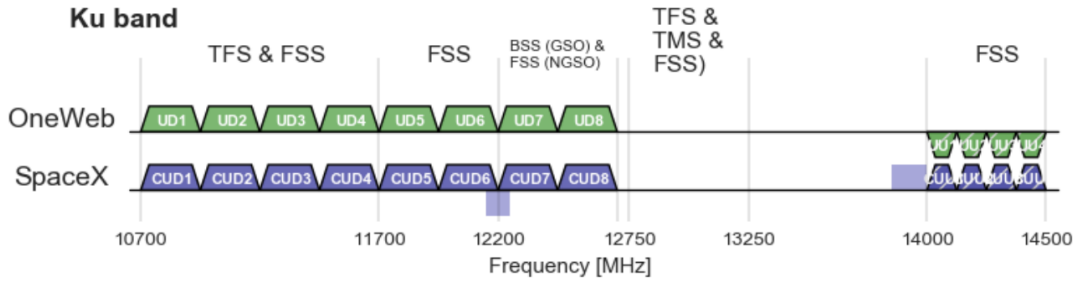


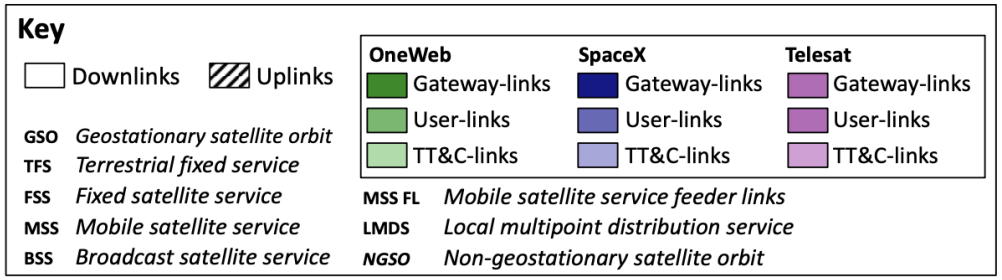


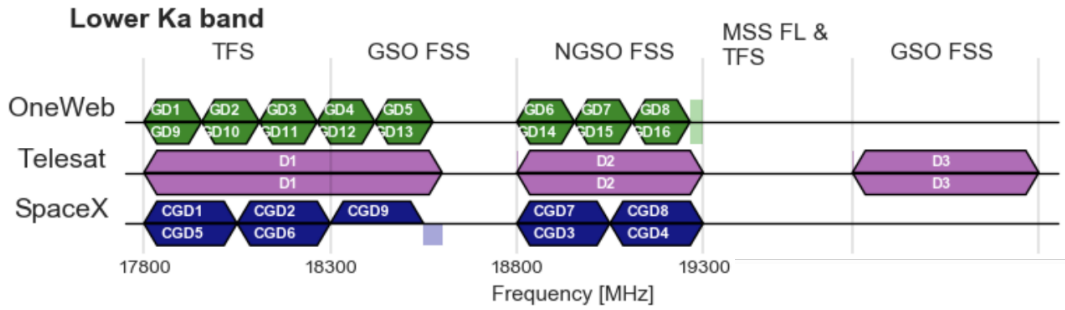
ty Lab

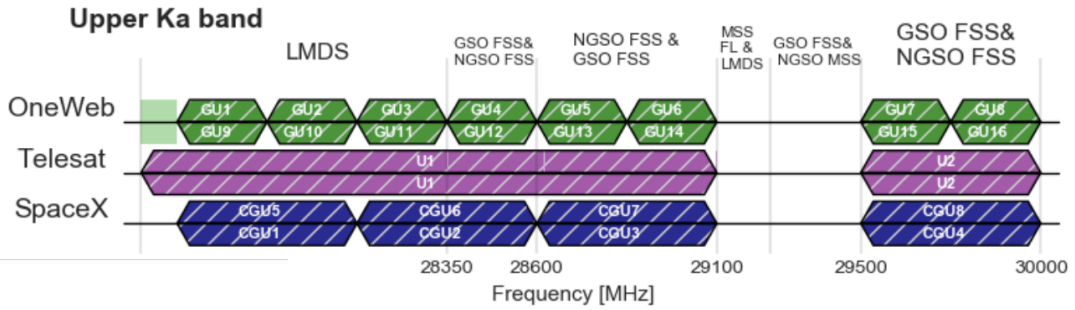
Ask a question

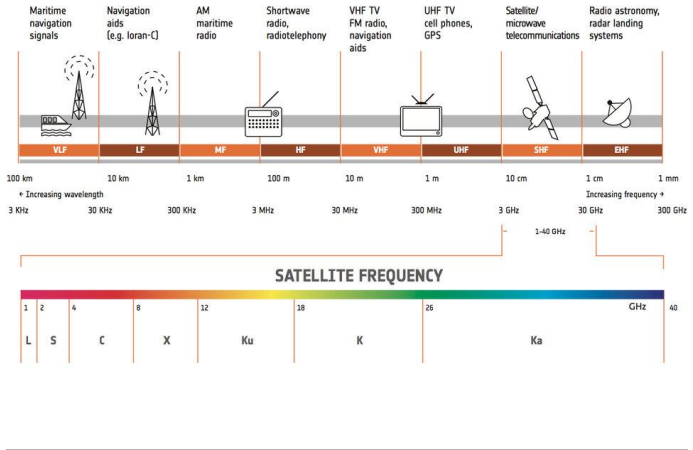
Satellite frequency band









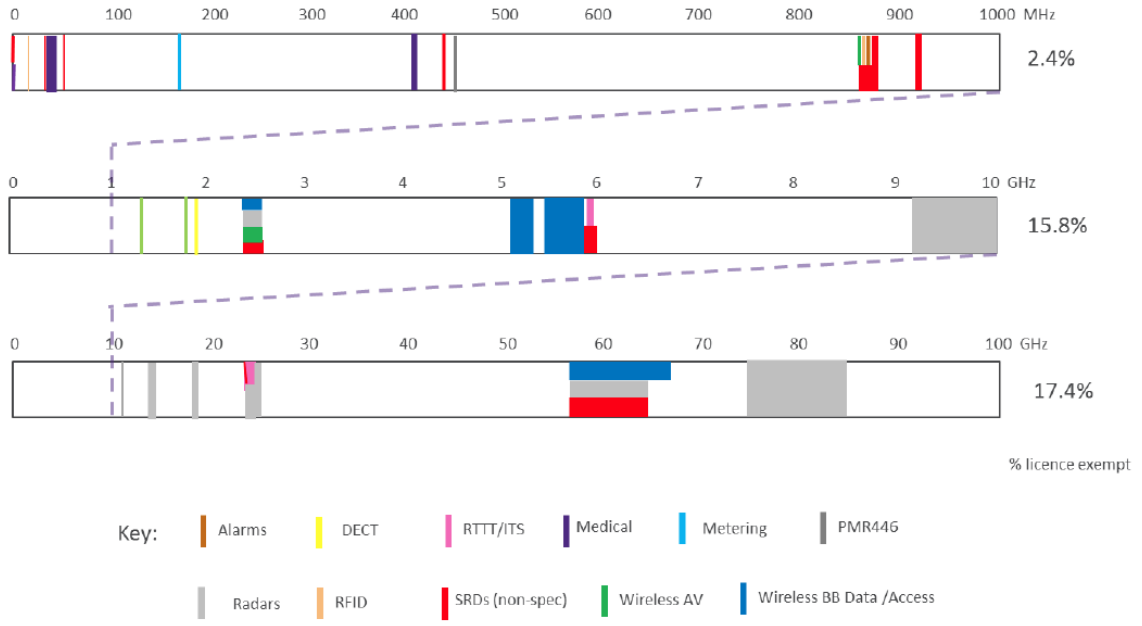


國立中正大學
Cybersecurity Lab

Wireless Links

- Devices that use license-exempt frequencies are still subject to certain restrictions
  - The first is a limit on transmission power
  - This limits the range of signal, making it less likely to interfere with another signal
    - For example, a cordless phone might have a range of about 100 feet.

Figure 3-2: Principal European Licence Exempt Frequency Bands



Via: The 3G4G Blog - blog.3g4g.co.uk

Why AT&T needs to delay 5G near the airport

CNET

FAA Reportedly Wants Smaller Telecoms to Stop Using 5G Around Airports, Too

To keep easing the US aviation industry into the 5G era, Verizon and AT&T earlier this year agreed to keep some 5G signal frequencies turned...

Oct 25, 2022

Fierce Wireless

C-band upgrades may cost airline industry $637M: IATA

The FAA previously pegged the costs at $26 million, but the International Air Transport Association said it's more likely to cost $637.6...

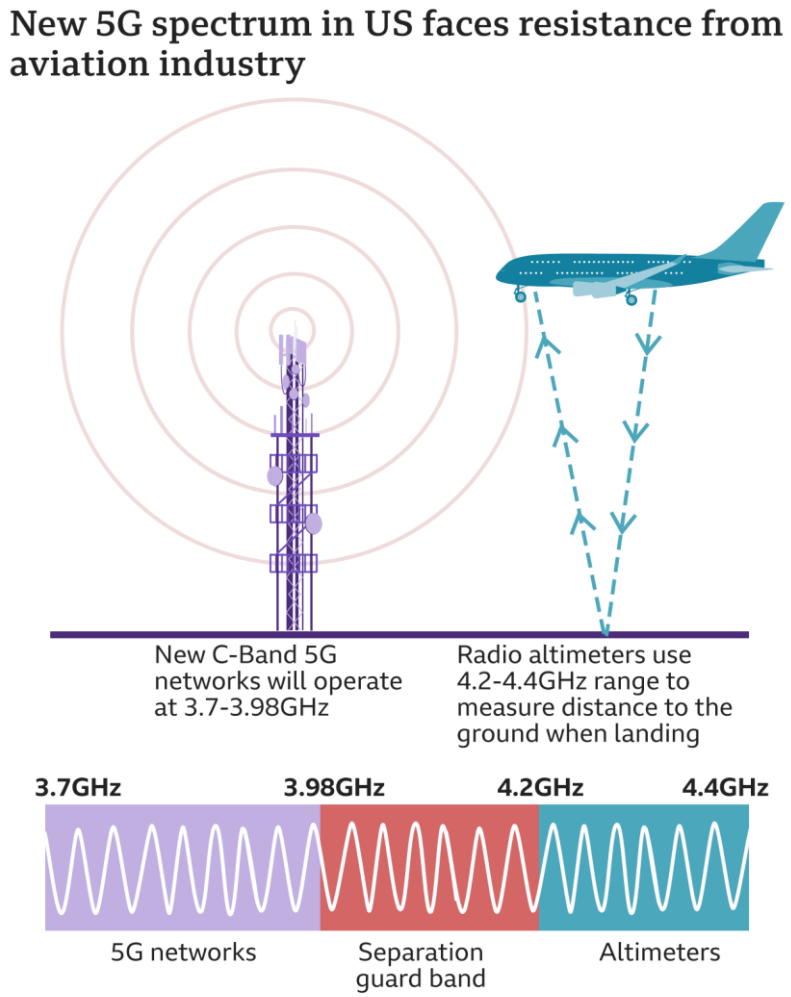
Feb 10, 2023

NPR

Verizon and AT&T agree to delay 5G rollout near airports

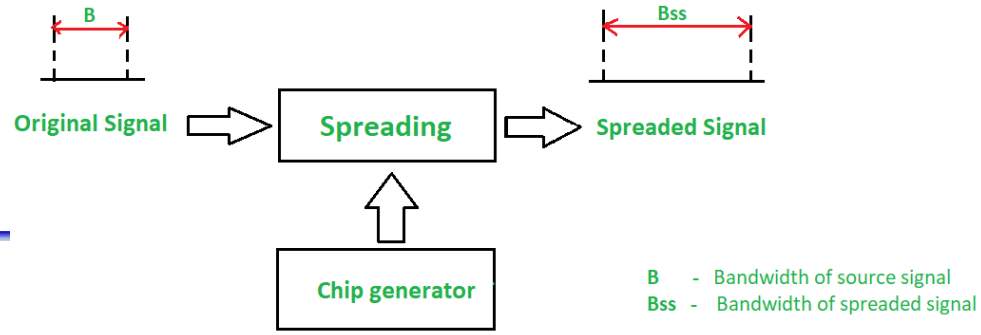
Wireless carriers Verizon and AT&T say they will go ahead with plans to switch on high speed 5G service nationwide Wednesday, except near...

Jan 18, 2022

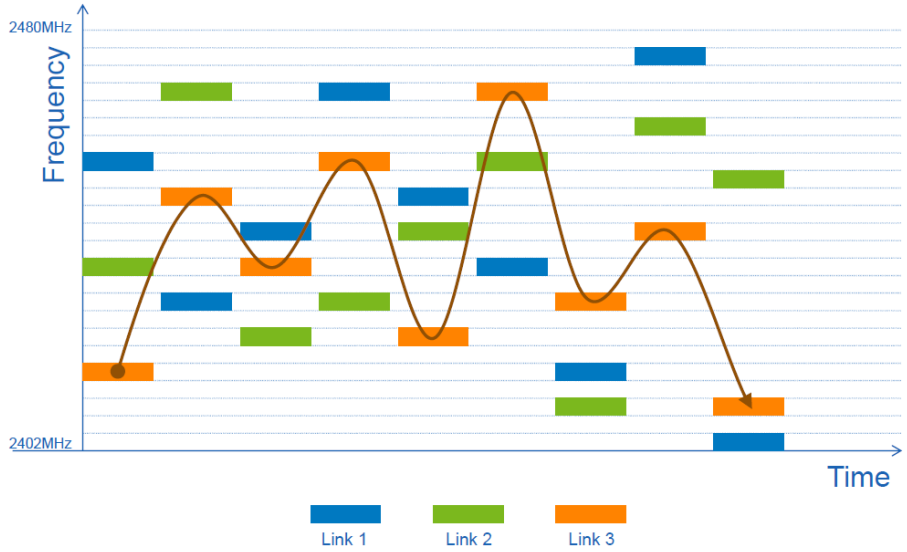


Since it can interfere the signal of safety services, e.g., height estimation when landing!

Wireless Links



- The second restriction requires the use of **Spread Spectrum** technique
  - Idea is to spread the signal over a wider frequency band
    - So as to minimize the impact of interference from other devices
    - Originally designed for military use
  - ***Frequency hopping***
    - Transmitting signal over a random sequence of frequencies
      - First transmitting at one frequency, then a second, then a third…
      - The sequence of frequencies is not truly random, instead computed algorithmically by a pseudorandom number generator
      - The receiver uses the same algorithm as the sender, initializes it with the same seed, and is
        - Able to hop frequencies in sync with the transmitter to correctly receive the frame

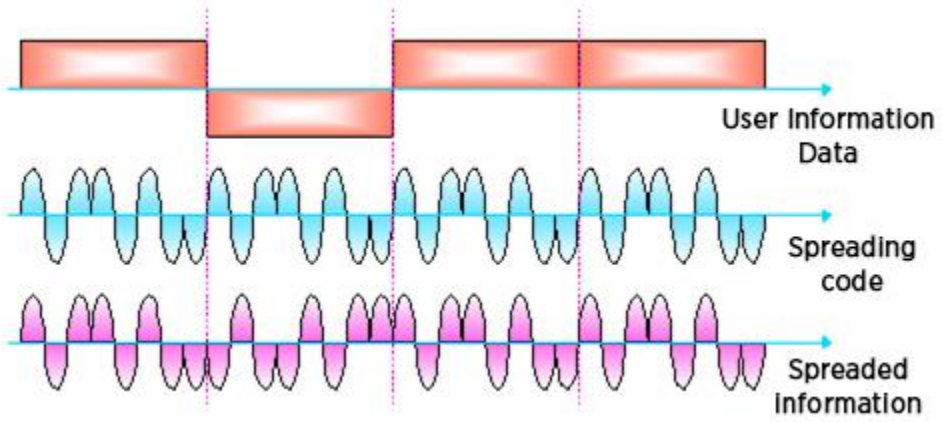


Frequency hopping

Ask a question

Wireless Links

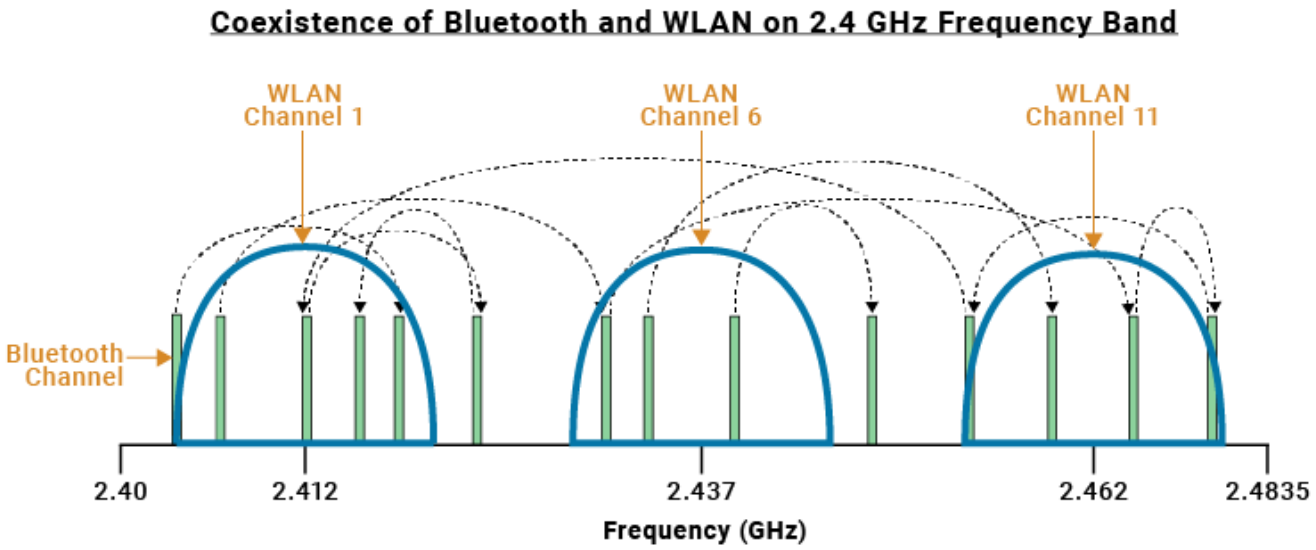
- A second spread spectrum technique called ***Direct sequence***
  - Represents each bit in the frame by multiple bits in the transmitted signal.
  - For each bit the sender wants to transmit
    - It actually sends the exclusive OR of that bit and *n* random bits
  - The sequence of random bits is generated by a pseudorandom number generator known to both the sender and the receiver.
  - The transmitted values, known as an ***n*-bit chipping code**, spread the signal across a frequency band that is *n* times wider

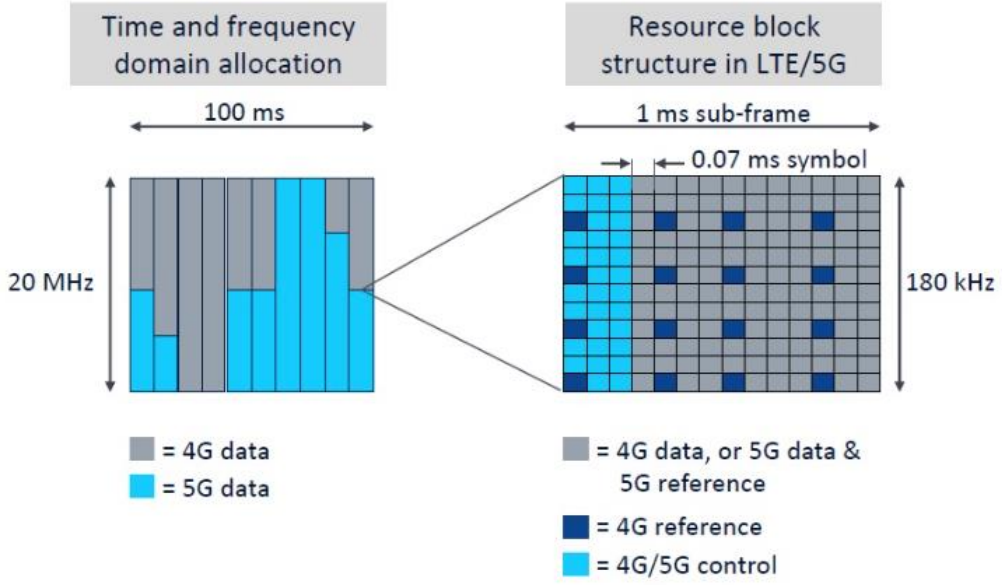


Ask a question

Coexistence frequency band

- Exploit the coexistence of many frequency bands to serve multiple devices (legacy + new generation)





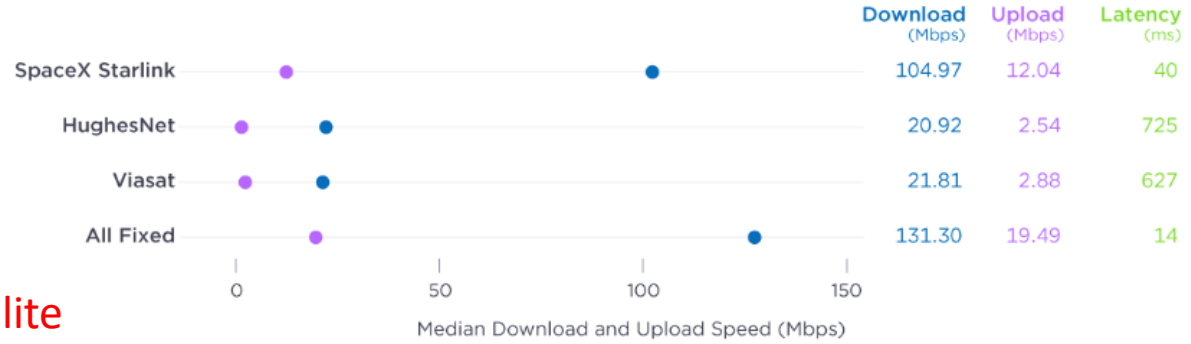
Wireless Links

- Wireless technologies differ in a variety of dimensions
  - How much bandwidth they provide
  - How far apart the communication nodes can be
- Prominent wireless technologies
  - Satellite networks
  - 4G/5G cellular wireless
  - Bluetooth
  - Wi-Fi (more formally known as 802.11)
  - WiMAX (802.16)

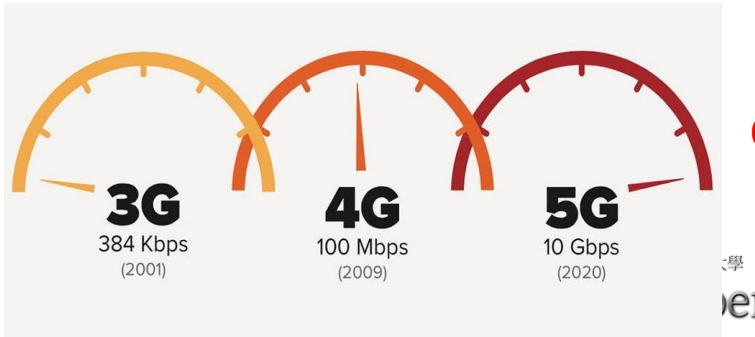
	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

Generation / IEEE Standard	Max Linkrate	Adopted	Frequency	Channel Bandwidth
Wi-Fi 6 (802.11ax)	600–9608 Mbit/s	2019	2.4/5 GHz 1 – 6 GHz	20/40/**80/160** MHz
Wi-Fi 5 (802.11ac)	433-6933 Mbit/s	2014	5 GHz	20/40/**80/160** MHz
Wi-Fi 4 (802.11n)	72-600 Mbit/s	2009	2.4/5 GHz	20/40 MHz
Wi-Fi 3 (802.11g)	3-54 Mbit/s	2003	2.4 GHz	20 MHz
Wi-Fi 2 (802.11a)	1.5-54 Mbit/s	1999	5 GHz	20 MHz
Wi-Fi 1 (802.11b)	1-11 Mbit/s	1999	2.4 GHz	20 MHz
(Wi-Fi 1, Wi-Fi 2, and Wi-Fi are unbranded)				

WiFi



Satellite



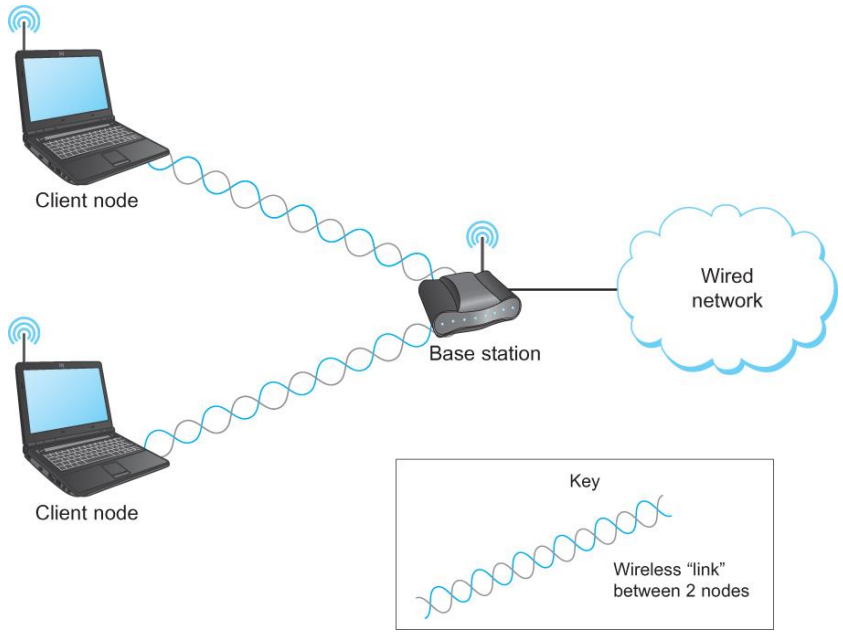
Cellular networks

ersecurity Lab

Ask a question

Wireless Links

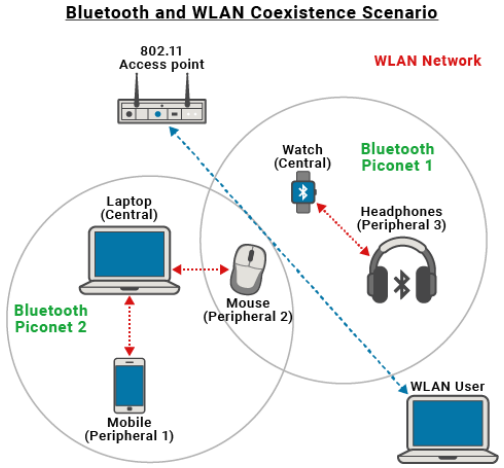
- Mostly widely used wireless links today are usually asymmetric
  - Two end-points are usually different kinds of nodes
    - One end-point usually has no mobility, but has wired connection to the Internet (known as base station)
    - The node at the other end of the link is often mobile

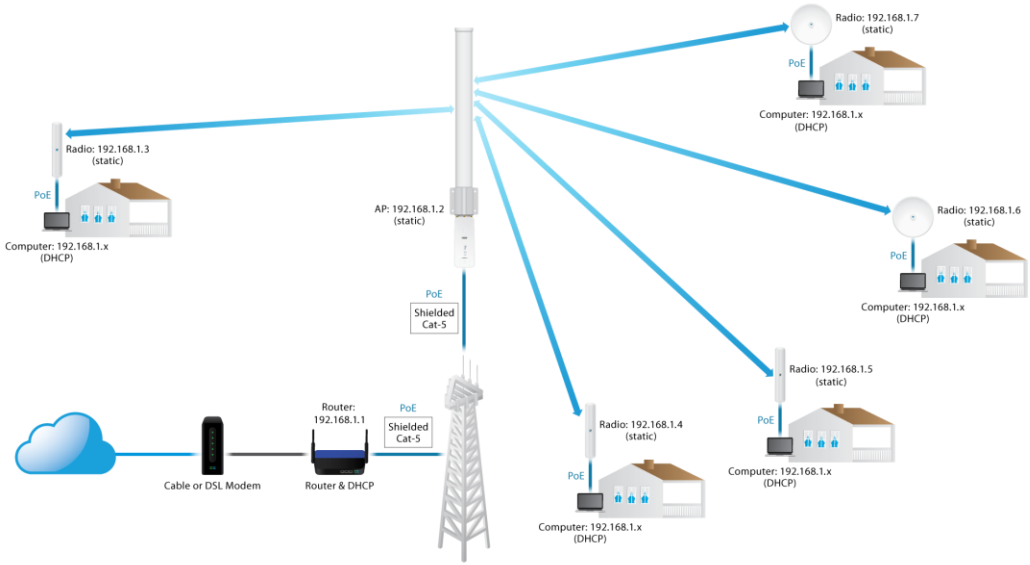


A wireless network using a base station

Wireless Links

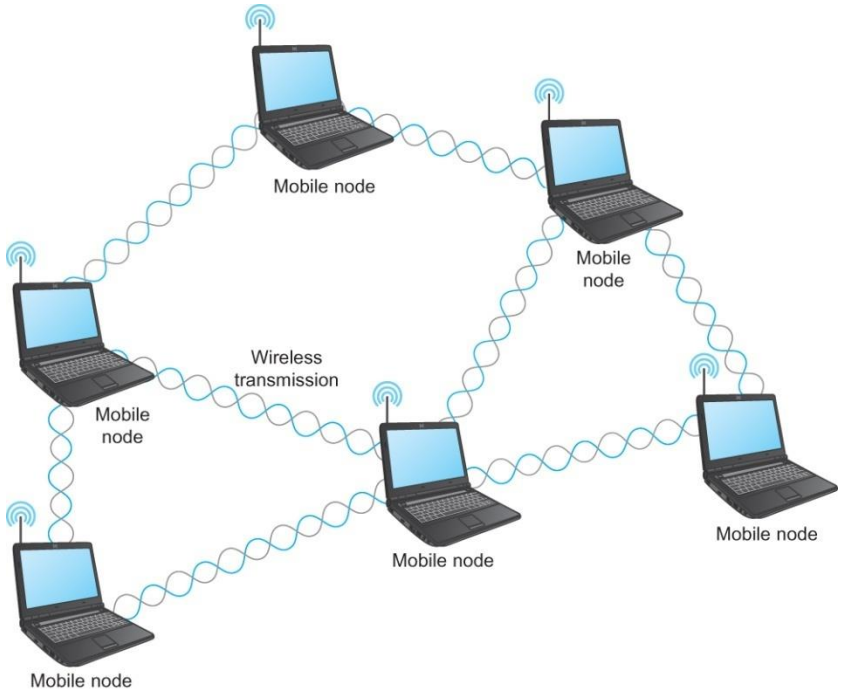
- Wireless communication supports point-to-multipoint communication
- Communication between non-base (client) nodes is routed via the base station
- Three levels of mobility for clients
  - **No mobility**: the receiver must be in a fixed location to receive a directional transmission from the base station (initial version of WiMAX)
  - Mobility is within the range of a base (Bluetooth)
  - **Mobility** between bases (Cell phones/Wi-Fi, satellites)



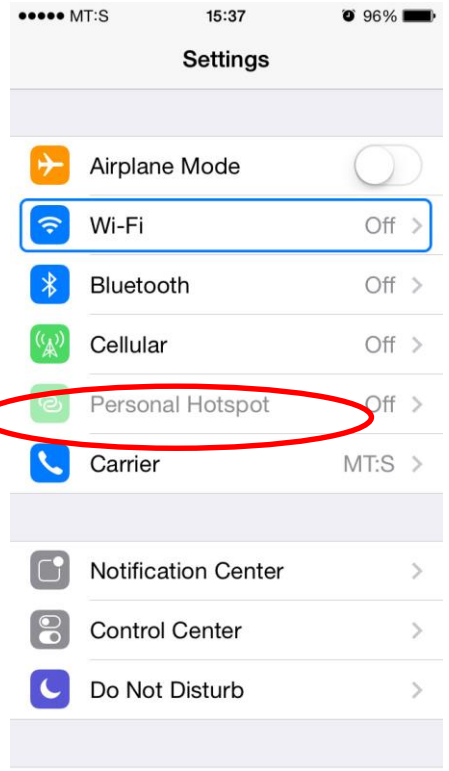


Wireless Links

- Mesh or Ad-hoc network
  - Nodes are peers
  - Messages may be forwarded via a chain of peer nodes



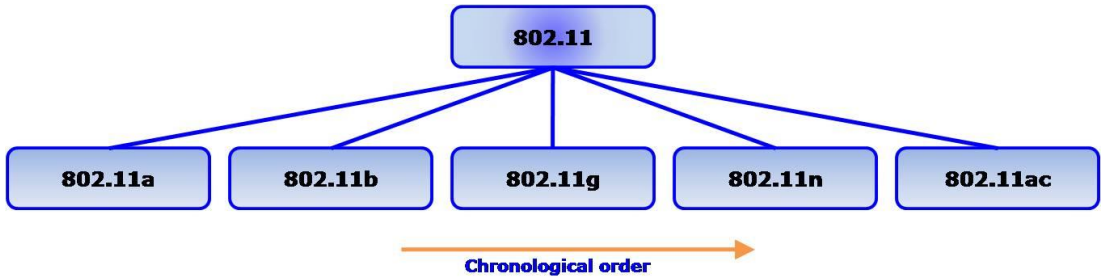
A wireless ad-hoc or mesh network



Ask a question

IEEE 802.11

- Also known as Wi-Fi
- Like its Ethernet and token ring siblings, 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses)
  - Primary challenge is to mediate access to a shared communication medium – in this case, signals propagating through space
- 802.11 supports additional features
  - power management and
  - security mechanisms

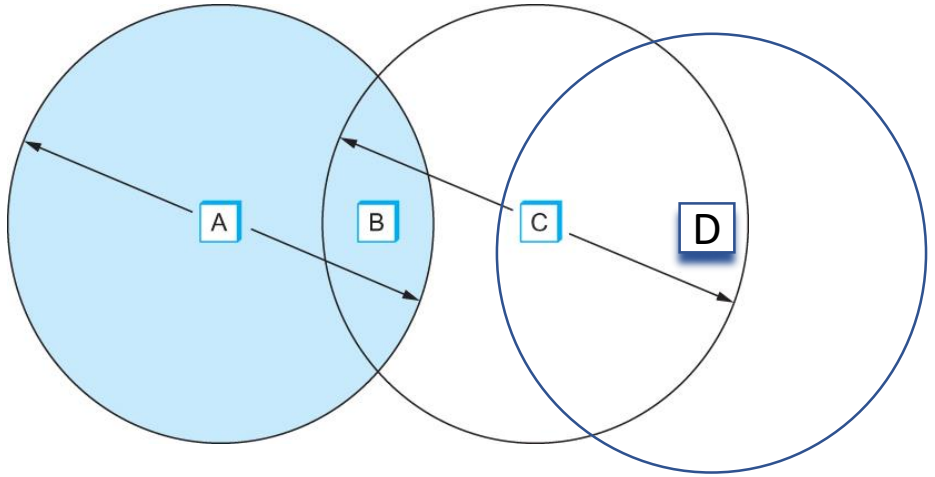


Wi-Fi Gen	IEEE Standard	Release Date	2.4 GHz	5 GHz	Max Data Rate
Wi-Fi	802.11	1997	Yes	No	2 Mbps
Wi-Fi 1	802.11b	1999	Yes	No	11 Mbps
Wi-Fi 2	802.11a	1999	No	Yes	54 Mbps
Wi-Fi 3	802.11g	2003	Yes	No	54 Mbps
Wi-Fi 4	802.11n	2009	Yes	Yes	600 Mbps
Wi-Fi 5	802.11ac	2013	No	Yes	6.93 Gbps
Wi-Fi 6	802.11ax	2019	Yes	Yes	14 Gbps

Ask a question

IEEE 802.11 – Collision Avoidance

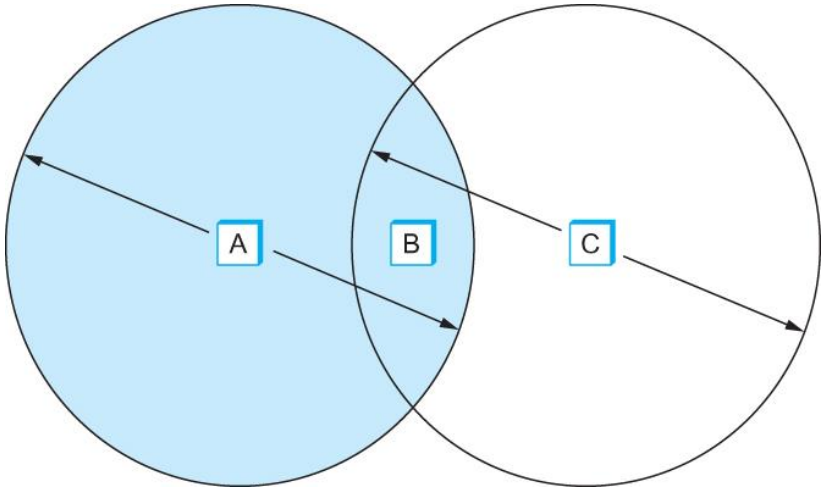
- Consider the situation in the following figure where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
  - For example, B can exchange frames with A and C, but it cannot reach D
  - C can reach B and D but not A



Example of a wireless network

IEEE 802.11 – Collision Avoidance

- Suppose both A and C want to communicate with B and so they each send it a frame.
  - A and C are unaware of each other since their signals do not carry that far
  - These two frames collide with each other at B
    - But unlike an Ethernet, neither A nor C is aware of this collision
  - A and C are said to *hidden nodes* with respect to each other

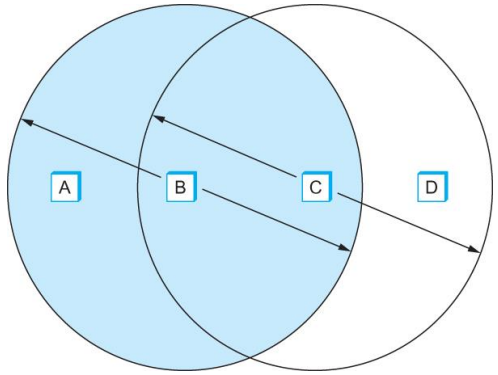


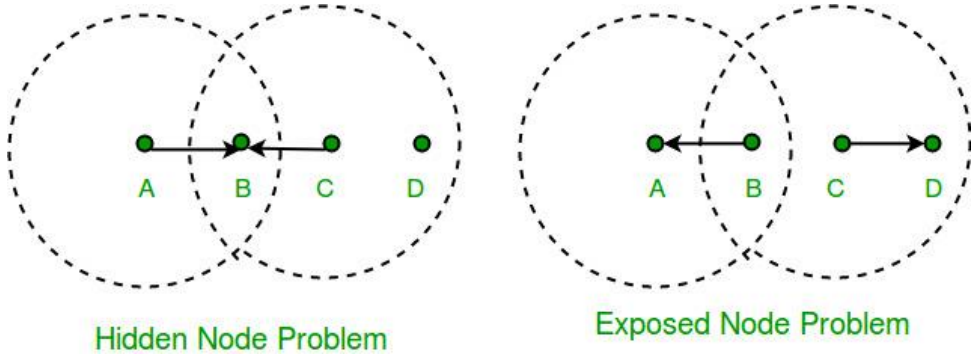
A and C are unaware that
They are using the same channel
at the same time

The “Hidden Node” Problem. Although A and C are hidden from each other, their signals can collide at B. (B’s reach is not shown.)

IEEE 802.11 – Collision Avoidance

- Another problem called *exposed node* problem occurs
  - Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
  - It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
  - Suppose C wants to transmit to node D.
  - This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.





Hidden Node Problem

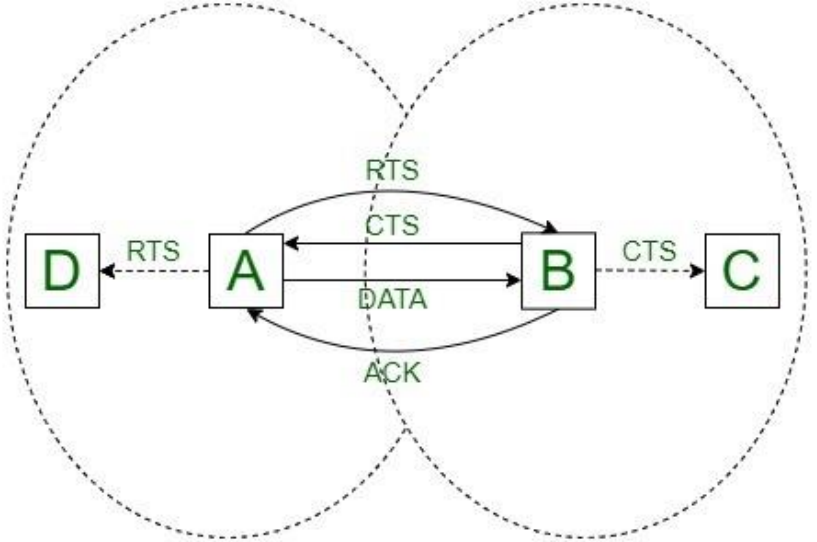
Exposed Node Problem

Comparison

Exposed Node Problem. Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A and D's reaches are not shown.)

IEEE 802.11 – Collision Avoidance

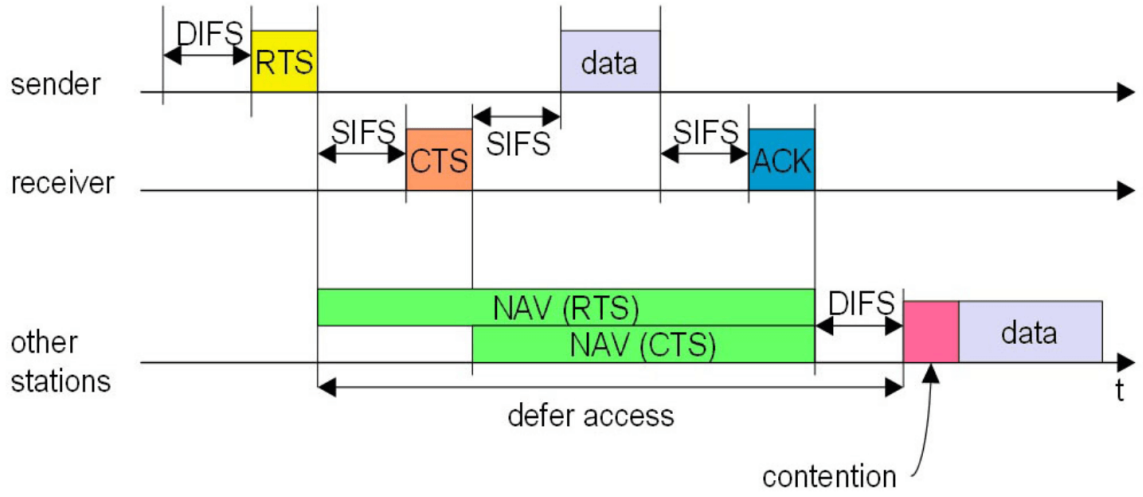
- 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).
- Key Idea
  - Sender and receiver exchange control frames with each other before the sender actually transmits any data.
  - This exchange informs all nearby nodes that a transmission is about to begin
  - Sender transmits a *Request to Send* (RTS) frame to the receiver.
    - The RTS frame includes a field that indicates how long the sender wants to hold the medium
      - Length of the data frame to be transmitted
  - Receiver replies with a *Clear to Send* (CTS) frame
    - This frame echoes this length field back to the sender



Ask a question

IEEE 802.11 – Collision Avoidance

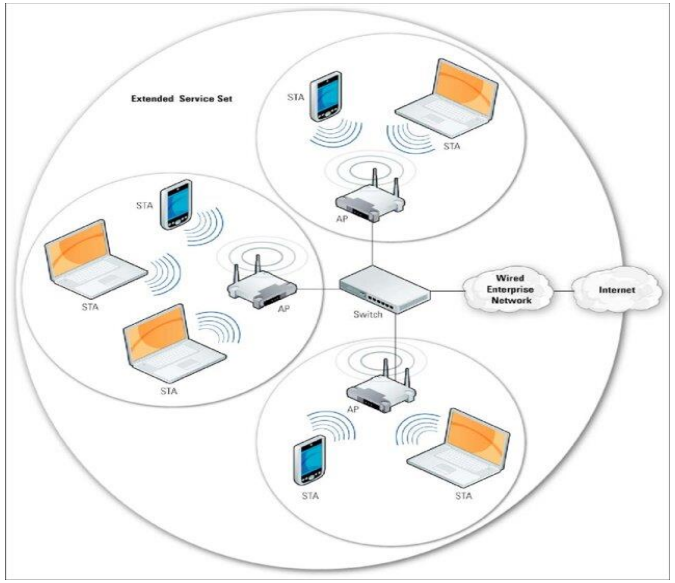
- Any node that sees the CTS frame knows that
  - it is close to the receiver, therefore
  - cannot transmit for the period of time it takes to send a frame of the specified length
- Any node that sees the RTS frame but not the CTS frame
  - is not close enough to the receiver to interfere with it, and
  - so is free to transmit



IEEE 802.11 – Distribution System

- 802.11 is suitable for an ad-hoc configuration of nodes that may or may not be able to communicate with all other nodes.
- Nodes are free to move around
- The set of directly reachable nodes may change over time
- To deal with this mobility and partial connectivity,
  - 802.11 defines additional structures on a set of nodes
  - Instead of all nodes being created equal,
    - some nodes are allowed to roam
    - some are connected to a wired network infrastructure

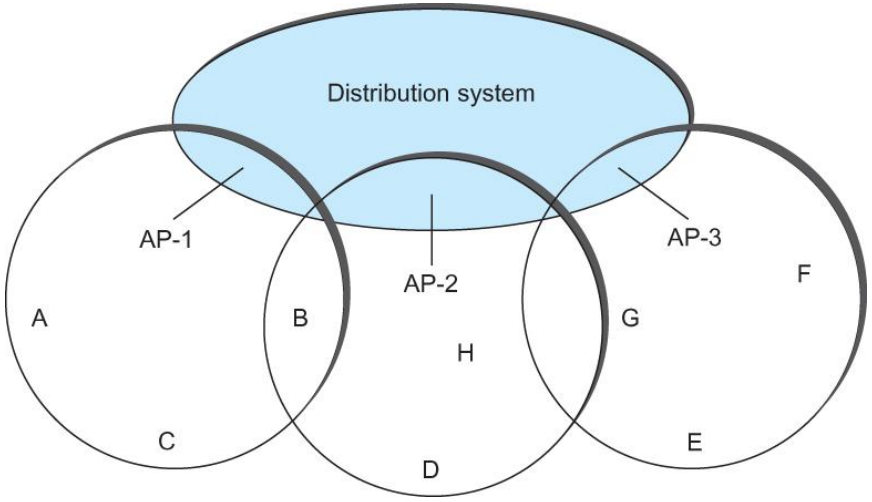
      - they are called *Access Points* (AP) and they are connected to each other by a so-called *distribution system*

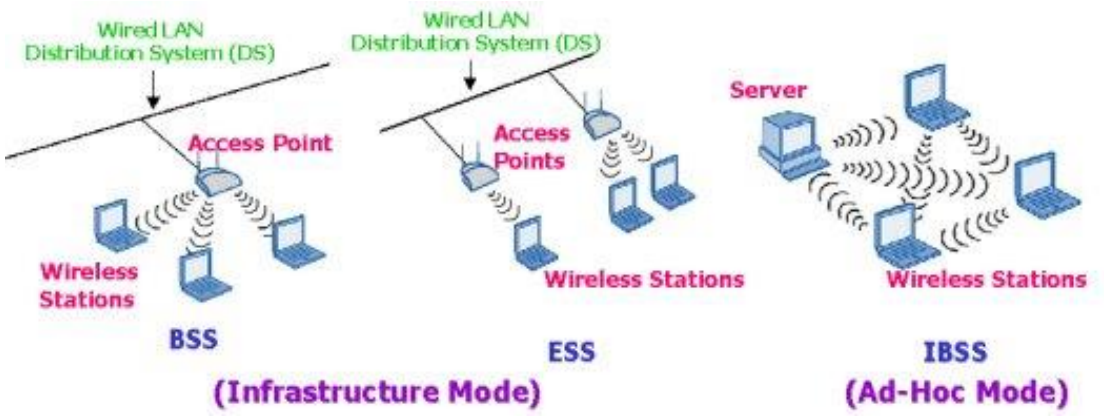


Ask a question

IEEE 802.11 – Distribution System

- Following figure illustrates a distribution system that connects three access points, each of which services the nodes in the same region
- Each of these regions is analogous to a cell in a cellular phone system with the APIs playing the same role as a base station
- The distribution network runs at layer 2 of the ISO architecture



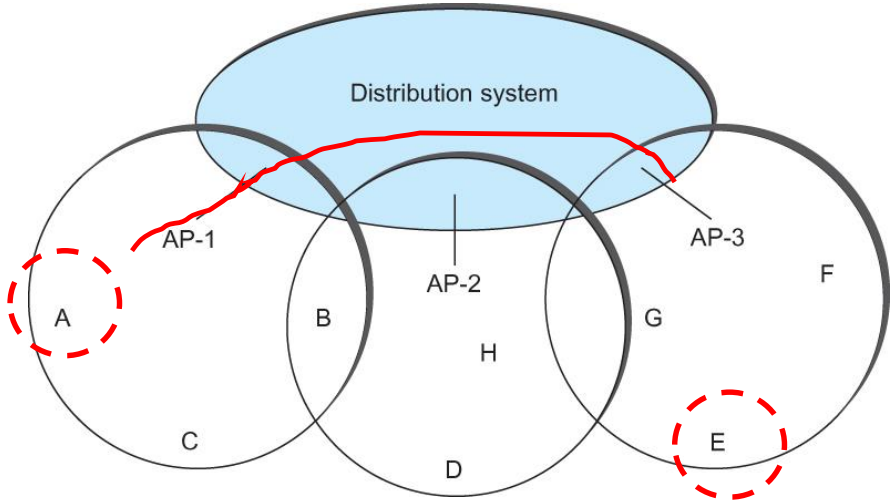


Access points connected to a distribution network

Ask a question

IEEE 802.11 – Distribution System

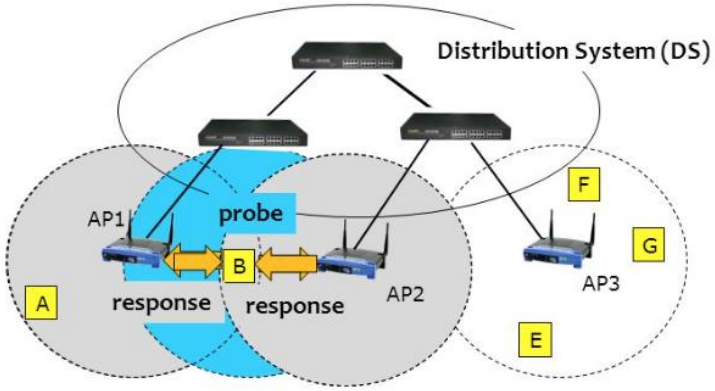
- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is
  - Each nodes associates itself with one access point
  - For node A to communicate with node E, A first sends a frame to its AP-1 which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E



Access points connected to a distribution network

IEEE 802.11 – Distribution System

- How do the nodes select their access points?
- How does it work when nodes move from one cell to another?



Scanning to select an associated AP
(Probe + Response)

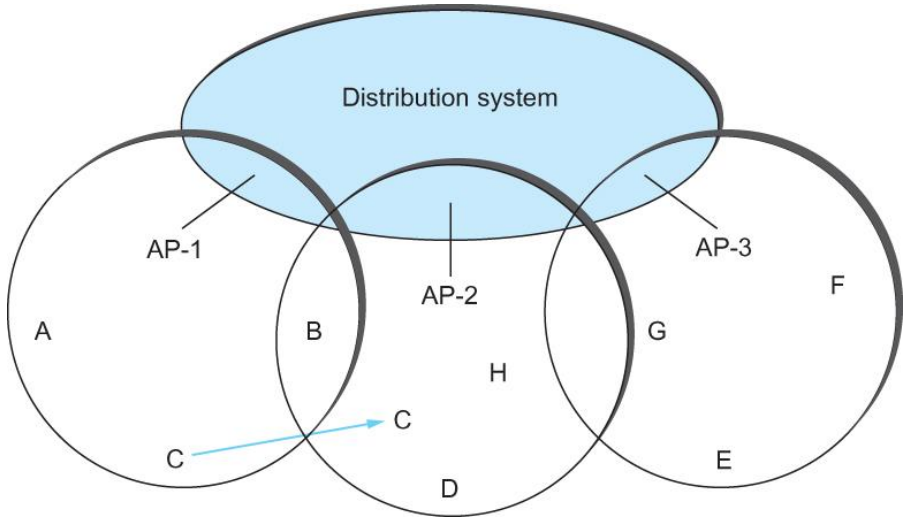
- The technique for selecting an AP is called *scanning*
  - Node A sends a *Probe* frame
  - All APs within reach reply with a *Probe Response* frame
  - Node A selects one of the access points and sends that AP an *Association Request* frame
  - AP1 replies with an *Association Response* frame

- A node engages this protocol whenever
  - it joins the network, as well as
  - when it becomes unhappy with its current AP
    - This might happen, for example, because the signal from its current AP has weakened due to the node moving away from it
    - Whenever a node acquires a new AP, the new AP notifies the old AP of the change via the distribution system

Ask a question

IEEE 802.11 – Distribution System

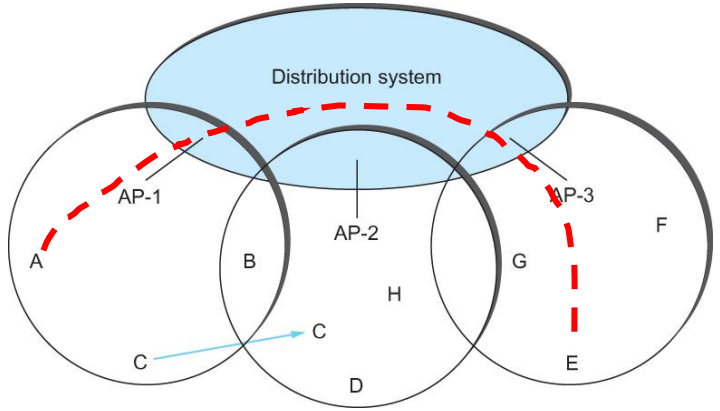
- APs also periodically send a *Beacon* frame that advertises the capabilities of the access point; these include the transmission rate supported by the AP
  - This is called *passive scanning*
  - A node can change to this AP based on the *Beacon* frame simply by sending it an *Association Request* frame back to the access point.



Node Mobility

IEEE 802.11 – Frame Format

- Source and Destinations addresses (MAC address): each 48 bits
- Data: up to 2312 bytes
- CRC: 32 bit
- Control field: 16 bits
  - Contains three subfields (of interest)
    - 6 bit **Type** field: indicates whether the frame is an RTS or CTS frame or being used by the scanning algorithm
    - A pair of 1 bit fields : called **ToDS** and **FromDS**



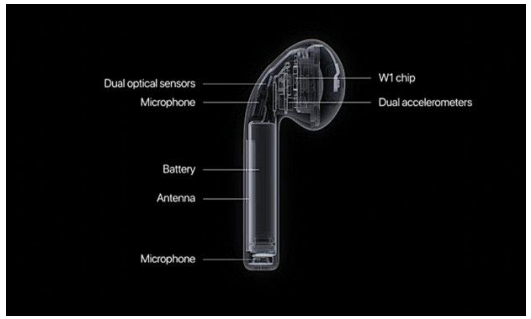
Addr1: E, Addr2: AP-3, Addr3: AP-1, Addr4: A

Frame Format

Addr1: identifies the ultimate destination,
Addr2: identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)
Addr3: identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded across the distribution system)
Addr4: identifies the original source

Bluetooth®

- Used for very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices
- Operates in the license-exempt band at 2.45 GHz
- Has a range of only 10 m
- Communication devices typically belong to one individual or group
  - Sometimes categorized as Personal Area Network (PAN)
- Power consumption is low



Bluetooth Version	Maximum transmission rate
Bluetooth 1.0a and 1.0b	732.2 kbps
Bluetooth 1.1	732.2 kbps
Bluetooth 1.2	1 Mbps
Bluetooth 2.0 and 2.1	2.1 Mbps
Bluetooth 3.0	24 Mbps
Bluetooth 4.0	24 Mbps
Bluetooth 4.1 and 4.2	25 Mbps
Bluetooth 5.0, 5.1, and 5.2	50 Mbps

Apple Airpods use Bluetooth 5

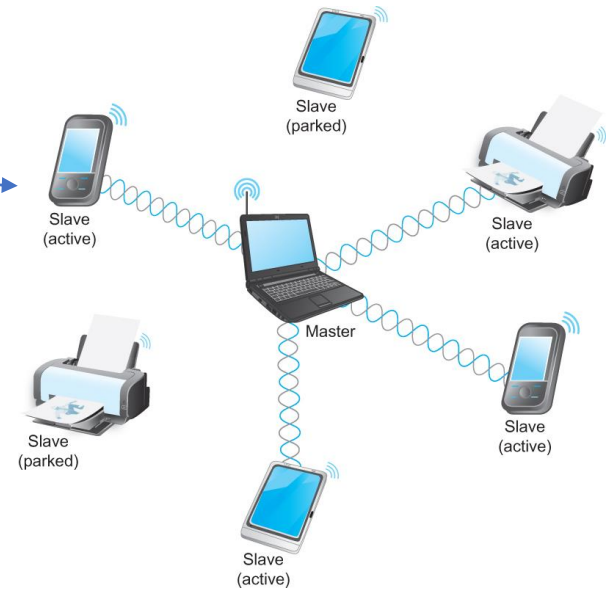
Earbuds

Airpods

Ask a question

Bluetooth

- Bluetooth is specified by an industry consortium called the Bluetooth Special Interest Group
- It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls *profiles*, for a range of applications
  - There is a profile for synchronizing a PDA with personal computer
  - Another profile gives a mobile computer access to a wired LAN
- The basic Bluetooth network configuration is called a *piconet*
  - Consists of a master device and up to seven slave devices
  - Any communication is between the master and a slave
  - The slaves do not communicate directly with each other
  - A slave can be *parked*: set to an inactive, low-power state

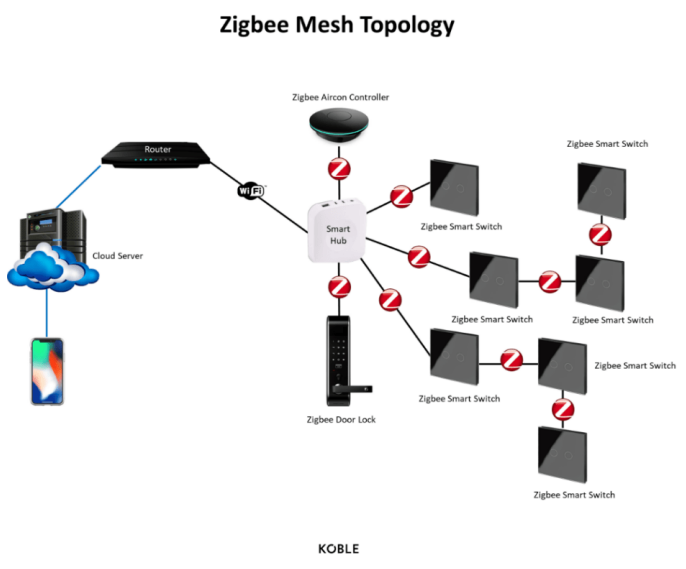


A Bluetooth Piconet

Ask a question

ZigBee

- ZigBee is a new technology that competes with Bluetooth
- Devised by the ZigBee alliance and standardized as IEEE 802.15.4
- It is designed for situations where the bandwidth requirements are low and power consumption must be very low to give very long battery life
- It is also intended to be simpler and cheaper than Bluetooth, making it financially feasible to incorporate in cheaper devices such as a wall switch that wirelessly communicates with a ceiling-mounted fan



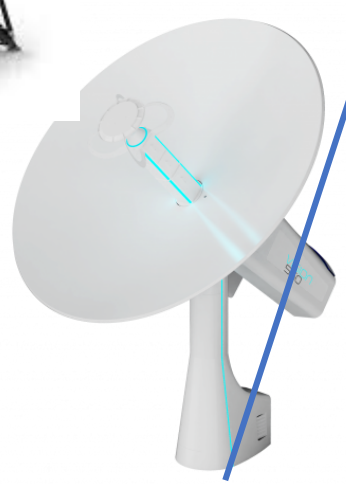
Ask a question

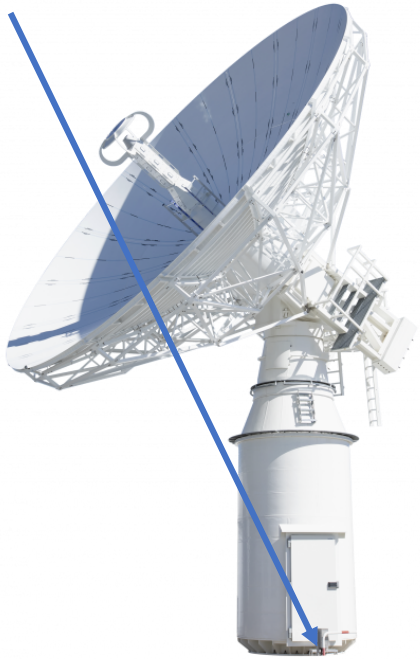
Other wireless technologies

- LoRA
- NB-IoT
- Z-Wave
- LTE/4G
- 5G
- Satellite

Satellite

Satellite

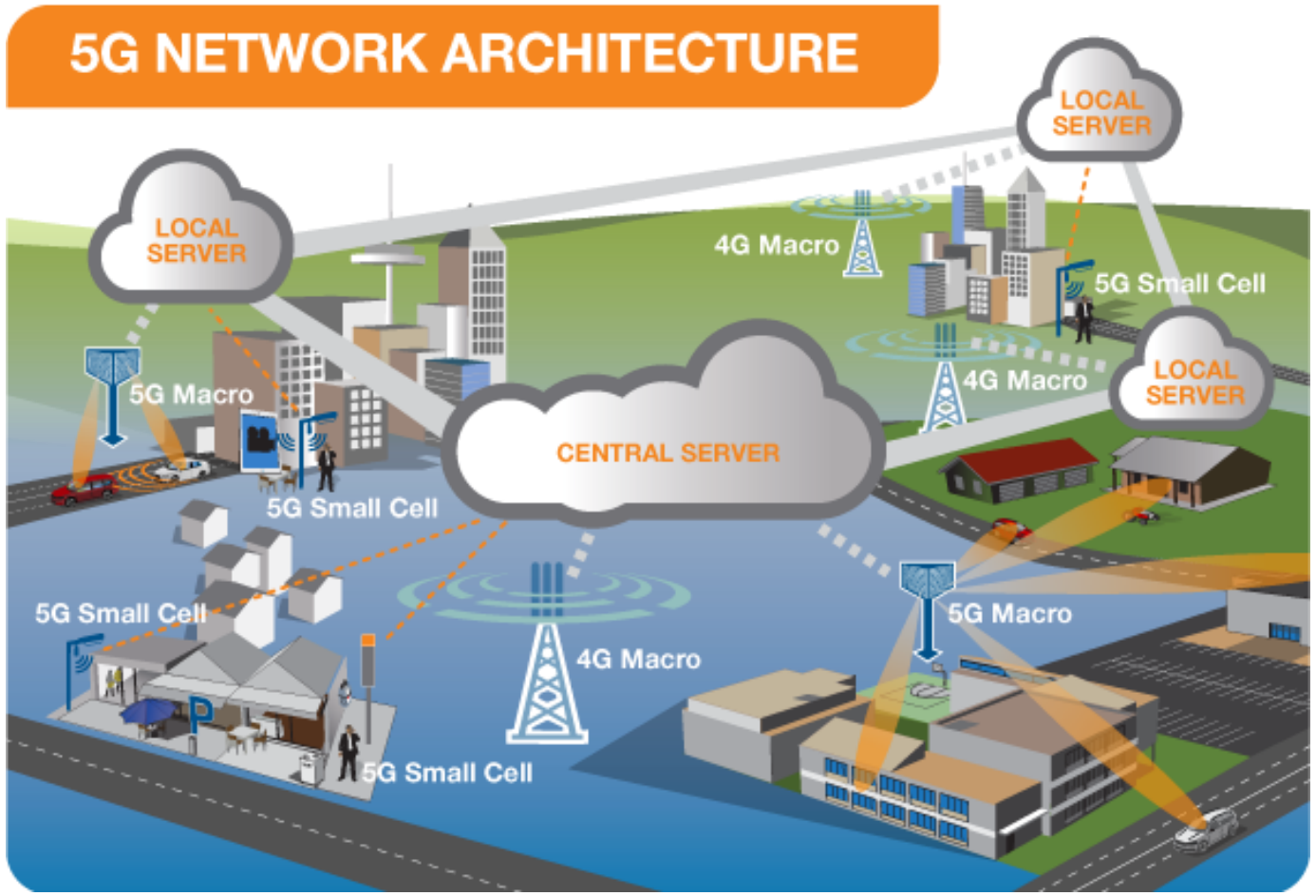




Satellite terminal

Ground station

4G/5G networks



Credit to EMF Explained

Mid-term exam (120 minutes)

- Week1- Week 8 (lecture slides): 9 questions
- Homework + outside: 1 question
- Electric devices or books/slides are not allowed
- You can bring 1-2 empty/blank A4 to write the answer.
- You can prepare a note in 2 A4 sheets

Ask a question

Sample questions

- Given the WiFi network with 2.4GHz, a User A with power transmission at 23dB and single antenna, what is the data rate the user can gain. Assume the noise is unremarkable

- Check the following figure and figure out what is wrong?