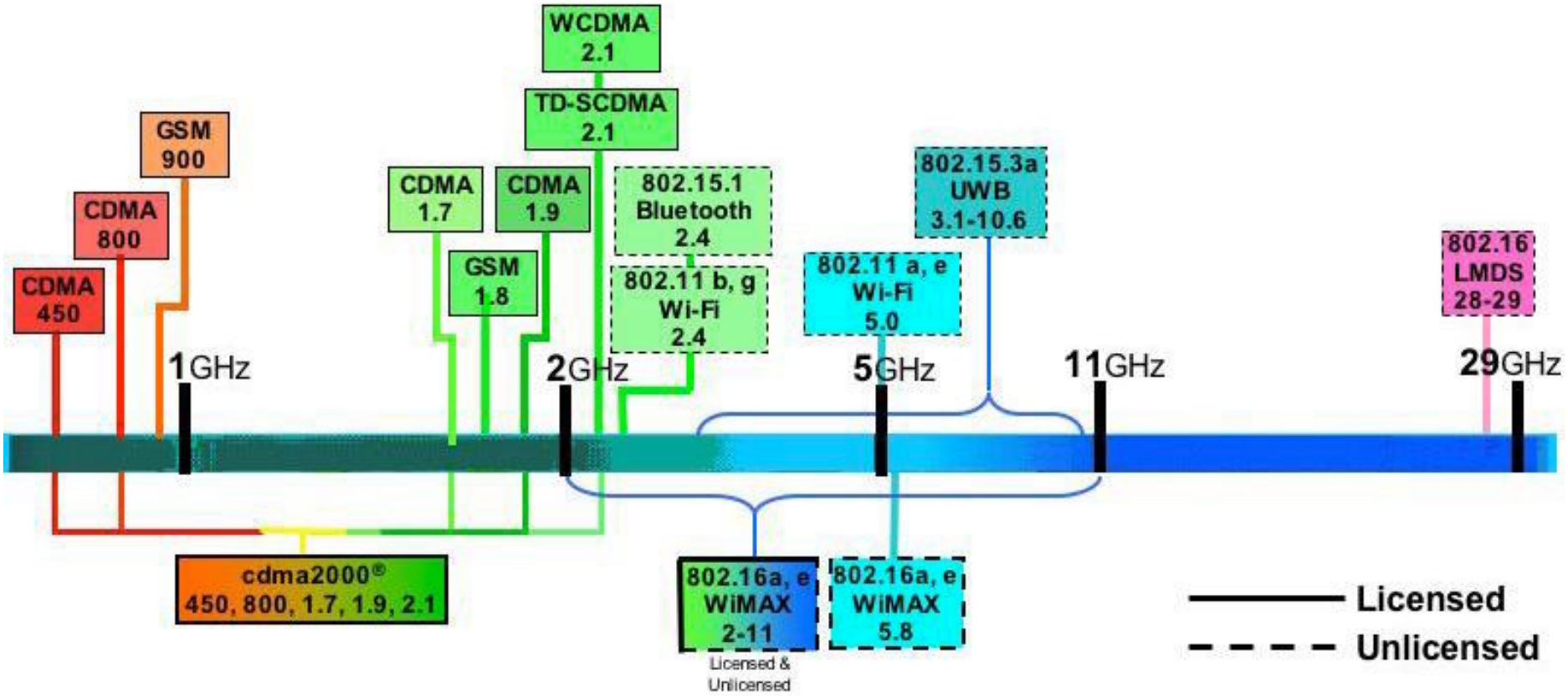
Lecture 19: Wi-Fi

Jianjun Chen (Jianjun.Chen@xjtlu.edu.cn)

Wi-Fi and WLAN

- We learned that wireless network is classified as:
  - WWAN – Wireless Wide Area Networks
    - 2G/3G/4G/5G cellular networks
    - Uses licensed frequency bands. Only those who have the license can create networks.
  - WLAN – Wireless Local Area Networks
    - Wi-Fi (wireless fidelity), Li-Fi (Light fidelity)
    - Wi-Fi uses unlicensed frequency bands. Everyone is free to create a network using these frequency bands. Thus suitable for creating local networks.
  - WPAN – Wireless Personal Area Networks
    - Bluetooth

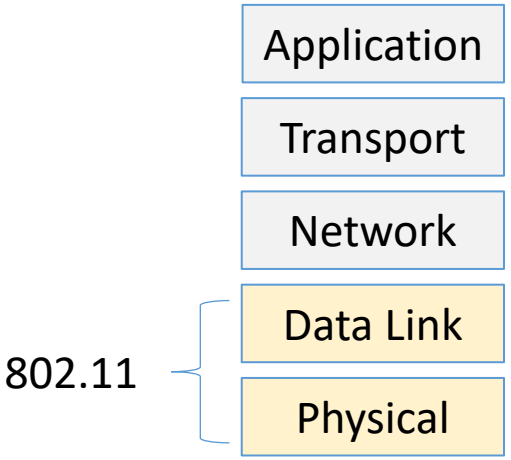

WCDMA
2.1
TD-SCDMA
2.1
GSM
900
CDMA
800
CDMA
450
CDMA
1.7
CDMA
1.9
GSM
1.8
802.15.1
Bluetooth
2.4
802.11 b, g
Wi-Fi
2.4
802.15.3a
UWB
3.1-10.6
802.11 a, e
Wi-Fi
5.0
802.16
LMDS
28-29
1GHz
2GHz
5GHz
11GHz
29GHz
cdma2000®
450, 800, 1.7, 1.9, 2.1
802.16a, e
WiMAX
2-11
Licensed &
Unlicensed
802.16a, e
WiMAX
5.8
Licensed
Unlicensed

Wi-Fi Basics

- What is Wi-Fi
  - Wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.
- What is IEEE 802.11
  - A set of media access control (MAC) and physical layer (PHY) specifications for implementing WLAN communication in the 2.4, 3.6, 5 and 60 GHz frequency bands

IEEE 802.11

- Published in June 1997
- Use unlicensed frequencies
- Multiple different versions
  - 802.11a
  - 802.11b
  - 802.11d
  - 802.11g
  - 802.11n
  - 802.11s
  - …



IEEE 802.11a

- Ratified in 1999
- Operates in 5.8 GHz band
- Runs on 12 channels
- Data Rate: 54 Mbps
- Reality: 25 to 27 Mbps
- Not compatible with 802.11b
- Uses Orthogonal Frequency Division Multiplexing (OFDM)

IEEE 802.11b

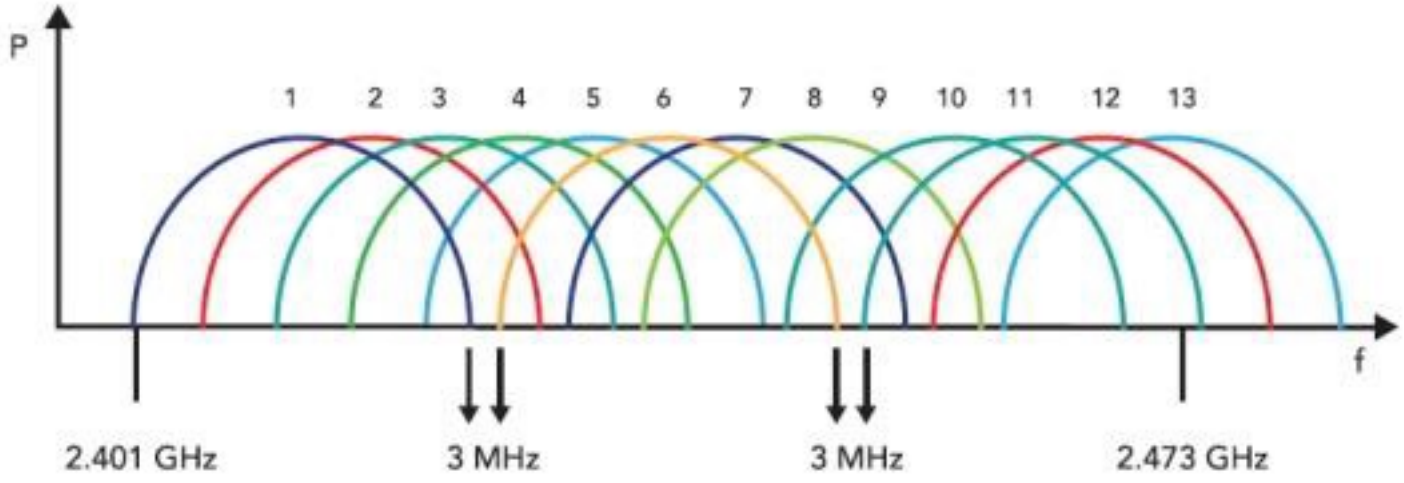
- Ratified in 1999
- Operates in 2.4 GHz band
- Shared by cordless phones, microwave ovens, and many Bluetooth products
- Runs on 13 channels (3 used in most cases)
- Data Rate: 11 Mbps
- Reality: 5 to 7 Mbps
- Most widely deployed today

IEEE 802.11g/n

- IEEE 802.11g
  - An extension to 802.11b
  - Data rate: 54 Mbps
  - 2.4-Ghz band
- IEEE 802.11n
  - An extension to 802.11a/g
  - Data rate: 600 Mbps
  - 2.4 or 5 Ghz band

Channels & Frequency

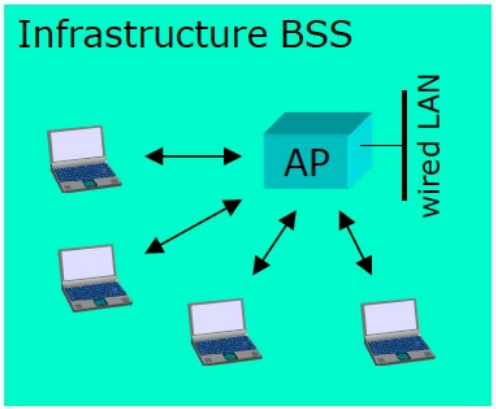
- Take 802.11b as an example
  - 13 free channels, channel 14 is usually restricted
  - 22 MHz bandwidth for each channel

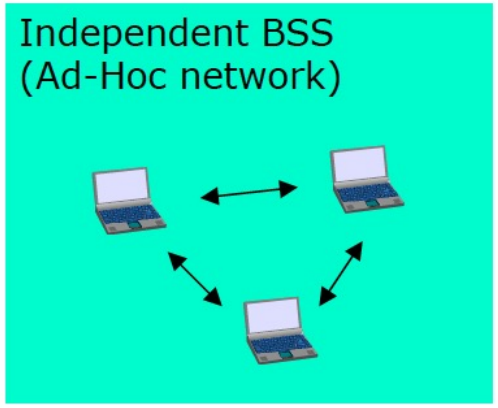


Wi-Fi: Network Architecture

Wi-Fi Architecture

- 802.11 defines two Wi-Fi network options:

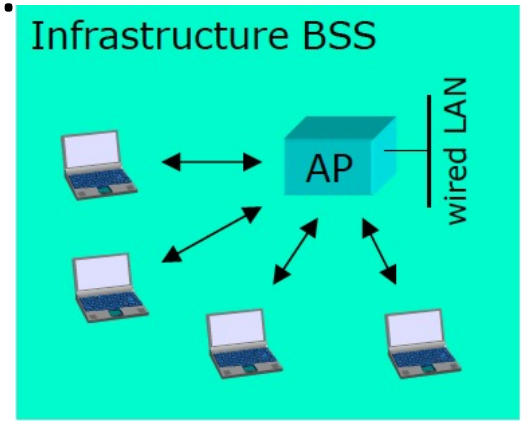




- Access Point (AP): A device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards

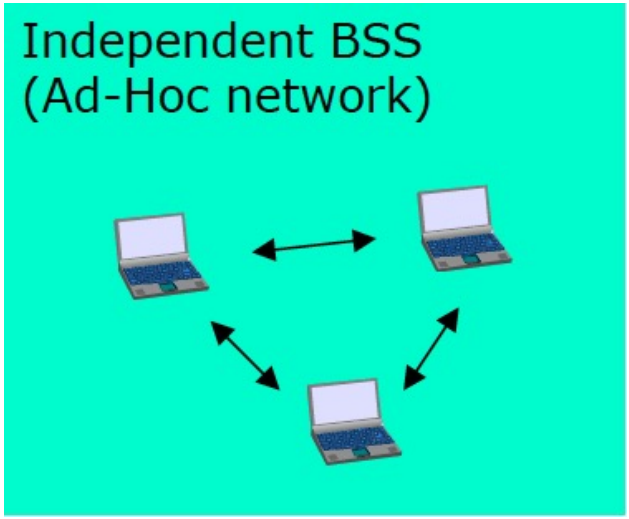
Infrastructure Network

- “Infrastructure” refers to real-world infrastructures like AP and wired LAN that are used to support the network
  - This is the most common way of implementing Wi-Fi.
- Wireless stations (Computers) in an infrastructure network must always communicate via the AP (never directly).



Independent Network

- Mainly of interest for military applications and research.
- No AP is required, computers can communicate directly.

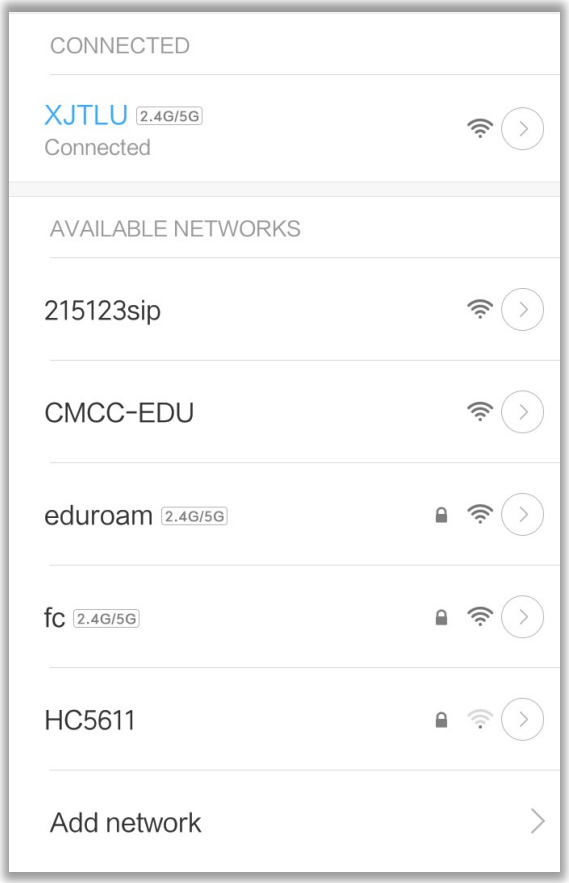


Basic Service Set (BSS)

- A single AP together with all associated mobile users is called a basic service set (BSS)
- For an infrastructure network, the access point's MAC address is used as the ID of a BSS (BSSID).
- For an independent network, a 48-bit string of numbers that looks and functions just like a MAC address is generated.
  - This BSSID goes in every packet

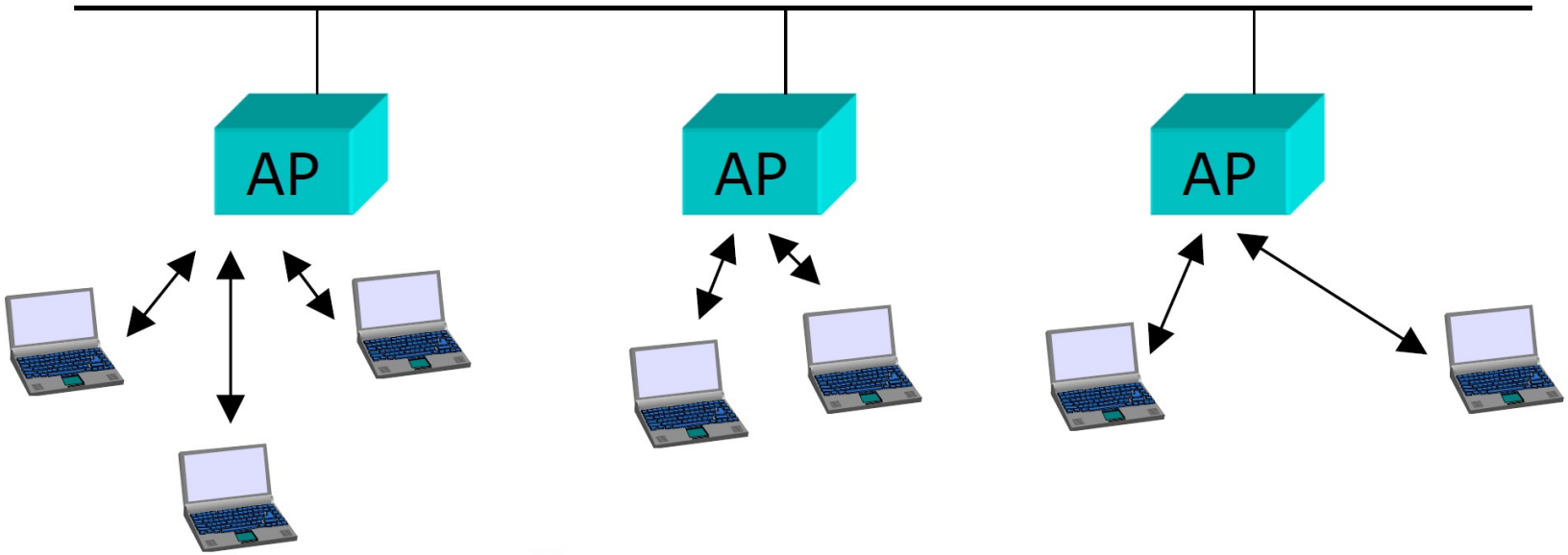
Service Set ID (SSID)

- Issues with BSSID:
  - BSSID is hard to remember.
  - For ad-hoc networks, BSSID is randomly generated each time.
- Thus, another level of naming called a Service Set Identifier (SSID) is created.
  - 32-byte identification string
  - E.g. our XJTLU network.
- You can create a Wi-Fi network with hidden SSID.



Extended Service Set (ESS)

- A larger Wi-Fi consisting of a number of BSS networks interconnected via a common backbone



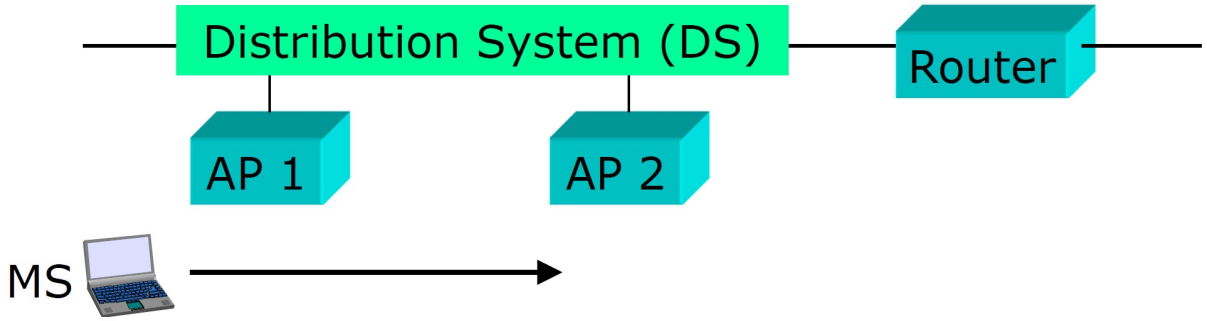
802.11 supports link-layer mobility within an ESS (but not outside the ESS)

Extended Service Set ID (ESSID)

- In a Wi-Fi network contains multiple APs. The SSID then becomes the SSID for all APs, it’s also called ESSID.
- ESSID and SSID refers to the same concept.
  - They are just human readable names for networks.
- SSID is used more commonly though.

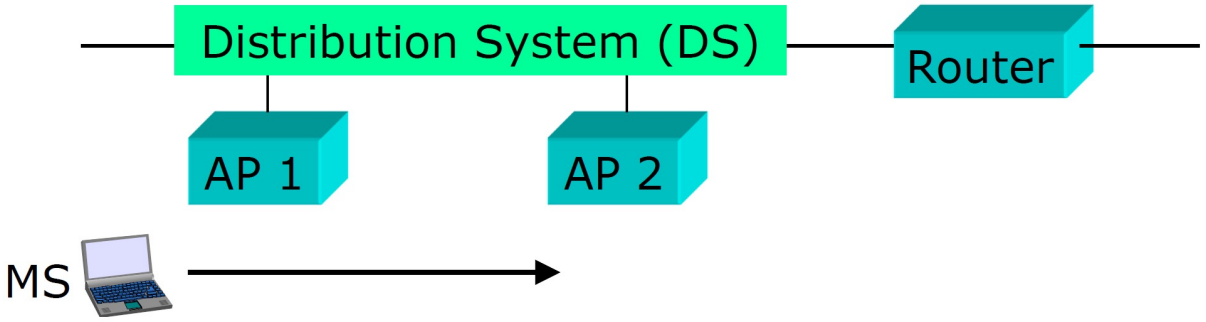
Mobility in Wi-Fi

- How does such a network handle mobility issues?
  - A computer moves from one AP to another.



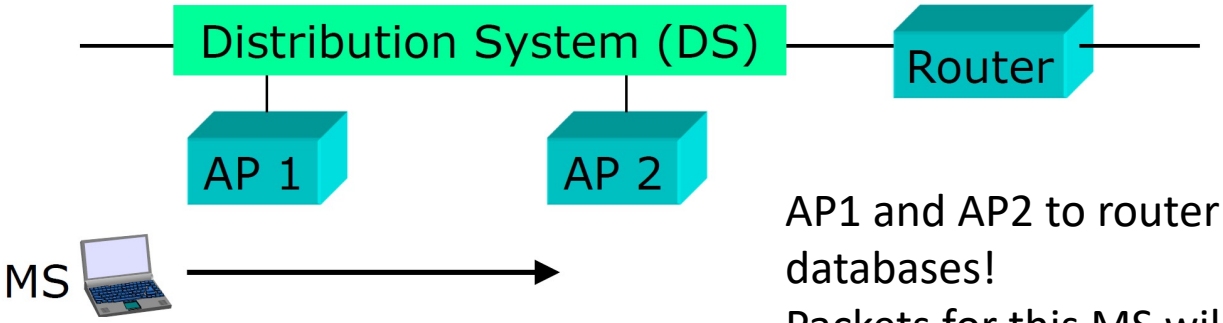
Mobility in Wi-Fi

- The handoff detection and decision process is vendor specific and is not specified by 802.11 standards.
- The user has more control on the handoff decision process.
- The signal strength and signal to noise ratio are the most used metrics.



Distribution System

- A mechanism by which APs and other nodes in wired IP subnetwork communicate with each other.
- When a computer moves from one BSS to another, all nodes must update their databases, so that the DS can distribute packets via the correct AP.



MS moves to another BSS

AP1 and AP2 to router: update your databases!
Packets for this MS will now be routed via AP 2.

Wi-Fi Security

Security

- Wireless brings security threats
  - Eavesdropping
  - Impersonating/spoofing
  - Jamming
  - …
- How to deal with these problems in 802.11
  - Service Set Identifier (SSID) hiding
  - MAC address filtering
  - Wired Equivalent Privacy (WEP) protocol

SSID Hiding

- Hiding the network name SSID from being broadcast publicly (Network cloaking)
  - Can only stop some inexperienced users from gaining access to your AP
  - There are other ways to discover the SSID
    - Probe requests/Probe responses
    - Association requests/Re-association requests
- Therefore, SSID hiding is not considered a security reliable measure.
  - https://www.howtogeek.com/howto/28653/debunking-myths-is-hiding-your-wireless-ssid-really-more-secure/

MAC Address Filtering

- Control access by allowing only valid MAC addresses to access the network
- Pros
  - Provides a stronger security than SSID hiding
- Cons
  - Increases administrative overhead
  - Reduces scalability
  - Determined hackers can still break it by spoofing MAC addresses with software

Wi-Fi Security

- Only unauthorized users can access the Wi-Fi
- Data communication between mobile terminal and AP should be protected.
- WEP: Wired Equivalent Privacy
- WPA: Wi-Fi Protected Access
- IEEE 802.11i/WPA2

WEP

- Published in 1999, WEP is the security component at the data-link layer of 802.11b
- Requirements: All computers and APs in the same WLAN have to share the same secret key K (called the WEP key)
- Proved to be vulnerable to brutal force attack because of limited keys available (24 bits)

Cracking WEP Network

- Assume we have a computer trying to guess the password of the AP. Each attempt constantly sends a 1500 byte packet and the network speed is at 11Mbps (Million bits per second: 1000,000 bits/s). How long does it take to enumerate through all password possibilities?

Answer is covered

Wi-Fi Protected Access (WPA)

- Published in 2003 by the Wi-Fi Alliance
- Based on an early version (draft 3) of the IEEE 802.11i standard
- Three major objectives:
  - Correct all the security flaws in WEP
  - Make existing WEP hardware also support WPA
  - Ensure WPA is compatible with the 802.11i standard

WPA2

- Strong encryption and authentication for infrastructure and ad-hoc networks (WPA1 is limited to infrastructure networks)
- Use AES instead of RC4 for encryption
- From 2006, WPA2 certification has become mandatory for all new equipment certified by the Wi-Fi Alliance

Wireless Data Link Layer: Traffic Management

Collision Avoidance

MAC layer of 802.11

- The following three basic access mechanisms have been defined for IEEE 802.11:
  - The mandatory basic method based on a version of CSMA/CA. (Next slide)
  - An optional method avoiding the hidden terminal problem.
  - A contention-free polling method for time-bounded service.

Not commonly used

The MAC mechanisms are also called **distributed foundation wireless medium access control (DFWMAC)**.

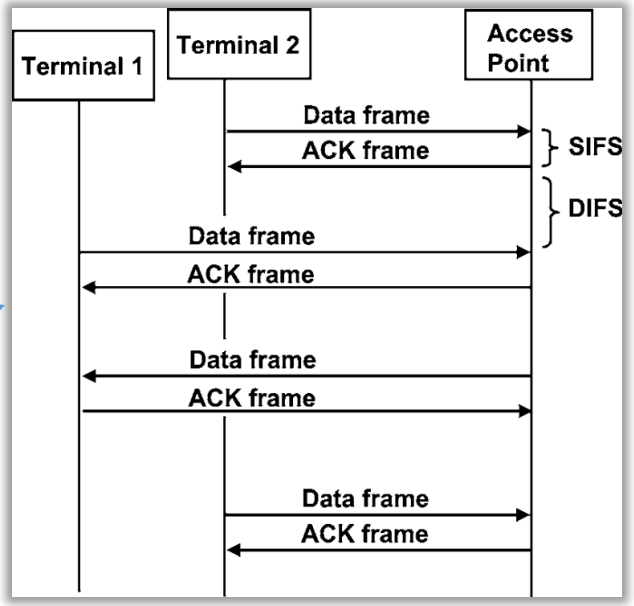
These two putting together are called distributed coordination function (DCF)

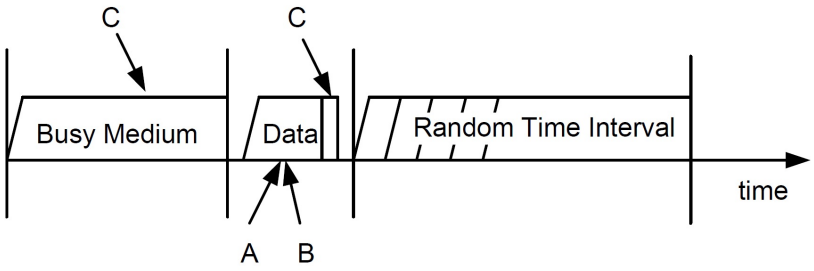
Called point coordination function (PCF)

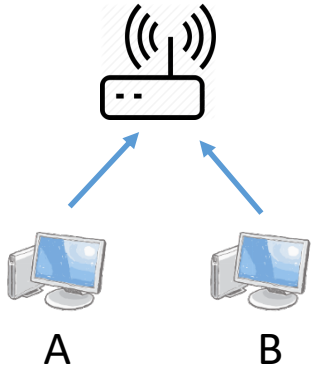
CSMA/CA without RTS/CTS

This is the “mandatory basic method”

1. Listen to medium and wait until it is free.
2. When the medium is free, wait for another time interval, then send the data packet.
    1. The AP will reply with an ACK frame to confirm.
3. If collision happens, AP will ask all senders to stop sending and wait a random time interval before sending again.







Inter-frame Spacing

- The wait between a data frame and an ACK frame is defined as short inter-frame space (SIFS).
- All other devices have to delay their transmission by at least a DCF inter-frame space
  - distributed coordination function inter-frame space, or DIFS for short

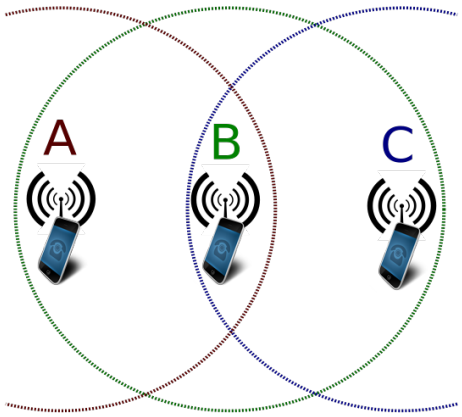
The Hidden Terminal Problem

"In wireless networking, the hidden node problem or hidden terminal problem occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP. This leads to difficulties in medium access control sublayer since multiple nodes can send data packets to the AP simultaneously, which creates interference at the AP resulting in neither packet getting through."

https://en.wikipedia.org/wiki/Hidden_node_problem

The Hidden Terminal Problem

- For example, B is an AP and A and C are computers.
  - A and C are so far away that they cannot detect the signal of each other.
  - Carrier sense multiple access with collision detection (CSMA/CD) does not work.
    - A cannot detect the signal of C.
  - CSMA/CD without RTS/CTS will be less efficient.



https://er.yuvayana.org/hidden-terminal-and-exposed-terminal-problem-and-its-solution/

CSMA/CA with RTS/CTS

- To prevent the hidden terminal problem, CSMA/CA with RTS/CTS is introduced.
  - This is an optional function.

- Essentially, devices can reserve the air interface prior to the transmission of a data frame.
  - Request to send (RTS): Asking the AP to allocate a time.
  - Clear to send (CTS): AP arranges the time and then tell everyone in the network.

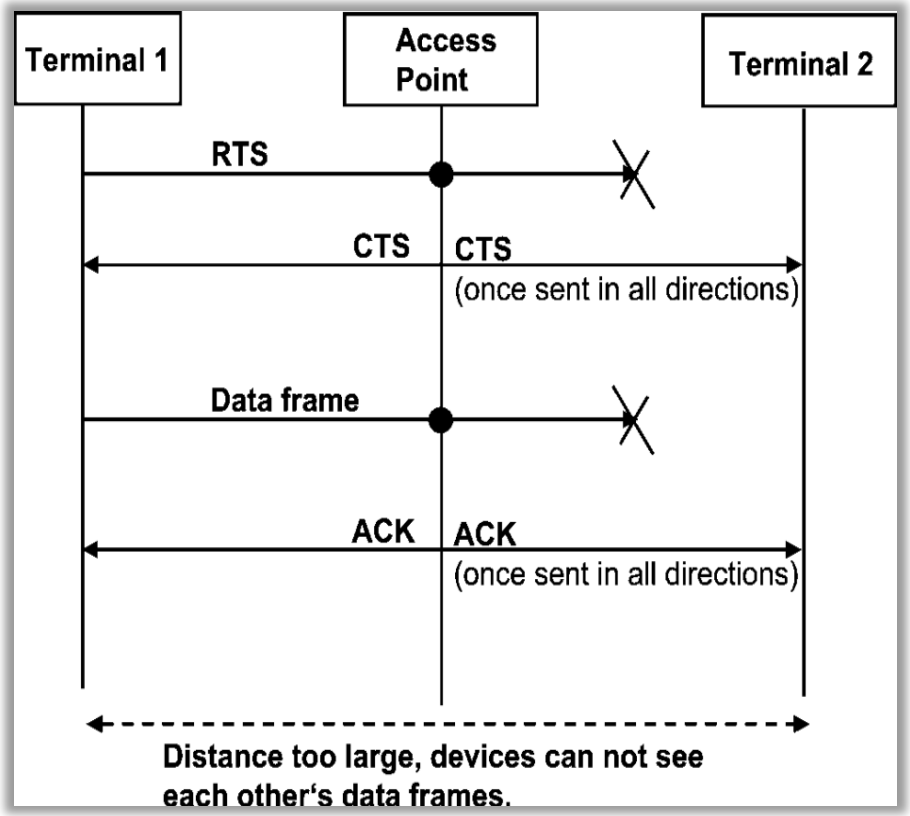
RTS and CTS Packets

- Both RTS and CTS frames contain a so-called network allocation vector (NAV) to inform other devices for which period of time the air interface is reserved.

- RTS/CTS sequences slow down the throughput of a device. Therefore this mechanism should only be used:
  - If a very high network load is expected.
  - And the client devices are dispersed over a wider area.

CSMA/CA with RTS/CTS

- Listen to medium and wait until it is free
- When the medium is free, send a "request to send" (RTS)
- Wait for a "clear to send" (CTS) from the receiver
- Transmit actual data packet after receiving the CTS
- Receive an acknowledgement (ACK) from the receiver



The Exposed Terminal Problem

- **Mandatory** extended reading: the exposed terminal problem.

- Check these two links for the description:
  - https://er.yuvayana.org/hidden-terminal-and-exposed-terminal-problem-and-its-solution/
  - https://en.wikipedia.org/wiki/Exposed_node_problem

- Answer will be revealed in the next time.