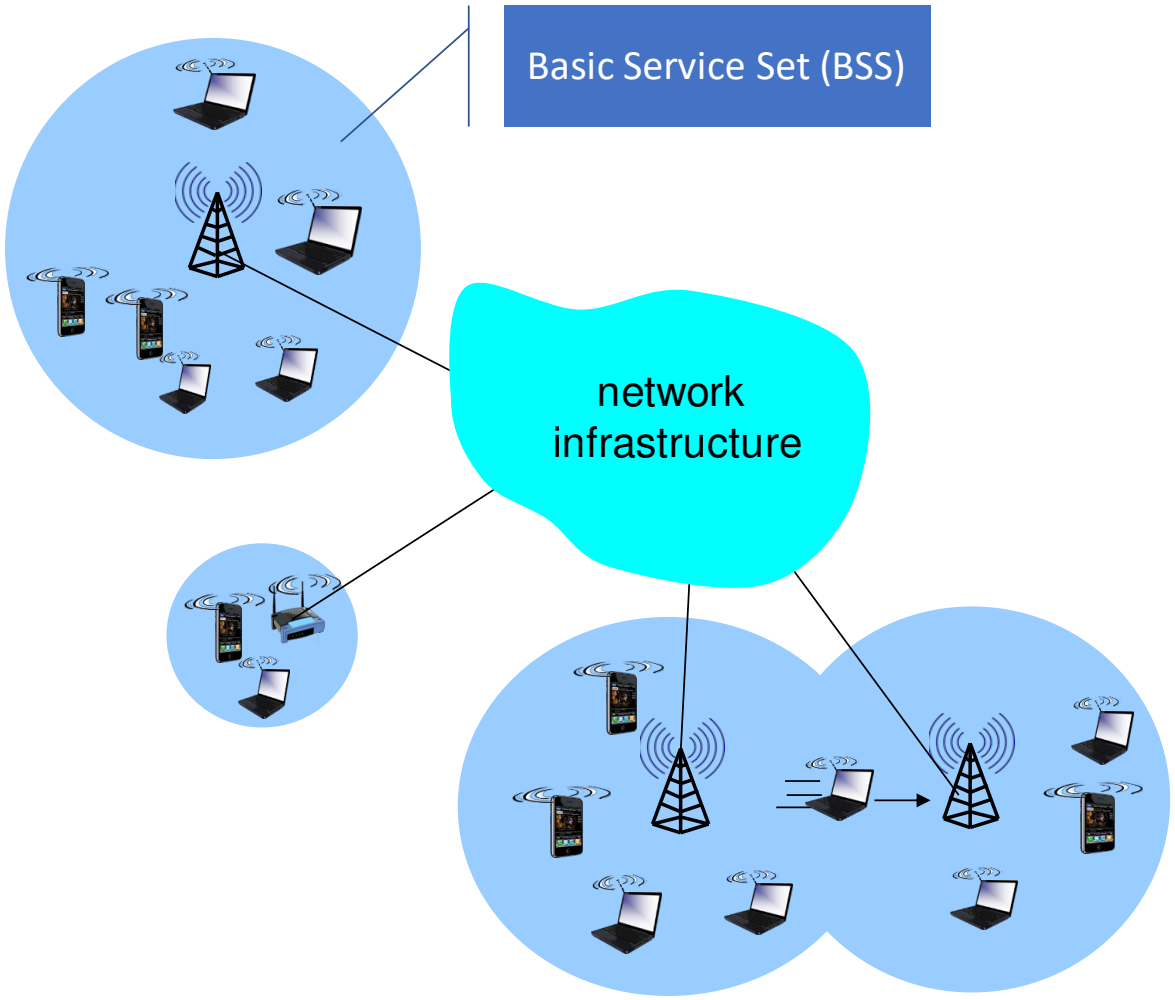
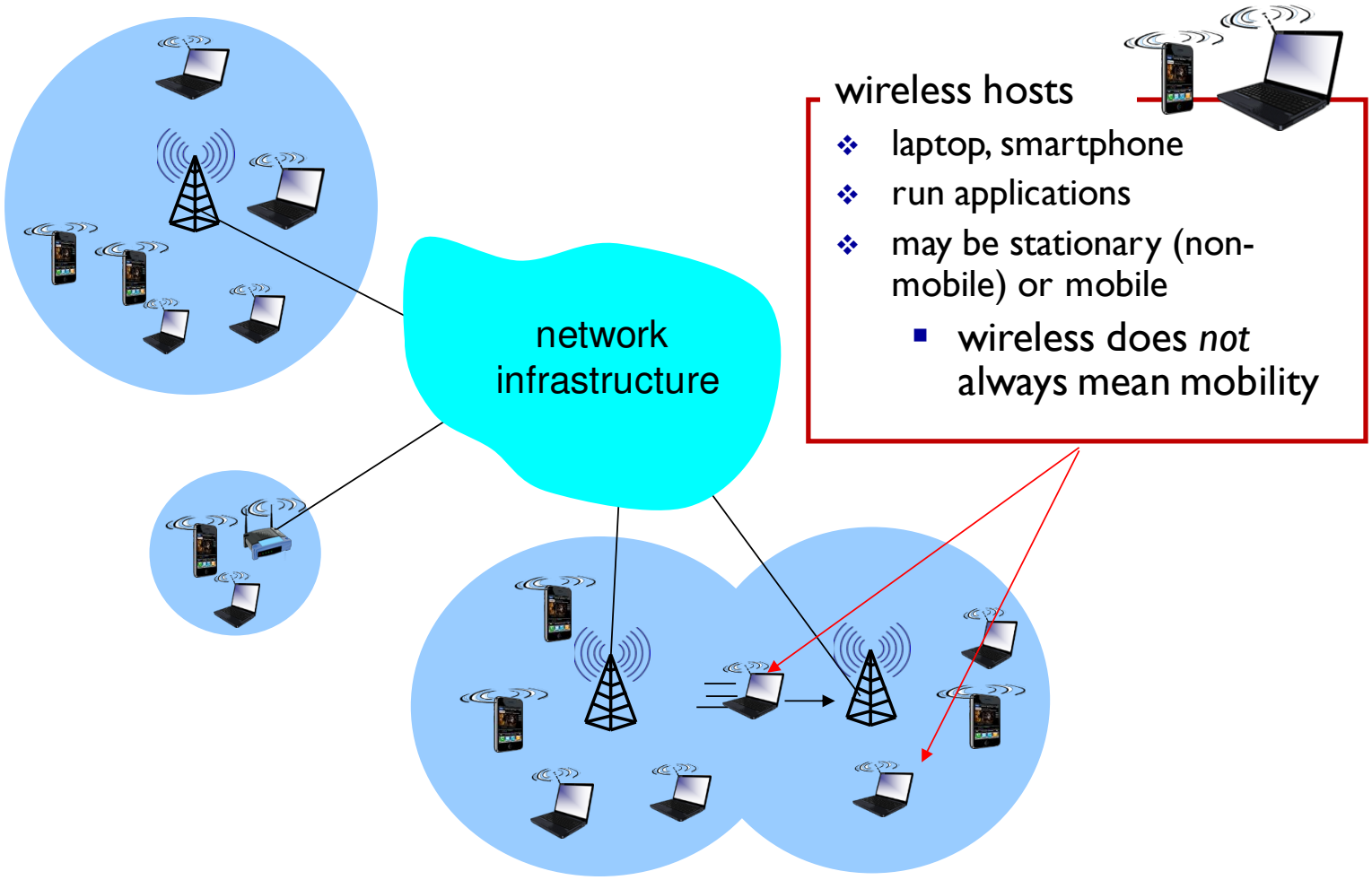
WiFi

Elements of a Wireless Network



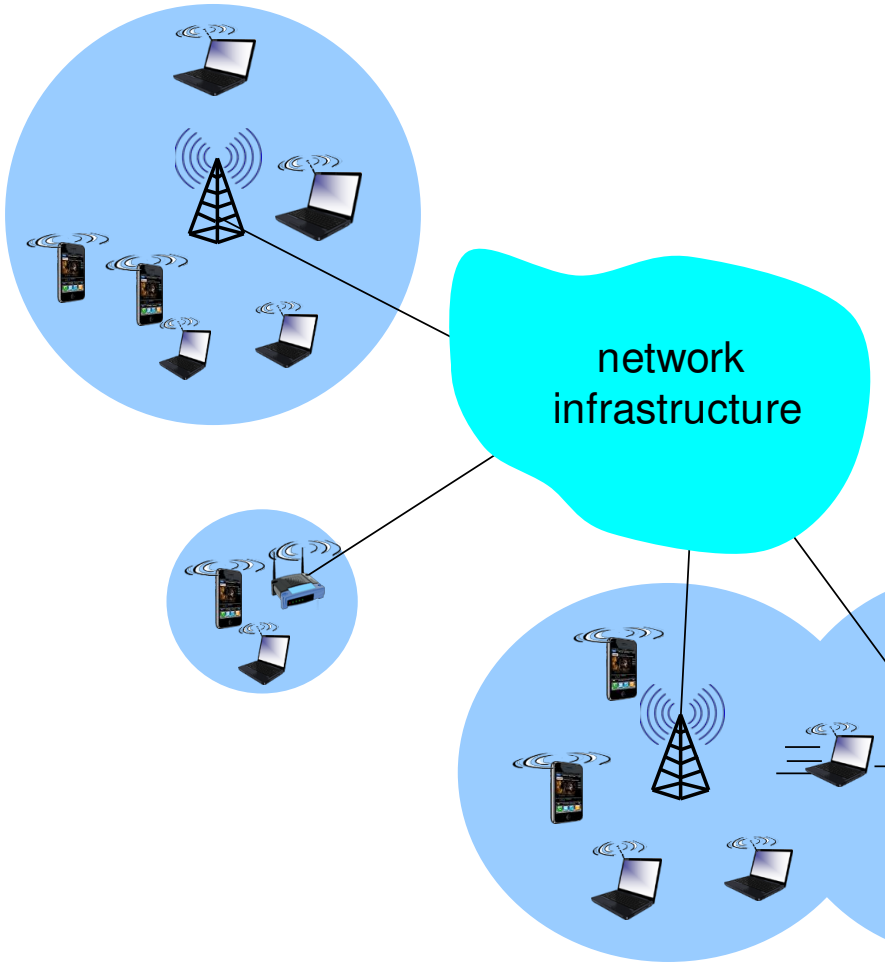
Elements of a Wireless Network



wireless hosts

- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

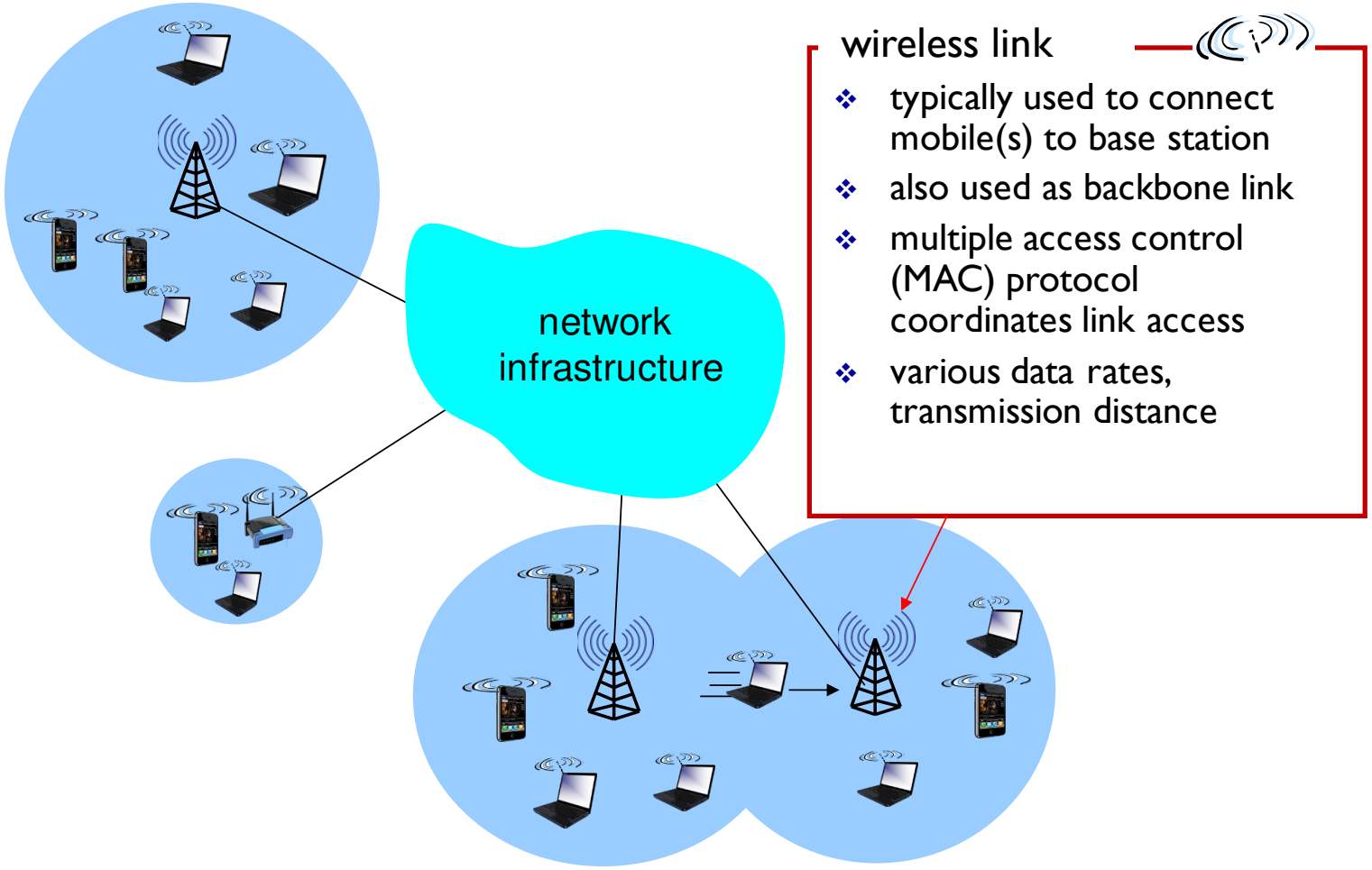
Elements of a Wireless Network



base station

- typically connected to wired network
- Routing - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

Elements of a Wireless Network

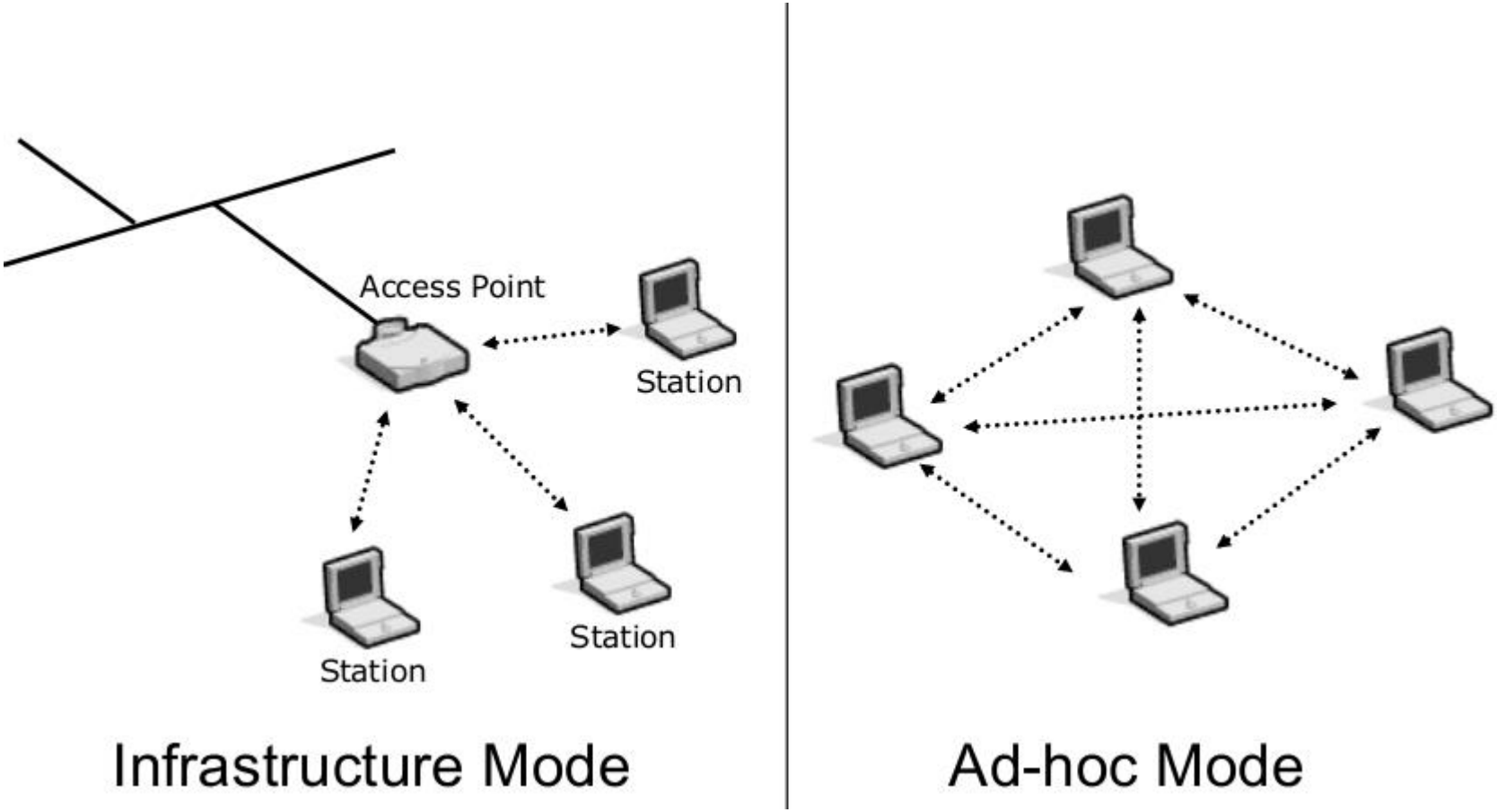


Wireless LAN Technologies and Wi-Fi

IEEE Standard	Frequency Band	Data Rate	Modulation Technique	Multiplexing Technique
original 802.11	2.4 GHz	1 or 2 Mbps	FSK	DSSS
	2.4 GHz	1 or 2 Mbps	FSK	FHSS
	InfraRed	1 or 2 Mbps	PPM	– none –
802.11a	5.725 GHz	6 to 54 Mbps	PSK or QAM	OFDM
802.11b	2.4 GHz	5.5 and 11 Mbps	PSK	DSSS
802.11g	2.4 GHz	22 and 54 Mbps	various	OFDM
802.11n	2.4/5 GHz	54 – 600 Mbps		MIMO/SDM
802.11ac	5GHz	433-2,600 Mbps	QAM	MIMO/SDM

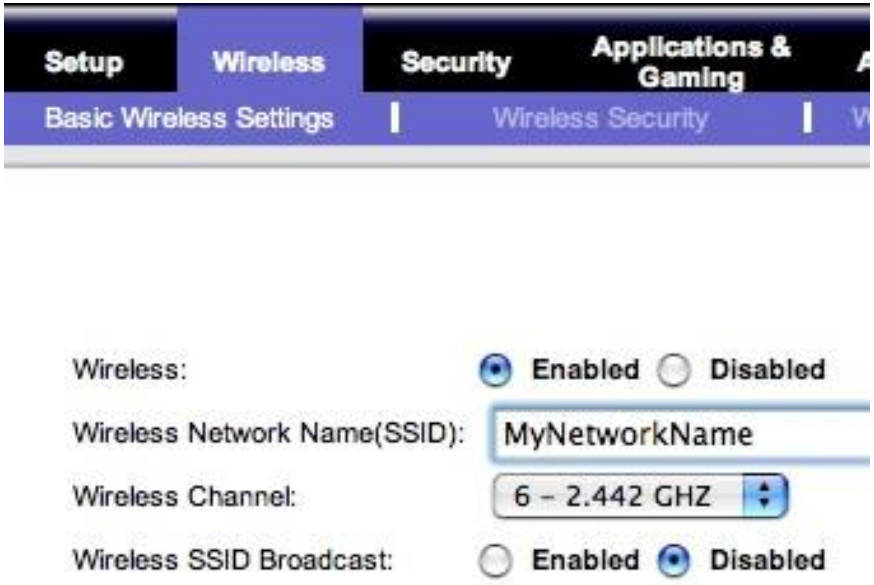
Key wireless standards certified by the Wi-Fi Alliance.

Wireless LAN – Modes of operation



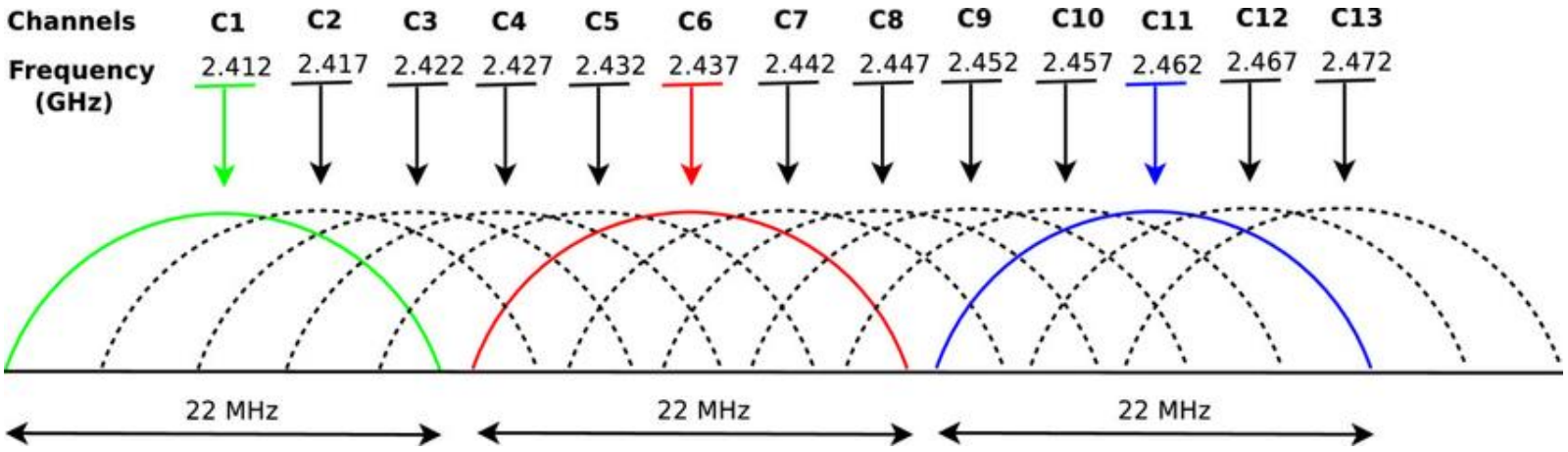
SSID(Service Set ID)

- At a minimum a client station and the access point must be configured to be using the same SSID.
  - An SSID is between 2 and 32 alphanumeric characters
  - Spaces allowed
  - Must match EXACTLY, including upper and lower case
  - Beware of typing spaces at the end of your SSIDs in both AP config and client config...



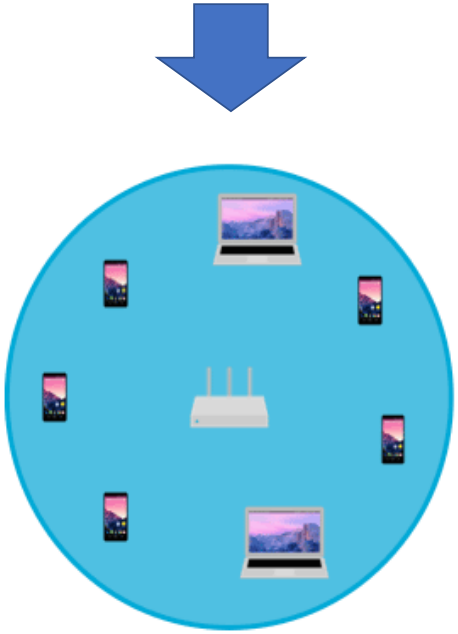
802.11: Channels, association

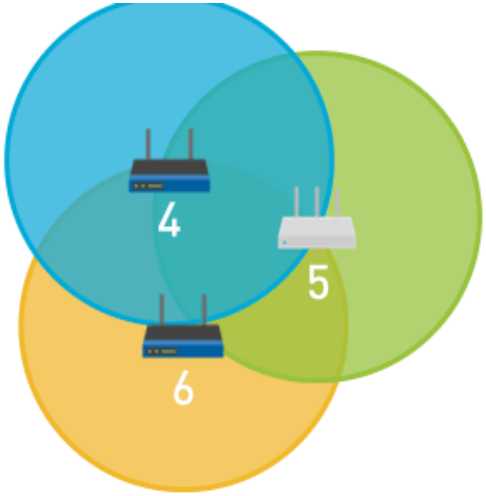
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

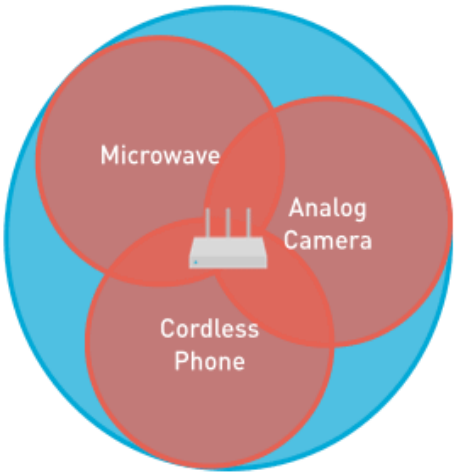


Wireless Network Interference

- Co-Channel:
  - Every device on same channel
  - What if they start to talk at the same time?
- Adjacent Channel
  - Every device/access point on adjacent channels
- Other devices not on 802.11 network
  - Interference from other non-networked devices in the environment





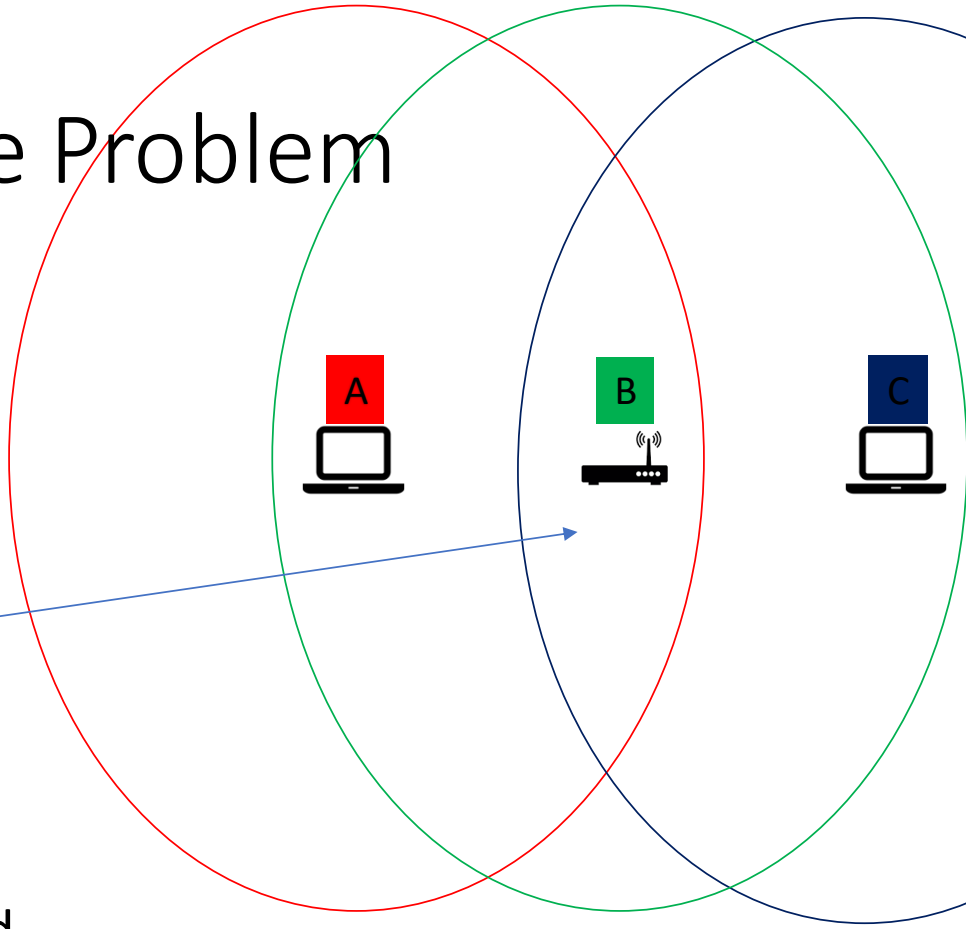


Carrier Sense Multiple Access – Collision Avoidance

- The wireless 802.11 standard uses CSMA/CA or "collision avoidance."
- The method is used because the wireless stations have no way to detect collisions WHILE sending.
  - Attempts to avoid collisions rather than detect them
- How it works:
  - Transmitting device listens to the network (senses the carrier) and waits for it to be free
  - Device then waits a random period of time and transmits.
  - If the receiver gets the frame intact, it sends back an ACK to the sender.
  - If no ACK is received, the message is re-transmitted.
  - If the channel is not clear, the node waits for a randomly chosen period of time (backoff factor), and then checks again to see if the channel is clear.

Interference - Hidden Node Problem

- What if this happens:
- **A** and **C** start to send packets simultaneously
  - **A** and **C** are out of range of each other so can't detect respective signals
- Collisions occur at access point region.
- Request-to-send/clear-to-send (RTS/CTS) handshaking (IEEE 802.11 RTS/CTS) is implemented in conjunction with CSMA/CA scheme.
- The same problem can happen in a mobile ad hoc network (MANET).



Contention and Contention-Free Access

- The original 802.11 standard defined two general approaches for channel access
- Point Coordinated Function (PCF) for contention-free service
    - an AP controls stations in the Basic Service Set (BSS) to insure that transmissions do not interfere with one another
    - For example, an AP can assign each station a separate frequency
    - In practice, PCF is never used
- Distributed Coordinated Function (DCF) for contention-based service
    - arranges for each station in a BSS to run a random access protocol

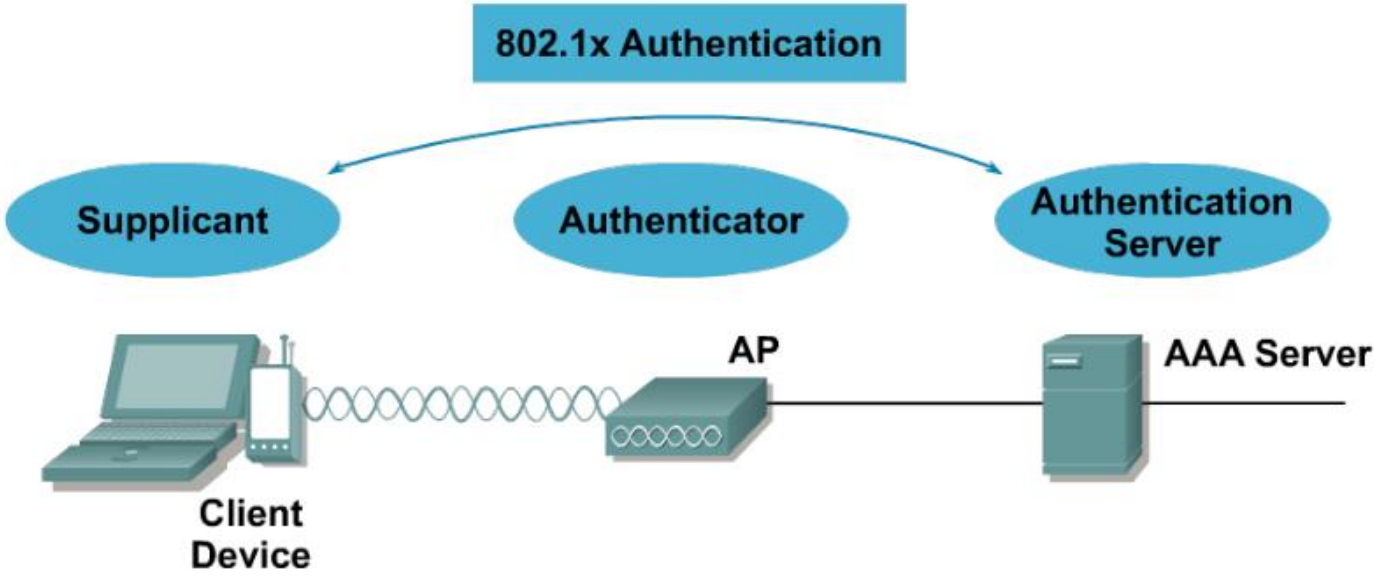
Interference

- Physical separation among stations and electrical noise makes it difficult to distinguish between
  - weak signals, interference, and collisions
- Hardware does not attempt to sense interference during a transmission
  - Instead, a sender waits for an acknowledgement (ACK) message
  - If no ACK arrives, the sender assumes the transmission was lost and employs a back-off strategy similar to the strategy in wired Ethernet
- In practice, 802.11 networks that have few users and do not experience electrical interference seldom need retransmission
- However, other 802.11 networks experience frequent packet loss and depend on retransmission

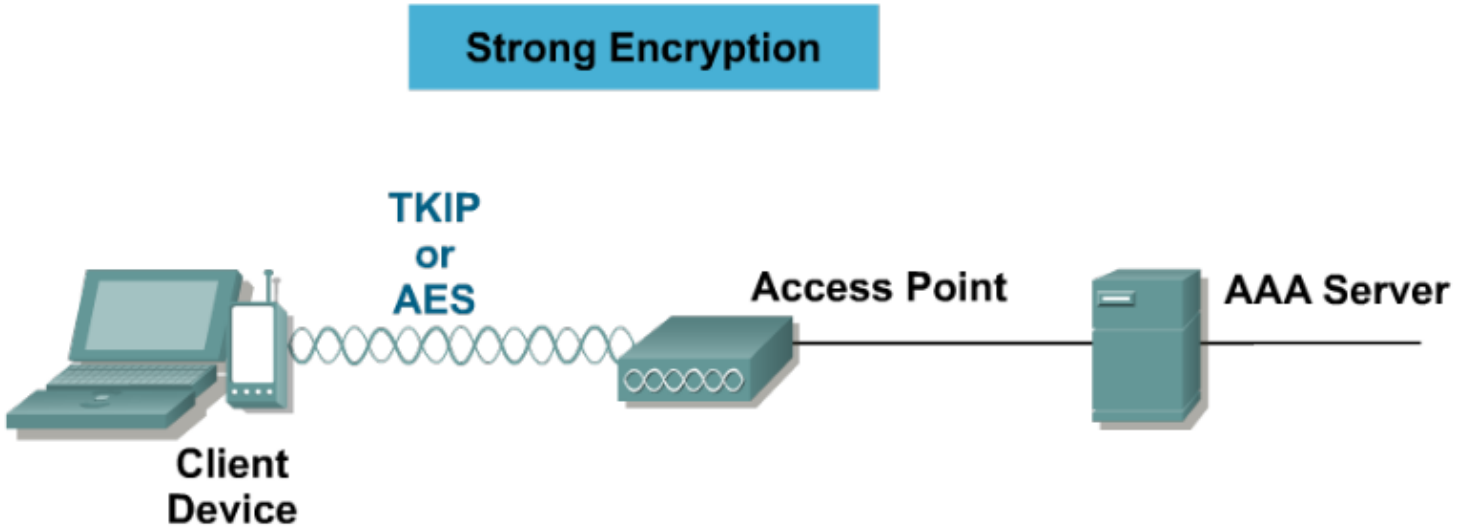
WLAN Security Concerns...

- Wide availability of low cost WLAN equipment
- Rush to market for IoT devices
- 802.11 almost too easy to use/deploy
- Sniffers
- Mitigating Threats
  - Authentication:
    - Ensure legitimate clients and trusted Aps
  - Encryption:
    - Protect data as it’s transmitted
  - Intrusion Detection
    - Track/Mitigate unauthorised access/attacks

WPA/WPA2 Authentication



WPA/WPA2 Encryption



Wireless Protocol Security Overview

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i