Wireless Networks

Dr. Frank Walsh

Dr. Kumar Yelamarthi

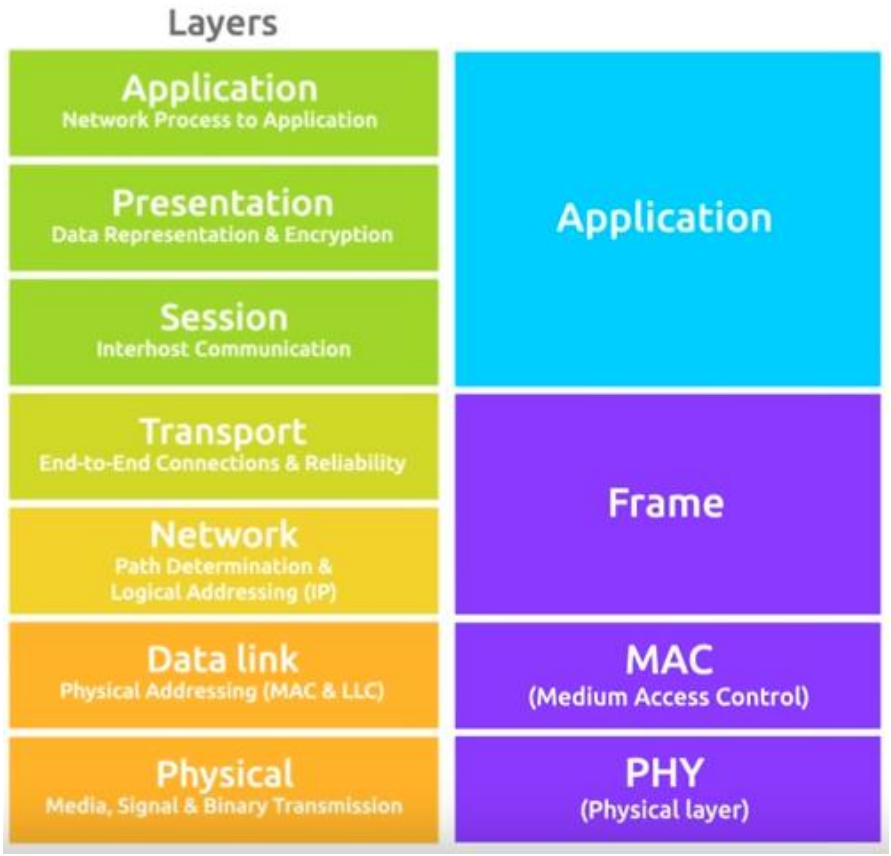
Wireless Network Protocols & IoT

- Vital enabler for IoT
  - Vast majority of IoT solutions will include one or more wireless technologies
- Expected 8-fold growth in mobile data between 2015 and 2020
- Wireless enabled devices are a major reason for explosion in connected devices and the IoT

Ulusar, Umit Deniz, Fadi Al-Turjman, and Gurkan Celik. "An overview of Internet of things and wireless communications." *Computer Science and Engineering (UBMK), 2017 International Conference on*. IEEE, 2017.

Network Protocol Suites & Standards

- A Protocol Suite is a group of protocols designed to work together
- Typically use open, widely used protocols.
  - Example: Wifi, HTTP, FTP, TCP, IP...
- Protocol Standards established by Institute of Electrical and Electronics Engineers (IEEE) or the Internet Engineering Task Force (IETF)
- Protocol suites based on open standards ensures that products from different manufacturers can work together for efficient communications



Wireless Advantages

- Look – no wires!
- Mobility
- Deployment
- Productivity
- Convienence

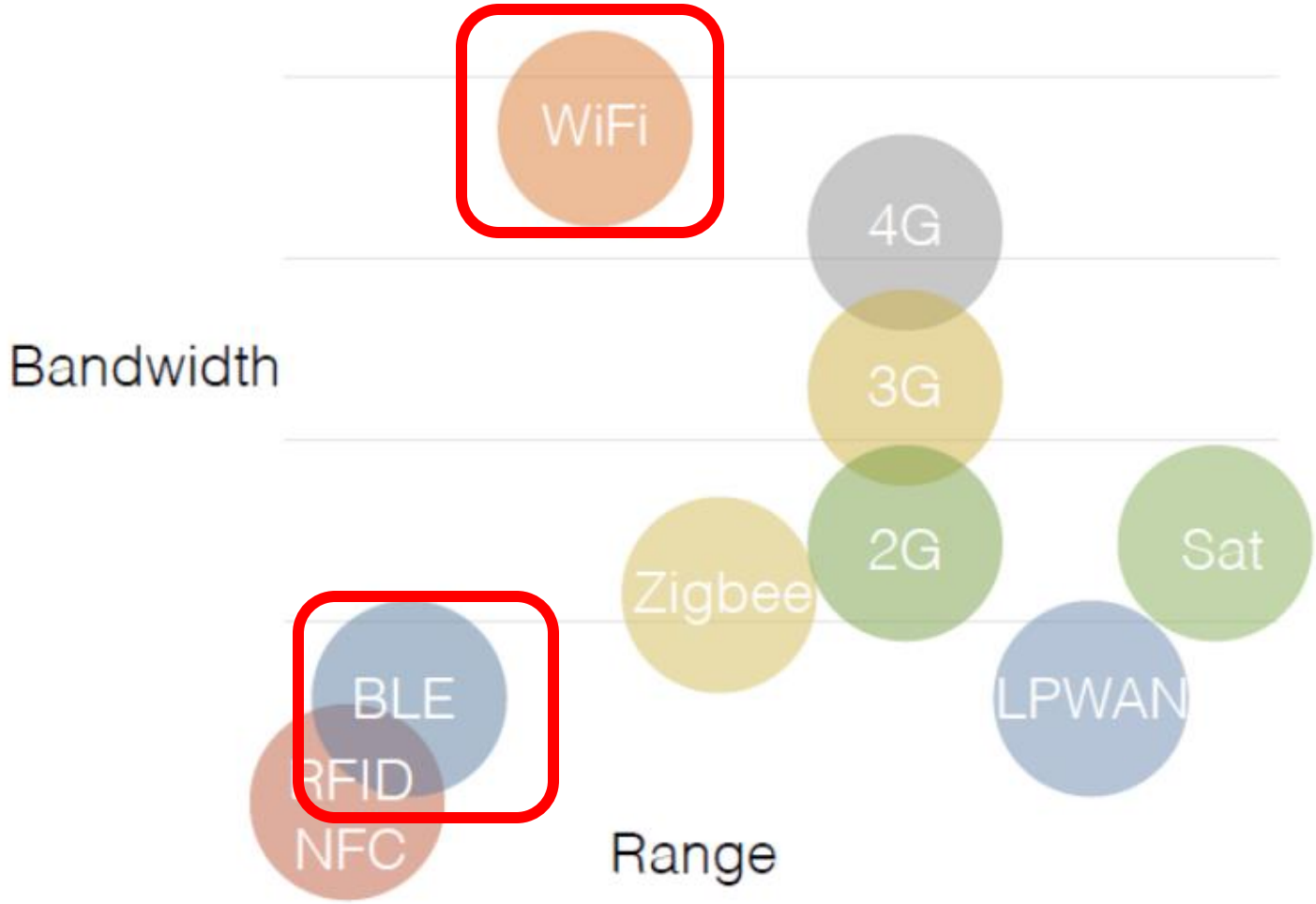
Problems

Physical differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation:* radio signal reflects off objects ground, arriving at destination at slightly different times

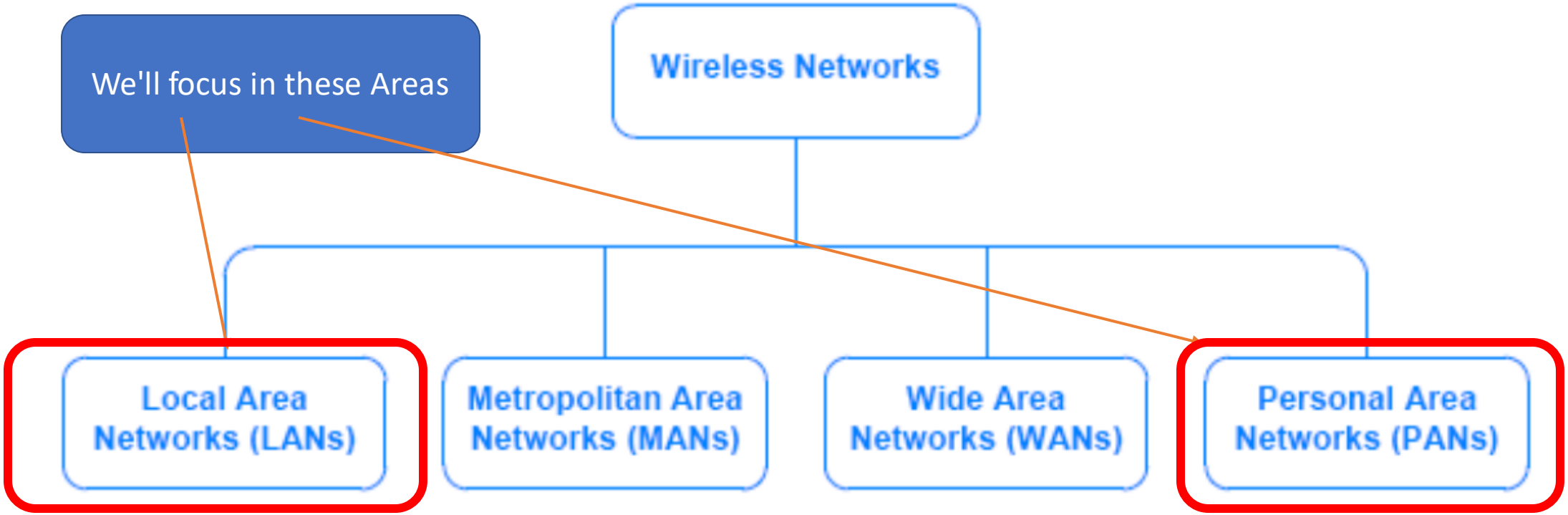
- make communication across (even a point to point) wireless link much more “difficult”
- Security/Speed/

Wireless Technologies Comparison



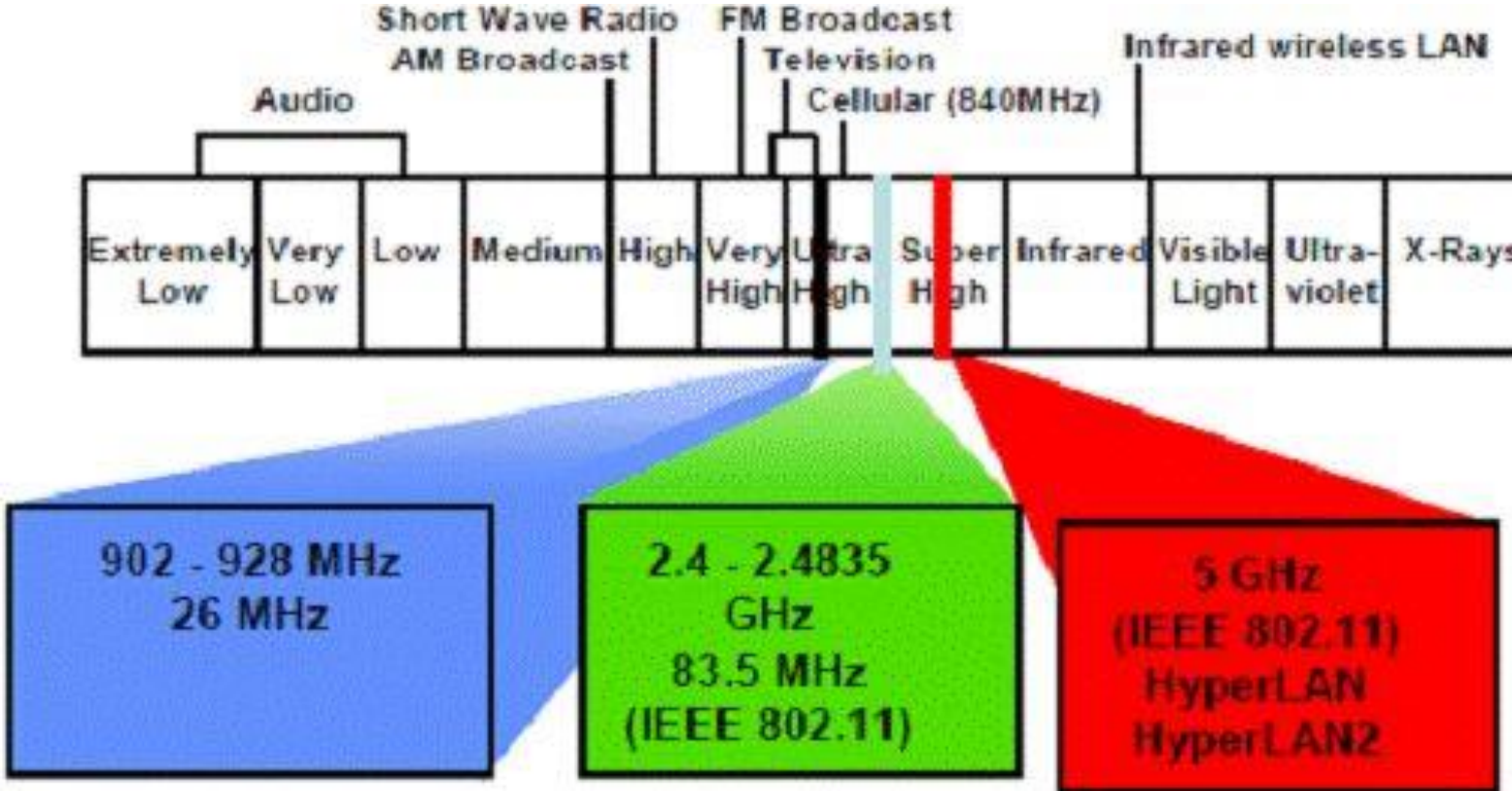
Wireless Networks Classification

- Wireless technologies can be classified **broadly** according to network type:



ISM Wireless Bands

- A region of electromagnetic spectrum is reserved for use by Industrial, Scientific, and Medical (ISM) groups
- These frequencies are not licensed to specific carriers
  - are broadly available for products, and are used for LANs and PANs

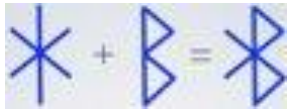


Personal Area Networks (PANs)

- A PAN technology provides communication over a short distance
- It is intended for use with devices that are owned and operated by a single user. For example
  - between a wireless headset and a cell phone
  - between a computer and a nearby wireless mouse or keyboard
- Several standards
  - Frequencies dedicated to Industrial, Scientific and Medical (ISM) band
  - Bluetooth, Near Field Comms(NFC)

Bluetooth

QI: The name "Bluetooth" comes from 10th century Danish king who united Danish tribes into a single kingdom.



- Used for short distance data exchanging, such as Personal Area Network
- RF from 2.4 to 2.485 GHz
- Originally invented by Ericsson (a telecom vendor) in 1994
- Now managed by the Bluetooth Special Interest Group (SIG)
- Frequency hopping spread spectrum (FHSS)
- 16000+ SIG member companies
- Billions of products shipped

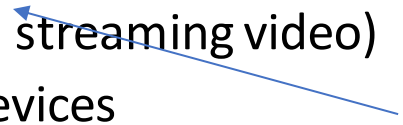
Bluetooth Classification

Bluetooth “classic”

- The “conventional” Bluetooth
- Operates in 2.4GHz
- Range: 1m - 100m (10m typical)
- Connection-oriented: audio, file transfer, networking
- Reasonably fast data rate: **2.1** Mbps
- Power consumption:
  - < Wifi < 3G

Bluetooth Low Energy

- "Bluetooth Smart“
- Light-weight subset of classic Bluetooth
  - Operates in same freq. Range, 2.4GHz
  - introduced as part of the Bluetooth 4.0 core specification
- Target Apps:
  - Wireless battery-powered sensors eg. heart rate, thermometer, wearables
  - Low bandwidth (you won't be streaming video)
  - Not always on, constrained devices



All good for IoT devices!

BLE vs Classic

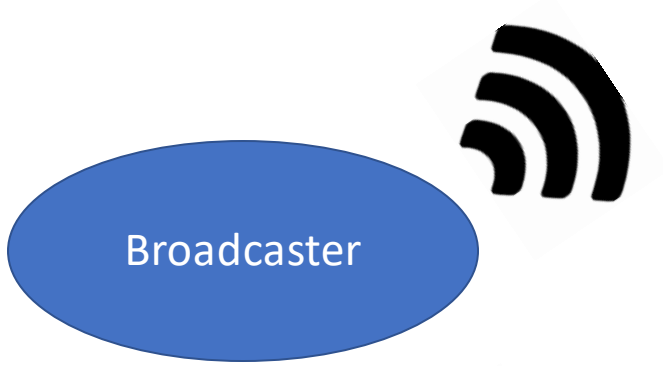
- Bluetooth and Bluetooth Low Energy are used for different purposes
- Bluetooth Classic
  - can handle a lot of data
  - consumes battery quickly
- BLE
  - used for applications that do not need to exchange large amounts of data
  - cheap
  - Marginally further range

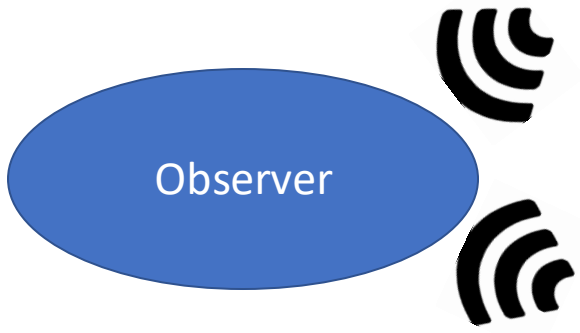
Bluetooth History

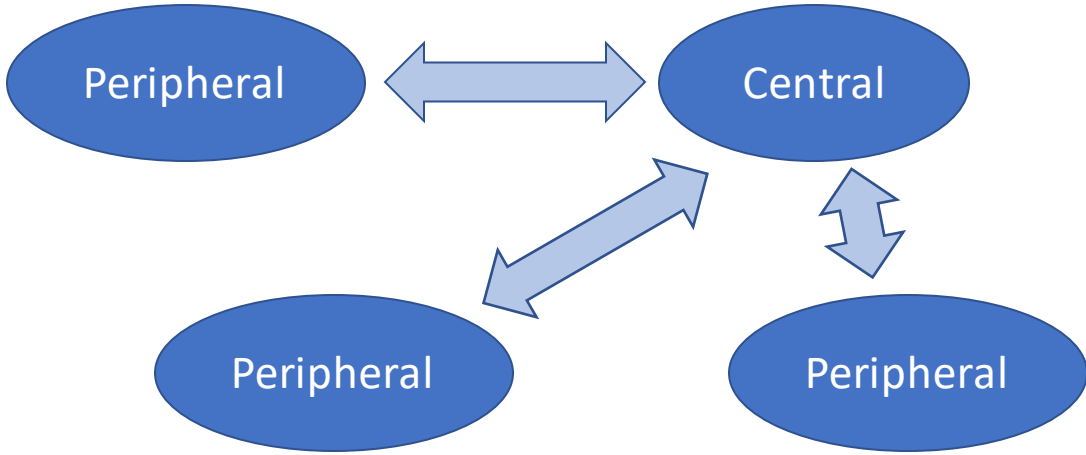
- Bluetooth 1.1
  - Published in 2002
  - Data rate: 1 Mbit/s
  - First widely implemented version
- Bluetooth 2.0 + Enhanced Data Rate (EDR)
  - Published in 2004
  - Data rate: 3 Mbit/s
- Bluetooth 3.0 + High Speed (HS)
  - Published in 2009
  - Data rate: 24 Mbit/s
- Bluetooth 4.0 +
  - Published in 2010
  - Data rate: 24 Mbit/s
  - Also called Bluetooth Smart
  - Includes Classic Bluetooth, Bluetooth high speed and Bluetooth low energy protocols
  - Bluetooth 4.2 (2014) - Introduces some key features for IoT

BLE Roles

- Broadcaster
  - Transmitter only
- Observer
  - Receiver only
- Peripheral(Slave)
- Central(Master)
  - Can take multiple connections
  - Initiates connection to peripheral
- One Device can have multiple roles





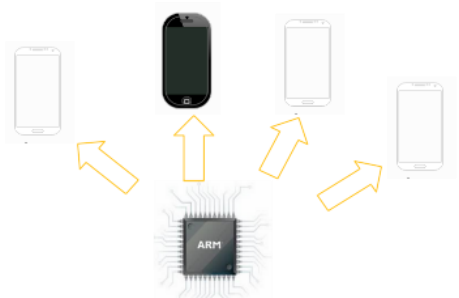


BLE Operation Modes

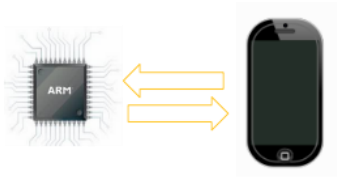
Peripheral and Central Devices	**Master/central :** will typically have more computing resources and available energy - a computer or a tablet, for example.
	Slave/peripheral : an embedded device - will be constrained in both computing resources and energy.
Servers and Clients	**Server :** the device that has information it wishes to share, and in BLE that is typically the peripheral (the embedded device).
	Client : the device that wants information and services, and in BLE that is typically the central device - the phone

BLE Connections

- Initiating Connections
  - The central is free to establish or terminate a connection
  - The peripheral (the BLE device) cannot force the central to scan for BLE devices
- The two modes BLE uses are:
  - Advertising mode : the peripheral sends out Generic Access Profile (GAP) that any device in the area can pick up; this is how central devices know that there are peripherals around.
  - Connected mode : the peripheral and a central device establish a one-to-one conversation. This is how they can exchange complex information.



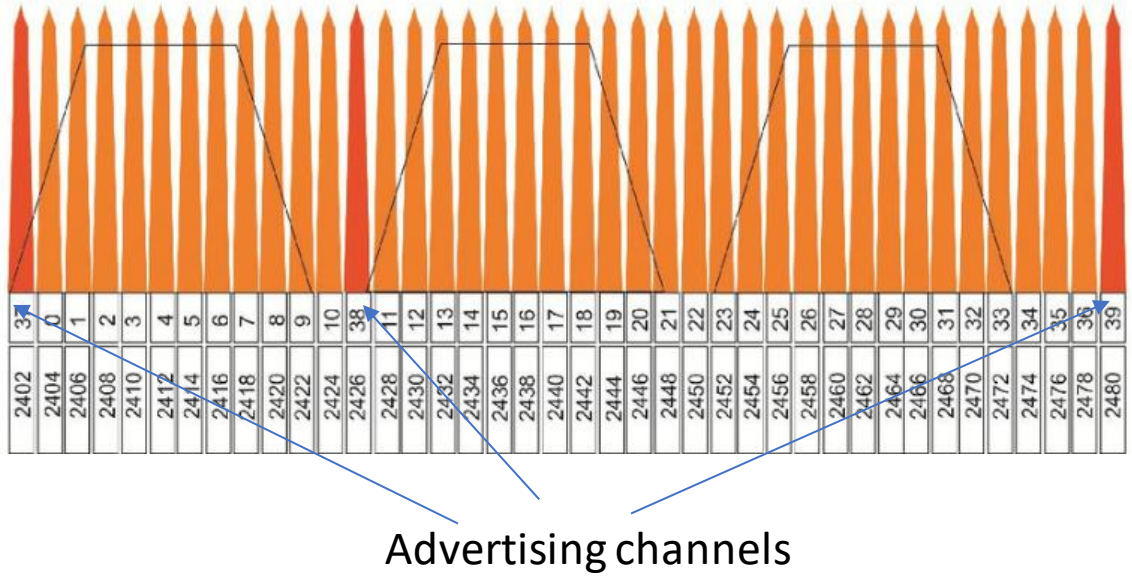
Advertising mode

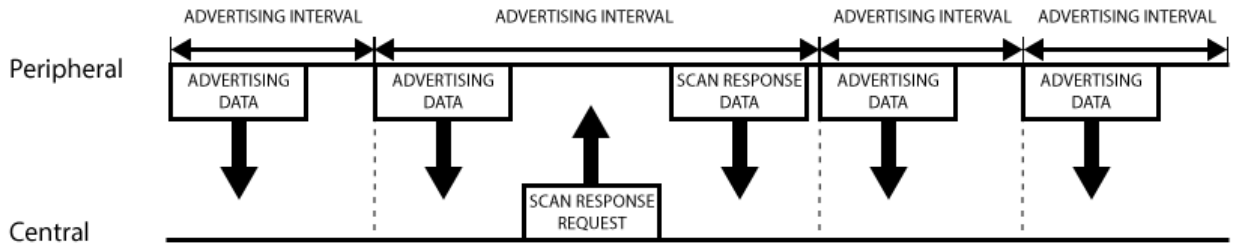


Connected mode

Advertising process

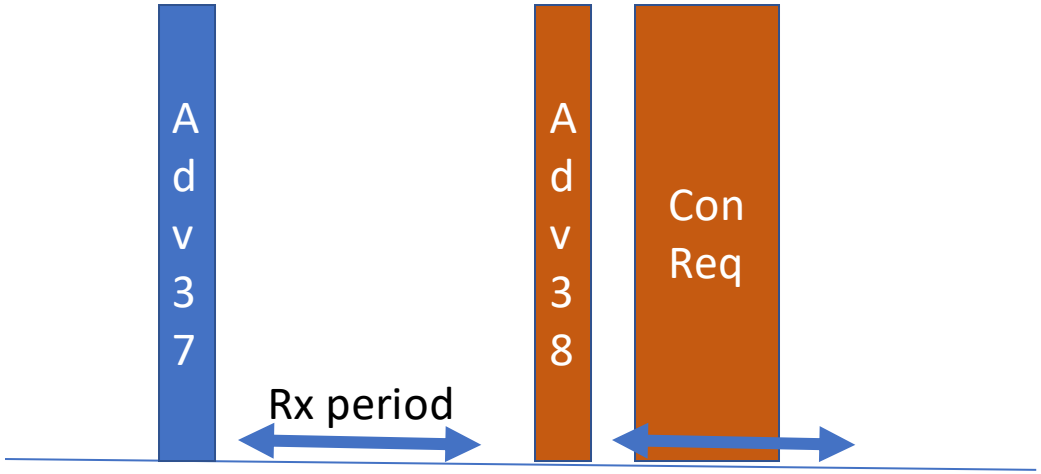
- Operates in 2.4 GHz Band
- Peripheral sets a specific advertising interval and transmit advertising packet
  - longer delays saves power but less responsive
- Transmits on all advertising channels in each interval(channel 37/38/39)
- A listening device interested in the scan response payload can optionally request the scan response payload, and the peripheral will respond with the additional data.





Connection Process

- Initiated by central device in a specific response period
- Central can issue connection request after receiving advertisement



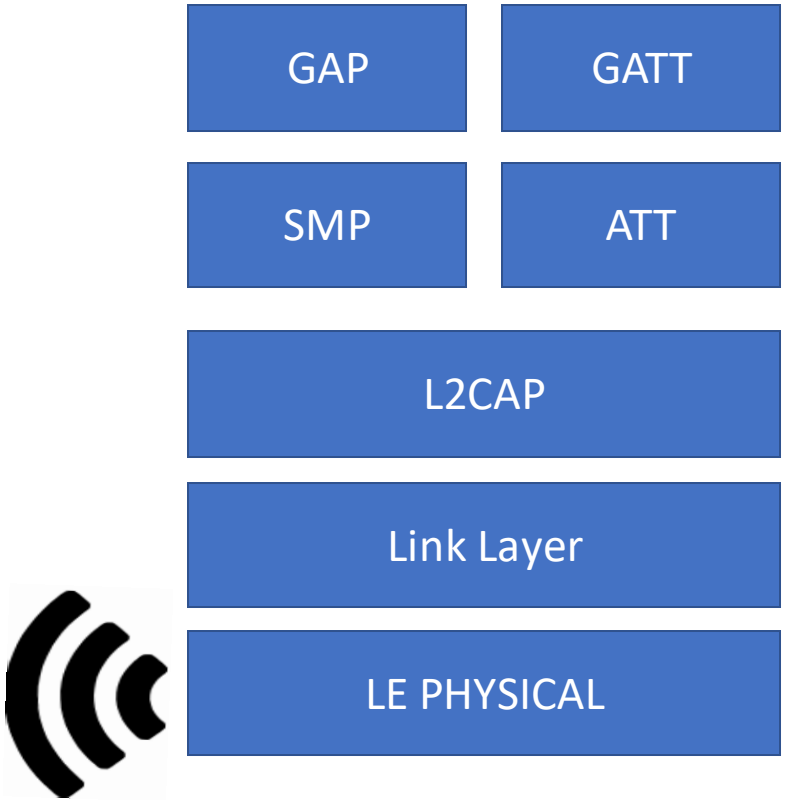
- Peripheral stops advertising after connection request (becomes a slave)
- Slave waits for packets from Master.
  - When received, connection established

Bluetooth LE Device Address

- The Bluetooth ***Device Address*** is a 48-bit (6-byte) number uniquely identifies a device among peers.
  - Similar to an Ethernet Media Access Control (MAC) address
- Think of it as a unique address of a device
- There are two types of device addresses and one or both can be set on a device:
  - Random Address:
    - Random number according to the Bluetooth SIG. Can be static(can only change on power cycle) or Private(resolvable/non-resolvable)
  - Public Address:
    - Calculated just like IEEE Ethernet LAN address

GAP and GATT for BLE

- Generic Access Profile (GAP) or Advertising
  - Information advertised to central before connection
  - Name of peripheral
  - Is it connectable?
  - Supported features (services)
- Generic Attribute Profile (GATT)
  - How to exchange data once connected
  - Identifies Services, Characteristics and Descriptors

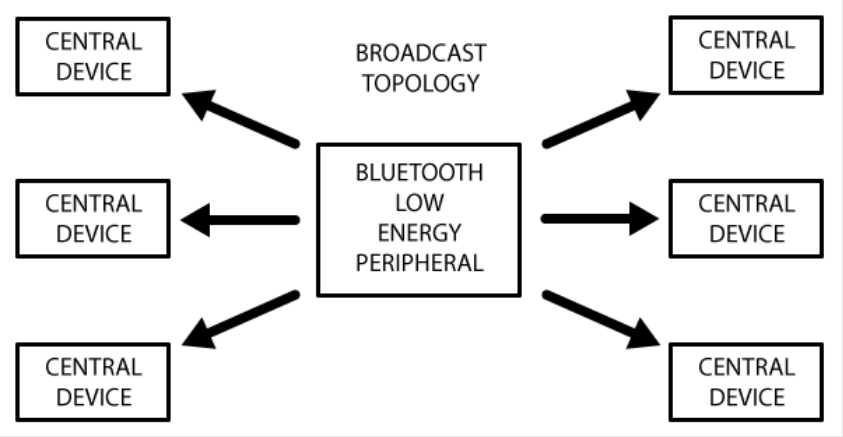


Generic Access Profile (GAP)

- GAP responsible for “device visibility.”
- Determines how two devices can (or can't) interact with each other.
- 2 ways for a device to advertise with GAP
  - *Advertising Data* payload
  - *Scan Response* payload.
- Advertising data payload is mandatory
- Scan response payload is optional
  - allows device designers to fit more information in the advertising payload such a strings for a device name, etc.

Broadcast Network Topology

- Some devices/apps only require advertise data.
  - E.g. app requires peripheral to send data to more than one device at a time.
- Can include small amount of custom data in **31** byte advertising or scan response payloads.
- In this way, BLE peripheral can send data one-way to any devices in listening range
  - BLE Beacons

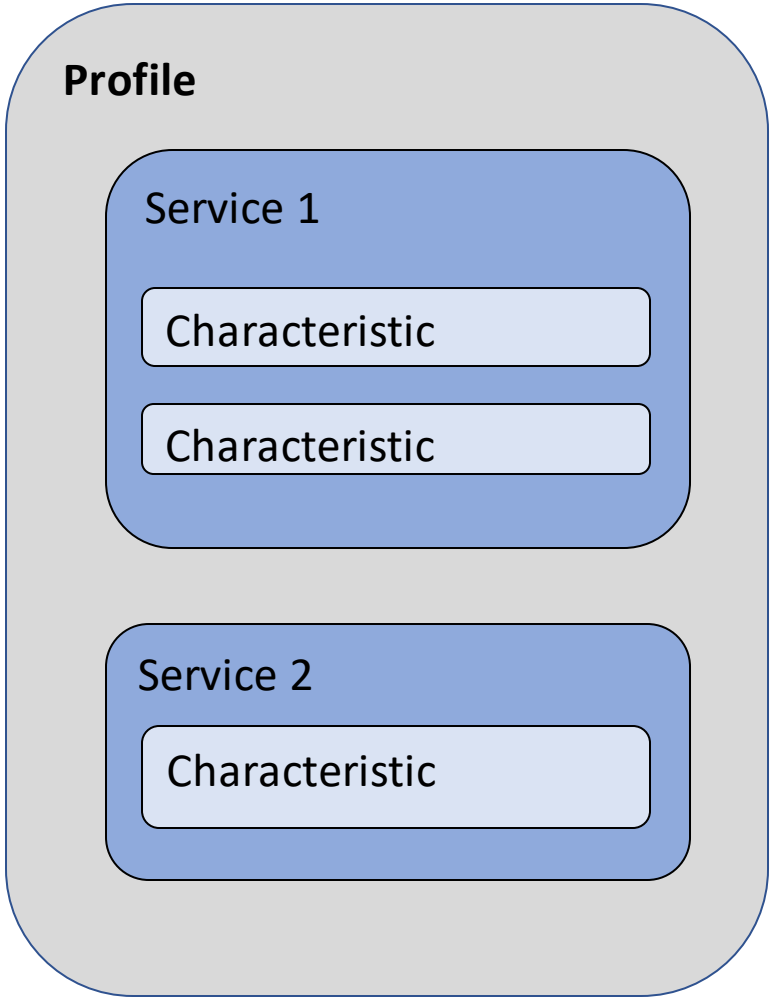


Bluetooth Connection

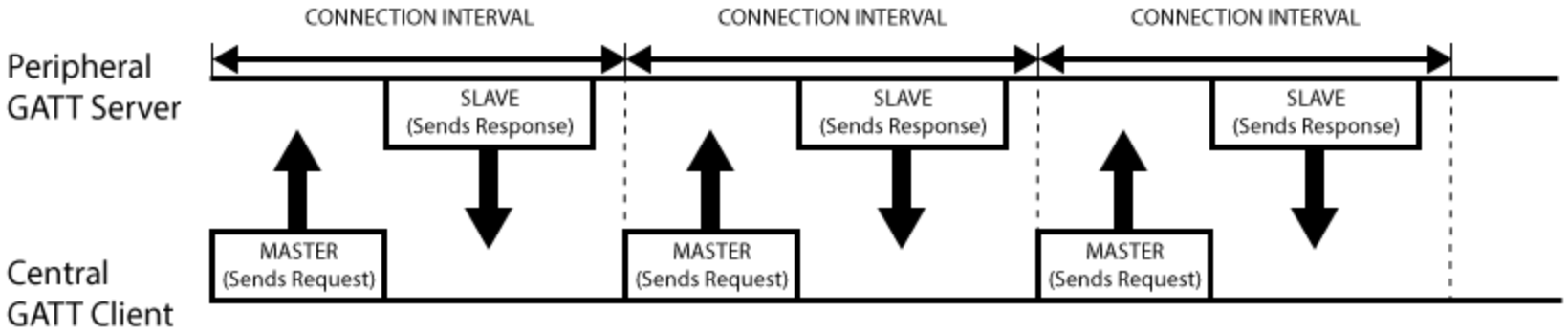
- Establishing a connection between a peripheral and a central device results in 1 to 1 communication
  - the advertising process will stop
  - no longer be able to send advertising packets
- Communication in both directions
- Must use GATT services and characteristics to communicate

Generic Attribute Profile - GATT

- A pre-defined collection of Services that has been compiled by either the Bluetooth Special Interest Group or by the peripheral designers.
  - E.g. The Heart Rate Profile
  - combines the Heart Rate Service and the Device Information Service.
- Complete list of GATT-based profiles can be found here: Profiles Overview
- Defines the way that two Bluetooth Low Energy devices transfer data back and forth
- Uses **Services** and **Characteristics**.
- With GATT, a BLE peripheral can only be connected to one central device (e.g. a mobile phone, etc.)

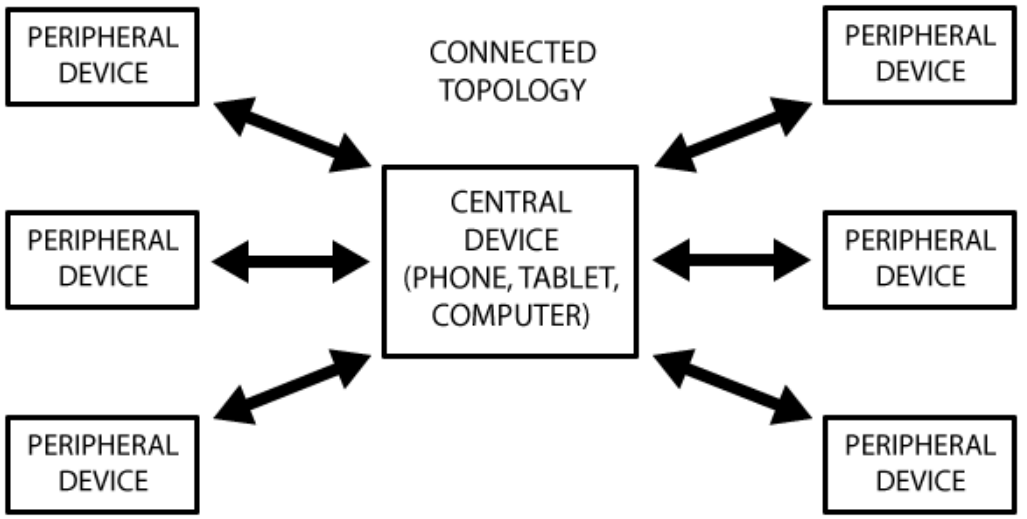


GATT Transactions



BLE Connected Network Topology

- A peripheral can only be connected to one central device
- Communication is **2** -way
- Central device can be connected to multiple peripherals.
- If data needs to be exchanged between two peripherals, a custom messaging system will need to be implemented
  - all messages pass through the central device.



GATT Services

- Breaks data up into logic entities
- Contains one or more **characteristics**
- Each service distinguished by unique numeric ID called a UUID
  - 16 bit
- Set of officially adopted BLE services can be seen on the Services
- E.g. official Heart rate service
  - service has a 16-bit UUID of 0x180D
  - contains up to 3 characteristic
    - ***Heart Rate Measurement***, ***Body Sensor Location*** and ***Heart Rate Control Point***.

GATT Characteristics

- Represents a single data point
- Similarly to Services, each Characteristic distinguishes itself via a pre-defined UUID
  - Also use standard characteristics defined by the Bluetooth SIG
- E.G Heart Rate:
  - the Heart Rate Measurement characteristic is mandatory for the Heart Rate Service
  - Heart rate measurement has UUID of 0x2A37
- If you write apps that use BLE, **characteristics** are what you will be after with your BLE peripheral

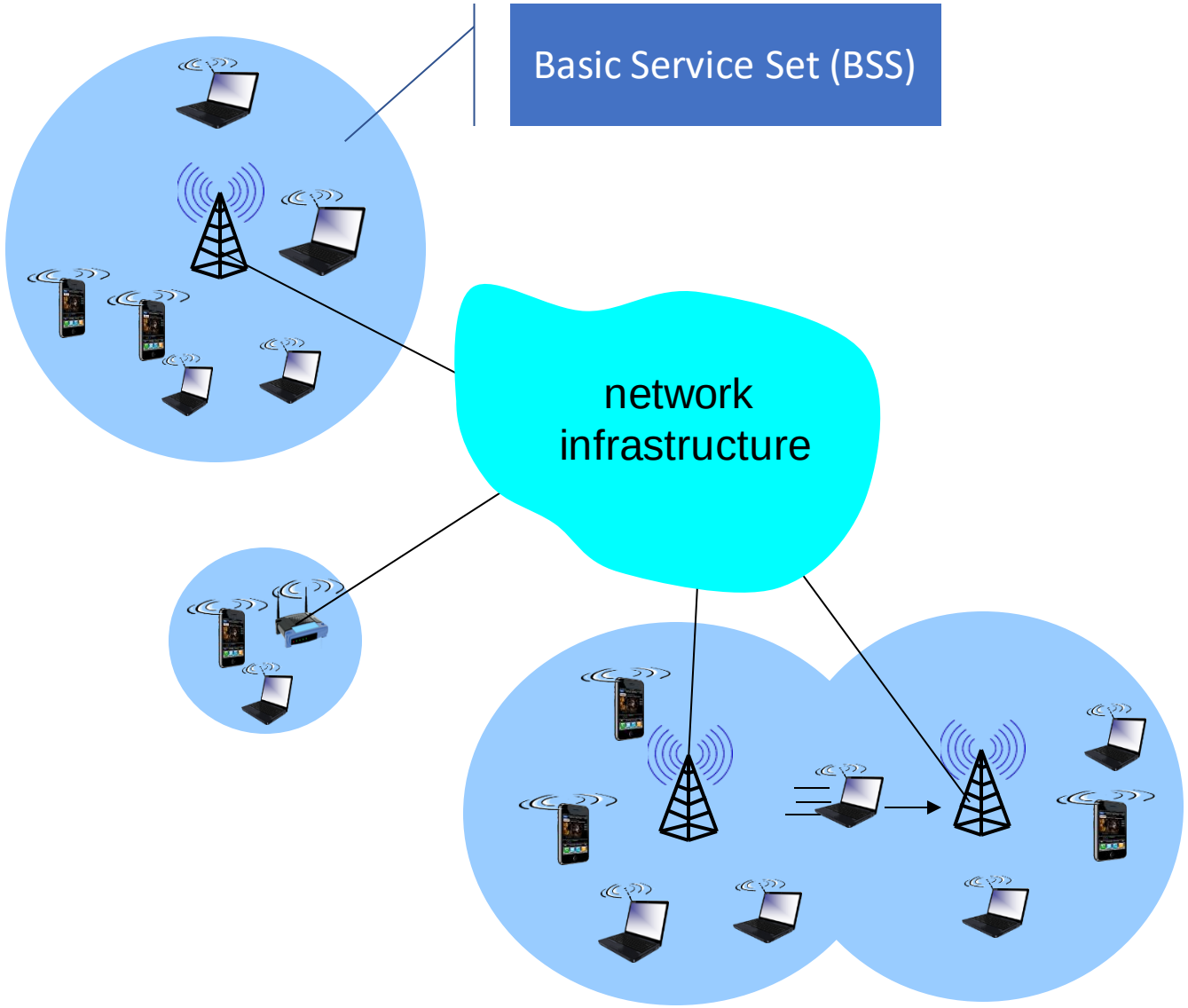
BLE Power consumption

Chipset	Advertising Interval	Est. Battery Life CR2032	Est. Battery Life CR2045	Est. Battery Life CR2477
Gimbal	100ms	n/a	n/a	n/a
Gimbal	645ms	1 month	2.5 months	4.1 months
Gimbal	900ms	n/a	n/a	n/a
Nordic Semiconductors	100ms	1.2 months	3.1 months	5.1 months
Nordic Semiconductors	645ms	7.0 months	18.19 month	29.3 months
Nordic Semiconductors	900ms	11.1 months	28.7 months	46.29 months
Bluegiga	100ms	0.9 months	2.4 months	3.8 months
Bluegiga	645ms	5.9 months	15.4 months	24.8 months
Bluegiga	900ms	9.3 months	23.9 months	38.5 months
Texas Instruments	100ms	0.7 months	1.8 months	2.9 months
Texas Instruments	645ms	4.1 months	10.6 months	17.1 months
Texas Instruments	900ms	5.6 months	14.4 months	23.1 months

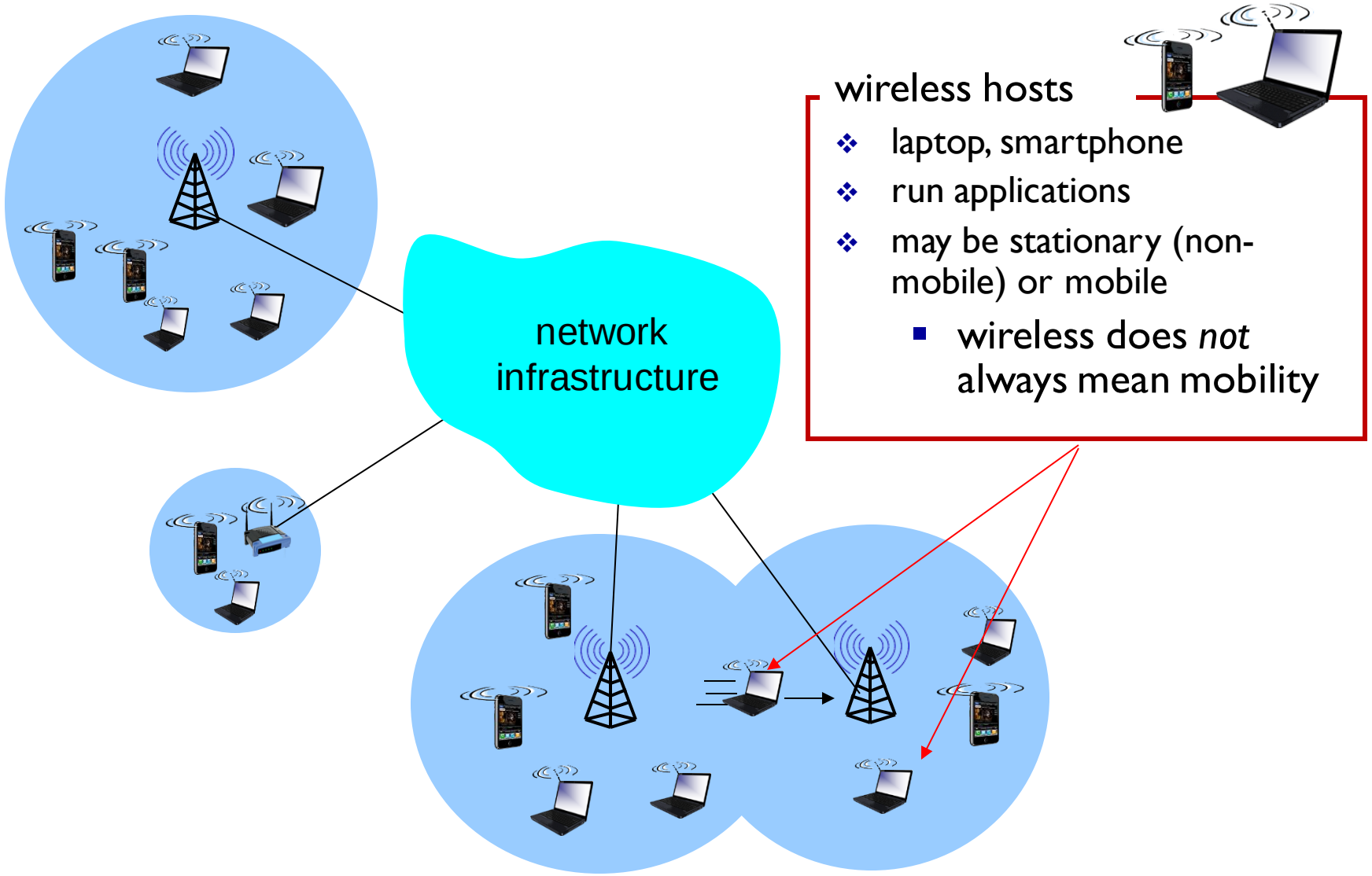
Aislelabs

WiFi

Elements of a Wireless Network



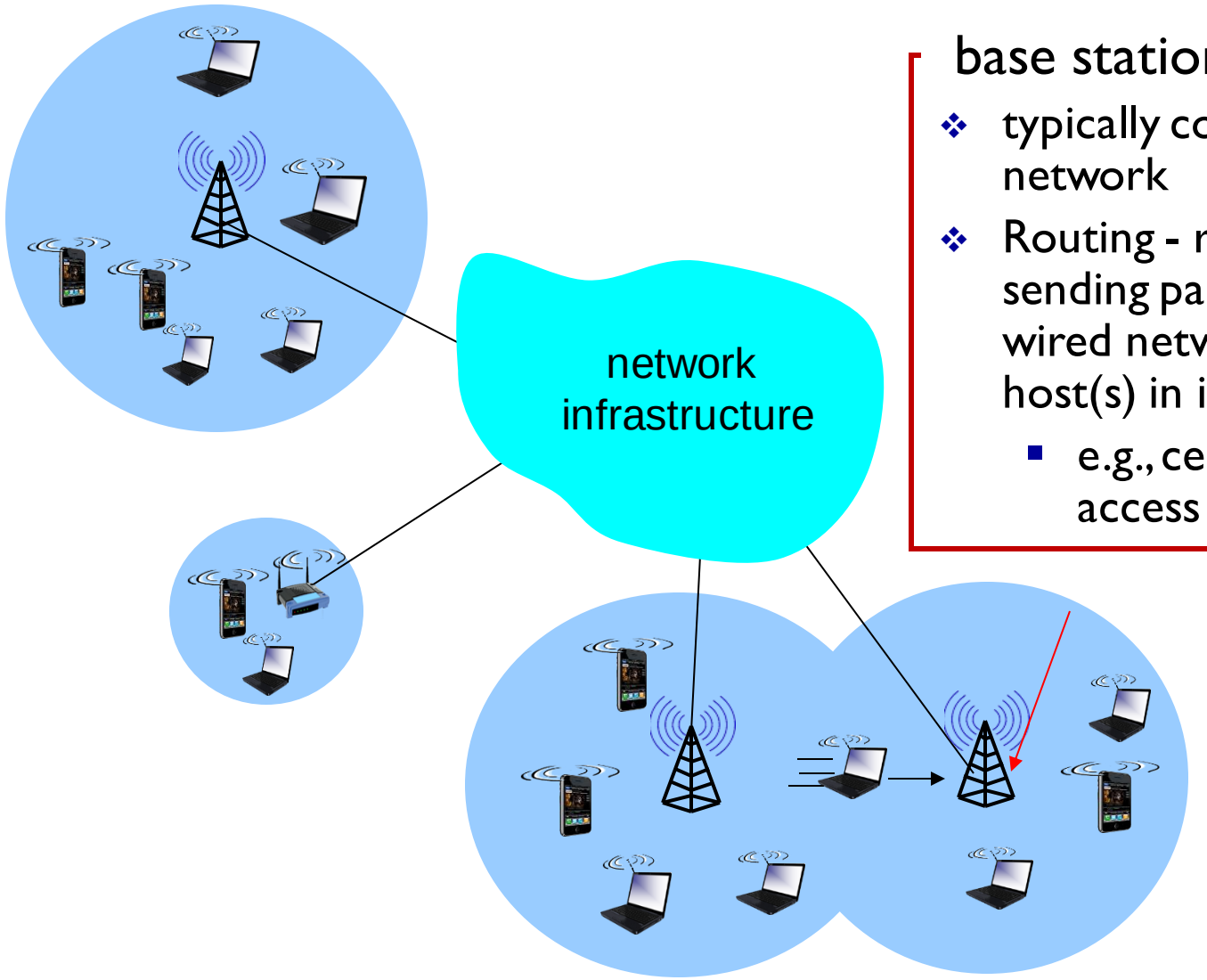
Elements of a Wireless Network



wireless hosts

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

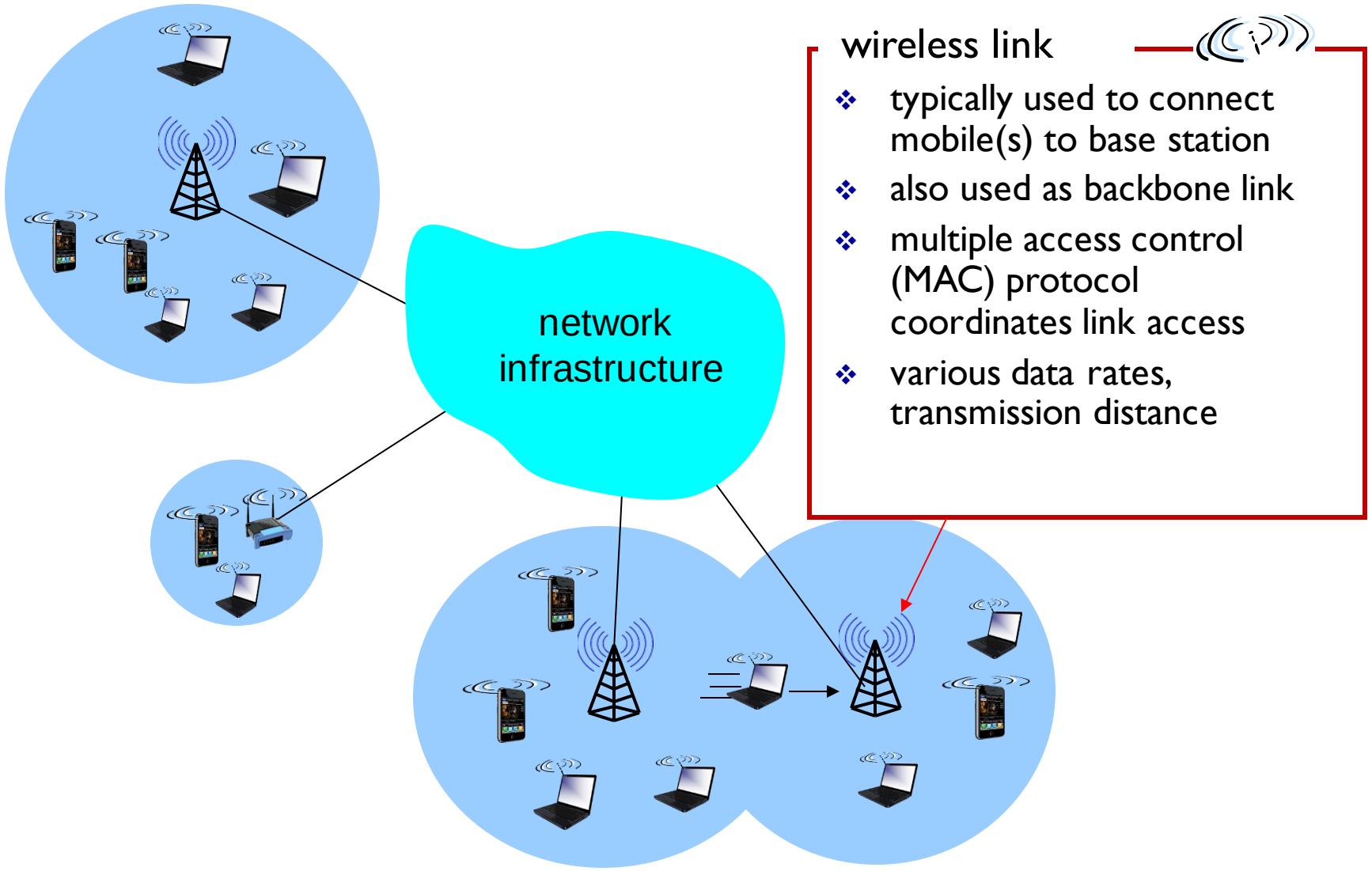
Elements of a Wireless Network



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 link

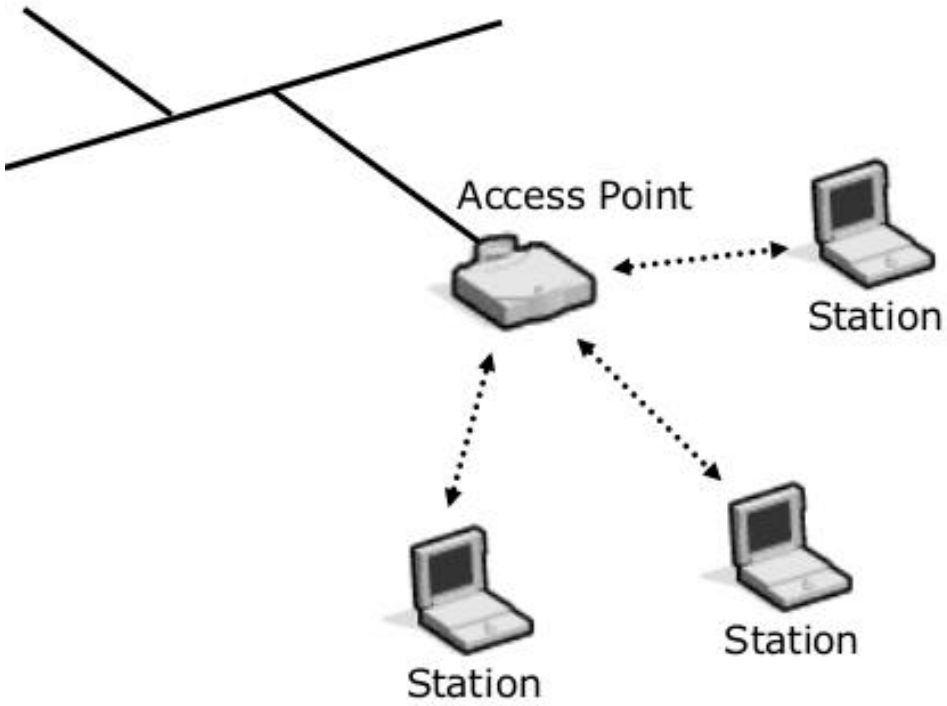
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access control (MAC) protocol coordinates link access
- various data rates, transmission distance

Wireless LAN Technologies and Wi-Fi

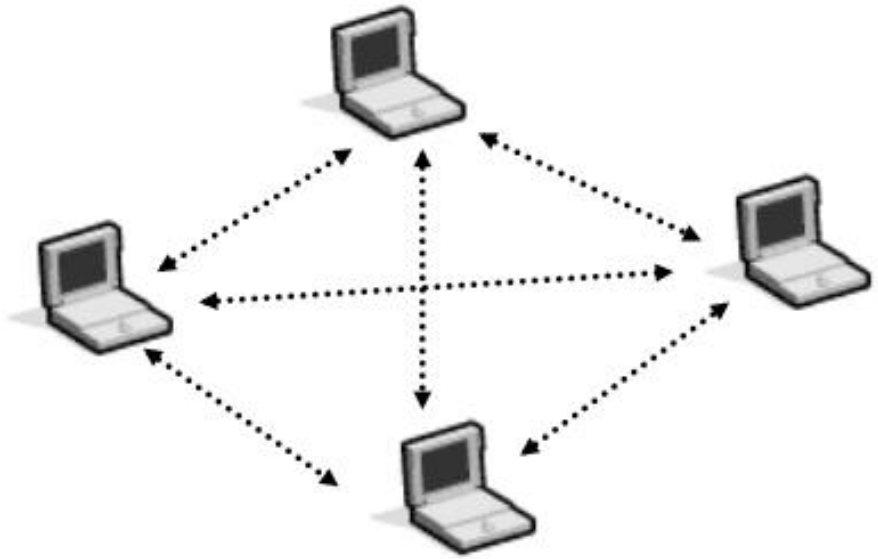
IEEE Standard	Frequency Band	Data Rate	Modulation Technique	Multiplexing Technique
original 802.11	2.4 GHz	1 or 2 Mbps	FSK	DSSS
	2.4 GHz	1 or 2 Mbps	FSK	FHSS
	InfraRed	1 or 2 Mbps	PPM	– none –
802.11a	5.725 GHz	6 to 54 Mbps	PSK or QAM	OFDM
802.11b	2.4 GHz	5.5 and 11 Mbps	PSK	DSSS
802.11g	2.4 GHz	22 and 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



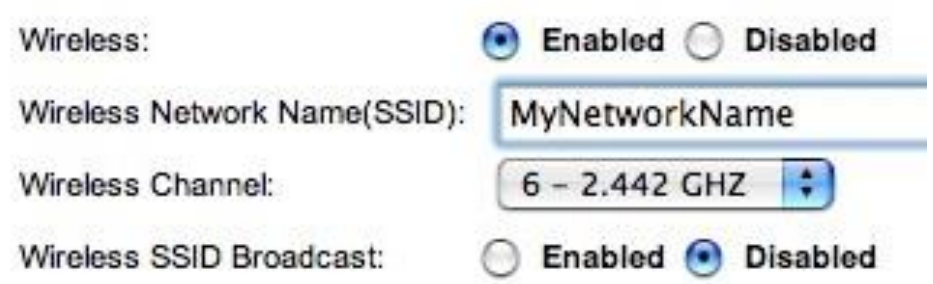
Infrastructure Mode



Ad-hoc Mode

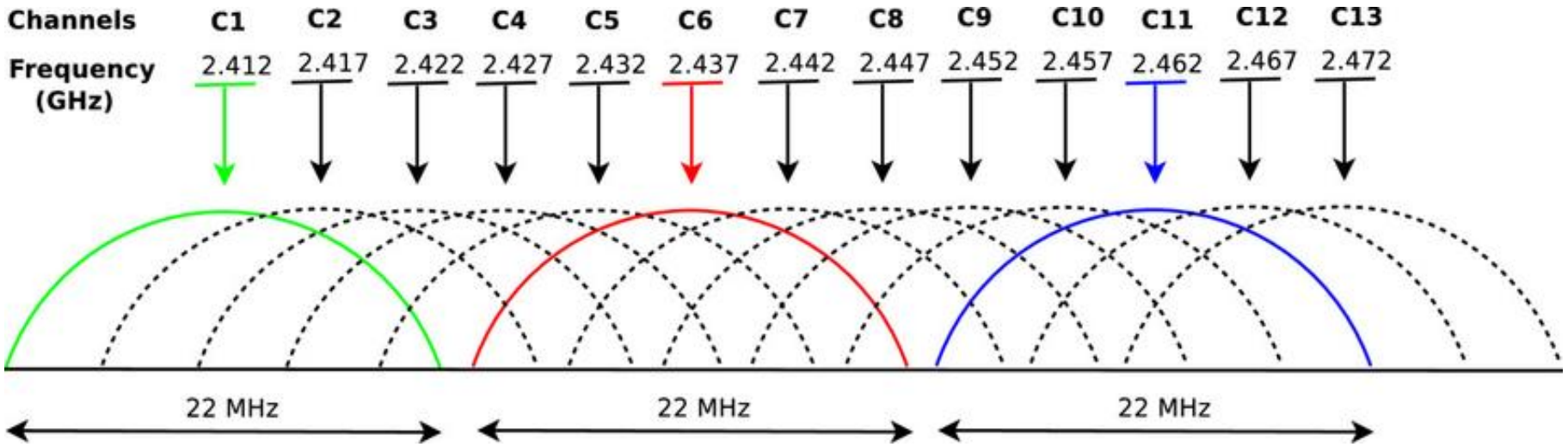
SSID(Service Set ID)

- 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...



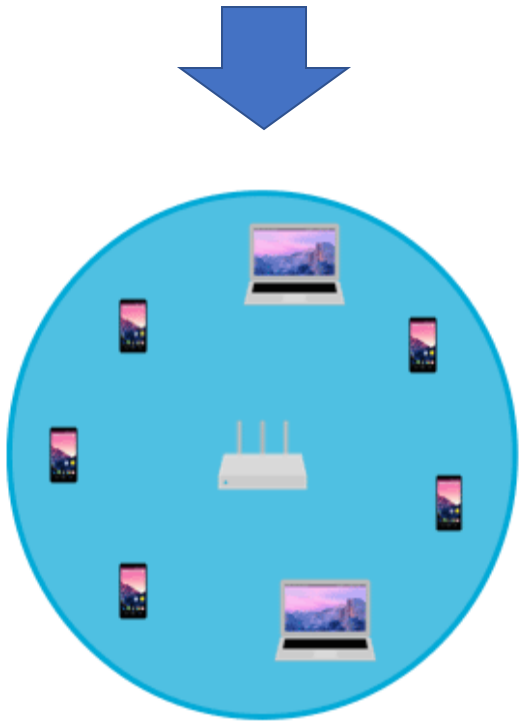
802.11: Channels, association

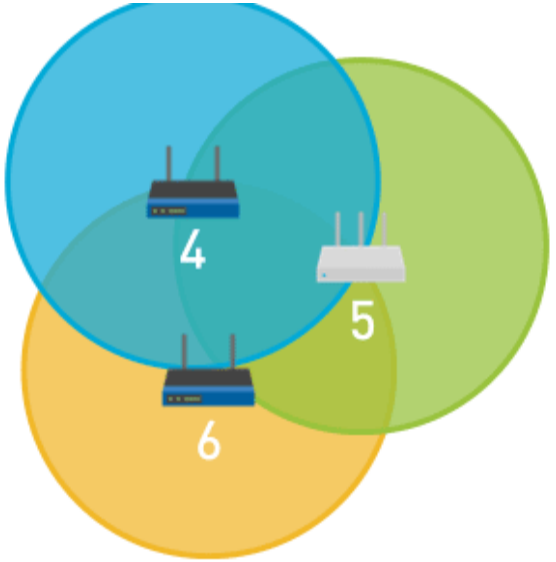
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

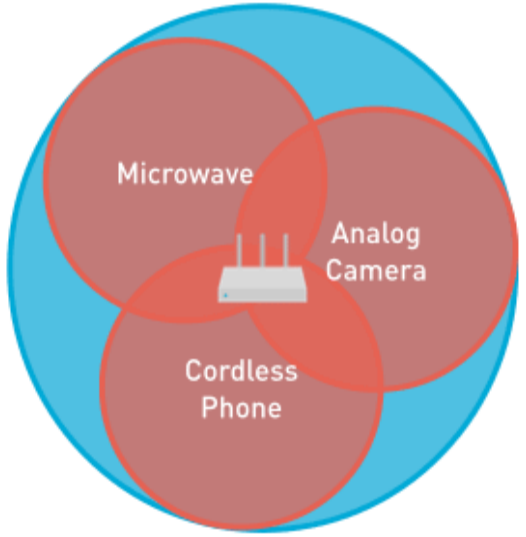


Wireless Network Interference

- 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





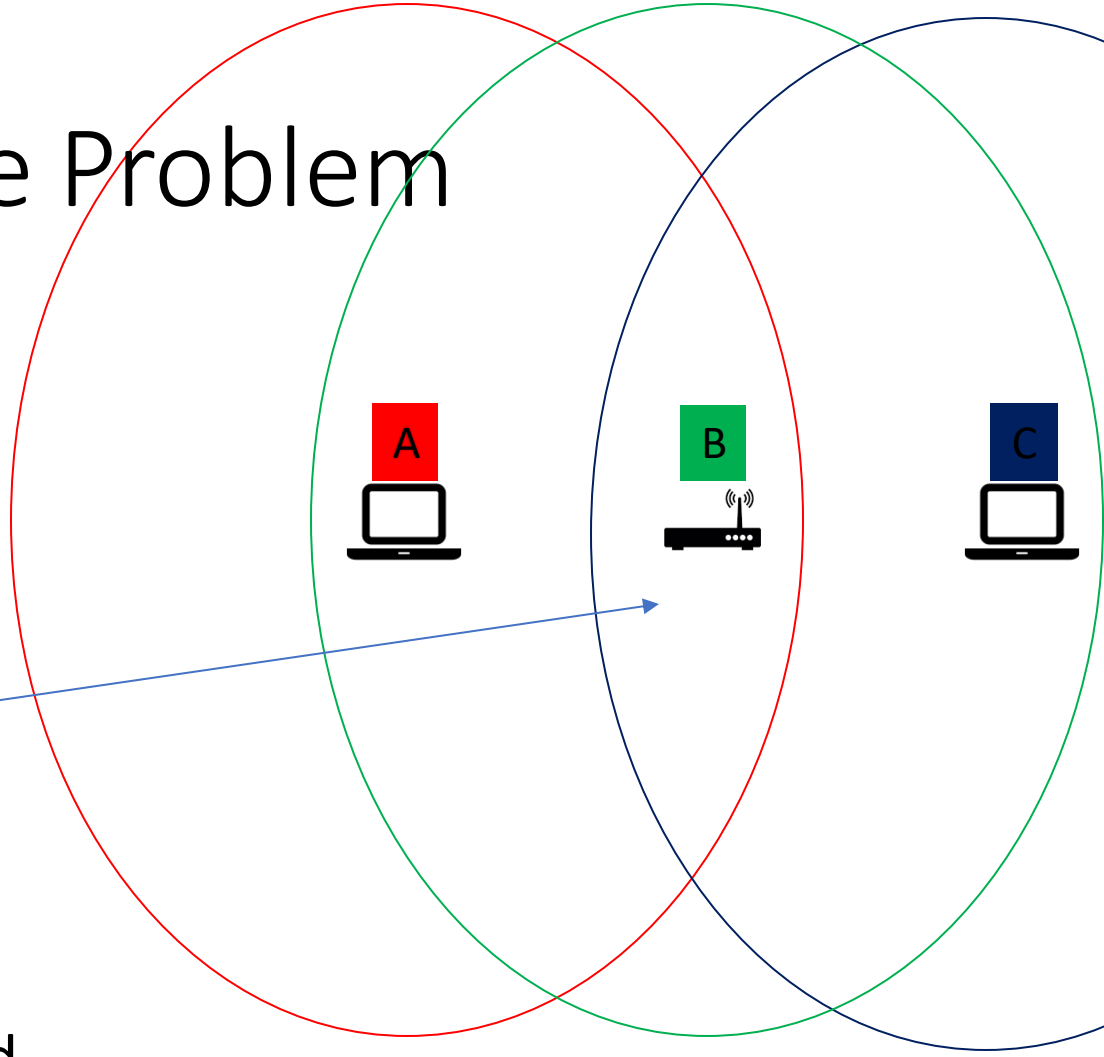


Carrier Sense Multiple Access – Collision Avoidance

- 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

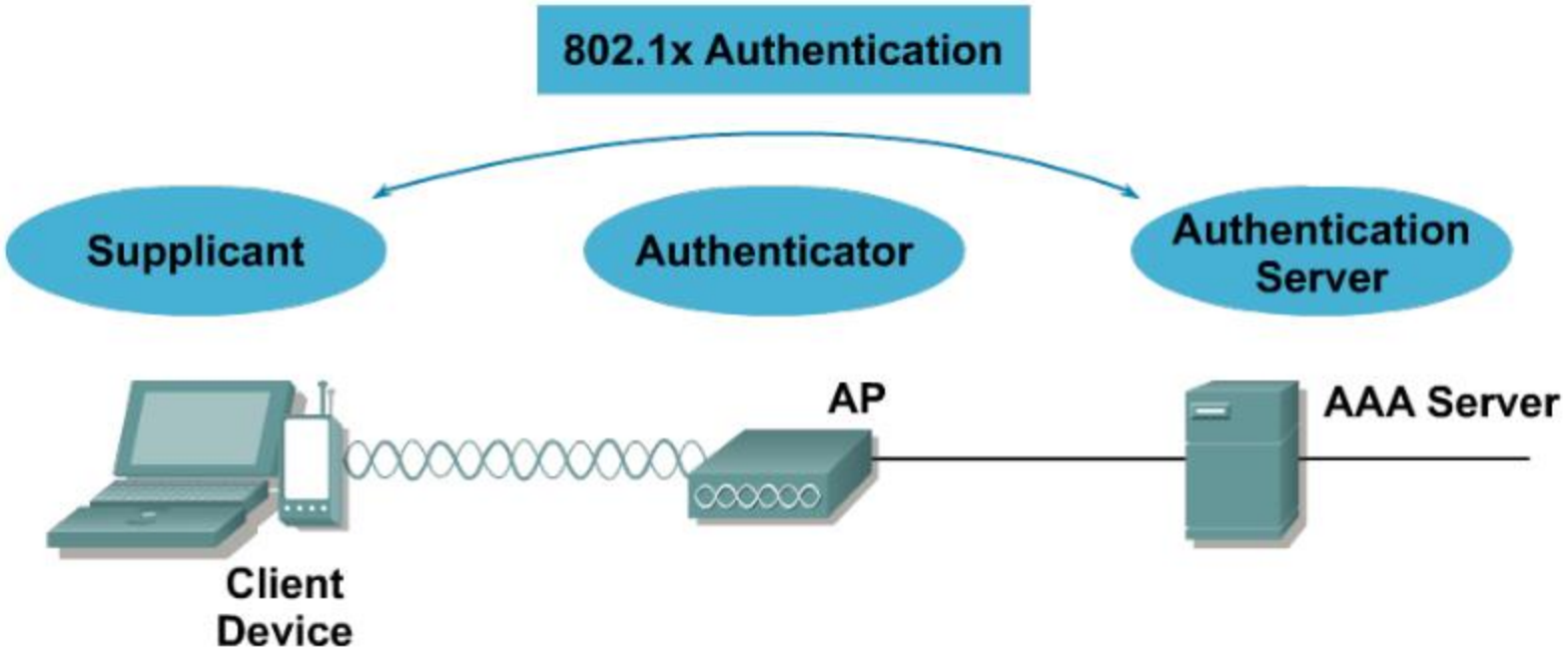
Interference

- 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

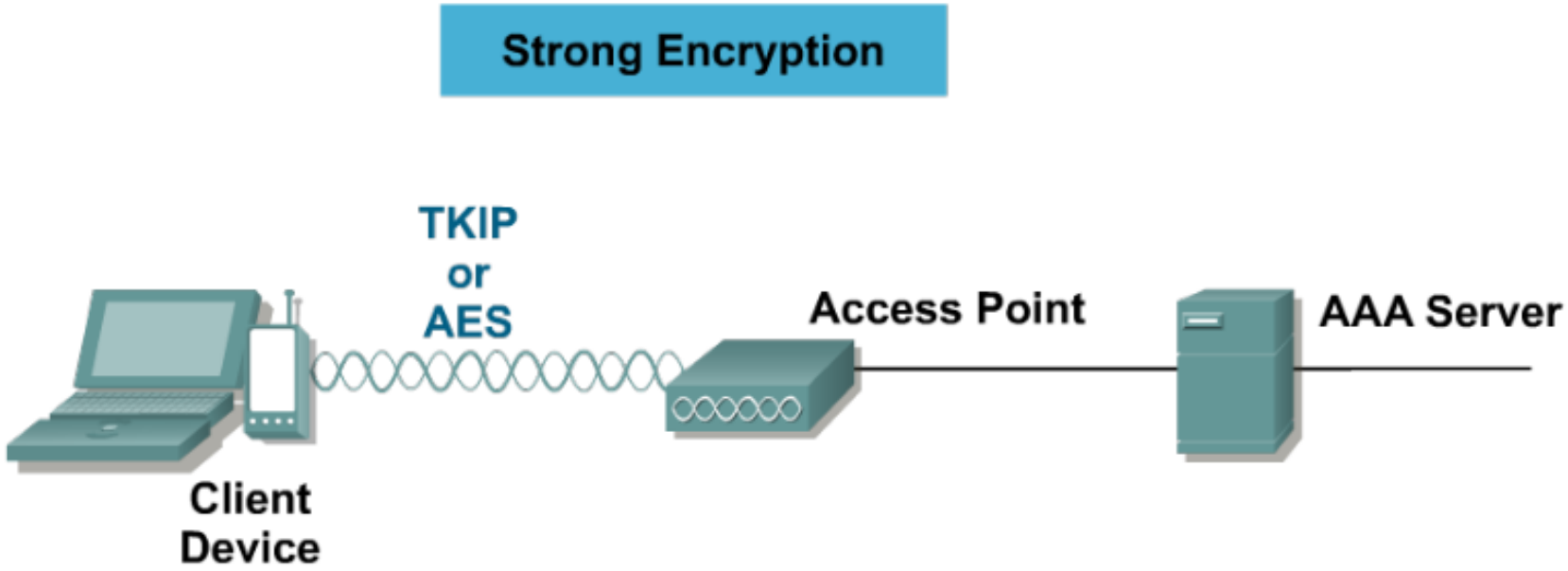
WLAN Security Concerns...

- 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