Wireless and Mobile Networks

INTRODUCTION

- Wireless networks are composed of the relationship between a wireless host, the link and network layers and a device that may be mobile or not
- Wireless devices have the advantage of portability and immediate global access to the internet over their wired counterparts. They also less expensive and easier to install
- The growth of mobile subscribers has from 34 million subscribers in 1993 to 5 billion unique subscribers in 2017 surpassing the amount of wired telephone lines
- Asia Pacific has the highest amount of mobile subscribers with more than half (55%) of the worldwide subscribers being in this area
- 80% of the North American population are part of a mobile subscriber network
- The host, link, base station, and infrastructure of wireless communications are the backbone to wireless networks
- Let’s begin by introducing these topics

Wireless Hosts

- Hosts are the devices that run applications. As stated in earlier chapters, these are laptops, cell phones, computers and tablets. These also can include security systems, power transfers and communication based projects
- However, in the case of wireless networks, the actual hosts are the devices that connect clients to the networks.
- In this case, the clients are the laptops, cellphones etc, while the hosts are routers and switches. Hosts can also be categorized as nodes. All hosts are nodes but not all nodes are hosts.
- Hosts require an IP address to get a connection running

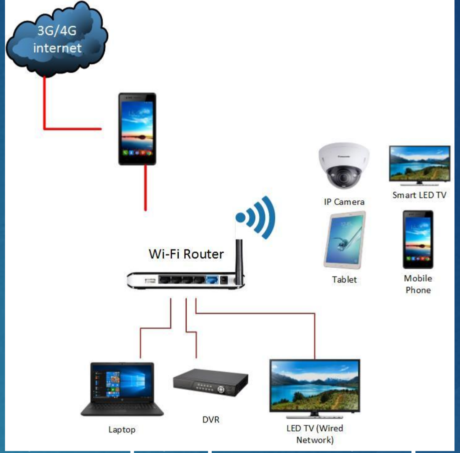
Wireless Links

- A host can connect to another host through a wireless communication link
- Wireless links connect wireless hosts located at the edge of the network into the larger network infrastructure
- Examples of wireless links include satellite transmission, infrared, broadcast radio, microwave and the most familiar, Wi-Fi networks such as 3G or 4G

Base station

- The base station is a short-range transceiver which connects a wireless device to a central hub and allows connection to a network.
- It connects to an antenna that receives and transmits the signals in the cellular network to customer phones and cellular devices
- The base station is important for mobile networks; it allows mobile devices to work properly. If there are not enough base stations in a given area, the service quality decreases.
- Cell towers and access points in 802.11 wireless LANs are examples of base stations

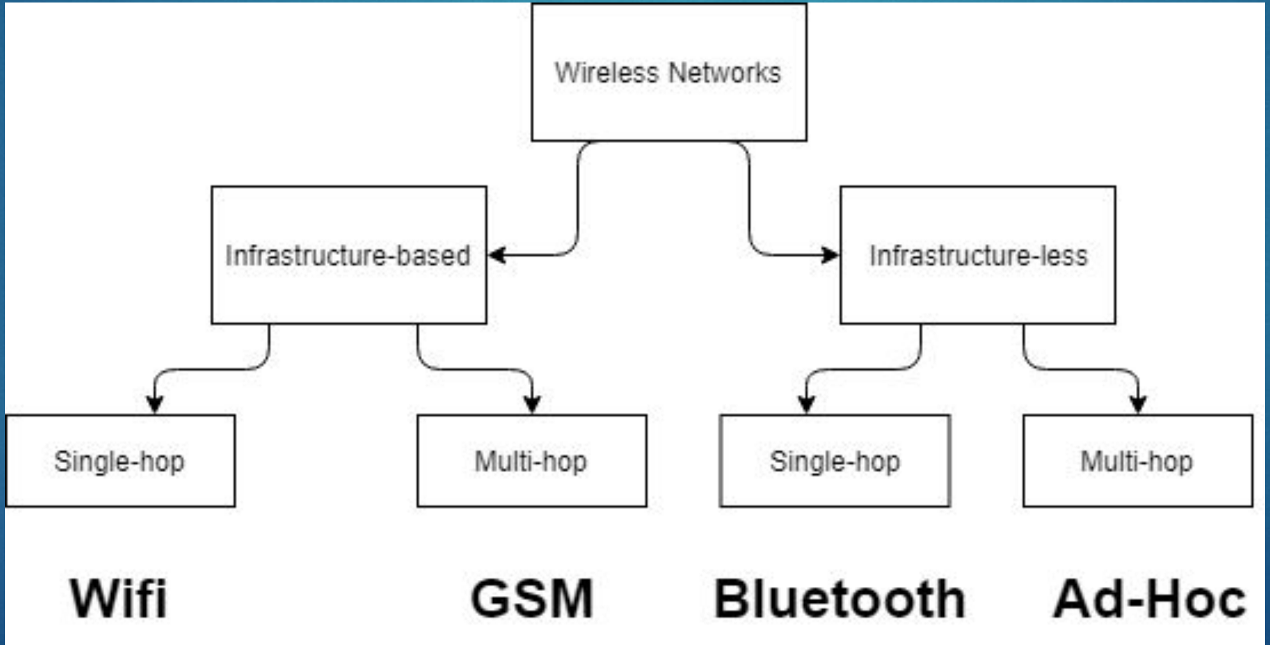
Infrastructure



- The network infrastructure is the larger network in which a wireless host may wish to communicate
- It is the hardware and software resources of an entire network that enables network connectivity, communication, operations and management of an enterprise network
- The host-base station relationship is known as the infrastructure mode
- There are ways for computers to connect to each other without an infrastructure; one method is known as an ad-hoc network. This can be used to share data without access to a wifi network. A user can connect with many other users through ad hoc

Types of Infrastructures

- Just like networks, the types of wireless infrastructures also vary. These can be classified based on number of wireless hops and the availability of an infrastructure



Wired vs Wireless Links

- Wireless Links have the advantage of lower maintenance and installation cost
- Internet can be accessed from anywhere
- Helpful to workers; travelling workers can be in touch with their colleagues from remote locations
- Disadvantages
- Any unauthorized persons can capture wireless signals
- Can be hijacked through security vulnerabilities
- Can lose connection due to interference from other sources
- Can be interrupted or disrupted by unwanted noise

What is Unwanted Noise?

- Unwanted noise is naturally occurring and must be considered when trying to understand signals and transmitted waves
- Every circuit has atoms that vibrate randomly due to temperature; this in turn produces electrical noise
- This is also known as electromagnetic interference when signals are transmitted through environments full of wired lines, equipment and even the sun
- In order to understand this unwanted noise, we use the Signal-To-Noise ratio to calculate unwanted noise.

Signal-To-Noise

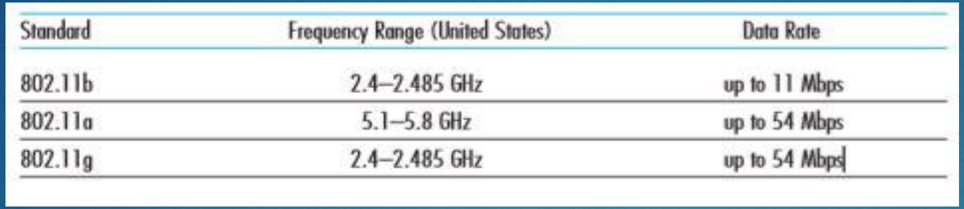
- SNR is the measurement of the strength of a received signal and the unwanted noise
- SNR is measured in decibels (dB) e.x. 80 dB = 8 billion
- The problem is that raw signals and noise values can be measured in units like volts and watts
- We can get the dB units by using the logarithm on the ratio
- Just as the name says, we can find SNR by finding the signal/noise ratio and applying logarithm.
- If the signal values are units of power, we multiply by 20. If they are in units of voltage, we multiply by 10

- TPS:
- We have a scientist that wishes to measure the SNR of 2 carriers
- Carrier A has a noise value is 3 kilovolts while the signal value is 400 millivolts
- Carrier B has a noise value of 2 milliwatts while the signal value is 200 watts
- Find the SNR ratios and determine which carrier has the more desirable signal
- Determine what happens to carrier B. What does the value you've found mean in terms of noise vs signal

WIFI: 802.11 Wireless LANs

- After years of developing many technologies and standards for Wireless LANs dating back to 1990s one made it to the top dues to its effectiveness it is the IEEE 802.11 wireless LANs.
- The reason of its success was because of its Frame Structure, medium access protocol, and its internetworking of 802.11 LANs with wired Ethernet LANs.
- Institute of Electrical and Electronics Engineer(IEEE)

802.11 Wireless LANs Standards

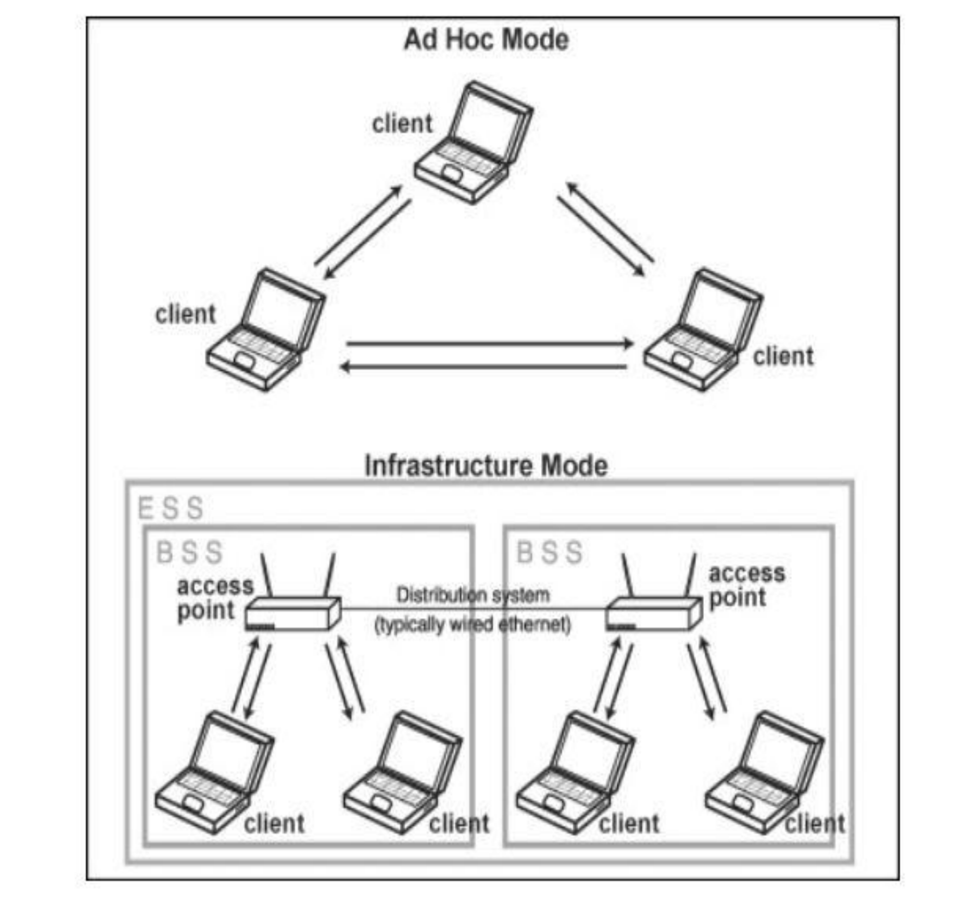


Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

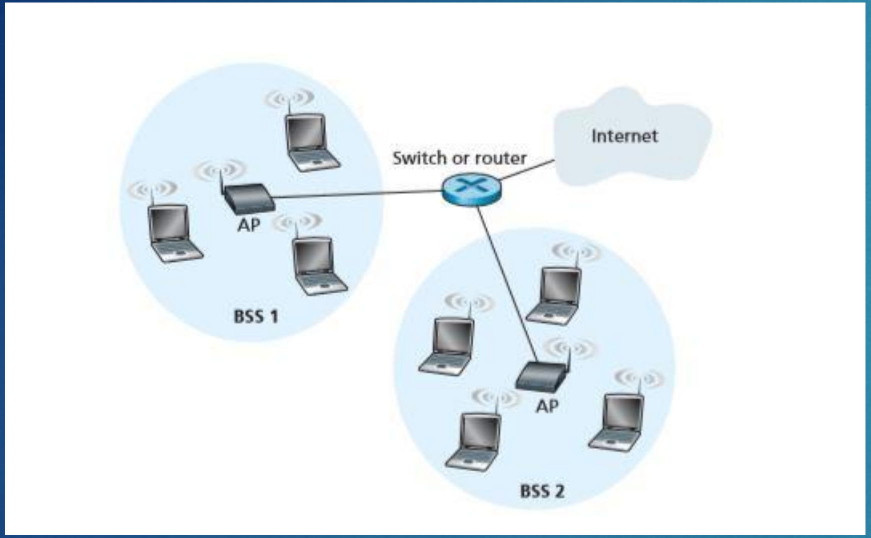
- 802.11b being in the unlicensed frequency band of 2.4-2.485GHz are competing with other devices in the same frequency such as microwave ovens.
- 802.11a can run at a much higher bit rates in order to do so the frequency rate had to be much higher despite the fast rate it suffers on other characteristic such as distances
- 802.11g is on the same frequency rate as 802.11b with the capability to be backward compatible with 802.11b with the data rate of 54mbps.
- All three standards allow for both “infrastructure mode” and “ad hoc mode”
- 802.11g is by the far the most popular standard, despite all three standards sharing the same medium access protocol CSMA/CA, as well as frame structure for the use of link-layer. They can reduce their transmission rate in order to reach out great distances if need be.

Infrastructure mode vs Ad Hoc mode?

- Infrastructure mode are usually connected to the internet via ethernet cables, even on our devices our request for data is sent on the ethernet cable when we are on campus.
- It is usually used in settings where the connection will be needed all year round.(School, Businesses etc.)
- Ad Hoc mode is a peer-to-peer wireless network where computers, tablets, and iPad can communicate with each other via Bluetooth to share data without the use of AP(Access Point). They are usually used for temporary need for a LAN setup that can be deployed quickly.



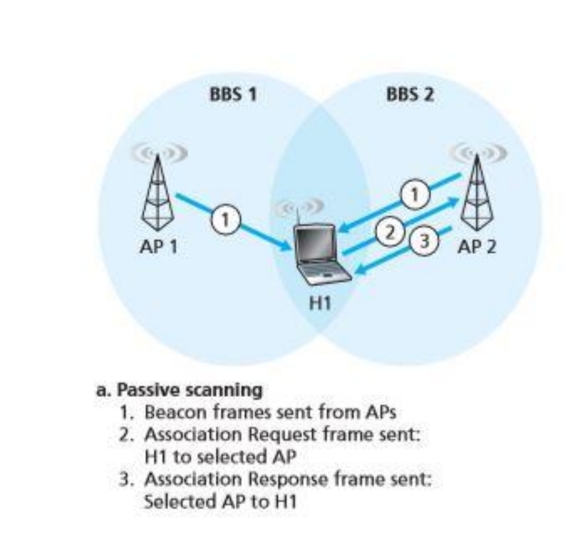
The architecture of 802.11 Standard



- Basic Service Set(BSS) is made up of many wireless stations.
- Access Point(AP) is the central base station of the Basic Service Set.
- Each BSS are connected to an AP in order to gain access to the internet
- Devices that are able to access the internet via "Ethernet" or "Wireless" have a unique MAC address

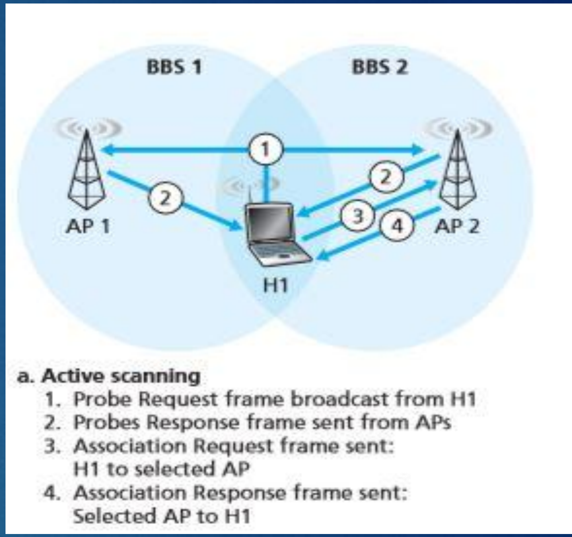
Difference between WLANs Passive Scanning & Active Scanning

Passive Scanning is the process of scanning on a radio listening on every channel for beacons periodically sent by an AP. Passive scans take longer because the client must listen and wait for beacons on every channel



a. Passive scanning
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

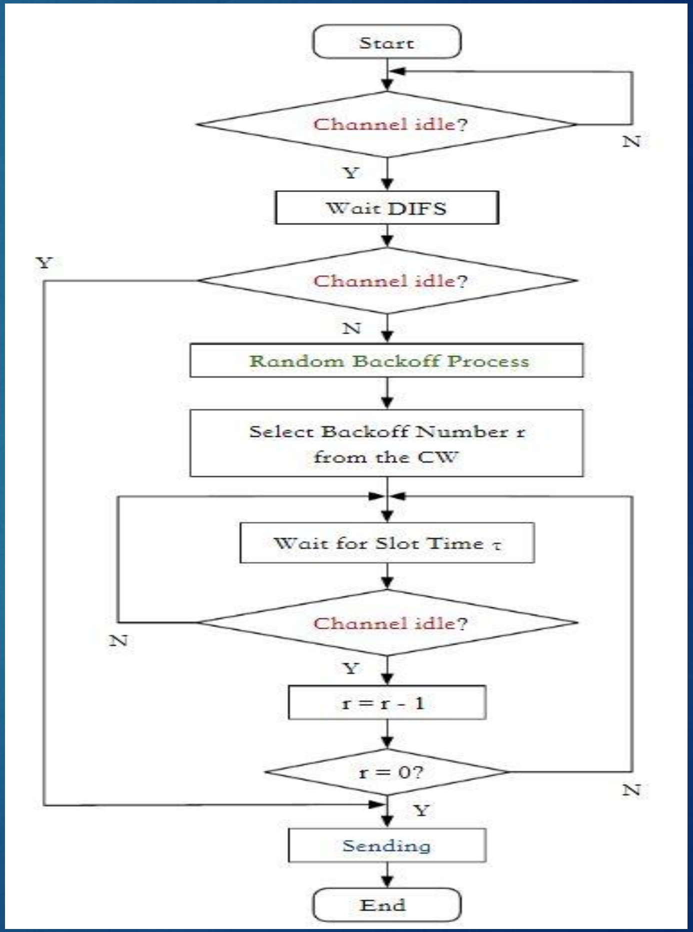
Active Scanning is when a probe request is sent and then awaits response from an AP. Is more effective as you actively look for an AP instead of waiting on every channel for a probe response.



a. Active scanning
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

802.11 Wireless LANs Protocol

- It has many protocols but we will focus on CSMA/CD & CSMA/CA the random access protocols assigned to WLANs.
- CSMA/CD stands for Carrier Sense Multiple Access Collision Detection
- CSMA/CA is Carrier Sense Multiple Access Collision Avoidance
- CSMA/CA is when the channel is checked for data traffic before transmitting a data that needs to be transmitted.
- CSMA/CD are used on early ethernet network which are half duplex using coaxial cable. Must only send data one computer at a time.



CSMA/CA

● Mobility management functions

- A mobile user can also connect to the wireless networks in the office. The wireless network and the home’s ISP address.
- Many people rely on their electronics to surf the web, do schoolwork, contact friends and family as well as for other reasons
- The foreign network assists the mobile node doing mobility management functions working along with the foreign agent.
- The foreign network advertises all networks having the routing infrastructure make a few changes to it

Mobility management functions

- Many of us have wireless applications in our household we use to connect to the internet. One of these products would be the wireless routers.
- The routers help us pass signals in order to connect through the internet.
- Routers can experience signal problems and one of them is comparing to the same channel.
- Products that can interfere with the connection of a router can be a cordless phone or a microwave oven

Mobile IP

- A mobile IP is consisted of three components.
- The mobile node is an electronic device that enables roaming capabilities such as a phone, laptop or headphones as one of the components.
- A home agent is a router that serves up communication in order to keep up with the mobile node.
- The foreign agent is a router that delivers packets as it roams with a foreign network trying to deliver it to the foreign node.

Mobile IP

- The purpose of an IP address is to provide identification for a network of machine and also the location of the machine.
- There are two types of IP addresses, one of them is the internet protocol version 4 and the internet protocol version 6.
- The IPV4 is still used today that has a 32 bit number and it was one of the first ones introduced. The IPV6 was the one that came out recently in 1995 that has 128 bits.
- It is recommended that you have a unique IP address because it provides reliability and security.

Mobile IP

- The way a mobile IP works is the process of going through three stages that are agent discovery, registration and tunneling.
- The agent discovery is where the home agent and foreign agent advertises their services to the router discovery protocol. This is where the mobile node determines if the advertisement belongs to a home network or a foreign network.
- A second phase of how Mobile IP works is where the mobile node is connected to the home IP address and the network access identifier.
- The last phase is tunneling where the mobile node uses the home IP address to send packets to the foreign agent trying to get it to the corresponding node.

Types of Wireless Networks

- Due to the different types of connections, networks can be split into categories that can vary depending on range coverage
- WPANS are the shortest ranged and stands for Wireless Personal Area Networks. These allow connections within a small area. These include Infra Red and Bluetooth
- WLANS are the next step up and what we are probably most familiar with. This stands for Wireless Local Area Networks and allows connections in local areas such as libraries and homes. This will be covered later on
- WMANS stand for Wireless Metropolitan Area Networks and covers ranges from building to building in a large area
- WWANS (Wireless Wide Area Networks) cover cities and countries through satellite and antenna systems. This is the worldwide connection