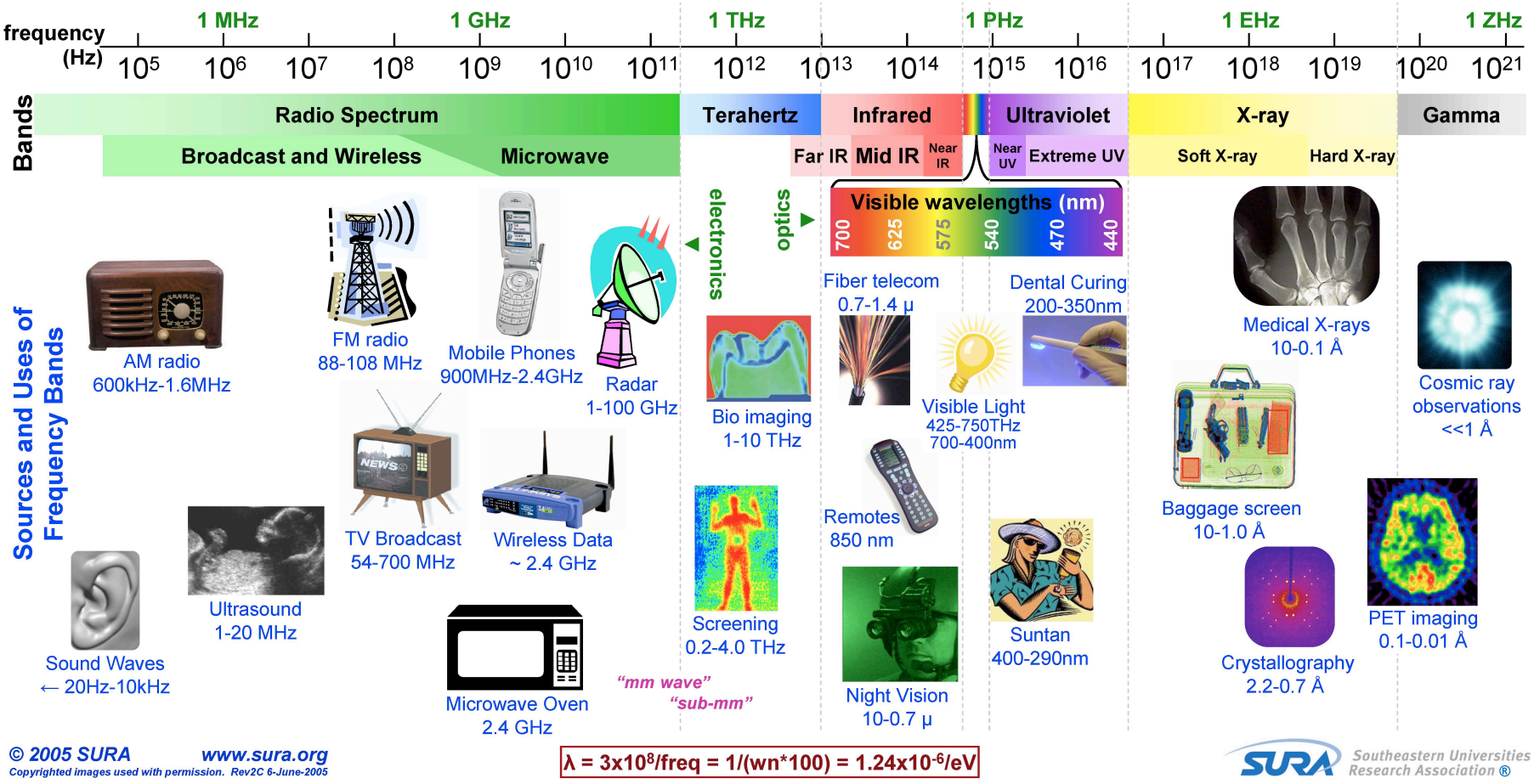
Wireless Networking

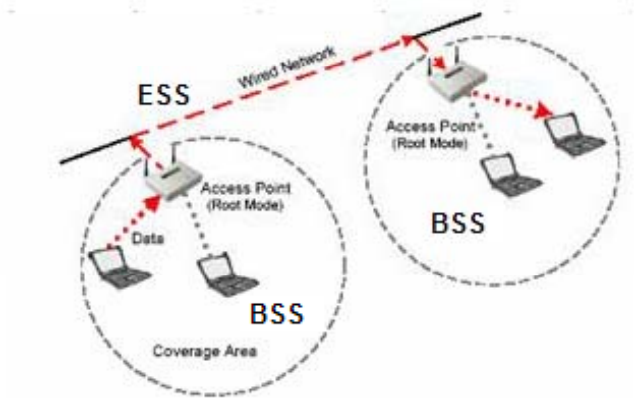
CS 640 2015-02-12 Dale W. Carder

Spectrum

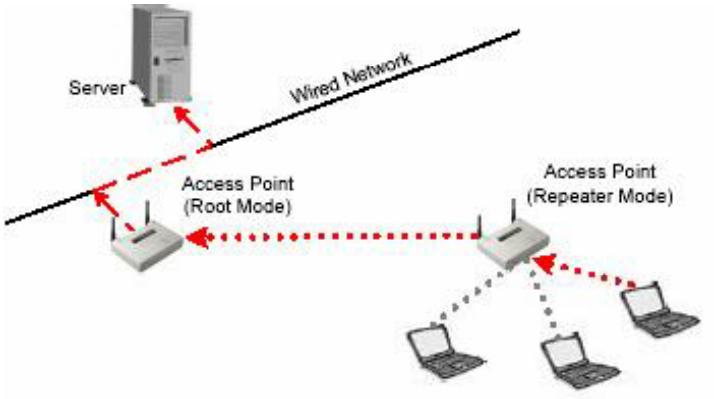


$\lambda = 3x10^8/freq = 1/(wn*100) = 1.24x10^{-6}/eV$

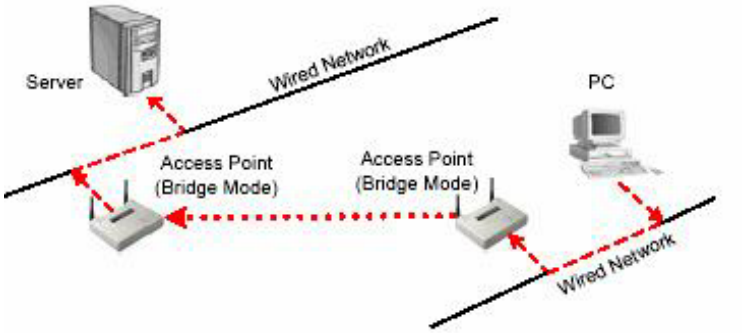
Wireless Network Topologies



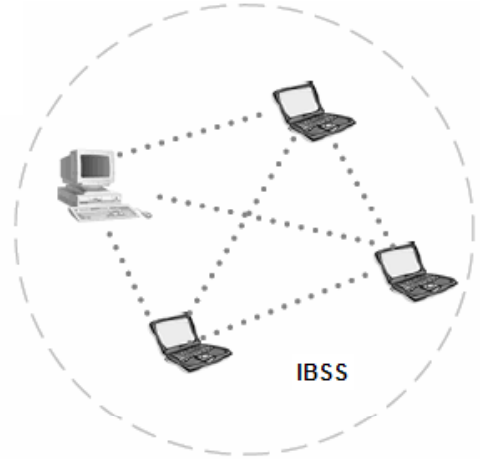
Infrastructure Mode



Repeater Mode



Bridge Mode



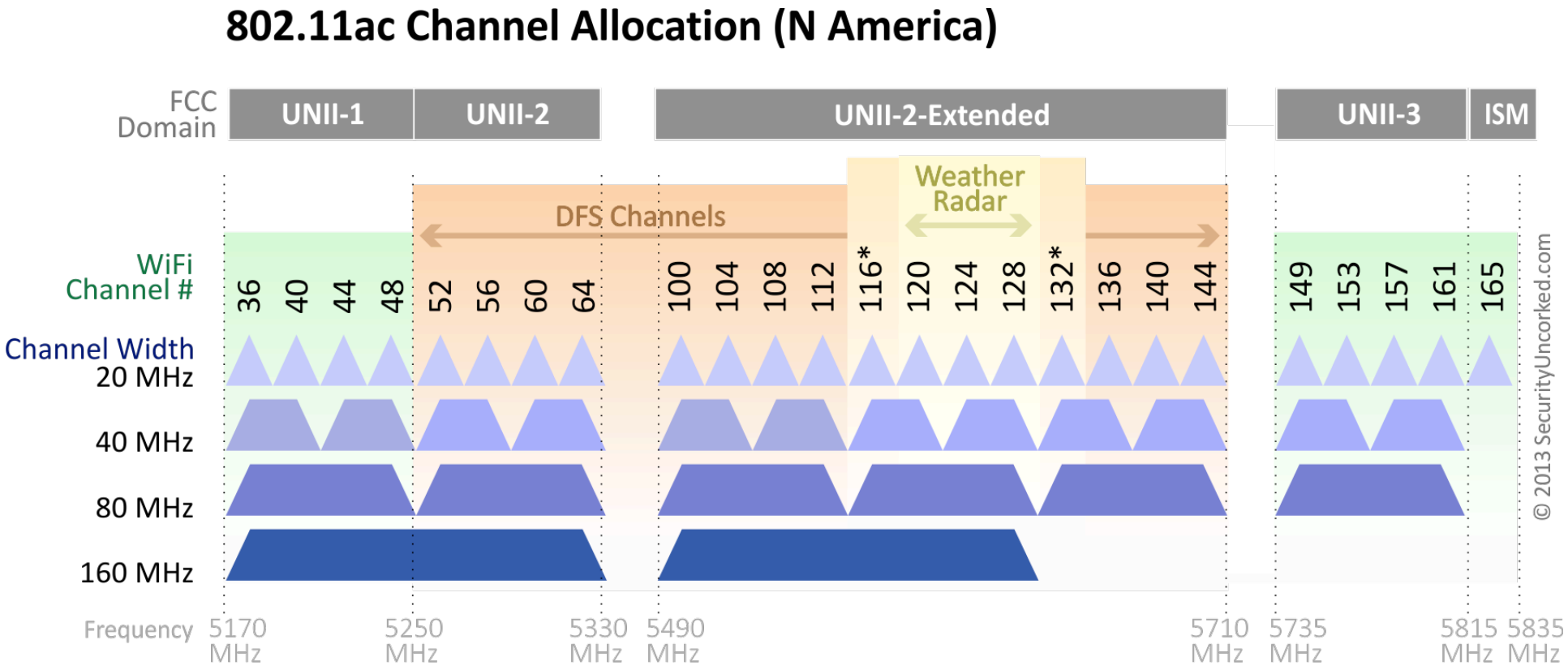
Ad-hoc Mode

veriwave

Also: Cell towers, sensor networks, and so on

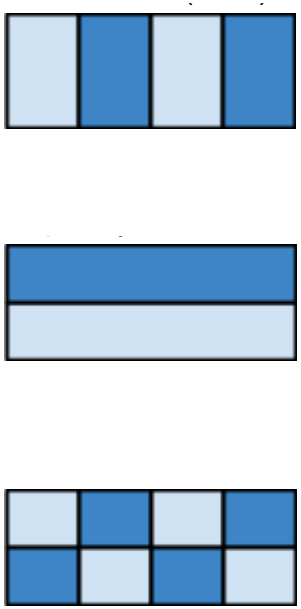
Channel Allocation for WI-FI

- 20, 40, 80, 160MHz channel width defined



*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

Multiplexing



- Time division (TDM) -- each host (or group of hosts) sends at a different time
- Frequency division (FDM) -- each host (or group of hosts) uses a different frequency
- Frequency Hop Spread Spectrum (FHSS) -- each host (or group of hosts) uses a different frequency at a different time
  - Code Division Multiple Access (CDMA) is a specific version of this used in cellular networks

Quadrature amplitude modulation (QAM)

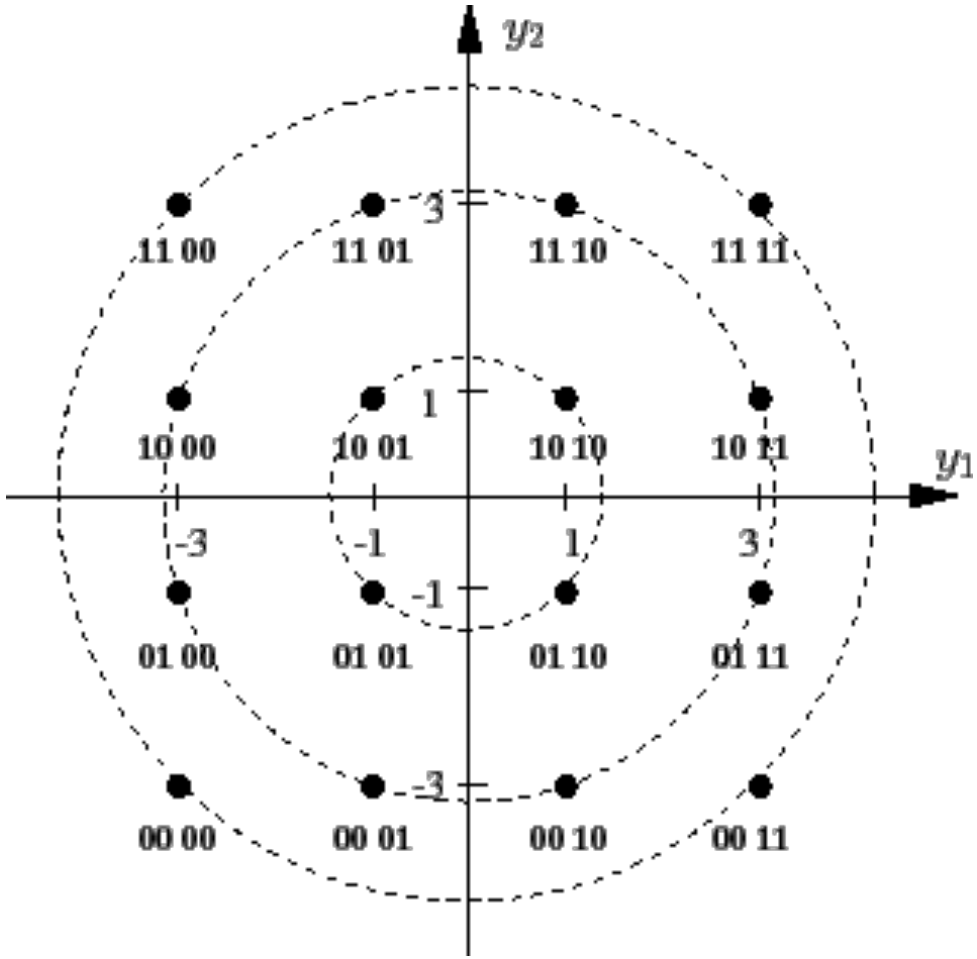
In this example: 16-QAM

1) Encode data into symbols
2) Modulate amplitude (intensity)
3) Modulate phase (angle)
4) Sum it up

Also: 64-QAM, 256-QAM, …

Uses:

- Modern WI-FI data rates
- Digital Cable TV
- Cable Modems
- …even (very sophisticated) fiber optics
- 32768-QAM for DSL, really!



- Higher modulations pack more data into the transmission, but they require much higher signal-to-noise ratios.
- One of the fundamental attributes of an error-correcting code is that it adds redundant information in a proportion described by the code rate.
- A code at rate R=1/2 transmits one user data bit (the numerator) for every two bits (the denominator) on the channel.
- Higher code rates have more data and less redundancy at the cost of not being able to recover from as many errors.
- Modern WI-FI uses 1/2, 3/4, and 5/6

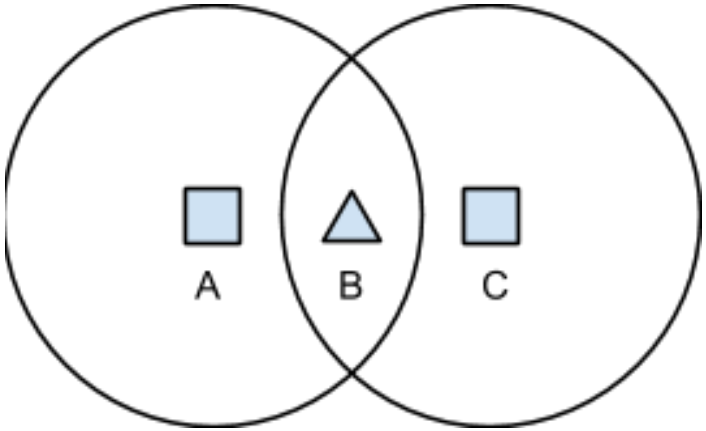
Data Rate all depends on Signal/Noise Ratio

Lots of overhead (as we will see)

Lots of interference, even with error-correction

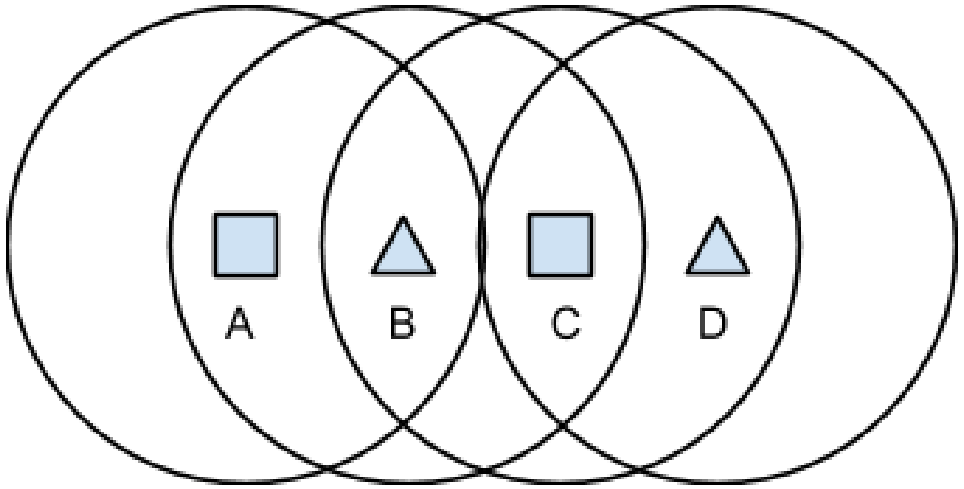
• 802.11	2Mbit/sec	900MHz, 2.4GHz
• 802.11a	2-54Mbit/sec	5 GHz
• 802.11b	2-11Mbit/sec	2.4GHz
• 802.11n	15-135ish Mbit/sec	
• 802.11ac	150-2400ish Mbit/sec	2.4 & 5
• 802.11af		54-698 MHz, sorta
• Cellular 3G/4G		850MHz, 1.9GHz

Hidden node problem

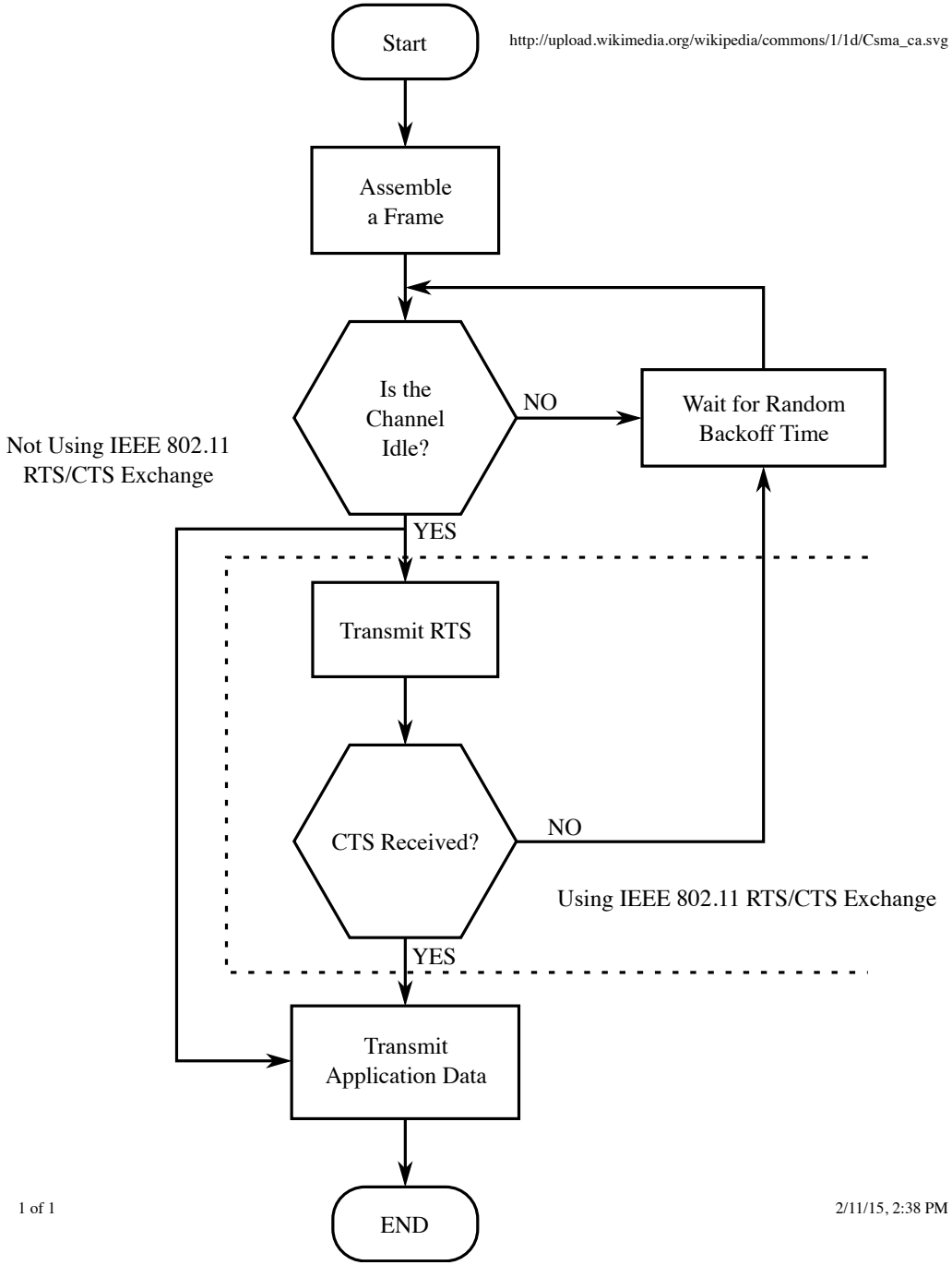


- B can hear transmissions from A and C and vice versa
- C cannot hear transmissions from A and vice versa
- While A is transmitting to B, C may think the frequency is idle and can transmit; however, transmissions from A & C will collide at B

Exposed node problem



- B can hear transmissions from A and C and vice versa
- C can hear transmissions from B and D and vice versa
- While B is transmitting to A, C can hear this and thinks the frequency is not idle; however, C could transmit to D because C's signal does not reach D and would not interfere with A's ability to receive the signal from B



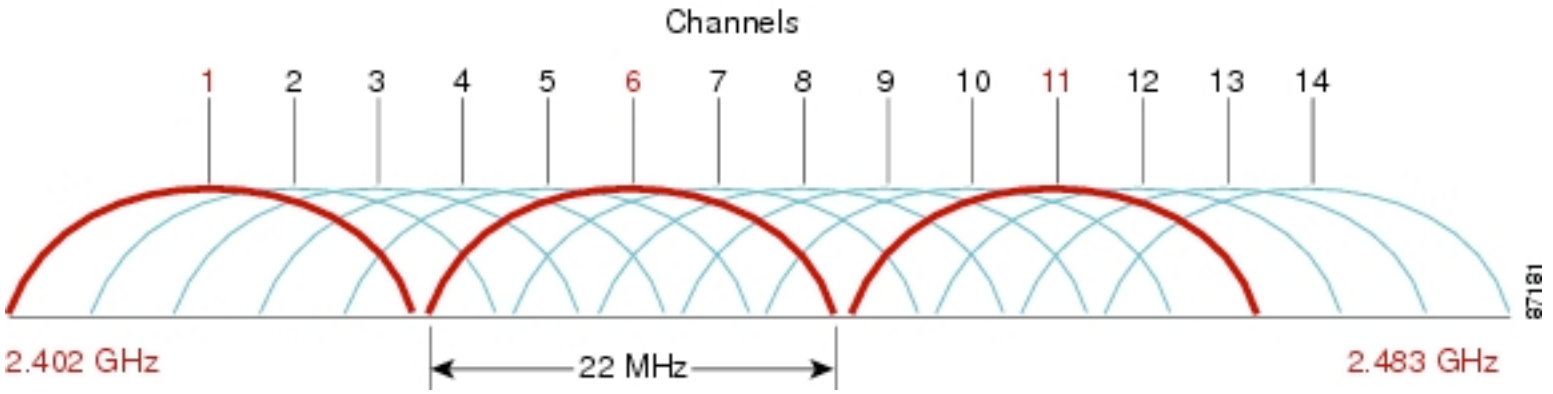
80% Solution:

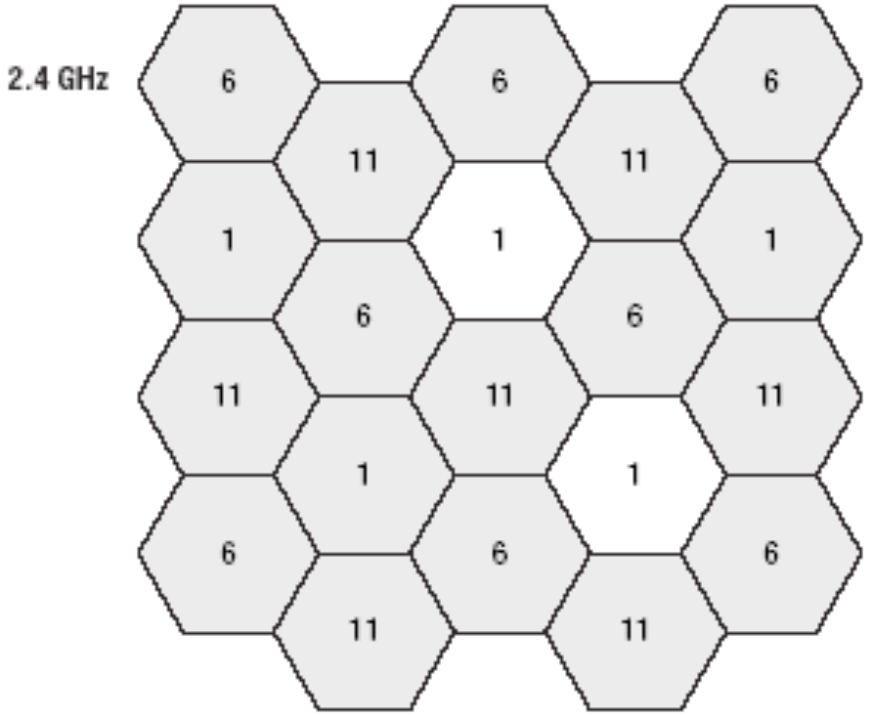
CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance

20% Solution: Prudent Cell Layout

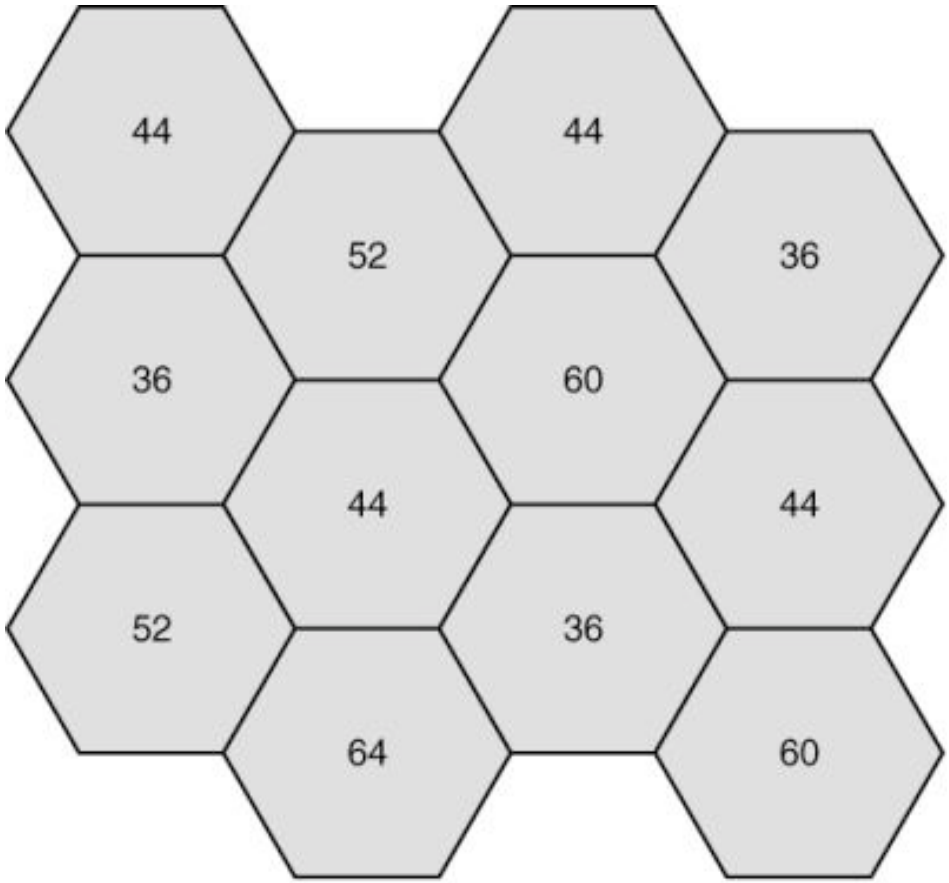
Cell Spacing – 2.4GHz





Images from cisco.com

Cell Spacing – 5GHz



No two adjacent cells use the same channel.

Source: Cisco

Oh, so many Frames

- Management Frames
  - Beacon, Probe Request / Reply, Association Request/ Response
- Control Frames
  - ACK, RTS, CTS, Power Save
- Data Frames
  - Data, Null Data, Data+CF…

- Left as an exercise for the reader

Scanning

- Active scanning
  - Node sends probe
  - AP which receive probe frame reply with probe response
  - Node selects an access point and sends an association request
  - AP replies with an association response
- Passive scanning
  - APs periodically broadcast beacon with SSID (Service Set Identification)
  - Node hears broadcast and sends association request

Roaming

- Process of changing which access point/base station a node is associated with
- Goal is to minimize disruption to connection
- Especially important in cellular networks when call is in progress

- Basic process
  - Node continuously measures signal-to-noise ratio (SNR) for transmissions to/from current AP/base station and decides to switch when threshold is crossed
  - Selects new AP/base station with better SNR
  - Tells old AP/base station that it is moving
  - Associates with new AP/base station
  - In wired back-end, routing is updated to send traffic to new AP/ base station
  - Problems: Crypto, fast movement, large amount of movement

Antennas

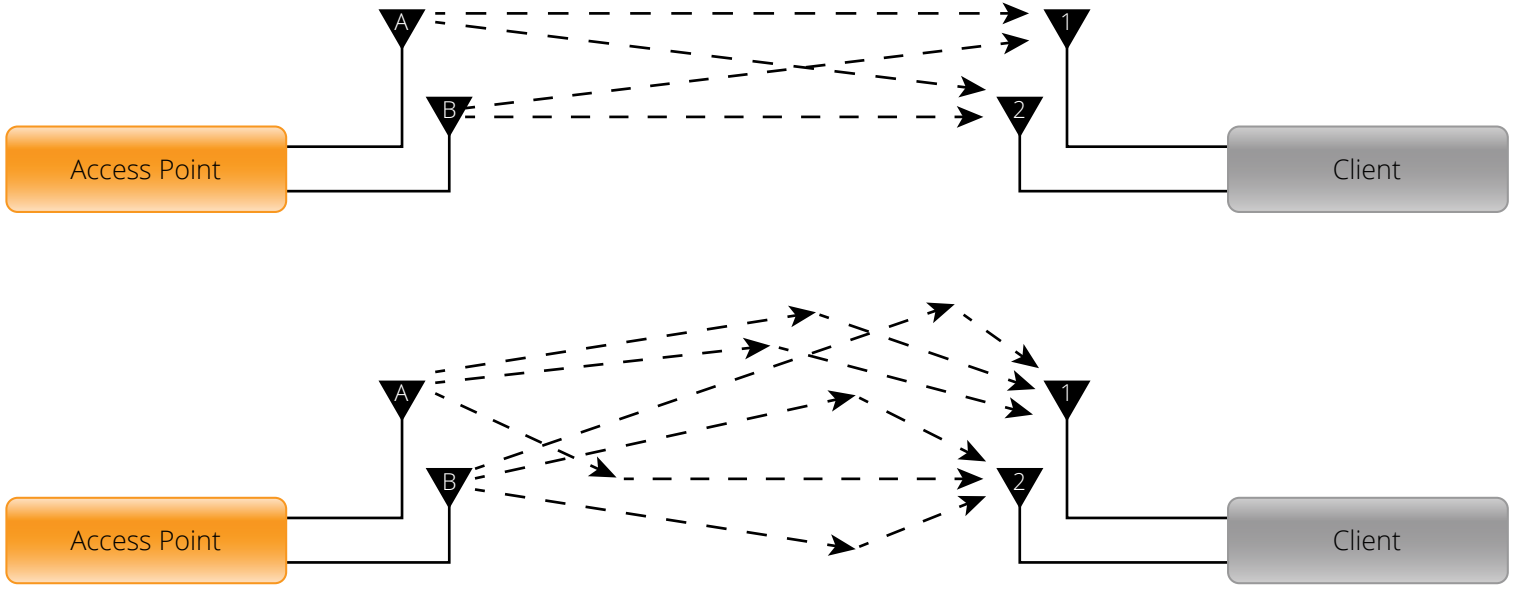
- Antenna / Access Point Placement
- # of Antennas per radio
- Antenna system Diversity

Multi-Input Multi-Output (MIMO)

- Exploit multi-path
- Space Division Multiple Access (SDMA)
- Typical implementations today: 3 spatial streams
- Typically 1←→1 communication, but multi-user (MU-MIMO) on its way.
- Beamforming!

MIMO AND DRIVEN ANTENNAS, 802.11N AND 802.11AC

MIMO WITH LINE-OF-SIGHT AND MULTIPATH, 802.11N AND 802.11AC



Source: Aruba Networks Whitepaper “802.11ac In-Depth”

Power Management

- Negotiate lowest power level possible
- Receive often, but only Transmit in bursts

- AP stores all packets destined to the host in a per-host queue
- Host wakes up, looks at beacon frame to see if it has data, and pulls it down if needed.
- Not awesome for real-time applications (voice). Simple optimization is to use a pre-defined polling interval.

Autonomous AP Challenges

- Managing RF is hard!
- Client devices are unruly
- Need to orchestrate roaming
- Need to fudge multicast & broadcast
- Need to apply sophisticated policy
- At UW:
  - heading towards 6,000+ AP's
  - Less than 1 full-time employee

Centralized Controllers

- Access Points become just virtual ports on a virtual switch
- Encapsulate most (all) traffic to controller
- Apply policy
- Emulate one big, happy network
- Lie to client devices
- Bonus: location tracking! Useful for 9-1-1, inventory systems, intrusive advertisements

Security

- "It seems as if it would be possible for every one who puts up a receiving station to catch the wireless energy and thus to easily steal it"
  - Ivan Narodny, *Technical World Magazine*, October, 1912
- Eavesdropping
- Jamming
- Spoofing

Security Protocol Soup

- WEP-SharedKey
- WPA-PSK
- WPA-EAP/TLS
- DWEP-EAP/TLS
- DWEP-PEAP/MSCHAPv2
- LEAP
- WPA-LEAP
- WPA-EAP/TTLS-GTC
- WPA-PEAP/MSCHAPv2
- WPA-EAP/FAST
- WPA2-PSK
- WPA-LEAP
- WPA2-PSK
- WPA2-LEAP
- WPA-PSK-AES
- WPA-EAP/TLS-AES
- WPA2-PSK
- WPA2-EAP/TLS
- WPA2-EAP/TTLS-GTC
- WPA2-PEAP/MSCHAPv2
- WPA-PEAP/MSCHAPv2-AES
- WPA2-PSK-TKIP
- WPA2-EAP/TLS-AES
- WPA2-EAP/FAST
- WPA2-PEAP/MSCHAPv2-TKIP

This is why we can’t have nice things.

802.1X