Introduction To Data Comm & Networking Module 2 - Wireless

Mr. Donald Privitera

Kennesaw State University

Marietta Campus

College of Computing and Software Engineering

IT Department

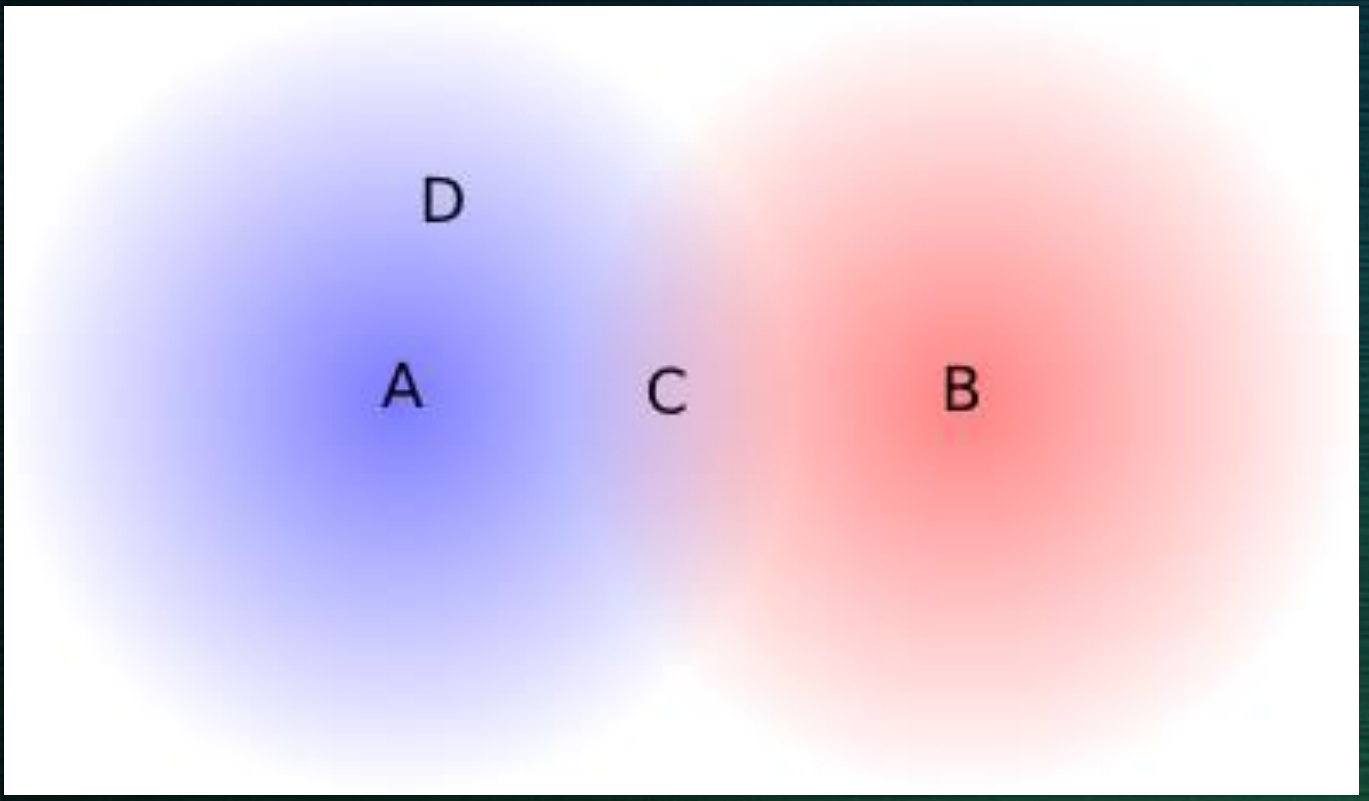
dprivit2@kennesaw.edu

Peter L Dordal, An Introduction to Computer Networks

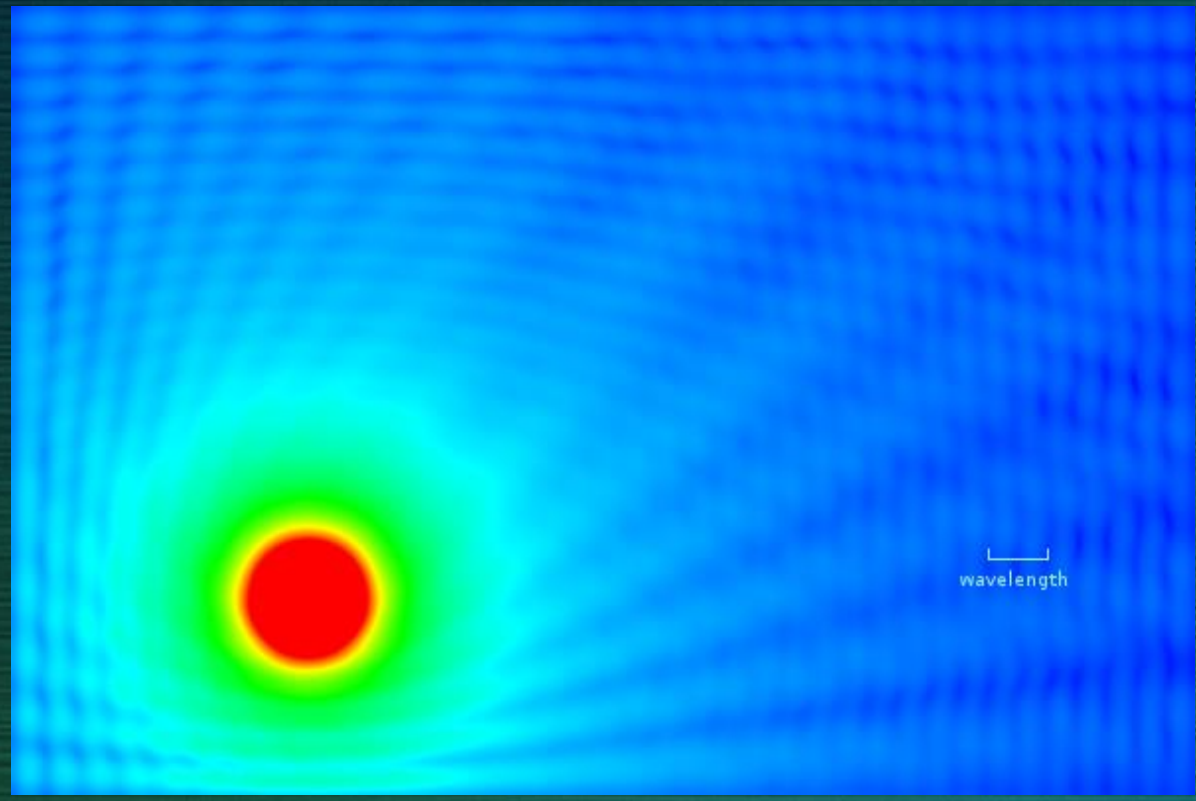
Wireless = Radio = Unguided Media

- Band Width (signal f range) ≠ Bandwidth (data rate)
- Collisions, noise, and interference present challenges

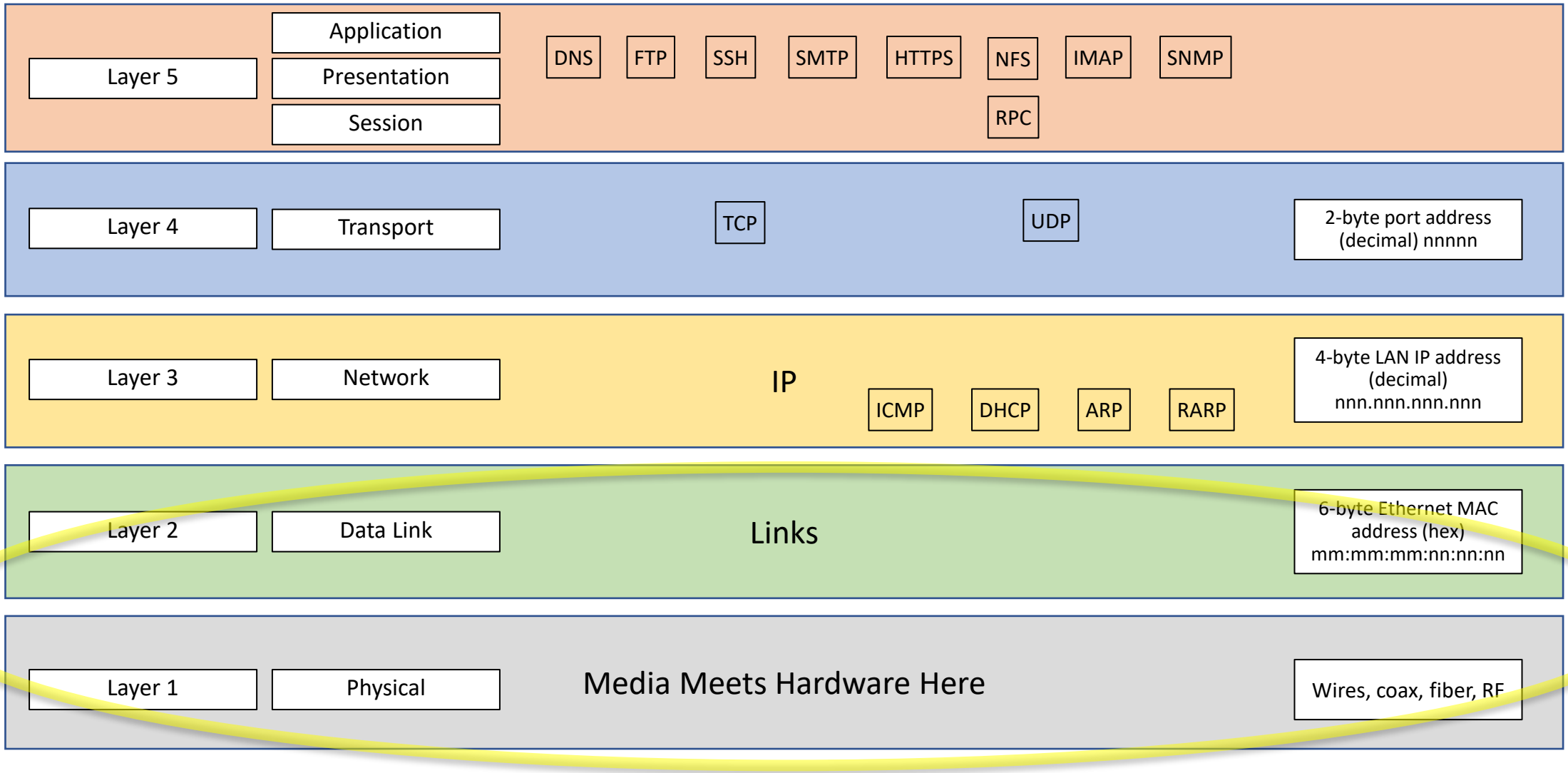
Hidden Node Problem



Multipath interference



TCP/IP 5-Layer Network Stack

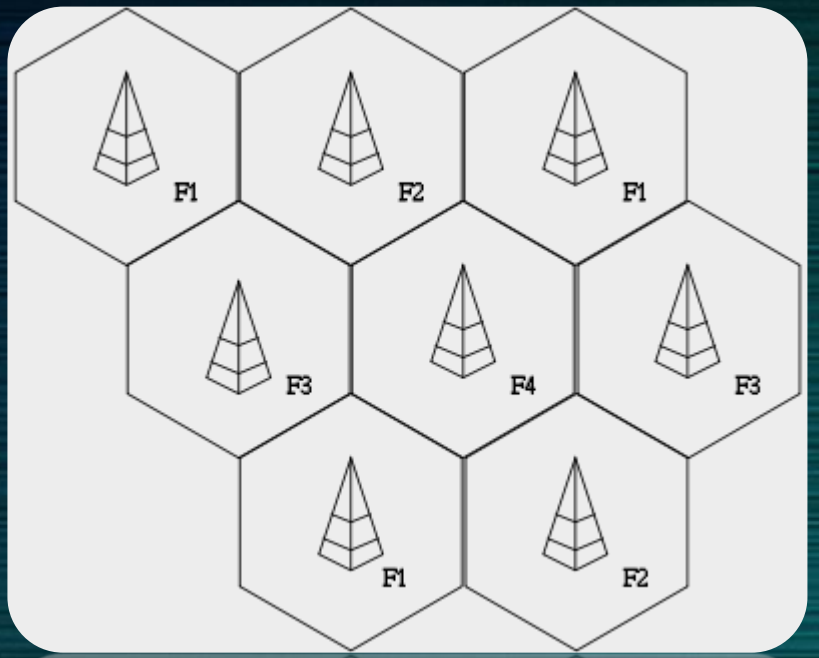


Wireless Technologies

- Cellular
- Bluetooth
- Z-Wave
- Zigbee
- Near Field Communication (NFC)
- Wireless Fidelity (WiFi)
- …to name just a few wireless standards

Cellular

- Fixed towers spread out
- Several towers serve a cell
- Frequencies reused
- Mobile devices handed off



https://en.wikipedia.org/wiki/Cellular_network#/media/File:Frequency_reuse.svg

Cellular Evolution

Generation	1G	2G	3G	4G	5G
Signaling	Analog	Digital	Digital	Digital	Digital
Key Technology	Mobile Voice Calls	SMS	Mobile Internet	Mobile Video	Internet of Things
Circa (approx.)	1981	1991	1998	2008	2019

Cellular

- x Division Multiple Access
- Frequency DMA
- Time DMA
- Code DMA
- Orthogonal Freq DMA

Cellular frequencies in the US - Wikipedia

Frequency (MHz)	Cell radius (km)	Cell area (km^2)	Relative cell count
450	48.9	7521	1
950	26.9	2269	3.3
1800	14.0	618	12.2
2100	12.0	449	16.2

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

Bluetooth 2.4 GHz

Bluetooth®

The global standard for simple, secure device communication and positioning

Bluetooth® Classic

Solution Areas

AUDIO STREAMING

DATA TRANSFER

Device Communication

POINT-TO-POINT

Basic Rate/ Enhanced Data Rate Radio

Bluetooth® Low Energy

Solution Areas

AUDIO STREAMING
(COMING)

DATA TRANSFER

LOCATION SERVICES

DEVICE NETWORKS

Device Communication

POINT-TO-POINT BROADCAST MESH

Device Positioning

PRESENCE PROXIMITY DIRECTION DISTANCE
(COMING)

Low Energy Radio

https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

Z-Wave

- A 900Mhz RF mesh network
- Typically used for home automation
- Low bandwidth
- Low power
- Highly standardized and controlled
- Maximum compatibility for plug-and-play

https://www.youtube.com/watch?v=v8-VNIQQiQE

Zigbee

- 2.4 Ghz RF
- Mesh network
- Low bandwidth
- Low power
- Typically used for home automation
- Not quite a plug-and-play standard

https://www.youtube.com/watch?v=v8-VNIQQiQE

Near Field Communication (NFC)

- 13.56 Mhz
- Close-up design up to 10cm max
- 424 Kbps
- Not a secure form of communication
- For tiny amounts of data

https://en.wikipedia.org/wiki/Near-field_communication

IEEE 802.11 (WiFi) versions

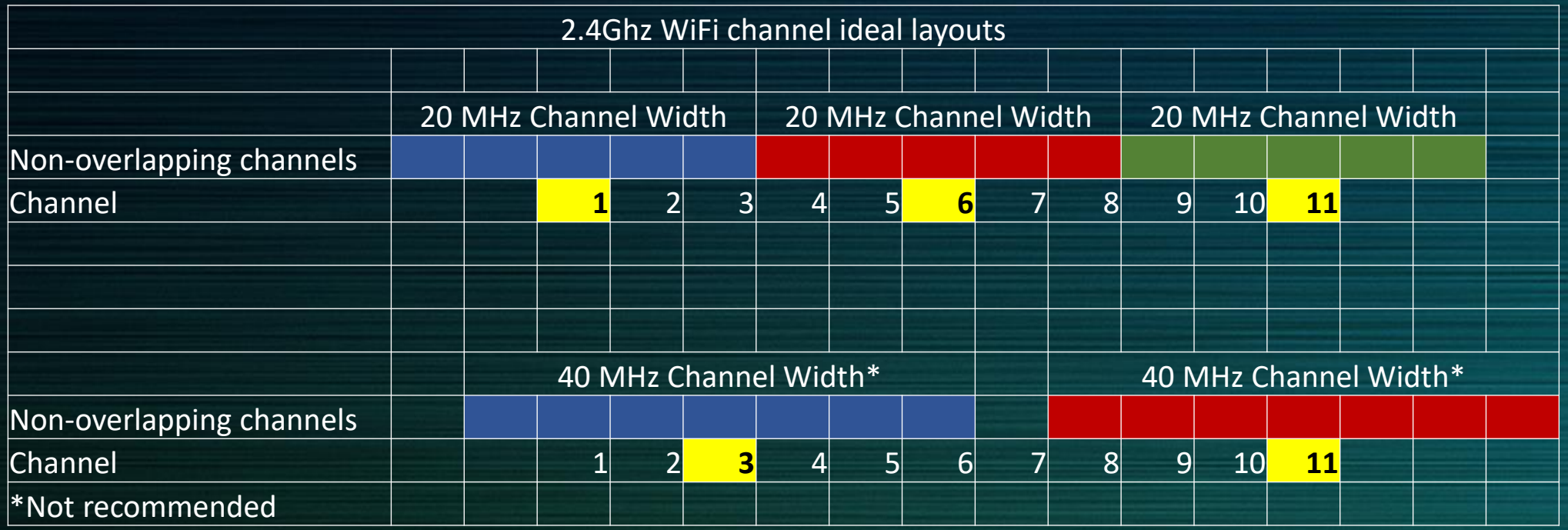
Year	WiFi Generation	IEEE Name	New Name
1999	First	802.11b	WiFi 1
1999	Second	802.11a	WiFi 2
2003	Third	802.11g	WiFi 3
2009	Fourth	802.11n	WiFi 4
2014	Fifth	802.11ac	WiFi 5
2019	Sixth	802.11ax	WiFi 6

IEEE 802.11 (WiFi) characteristics

IEEE Name	Max Bit Rate (Mbps)	Frequency (GHz)	Channel Width (MHz)	New Name
802.11a	54	5	20	
802.11b	11	2.4	20	
802.11g	54	2.4	20	
802.11n	65-150	2.4 & 5	20-40	WiFi 4
802.11ac	78-867	5	20-160	WiFi 5
802.11ax	1200	2.4, 5, 6	20-160	WiFi 6

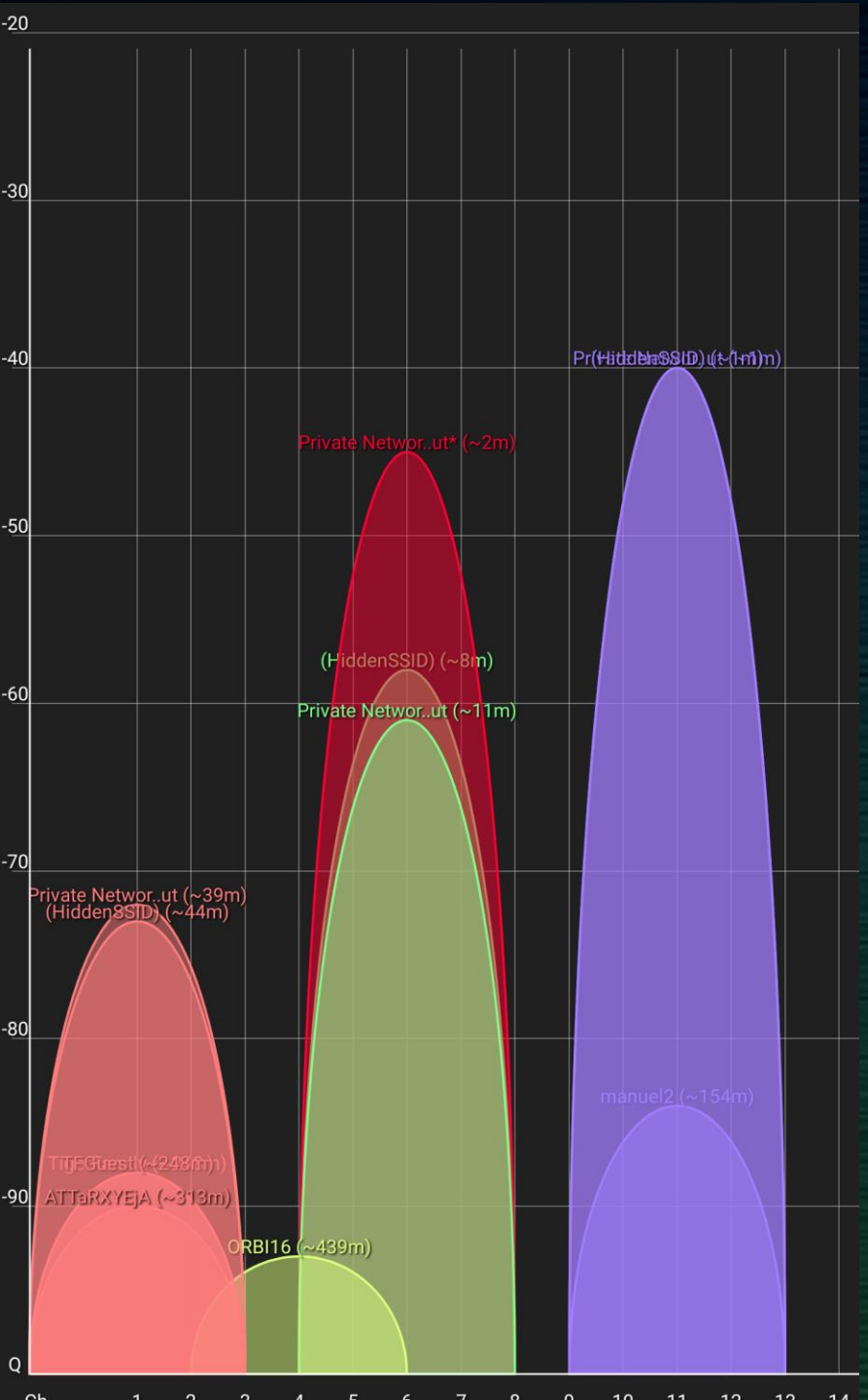
http://intronetworks.cs.luc.edu/current2/html/wireless.html

WiFi 2.4GHz Ideal Channels

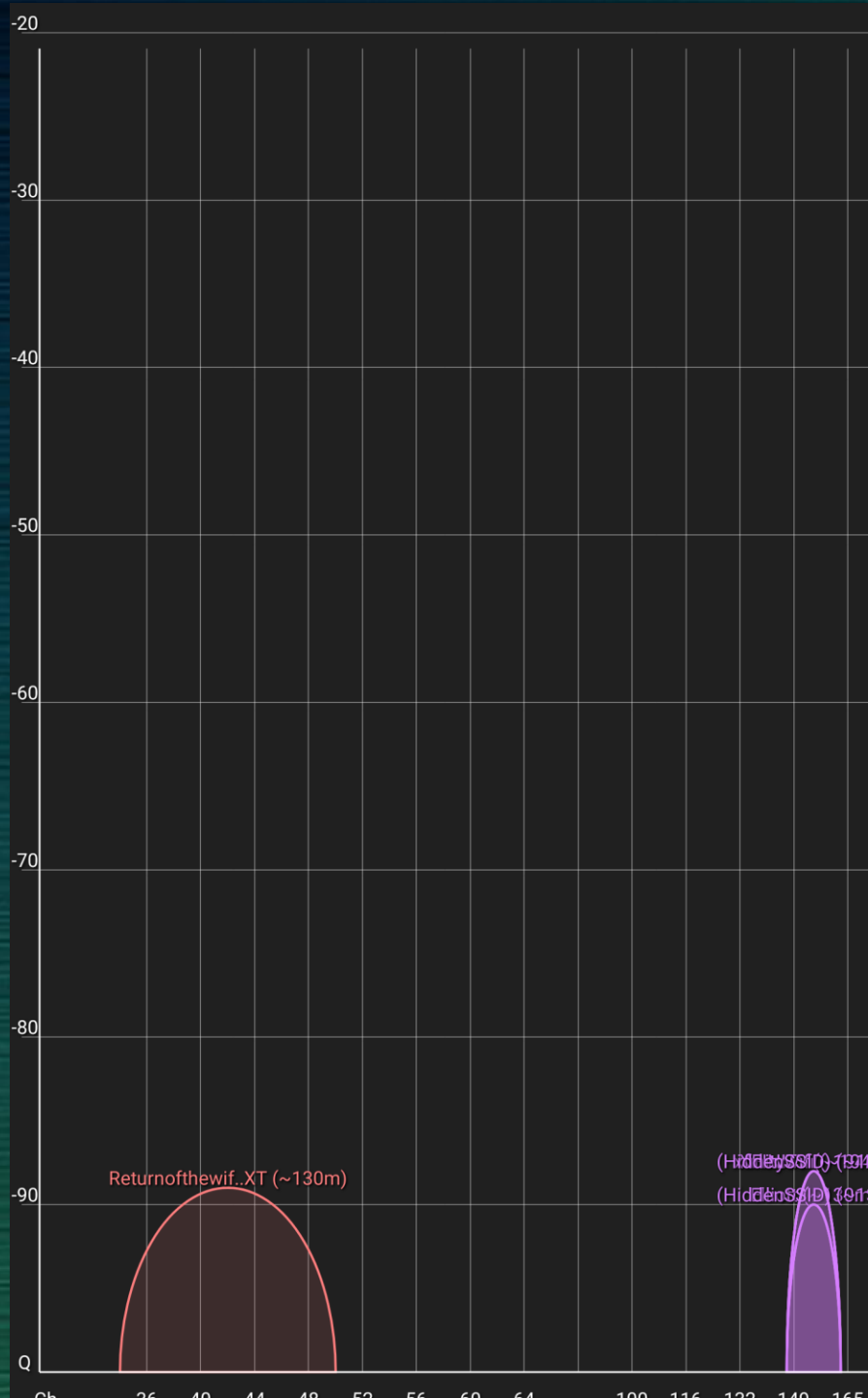


Peter L Dordal, An Introduction to Computer Networks

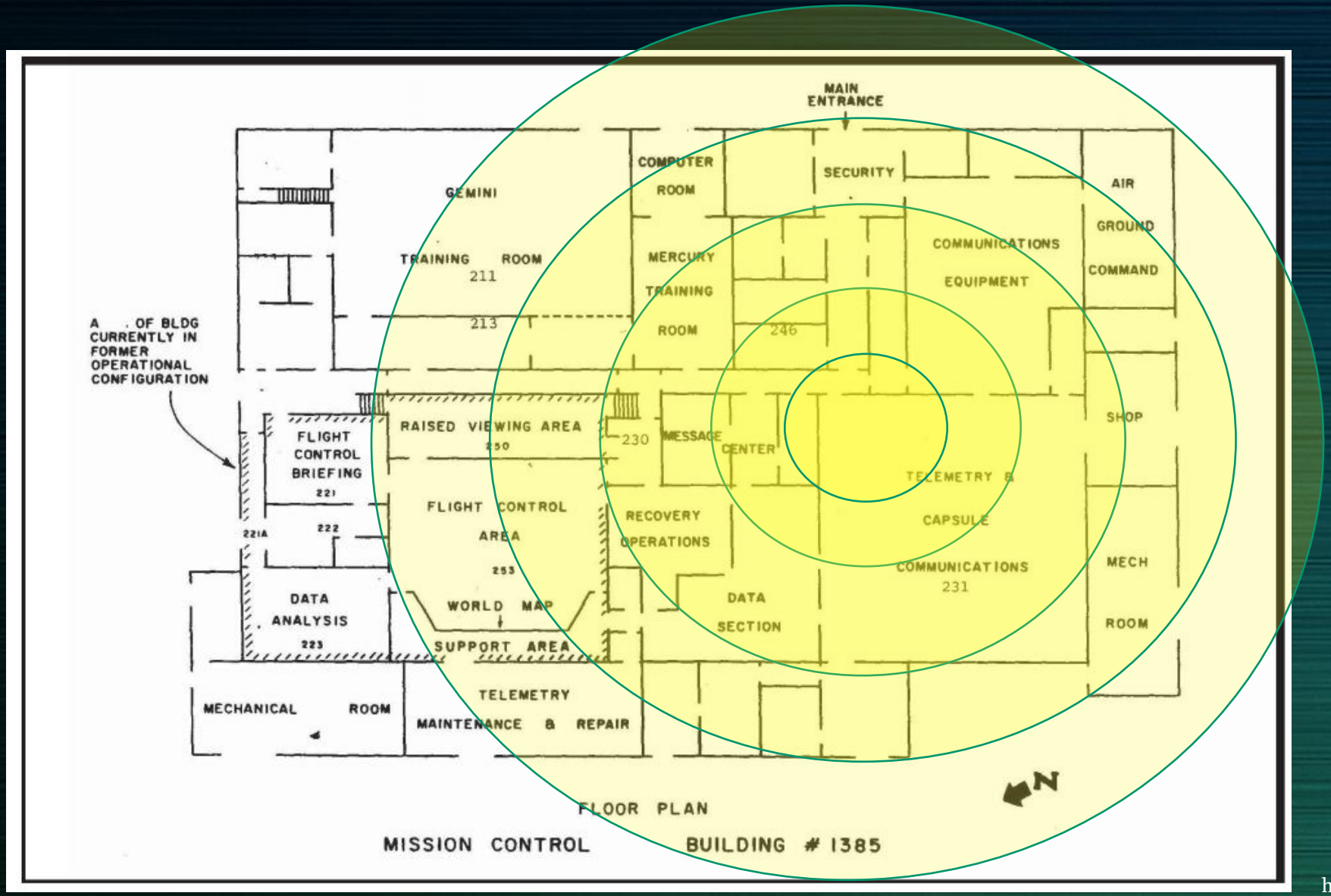
WiFi 2.4 (left) & 5 (right) GHz Channel Scans



1. Left scan shows crowded channel allocation.
2. Ideal 2.4GHz channels are 1, 6, and 11 only.
3. A faint SSID on channel 4 can cause problems due to overlapping frequencies.
4. SSID's on the same channel share bandwidth cooperatively.
5. Right scan shows open and available channels.
6. Power (dBm) is in vertical logarithmic scale so -80 is twice the power of -90.



IEEE 802.11 (WiFi) site survey



- WiFi signals can be measured and graphed on top of a floorplan to provide a visual representation of signal strength.
- Signal strength diminishes mostly due to:
  1. distance from Wireless Access Points (WAP's);
  2. obstructions within line of sight of the WAP;
  3. interference with signals using the same base frequency.
- Multiple WAP's are often needed to fully cover an area.

https://commons.wikimedia.org/wiki/File:MCC_floorplan.png#/media/File:MCC_floorplan.png

Peter L Dordal, An Introduction to Computer Networks

WiFi adds control packets

- Band Width (signal f range) ≠ Bandwidth (data rate)
- Inter-Frame Spacing (IFS)
- Distributed IFS (DIFS)
- Short IFS (SIFS)
- Slot time: 20 micro-seconds
- IFS: 50 micro-seconds
- SIFS: 10 micro-seconds
- This control function helps make sure frames get to their destinations unlike the regular link layer

WiFi Collisions

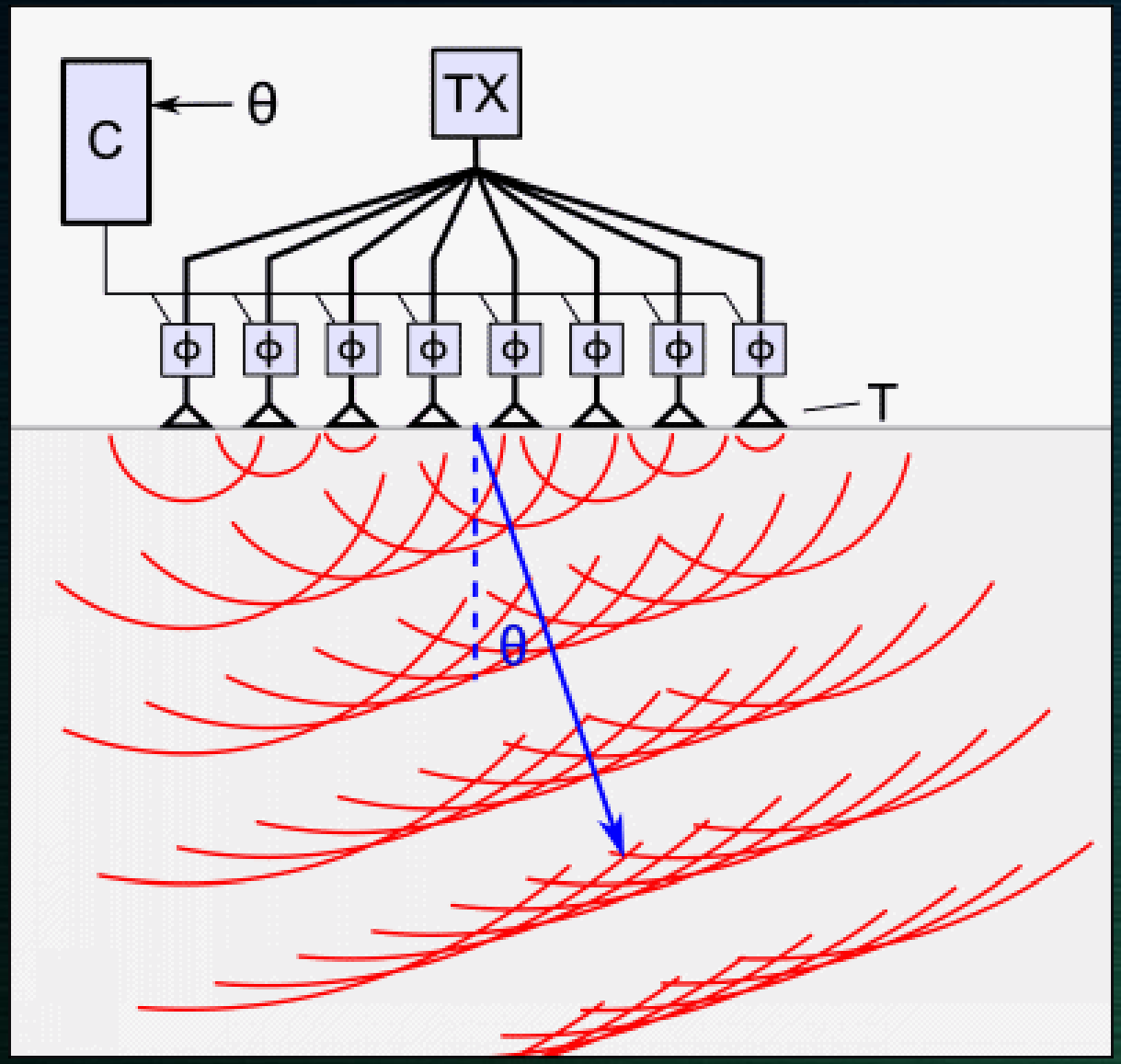
- WiFi cannot avoid collisions
- Need a better algorithm than old CSMA-CD
- Carrier Sense Multiple Access with Collision Avoidance
- CSMA-CA (includes backoff)
- RTS/CTS can help with the hidden node problem
- WiFi can do Dynamic Rate Scaling/Control based on error conditions it can reduce/increase bit-rate circa 802.11g

WiFi Optimizations (MIMO)

- Multiple In Multiple Out (MIMO) uses multiple channels simultaneously to improve bandwidth.
- Wireless routers use this because they connect many devices.
- Multiple antennas are typical for routers which use this approach.

https://upload.wikimedia.org/wikipedia/commons/8/8e/3Com_OfficeConnect_ADSL_Wireless_11g_Firewall_Router_2012-10-28-0862.jpg

WiFi Optimizations (beamforming)



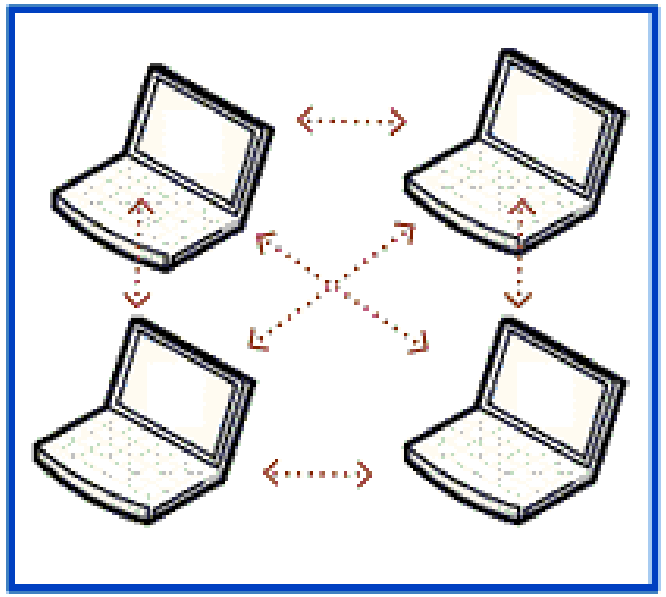
Beamforming and beam-steering allow a fixed set of transmitters in an array to transmit waves offset in time thereby leveraging wave interference characteristics to effectively form a directed beam. This improves communications by focusing energy directly at the target.

https://commons.wikimedia.org/wiki/File:Phased_array_imaging_animation.gif#/media/File:Phased_array_imaging_animation.gif

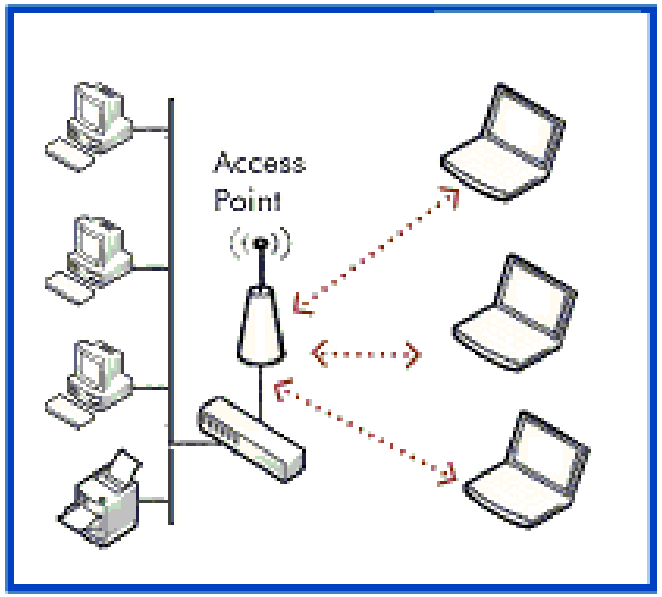
Peter L Dordal, An Introduction to Computer Networks

WiFi Access Modes

- Infrastructure mode is most common. Ad-Hoc can also be used to relay data peer-to-peer without a dedicated router.



Ad-hoc mode



Infrastructure mode

https://www.researchgate.net/profile/Viraj-Shah-5/publication/316175326/figure/fig1/AS:495727332610048@1495202014846/Ad-hoc-mode-vs-Infrastructure-mode-IEEE80211-introduced-many-types-of-the-Wi-Fi.png

Peter L Dordal, An Introduction to Computer Networks

WiFi Access Points (Infrastructure)

- SSID beacon every 100ms (can be hidden but not secure)
- Process for getting on a WiFi
  - Scanning (or active probing)
  - Open-authentication and association
  - True authentication
  - DHCP
- Roaming - Extended Service Set (ESS) allows same SSID to be used by multiple WAP's. ESS is unique for each WAP.
- MAC address randomization can help with privacy

Q: WiFi what's this?

https://www.flickr.com/photos/37996580417@N01/35460674813

A: WiFi what's this?

This is a mobile wardriver at DefCon. He has many access points used to massively collect data about every WiFi device around him.

https://www.flickr.com/photos/37996580417@N01/35460674813

WiFi - Encryption

- Open
- WEP – cracked – don’t use
- WPA – cracked – don’t use
- WPA2 – cracked – don’t use
- WPA3 – current

WiFi – Encryption types

- Personal – one shared key for all
- Enterprise – unique keys for each with RADIUS mode

WiFi – Enterprise Encryption

- Powerful security
- Extensible Authentication Protocol (EAP)
- Username/Password
- Security certificate
- Encryption can be different for supplicants.

WiFi – Monitoring

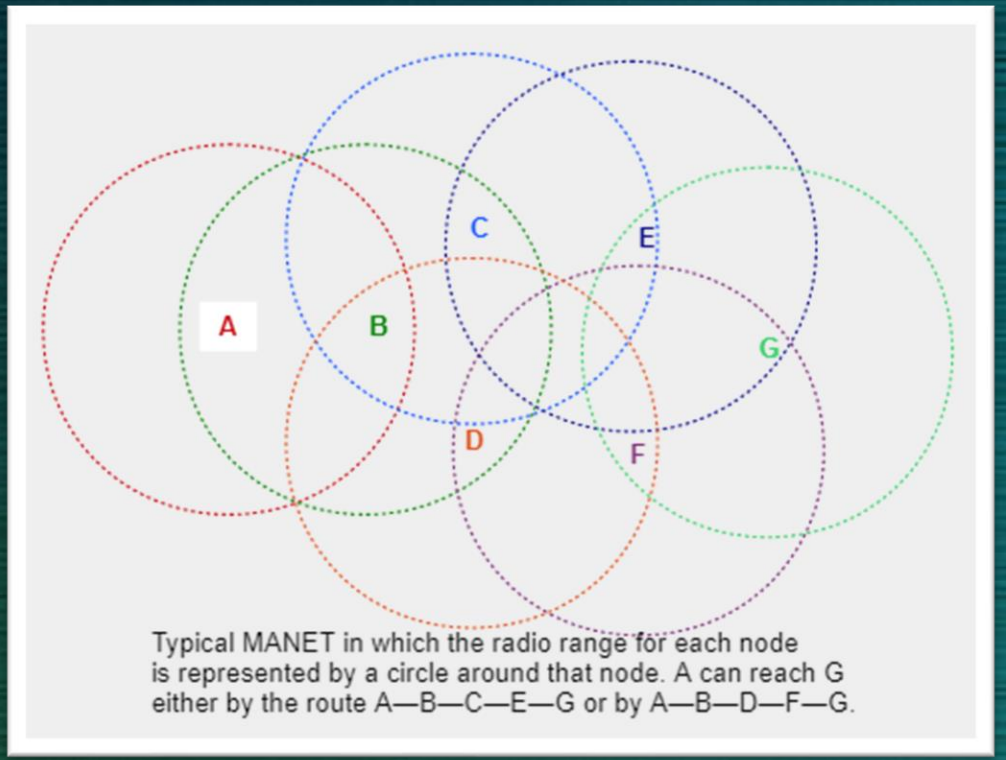
- Tools can be used to snoop WiFi:
- Aircrack-ng
- Kismet
- Wireshark monitor mode

WiFi – Polling mode

- WiFi has seldom used option to eliminate collisions
- Point Coordination Function (PCF)

WiFi – MANET

- Mobile Ad-hoc Network (MANET)
- Point-to-point wireless networking
- No access point



Typical MANET in which the radio range for each node is represented by a circle around that node. A can reach G either by the route A—B—C—E—G or by A—B—D—F—G.

http://intronetworks.cs.luc.edu/current2/html/wireless.html