802.11 Wireless Networking

IEEE Working Groups

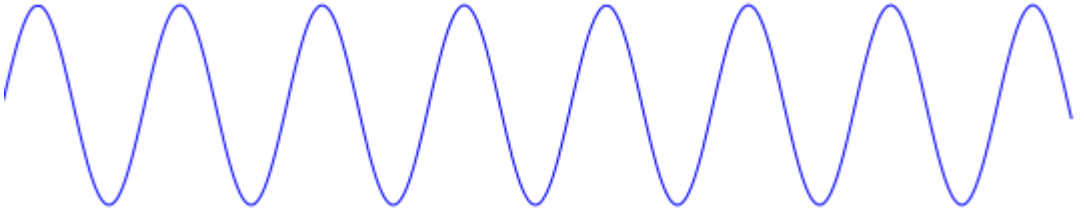
- 802.3 – Wired Ethernet
- 802.11 – Wireless

IEEE 802.11

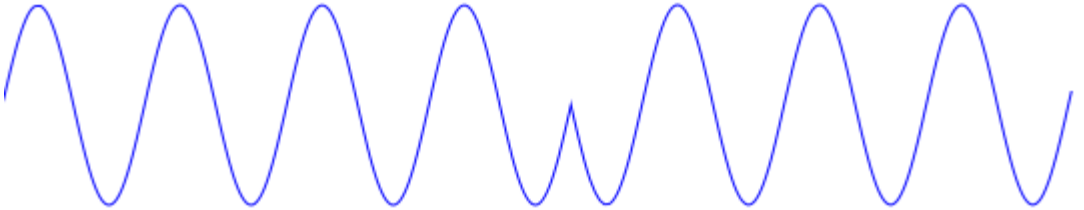
- First introduced in 1997 (not widely used)
- Updated to 802.11a & 802.11b in 1999
- 802.11a - 5 GHz, OFDM, 54 Mbit/s
- 802.11b - 2.4 GHz, CCK, 11 Mbit/s
- The 54Mbit protocol was technically ambitious for the time
- The simpler protocol (802.11b) was the first widely deployed standard

A simplified model of phase-shift keying

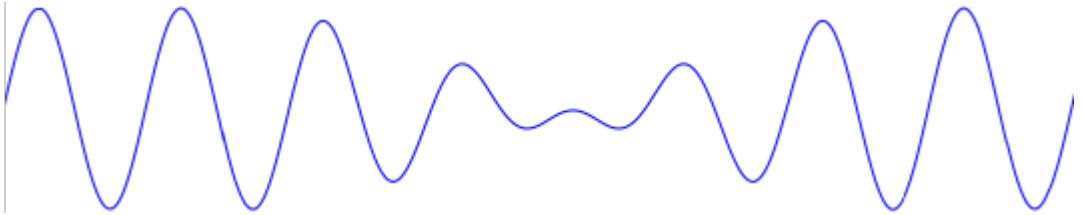
Carrier wave



Phase shift



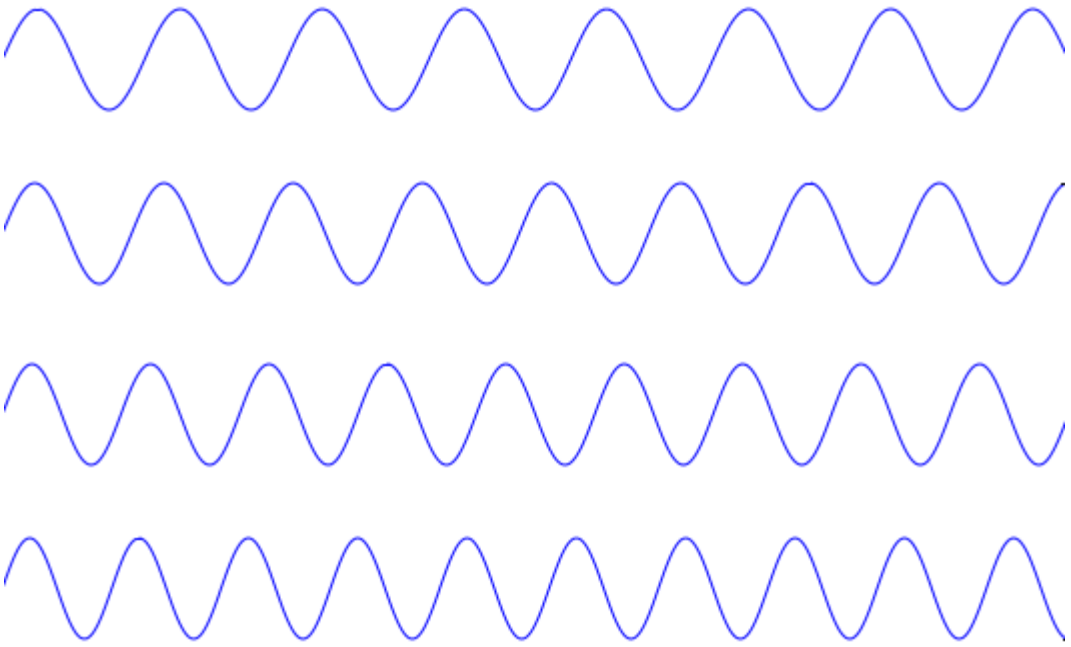
Filter sidebands



Channels and Frequencies

Channel 1	2.412 GHz
Channel 2	2.417 GHz
Channel 3	2.422 GHz
Channel 4	2.427 GHz
Channel 5	2.432 GHz
Channel 6	2.437 GHz
Channel 7	2.442 GHz
Channel 8	2.447 GHz
Channel 9	2.452 GHz
Channel 10	2.457 GHz
Channel 11	2.462 GHz
Channel 12	2.467 GHz
Channel 13	2.472 GHz

Orthogonal frequency-division multiplexing (OFDM)



Multiple carrier waves, lower data rate on each
Encoded/decoded using fast fourier transform (FFT)

Wireless Configuration (iwconfig)

```
~# iwconfig wlan0
wlan0     IEEE 802.11bg  ESSID:"CMU"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:00:36:2E:9A:02
          Bit Rate=54 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-31 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

dBm = decibels milliwatts

0 dBm = 1 mW
10 dBm = 10 mW
20 dBm = 100 mW
30 dBm = 1000 mW

Wireless Configuration (iwconfig)

```
~# iwconfig wlan0
wlan0     IEEE 802.11bg  ESSID:"CMU"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:00:36:2E:9A:02
          Bit Rate=54 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-31 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Power Management – varies by vendor,
but usually a squelch setting on the radio

802.11 updates

- 802.11g (2003) – Combines features of a & b, 54 Mbps in 2.4 GHz band
- 802.11n (2009) – Doubles bandwidth (40 MHz channels instead of 20 MHz)
- 802.11ac (2014) – 160 MHz bandwidth in 5 GHz band

Service Set Identifier (SSID)

- 32-byte network name
- Beacons typically broadcast ten times per second
- When not connected, clients scan through different frequencies looking for beacons

802.11 weak encryption protocol “Wired Equivalent Privacy” (WEP)

- Quick, sloppy, “security” protocol
- Single shared 40-bit or 104-bit RC4 key
- Anyone on the network can see anything (like old wired ethernet)
- No password hash, keys typically entered as 10 hexadecimal digits

RC4 encryption

XOR with pseudorandom bit stream

Plaintext	1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
RC4	1 0 0 1 1 0 1 0 0 1 1 1 0 1 0 1
Cyphertext	0 1 1 0 1 0 1 0 1 0 0 0 0 1 0 1

RC4 encryption in WEP

- 40 bit static key + 24 bit counter to generate key per packet
- Bitstream repeats after 2^{24} packets
- No additional data integrity check
- Challenge-response authentication (yes just xor, totally useless)
- RC4 is statistically not random enough

AirCrack

- `airodump` records packets
- `aircrack` can derive WEP key with ~10,000 ARP packets or ~100,000 TCP packets
- Possible to speed things up by reinjecting ARP packets

WiFi Protected Access

- WPA fixed most of the security problems with WEP, but retained RC4
- WPA2 uses AES
- Pre-shared key (PSK) challenge-response subject to brute-force password guessing
- PEAP-TLS is a more secure alternative (SSL/TLS protocol)

Security is hard,
let's make things easier...

- 8-digit PIN can be guessed
- Push-button insecurity (“easy setup button”)