# Versions of 802.11

*Source: S. Kopp, "802.11: Leaving the Wire Behind," IEEE Internet Computing, Jan-Feb 02*

**802.11:** Original version, 1 or 2 Mbps
Didn't sell well, price/performance not a good match.

**802.11b:** Popular 1999 standard, seven million systems sold in 2002.
11 Mbps (1/2 that if using Wired Equivalency Protocol (WEP) for security)
11 Mbps at 100-150 feet
2 Mbps at 250-350 feet t
Transfer speed steps down with distance to 1 Mbps, then cuts off.

Operates at 2.4 GHz with 3 techniques:
Direct Sequence Spread Spectrum (DSSS)
Frequency Hopping (FH)
Infrared (largely unused)
DSSS taking over (defacto standard at 11 Mbps)

**802.11a:** Developed after 802.11b (go figure)
54 Mbps
Uses UNI (Unlicensed Infrastructure Band)
UNI-1: 5.2 GHz Band
UNI-2: 5.7 GHz Band
UNI-3: 5.8 GHz Band

802.11b has seven times the range of 802.11a
(though there is some disagreement on this point)

**802.11e:** 802.11 with Ethernet Quality of Service (QOS)
Applies to all implementations (b,a,g)
Standard was to be ratified in early 2002

**802.11g:** Or known as 802.11b extended
Purpose is to increase 2.4 GHz band throughput
Initially at 22 Mbps, will then go to 54 Mbps and farther

**802.11h:** Uniform standard for power usage and transmission power

## ***Improved Security***

**802.11x:** Lightweight version of Extended Authentication Protocol (EAP)

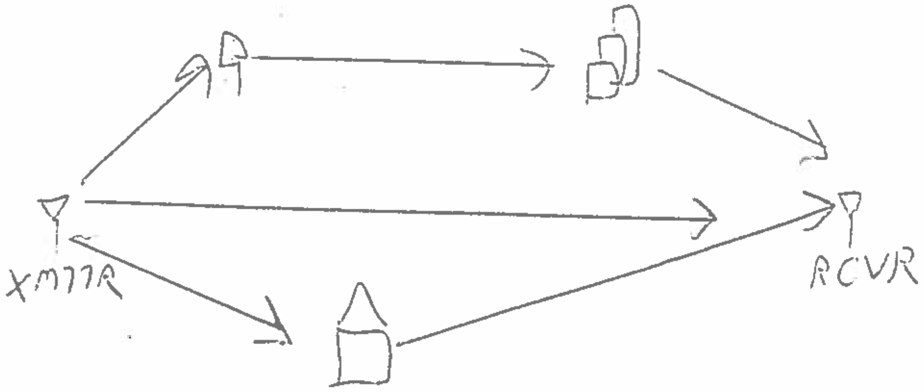
**802.11i:** WEP2 or AES for stronger encryption

## 802.11n

Standards work started 2004, approved 2007.

Higher speeds (theoretical max of 600 Mbps – real world 100 Mbps) and longer distances (up to 50 meters). Uses two 20 MHz channels.

Uses MIMO (Multiple Input Multiple Output) technology. That is, parallel flows of multiple signals.



*[1] S.J. Vaughn-Nichols, "Will the New WiFi Fly?", Computer, Oct. 2006, pp. 16-18.*

*More Recent 802.11 Versions*

**802.11ac**

Throughput close to 1 Gbps

Channel bandwidth can be 20, 40, 80 (mandatory) or 160 MHz (optional) by bonding group of adjacent 20 MHz channels.

Uses MU-MIMO (multiple user – multiple input multiple output) technology. Downlink only. Access Point can have a max of 8 antennas and xmt four or less streams to two distinct users or two or less streams to four distinct users concurrently.

**802.11ad**

Known as WiGi – operates in 60 GHz unlicensed frequency region.

Propagation loss and signal attentuation worse at 60 GHz, range is shorter but bandwidth is larger than lower frequencies such as 2.4 and 5 GHz.

Can reflect off walls but not penetrate walls so communication handed off to a lower frequency 802.11 protocol by access point in that case.

**802.11ax**

As more access points deployed, more overlapping "basic service sets".

802.11ax seeks to enhance the area and personal throughput in crowded environments by improving physical and MAC layers.

**802.11aa**

Seeks to improve performance of real-time multimedia content transmission.

**802.11af**

Uses TV white space (analog bandwidth opened up by switch to digital TV) at hundreds of MHZ.

Available to unlicensed users as long as don't interfere with licensed users.

Geolocation databases used to store location based information on available spectrum and usage schedules. Location aware access points used.

Uses 802.11ac features such as MU-MIMO since its physical layer is built on 40 MHz 802.11ac.

**802.11ah**

Uses unlicensed spectrum to provide long distance, lower data rate connectivity for applications such as sensor networks, the smart grid and the Internet of Things.

Below 1 GHz alternative to 802.11af. Fear 802.11af won't work in crowded urban areas.

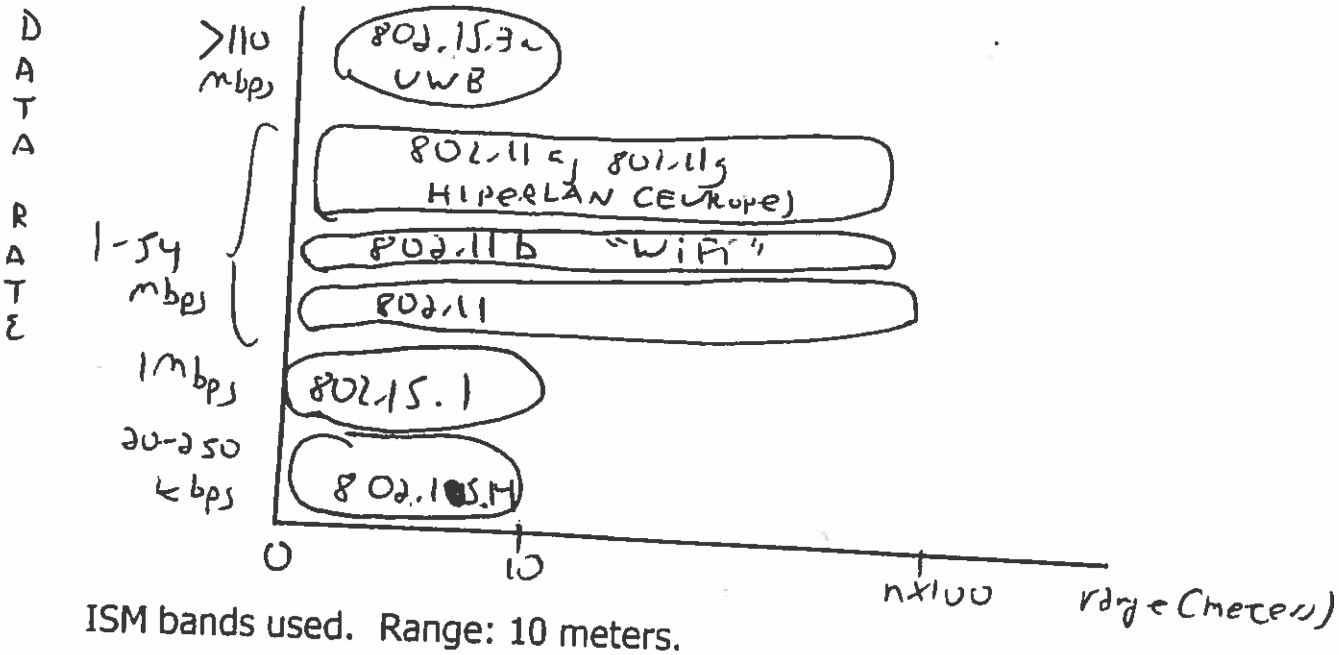
A below 1 GHZ implementation of 802.11ac. Channel widths of 1 and 2 MHz, some countries support channel widths of 4, 8 and 16 MHz. Minimum data rate of 100 kbps.

Efficient power savings techniques for applications such a sensor networks.

## IEEE 802.15.4 Low Data Rate, Low Power Bluetooth

*Goal:* A low data rate, low power, inexpensive protocol for connecting stand alone devices to a network. Original Bluetooth standard encountering market difficulties as 802.11 WiFi pricing better and original Bluetooth standard more complex than originally intended.

*Zigbee Alliance:* 60 companies developing standard including Motorola and Samsung ("Zigbee": Bees zig zag)



ISM bands used. Range: 10 meters.

16 channels x 250 kbps/channel in 2.4 GHz band.
10 channels x 40 kbps/channel in 915 MHz band.
1 channel x 20 kbps/channel in 868 MHz band.

Total=27 channels

Toplogy

(a) One hop star or
(b) Multihop communication if distance greater than 10 meters

One 802.15.4 net can accommodate 64,000 devices (16 bit address).

Direct data transfer between device and coordinator uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) in either slotted or unslotted mode.

Low Power

(a) Device in "sleep" mode if no pending packet.
(b) Device/coordinator on 1/64th of time.

3 Security Levels

(a) "None Security" mode.
(b) Access Control List (for authorization).
(c) AES (Advanced Encryption Standard—DES successor) used.

Beacon Enabled Mode

Coordinator broadcasts beacons periodically to synchronize attached devices and for other purposes.

Non-Beacon Enabled Mode

Coordinator does not broadcast beacons periodically but will send a beacon to a device soliciting beacons.

Source: J. Zheng and M.J. Lee, "Will IEEE 802.15.4 Make Ubiquitous Nteworking a Reality?," IEEE Communications Magazine, June 2004, pp. 140-146 (available like other post 1998 IEEE articles on ieeexplore data base/electronic journals on Stony Brook library page).

# 802.11 Security Issues

*Source: J. Williams, "The IEEE 802.11b Security Problem," Part I, IEEE ITPro (Info technology Professional) Nov/Dec 2001*

## 802.11b Security Problems:

(1) Products shipped with all security features disabled by default.

(2) Access Points transmit hopping codes in plaintext.

(3) Administrators *can* configure access points to broadcast its SSID (segmentation ID number). This is normally used for segmenting network by floors and/or departments. Then any computer can sniff the SSID in every packet and gain access to the access point.

(4) MAC address used by station for ID. A determined hacker could identify and counterfeit MAC addresses.

(5) In WEP (Wired Equivalency Protocol) each station/access point in practice uses a single shared key.

(6) The same shared key is used for authentication and encryption:
a major risk.

(7) WEP security not available in ad hoc 802.11 networks.

(8) Most corporate users not using or misusing WEP – articles on people who drive around sniffing corporate nets.

(9) There is high degree of manual management in WEP for moderate to large size networks (in maintaining WEP encryption keys on clients/access points and in maintaining a list of valid MAC addresses at access points). WEP is

impractical in these terms.

**(10)** WEP keys not replaced frequently enough.

**(11)** Throughput drops 50% or more with WEP.