Modulation is the processes of impressing message information onto a carrier signal.
Sidebands AM (Amplitude Modulation) f_c +/- f_m
PM (Phase Modulation) f_c +/- f_m +/- $2f_m$ +/- $3f_m$.....
Bandwidth, S/N and Shannon's Law Channel Capacity $C = B*\log_2(1+S/N)$
Spectral Efficiency often expressed as bits per second per hertz of bandwidth.

Multiplexing (Muxing) enables multiple, separate, information signals to operate over a shared medium. Muxing methods can be combined. Example, GSM mobile-phones use both FDMA & TDMA.
FDMA—Frequency Division Multiple Access
TDMA—Time Division Multiple Access
CSMA*[1]—Carrier Sense Multiple Access (a subset of TDMA)
CDMA—Code Division Multiple Access
SDMA—Space-Division Multiple Access allows a terminal to transmit (or receive) signal to (or from) multiple users in the same band simultaneously.
MIMO—Multiple-Input and Multiple-Output, is a form of SDMA using more than one Tx—antenna—Rx chain, it increases data throughput without additional bandwidth, but it increases complexity.
"*Any sufficiently advanced technology is indistinguishable from magic*"—Arthur C. Clarke, 1973

QAM (Quadrature Amplitude Modulation) is the application of both AM & PM to a single carrier.
OFDM (Orthogonal Frequency-Division Multiplexing) is a form of FDMA using a number of closely spaced orthogonal (independent) QAM sub-carriers. Examples digital TV, ADSL.
DSSS (Direct-Sequence Spread Spectrum) directly combines the information signal with a higher rate pseudo-random-number (PRN) sequence signal called "chips", prior to phase modulation. The key for the chips PRN must be known by both Tx and Rx. The lower spectral efficiency of DSSS is compensated for by its **CDMA** multiple Tx sharing property. Examples GPS & Bluetooth.

IEEE 802 is a family of *physical layer* protocols (link-to-link, MAC*[2] to MAC) for networks carrying *variable-size packets* in LANs using **CSMA** (Carrier Sense Multiple Access). The packet size is called the **MTU** (Maximum Transmission Unit) *[1]**CSMA** requires each *node* to verify the channel appears free before transmitting; if the channel is busy then the transmission is delayed for a random interval, if a collision is detected the transmission is terminated and recommenced after a random delay.

NIC - **N**etwork **I**nterface **C**ontroller (card) interfaces computer to a wired network
WNIC - **W**ireless **N**etwork **I**nterface **C**ontroller (card) interfaces a computer to a wireless network.
***[2]MAC** (**M**edia **A**ccess **C**ontrol) is a unique 48 bit address assigned to each NIC/WNIC by its manufacturer and is stored in the device's firmware.

An **IEEE 802 frame** (packet) includes MAC destination (6), MAC source (6), Length (2), IP payload (46 - 1500), CRC (4)
CRC (Cyclic Redundancy Check) also called **FCS** (Frame Check Sequence) is for an integrity check of received frames. Immediately before each frame is sent the CRC is calculated and appended, when each frame is received the CRC is re-calculated and compared to the original transmitted CRC.
TCP is an 'application to application' protocol, it keeps track of the individual packets of data, arranging them in their original order at the receiving end. TCP provides reliable data delivery but causes delays when requesting re-transmission of lost data. so it is not suited to real-time usage e.g. VOIP.
IP handles the delivery of data packets (eg TCP) to a destination IP address (i.e. another computer).
{Physical Layer Protocol$_{mac}$ [IP$_{ipv4/6}$ (TCP contains your application data)] }

Ethernet (IEEE 802.3) is a '*wired physical layer*' protocol. It includes specifications for cable characteristics, length and termination.

WiFi (IEEE 802.11 a/b/g/n) is a family of '*wireless physical layer*' protocols related to .IEEE 802.3.
A **WAP** (**W**ireless **A**ccess **P**oint) provides 802.11 wireless devices with a connection point to a wired network. The WAP may also self-contain a DHCP server, router, an ethernet switch, NAT, modem etc.

802.11b and **802.11g** are the most commonly used, they utilise the 2.4 GHz band.
802.11n is a new multi-streaming modulation technique utilising 2.4GHz and/or 5GHz band.
The Spectrum Ref. - http://en.wikipedia.org/wiki/List_of_WLAN_channels
The 2.4 GHz DSSS band has 13 overlapping 22 MHz channels spaced @ 5MHz and is shared with microwave ovens, cordless phones and Bluetooth.
802.11b uses DSSS & has a max. raw data rate of 11 Mbit/s prefered are chans 1, 6, 11.
802.11g uses OFDM, max. raw data rate bit rate of 54 Mbit/s, the prefered chans are 1, 5, 9, 13,
802.11g can use DSSS for 802.11b compatibility but this will reduce the overall network data rate.
802.11n uses OFDM, raw data rate 54 Mbit/s to 600 Mbit/s. It can use multiple-input multiple-output antennas (MIMO). When using four spatial streams it has a channel width of 40 MHz. Some 802.11n WAPs are dual band and may operate 2.4GHz & 5GHz simultaneously

A **Basic Service Set** (BSS) is one WAP and its clients, the **BSSID** is the MAC of the WAP
A **Service Set** (SS) is all the devices linked into a particular **WLAN Infrastructure**.
The **SSID** or **ESSID** is an identifying alphanumeric network name, (from 2 to 32 chars) for a SS .
An **Ad Hoc** network or **Independent Basic Service Set** (IBSS), is a direct connection between two or more WNICs, (no WAP)

Security. The older encryption scheme, **WEP** (Wired Equivalent Privacy) is easy to crack;
WPA (Wi-Fi Protected Access)and **WPA2**, are reasonably secure with a strong password/pass-phrase.
- **Pre Shared Key (PSK) or Personal Mode** Uses a manually configured encryption key on all devices on the wireless network.
- **Enterprise Mode** facilitates *Access Control* for commercial enterprises.

Access Controlled WLANs, use a RADIUS or similar server system to provide authentication, authorisation and accounting).
A **hotspot** is a publicly accessible WAP. which usually has some form of access control.

Sniffers are both a security tool & threat. Examples - Aircrack-ng, Kismet, SWScanner, *BackTrack* os.

Raw Data Rate is depreciated by **overheads** e.g. encryption, access control, packet collision, congestion due to one or more users' retransmission requests due to interference, poor S/N (faulty Rx, trans. line, aerial) the **Actual Data Rate** is usually about half the raw data rate.
To avoid interference to other WAPs keep Tx (Transmitter) power as low as practical.

Atheros Chipsets are your best choice for FOSS drivers. Don't need grief? Don't use TI chipsets!
https://help.ubuntu.com/community/WifiDocs/WirelessCardsSupported
http://linux-wless.passys.nl/

ndiswrapper - can be a saviour in a tight spot but avoid if possible by choosing a better chipset.
http://sourceforge.net/apps/mediawiki/ndiswrapper/index.php?title=Main_Page

Some Useful Bash Commands - usefulness of some commands depends on the WNIC and its driver.
`sudo lshw` `hardware info or` *`sudo`* **`lshw -html`** to output a html formatted file
`uname -rp` kernel release & CPU type **`ifconfig -a`** interface configuration info.
`lspci|grep -i` *`wireless`* wireless chipset.
`modinfo` *`iwlagn`* WNIC driver info **`lsmod`** show the status of modules
`sudo` **`ifconfig`** *`wlan0 up/down`* Enable/Disable your wireless device.
`sudo` **`iwlist`** *`wlan0 scan`* List the available WAPs, use with `|egrep -i` refer follwing example →.
`sudo` **`iwlist`** *`wlan0 scan`*`|`**`egrep -i`** `'`*`address|channel|frequency|essid|quality`*`'`
`sudo` **`iwconfig`** *`wlan0 essid NETWORK_ID key WIRELESS_KEY`* Configure your wireless connection.
`sudo` **`dhclient`** *`wlan0`*: Request IP address via dhcp.

Some GUI Network Managers
NetworkManager, WiCd, KWiFiManager

Some Useful Sites

http://wiki.debian.org/WiFi
http://linuxwireless.org/
http://madwifi.org/
http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch13_:_Linux_Wireless_Networking
modulation - http://www.maxim-ic.com/app-notes/index.mvp/id/1890