Wireless networking terminology

NIC: http://en.wikipedia.org/wiki/Network_interface_controller

A **network interface controller** (also known as a **network interface card**, **network adapter**, **LAN adapter** and by similar terms) is a computer hardware component that connects a computer to a computer network.

MAC address: http://en.wikipedia.org/wiki/MAC_address

A **Media Access Control address** (**MAC address**) is a unique identifier assigned to network interfaces for communications on the physical network segment.

Wi-Fi: http://en.wikipedia.org/wiki/Wi-fi

WiFi, is a mechanism that allows an electronic device to exchange data wirelessly over a computer network. A device enabled with Wi-Fi, such as a personal computer, video game console, smartphone, tablet, or digital audio player, can connect to a network resource such as the Internet via a wireless network access point.

LAN: http://en.wikipedia.org/wiki/LAN

A **local area network (LAN)** is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.

****

****

Wireless networking devices:

Router: http://en.wikipedia.org/wiki/Router_(computing)
A **router** is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it gets to its destination node.

Dial-up modem http://en.wikipedia.org/wiki/Dial-up_modem

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information.

Note: There is a very long discussion on the Wikipedia site about the development of various dial-up modems. At the end, the data speed is limited to 56kbps unless data compression is used to (seemingly) exceed that limit.

DSL modem http://en.wikipedia.org/wiki/DSL_modem

A **digital subscriber line** (**DSL**) **modem** is a device used to connect a computer or router to a telephone circuit that has digital subscriber line service configured. Like other modems, it is a type of transceiver.

Compared to voice-band modem

A DSL modem modulates high-frequency tones for transmission to a digital subscriber line access multiplexer (DSLAM), and receives and demodulates them from the DSLAM. It serves fundamentally the same purpose as the voice-band modem that was a mainstay in the late 20th century, but differs from it in important ways.

- DSL modems transfer data at a rate which is typically 10 to 20 times that of a voice-band modem.
- A single telephone line can be used for simultaneous voice and data with a DSL modem whereas a voice-band modem precludes simultaneous voice traffic.

Note: there is MUCH more detail on the Wikipedia page that time will not allow discussion for at our meeting. I would like to point out that DSL is limited to customers within 3 miles of a phone company Central Office and speed is degraded progressively as one is farther from the C.O. I have seen my neighbor's DSL line test as high as 2.5Mbps while our friend's DSL managed only 0.19Mbps. For the $20/month they each pay, compared to the $35/month I pay for my unbundled* cable connection that gives me download speeds of 16-17Mbps, they may not seem so much of a bargain, but each user should decide services based on their needs. As our friend only uses hers to check her bank statement and do a little email, 0.19Mbps is enough for her.

***Unbundled: Charter offers cheaper broadband prices than I pay, but only it's only cheaper if you get it bundled with other services. Charter offers speeds up to 100Mbps in my location.**

Cable modem http://en.wikipedia.org/wiki/Cable_modem

A **cable modem** is a type of network bridge and modem that provides bi-directional data communication via radio frequency channels on a HFC* and RFoG infrastructure. Cable modems are primarily used to deliver broadband Internet access in the form of cable Internet, taking advantage of the high bandwidth of a HFC and RFoG network.

***HFC:** http://en.wikipedia.org/wiki/Hybrid_fibre-coaxial

Hybrid fiber-coaxial (**HFC**) is a telecommunications industry term for a broadband network which combines optical fibre and coaxial cable. It has been commonly employed globally by cable television operators since the early 1990s.

Side note: cable modems might be rented from the cable company and if you buy your own, you can get them to drop that modem rental charge off your monthly bill. If the modem you buy fails, it's your problem, not theirs, but maybe that risk suits some people like it does me. For my choice of cable modem, I bought a Motorola Surfboard model SB6120 which is compliant with the DOCSIS 3.0 standard and has proven very stable. DOCSIS 2.0 vs 3.0: Basically, the DOCSIS 3.0 cable modems can use more channels for signal which allows them to provide higher speeds from the cable provider.

Wireless networking protocols:

Most home wireless networks (LAN's) use either wireless B/G or wireless N protocols. These refer to the protocols listed below:

802.11 standard:

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g and 802.11n versions to provide wireless connectivity in the home, office and some commercial establishments.

Wireless A: http://en.wikipedia.org/wiki/802.11a

IEEE 802.11a-1999 or **802.11a** is an amendment to the IEEE 802.11 specification that added a higher data rate of up to 54 Mbit/s using the 5 GHz band. It has seen widespread worldwide implementation, particularly within the corporate workspace.

Wireless B: http://en.wikipedia.org/wiki/802.11b

IEEE 802.11b-1999 or **802.11b**, is an amendment to the IEEE 802.11 specification that extended throughput up to 11 Mbit/s using the same 2.4 GHz band. This specification under the marketing name of Wi-Fi has been implemented all over the world.

Description

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s using TCP and 7.1 Mbit/s using UDP.

802.11b products appeared on the market in mid-1999, since 802.11b is a direct extension of the DSSS (Direct-sequence spread spectrum) modulation technique defined in the original standard. The Apple iBook was the first mainstream computer sold with optional 802.11b networking. Technically, the 802.11b standard uses Complementary code keying (CCK) as its modulation technique. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones. Interference issues and user density problems within the 2.4 GHz band have become a major concern and frustration for users.

Wireless G: http://en.wikipedia.org/wiki/802.11g

IEEE 802.11g-2003 or **802.11g** is an amendment to the IEEE 802.11 specification that extended throughput to up to 54 Mbit/s using the same 2.4 GHz band as 802.11b. This specification under the marketing name of Wi-Fi has been implemented all over the world.

Wireless N: http://en.wikipedia.org/wiki/802.11n

IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over the two previous standards—802.11a and 802.11g—with a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s (slightly higher gross bit rate including for example error-correction codes, and slightly lower maximum throughput) with the use of four spatial streams at a channel width of 40 Mhz. 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements, among other features.

Description

IEEE 802.11n is an amendment to IEEE 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, and IEEE 802.11w-2009, and builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the PHY (physical layer), and frame aggregation to the MAC layer.

MIMO is a technology which uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing (SDM). SDM spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver. In addition, MIMO technology requires a separate radio frequency chain and analog-to-digital converter for each MIMO antenna which translates to higher implementation costs compared to non-MIMO systems.

Channels operating at 40 MHz are another feature incorporated into 802.11n which doubles the channel width from 20 MHz in previous 802.11 PHYs to transmit data. This allows for a doubling of the PHY data rate over a single 20 MHz channel. It can be enabled in the 5 GHz mode, or within the 2.4 GHz if there is knowledge that it will not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using those same frequencies.

Coupling MIMO architecture with wider bandwidth channels offers increased physical transfer rate over 802.11a (5 GHz) and 802.11g (2.4 GHz).

****

****

Wireless Networking Security:

Most modems do not provide any firewall or encryption security. I have seen one that did, but it was in use at the home of a person who worked for NSA and is a device not generally available to the public.

Modems, whether dial-up, DSL, or Cable, provide only a connection for ONE device in the home. If you wish to connect more than one device, which is when you create a LAN or Local Area Network, you will need either a Network Hub, or a Router. As a Network Hub provides no built-in security, but only provides a many-to-one connection, I will not be discussing hubs here except to mention them in passing. Most people will get a Router to connect their multiple computing devices to the Internet through their broadband modem. I have not used a hub to connect two PC's to the Internet since back in 1998 when I was still using a dial-up modem. If you are planning to get a router, choose a well-known brand name and get one that has 4 cable ports in the back (the 5th goes to the modem) and wireless N capability.

WEP, WPA, WPA2, TKIP AES: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Wired Equivalent Privacy (**WEP**) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals".

Simply put security options:

None = none

WEP = old and hacked

WPA-PSK(TKIP) = newer, but TKIP has also been hacked

WPA2-PSK(AES)* = newer, and AES is more secure than TKIP

WPA-PSK(TKIP)+WPA2-PSK(AES) = might be used where some wireless devices are not new enough to support the WPA2-PSK(AES) standard, but less secure than using WPA2-PSK(AES) alone.

I use WPA2-PSK(AES) on my own home LAN and have also enabled other security features* available in my router, which is a Netgear

***Wireless Card Access List & Access Control enabled: The router is programmed with a list of MAC addresses of specific devices which are those you say are the only wireless devices to be allowed to connect (wirelessly) through your router. This makes it harder for hackers to get in.**