SDSU MASTERS of HOMELAND SECURITY

GEOL600 SENSOR NETWORKS

NETWORKING TECHNOLOGIES

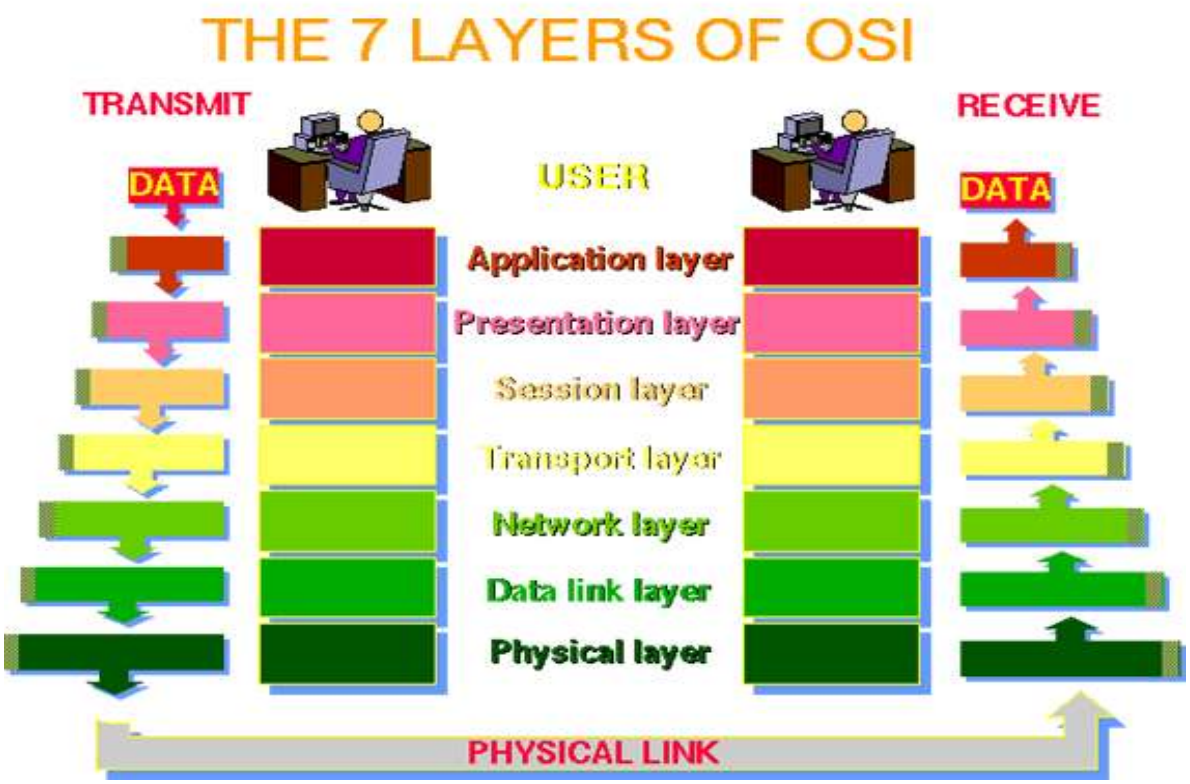
802.11

53955.29611

Open System Interconnection Model
Physical Link: Cables
Fiber Optic Advantages
Color codes for RJ45
Physical Link: RF transmission
Inverse square law
Spread spectrum modulation
OFDM
802.11 In the beginning
ISM Band
802.11b The defacto standard
802.11g Like 802.11b but faster
802.11a Betamax of 802.11
802.11n Next Generation
Crippling Mixed Mode

802.11 MAC Layer
802.11 MAC Layer Functions
Packets / Frames
802.11b PHY Layer
802.11b PLCP Frame format
MAC Layer and Data payload
802.11 DSSS Spreading Function
802.11 DSSS Modulation
802.11b Transmission Frequencies
802.11a PHY Layer
802.11g PHY Layer
802.11 Architectures
IEEE 802.11 Task Groups

OPEN SYSTEM INTERCONNECTION MODEL



- Defines networking framework for implementing protocols in seven layers
- Control is passed from Application layer to Physical layer in one station, transmitted across a physical channel to the next station and back up the hierarchy

Application
Layer 7

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level.

Presentation
Layer 6

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.

Session
Layer 5

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Transport
Layer 4

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network
Layer 3

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link
Layer 2
LLC
MAC

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical
Layer 1
PHY

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

www.webopedia.com

PHYSICAL LINK : Cables

copper cables

fiber optic cables

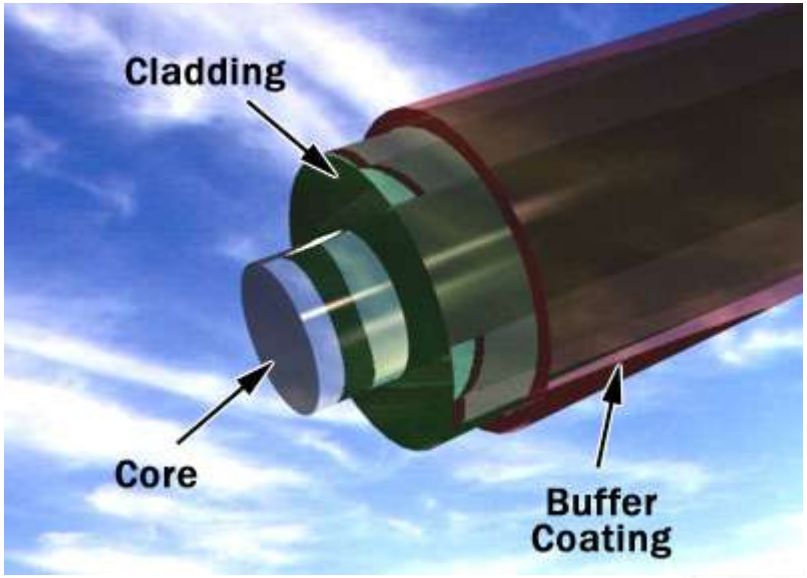
Ethernet networks use unshielded twisted pair (UTP) Category 5 cable.
CAT5 cable runs should not exceed 100 meters.

CAT5 cables are typically terminated with RJ-45 connectors

Both single mode and multimode fiber optic cable may be used in Ethernet network designs. Although multi-mode fiber has a specific distance limitation of 2km, distance limitations of single-mode fiber vary according to the proprietary system in use. All are in excess of 2km
There are two common fiber optic connectors: SC and ST

FIBER OPTIC ADVANTAGES

- SPEED: Fiber optic networks operate at high speeds - up into the gigabits
- BANDWIDTH: large carrying capacity
- DISTANCE: Signals can be transmitted further without needing to be "refreshed"
- RESISTANCE: Greater resistance to EM noise such as radios, motors or nearby cables.
- MAINTENANCE: Fiber optic cables costs much less to maintain.



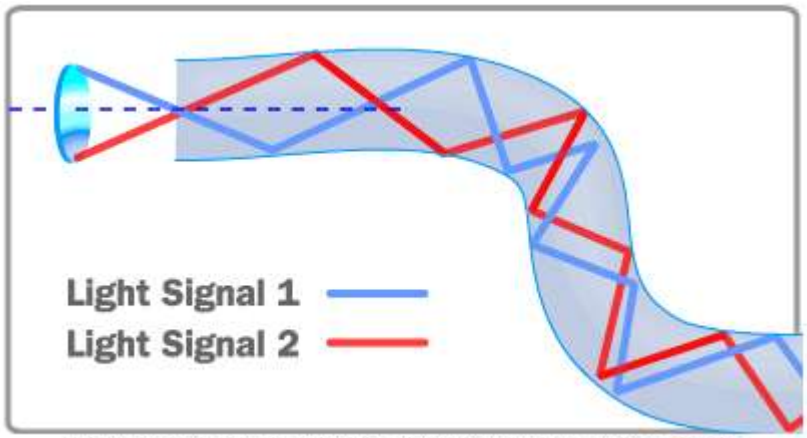
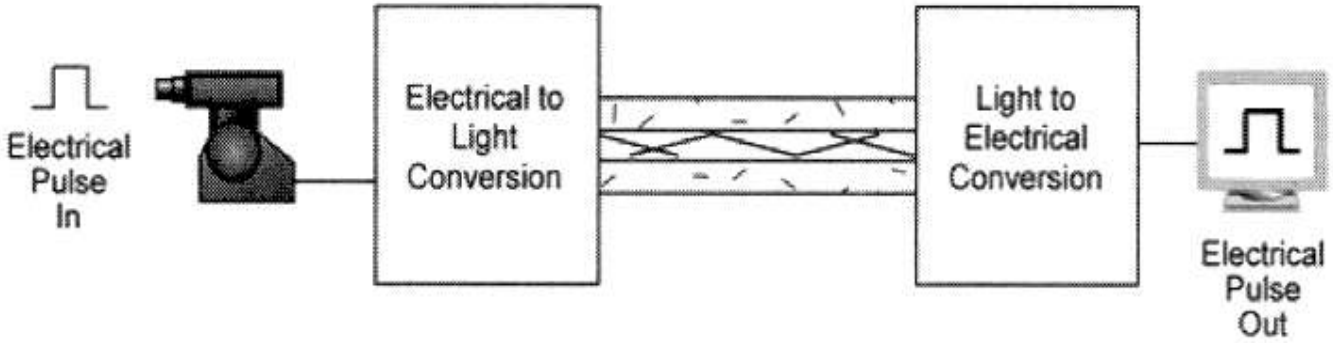


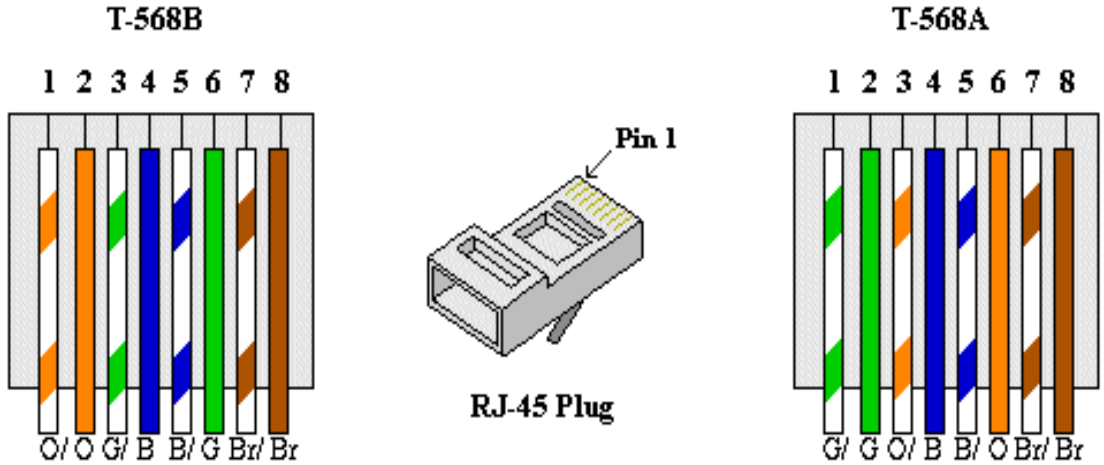
Diagram of total internal reflection in an optical fiber



COLOR CODES FOR RJ-45 Ethernet Plug

Eight-conductor data cable (Cat 3 or Cat 5) contains 4 pairs of twisted wires. To maintain reliability, you should not untwist them more than necessary (1/4”)

The pairs designated for 10BaseT Ethernet are orange and green. The other two pairs, brown and blue, are unused.



There are two wiring standards for these cables, called T-568A and T-568B. They differ only in pin assignments, not in uses of the various colors. T-568A is supposed to be standard for new installations, and T-568B the alternative. However, most off-the-shelf data equipment and cables seem to be wired to T568B.

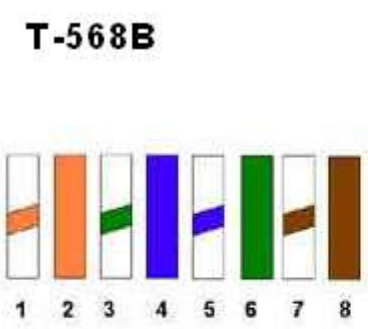
Straight-Through vs Cross-Over

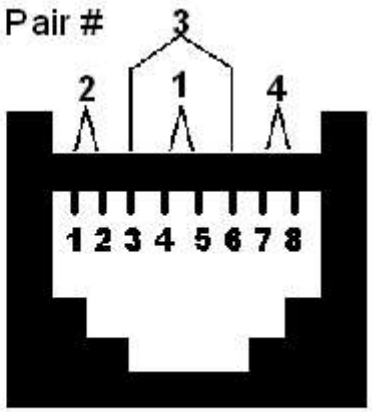
The only time you cross connections in 10BaseT is when you connect two Ethernet devices directly together without a hub or connect two hubs together. Then you need a "cross-over" patch cable, which crosses the transmit and receive pairs.

To make a cross-over cable wire one end with the T-568A standard and the other with the T-568B standard.

T-568B

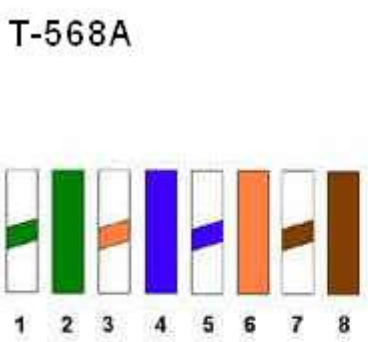
Pin	Color	Pair	Description
1	white/orange	2	TxData +
2	orange	2	TxData -
3	white/green	3	RecvData +
4	blue	1	Unused
5	white/blue	1	Unused
6	green	3	RecvData -
7	white/brown	4	Unused
8	brown	4	Unused

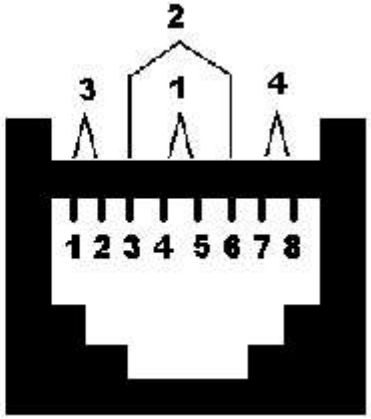




T-568A

Pin	Color	Pair	Description
1	white/green	3	RecvData +
2	green	3	RecvData -
3	white/orange	2	TxData +
4	blue	1	Unused
5	white/blue	1	Unused
6	orange	2	TxData -
7	white/brown	4	Unused
8	brown	4	Unused





Note: Odd pin numbers are always the striped wires..

PHYSICAL LINK : RF transmission

IEEE 802.11 (WiFi)WLAN 802.11a/b/g/n
Wireless LAN technology including WiFi.

IEEE 802.15 WPAN / ZIGBEE
Wireless Personal Area Networking

IEEE 802.16 WiMAX WMAN
Wireless Metropolitan Area Networking
and WiMAX technology

HiperLAN,HiperLAN2
Wireless LAN technology.

Bluetooth
Short-range radio

CDMA
Code Division Multiple Access

UMTS / 3G
Universal Mobile Telephony System
Third Generation Mobile

GPRS
General Packet Radio Service

GSM
General System for Mobiles

UWB
Ultra Wide Band

Satellite
Communications, TV, Remote Sensing

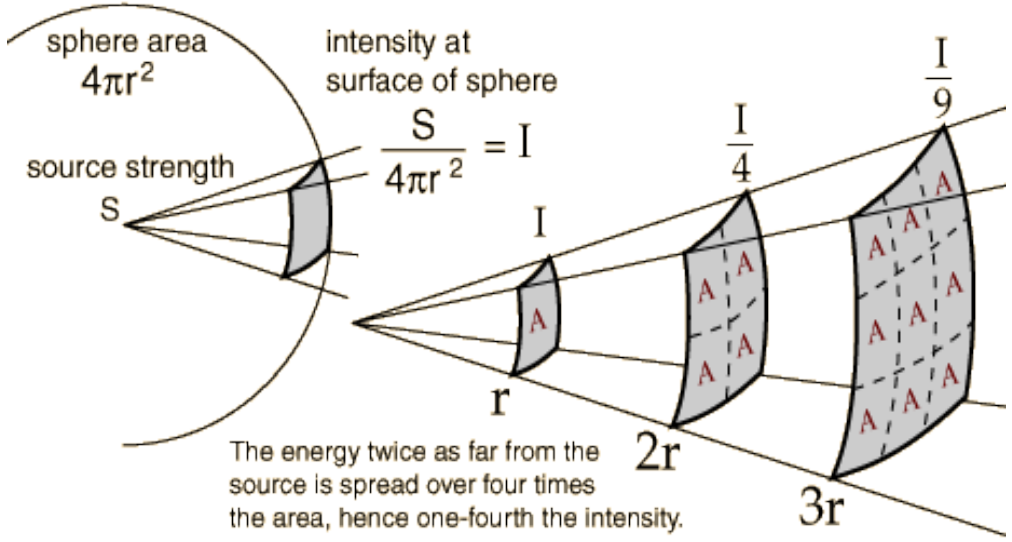
RADAR
Radio and Distance Ranging

GPS
Global Positioning System

INVERSE SQUARE LAW

Any point source which spreads its influence equally in all directions without a limit to its range will obey the inverse square law. This comes from strictly geometrical considerations.

The intensity of the influence at any given radius r is the source strength divided by the area of the sphere. Being strictly geometric in its origin, the inverse square law applies to diverse phenomena. Point sources of gravitational force, electric field, light, sound or radiation obey the inverse square law.

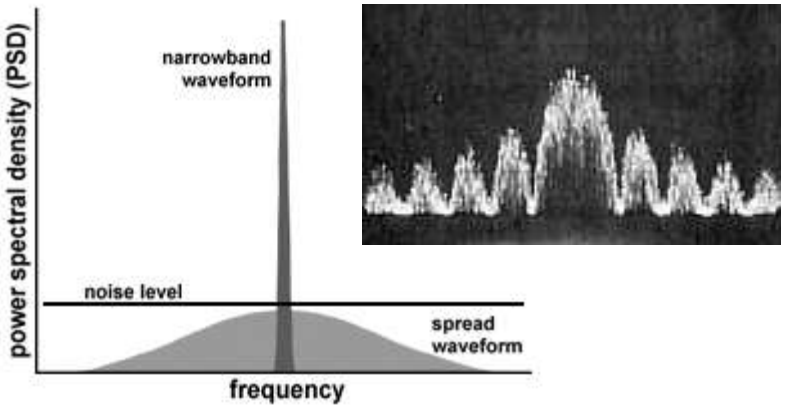


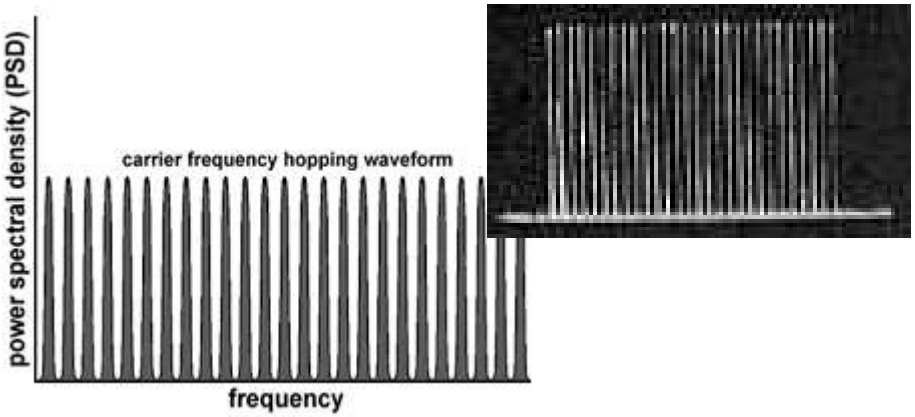
Will the smell of a skunk on top of a flag pole (point source) drop off according to the inverse square law?

hyperphysics.phy-astr.gsu.edu/hbase/forces/isq.html

SPREAD SPECTRUM MODULATION

Spread Spectrum (**SS**) modulation spreads data, by using a coding sequence, over an RF bandwidth wider than would normally be required by the content of the original data stream (data bandwidth). This technique provides high levels of communication reliability and security, and typically enables higher data transmission rates than are achieved with narrowband carriers.





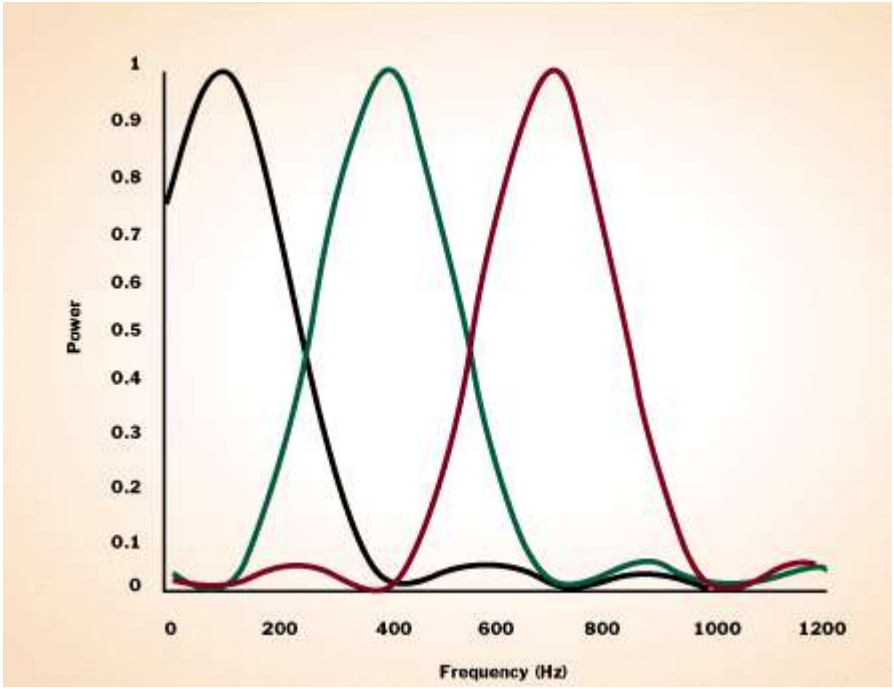
Direct Sequence (**DSSS**) modulation uses a code sequence to directly modulate a narrowband carrier (usually by phase-shift keying) and continuously distribute or spread the narrowband carrier over a much broader portion of an assigned frequency range. The code sequence is duplicated and synchronized at the receiver, where the signal is compressed or correlated back into its original narrowband form.

Frequency Hopping (**FHSS**) involves the transmitter and receiver in a system synchronously changing carrier frequencies (of narrowband waveform) rapidly based on a pattern derived from a code sequence. In this way, the data signal is spread over a broad RF band through continual narrowband frequency "hopping"

OFDM : Orthogonal Frequency Division Multiplexing

An OFDM-based system divides a high-speed serial information signal into multiple lower-speed sub-signals that the system transmits simultaneously at different frequencies in **parallel.** This parallel-form of transmission over multiple subcarriers enables OFDM-based WLANs to operate at higher aggregate data rates

The benefits of OFDM are high spectral efficiency, resiliency to RF interference, and lower multi-path distortion. The orthogonal nature of OFDM allows subchannels to overlap, having a positive effect on spectral efficiency. Each one of the subcarriers transporting information are just far enough apart from each other to theoretically avoid interference.



www.commsdesign.com/story/OEG20010122S0078

802.11 In the beginning 2.4 GHz 2Mbps

The first wireless standard to be defined in the 802 wireless family was 802.11. It was approved by the IEEE in 1997, and defines three possible physical layers:

- **FHSS** Frequency Hopping Spread Spectrum at 2.4 GHz,
- **DSSS** Direct Sequence Spread Spectrum at 2.4 GHz, and
- **Infrared**.

802.11 could achieve data rates of 1 or 2 Mbps. 802.11 radios that use DSSS are interoperable with 802.11b and 802.11g radios at those speeds, while FHSS radios and Infrared obviously are not.

The original 802.11 devices are increasingly hard to come by, but can still be useful for point-to-point links with low bandwidth requirements.

PROS

- Very inexpensive (a few dollars or even free) when you can find them.
- DSSS cards are compatible with 802.11b/g.
- Infrared 802.11 cards (while rare) can offer interference-free wireless connections, particularly in noisy RF environments.
- Infrared also offers increased security due to significantly shorter range.

CONS

- No longer manufactured.
- Low data rate of 1 or 2 Mbps.
- FHSS radios are incompatible with everything else.

Probably best avoided altogether.

ISM BAND

802.11 operates in the highly populated and unlicensed **2.4 GHz ISM** (Industrial Scientific Medical) GHz ISM band (2.40 to 2.4835 GHz), which provides only 83 MHz of spectrum to accommodate a variety of other radiating products, including cordless phones, microwave ovens, other WLANs, and personal area networks (PANS). This makes susceptibility to interference a primary concern.

Frequency Bands Comparisons

Frequency	ISM	WLAN	U-NII	HiperLAN
902-928 MHz	**1**	**1**	0	0
2400 -2483.5 GHz	**1**	**1**	0	0
5150 – 5350 GHz	0	0	**1**	**1**
5470 -5725 GHz	0	0	0	**1**
5725-5850 GHz	**1**	**1**	**1**	0

Wireless LAN radios operate at power levels five to six times lower than most cell phones or handheld radios , and operate on a non-interference basis. Non-interference means that they may not cause harmful interference but they must accept harmful interference (including interference that disrupts service).

Power comparisons

Transmitter	Frequency	Power output (W, EIRP)
VHF handheld radio	150 Mhz	3
Cellular phone	860 Mhz	0.6
Wifi PCMCIA card	2.4 GHz	0.1

802.11 b The De Facto Standard 2.4 GHz 11Mbps

It is the de facto wireless networking standard of the last few years. It offers good range and respectable throughput. It operates using **DSSS** at 2.4 GHz, and automatically selects the best data rate (either 1, 2, 5.5 or 11 Mbps), depending on available signal strength.

Its greatest advantage at this point is its ubiquity: millions of 802.11b devices have shipped, and the cost of client and access point gear is plummeting.

PROS

- Cheap and ubiquitous in consumer devices, add-on cards, and APs.
- 802.11b "hot spots" are available in many public areas.
- With many people using and experimenting with it, 802.11b is arguably the most hackable (and customizable) wireless protocol on the planet.

CONS

- The 11 Mbps data rate of 802.11b is already surpassed by 802.11 a / g.
- 802.11 b's channel scheme allows only for 3 nonoverlapping channels. (1, 6, 11)
- Standard 802.1 1b security features are less than effective.

Raw	Actual data rate
11 Mbps	**5 Mbps**

Average Internet speeds still being slower than 802.11 b, it is likely to be used as a mechanism for providing access for some time yet.
802.11b will probably get a life extension from its competitor 802.11g, as the newer 802.11 g equipment will work with existing 802.11 b access points.

802.11 g Like 802.11b but Faster 2.4 GHz 54Mbps

802.11g uses the **OFDM** encoding of 802.11 a in the 2.4 GHz band, and also falls back to **DSSS** to maintain backwards compatibility with 802. 11b radios. This is a very promising technology-so promising, in fact, that the lack of ratification didn't stop some manufacturers from shipping gear that used the draft standard, even before it was ratified.

PROS

- Very high data rates of up to 54 Mbps. (108 with vendor specific options)
- Backwards compatibility with 802.11b offers simple upgrade path for existing users.
- 802.11g uses the same band as 802.11b, so antennas and feed lines can be reused.
- Allows existing 802.11b users to continue to use the network, while offering a speed boost for 802.11g users.

CONS

- Slightly more expensive than 802.11b, but prices are expected to drop.
- As it uses the 2.4 GHz ISM band, 802.11g will have to contend with many other devices, leading to more interference in crowded areas.

Raw	Actual data rate
54 Mbps	**25 Mbps**

If you are building a network from scratch, strongly consider 802.11g.
802.11g will likely be the next massively ubiquitous wireless technology, as it promises many of the advantages of 802.11a without significantly raising cost or breaking backwards compatibility.

Flickenger: Wireless Hacks, O'Reilly

802.11 a Betamax of 802.11 5.8 GHz 54Mbps

Early on, 802.11a was widely touted as the "802.11b killer" but still isn't popular.

802.11 a offers more channels, higher speed, and less interference than other protocols. It uses Orthogonal Frequency Division Multiplexing (**OFDM**) encoding believed to cope better with reflections caused by obstacles (multipath)

PROS

- Very fast data rates: up to 54 Mbps (raw), with some vendors providing 72 Mbps or faster with proprietary extensions.
- Uses the much less cluttered (for now, in the U.S.) UNII band, at 5.8 GHz.

CONS

- Limited range compared to 802.11b and 802.1 1g at the same power levels and gain. Signals at 5 GHz appear to travel only half as far as signals at 2.4 GHz
- Most 802.11a client devices are add-on cards, and the technology is built into few consumer devices (specifically laptops).
- Upgrading from 802.1 1b can be painful, as 5.8 GHz radiates very differently from 2.4 GHz, requiring a new site survey and likely more APs.

Raw	Actual data rate
54 Mbps	**27 Mbps**

These devices are sometimes labelled "Wi-Fi," just like the incompatible 802.11b. Be sure to look for the specification's real name (802.11a) when purchasing. Would make good point-to-point systems if external antennas were more readily available.

802.11 n Next Generation 100 Mbps

In January 2004 IEEE announced that it had formed a new 802.11 Task Group (TGn) to develop a new amendment to the 802.11 standard for local-area wireless networks
The standardization process is expected to be completed by the end of 2006..

The actual data throughput will be at least 100 Mbit/s (which may require an even higher raw data rate at the PHY level), and so up to 4–5 times faster than 802.11a or 802.11g, and perhaps 20 times faster than 802.11b.

802.11n will also offer a greater operating distance than current 802.11 networks.

802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output) antenna techniques. These additional transmitter and receiver antennas allow for increased data throughput and greater range by exploiting the multipath electromagnetic waves propagation (a.k.a "spatial multiplexing" or "spatial diversity").

Belkin is shipping (01.2005) Pre-N router and NIC which does not drop to the lowest networking speed in a mixed-mode environment - Pre-N products will continue to transmit at a link rate of 108Mbps.

catalog.belkin.com/IWCatProductPage.process?Product_Id=184316

CRIPPLING MIXED MODE b/g

Mixed-mode wireless networks -- those that simultaneously run clients with both 802.11b and g can suffer speed wise.
Specifically, use of the slower 802.11b can drag down throughput on 11g.

Furthermore, as transmission speed drops with distance, even devices rated for higher speeds will throttle the network if they are at a range exceeding optimal parameters. Any wireless devices running at a higher speed is going to be impacted by a slower device on the same channel.

Traffic analogy:slower wifi clients ahead in the queue

802.11 MAC LAYER

The 802.11 standard specifies a common **medium access control** (MAC) Layer, which provides a variety of functions that support the operation of 802.11-based wireless LANs. The MAC Layer manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium.

Often viewed as the "brains" of the network, the 802.11 MAC Layer uses an 802.11 Physical (PHY) Layer, such as 802.11b or 802.11a, to perform the tasks of carrier sensing, transmission, and receiving of 802.11 frames.

Medium access basics

Before transmitting frames, a station must first gain access to the medium, which is a radio channel that stations share. The 802.11 standard defines two forms of medium access, distributed coordination function (DCF) and point coordination function (PCF).

DCF is mandatory and based on the CSMA/CA (carrier sense multiple access with collision avoidance) protocol. With DCF, 802.11 stations contend for access and attempt to send frames when there is no other station transmitting. If another station is sending a frame, stations are polite and wait until the channel is free

No known wireless NICs or access points on the market today implement PCF.

802.11 MAC LAYER FUNCTIONS

The following lists primary 802.11 MAC functions, especially as they relate to infrastructure wireless LANs:

Scanning: The 802.11 standard defines both passive and active scanning; whereby, a radio NIC searches for access points.

Authentication: Authentication is the process of proving identity, and the 802.11 standard specifies two forms: Open system authentication and shared key authentication.

Association: Once authenticated, the radio NIC must associate with the access point before sending data frames. Association is necessary to synchronize the radio NIC and access point with important information, such as supported data rates.

RTS/CTS: The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS.

Power Save Mode: The optional power save mode that a user can turn on or off enables the radio NIC to conserve battery power when there is no need to send data.

Fragmentation: The optional fragmentation function enables an 802.11 station to divide data packets into smaller frames. This is done to avoid needing to retransmit large frames in the presence of RF interference.

www.wi-fiplanet.com/tutorials/article.php/1216351

Packets / Frames / Datagrams / PDUs

A packet can be defined as the unit of data at any layer of the protocol stack, prior to, or after transmission. It describes chunks of data created by software, not hardware.

A frame is a packet which has been encoded for transmission over a particular link.A frame can be defined as the unit of data transferred across the network, defined at the datalink (network access) layer of the protocol stack.

A datagram is a self-contained packet, one which contains enough information in the header to allow the network to forward it to the destination independently of previous or future datagrams.

A PDU (Protocol Data Unit) is a chunk of data created and/or labelled by a particular protocol. TCP, UDP and IP all create "protocol data units". The term is somewhat synonymous with packet or frame.

802.11b PHY LAYER

In addition to MAC layer, 802.11 comprises several physical layers that specify the transmission and reception of 802.11 frames:
Physical Layer Convergence Procedure (PLCP) sublayer and
Physical Medium Dependent (PMD) sub-layer.

These terms divide the major functions that occur within the Physical Layer.
PLCP prepares 802.11 frames for transmission and directs the
PMD to actually transmit signals, change radio channels, receive signals, and so on.

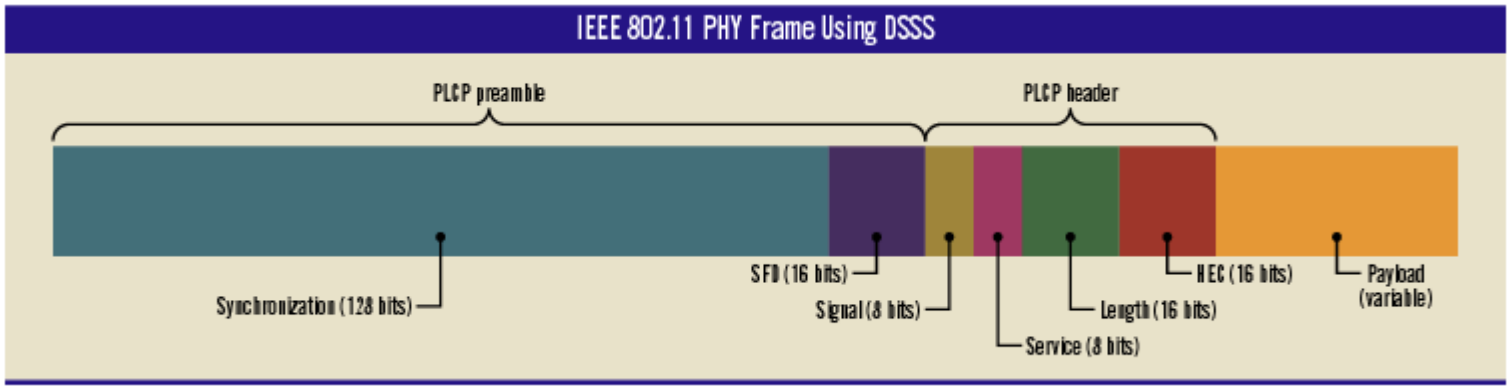
802.11b PLCP FRAME FORMAT

PLCP takes each 802.11 frame that station has to transmit and forms a PLCP protocol data unit (PPDU). The resulting PPDU includes the following fields in addition to the frame fields imposed by the MAC Layer.

		Size (bits)
PLCP Preamble	Synchronization, radio gain, CCA	128
	Start Frame Delimiter (SFD)	16
PLCP Header	Signal - transmission speed (1, 2, 5.5 or 11 Mbps)	8
	Service - reserved for future use	8
	Length - time to transmit PPDU marks end of frame	16
	HEC - header checksum	16
PSDU	Physical Layer Service Data Unit (actual 802.11 frame)	~
		192

Note the overhead (24 bytes) compared to wired Ethernet (8 byte preamble)

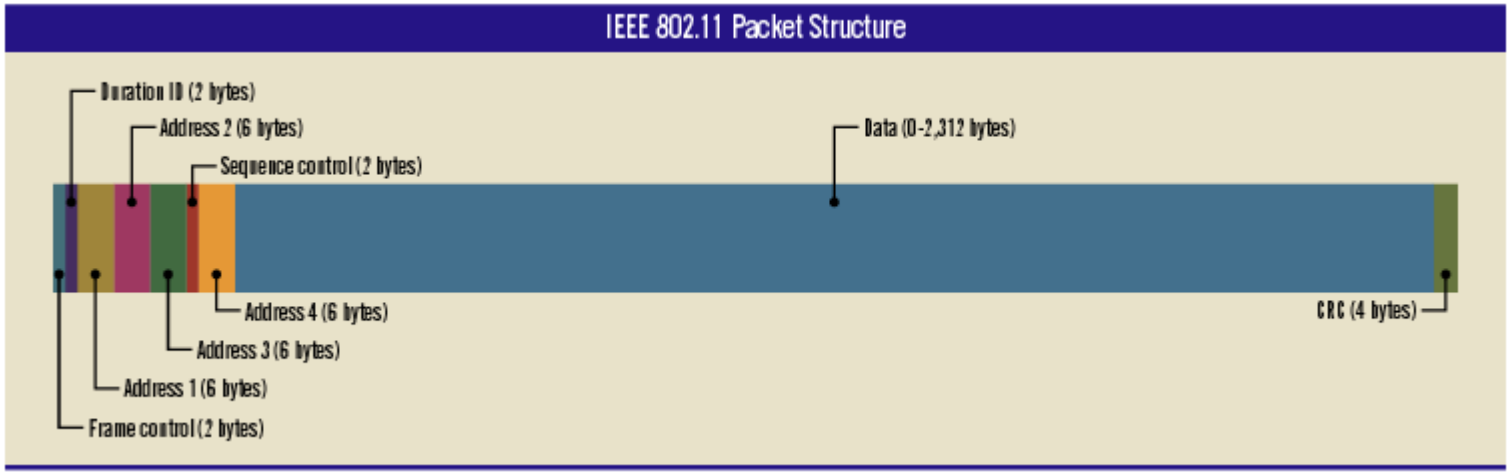
For compatibility reasons, the 192-bit header PLCP fields are always transmitted at
1 Mbps.even for faster data rates. For this reason, 802.11b is at best only 85% efficient at the physical layer

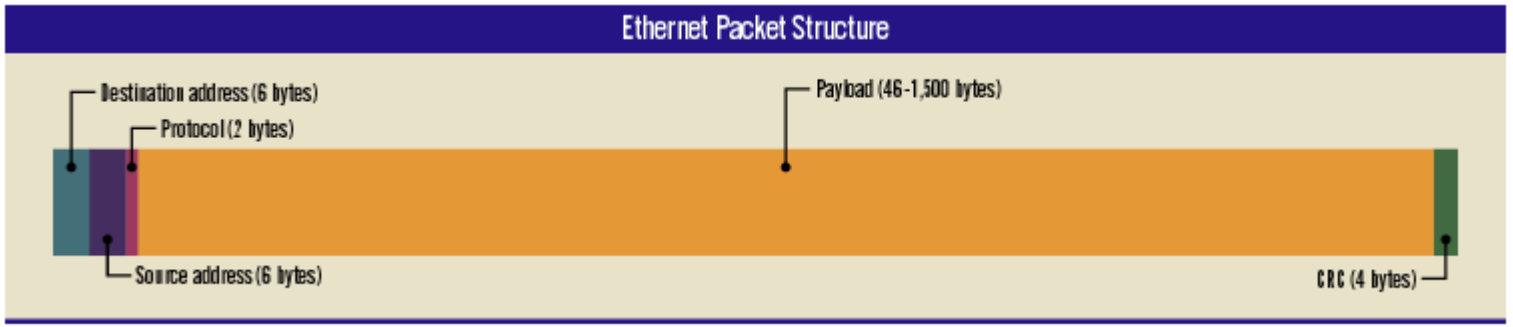


www.networkcomputing.com/1115/1115ws2.html

MAC Layer and Data Payload

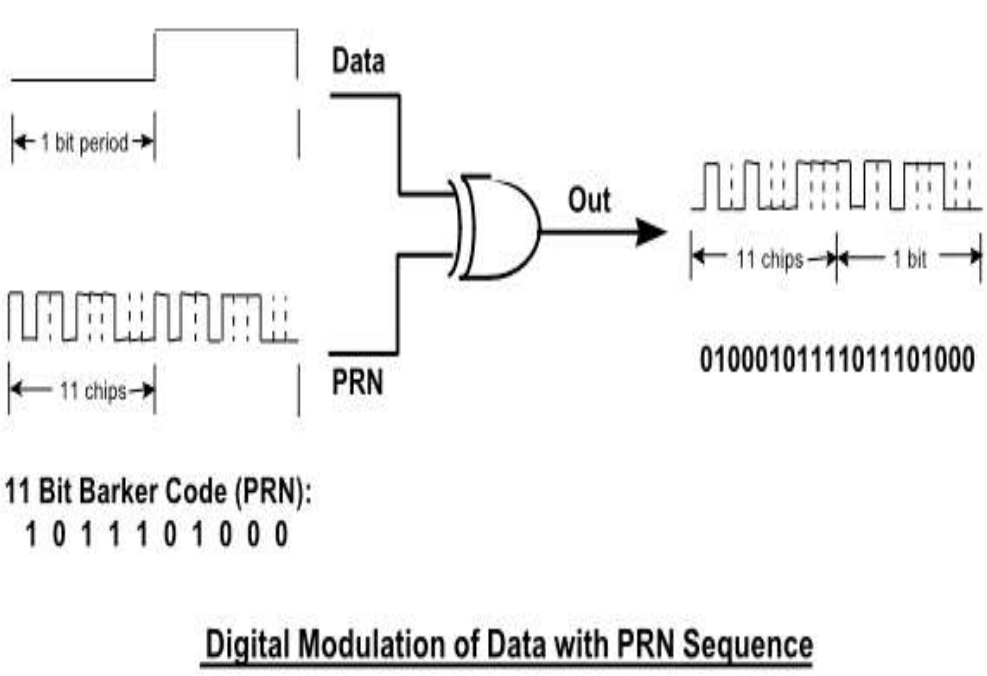
In addition to collision avoidance, timing and roaming, the MAC layer is also responsible for identifying the source and destination address of the packet being sent, as well as the data payload and a CRC. The entire payload of the packet, including the MAC header, is transmitted at the rate specified in the PLCP



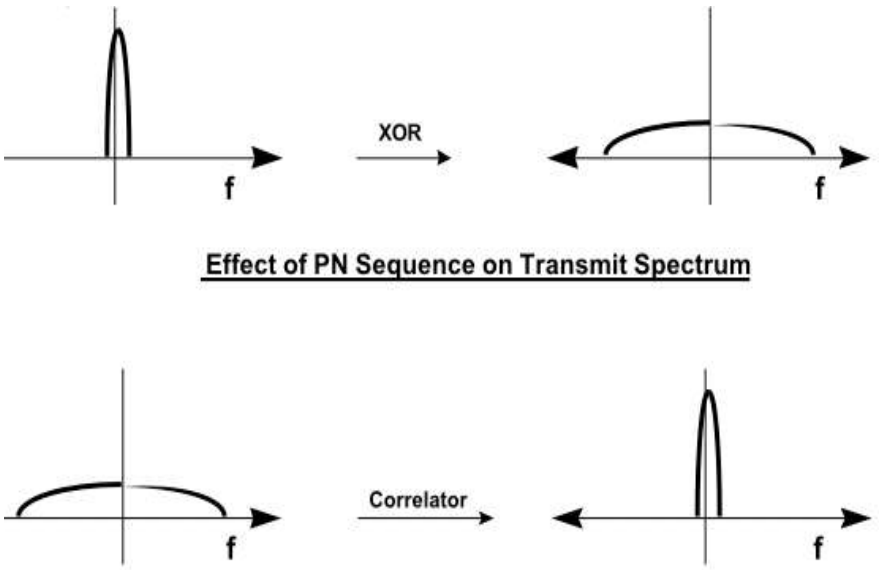


802.11b DSSS SPREADING FUNCTION

802.11b uses DSSS to disperse the data frame signal over a relatively wide (22 MHz) portion of the 2.4 GHz ISM band.



Digital Modulation of Data with PRN Sequence



Received Signal is Correlated with PN to Recover Data and Reject Interference

The transmitter combines the PPDU with a spreading sequence through the use of a binary adder. The spreading sequence is a binary code.
For 1- 2 Mbps operation, spreading code is the **11-chip Barker PN sequence**.

The binary adder effectively multiplies the length of the binary stream by the length of the sequence, which is 11. This increases the signalling rate and makes the signal span a greater amount of frequency bandwidth.

The receiver needs to use the same sequence to pull the signal out of the noise.

802.11b DSSS MODULATION

Modulator converts the spread binary signal into an analog waveform through the use of different modulation types, depending on which data rate is chosen.

1-Mbps transmission uses BPSK (Binary Phase Shift Keying) (one phase shift per bit),
This shifts the phase of the center transmit frequency to distinguish a binary 1 from a binary 0 within the data stream.

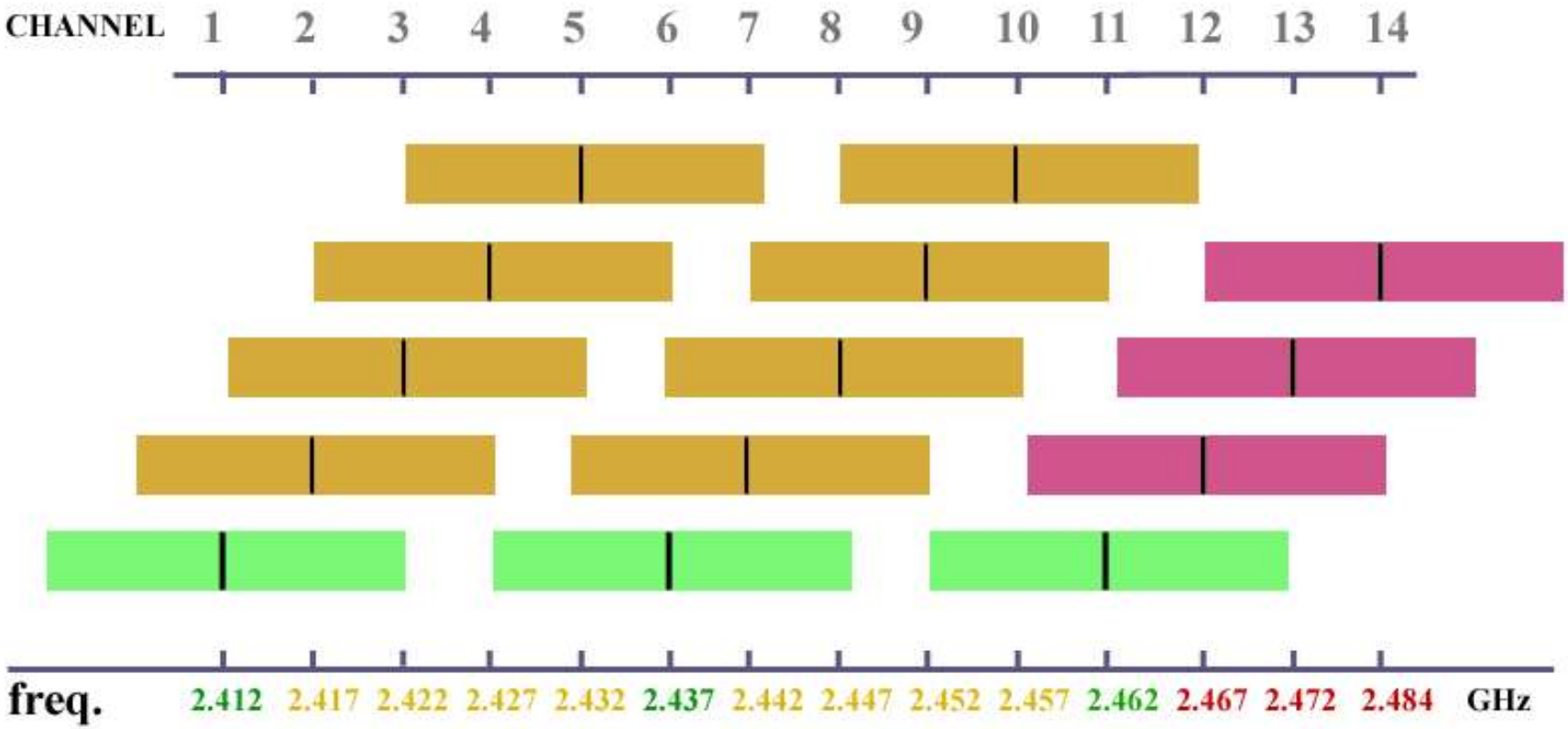
2-Mbps transmission uses QPSK (Quadrature Phase Shift Keying). QPSK uses four rotations (0, 90, 180 and 270 degrees) to encode 2 bits of information in the same space as BPSK encodes 1.
This process enables the data stream to be sent at 2Mbps while using the same amount of bandwidth as the one sent at 1Mbps. The modulator uses similar methods for the higher, 5.5Mbps and 11Mbps data rates.

5.5Mbps and 11Mbps operation of 802.11b doesn't use the Barker sequence. **Complementary Code Keying** (CCK) provides the spreading sequences for these higher data rates.
CCK derives a different spreading code based on fairly complex functions depending on the pattern of bits being sent. 64 unique code words can be used to encode the signal, up to 6 bits can be represented by any one particular code word (instead of the 1 bit represented by a Barker symbol)

The modulator simply refers to a table for the spreading sequence that corresponds to the pattern of data bits being sent. This is necessary to obtain the most efficient processing of the data in order to achieve the higher data rates.

802.11b TRANSMISSION FREQUENCIES

The transmitter's modulator translates the spread signal into an analog form with a center frequency corresponding to the radio channel chosen by the user.
The occupied bandwidth of the spread-spectrum channel is 22 MHz, so the ISM band accommodates only three non-overlapping channels spaced 25 MHz apart



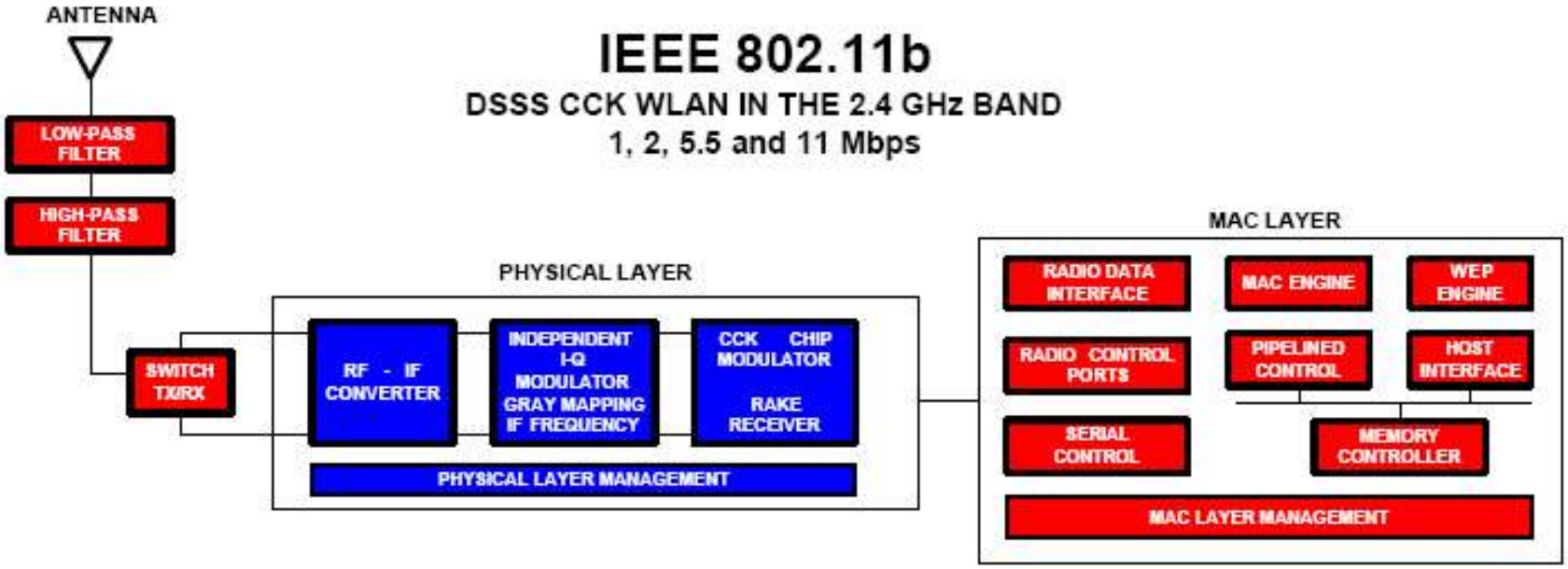
Channel overlap can cause reductions in performance.
In the U.S channels 1, 6, and 11 are the only non-overlapping channels available.

Various countries limit the use of these channels:
the U.S. only allows the use of channels 1 through 11,
the U.K. can use 1 through 13. Japan authorizes the use of all 14 channels.

IEEE 802.11b

DSSS CCK WLAN IN THE 2.4 GHz BAND

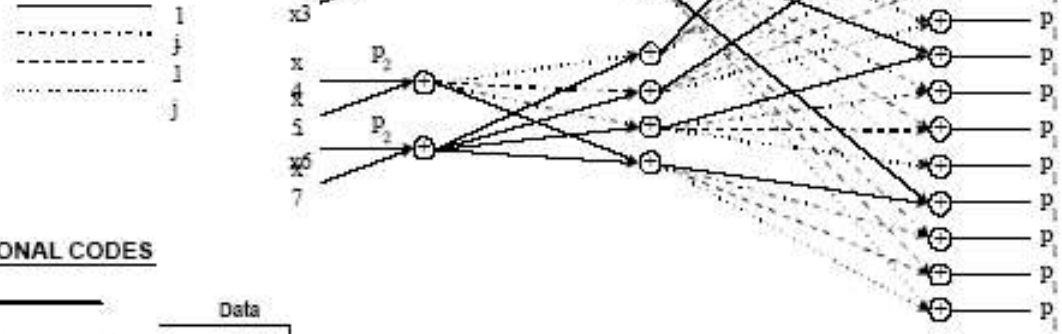
1, 2, 5.5 and 11 Mbps



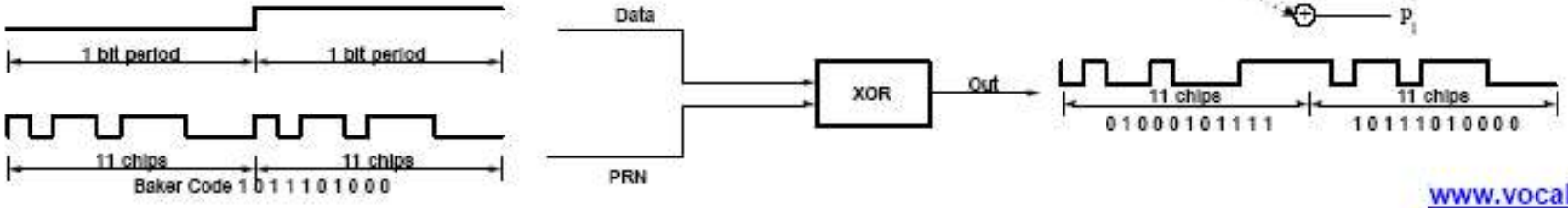
→ RECEIVER . Modified Fast Walsh Transform

$p = 1, j, -1, -j$

$p^2 = 1, j, -1, -j$



→ TRANSMITTER: 64 PRN ORTHOGONAL CODES



www.vocal.com

802.11a PHY LAYER

802.11a PLCP Frame Fields

802.11a PLCP transforms each frame into a PPDU, that includes the following fields:

PLCP Preamble of 12 symbols that enables acquisition of incoming OFDM signals.
Rate identifies the data rate of the frame. As with 802.11b, the 802.11a PLCP fields, however, are always sent at the lowest rate of 6Mbps.
Service synchronize the descrambler in the receiver
Pad Bits contains a number of bits in order to modify the frame size to equal a specific multiple of bits coded in an OFDM symbol

OFDM in Operation

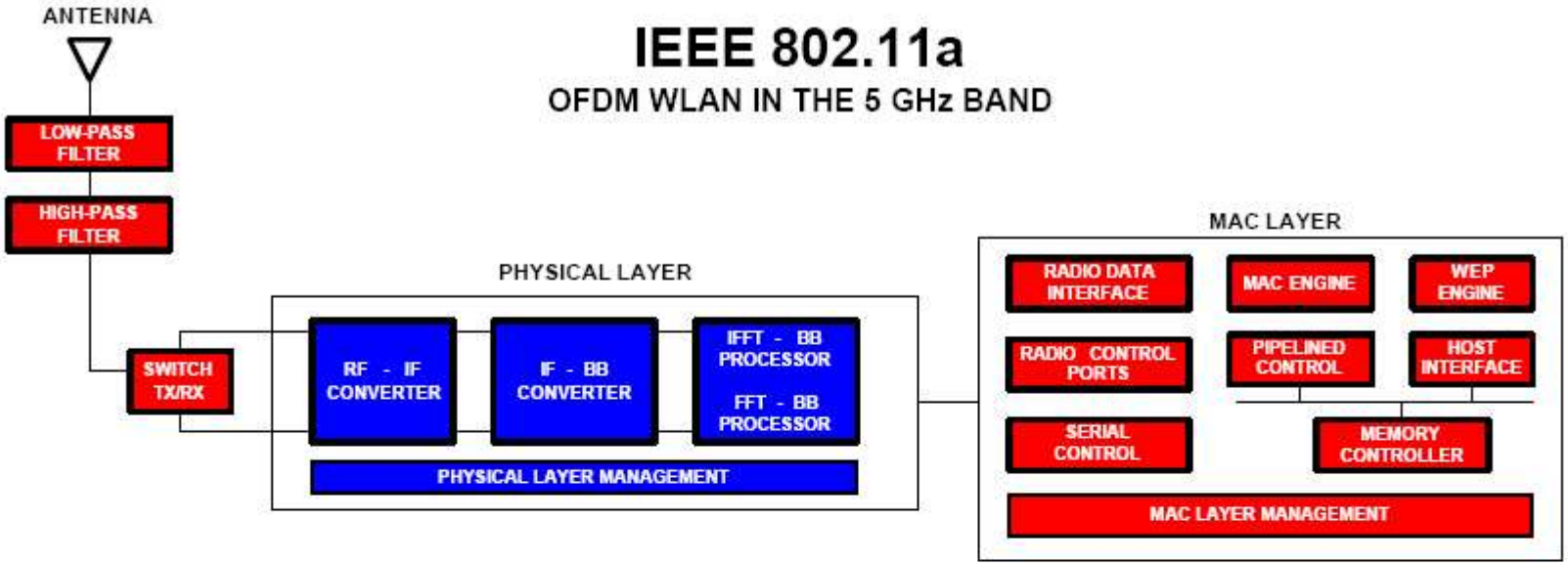
OFDM divides a data signal across 48 separate sub-carriers within a 20MHz channel to provide transmissions of 6, 9, 12, 18, 24, 36, 48, or 54Mbps. Data rates of 6Mbps, 12Mbps, and 24Mbps are mandatory for all 802.11-compliant products.

Different modulation types are used depending on which data rate is chosen. For 6Mbps operation, the PMD uses binary phase shift keying (BPSK), which shifts the phase of the transmit center frequency to represent different data bit patterns. The higher data rates, such as 54Mbps, employ quadrature amplitude modulation (QAM) to represent data bits by varying the transmit center frequency with different amplitude levels in addition to phase shifts.

The U.S. operating frequencies fall into the national information structure (U-NII) bands: there are twelve, 20MHz channels, with different output power limits.

IEEE 802.11a

OFDM WLAN IN THE 5 GHz BAND



Modulation Techniques

Data Rate (Mbps)	Modulation	Coding Rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	8	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	1/2	4	192	144
48	16-QAM	3/4	4	288	192
54	64-QAM	2/3	6	288	216

OFDM Operating Bands and Channels

Band	Channel numbers	Frequency (MHz)	Maximum output power
U-NII lower band 95.15 to 5.25 MHz	36	5180	40mW (2.5mW/MHz)
	40	5200	
	44	5220	
	48	5240	
U-NII lower band 95.15 to 5.25 MHz	52	5260	200mW (12.5mW/MHz)
	56	5280	
	60	5300	
	64	5320	
U-NII lower band 95.15 to 5.25 MHz	149	5745	800mW (50mW/MHz)
	153	5765	
	157	5785	
	161	5805	

Frame Format

www.vocal.com

802.11g PHY LAYER

802.11g's higher speed comes from using the Orthogonal Frequency Division Multiplexing (OFDM) modulation scheme - the same as used in 802.11a. Backward compatibility comes from using the 2.4GHz band, supporting the old Complementary Code Keying (CCK) modulation scheme used by 802.11b, and new "protection" mechanisms.

OFDM is becoming very popular for high-speed transmission. In addition to being selected for use within the 802.11g PHY Layer, OFDM is the basis for the European-based HiperLAN/2 wireless LAN standards. In fact the 802.11a PHY Layer is very similar to the HiperLAN/2 PHY.

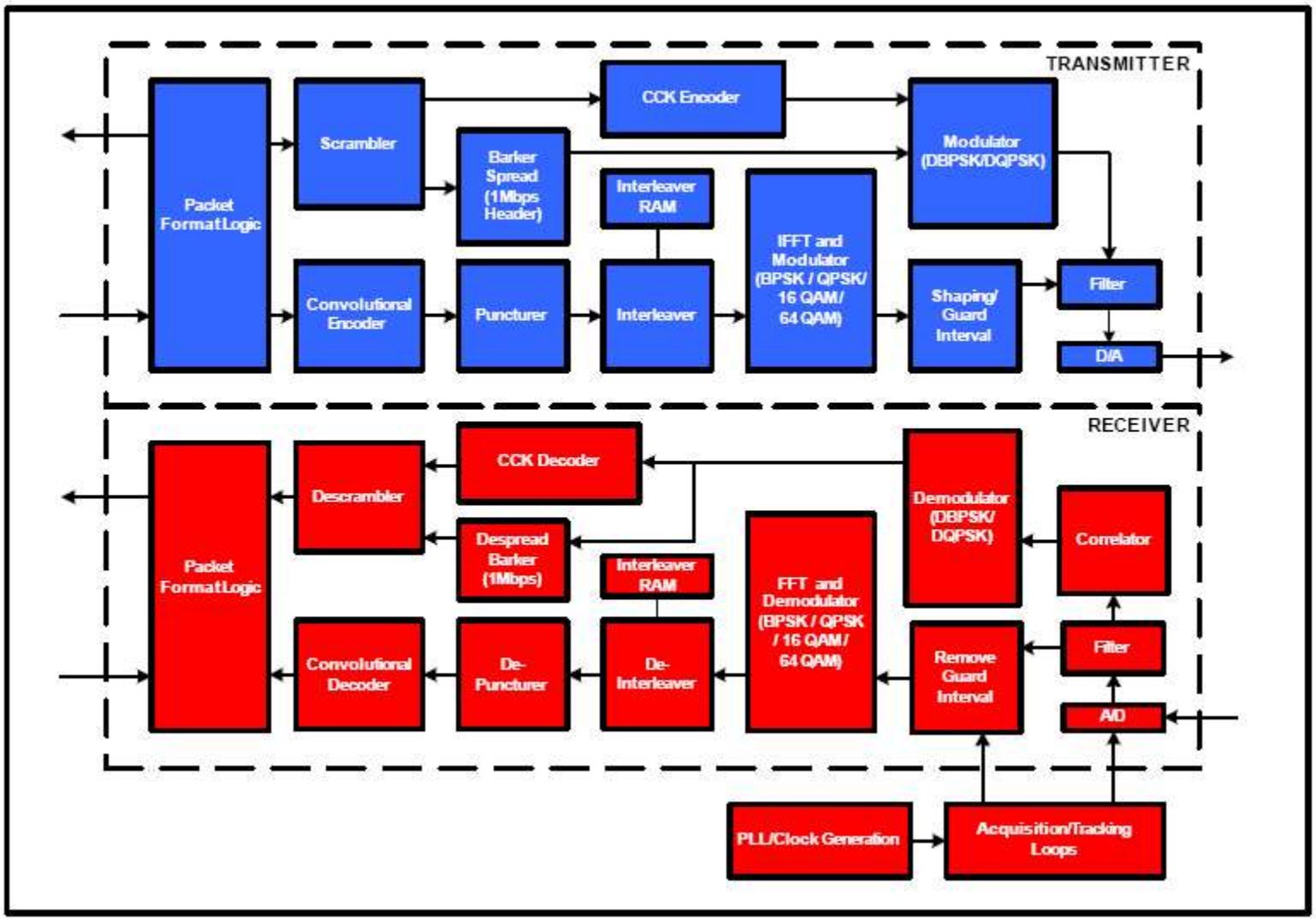
802.11g also includes:

A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the **extended rate PHY (ERP)**. The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds).
The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

An optional MAC mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate. RTS/CTS is also optional in 802.11b.

IEEE 802.11g

ERP WLAN in the 2.4 GHz Band

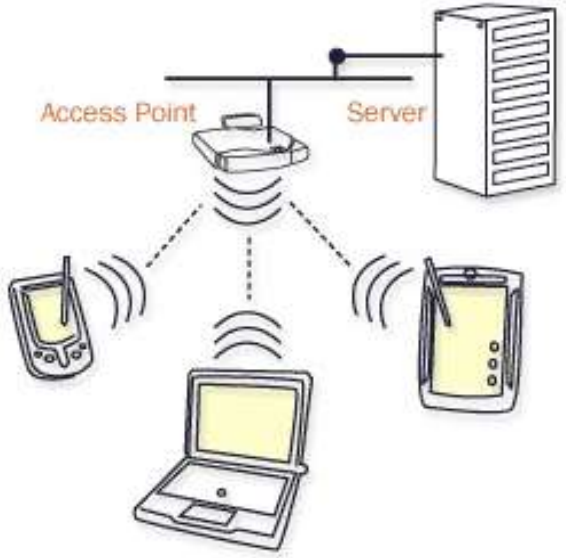


802.11 ARCHITECTURES

802.11b defines two possible (and mutually exclusive) radio modes that stations can use to intercommunicate: BSS and IBSS.

BSS Basic Service Set.

In this operating mode, one station (BSS master, usually an access point) acts as a gateway between the wireless and a wired (likely Ethernet) backbone. Before gaining access to the wired network, wireless clients (BSS clients) must first establish communications with an access point within range. Once the AP has authenticated the wireless client, it allows packets to flow between the client and the attached wired network, either routing traffic at Layer 3, or acting as a true Layer 2 bridge.

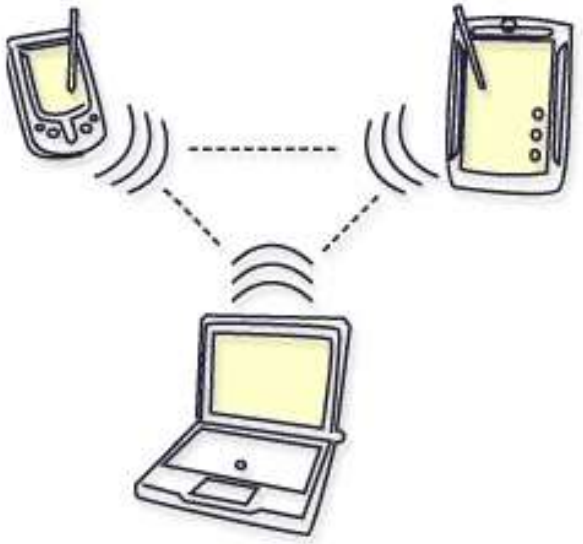


ESS Extended Service Set

In this mode a physical subnet that contains more than one access point (AP). In this sort of arrangement, the APs can communicate with each other to allow authenticated clients to "roam" between them, handing off IP information as the clients move about. Note that (as of this writing) there are no APs that allow roaming across networks separated by a router.

Basic / Extended Service Sets are also referred to as **INFRASTRUCTURE mode**

IBSS (Independent Basic Service Set)



Referred to as **Ad-Hoc** or **Peer-to-Peer** mode.
In this mode, no hardware AP is required.
Any network node that is within range of any other can communicate if both nodes agree on a few basic parameters.
If one of those peers also has a wired connection to another network, it can provide access to that network.

Ad-hoc networks are useful for setting up point-to-point connections between two fixed devices, or if a couple of laptops need to exchange files and there is no other network available.

Ad-Hoc Demo mode is a manufacturer specific implementation of their own version of IBSS. Such devices tend to only be able to communicate with each other and aren't compatible with true IBSS mode.

802.11b radios must be set to work in either BSS or IBSS mode, but cannot work in both simultaneously.

Flickenger: Wireless Hacks, O'Reilly

IEEE 802.11 TASK GROUPS: Whats next ?

The following standards and task groups exist within the working group:

IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard

IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)

IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)

IEEE 802.11d –– international (country-to-country) roaming extensionsNew countries

IEEE 802.11e - Enhancements: QoS, including packet bursting

IEEE 802.11f - Inter-Access Point Protocol (IAPP)

IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)

IEEE 802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control (TPC) for European compatibility

IEEE 802.11i (ratified 24 June 2004) - Enhanced security

IEEE 802.11j - Extensions for Japan

IEEE 802.11k - Radio resource measurements

IEEE 802.11n - Higher throughput improvements

IEEE 802.11p - WAVE - Wireless Access for the Ability in Vehicular Environments (such as ambulances and passenger cars)

IEEE 802.11r - Fast roaming

IEEE 802.11s - Wireless mesh networking

IEEE 802.11t - Wireless Performance Prediction (WPP) - test methods and metrics

IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)

IEEE 802.11v - Wireless network management

INVERSE SQUARE LAW (reminder)