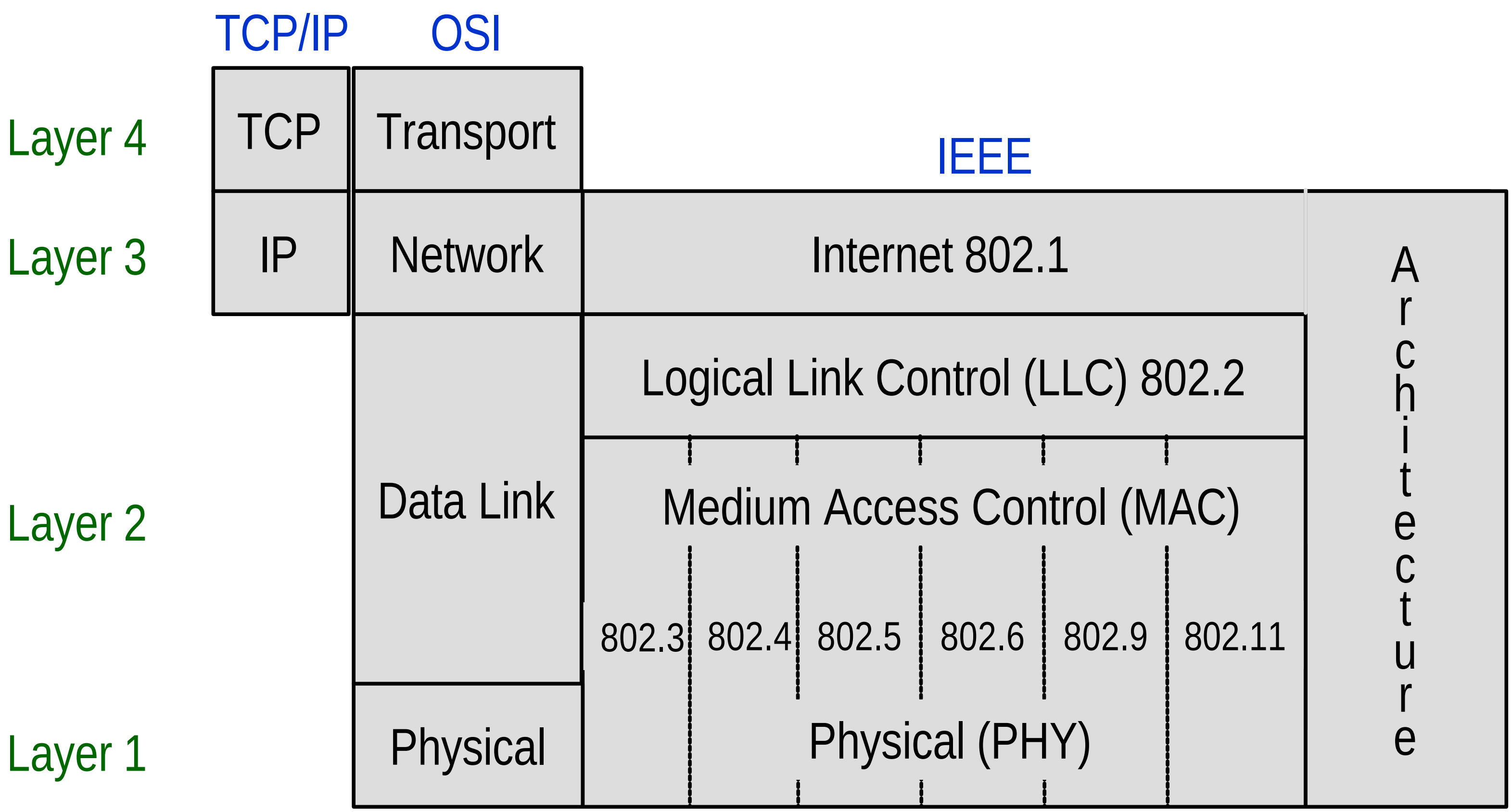
IEEE 802.11

WLANA
The Wireless LAN Association

XILINX®

Protocol Layers & 802 Protocols



IEEE 802.3 - Ethernet
“The Wired LAN”

- Ethernet is CSMA/CD
- CSMA (Carrier Sense Multiple Access)
  - Great for wireless
  - Distributed control with listen before talk
- CD (Collision Detect)
  - Not good for wireless & will not work well in an RF system
  - Transmitting signal hears its own signal perfectly
- Radio has much higher packet error rate

What's Different About Wireless?

- Stations are not always connected
  - Mobility & power management
- Stations destination address does not equal destination location
  - In wired LANs an address is equivalent to a physical location
    - This is implicitly assumed in the design of wired LANs
    - In 802.11, the addressable unit is a station (STA) which is a message destination, but usually not a fixed location
- Packet error rate of RF is much higher than cable
  - Interference is possible from other sources
- Not all stations "hear" the same thing
  - Hidden node problem

What is IEEE 802.11?

- IEEE standard addressing the 2.4 & 5 GHz WLAN market
- Spec is steered by the IEEE committee
  - Specifies "over the air" interface between a wireless client & a base station (or access point) or wireless clients
  - Conceived in 1990, final draft approved in June 1997
  - Like the IEEE 802.3 Ethernet & 802.5 Token Ring Standards
    - Addresses both PHY & MAC Layers

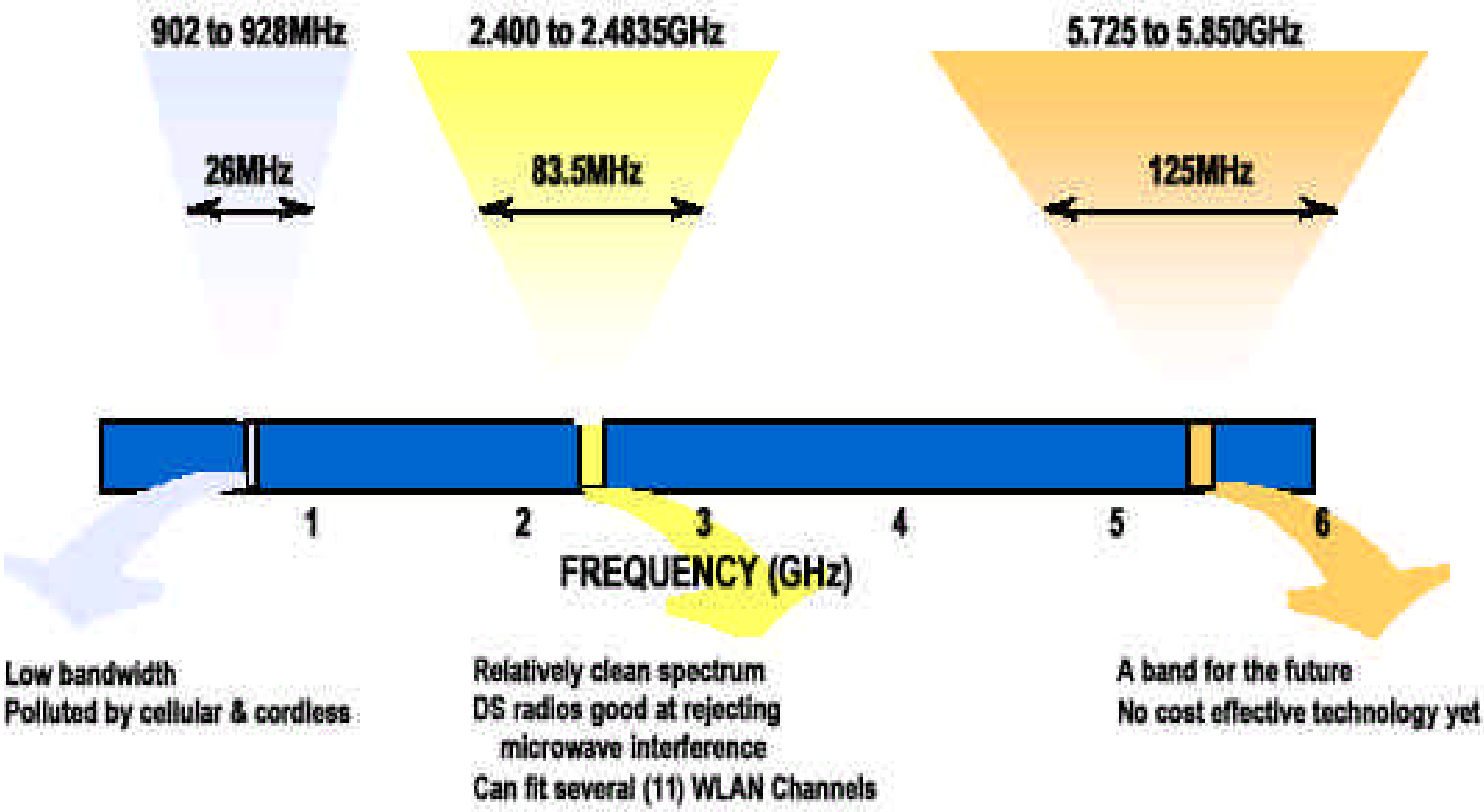
IEEE 802.11 WLAN Standards Requirements

- Providing reliable, efficient wireless data networking
- Defining MAC & PHY layer specifications
- Providing a single MAC layer to work with multiple PHYs
- Allowing for overlapping of multiple networks
- Being robust against interference
- Providing mechanism to handle hidden nodes
- Supporting peer-to-peer & infrastructure configurations
- Supporting time bounded services

IEEE 802.11 Draft Standard Description

- Mandatory support for a 1 Mbps WLAN is specified
  - Optional support for 2 Mbps data transmission rate
- Mandatory support for asynchronous data transfer is specified
  - Asynchronous data transfer refers to traffic that is insensitive to time delay such as available bit rate traffic like e-mail and file transfer
- Optional support for distributed time-bounded services (DTBS)
  - Time-bounded traffic is bounded by specific time delays to achieve an acceptable QoS for packetized voice and video
- Support for 2 fundamentally different MAC schemes to transport asynchronous & time-bounded services
  - DCF (distributed coordination function) & PCF (point coordination function)

ISM Bands



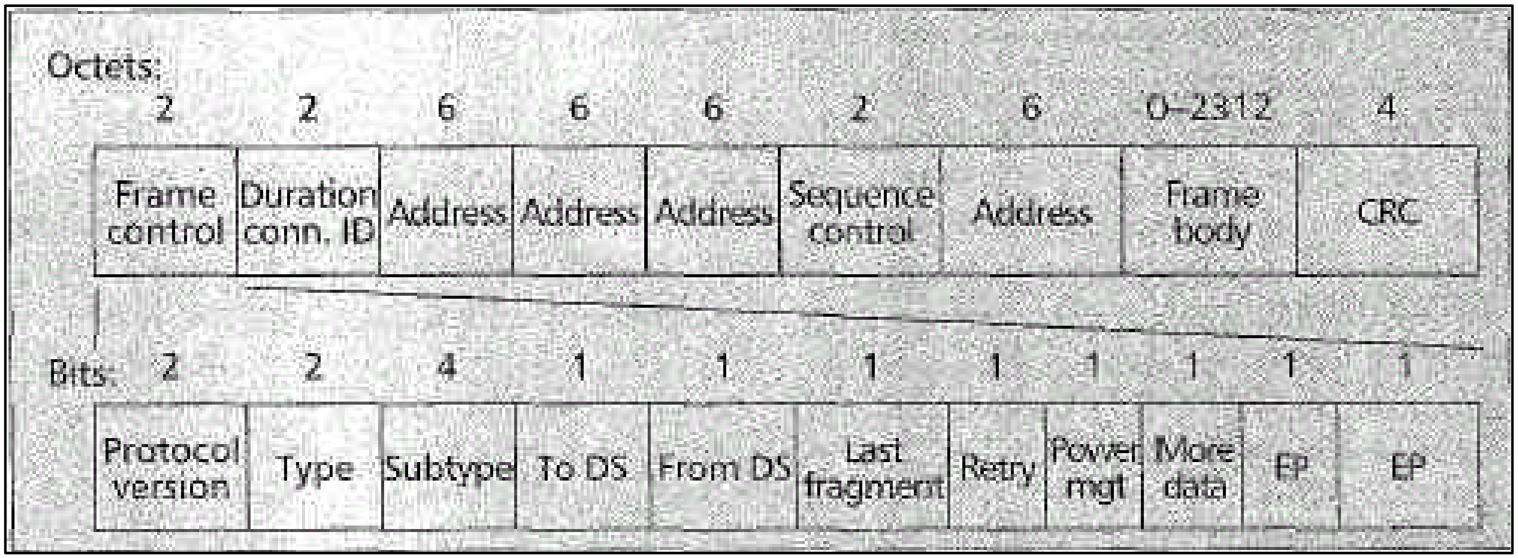
Courtesy: Compaq

2.4GHz ISM Band Channels 802.11 DSSS

CHNL_ID	Frequency	Regulatory Domains					
		10h FCC	20h IC	30h ETSI	31h Spain	32h France	40h MKK
1	2412 MHz	X	X	X	-	-	-
2	2417 MHz	X	X	X	-	-	-
3	2422 MHz	X	X	X	-	-	-
4	2427 MHz	X	X	X	-	-	-
5	2432 MHz	X	X	X	-	-	-
6	2437 MHz	X	X	X	-	-	-
7	2442 MHz	X	X	X	-	-	-
8	2447 MHz	X	X	X	-	-	-
9	2452 MHz	X	X	X	-	-	-
10	2457 MHz	X	X	X	X	X	-
11	2462 MHz	X	X	X	X	X	-
12	2467 MHz	-	-	X	-	X	-
13	2472 MHz	-	-	X	-	X	-
14	2484 MHz	-	-	-	-	-	X

Courtesy: Compaq

Standard IEEE 802.11 Frame Format



Courtesy: IEEE

IEEE 802.11 PHY Layer

- At the PHY layer, IEEE 802.11 defines three physical characteristics for wireless LANs
  - Diffused infrared operating at baseband
  - DSSS operating at 2.4 GHz band - Used in IEEE 802.11b
  - FHSS operating at 2.4 GHz band
- All three PHYs specify support 1Mbps & 2Mbps data rates
  - All 11 Mbps radios are DSSS
  - Choice between FSSS & DSSS depends on the users applications & environment that the system will be operating
- PHY Layer with OFDM operating at 5 GHz band - Used in IEEE 802.11a

802.11 PHY Layer

- 2.4 GHz band
  - Occupies 83 MHz of bandwidth from 2.400 GHz to 2.483 GHz
  - Part of ISM band
  - Global band
  - Primarily set aside for industrial, scientific & medical use
  - Can be used for operating wireless LAN devices without the need for end-user licenses
- Interoperability for wireless devices
  - Requires conforming to the same PHY standard

IEEE 802.11 WLAN Standard Physical Layer Specs

Technology	Frequency Band	Radiated Peak Power Limitation	Modulation Signalling Method	Data Rates
Direct Sequence Spread Spectrum	2.4-2.483GHz	1W for the US, 10mW per 1Mhz in Europe & 10mW for Japan	Differential BPSK (DBPSK) & DQPSK	1Mbps or 2Mbps
Frequency Hopping Spread Spectrum	2.4-2.483GHz	1W for the US, 10mW per 1Mhz in Europe & 10mW for Japan	2-4 level Gaussian FSK	1Mbps
Infrared	850-950nM	2W	4- or 16-level pulse positioning	1Mbps or 2Mbps

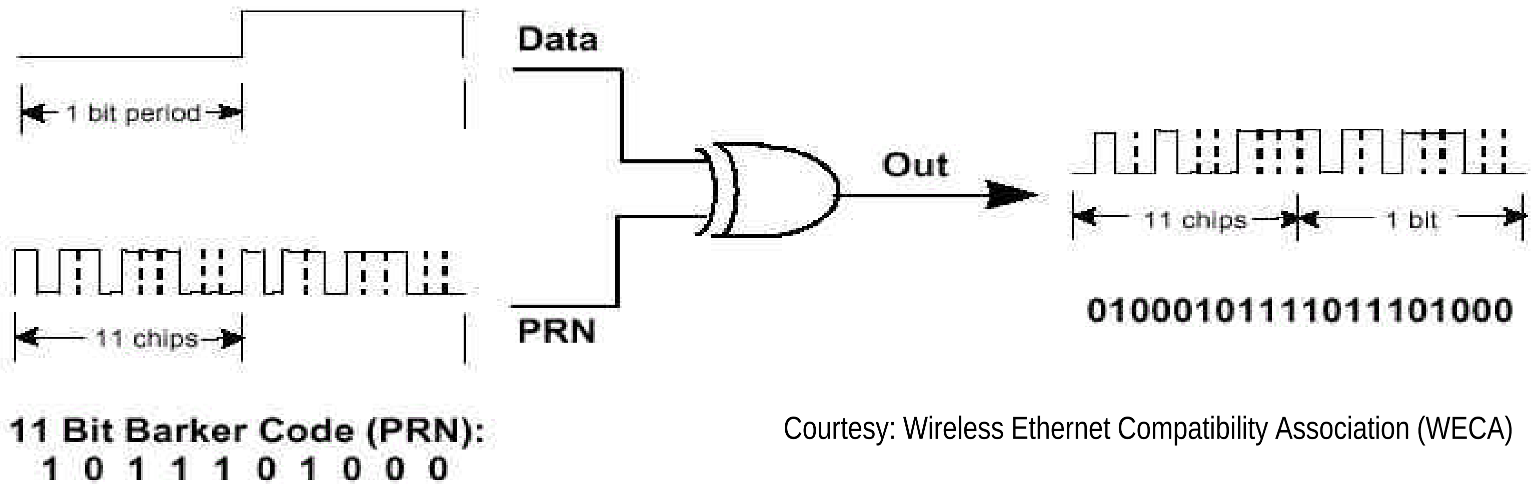
DSSS PHY Layer

- Uses an 11-bit Barker Sequence to spread data before it is transmitted
  - Each bit transmitted is modulated by the 11-bit sequence
  - This process spreads the RF energy across a wider bandwidth than would be required to transmit the raw data
- Processing gain of a system
  - Defined as 10x the log of the ratio of spreading rate (also known as the chip rate) to the data
- Receiver
  - Despreads the RF input to recover the original data

DSSS PHY Layer

- Advantage of the DSSS technique
  - Reduces the effect of narrowband sources of interference
  - Provides 10.4dB of processing gain which meets the minimum requirements for rules set forth by the FCC
- Spreading architecture used in direct sequence is not to be confused with CDMA
  - All 802.11 compliant products utilize the same PN (pseudo-random numerical) code
  - Therefore do not have a set of codes available as is required for CDMA operation

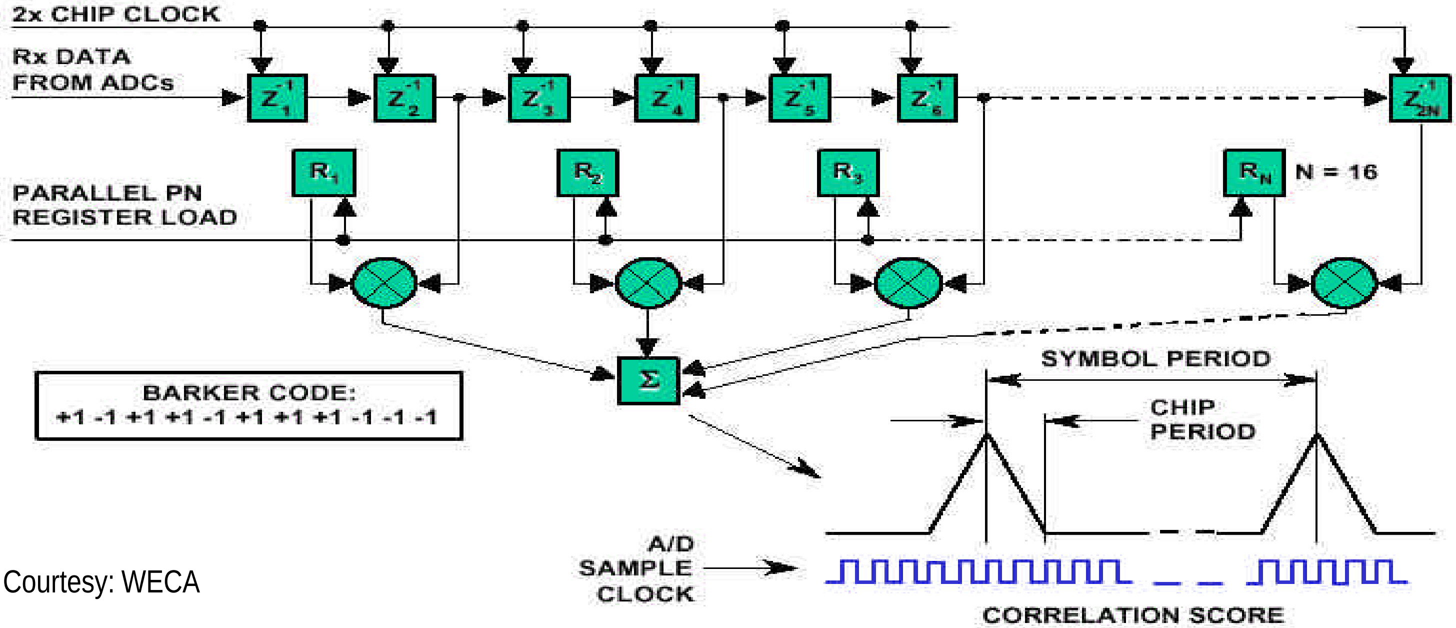
Digital Modulation of Data With PN Sequence



Courtesy: Wireless Ethernet Compatibility Association (WECA)

- DSSS systems use technology similar to GPS satellites and some types of cell phones
- Each information bit is combined via an XOR function with a longer Pseudo-random Numerical (PN) sequence as shown in figure
  - The result is a high speed digital stream which is then modulated onto a carrier frequency using Differential Phase Shift Keying (DPSK)

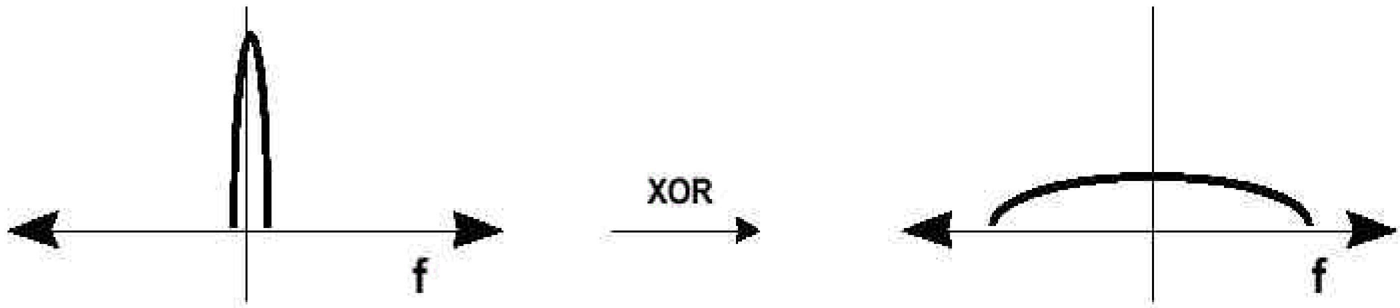
Reception of DSSS Signal



Courtesy: WECA

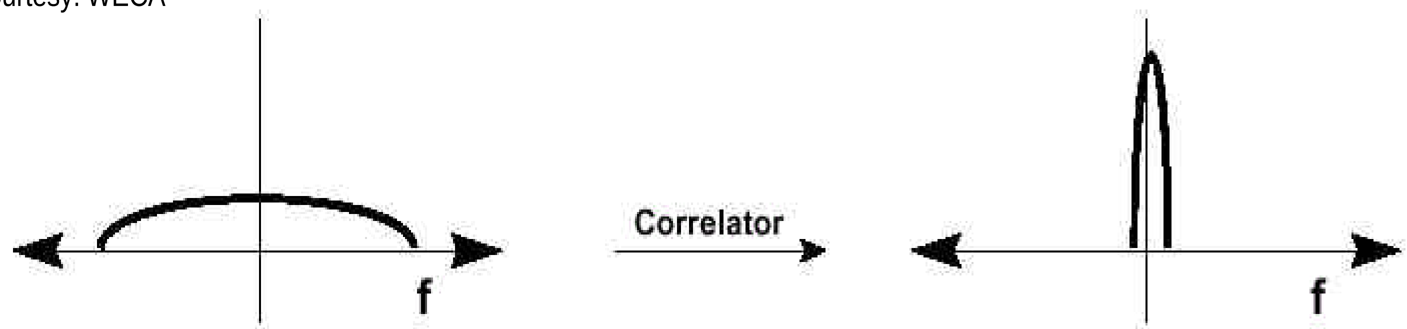
- A matched filter correlator is used for receiving the DSSS Signal
  - Correlator removes the PN sequence & recovers the original data stream
- Complimentary Code Keying (CCK)
  - High rate modulation method
  - To achieve higher data rates of 5.5-11 Mbps DSSS receivers use different PN codes & a bank of correlators to recover the transmitted data stream

Effect of PN Sequence on Transmit & Receive Signal



Effect of PN Sequence on Transmit Spectrum

Courtesy: WECA

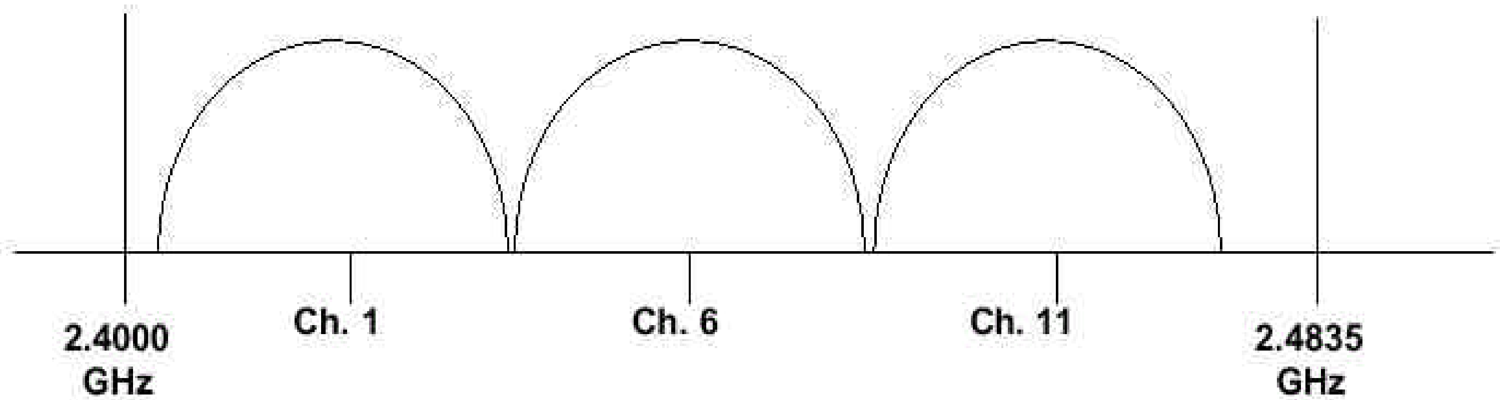


Received Signal is Correlated with PN to Recover Data & Reject Interference

Effect of PN Sequence on Transmit & Receive Signal

- The PN sequence spreads the transmitted bandwidth of the resulting signal
  - Thus the term "spread spectrum"
  - Reduces peak power
    - The total power however remains unchanged
- Upon reception
  - Signal is correlated with the same PN sequence to reject narrow band interference and recover the original binary data

Three Non-Overlapping DSSS Channels in the ISM Band



Courtesy: WECA

- Regardless of whether the data rate is 1, 2, 5.5, or 11 Mbps, the channel bandwidth is about 20 MHz for DSSS systems
- Hence the ISM band will accommodate up to three non-overlapping channels

FHSS PHY Layer

- Has 22 hop patterns to choose from
- Frequency hop physical layer is required to hop across the 2.4 GHz ISM band covering 79 channels
- Each channel occupies 1MHz of bandwidth
  - Must hop at the minimum rate specified by the regulatory bodies of the intended country
    - Minimum hop rate of 2.5 hops per second is specified for the US

PHY Layer Header

- Each physical layer uses their unique header
  - To synchronize the receiver & determine signal modulation format & data packet length
- PHY layer headers are always transmitted at 1Mbps
- Predefined fields in headers provide the option to increase the data rate to 2Mbps for the actual data packet

The MAC Sub-layer

- MAC specification for 802.11 has similarities to 802.3 Ethernet wired line standard
  - CSMA/CA protocol used for 802.11
    - Uses carrier-sense, multiple access, collision avoidance
    - Avoids collisions instead of detecting a collision like the algorithm in 802.3
    - Collision avoidance is used because it is difficult to detect collisions in an RF transmission network

MAC & PHY Layer Operation

- MAC layer operates together with the PHY layer by sampling the energy over the medium transmitting data
- PHY layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear
  - This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal
    - This measured signal is commonly known as RSSI
  - If the received signal strength is below a specified threshold the channel is declared clear and the MAC layer is given the clear channel status for data transmission
  - If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules
  - The standard provides another option for CCA that can be alone or with the RSSI measurement

MAC & PHY Layer Operation

- Carrier sense can also be used to determine if the channel is available
  - This technique is more selective sense since it verifies that the signal is the same carrier type as 802.11 transmitters
- The best method to use depends upon the levels of interference in the operating environment
- CSMA/CA protocol allows options to minimize collisions
  - Using request to send (RTS), clear-to-send (CTS), data & acknowledge (ACK) transmission frames in a sequential fashion

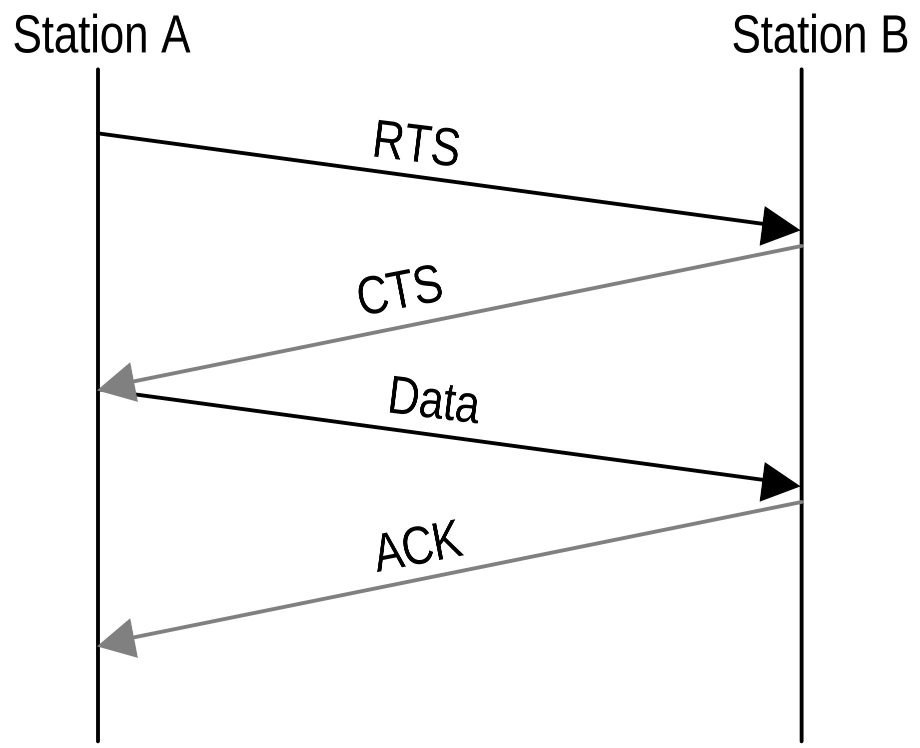
CSMA/CA Protocol Minimizes Collisions

- Communication is established when one of the wireless nodes sends a short message RTS frame
- The RTS frame includes the destination and the length of message
- The message duration is known as the network allocation vector (NAV)
- The NAV alerts all others in the medium, to back off for the duration of the transmission

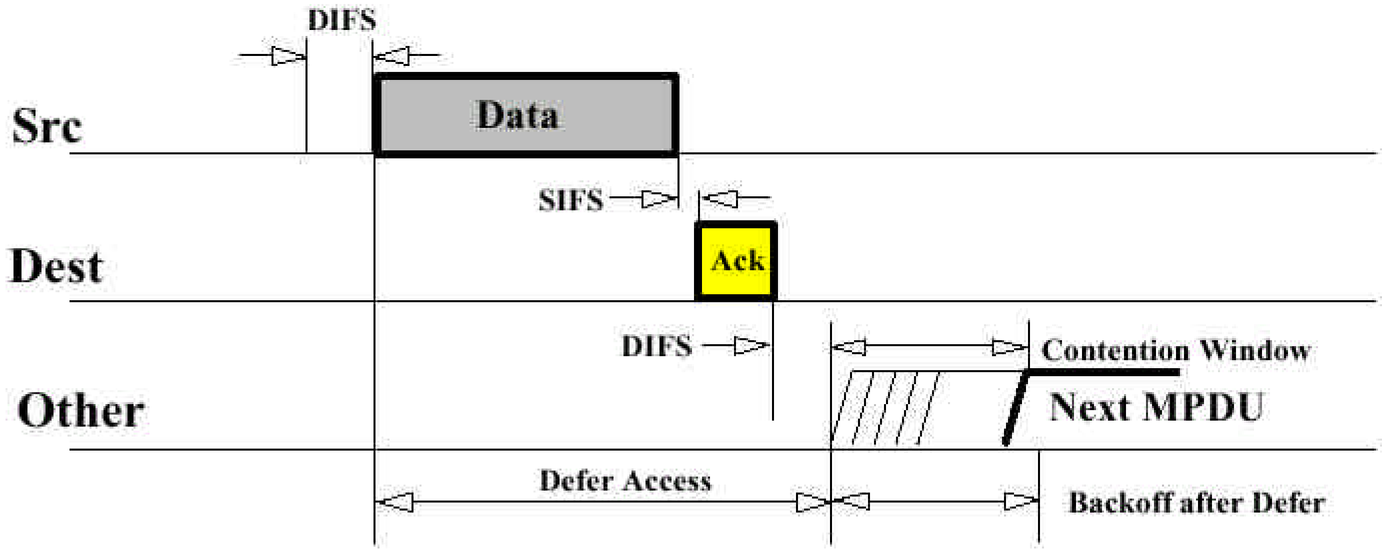
CSMA/CA Protocol Minimizes Collisions

- The receiving station issues a CTS frame which echoes the senders address and the NAV
- If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over
- After the data frame is received, an ACK frame is sent back verifying a successful data transmission

RTS/CTS/ACK Protocol



CSMA/CA Back-off Algorithm



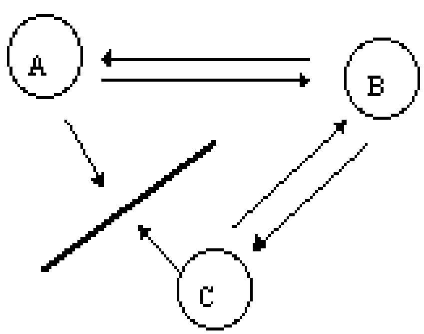
- Packet reception in DCF requires acknowledgment
- The period between completion of packet transmission and start of the ACK frame is one Short Inter Frame Space (SIFS)
- ACK frames have a higher priority than other traffic
  - Fast acknowledgement is one of the salient features of the 802.11 standard, because it requires ACKs to be handled at the MAC sublayer

Hidden Node Problem

- A common limitation with wireless LAN systems is the "hidden node" problem
  - This can disrupt 40% or more of the communications in a highly loaded LAN environment
  - It occurs when there is a station in a service set that cannot detect the transmission of another station to detect that the media is busy

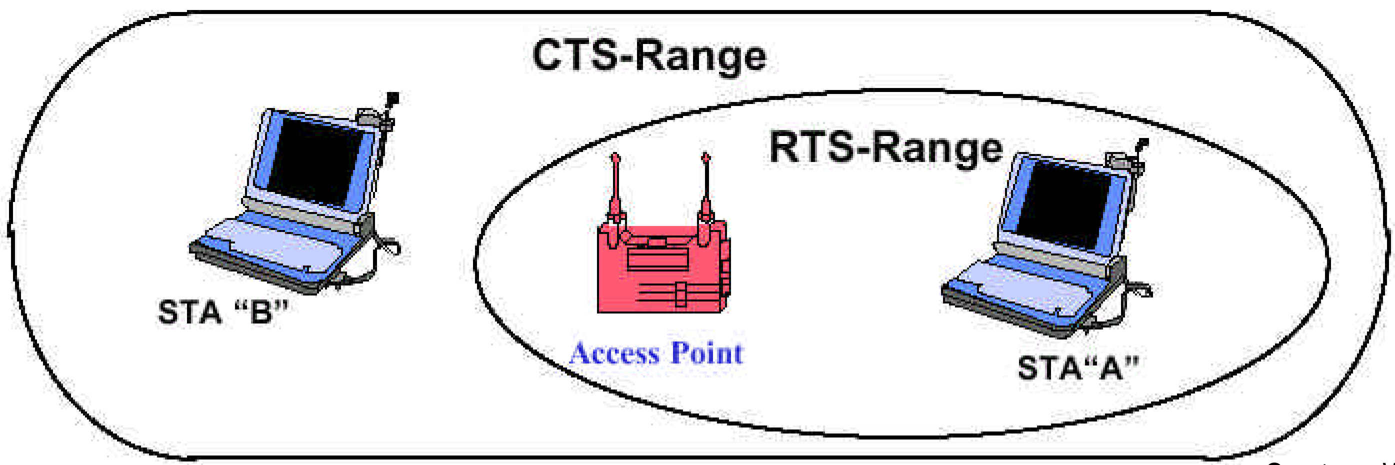
Hidden Node Problem

- The figure shows how stations A and B can communicate
  - However an obstruction prevents station C from receiving station A and it cannot determine when the channel is busy
  - Therefore both stations A and C could try to transmit at the same time to station B
  - The use of RTS, CTS, Data and ACK sequences helps the prevent the disruptions caused by this problem



Courtesy: Wireless LAN Association

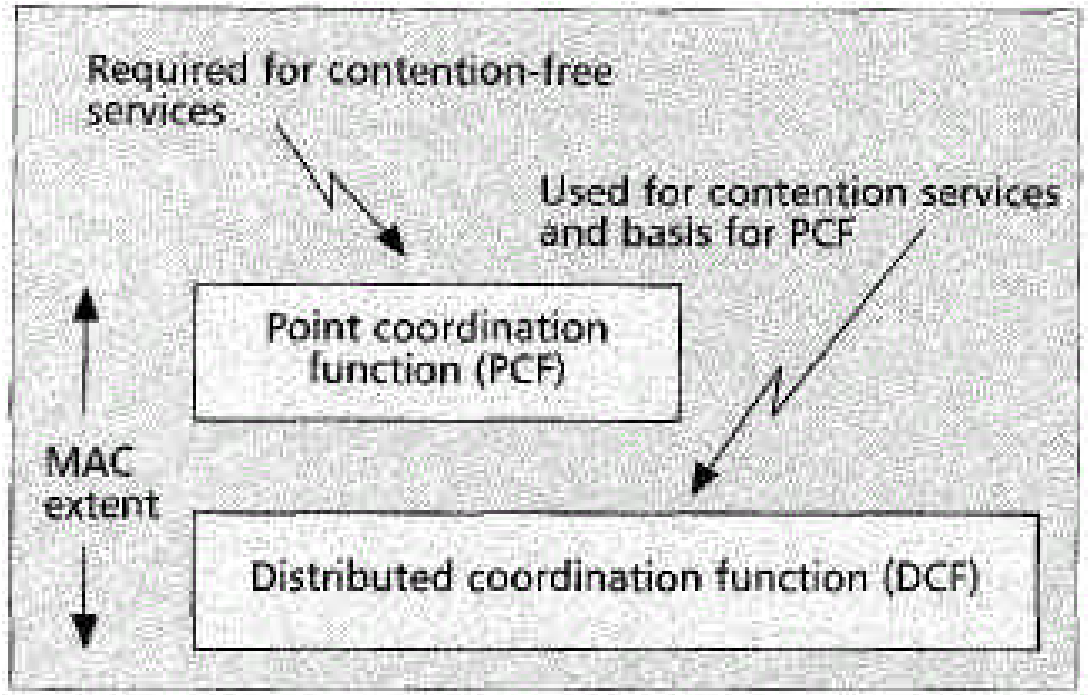
Hidden Node Example



Courtesy: WECA

- From the figure
  - The AP is within range of the STA-A, but STA-B is out of range
  - STA-B would not be able to detect transmissions from STA-A, and the probability of collision is greatly increased
  - This is known as the Hidden Node

MAC Architecture



Courtesy: IEEE

MAC Schemes

- Distributed Coordination Function (DCF)
  - Similar to traditional legacy packet networks supporting best packet delivery of the data
  - DCF is designed for asynchronous data support
    - All users with data to transmit have an equally fair chance of accessing the network
- Point Coordination Function (PCF)
  - Based on polling that is controlled by an access point
  - Primarily designed for the transmission of delay-sensitive traffic
- Ad hoc network (DCF only) & Infrastructure network (DCF & PCF)

802.11 MAC Layer

- The MAC is concerned with rules for accessing the wireless medium
  - It is supported by underlying PHY layer
- Basic Service Set (BSS)
  - Consists of 2 or more wireless nodes or stations (STAs)
    - Recognize each other & have established communications
  - Contains an Access Point (AP)
    - Form bridges between wireless & wired LANs
    - Analogous to a base station used in cellular phone networks
    - Immobile & part of the wired network infrastructure
    - All communications between STAs or between a station & a wired network client go through the AP

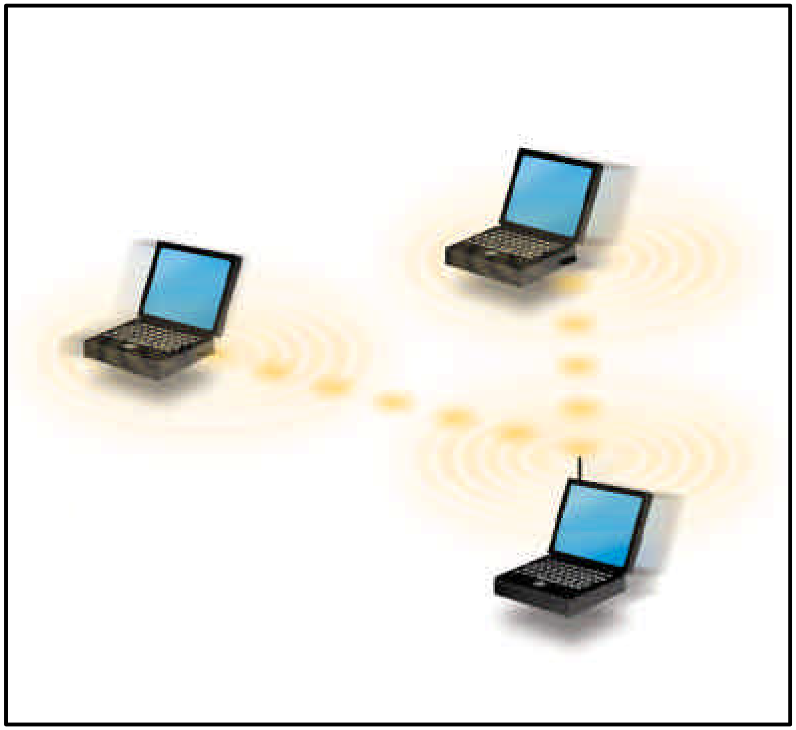
What is an Access Point?

- Wireless Hub
- Gateway for non wireless network to wired network
- Network police and policy manager
- Network management tool

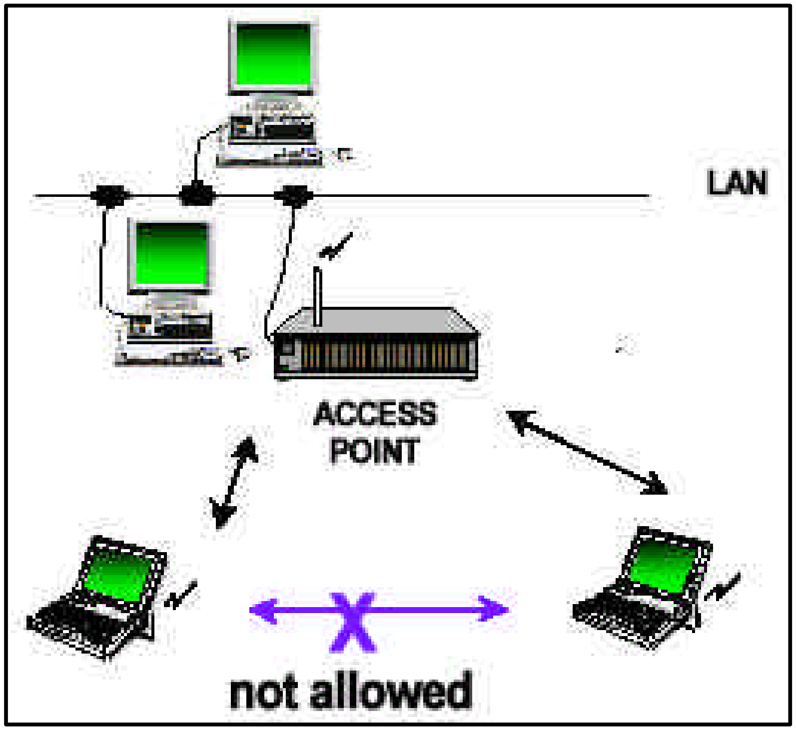
IEEE 802.11 Networking Modes

- 802.11 MAC layer has 2 defined networking architectures
  - "Ad-Hoc" Network architecture
    - Used to support mutual communication among wireless clients
    - Created spontaneously
    - Does not support access to wired networks
    - Does not need an AP to be part of the network
    - Perfect for conference room setups
  - "Infrastructure" Network architecture
    - Provides communication between wireless clients & wired network resources
    - Transition of data from wireless to wired medium is via an AP
    - Coverage area is defined by APs & associated wireless clients
      - Together all devices form a Basic Service Set (BSS)

Ad-Hoc vs. Infrastructure Networking Modes

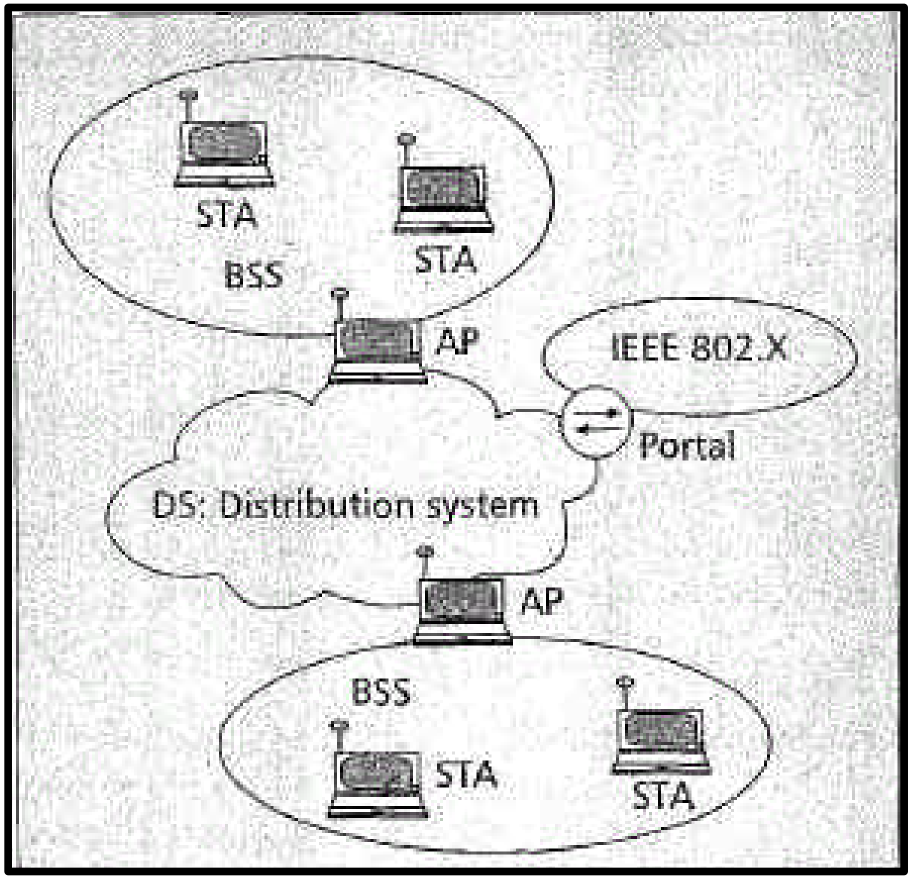


Ad Hoc Network



Infrastructure Network

Sketch of an Infrastructure Network



Courtesy: IEEE

Services Provided by MAC Layer

- Data transfer
  - Wireless clients use CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) algorithm as media access scheme
- Association
  - Service enables establishment of wireless links between wireless clients & APs in Infrastructure Networks
- Reassociation
  - Occurs when wireless client moves from one BSS to another
  - 2 adjoining BSS form an Extended Service Set (ESS)
    - Defined by common ESSID
    - If common ESSID is defined, wireless client can roam from one area to another

Services Provided by MAC Layer

- Power management
  - IEEE 802.11 supports 2 power modes at the MAC level for those applications requiring mobility under battery operation
  - Active Mode
    - Wireless client is powered to transmit & receive
  - Power Save Mode - "Sleep" mode
    - Provisions are made in the protocol for the portable stations to go to low power "sleep" mode during a time interval defined by the base station
    - Consumes less power
    - Client is unable to transmit or receive

Services Provided by MAC Layer

- Authentication
  - Process of proving client identity
  - Takes place prior to a wireless client associating with an AP
  - True Authentication
    - Use of Wired Equivalent Privacy (WEP)
    - Shared Key is configured into the AP & its wireless clients
    - Valid Shared Key allows association with AP

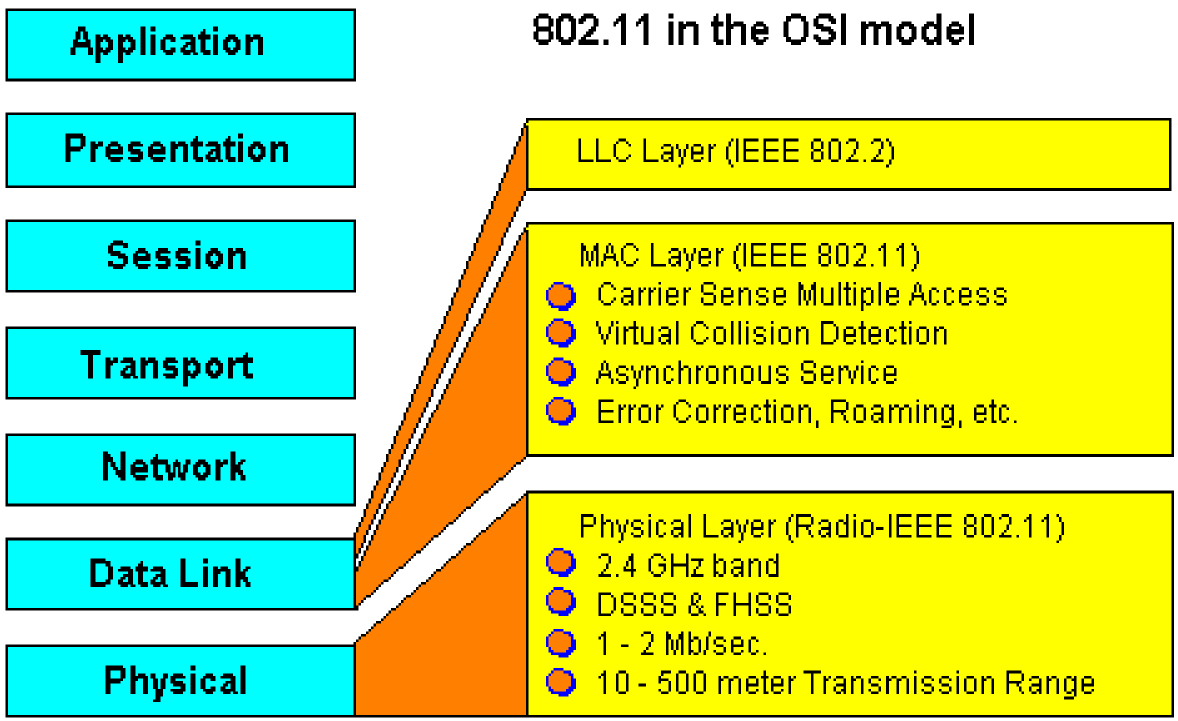
Services Provided by MAC Layer

- Security and privacy
  - Addressed in the 802.11 standard as an optional feature for those concerned about eaves dropping
    - Data is transferred “in the clear”
      - Any 802.11 device can eavesdrop on traffic that is within range
  - Data security is accomplished by a complex encryption technique know as Wired Equivalent Privacy Algorithm (WEP)
    - WEP encrypts data before it is sent wirelessly

WEP

- Protects the transmitted data over the RF medium using a 64-bit seed key & the RC4 encryption algorithm
  - Only wireless clients with the exact Shared Key can correctly decipher the data
  - The same Shared Key is used in authentication to encrypt & decrypt data
- WEP only protects the data packet information
  - It does not protect the PHY header so that other stations on the network can listen to the control data needed to manage the network
  - However, other stations cannot decrypt the data portions of the packet

IEEE 802.11 Summary



Wireless Devices Interoperability through IEEE 802.11 Spec

- Interoperability among devices
  - 3 physical layer modulation schemes (IR, DSSS, FHSS) are <u>incompatible</u> with each other
- Multivendor interoperability requires a standard for
  - AP-to-AP coordination for roaming
    - Standard does not specify the handoff mechanism to allow clients to roam
  - Data frame mapping
    - Standard does not state how an AP addresses data framing between wired & wireless media
  - Conformance test suite
    - Verification of device compliance with IEEE 802.11 spec needs to be specified by a conformance test suite

IEEE 802.11 WLAN Types

- IEEE 802.11 a
  - PHY layer: 5 GHz, OFDM
  - Data rate: 40 Mbps
- IEEE 802.11 b
  - PHY layer: 2.4 GHz, DSSS
  - Data rate: 11 Mbps

IEEE 802.11b Security

IEEE 802.11b

- Wireless version of the IEEE 802.3 wired Ethernet
  - Delivers a data rate of up to 11Mbps
  - Uses spread spectrum - FHSS or DSSS
  - 802.11b compliant radio frequency is around 2.4 GHz
    - Subject to national regulations & can hence vary from country to country
  - Requires equivalent encryption as IEEE 802.3
- Encryption goal - provide “Wired Equivalent Privacy”
  - Intruders should not be able to access network resources
  - Intruders should not capture WLAN traffic (eavesdropping)
  - Worldwide usable

Simply - Here's How it Works

- Authentication
  - A, to sign a message, does a computation involving both her private key and the message itself; the output is called the digital signature and is attached to the message, which is then sent
  - B, to verify the signature, does some computation involving the message, the purported signature, and A's public key
  - If the results properly hold in a simple mathematical relation, the signature is verified as genuine; otherwise, the signature may be fraudulent or the message altered, & they are discarded

Simply - Here's How it Works

- Encryption
  - When A wishes to send a message to B, she looks up B's public key in a directory, uses it to encrypt the message and sends it off
  - B then uses his private key to decrypt the message and read it
  - No one listening in can decrypt the message
  - Anyone can send an encrypted message to B but only B can read it
  - Clearly, one requirement is that no one can figure out the private key from the corresponding public key.

Data Encryption
Secure Transmission of Information

- Physical layer
  - Physical security of data transmission is gained by using spread spectrum technology which makes it less vulnerable to interference
- MAC (Medium Access Control) layer
  - Encryption algorithm is called Wired Equivalent Privacy (WEP)
    - 2 part process - WEP encrypts the plaintext data (RC4) & protects against unauthorized data modification (CRC-32)
    - WEP is only supplied between stations & not on an end-to-end basis

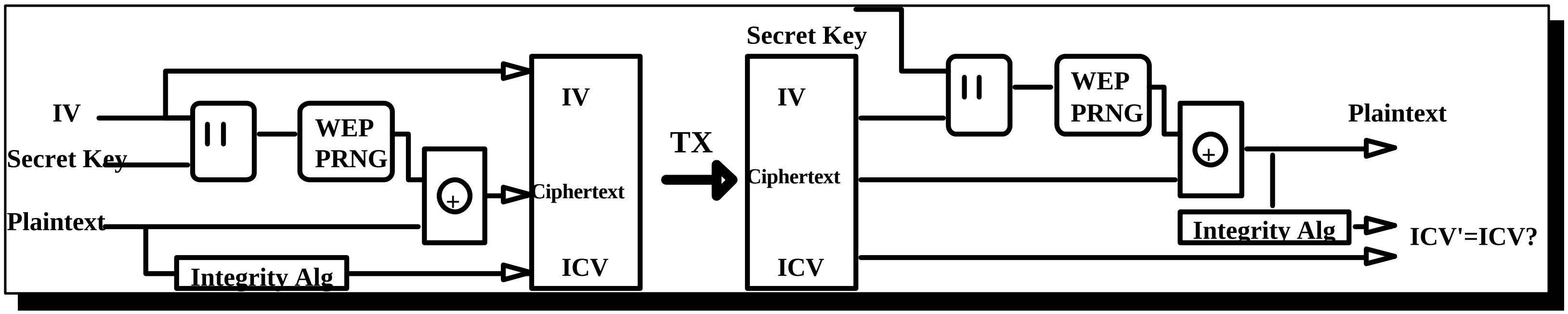
MAC Authentication Mechanism

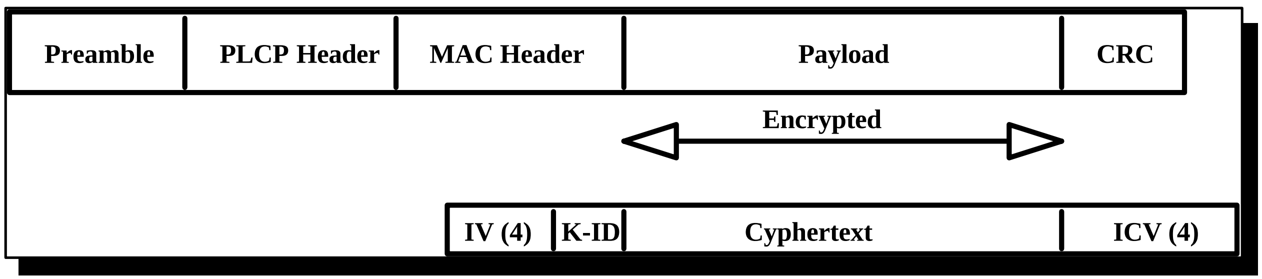
- Aids in access control
  - Performed by assigning a ESSID (Extended Service Set ID) to each Access Point (AP) in the network
- The network does not provide anonymity
  - The source & destination information is visible in the frames despite of the optional encryption
  - The WEP only encrypts the data field of a frame while leaving headers unencrypted
    - Gives an eavesdropper the ability to gather information about the usage of APs & work routines in a building using WLANs
- Has provisions for “OPEN”, “Shared Key” or proprietary authentication extensions

WEP Privacy Mechanism

- Provides encryption
  - Uses RSA Data Security Inc.'s 40-bit RC4 algorithm for encrypting data (plain text) contained in the frames
    - PRNG algorithm & output of the generator (key) is XORed with the data stream (stream cipher)
    - Based on 40-bit secret key & has a 24 bit initialization vector that is sent with the data (total key size is 64-bit)
    - 128-bit RC4 keys can be used
      - Using a 40-bit symmetric cipher is not secure because its key space so small that a brute-force attack is feasible
- Provides protection against unauthorized data modification
  - Integrity algorithm (CRC-32) operates on the the plaintext to produce the integrity check value
  - Produces the ciphertext

WEP Privacy Mechanism



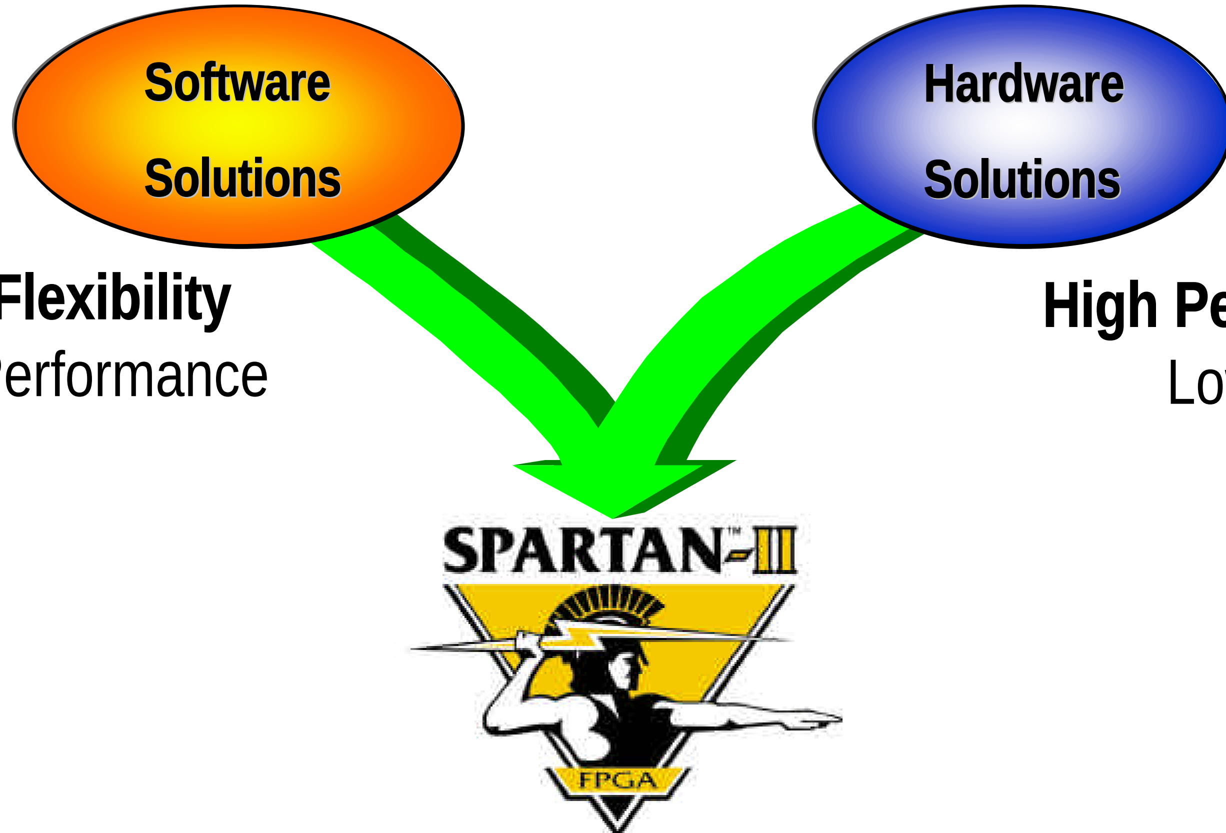


- WEP bit in Frame Control Field indicates WEP used
  - Each frame can have a new IV, or IV can be reused for a limited time
  - If integrity check fails then frame is ACKed but discarded
- Limited for Station-to-Station traffic, so not “end to end”
  - Embedded in the MAC entity

802.11 Selected WEP Protocol Because It Is

- Reasonably strong
  - Brute-force attack is difficult because every frame is sent with an Initialization vector which restarts the PRNG for each frame
- Self synchronizing
  - The algorithm re-synchronizes for each message to work in a connection-less environment, where packets may get lost
- Computationally efficient
  - Can be implemented in hardware & software
- Exportable outside the US
- Optional - Defined as an optional functionality of the MAC

Spartan-II Advantages Over Hardware & Software Solutions



High Flexibility
Low Performance

High Performance
Low Flexibility

High Performance
High Flexibility

Enhanced Security & Performance