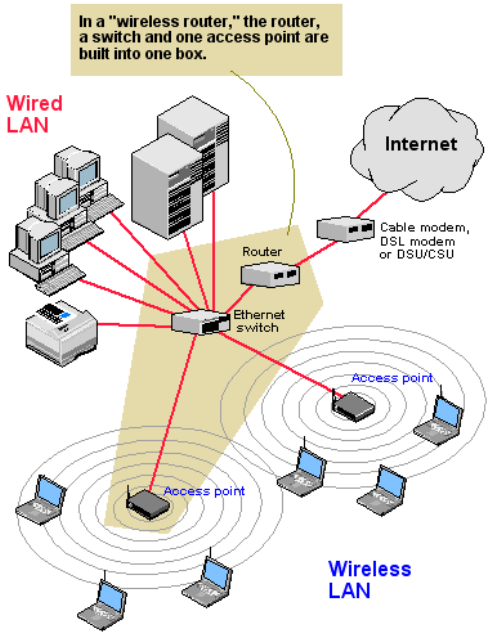
# CoNeT Mobile Lab
# Wireless Communication






**(Version 2)**





Education and Culture DG
Lifelong Learning Programme

# CoNeT Mobile Lab
# Wireless Communication

## PART 1: Theoretical Aspects of Wireless Communication







Education and Culture DG
Lifelong Learning Programme

# Content Theoretical Aspects

1 Differentiating between Wireless Technologies

2 IEEE 802.11 Standards

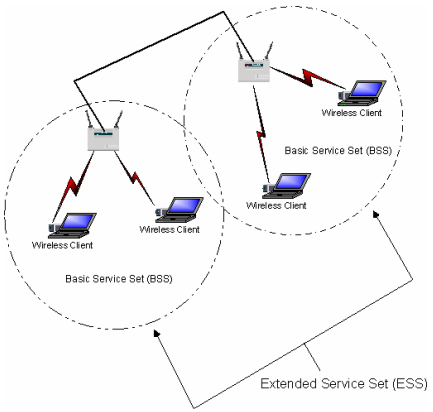
3 IEEE 802.11 Architecture

4 IEEE 802.11 Layers Description

5 Power Management

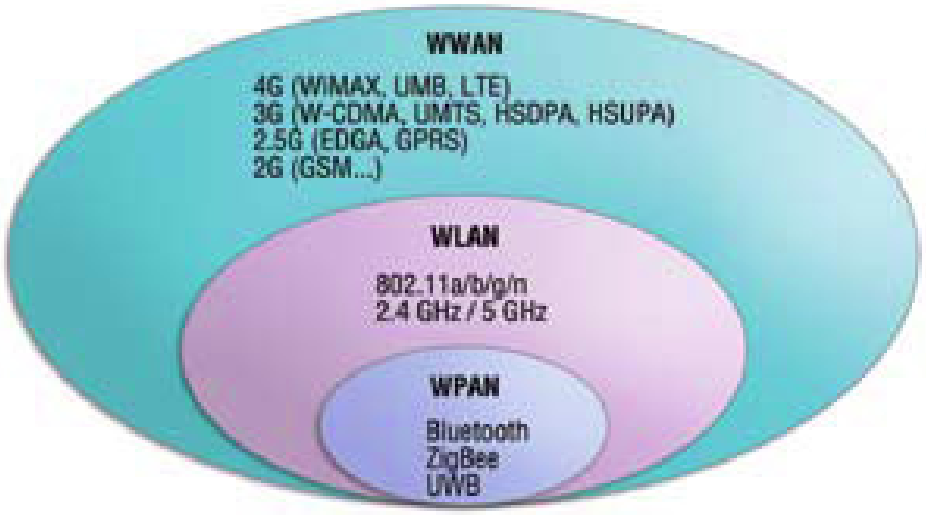
6 WLAN Security principles

7 IEEE 802.11 Frame Types

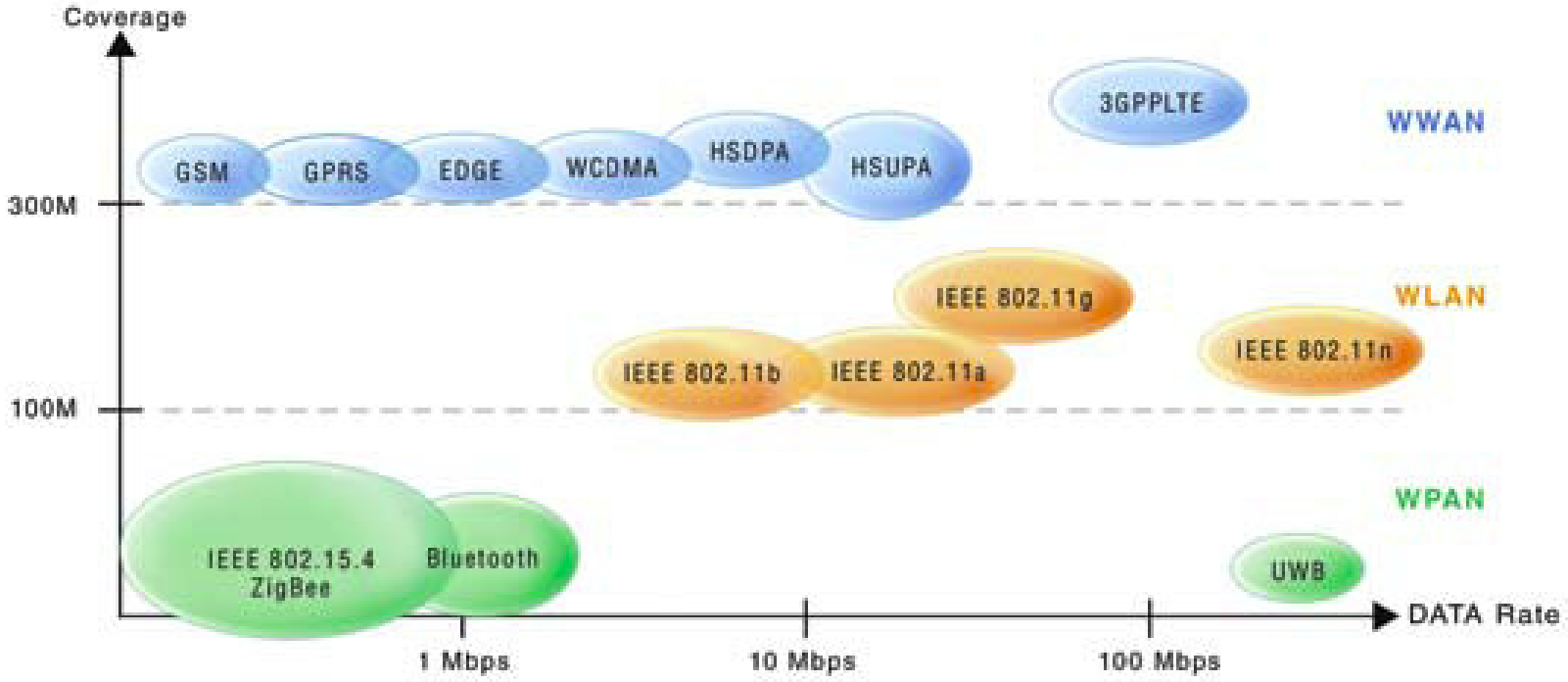


# 1. Differentiating between Wireless Technology

- WWAN vs. WLAN vs. WPAN
  - ✓ WWAN (Wireless Wide Area Network)
  - ✓ WLAN (Wireless Local Area Network)
  - ✓ WPAN (Wireless Personal Area Network)



# The industrial Wireless Technology Landscape



# 1.2 Mayor involved bodies

## 1.2.1 Main Standardization committees involved in WLANS

- ✓ ITU – The International Telecommunication Union
- ✓ ETSI - European Telecommunications Standards Institute
- ✓ IEEE - Institute of Electrical and Electronic Engineers

## 1.2.2 Supervisory bodies and standardization bodies

- ✓ US: FCC
- ✓ Europe CEPT, ETSI
- ✓ Japan:MKK
- ✓ IEEE802.1x LAN standards
- ✓ WIFI (Wireless Fidelity) alliance

# 1.2 Mayor involved bodies (2)

## 1.2.1 Main Standardization committees involved in WLANS

- ✓ ITU – The International Telecommunication Union
- ✓ ETSI - European Telecommunications Standards Institute
- ✓ IEEE - Institute of Electrical and Electronic Engineers

## 1.2.2 Supervisory bodies and standardization bodies

- ✓ US: FCC
- ✓ Europe CEPT, ETSI
- ✓ Japan:MKK
- ✓ IEEE802.1x LAN standards
- ✓ WIFI (Wireless Fidelity) alliance

# 2. IEEE 802.11x standards (1)

## 2.1 IEEE 802.11x evolving and evolution standards (1)

| | |
|---|---|
| IEEE 802. 11 | 2 Mbps, 2.4 GHz band, 1997, MAC/Physical Standard |
| IEEE 802. 11a | 54 Mbps, 5 GHz band, 1999, MAC/Physical Standard |
| IEEE 802. 11b | 11 Mbps, 2.4 GHz Band, 1999, MAC/Physical Standard |
| IEEE 802. 11c | MAC Layer Bridging to support IEEE802.1D |
| IEEE 802. 11d | Automatic settings for different countries |
| IEEE 802. 11e | Quality of Service (QoS) |
| IEEE 802. 11f | IAPP, Inter-Access Point Protocol, cancelled by IEEE after February, 2006 |
| IEEE 802. 11g | 54 Mbps, 2.4 GHz Band, 2003, MAC/Physical Standard |
| IEEE 802. 11h | Support more channels on 5GHz spectrum, 2004 |
| IEEE 802. 11i | Wireless security, 2004 |

# IEEE 802.11x evolving and evolution standards (2)

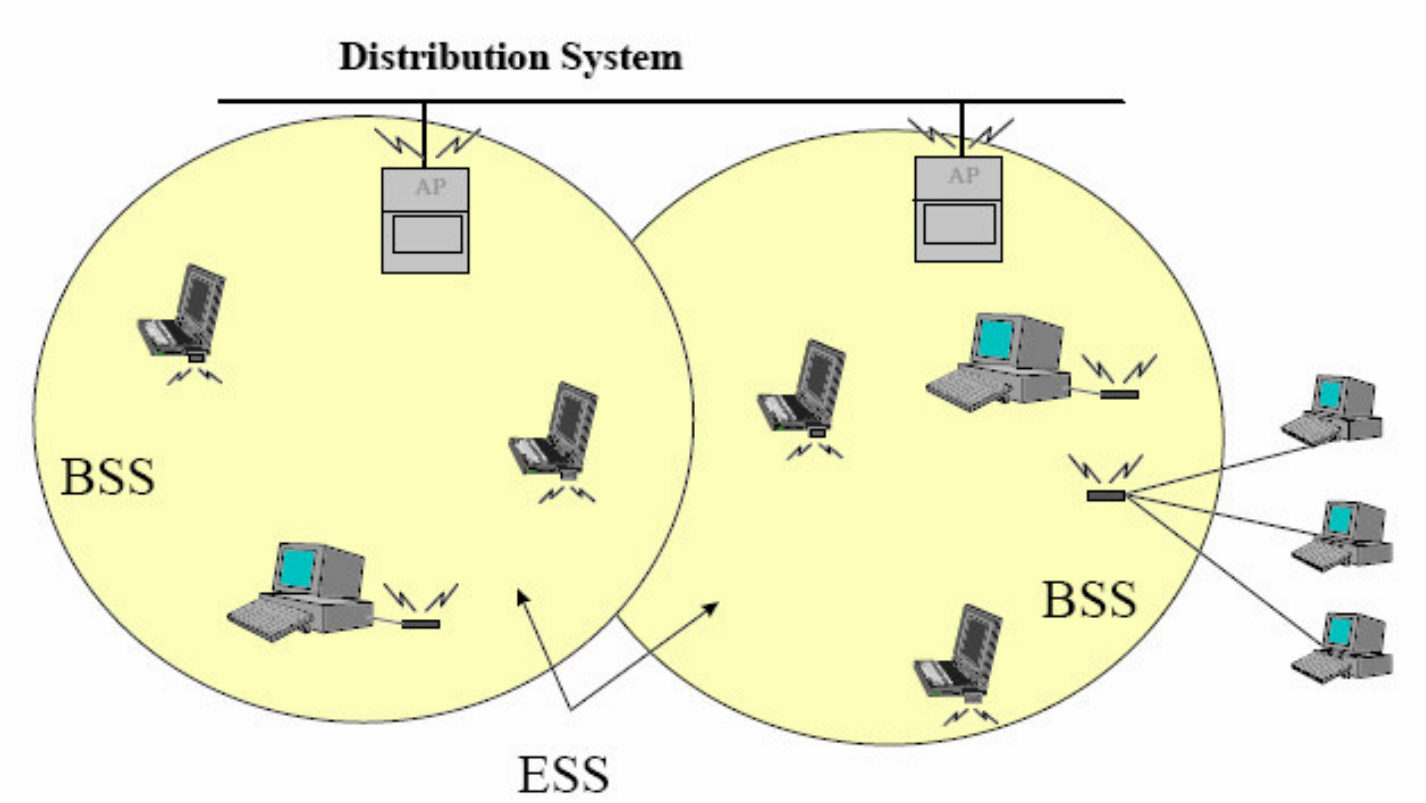
| | |
|---|---|
| IEEE 802. 11j | Japanese Standard upgrade, 2004 |
| IEEE 802. 11k | Define measurement items and protocol |
| IEEE 802. 11l | Reserved |
| IEEE 802. 11m | Maintenance Standard |
| IEEE 802. 11n | Draft version at this moment, using MIMO (Multi-input Multi Output) Technology to increase transmission speed to 300–600Mbps |
| IEEE 802. 11r | Define implementations of WLAN roaming, enables 802.11 able to be applied to mobile and VoIP applications |
| IEEE 802. 11s | Standard for Mesh under standard architecture |

# 2.2 Basic features IEEE 802.11x and WLAN Modes

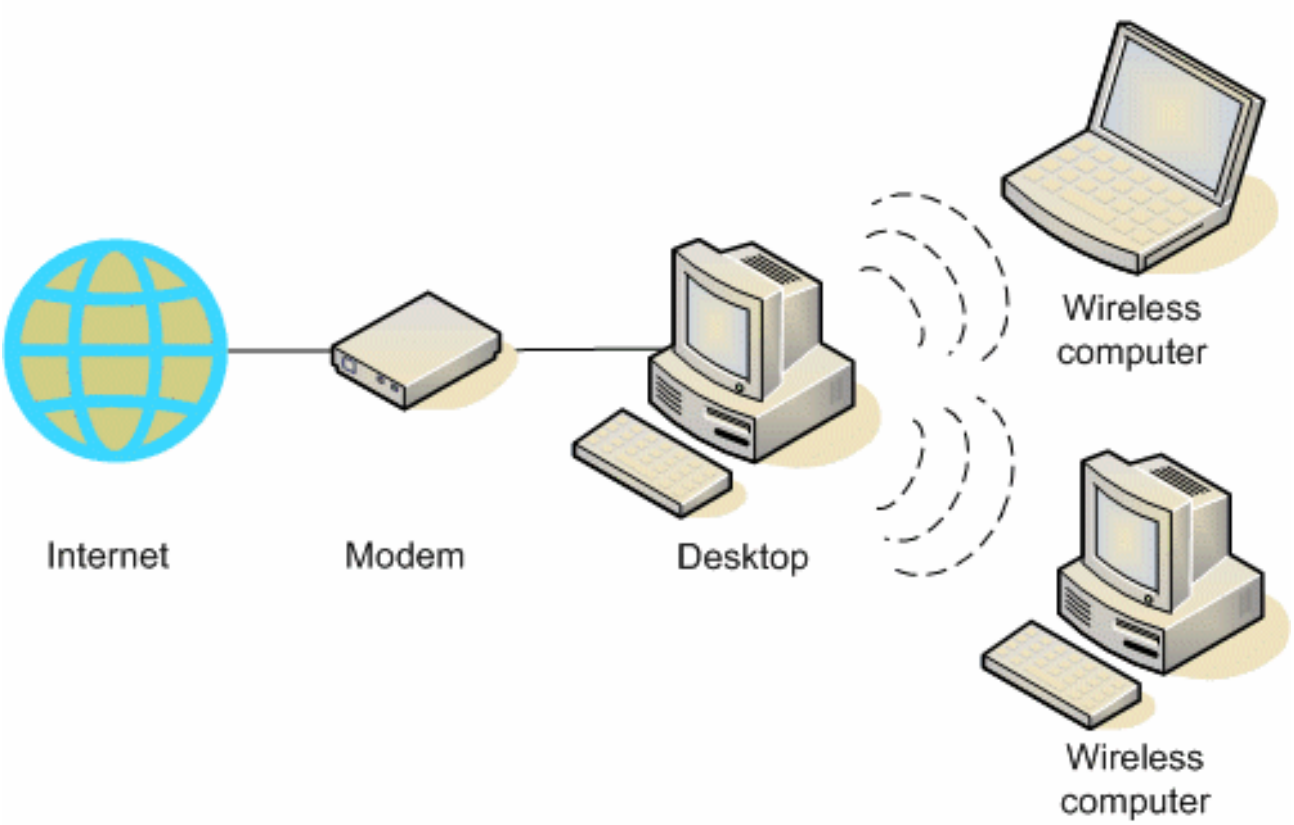
| Protocol | Release Date | Spectrum | Max. Speed | Typical Range (indoor) | Typical Range (outdoor) |
|---|---|---|---|---|---|
| 802.11 | 1997 | 2.4–2.5 GHz | 2 Mbps | --- | --- |
| 802.11a | 1999 | 5.15–5.35/5.47–5.725/ 5.725–5.875 GHz | 54 Mbps | 30 m | --- |
| 802.11b | 1999 | 2.4–2.5 GHz | 11 Mbps | 30 m | 100 m |
| 802.11g | 2003 | 2.4–2.5 GHz | 54 Mbps | 30 m | 100 m |
| 802.11n | 2008 | 2.4 GHz or 5 GHz bands | 600 Mbps | 50 m | 125 m |

# 3. IEEE 802.11 Architecture

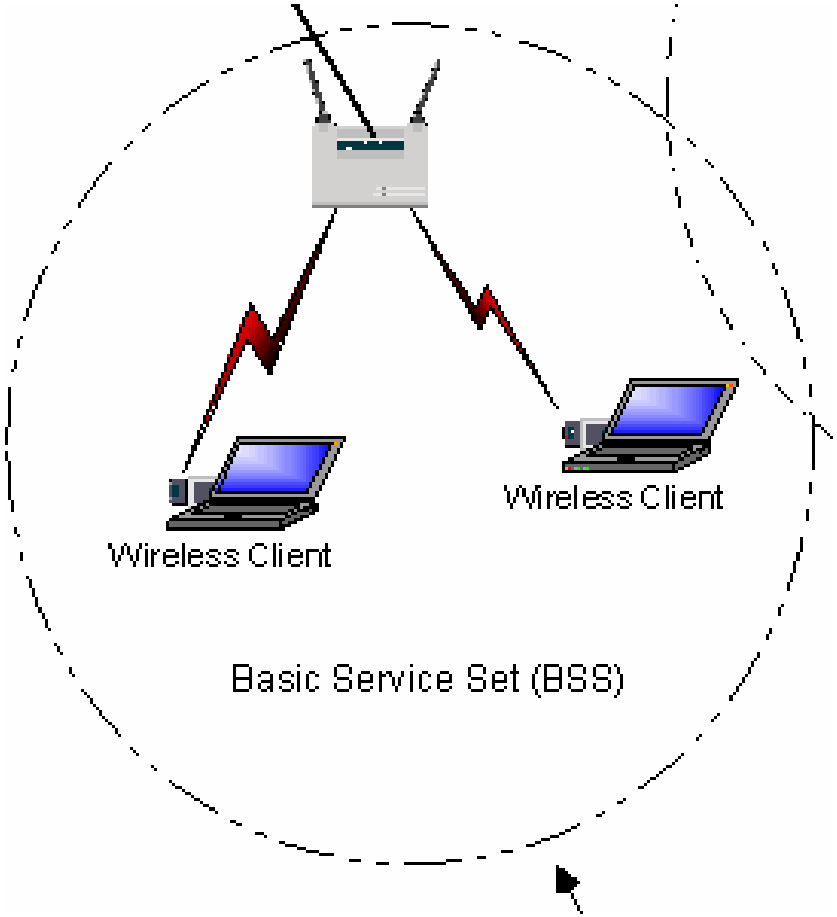
## 3.1 Architecture Components



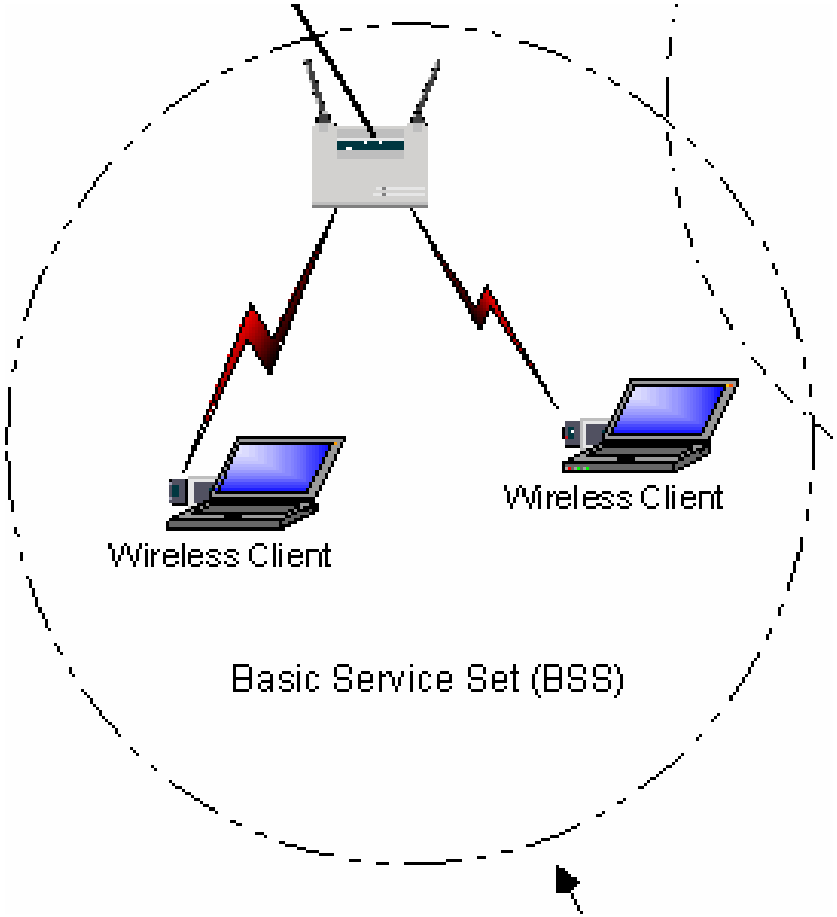
# 3.2 Ad-Hoc operating mode



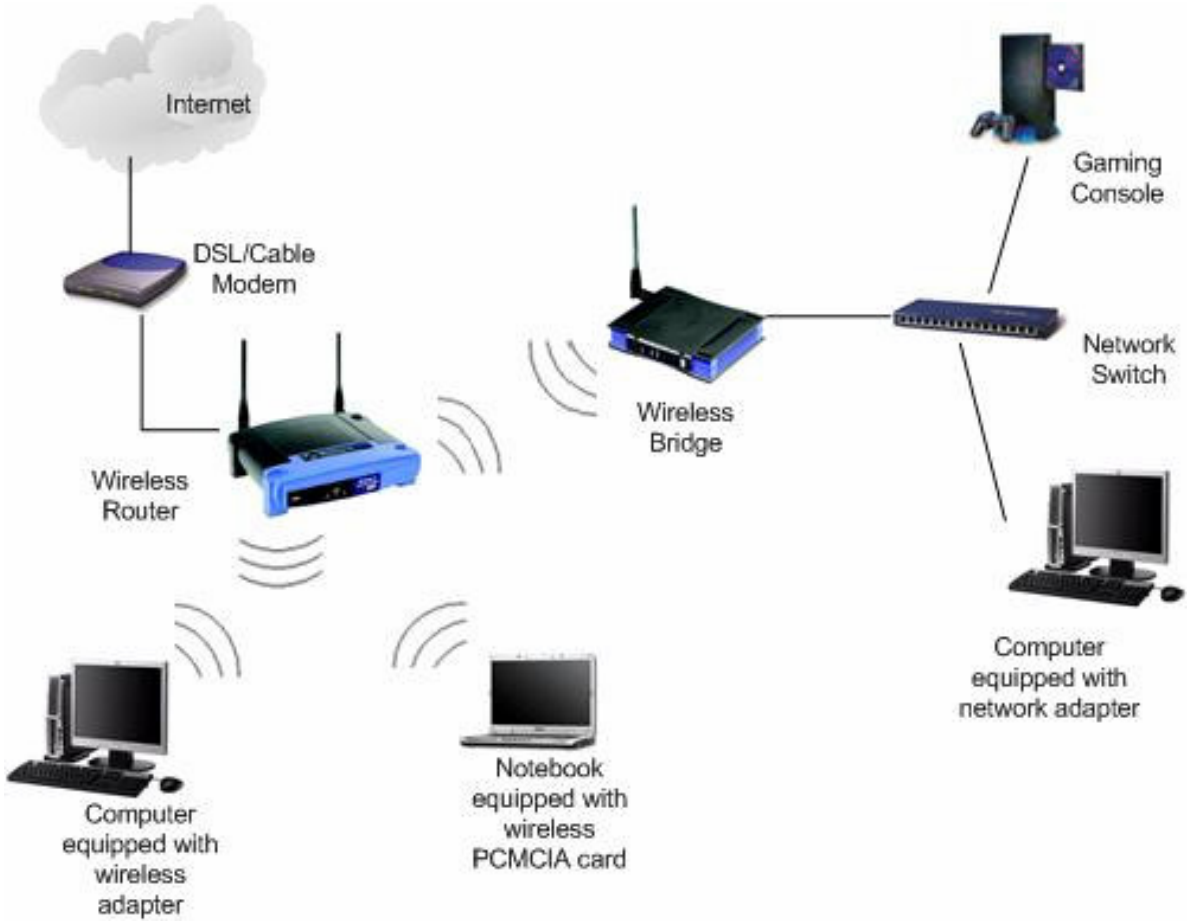
# 3.3 Infrastructure operating mode



# 3.3 Infrastructure operating mode 2

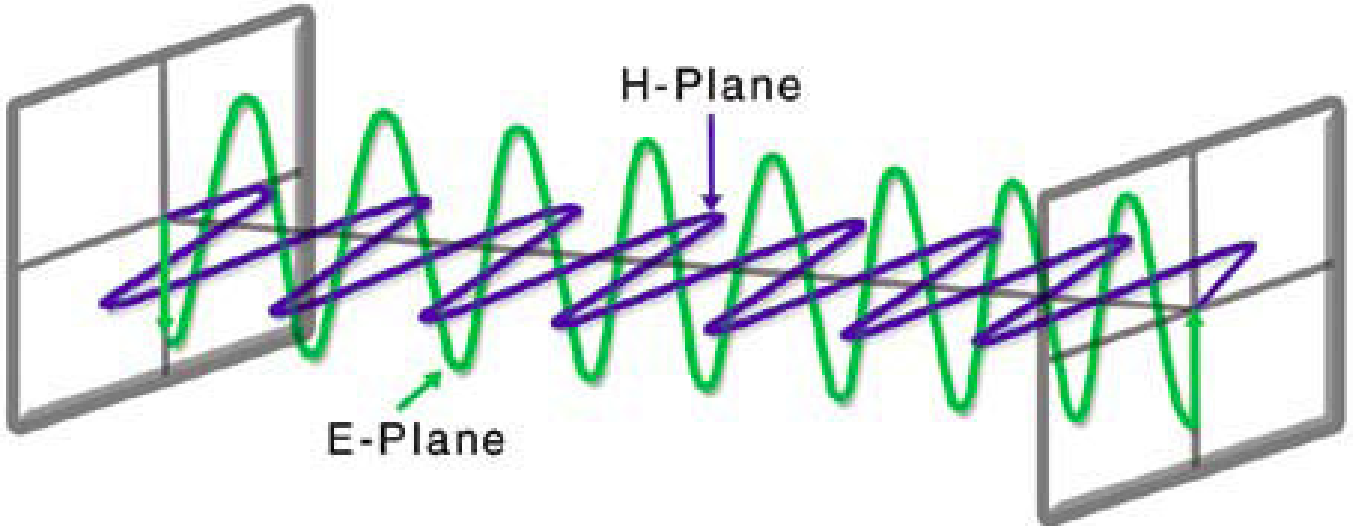


# 3.4 Bridge operating mode

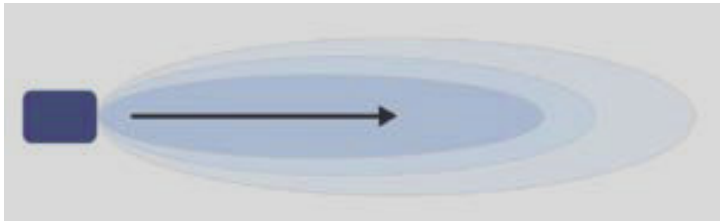


# 3.5 IEEE802.11 Radio Basics

## 3.5.1. Electromagnetics waves




Antenna

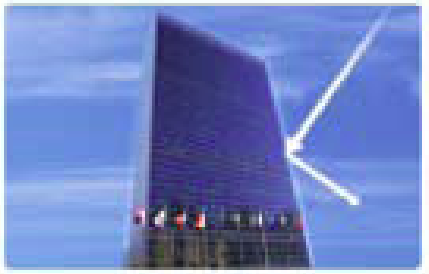


# 3.5.1. Electromagnetics waves

- **Diffraction (Shadow Fading)**

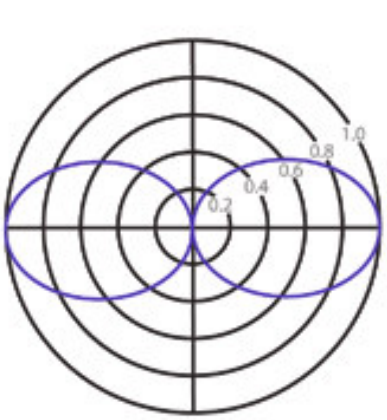
- **Scattering**

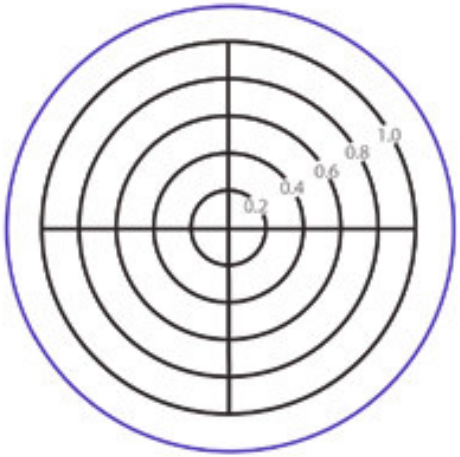
- **Reflection**



# 3.5.2 Types of Antennas

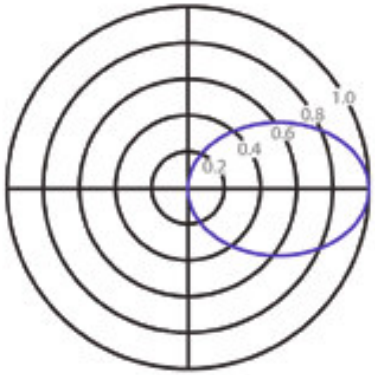
- **omni-directional**

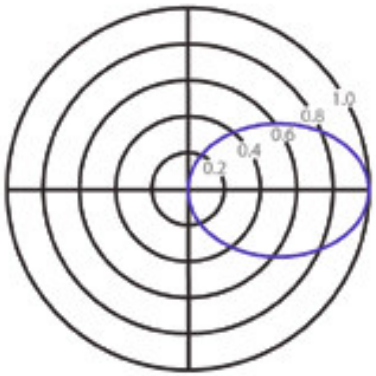



E-plane H-plane

- **Uni-directional**

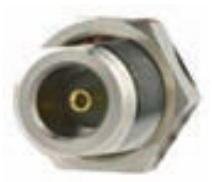



# 3.5.3 Antenna Specifications

- Connector types


N-type (male)


N-type (female)


RP-SMA (male)


RP-SMA (female)


SMA (female)

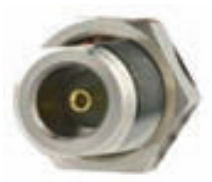

SMA (male)

- Half-Power Beam Width (HPBW)
- Antenna Polarity
- Frequency

# 3.5.3 Antenna Specifications

- Connector types


N-type (male)


N-type (female)


RP-SMA (male)

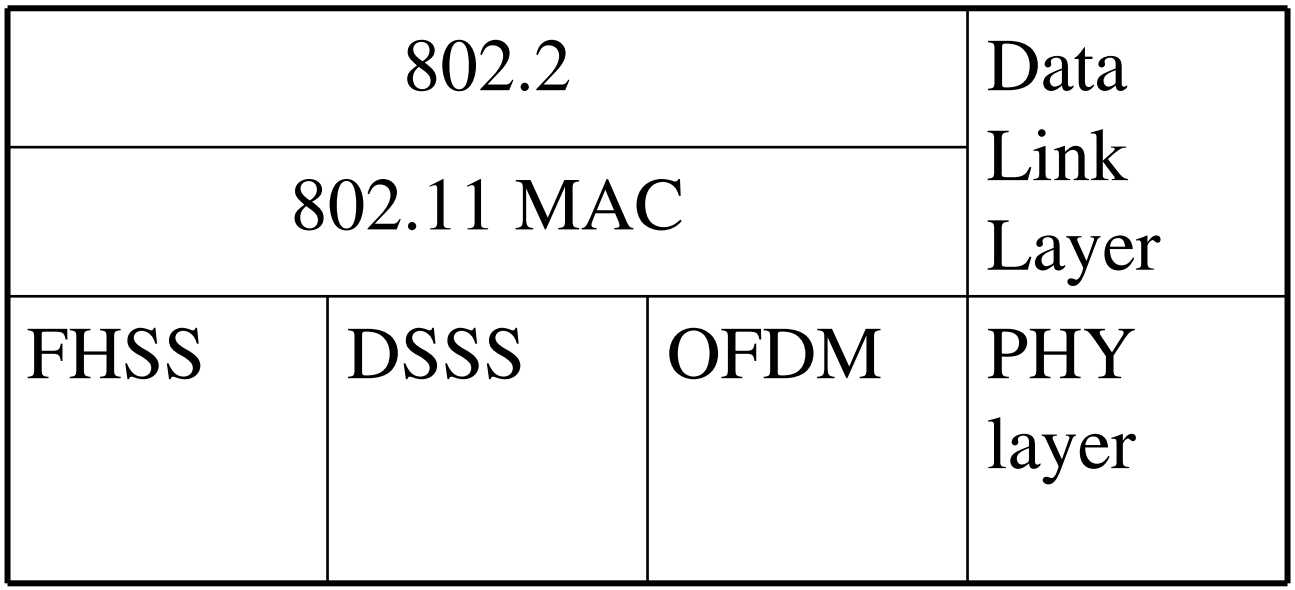

RP-SMA (female)


SMA (female)


SMA (male)

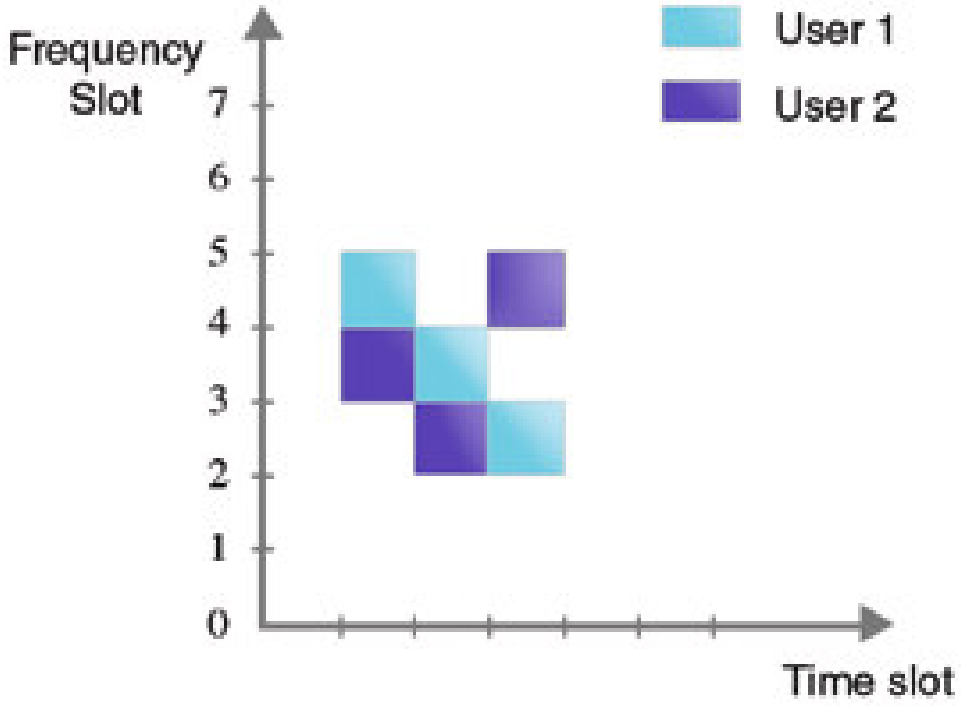
- Half-Power Beam Width (HPBW)
- Antenna Polarity
- Frequency

# 4. IEEE 802.11 Layers Description



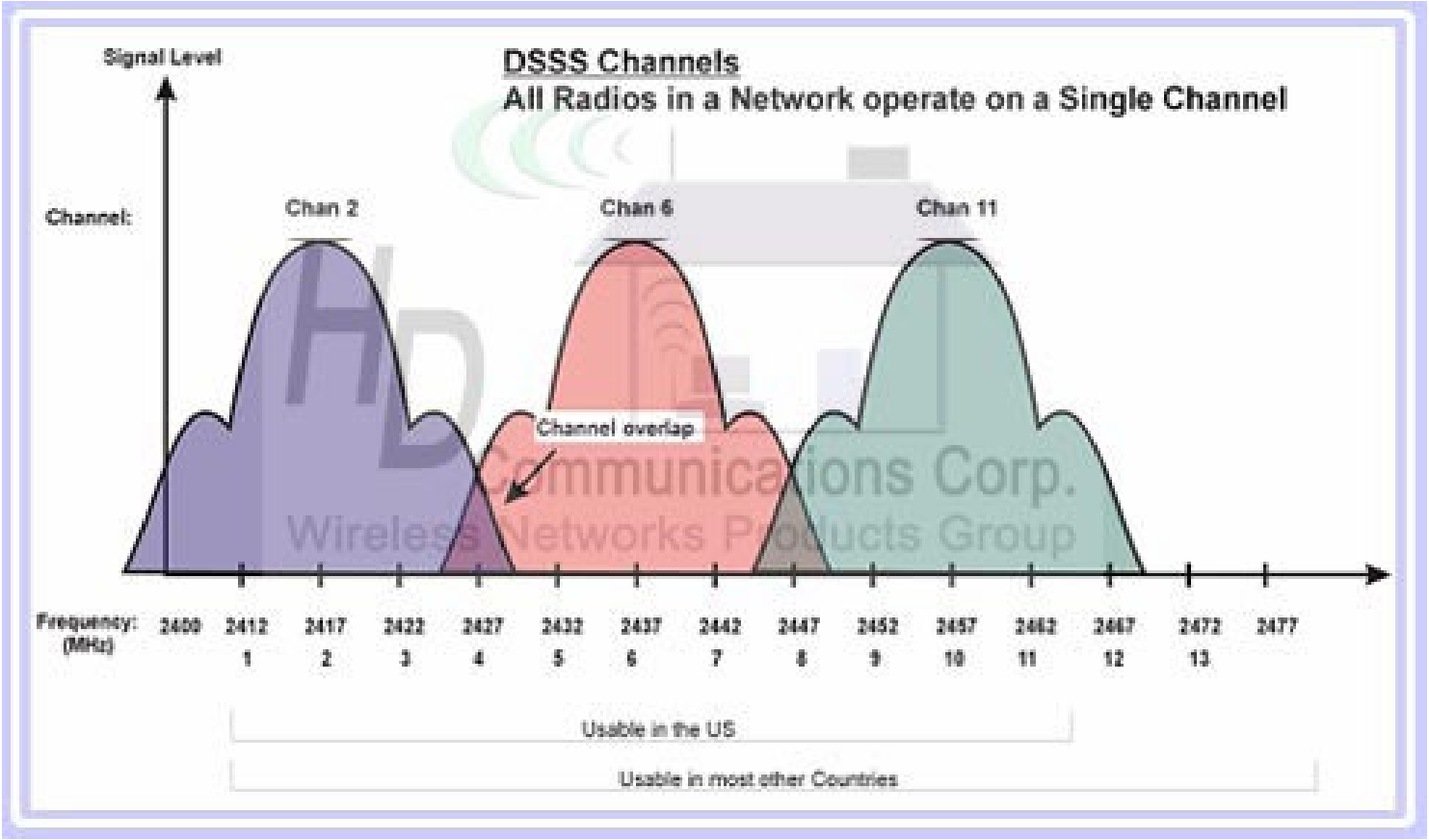
# 4.1. Modulation Technologies (1)

## 4.1.1 Frequency Hopping Spread Spectrum (FHSS)



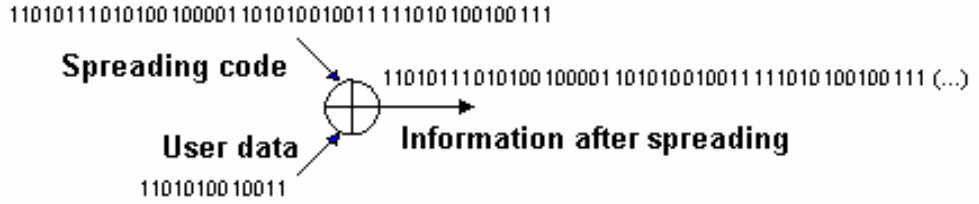
# 4.1. Modulation Technologies (2)

## 4.1.2 Direct Sequence Spread Spectrum (DSSS)



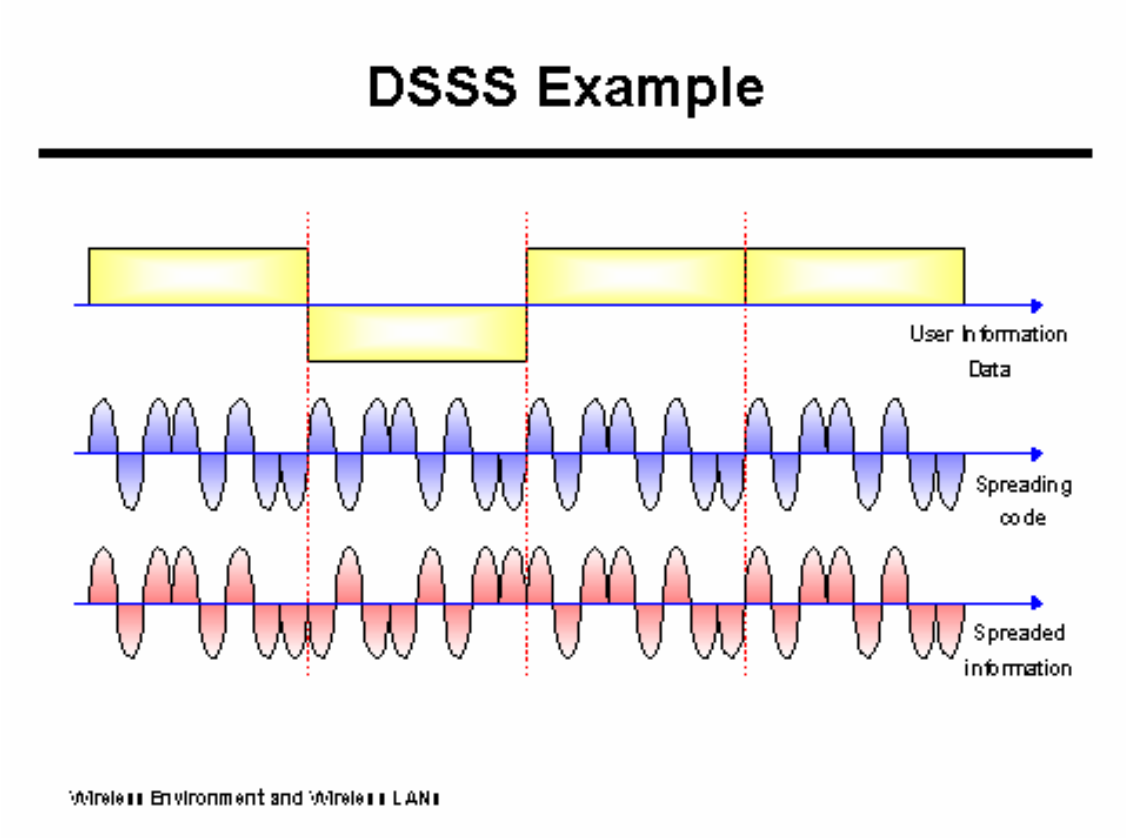
# Principle DSSS

## Direct Sequence Spread Spectrum (DSSS)

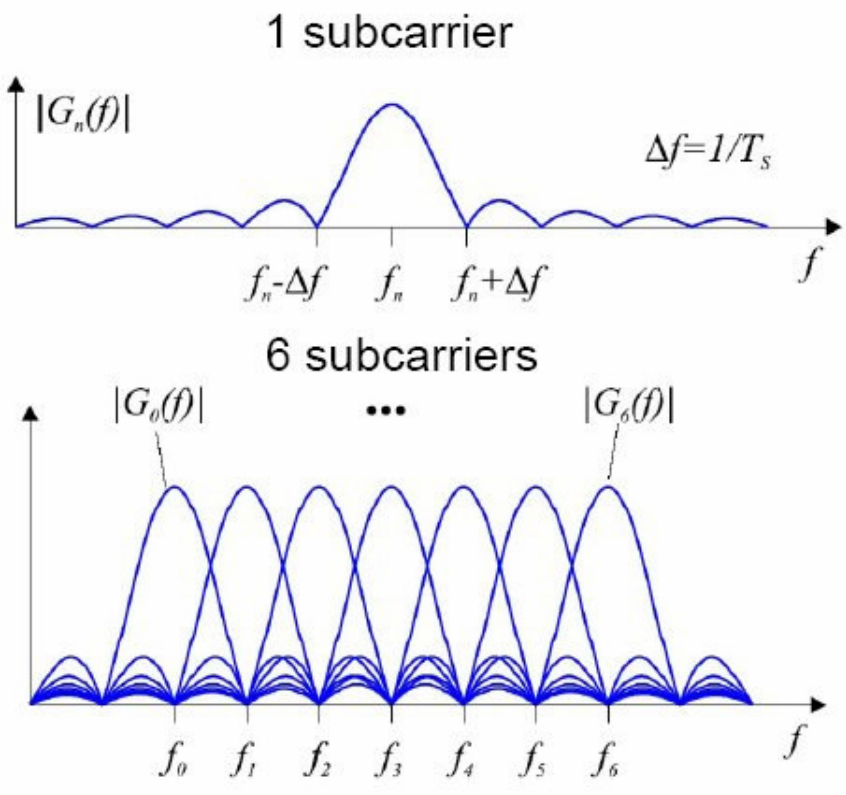



- Data signal is multiplied by a spreading code, and resulting signal occupies a much higher frequency band
- Spreading code is a pseudo-random sequence

# Example DSSS



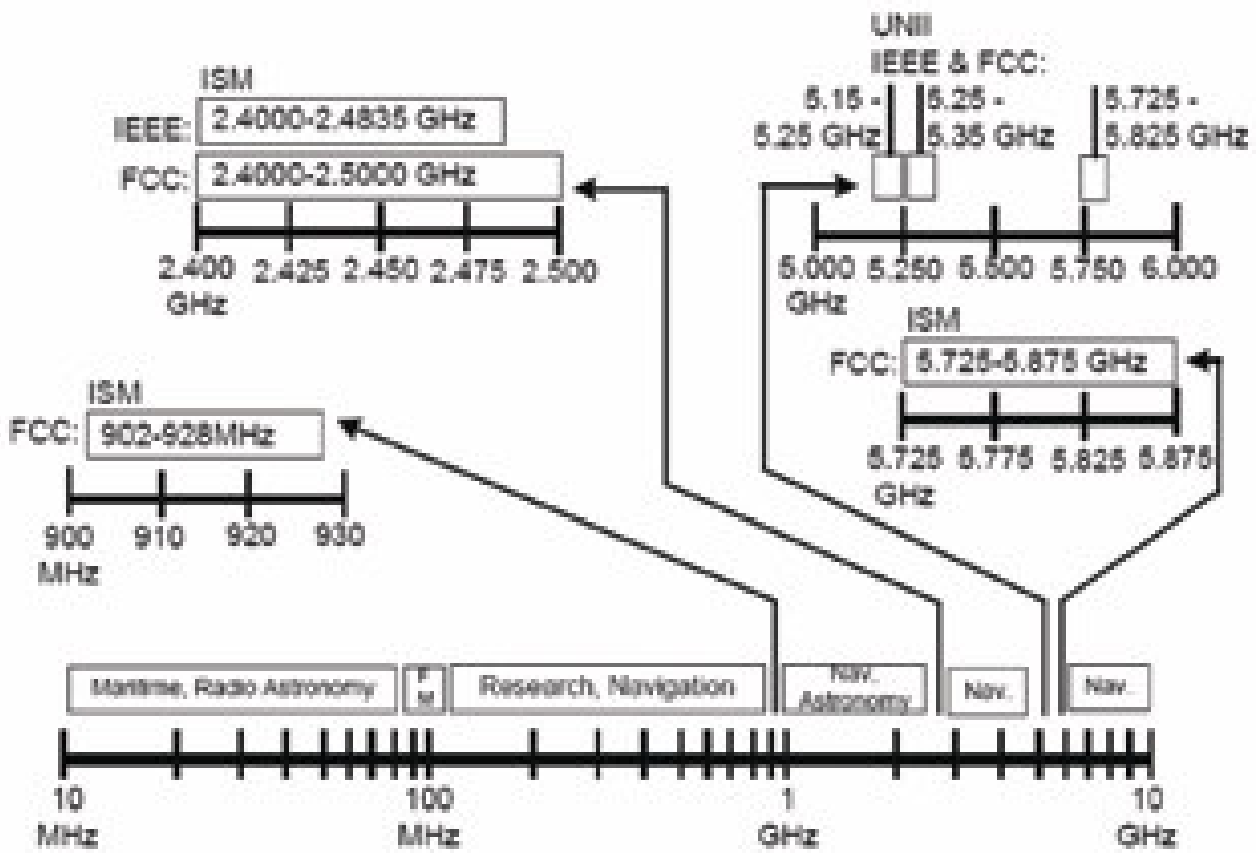
# 4.1.3 OFDM (Orthogonal Frequency Division Multiplexing)



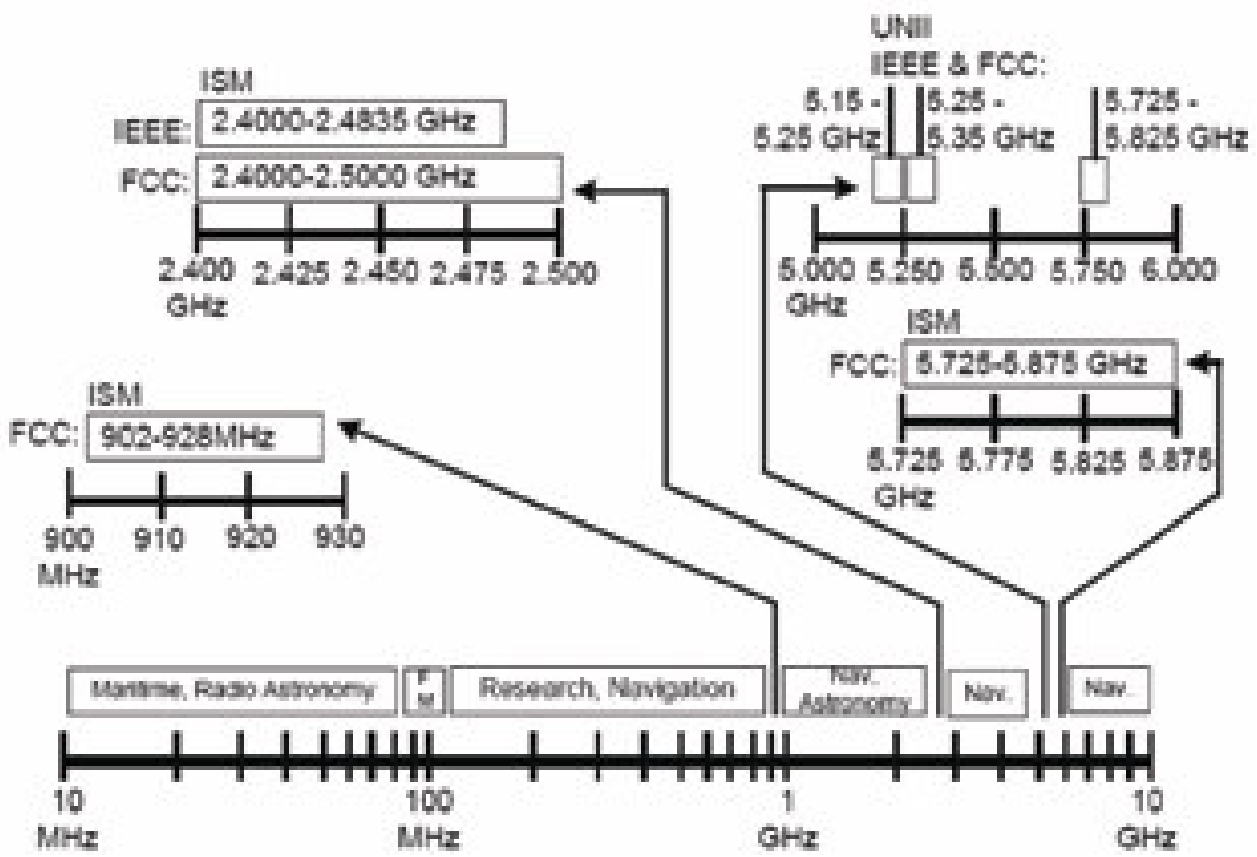
# 4.1.4 Summary modulation techniques

| Modulation Technique | DSSS | FHSS | OFDM |
|---|---|---|---|
| Narrowband Interference | Less resistance (22 MHz wide contiguous bands) | more resistance (79 MHz wide contiguous | Much less (multicarrier modulation) |
| Interference susceptibility | Medium | High | Low |
| Compatibility | 802.11b (WiFi Alliance) | None | 802.11a, 802.11g |
| Implementation Cost | Comparatively less | Comparatively more | High |
| Throughput | 5 – 6 Mbps | 2 Mbps for 802.11 | 25 Mbps |

# 4.1.5 Un-licensed bands ISM and UNII



# 4.1.5 Un-licensed bands ISM and UNII



# • 2.4 GHz ISM Band/country

| Channel | Center Frequency | Eu, M. East, Asia | USA | Japan |
|---|---|---|---|---|
| 1 | 2.412 GHz | Y | Y | Y |
| 2 | 2.417 GHz | Y | Y | Y |
| 3 | 2.422 GHz | Y | Y | Y |
| 4 | 2.427 GHz | Y | Y | Y |
| 5 | 2.432 GHz | Y | Y | Y |
| 6 | 2.437 GHz | Y | Y | Y |
| 7 | 2.442 GHz | Y | Y | Y |
| 8 | 2.447 GHz | Y | Y | Y |
| 9 | 2.452 GHz | Y | Y | Y |
| 10 | 2.457 GHz | Y | Y | Y |
| 11 | 2.462 GHz | Y | Y | Y |
| 12 | 2.467 GHz | Y | | Y |
| 13 | 2.472 GHz | Y | | Y |
| 14 | 2.484 GHz | | | Y |

# • Signal Power limit

| ISM Bands | Power Limit |
|---|---|
| **902 - 928 MHz** | |
| Cordless phones | 1 W |
| Microwave ovens | 750 W |
| Industrial heaters | 100 kW |
| Military radar | 1000 kW |
| **2.4 - 2.4835 GHz** | |
| Wi-Fi - 802.11b/g | 1 W |
| Microwave ovens | 900 W |
| **5 GHz** | |
| 5.725 - 5.825 GHz | 4 W |
| Wi-Fi - 802.11a/n | |
| **U-NII 5 GHz Bands** | |
| Wi-Fi - 802.11a/n | |
| 5.15 - 5.25 GHz | 200 mW |
| 5.25 - 5.35 GHz | 1 W |
| 5.47 - 5.725 GHz | 1 W |
| 5.725 - 5.825 GHz | 4 W |

# • Signal Power limit

| ISM Bands | Power Limit |
|---|---|
| **902 - 928 MHz** | |
| Cordless phones | 1 W |
| Microwave ovens | 750 W |
| Industrial heaters | 100 kW |
| Military radar | 1000 kW |
| **2.4 - 2.4835 GHz** | |
| Wi-Fi - 802.11b/g | 1 W |
| Microwave ovens | 900 W |
| **5 GHz** | |
| 5.725 - 5.825 GHz | 4 W |
| Wi-Fi - 802.11a/n | |
| **U-NII 5 GHz Bands** | |
| Wi-Fi - 802.11a/n | |
| 5.15 - 5.25 GHz | 200 mW |
| 5.25 - 5.35 GHz | 1 W |
| 5.47 - 5.725 GHz | 1 W |
| 5.725 - 5.825 GHz | 4 W |

# 4.2 MAC layer in WLAN

3 different MAC mechanisms:

- DCF (Direct or Distribution Coordination Function)
  - ✓Must be supported
  - ✓Uses CSMA/CA
  - ✓For Asynchronous data transfer
- DCF (CSMA/CA) with RTS/CTS
  - ✓Optional
  - ✓Introduced to solve the hidden node problem
  - ✓Reduces the number of collisions
- PCF (Point Coordination Function)
  - ✓Optional
  - ✓Based on DCF+RTS/CTS
  - ✓For Infrastructure mode (AP)
  - ✓Combines polling with asynchronous data transfer

# 4.2.1 DCF (Direct or Distribution Coordination Function)

## 4.2.1.1 CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- Channel access mechanism (is the part of the protocol which specifies how the node uses the medium: when to listen, when to transmit..) used by most wireless LANs in the ISM bands
- The basic principles of CSMA/CA are listen before talk and contention: This is an asynchronous message passing mechanism (connectionless), delivering a best effort service, but no bandwidth and latency guarantee.
- Main advantages:
    - suited for network protocols such as TCP/IP
    - adapts quite well to variable traffic conditions
    - quite robust against interferences
- CSMA/CA is fundamentally different from the channel access mechanism used by cellular phone systems
- CSMA/CA is derived from CSMA/CD (Collision Detection), which is the basis of Ethernet. The main difference is collision avoidance: the protocol can't directly detect collisions (Ethernet protocols can) and only tries to avoid them.

# How a CSMA (Carrier Sense Multiple Access) works

A CSMA protocol works as follows:

- A station desiring to transmit senses the medium,
- if the medium is busy (ie some other station is transmitting) then the station will defer its transmission to a later time
- if the medium is sensed free then the station is allowed to transmit.

# Principle of CD (Collision Detection)

- CSMA is very effective when the medium is not heavily loaded, since it allows stations to transmit with minimum delay
- But there is always a chance of stations transmitting at the same time (collision), caused by the fact that the stations sensed the medium free and decided to transmit at once.
- These collision situations must be identified, so the MAC layer can retransmit the packet by itself and not through upper layers, which would cause significant delay.
- In the 'wired' Ethernet case this collision is recognized by the transmitting stations which go to a retransmission phase based on an exponential random backoff algorithm.

Collision Detection mechanisms are a good idea on a wired LAN, but they cannot be used in a Wireless LAN environment

# Why CD is not possible in WLAN

CD cannot be used on a Wireless LAN environment, for two main reasons:

- Implementing a CD mechanism would require the implementation of a Full Duplex radio, capable of transmitting and receiving at once, an approach that would increase the price significantly.
- In a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the CD), and the fact that a station is willing to transmit and senses the medium free, doesn't necessarily mean that the medium is free around the receiver area.

The 802.11 uses a Collision Avoidance (CA) mechanism together with a Positive Acknowledge scheme

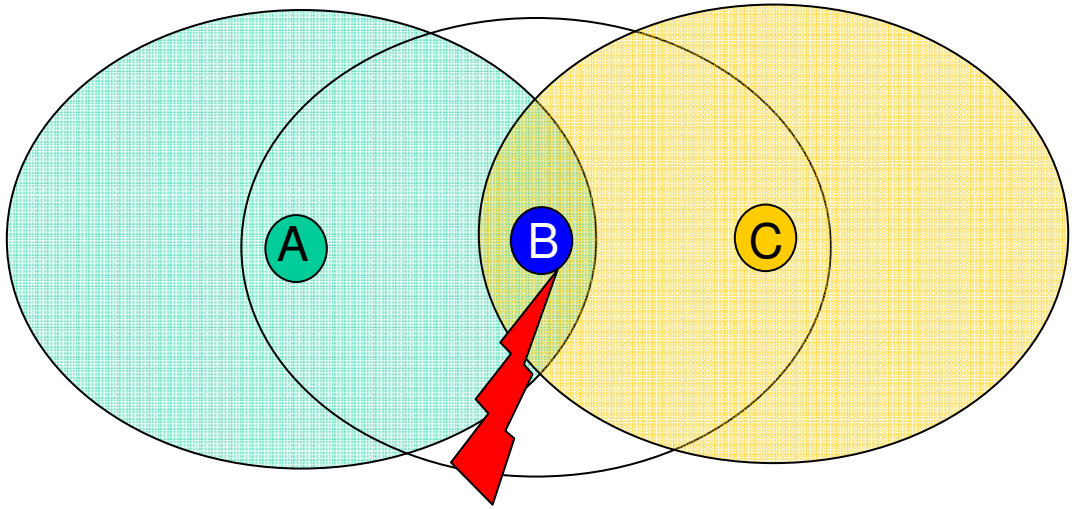
## 4.2.1.2 DCF = CSMA/CA with Positive Acknowledgement (ACK)

A station willing to transmit senses the medium:

- If the medium is busy then it defers
- If the medium is free for a specified time (called DIFS, Distributed Inter Frame Space, in the standard) then the station is allowed to transmit
- The receiving station will check the CRC of the received packet and send an acknowledgment packet (ACK)
- Receipt of the ACK will indicate to the transmitter that no collision occurred.
- If the sender does not receive the ACK then it will retransmit the fragment until it is acknowledged or discard it after a given number of retransmissions

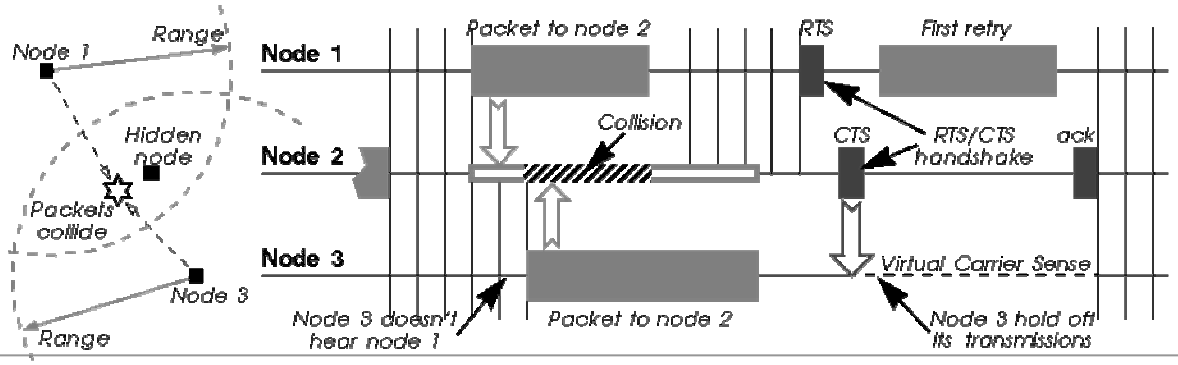
# Hidden Node problem

- Station A senses the channel (CS) and transmits to station B when channel is idle
- Station C cannot detect the transmission of station A and think s the channel is idle (CS fails)
- Station C transmits and a collision occurs at station B
- Station A does not detect the collision because Sation A is hidden from C

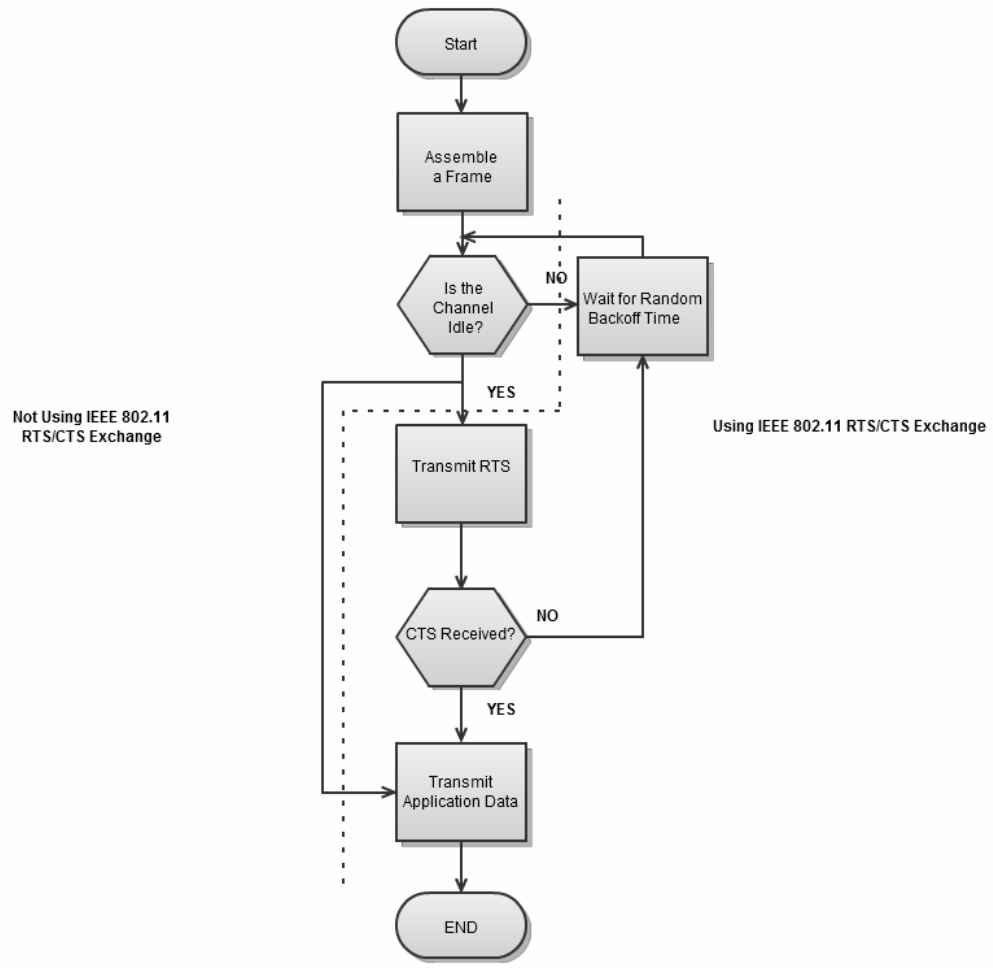


# 4.2.2 DCF with RTS/CTS ‚Virtual Carrier Sense‘

- In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a ‘Virtual Carrier Sense mechanism:
- A station willing to transmit a packet will first transmit a short control packet called RTS (Request To Send), which will include the source, destination, and the duration of the following transaction (ie the packet and the respective ACK )
- The destination station will respond (if the medium is free) with a response control Packet called CTS (Clear to Send), which will include the same duration information.
- All stations receiving either the RTS and/or the CTS, will set their Virtual Carrier Sense indicator (called NAV, for Network Allocation Vector), for the given duration, and will use this information together with the Physical Carrier Sense when sensing the medium.

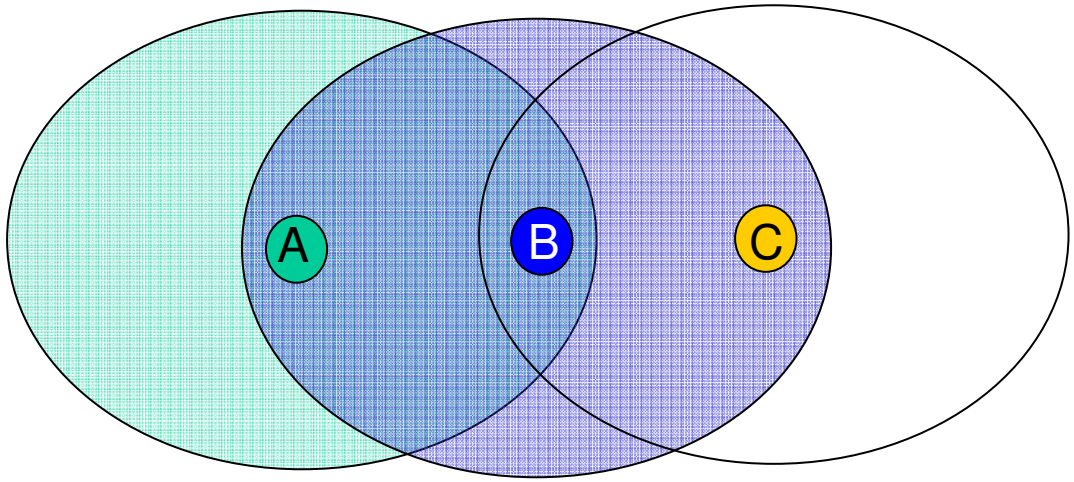


# DCF (CSMA/CA) without/with RTS/CTS schematic



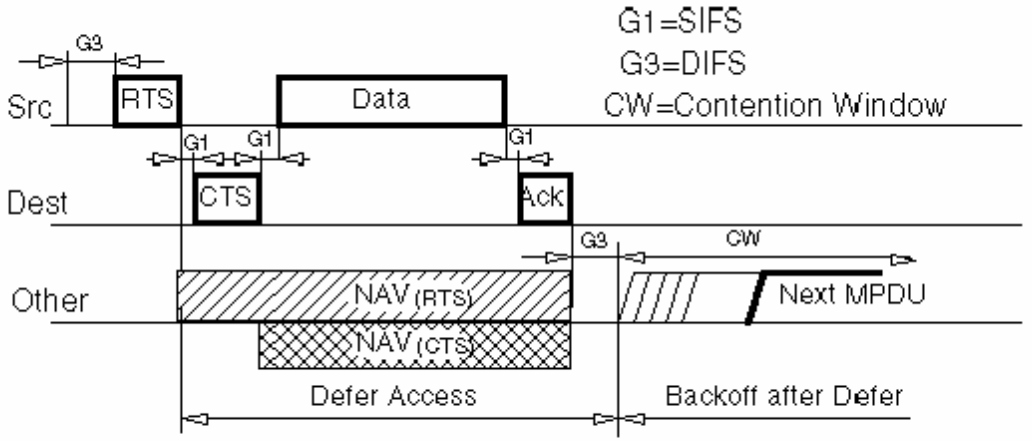
# RTS/CTS/NAV mechanism (Solution ‚Hidden nodes‘)

- Station A  senses the channel (CS) and transmits RTS to station B when channel is idle (RTS contains duration of the transmission)
- On reception of RTS, station  B transmits CTS to A
- Station C also receives this CTS (C is not hidden for B) and knows now the channel is busy for a while and must wait



# Diagram of the RTS/CTS/NAV mechanism

- The following diagram shows a transaction between two stations A (Src) and B (Dest), and the NAV setting of their neighbours (Other)
- On reception of RTS, station B transmits CTS to A
- Station C (Other) also receives this CTS (C is not hidden from B) and knows now the channel is busy for a while and must wait
- The NAV State is combined with the physical carrier sense to indicate the busy state of the medium.



# Advantages DCF with RTS/CTS

- Reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter, to the short duration of the RTS transmission, because the station will hear the CTS and “reserve” the medium as busy until the end of the transaction
- The duration information on the RTS also protects the transmitter area from collisions during the ACK (by stations that are out of range of the acknowledging station)
- RTS and CTS are short frames. This also reduces the possibility of collisions, since these are recognized faster than they would be if the whole packet were transmitted, (this is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transaction, and this is controlled per station by a parameter called RTSThreshold ).

# 4.2.3 PCF (Point Coordination Function)

- Point Coordination Function (PCF) supports time-sensitive traffic flows
- Wireless access points periodically send beacon frames to communicate network identification and management parameters specific to the wireless network.
- Between the sending of beacon frames, PCF splits the time into a contention-free period and a contention period. With PCF enabled, a station can transmit data during contention-free polling periods.
- However, PCF hasn't been implemented widely because the technology's transmission times are unpredictable.

# 4.3 Roaming

## 4.3.1 What is Roaming?

- Roaming is the process of moving from one cell (or BSS) to another without losing connection.
- Slow roaming speed between mobile network's access points sometimes hinders the performance of industrial applications.
- 'High speed roaming' may be the solution

  Two principles:

  ✓Roaming by Signal

  ✓Roaming by Channel

# 4.3 Roaming

## 4.3.1 What is Roaming?

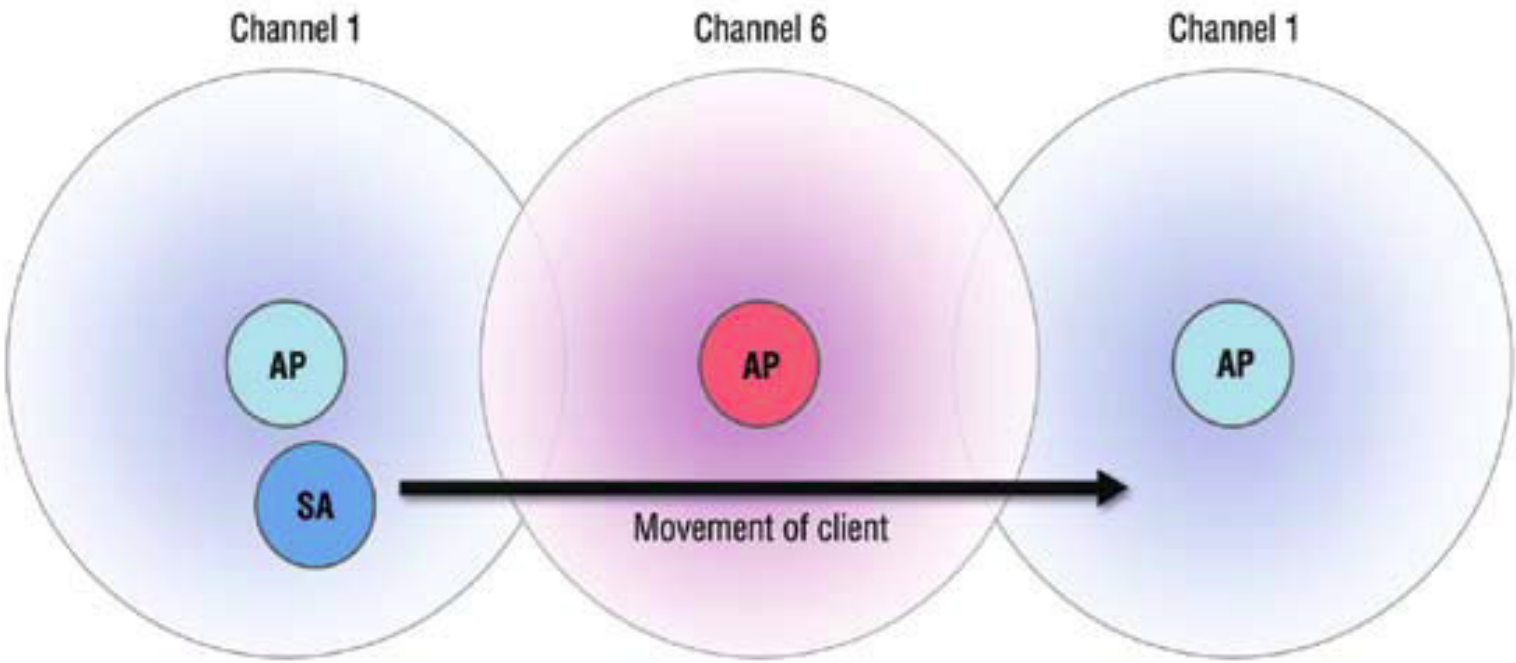
- Roaming is the process of moving from one cell (or BSS) to another without losing connection.
- Slow roaming speed between mobile network's access points sometimes hinders the performance of industrial application.
- 'High speed roaming' may be the solution

  Two principles:

  ✓Roaming by Signal

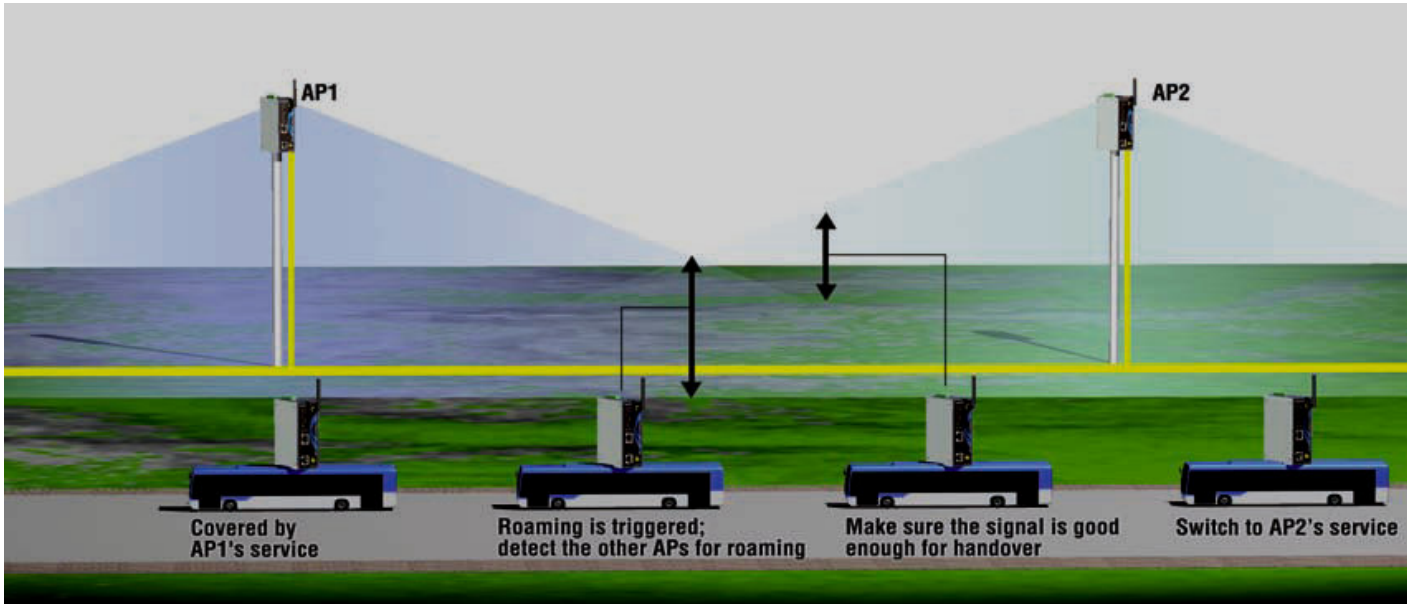
  ✓Roaming by Channel

# 4.3.2 Basic Roaming (Slow Roaming)



# 4.3.3 High Speed Roaming

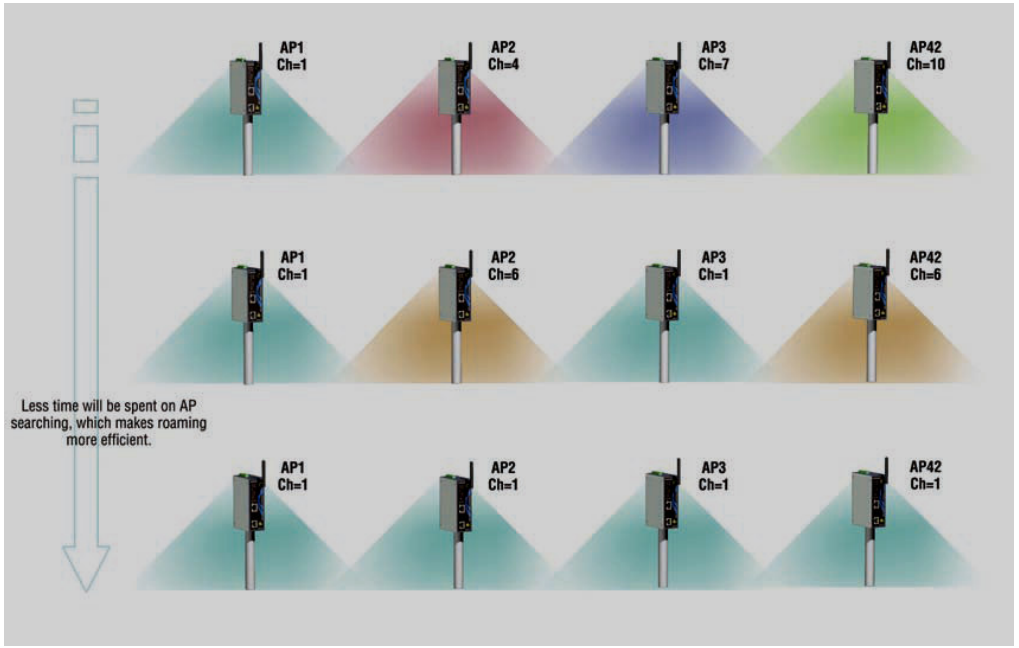
## ➢ Roaming by Signal




- Roaming by Signal allows roaming only when the current AP's signal drops below a certain threshold and roaming to another AP will improve transmission quality and provide a stronger signal.

# 4.3.3 High Speed Roaming

## ➢ Roaming by Channel




- Roaming by Channel unifies AP channels to avoid wasting channel hopping time during roaming.

# 5. Power Management (PSM)

## 5.1 PSM in Wireless LANs

- PSM is based on a synchronous sleep scheduling policy, in which wireless nodes (stations) are able to alternate between an active mode and a sleep mode.
- As a wireless station using PSM first joins an infrastructure based WLAN, it must notify its access point that it has PSM enabled. The access point then synchronizes with the PSM station allowing it to begin running its synchronous sleep schedule.
- When packets arrive for each of these PSM stations, the access point buffers them until their active period comes around again. At the beginning of each active period, a beacon message is sent from the access point to each wireless station in order to notify them of these buffered packets. PSM stations then request these packets and they are forwarded from the access point. Once all buffered frames have been received, a PSM station resumes with its sleep schedule wherever it left off. Whenever a PSM station has data to send, it simply wakes up, sends its packet, and then resumes its sleep schedule protocol as appropriate.
- The throughput achieved with these techniques is significantly less than with them disabled.
- While PSM may significantly reduce the energy consumed by a wireless station, many users prefer to sacrifice these power savings for an increase in performance.

# 5. Power Management (PSM)

## 5.1 PSM in Wireless LANs

- PSM is based on a synchronous sleep scheduling policy, in which wireless nodes (stations) are able to alternate between an active mode and a sleep mode.
- As a wireless station using PSM first joins an infrastructure based WLAN, it must notify its access point that it has PSM enabled. The access point then synchronizes with the PSM station allowing it to begin running its synchronous sleep schedule.
- When packets arrive for each of these PSM stations, the access point buffers them until their active period comes around again. At the beginning of each active period, a beacon message is sent from the access point to each wireless station in order to notify them of these buffered packets. PSM stations then request these packets and they are forwarded from the access point. Once all buffered frames have been received, a PSM station resumes with its sleep schedule wherever it left off. Whenever a PSM station has data to send, it simply wakes up, sends its packet, and then resumes its sleep schedule protocol as appropriate.
- The throughput achieved with these techniques is significantly less than with them disabled.
- While PSM may significantly reduce the energy consumed by a wireless station, many users prefer to sacrifice these power savings for an increase in performance.

# 5.2 PSM in Wireless PANs (Bluetooth)

- Wireless nodes in a Bluetooth network are organized into groups known as piconets, with one node dedicated as the master node and all others as slave nodes.
- Up to seven active nodes can exist in a piconet at any given time, with up to 256 potential members (249 inactive).
- All nodes operate using a synchronous sleep scheduling policy in order to exchange data. A beacon messaging system similar to the one for 802.11 based networks is used to exchange messages between slave nodes and their master.
- All nodes are able to communicate with all other nodes within the Piconet, but messages between slaves must be sent exclusively through the master node.
- Bluetooth defines eight different operational states, 3 of which are dedicated to low power operations. These three low power states are known as Sniff, Hold, and Park.
- While in the Sniff state, an active bluetooth device simply lowers its duty cycle and listens to the piconet at a reduced rate.
- When switching to the Hold state, a device will shut down all communication capabilities it has with a piconet, but remain "active" in the sense that it does not give up its access to one of the seven active slots available for devices within the piconet.
- Devices in the Park state disable all communication with the piconet just as in the Hold state, except that they also relinquish their active node status.

# 6. WLAN Security

## The Evolution of Wireless Encryption

### 6.1 Basic Aspects

- AUTHENTICATION:
  to check a user's credentials and determine if the user should be given access to the data and resources provided by the protected network

- ENCRYPTION:
  encodes the data so that anyone who does not have the secret "key" will not be able to read the data

# 6.2 Authentication

- The 802.1X standard dictates how authentication on wired and wireless LANs is carried out.
- 802.1X is an authentication method that prevents unauthorized users from entering the network. It is used with WPA to form a complete WLAN security system.
- On many wireless systems, users either log into individual access points, or can freely enter the wireless network but cannot get further without additional authentication.
- 802.1X makes users authenticate to the wireless network itself, not an individual AP or another level like a VPN. This is more secure, as unauthorized traffic can be denied right at the AP.
- 802.1X authentication uses port-based access control, which means that the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" at each port to prevent unauthorized users from gaining access to protected data.

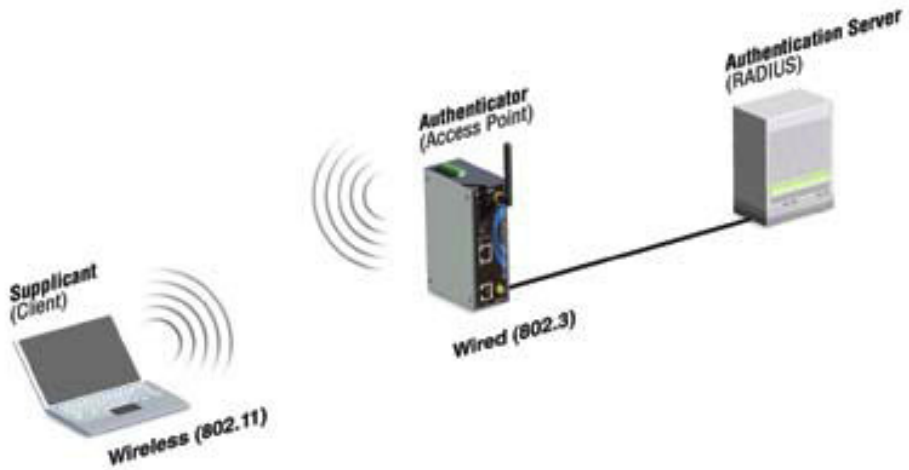
# 6.2 Authentication

- The 802.1X standard dictates how authentication on wired and wireless LANs is carried out.
- 802.1X is an authentication method that prevents unauthorized users from entering the network. It is used with WPA to form a complete WLAN security system.
- On many wireless systems, users either log into individual access points, or can freely enter the wireless network but cannot get further without additional authentication.
- 802.1X makes users authenticate to the wireless network itself, not an individual AP or another level like a VPN. This is more secure, as unauthorized traffic can be denied right at the AP.
- 802.1X authentication uses port-based access control, which means that the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" at each port to prevent unauthorized users from gaining access to protected data.

# Authentication procedure

The 802.1X authentication procedure involves three basic players:

- The supplicant is the client (PC or laptop computer, for example) who would like to gain access to network resources through the wireless network.
- The authenticator, which is usually an access point (AP) for a wireless network and plays the role of gatekeeper.
- The authentication server, which connects to the AP over a wired network and handles the authentication procedure.



# Authentication procedure WEP (Wired Equivalent Privacy)

- WEP provides a basic level of security to prevent unauthorized access to the network and protect wireless data.
- The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key
- Static shared keys (fixed length alphanumeric/hexadecimal strings) are used to encrypt data and are manually distributed to all wireless stations that want to use the wireless network.
- WEP has been found to have serious flaws
- WEP is not recommended for networks that require a high level of security.

# 6.2.1. WEP Open System Authentication

- The following steps occur when two devices use Open System Authentication:
  1. The station sends an authentication request to the access point.
  2. The access point authenticates the station.
  3. The station associates with the access point and joins the network.

# 6.2.2 WEP Shared Key Authentication

- The following steps occur when two devices use Shared Key Authentication:
  1. The station sends an authentication request to the access point.
  2. The access point sends challenge text to the station.
  3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point.
  4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station.
  5. The station connects to the network. If the decrypted text does not match the original challenge text (that is, the access point and station do not share the same WEP key), then the access point will refuse to authenticate the station, and the station will be unable to communicate with either the 802.11 network or the Ethernet network.

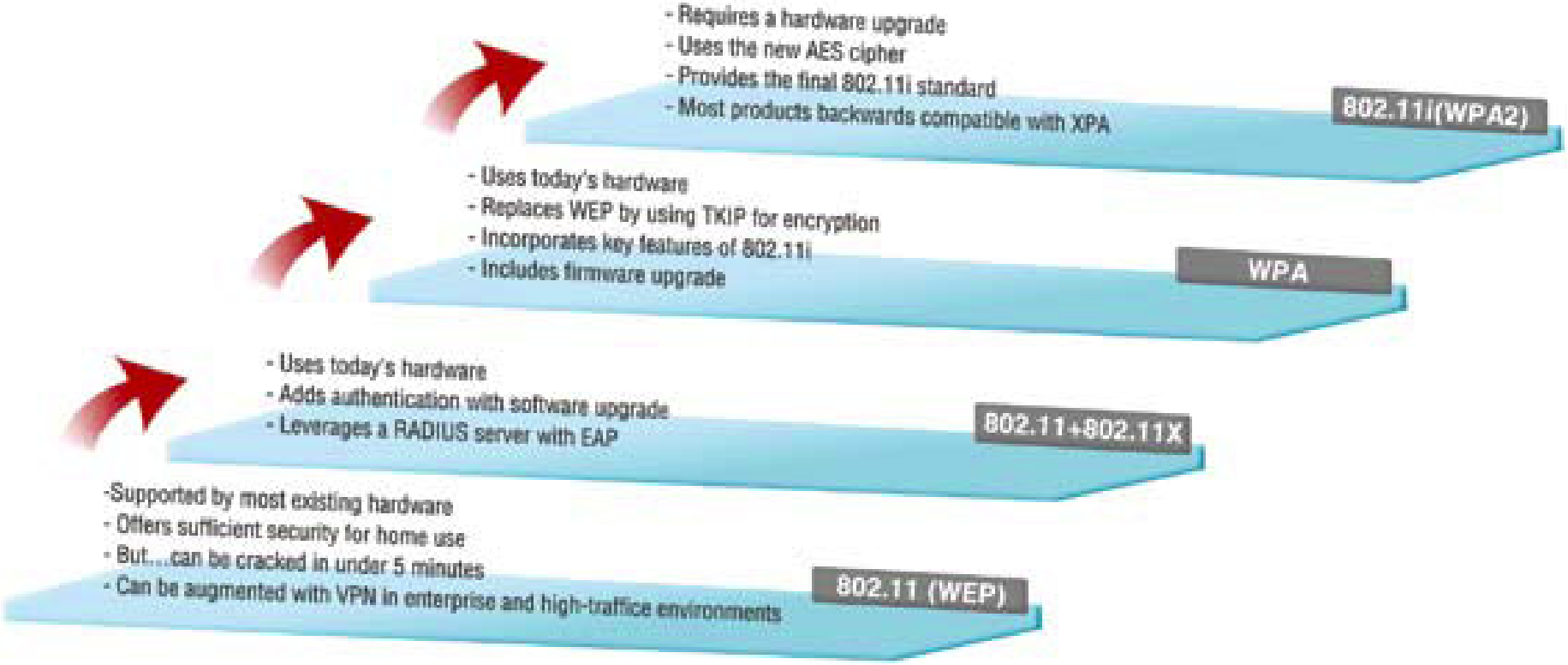
# 6.2.2 WEP Shared Key Authentication

- The following steps occur when two devices use Shared Key Authentication:
  1. The station sends an authentication request to the access point.
  2. The access point sends challenge text to the station.
  3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point.
  4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station.
  5. The station connects to the network. If the decrypted text does not match the original challenge text (that is, the access point and station do not share the same WEP key), then the access point will refuse to authenticate the station, and the station will be unable to communicate with either the 802.11 network or the Ethernet network.

# 6.3 Encryption

- The science of encryption or the making and breaking of codes, is one of the most crucial aspects of WLAN technology. This is because the radio waves used to transmit data packets between your computer and the wireless access point can pass through walls, floors, and other barriers.
- People who use laptops that have a wireless LAN card will know this first-hand, since it is often possible to pick up signals from wireless access points located in nearby apartments.
- Using a password to restrict entry to your network may not provide enough protection, since a reasonably clever person can still intercept your data packets.
- In fact, if the person intercepting the wireless data is more than reasonably clever, he or she may also be able to download and read the contents of the packets.

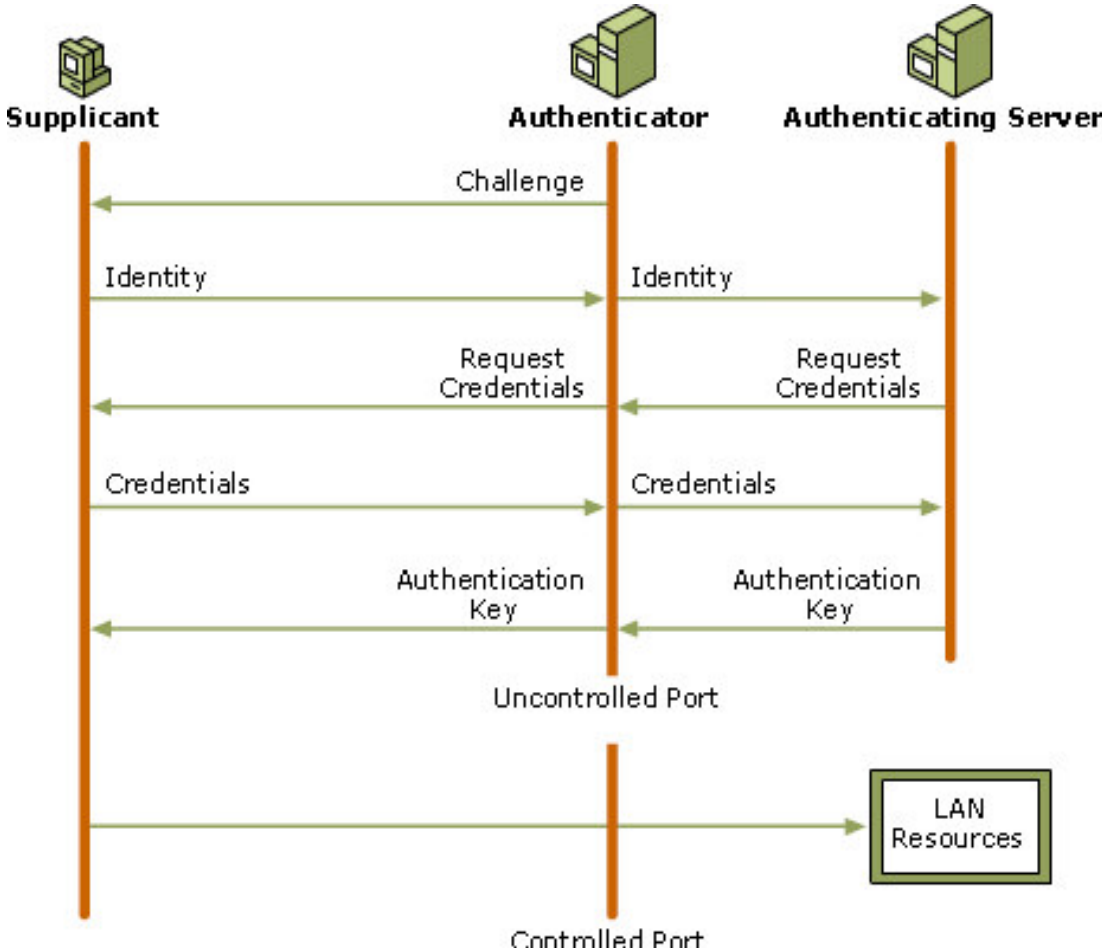
# Evolution of methods of Encryption



# 6.3.1 WPA (Wi-Fi Protected Access)

- WPA is a stronger security method that was created in response to the flaws discovered in WEP.
- WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption
- It was intended as an intermediate measure until further 802.11i security measures were developed.
- When implemented with authentication methods such as RADIUS, WPA is considered secure enough for all but the most sensitive enterprise applications.
- For most home and small business use, an effective level of security can be obtained by using WPA with a pre-shared key (PSK) that is shared by all users.

# WPA (Wi-Fi Protected Access)



# 6.3.2 WPA2 (Wi-Fi Protected Access 2nd generation)

- WPA2 is the second generation of WPA.
- The primary difference between WPA and WPA2 is the technology used for data encryption.
- WPA2 uses Advanced Encryption Standard (AES), a stronger encryption technology suitable for industries that require highly secure networks.

# 6.4 Firewall as additional Safeguard

- One of the most basic aspects of maintaining the security of your network involves using a firewall to filter out unwanted traffic.
- To protect a private LAN from unwanted traffic originating outside the LAN, firewall software often runs on a gateway that connects the LAN to the Internet.
- The firewall is configured to filter out traffic based on various characteristics of the incoming packets, such as IP address, MAC address (MAC Address Authentication), type of protocol, etc.
- Even if your private LAN does not connect to a public network, once you allow access to the LAN through a wireless AP, you open the network to possible external attack. As an added safeguard, some manufacturers include firewall software on the access point to filter out traffic accessing the network through the AP.
- Most APs support the encryption technology (WEP, WAP, WAP2) and allows system managers to filter traffic by MAC address, SSID Disable broadcast, IP, as well as TCP/UDP filtering options.

# 6.5 How a station joins an existing cell (BSS) (1)

- When a station wants to access an existing BSS (either after power-up, sleep mode, or just entering the BSS area), the station needs to get synchronization information from the Access Point (or from the other stations when in ad-hoc mode).
- The station can get this information by one of two means:
  1. **Passive scanning:** In this case the station just waits to receive a Beacon Frame from the AP. The beacon frame is a periodic frame sent by the AP with synchronization information such as:
     - SSID which is a readable string like “KDGACCESS”
     - AP capabilities such as supported data rates
     - Beacon Period
     - Traffic Indication Map(TIM)
     - MAC address of AP and Time stamp
  2. **Active Scanning**: In this case the station tries to find an Access Point by transmitting Probe Request Frames and waiting for Probe Response from the AP.
- The two methods are valid, and either one can be chosen according to the power consumption/performance tradeoff.

# How a station joins an existing cell (BSS) (2)

**The Authentication Process**

- Once the station has found an Access Point and decided to join its BSS it will go through the ***Authentication Process***
  - ✓ This is the interchange of information between the AP and the station, where each side proves it knows a given password.

**The Association Process**

- When the station is authenticated it will start the ***Association Process***
  - ✓ This is the exchange of information about the stations and BSS capabilities and which allows the DSS (the set of APs) to know about the current position of the station.

- A station is capable of transmitting and receiving data frames only after the association process is completed!

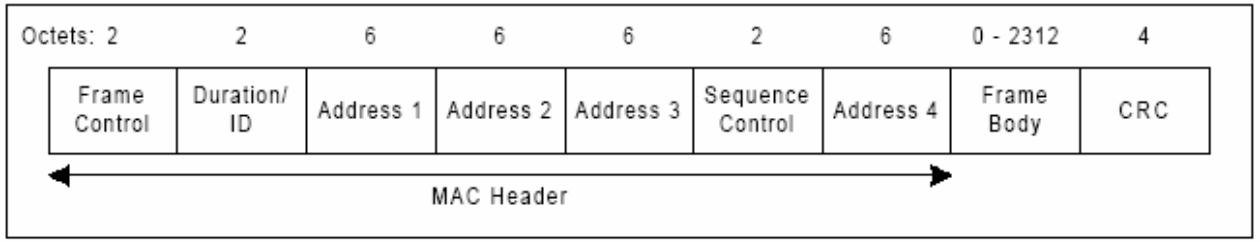
# 7. IEEE 802.11 Frame Types (overview)

- There are three main types of frames:
  - **Data Frames:** which are used for data transmission
  - **Control Frames:** which are used to control access to the medium (eg RTS, CTS, and ACK), and
  - **Management Frames:** which are frames that are transmitted the same way as data frames to exchange management information, but are not forwarded to upper layers.
- Each of **these types is further subdivided** into different Subtypes, according to their specific function.

- All 802.11 frames **are composed of the following** components:

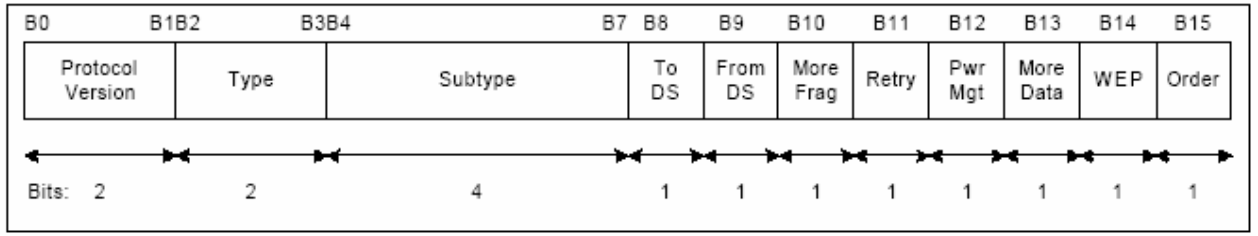
# • MAC Data Frame with the Frame Control Field

*The following figure shows the general MAC Data Frame*



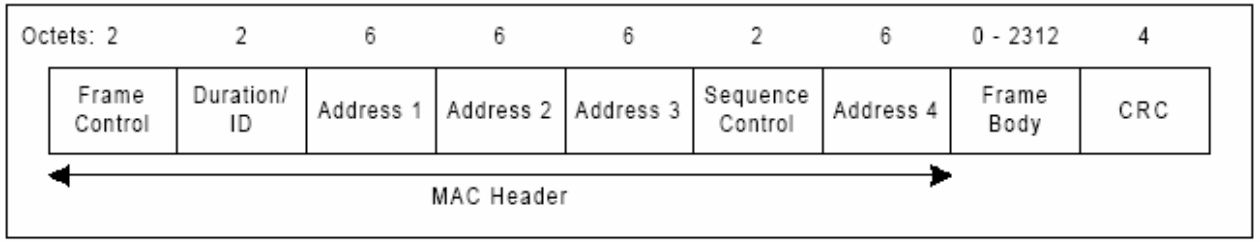

***Frame Control Field***

*The Frame Control Field contains the following Information:*



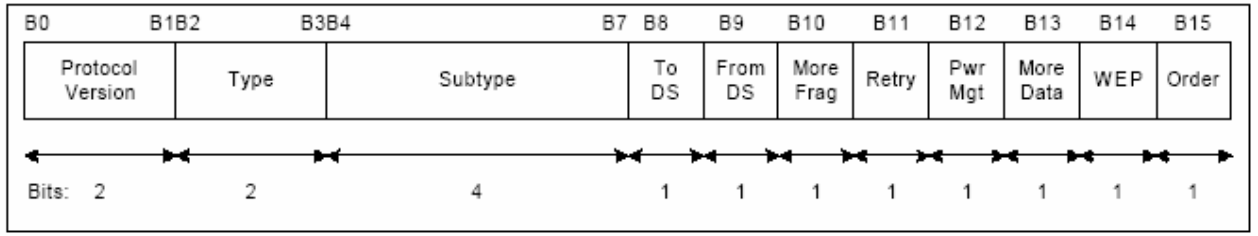
# • MAC Data Frame with the Frame Control Field

*The following figure shows the general MAC Data Frame*



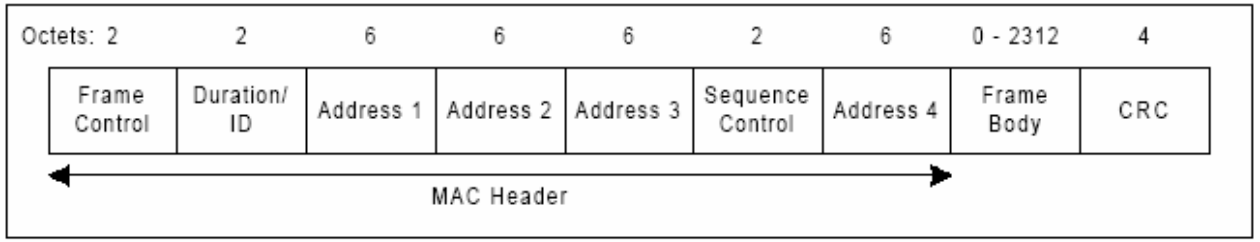

***Frame Control Field***

*The Frame Control Field contains the following Information:*



# • Address Fields in MAC Data Frame

*The following figure shows the general MAC Data Frame*




***Address Fields***

*A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:*

| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | N/A |
| 0 | 1 | DA | BSSID | SA | N/A |
| 1 | 0 | BSSID | SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |