

The IEEE 802.11 Protocol

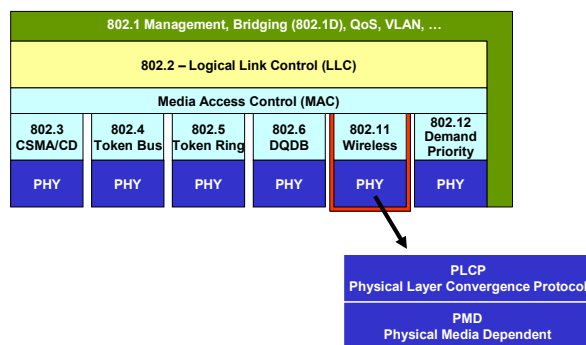
Layers and Frames

(C) Herbert Haas 2006/4/1

Protocol Layers



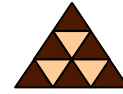
- **MAC layer**
 - ♦ Medium access control
 - ♦ Fragmentation
- **PHY layer = PLCP + PMD**
 - ♦ Established signal for controlling
 - ♦ Clear Channel Assessment (CCA)
 - ♦ Service access point
- **Physical Layer Convergence Protocol (PLCP)**
 - ♦ Synchronization and SFD
 - ♦ Header
- **Physical Medium Dependent (PMD)**
 - ♦ Modulation and coding



(C) Herbert Haas 2006/4/1

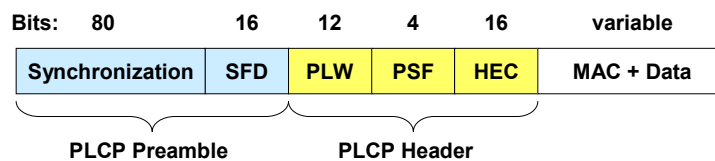
2

Clear Channel Assessment



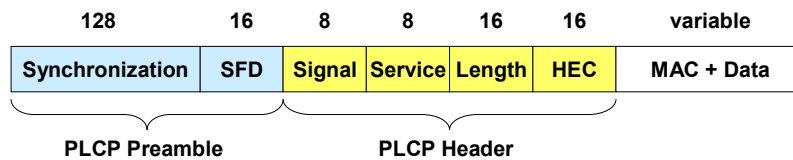
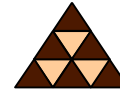
- CCA is an algorithm to determine if the channel is clear
- But what is "clear" ?
 - ♦ Either measuring only WLAN carrier signal strengths
 - ♦ Or measuring the total power of both noise and carriers
- Minimum RX signal power levels should be configured at receivers (APs & clients)
 - ♦ CSMA would not allow to send any frames if the environmental noise level is too high
- Part of PHY, used for MAC

FHSS Frame Format



- PLCP header runs always with 1 Mbit/s
- User data up to 2 Mbit/s
- Synchronization with 80 bit string "01010101..."
- All MAC data is scrambled by a $s_{(z)}=z^7+z^4+1$ polynomial to block any DC component
- Start Frame Delimiter (SFD)
 - ♦ Start of the PLCP header
 - ♦ 0000110010111101 bit string
- PLCP Length Word (PLW)
 - ♦ Length of user data inclusive 32 bit CRC of the user data (value between 0 and 4095)
 - ♦ Protects user data
- PLCP Signaling Field (PSF)
 - ♦ Describe the data rate of the user data
- Header Error Check (HEC)
 - ♦ 16 bit CRC
 - ♦ Protect Header

DSSS Frame Format



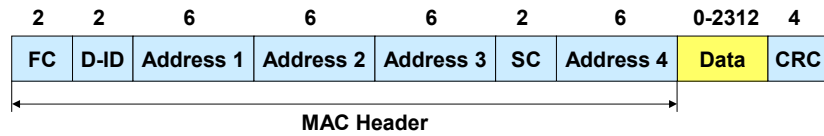
- PLCP header runs always with 1 Mbit/s (802.11 standard)
- User data up to 11 Mbit/s (802.11b standard)
- Synchronization (128 bit)
 - Also used for controlling the signal amplification
 - And compensation for frequency drifting
- Start Frame Delimiter (SFD)
 - 1111001110100000
- Signal (Rate)
 - 0x0A → 1 Mbit/s (DBPSK)
 - 0x14 → 2 Mbit/s (DQPSK)
 - Other values reserved for future use
 - 11 Mbit/s today with CCK
- Service
 - 0x00 → 802.11 frame
 - Other values reserved for future use
- Length
 - 16 bit instead of 12 bit in FHSS
- Header Error Check (HEC)
 - 16 bit CRC (ITU-T-CRC-16 Standardpolynom)

MAC Principles



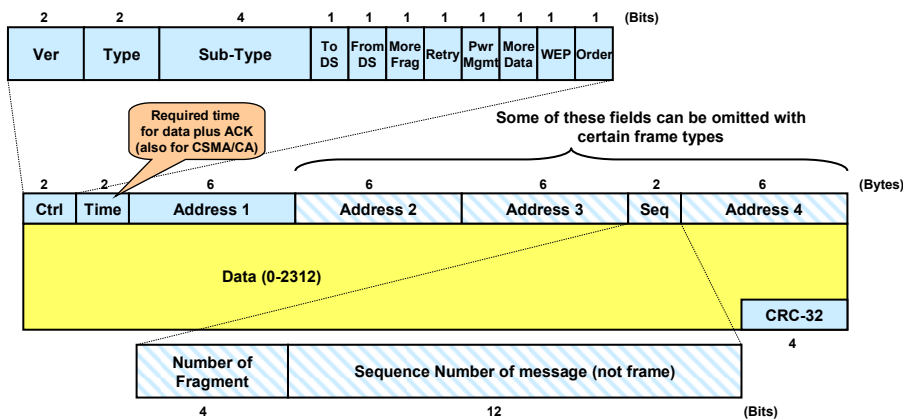
- **Responsible for several tasks**
 - ♦ Medium access
 - ♦ Roaming
 - ♦ Authentication
 - ♦ Data services
 - ♦ Energy saving
- **Asynchronous data service**
 - ♦ Ad-hoc and infrastructure networks
- **Realtime service**
 - ♦ Only infrastructure networks

MAC Header – Overview



- **Frame Control (FC) includes**
 - ♦ Protocol version, frame type
 - ♦ Encryption information
 - ♦ 2 Distribution System Bits (DS)
- **Duration ID (D-ID) for virtual reservations**
 - ♦ Includes the RTS/CTS values
- **Addresses are interpreted according DS bits**
- **Sequence Control (SC) to avoid duplicates**

MAC Header – More Specific



- **Header length: 10-30 Bytes**
- **Total maximum length: 2346 Bytes (without CRC)**
- **Time field also used for power saving**

Header Details – Addresses



Ctrl		Address 1	Address 2	Address 3	Address 4	
To DS	From DS					
0	0	Receiver	Sender	Cell	--	Used for all mgmt and ctrl frames. Used for data frames in Ad-hoc or broadcast situations.
0	1	Receiver	Cell	Sender	--	Communication inside BSS: Frame from AP to Receiver. Sender is originator. ACK must be sent to AP.
1	0	Cell	Sender	Receiver	--	Communication inside BSS: Frame from Sender to AP. Should be relayed to receiver.
1	1	Cell	Cell	Receiver	Sender	Communication between APs. Address1 is receiving AP, address2 is sending AP.

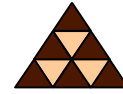
- **Infrastructure network:
Cell address = AP's MAC address**

Note

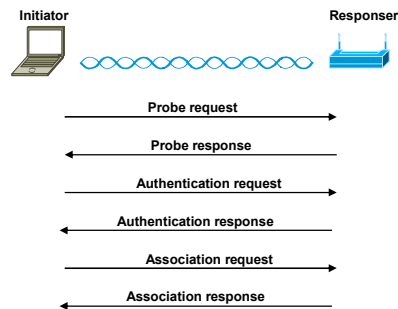


- **If an AP is used, ANY traffic runs over the AP**
 - ◆ Because stations do not know whether receiver is associated to this AP or another AP
- **Cell address = AP's MAC address**
 - ◆ Always specified in header
 - ◆ Not *needed* in Ad-hoc network

Service Set Management Frames



- **Beacon frame**
 - Sent periodically by AP to announce its presence and relay information, such as timestamp, SSID, and other parameters
 - Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with
- **Probe request frame**
 - Once a client becomes active, it searches for APs in range using probe request frames
 - Sent on every channel in an attempt to find all APs in range that match the SSID and client-requested data rates
- **Probe response frame**
 - Typically sent by APs
 - Contains synchronization and AP load information (also other capabilities)
 - Can be sent by any station (ad hoc)

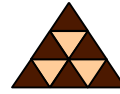


Authentication and Association



- **Authentication frame**
 - AP either accepts or rejects the identity of a radio NIC
- **Deauthentication frame**
 - Sent by any station that wishes to terminate the secure communication
- **Association request frame**
 - Used by client to specify: cell, supported data rates, and whether CFP is desired (then client is entered in a polling list)
- **Association response frame**
 - Sent by AP, contains an acceptance or rejection notice to the radio NIC requesting association
- **Reassociation request frame**
 - To support reassociation to a new AP
 - The new AP then coordinates the forwarding of data frames that may still be in the buffer of the previous AP waiting for transmission to the radio NIC
- **Reassociation response frame**
 - Sent by AP, contains an acceptance or rejection notice to the radio NIC requesting reassociation
 - Includes information regarding the association, such as association ID and supported data rates
- **Disassociation frame**
 - Sent by any station to terminate the association
 - E. g. a radio NIC that is shut down gracefully can send a disassociation frame to alert the AP that the NIC is powering off

Beacon Details



- Clients verify their current cell by examine the beacon
- Beacon is typically sent 10 times per second
- Information carried by beacon:
 - ♦ Timestamp (8 Bytes)
 - ♦ Beacon Interval (2 Bytes, time between two beacons)
 - ♦ Cell address (6 Bytes)
 - ♦ All supported data rates (3-8 Bytes)
 - ♦ Optional: FH parameter (7 Bytes, hopping sequenz, dwell time)
 - ♦ Optional: DS parameter (3 Bytes, channel number)
 - ♦ ATIM (4 Bytes, power saving in ad-hoc nets) or TIM (infrastructure nets)

SSID



- 32 bytes, case sensitive
 - ♦ Spaces can be used, but be careful with *trailing spaces*
- Multiple SSIDs can be active at the same time; assign the following to each SSID:
 - ♦ VLAN number
 - ♦ Client authentication method
 - ♦ Maximum number of client associations using the SSID
 - ♦ Proxy mobile IP
 - ♦ RADIUS accounting for traffic using the SSID
 - ♦ Guest mode
 - ♦ Repeater mode, including authentication username and password
- Only "Enterprise" APs support multiple SSIDs
 - ♦ Cisco: 16
 - ♦ One broadcast-SSID, others kept secret
 - ♦ Repeater-mode SSID

```
AP# configure terminal
AP(config)# configure interface dot11radio 0
AP(config-if)# ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# end
```