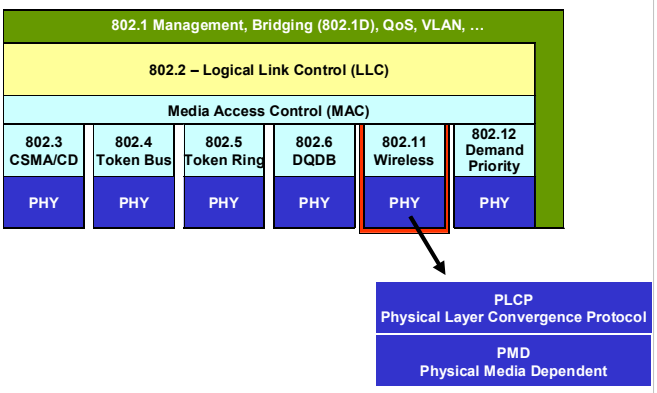
WLAN

Protocol

In this chapter we discuss basic communication issues, such as synchronization, coding, scrambling, modulation, and so on.

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 2010/02/15 2

The 802.11 standard only describes the physical and the MAC layer. The physical layer is split into the PLCP and the PMD protocol. The Medium Access Control takes-over the layer 2 functions.

Every 802.11 layer takes-over different tasks. The MAC layer is necessary for the medium access and fragmentations. The PLCP part of the physical layer is necessary for the controlling of the CCA signal. The PMD part enfolded the data modulation and the coding.

Clear Channel Assessment

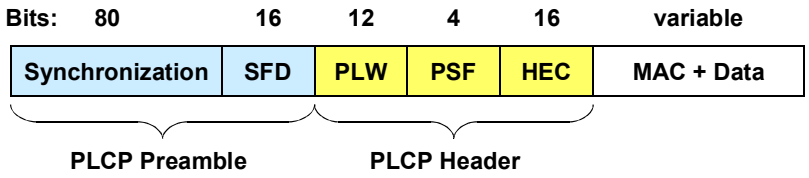
- CCA is an algorithm to determine if the channel is clear
- But what is *"clear"* ?
  - Either measuring only WLAN carrier signal strengths
  - Or measuring the total power of both noise and carriers
- Minimum RX signal power levels should be configured at receivers (APs & clients)
  - CSMA would not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

The Clear Channel Assessment (CCA) algorithm is a fundamental method used in all wireless technologies to determine whether a channel is currently occupied or not.

Basically a minimum power level threshold must be specified. If the currently measured RX power level for a given channel is below that threshold the channel is considered non-occupied and a data frame can be sent.

Therefore the CCA threshold is the minimum allowable power level for legal WLAN clients or equivalently the maximum allowable noise power level.

FHSS Frame Format

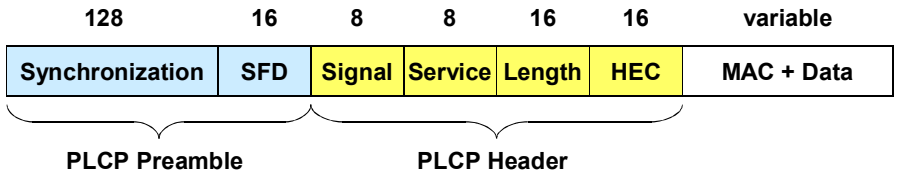


- PLCP header runs always with 1 Mbit/s
- User data up to 2 Mbit/s
- Synchronization with 80 bit string "01010101…"
- All MAC data is scrambled by a $s_{\ddagger}=z^7+z^4+1$ polynomial to block any DC component
- Start Frame Delimiter (SFD)
  - Start of the PLCP header
  - 0000110010111101 bit string
- 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

The FHSS frame format is only presented for historical interests…if there are any.

Note that some vendors still produce FHSS-based 802.11 devices for special purposes (high interference environments).

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)

802.11g and 802.11a use similar frame format

(C) Herbert Haas 2010/02/15 5

The DSSS frame format shown here is used by 802.11b but the frame format is also valid with 802.11g and 802.11a except that the values for the fields are different.

The most important thing to understand here is that only the PLCP headers are sent with the **lowest supported data rate**. The following MAC header and the payload can be sent with a higher data rate.

The symbol rate is constant from the very beginning of the frame to the very end. What changes is only a 'jump' in the QAM family (i. e. in the code complexity) which causes a change in the information rate.

Even a distant receiver should at least be able to decode the PLCP (because the PLCP has a low data rate) in order to determine the QAM code required to decode the remainder of the frame (the data part).

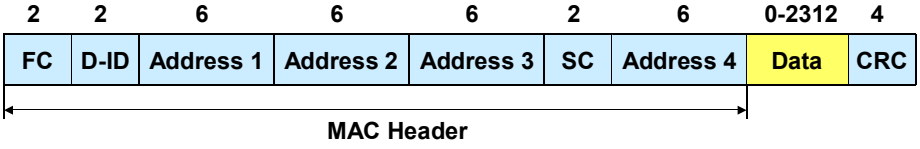
MAC Principles

- 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

The MAC layer is responsible for many tasks. The important one is the controlling of the medium access. But also the roaming, authentication and energy saving mechanisms are included here. The basic services are the Asynchronous data service, for Ad-hoc and infrastructure networks, and the Time-bounded service, for infrastructure networks only. With the Asynchronous data service broadcast and multicast frames are possible.

General rule: Collisions cannot be detected, so each packet is acknowledged (except MAC-level retransmissions).

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

The picture above shows the standard MAC header with it fields.

Frame Control (FC). These 2 bytes contains information about the protocol version, the frame type, encryption information and the important DS bits.

Duration ID (D-ID). These field include the RTS/CTS values. These field includes the NAV values.

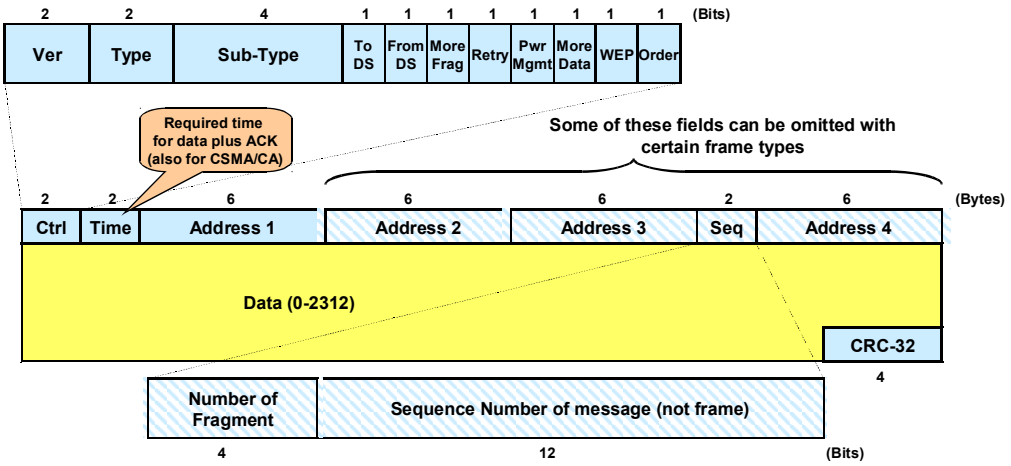
Address. These 4 address fields constrains IEEE 802.11 MAC addresses. The interpretation of this addresses depends on the DS bits.

Sequence Control (SC). The Sequence control is a value to avoid frame duplications.

Data. A MAC frame can include any kind of data (max 2.312 bytes).

Checksum (CRC). A 32 bit sum to protect the frame.

MAC Header – More Specific



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

(C) Herbert Haas 2010/02/15 8

2312 bytes max frame length without encryption etc.

Most adapters allow at least 2346 byte frames (total length).

Header Details – Addresses

Ctrl To DS	Ctrl From DS	Address 1	Address 2	Address 3	Address 4	
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**

(C) Herbert Haas 2010/02/15 9

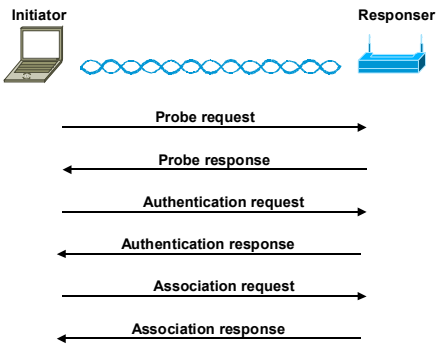
Four addresses are used in bridging mode but bridging is a very proprietary feature with lots of additional undocumented tricks.

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 frame: 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC. The NIC begins the process by sending an authentication frame containing its identity to the access point. With open system authentication (the default), the radio NIC sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection). With the optional shared key authentication, the radio NIC sends an initial authentication frame, and the access point responds with an authentication frame containing challenge text. The radio NIC must send an encrypted version of the challenge text (using its WEP key) in an authentication frame back to the access point. The access point ensures that the radio NIC has the correct WEP key (which is the basis for authentication) by seeing whether the challenge text recovered after decryption is the same that was sent previously. Based on the results of this comparison, the access point replies to the radio NIC with an authentication frame signifying the result of authentication.

Deauthentication frame: A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

Authentication and Association

- Authentication frame
  - AP either accepts or rejects the identity of a radio NIC
- Deauthentication frame
  - Send 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
  - Send 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
  - Send 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

Association request frame: 802.11 association enables the access point to allocate resources for and synchronize with a radio NIC. A NIC begins the association process by sending an association request to an access point. This frame carries information about the NIC (e.g., supported data rates) and the SSID of the network it wishes to associate with. After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.
Association response frame: An access point sends an association response frame containing an acceptance or rejection notice to the radio NIC requesting association. If the access point accepts the radio NIC, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the radio NIC can utilize the access point to communicate with other NICs on the network and systems on the distribution (i.e., Ethernet) side of the access point.
If a radio NIC roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a reassociation frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC.
An access point sends a reassociation response frame containing an acceptance or rejection notice to the radio NIC requesting reassociation. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.
Disassociation frame: A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the access point that the NIC is powering off. The access point can then relinquish memory allocations and remove the radio NIC from the association table.

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)
  - Optional but very common: vendor-specific INFORMATION ELEMENTS (IEs)
- Problem: Beacons reveals features and existence of cell

Security relevance: The beacon is always sent with the lowest supported data rate (1 Mbit/s for 802.11b/g or 6 Mbit/s with 802.11a) and therefore even in large distances the beacon reveals the existence of a cell.

However there is no real workaround against it as you cannot disable beacons.

One could specify an increased 'required' data rate and disable lower 'required' rates. Only 'required' rates are used for management frames. This reduces the detection range.

Additionally you can increase the beacon interval from 100 msec to e. g. 1 second. However this may affect the roaming service.

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
```

(C) Herbert Haas 2010/02/15 14

If you want the access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. The access point's default SSID, tsunami, is set to guest mode. However, to keep your network secure, you should disable the guest mode SSID on most access points.

If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

SSID broadcasting. In some cases, such as public Internet access applications, you can broadcast the SSID to enable user radio cards to automatically find available access points. For private applications, it's generally best to not broadcast the SSID for security reasons -- it invites intruders. Multiple SSIDs means you can mix and match the broadcasting of SSIDs.

The IEEE 802.11 Protocol

CSMA/CA

Access Methods - CSMA/CA

"Distributed Foundation Wireless Medium Access Control" (DFWMAC)

DCF (CSMA/CA)

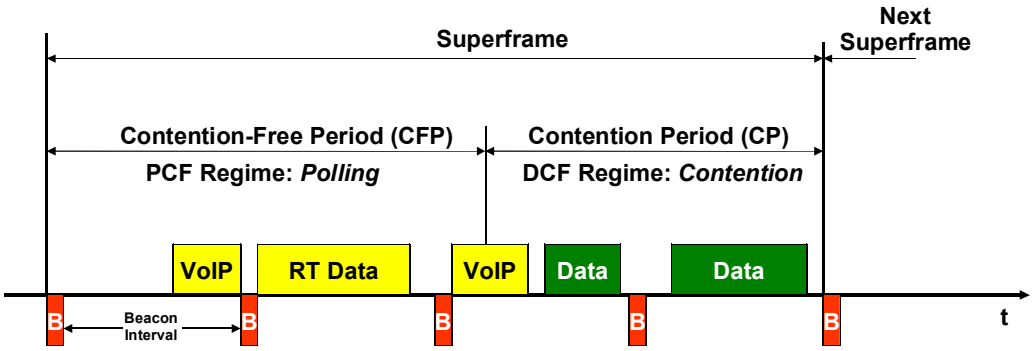
PCF

- **Distributed Coordination Function (DCF)**
  - **Asynchronous data service**
  - **Optionally with RTS/CTS**
- **Point Coordination Function (PCF)**
  - **Intended for realtime service (e. g. VoIP)**
  - **Polling method**
  - **Optional**

In the 802.11 standard 3 access methods are defined. One method that based on a CSMA/CA version (must be supported), one optional method which avoid the problem of invisible devices and a optional, collision free method. The first two methods are called Distributed Coordination Function (DCF) and third method is a so called Point Coordination Function (PCF). DCF methods can only support asynchronous services, PCF supports asynchronous and time-bounded services. But a access point is necessary for PCF methods.

Note: The PCF is optional and only very few APs or Wi-Fi adapters actually implement it.

Superframe



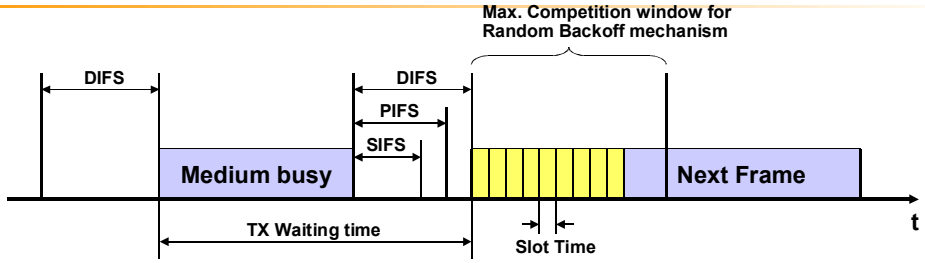
- Beacon is sent by "Point Coordinator" (PC=AP)
- Minimum CP period guaranteed
  - To avoid starvation of non-realtime data
  - At least one frame can be sent
- Note: Poll-Frames and ACKs omitted in this picture!

(C) Herbert Haas 2010/02/15 17

Typically the Point Coordinator (PC) is integrated in the AP but this is not required. In order to give an idea of the basic principle o the superframe, the CFP and the CP, many details have been omitted. The details of both periods are explained in the following slides.

Note that the Beacon frames are primarily used to detect stations within this cell.

CSMA Access Method



Basic Ideas

- **No standing waves in free space => no Ethernet-like collision detection possible**
- **Collision is detected by missing ACKs!**
- **Truncated Random Exponential Backoff like in Ethernet and 802.3**
- **Simple fragmentation mechanism**
  - **Ethernet compatibility**
  - **Performance (interferences)**
- **CCA to determine medium state**
- **CSMA: "Listen before talk"**
- **A safety Inter-frame Space (DIFS | PIFS | SIFS, plus Backoff) must be awaited before TX**

Details

- CW is multiple of Ethernet slot time
  - If medium is busy: Backoff
  - Slot time: 47 µs (9 µs)
- DCF Inter-Frame Space (DIFS)
  - Longest waiting time, 128 µs (34 µs)
  - Used for asynchronous data services
- PCF Inter-Frame Space (PIFS)
  - Used for APs to stop user communication, 78 µs (25 µs)
- Short Inter-Frame Space (SIFS)
  - Shortest waiting time, highest priority, 28 µs (16 µs)
  - Used for ACKs

(C) Herbert Haas 2010/02/15 18

The picture above shows some important parameters which are necessary before a device can access on a medium. DIFS, PIFS and SIFS control the priority before a device can have access. A medium can be full or busy, the current status will be detect with the help of the CCA signal.

Real Collision Detection would require a full-duplex connection to detect collisions also at the "end" of a wireless connection. This would be too expensive for wireless LAN hardware.

Note the whole frame with all control information, FCS, etc is up to 2346 bytes long.

The **DIFS** parameter describes the longest waiting time and consequently the less priority. It is used for the data transfer.

The **PIFS** is used for time-bounded services. If a access point need to scan some devices, the access point only need to wait PIFS.

The shortest waiting time has the **SIFS**, data which use the SIFS have the highest priority. All controlling frames (e.g. acknowledgements) using these time. So they cannot be blocked by data transfer.

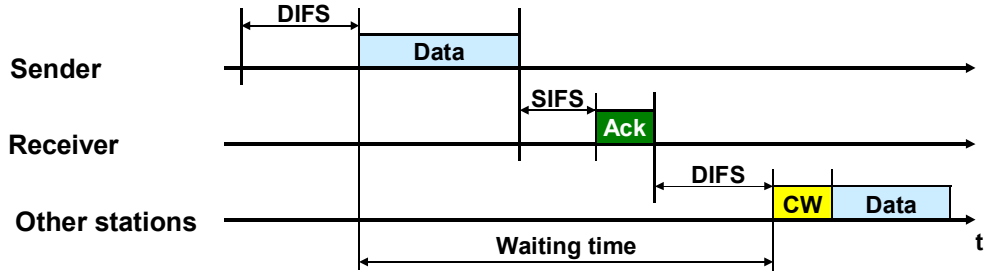
Note: The numbers in brackets relate to the 802.11a standard values.

Backoff Policies

- Random backoff reduces collisions
- Competition window (CW)
  - Start value of 7 slot times
  - After every collision → CW doubled
  - To a max of 255
- Post-backoff
  - After successful transmission
  - To avoid "channel-capture"
- Exception: Long silent durations
  - Station may send immediately after DIFS

The random slot time is a value of slots. Every competition window starts with a slot number of 7. Every collision the competition value is doubled till a max of 255. The DFWMAC with CSMA/CA method works fine with less devices, but there will be to much collisions with to many devices.

CSMA/CA in Action



- Point-to-point communication
- Acknowledgment is send after SIFS
  - Before all other communications
  - Guaranteed collision free
- Re-transmitted frames have no higher priority over other frames

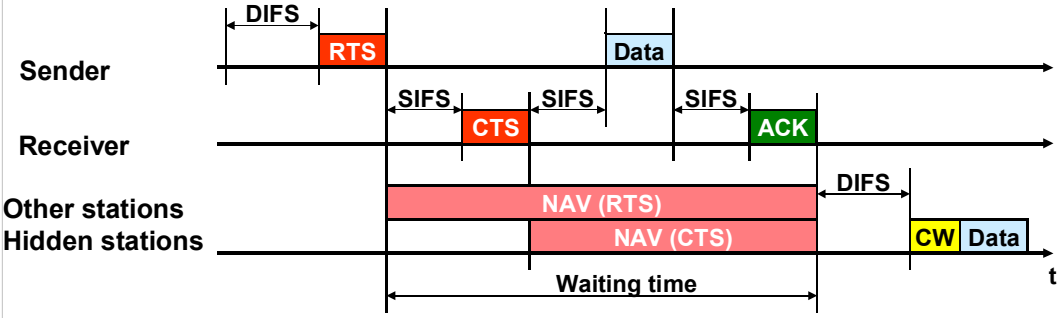
The picture above shows the DFWMAC with CSMA/CA method with a point-to-point communication. After the user data a acknowledgement is send. This acknowledgement is send after SIFS, so it will be transfer collision free and before all other communication. If a data packet need to be re-transmitted, the device need to wait DIFS and also using the normal backoff mechanism. This re-transmitted frames have no advantages compared with others.

CSMA/CA with RTS/CTS

Access Method

- Avoid the problem of invisible devices or "Hidden Stations"
  - Station receives data from two other devices
  - The two other devices didn't see each other
  - Each device thinks medium is free → Collision
- 2 special packets → RTS and CTS
  - Every station must listen to this packets

Four-way handshake:
1. RTS
2. CTS
3. Data
4. ACK



(C) Herbert Haas 2010/02/15 21

To avoid the problem of invisible devices (devices who didn't see each other) the DFWMAC with RTS/CTS method was created. Two special packets, the RTS and CTS packet, help to fix this problem. Every 802.11 device must listen to these packets.

If a station (sender) want to send out some packets it sends out a RTS packet first. This RTS packet include information about the target device (receiver) and about the approximate transfer time. All other station will receive this RTS packet. The stations safes the approximate transfer time into a so called Net Allocation Vector (NAV). For this time now, the other stations will not send out any packets. Also the receiver station will receive this packet and send out a CTS packet after SIFS. The CTS packet is a signal for the sending station to start their transmission. It also include more exact information about the transfer time. All other station receive this packet too and adjust their NAV. After the NAV the medium is free for all, and a new completion can start.

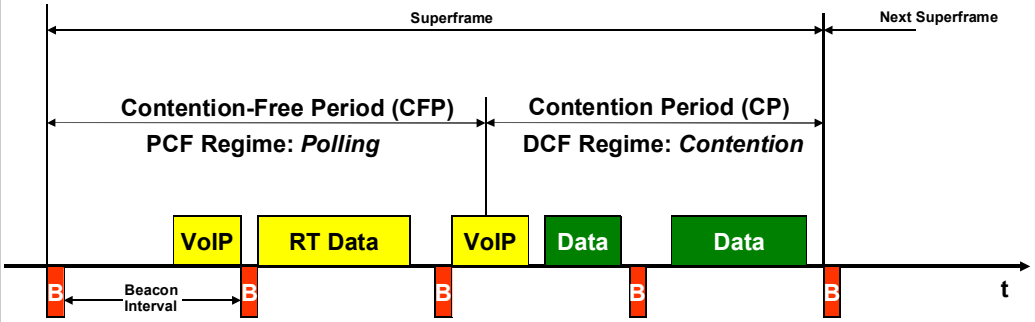
RTS/CTS => "Virtual Reservation"

- Collision can only occur at the begin or after a transmission
- Much more overhead
  - RTS/CTS packets increase the total access-delay
- Usage guidelines
  - Only when longer frames are sent on average (> 500 Bytes)
  - When hidden stations are expected

This process is called „virtual reservation“. Collisions can only occur at the begin or at the end of a transmission, within the competition window. The big disadvantage of the DFWMAC with RTS/CTS method is the traffic. The RTS/CTS packets increase the traffic and so the access-delay. This method is only using with longer frames.

PCF – Polling Principle

- Guaranteed transmission parameters
  - Minimum data rate
  - Maximum access-delay
- AP necessary (!)
  - For medium access control
  - Polling and time-keeping
  - Acts as "point coordinator“
- Point Coordinator (PC) splits access time into a Superframe
  - Contention-free period (PCF method)
  - Contention period (DCF method)
- Target Beacon Transmission Time (TBTT) is announced in each beacon



(C) Herbert Haas 2010/02/15 23

Both DCF methods didn‘t support transfer guaranties. With DFWMAC-PCF some parameters can be defined, such as a minimal bandwidth or a maximal access delay. For this PCF method a access point is necessary, so it can be only used within infrastructure networks. The access point in necessary to control the medium access and for interrogation between the different stations (polling).

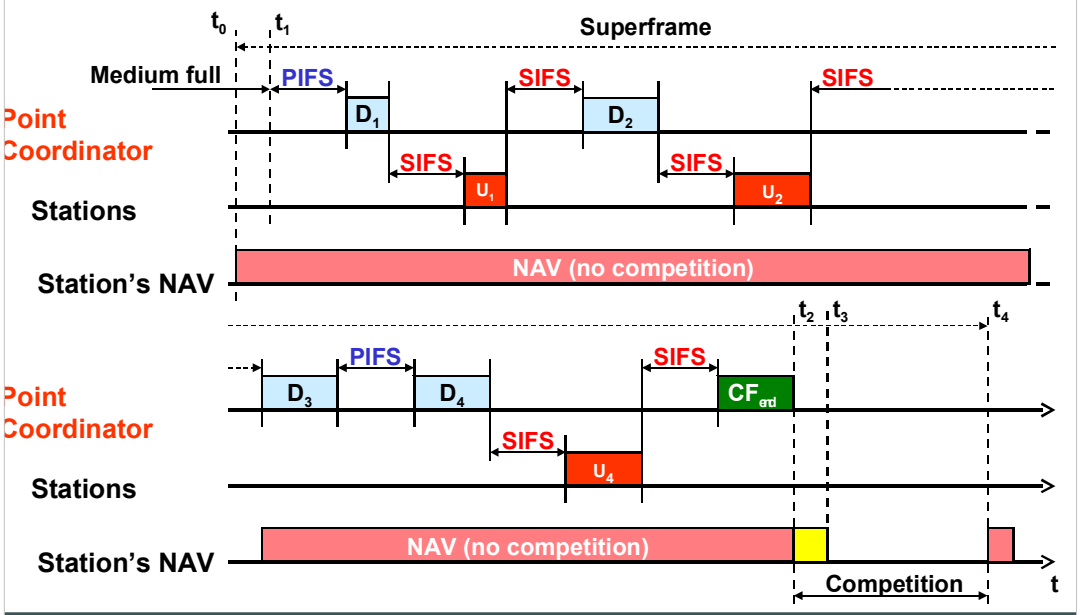
The access time of the medium is split into a so called „Superframe“ by the point coordinator. The Superframe consists of a competition period (CP) and a competition free period (CFP). The CFP is only optional and does not need to be supported by the AP. If it is supported, then the AP also controls the changes from one phase to the other. The Beacon is sent periodically, primarily to detect other stations in the cell. Additionally, the Superframe always begins with a beacon. Note that the Superframe is sometimes also called CFP-Interval.

CFP Policy

- Beacon starts CFP by announcing maximum duration of CFP
  - Can be multiple of Beacon intervals
  - Intermediate Beacons indicate the remaining CFP duration
- Between two successive CFPs there must be space to send at least on frame in the CP mode!
- The AP may finish the CFP earlier!
  - Sending the CF-End Control Frame
- CFP is *optional*
  - CSMA/CA-only clients must not interfere
  - CFP also relies on CSMA/CA

Not all clients need to support CFP. NAV is set by beacon frame for all stations.

PCF Medium Access



The picture above shows the schematic view of the DFWMAC-PCF method. Remember the data transfer take place by the point coordinator. All data will be send or received from or by the point coordinator. D_n and U_n are data/user-data from or to the point coordinator.

PCF Algorithm

- At t_0 starts the competition free zone
- Medium gets free at t_1
- After PIFS the PC can access the medium
  - No other station can access because PIFS is smaller than DIFS
- Now PC polls first station (D1)
- Stations may answer with user data after SIFS
- Stations must Ack within PIFS
  - PIFS is shortest idle period within CFP
- All frames are sent through AP !!!
- AP maintains list of all stations that should be polled
  - Announced by association process
  - PC continuously polls listed stations
- PC can send data together with beacon (piggy-back)
- By sending a CF_{end} frame the PC starts the CP

After the medium gets free at t_1, the point coordinator waits PIFS before he can access to the medium. PIFS is smaller then DIFS, so no other station can get an access on the medium before the point coordinator. Now the point coordinator can start sending the data to the first station. The station can answer immediately after SIFS.

Now the point coordinator starts to send out the data to station 2. With the CF_{end} packet the point coordinator opens the competition period.

Within this modus the complete controlling takes place by the access point. With a consistent query to all station it is possible to get fix a bandwidth. But also this method has a disadvantage. If some station didn't have anything to send, much bandwidth will be unused.

802.11g/b Compatibility

- "b" expects CCK preamble and cannot detect OFDM signals
  - Therefore collisions with legacy "b"
- Compatibility mode
  - g-devices only use RTS/CTS
    - Always 1 Mbit/s and BPSK
    - Newer "g" sends a CCK-based CTS before each OFDM-based data frame
  - "g" suffers from reduced throughput
    - 8-14 Mbit/s instead of 22 Mbit/s
- "g" reaches longer distances (=>OFDM)
  - Cell design must consider b-only clients
  - Only when same power level used !

Realtime Problems with 802.11

- Available BW is shared among clients
- No traffic priorities
- Once a station gains access it may keep the medium for as long at it choses
  - Low bitrate stations (e. g. 1 Mbit/s) will significantly delay all other stations
- No service guarantees
- PCF does not support traffic classes
  - However, the PCF is typically not implemented in APs and client adapters

Originally (1999) WLAN QoS was only provided by the PCF algorithm which was actually never implemented in any products.

Specific PCF Problems

- Irregular Beacon delays
  - Stations may finish each transmission even if TBTT already expired
  - Up to 2304 bytes (2312 bytes if encrypted, new: even 2342 bytes allowed)
  - Station may even send all fragments of a L2-fragmented packet
- Hidden station and interferences
- No traffic classes means: All applications have equal TX opportunity

Since the beacon is sent using CSMA rules, significant delays are possible.

802.11a: 250 usec delay on average, but can reach 4.9 ms(!)

802.11e – EDCF and HCF

- New coordinate functions relying on Traffic Classes (TCs)
- Enhanced DCF (EDCF)
  - Better CHANCES for high-priority classes
  - But NO GUARANTEES ("best effort QoS")
  - Performed within CP
- Hybrid Coordination Function (HCF)
  - Is an enhanced PCF
  - Allows precise QoS configurations on the HC:
    - BW control
    - Guaranteed throughput
    - Fairness between stations
    - Classes of traffic
    - Jitter limits
  - Performed within CFP

The HCF is the most complex coordinate function for WLANs.

802.11e – HCF Details

- Stations announce their TC queue lengths
- The Hybrid Coordinator (HC=AP) does not need to follow round robin but any coordination scheme
- Stations are given a Transmit Opportunity (TXOP)
  - They may send multiple packets in a row, for a given time period
- During the CP, the HC can resume control of the access to the medium by sending CF-Poll packets to stations
- Also allows to send multiple data frames followed by single ACK

802.11e – Facts

- **Concept Summary**
  - **CP allows to prioritize certain TCs instead stations**
    - **More important traffic classes will be preferred— statistically**
  - **CFP allows bandwidth reservation by stations and non-round-robin polling**
    - **Not yet implemented (Fall 2004)**
- **Hybrid Controller (HC) required**
  - **Controls all other "enhanced stations"**
  - **Typically implemented within AP (not necessarily)**
  - **"QBSS" instead of BSS**
- **Main driver for QoS is "Voice over Wireless IP" (VoWIP)**

802.11e uses the Enhanced Distributed Coordination Function (EDCF) and the Hybrid Coordination Function (HCF). All stations which support the Enhanced Distributed Coordination Function are called “Enhanced Stations”. One of these Enhanced Stations will control all other stations and is called “Hybrid Controller”.

The EDCF is used while the CP and the HCF is used while CP and CFP (complete Superframe). In 802.11e there are different Traffic Categories (TCs). For every TC a Enhanced Stations need to set a own back-off timer and other parameters. The TC prevent collisions if the timer of two or more stations reached zero at the same time.

802.11e – Algorithm (1)

- All traffic is separated into TCs
  - Enhanced stations must maintain a separate back-off timer for each TC
- Up to 8 priority queues for each TC
  - "Virtual Stations" inside enhanced stations
- Each TC has different priority value
  - To avoid collisions if the counters of two TCs expire
- TCs compete within Arbitration Interframe Space (AIFS)
  - Different AIFS for each TC possible
  - At least one DIFS long
- Persistence factor (PF) solves collision
  - Used to calculate new back-off values
  - PF=1..16
- Legacy stations must have a CWmin=15 and PF=2

A so-called Persistence Factor (PF) is used if a collision of TCs from different stations occurs.

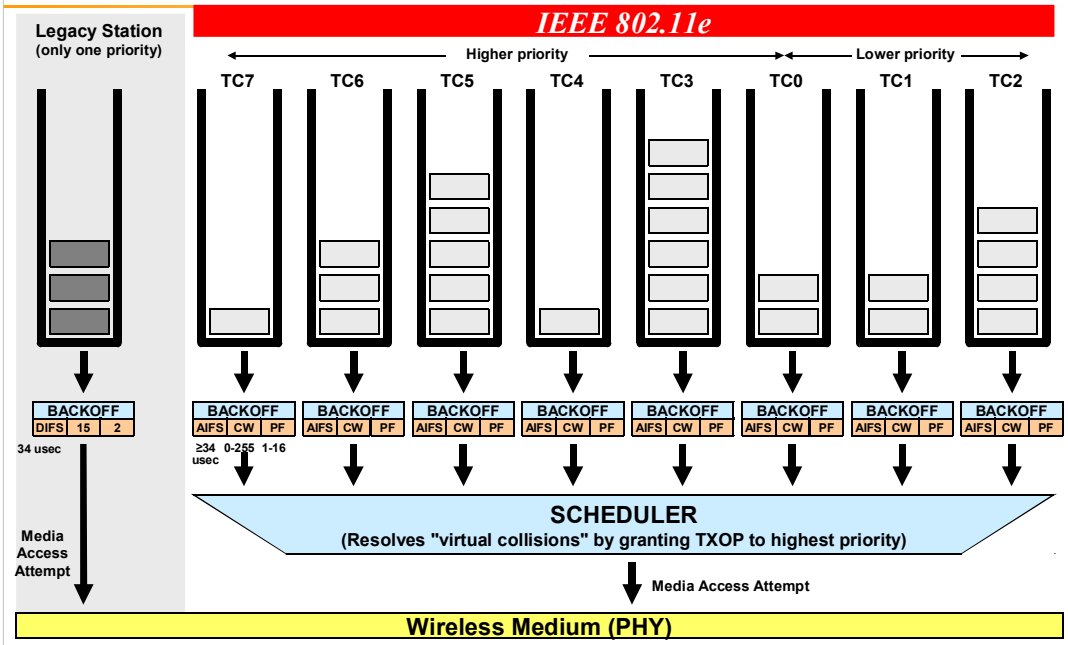
Enhanced Stations have a CWmin of 0..255.

802.11e – Algorithm (2)

- Transmission Opportunity (TXOP)
  - Time slot during a station may send
- EDCF-TXOP
  - Issued by EDCF algorithm
  - Limited by system-wide TXOP-limit announced in beacon frames
- Polled-TXOP
  - Issued by HCF
  - Limited by parameter announced in poll-frame
- HCF can redefine TXOP at each time
  - And finish the CP earlier
- HC also supports controlled contention
  - Polling frames announce sending desire of other stations
  - Legacy stations must wait until end of controlled contention period

The Polled-TXOP is limited by a parameter which is announced in poll-frames and which replaces the NAV timer.

802.11e – Queuing Concept



Legacy DCF uses an AIFS=34 usec, CWmin=15, PF=2

Enhanced stations perform EDCF with AIFS[TC]>= 34 usec, CWmin[TC]=0-255, PF[TC]=1-16

WiFi Multimedia – WMM

- WMM implements a subset of 802.11e to satisfy urgent QoS needs
  - Certification start: 09/2004
- Only supports prioritized media access:
  - 4 access categories per device: voice, video, best effort, and background
  - Does not support guaranteed throughput

Cisco 1100/1200 APs already provide a subset of 802.11e

Legacy QoS

- ***Most legacy (no 802.11e) APs only support downstream QoS***
  - On the AP, create QoS policies and apply them to VLANs
  - If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports
- ***Note: APs do not classify packets!***
  - Only already classified packets are prioritized (DSCP, client type, 802.1p)
  - EDCF-like queuing is performed on the Radio port; only FIFO on Ethernet egress port
  - Only 802.1Q tagging supported – no ISL !!!

802.1x and WAN Congestion

- Congestion on WAN links: prioritize 802.1x packets
- Classify and mark RADIUS packets using the Cisco Modular QoS Command Line (MQC)
  - Method to determine the appropriate queue size for the 802.1x/RADIUS packets
  - And to determine how to enable queuing on router interfaces

```
ip access-list extended LEAPACL                          !!! Create ACL for interesting traffic
 permit udp any host 172.24.100.156 eq 1645

class-map match-any LEAPCLASS                            !!! Classify
 match access-group name LEAPACL

policy-map MARKLEAP                                      !!! This is a policy group
  class LEAPCLASS
   set ip dscp 26                                        !!! Corresponds to AF31 (Class=3, 1=low drop)

interface FastEthernet0/0.100                            !!! Attach marker on interface
 encapsulation dot1Q 100
 service-policy input MARKLEAP                           !!! Mark inbound (input) packets only

policy-map LEAPQUEUE
  class LEAPCLASS
   bandwidth 8                                           !!! 8kb/s if needed (dynamical management)

interface Serial3/0:0                                    !!! Attach policy-map on WAN interface
 ip address 172.24.100.66 255.255.255.252
 load-interval 30
 service-policy output LEAPQUEUE
```


Remember that the DSCP has the following format: XYZPP0, where XYZ selects one of four assured forwarding classes (like “premium”, “gold”, “silver”, and “bronze”) and “PP” represents the drop precedence bits (RFC 2597, “low”, “medium”, and “high”).