Wireless Mesh and Vehicular Networks

802.11MAC Fundamentals

Renato Lo Cigno

ANS Group – locigno@disi.unitn.it

http://disi.unitn.it/locigno/teaching-duties/wmvn

Quest'opera è protetta dalla licenza:

Creative Commons
Attribuzione-Non commerciale-Non opere derivate
2.5 Italia License

Per i dettagli, consultare
http://creativecommons.org/licenses/by-nc-nd/2.5/it/

IEEE 802.11

- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients

- Defines the PHY and MAC layer (LLC layer defined in 802.2)

- Physical Media: radio or diffused infrared (not used)

- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, then '03, '05, ... '12)
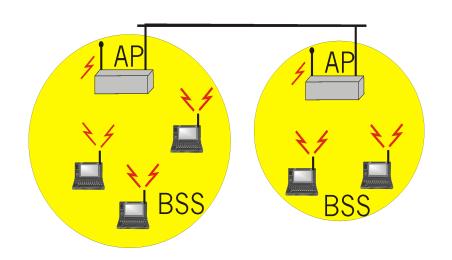
- BSS (Basic Service Set): set of nodes using the same coordination function to access the channel

- BSA (Basic Service Area): spatial area covered by a BSS (WLAN cell)

- BSS configuration mode
  - ad hoc mode
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the so-called Access Point (AP)

- BSS contains:

  - wireless hosts

  - access point (AP): base station

- BSS's interconnected by distribution system (DS)

Ad Hoc WLANs

- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS

- Applications:

  - Vehicular Networks

  - Meeting in conference room

  - Interconnection of "personal" devices

  - Battlefield

  - ….

- IETF MANET (Mobile Ad hoc Networks) working group; VANET; V2V; V2X; …
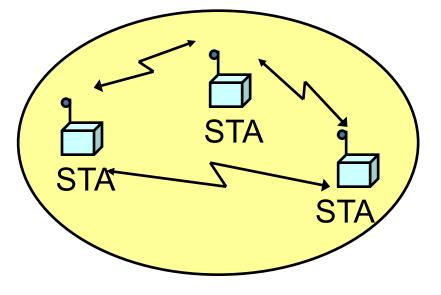
BSS

Extended Service Set (ESS)

- Several BSSs interconnected with each other at the MAC layer

- The backbone interconnecting the BSS APs (Distribution System) can be a:
  - LAN (802 family)
  - wired MAN
  - IEEE 802.11 WLAN, possibly meshed (a large part of our course)

- An ESS can give access to the fixed Internet network through a gateway node
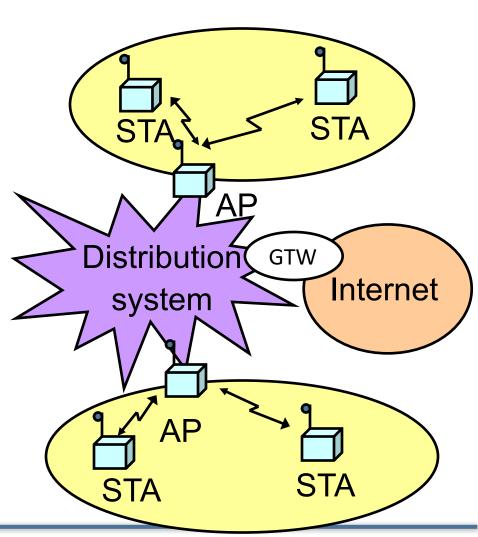
Ad hoc networking
Independent BSS (IBSS)

Network with infrastructure
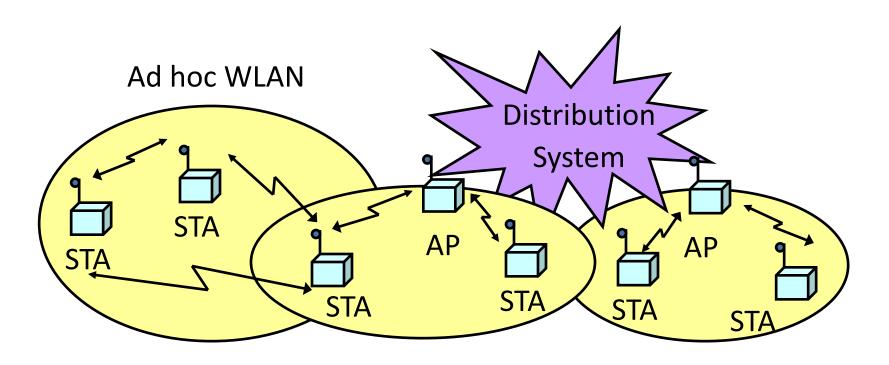
Ad hoc WLAN

Distribution System

WLANs with infrastructure

- Between the PHY/MAC and the 802.2 LLC (or IP) there are additional functions for registering one interface to the others

  – With infrastructured systems we say to "join a BSS/AP"

- Without proper association a network is not formed and STA do not communicate

  – Exception: 802.11p → Vehicular Networks

Scanning	→	Authentication	→	Association

- BSS with AP: Both authentication and association are necessary for joining a BSS

- Independent BSS: Neither authentication neither association procedures are mandatory or specified in the standard an IBSS → ad-hoc, proprietary, none

A station willing to join a BSS must get in contact with the AP. This can happen through:

1. Passive scanning

    - The station scans the channels for a Beacon frame that is periodically (100ms) sent by every AP

2. Active scanning (the station tries to find an AP)

    - The station sends a ProbeRequest frame on a given channel

    - All AP's within reach reply with a ProbeResponse frame

- Active Scanning may be more performing but waste resources

- Beacons are broadcast frames transmitted periodically (default 100ms). They contain:
  - Timestamp
  - TBTT (Target Beacon Transmission Time) – also called Beacon Interval
  - Capabilities
  - SSID (BSSID is AP MAC address + 26 optional octets)
  - PHY layer information
  - System information (Network, Organization, …)
  - Information on traffic management if present
  - …
- STA answer to beacons with a ProbeResponse containing the SSID

- **Directed probe**: The client sends a probe request with a specific destination SSID; only APs with a matching SSID will reply with a probe response
  - It is often considered "secure" if APs do not broadcast SSIDs and only respond to Directed Probes …
- **Broadcast probe**: The client sends a null SSID in the probe request; all APs receiving the probe-request will respond with a probe-response for each SSID they support
  - Useful for service discovery systems

Once an AP is found/selected, a station goes through authentication

- Open system authentication
    - Station sends authentication frame with its identity
    - AP sends frame as an ack / nack
- Shared key authentication (WEP)
    - Stations receive shared secret key through secure channel independent of 802.11
    - Stations authenticate because they use the secret key (weak)
- Per Session Authentication (WPA2)
    - Encryption is AES
    - The key can be shared (home networks) or user-based (enterprise)
    - Encryption is always per-station plus one for broadcast

Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming

- ▪ STA → AP: AssociateRequest frame

- ▪ AP → STA: AssociationResponse frame

- ▪ In case of Roaming: New AP informs old AP via DS

- Only after the association is completed, a station can transmit and receive data frames

Performs the following functions:

- Resource allocation

- Data segmentation and reassemby

- MAC Protocol Data Unit (MPDU) addressing

- MPDU (frame) format

- Error control

Three frame types are defined

1. **Control:** positive ACK, handshaking for accessing the channel (RTS, CTS)

2. **Data Transfer:** information to be transmitted over the channel

3. **Management:** connection establishment/release, synchronization, authentication.
   Exchanged as data frames but are not reported to the higher layer

- ➢ Asynchronous data transfer for best-effort traffic

    - ➢ DCF (Distributed Coordination Function)

    - ➢ Coordination is done through Inter Frame Spaces

- ➢ Synchronous data transfer for real-time traffic (like audio and video)

    - ➢ PCF (Point Coordination Function): based on the polling of the stations and controlled by the AP (PC)

    - ➢ Its implementation is optional, not really implemented in devices, but custom implementations are used for P-t-P links

- The system is semi-synchronous

  - Maintained through Beacon frames (sent by AP)

- Time is counted in intervals called slots

- A slot is the system unit time

  - its duration depends on the implementation of the physical layer and specifically on the

  - 802.11b: 20μs

  - 802.11a/h/g/n/ac: 9μs

    - g/n are forced to use 20 when coexisting with b

- Interframe space (IFS)

  - time interval between frame transmissions

  - used to establish priority in accessing the channel

- 4 types of IFS:

  - Short IFS (SIFS)

  - Point coordination IFS (PIFS) > SIFS

  - Distributed IFS (DIFS) > PIFS

    - AIFS(c) for Quality Enabled MAC, different for different traffic classes

  - Extended IFS (EIFS) > DIFS

- Duration depends on physical level implementation
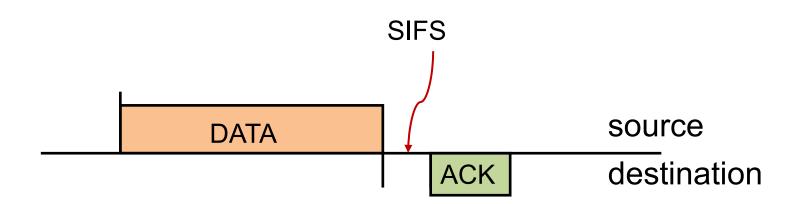
- Separates transmissions belonging to the same dialogue

- Gives the highest priority in accessing the channel

- Its duration depends on:

  - Propagation time over the channel

  - Time to convey the information from the PHY to the MAC layer

  - Radio switch time from TX to RX mode

  - 2.4GHz: 10μs

  - 5.5GHz: 16μs

- ## An exchange of frames that follows a successful contention for the channel

  - E.g.: a data frame followed by and ACK

- Used to give priority access to Point Coordinator (PC) → Normally the AP

- Only a PC can access the channel between SIFS and DIFS

- PIFS=SIFS + 1 time slot

- Used by stations waiting to start a contention (for the channel)

- Set to: PIFS + 1 time slot

  - 802.11b: 50µs
  - 802.11a/h/g/n/ac: 34µs

Extended IFS (EIFS)

- Used by every station when the PHY layer notifies the MAC layer that a transmission has not been correctly received

- Avoids that stations with bad channels disrupt other stations' performance

- Forces fairness in the access if one station does not receive an ACK (e.g., hidden terminal)

- Reduce the priority of the first retransmission (indeed make it equal to all others)

- Set to: DIFS + 1 ACK time

DCF Access Scheme

- Based on the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme:

  - Stations that have data to transmit contend for accessing the channel

  - A station has **to repeat** the contention procedure **every time** it has a data frame to transmit

  - What is Collision Avoidance? → Answer later

802.11 CSMA sender:

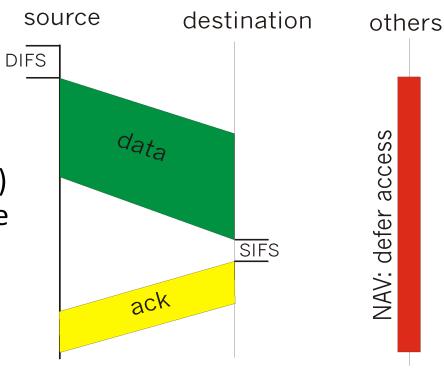- if sense channel idle for **DISF** sec.

    then transmit frame

- if sense channel busy
    then random access over a
    contention window CWmin (CA)
    when the channel becomes free

802.11 CSMA receiver:

if received OK

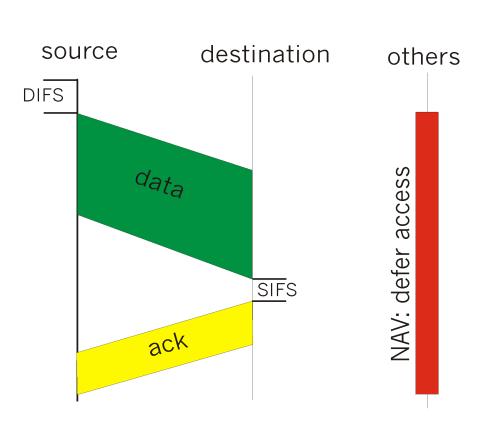   return ACK after **SIFS**

source   destination   others

DIFS

data

SIFS

ack

NAV: defer access

802.11 CSMA Protocol others:

- **NAV**: Network Allocation Vector

  - transmission length field

  - others (hearing data) defer access for NAV time units

  - NAV is contained in the header of **all** frames

  - Allows reducing energy consumption

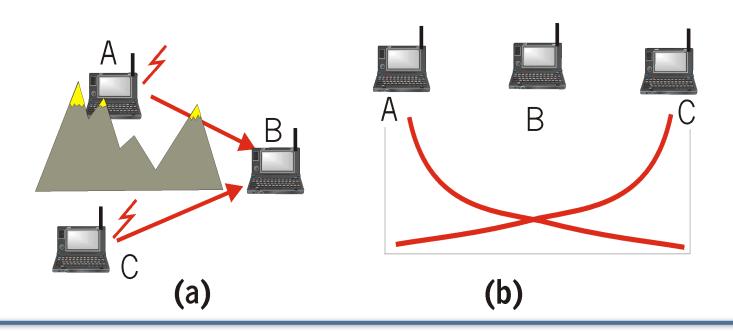 - Helps reducing hidden terminals problems

- hidden terminals: **A, C cannot hear each other**
  - obstacles, signal attenuation → (deterministic) collisions at B
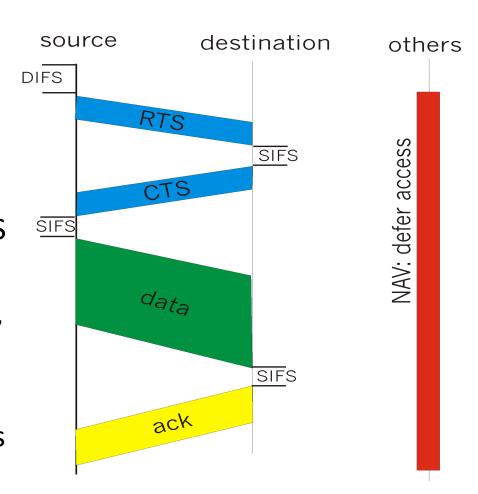- goal: avoid collisions at B
- **CSMA/CA with handshaking**

(a)   (b)

- **CSMA/CA: explicit channel reservation**
  - sender: send short RTS (request to send)
  - receiver: reply with short CTS (clear to send)
- **CTS reserves channel for sender, notifying (possibly hidden) stations**
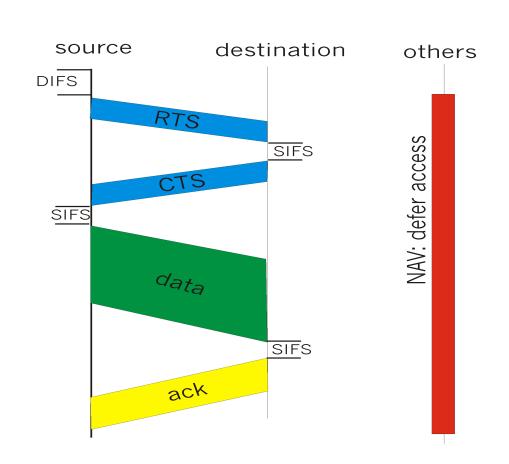- **reduces hidden station collisions**
- **increase overhead**

- RTS and CTS are short:
  - collisions of shorter duration, hence less "costly"

- DCF allows:
  - CSMA/CA
  - CSMA/CA with handshaking

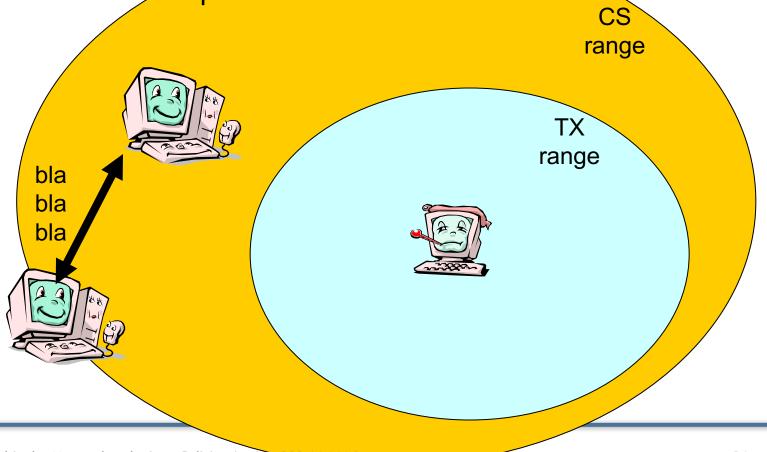- Sensing range is normally larger than receiving range
- Terminals may be "exposed" in that they sense the channel occupied, but cannot compete for it

CS
range

TX
range

bla
bla
bla

DCF
Basic & Enhanced Access Mode

- Used to determine whether the channel is busy or idle

- Performed at the physical layer (physical carrier sensing) and at the MAC layer (virtual carrier sensing)

  - Physical carrier sensing: detection of nearby energy sources

  - Virtual carrier sensing: the frame header indicates the remaining duration of the current Channel Access Phase (till ACK is received) → NAV

➢ Used by the stations nearby the transmitter to store the duration of the dialogue that is occupying the channel

➢ The channel will become idle when the NAV expires

➢ Upon the NAV expiration, stations that have data to transmit sense to the channel again

- Transmitter:
  - sense the channel
  - if the channel is idle, wait a time equal to DIFS
  - if the channel remains idle for DIFS, transmit MPDU
- Receiver:
  - compute the checksum verifying whether the transmission is correct
  - if so, it sends an ACK after a time equal to SIFS
  - ACK is only a header with a Tx rate less than or equal to the one used by the transmitter and no larger than
    - 2 Mbit/s in 802.11b
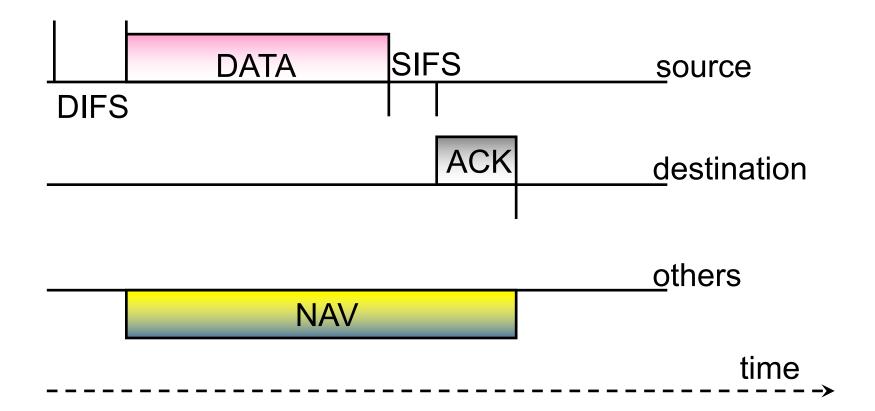   - 6/12 Mbit/s in 802.11g/a/h/n/ac

➢ Neighbors:

    ➢ set their NAV to the value indicated in the transmitted MPDU

    ➢ NAV set to: the MPDU tx time + 1 SIFS + ACK time

- A frame transmission may fail because of collision or errors on the radio channel

- A failed transmission is re-attempted till a max no. of retransmissions is reached

- ARQ scheme: Stop&Wait

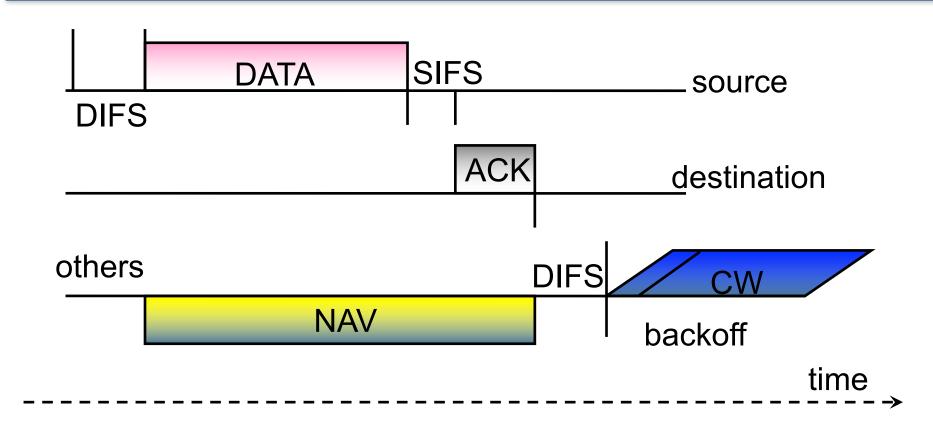The backoff procedure is run also if no collisions occurred yet but the channel is busy

- If a station senses the channel busy, it waits for the channel to be idle

- As soon as the channel is idle for DIFS, the station

    - computes the backoff time interval

    - sets the backoff counter to this value

- The station will be able to transmit when its backoff counter reaches 0

CW=Contention Window

➢ Integer value corresponding to a number of time slots

➢ The number of slots is a r.v. uniformly distributed in [0,CW-1]

➢ CW is the Contention Window and at **each transmission attempt of the same frame** is updated as:

  ➢ For i=1, $CW_1=CW_{min}$

  ➢ For i>1, $CW_i=2CW_{i-1}$ with i>1 being the no. of consecutive attempts for transmitting the MPDU

  ➢ For any i, $CW_i \leq CW_{max}$

  ➢ After a successful transmission $CW_1=CW_{min}$

➢ While the channel is busy, the backoff counter is frozen

➢ While the channel is idle, and available for transmission (after sensing it free for DIFS) the station decreases the backoff value (-1 every slot) until

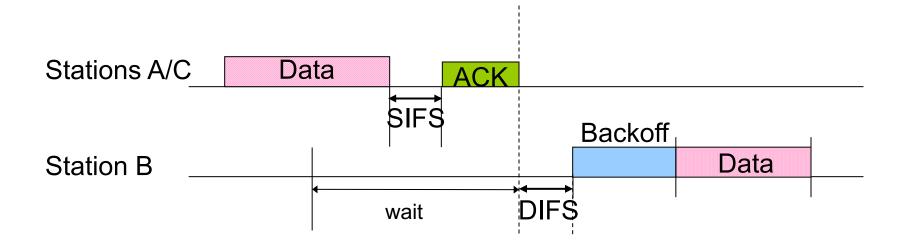 ➢ the channel becomes busy or

  ➢ the backoff counter reaches 0

➢ **If more than one station decrease their counter to 0 at the same time → collision**

➢ **Colliding stations have to re-compute a new backoff value**

➢ **A station that lost a contention keeps counting down the old backoff**

Stations A/C — Data — ACK — SIFS

Station B — wait — DIFS — Backoff — Data

➢ A station recontends for the channel when

  ➢ it has completed the transmission of an MPDU, but still has data to transmit

  ➢ a MPDU transmission fails and the MPDU must be retransmitted → binary backoff

➢ Before recontending the channel after a successful transmission, a station must perform a backoff procedure with CWmin

DCF
ACCESS WITH HANDSHAKING

- ## Used to reserve the channel

- ## Why?

  – Hidden stations

  – Colliding stations keep transmitting their MPDU; the larger the MPDU involved in the collision, the more bandwidth is wasted

  – Need to avoid collisions, especially when frame is large

  – Particularly useful when a large no. of STAs contend for the channel

- ➢ Handshaking procedure uses the Request to send (RTS) and Clear to send (CTS) control frames

- ➢ RTS / CTS should be always transmitted @1 (b) (6 a/g/h/n/ac) Mbit/s (they are only headers)

- ➢ Access with handshaking is used for frames larger than an RTS_Threshold

- ✓ **Transmitter:**
  - ✓ send a RTS (20 bytes long) to the destination
- ✓ **Neighbors:**
  - ✓ read the duration field in RTS and set their NAV
- ✓ **Receiver:**
  - ✓ acknowledge the RTS reception after SIFS by sending a CTS (14 bytes long)
- ✓ **Neighbors:**
  - ✓ read the duration field in CTS and update their NAV
- ✓ **Transmitter:**
  - ✓ start transmitting upon CTS reception

802.11e:
Improved Efficiency
and Service Differentiation

Novel MAC standardized in 2007 & "default" with /n/ac PHY

- Definition: A **flow** is a packet stream from a source to a destination, belonging to the same application

- Definition: **QoS** is a set of service requirements to be met by the network while transporting a flow

- Typical QoS metrics include: available bandwidth, packet loss rate, estimated delay, packet jitter, hop count and path reliability

- A flow is easily identified with the 5-tuple {IPs,IPd,Transport,PORTs,PORTd}

- QoS schemes in wired networks are NOT suitable for wireless networks

  - e.g., current wired-QoS routing algorithms require accurate link state and topology information

  - time-varying capacity of wireless links, limited resources and node mobility make maintaining accurate information difficult

- Supporting QoS in wireless networks is very challenging

- The IEEE 802.11 TG E was formed in 1999

- The Project Authorization Request (PAR) was approved in March 2000

- **Scopes of the IEEE 802.11 Task Group E**

    - Enhance the current 802.11 MAC to improve and manage QoS

    - Consider efficiency enhancements in the areas of DCF and PCF

    - Provide different classes of service (4 TCs)

- Released 2007 (effective 2009/10, widespread 2012 on)
- PHY unchanged (use a/b/g/n/ac/ad)
- MAC Enhanced: Goals
  - Increase MAC efficiency
  - Traffic Differentiation and Guarantee
  - TSPEC and CAC
  - Interoperation with legacy 802.11
- It's also used in 802.11n/ac/ad PHY … where it's fundamental

- A station using 802.11e is called *QoS Enhanced Station* (QSTA)

- An AP using 802.11e is called *QoS Access Point* (QAP)

- QSTA e QAP works within a *QoS Basic Service Set* (QBSS)

- The two coordination functions DCF e PCF are substituted by a single *Hybrid Coordination Function (HCF)*

- ## Hybrid Coordination Function, alternates:

  - EDCA (Enhanced Distributed Channel Access), contention based, conceived to support legacy stations and provide some *stochastic* level of differentiation

  - HCCA (HCF Coordinated Channel Access), polling based, provides collision free periods with guaranteed assignment and *deterministic* differentiation

  - HCCA duration can be zero
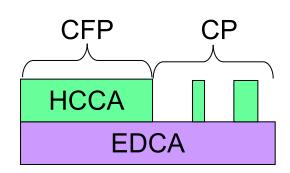
802.11e proposes a new access scheme: **Hybrid Coordination Function (HCF),** composed of two coordination functions

- **Enhanced Distributed Channel Access (EDCA)**

  – A basis layer of 802.11e; always "running" operates in Contention Periods (CP)

- **HCF Controlled Channel Access (HCCA)**

  – HCCA operates in CFP and it is superimposed on EDCA and can interrupt CPs

- TXOP: Transmission Opportunity

  – Time interval during which a QSTA has the right to transmit

  – A channel contention/access is done for ta TXOP and not for a single frame

  – It is characterized by a starting time and a maximum duration (TXOP_Limit)

  – Used in both CP and CFP

- MAC-level FEC (Hybrid I and II)

- **Ad hoc features:**

  - Direct Communication / Side Traffic

  - WARP: Wireless Address Resolution Protocol

  - AP mobility

- Within a QBSS a centralized controller is needed to coordinated all QSTAs. This is the *Hybrid Coordinator* (HC), normally implemented within a QAP

- An HC has the role of splitting the transmission superframe in two phases continuously alternating:

  – *Contention Period* (CP), where QSTAs content for the channel using EDCA

  – *Contention-Free Period* (CFP), where HC defines who is going to use the channel and for what time with a collision free polling protocol

Beacon

Beacon

CAP

CAP

CFP

CP

Beacon Interval (BI)

	EDCA
	HCCA

CFP/CAP can be simply absent … the case in most access BSS

- The *Enhanced Distributed Coordination Function* (EDCF) define a differentiated access scheme based on an improved (yet complex) contention scheme

- It is an evolution of CSMA/CA DCF, with the add-on of traffic classes to support QoS and differentiate traffic

- EDCF is designed to support frames with the same 8 priority levels of 802.1d, but mapping them on only 4 access categories

- Every frame passed to the MAC layer from above, must have a priority identifier (from 0 to 7), called *Traffic Category Identification* (TCId)
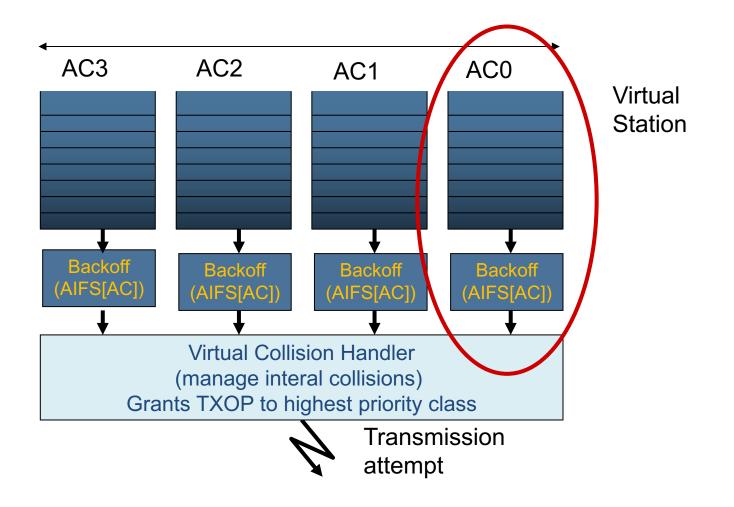
- TCId is written in one header field of the MAC frame
- Each 802.11e QSTA & QAP MUST have four separated AC queues

- **Each AC queue is FIFO and behaves independently from the others as far as the CSMA/CA MAC protocol is concerned**

AC3   AC2   AC1   AC0   Virtual
                                            Station

Backoff   Backoff   Backoff   Backoff
(AIFS[AC]) (AIFS[AC]) (AIFS[AC]) (AIFS[AC])

Virtual Collision Handler
(manage interal collisions)
Grants TXOP to highest priority class

Transmission
attempt

- ACs are differentiated based on their CSMA parameters:
  - **IFS**
  - **CWmin**
  - **CWmax**
  - **Backoff exponent**

- Higher priority ACs are assigned parameters that result in shorter CWs so that a statistical advantage is gained in accessing the channel

- Protocol parameters become vectors
  - CWmin[AC]
  - CWmax[AC]
  - AIFS[AC]
  - bck[AC]

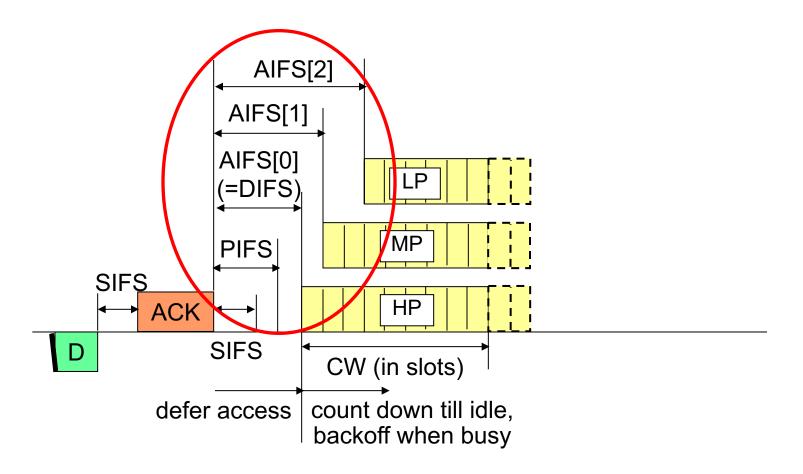- CW[AC,t]   is derived with the usual CSMA/CA rules

- Arbitration InterFrame Space (AIFS) substitute the common DIFS

- Each AIFS is at least DIFS long

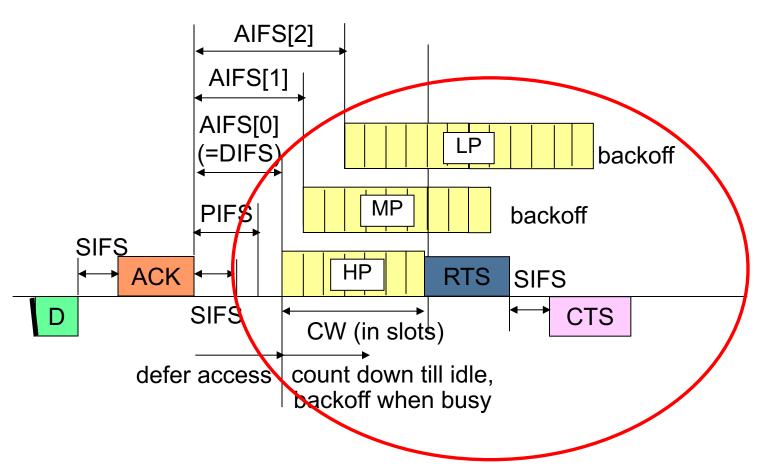- Befor entering the backoff procedure each *Virtual Station* will have to wait AIFS[AC], instead of DIFS

802.11a: slot=9 μs, SIFS=6 μs, PIFS=15 μs, DIFS=24 μs, AIFS $\geq$34 μs

802.11a: slot=9 μs, SIFS=16 μs, PIFS=25 μs, DIFS=34 μs, AIFS $\geq$34 μs

- Each AC queue behaves like a different virtual station (independent sensing and backoff)

- If the backoff counters of two or more parallel ACs in the same QSTA reach 0 at the same time, a scheduler inside the QSTA avoids l collision by granting the TXOP to the AC with the highest UP

- **The lowest priority colliding behaves as if there were an external collision**

- Values of AIFS[AC], CWmin[AC] e CWmax[AC] are determined by the QAP and transmitted within beacon frames (normally every 100 ms)

- QSTAs must abide to the received parameters

- QSTAs may use these parameters to chose the QAP the prefer to connect to (estimate of the expected performance)

- TXOP is the time interval in which a STA may use the channel
- It's an initial time plus a duration, indeed the contention is no more for a PDU, but can be for many aggregated PDUs

- CW[AC] is managed with usual rules of increment (after collisions/failures) and decrement (during idle cahnnel):

NewCW[AC] = ((OldCW[AC] + 1) * 2) - 1

Sample allocation of TCId to ACs:

TCID	CA	Traffic description
0	0	Best Effort
1	0	Best Effort
2	0	Best Effort
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

- Once the station has gained access to the medium, it can be allowed to send more than one frame without contending again

- The station cannot transmit longer than TXOP_Limit

- ACK frame by frame or Burst ACK

- SIFS is used between frames within the same TXOP to maintain the channel control when assigned

- **Pros**

  – Reduces network overhead

  – Increases throughput (SIFS and burst ACKs)

  – Better fairness among the same priority queues: independently of the frame size, a QSTA gets a TXOP every time it wins a contention

    - E.g., STA A uses 500 B frame; STA B uses 1K B frame. Thus B would get higher throughput in 802.11, while in 802.11e both can get approximately same throughput

- **Cons**

  – Possible increasing of delay jitter

  – TXOP_Limit must be longer than the time required for transmitting the largest data frame at the minimum speed

- In any case EDCA does not solve the downlink/uplink unfairness problem

- HC may allocate TXOPs to himself (QAP) or to other QSTAs

- Self allocation is done to transmit MSDUs, allocation of resources may solve the uplink/downlink unfairness

- Allocation to AP can be done after a Point coordination InterFrame Space (PIFS) con PIFS < DIFS

- HC (QAP) has priority over other stations and may interrupt a CP to start a CFP transmitting a Poll frame

- Time is divided between contention free periods (CFP) and contention periods (CP), that are alternated roughly cyclically

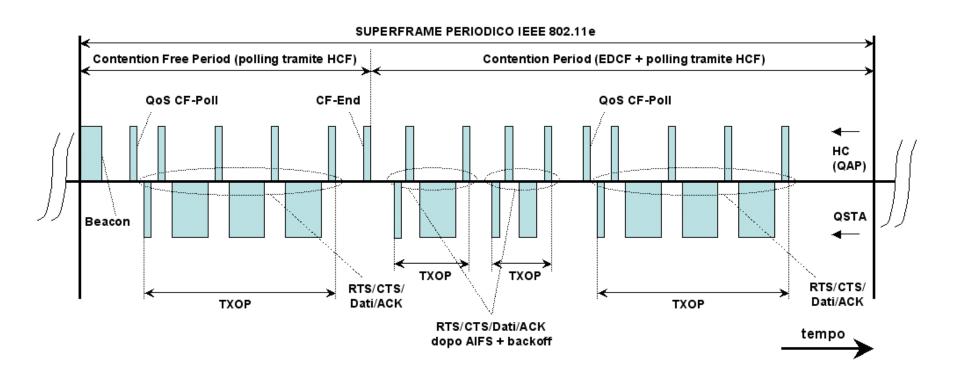- A sequence CFP + CP defines a Periodic Superfame of 802.11e

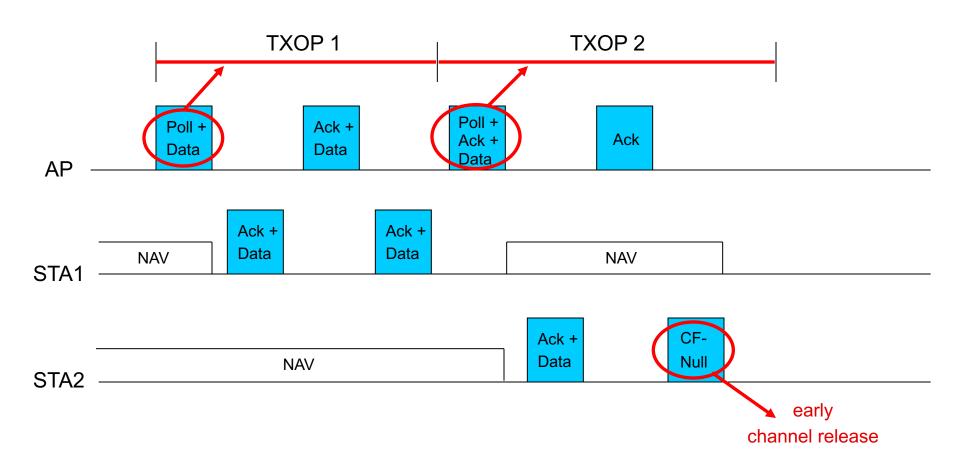- The CP can be interrupted by other contention free periods called CAPs

SUPERFRAME PERIODICO IEEE 802.11e

- Within a CP, TXOP is determined either:

  - Through EDCF rules (free channel + AIFS + BO + TXtime)

  - Through a poll frame, called QoS CFPoll, sent by HC to a station

- QoS CFPoll is sent after PIFS, so with priority wrt any other traffic

- Indeed there is not a big difference between a CFP and CAPs

- During CFP, TXOPs are again determined by HC and QoS CFPoll can be piggybacked with data and ACKs if needed

- Stations not polled set NAV and cannot access the channel

- The CFP must terminate within a time specified in beacons and it is terminated by the CF-End frame sent by HC

- QoS CF-Poll frame was introduced with the 802.11e amendment, for backward compatibility it contains a NAV field the legacy stations can use to avoid interfering

- NAV specify the whole TXOP duration

- Legacy stations in HCF can only use the CP period

- HCCA effectively provides policing and deterministic channel access by controlling the channel thrugh the HC

- It is backward compatible with basic DCF/PCF

- Based on polling of QSTAs by the HC

Crucial features of HCCA

- HCCA operates in CP and CFP

- Uses TXOPs which are granted through HC

  – HC allocates TXOPs by using QoS CF-Poll frames

  – In CPs, the time interval during which TXOPs are polled by HC is called CAP (Controlled Access Period)

  – 4 Traffic Categories (TCs)

- According to HCCA:

  - HC may allocate TXOPs to itself to transmit MSDUs whenever it wants, however only after having sensed the channel idle for PIFS

  - In CP, the HC can send the CF-Poll frame after a PIFS idle period, thus starting a CAP

  - In CFP, only the HC can grant TXOPs to QSTAs by sending the CF-Poll frame

  - The CFP ends after the time announced by HC in the beacon frame or by the CF-End frame from HC
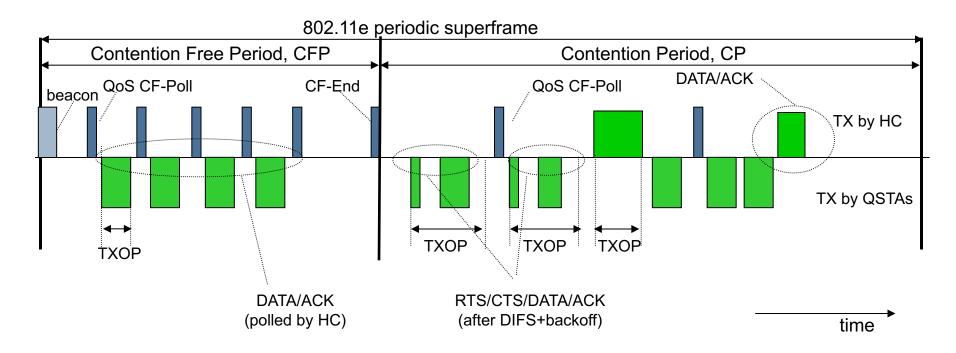
- **A QSTA behaves as follows**

  – In CP QSTAs can gain a TXOP thanks to a CF-Poll frame issued by HC during CAPs, otherwise they can use EDCA

  – In CFP, QSTAs do not attempt accessing the channel on their own but wait for a CF-Poll frame from the HC

- The HC indicates the TXOP duration to be used in the CF-Poll frame (QoS-control field)

  – Legacy stations kept silent by NAV whenever they detect a CF-Poll frame

802.11e periodic superframe

Contention Free Period, CFP — Contention Period, CP

beacon — QoS CF-Poll — CF-End — QoS CF-Poll — DATA/ACK — TX by HC — TX by QSTAs

TXOP — TXOP — TXOP — TXOP

DATA/ACK (polled by HC)

RTS/CTS/DATA/ACK (after DIFS+backoff)

time

During the CP, a TXOP may begin because:

- The medium is determined to be available under EDCA rules (EDCA-TXOP)

- The STA receives a special polling frame from HC (polled-TXOP)

- Polling list is a crucial key in HCCA

  – Traffic scheduling (i.e., how QSTAs are polled) is not specified

  – QSTAs can send updates to the HC on their queue size as well as on the desired TXOP, (through the QoS control field in data frames)

  – QSTAs can send ADDTS requests to initiate a new traffic stream

- Two types of signaling traffic are supported:

    – Connectionless queue state indicator

      - E.g., Arrival rate measurement: notification and not negotiation between peer entities is used

    – TSPEC (Traffic Specification) between HC and QSTAs

      - E.g., service negotiation and resource reservation

- TSPEC are the base for CAC

- QoS without CAC is impossible

- QoS is granted to flows not to packets

- Flows are persistent (normally)

- Flows can be predicted (sometimes)

- Not essential to backward compatibility
  - The standard has just a reference impl. (SS)
- HCF is implemented in the AP
  - HCCA scheduling is a function of HCF
- Requirements of traffic flows are contained in the *Traffic Specifications* (TSPEC):
  - Maximum, minimum and mean datarate
  - Maximum and nominal size of the MSDUs
  - Maximum Service Interval and ***Delay Bound***
  - Inactivity Interval
  - ...