S-72333 PhD Seminar on Radio Communications

The IEEE 802.11 Medium Access Control (MAC)

Laselva Daniela

dlaselva@cc.hut.fi

09.03.2004

Contents

MAC functionalities

- MAC is a logical entity that **controls / coordinates the access of the stations** (STAs) **into the medium** (radio channel) and utilizes mainly **structures** and **protocols** to enhance communications over the medium.

- MAC provides the core framing operation and the **interaction with a wired network (NT) backbone and the STAs**. It handles the **data moving between PHY and NT layers**.

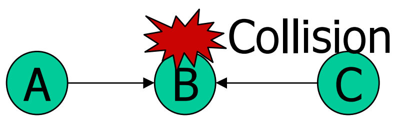
Challenges for MAC

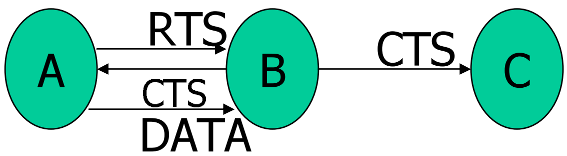
a) RF link quality: noise, interference, fading, unlicensed devices within ISM bands.

Counter-measure: atomic operations are not interrupted and frames are acknowledged.

b) Hidden Node: 'hidden' nodes might transmit simultaneously and collision is not detectable.

Counter-measure: **RTS/CTS** signal exchange to clear out the area before the frame.



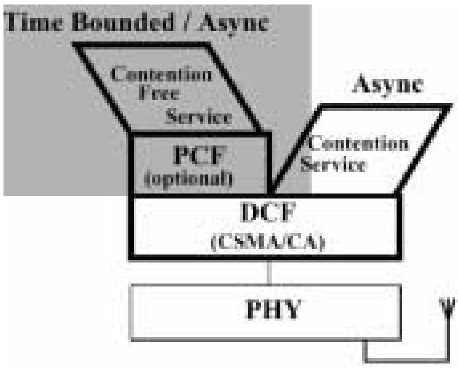


MAC Access and Timing

Access to the medium through *coordinated functions* (**CF**s) to support both asynchronous and time-bound traffic:

- DCF (Distributed CF): basis of CSMA/CA access scheme (Ethernet-like), provides contention-based access.

- PCF (Point CF), for infrastrucure NTs, not widely implemented, provides contention-free services.



Carrier-sensing Functions

Carrier-sensing functions determine if the medium is available.
If busy, MAC reports to higher layers.

1. **PHY carrier-sensing**: detects signal strength from other sources at PHY; it depends on medium and modulation.
   Cons:
   - Expensive HW sensing for RF-based media.
   - Hidden node at PHY.
2. **Virtual carrier-sensing**: at MAC by NT Allocation Vector (**NAV**) using a *duration field* within 802.11 frames.
   - NAV = timer that reserves the medium for a fixed time, set in stations. Other stations count down from NAV ->0: NAV>0 → the medium busy, otherwise idle. NAV assures that atomic operations are not interrupted.

Channel is said to be idle only when both the mechanisms report idle!

Interframe Spacing

- Interframe Space (**IFS**) = **time interval between transmission of frames**, indep. of transmission speed.

- Stations delay transmission of certain spacings untill medium idle. By varying the spacings, MAC creates different **priority** levels for different types of traffic (i.e., high-priority traffic wait less). Priority access to the medium is controlled through three IFS intervals.

1. **SIFS** (Short IFS): for the highest-priority traffic (RTS/CTS, ack frame,..)
2. **PIFS** (PCF IFS): in contention-free period stations transmit data after PIFS and preempt any contention-based traffic.
3. **DIFS** (DCF IFS): minimum medium idle time for contention-based services.
4. **EIFS** (Extended IFS): used only when there is an error in transmission.

SIFS < PIFS < DIFS < EIFS

DCF (contention-based access)

DCF allows multiple stations to interact without central control.

Basic DCF-based MAC rules:

1. Before transmission, each station checks whether the medium is idle. If the *medium idles* for longer than DIFS: immediate transmission is possible. Both carrier-sensing functions applied.
   - After a frame is received with no errors, the medium must be free for minimum DIFS (otherwise for EIFS).
2. If the *medium busy*, station waits as *access deferral* for DIFS and retries after an ***exponential backoff delay***.

DCF (contention-based access)

(cont.)

Additional DCF-based MAC rules:

1. **Error recovery**: Sender station is responsible for error detection and recovery. It waits for positive acknowledgment per each frame (unicast data).
   - Transmission retried till ack arrives otherwise considered lost.
   - Any frame/fragment failure (due to error detection, lack of ack or failure in gain access to medium) increments a (**short** or **long**) ***retry counter*** associated to the frame/ fragment. Otherwise it is set to 0.

     - Short/long counter associated to short/long frame compared to RTS threshold (longer congestion window when transmission retried).

     - If retry limit reached frame discarded!

DCF (contention-based access)

(cont.)

Additional DCF-based MAC rules:

2. Multiframe sequences may **update NAV** within each step in transmission, on frame-by-frame basis.
   - If station receives NAV''>NAV'→It updates NAV to value NAV''.
3. Ack, CTS and fragments frames are transmitted after SIFS (i.e., received with **max priority**)
   - When station gains controls over the channel, channel is locked to other stations by using SIFS<DIFS
4. Extended frame sequences are required for higher-level packets larger than configured (RTS and fragmentation) thresholds.

Exponential backoff algorithm

After transmission complete + DIFS elapsed, other stations might attempt to transmit congestion-based data.

Backoff Window (also **Contention Window**,CW).

- Increases with # of attempts to the medium.
- Its size depends on and is limited by PHY, but generally when retry counter increases, it moves to the next power of 2.
- Slot length is medium-dependent (short if higher-speed PHY).
- Reset when retry counter associated reached or frames successfully.

- **CW assignment:** each station picks a random slot (a random uniformly likely selectable value between 0 and CW) and waits for it before transmitting. The station with first slot (the lowest random number) transmits first.

Summary of DCF operations

1. A station before transmitting senses the medium:
   - If it is idle, waits for DIFS interval, and senses it again.
   - If the medium is free, sender gains access to the medium: RTS is transmitted.
2. Target receiver replies with CTS after SIFS.
3. Sender now can transmit data frame (all other STAs set NAV).
4. If the receiver gets the frame correctly, it sends an ACK to the sender after a SIFS interval.
5. Any other station which attempts to the medium waits for DIFS, the medium is found to be busy either in step 1, 2, 3 and 4: back-off procedure is invoked

Within an atomic operation, station waits for SIFS<DIFS:

NAV & SIFS → Medium is seized!

Summary of DCF operations

(cont.)

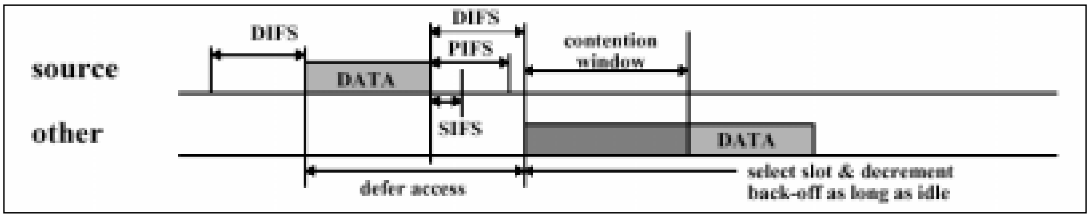


Fig.1 CSMA/CA: direct access if medium free for > DIFS, else defer & backoff

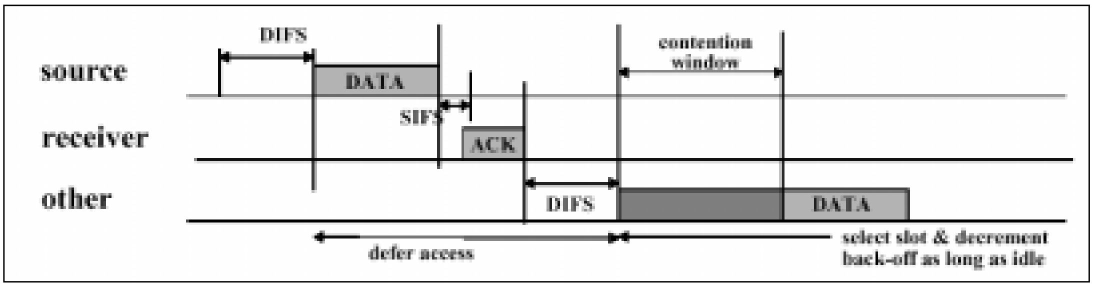


Fig.2 CSMA/CA + ACK: receiver sends ACK immediately if CRC okay
(if no ACK, retransmit frame after a random back-off)

RTS/CTS with duration: distribute medium reservation information, also used in the defer decision ("virtual carrier sensing")

Fragmentation and Reassembly

-**Fragmentation: why?**

- It allows higher-level packets and management frames to go through the channel broken in smaller pieces.
- It improves reliability and increasing throughput when interference exists by reducing percentage of data corrupted by interference.

- **Fragmentation: when?**

- If packet's length exceeds fragmentation threshold.

- **Fragmentation: how?**

- All fragments: same frame sequence number, ascending fragment number and a frame control (accounts for # of fragments).
- All the fragmets within a frame sent in a fragmentation burst.

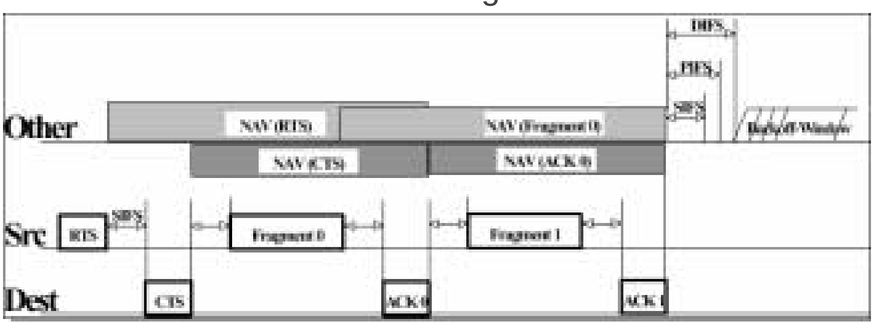


Fig.3

Fragmentation burst

Frame Format

Classes of frames:

- **Management Frames:**
  - Used for Station association, dissociation, timing and synchr., authentication.
- **Control Frames:**
  - Used for Handshaking (RTS/CTS) and ACK frames during CP.
- **Data Frames**:
  - Used for Sending data during CP and CFP.

Bytes: 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header (Frame Control through Addr 4)

Fig.4 Generic 802.11 MAC frame

Frame Format (cont.)

Frame control subfields:

- Protocol version: so far only 1 version (number 0).
- Type and subtype: due to different classes of frames.
- ToDS and FromDS bits: indicate if frame destined/from to/a distribution system. For infrastructure NTs equals to "1".
- More fragments bit: it equals to "1" in any non-final fragments of a fragmented frame. Otherwise it set to "0".
- Retry bit: any retransmitted frame sets it to "1".

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

Frame Control Field

Fig.5 Frame control field

Frame Format
(cont.)

Frame control subfields (follows):

- Power management bit: (after completion of current atomic exchange) ”1” means devices are in power-saving mode, ”0” active. (APs not allowed to power-save mode because perform management functions).
- More data bit: APs buffer frames from distribution system towards power-saving mode stations.
- WEP bit: set to ”1” when frame encrypted.
- Order bit: set to ”1” when fragments and frames transmitted in order.

Frame Format
(cont.)

Duration/ID Field:

- When bit 15 equals to ”0”: *duration field used to set NAV*. NAV = # microseconds the medium is reserved (busy) due to current transmission. All the stations monitor the header of received frames and update NAV.
- During contention-free periods: bit14 =0, bit15 =1, all other bits =0 → field value = 32 768 interpreted as NAV. Any station that did not hear Beacon (announce contention free period) updates NAV avoiding collision.
- In PS-Poll frames bit14 and bit15 =0. For battery saving stations turn antennas off. When they wake up periodically transmit a PS-Poll and check if any buffered data from AP. An association ID (AID, identifies to which BSS they belong to) is included.

Frame Format
(cont.)

Address Fields:

• Four address fields: 48 bits long (as in Ethernet); not always used; not for all the MAC frames: they depend on frame type.

*Different types of addresses (**48-bit MAC identifier**):*

- *Destination* address (i.e, final destination)
- *Source* address (i.e, originated frame)
- *Receiver* address
- *Transmitter* address
- *Basic Service Set ID* (*BSSID*)
- Rule of thumb: address1 used for the receiver; address2 used for the transmitter; address 3 used for filtering by the receiver (frames discarded from a BSS other than the associated one).

• When first bit towards medium is "0" → address represents a single station (*unicast*);

• When first bit is "1" → address represents a group of physical stations (*multicast*);

• If all bits are "1" → the frame is a *broadcast*.

Frame Format
(cont.)

Sequence control field:

Used for de-fragmentation and discarding duplicate frames. It includes:

• 4-bit *fragment number* field: associated to fragments. It has value "0" for the first fragment. The successive ones increment it by 1.

• 12-bit *sequence number* field: associated to higher-level frames.

It operates as modulo-4096 counter of the frames transmitted.

It begins as "0", increments by "1" for each higher-level packet handled by the MAC.

- Retransmitted frames or fragments keep the same seq. number.

Frame Format

(cont.)

Frame body (also **Data Field**):

Moves the higher-layer payload from station to station.

- 802.11 can transmit frames with a maximum payload of 2312 bytes of higher-level data (8 bytes header of 802.2 LLC + 2296 bytes of NT payload + WEP overhead).
- Empty field for control and management frames.

Frame Check Sequences (FCS) referred as Cyclic Redundancy Check (CRC):

- Allows to check the integrity of received frames (all the fields included into FCS).
- Recalculated by APs because MAC address in 802.11 differs from 802.3.

Contention-Based and Contention-Free Data services

Summary of atomic exchanges that move data on 802.11:

- Unicast data always acknolewdged.
- The exchange includes 2 frames but represents a single (atomic) operation.
- If any part fails, operation is retried.

Two different sets of atomic exchanges:

1. ***Contention-based used by DCF***: dominate 802.11 MAC

2. Contention-free used by PCF: tricky and not used in commercial products!

Contention-Based (CB) access: Management frames

Broadcast and multicast management frames have simpler exchange (e.g. no ack). They include:

- Request/response of (Re-)Association, Probe, Privacy frames;
- Beacon (Time stamp, beacon interval, TDIM period, TDIM count, channels sync info, ESS ID, TIM broadcast indicator) frame, for Registration (Association);
- TIM (Traffic Indication Map) indicates traffic to a dozing node;
- Dissociation frame;
- Authentification frame.

- Broadcast/multicast management frames have broadcast /multicast address in Address1 field.

-Frames for group addresses are not fragmented & not acknowledged.

- After transmission all the stations wait for DIFS and count down the random interval in back off window.

- Since single-frame sequence: NAV = 0 and no carrier-sense method.

CB access: unicast frames

Frames destined to a single station: directed data/unicast such as:

1. **Acknowledgments**: if frame is not ack.ed → is supposed lost. NAV locks the medium for time necessary for transmitting frame, its ack, and SIFS. (NAV in the ack set to 0).
2. **Fragmentation:** First data frame sets NAV to lock the channel for its ack, next fragment, following ack. MAC sets More Fragments (MF) bit = 1. All the no-final fragment extend the reservation increasing the NAV. The last data frame (MF bit = 0)
3. **RTS/CTS***:* locks medium for uninterrupted transmission for larger frames (>threshold)
4. **RTS/CTS with fragmentation***:* long fragmented frames uses RTS/CTs for exclusive access to the medium.

CB access: Power saving (PS) sequences for Infrastructure NT

Amplifiers in RF systems are the most power-consuming components: battery life optimized by shutting down radio transceiver.

- **During sleeping periods (low-power mode) APs buffer unicast data frames and announce them with Beacon frames. Awakened station (in active mode) retrievs its data with PS-Poll frames.**

- *Immediate response*: AP replies immediately (after SIFS) to PS-Poll frames.

- *Deferred response*: AP replies to PS-Poll frames immediately with ack and deliver data at any point.

- Awakened station returns to sleep mode after receiving Beacon frame with Traffic Indication Mapping (TIM) is clear (indicates that no more traffic is buffered).

CB acces: PS sequences for Ad Hoc NT

-A STA announces to enter PS-mode anytime after completing data frame handshake with the power management bit set.

- The STA wakes regularly up when receives beacon frame and for a Ad Hoc TIM (ATIM) window after the beacon. During this window other STAs might announce their frames to the PS-STA.

-**All the functions need to be performed by sending STA:**

- **It has to track the STAs in PS-mode.**
- **It sends announcement frame to PS-STA.**
- **It has to buffer the data frame to PS-STA before receiving the announcement ack from PS-STA thus sending the data frame.**

Each transmission consumes power for the sending STA.

Conclusions

Issues/problems at MAC layer	802.11 solutions
Session mng: Authentification / Association	Management frames
Synchronous and asynchronous traffic	DCF and PCF
Gain access to the medium Hidden problem	RTS/CTS handshake (e.g., RTS/CTS/Data...)
Medium reservation	NAV
Half duplex (error detection not possible)	ACK (e.g.,RTS/CTS/Data/ACK,.)
Fragmentation	Frames fields
Avoid collisions	Back off delay
Power mng:Power save mode	Sleep and awake mode

Abbreviations

AP Access Point

ATIM Ad HocTraffic Indication Mapping

BSSID Basic Service Set ID

CSMA/CD Carrier Sense Multiple Access /Collision Detection

CSMA/CA Carrier Sense Multiple Access /Collision Avoidance

CTS Clear to Send

CRC Cyclic Redundancy Check

CW Contention Window

DCF Distributed Cordination Function

DIFS Distributed Interframe Space

DSAP Destination Service Access Point

EIFS Extended Interframe Space

HDLC High-level Data Link Control

ISM Industrial, Scientific and Medical

LLC Logical Link Control

Abbreviations

MAC Medium Access Control

NT Network

OUI Organizationally Unique Identifier

PCF Point Cordination Function

PHY Physical

PIFS PCF Interframe Space

PS-Poll Power Saving Poll

RTS Request to Send

SSAP Source Service Access Point

SIFS Short Interframe Space

SNAP Sub-NT Access Protocol

STA station

TIM Traffic Indication Mapping

TDIM Traffic Delivery Information Message

WEP Wired Equivalent Privacy

References

I. IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999
Available: http://standards.ieee.org/getieee802/download/802.11-1999.pdf

I. 802.11 Wireless Networks, The definitive guide, Matthew S. Gast, O'Reilly 2002

II. OFDM Wireless LANs: A Theorethical and Practical Guide, Juha Heiskala, John Terry, Sams Publishing 2002

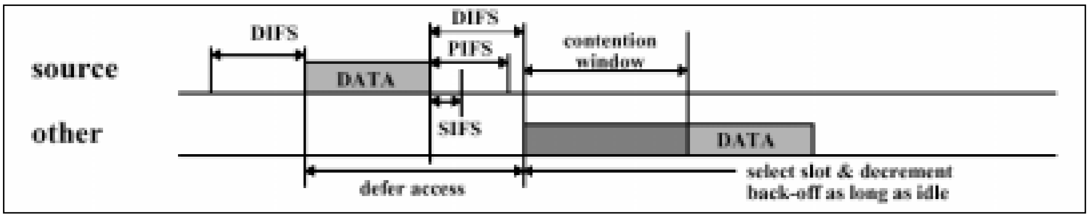
III. Shugong X., Saadawi T., "Does the IEEE 802.11 MAC Protocol work Well in Multihop Wireless Ad Hoc Networks?", IEEE Comm. Magazine, Page(s): 130-137, June 2001

IV. Srivastava M., " Sharing the Wireless Link: Part II", University of California, EE Department, 2002

Annex1: PCF (optional capability)

PCF offers to infrastructure NT Contention-Free Access and Service for supporting time-sensitive data via a totally centralized polling mechanism.

- PCF relies on the Point Coordinator (PC) to perform polling.
- Polled stations are allowed to transmit data sequentially, thus removing contention.
- PCF and DCF alternate with each other (coexistence).
- CFP_Rate (contention free period rate) determines the frequency with which PCF occurs.



Annex1: PCF

(cont.)

- Within an interval, a portion of the time is allocated for CFP, and the rest for CP. A limit is set on the duration of CFP so that the DCF traffic is not degraded too much.

- AP initiates the PCF by sending a beacon frame.
  - AP uses DCF to send the frame.
  - It senses the channel only for PIFS time.
  - Since contention is involved in starting the PCF mode, its duration may vary between intervals.

•If the station has no frame to transmit, it sends a Null function frame to the PC.

•If a PC fails to receive an ACK for a CF-Poll frame, it waits for PIFS interval, and polls the next station in the sequence.

Homework

1. Describe briefly the MAC services (data services: e.g., medium access operations; management services: e.g., power saving, privacy) how they are specified in terms of MAC frames exchange.
2. What is the function of atomic operations in MAC frames/sequence exchange?
3. Typically stations receive data in burst, but they should remain in receive state constantly. -How can we power off during idle periods, but maintain the session?