Nomadic Communications

WLAN (802.11)

UNIVERSITÀ DEGLI STUDI DI TRENTO

Renato Lo Cigno
LoCigno@disi.unitn.it - Tel: 2026

Dipartimento di Ingegneria e Scienza dell'Informazione

Home Page: http://isi.unitn.it/locigno/index.php/teaching-duties/nomadic-communications

Copyright

IEEE 802.11

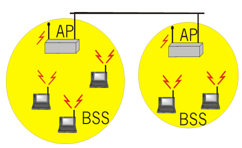
- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients
- Defines the PHY and MAC layer (LLC layer defined in 802.2)
- Physical Media: radio or diffused infrared
- Standardization process begun in 1990 and is still going on (1st release '97, 2nd release '99, then '03, '05, ...)

802.11 Architecture

- 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)

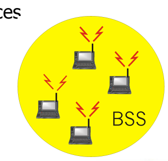
WLAN with Infrastructure

- BSS contains:
  - wireless hosts
  - access point (AP): base station
- BSS's interconnected by distribution system (DS)



Ad Hoc WLANs

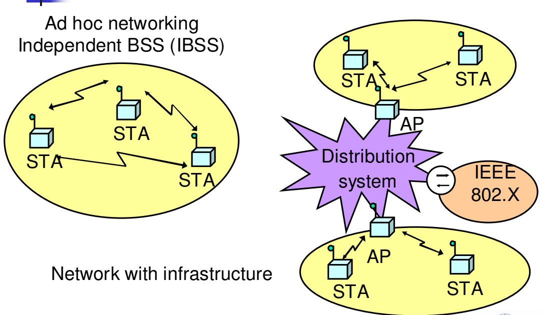
- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS
- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield
- IETF MANET (Mobile Ad hoc Networks) working group



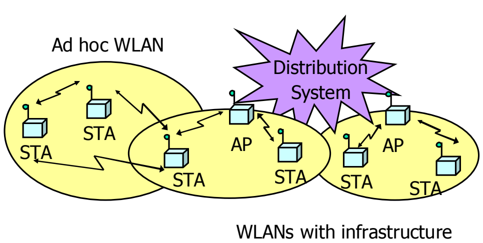
Extended Service Set (ESS)

- Several BSSs interconnected with each other at the MAC layer
- The backbone interconnecting the BSS APs (Distribution System) can be a:
  - LAN (802.3 Ethernet/802.4 token bus/802.5 token ring)
  - wired MAN
  - IEEE 802.11 WLAN, possibly meshed (routing problems!)
- An ESS can give access to the fixed Internet network through a gateway node
  - If fixed network is a IEEE 802.X, the gateway works as a bridge thus performing the frame format conversion

Possible Scenarios (1)



Possible Scenarios (2)



Joining a BSS

Scanning — Authentication — Association

- BSS with AP: Both authentication and association are necessary for joining a BSS
- Independent BSS: Neither authentication neither association procedures are required for joining an IBSS

Joining BSS with AP: Scanning

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

- Active Scanning may be more performant bu wase resources

Passive Scan

- 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

Active Scan

- **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

Joining BSS with AP: Authentication

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

- **Open system authentication** (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack
- **Shared key authentication**
  - Stations receive shared secret key through secure channel independent of 802.11
  - Stations authenticate through secret key (requires encryption via WEP)
- **Per Session Authentication (WPA2 – more later)**

Joining BSS with AP: Association

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
- New AP informs old AP via DS

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

IEEE 802.11 MAC Protocol

Performs the following functions:

- Resource allocation
- Data segmentation and reassemby
- MAC Protocol Data Unit (MPDU) address
- MPDU (frame) format
- Error control

MAC Frames

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

Data Transfer

- Asynchronous data transfer for delay-tolerant traffic (like file transfer)
  - **DCF** (Distributed Coordination Function)
- 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)

Time Slot

- Time is divided into intervals, called **slots**
- A slot is the system unit time and its duration depends on the implementation of the physical layer
  - 802.11b: **20µs;** 802.11a: **9µs**
  - Stations are **synchronized** with the AP in the infrastructure mode and among each other in the ad hoc mode ⇒ the system is **synchronous**
- Synchornization maintained through Beacon frames

locigno@disi.unitn.it 19

IFS

- 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
  - Extended IFS (EIFS) > DIFS
- Duration depends on physical level implementation

locigno@disi.unitn.it 20

Short IFS (SIFS)

- **To separate transmissions belonging to the same dialogue**
- Associated to the highest priority
- 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
- 802.11b: 10µs; 802.11a: 16µs

locigno@disi.unitn.it 21

Point Coordination IFS (PIFS)

- Used to give priority access to Point Coordinator (PC)
- Only a PC can access the channel between SIFS and DIFS
- PIFS=SIFS + 1 time slot

Distributed IFS (DIFS)

- Used by stations waiting for a free channel to contend
- Set to: PIFS + 1 time slot
- 802.11b: 50μs; 802.11a: 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 is 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 slot

DCF Access Scheme

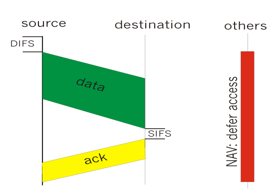
Basic Characteristics

- Its implementation is mandatory
- DCF is 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

IEEE 802.11 MAC Protocol Overview: CSMA/CA

802.11 CSMA: sender
- if sense channel idle for **DISF** sec.
  then transmit entire frame (no collision detection)
- if sense channel busy
  then random access over a contention window CWmin (CA)

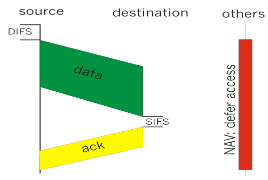
802.11 CSMA receiver:
if received OK
  return ACK after **SIFS**



IEEE 802.11 MAC Protocol Overview

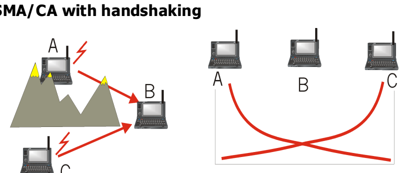
802.11 CSMA Protocol: others

- **NAV**: Network Allocation Vector
  - 802.11 frame has transmission time field
  - others (hearing data) defer access for NAV time units
  - NAV is contained in the header of frames
  - Allows reducing energy consumption
  - Helps reducing hidden terminals problems



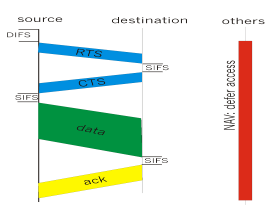
Hidden Terminal Effect

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



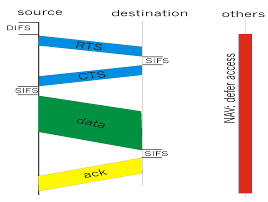
IEEE 802.11 MAC Protocol Overview: Handshaking

- 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
- avoid hidden station collisions



IEEE 802.11 MAC Protocol Overview: Handshaking

- RTS and CTS are short:
  - collisions of shorter duration, hence less “costly”
  - the final result is similar to collision detection
- DCF allows:
  - CSMA/CA
  - CSMA/CA with reservations

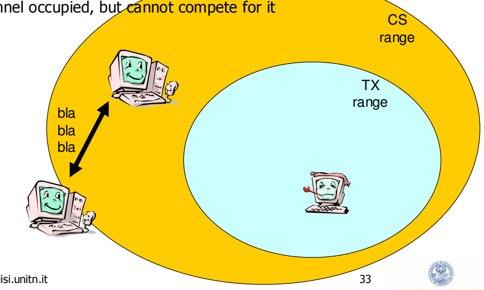


The DCF Access Scheme

- **Basic**
  - the simplest scheme
  - used when the data frames to be transmitted have a fairly short duration
- **With handshaking**
  - Uses additional control frames for channel access
  - Designed to solve the problems of hidden terminals
  - Provides higher reliability in data transmission

The exposed terminal problem

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



DCF
The Basic Access Mode

Carrier Sensing

- 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)

Network Allocation Vector (NAV)

- Used by the stations nearby the transmitter to store the duration of the frame that is occupying the channel
- The channel will become idle when the NAV expires
- Upon the NAV expiration, stations that have data to transmit listen to the channel again

Using DIFS and SIFS

- **Transmitter:**
  - senses the channel
  - if the channel is idle, it waits a time equal to DIFS
  - if the channel remains idle for DIFS, it transmits its MPDU

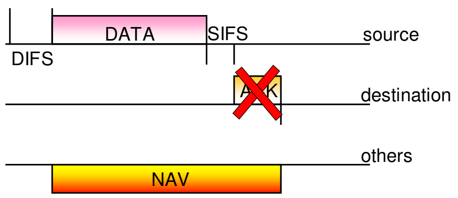
Using DIFS and SIFS

- **Receiver:**
  - computes the checksum thus verifying whether the transmission is correct
  - if so, it sends an ACK after a time equal to SIFS
  - it should always transmit an ACK with a 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

Using DIFS and SIFS

- **Neighbors:**
  - set their NAV to the value indicated in the transmitted MPDU
  - NAV set to: the MPDU tx time + 1 SIFS + ACK time

MPDU Transmission



Frame Retransmissions

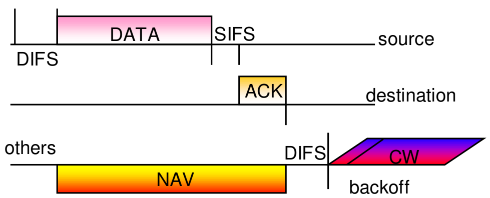
- A frame transmission may fail because of collision or errors on the radio channel
- A failed transmission is re-attempted till a max no. of retransmissions is reached
- ARQ scheme: Stop&Wait

Collision Avoidance (CA)

Backoff procedure

- If a station senses the channel busy, it waits for the channel becoming 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

MPDU Transmission



CW=Contention Window

Backoff Value

- 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 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, $CW_i \leq CW_{max}$

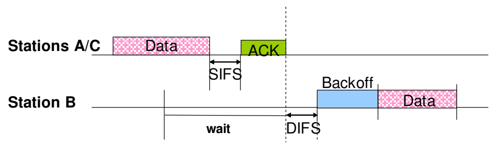
Backoff Decrease

- While the channel **is busy**, the backoff counter **is frozen**
- While the channel is idle, and available for transmissions the station decreases the backoff value (-1 every slot) until
  - the channel becomes busy or
  - the backoff counter reaches 0

Accessing the Channel

- If more than one station decrease their counter to 0 at the same time → collision
- Colliding stations have to recompute a new backoff value

Basic DCF: An Example



Data Fragmentation (1)

- A MSDU is fragmented into more than one frame (MPDU) when its size is larger than a certain **fragmentation threshold**
  - In the case of failure, less bandwidth is wasted
- All MPDUs have same size except for the last MPDU that may be smaller than the fragmentation threshold
- PHY header is inserted in every fragment → convenient if the fragmentation threshold is not too little

Data Fragmentation (2)

- MPDUs originated from the same MSDU are transmitted at distance of SIFS + ACK + SIFS
- The transmitter releases the channel when
  - the transmission of all MPDUs belonging to a MSDU is completed
  - the ACK associated to an MPDU is lost

Data Fragmentation (3)

- Contentio Window (Backoff counter) is increased for each fragment retransmission belonging to the same frame
- The receiver reassembles the MPDUs into the original MSDU that is then passed to the higher layers
- Broadcast and multicast data units are never fragmented

Recontending for the Channel

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

DCF
Access with handshaking

Access with Handshake

- 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

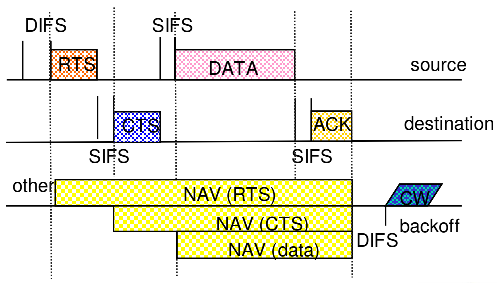
RTS/CTS

- Handshaking procedure uses the Request to send (RTS) and Clear to send (CTS) control frames
- RTS / CTS should be always transmitted @1 (6a/g/h) Mbit/s (they are only headers)
- Access with handshaking is used for frames larger than an RTS_Threshold

DCF with Handshaking

- 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

MPDU Transmission & NAV

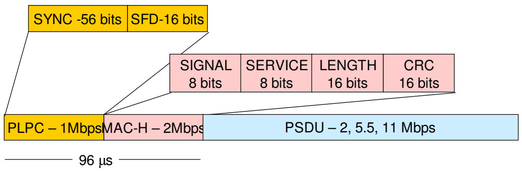


Examples of frame format

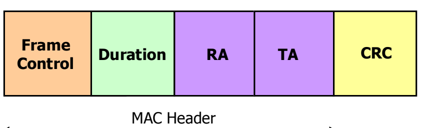
Generic DSSS (802.11b) packet

SFD – Start Frame Delimiter

PLPC – Physical Layer Convergence Protocol

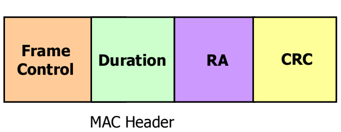


Example: RTS Frame



- **Duration** (in μs): Time required to transmit next (data) frame + CTS + ACK + 3 SIFs
- **RA**: Address of the intended immediate recipient
- **TA**: Address of the station transmitting this frame

Example: CTS Frame



- **Duration** (in μs): Duration value of previous RTS frame – 1 CTS time – 1 SIFS
- **RA**: The TA field in the RTS frame

Example: ACK Frame

Frame Control	Duration	RA	CRC

MAC Header

- **Duration**: set to 0 if More Fragments bit was 0, otherwise equal to the duration of previous frame – 1 ACK – 1 SIFS
- **RA**: copied from the Address 2 field of previous frame

Some Numerical Values…

- PHY_{HDR}: 16 bytes, transmitted @ 1 Mbps
- MAC_{HDR}: 34 bytes, transmitted @ 1 Mbps
  - If slot=20μs, PHY_{HDR}+ MAC_{HDR}=20 slots
- ACK=PHY_{HDR}+14 bytes , transmitted @ 1 Mbps
  - If slot=20μs, ACK=12 slots

Detailed MAC Format (bytes)

Frame Control	Duration ID	Address1 (source)	Address2 (destination)	Address3 (rx node)
2	2	6	6	6

Sequence Control	Address4 (tx node)	Data	FCS
2	6	0 - 2,312	4

MAC Format fields

Field	Bits	Notes/Description
Frame Control	15 - 14	Protocol version. Currently 0
	13 - 12	Type
	11 - 8	Subtype
	7	To DS. 1 = to the distribution system.
	6	From DS. 1 = exit from the Distribution System.
	5	More Frag. 1 = more fragment frames to follow (last or unfragmented frame = 0)
	4	Retry. 1 = this is a re-transmission.
	3	Power Mgt. 1 = station in power save mode, 1 = active mode.
	2	More Data. 1 = additional frames buffered for the destination address (address x).
	1	WEP. 1 = data processed with WEP algorithm. 0 = no WEP.
	0	Order. 1 = frames must be strictly ordered.

MAC Format fields

Field	Bits	Notes/Description
Duration ID	15 - 0	For data frames = duration of frame. For Control Frames the associated identity of the transmitting station.
Address 1	47 - 0	Source address (6 bytes).
Address 2	47 - 0	Destination address (6 bytes).
Address 3	47 - 0	Receiving station address (destination wireless station)
Sequence Control	15 - 0	
Address 4	47 - 0	Transmitting wireless station.
Frame Body		0 - 2312 octets (bytes).
FCS	31 - 0	Frame Check Sequence (32 bit CRC). defined in P802.11.