UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

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

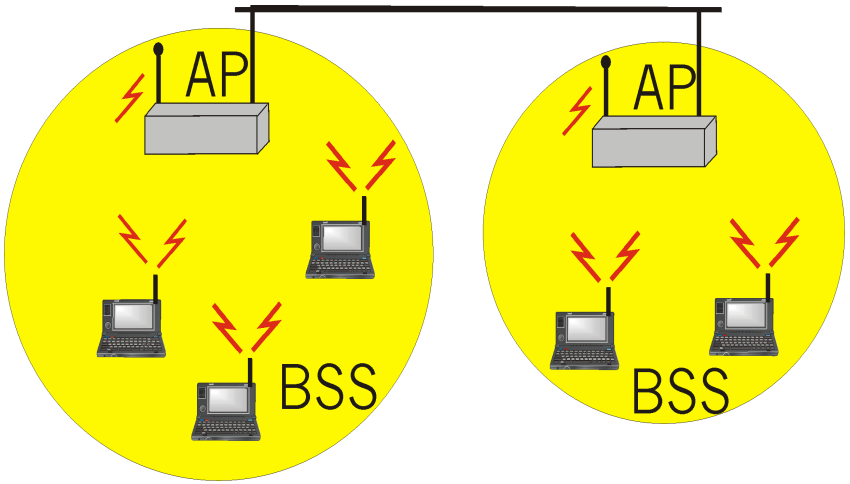
IEEE 802.11

- 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)

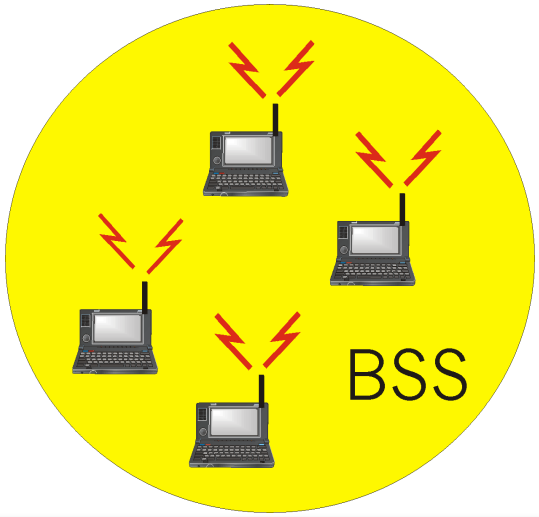
WLAN with Infrastructure

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



Ad Hoc WLANs

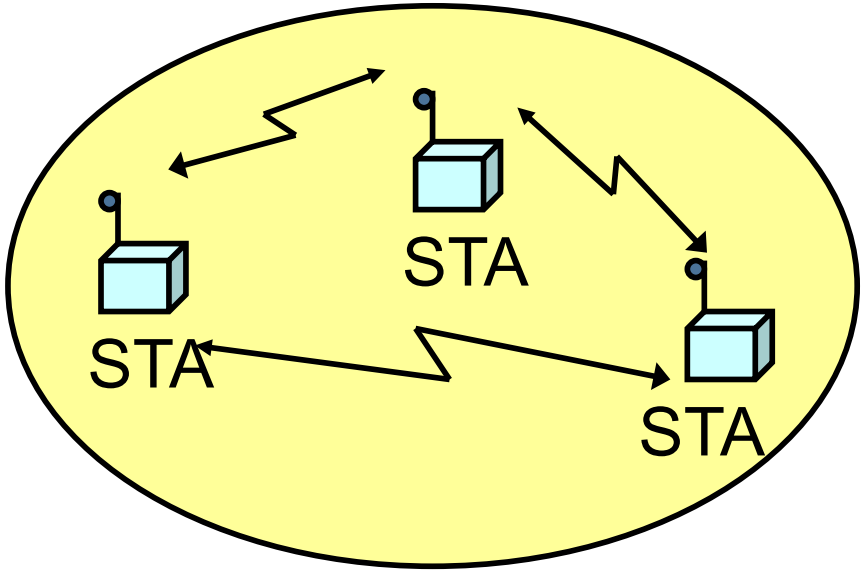
- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS
- Applications:
  - Vehicular Networks
  - Meeting in conference room
  - Interconnection of “personal” devices
  - Battlefield
  - ….
- IETF MANET (Mobile Ad hoc Networks) working group; VANET; V2V; V2X; ...



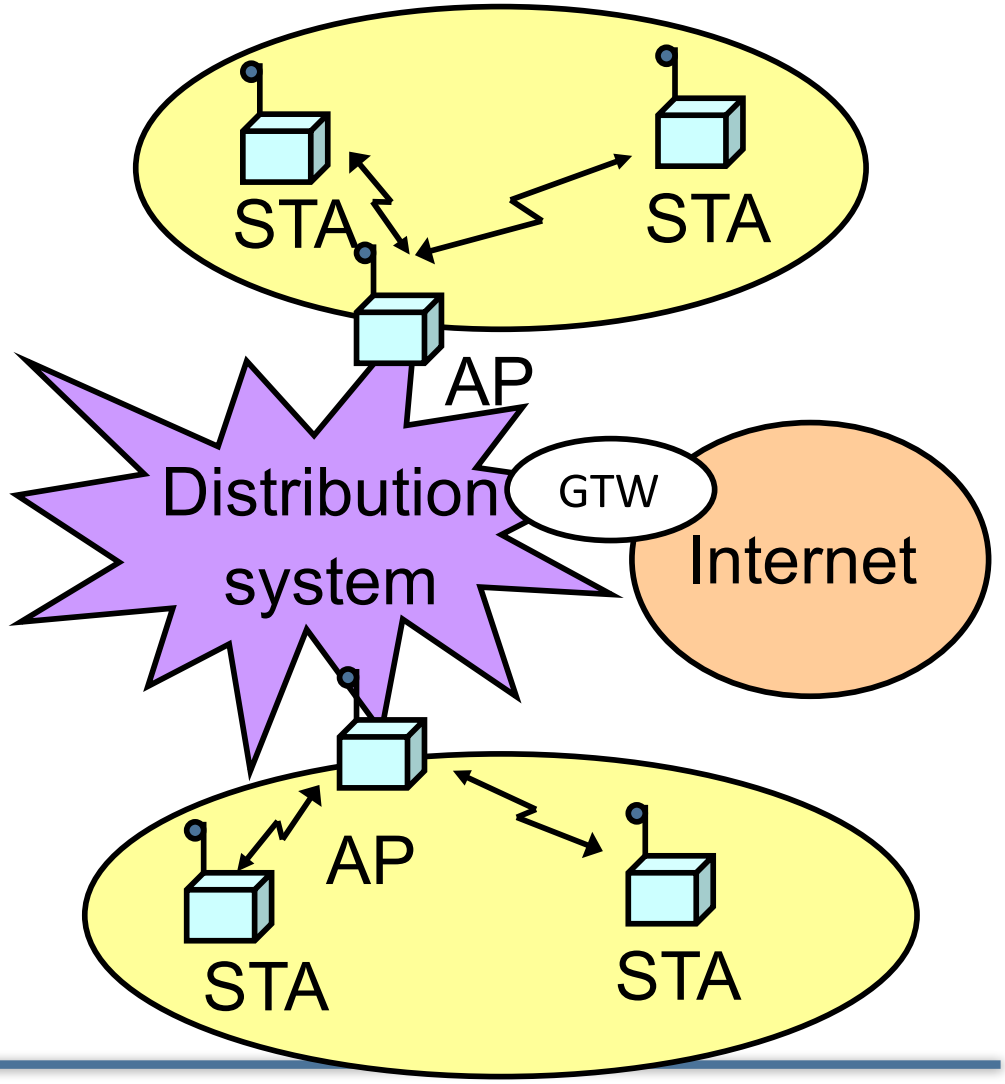
Extended Service Set (ESS)

- 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

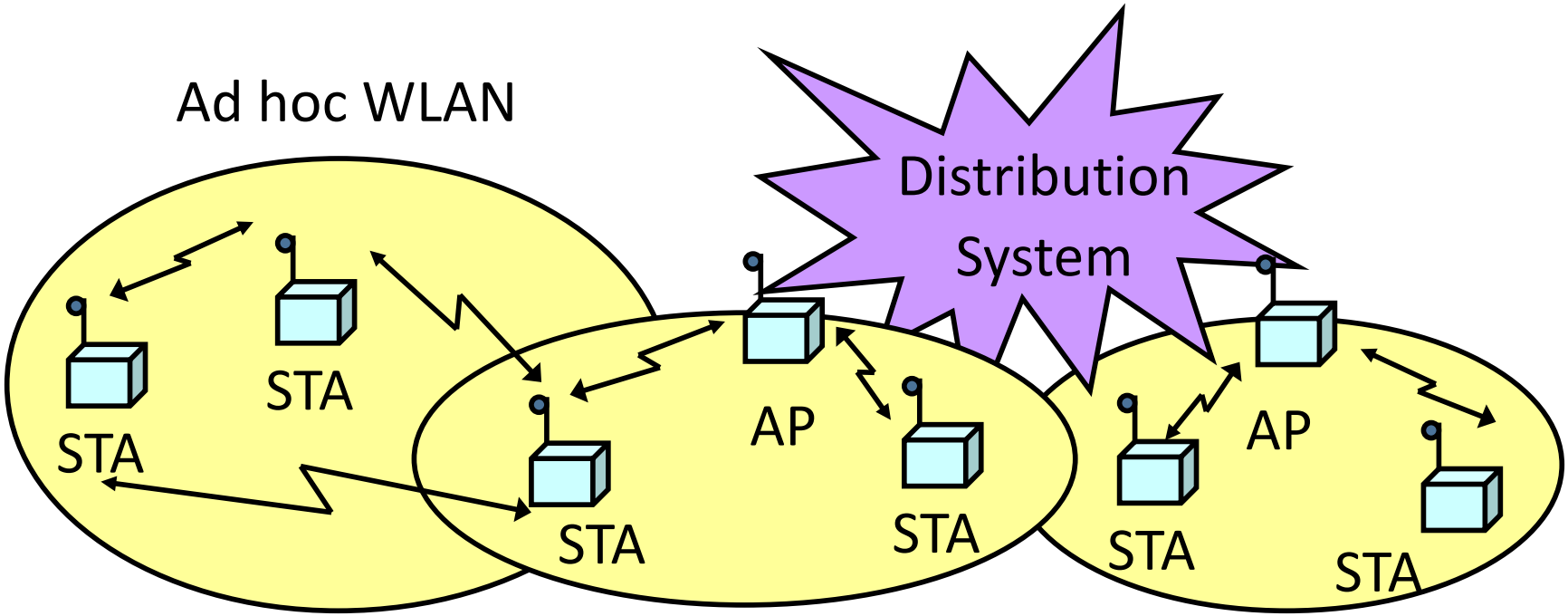
Ad hoc networking
Independent BSS (IBSS)



Network with infrastructure



Possible Scenarios (2)



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

- 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

UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

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

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
- 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

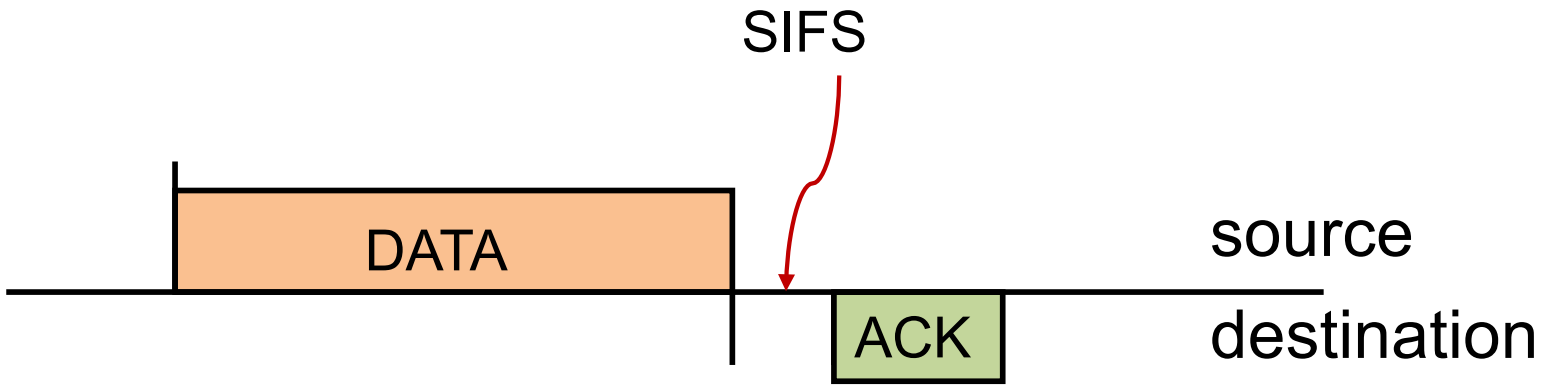
- The system is semi-synchronous
  - Maintained through Beacon frames (sent by AP)
- Time is counted in intervals called slots
- A slot is the system unit time
  - its duration depends on the implementation of the physical layer and specifically on the
  - 802.11b: 20μs
  - 802.11a/h/g/n/ac: 9μs
    - g/n are forced to use 20 when coexisting with b

UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

- 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



UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

- 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

- 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

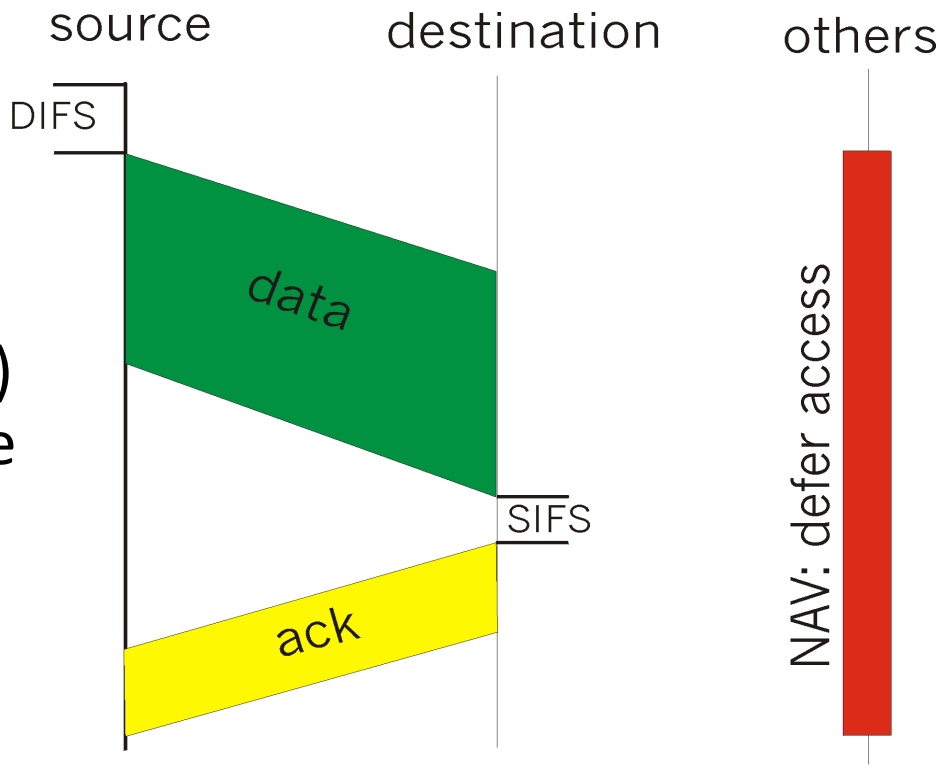
- if sense channel busy

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

802.11 CSMA receiver:

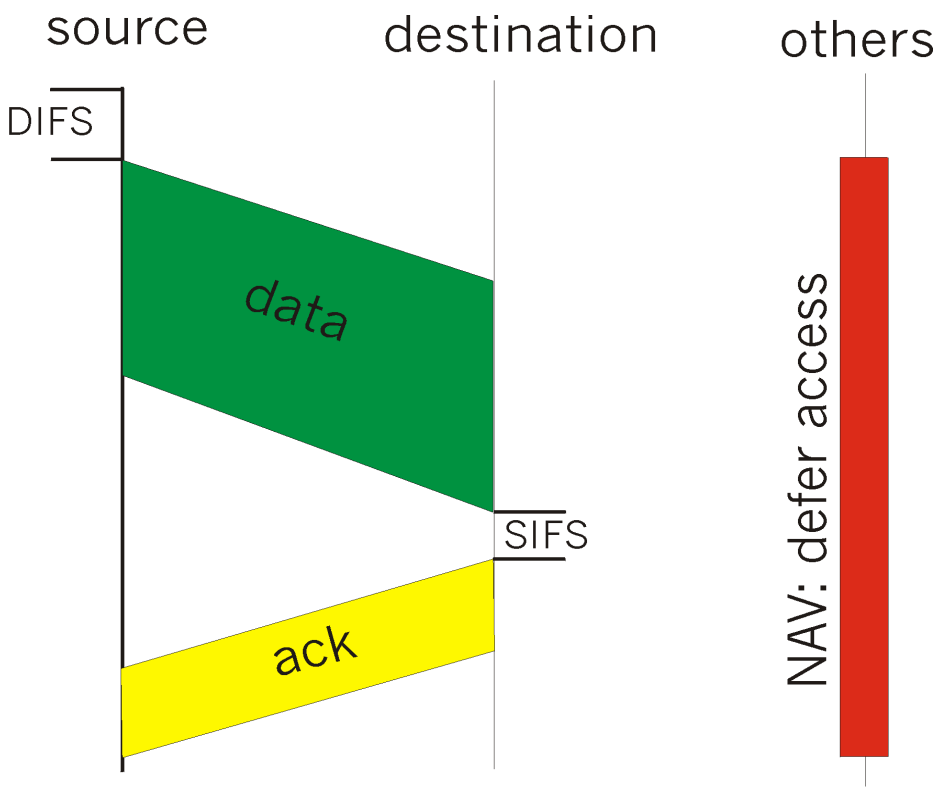
if received OK

return ACK after **SIFS**



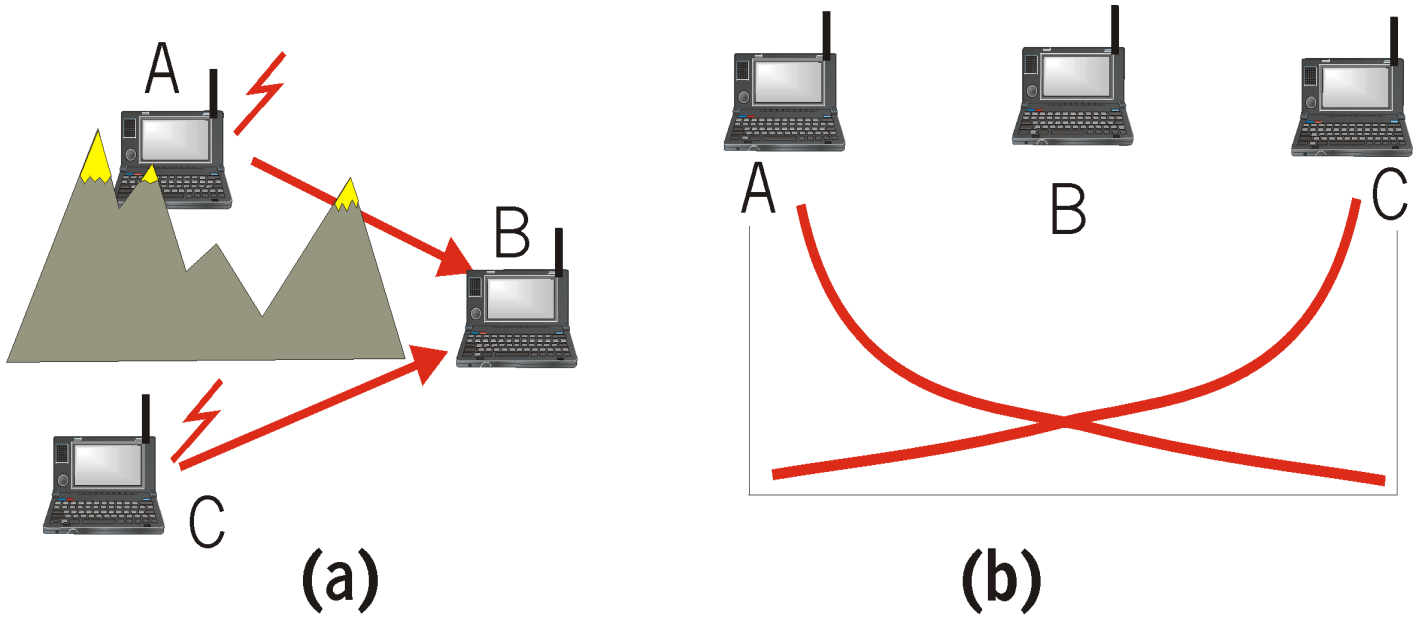
802.11 CSMA Protocol others:

- **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



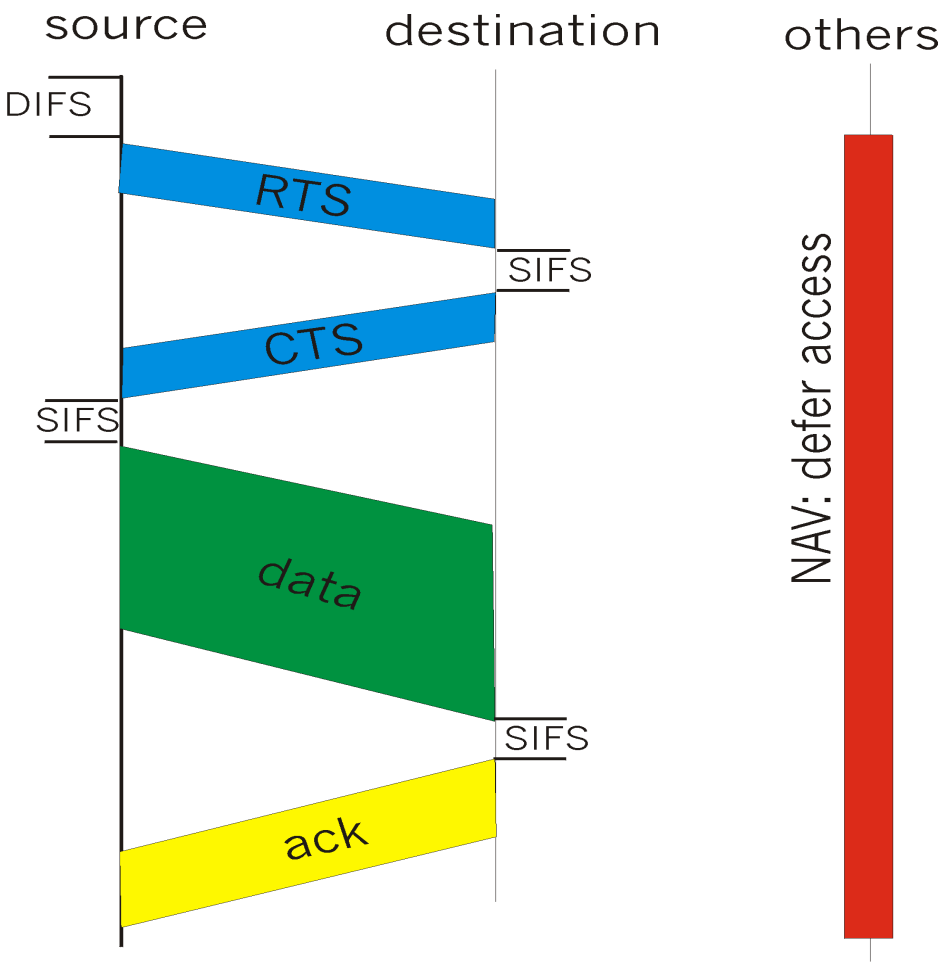
Hidden Terminal Effect

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

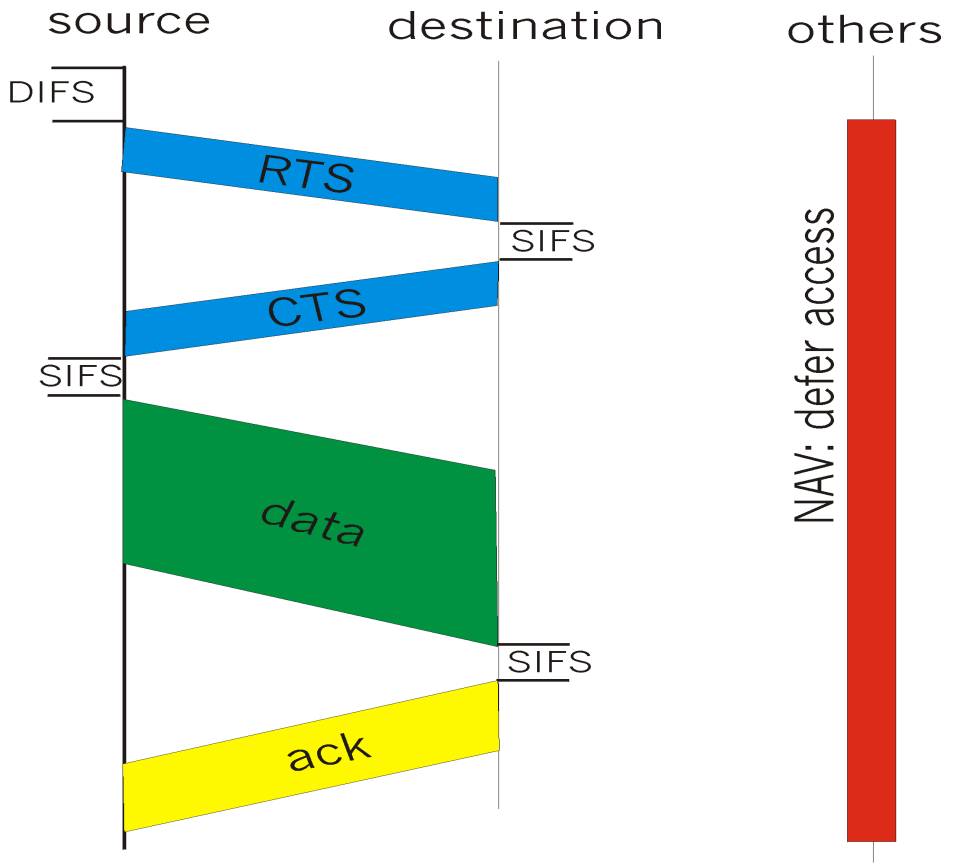


MAC Handshaking

- 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
- 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



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