Wireless Local Area Networks: WLANs

University Carlos III of Madrid
Service Engineering Laboratory

Antonio de la Oliva
Jaume Barceló
Ruben cuevas
Ignacio soto

Lecture plan

- Introduction
  - Origins
  - Properties
- Wireless local-area network technologies:
  - Topology and structure
  - Physical medium
  - MAC layer protocols
  - Security
- IEEE 802.11
- Other standards
- Conclusions

Introduction: What is a Wireless LAN Network ?

- Wireless:
  - Transmission is without cables.
  - Radio- or infrared communications.
- Local-area networks:
  - Coverage (range) is limited (~ 50m).
    e.g. in building on campus
  - Speed of mobility of wireless devices limited by size of cells.

Introduction: Why go wireless ?

- No need for cables:
  - High flexibility (changes, terminal additions, …)
  - New cabling infrastructure expensive and difficult to deploy in existing buildings.
  - WLAN can be installed in relatively short time with minimum planning (mobile equipment, temporary installations, …)
  - Resilient to damage from natural disasters (earthquakes, fire)
  - Adding a user is a matter of authorization, no need of new infrastructure

Introduction: Why not get rid of wired LANs?

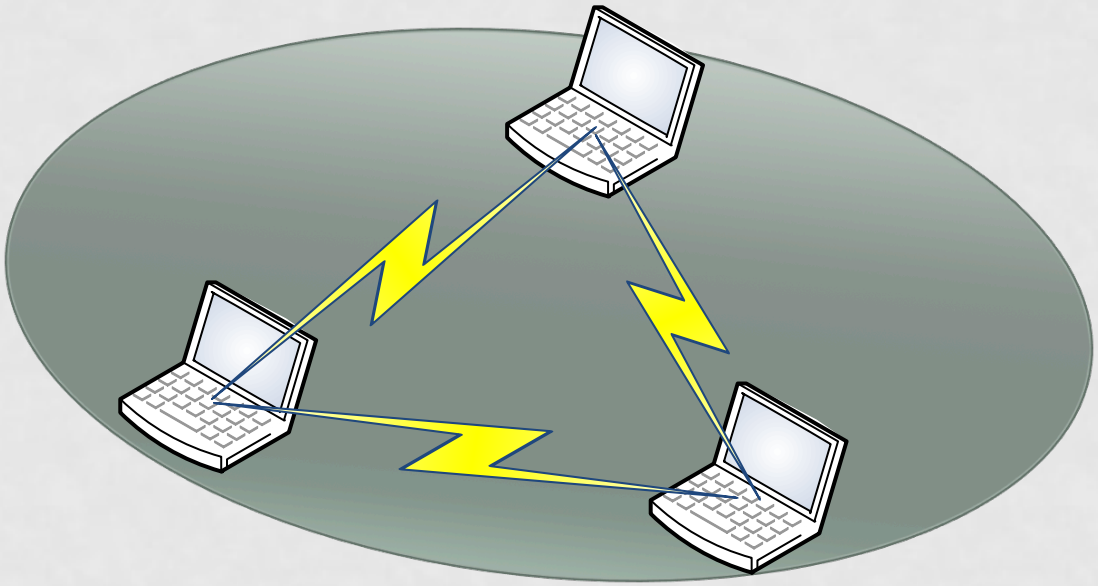
- Offer higher bandwidth
- Long time available in the market
  - Proven interoperability
  - No proprietary solutions
- WLANs uses wireless medium
  - Scarse
- Quality of transmission difficult to guarantee, spectrum is a shared resource
- Lack of physical boundary, security implications
- Dynamic physical medium
  - Physical medium changes a lot
  - Losses, fading, interferences, channel planning

Introduction: What do we expect from WLANs?

High speed transmission	54 Mbps at most (VHT?)
Low cost	Compared with ethernet card?
Ability to provide coverage to buildings, campuses and open spaces	Difficult to determine the coverage
Low power consumption (usage with laptops)	Still looking for energy efficient solutions
Robustness , low interference, compatibility with existing wireless and wired networks (i.e. Bluetooth)	No way…
Easy instalation, configuration and use	Ok, unless it is not
Support for secure communications	WPA2 maybe (GPU attacks)
Safety (health)	Nothing has proved they are bad
Transparency for higher-layer protocols	But not very efficient (TCP over wireless)

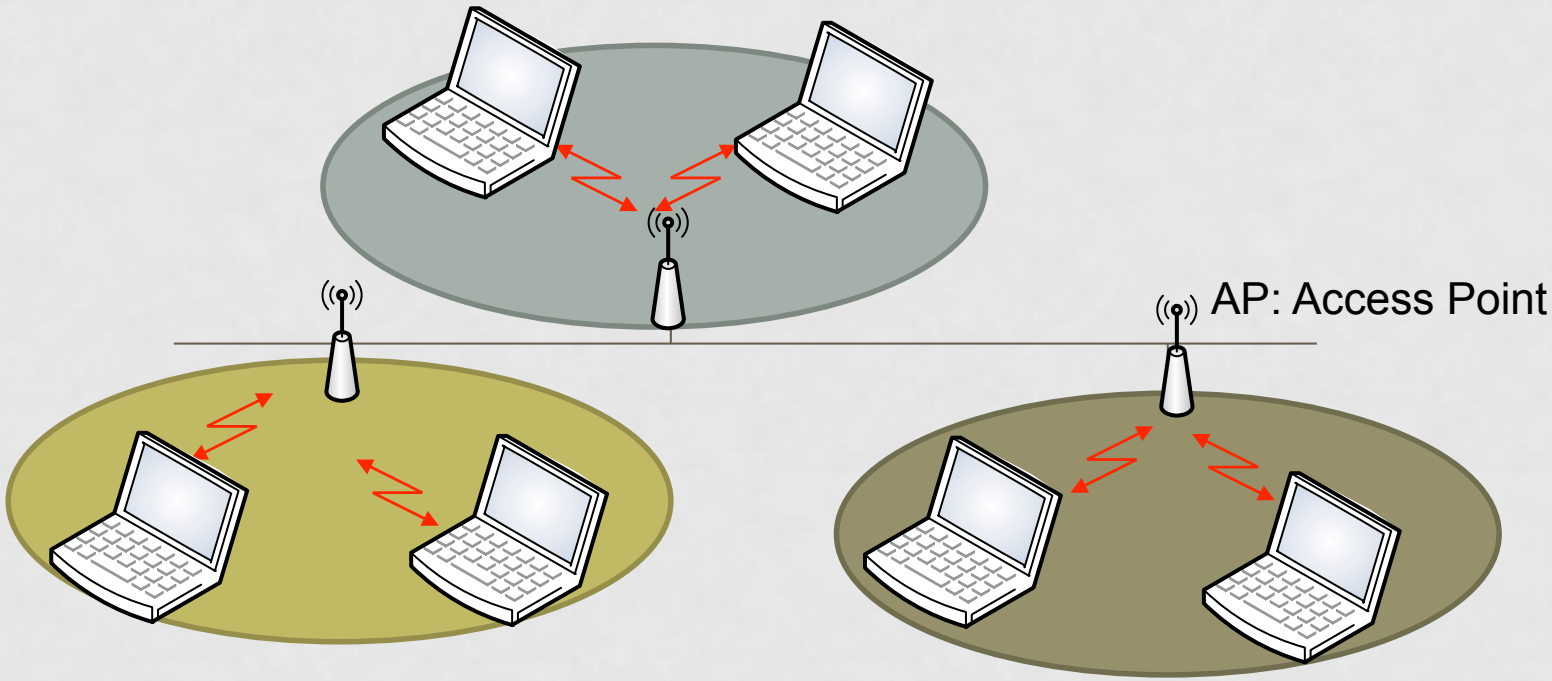
Topologies of wireless networks

- Independent mode (ad-hoc):



Topologies of wireless communications networks

- Infrastructure mode (managed mode):



Technology: Physical medium Infrared or Radio

- IR: 10^{12} to 10^{15} Hz
- Higher frequency, hence more attenuation
- AP in each room
- Interferences with sun or other sources of heat
- Short range: low interference, more secure
- Unlicensed band
- Cheap IR transmiters/receivers
- Low bandwidth
- Example: IrDA (Infrared Data Association)

- Radio: 2,4 GHz, 5 GHz
- Can go through walls. Coverage: ~50m (Depends on the wall)
- AP can cover several rooms
- Interferences with electrical appliance, microwaves, lights, no transmission through the fridge
- Security problems due to propagation distances
- Regulated spectrum (FCC – Federal Telecommunications Commision, CEPT – Conference of European PTs)

ISM(industrial,scientific and medical)Bands

Band	Frequency range
UHF ISM	902-928 MHz
S-Band	2-4 GHz
S-Band ISM	2.4-2.5 GHz
C-Band	4-8 GHz
C-Band satellite downlink	3.7-4.2 GHz
C-Band Radar (weather)	5.25-5.925 GHz
C-Band ISM	5.725-5.875 GHz
C-Band satellite uplink	5.925-6.425 GHz
X-Band	8-12 GHz
X-Band Radar (police/weather)	8.5-10.55 GHz
Ku-Band	12-18 GHz
Ku-Band Radar (police)	13.4-14 GHz 15.7-17.7 GHz

Technology: Physical medium for radio communications

- ISM band (Industrial, Scientific, and Medical): 2,4 GHz. Use on conditions of a secondary user:
  - Techniques for spread spectrum
  - Limits to transmitted power
- In Europe: frequency band 150 MHz at 5,1 GHz originally for HiperLAN, now open for other standards
- Unlicensed-PCS: in USA, frequency band for use as primary user. No need to get license (2,39 GHz; 5,1GHz)

FHSS and DSSS

- Techniques for efficient spectrum utilisation
- FHSS (Frequency Hopping Spread Spectrum) :
  - Frequency band is divided into channels.
  - In subsequent time intervals data is sent in one of these channels.
  - The receiver has to follow the frequency hops.
    Different channels are distinguished by different hop pattern.
- DSSS (Direct Sequence Spread Spectrum) :
  - Digital data bits are multiplied by a certain value (spreading code)
  - Each bit of data is converted into several bits (chips)
  - The frequency spectrum needed to carry encoded data is broaded for encoded data than for original digital signal.
  - The receiver uses the same spreading code to 'decode' the original signal out of the encoded one.
- OFDM (Orthogonal Frequency Division Multiplexing)
  - The future and present of wireless communications
  - FDM technique for transmitting large amounts of digital data over a radio wave
  - OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver.
  - Reduces interference by shuting down sub-carriers

Benefits of Spread Spectrum

- The transmission energy of the encoded signal can be low.
- Broadband frequency spectrum is resilient to high-energy selective interferences which typically concentrate at some specific frequencies.
- FHSS allows for more communication channels, but lower data bitrates than DSSS. DSSS is extremely bad at interference (in reality). OFDM is the modulation used in reality

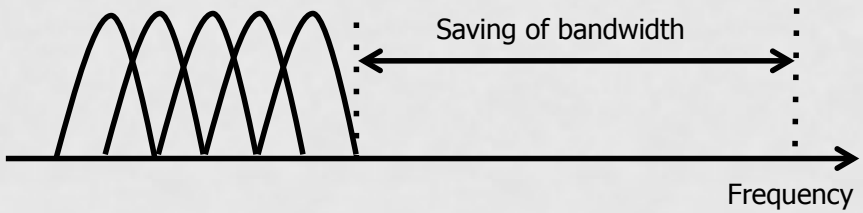
The OFDM Signal

Conventional FDM

- In a conventional Frequency Division Multiplexing system (FDM), the different sub-carriers are separated by guard bands so that the signals can be received using conventional filters and demodulators. This results in a reduction of spectral efficiency.

Orthogonal FDM

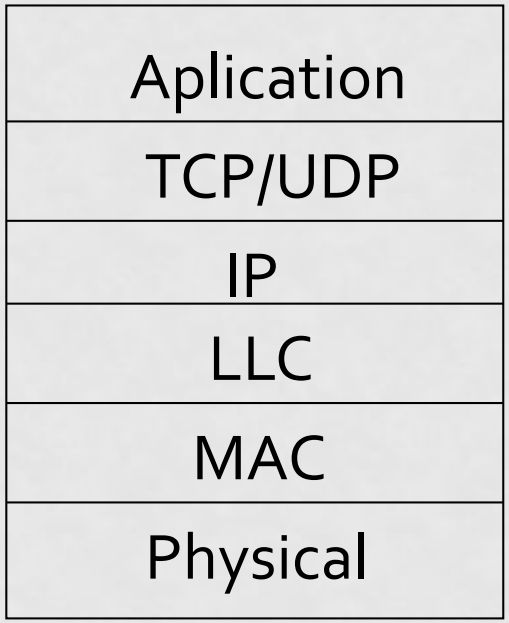
- It is possible to overlap the sub-carriers and still be able to receive them with no interferences. For this, the sub-carriers must be mathematically orthogonal.



- The subcarriers will be orthogonal if their spacing is a multiple of the inverse of its symbol period.

Medium Access Control protocols

- TCP– Transmission Control Protocol
- IP– Internet Protocol
- LLC – Logical Link Control
  - Multiplexing protocols transmitted over the MAC layer (when transmitting) and de-multiplexing them (when receiving).
  - Providing flow and error control
- MAC – Medium Access Control:
  - how to share a channel between several users.

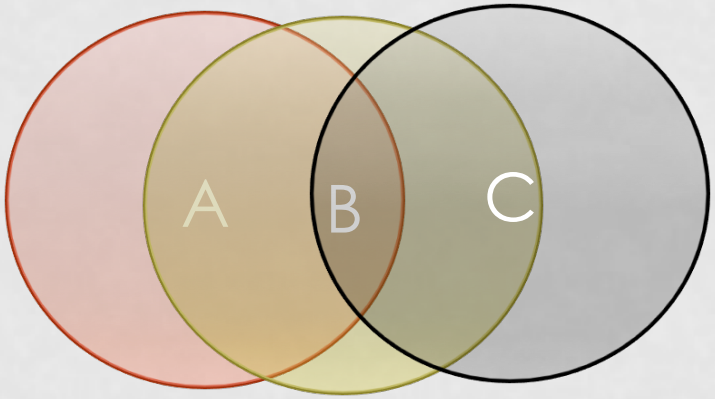


Medium Access Control protocols

- WLANs rely on *contention-based* MAC protocols :
  - Efficient sharing of radio resource
  - Side effect: variable transmission delay
- CSMA/CD: CSMA with collision detection.
  - This protocol is used in Ethernet (IEEE 802.3):
  - Detect the collision and abandon (stop) transmission
    - Required listen while transmitting
    - Jam signal
- CSMA in a radio channel:
  - It is not feasible to do collision detection in WLAN medium
    - You are receiving or transmitting but cannot do both things at the same time
  - Difficult to decide at what signal level it is considered that the channel is busy.

Medium Access Control protocols

- Hidden station problem:



- A listens to B and C listens to B, B listens to both A and C, but C and A do not hear each other !
- Loss of performance: CSMA degenerates to Aloha.

Security in WLANs

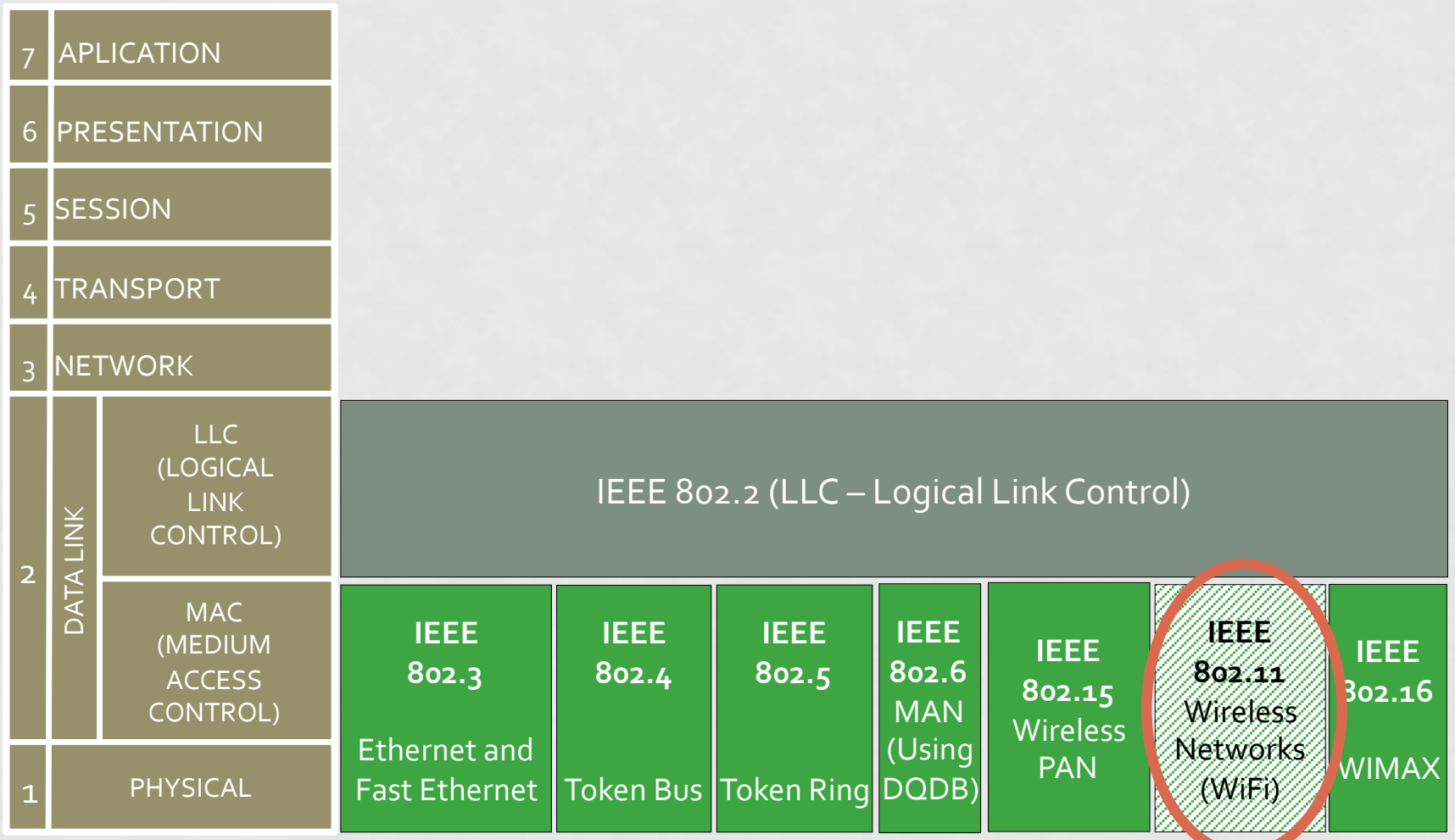
- Are wired networks secure ?
- WLANs are not as secure.
  - The problem has been considered since the beginning
- Two issues:
  - Station authentication to avoid intruders misuse of the network resources.
  - Privacy of information (encryption)
- Public key, symmetric or mixed ciphering systems.
- We will see more of this later

IEEE 802.11 overview

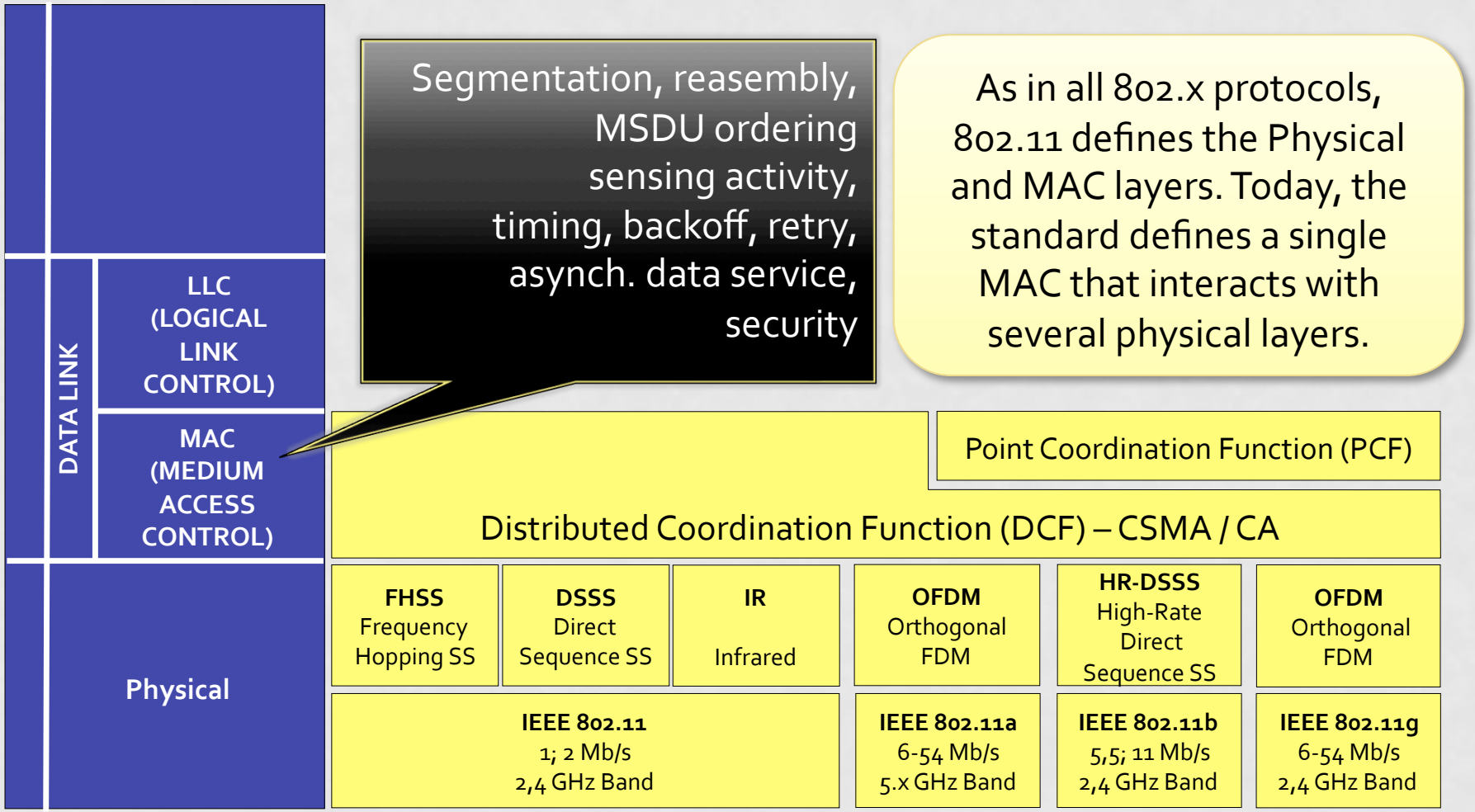
- IEEE standard to facilitate connectivity of fixed and portable/ mobile stations that change their point of attachment between LANs
- The standard defines the PHY and MAC layers

Application		
TCP/UDP		
IP		
LLC	←	segmentation, reasembly
MAC	←	sensing activity, timing, backoff, retry, asynch. data service..
PHY	←	modulation, transmission

IEEE 802.x Protocol Family



IEEE 802.11


DATA LINK
LLC (LOGICAL LINK CONTROL)
MAC (MEDIUM ACCESS CONTROL)
Physical
Segmentation, reasembly, MSDU ordering sensing activity, timing, backoff, retry, asynch. data service, security
As in all 802.x protocols, 802.11 defines the Physical and MAC layers. Today, the standard defines a single MAC that interacts with several physical layers.
Point Coordination Function (PCF)
Distributed Coordination Function (DCF) – CSMA / CA
FHSS Frequency Hopping SS
DSSS Direct Sequence SS
IR Infrared
OFDM Orthogonal FDM
HR-DSSS High-Rate Direct Sequence SS
OFDM Orthogonal FDM
IEEE 802.11 1; 2 Mb/s 2,4 GHz Band
IEEE 802.11a 6-54 Mb/s 5.x GHz Band
IEEE 802.11b 5,5; 11 Mb/s 2,4 GHz Band
IEEE 802.11g 6-54 Mb/s 2,4 GHz Band

IEEE 802.11 overview

- Characteristics of the standard:
  - Supports transmission of asynchronous data and with real-time requirements
  - Service continuity in extended areas through the use of a distribution system
  - Transmission speeds:
    - IEEE 802.11: 1 and 2 Mbps;
    - IEEE 802.11b: 1, 2, 5,5 and 11 Mbps
    - IEEE 802.11g: 11b + 6; 12; 24 Mbps - mandatory
    - 36; 48; 54 Mbps - optional
  - Coverage:
    - closed-space area: 25 a 50 m,
    - open-space area: 160 a 550 m
  - Supports broadcast and multicast
  - Network management services
  - Registration and authentication services

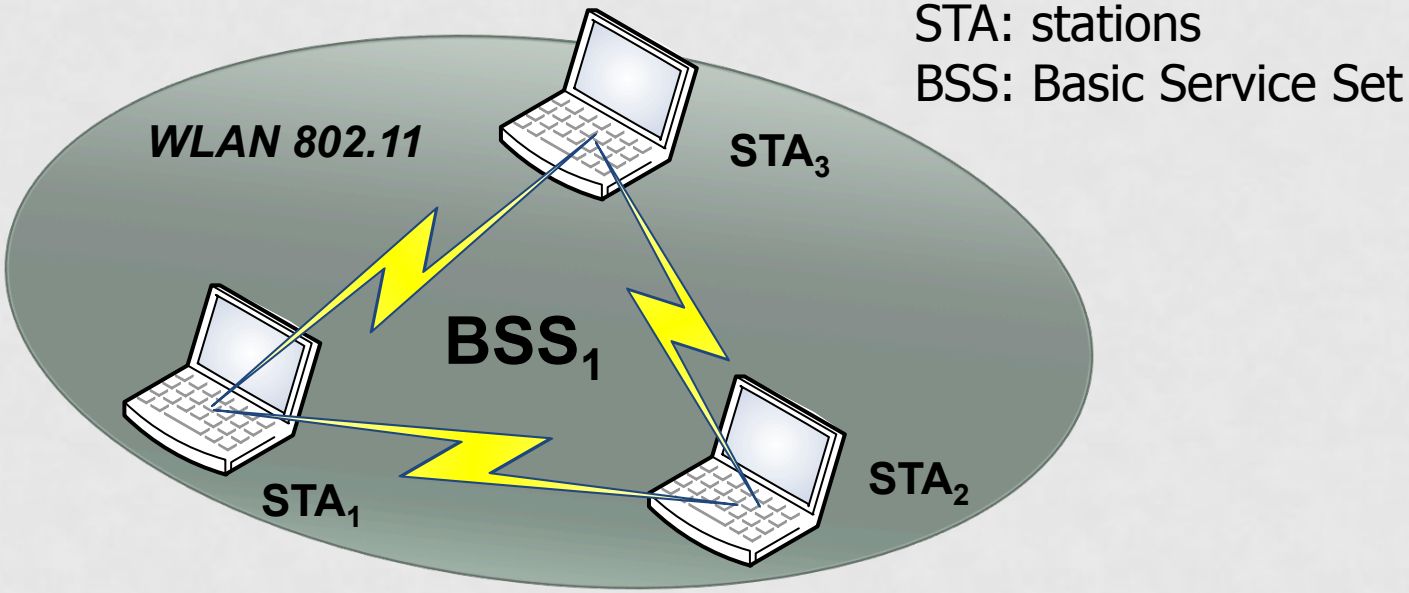
IEEE 802.11

Some important aspects covered in the standard relative to wireless characteristics:

- Power-saving requirements
  - MAC layer of IEEE 802.11 supports functions for stations to save battery when they're idle.
- Frequency bands
  - Radio frequency is in ISM at 2,4 GHz and 5 GHz. Allows for bitrates up to 54 Mbps (g version)
- Security features

IEEE 802.11: architecture

- Ad-hoc network or independent mode (IBSS)



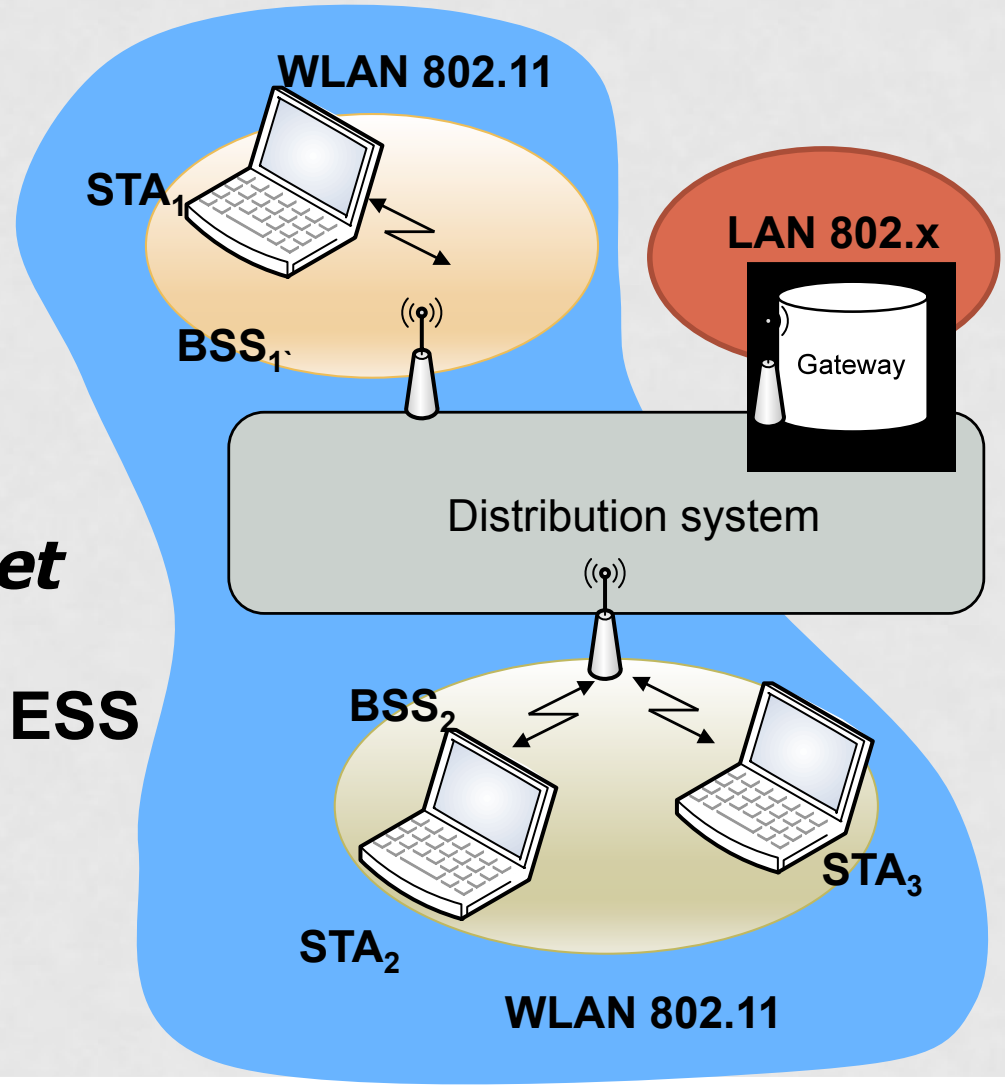
Infrastructure

- All communications go through the AP. This reduces the available capacity
- The distance with the AP is important, the distance between the nodes is not important unless hidden node problem
- Allows power saving, since there is an entity in charge of the communication
- An station can only be associated to one AP
- Requires an association process

IEEE 802.11: architecture

- Intrastructure mode:

ESS: Extended Service Set



Distribution Service

- A user can move within an ESS IEEE 802.11
- All AP connected to a L2 backbone
- The gateway connecting the ESS to the external world communicates with the stations using their MAC address, independently from the AP the station is connected to
- All APs talk between them to distribute the list of attached users. This protocols usually are proprietary (IAPP)
- No standardized protocols for this, the standard only defines functionality
- The distribution system (backhaul) can be wireless, but 1 hop at IP level
- No mobility between ESS, only between BSS

IEEE 802.11: Layers and functions

- MAC layer:
  - Medium access mechanisms, fragmentation, ciphering, packet retransmission, acknowledgements.
  - Management functions: synchronization, roaming, power management (battery), MIB
- PHY layer. 2 sub-layers:
  - PLCP – Physical Layer Convergence Protocol: CCA (Clear Channel Assessment)
  - PMD – Physical Medium Dependent: modulation and bit coding
  - Management functions: MIB and channel selection

IEEE 802.11: physical layer

- IEEE 802.11: IR, FHSS and DSSS
- IEEE 802.11b
  - DSSS
  - ISM band a 2,4 GHz. 14 channels available (depends on country, in Europe: 13). Only 3 non-interfering (ie. 1-6-11)
  - Modulation: Baker codes (1 and 2 Mbps) and Complementary Code Keying – CCK (5,5 and 11 Mbps)
  - Máximum power: 100 mW in Europe
- IEEE 802.11g
  - DSSS and OFDM (orthogonal frequency division multiplexing)
  - ISM band in 2,4 GHz. 14 channels available (some countries, in Europe 13). Only 3 without overlap (e.g. 1-6-11)
  - Modulation:
    - DSSS (constellations: DBPSK, DQPSK): Baker codes (1 y 2 Mbps) and complementary code keying –CCK- (5,5 y 11 Mbps)
    - OFDM (52 sub-carriers using BPSK, QPSK, 16-QAM or 64-QAM constellations and FEC codes): 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Physical layer: Interference

- 802.11b, 802.11g, OpenAir, HomeRF and Bluetooth operate in the same 2,4 GHz band.
  - Possibility of interference. Interference degree depends on several factors, including:
    - Distance between devices
    - Interference immunity rejection offered by each radio technology
- 802.11a operates in the 5 GHz band.
  - Can coexist with all 2,4 GHz standards without interferences. However, in Europe there are military devices in the band.
  - European 802.11a version: 802.11h – dynamic power control plus dynamic channel selection.
- El 802.11g is compatible with 802.11b

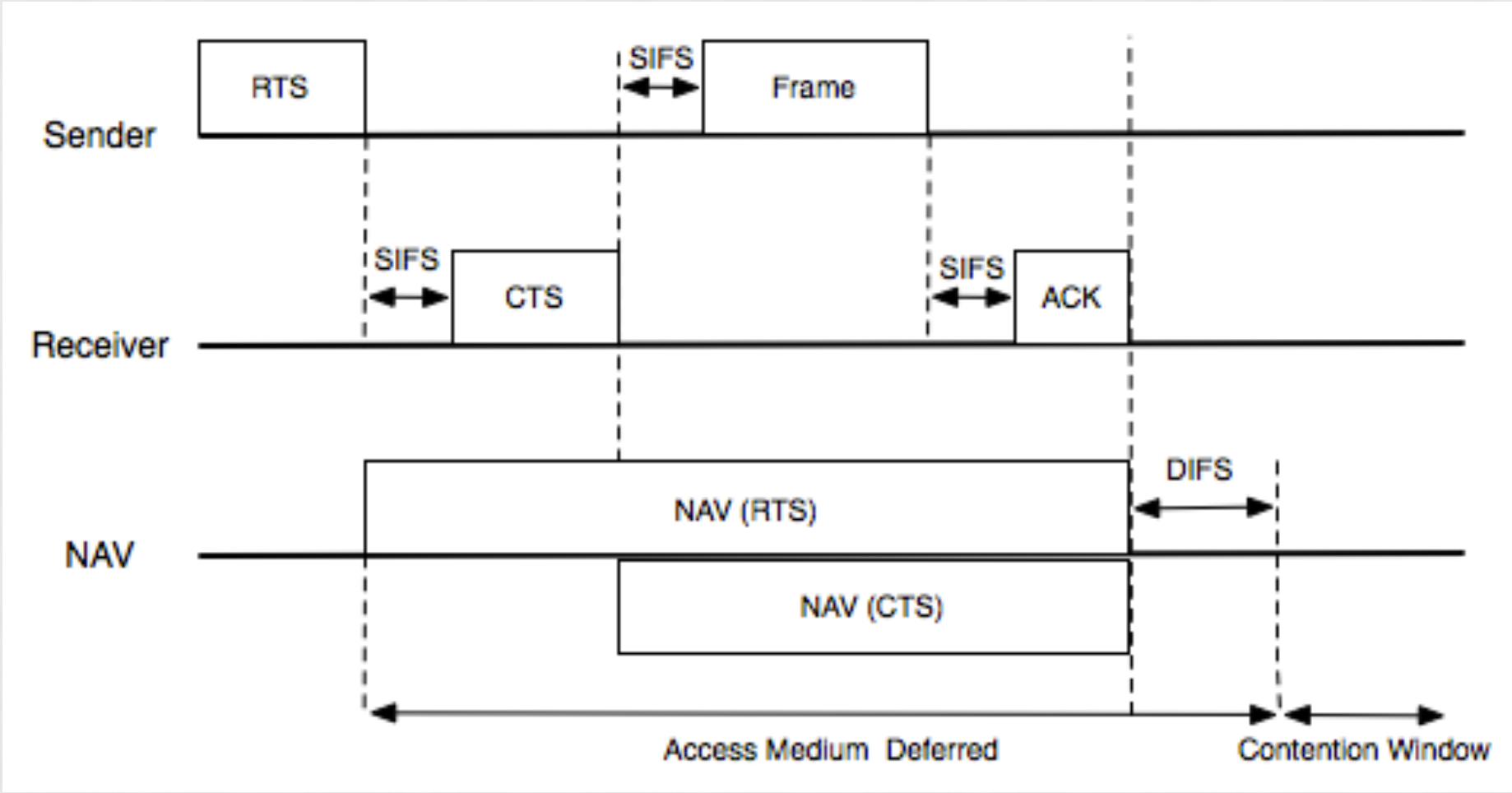
Access Control mechanisms in IEEE 802.11

- Two modes of access for two data transmission services:
  - Asynchronous Data Service
    - Data transmitted as "best-effort".
    - Implemented using the Distributed Coordination Function (DCF).
  - Real-time services
    - Implemented using thePoint Coordination Function (PCF)

Virtual Carrier Sensing

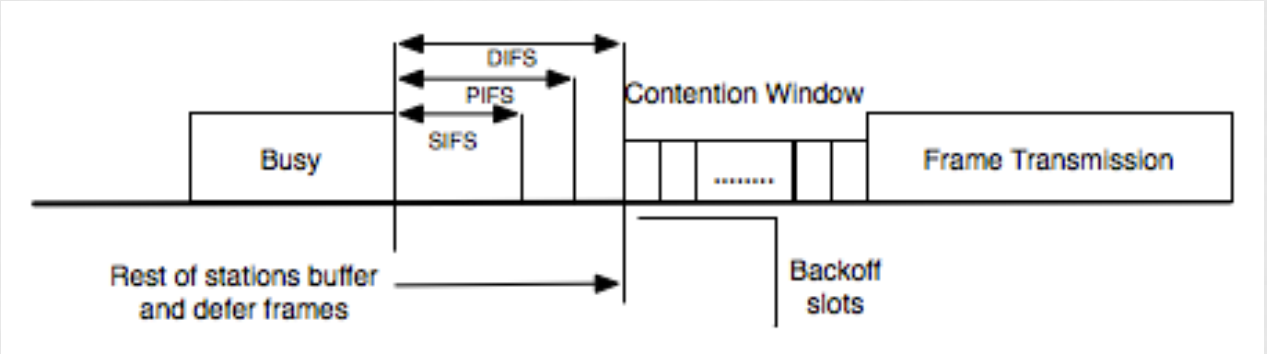
- In radio systems it is difficult to detect collisions since the transceivers can only work in transmission or reception separately
- The Network Allocating Vector is used for the detection of virtual carrier
- NAV indicates the time the channel is reserved for a certain transmission
- While sending a packet the NAV is set to the time reserved for this transmission and the rest of stations count to 0
- While trying to transmit if the NAV is different from 0, the channel is busy

Virtual Carrier Sensing



IEEE 802.11: MAC timing

- Slot Time: an slot time is the amount of time requied for a station to determine if another station has acceded to the medium at the beginning of the time slot.
- Intervalos entre tramas:
  - SIFS (Short Inter Frame Space): Divide frames belonging to the same dialogue. It is equal to the minimum time required to switch between Rx and Tx plus MAC processing.
  - PIFS (Point Coordination IFS): SIFS + 1 time slot. The AP uses this time to gain priority while accessing the medium. It is used in PCF.
  - DIFS (Distributed IFS): PIFS + 1 intervalo de tiempo (2Ts+SIFS). Time between frames that a station must wait before starting a new transmission.
  - EIFS (Extended IFS): Waiting time of a station receiving a frame that it cannot decode.



802.11 Medium access mechanism for asynchronous data

- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):
  - A station which wants to transmit should listen to the medium and defers transmission if medium is busy.
  - If the medium is free during DIFS units of time, the station can begin transmission
  - Reception is confirmed with acknowledgement.
  - Exponential backoff mechanism is used to reduce the number of collisions.
  - Backoff takes place in the following situations:
    - busy medium was sensed,
    - after each transmission,
    - after each retransmission.

IEEE 802.11: MAC level

- If medium is free more than DIFS, the station can transmit immediately (taking NAV into account)
  - If previous transmission was without errors, wait DIFS
  - Otherwise, wait EIFS
- If medium is busy, wait DIFS and perform exponential backoff.

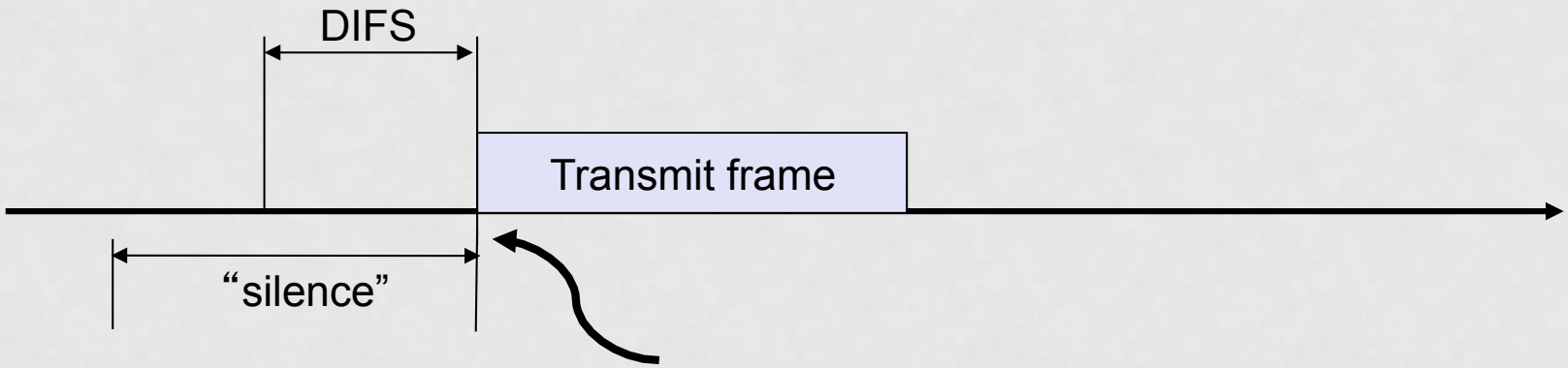
IEEE 802.11: MAC level

- Error recovery depends on the station sending the frame, ACK for each frame is expected.
  - The only indication of success is the ACK, if fragmentation is needed, ACK per fragment is expected.
  - Broadcast and multicast are not ACK.
  - Each transmission failure increases a counter. Once the maximum of the counter is reached the frame is discard.

IEEE 802.11: MAC level

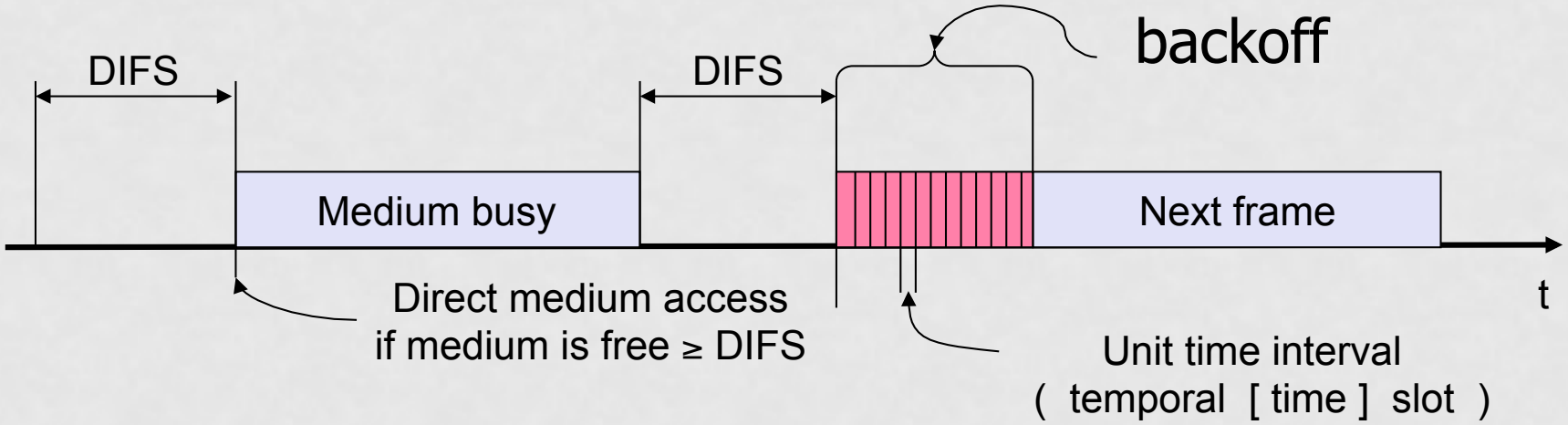
- Transmission of frames requiring fragmentation must update the NAV on each fragment transmission.
- ACKs, CTS (RTS/CTS) and fragments are sent using SIFS.

IEEE 802.11: Collision Avoidance

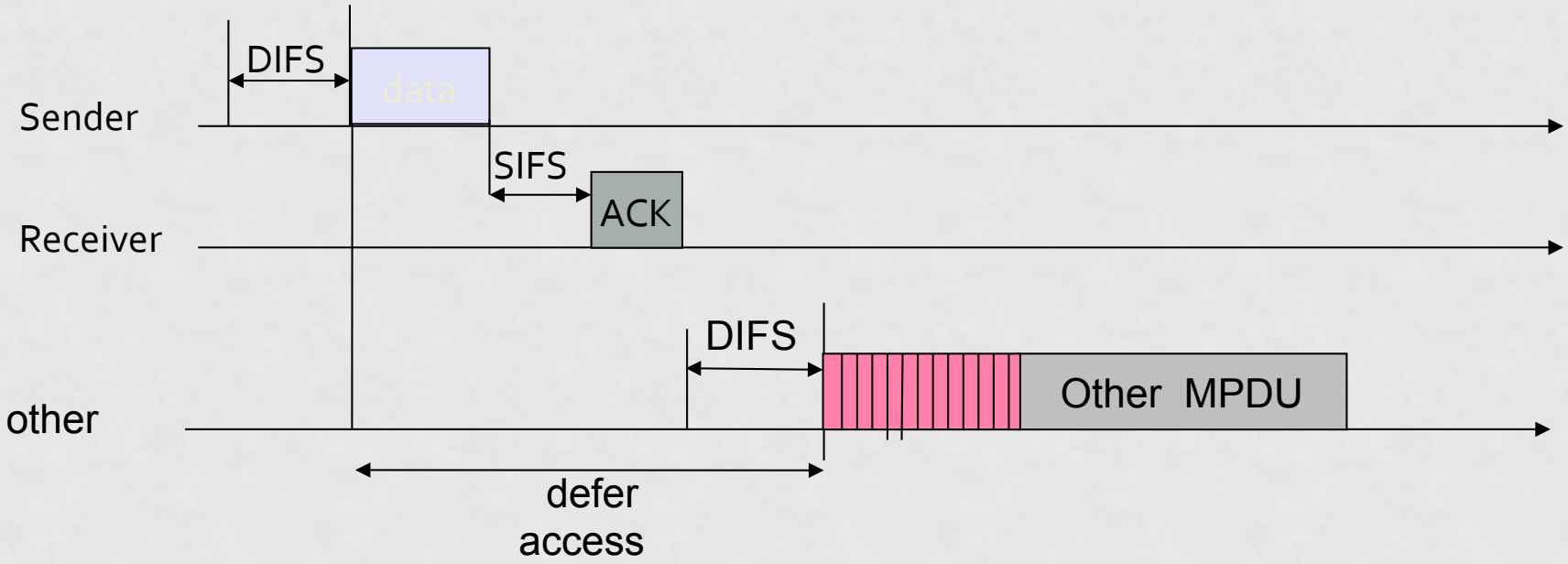


IEEE 802.11: ACK

IEEE 802.11: Backoff



IEEE 802.11: CSMA/CA with ACK



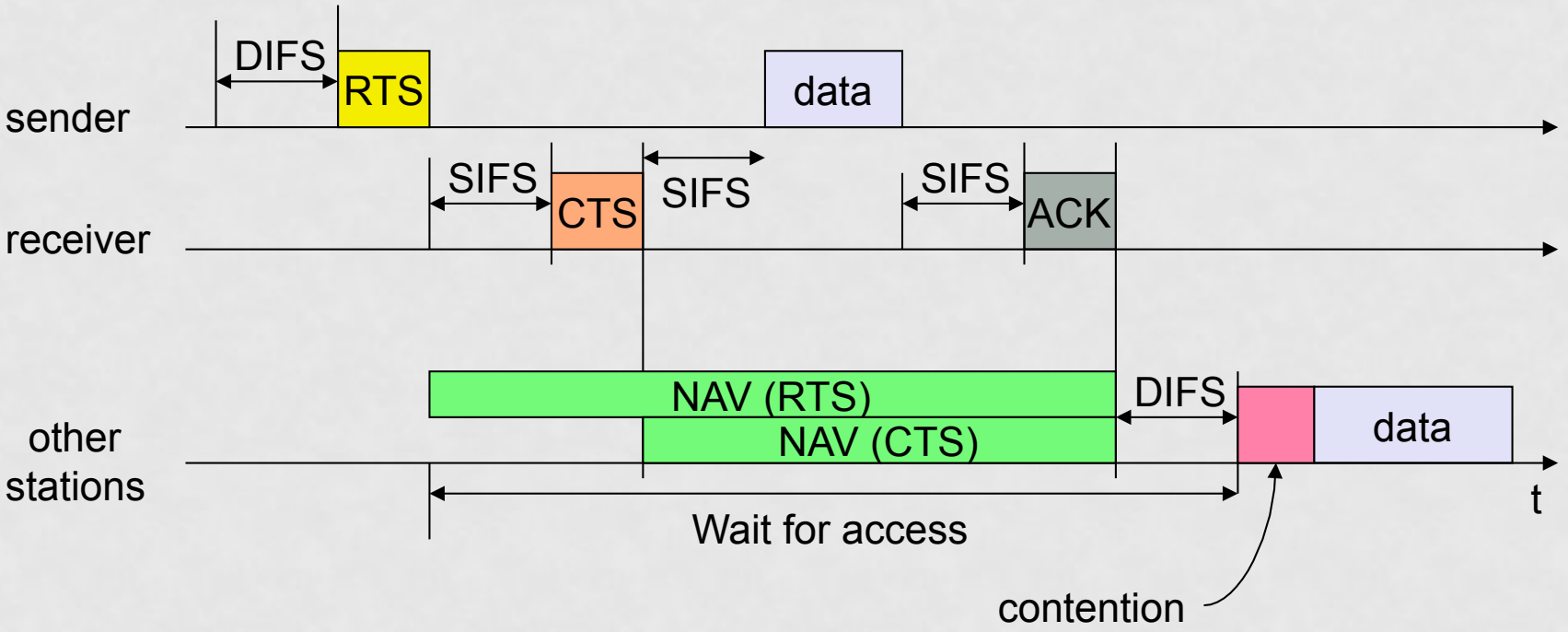
802.11 Medium access mechanism for asynchronous data: variant 2

- Virtual Carrier Sense: RTS + CTS to solve the problem of hidden stations:
  - Use is optional, but all stations must implement and support it
  - RTS with information about duration of the next transaction (Data + ACK). CTS copies it.
  - Any station within radio coverage of sender or receiver (which receives RTS or CTS) will defer transmission.
  - Updates its own NAV (Network Allocation Vector), this information is maintained and computed to know when medium is free or busy
  - Duration of collision for not hearing the sender: duration of the RTS. Collision duration: lower because of shorter RTS frame. Problem: tiny data frames: RTS threshold

802.11 Medium access mechanism for asynchronous data: variant 2

- Virtual Carier-sense is a distributed reservation mechanism
- Enhanced medium access mechanism for asynchronous data
- All the stations near the sender will hear the reservation requests
- All the stations near the receiver will hear the reservation confirmations

IEEE 802.11: MAC layer

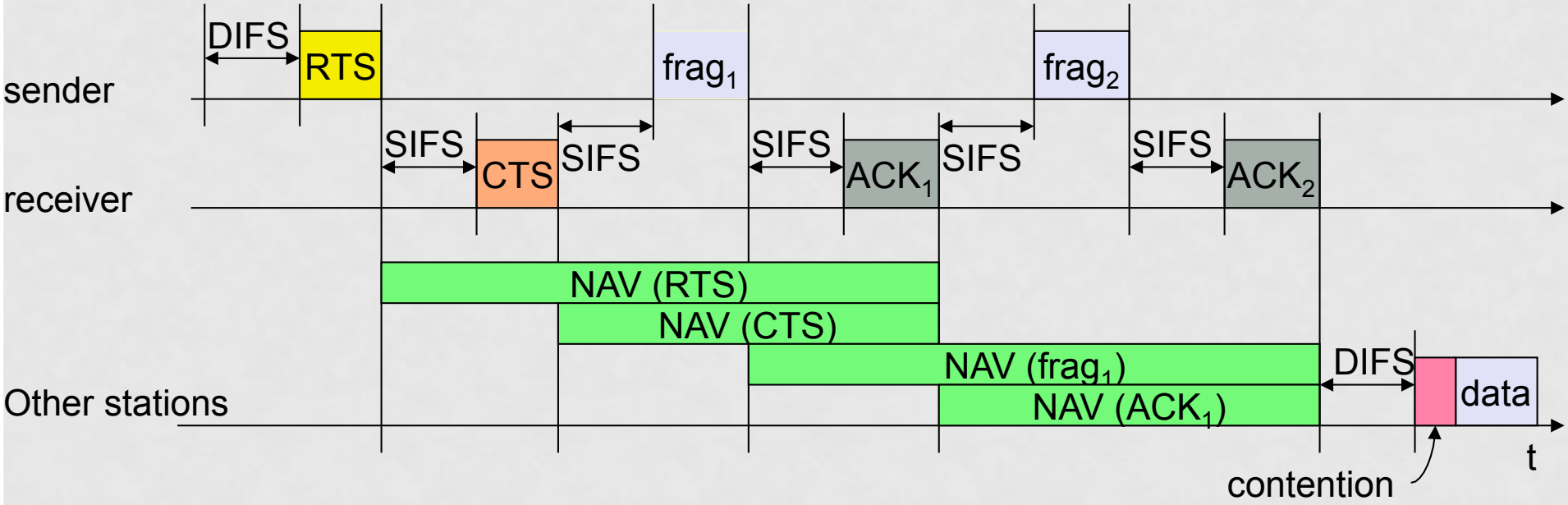


Fragmentation and reassembly in MAC layer

- In LAN protocols frames are typically very large.
- In WLANs there are reasons to make data packets small:
  - High probability of transmission errors
  - Small packets allow for lower waste of bandwidth when re-transmitted
- LLC interface should not be changed, therefore fragmentation is carried at MAC layer.
- MSDUs are divided in multiple fragments.
- Use stop-and-wait technique: don't send next fragment untill ACK of the previous one is received.

IEEE 802.11: MAC layer

- Fragmentation and reassembly with RTS/CTS:



IEEE 802.11: MAC layer

- PCF: Point Coordination Function
  - Invented to introduce contention-free transmission of frames.
  - Allows to introduce real-time services.
  - Access point acts as a device coordinating the transmission.
  - Uses PIFS to win access o medium (because it has the highest priority). Polls the stations asking if they have data to transmit. This way it defines a contention-free period.
  - RTS/CTS is not used in the contention free period.
  - The access point should leave enough time between contention-free periods so that data can be transmitted via DCF.
  - PCF is optional.

IEEE 802.11: Format of the frame

- Preamble: depends on the physical medium and includes synchronisation field and delimiter of beginning of a frame

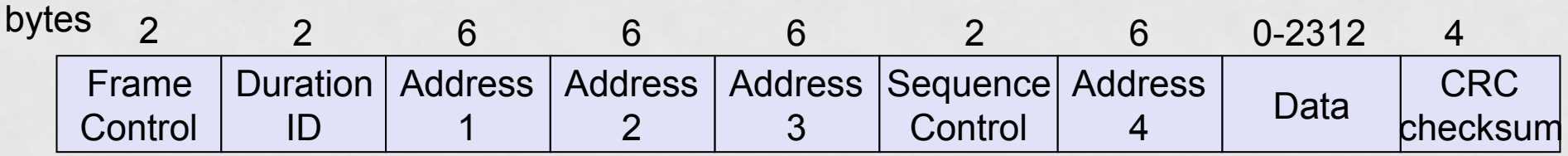
- PLCP header: contains length, signalling (transmission speed of the frame), service (indicates different options related to 802.11b, for example use of PBCC -Packet Binary Convolutional Code), and CRC of the PLCP header

IEEE 802.11: Format of the MAC frame

- Three types (and formats) of frame:
  - Data frames
  - Control frames
  - Management frames
    (same as data frames but not forwarded to upper layers upon reception)
- Each type has several sub-types

IEEE 802.11: Format of the MAC frame

- Frame control = type of frame
- Sequence control = frame number and fragment number to allow identify duplicated fragments in case an ACK was lost.



IEEE 802.11: Format of the Frame Control

Protocol version	Type	Subtype	To DS	From DS	More Frags	Re tran smit	Power mgmt	More data	WEP	Order

Type: 00 Management, 01 Control, 10 Data (control = eg. RTS/CTS)
To DS: value of 1 if the frame goes to DS, including a station inside the BSS
From DS: value of 1 if the frame comes from DS
More fragments: do we have more fragments ?
Retransmit: value of 1 if the frame is being retransmitted
Power management: station changes its transmit power after sending this frame
More data: AP informs if it has more data buffered for this station (useful for power management)
WEP: set to 1 when the frame payload (data) are encrypted

IEEE 802.11: Address Fields in MAC frame

Scenario	to DS	from DS	Addr 1	Addr 2	Addr 3	Addr 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution system
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Identifier Basic Service Set
RA: Receiver Address
TA: Transmitter Address

IEEE 802.11: Mangement functions

- Incorporation of a STA to a BSS:
  - STA needs to get synchronisation information from AP or other STA (when in ad-hoc mode)
    - Passive scanning strategy (await for beacon frames)
    - Active scanning (probe request frame with right SS_ID sent from STA)
  - Authentication process
    - AP and STA exchange authentication information to prove that they posses shared secret key
  - Association process:
    - Exchange of information about the operating speeds of STA and AP. The DS knows where the station is associated.

IEEE 802.11: Mobility management

- Handover:
  - A station should be able to change its point of attachment
  - The standard does not define technical means for roaming between access points. This gives rise to interoperability issues (propietary protocols).
  - Handover process:
    - After loss of connection or very low quality the station scans the channels searching for New AP.
    - The station sends re-association request to the new AP. If the answer is positive, it can start communication. If not, back scanning.
    - The New AP notifies other Aps (via the DS) to inform that he is the new point-of-attachment for the station. The Old AP will now release the resources
    - If the two APs (old and new) are in different networks additional [higher layer] protocols may be needed → e.g. Mobile IP.

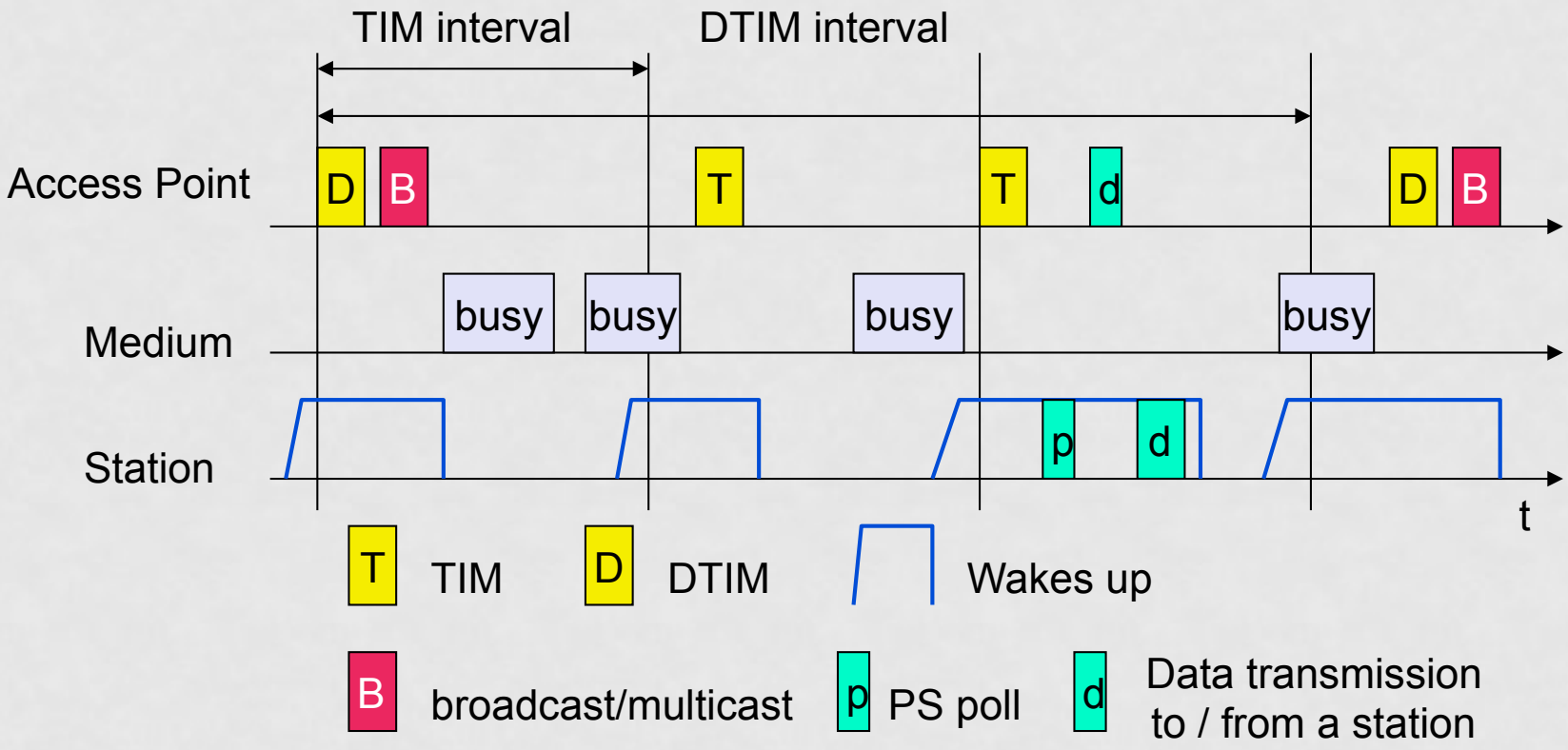
IEEE 802.11: Handover

- IAPP: Inter-Access Point Protocol (802.11f)
  - Devised to facilitate L2 handover between APs of different manufacturers.
  - Uses UDP/IP for info. exchange between APs:
    - Allows to know APs between themselves
    - After the handover, the new AP informs the 'old' AP that handover is completed.
    - The 'old' AP can release resources (free up memory) and re-send stored frames for the corresponding STA.

IEEE 802.11: MAC management

- Energy management (battery power mgmt.):
  - Idea: switch the network transceiver to low power consumption when not used. The station is in sleeping-mode.
  - An AP remembers the state of all stations in his own BSS and buffers packets for them. The packets are sent when solicited by the STA or when its power state changes to wake-up.
  - AN AP sends periodically beacon frames which contain TIM (Traffic Indicator Map), with bindings of dormant stations with their pending frames. Stations wake up regularly to listen to beacons
  - An AP also buffers broadcast and multicast frames. Information about these is included in the DTIM (Delivery TIM), included in beacon frames from time to time.
  - Beacon frame is used by stations to synchronize with the AP, which includes its transmit periodicity. This permits the STAs to wake up just to listen to the beacon.
  - If the STA does not wake up in the DTIM frames are lost. Usually the station syncs its TIM to the DTIM of the AP.
  - First the broadcast and multicast frames are transmitted then unicast frames
  - The stations are able to sync with beacons since these frames carry their transmission time

IEEE 802.11: MAC management



IEEE 802.11: MAC management

- Security:
  - Standard: WEP (Wired Equivalent Privacy):
    - An intruder should not be able to use network resources
    - WEP Should guarantee privacy of users
  - Security is based on pre-shared keys:
    - Authentication (the station must present a proof that it knows the key)
    - Privacy (WEP is used to encode data frames: based on the secret key, a pseudo-random sequence is generated which is added to the actual data of a frame)
  - WPA, WPA2 (802.11i)

Is WEP “secure”?

- Manual Key management
  - Usually keys are not changed
- 24 bit Initialization Vector (IV, 17M)
- Decryption dictionaries
- Injection
- MAC filtering is useless

WPA-WPA2

- Wi-Fi Protected Access
- Designed to correct WEP
- Implements most of IEEE 802.11i
- Designed to use a RADIUS server, used to distribute user keys
- It has also a weaker mode using pre-shared keys.

WPA-WPA2

- Stronger ciphering than WEP. Ciphering algorithm RC_4 with 128 bits keys and 48 bits IVs.
- Implements TKIP (Temporal Key Integrity Protocol) allowing dynamic key modification
- Bigger IV makes more difficult statistical attacks

WPA2

- WPA2 is the certified version in 802.11i
- Pre-shared key: WPA2-Personal
- With authentication 802.1x/EAP WPA2-Enterprise
- Includes AES ciphering

802.1x

- Based in EAP (IETF, Extensible Authentication Protocol)
- It is a protocol defining an encapsulation enabling the use of different authentication protocols.
- The protocol works by the definition of message handshakes and challenges, ciphering each message with the user key
- 802.1x includes methods for communicating with RADIUS

Interoperability between 802.11b and 802.11g

- Three scenarios:
  - AP is 802.11b and the stations are 802.11b and 802.11g
    - 802.11g stations work like regular 802.11b. Capabilities of an AP are discovered during the association process.
    - Maximum expected performance: 5,8 Mbps (TCP) y 7,1 Mbps (UDP)
  - AP is 802.11g and the stations are 802.11b and 802.11g
    - The setup is perfectly compatible, but inefficiency is introduced by mechanisms to make the stations 802.11b and 802.11g compatible.
    - Maximum performance for stations 802.11g because of use of compatibility mechanism: 14,4 Mbps (TCP) and 19,5 Mbps (UDP).
    - The presence of 802.11b stations degrade performance (they use more spectrum time to transmit the same data).
  - AP is 802.11g and the stations are 802.11g
    - Maximum performance of 802.11g will be achieved: 24,4 Mbps (TCP) y 30,5 Mbps (UDP)

Compatibility between 802.11b and 802.11g

- AP is 802.11g ; stations are 802.11b and 802.11g
  - Problem: 802.11b stations don't recognize that medium is busy when the transmission is with OFDM
- Solution:
  - RTS/CTS is sent with CCK when the station wants to transmit to indicate busy medium
    (needed only if the transmission is going to use OFDM)
  - Alternatives:
    - Preamble CCK – payload uses OFDM
    - Preamble CCK – payload uses PBCC (Packet Binary Convolutional Code)

Related standards

- HiperLAN (High Performance Wireless LAN): estándar europeo para WLANs de alta velocidad: 24 Mbps. Banda de 5,1 GHz. No hay productos comerciales.
- IEEE 802.11a, MAC compatible IEEE 802.11 pero para la banda de 5 GHz. Permite velocidades de 54 Mbps. Está cerrado desde el 1999 y empezaron a salir productos comerciales a finales del 2002
- IEEE 802.11h versión europea del 802.11a con mejoras para prevenir interferencias. Aprobado en el 2003. Hay productos comerciales desde antes de la aprobación de estándar que eran 802.11a con modificaciones que están autorizados en algunos países europeos
- IEEE 802.11e, el MAC incluye soporte de QoS (opciones: prioridades de tráfico y sondeo). Trabajo en marcha.
- IEEE 802.11f, estandariza cómo hacer la itinerancia entre dos puntos de acceso. Aprobado en el 2003.

Related standards

- IEEE 802.11g, velocidades de hasta 54 Mbps en la banda de 2,4GHz, usando modulación OFDM (Orthogonal Frequency Division Multiplexing). Es compatible con 802.11b. Aprobado en el 2003.
- IEEE 802.11i, define el uso de protocolos criptográficos para mejorar la seguridad de WLANs. Trabajo en marcha.
- IEEE 802.15, familia de estándares para redes inalámbricas de área personal (ej. 15.1 variante de Bluetooth)
- IEEE 802.16, familia de estándares para redes de banda ancha metropolitanas (WiMAX)
- HomeRF - SWAP (Shared Wireless Access Protocol): banda ISM de 2,4 GHz, FHSS, 2 Mbps. Comunicación inalámbrica a bajo coste de voz y datos.
- Bluetooth: Banda ISM de 2,4 GHz, FHSS, 1Mbps. Especificación de comunicación inalámbrica de voz y datos a corta distancia y bajo coste de todo tipo de terminales. (Ericsson, IBM, Nokia, Toshiba, ...)

Certification

- Standarization: IEEE
- Conformance testing:
  - Wi-Fi Alliance (previously: WECA – Wireless Ethernet Capability Alliance)
  - Wi-Fi Certificates
  - Security: WPA (pre-802.11i) and WPA2 (802.11i)
  - QoS: WMM (Wi-Fi Multimedia)

References

- Wireless LANs: Implementing Interoperable Networks; Jim Geier; Macmillan, 1999.
- Mobile Data & Wireless LAN Technologies; Rifaat A. Dayem; Prentice Hall, 1997.
- Wireless Multimedia Communications, Networking Video, Voice, and Data; Ellen Kayata Wesel; Addison-Wesley, 1998
- Homepage of IEEE: http://www.ieee.org
- Document on wireless networks:
- http://www.wireless-nets.com/whitepapers.htm
- Homepage of Bluetooth: http://www.bluetooth.com
- Wi-Fi Planet, http://www.wi-fiplanet.com/
- Tutorial on WLANs: http://www.wirelesslan.com
- Mobile Communications, Chapter 7: Wireless LANs; Jochen Schiller; http://page.mi.fu-berlin.de/~schiller/publications.htm