802.11

Markku Renfors

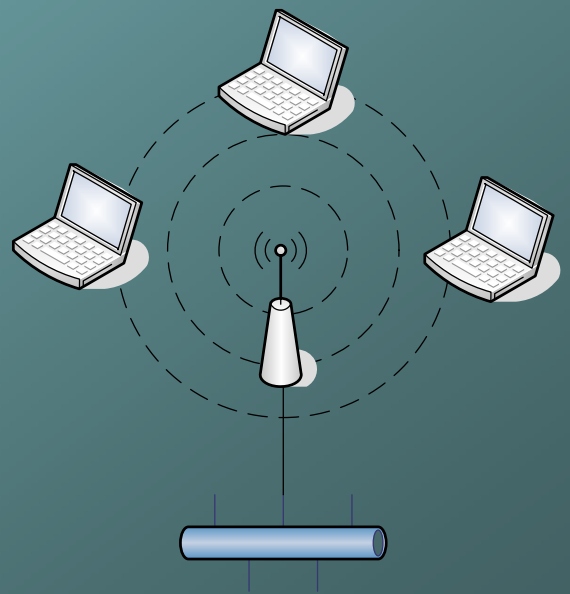
Partly based on student presentation by:

Lukasz Kondrad
Tomasz Augustynowicz
Jaroslaw Lacki
Jakub Jakubiak

Contents

- 802.11 Overview & Architecture
- 802.11 MAC

IEEE 802.11 – Overview and Architecture



The purpose of 802.11 standard

- Describes the functions and services required by an IEEE 802.11 compliant device to operate within ad hoc and infrastructure networks, as well as the aspects of station mobility (transition) within those networks.
- Defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services.
- Defines several PHY signaling techniques and interface functions that are controlled by the IEEE 802.11 MAC.

The purpose of 802.11 standard

- Permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may coexist with multiple overlapping IEEE 802.11 wireless LANs.

- Describes the requirements and procedures to provide privacy of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices.

Components

- STA - Station
- AP - Access Point
- BSS - Basic Service Set
- IBSS - Independent BSS
- ESS - Extended Service Set
  - A set of infrastructure BSSs.
  - Connection of APs
  - Tracking of mobility
- DS - Distribution System
  - AP communicates with another

IEEE 802 .11 Terminology

Access-Point (AP)

- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations

- Most often infra-structure products that connect to wired backbones
  - *Stations select an Access-Point and "associate with it*

- Access-Points :
  - *Support roaming*
  - *Provide time synchronization functions (beaconing)*
  - *Provide Power Management support*

- Traffic typically flows through Access-Point
  - *In IBSS direct Station-to-Station communication takes place*

IEEE 802 .11 Terminology

Station (STA)

• Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system

• Most often end-stations available in terminals (work-stations, laptops etc.)

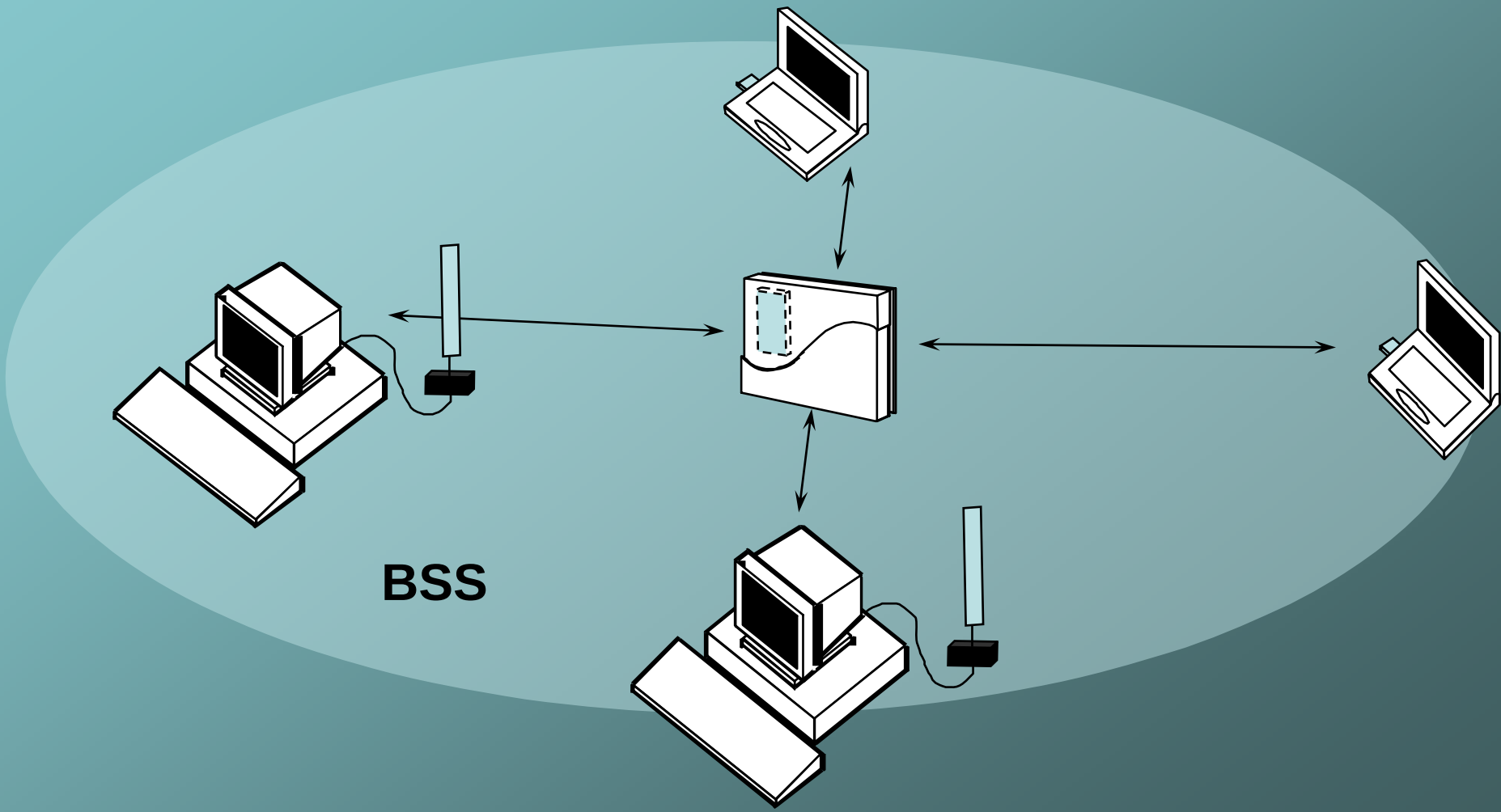
IEEE 802 .11 Terminology

Basic Service Set (BSS)

• A set of stations controlled by a single “Coordination Function” (=the logical function that determines when a station can transmit or receive)

• A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only)

Basic Service Set (BSS)

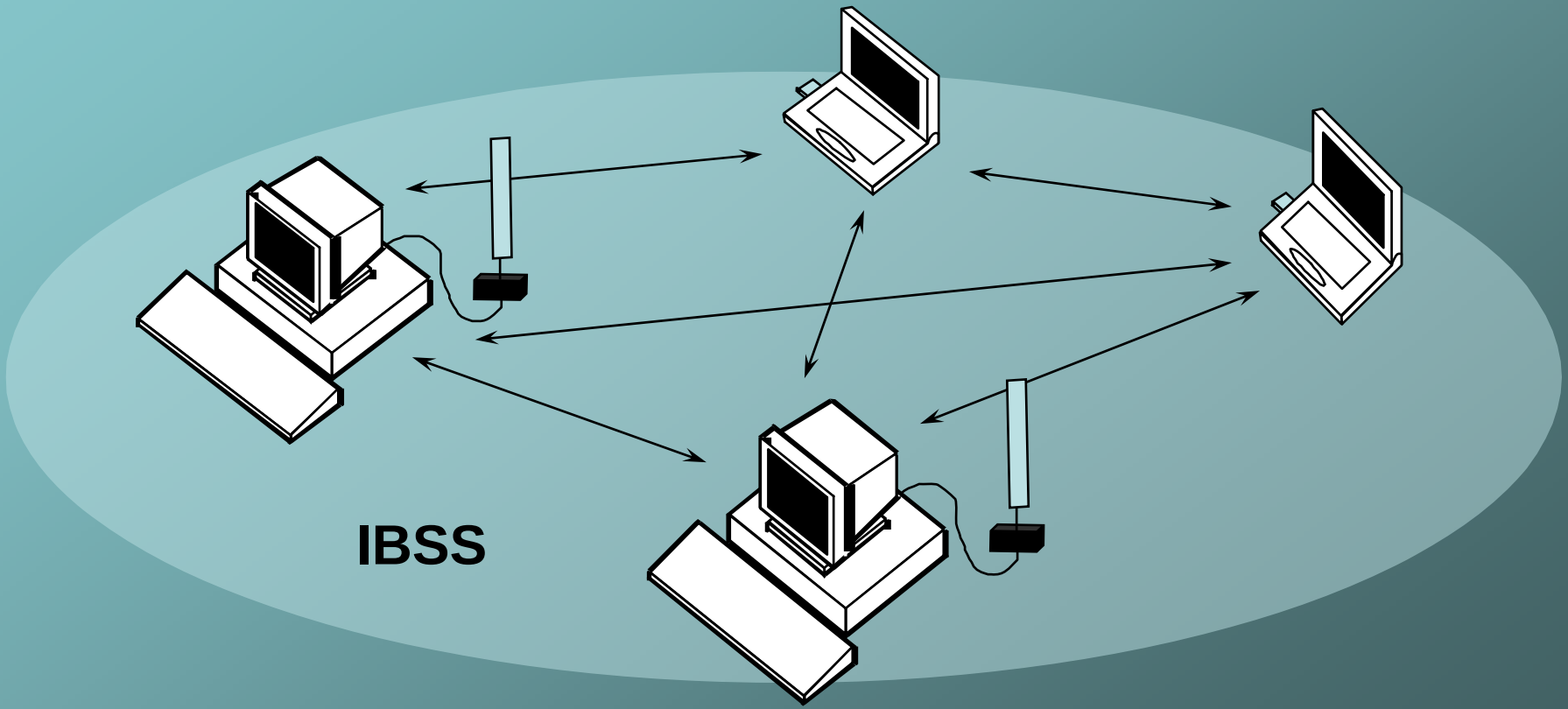


IEEE 802 .11 Terminology

Independent Basic Service Set (IBSS)

- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function
- Diameter of the cell determined by coverage distance between two wireless stations

Independent Basic Service Set (IBSS)



IEEE 802 .11 Terminology

Extended Service Set (ESS)

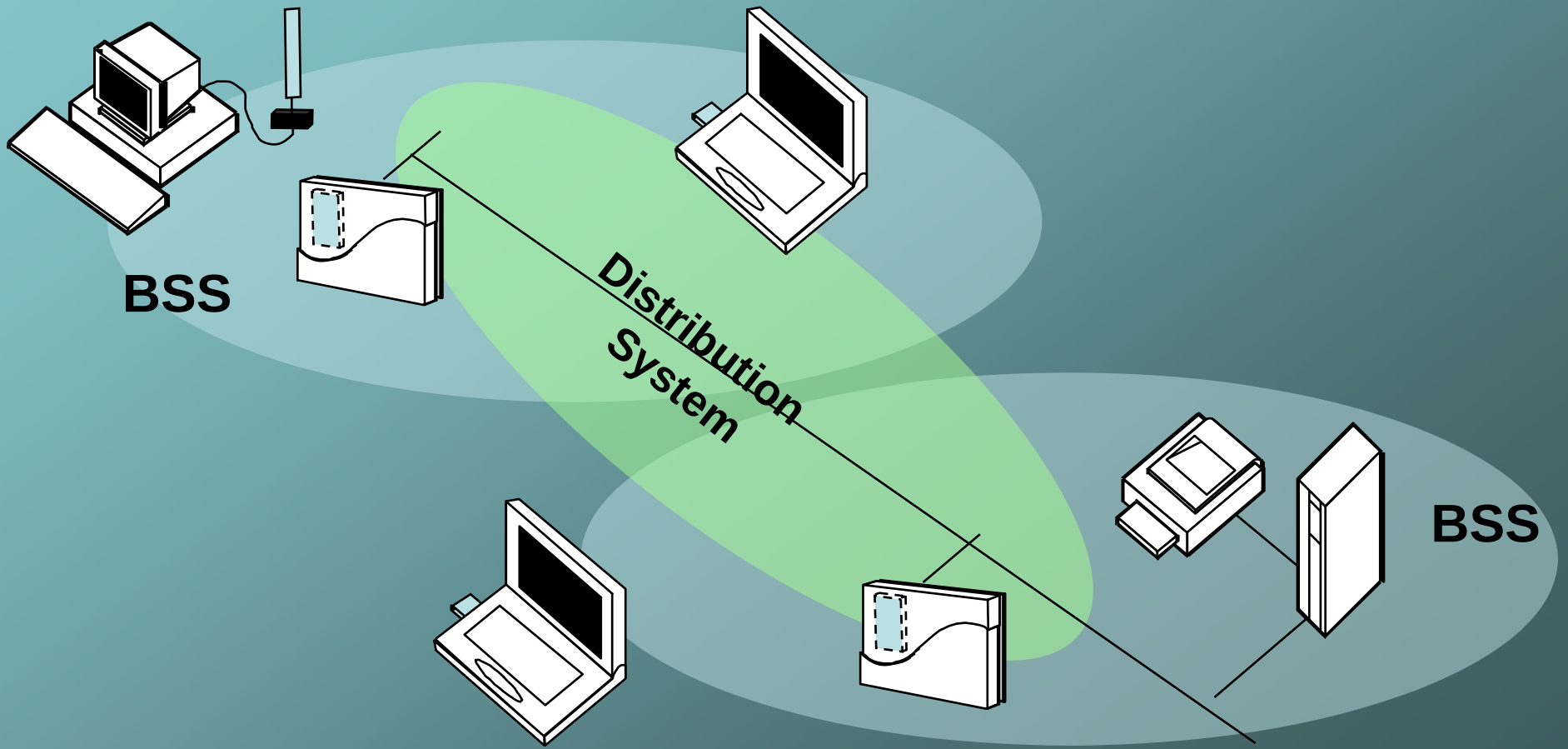
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point
- Diameter of the cell is double the coverage distance between two wireless stations

Distribution System (DS)

- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access-Point in a standalone network
  - Wired; Using cable to interconnect the Access-Points
  - Wireless; Using wireless to interconnect the Access-Points

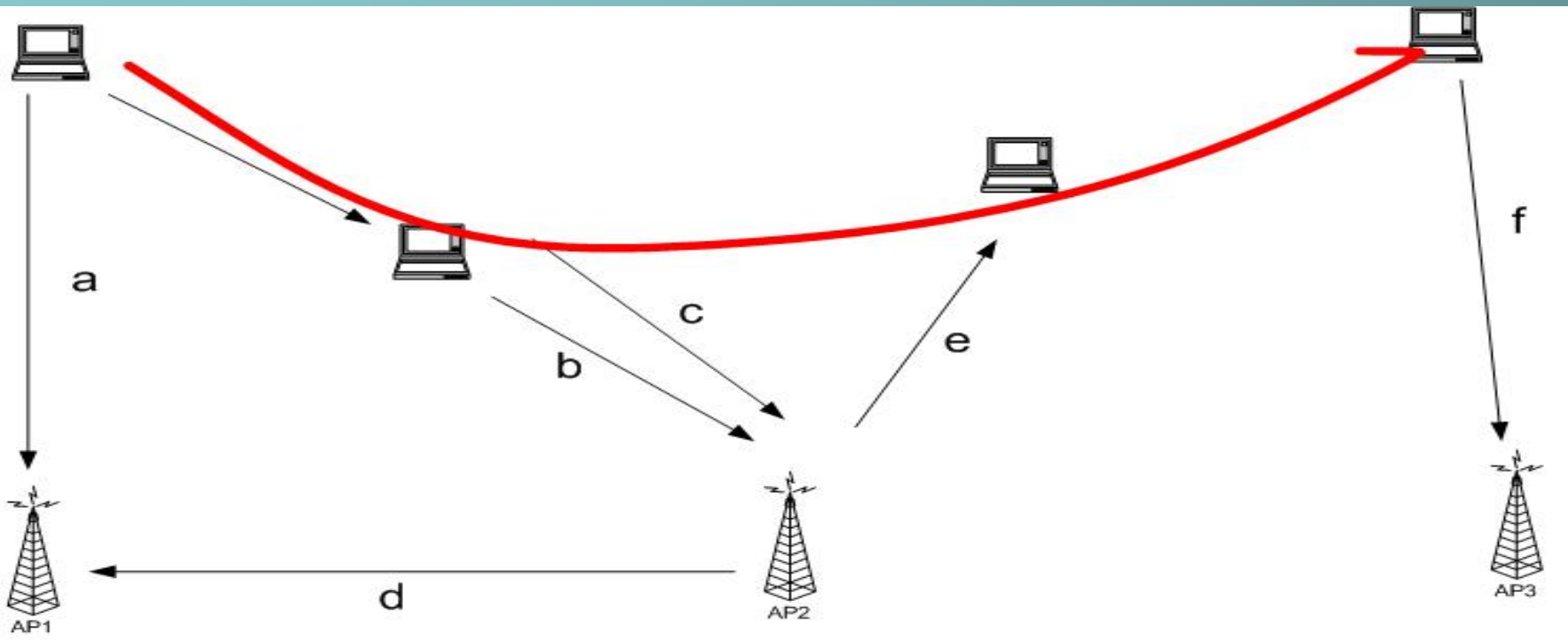
Extended Service Set (ESS)

BSS's with wired Distribution System (DS)



Services

- **Station services:**
  - authentication,
  - de-authentication,
  - key distribution
  - data-authentication
  - replay protection
  - privacy,
  - delivery of data
- **Distribution Services** *(A thin layer between MAC and LLC sublayer)*
  - association
  - disassociation
  - reassociation
  - distribution
  - Integration



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

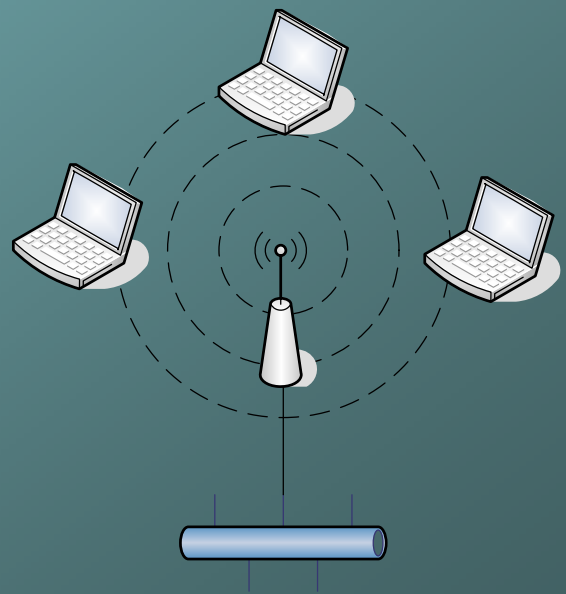
(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

802.11 – Medium Access Control (MAC) layer



What is MAC?

- Medium Access Control protocol is a one of sublayers of Data Link layer in OSI model.
- The MAC is a set of rules to determine how to access the medium and data link components. The MAC rides on every transmission of user data into the air. It provides the core framing operations and the interaction with a wired network backbone.
- MAC purpose:
  - Coordinates and shares use of bandwidth
  - Timing synchronization
  - User datagram transfer function
  - MAC layer management functions

Requirements of MAC for WLAN

- The MAC protocol must be independent of the underlying physical layer
- The access mechanism must be efficient for both bursty and periodic traffic
- The MAC must handle mobile users

Why CSMA/CD can’t be used in wireless LAN?

- Require the implementation of a full duplex radio that would increase the price significantly.
- All the stations may not hear each other on a wireless environment (which is the basic assumption of the CD scheme).

MAC mechanism in 802.11

- 802.11 uses CSMA/CA mechanism (Carrier Sense Multiple Access with Collision Avoidance)
- It is considered to be ‘fair’ for all users because treats them equally.
- Two mechanisms:
  - **Basic access**
  - **RTS/CTS**

MAC modes

- The 802.11 MAC protocol designed with two modes of communication
- **Distributed Coordination Function (DCF)** based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - all stations are equal
  - "listen before talk”
  - station waits for quiet period on network
  - begins to transmit data
  - detects possible collisions
- **Point Coordination Function (PCF)**
  - Time is split into a contention-free period and a contention period
  - During the contention-free polling periods, a station transmits data under the control of the AP.

MAC mechanism in 802.11 – DCF Case

CSMA/CA basic access - 1

- With DCF, stations contend for access and attempt to send frames when there is no other station transmitting. If another station is sending a frame, stations are polite and wait until the channel is free.
  - After the medium is detected to be idle, the stations (with packets to transmit) start transmitting after a random back-off time (contention!).
    - o A synchronization mechanism which enables all stations to start the contention at the same time.
  - Receiving station needs to send an acknowledgement (ACK) if it detects no errors in the received frame.
  - Possible collisions are detected through missing ACKs.
    - o The transmitting station re-transmits its data frame, after new contention.

MAC mechanism in 802.11 – DCF Case

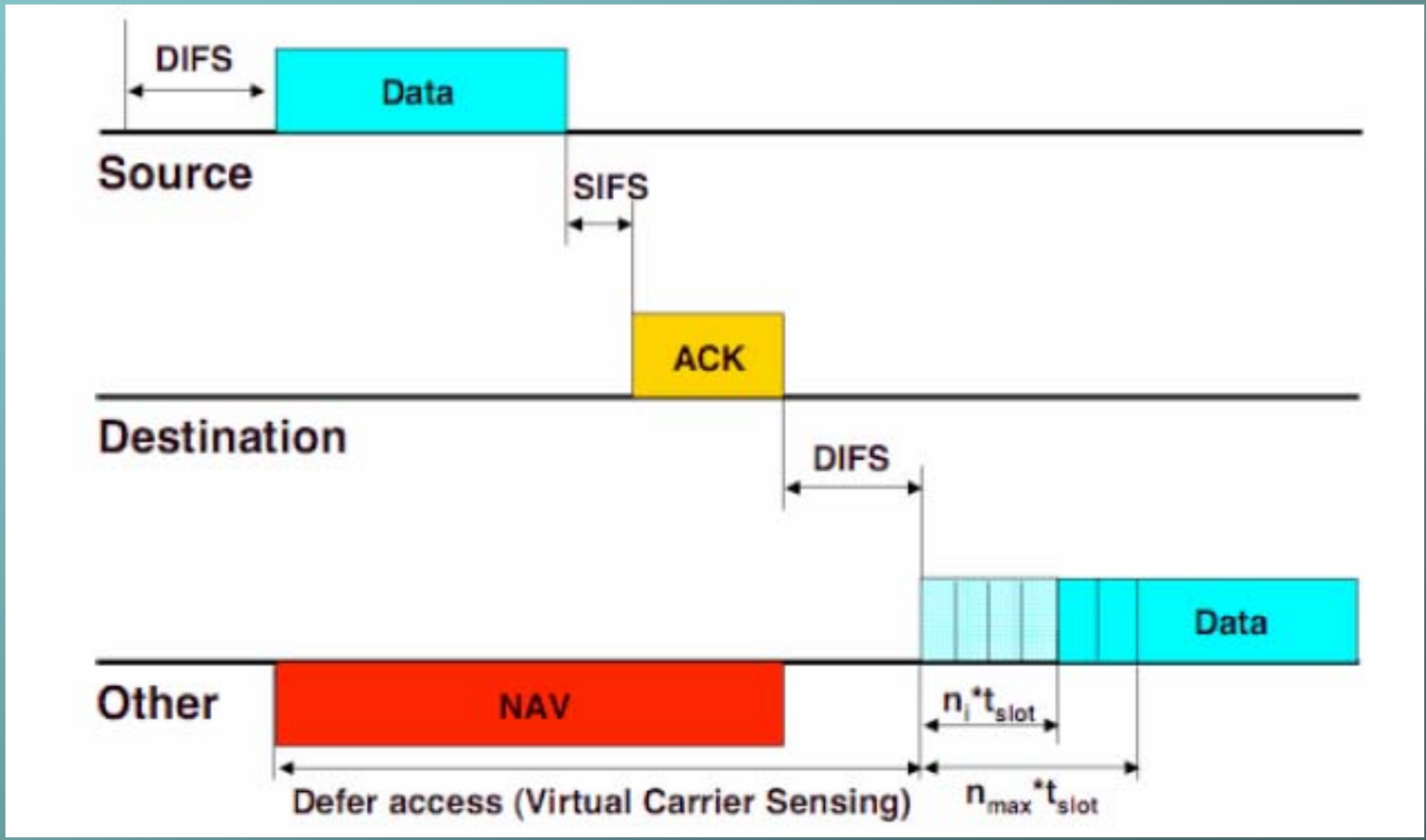
CSMA/CA basic access – 2

- To reduce possibility of collisions, carefully selected guard-times, interframe spaces (IFSs) are used between different transmissions.
  - Distributed IFS (DIFS): minimum delay before starting transmission after the channel is expected to be idle
  - Short IFS (SIFS): delay between end of transmission and ACK
  - Extended IFS (EIFS): waiting time after latest transmission if ACK is not detected

    EIFS=SIFS+DIFS+max length of ACK frame
- The channel is expected to be idle if:
  - No transmissions are detected (physical carrier sensing) *and*
  - NAV (Network allocation vector) counter is zero (virtual carrier sensing). A station listens to the MAC headers of all the frames in the air, and updates the counter based on the frame length informatioin in each MAC header. The NAV mechanism *partly* avoids the problems due to hidden nodes.

MAC mechanism in 802.11 – DCF Case

CSMA/CA basic access - 3



MAC mechanism in 802.11

IFS values

• The SIFS duration and slot length (data frame is a multiple of slots) depend on the physical layer used as follows:

	802.11b	802.11a	802.11g
Slot length	20 μs	9 μs	20 or 9 μs
SIFS	10 μs	16 μs	10 or 16 μs

• SIFS is the sum of maximum expected/specified values for
  • Transceiver turn-around time (switching between transmit to receive mode and back to transmit mode)
  • Physical propagation delay
  • MAC processing delay
  • PHY delay
• DIFS=SISF + 2 slots;

MAC mechanism in 802.11

Backoff timers

- The station's random waiting time in slots is uniformly distributed between 0 and CW (contention window, CW=31 for 802.11b and CW=15 for 802.11a and 802.11g).
- The backoff timer is decremented by one during each idle time-slot within the contention periods. If a contention was not successful for a station, it continues during a new contention period from the end value reached during the previous contention period.
- A station starts transmitting when the timer reaches zero.

MAC mechanism in 802.11, DCF with RTS/CTS

- 4-way handshake (RTS, CTS, DATA, ACK), protocol
- When a sending station wants to transmit data, it first sends (through contention) an RTS (request to send) frame and waits for the destination to reply with a CTS (clear to send) frame. If CTS is detected, then data is transmitted and destination sends an ACK if the data was received completely and correctly.
- If CTS is not detected, the sending station goes back to compete for the media, in the CSMA/CA mode
- All other stations that hear RTS or CTS would defer transmission in the duration indicated in RTS or CTS.
- Both RTS and CTS include the estimated transmission time in the MAC header, so stations which hear either of them, know when the channel is going to be free again, through the NAV mechanism.
- RTS is not used for short packets, for which the cost of collision is lower. RTS packets of different stations may collide anyway. And the RTS/CTS mechanism would cause significant overhead for small packets.

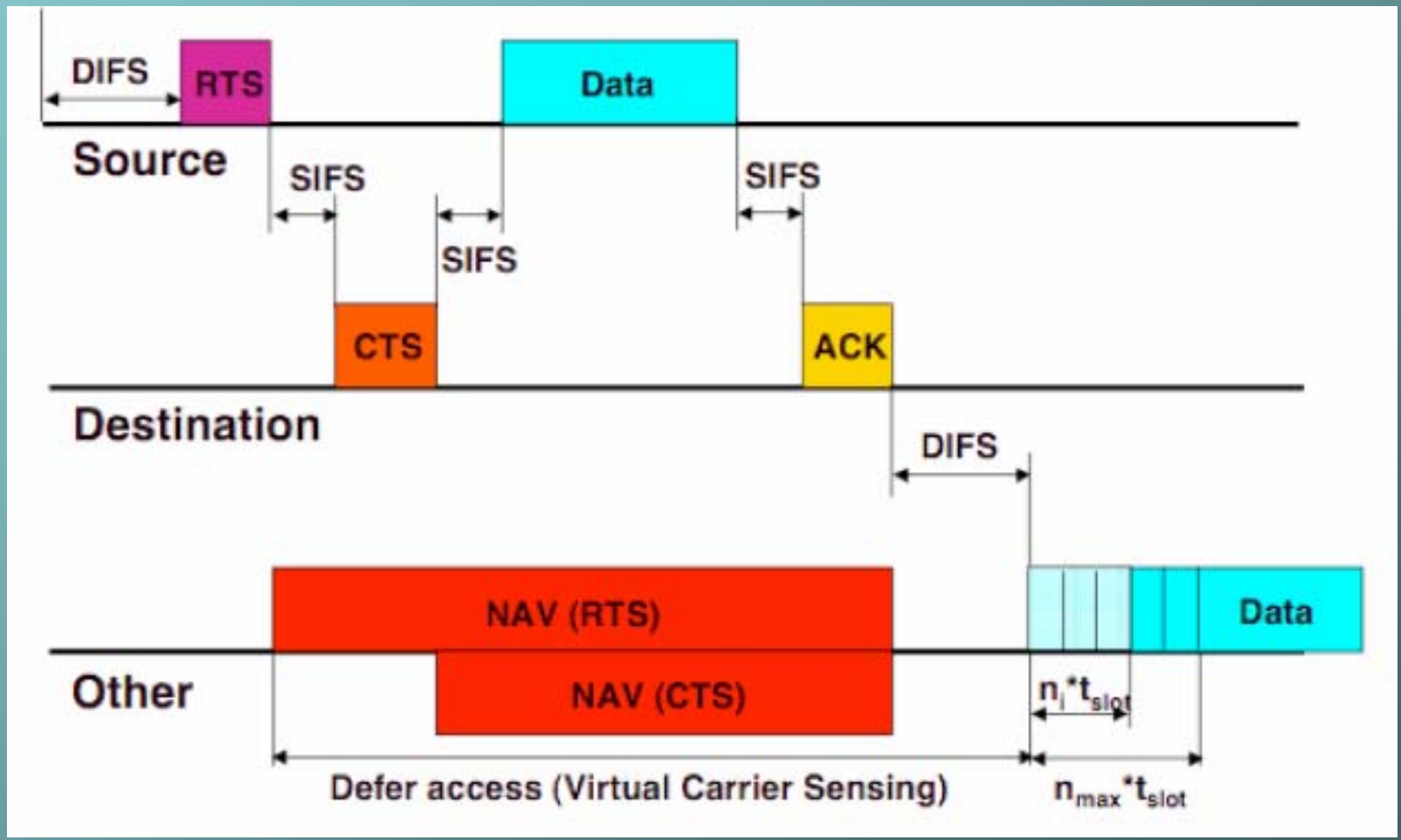
MAC mechanism in 802.11, DCF with RTS/CTS

Retransmissions

- In case of missing ACK
  - Transmitting station increments the retry counter.
  - Doubles the CW (up to a certain limit) and gets a new back-off timer value.
  - Backoff count-down starts again.
  - When the maximum number of retransmissions is reached, the packet is discarded.
- The are different retry counters for short and long packets, based on a given threshold.

MAC mechanism in 802.11, DCF with RTS/CTS

CSMA/CA with RTS/CTS



MAC mechanism in 802.11, PCF mode

Point Coordination Function (PCF)

- AP periodically sends beacon frames, which communicate network identification and management parameters specific to the network
- PCF splits the time in such a way that each superframe includes first a contention-free period (CFP) and then *possibly* a contention period (CP).
- DCF mechanisms are used during the contention period.
  - Stations can request to be includedin the polling list of the Point Coordinator (usually combined with the AP).
  - DCF mechanisms can be used also for data transmission, e.g., for short packets.
- Station can transmit data during contention-free polling periods, under the control of the AP

MAC mechanism in 802.11, PCF mode

- In the beginning of each superframe, the PCF waits until the channel becomes free (the end of the previous superframe is somewhat unpredictable) and then takes control of the channel.
  - Actually, the AP is contending for the medium at this stage. It has a priority, because PIFS<DIFS (see later).
- During the contention-free period (CFP)
  - First AP sends beacon frame.
  - Starts to delivers qued data to stations *and simultaneously*
  - Starts polling the stations by sending CF-Poll frames. Stations with data to transmit respond, each in turn with a single frame of data. Stations without data don't respond.
  - AP waits for the time of PISF (point coordination function IFS, PISF=SIFS+1) before sending CF-Poll frame for the next station

MAC mechanism in 802.11, PCF mode

- To enhance throughput, the ACK frame for the previous station, the CF-Poll frame for the new station, and possible data frame for the new station are combined. So there are four types of frames transmitted from AP during the polling period:
  - CF-Poll / CF-Ack-Poll / CF-Data-Poll / CF-Data-Ack-Poll
- Beacon frames sent regularly (with some uncertainty)
  - The next Target Beacon Transmit Time is included in the beacon frame
  - The length of the CFP is announced in the beacon frame; it may cover multiple beacon intervals.

MAC mechanism in 802.11, PCF mode

Miscelenious

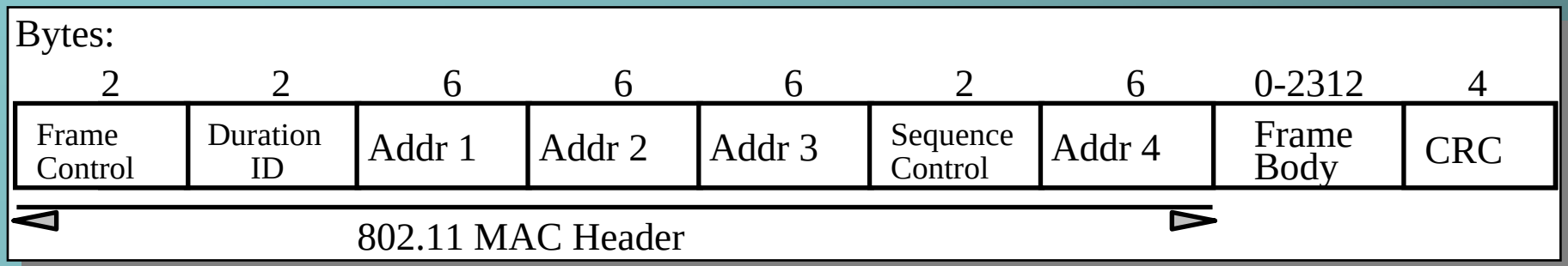
- The standard doesn't specify in which order the stations are polled. => round robin, prioritization, proprietary solutions
- If all transmissions are completed before the end of the CFP (light traffic), the AP may send a special frame to start CF period before the target time.
- Stations may enter into an idle mode to save power.
  - In this mode, they can send PS-Poll frame to check if the AP has any data in queue.

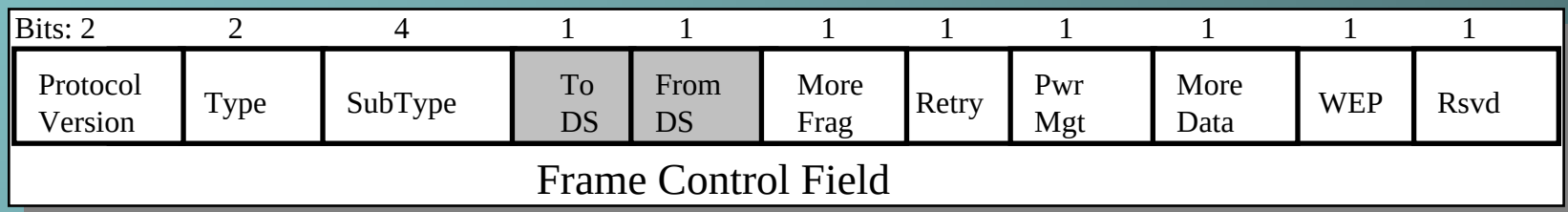
MAC mechanism in 802.11, PCF mode

Miscelenious

- When transmitting long data packets, so-called fragmentation can be used
  - The packet is split into a number of *fragments* which area transmitted separately, with separate ACK for each. Using the spacing of SIFS between an acknowledgement and the next fragment, a station can hold the channel over a sequence of fragment transmissions.
- If a hidden node misses the reception of beacons, then collisions may take place.
- There is also a mechanism to initiate beacon transmissions in the IBSS (ad-hoc) case.

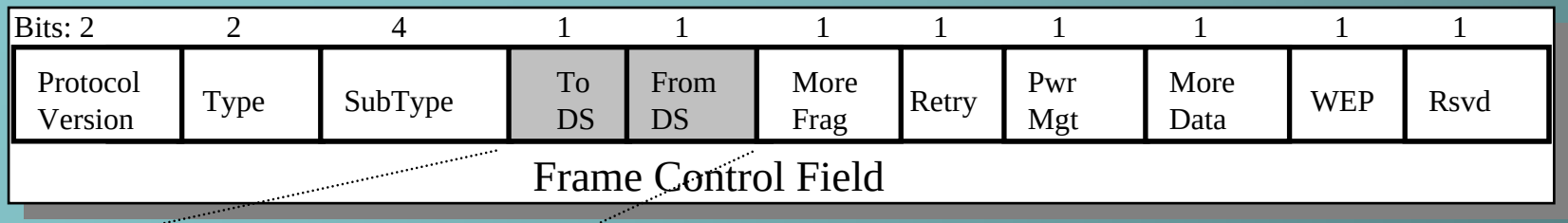
802.11 MAC frame format





- MAC Header format differs per Type:
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames

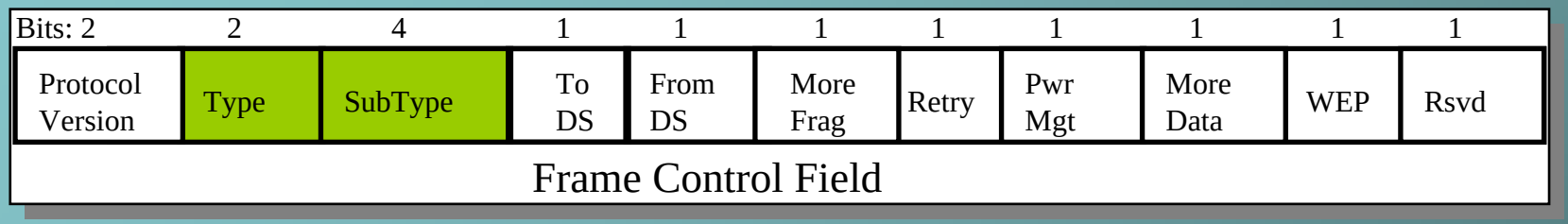
802.11 MAC frame format (cont.)



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- Addr. 1 = All stations filter on this address.
- Addr. 2 = Transmitter Address (TA), Identifies transmitter to address the ACK frame to.
- Addr. 3 = Dependent on *To* and *From DS* bits.
- Addr. 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames

802.11 MAC frame format (cont.)



Type and subtype identify the function of the frame:

- Type=00 Management Frame
  - Beacon (Re)Association
  - Probe (De)Authentication
  - Power Management
- Type=01 Control Frame
  - RTS/CTS ACK
- Type=10 Data Frame

MAC management services

Scanning

For station to begin communication, it must first locate either stations or AP. Scanning may be passive or active. Passive scanning involves only listening for 802.11 traffic, active requires the scanning station to transmit and elicit responses from other stations and APs. (In ad-hoc case, two passive scnners will never find each other!)

Authentication

It consists of an exchange of questions, proofs, assertions and results. If the proofs exchanged are acceptable, each station would then tell the other that its assertion of indentity is believed. Two forms of authentication: open system authentication and shared key.

MAC management services

Association

A WLAN requires a station to associate itself within a BSS because the stations can move from one BSS to another. It is a process of mobile station connecting to an AP within BSS and through that the station lets the network know its current position in ESS

Privacy

The need of secure communications is strong when wireless medium is used. The IEEE 802.11 Wired Equivalent Privacy (WEP) mechanism is designed to provide a protection level that is perceived as being equivalent to that of a wired LAN.

WEP has severe security problems, which are mostly solved by 802.11i (WPA2).

802.11e – QoS

- 802.11e is standard from the IEEE that defines new QoS capabilities for WLANs
- Support delay sensitive applications such as voice and video
- Used for both DCF and PCF MAC modes

QoS needed

- Special characteristics of wireless link such

  - high loss rate
  - bursts of frame loss
  - packet re-ordering
  - packet delay
  - jitter

- Above characteristics may vary over time and location.
- Mobility of users may cause the end to end path to change when users moves but users should receive same QoS

Main idea of DCF enhancement

- DCF - Enhanced Distribution Coordination Function (EDCF)
- Concept of traffic categories
- Each station has eight traffic categories - priority levels.
- Stations detects if the medium is idle
- Waits a period of time corresponding traffic category
- Arbitration Interframe Space (AIFS) is defined for each traffic category
  - Higher-priority traffic category have shorter AIFS than lower-priority traffic category