King Fahd University of Petroleum & Minerals
Computer Engineering Dept

COE 543 – Mobile and Wireless Networks

Term 032

Dr. Ashraf S. Hasan Mahmoud

Rm 22-148-3

Ext. 1724

Email: ashraf@ccse.kfupm.edu.sa

Lecture Contents

1.

Introduction to WLANs

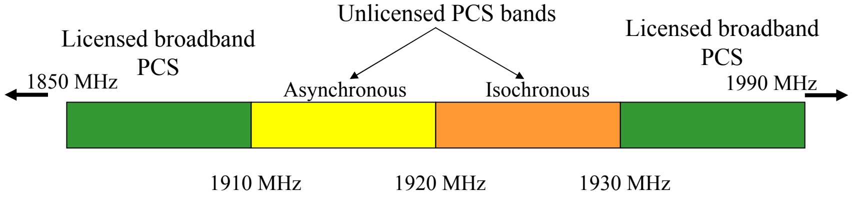
- **Read** Chapter 10 – background material
  - Historical Overview of LAN industry
  - Evolution of WLAN industry
  - Wireless Home Networking Concepts

Bands of Operation

- ISM: 902-928 MHz, 2.4-2.4835 GHz, 5.725-5.875 GHz
- Unlicensed PCS: 1910-1930 MHz
- U-NII: 5.15-5.25 GHz, 5.25-5.35 GHz, 5.725-5.825 GHz

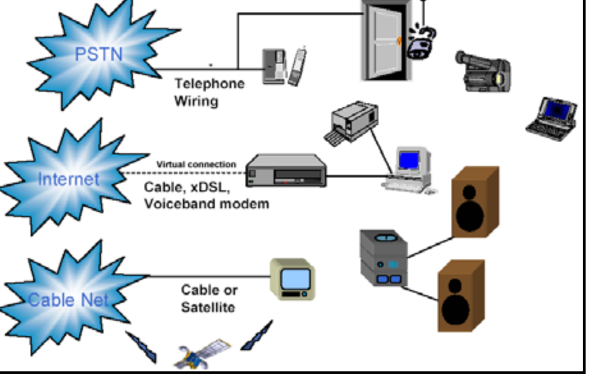
Unlicensed PCS bands

- Band Etiquettes:
  - Listen before talk (LBT protocols)
  - Low Transmitter power
  - Restricted duration of transmission



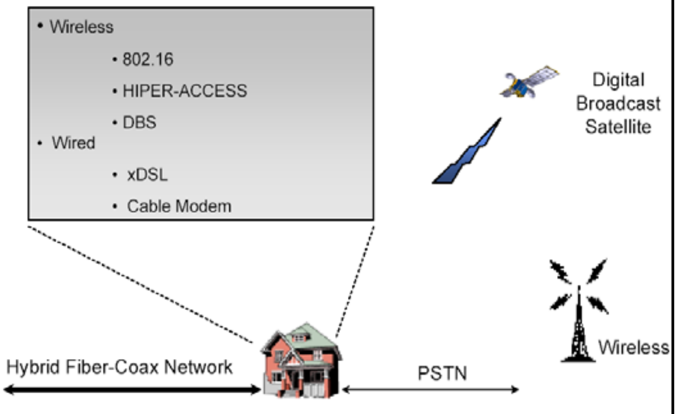
Home Networking (HAN)

- Expanding market
  - Doubling every year
- What is a HAN?
  - Infrastructure to interconnect a variety of home appliances and enable them to be accessible using the internet
- Why do we need a HAN?
  - User-friendly
  - Performance – multimedia
  - Flexible and scalable
  - Etc.
- HAN technologies:
  - Use existing wiring
    - HPNA (Home phone network Alliance)
    - Power line modems
    - Wireless solutions



Home-Access Networking

- How to connect the home to the outside world?
- IEEE802.16 – WMAN for US
- HIPER-ACCESS - WMAN for EU
- LMDS (local multipoint distributed services) – also known as LMCS
- Refer to the other wired solutions

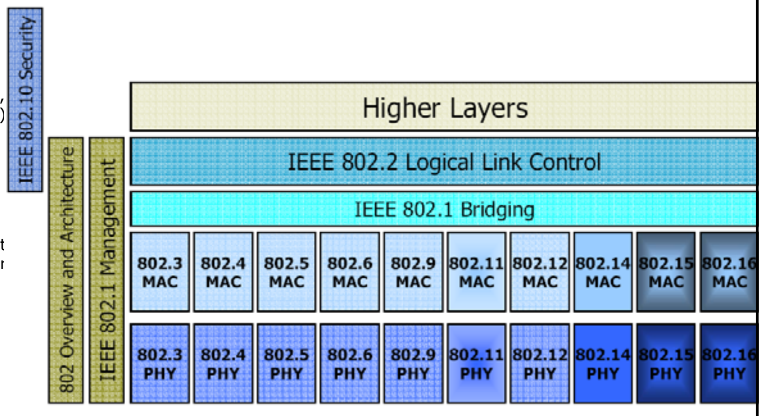


IEEE802.11 and its Derivatives

- Chapter 11

Overview of IEEE802 Protocols

- 802.1 and 802.2 are common
- 802.10 - security
- 802.3 (CSMA/CD), 802.4 (Token Bus), 802.5 (Token Ring) – all wired LANs
- 802.6 DQDB – MLAN
- 802.7 - broadband
- 802.8 - FDDI
- 802.9 ISO-Ethernet – voice & data over Ethernet
- 802.11,15, &16 WLAN
- 802.12 – 100BaseVG; priority
- 802.14 cable network
- 802.16 - WMAN



Overview of IEEE802.11

- History:
  - 1997: completion of first IEEE802.11 standards (1 and 2 Mb/s) – PHY: DSSS, FHSS, and DFIR
  - Afterwards: IEEE802.11b – 11 Mb/s using CCK and IEEE802.11a – 54 Mb/s using OFDM
- Same MAC layer for all three
  - CSMA/CA-based for contention data
  - Support RTS/CTS mechanism to solve hidden terminal problem
  - Point coordination function (PCF) – optional; for real-time traffic
- Topology
  - Centralized – through AP
  - Ad-hoc – supporting peer-to-peer communication between terminals

WLAN Protocol Concerns

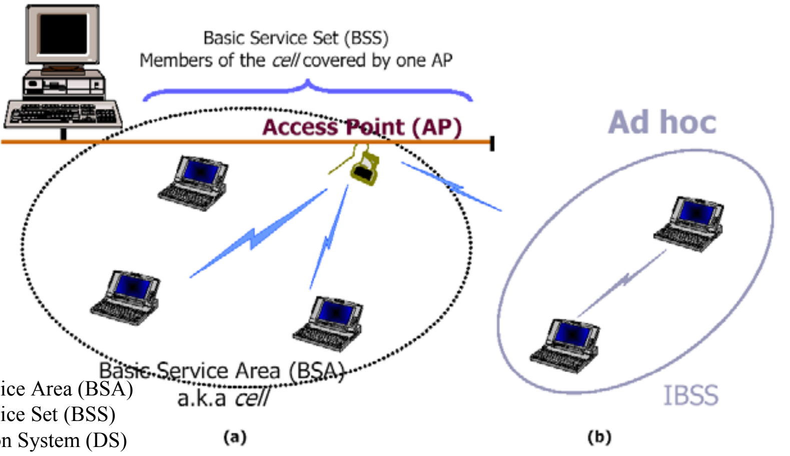
- Mobility
- Connection management: reliability and power
- Security

IEEE802.11 Requirements

- Single MAC supporting multiple PHYs
- Mechanism to allow multiple overlapping networks in the same area
- Provisions to handle the interference from other ISM band radios and microwave ovens
- Mechanism to handle “hidden” terminal problem
- Options to support time-bounded services
- Provisions to handle privacy and access security

Reference Architecture

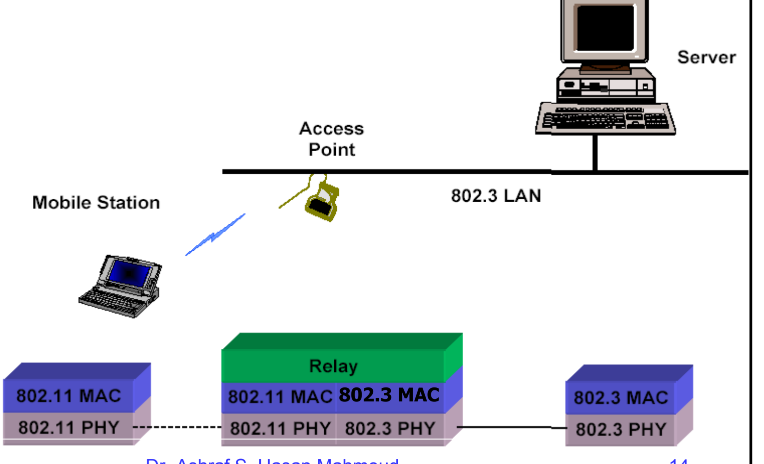
(a) Infrastructure Network (b) Ad-Hoc Network



Basic Service Area (BSA)
Basic Service Set (BSS)
Distribution System (DS)
Extended Service Set (ESS)

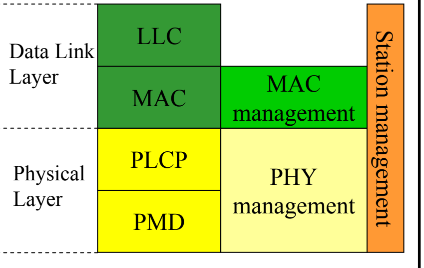
Typical Deployment

- Extended Service Set (ESS)



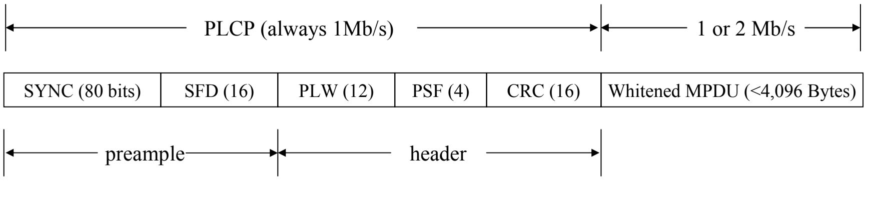
Protocol Architecture

- MAC sublayer responsibilities:
  - Access mechanism
  - Fragmentation and reassembly of packets
- MAC management sublayer responsibilities:
  - Roaming within ESS
  - Power management
  - Registration: Association, disassociation, and re-association
- PLCP responsibilities:
  - Carrier sensing
  - Forming packets for different PHYs
- PMD responsibilities:
  - Modulation, Coding
- PHY layer management: channel tuning to different options within PHY
- Station management sublayer:
  - Coordination and interaction between MAC and PHY



PMD: Physical Medium dependent
PLCP: Physical layer convergence protocol

IEEE802.11 PHY Layer - FHSS



SYNC: Alternating 0s and 1s
SFD: Start of frame delimiter – 0000110010111101
PLW: Packet length width – max of 4 kB
PSF: Packet signaling field – data rate in 500 kb/s step
CRC: PLCP header coding

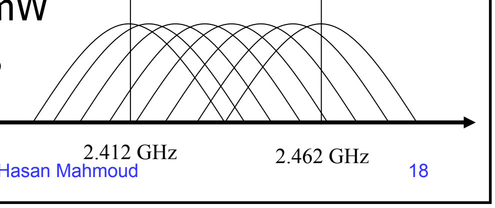
Example:
PSF = 0000 → R = 1Mb/s
= 0010 → R = 2 Mb/s
Maximum rate:
PSF = 1111 → $1 + 15 \times 0.5 = 8.5$ Mb/s

IEEE802.11 FHSS

- FHSS PMD hops over 78 channels of 1 MHz each in the centre of the 2.44 GH ISM band
- Modulation is (2 or 4-level) GFSK: 1 bit/symbol → 1 Mb/s or 2 bit/symbol → 2 Mb/s
- BSS selects (PHY management sublayer) one of three hopping patterns:
  - (0,3,6,9,…,75),
  - (1,4,7,10,…,76), or
  - (2,5,8,11,…,77)
- Hopping rate: 2.5 hops per second
- Therefore up to three APs can coexist in the same area ➔ maximum throughput of 6 Mb/s
- Maximum transmit power = 100 mW
- Scrambling (whitening) of MPDU – randomization and elimination of DC component

IEEE802.11 DSSS

- DSSS PMD uses 26 MHz chunks to transmit 11 Mc/s – refer to figure
- Modulation: DBPSK for 1 Mb/s and DQPSK for 2 Mb/s
- ISM band at 2.4 GHz ➔ 11 overlapping channels with 5 MHz spacing
- Coexisting – 5 choices per BSS
- Max tx power = 100 mW
- Wider range the FHSS



IEEE802.11 PHY Layer - DSSS

- PLCP frame for the DSSS of the IEEE802.11

PLCP (always 1Mb/s)

SYNC (128 bits)	SFD (16)	Signal(8)	Service (8)	Length (16)	FCS (8)	MPDU

preample | header

SYNC: Alternating 0s and 1s
SFD: Start of frame delimiter – 1111001110100000
Signal: Data rate in 100 kb/s steps
Service: reserved for future use
Length: length of MPDU in microseconds
FCS: PLCP header coding

Example:
Signal = 00001010 → R = 1 Mb/s
= 00010100 → R = 2 Mb/s
For IEEE802.b:
Signal = 001101110 → 5.5 Mb/s
= 01101110 → 11 Mb/s
Maximum:
Signal = 11111111 → 255X0.1 = 25.5 Mb/

IEEE802.11 DFIR

- DFIR PMD utilizes 250 ns pulses
- Pulse Position Modulation (PPM)
  - 16-PPM for the 1 Mb/s option
  - 4-PPM for the 2 Mb/s option

PLCP (250 ns pulses)

SYNC (57-73 bits)	SFD (4)	Data Rate (3)	DCLA (32)	Length (16)	FCS (16)	MPDU (<2,500 Bytes)

preample | header

SYNC: Alternating 0, 1 pulses
SFD: Start of frame delimiter – 1001
Data rate: 000 and 001
DCLA: DC level adjustment sequence
Length: length of MPDU in microseconds
FCS: PLCP header coding

IEEE802.11a, b PHY

- IEEE802.11a:
  - OFDM @ 5 GHz U-NII bands – same as HIPERLAN-2
  - Rates up to 54 Mb/s
- IEEE802.11b:
  - CCK @ 2.4GHz
  - Rates up to 5.5 and 11 Mb/s
  - Same PLCP as IEEE802.11 DSSS

IEEE802.11 family and Carrier Sensing

- PHY Sensing - Clear Channel Assessment (CCA) signal
  - Generate by the PLCP
  - Sensing: Detected data sensing vs Carrier Sensing
    - Any detected bits?, or – slow but reliable
    - RSS of carrier against threshold – fast but many false alarms
- Virtual carrier sensing:
    - Network Allocation Vector (NAV) signal supported by the RTS/CTS and PCF mechanisms at MAC – indicates the medium is occupied for a given (length field) time duration
    - Used for RTS/CTS and PCF based schemes only

IEEE802.11 MAC

- MAC Layer:
  - MAC sublayer
  - MAC layer management sublayer
- Major responsibilities of MAC sublayer:
  - Define access scheme
  - Define packet formats
- Major responsibilities of management sublayer:
  - Support ESS
  - Power management
  - Security

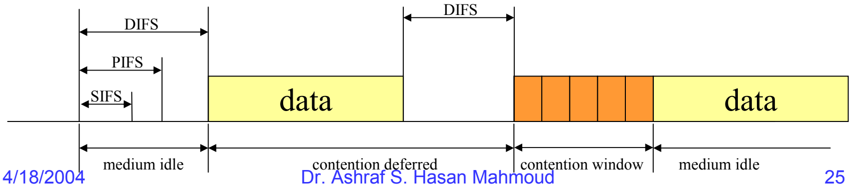
MAC Sublayer

- Supported access schemes
  - CSMA/CA – contention data
  - RTS/CTS – contention-free

  These two modes are refered to as DCF
  - PCF – contention-free - for time-bounded traffic
- Inter-frame spacing (IFS) – can be used to prioritize users
  - Short – SIFS - highest priority terminal
  - Point – PIFS – used in conjunction with PCF function
  - Distributed – DIFS – lowest priority terminal – used with DCF
- Refer to CSMA/CA slides

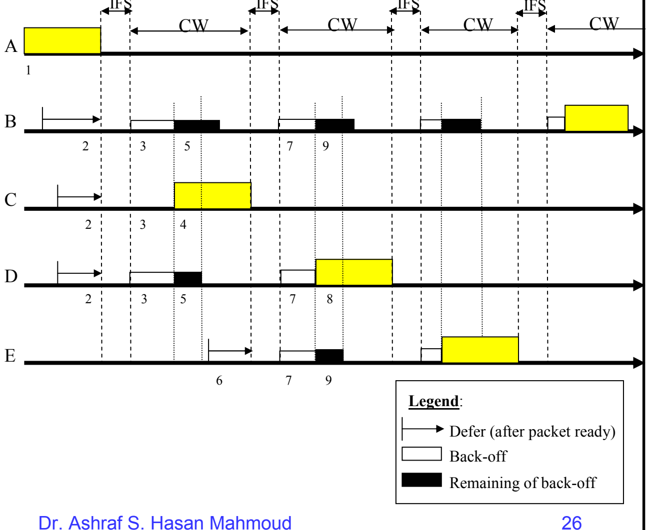
Primary Operation of CSMA/CA

- Primary operation of CSMA/CA as shown in figure
- After the completion of a transmission all terminals having data to transmit must wait S/DIFS – depending on their priority before they start their back-off timers
- Binary exponential back-off scheme is used to minimize probability of collision



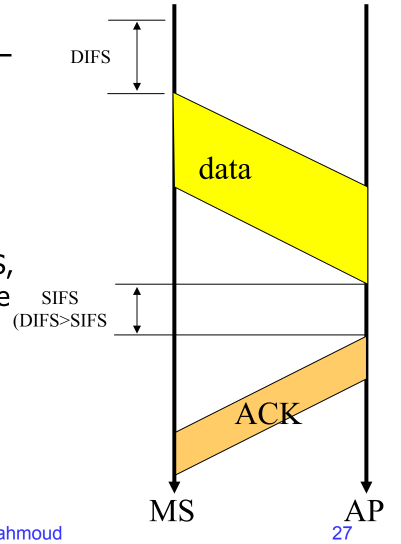
Operation of CSMA/CA in IEEE802.11 – Example 4.18

1. A is transmitting
2. B, C, & D persist on sensing the channel and defer their transmission until A is done
3. B,C, & D wait for IFS and then start their back-off counters
4. C finishes back-off first – it starts transmission
5. B & D freeze their back-off timers
6. During C's transmission, E senses the channel and finds it busy – it defers transmission
7. After the completion of C's transmission and the passing of IFS, B & D restart their frozen back-off counters, while E starts its back-off counter
8. D finishes its back-off counter first – it starts transmission
9. B & D freeze their counters
10. Etc.



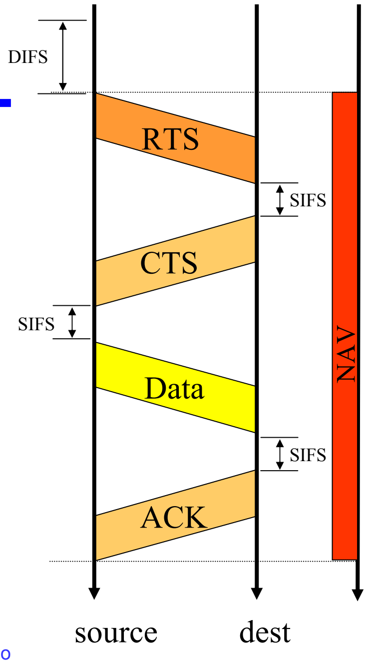
Operation of CSMA/CA with ACK for MAC Recovery

- Note that IEEE802.3 does not support ACK on the MAC level – connectionless
- For IEEE802.11 ACK for MAC recovery is an option
- AP waits for SIFS before ACK
  - Since SIFS is shorter than DIFS, all stations hear the ACK before they attempt transmission
- Not implemented in most IEEE802.11 products – ACK is left for upper layers



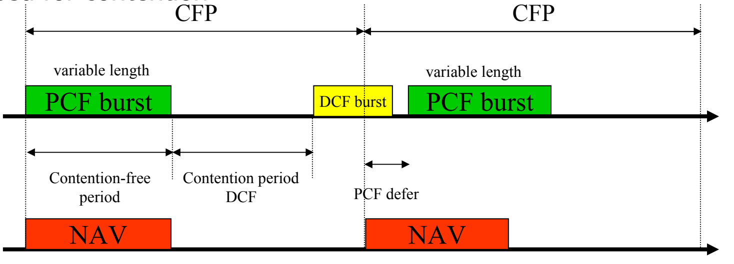
RTS/CTS Operation

- When source is ready – RTS (20 bytes) is sent
- Destination responds with CTS (16 bytes) after SIFS
- Source terminal received CTS and after SIFS sends data
- Destination terminal sends ACK after SIFS
- Other terminal listening to RTS/CTS will turn their NAV signal on – used for virtual carrier sensing
- NAV signal turned off when after the transmission and reception of the ACK frame



PCF for Contention-Free Access

- Optional MAC service – Not implemented by all manufacturers
- Available only for infrastructure networks – not Ad-hoc
- AP – point coordinator organizes periodical contention-free periods (CFP) for delay-sensitive services
- PCF operation
- During PCF operation (part of CFP) NAV signal is on –
- During the remainder of the CFP NAV signal is off and that can be used for contention



MAC Frames Formats

- Refer to sections 11.4.1 and 11.4.2

MAC Management Sublayer – Beacon Message

- Management frame transmitted quasi-periodically by the AP to establish the time synchronization function (TSF)
- Contains: BSS-ID, time-stamp, traffic indication map (for sleep mode), power management, and roaming info.
- RSS measurements are made on the beacon message
- Used to identify the AP and the network

MAC Management Sublayer – Registration

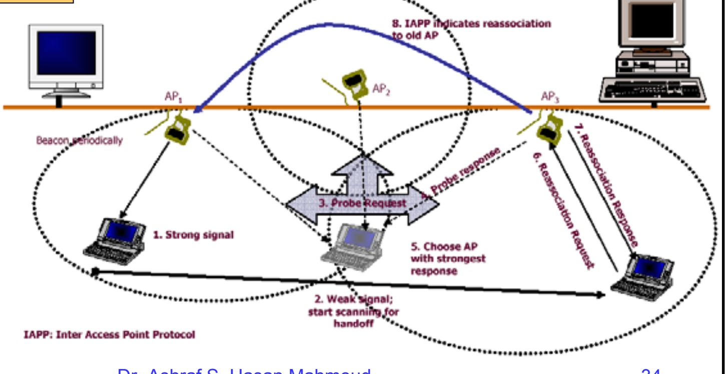
- Association: procedure by which an MS "registers" with an AP
  - After association, the MS can send/receive from AP
  - MS sends an "association request" frame to AP
  - AP grants permission

MAC Management Sublayer – Handoff

- Definitions:
  - No transition: MS is static or moves within BSA
  - BSS transition: MS moves from one BSS to another within the same ESS
  - ESS transition: MS moves from one ESS to another – upper layer connections may break unless a protocol like mobile IP is operating!
- Re-association service is used when an MS moves from BSS to another within the same ESS
  - MS initiates this service
- Dissociation service is used to terminate an association
  - MS or AP can initiate this service
  - Notification – not a request

MAC Management Sublayer – Handoff (2)

- Passive vs. active scanning:
  - probe request ←→ proble response (similar to beacon)
- Re-association request ←→ re-association response
- Re-association request contains info about the MS and old AP

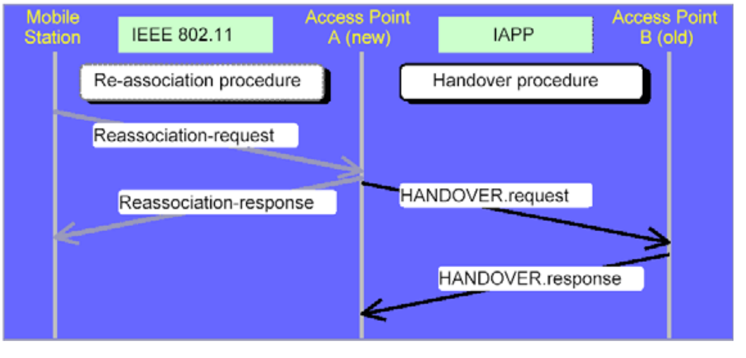


MAC Management Sublayer – Handoff - IAPP

- IAPP: Inter-Access Point Protocol
  - Not standardized yet – proprietary procedures
- PDUs exchanged between old AP and new AP – using UDP-IP over the wired infrastrucutre
- IAPP is used to announce the existence of APs and the creation of APs database within each AP
- If AP does not have an IP address, alternatively, the subnetwork access protocol (SNAP) may be used.

MAC Management Sublayer – Handoff – IAPP (2)

- IAPP: Inter-Access Point Protocol



MAC Management Sublayer – Power Management

- The main power consuming state is the idle receive mode – not existent ant for cellular telephony
  - MS does not know when traffic will be sent to it – remains ready and powered on → huge waste of power
- How to conserve power?
  - MS goes to "sleep"
  - Data buffered at AP and sent to MS only when it is "awake"
  - MS uses the power management bit in the frame control field to announce its sleep strategy
  - MS wakes up at beacon times (STF)
  - TIM field within beacon informs MS whether there is data buffered at AP or not
  - MS with data buffered at AP sends a power-save poll to AP – AP responds with data when MS is in active mode.

MAC Management Sublayer – Security

- Very active area of research
- Two types of authentication
  - Open system authentication - default
  - Shared key authentication
    - Involves a challenge-response identification protocol

MAC Management Sublayer – Privacy

- Wired-Equivalent Privacy (WEP) specification
- A pseudorandom generator is used along with the 40-bit secret key to create a key sequence that is simply XOR-ed with the plaintext message
  - Very susceptible to planned attacks