Introduction to Wireless Networks

Chapter 2: Introduction to IEEE 802.11

Prof. Yuh-Shyan Chen
Department of CSIE
National Taipei University
Chapter 2: Introduction to IEEE 802.11

- IEEE 802.11
  - PHY
  - MAC
  - Roaming
  - .11a, b, g, h, i …

- HIPERLAN
  - Standards overview
  - HiperLAN2
  - QoS
Comparison: infrastructure vs. ad-hoc networks

infrastructure network

wired network

ad-hoc network

AP: Access Point
802.11 - Architecture of an infrastructure network

Station (STA)
- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)
- group of stations using the same radio frequency

Access Point
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS
802.11 - Architecture of an ad-hoc network

Direct communication within a limited range

- **Station (STA):** terminal with access mechanisms to the wireless medium
- **Independent Basic Service Set (IBSS):** group of stations using the same radio frequency
IEEE standard 802.11

- Mobile terminal
- Access point
- Fixed terminal

Application layers:
- TCP
- IP
- LLC
- 802.11 MAC
- 802.11 PHY

Layer 2:
- 802.11 PHY
- 802.11 MAC
- 802.3 PHY
- 802.3 MAC

Infrastructure network
802.11 - Layers and functions

**MAC**
- access mechanisms, fragmentation, encryption

**MAC Management**
- synchronization, roaming, MIB, power management

**PLCP**
- Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)

**PMD**
- Physical Medium Dependent
  - modulation, coding

**PHY Management**
- channel selection, MIB

**Station Management**
- coordination of all management functions

---

**DLC**
- **LLC**
- **MAC**
  - MAC Management
- **PLCP**
  - PHY Management
- **PMD**
802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)
- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)
- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, -1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared
- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization
FHSS PHY packet format

Synchronization
- synch with 010101... pattern

SFD (Start Frame Delimiter)
- 0000110010111101 start pattern

PLW (PLCP_PDU Length Word)
- length of payload incl. 32 bit CRC of payload, PLW < 4096

PSF (PLCP Signaling Field)
- data of payload (1 or 2 Mbit/s)

HEC (Header Error Check)
- CRC with $x^{16} + x^{12} + x^5 + 1$
DSSS PHY packet format

Synchronization
- synch., gain setting, energy detection, frequency offset compensation

SFD (Start Frame Delimiter)
- 1111001110100000

Signal
- data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)

Service
- future use, 00: 802.11 compliant
- length of the payload

HEC (Header Error Check)
- protection of signal, service and length, $x^{16}+x^{12}+x^{5}+1$

<table>
<thead>
<tr>
<th>128</th>
<th>16</th>
<th>8</th>
<th>8</th>
<th>16</th>
<th>16</th>
<th>variable</th>
<th>bits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>synchronization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SFD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>length</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HEC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>payload</td>
<td></td>
</tr>
</tbody>
</table>

PLCP preamble

PLCP header
**802.11 - MAC layer I – DFWMAC (distributed foundation wireless medium access control)**

**Traffic services**
- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

**Access methods**
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized “back-off” mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list
Priorities
- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service

Direct access if medium is free $\geq$ DIFS
802.11 - CSMA/CA access method I

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
802.11 - competing stations - simple version

station$_1$  station$_2$  station$_3$  station$_4$  station$_5$

DIFS  DIFS  DIFS  DIFS

<table>
<thead>
<tr>
<th>bo$_e$</th>
<th>bo$_r$</th>
<th>bo$_e$</th>
<th>bo$_e$</th>
<th>bo$_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>busy</td>
<td>busy</td>
<td>busy</td>
<td>busy</td>
<td>busy</td>
</tr>
</tbody>
</table>

DIFS

<table>
<thead>
<tr>
<th>bo$_e$</th>
<th>bo$_r$</th>
<th>bo$_e$</th>
<th>bo$_r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>busy</td>
<td>busy</td>
<td>busy</td>
<td>busy</td>
</tr>
</tbody>
</table>

DIFS

<table>
<thead>
<tr>
<th>bo$_e$</th>
<th>bo$_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>bo$_e$</td>
<td>bo$_r$</td>
</tr>
</tbody>
</table>

DIFS

<table>
<thead>
<tr>
<th>bo$_e$</th>
<th>bo$_r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>bo$_e$</td>
<td>bo$_r$</td>
</tr>
</tbody>
</table>

DIFS

<table>
<thead>
<tr>
<th>bo$_e$</th>
<th>bo$_r$</th>
</tr>
</thead>
</table>

**Definitions:**
- **busy**: medium not idle (frame, ack etc.)
- **bo$_e$**: elapsed backoff time
- **bo$_r$**: residual backoff time
- **DIFS**: packet arrival at MAC
Sending unicast packets

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors
Hidden-Terminal and Exposed-Terminal Problems

Fig. 1: (a) the hidden terminal problem, (b) the exposed terminal problem
Sending unicast packets

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS
Fragmentation

![Fragmentation Diagram]

- **Sender**:
  - DIFS
  - RTS
  - SIFS
  - CTS
  - SIFS
  - NAV (RTS)
  - NAV (CTS)
  - NAV (frag1)
  - NAV (ACK1)
  - SIFS
  - ACK1
  - SIFS
  - ACK2

- **Receiver**:
  - DIFS
  - RTS
  - CTS
  - NAV (RTS)
  - NAV (CTS)
  - NAV (frag1)
  - NAV (ACK1)
  - SIFS
  - ACK2

- **Other Stations**:
  - DIFS
  - data
  - NAV (frag1)
  - NAV (ACK1)

- **Contention**
  - DIFS

NTFU, Department of Computer Science and Information Engineering
DFWMAC-PCF I

- D1
- D2
- U1
- U2

- PIFS
- SIFS

- medium busy
- point coordinator
- wireless stations
- stations' NAV

- SuperFrame
- \( t_0 \)
- \( t_1 \)
- NAV
DFWMAC-PCF II

- Point coordinator:
  - D3
  - D4
  - SIFS
  - CFend

- Wireless stations:
  - PIFS
  - U4
  - SIFS

- Stations' NAV:
  - contention free period
  - contention period

- NAV timeline:
  - t2
  - t3
  - t4
## 802.11 - Frame format

### Types
- control frames, management frames, data frames

### Sequence numbers
- important against duplicated frames due to lost ACKs

### Addresses
- receiver, transmitter (physical), BSS identifier, sender (logical)

### Miscellaneous
- sending time, checksum, frame control, data

<table>
<thead>
<tr>
<th>bytes</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>6</th>
<th>0-2312</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Duration/ID</td>
<td>Address 1</td>
<td>Address 2</td>
<td>Address 3</td>
<td>Sequence Control</td>
<td>Address 4</td>
<td>Data</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bits</th>
<th>2</th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol version</td>
<td>Type</td>
<td>Subtype</td>
<td>To DS</td>
<td>From DS</td>
<td>More Frag</td>
<td>Retry</td>
<td>Power Mgmt</td>
<td>More Data</td>
<td>WEP</td>
</tr>
</tbody>
</table>

2.21
## MAC address format

<table>
<thead>
<tr>
<th>scenario</th>
<th>to DS</th>
<th>from DS</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad-hoc network</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, from AP</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, within DS</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

DS: Distribution System  
AP: Access Point  
DA: Destination Address  
SA: Source Address  
BSSID: Basic Service Set Identifier  
RA: Receiver Address  
TA: Transmitter Address
### Special Frames: ACK, RTS, CTS

#### Acknowledgement

<table>
<thead>
<tr>
<th>bytes</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Duration</td>
<td>Receiver Address</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

#### Request To Send

<table>
<thead>
<tr>
<th>bytes</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Duration</td>
<td>Receiver Address</td>
<td>Transmitter Address</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

#### Clear To Send

<table>
<thead>
<tr>
<th>bytes</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Duration</td>
<td>Receiver Address</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>
802.11 - MAC management

Synchronization
- try to find a LAN, try to stay within a LAN
- timer etc.

Power management
- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

Association/Reassociation
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base
- managing, read, write
Synchronization using a Beacon (infrastructure)

![Diagram showing beacon intervals and medium access points]

- Beacon interval
- Access point
- Medium
- Busy
- Value of the timestamp
- Beacon frame

$t$
Synchronization using a Beacon (ad-hoc)

beacon interval

station₁

B₁

station₂

B₂

B₂

medium

busy

busy

busy

B

value of the timestamp

beacon frame

random delay

t
Power management

Idea: switch the transceiver off if not needed

States of a station: sleep and awake

Timing Synchronization Function (TSF)
- stations wake up at the same time

Infrastructure
- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

Ad-hoc
- Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)
Power saving with wake-up patterns (infrastructure)

- TIM interval
- DTIM interval
- Busy
- Transmission to/from the station
- Poll
- Broadcast/multicast
- Awake
Power saving with wake-up patterns (ad-hoc)

- **Station 1**
  - Beacon frame \( B_1 \)
  - Random delay
  - Transmits ATIM \( A \)
  - Transmits data \( D \)
  - Wake up

- **Station 2**
  - Beacon frame \( B_2 \)
  - Random delay
  - Acknowledges ATIM \( a \)
  - Acknowledges data \( d \)

- **Timing**
  - ATIM window
  - Beacon interval

---

2.29
802.11 - Roaming

No or bad connection? Then perform:

Scanning
- scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request
- station sends a request to one or several AP(s)

Reassociation Response
- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request
- signal the new station to the distribution system
- the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources
Layer-2 handoff

infrastructure network

AP: Access Point

wired network
Layer-2 handoff procedure in WLAN
WLAN: IEEE 802.11b

Data rate
- 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s

Transmission range
- 300m outdoor, 30m indoor
- Max. data rate ~10m indoor

Frequency
- Free 2.4 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Cost
- 100€ adapter, 250€ base station, dropping

Availability
- Many products, many vendors

Connection set-up time
- Connectionless/always on

Quality of Service
- Typ. Best effort, no guarantees (unless polling is used, limited support in products)

Manageability
- Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages
- Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only
IEEE 802.11b – PHY frame formats

**Long PLCP PPDU format**

- **128** synchronization
- **16** SFD
- **8** signal
- **8** service
- **16** length
- **16** HEC
- **variable** bits

- **PLCP preamble**
- **192 µs** at **1 Mbit/s** DBPSK
- **1, 2, 5.5 or 11 Mbit/s**

**Short PLCP PPDU format (optional)**

- **56** short synch.
- **16** SFD
- **8** signal
- **8** service
- **16** length
- **16** HEC
- **variable** bits

- **PLCP preamble** (1 Mbit/s, DBPSK)
- **96 µs**
- **2, 5.5 or 11 Mbit/s**

- **PLCP header** (2 Mbit/s, DQPSK)
Channel selection (non-overlapping)

Europe (ETSI)

- Channel 1: 2400 - 2412 MHz
- Channel 7: 2442 - 2444 MHz
- Channel 13: 2472 - 2483.5 MHz

US (FCC)/Canada (IC)

- Channel 1: 2400 - 2412 MHz
- Channel 6: 2437 - 2439 MHz
- Channel 11: 2462 - 2483.5 MHz

Bandwidth: 22 MHz
WLAN: IEEE 802.11a

Data rate
- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- 6, 12, 24 Mbit/s mandatory

Transmission range
- 100m outdoor, 10m indoor
  - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30 m, 18 up to 40 m, 12 up to 60 m

Frequency
- Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Cost
- 280€ adapter, 500€ base station

Availability
- Some products, some vendors

Connection set-up time
- Connectionless/always on

Quality of Service
- Typ. best effort, no guarantees (same as all 802.11 products)

Manageability
- Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages
- Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
- Disadvantage: stronger shading due to higher frequency, no QoS
IEEE 802.11a – PHY frame format

<table>
<thead>
<tr>
<th>bits</th>
<th>4</th>
<th>1</th>
<th>12</th>
<th>1</th>
<th>6</th>
<th>16</th>
<th>variable</th>
<th>6</th>
<th>variable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rate</td>
<td>reserved</td>
<td>length</td>
<td>parity</td>
<td>tail</td>
<td>service</td>
<td>payload</td>
<td>tail</td>
<td>pad</td>
</tr>
</tbody>
</table>

PLCP header

PLCP preamble | signal | data

- 12 symbols at 6 Mbit/s
- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
Operating channels for 802.11a / US U-NII

Center frequency = 5000 + 5*channel number [MHz]
OFDM in IEEE 802.11a (and HiperLAN2)

OFDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot
- (plus 12 virtual subcarriers)
- 312.5 kHz spacing

![Diagram of OFDM subcarrier arrangement]
WLAN: IEEE 802.11 – future developments (08/2002)

802.11d: Regulatory Domain Update – completed
802.11e: MAC Enhancements – QoS – ongoing
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
802.11f: Inter-Access Point Protocol – ongoing
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system.
802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM – ongoing
802.11h: Spectrum Managed 802.11a (DCS, TPC) – ongoing
802.11i: Enhanced Security Mechanisms – ongoing
  - Enhance the current 802.11 MAC to provide improvements in security.

Study Groups
  - 5 GHz (harmonization ETSI/IEEE) – closed
  - Radio Resource Measurements – started
  - High Throughput – started
ETSI - HIPERLAN

ETSI standard
- European standard, cf. GSM, DECT, ...
- Enhancement of local Networks and interworking with fixed networks
- Integration of time-sensitive services from the early beginning

HIPERLAN family
- One standard cannot satisfy all requirements
  - Range, bandwidth, QoS support
  - Commercial constraints
- HIPERLAN 1 standardized since 1996 – no products!

HIPERLAN layers
- Medium access control layer
- Channel access control layer
- Physical layer

OSI layers
- Higher layers
- Network layer
- Data link layer
- Physical layer

IEEE 802.x layers
- Logical link control layer
- Medium access control layer
- Physical layer
### Overview: original HIPERLAN protocol family

<table>
<thead>
<tr>
<th></th>
<th>HIPERLAN 1</th>
<th>HIPERLAN 2</th>
<th>HIPERLAN 3</th>
<th>HIPERLAN 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>wireless LAN</td>
<td>access to ATM fixed networks</td>
<td>wireless local loop</td>
<td>point-to-point wireless ATM connections</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>5.1-5.3GHz</td>
<td>17.2-17.3GHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>decentralized ad-hoc/infrastructure</td>
<td>cellular, centralized</td>
<td>point-to-multipoint</td>
<td>point-to-point</td>
</tr>
<tr>
<td><strong>Antenna</strong></td>
<td>omni-directional</td>
<td>directional</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>50 m</td>
<td>50-100 m</td>
<td>5000 m</td>
<td>150 m</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>statistical</td>
<td>ATM traffic classes (VBR, CBR, ABR, UBR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td>&lt;10m/s</td>
<td></td>
<td>stationary</td>
<td></td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>conventional LAN</td>
<td>ATM networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data rate</strong></td>
<td>23.5 Mbit/s</td>
<td>&gt;20 Mbit/s</td>
<td>155 Mbit/s</td>
<td></td>
</tr>
<tr>
<td><strong>Power conservation</strong></td>
<td>yes</td>
<td></td>
<td>not necessary</td>
<td></td>
</tr>
</tbody>
</table>

HIPERLAN 1 never reached product status, the other standards have been renamed/modified!
Homework #2

1. What’s the hidden-terminal and exposed-terminal problems occurred in DFWMAC-DCF CSMA/CA?
2. How to use RTS/CTS messages (DFWMAC-DCF w/ RTS/CTS) to reduce the hidden-terminal problem?
3. How the PCF (Point Coordination Function) works?
4. What’s the main operations of IEEE 802.11 roaming (layer-2 handoff procedure)?
5. What’s the power management in infrastructure and ad hoc modes?