Chapter 14

Wireless LANs
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

**Topics discussed in this section:**
- Architecture
- MAC Sublayer
- Physical Layer
A BSS without an AP is called an ad hoc network; a BSS with an AP is called an infrastructure network.
**Figure 14.1** Basic service sets (BSSs)

**BSS:** Basic service set  
**AP:** Access point

Ad hoc network (BSS without an AP)  
Infrastructure (BSS with an AP)
Figure 14.2  *Extended service sets (ESSs)*

- **ESS**: Extended service set
- **BSS**: Basic service set
- **AP**: Access point
Figure 14.3  *MAC layers in IEEE 802.11 standard*

Diagram showing the MAC layers in the IEEE 802.11 standard, with layers for LLC sublayer, MAC sublayer, and Physical layer, and protocols 802.11 FHSS, 802.11 DSSS, 802.11 Infrared, 802.11a DSSS, 802.11a OFDM, and 802.11g DSSS.
Figure 14.4  CSMA/CA flowchart
Figure 14.5  **CSMA/CA and NAV**

Source

DIFS

SIFS

SIFS

Time

RTS

CTS

Data

ACK

Destination

SIFS

SIFS

Time

All other stations

Time

NAV
(No carrier sensing)
Figure 14.6 *Example of repetition interval*

B: Beacon frame
CF: Contention-free

PIFS  SIFS    Poll      SIFS  ACK + poll  ...  CF end

ACK + data

NAV

14.9
Figure 14.7  Frame format

Diagram showing the frame format with the following fields:
- 2 bytes: FC
- 2 bytes: D
- 6 bytes: Address 1
- 6 bytes: Address 2
- 6 bytes: Address 3
- 2 bytes: SC
- 6 bytes: Address 4
- 0 to 2312 bytes: Frame body
- 4 bytes: FCS

Below the diagram:
- Protocol version: 2 bits
- Type: 2 bits
- Subtype: 4 bits
- To DS: 1 bit
- From DS: 1 bit
- More flag: 1 bit
- Retry: 1 bit
- Pwr mgmt: 1 bit
- More data: 1 bit
- WEP: 1 bit
- Rsvd: 1 bit
Table 14.1  *Subfields in FC field*

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Current version is 0</td>
</tr>
<tr>
<td>Type</td>
<td>Type of information: management (00), control (01), or data (10)</td>
</tr>
<tr>
<td>Subtype</td>
<td>Subtype of each type (see Table 14.2)</td>
</tr>
<tr>
<td>To DS</td>
<td>Defined later</td>
</tr>
<tr>
<td>From DS</td>
<td>Defined later</td>
</tr>
<tr>
<td>More flag</td>
<td>When set to 1, means more fragments</td>
</tr>
<tr>
<td>Retry</td>
<td>When set to 1, means retransmitted frame</td>
</tr>
<tr>
<td>Pwr mgt</td>
<td>When set to 1, means station is in power management mode</td>
</tr>
<tr>
<td>More data</td>
<td>When set to 1, means station has more data to send</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired equivalent privacy (encryption implemented)</td>
</tr>
<tr>
<td>Rsvd</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Figure 14.8  Control frames

2 bytes  2 bytes  6 bytes  6 bytes  4 bytes
FC  D  Address 1  Address 2  FCS

2 bytes  2 bytes  6 bytes  4 bytes
FC  D  Address 1  FCS

RTS

CTS or ACK
### Table 14.2  Values of subfields in control frames

<table>
<thead>
<tr>
<th>Subtype</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1011</td>
<td>Request to send (RTS)</td>
</tr>
<tr>
<td>1100</td>
<td>Clear to send (CTS)</td>
</tr>
<tr>
<td>1101</td>
<td>Acknowledgment (ACK)</td>
</tr>
</tbody>
</table>
### Table 14.3 Addresses

<table>
<thead>
<tr>
<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>0</td>
<td>0</td>
<td>Destination</td>
<td>Source</td>
<td>BSS ID</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Destination</td>
<td>Sending AP</td>
<td>Source</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Receiving AP</td>
<td>Source</td>
<td>Destination</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Receiving AP</td>
<td>Sending AP</td>
<td>Destination</td>
<td>Source</td>
</tr>
</tbody>
</table>
Figure 14.9  Addressing mechanisms

a. Case 1

b. Case 2

c. Case 3

d. Case 4
Figure 14.10 *Hidden station problem*

B and C are hidden from each other with respect to A.
The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.
Figure 14.11 Use of handshaking to prevent hidden station problem
Figure 14.12 Exposed station problem

C is exposed to transmission from A to B.
Figure 14.13  
Use of handshaking in exposed station problem
### Table 14.4 Physical layers

<table>
<thead>
<tr>
<th>IEEE</th>
<th>Technique</th>
<th>Band</th>
<th>Modulation</th>
<th>Rate (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>FHSS</td>
<td>2.4 GHz</td>
<td>FSK</td>
<td>1 and 2</td>
</tr>
<tr>
<td></td>
<td>DSSS</td>
<td>2.4 GHz</td>
<td>PSK</td>
<td>1 and 2</td>
</tr>
<tr>
<td></td>
<td>Infrared</td>
<td></td>
<td>PPM</td>
<td>1 and 2</td>
</tr>
<tr>
<td>802.11a</td>
<td>OFDM</td>
<td>5.725 GHz</td>
<td>PSK or QAM</td>
<td>6 to 54</td>
</tr>
<tr>
<td>802.11b</td>
<td>DSSS</td>
<td>2.4 GHz</td>
<td>PSK</td>
<td>5.5 and 11</td>
</tr>
<tr>
<td>802.11g</td>
<td>OFDM</td>
<td>2.4 GHz</td>
<td>Different</td>
<td>22 and 54</td>
</tr>
</tbody>
</table>
Figure 14.14  *Industrial, scientific, and medical (ISM) band*
Figure 14.15 Physical layer of IEEE 802.11 FHSS

1 or 2 Mbps
Digital data

Modulator
2-Level or 4-level FSK

Pseudorandom sequence

Frequency synthesizer

1-MHz Analog signal
Figure 14.16  Physical layer of IEEE 802.11 DSSS
Figure 14.17  Physical layer of IEEE 802.11 infrared

Diagram showing the flow of data from 1 or 2 Mbps digital data through an encoder and modulator to an analog signal. The encoder processes data from 4 to 16 or 2 to 4, and the modulator uses pulse position modulation.
Figure 14.18  *Physical layer of IEEE 802.11b*
**14-2 BLUETOOTH**

*Bluetooth* is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. *A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.*

**Topics discussed in this section:**
- Architecture
- Bluetooth Layers
- Baseband Layer
- L2CAP
Figure 14.19  Piconet
Figure 14.20  *Scatternet*
Figure 14.21 Bluetooth layers

Applications

Profiles

Data

L2CAP layer

Baseband layer

Radio layer
**Figure 14.22** Single-secondary communication
Figure 14.23  *Multiple-secondary communication*
Figure 14.24  Frame format types

- Access code: 72 bits
- Header: 54 bits
- Data: 0 to N bits

Address: 3 bits
Type: 4 bits
FAS: 1 1 1
HEC: 8 bits

N = 240 for 1-slot frame
N = 1490 for 3-slot frame
N = 2740 for 5-slot frame

This 18-bit part is repeated 3 times.
Figure 14.25  L2CAP data packet format