IEEE 802.11 Wireless LANs
Part I: Basics

Raj Jain
Professor of Computer Science and Engineering
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this class lecture are available at:
http://www.cse.wustl.edu/~jain/cse574-18/
Overview

1. IEEE 802.11 Features
2. IEEE 802.11 Physical Layers
3. IEEE 802.11 MAC
4. IEEE 802.11 Architecture
5. Frame Format
6. Power Management

Note: This is 1st of 2 lectures on Wi-Fi. The 2nd lecture covers recent developments such as high-throughput Wi-Fi, white spaces, etc.
IEEE 802.11 vs. Wi-Fi

- IEEE 802.11 is a standard
- Wi-Fi = “Wireless Fidelity” is a trademark
- Fidelity = Compatibility between wireless equipment from different manufacturers
- Wi-Fi Alliance is a non-profit organization that does the compatibility testing (WiFi.org)
- 802.11 has many options and it is possible for two equipment based on 802.11 to be incompatible.
- All equipment with “Wi-Fi” logo have selected options such that they will interoperate.
IEEE Standards Numbering System

IEEE 802.* and IEEE 802.1* standards (e.g., IEEE 802.1Q-2011) apply to all IEEE 802 technologies:
- IEEE 802.3 Ethernet
- IEEE 802.11 Wi-Fi
- IEEE 802.16 WiMAX

<table>
<thead>
<tr>
<th>802 Overview and Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.2 Logical Link Control</td>
</tr>
<tr>
<td>802.1 Bridging</td>
</tr>
<tr>
<td>802.1 Management</td>
</tr>
<tr>
<td>802.10 Security</td>
</tr>
<tr>
<td>802.3 Ethernet</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>802.11 Wi-Fi</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>802.17 Resilient Packet Ring (RPR)</td>
</tr>
</tbody>
</table>
IEEE Standards Numbering (Cont)

- IEEE 802.11* (e.g., 802.11i) standards apply to all Wi-Fi devices but may not apply to ZigBee devices which are based on 802.15,

- Standards with all upper case letters are base standards, e.g., IEEE 802.1AB-2009

- Standards with lower case are additions/extensions/revisions. Merged with the base standard in its next revision. e.g., IEEE 802.1w-2001 was merged with IEEE 802.1D-2004

- Standards used to be numbered, sequentially, e.g., IEEE 802.1a, …, 802.1z, 802.1aa, 802.1ab, …

- Recently they started showing base standards in the additions, e.g., IEEE 802.1Qau-2010
IEEE 802.11 Features

- Original IEEE 802.11-1997 was at 1 and 2 Mbps. Newer versions at 11 Mbps, 54 Mbps, 108 Mbps, 200 Mbps, …
- All versions use “License-exempt” spectrum
- Need ways to share spectrum among multiple users and multiple LANs ‐ Spread Spectrum (CDMA)
- Three Phys:
  - Direct Sequence (DS) spread spectrum using ISM band
  - Frequency Hopping (FH) spread spectrum using ISM band
  - Diffused Infrared (850-900 nm) bands
- Supports multiple priorities
- Supports time-critical and data traffic
- Power management allows a node to doze off
### ISM Bands

- Industrial, Scientific, and Medical bands. License exempt

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Bandwidth</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.765 MHz</td>
<td>6.795 MHz</td>
<td>30 kHz</td>
<td></td>
</tr>
<tr>
<td>13.553 MHz</td>
<td>13.567 MHz</td>
<td>14 kHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>26.957 MHz</td>
<td>27.283 MHz</td>
<td>326 kHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>40.660 MHz</td>
<td>40.700 MHz</td>
<td>40 kHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>433.050 MHz</td>
<td>434.790 MHz</td>
<td>1.74 MHz</td>
<td>Europe, Africa, Middle east, Former Soviet Union</td>
</tr>
<tr>
<td>902.000 MHz</td>
<td>928.000 MHz</td>
<td>26 MHz</td>
<td>America, Greenland</td>
</tr>
<tr>
<td>2.400 GHz</td>
<td>2.500 GHz</td>
<td>100 MHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>5.725 GHz</td>
<td>5.875 GHz</td>
<td>150 MHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>24.000 GHz</td>
<td>24.250 GHz</td>
<td>250 MHz</td>
<td>Worldwide</td>
</tr>
<tr>
<td>61.000 GHz</td>
<td>61.500 GHz</td>
<td>500 MHz</td>
<td></td>
</tr>
<tr>
<td>122.000 GHz</td>
<td>123.000 GHz</td>
<td>1 GHz</td>
<td></td>
</tr>
<tr>
<td>244 GHz</td>
<td>246 GHz</td>
<td>2 GHz</td>
<td></td>
</tr>
</tbody>
</table>


©2018 Raj Jain
North American Channels

2.4 GHz Band: 14 5-MHz Channels. Only 12 in USA.
20 MHz Þ Only 3 non-overlapping channels

Channel 1  Channel 3  Channel 5  Channel 6  Channel 7  Channel 9  Channel 11

2400 2402 2412 2422 2432 2442 2452 2462 2472 2482

5 GHz Band: 12 non-overlapping channels

36 40 44 48 52 56 60 64

5150 5180 5200 5220 5240 5260 5280 5300 5320 5350

149 153 157 161

5725 5745 5765 5785 5805 5825
IEEE 802.11 Physical Layers

- Issued in several stages
- First version in 1997: IEEE 802.11
  - Includes MAC layer and three physical layer specifications
  - Two in 2.4-GHz band and one infrared
  - All operating at 1 and 2 Mbps
  - No longer used
- Two additional amendments in 1999:
  - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz, **OFDM**
  - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/22 MHz
- Fourth amendment:
  - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, **OFDM**
A can hear B, B can hear C, but C cannot hear A.

C may start transmitting while A is also transmitting

⇒ A and C can't detect collision.

CSMA/CD is not possible

⇒ Only the receiver can help avoid collisions
4-Way Handshake

Access Point

Mobile Node

Ready to send

Clear to send

Data

Ack
IEEE 802.11 MAC

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- Avoids collision by sending a short message: Ready to send (RTS)
  RTS contains dest. address and duration of message.
  Tells everyone to back off for the duration.
- Destination sends: Clear to send (CTS)
  Other stations set their network allocation vector (NAV) and wait for that duration
- Can not detect collision $\Rightarrow$ Each packet is acked.
- MAC-level retransmission if not acked.
IEEE 802.11 Priorities

- Initial interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (SIFS)
- Medium priority time-critical frames use “Point Coordination Function IFS” (PIFS)
- Asynchronous data frames use “Distributed coordination function IFS” (DIFS)
Time Critical Services

- Timer critical services use **Point Coordination Function**
- The point coordinator allows only one station to access
- Coordinator sends a beacon frame to all stations. Then uses a polling frame to allow a particular station to have contention-free access
- Contention Free Period (CFP) varies with the load.
IEEE 802.11 DCF Backoff

- MAC works with a single FIFO Queue
- Three variables:
  - Contention Window (CW)
  - Backoff count (BO)
  - Network Allocation Vector (NAV)
- If a frame (RTS, CTS, Data, Ack) is heard, NAV is set to the duration in that frame. Stations sense the media after NAV expires.
- If the medium is idle for DIFS, and backoff (BO) is not already active, the station draws a random BO in [0, CW] and sets the backoff timer.
- If the medium becomes busy during backoff, the timer is stopped and a new NAV is set. After NAV, back off continues.
Initially and after each successful transmission:

\[ CW = CW_{\text{min}} \]

After each unsuccessful attempt

\[ CW = \min\{2CW + 1, CW_{\text{max}}\} \]

Example: \( CW_{\text{min}} = 3, \quad CW_{\text{max}} = 127 \)

3, 7, 15, 31, 63, 127, 127, 127, …
**Typical Parameter Values**

- For DS PHY: Slot time = 20 us, SIFS = 10 us, CWmin = 31, CWmax = 1023
- For FH PHY: Slot time = 50 us, SIFS = 28 us, CWmin = 15, CWmax = 1023
- 11a: Slot time = 9 us, SIFS= 16 us, CWmin= 15, CWmax=1023
- 11b: Slot time = 20 us, SIFS = 10 us, CWmin= 31, CWmax=1023
- 11g: Slot time = 20 us or 9 us, SIFS = 10 us, CWmin= 15 or 31, CWmax=1023
- PIFS = SIFS + 1 slot time
- DIFS = SIFS + 2 slot times
Virtual Carrier Sense

- Every frame has a “Duration ID” which indicates how long the medium will be busy.
  - RTS has duration of \( \text{RTS} + \text{SIF} + \text{CTS} + \text{SIF} + \text{Frame} + \text{SIF} + \text{Ack} \)
  - CTS has duration of \( \text{CTS} + \text{SIF} + \text{Frame} + \text{SIF} + \text{Ack} \)
  - Frame has a duration of \( \text{Frame} + \text{SIF} + \text{ACK} \)
  - ACK has a duration of \( \text{ACK} \)

- All stations keep a “Network Allocation Vector (NAV)” timer in which they record the duration of each frame they hear.

- Stations do not need to sense the channel until NAV becomes zero.
DCF Example

- Example: Slot Time = 1, CWmin = 5, DIFS=3, PIFS=2, SIFS=1
- T=1 Station 2 wants to transmit but the media is busy
- T=2 Stations 3 and 4 want to transmit but the media is busy
- T=3 Station 1 finishes transmission.
- T=4 Station 1 receives ack for its transmission (SIFS=1)
  - Stations 2, 3, 4 set their NAV to 1.
- T=5 Medium becomes free
- T=8 DIFS expires. Stations 2, 3, 4 draw backoff count between 0 and 5.
  - The counts are 3, 1, 2

![DCF Diagram](image-url)
DCF Example (Cont)

- T=9 Station 3 starts transmitting. Announces a duration of 8 (RTS + SIFS + CTS + SIFS + DATA + SIFS + ACK). Station 2 and 4 pause backoff counter at 2 and 1 resp. and wait till T=17.
- T=15 Station 3 finishes data transmission.
- T=16 Station 3 receives Ack.
- T=17 Medium becomes free.
- T=20 DIFS expires. Station 2 and 4 notice that there was no transmission for DIFS. Stations 2 and 4 start their backoff counter from 2 and 1, respectively.
- T=21 Station 4 starts transmitting RTS.
IEEE 802.11 Architecture

- Station
- Access Point
- Basic Service Set
- Server
- Distribution System
- IBSS
- Ad-hoc Station
- Ad-hoc network
- 2nd BSS
- Station
IEEE 802.11 Architecture (Cont)

- **Basic Service Area (BSA)** = Cell
- Each BSA may have several access points (APs)
- **Basic Service Set (BSS)**
  = Set of stations associated with one AP
- **Distribution System (DS)** - wired backbone
- **Extended Service Area (ESA)** = Multiple BSAs interconnected via a distribution system
- **Extended Service Set (ESS)**
  = Set of stations in an ESA
- **Independent Basic Service Set (IBSS)**: Set of computers in ad-hoc mode. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks
### Frame Format

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Adr 1</th>
<th>Adr 2</th>
<th>Adr 3</th>
<th>Seq Control</th>
<th>Adr 4</th>
<th>Info</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>16b</td>
<td>16b</td>
<td>48b</td>
<td>48b</td>
<td>48b</td>
<td>16b</td>
<td>48b</td>
<td>32b</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prot. Ver.</th>
<th>Type</th>
<th>Sub type</th>
<th>To DS</th>
<th>From DS</th>
<th>More Frag.</th>
<th>Retry</th>
<th>Power mgt</th>
<th>More Data</th>
<th>WEP</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>2b</td>
<td>2b</td>
<td>4b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
<td>1b</td>
</tr>
</tbody>
</table>

- **Type**: Control, management, or data
- **Sub-Type**: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, …
- **Retry/retransmission**
- **Going to Power Save mode**
- **More buffered data at AP for a station in power save mode**
- **Wireless Equivalent Privacy (Security) info in this frame**
- **Strict ordering**
MAC Frame Fields

- **Duration/Connection ID:**
  - If used as duration field, indicates time (in us) channel will be allocated for successful transmission of MAC frame. Includes time until the end of Ack
  - In some control frames, contains association or connection identifier

- **Sequence Control:**
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver
802.11 Frame Address Fields

- All stations filter on “Address 1”

<table>
<thead>
<tr>
<th>To Distribution System</th>
<th>From Distribution System</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>Destination Address</td>
<td>Source Address</td>
<td>BSS ID</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Destination Address</td>
<td>BSS ID</td>
<td>Source Address</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>BSS ID</td>
<td>Source Address</td>
<td>Destination Address</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Receiver Address</td>
<td>Transmitter Address</td>
<td>Destination Address</td>
<td>Source Address</td>
</tr>
</tbody>
</table>
802.11 Power Management

- Station tells the base station its mode: Power saving (PS) or active
- Mode changed by power mgmt bit in the frame control header.
- All packets destined to stations in PS mode are buffered
- AP broadcasts list of stations with buffered packets in its beacon frames: Traffic Indication Map (TIM)
- Subscriber Station (SS) sends a PS-Poll message to AP, which sends one frame. More bit in the header Þ more frames.
- With 802.11e unscheduled Automatic Power Save Delivery (APSD): SS transmits a data or null frame with power saving bit set to 0. AP transmits all buffered frames for SS.
- With Scheduled APSD mode: AP will transmit at pre-negotiated time schedule. No need for polling.
- Hybrid APSD mode: PS-poll for some. Scheduled for other categories
Summary

1. 802.11 uses Frequency hopping, Direct Sequence CDMA, OFDM
2. 802.11 PHYs: 802.11, 802.11a, 802.11b, 802.11g
3. Allows both: Ad-Hoc vs. Infrastructure-based
4. 802.11 supports single FIFO Q. Uses SIFS, PIFS, DIFS
Two 802.11 stations get frames to transmit at time $t=0$. The 3rd station (AP) has just finished transmitting data for a long packet at $t=0$ to Station 1. The transmission parameters are: Slot time=1, SIFS=1, DIFS=3, CWmin=5, CWmax=7. Assume that the pseudo-random number generated are 1, 3. The data size for both stations is 3 slots. Draw a transmission diagram. At what time the two packets will get acknowledged assuming no new arrivals.
Reading List

Wikipedia Links

- http://en.wikipedia.org/wiki/Wi-Fi
- http://en.wikipedia.org/wiki/Distributed_Coordination_Function
- http://en.wikipedia.org/wiki/Carrier_sense_multiple_access
- http://en.wikipedia.org/wiki/Multiple_Access_with_Collision_Avoidance_for_Wireless
- http://en.wikipedia.org/wiki/Point_Coordination_Function
- http://en.wikipedia.org/wiki/Wi-Fi_Alliance
Acronyms

- Ack: Acknowledgement
- AP: Access Point
- APSD: Automatic Power Save Delivery
- BO: Backoff
- BSA: Basic Service Area
- BSS: Basic Service Set
- BSSID: Basic Service Set Identifier
- CA: Collision Avoidance
- CD: Collision Detection
- CDMA: Code Division Multiple Access
- CFP: Contention Free Period
- CRC: Cyclic Redundancy Check
- CSMA: Carrier Sense Multiple Access
- CTS: Clear to Send
- CW: Congestion Window
- CWmax: Maximum Congestion Window
Acronyms (Cont)

- CWmin: Minimum Congestion Window
- DA: Destination Address
- DCF: Distributed Coordination Function
- DIFS: DCF Inter-frame Spacing
- DS: Direct Sequence
- ESA: Extended Service Area
- ESS: Extended Service Set
- FH: Frequency Hopping
- FIFO: First In First Out
- GHz: Giga Hertz
- IBSS: Independent Basic Service Set
- ID: Identifier
- IEEE: Institution of Electrical and Electronics Engineers
- IFS: Inter-frame spacing
- ISM: Instrumentation, Scientific and Medical
- LAN: Local Area Network
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MHz</td>
<td>Mega Hertz</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>NAV</td>
<td>Network Allocation Vector</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>PCF</td>
<td>Point Coordination Function</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PIFS</td>
<td>PCF inter-frame spacing</td>
</tr>
<tr>
<td>PS</td>
<td>Power saving</td>
</tr>
<tr>
<td>RA</td>
<td>Receiver Address</td>
</tr>
<tr>
<td>RPR</td>
<td>Resilient Packet Ring</td>
</tr>
<tr>
<td>RTS</td>
<td>Ready to Send</td>
</tr>
<tr>
<td>SA</td>
<td>Source Address</td>
</tr>
<tr>
<td>SIFS</td>
<td>Short Inter-frame Spacing</td>
</tr>
</tbody>
</table>
Acronyms (Cont)

- SS  Subscriber Station
- TA  Transmitter's Address
- TIM Traffic Indication Map
- WEP Wired Equivalent Privacy
- Wi-Fi Wireless Fidelity
- WLAN Wireless Local Area Network
Scan This to Download These Slides

Raj Jain
http://rajjain.com
Related Modules

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWQSPMh8Azegy5e_10TiDw

Recent Advances in Networking (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFeXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wNP9-ruOzQMs-8NUw