IEEE 802.11 details

- 802.11 standards group: http://grouper.ieee.org/groups/802/11/
- Standards on IEEE Xplore: http://www.ieee.org/ieeexplore
- WiFi: www.weca.net

802.11 around the world:
- Uniwide network: www.uniwide.unsw.edu.au
- Sydney wireless: www.sydneywireless.com
- 802.11 Planet: www.80211-planet.com

Topics covered:
- Layering and varieties of 802.11
- Types of 802.11 networks
- Types of 802.11 devices
- 802.11 MAC & frame types
- Discovering & associating with wireless LANs
- Error control

Not covered: security
Warning about standards language

They have to be precise and specific, so they often invent their own words/abbreviations so that existing words are not interpreted in unintended ways.

e.g.:

- **IEEE 802.11:**
  - Medium Access Control Protocol Data Unit (MPDU) ~ frame
  - Independent Basic Service Set (IBSS) ~ ad hoc network

- **octet: 8 bits ~ byte** (but not for ancient computers with 9b or 10b bytes)
Sublayering of 802.11 link “layer”

TCP/IP theory

- Application
- Transport
- Network
- Link

Reality

- Driver interface
  - LLC
  - 802.1 bridging
  - MAC
  - PLCP
  - PMD

Linux Wireless Extensions
Windows Network Device Interface Spec.

Logical Link Control
(not always used)

(Present in switches, but not end-systems)

802.11, 802.11e

Physical Layer Convergence Protocol:
frame tx/rx and channel status (carrier sense)

Physical Medium Dependent:
RF, modulation & transmission
802.11 (IR, FHSS, DSSS), 802.11a, b, g

= not always present
# 802.11 Physical Layers

<table>
<thead>
<tr>
<th>Standard</th>
<th>802.11</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>1997</td>
<td>1999</td>
<td>2003</td>
<td>1999</td>
</tr>
<tr>
<td>Frequency</td>
<td>850-950nm Infrared</td>
<td>2.4GHz FHSS</td>
<td>2.4GHz HR DSSS</td>
<td>5GHz OFDM</td>
</tr>
<tr>
<td>Modulation</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Supported rates (Mb/s):</td>
<td>2</td>
<td>2</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>5.5</td>
<td>5.5</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>11</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>24</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>36</td>
<td>48</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes about rates:**

- Transmission rate often auto-selected, depending on signal strength and range supported by local network.
- Compatibility achieved by sending RTS/CTS at base rate.
- These are nominal rates > achievable rate, because of transmission errors, Phy headers, MAC spaces (IFS, CW etc).

- e.g. 6Mb/s TCP/IP over 11Mb/s 802.11b

*SS = spread spectrum*

*FHSS = Frequency Hopping SS*

*DSSS = Direct Sequence SS*

*HR = (relatively) High Rate*

*OFDM = Orthogonal Frequency Division Multiplexing*
802.11 networks

2 types:

**Infrastructure**: Contain end-system stations, as well as **Access Points** (equivalent to Base Stations in cellular telephony systems)

- A Distribution System (often wired, e.g. Ethernet, but can also use 802.11) may be used to connect APs.
- APs may provide connectivity to other networks that connect end-systems, e.g. bridge to Ethernet LAN. That LAN may then provide wider connectivity, e.g. to the Internet.
- Area covered by AP(s) is often called a “hotspot”

**“ad hoc”** (IBSS) – no infrastructure. Stations communicate directly with each other. (802.11 notion of “ad hoc” is slightly different from the network layer notion of stations routing each other’s traffic.)
Geographically overlapping networks

Multiple networks may cover same physical area:
• emanations from private properties (e.g. adjacent apartments, businesses, etc)
• competition for the same spaces (e.g. airport terminal, parks, business premises)
• overlapping for fault tolerance

They may be separated by:
• using different channels, particularly if they are coordinated (e.g. deliberate overlap for fault tolerance)
• sharing the medium over time

Logically distinct networks have distinct identifiers (“Service Set Identifiers”), which stations can use to select which network they wish to use.
802.11 devices

† A strange term, given that they needn’t be stationary. Used because of traditional use in other 802 standards & the time-varying characteristics of the wireless medium prevent distinction at the MAC layer between stationary & mobile devices.

Photos from www.symbol.com
Cisco Aironet 240 NIC

256KB Flash RAM
AMD AM29LV002BB

RF-IF convertor
HFA3683A

Power amp
HFA3983

oscillator
DS1073

Aironet MAC chip
608-004808-1

Baseband Processor
HFA3861B

128k×16 SRAM
IS61LV12B16-15LQ

IQ modem
HFA3783

Serial #
DS2401

D-Link DWL-1000AP
Intersil chipset:
3983: 2.4GHz power amp & detector
3683: 2.4GHz RF converter &
3783: I/Q modem
Spreading & attenuating wireless signals

802.11 MAC

2 modes (“Coordination Functions”):

• **Distributed Coordination Function**:
  • Random access
  • Uses immediate acknowledgements
  • RTS & CTS (stations adhere to RTS, if they hear it)
    • Virtual carrier is recorded in a “Network Allocation Vector”. e.g. see fragmentation slide

• **Point Coordination Function**: for Contention-Free (CF†) access.
  Uses AP polling, and can provide service guarantees.
  Rarely implemented. Likely to be succeeded by new 802.11e Hybrid CF.

† Yes, another meaning for the same abbreviation.
Typical frame exchanges

Figure 49—Some IFS relationships

Figure from 802.11 standard

Copyright © 2003, Tim Moors
Interframe spaces (IFS)

Stations leave medium idle for an “interframe space” (IFS) before transmitting. Larger IFS gives lower priority:

**Short IFS** (10µs) – used to separate consecutive frames in an exchange (e.g. frame→SIFS→ack). Gives the radio time to turnaround.

**PCF IFS** (30µs) – Gives Coordinator priority over DCF

**DCF IFS** (50µs) – Distributed access

**Extended IFS** (DIFS+SIFS+ACK time): Receiver of erroneous frame can’t transmit for this interval after reception of the frame.

If the error was in the DA, this gives the proper destination time to transmit an ACK.

If the error was elsewhere in the frame, this gives the source time to timeout on waiting for ACK & to start retransmission.
MAC frame types

All frames are prefaced by a Phy preamble and header. The duration of these depends on the Phy, but is considerable, e.g. 96µs or 192µs for 802.11b (compare to 224b MAC header @ 11Mb/s = 20.4µs)

All MAC Frames start with:
• a **Frame Control** field (2B) which includes:
  • Type field: which of 3 major types of frame
  • Subtype indicates which specific frame it is & structure of remainder of header.
• a **Duration** field (2B), indicating duration of this frame (& associated follow-on frames) for virtual carrier.
• an **Address** (6B) of the intended receiver of this frame

Frame types:
• **Data frames** – see next slide
• **Control frames** – supports data transfer, Subtypes: RTS/CTS & ACK, CF-End, PS-Poll (for PCF with power saving)
• **Management frames** – Subtypes: for discovery (Beacons, Probes), Association, Authentication
IEEE 802.11 Data frames

- Maximum 802.11 payload = 2312B > 1500B of Ethernet ⇒ potential problems when bridging between the two.
- tail of “Payload” may contain 7B of encryption keys for Wired Equivalent Privacy (WEP)
Discovering wireless LANs

Advertising:
Access Points can be configured to periodically emit “Beacon” frames, disclosing (amongst other things) their identifier (SSID) (ASCII string of 0-32B) & their presence.

Soliciting by station:
• Station can send a “Probe” frame, indicating the identifier of the AP that they wish to discover & rates that the station supports.
• AP then (if it wants to) sends a “Probe response” that carries the same information as a Beacon. (Better than a Beacon, since it can be encrypted & isn’t disclosed as often.)
802.11 “association”

After a station discovers wireless LANs that cover its location, it needs to “associate” itself with one of them.

Association (deassociation & reassociation) allows:

• Mobile station to tell APs where it is located, so they can forward traffic towards it.
• Station to select which (physically overlapping) wireless LAN it wants to use
• APs to select which stations they are willing to support (e.g. based on load balancing).

A station that isn’t associated can still transmit using the shared medium, but AP won’t forward its traffic (e.g. onto the Internet) ⇒ rogue station can deny service to others, but can’t steal service for itself.
Beacon frames

Carry:

• **Identifier for wireless network:** (SSID)

• **Phy parameters**, e.g. supported rates (aBasicRateSet) ⇒ what rate to use for RTS/CTS & multicast

• **Power management** info, e.g. indicating if AP offers buffering service, providing synchronisation info allowing stations to sleep.

• **Indicate start of Contention Free Period** (for PCF)
802.11 error control

Acknowledgements – also used for MAC (collision detection)
Receiver sends ACK one SIFS after receiving a unicast frame.
• Disabled for multicast (& ⇒ broadcast)
• All other payload-bearing frames are delivered reliably.
  MAC Service interface doesn’t allow higher layers to indicate whether data
  needs acknowledgement. Even unicast UDP packets are delivered reliably.
• 802.11 has retry limits (LongRetryLimit=4 & ShortRetryLimit=7)
  which limit the persistence of retransmission attempts.
• MAC layer retransmissions introduce possibility of duplication
  ⇒ Sequence Control field to detect & recover from this.
• MAC layer retransmissions can interfere with transport layer,
  e.g. transport may timeout while MAC is still retransmitting ⇒ transport
  retransmits, but MAC retransmission would have succeeded
802.11 fragmentation

Large packets have high probability of incurring an error & have high cost (long useless errored tx + long retx)
⇒ Fragmentation: Break large frames (size exceeding “aFragmentationThreshold” parameter) into smaller frames (of “aFragmentationThreshold” bytes)

802.11 uses a stop-and-wait protocol:
1. Send fragment.
2. Stop, and wait for ACK before sending next fragment
3. If timeout before receiving ACK:
   1. Source halts transmission of the frame
   2. Recontends for channel access
   3. Continues with the last unacknowledged fragment.

Transmission duration when using fragmentation depends on the number of errors experienced ⇒ extend virtual carrier (NAV) one fragment at a time, and recontend for access if don’t receive ACK (to prevent hogging by station that can’t receive ACKs)
Frame exchange & virtual carrier with frag

time

- RTS
- Fragment 0
- Fragment 1
- Frag. 2

frame exchange

- CTS
- ACK 0
- ACK 1
- ACK 2

virtual carrier

"Network Allocation Vector"

- NAV (RTS)
- NAV (CTS)
- NAV (Fragment 0)
- NAV (Fragment 1)
- NAV (ACK 0)
- NAV (ACK 1)
- NAV (Frag. 2)

= information heard near source. NAV(X) indicates NAV carried in frame X
= information heard near destination
= SIFS spacing

Copyright © 2003, Tim Moors
Power issues

Many devices using wireless communications are designed to be mobile ⇒ energy efficiency is important:
• no connection to mains power
• small batteries for small form factor
• don’t want to have to regularly recharge batteries
• minimise emission power for human safety

Energy efficiency also increases spectral capacity through spatial reuse.

802.11 Approach to power management:
• Synchronize stations (using Beacon) & transmit multicast at known times ⇒ stations with limited power needn’t always listen.

  2 frames (1 multicast, and a latter one unicast) may be destined to one receiver. It may receive them out of order (unlike conventional LANs) because of power-saving multicast sync. ⇒ strictly ordered service (O bit in header)

• Access Point (if it exists) can buffer frames destined to sleeping stations & forward them when stations are known to awaken.

Implications for higher layers: Synchronisation to save power may delay frames
Recap on multicast issues

Implosion problem:
• Can’t detect collisions using ACKs
• Can’t use RTS/CTS to avoid collisions.
Can “avoid” collisions with random delay before transmission.

Prefer to schedule multicast transmissions to enable power conservation.
May lead to misordering of unicast traffic relative to multicast traffic, unless costly precautions are taken.