Outline

LANs: IEEE 802.11
MANs: 802.16 "Broadband" Wireless
PANS: IEEE 802.15
  * 802.15.1: Bluetooth
     • much fanfare late 90s, but too complicated/expensive to take off?
  * 802.15.3a: Ultrawideband
  * 802.15.4: ZigBee

802.15.2 addresses coexistence of wireless LANs and PANs
802.20 is another MAN standard focusing on mobility

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:
  * UNSW Uniwide network: www.uniwide.unsw.edu.au
  * Sydney wireless: www.sydneywireless.com
  * WiFi Planet: www.wifiplanet.com

Topics covered:
  * Layering and varieties of 802.11
  * 802.11 MAC
  * 802.11 frame types
  * Discovering & associating with wireless LANs

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>
<th>802.11n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>1997</td>
<td>1999</td>
<td>2003</td>
<td>1999</td>
<td></td>
</tr>
<tr>
<td>Frequency</td>
<td>850-950nm Infrared</td>
<td>2.4GHz FHSS</td>
<td>2.4GHz DSSS</td>
<td>2.4GHz OFDM</td>
<td>5GHz OFDM</td>
</tr>
<tr>
<td>Modulation</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Supported rates (Mb/s)</td>
<td>54</td>
<td>48</td>
<td>36</td>
<td>24</td>
<td>18</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
Physical layer
headers/preambles

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)

e.g. sending one TCP acknowledgement @ "11Mb/s" requires:

\[
\begin{align*}
\text{RTS} &= 11\mu s = 96\mu s + 20B@11Mb/s \\
\text{SIFS} &= 10\mu s \\
\text{CTS} &= 106\mu s = 96\mu s + 14B@11Mb/s \\
\text{data} &= 15\mu s + 28B\text{ MAC hdr} + 40B\text{ TCP/IP ACK}@11Mb/s \\
\text{SIFS} &= 10\mu s \\
\text{ACK} &= 106\mu s = 96\mu s + 14B@11Mb/s \\
\text{data} &= 145\mu s = 96\mu s + (28B\text{ MAC hdr} + 40B\text{ TCP/IP ACK})@11Mb/s \\
\text{SIFS} &= 10\mu s \\
\text{ACK} &= 106\mu s = 96\mu s + 14B@11Mb/s \\
\text{total} &= 498\mu s \\
\end{align*}
\]

\[\frac{40B}{498\mu s} = 0.64\text{Mb/s} \text{ omitting randomisation delays and errors}\]

More realistically: 2 × 1500B TCP segments + 1 ACK takes 3616µs = 6.6Mb/s

\[\Rightarrow \text{throughput} \ll \text{nominal rate}\]

Outline

802.11 MAC

2 modes ("Coordination Functions" – CF):

• **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.
  - Has priority over DCF by virtue of using shorter interframe spaces (PIFS < DIFS)
  - 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.

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 Point Coordinator priority over DCF

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

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

- If the error was in the DA and limited to this receiver, 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 MAC Frames start with:
- a **Frame Control** field (2B) which includes:
  - **Type field**: which of 3 major types of frame:
    - 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
  - **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 & allows sleep.
- an **Address** (6B) of the intended receiver of this frame

IEEE 802.11 Data frames

```
+----------+----------+------------------------------+-----------------+-------------------+-------------------+
| Ver|Typ|Subtype|Dir|F|R|P|D|W|O|            Duration           |
+----------+----------+------------------------------+-----------------+-------------------+-------------------+
|                   Destination Address                         |
+                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |       Source Address          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |                                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Basic Service Set Identifier                      |
+                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               | Frag# |   Sequence number     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Frame Check Sequence                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- **Dir**: Direction: 2 flags indicating to/from Distribution System
- **F**: More fragments, **R**: Retry, **P**: Power management, **D**: More data, **W**: WEP, **O**: Order
- **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)**

Control frames

Standard frames for distributed wireless MAC:
- **Request To Send**
- **Clear To Send**
- **Acknowledgement**

Frames to support PCF MAC:
- **Contention-Free End**: Marks transition from PCF to DCF access
- **CF-End + CF-ACK**: CF-End with a piggybacked acknowledgement to the station that transmitted a frame to the Access Point
- **Power Save Poll**: Station that was sleeping asks Access Point for any data stored for it.

Management frames

11 different subtypes, shown in blue. Described on coming slides.

- **Discovering Access Points**:
  - Beacon
  - Probe request/response
- **Selecting Access Points**:
  - Association request/response
  - Reassociation request/response: Change Access Point
  - Disassociation: Relinquish access (for security)
- **Checking credentials**:
  - Authentication
  - Deauthentication
- **Power management**:
  - Announcement Traffic Indication Message
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)

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:
- Stations to select which (physically overlapping) wireless LAN they want to use
- APs to select which stations they are willing to support
  - e.g. reject an association request in order to reduce load, for 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 gain service (through the AP) for itself.
- Handover: Mobile station to tell APs where it is located, so they can forward traffic towards it as it moves.

Outline
Wireless MANs

IEEE 802.16 aka WiMax
( Worldwide Interoperability for Microwave Access )

Intended to address the last mile problem: connecting customers to local exchanges. (e.g. unwired.com.au )

Why 802.11 (for LANs) may be inappropriate for MANs:
- Mobility features (e.g. association) aren’t needed for stationary nodes
- Many users share a MAN link
  - Prepared to pay for more expensive radio gear
  - Use different frequencies than for LANs: .16: 10-66 GHz, .16a: 2-11GHz, .16b: 5GHz (blurring the distinction)
- MAN users pay for service and want guarantees
  ⇒ 802.16 is connection oriented and has polling-based MAC

802.16 access

Duplex communication can be provided by time division:
- Separate intervals for:
  - Downstream transmission (from base station), and
  - Upstream transmission (to base station)

Various classes of upstream access:
- Constant Bit Rate: Certain slots are dedicated to a subscriber.
- Polling service: Base station polls subscriber
  - Real-time: Regular polling
  - Non-real-time: Irregular polling, and subscriber indicates if it has more to transmit (request to be polled again)
- Best Effort: Contention-based access to residual slots and exponential backoff if unsuccessful.

The 802.16 Frame Structure

<table>
<thead>
<tr>
<th>Bit 1</th>
<th>Bit 2</th>
<th>Bit 3</th>
<th>Bit 4</th>
<th>Bit 5</th>
<th>Bit 6</th>
<th>Bit 7</th>
<th>Bit 8</th>
<th>Bit 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type</td>
<td>Length</td>
<td>Connection ID</td>
<td>Header CRC</td>
<td>Data</td>
<td>CRC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) A generic frame.
(b) A bandwidth request frame.
  (i) Type: are packing and fragmentation present?
  a. normal data frame, or
  b. bandwidth request frame
  "Bytes needed"

Outline
Some PAN technologies (e.g. Bluetooth/ZigBee) sacrifice rate/range for cost and power conservation.

**ZigBee / IEEE 802.15.4 LR-WPAN**

ZigBee Alliance [www.zigbee.org]
IEEE 802.15.4 defines link layer aspects of ZigBee (not network and higher layers)

For details, see:

† Institution of Electrical and Electronics Engineers Low Rate Wireless Personal Area Network. The name “ZigBee” is much less of a mouthful/more “user friendly” and “is derived from the communication method used by bees for living. Bees dance in zigzags to share information on the position, distance, and direction of the food they find.” [Zheng04]

**A word about Bluetooth**

- Low-power, small radius, wireless networking technology
  - 10-100 meters
- Omnidirectional
- Not line-of-sight infrared
- Interconnects gadgets
- 2.4-2.5 GHz unlicensed radio band
- Up to 721 kbps

- Interference from wireless LANs, digital cordless phones, microwave ovens:
  - Frequency hopping helps
- MAC protocol supports:
  - Error correction
  - ARQ
- Each node has a 12-bit address

**Bluetooth Architecture**

Two piconets can be connected to form a scatternet.

This slide is from Kurose and Ross