Wireless / Mobile Networks

• Contents
  1. Wireless technologies overview
  2. Radio technology
  3. Radio technology problems
  4. 802.11 WLAN Wireless LAN
  5. Overview 1G / 2G / 2.5G / 2.75G / 3G / 4G networks
  6. 2G / 2.5G / 3G networks
  7. 4G LTE – Long Term Evolution
  8. Satellite Internet Access
  9. Wireless mobility
  10. Mobile IP RFC2002
### Wireless technologies overview (1/3):

<table>
<thead>
<tr>
<th>Standard</th>
<th>F-Spectrum</th>
<th>Data rate</th>
<th>Range</th>
<th>Power cons.</th>
<th>Applications / comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DECT</strong></td>
<td></td>
<td>552Kbps</td>
<td>100m</td>
<td>Low (by design)</td>
<td>Digital Enhanced Cordless Telephony. TDMA. Well established</td>
</tr>
<tr>
<td><strong>WLL</strong></td>
<td></td>
<td></td>
<td></td>
<td>High</td>
<td>Wireless Local Loop.</td>
</tr>
<tr>
<td><strong>IrDA</strong></td>
<td>IrDA</td>
<td>1.6Mbps</td>
<td>8m</td>
<td>Low</td>
<td>Infrared; transmission needs line of sight. Mostly used for remote controls.</td>
</tr>
<tr>
<td><strong>BlueTooth</strong></td>
<td>802.15.1</td>
<td>2.45MHz ISM</td>
<td>1Mbps</td>
<td>Medium</td>
<td>Consumer market (mice, PDAs, keyboards). Pretty complex technology.</td>
</tr>
<tr>
<td><strong>WiBree</strong></td>
<td>WiBree / BT</td>
<td>2.45MHz ISM</td>
<td>1Mbps</td>
<td>Very low</td>
<td>Derived from Bluetooth; targets very low power applications. Integrated in Bluetooth standard in 2007 as ULP (Ultra Low Power). Apps: consumer, medical, sports &amp; wellness (watches etc.).</td>
</tr>
<tr>
<td><strong>UWB</strong></td>
<td>802.15.3a</td>
<td>&lt;8m</td>
<td>&lt;480Mbps</td>
<td>10m</td>
<td>Ultra Wide Band. Very high BW for PANs.</td>
</tr>
<tr>
<td><strong>WirelessHD</strong></td>
<td>802.15.3c</td>
<td>57-64GHz</td>
<td>3GBbps</td>
<td>10m</td>
<td>Wireless PHY and MAC layer for use in HD WVAN (Wireless Video Area Network)</td>
</tr>
<tr>
<td><strong>ZigBee</strong></td>
<td>802.15.4</td>
<td>2.4GHz</td>
<td>915MHz (US)</td>
<td>128Kbps</td>
<td>Low (by design)</td>
</tr>
<tr>
<td><strong>MIWI</strong></td>
<td>802.15.4, MIWI</td>
<td>908.42MHz (US)</td>
<td>9.6Kbps</td>
<td>100m</td>
<td>ZigBee alternative from Microchip. Uses IEEE 802.15.4 radio; low cost (licenses!) alternative to ZigBee. No certification required.</td>
</tr>
<tr>
<td><strong>Z-Wave</strong></td>
<td>Z-Wave Alliance</td>
<td>902-928MHz (US)</td>
<td>9.6Kbps</td>
<td>100m</td>
<td>Home appliances, sensors. Designed for robustness (crowded frequency bands).</td>
</tr>
<tr>
<td><strong>Ant</strong></td>
<td>Proprietary (Dynastream)</td>
<td>2.4GHz</td>
<td>&lt;57Kbps</td>
<td>30m</td>
<td>Very low</td>
</tr>
<tr>
<td><strong>HomeRF</strong></td>
<td>?</td>
<td>2.4GHz</td>
<td>20Mbps</td>
<td>Very low</td>
<td>Was competitor to 802.11. Now defunct</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11a</td>
<td>5GHz</td>
<td>&lt;54Mbps</td>
<td>150m</td>
<td>High</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11b</td>
<td>2.45GHz ISM</td>
<td>&lt;11Mbps</td>
<td>100m</td>
<td>High</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11g</td>
<td>2.45GHz ISM</td>
<td>&lt;54Mbps</td>
<td>100m</td>
<td>High</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11n</td>
<td>2.4GHz ISM</td>
<td>100-200Mbps</td>
<td>100m</td>
<td>High</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11ac</td>
<td>5GHz</td>
<td>&lt;1Gbps</td>
<td>100m</td>
<td>High</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td>802.11ad</td>
<td>2.4GHz</td>
<td>&lt;7Gbps</td>
<td>&lt;10m</td>
<td>High</td>
</tr>
<tr>
<td><strong>HiperLAN2</strong></td>
<td>HiperLAN</td>
<td>5GHz</td>
<td>&lt;480Mbps</td>
<td>10m</td>
<td>High</td>
</tr>
<tr>
<td><strong>Wireless USB</strong></td>
<td>CWUSB</td>
<td>&lt;8m</td>
<td>&lt;480Mbps</td>
<td>10m</td>
<td>?</td>
</tr>
<tr>
<td><strong>RFID</strong></td>
<td>EPCglobal Gen2 ISO/IEC 18000</td>
<td>Div. (13.56MHz, 135kHz, 2.45GHz, 860 MHz to 960 MHz, 433MHz)</td>
<td>100Kbps</td>
<td>1m</td>
<td>Zero</td>
</tr>
</tbody>
</table>
### Wireless technologies overview (2/3):

<table>
<thead>
<tr>
<th>Technology</th>
<th>Standard</th>
<th>F-Spectrum</th>
<th>Data rate</th>
<th>Range</th>
<th>Power cons.</th>
<th>Applications / comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WiMAX</strong></td>
<td>802.16a, d</td>
<td>Div.</td>
<td>75Mbp/s</td>
<td>6km</td>
<td>High</td>
<td>Mobile MAN (users with PDAs, nomads). Will probably be supplanted by LTE.</td>
</tr>
<tr>
<td><strong>WRAN</strong></td>
<td>802.22</td>
<td>TV broadcast frequencies</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>WRAN is a new working group in IEEE for using TV frequency for broadband access.</td>
</tr>
<tr>
<td><strong>WiBro</strong></td>
<td>802.16e</td>
<td>2.3GHz</td>
<td>1Mbp/s</td>
<td>&lt;=1km</td>
<td>Low</td>
<td>South Korean competitor to WiMAX. Mobile (60km/h moving mobile devices).</td>
</tr>
<tr>
<td><strong>GSM (G2)</strong></td>
<td>Div.</td>
<td>850/1800/1900</td>
<td>14.4Kbp/s</td>
<td>15km</td>
<td>Low</td>
<td>2nd generation mobile telephony technology.</td>
</tr>
<tr>
<td><strong>CDMA (G2)</strong></td>
<td>Div.</td>
<td>?</td>
<td>2Mbps</td>
<td>15km</td>
<td>Low</td>
<td>G2 technology used in US and other countries (competitor to GSM).</td>
</tr>
<tr>
<td><strong>EDGE (G2.5)</strong></td>
<td>850/1800/1900</td>
<td>?</td>
<td>384Kbps</td>
<td>15km</td>
<td>Low</td>
<td>Enhanced Data rates for GSM Evolution (2.5G); technology between G2 (GSM) and UMTS (G3).</td>
</tr>
<tr>
<td><strong>CDMA2000 (G3)</strong></td>
<td>?</td>
<td>?</td>
<td>144Kbps</td>
<td>?</td>
<td>?</td>
<td>Competitor to UMTS</td>
</tr>
<tr>
<td><strong>UMTS (G3)</strong></td>
<td>Div.</td>
<td>?</td>
<td>2Mbps</td>
<td>15km</td>
<td>Low</td>
<td>Would-be successor to GSM. Slow adoption rate, but picking up speed.</td>
</tr>
<tr>
<td><strong>LTE (G3.9/G4)</strong></td>
<td>3GPP LTE</td>
<td>Candidate: 2.6GHz</td>
<td>160 Mbp/s (DL)</td>
<td>&lt;30km</td>
<td>?</td>
<td>4G technology, potential successor to UMTS. Based on TCP/IP, no TDM. Low latency (&lt;5ms) for IP packets.</td>
</tr>
<tr>
<td><strong>io-homecontrol</strong></td>
<td>io-homecontrol</td>
<td>868MHz</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>Low</td>
</tr>
<tr>
<td><strong>WHDI</strong></td>
<td>WHDI 1.0</td>
<td>5GHz</td>
<td>&lt;3Gbps</td>
<td>30m</td>
<td>High</td>
<td>Home entertainment. Industry initiative (Sony et.al.). Competitor of WirelessHD.</td>
</tr>
<tr>
<td><strong>WiGig</strong></td>
<td>802.11MAC 1.0</td>
<td>2.4/5/60GHz</td>
<td>&lt;7Gbps</td>
<td>?</td>
<td>High?</td>
<td>Home entertainment. Industry initiative by HW vendors (Atheros, Nokia et.al.). Competitor of WirelessHD. Uses 802.11 MAC for compatibility.</td>
</tr>
<tr>
<td><strong>VSAT</strong></td>
<td>?</td>
<td>~0.5Mbp/s</td>
<td>3000km</td>
<td>High</td>
<td>Very small aperture Satellite</td>
<td></td>
</tr>
<tr>
<td><strong>TETRAPOL</strong></td>
<td>ETSI</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>Voice and data radio technology for public services (police etc.).</td>
</tr>
</tbody>
</table>
Wireless / Mobile Networks

- Wireless technologies overview (3/3):

<table>
<thead>
<tr>
<th>Technology</th>
<th>Bandwidth [Mb/s]</th>
<th>Range [km]</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.15.3a UWB</td>
<td>110-480</td>
<td>10</td>
<td>WPAN</td>
</tr>
<tr>
<td>IEEE 802.15.1 BlueTooth</td>
<td>723</td>
<td>10</td>
<td>WPAN</td>
</tr>
<tr>
<td>IEEE 802.15.4 / ZigBee</td>
<td>128</td>
<td>100</td>
<td>WPAN / HAN</td>
</tr>
<tr>
<td>DECT</td>
<td>552</td>
<td>100</td>
<td>TDMA</td>
</tr>
<tr>
<td>RFID</td>
<td>~0</td>
<td>&lt;1</td>
<td>B/s</td>
</tr>
<tr>
<td>CDMA2000</td>
<td>EDGE (2.75G)</td>
<td>384KBps</td>
<td>15km</td>
</tr>
<tr>
<td>CDMA2000</td>
<td>HSDPA (3.5G)</td>
<td>2Mbps</td>
<td>15km</td>
</tr>
<tr>
<td>GSM (2G, HSCSD)</td>
<td>GPRS (2.5G)</td>
<td>CDMA</td>
<td>10KB/s</td>
</tr>
</tbody>
</table>

PAN: Personal Area Network  MAN: Metropolitan Area Network
HAN: Home Area Network  WAN: Wide Area Network
LAN: Local Area Network
Wireless / Mobile Networks

• Radio technology:
  ➔ Technological drivers of radio technology:
  1. Hardware: Better batteries, less power consumption, processors with higher performance.
  2. Link: Better / more sophisticated antennas, modulation and coding; DSPs with higher perf.
  3. Network: Mobility support; dynamic resource allocation.
  And: Radio is more and more becoming a software technology (DSP, protocols).

  ➔ Reuse of spectrum through spread-spectrum:
  Despite the trend that newer technologies use higher frequencies, radio bandwidth remains limited.
  Spread spectrum is a technology used to distribute the signal over a wide frequency range. Spread spectrum makes the signal less susceptible to interference and noise.

  ![Original signal]

  ![The signal is “spread“ over the frequency spectrum. The spread signal is immune against a jamming signal. The signal interferes less with other signals due to lower power level.]

  ![The receiver reconstructs signal.]

Wireless / Mobile Networks

• Radio technology problems (1/2):
Radio networks differ from wired networks in a number of aspects. Wireless protocols on layer 1 (physical) and 2 (data link) have to be augmented with the necessary functions to address these issues.

1. Hidden station problem:
A wireless station STA3 does not „hear“ STA1 (hidden station). Both STA1 and STA3 may start sending at the same time thus causing contention at STA2.

2. Eavesdropping:
Wireless networks are inherently open to eavesdropping. This means that wireless networks need protection (strong encryption) right from the start.

3. Reliability of wireless connections:
Wireless networks suffer from interference, reflections, dropouts etc. Thus wireless connections are less reliable. New (wireless) routing protocols can be used to provide multipath routing for better reliability.
Wireless / Mobile Networks

• Radio technology problems (2/2):

4. Power consumption of wireless devices:
Wireless devices inherently suffer from a power problem (wireless = mobile = runs-on-battery). Often wireless technologies (ZigBee 802.15.4, DECT, GSM) are targeted at low power applications. Other technologies like 802.11 or WiMAX 802.16 are not particularly suited for low-power applications. Usually a greater distance between the antennas requires more transmission power and thus increases the power consumption.

5. Limited bandwidth, need for frequency licensing:
Every country has its own frequency plan that regulates the use or licensing of radio frequencies. Obtaining a license is costly, thus the number of frequency license holders is limited.
In order to allow the use of certain frequencies without a costly and time consuming licensing process, most countries allow using the frequencies in the ISM (Industrial, Science, Medical) bands as defined by ITU-R (International Telecommunication Union – Radio). In recent years a number of new radio technologies emerged as a consequence of advances in technology (cheaper hardware, new modulation technologies etc.). Naturally many of these technologies (WLAN, Bluetooth, Zigbee) use the (unlicensed) ISM bands. This in turn means that interferences between different senders become a problem.
802.11 WLAN Wireless LAN (1/10):

WLAN technology:

- 802.11 networks use free frequency bands (ISM: Industrial, Science, Medical). Thus everybody can run 802.11 devices without licensing a frequency band.

Different 802.11 standards:

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps (5 GHz band).
- **802.11b**: Up to 11Mbps, simple (cheap) technology.
- **802.11g**: Up to 54Mbps.
- **802.11n**: <600Mbps (MIMO=Multiple In Multiple Out antenna technology, uses multi-path transmission for better signal recovery at the receiver).
- **802.11ac**: Forthcoming standard for higher throughput (802.11n enhancements).
- **802.11ad**: Standard in progress, even higher throughput (<7Gpbs).

802.11 Pros and Cons:

- Mobility
- Flexible configuration
- Relatively cheap
- Weak security (WEP Wired Equivalent Protection, but fixed with WPA Wired Protection Access)
- Relatively low bandwidth for data (compared to wired networks)
- Electromagnetic interference with other devices (Bluetooth)
- Simple installation, but high skills needed for exploitation of full potential of technology
Wireless / Mobile Networks

- **802.11 WLAN Wireless LAN (2/10):**
  Operation modes of 802.11:

  **Ad-hoc mode:**
  No access points; STAs communicate directly with each other.

  **Infrastructure mode:**
  Usage of access points interconnected with wired LAN.

**IBSS:**
Independent Basic Service Set

**ESM:**
Extended Service Set (Multiple cells)

**STA (STAtion):**
Station

**AP:**
Access Points

**Handover**

**DS:**
Distribution System (wired LAN)

**BSS:**
Basic Service Set (Single cell)
• 802.11 WLAN Wireless LAN (3/10):

802.11 protocol stack:

802.11 Physical layer:
The physical layer either uses OFDM or DSSS modulation.

a. OFDM:
Orthogonal Frequency Division Multiplexing (BSPK or QPSK or 16-QAM or 64-QAM).
→ Achieves more bits per frequency than DSSS (=more throughput).

b. DSSS:
Direct Sequence Spread Spectrum.

802.11 MAC:
The MAC layer controls the media access (see below).

LLC:
LLC (Logical Link Control) is not part of the WLAN stack, but is often used to provide a generic access layer to the lower (link) layers.
**802.11 WLAN Wireless LAN (4/10):**

802.11 frame structure:
The 802.11 frame structure depends on the frame type (see below).
The general 802.11 frame structure looks as follows:

- **Field length (bytes):** 2 2 6 x

- **PV To DS From DS More frag. Retry Power mgt. More data WEP Order**

- **Protocol version=0**
  - Management: Beacon, Probe etc. (see below)
  - Control: RTS, CTS, Ack
  - Data: No subtypes (always =0)

- **Dur:** Time in microseconds that the sender needs for sending the frame.
- **Address:** Receiver's MAC address
- **DS:** Distribution System (wired or wireless „backbone“ of WLAN)
- **FC:** Frame Control

- **More frag.:** 1 indicates that this is a fragmentation frame
- **Retry:** Set to 1 if this is a retransmission frame
- **Power mgt:** Power management bit
- **More data:** Indicates that >= frames are available.
  - Used for power management.
- **WEP:** WEP bit; obsolete (WEP replaced by WPA2).
- **Order:** Set to 1 if strict ordering of frames is used.
802.11 WLAN Wireless LAN (5/10):

802.11 frame types (1/3):

1. Management frame:
   Management frames are used to establish and maintain communication.

**Management frame structure:**

```
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
|    FC  |    Len |  Address 1 |  Address 2 |  Address 3 |     Seq |     Mgt. info |
+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
```

**Management frame supatypes:**
The management frames are basically used for associating a STA to an AP (procedure see below).

a. Authentication frame:  Basic authentication, e.g. based on MAC-address.
b. Deauthentication frame  STA sends deauthentication frame to terminate communication.
c. Association request frame  STA requests AP to allocate resources for communication.
d. Association response frame  Response of an AP to an association request.
e. Reassociation request frame  Sent by STA when it roams to another AP.
f. Reassociation response frame  Response from the new AP to the reassociation request.
g. Disassociation frame  STA requests disassociation from AP.
h. Beacon frame  AP periodically sends beacon frames with its identity.
i. Probe request frame  When the STA is not associated to an AP, it sends probe request frames.
j. Probe response frame  Response from an AP to a probe request frame.
• 802.11 WLAN Wireless LAN (6/10):

802.11 frame types (2/3):

2. Control frame:
Control frames are optional and are used for assisting in the delivery of data frames between stations. Control frames are used in a handshake procedure in the CSMA/CA protocol (see below).

**Control frame structure:**

<table>
<thead>
<tr>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>Len</td>
<td>Rx address</td>
<td>Tx address</td>
</tr>
<tr>
<td>RTS (Request To Send) frame</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>2</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>Len</td>
<td>Rx address</td>
</tr>
<tr>
<td>CTS (Clear To Send) frame</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>2</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>Len</td>
<td>Rx address</td>
</tr>
<tr>
<td>Ack frame</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rx: Receiver
Tx: Transmitter
• 802.11 WLAN Wireless LAN (7/10):

802.11 frame types (3/3):

3. Data frame:
Data frames carry user data. Data frames are acknowledged and retransmitted if they are lost.

Data frame structure:

<table>
<thead>
<tr>
<th>FC</th>
<th>Len</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Seq</th>
<th>Optional field</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

WEP parameters (4 bytes) if data is WEP-protected.
Address 4 (6 bytes) if frame is an AP→AP frame.

Data frame addresses and DS bits:
Since data frames may be transported between APs over a wired distribution system, 2 additional MAC addresses are required in the WLAN frame header.
The DS bits indicate the meaning of the different addresses fields as follows:
Destination = MAC address of final destination node.
Source = MAC address of original sending node.
Sender & receiver: Sending and receiving AP’s MAC addresses.

<table>
<thead>
<tr>
<th></th>
<th>To DS</th>
<th>From DS</th>
<th>Addr. 1</th>
<th>Addr. 2</th>
<th>Addr. 3</th>
<th>Addr. 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to Client</td>
<td>0</td>
<td>0</td>
<td>Dest.</td>
<td>Source</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>AP to Client</td>
<td>0</td>
<td>1</td>
<td>Dest.</td>
<td>BSSID</td>
<td>Source</td>
<td>N/A</td>
</tr>
<tr>
<td>Client to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>Source</td>
<td>Dest.</td>
<td>N/A</td>
</tr>
<tr>
<td>AP to AP</td>
<td>1</td>
<td>1</td>
<td>Receiver</td>
<td>Sender</td>
<td>Dest.</td>
<td>Source</td>
</tr>
</tbody>
</table>
• **802.11 WLAN Wireless LAN (8/10):**

802.11 MAC (Media Access Control) differs from 802.3 (Ethernet) MAC:

**802.3 Ethernet MAC uses CSMA/CD Collision Detection:**
1. Before sending check if the line is free (nobody else is sending).
2. If the line is free send the data. At the same time monitor the own data on the line. If the data is scrambled there is a collision (another device is sending at the same time).
3. In case of a collision wait some time (backoff time) and restart at 1.

**802.11 WLAN MAC uses CSMA/CA Collision Avoidance:**
Collisions are costly and difficult to detect in radio networks, thus 802.11 tries to avoid them.
1. Before sending check if the air is free (nobody else is sending).
2. If the air is free send the data. Unlike in wired Ethernet the monitoring of the own data is useless since the power level of the sender itself is much higher than the power level of another sender. In addition a sender can not detect collisions at the receiver due to the “hidden station” problem.
3. Optionally the sender can reserve the air medium for the transmission of a frame with the (optional) RTS/CTS procedure (Request To Send / Clear To Send) as follows:

The CTS/RTS procedure is usually only used for small frames.
STA1 requests air interface by sending an RTS frame containing the amount of data to be sent (time interval).
STA2 „hears“ RTS and refrains from sending any frames during requested time interval.
AP grants air interface with CTS frame.
STA1 sends data.
AP sends ACK to finish transaction.
Wireless / Mobile Networks

- **802.11 WLAN Wireless LAN (9/10):**

  802.11 registration with an access point (1/2):
  Unlike Ethernet, WLAN stations register with an access point.

```
1. Probing / scanning
2. Authentication (exchange pattern depends on authentication scheme)
3. Association
4. Data exchange
```

**Diagram:**

- **STA**
  - Probe request frame
  - Beacon or probe response frame
  - Auth. request
  - Ack
  - Assoc. request
  - Ack
  - Assoc. response
  - Ack
  - Data
  - Ack

- **AP**
Wireless / Mobile Networks

• 802.11 WLAN Wireless LAN (10/10):

802.11 registration with access point (2/2):

1. Probing / scanning:
The STA attempts to find an AP through:
   a. (Optional) active scanning (probe request frames) or
   b. Passive scanning (client waits for AP’s beacon frames sent in regular intervals).
The user then selects to which AP to associate based on the SSID (beacon contains the SSID).

2. Authentication:
STA authenticates with AP.
Possible authentication schemes:
   a. Open (no authentication).
   b. PSK (Pre-Shared Key) with WEP (deprecated).
   c. 802.1X EAPOL (EAP Over LAN) used with WPA / WPA2.

3. Association:
STA enters the service set serviced by the AP. STA informs AP of its supported data rates.
AP allocates buffers and other data structures for the communication with the STA.

4. Send / receive data:
STA starts sending and receiving data (direct or with RTS/CTS mechanism).
N.B.: All frames are acknowledged with WLAN. Lost frames are retransmitted.
Wireless / Mobile Networks

- Public mobile networks (1/x):
  - Evolution of mobile networks and technologies:
    - **AMPS** Analog Mobile Phone Service (e.g. “Natel A – C”).
    - **GSM** Global System for Mobile Telecommunication.
      - 2G technology: 2nd generation (digital cellular networks).
      - 2.5G technology: addition to GSM service.
    - **EDGE** Enhanced Data Rates for GSM Evolution; enhancement (data rates) of GPRS service (mainly software based, can be deployed in existing GPRS networks with software upgrades).
      - 2.75G technology: Sometimes also seen as a 3G technology. EDGE is actually a step between GPRS and UMTS.
    - **UMTS** Universal Mobile Telecommunication System.
      - 3G technology: Incompatible with 2G and thus requires new network infrastructure. Does the same as GSM so adoption rate is slow (but picking up lately).
    - **HSDPA** High Speed Downlink Packet Access.
      - 3.5G technology: Enhancement of UMTS for higher speeds in Network-to-mobile direction. Mainly a software based improvement over plain UMTS.
    - **HSUPA** High Speed Uplink Packet Access.
      - 3.75G technology: Further enhancement (higher speeds in mobile-to-network direction) of UMTS and HSDPA service.
    - **LTE** Long Term Evolution.
      - 4G technology, UMTS successor, competitor to WiMAX.
Wireless / Mobile Networks

• Public mobile networks (2/x):
  ➔ 2G / 2.5G / 3G networks:
  - Base Transmission Station ("Base Station"):  
    - Control of radio interface, antenna, sender + receiver.
  - Mobile Switching Center:  
    - Acts as a phone switch.
    - Route calls through GMSC (even mobile-to-mobile calls).
  - Serving GPRS Support Node:  
    - Similar to MSC, but packet-oriented (does packet routing).
    - End user authentication and billing.
    - Selection of appropriate GGSN based on APN from mobile device.
    - Tunnel endpoint (GTP protocol)
    - Similar to an FA in Mobile IP.
  - Gateway GPRS Support Node:  
    - Tunnel endpoint (GTP protocol).
    - Gateway (router with NAT) to Internet or customer Intranet.
    - Customer management (IP address assignment etc.).
    - Similar to a HA in Mobile IP.
  - Visitor Location Register:  
    - Database with mobile devices that are currently attached to this MSC.
  - HLR:  
    - Central database of all customers of an operator.
  - VLR:  
    - Database with mobile devices that are currently attached to this MSC.
  - GMSC:  
    - Gateway (router with NAT) to Internet or customer Intranet.
    - Customer management (IP address assignment etc.).
  - BSC:  
    - Control of multiple Base Stations.
    - Control of handover (moving from cell to cell).
    - Control of time slots on radio interface.
  - SGSN:  
    - Similar to MSC, but packet-oriented (does packet routing).
    - End user authentication and billing.
    - Selection of appropriate GGSN based on APN from mobile device.
    - Tunnel endpoint (GTP protocol)
    - Similar to an FA in Mobile IP.
  - GMSC:  
    - Gateway (router with NAT) to Internet or customer Intranet.
    - Customer management (IP address assignment etc.).
    - Similar to a HA in Mobile IP.
  - PSTN:  
    - Internet:  
    - Similar to an FA in Mobile IP.
Public mobile networks (3G/4G):

GSM protocol stacks:
The data service (TCP/IP) on GSM networks requires a rather complex protocol stack to achieve transparent mobility (handover between radio cells).

LTE may use a different approach based on PMIPv6 (Proxy Mobile IPv6, RFC5213).
**Wireless / Mobile Networks**

- **Public mobile networks (4/x):**
  LTE (Long Term Evolution) is the 4th generation of mobile networks to replace G3 networks. LTE provides far greater bandwidths, even for moving mobile devices:


  **LTE features:**
  - High bandwidths (< 100Mbps)
  - Low latency (5ms)
  - Mobility support (< 500km/h, see above)
  - High spectral efficiency (3-4 times that of UMTS / HSPA)

  N.B.: First release of LTE is “only” 3.9G as it does not fully meet the 4G criteria (all IP). First version of LTE still supports TDM services.
Wireless / Mobile Networks

• Satellite Internet Access:
  ➔ Satellite Internet access is relatively cheap to deploy in areas where wired Internet access is difficult or impossible (remote areas).
  ➔ Satellite access is also possible for moving hosts, e.g. Panasonic exConnect for Internet access & GSM phone service aboard long-haul flights.
  ➔ A satellite system is usually optimized for one-way transmission (TV, radio). Downlink bandwidth is much cheaper than uplink bandwidth.
Wireless / Mobile Networks

• Wireless mobility:
  ➔ Mobility not only means obtaining an IP address dynamically (PPP, DHCP). Mobility means that a mobile host is always reachable irrespective of its current location (location transparency).

  ➔ Mobility (location transparency) can be implemented at:
  1. Datat link layer (L2):
    Examples: IEEE 802.11r Fast Roaming (not widely used) or GSM/CDMA.
    Allows to roam between access points (handover).
    😊 No changes to clients (mobile nodes) needed.
    😞 Works only for and within specific wireless technologies.

  2. Application layer (L5-L7):
    Examples: SIP registrations, DNS/dynDNS.
    😊 No changes to clients (mobile nodes) needed.
    😞 Disruptive (an open connection will be dropped), thus only suited for quasi-static attachment to network using PPP, DHCP or PPPoE for obtaining IP address, e.g. once a day).

  3. Network layer (L3):
    Examples: Mobile IP MIP RFC2002 (see below), Proxy MIP RFC5213.
    😊 Transparent to transport protocols; thus applications are unaware of changes of network attachment (handover).
    😊 Works for different wireless technologies.
    😞 Changes in OS for mobile nodes required.
Mobile IP RFC2002 (1/5):

- Mobile IP model:

  - HA acts as an 'anchor point'.
  - MN has always a relationship to HA (is registered with HA).
  - FA acts as tunnel endpoint.
  - N.B.: Mobile IP is not specifically restricted to wireless networks.

Cell (e.g. WLAN BSS) / Home Network

Cell (e.g. WLAN BSS) / Foreign Network

- MN: Mobile Node
- HA: Home Agent
- FA: Foreign Agent
- CoA: Care of address (c/o)
- BSS: Basic Service Set (radio cell)
- CN: Correspondent Node (is either Mobile or stationary)
• Mobile IP RFC2002 (2/5):

➡ MIP components:

1. Home Agent HA:
   An MN registers with its Home Agent and informs it about its CoA. A HA is a special process running on a router.

2. Foreign Agent FA:
   Establishes a tunnel with HA and forwards packets to/from MN from/to tunnel. An FA is a special process running on a router.

3. Corresponding Node CA:
   Communication partner for MN; a CA needn’t have any knowledge about Mobile IP; CA is either a mobile itself or stationary.

4. Mobile Node MN:
   Any wireless appliance (handy, PDA, laptop, server aboard an airplane etc.).

➡ MIP objectives:

Mobile IP (RFC2002) aims at making the location of machines transparent to applications. If a user moves around the application communication should not be disrupted (TCP connections remain open even though MN obtains new IP address = ‘session continuity’). Since a TCP connection is defined by the quadruplet {src IP, src port, dst IP, dst port} it is required that the MN retain its IP address when roaming (point of attachment changes). This in turn means that IP tunneling must be used. In a way mobile IP is similar to GSM where a user moves (roams) but can always be called from another phone, irrespective of his current location (handover/roaming even works during a call!).
Wireless / Mobile Networks

• Mobile IP RFC2002 (3/5):
  ➔ How Mobile IP works:

1. MN Address:
   MN has fixed *Home Address* that never changes. A roaming MN is identified/addressed through this *Home Address*.

2. MIP Agent Discovery:
   During agent discovery MN finds HA or FA. MIP uses extensions to RFC1256 Router Advertisements. HA and FA advertise their capability to act as HA/FA through broadcasts at regular intervals (*agent advertisements* every few seconds containing a list of CoAs, also called beacons).
   If NN does not want to wait for router advertisement it can request a CoA through broad- or multicast (*agent solicitation*).

3. MIP Registration:
   MN registers CoA (endpoint address of tunnel that will be initiated by HA) with HA when it changes point of attachment (roams).

4. HA routing:
   HA adjusts its routing table to deliver (tunnel) packets destined to MN to make the connections to the MN transparent for applications.
   4. Packets from MN to CN are either directly delivered (triangular routing) or the FA routes them back through the tunnel (‘reverse tunneling’).
• Mobile IP RFC2002 (4/5):
  Colocated CoA versus CoA:
  The FA either resides on the MN itself (colocated CoA) or on a dedicated device (shared CoA).

1. Colocated CoA:
  Mobile Node obtains IP address through some external means (DHCP, PPP) and uses it as tunnel endpoint address. The MN itself terminates the tunnel, decapsulates the tunnel packets (removes outer header) and delivers (routes, forwards) the packet to the application.
  ☝️ No foreign agent required.
  🙁 Multiple IP‘s required to support multiple mobile nodes

2. Shared CoA:
  All MN‘s in a foreign network have the same CoA address. The CoA is simply the IP address of the FA. The FA termates the tunnel, decapsulates the tunnel packets (removes outer header) and delivers the packet to the according MN.
  ☝️ 1 IP address for multiple nodes
  🙁 FA required
• Mobile IP RFC2002 (5/5):

Mobile IP routing / packet forwarding:

1. CN sends packet to MNs home address. HA performs proxy ARP to deliver L2 address on behalf of (absent) MN. When MN leaves home network the HA sends gratuitous ARPs (with HA’s link layer address in order to update the ARP caches of hosts in the home network).

2. HA finds out that MN is not on home network but reachable through tunnel (routing entry) and sends packet to CoA (tunnel endpoint address of FA).

3. FA delivers the packet to the MN.

4. MN sends the reply back to the FA.

5a. FA sends packet directly to CN (= „triangular routing“); the problem with this approach is that the reply packet does not take a topologically correct route (packet with IP-source=MN-home address comes from FA). Firewalls / packet filters along the way with ingress filtering thus may drop the packet.

5b. Instead of directly routing the packet back to the CN the FA routes the packet back to the HA through the tunnel (= reverse tunneling).

N.B.: MN’s home address may be private and thus not unique in the foreign network. Thus FA’s routing entries must consist of a combination of link layer address (MAC), tunnel identification and MN-IP-address.