IEEE 802.11
Wireless LAN

Gianluca Reali
What is IEEE 802.11?

• Local, high-speed wireless connectivity for fixed, portable and moving stations
  – stations can be moving at pedestrian and vehicular speed

• Standard promises interoperability
  – vendors products on the same physical layer should interoperate

• Target use
  – inside buildings, outdoor areas, anywhere!
Glossary of 802.11 Wireless Terms

- **Station (STA):** A computer or device with a wireless network interface.
- **Access Point (AP):** Device used to bridge the wireless-wired boundary, or to increase distance as a wireless packet repeater.
- **Ad Hoc Network:** A temporary one made up of stations in mutual range.
- **Infrastructure Network:** One with one or more Access Points.
- **Channel:** A radio frequency band, or Infrared, used for shared communication.
- **Basic Service Set (BSS):** A set of stations communicating wirelessly on the same channel in the same area, Ad Hoc or Infrastructure.
- **Extended Service Set (ESS):** A set of BSSs and wired LANs with Access Points that appear as a single logical BSS.
- **BSSID & ESSID:** Data fields identifying a station's BSS & ESS.
- **Clear Channel Assessment (CCA):** A station function used to determine when it is OK to transmit.
- **Association:** A function that maps a station to an Access Point.
- **MAC Service Data Unit (MSDU):** Data Frame passed between user & MAC.
- **MAC Protocol Data Unit (MPDU):** Data Frame passed between MAC & PHY.
- **PLCP Packet (PLCP_PDU):** Data Packet passed from PHY to PHY over the Wireless Medium.
802.11 Task Groups

- 802.11a - Standard for WLAN operation in the 5 GHz band, with data rates of up to 54 Mbps. Published in 1999. Products based on this standard was presented in early 2002. e.g. see Atheros (http://atheros.com/). Work completed.

- 802.11b - Standard (also known as WiFi) for WLAN operations in the 2.4 GHz band, with data rates of up to 11 Mbps. Published in 1999. Work completed.

802.11 Task Groups

• 802.11d - Publishing definitions and requirements to allow the 802.11 standard to operate in countries not currently served by the standard. Ongoing.

• 802.11e - Attempting to enhance the 802.11 MAC to introduce quality of service. Improvement in capabilities and efficiency are planned to allow applications such as voice, video, or audio transport over 802.11 wireless networks. Ongoing.

• 802.11f - Developing recommended practices for implementing the 802.11 concepts of Access Points and Distribution Systems. The purpose is to increase compatibility between Access Point devices from different vendors. Ongoing.
802.11 Task Groups

- **802.11g** - Developing a higher-speed PHY extension to the 802.11b standard, while maintaining backward compatibility with current 802.11b devices. The target data rate for the project is at least 20 Mbps. Ongoing.

- **802.11h** - Enhancing the 802.11 MAC and 802.11a PHY to provide network management and control extensions for spectrum and transmit power management in the 5 GHz band. This will allow regulatory acceptance of the standard in some European countries. Ongoing.

- **802.11i** - Enhancing the security and authentication mechanisms of the 802.11 standard. Ongoing.
IEEE 802.11 basic

• Uses Direct Sequence spread spectrum (DSSS) technology
  – Frequency-Hopping spread spectrum (FHSS) can only be used for 1 or 2 Mbps in US due to FCC regulations

• Operates in unlicensed 2.4 GHz ISM band
  – ISM: Industrial, Scientific and Medical
  – ISM regulatory range:
    » 2.4 GHz to 2.4835 GHz for North America
IEEE 802.11 basic

- Supported Speeds and Distances
  - 1, 2, 5.5, 11 Mbps at distances of 150-2000 feet without special antenna
  - Greater distances can be achieved by using special antennas
  - Reachable Distance (or signal strength) greatly depends on environment (buildings, walls, moving objects...)
  - Maximum obtainable speed depends on signal strength
IEEE 802.11b

• ‘b’ in IEEE 802.11b
  – September 1999, 802.11b “High Rate” amendment was ratified by the IEEE
  – 802.11b amendment to 802.11 only affects the physical layer, the basic architecture is the same
    » Added two increased transmission speed
      • 5.5 and 11 Mbps
    » More robust connectivity

• 802.11b also known as Wi-Fi (Wireless Fidelity)
IEEE 802.11a

- “Fast Ethernet” standard of wireless LANs

- Transmission speeds up to 54 Mbps

- 5 GHz (U-NII band) instead of 2.4 GHz
  - Unlicensed National Information Infrastructure

- OFDM instead of DSSS for encoding
  - Orthogonal Frequency Division Multiplexing

- 802.11a products are currently on the market
IEEE 802.11a

• Advantages
  – higher speed
  – less RF interference than 2.4 GHz in US
    » 2.4 GHz used by Bluetooth, cordless/cellular phones, etc.
  – some interoperability, vendors currently have “dual-standard” 802.11a/b equipment

• Disadvantages
  – shorter range, need to increase AP density or to increase power to compensate
IEEE 802.11g

- Another high-speed standard
- Viewed as a ‘step’ towards 802.11a
- Speeds of up to 54 Mbps
  - may be more like 20+ Mbps
- Still works at 2.4 GHz
  - not in the 5 GHz range like 802.11a
- Advantages
  - compatible with 802.11b
  - better range than 802.11a, by now
IEEE 802.11e

• Another upcoming standard for WLANs
  – adds quality-of-service features to MAC layer of 802.11b compatible networks
    » error correction
    » better bandwidth management
      • significantly improves multimedia performance
  » works around RF interference
    • handles interference by moving away from it
    • i.e., moves to a new frequency when interference from a 2.4 GHz cordless phone is detected
IEEE 802.11 Topologies

• Three basic topologies for WLANs
  – IBSS: Independent Basic Service Set
  – BSS: Basic Service Set
  – ESS: Extended Service Set

• Independent of type of PHY chosen
IEEE 802.11 IBSS

- IBSS: Independent Basic Service Set
  - Peer-to-peer or ad-hoc network
  - Wireless stations communicate directly with one another
  - Generally are not connected to a larger network
  - No Access Point (AP)
IEEE 802.11 BSS

- **BSS: Basic Service Set**
  - Infrastructure mode
  - An AP connects clients to a wired network
IEEE 802.11 ESS

- **ESS: Extended Service Set**
  - Infrastructure mode
  - Consists of overlapping BSSs (each with an AP)
    » DS connects APs together, almost always Ethernet
    » ESS allows clients to seamlessly roam between APs
Access Points (APs)

- Broadcasts service
  - uses beacon management frames
- Number of clients supported
  - device dependent
    » memory size, congestion,
    » SMC2652W - 128 clients
    » Cisco Aironet 340 - 2,048 clients
IEEE 802.11 and the ISO stack

Network Operating System (NOS)

802.11

Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP
IP

Logical Link Control (LLC) – 802.2
Media Access Control (MAC) – Power Security, Etc.

FH, DS, IR, CCK(b), OFDM(a)
IEEE 802.11 Physical Layer

- **802.11 Physical Layer Specifications**
  - include FHSS, DSSS, IR

- **PLCP: Physical Layer Convergence Protocol**
  - interface used by the other physical layer specs
  - maps data units into a suitable framing format

- **PMD system: Physical Medium Dependent**
  - defines the characteristics/method of Tx/Rx data through a wireless medium between 2 or more stations
IEEE 802.11 Data Link Layer

- 2 Sublayers
  - Logical Link Control (LLC)
  - Media Access Control (MAC)
- MAC sublayer is unique in 802.11

- 802.11 uses the same 802.2 LLC
  - same 48-bit addressing as other 802 LANs
    » MAC address is 6 bytes or 48 bits
  - allows for simple bridging to wired networks
802.11 Protocol Entities

- **LLC**
- **MAC Sublayer**
  - **PLCP Sublayer**
  - **PMD Sublayer**
- **MAC Layer Management**
- **PHY Sublayer**
- **PHY Layer Management**
- **Station Management**
IEEE 802.11 MAC Sublayer

- MAC: Regulates access to the medium
- Wired IEEE 802 LANs use CSMA/CD
- 802.11 uses CSMA/CA
- CSMA: carrier sense multiple access
  - CD: with collision detection
  - CA: with collision avoidance
- Collision detection is not possible in 802.11
  - near/far problem: can’t transmit and “hear” a collision at the same time
IEEE 802.11 MAC Sublayer

- CSMA/CA avoids collisions by explicit packet acknowledgment (ACK)
  - station wishing to transmit first senses the medium
  - if no activity detected, station waits an additional, random amount of time then transmits if the medium is still free
  - ACK packet is sent by receiving station to confirm the data packet arrived intact
  - collision assumed if sending station doesn’t get ACK, data is retransmitted after a random time
IEEE 802.11 MAC Sublayer

- Other unique features in 802.11
  - IFS: Inter Frame Space
    » time interval between frames
  - Handling hidden stations (hidden-node problem)
    » virtual carrier sense
  - Power management functions
  - Data security (MAC address, WEP)
    » WEP: Wired Equivalent Privacy
  - Multirate support
  - Fragmentation / Defragmentation
Main Requirements

- Single MAC to support multiple PHYs.
  - Support single and multiple channel PHYs.
  - and PHYs with different *Medium Sense* characteristics

- Should allow overlap of multiple networks in the same area and channel space.
  - Need to be able to share the medium.
  - Allow re-use of the same medium.

- Need to be *Robust for Interference*.
  - Microwave interferers
  - Other un-licensed spectrum users
  - Co-channel interference

- Need mechanisms to deal with *Hidden Nodes*.

- Need provisions for *Time Bounded Services*.

- Need provisions for Privacy and Access Control.
Basic Access Protocol Features

• Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions.
  – Use CSMA with Collision Avoidance derivation.
  – Based on Carrier Sense function in PHY called Clear Channel Assessment (CCA).

• Robust for interference.
  – CSMA/CA + ACK for unicast frames, with MAC level recovery.
  – CSMA/CA for Broadcast frames.

• Parameterized use of RTS / CTS to provide a Virtual Carrier Sense function to protect against Hidden Nodes.
  – Duration information is distributed by both transmitter and receiver through separate RTS and CTS Control Frames.

• Includes fragmentation to cope with different PHY characteristics.

• Frame formats to support the access scheme
  – For Infrastructure and Ad-Hoc Network support
  – and Wireless Distribution System.
802.11 - Inter Frame Spacing

- **SIFS (Short Inter Frame Spacing)**
  - highest priority, for ACK, CTS, polling response
  - Calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incoming packet (28 µs)

- **PIFS (PCF IFS)**
  - medium priority, for time-bounded service using PCF
  - Calculated as SIFS plus a Slot Time (78 us)

- **DIFS (DCF, Distributed Coordination Function IFS)**
  - lowest priority, for asynchronous data service
  - Calculated as PIFS plus a Slot Time (128us)

- **EIFS (Extended IFS)**

![Diagram showing the timing of different inter frame spacings with a note that direct access if medium is free ≥ DIFS]
CSMA/CA Explained

Free access when medium is free longer than DIFS

- DIFS
- PIFS
- SIFS
- Contention Window
- Backoff-Window
- Next Frame
- Slot time
- Defer Access
- Select Slot and Decrement Backoff as long as medium is idle.

- Reduce collision probability where mostly needed.
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.

- Efficient Backoff algorithm stable at high loads.
  - Exponential Backoff window increases for retransmissions.
  - Backoff timer elapses only when medium is idle.

- Implement different fixed priority levels.
  - To allow immediate responses and PCF coexistence.
Backoff Interval

- When transmitting a packet, choose a backoff interval in the range $[0,cw]$
  - $cw$ is contention window

- Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy

- When backoff interval reaches 0, transmit RTS
Example

B1 = 25

```
wait
```

B1 = 5

```
data
```

B2 = 20

```
data
```

B2 = 15

```
wait
```

B2 = 10

```
data
```

\[ \text{cw} = 31 \]

B1 and B2 are backoff intervals at nodes 1 and 2
**CSMA/CA + ACK protocol**

- Defer access based on *Carrier Sense*.
  - CCA from PHY and *Virtual Carrier Sense* state.
- Direct access when medium is sensed free longer than DIFS, otherwise defer and backoff.
- Receiver of directed frames to return an ACK immediately when CRC correct.
  - When no ACK received then retransmit frame after a random backoff (up to maximum limit).
Throughput Efficiency

- Efficient and stable throughput.
  - Stable throughput at overload conditions.
  - To support “Bursty Traffic” characteristics.
The Hidden Terminal Problem

- A is sending to B, but C cannot receive from A
  - Friis Law (power decay proportional to distance square)
- Therefore C sends to B, without detecting the transmission from A to B
- In summary, A is “hidden” for C
- Implication: How to do carrier sense and collision detection?
“Hidden Node” Problem

• Transmitters contending for the medium may not “Hear each other” as shown below.

  - Stations do not hear each other
  - But they hear the AP.

• Separate Control frame exchange (RTS / CTS) between transmitter and receiver will Reserve the Medium for subsequent data access.
  - Duration is distributed around both Tx and Rx station.
"Hidden Node" Provisions

- Duration field in RTS and CTS frames distribute Medium Reservation information which is stored in a Network Allocation Vector (NAV).
- Defer on either NAV or "CCA" indicating Medium Busy.
- Use of RTS / CTS is optional but must be implemented.
- Use is controlled by a RTS_Threshold parameter per station.
  - To limit overhead for short frames.
Collision Avoidance: RTS-CTS + ACK

DIFS: Distributed Inter-Frame Spacing
SIFS: Short Inter-Frame Spacing
RTS/CTS Overhead Impact

Good mixed Throughput (long inbound frames) efficiency.
Optional Point Coordination Function (PCF)

• Contention Free Service uses Point Coordination Function (PCF) on a DCF Foundation.
  – PCF can provide lower *transfer delay* variations to support *Time Bounded Services*.
  – Async Data, Voice or mixed implementations possible.
  – Point Coordinator resides in AP.

• Coexistence between Contention and optional Contention Free does not burden the implementation.
**Contention Free operation**

- Alternating *Contention Free* and *Contention* operation under PCF control.
- NAV prevents *Contention* traffic until reset by the last PCF transfer.
  - So variable length *Contention Free* period per interval.
- Both PCF and DCF defer to each other causing PCF Burst start variations.
PCF Burst

- CF-Burst by Polling bit in CF-Down frame.
- Immediate response by Station on a CF_Poll.
- Stations to maintain NAV to protect CF-traffic.
- Responses can be variable length.
- “Reset NAV” by last (CF_End) frame from AP.
- "ACK Previous Frame" bit in Header.
Fragmentation

- A hit in a large frame requires re-transmission of a large frame
- Fragmenting reduces the frame size and the required time to re-transmit
- Burst of Fragments which are individually acknowledged.
  - For Unicast frames only.
- Random backoff and retransmission of failing fragment when no ACK is returned.
- *Duration* information in data fragments and Ack frames causes NAV to be set, for medium reservation mechanism.
802.11a vs 802.11b
IEEE 802.11 Frame Types

- Three types of frames
  - Control
    » RTS, CTS, ACK, Contention-Free (CF), PS-Poll
  - Management
    » Probe request/response
    » Beacon
      • supported rates, timestamp, traffic indication map
    » Authentication / deauthentication
    » Announcement traffic indication message (ATIM)
      • sent after each frame
  - Data
Frame Formats

Bytes:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Frame Control</td>
</tr>
<tr>
<td>2</td>
<td>Duration ID</td>
</tr>
<tr>
<td>6</td>
<td>Addr 1</td>
</tr>
<tr>
<td>6</td>
<td>Addr 2</td>
</tr>
<tr>
<td>6</td>
<td>Addr 3</td>
</tr>
<tr>
<td>2</td>
<td>Sequence Control</td>
</tr>
<tr>
<td>6</td>
<td>Addr 4</td>
</tr>
<tr>
<td>0-2312</td>
<td>Frame Body</td>
</tr>
<tr>
<td>4</td>
<td>CRC</td>
</tr>
</tbody>
</table>

802.11 MAC Header

<table>
<thead>
<tr>
<th>Bits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Protocol Version</td>
</tr>
<tr>
<td>2</td>
<td>Type</td>
</tr>
<tr>
<td>4</td>
<td>SubType</td>
</tr>
<tr>
<td>1</td>
<td>To DS</td>
</tr>
<tr>
<td>1</td>
<td>From DS</td>
</tr>
<tr>
<td>1</td>
<td>More Frag</td>
</tr>
<tr>
<td>1</td>
<td>Retry</td>
</tr>
<tr>
<td>1</td>
<td>Pwr Mgt</td>
</tr>
<tr>
<td>1</td>
<td>More Data</td>
</tr>
<tr>
<td>1</td>
<td>WEP</td>
</tr>
<tr>
<td>1</td>
<td>Rsvd</td>
</tr>
</tbody>
</table>

Frame Control Field

- MAC Header format differs per Type:
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames

- Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.
## Frame Type

<table>
<thead>
<tr>
<th>Type Value b3 b2</th>
<th>Type Description</th>
<th>Subtype Value b7 b6 b5 b4</th>
<th>Subtype Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Management</td>
<td>0000</td>
<td>Association Request</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0001</td>
<td>Association Response</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0010</td>
<td>Reassociation Request</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0011</td>
<td>Reassociation Response</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0100</td>
<td>Probe Request</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0101</td>
<td>Probe Response</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>0110-0111</td>
<td>Reserved</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1000</td>
<td>Beacon</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1001</td>
<td>ATIM</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1010</td>
<td>Disassociation</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1011</td>
<td>Authentication</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1100</td>
<td>Deauthentication</td>
</tr>
<tr>
<td>00</td>
<td>Management</td>
<td>1101-1111</td>
<td>Reserved</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>0000-1001</td>
<td>Reserved</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1010</td>
<td>PS-Poll</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1011</td>
<td>RTS</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1100</td>
<td>CTS</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1101</td>
<td>ACK</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1110</td>
<td>CF End</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>1111</td>
<td>CF End + CF-ACK</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0000</td>
<td>Data</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0001</td>
<td>Data + CF-Ack</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0010</td>
<td>Data + CF-Poll</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0011</td>
<td>Data + CF-Ack + CF-Poll</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0100</td>
<td>Null Function (no data)</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0101</td>
<td>CF-Ack (no data)</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0110</td>
<td>CF-Poll (no data)</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0111</td>
<td>CF-Ack + CF-Poll (no data)</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>1000-1111</td>
<td>Reserved</td>
</tr>
<tr>
<td>11</td>
<td>Reserved</td>
<td>0000-1111</td>
<td>Reserved</td>
</tr>
</tbody>
</table>
Address Field Description

<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>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

- **Addr 1** = All stations filter on this address. It is the immediate recipient of the packet.
- **Addr 2** = Transmitter Address (TA)
  - Identifies transmitter to address the ACK frame to.
- **Addr 3** = Dependent on *To* and *From DS* bits.
- **Addr 4** = Only needed to identify the original source of **WDS (Wireless Distribution System)** frames, when a WDS is used.
Privacy and Access Control

- Goal of 802.11 is to provide “Wired Equivalent Privacy” (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control.
  - Has provisions for “OPEN”, “Shared Key” or proprietary authentication extensions.
- Optional (WEP) Privacy mechanism defined by 802.11.
  - Limited for Station-to-Station traffic, so not “end to end”.
    » Embedded in the MAC entity.
  - Only implements “Confidentiality” function.
  - Uses RC4 PRNG algorithm based on:
    » a 40 bit secret key (No Key distribution standardized)
    » and a 24 bit IV that is send with the data.
    » includes an ICV to allow integrity check.
  - Only payload of Data frames are encrypted.
    » Encryption on per MPDU basis.
• WEP bit in Frame Control Field indicates WEP used.
  – Each frame can have a new IV, or IV can be reused for a limited time.
  – If integrity check fails then frame is ACKed but discarded.
Support for Mobility

- LLC
- MAC Sublayer
- PLCP Sublayer
- PMD Sublayer
- MAC Layer Management
- PHY Layer Management
- Station Management
MAC Management Layer

• Synchronization
  – finding and staying with a WLAN
  – Synchronization functions
    » TSF Timer, Beacon Generation

• Power Management
  – sleeping without missing any messages
  – Power Management functions
    » periodic sleep, frame buffering, Traffic Indication Map

• Association and Reassociation
  – Joining a network
  – Roaming, moving from one AP to another
  – Scanning

• Management Information Base
Synchronization in 802.11

• Timing Synchronization Function (TSF)
• Used for Power Management
  – Beacons sent at well known intervals
  – All station timers in BSS are synchronized
• Used for Point Coordination Timing
  – TSF Timer used to predict start of Contention Free burst
• Used for Hop Timing for FH PHY
  – TSF Timer used to time Dwell Interval
  – All Stations are synchronized, so they hop at same time.
Synchronization Approach

• All stations maintain a local timer.
• Timing Synchronization Function
  – keeps timers from all stations in synch
  – AP controls timing in infrastructure networks
  – distributed function for Independent BSS
• Timing conveyed by periodic Beacon transmissions
  – Beacons contain Timestamp for the entire BSS
  – Timestamp from Beacons used to calibrate local clocks
  – not required to hear every Beacon to stay in synch
  – Beacons contain other management information
    » also used for Power Management, Roaming
Infrastructure Beacon Generation

- APs send Beacons in infrastructure networks.
- Beacons scheduled at Beacon Interval.
- Transmission may be delayed by CSMA deferral.
  - subsequent transmissions at expected Beacon Interval
  - not relative to last Beacon transmission
  - next Beacon sent at Target Beacon Transmission Time
- Timestamp contains timer value at transmit time.
Power Management

- Mobile devices are battery powered.
  - *Power Management* is important for mobility.
- Current LAN protocols assume stations are always ready to receive.
  - Idle receive state dominates LAN adapter power consumption over time.
- How can we power off during idle periods, yet maintain an active session?
- 802.11 Power Management Protocol:
  - allows transceiver to be off as much as possible
  - is transparent to existing protocols
  - is flexible to support different applications
    » possible to trade off throughput for battery life
**Power Management Approach**

- Allow idle stations to go to sleep
  - station’s power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF assures AP and Power Save stations are synchronized
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- Independent BSS also have Power Management
  - similar in concept, distributed approach
Infrastructure Power Management

- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after pre-known times called DTIM
  - DTIM interval is a multiple of TIM interval
Infrastructure Power Management

- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after pre-known times called DTIM
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected (D)TIM.
Infrastructure Power Management

- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected (D)TIM.
- If TIM indicates frame buffered
  - station sends PS-Poll and stays awake to receive data
  - else station sleeps again
Each Station is Associated with a particular AP
- Stations 1, 2, and 3 are associated with Access Point A
- Stations 4 and 5 are associated with Access Point B
- Stations 6 and 7 are associated with Access Point C
- Mobile stations may move…
• Mobile stations may move…
  – beyond the coverage area of their Access Point
• Mobile stations may move…
  – beyond the coverage area of their Access Point
  – but within range of another Access Point
• Mobile stations may move…
  – beyond the coverage area of their Access Point
  – but within range of another Access Point
• Reassociation allows station to continue operation
Roaming Approach

• Station decides that link to its current AP is poor
• Station uses scanning function to find another AP
  – or uses information from previous scans
• Station sends Reassociation Request to new AP
• If Reassociation Response is successful
  – then station has roamed to the new AP
  – else station scans for another AP
• If AP accepts Reassociation Request
  – AP indicates Reassociation to the Distribution System
  – Distribution System information is updated
  – normally old AP is notified through Distribution System
Scanning

• Scanning required for many functions.
  – finding and joining a network
  – finding a new AP while roaming
  – initializing an Independent BSS (ad hoc) network

• 802.11 MAC uses a common mechanism for all PHY.
  – single or multi channel
  – passive or active scanning

• Passive Scanning
  – Find networks simply by listening for Beacons

• Active Scanning
  – On each channel
    » Send a Probe, Wait for a Probe Response

• Beacon or Probe Response contains information necessary to join new network.
Active Scanning Example

Steps to Association:

Station sends Probe.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:
- Station sends Probe.
- APs send Probe Response.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.

Initial connection to an Access Point

Access Point A

Access Point C
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point
- ReAssociation follows a similar process
MAC Management Frames

- **Beacon**
  - Timestamp, Beacon Interval, Capabilities, ESS identifier (ESSID), Supported Rates, parameters
  - Traffic Indication Map

- **Probe**
  - ESSID, Capabilities, Supported Rates

- **Probe Response**
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - same for Beacon except for TIM

- **Association Request**
  - Capability, Listen Interval, ESSID, Supported Rates

- **Association Response**
  - Capability, Status Code, Station ID, Supported Rates
More MAC Management Frames

- **Reassociation Request**
  - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address

- **Reassociation Response**
  - Capability, Status Code, Station ID, Supported Rates

- **Disassociation**
  - Reason code

- **Authentication**
  - Algorithm, Sequence, Status, Challenge Text

- **Deauthentication**
  - Reason
Questions and answers