IEEE 802.11a

- 5 GHz (5.15-5.25, 5.25-5.35, 5.725-5.825 GHz)
- OFDM (Orthogonal Freq. Div. Multiplexing)
- 52 Subcarriers in OFDM
- BPSK/QPSK/QAM
- Forward Error Correction (Convolutional)
- Rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

802.11x

a → OFDM in the 5GHz band
b → High Rate DSSS in the 2.4GHz band
c → Bridge Operation Procedures
e → MAC Enhancements for QoS to improve QoS for better support of audio and video (such as MPEG-2) applications.
g → OFDM based 2.4 GHz WLAN.

Wired vs. Wireless

- 802.3 (Ethernet) uses CSMA/CD, Carrier Sense Multiple Access with 100% Collision Detect for reliable data transfer
- 802.11 has CSMA/CA (Collision Avoidance)
  - Large differences in signal strengths
  - Collisions can only be inferred afterward
  - Transmitters fail to get a response
  - Receivers see corrupted data through a CRC error
Spectrum

- 802.11 operates in the unlicensed band (ISM – Industrial Scientific and Medical band) ~ 3 such bands
  - Cordless Telephony: 902 to 928 MHz
  - 802.11b: 2.4 to 2.483 GHz
  - 3rd ISM Band: 5.725 to 5.875 GHz
  - 802.11a: 5.15 to 5.825 GHz

Data Rates and Range

- 802.11: 2Mbps (Proposed in 1997)
- 802.11b: 1, 2, 5.5 and 11 Mbps, 100M range (product released in 1999, no product for 1 or 2 Mbps)
- 802.11g: 54Mbps, 100M range (uses OFDM; product expected in 2003)
- 802.11a: 6 to 54 Mbps, 50M range (uses OFDM)

802.11 Wireless LAN Organization

- Infrastructure Mode
  - Access points govern and coordinate the network
    - E.g. DragonFly
- Ad hoc mode
  - Peer-to-peer network, all devices can transmit to any other

Basics of Infrastructure Mode

- Access Points (AP) advertise presence with beacon frames
  - Beacons are short ID and synchronization messages, 10x a second
- Hosts search for an AP by scanning 802.11 channels (11 channels) listening for a beacon
- When beacons are found, connections are selected based on signal strength
Some terms

- Service Set Identifier (SSID)
- Distributed interframe space (DIFS)
- Short Interframe space (SIFS)
- Distributed Coordination Function (DCF)
  - Provides CSMA/CA, may use CTS/RTS
- Point coordination function (PCF)
  - AP use PCFs to ensure contention-free services

Basic Service Set (BSS)

- Set of nodes logically associated with each other
  - Independent BSS
    - P2P communications for nodes in close range
  - Infrastructure BSS
    - Communications via a single access point
      - i.e. Home networks

Extended Service Set (ESS)

- Larger service areas
- Multiple access points
- Radio range of APs overlaps and APs communicate with each other (over the backbone network)
- Wireless medium acts as layer 2 connection and APs are bridges
- Link-layer mobility is supported but only if backbone is single layer domain
  - Shared ethernet

Network Services

Station/node services:
- Authentication
  - Establish identity prior to connection
- Deauthentication
  - Terminate authentication (and connection)
- Privacy
  - WEP, eavesdropping protection
- MAC Service Data Unit (MSDU) Delivery
  - Get data to endpoint

Distribution (AP-AP) services:
- Distribution
  - Determines destination in infrastructure networks
- Integration
  - Interconnection to non-802 networks
- Association
  - Connect mobile node with AP, use it as gateway
- Reassociation
  - Mobile node uses signal info to switch APs when moving
- Disassociation
  - Terminate association, removing mobility support
Mobility Support

- No transition
  - No action
- BSS transition
  - Move among APs on the same network (ESS)
- ESS transition
  - Move across different wireless networks
  - (very hard, not supported, kind of like cell phone roaming).

BSS Transition Example

Network messages during mobility

Physical Layer of 802.11
Base specifications

• Common MAC (Medium Access Control) for all 802.11 family
• Three Physical Layers:
  – FHSS (Frequency Hopping Spread Spectrum)
  – DSSS (Direct Sequence Spread Spectrum)
  – OFDM (Orthogonal Frequency Division Multiplexing)

PHY layer

• Two sublayers
  – Physical Layer Convergence Procedure (PLCP)
  – Physical Medium Dependant (PMD)
• The PLCP is essentially a handshaking layer that enables MAC protocol data units (MPDUs) to be transferred between MAC stations over the PMD
• PMD is the method of transmitting and receiving data through the wireless medium

Physical Layer Convergence Procedure (PLCP)

• It provides the interface, regardless of the PHY, for the transfer of data octets between MAC and the PMD
  – PLCP TX MAC to PHY: “start a transmission”
  – PLCP TX PHY to MAC: “transmission completed”
  – Similar at the receiver side
**DSSS PHY**

- Baseband signal is spread using Barker word (10 dB processing gain)
- Spread signal occupies approximately 22 MHz bandwidth
- Receiver recovers the signal by applying the same Barker word
- DSSS provides good immunity against narrowband interferer
- CDMA (multiple access) capability is not possible

---

**Operating Channels**

- Direct sequence spread spectrum
  - Each channel is 22 MHz wide
- Symbol rate
  - 1 Mb/s with DBPSK modulation
  - 2 Mbps with DQPSK modulation
  - 11, 5.5 Mb/s with CCK modulation
- Max transmit power
  - 100 Mw

---

**802.11b DSS Channels**

- DSS PHY has 14 channels, each 22MHz wide, placed 5MHz apart
- Channel 1 is placed at center freq. 2.412 GHz, Channel 2 at 2.417 GHz, and so on up to Channel 14 placed at 2.477 GHz
- Allowed channels
  - US/Canada 1 to 11 (2.412 – 2.462 GHz)
  - Europe (excluding France & Spain) 1 to 13 (2.412-2.472 GHz)
  - France 10 to 13 (2.457-2.462 GHz)
  - Spain 10 to 11 (2.457-2.462 GHz)
  - Japan 14 (2.477 GHz)
- 3 non-overlapping channels
Distributed Coordination Function (DCF) Scheme

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Binary exponential backoff

**PHY Functions**

- Wireless transmission mechanism for the MAC
- Assessing the state of the wireless medium and reporting it to the MAC
- Independence between MAC and PHY \( \rightarrow \) enhancements
- 802.11b, 802.11a, 802.11g PHYs use the same MAC

**Backoff example**

- CW max
- CW min
- Slot time = 20 µs

**MAC layer of 802.11**
Important PHY Parameters

- Wireless MAC’s need to be designed to deal with the following PHY parameters
  - Propagation delay (span of 1m, 10m or 1Km?)
  - Bit-rate (1 Mbps vs. 10 vs. 100?)
  - Modem acquisition & training delay
  - Radio coverage (hidden/exposed nodes)
  - Carrier sensing (yes/no), and its threshold
  - Spreading codes (yes/no), and capture
  - Link reliability

Higher Layer Considerations

- MAC also needs to consider higher layer requirements such as
  - Centralized AP vs. ad-hoc modes
  - Single vs. multi-hop usage
  - Flows and connectionless packets
  - Latency constraints
  - QoS needs, if any
  - Packet formats and fragmentation
  - Level of reliability required at layer 3

Some Challenges

Challenges in the MAC: RF Link Quality

- Transmissions subject to noise and interference
- Problems with path fading

- Example on subsequent pages
Experiment Setup

• 2 iPAQs positioned 900ft apart
• iPAQ 1 constantly running net-perf to measure effective throughput to iPAQ 2
• iPAQ 1 moves toward iPAQ 2 at the speed about 3.6 feet per second
• Experiment duration is about 250 seconds

Collected Data

• UDP protocol only
• Bit-rates set to values 11, 5.5, 2, 1 MBps
• Power set to 100mW, 50mW, 10mW
• Experiment repeated 3 times for each bit rate/power combination
• Producing roughly 60 data points for each experiment

UDP, Power 100mW, All Bit Rates

• Wireless networks have fuzzy boundaries
• What happens if H1 and H2 both try to talk to the AP?
  – Collisions
• Hard to detect hidden nodes in wireless
  – Nodes are 1/2 duplex

Hidden Node Problem
Solution: RTS, CTS

- RTS: Request to Send
  - Clears out an area, silences stations who hear it
- CTS: Clear to Send
  - Signals all clear, silences stations who hear it

Note:
- Consumes capacity
- When to use?
  - High capacity, high contention environments
- RTS Threshold can be set in device drivers
  - Small frames, just send… big ones clear the way.
  - Collisions on small frames just get resent when there is no ACK

MAC Coordination Design Options

- Several design options for wireless MAC
  - Slotted channel vs. asynchronous
  - Pure contention (ALOHA)
  - Carrier sensing (CS)
  - Collision detection (CD)
  - Collision avoidance (CA)
  - Locally synchronous scheduling
  - Time division multiple access (TDMA)
  - Code division multiple access (CDMA)
  - Polling, Reservations
  - RLC (reliable retransmission protocols)

802.11 Media Access Control

- Carrier Sense: Listen before talking
- Handshaking to infer collisions
  - DATA-ACK packets
- Collision Avoidance
  - RTS-CTS-DATA-ACK to request the medium
  - Duration information in each packet
  - Random Backoff after collision is determined
  - Net Allocation Vector (NAV) to reserve bandwidth
  - Hidden Nodes use CTS duration information
802.11 MAC Specifics

802.11 Media Access Control

• Fragmentation
  – Bit Error Rate (BER) goes up with distance and decreases the probability of successfully transmitting long frames
  – MSDUs given to MAC can be broken up into smaller MPDUs given to PHY, each with a sequence number for reassembly
    • Can increase range by allowing operation at higher BER
    • Lessens the impact of collisions
      – Trade overhead for overhead of RTS-CTS
      – Less impact from Hidden Nodes

802.11 Media Access Control

• Beacons used convey network parameters such as hop sequence
• Probe Requests and Responses used to join a network
• Power Savings Mode
  – Frames stored at Access Point or Stations for sleeping Stations
  – Traffic Indication Map (TIM) in Frames alerts awaking Stations

Accessing the medium

CSMA/CA

• Wireless LAN adapters cannot detect collisions:
  – Carrier Sensing - listen to the media to determine if it is free
  – Collision Avoidance - minimize chance for collision by starting (random) back-off timer, when medium is sensed free, and prior to transmission
CSMA/CA with MAC - level Acknowledgment

- Collisions still can occur (interference; incapability of sensing other carrier)
  - IEEE 802.11 defines “low-level” ACK protocol
  - Provides faster error recovery
  - Makes presence of high level error recovery less critical

Message Fragmentation

- IEEE 802.11 defines:
  - MAC level function to transmit large messages as smaller frames (user definable)
  - Improves performance in RF polluted environments
  - Can be switched off to avoid the overhead in RF clean environments

MAC Frame Formats

- Long messages get broken into Frames
  - Node can transmit next frame ASAP after ACK
  - But must do a backoff before sending next msg
- Transmitter reserves the channel with RTS
  - Receiver gives a CTS to initiate transmission
Basic 802.11 Messages

• Control
• Management
• Data

MAC Management Frames

• Beacon
  – Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  – Traffic Indication Map
• Probe
  – SSID, Capabilities, Supported Rates
• Probe Response
  – Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, parameters
  – same for Beacon except for TIM

Contents of a Beacon Frame

• Beacon interval
• Timestamp
• Service Set Identifier (SSID)
• Supported rates
• Parameter Sets
• Capability Information
• Traffic Indication Map (TIM)

MAC Management Frames

• Association Request
  – Capability, Listen Interval, SSID, Supported Rates
• Association Response
  – Capability, Status Code, Station ID, Supported Rates
• Re-association Request
  – Capability, Listen Interval, SSID, Supported Rates, Current AP Address
• Re-association Response
  – Capability, Status Code, Station ID, Supported Rates
MAC Management Frames

- Dis-association
  - Reason code

- Authentication
  - Algorithm, Sequence, Status, Challenge Text

- De-authentication
  - Reason

802.11 Frame Formats

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

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

MAC Header

- Contains source and destination address
- Destination address can be
  - Unicast: deliver to 1 device
  - Multicast
    - Multicast, deliver to several devices
    - Broadcast, deliver to all devices
- Four Addresses
  - Transmitter, Receiver, Source, Destination

Address Field Description

<table>
<thead>
<tr>
<th>Addr. 1</th>
<th>Addr. 2</th>
<th>Addr. 3</th>
<th>Addr. 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>N/A</td>
</tr>
<tr>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

Addr. 1 = All stations filter on this address.
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.
Type field descriptions

Type and subtype identify the function of the frame:
- Type=00 Management Frame
  - Beacon (Re)Association
  - Probe (De)Authentication
  - Power Management
- Type=01 Control Frame
  - RTS/CTS
  - ACK
- Type=10 Data Frame