IEEE 802.11 Wireless LANs
Medium Access Control (MAC)

Shyam Parekh & Pravin Varaiya
EECS 228A
October 7, 2003
Agenda

- Review
- Main Ideas
- Framing Details
- Management Operations
References*

- 802.11 Wireless Networks: The Definitive Guide, M. Gast, O'Reilly, 2002
- ANSI/IEEE Std 802.11, 1999 Edition
- ANSI/IEEE Std 802.11b-1999
- ANSI/IEEE Std 802.11a-1999
- Reading suggestions on the Syllabus page

* The lectures will make liberal use of drawings from the references
Key Points from Last Lecture

- 802.11 standards describe MAC and Physical layer Wireless LAN protocols
- A Basic Service Set is either Independent (Ad Hoc) or Infrastructure type
- Network services include authentication, association, and data transfer
Key Points from Last Lecture - 2

- **802.11b PHY** uses 2.4 GHz ISM band and supports up to 11 Mbps rate
  - A BSS typically uses 1, 6, or 11 based on frequency reuse criterion
  - Based on DSSS ideas
  - Each data symbol is mapped into a Complementary Codeword
  - There is substantial preamble and PLCP header overhead for each frame
- **802.11a PHY** uses 5 GHz NII bands and supports up to 54 Mbps
  - A BSS uses one of 12 channels
  - Based on OFDM ideas
  - Each data symbol encode with convolution code makes use of 48 orthogonal subcarriers
  - At high-end data rates, QAM is used
Main Ideas: Access Modes

- **MAC Access Modes:**
  - Distributed Coordination Function (DCF)
    - Basis of Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
  - Point Coordination Function (PCF)
    - Restricted to Infrastructure BSSs
    - Not widely implemented
    - Access Point polls stations for medium access
Main Ideas: WLAN Problems

- Hidden Terminal and Exposed Terminal problems

![Diagram showing hidden terminal and exposed terminal problems.](image)
Main Ideas: CSMA/CA

- Interframe Spacing (IFS)
  - Short IFS: For atomic exchanges
  - PCF IFS: For prioritized PCF access
  - DCF IFS: For Normal DCF access
  - Extended IFS: For access after error

- Medium Access
Main Ideas: CSMA/CA - 2

- If medium is idle for DIFS interval (based on physical or virtual sensing), transmission can begin immediately.
- If previous frame contained errors, medium must be free for EIFS.
- If medium is busy, access is deferred until medium is idle for DIFS and exponential backoff.
- Backoff counter is decremented by one if a time slot is determined to be idle.
- Unicast data must be acknowledged as part of an atomic exchange.
Main Ideas: Interframe Spacing

- Interframe Spacing values are physical layer dependent
- SIFS and Slot_Time are explicitly specified, and the others are derived
  - PIFS = SIFS + Slot_Time
  - DIFS = SIFS + 2·Slot_Time
  - EIFS = SIFS + DIFS + (Ack_Time @ 1 Mbps)
- For 802.11a and 802.11b
  - SIFS is 16 μs and 10 μs, respectively
  - Slot_Time is 9 μs and 20 μs, respectively
Main Ideas: Contention Window

- Backoff is performed for R slots: R is randomly chosen integer in the interval [0, CW]
- $CW_{\text{min}} \leq CW \leq CW_{\text{max}}$
  - $CW_{\text{min}} = 31$ slots and $CW_{\text{max}} = 1023$ slots (for 802.11b)
  - Up to $CW_{\text{max}}$, $CW = (CW_{\text{min}} + 1) \cdot 2^n - 1$, where $n = 0, 1, 2, \ldots$ is (re)transmission number
Error Recovery

- Each frame is associated with a retry counter based on frame size as compared to RTS/CTS threshold
  - Short retry counter
  - Long retry counter

- Fragments are given a maximum lifetime by MAC before discarding them
Main Ideas: WLAN Problems (Revisit)

- Hidden Terminal and Exposed Terminal problems

A wants to send to B but cannot hear that B is busy

B wants to send to C but mistakenly thinks the transmission will fail
Main Ideas: RTS/CTS Clearing

- RTS/CTS Clearing
- Used for frames larger than RTS/CTS threshold
- Tradeoff between overhead and retransmission costs
Main Ideas: Virtual Carrier Sensing

Virtual Carrier Sensing using Network Allocation Vector (NAV)
Main Ideas: Fragmentation Burst

- Fragmentation and RTS/CTS thresholds are typically set to the same value
Framing Details: Format

- **Generic 802.11 MAC Frame**

- **Frame Control Field**

- **Sequence Control Field**
Framing Details: Frame Types

- Type and Subtype Identifiers
  - Management Frames
  - Control Frames
  - Data Frames

<table>
<thead>
<tr>
<th>Subtype value</th>
<th>Subtype name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management frames (type=00)³</td>
<td>Association request</td>
</tr>
<tr>
<td>0000</td>
<td>Association response</td>
</tr>
<tr>
<td>0001</td>
<td>Reassociation request</td>
</tr>
<tr>
<td>0010</td>
<td>Reassociation response</td>
</tr>
<tr>
<td>0011</td>
<td>Probe request</td>
</tr>
<tr>
<td>0100</td>
<td>Probe response</td>
</tr>
<tr>
<td>1000</td>
<td>Beacon</td>
</tr>
<tr>
<td>1001</td>
<td>Announcement traffic indication message (ATIM)</td>
</tr>
<tr>
<td>1010</td>
<td>Disassociation</td>
</tr>
<tr>
<td>1011</td>
<td>Authentication</td>
</tr>
<tr>
<td>1100</td>
<td>Deauthentication</td>
</tr>
<tr>
<td>Control frames (type=01)b</td>
<td>Power Save (PS)-Poll</td>
</tr>
<tr>
<td>1010</td>
<td>RTS</td>
</tr>
<tr>
<td>1011</td>
<td>CTS</td>
</tr>
<tr>
<td>1100</td>
<td>Acknowledgment (ACK)</td>
</tr>
<tr>
<td>1110</td>
<td>Contention-Free (CF)-End</td>
</tr>
<tr>
<td>1111</td>
<td>CF-End+CF-Ack</td>
</tr>
<tr>
<td>Data frames (type=10)b</td>
<td>Data</td>
</tr>
<tr>
<td>0000</td>
<td>Data+CF-Ack</td>
</tr>
<tr>
<td>0001</td>
<td>Data+CF-Poll</td>
</tr>
<tr>
<td>0101</td>
<td>CF-Ack (no data transmitted)</td>
</tr>
<tr>
<td>0110</td>
<td>CF-Poll (no data transmitted)</td>
</tr>
<tr>
<td>0111</td>
<td>Data+CF-Ack+CF-Poll</td>
</tr>
</tbody>
</table>

(Frame type 11 is reserved)
Framing Details: Broadcast/Multicast

- No Acknowledgements for Broadcast or Multicast frames
Framing Details: NAV for Fragmentation

- Fragmentation threshold provides tradeoff between overhead and retransmission costs
- Chaining of NAV to maintain control of the medium
Framing Details: NAV for RTS/CTS and Power Save (PS)-Poll

- **RTS/CTS Lockout**

- **Immediate PS-Poll Response**

- **Deferred PS-Poll Response**
Framing Details:
Data Frames and Addresses

- **Generic Data Frames**

- **Addressing and DS Bits**
  - BSSID is MAC address of AP WLAN interface

<table>
<thead>
<tr>
<th>Function</th>
<th>ToDS</th>
<th>FromDS</th>
<th>Address 1 (receiver)</th>
<th>Address 2 (transmitter)</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBSS</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>not used</td>
</tr>
<tr>
<td>To AP (infra.)</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>not used</td>
</tr>
<tr>
<td>From AP (infra.)</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>not used</td>
</tr>
<tr>
<td>WDS (bridge)</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>
Framing Details: Illustrations of use of Addresses

- Frames to Distribution System
- Frames from Distribution System
- Wireless Distribution System
Framing Details: RTS/CTS Control Frames

- **RTS Frame**

- **CTS Frame**
Framing Details: Ack and PS-Poll Control Frames

- **Acknowledgement Frame**

- **Power-Save Poll (PS-Poll) Frame**
Framing Details: Management Frames

- Generic Management Frames
Framing Details: Fixed-Length Management Fields

- **Beacon Interval Field**
  - In 1024 $\mu$s Time Units (TUs)
  - Typically 100 TUs or about 0.1 Seconds

- **Capability Information**
  - Used in Beacon, Probe request and Probe Response Frames
Framing Details: Fixed-Length Management Fields - 2

- **Listen Interval**
  - Number of Beacon Intervals a station waits before listening to Beacon frames

- **Timestamp**
  - Allows synchronization
  - Number of microseconds timekeeper has been active
Framing Details: Management Information Elements

- **Generic Management Frame Information Element**

- **Service Set Identity (ASCII Identifier)**

- **DS Parameter Set**

- **Contention Free Parameter Set**
**Framing Details: Main Management Frames**

- **Beacon Frame**

- **Probe Request Frame**

- **Probe Response Frame**
Framing Details: Main Management Frames - 2

- **Authentication Frames**

- **Association Request**

- **(Re)Association Response**
Management Operations: Scanning

- Passive Scanning
- Active Scanning
Management Operations: Authentication and Association

- Shared key Authentication Exchange
  - Makes use of WEP

Association Procedure
Management Operations: Buffered Frame Retrieval

- **Unicast Buffered Frames**

- **Broadcast and Multicast Buffered Frames**
Reminder

- Please select your Presentation by end of this week
- Consider continuation of Presentation for Project work (possibly using OPNET)