Ad-hoc, DCF

Basics

- Ad-hoc mode AKA “Independent Basic Service Set” (IBSS)
- Senders/receivers can elect to use:
  - 2-frame exchange (Data – ACK)
  - 4-frame exchange (RTS – CTS – Data – ACK)
- All sends are done with a timeout – if no ACK before timeout, retransmit
### 802.11 Data frame format

<table>
<thead>
<tr>
<th>Cntl</th>
<th>Dur</th>
<th>Addr1</th>
<th>Addr2</th>
<th>Addr3</th>
<th>Seq</th>
<th>Addr4</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0-2312</td>
<td>4</td>
</tr>
</tbody>
</table>

- **Control:**
  - Version
  - Type of frame (Data, CTS, RTS, re-transmit...)
  - "ToDistributionSystem" and "FromDistributionSystem" flags (used in addressing)
  - Fragmentation support
- **Duration:**
  - The sender's calculation of the amount of time that the frame will take to transmit
  - Used by other nodes to estimate when they can do an RTS
- **Address 1,2,3,4:**
  - Standard 802-series MAC addresses
- **Seq:**
  - Sequence number for fragments
- **Data**
- **CRC**

### Why 4 addresses in a frame?

Needed to support a message from a wireless device, through the wired network to another wireless device

ToDistributionSystem = FromDistributionSystem = TRUE

---

G. W. Cox -- Fall 2007
### Addressing variations

<table>
<thead>
<tr>
<th>ToDS</th>
<th>FromDS</th>
<th>Addr1</th>
<th>Addr2</th>
<th>Addr3</th>
<th>Addr4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Dest (Wireless)</td>
<td>Source (Wireless)</td>
<td>Not used</td>
<td>Not used</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Dest (Wireless)</td>
<td>Sending AP</td>
<td>Source (Wired)</td>
<td>Not used</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Receiving AP</td>
<td>Source (Wired)</td>
<td>Dest (Wireless)</td>
<td>Not Used</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Receiving AP</td>
<td>Sending AP</td>
<td>Dest (Wireless)</td>
<td>Source (Wireless)</td>
</tr>
</tbody>
</table>

### 802.11 Control frame formats

**RTS/CTS**

<table>
<thead>
<tr>
<th>Cntl</th>
<th>Dur</th>
<th>Addr</th>
<th>Addr</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>

**ACK**

<table>
<thead>
<tr>
<th>Cntl</th>
<th>Dur</th>
<th>Addr</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>4</td>
</tr>
</tbody>
</table>
How duration is handled

- When a device hears an RTS/CTS sequence, it sets its “Network Allocation Vector” (NAV) according to the “duration” field of the RTS/CTS
- The time in the NAV is counted down.
- The device cannot do an RTS until the NAV=0 (and hears an ACK)

Frame fragmentation

- The fact that we have an inherently noisy medium introduces problems:
- Example:

<table>
<thead>
<tr>
<th>Probability of a bit error</th>
<th>Probability of frame being received correctly</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1,000 bit frame</td>
</tr>
<tr>
<td>10^-5</td>
<td>99.9%</td>
</tr>
<tr>
<td>10^-4</td>
<td>99%</td>
</tr>
<tr>
<td>10^-3</td>
<td>90%</td>
</tr>
</tbody>
</table>

- Senders have the option to break a frame that’s larger than a threshold value into smaller fragments.
- After the channel is acquired using RTS/CTS, the sender can send a stream of fragments (a “fragment burst”) using the stop-and-wait protocol
Timing and fairness

- 3 delay intervals govern timing:
  - SIFS (Short Interframe Space)
    - The shortest interval (supports DCF and PCF)
    - The interval generally used by sender and receiver between frames in an ongoing exchange. Examples:
      - Receipt of RTS to transmission of CTS
      - Receipt of CTS to transmission of Data
      - Receipt of Data to transmission of ACK
  - PIFS (PCF Interframe Space)
    - Next-shortest interval
    - Used by base station in PCS mode
  - DIFS (DCF Interframe Space)
    - Longest of the three
    - The interval generally used by sender when desiring to start a new exchange
- The IFS’s form a de-facto priority structure:
  1. On-going exchanges (DCF or PCF)
  2. PCF Base station actions
  3. New DCF exchanges

Infrastructure Mode, PCF
Basics

- Infrastructure mode AKA “Basic Service Set” (BSS)

How a wireless device connects to an AP

A device may want to connect to a new AP:
- when it is not presently connected to an AP
- when it is connected, but wishes to connect to a new AP (due to signal loss, movement, etc)

Methods

Active Scanning
1. Wireless device sends a **Probe** frame (“scanning”)
2. AP’s hearing the Probe frame (and willing to add devices), reply with a **Probe Response** frame
3. The device chooses one of the responding AP’s and sends an **Association Request** frame to it
4. The AP Sends an **Association Response** frame. If the device was previously associated with another AP, the new AP notifies the old one.

Passive scanning
1. AP’s broadcast advertisements periodically (**Beacon** frame).
2. A device hearing the beacon replies with an **Association Response** frame
Extending a net

Extended Service Set (ESS)

BSS 1

BSS 2

NOTE:
An L2 connection

PCF Control

• Base station periodically polls each device in its BSS to ask if the device has traffic to send
• No possibility for collision
Power saving

- Wireless nodes can enter a low-power “sleep” mode to save battery power
- Wireless device sets a flag in control field to inform AP that it is entering sleep mode.
- AP buffers traffic for the device until device reports it is awake again
- Device normally sets timeout to “wake up” to hear next beacon from AP

Security

- WEP
- WPA
- WPA2
WEP

• Wired Equivalent Privacy
• Original 802.11 security method (1999)
• Based on RC4 encryption algorithm (used in SSL)
• Originally, 40-bit keys. Later 104-bit.

• Cracked in 2001 – can now be broken in minutes
• Problem is not just key size – problem is inherent in the algorithm

• Replaced with WPA in 2003

WPA

• Based on early draft of 802.11i (security) standard
• Designed for compatibility with existing 802.11 NIC cards

• Method vs WEP
  – RC4 with 128-bit key
  – Dynamically changing keys
  – Improved Message Integrity method

• Far more secure than WEP, not perfect
WPA-2

• 2005

• Implementation of IEEE 802.11i

• Method versus WPA
  – AES algorithm
  – Same dynamic key changing and message integrity

• Considered to be fully secure