Demystifying the 802.11 Protocol

By: Brett L Neilson · hamcom@brettneilson.com
Who is Brett Neilson?

- Brett L Neilson – KC7IIB
- Author
  - Maximum Wireless Security
  - Maximum Security 4\textsuperscript{th} Edition

- By Day
  - Networking Security Professional
    - Intrusion Prevention
  - RF Field Technician Systems Admin
Agenda

• Standards
• IBSS, BSS & ESS
• Frequencies & Channels
• Frame Format
• Beacon Frames
• Connecting to the WLAN
• Joining to the WLAN
802.11 - 1997

• Project Authorization Request was submitted to the IEEE in May 1991
• Defined the Physical and Media Access methods for wireless connectivity
  – 1 and 2 Mbps transmission rates
  – Network management services
  – Registration and authentication
  – Power management
• Revision of the 1997 standard
• Three PHYs
  – Infrared
  – Frequency Hopping Spread Spectrum (FHSS)
  – Direct Sequence Spread Spectrum (DSSS)
802.11b

- 2.4 GHz Frequency range
- Direct Sequence Spread Spectrum (DSSS)
- 1, 2, 5.5 or 11 Mbit/sec (Auto Adjusting)
- Interoperability testing by WECA group
  - Wi-Fi compatibility seal on tested products
802.11a

- Primarily driven by the USA
- 5 GHz frequency range
- Orthogonal Frequency Division Multiplexing (OFDM)
- 6-54 Mbit/sec
802.11g

- 2.4 GHz Frequency Range
- Direct Sequence Spread Spectrum
- Up to 22 Mbps (Standard)
- Compatible with 802.11b
802.11i

- Stronger Encryption
- Supports 802.1x
- Dynamic Re-Keying
- First products due out the end of Q2 2004
802.15

- Started back in 1998 by Ericsson, IBM, Nokia and Toshiba
  - December of 1999, 3Com, Lucent, Microsoft and Motorola got involved
- Designed for short range networks
  - Called “Piconets”
- Wireless Personal-area Network (WPAN)
- Device connectivity
  - Laptops
  - Printers
  - Phones
  - PDAs
• 2.4 GHz Frequency range
  – Can interfere with 802.11 networks
• Uses FHSS
• Low power consumption
• Typical range is about 30 feet
Independent Basic Service Set

- IBSS or “Ad Hoc”
- No access point is used
- Generally only for temporary use
Basic Service Set

- BSS or “Infrastructure Mode”
- Nodes connect to an Access Point
- Doesn't require a connection to a wired LAN
Extended Service Set

• ESS of “Distribution System Mode”
• Multiple Access Points are used
  – Overlapping cells
• Devices can seamlessly roam between cells
Frequencies & Channels
The Radio Spectrum

- VLF
- LF
- MF
- HF
- VHF
- UHF
- SHF
- EHF

©2001 HowStuffWorks
• Transmissions are “Spread” across multiple frequencies
  – Makes signal less susceptible to noise
• More bandwidth than necessary is used to ensure reliability
• Two types of PHYs
  – Frequency Hopping Spread Spectrum (FHSS)
  – Direct Sequence Spread Spectrum (DSSS)
Frequency Hopping Spread Spectrum - FHSS

• Multiple frequencies are used
• Transmitter and Receiver “hop” between frequencies in unison
• Only one frequency is used at a time
• Typical delay or “dwell” on a frequency is no longer than 400 ms
  – About 2500 times per second
• Multiple frequencies are used
• Transmissions are spread across them
  – 22 MHz wide with 5 MHz spacing (Overlap)
• Frequencies are used simultaneously
## DSSS Channels and Frequencies

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency GHz</th>
<th>North America</th>
<th>Europe</th>
<th>Spain</th>
<th>France</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.412</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2.417</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2.422</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2.427</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2.432</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2.437</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2.442</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2.447</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2.452</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>2.457</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>11</td>
<td>2.462</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>2.467</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>13</td>
<td>2.472</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2.483</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
802.11 B Channel Overlap
# Frame Format

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

- **Frame Control**
- **Duration ID**
- **Address 1**
- **Address 2**
- **Address 3**
- **Sequence Control**
- **Address 4**
- **Frame Body**
- **FCS**

**Frame interpretation**
- Used to update the Network Allocation Vector (NAV) or ID
- BSSID
- Source MAC
- Destination MAC
- Fragment and Sequence numbers
- Used between distribution systems
- Data
- Error Checking
### Frame Control Field #1

<table>
<thead>
<tr>
<th>Subtype</th>
<th>Type</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 bits</td>
<td>2 bits</td>
<td>2 bits</td>
</tr>
</tbody>
</table>

**Sub Type**

- 1000 = Beacon
- 1100 = Deauthentication
- 0100 = Probe request
- 0101 = Probe response
- 0000 = Association request
- 0010 = Reassociation request

**Type**

- 00 = Management
- 01 = Control
- 10 = Data
- 11 = Reserved

**Protocol Version**

Currently must be 00
## Frame Control Field #2

<table>
<thead>
<tr>
<th>Order</th>
<th>WEP DS</th>
<th>More Data</th>
<th>Power Mgmt</th>
<th>Retry</th>
<th>More Flags</th>
<th>From DS</th>
<th>To DS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 bit</td>
<td>1 bit</td>
<td>1 bit</td>
<td>1 bit</td>
<td>1 bit</td>
<td>1bit</td>
<td>1bit</td>
<td>1bit</td>
</tr>
</tbody>
</table>

**From & To DS**  
To: 0 Fr: 0  Direct communication between two mobile  
To: 1 Fr: 0  Frame from mobile station to an AP  
To: 0 Fr: 1  Frame from AP to a mobile station  
To: 1 Fr: 1  WLAN is being used as a DS
1) The 00 shows that this is a Management Frame
2) The Subtype 1000 indicated that this is a Beacon Frame
3 & 4) Because this is a management frame these should be 0 & 0
5) Represented in HEX as 80 (1000 0000) & 00 (0000 0000)
Frame Control (Up-close)

1) The 10 shows that this is a Data Frame

2 & 3) Frame is being sent by a Mobile Station to the Access Point

4) WEP is not enabled

5) Represented in HEX as 08 (0000 1000) & 01 (0000 0001)

<table>
<thead>
<tr>
<th>DLC:</th>
<th>Frame Control Field #1 = 08</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLC:</td>
<td>10. . 00 = 0x2 Data Frame</td>
</tr>
<tr>
<td>DLC:</td>
<td>0000 . . = 0x0 Data (Subtype)</td>
</tr>
<tr>
<td>DLC:</td>
<td>Frame Control Field #2 = 01</td>
</tr>
<tr>
<td>DLC:</td>
<td>1. .... 1 = To Distribution System</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Not from Distribution System</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Last fragment</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Not retry</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Active Mode</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = No more data</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Wired Equivalent Privacy is off</td>
</tr>
<tr>
<td>DLC:</td>
<td>0. ..... 0 = Not ordered</td>
</tr>
</tbody>
</table>
Beacon Frames
Beacon Frames

• Typically sent by APs (10 per second)
  – Received by stations to determine network availability
    • Windows XP available networks
    • NetStumbler
  – Can be sent by stations when in Ad-Hoc mode
  – Helps roaming stations
Beacon Frames

• Information in a beacon
  – Supported data rates (1, 2, 5.5 & 11)
  – ESSID
    • Sometimes removed for security reasons
  – Time stamp
    • Helps with synchronization
Beacon (Up-Close)

1) ESS set to 0 (Not an AP)
2) IBSS set to 1 (Must be a client)
3) ANY is the SSID
1) “Default SSID” What else do you think is Default?

2) 1.0 Mbps is supported

3) 2.0 Mbps is supported but not for management frames
Connecting to the WLAN
Connecting to the WLAN

• On power up the device will begin to search for the network
  – Passive or Active Mode
• Passive Mode
  – Device scans the various channels listening for beacon frames.
  – When a beacon is heard, the connection is initiated with the AP
    • Stations can be configured to timeout and form their own network if a suitable network is not found.
Connecting to the WLAN

• Active Mode (More likely)
  – Station sends a probe request frame
    • Dedicated SSID
    • Broadcast SSID
  – Waits for a probe response frame

• Stations will then start the authentication and association process
Probe Request Frame

• Broadcast Frame
  – Destination Address (FFFFFFFFFFFFFFF)
  – Sent on a channel and if no response is heard another frame is sent on another channel

• Frame Body
  – Control Fields
  – Duration
  – Destination Address
  – Source MAC Address
  – BSSID (Specific or Broadcast)
  – SSID (Specific or Broadcast)
1) No BSSID is being specified by the client so any AP will do
   • Think about the potential security issues here (Can you say Rogue AP?)
2) The SSID that the client is looking for (might be blank)

Lost of Probe Request win no SSID may indicate NetStumbler
Probe Response Frame

• If a specific BSSID or SSID is specified in the Request that AP will respond
  – If no BSSID or SSID is specified, all APs will respond

• Frame Body
  – Timestamp
  – Beacon Interval
  – Capabilities
  – SSID
  – Supported Rates
  – Channel Number
Joining to the WLAN
Joining the WLAN

- Probe/Response or Beacon
- Authentication
  - Privacy options are negotiated and tested
    - Open / Shared Key
- Association
  - Link is established
  - AP updates its table of mobile units (route table)
Authentication

- **Open System (no authentication)**
  - Allows any station to request authentication
  - Typically the default setting

- **Shared Key**
  - Only specific stations with the correct encryption settings will be authenticated
  - Not available on all APs
Open Authentication

Probe Request
SSID of WLAN

Probe Response
SSID (accept or reject)
Channel Number

Authentication
Auth algorithm ID = Open

Authentication
Auth algorithm ID = Open
Results (accept or reject)
Shared Key Authentication

Probe Request
SSID of WLAN

Authentication
Auth algorithm ID = Shared Key

Authentication
Auth algorithm ID = Shared Key
Encrypted challenge test

Probe Response
SSID (accept or reject)
Channel Number

Authentication
Auth algorithm ID = Shared Key
128 bit Challenge test (clear)

Authentication
Auth algorithm ID = Shared Key
Result of authentication
(accept or reject)
Association

• Must take place before data can be sent
  – One AP to many stations
• Request
  – Capabilities, SSID, Rates
• Response
  – Status Code (Reason for failure)
  – Association ID (16 bit unique address)
  – Status Code (Reason for failure)
Deauthentication

• Sent when a station disassociates with another station
• Contains only a reason code
  – No longer valid (2)
  – Inactivity (4)
  – Not authenticated (9)

Mass Deauthentication frames may indicate an attack
Demystifying the 802.11 Protocol

By: Brett L Neilson · hamcom@brettneilson.com