

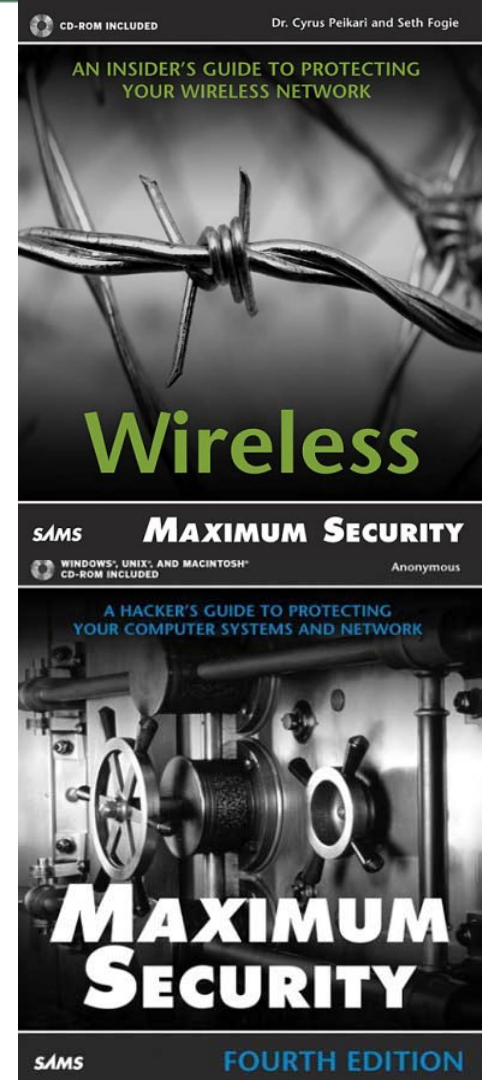


Demystifying the 802.11 Protocol

By: Brett L Neilson · hamcom@brettneilson.com

Who is Brett Neilson?

- Brett L Neilson – KC7IIB
- Author
 - Maximum Wireless Security
 - Maximum Security 4th 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



Standards



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



802.11 -1999

- 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



Bluetooth Details

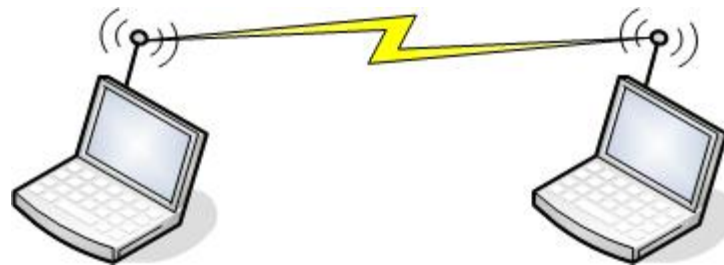
- 2.4 GHz Frequency range
 - Can interfere with 802.11 networks
- Uses FHSS
- Low power consumption
- Typical range is about 30 feet



IBSS, BSS & ESS

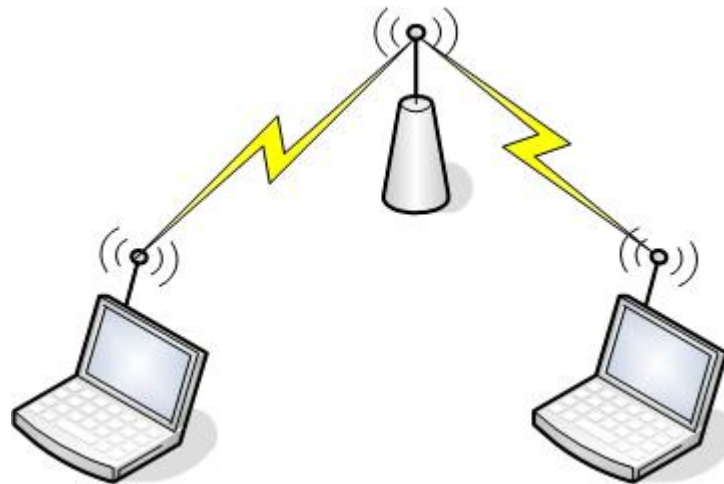
Independent Basic Service Set

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



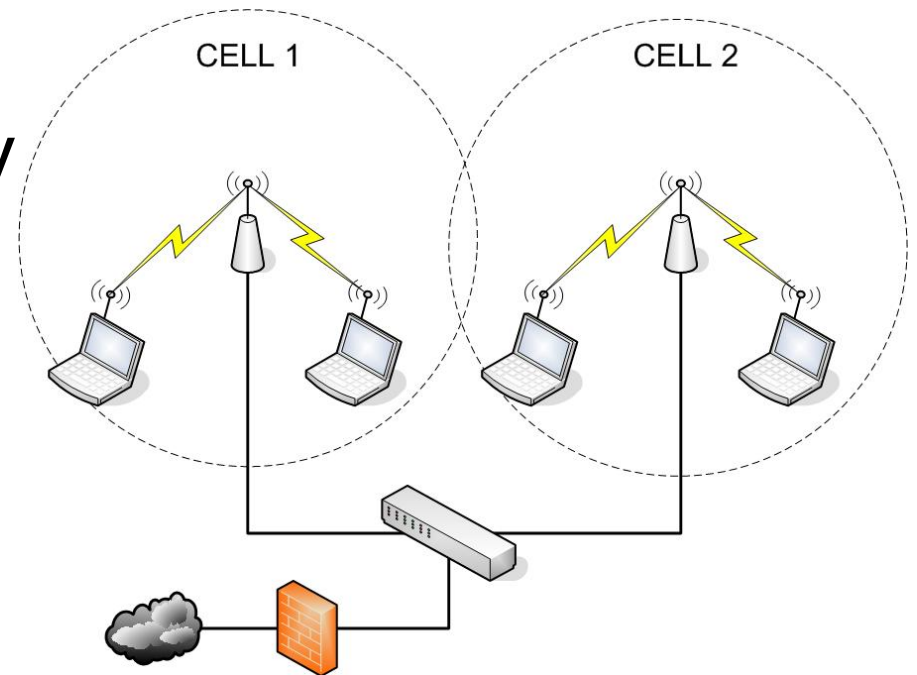
Basic Service Set

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



Extended Service Set

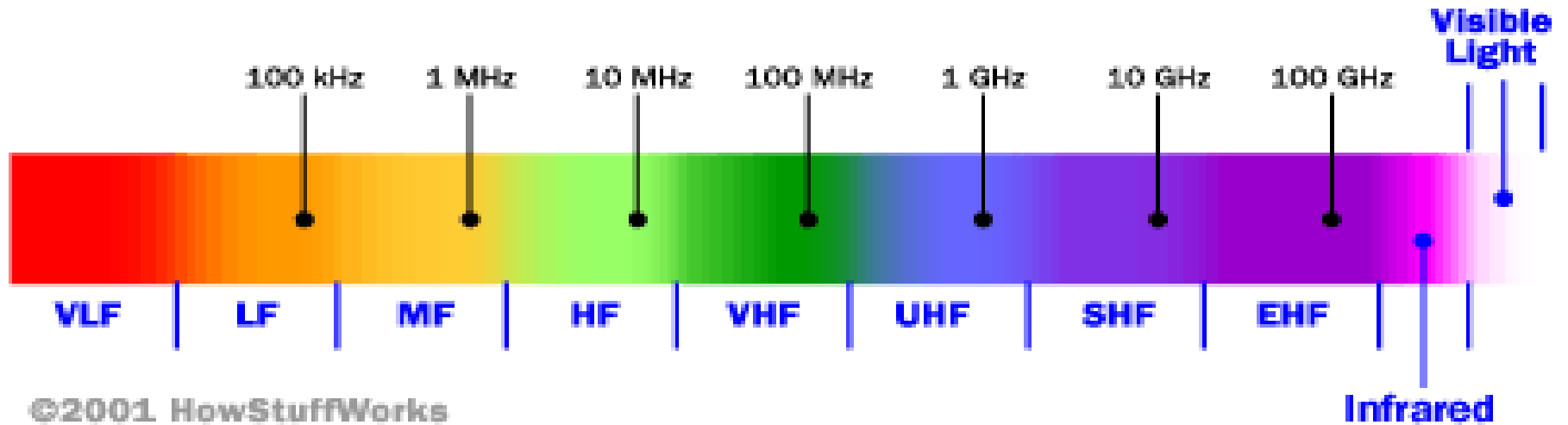
- ESS of “Distribution System Mode”
- Multiple Access Points are used
 - Overlapping cells
- Devices can seamlessly roam between cells





Frequencies & Channels

The Radio Spectrum



©2001 HowStuffWorks



Spread Spectrum

- 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



Direct Sequence Spread Spectrum - DSSS

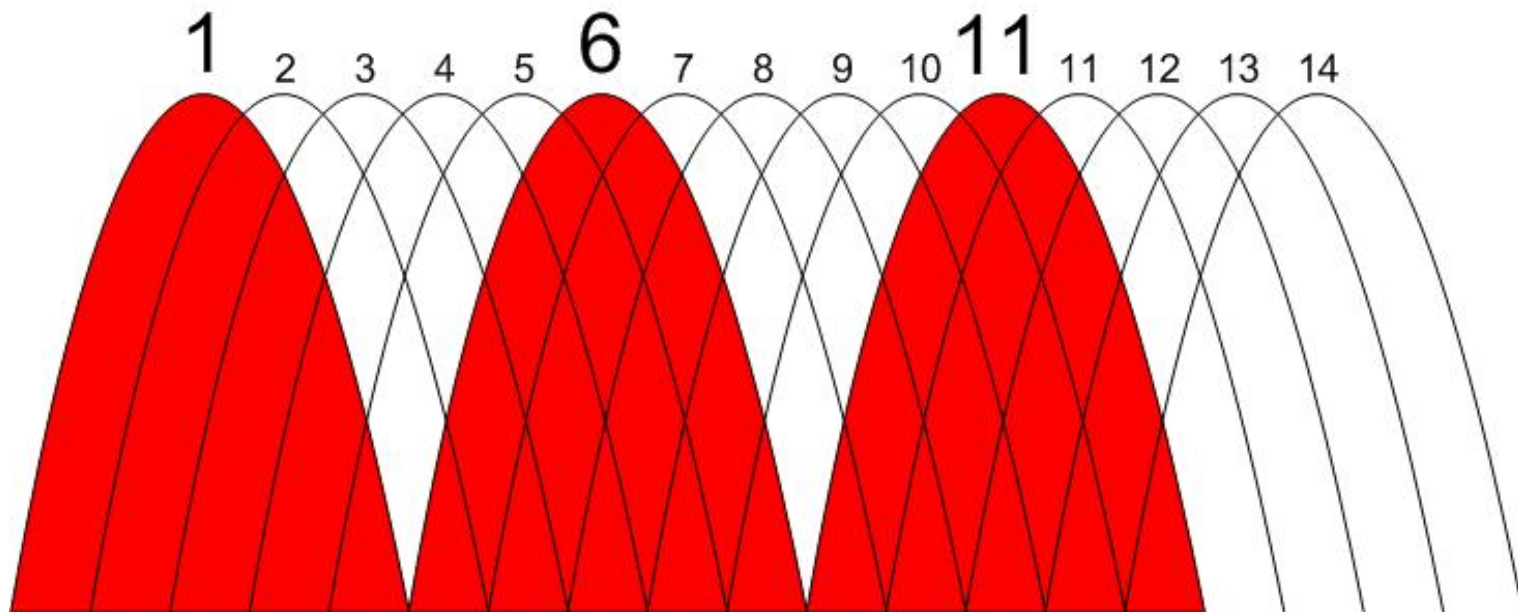
- Multiple frequencies are used
- Transmissions are spread across them
 - 22 MHz wide with 5 MHz spacing (Overlap)
- Frequencies are used simultaneously



DSSS Channels and Frequencies

Channel	Frequency GHz	North America	Europe	Spain	France	Japan
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X	X	X	
10	2.457	X	X	X	X	
11	2.462	X	X		X	
12	2.467		X		X	
13	2.472		X			
14	2.483					X

802.11 B Channel Overlap





Frame Format



Frame Format

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2	6	6	6	2	6	0-2312	4

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 Vexctor (NAV) or ID

BSSID

Source MAC

Destination MAC

Fragment and Sequence numbers

Used between distribution systems

Data

Error Checking

Frame Control Field #1

Control Field #1		
Subtype	Type	Protocol Version
4 bits	2bits	2bits

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

Control Field #2							
Order	WEP DS	More Data	Power Mgmt	Retry	More Flags	From DS	To DS
1 bit	1 bit	1 bit	1 bit	1 bit	1bit	1bit	1bit

From & To DS

To: 0 Fr: 0

To: 1 Fr: 0

To: 0 Fr: 1

To: 1 Fr: 1

Direct communication between two mobile

Frame from mobile station to an AP

Frame from AP to a mobile station

WLAN is being used as a DS

Frame Control (Up-close)

```
DLC: Frame Control Field #1 = 80
DLC:      .00 = 0x0 Protocol Version
DLC:      1 → 00.. = 0x0 Management Frame
DLC:      2 → 1000 .. = 0x8 Beacon (Subtype)
DLC: Frame Control Field #2 = 00
DLC:      3 → 0 = Not to Distribution System
DLC:      4 → 0. = Not from Distribution System
DLC:      ..0.. = Last fragment
DLC:      ....0... = Not retry
DLC:      ...0 .... = Active Mode
DLC:      ..0. .... = No more data
DLC:      .0.. .... = Wired Equivalent Privacy is off
DLC:      0... .... = Not ordered
```

```
00000: 80 00 00 00 ff ff ff ff ff ff 00 0d 29 eb 88 95 |...yyyyyy..)ë||
00010: 00 0d 29 eb 88 95 20 78 da a1 c5 e2 12 04 00 00 ..)ë|| xÜiÅÅ....
```

- 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)

```
DLC: Frame Control Field #1 = 08
DLC:      . . . . .00 = 0x0 Protocol Version
DLC:      1 → 10.. = 0x2 Data Frame
DLC:      0000 . . . . = 0x0 Data (Subtype)
DLC: Frame Control Field #2 = 01
DLC:      2 → 1 = To Distribution System
DLC:      3 → 0. = Not from Distribution System
DLC:      . . . . .0.. = Last fragment
DLC:      . . . . .0... = Not retry
DLC:      . . . 0 . . . . = Active Mode
DLC:      . . 0 . . . . . = No more data
DLC:      4 → 0. . . . . = Wired Equivalent Privacy is off
DLC:      5 ↓ 0 . . . . . = Not ordered
```

```
00000: 08 01 75 00 00 0d 29 eb 88 95 00 90 4b 64 de ae ..u... )ë||. |Kdb®
00010: 00 0c 30 5b bf 61 10 87 aa aa 03 00 00 00 08 00 ..0[za. |a.....
```

- 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)



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)

```
DLC: Timestamp = 205473 (in microseconds)
DLC: Beacon Interval = 100
DLC: Capability information field #1 = 02
DLC: 1. . . . . 0 = Extended Service Set is off
DLC: 2. . . . . 1 = Independent Basic Service Set is on
DLC: . . . . . 00.. = No point coordinator at Access Point
DLC: . . . 0 . . . . = No privacy
DLC: . . 0 . . . . = Short Preamble option is not allowed
DLC: . 0 . . . . = Packet Binary Convolutional Coding Modulation mode option
DLC: 0 . . . . = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC: 0000 0000 = Reserved
DLC:
DLC: Element ID = 0 (Service Set Identifier)
DLC: ...Length = 3 octet(s)
DLC: ...Service Set Identity = "ANY"
DLC:

00000: 80 00 00 00 ff ff ff ff ff ff 00 e0 29 91 8d 7a |...yyyyyy.à)'|z
00010: 8a 2b 42 fd cc 5f c0 00 a1 22 03 00 00 00 00 00 |+ByI_A.i".....
00020: 64 00 02 00 00 03 41 4e 59 01 04 82 84 0b 16 03 |d.....ANY..||...
00030: 01 0b 06 02 00 00 06 02 00 00 |.....
```

- 1) ESS set to 0 (Not an AP)
- 2) IBSS set to 1 (Must be a client)
- 3) ANY is the SSID

Beacon (Up-Close)

```
DLC: Element ID = 0 (Service Set Identifier)
DLC: ...Length = 12 octet(s)
DLC: ...Service Set Identity = "Default SSID" ← 1
DLC:
DLC: Element ID = 1 (Supported Rates)
DLC: ...Length = 2 octet(s)
DLC: ...Supported Rates information field = 82
DLC: 1... .. = Basic Service Set Basic Rate ← 2
DLC: .000 0010 = 1.0 Megabits per second
DLC: ...Supported Rates information field = 04
DLC: 0... .. = Not Basic Service Set Basic Rate ← 3
DLC: .000 0100 = 2.0 Megabits per second
DLC:
-----
00000: 80 00 00 00 ff ff ff ff ff ff 00 20 d8 00 da ea |...yyyyyy. @.Ùê
00010: 00 20 d8 00 da ea 50 38 d5 01 98 e7 01 00 00 00 |. @.ÙêP80. |ç....
00020: 80 00 09 00 00 0c 44 65 66 61 75 6c 74 20 53 53 |.....Default SS
00030: 49 44 01 02 82 04 03 01 01 05 04 03 05 00 00 |ID..|.....
```

- 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 (FFFFFFFFFFFFFF)
 - 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)

Probe Request (Up-Close)

```
DLC: Duration = 0 (in microseconds)
DLC: Destination Address = BROADCAST FFFFFFFF, Broadcast
DLC: Source Address = Station Symbol929F81
DLC: Basic Service Set ID = BROADCAST FFFFFFFF, Broadcast
DLC: Sequence Control = 0x0050
DLC: ...Sequence Number = 0x005 (5)
DLC: ...Fragment Number = 0x0 (0)
DLC: Element ID = 0 (Service Set Identifier)
DLC: ...Length = 6 octet(s)
DLC: ...Service Set Identity = "symbol"
DLC:
```

```
00000: 40 00 00 00 ff ff ff ff ff ff 00 a0 f8 92 9f 81 @...yyyyyy. ø'!!
00010: ff ff ff ff ff ff 50 00 00 06 73 79 6d 62 6f 6c yyyyyyP...symbol
00020: 01 04 02 04 0b 16
```

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

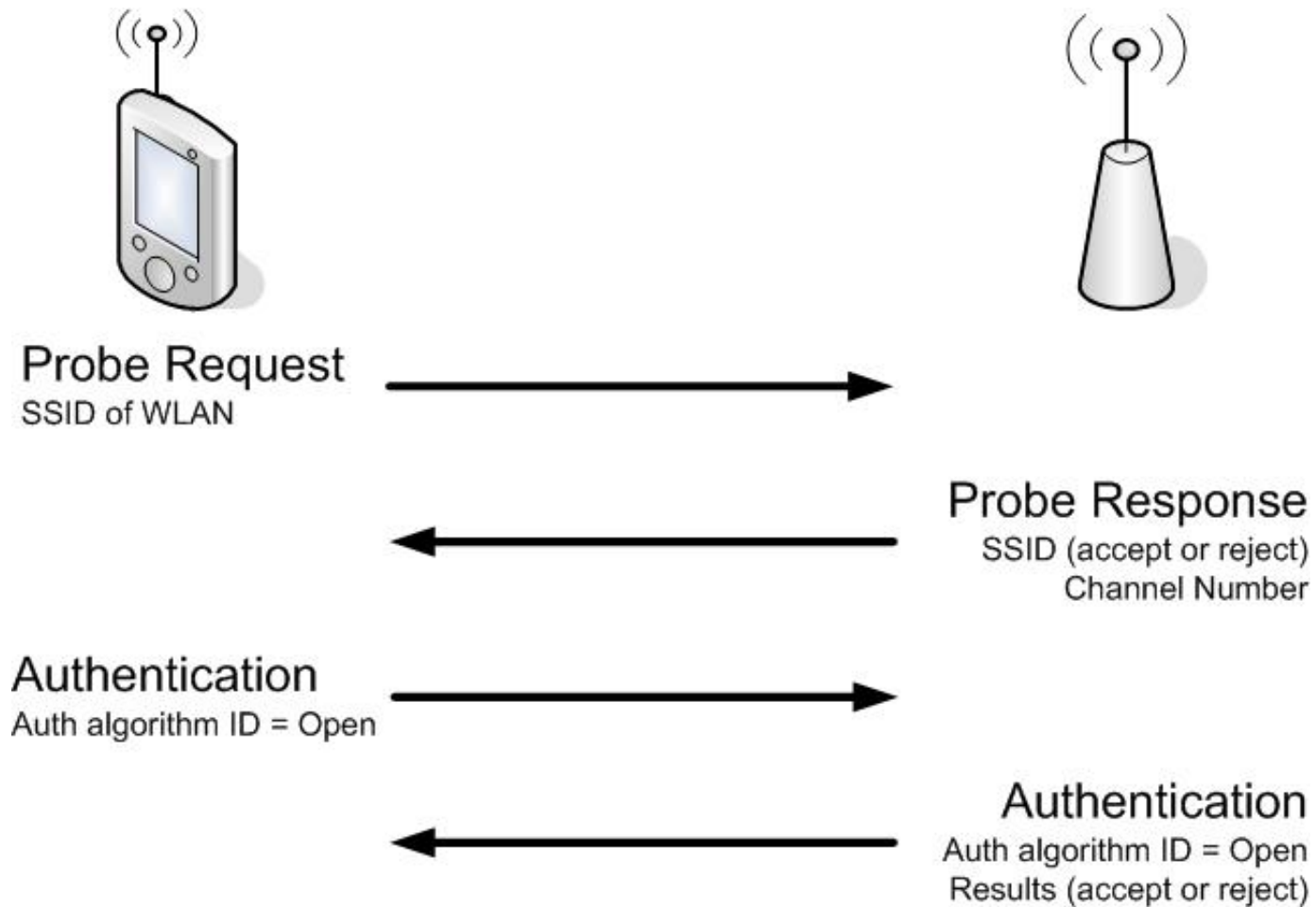
- Probe/Response or Beacon
- Authentication
 - Privacy options are negotiated and tested
 - Open / Shared Key
- Association
 - Link is established
 - AP updates its table of mobile units (route table)



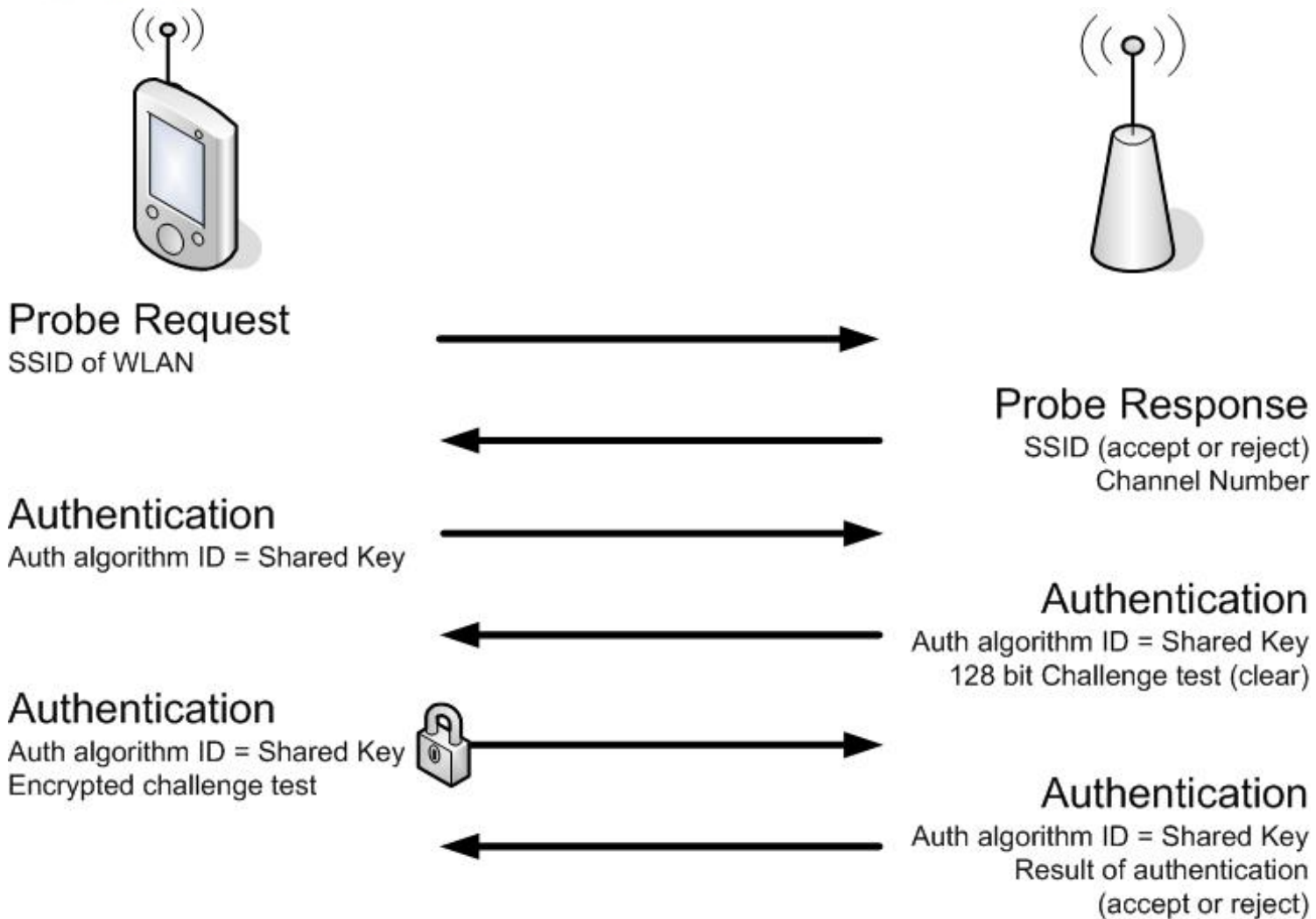
Authentication

- 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



Shared Key Authentication





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