IEEE 802.11 MAC (III)

รศ. ดร. อนันต์ ผลเพิ่ม

Assoc. Prof. Anan Phonphoem, Ph.D.

anan.p@ku.ac.th

Intelligent Wireless Network Group (IWING Lab)

http://iwing.cpe.ku.ac.th

Computer Engineering Department

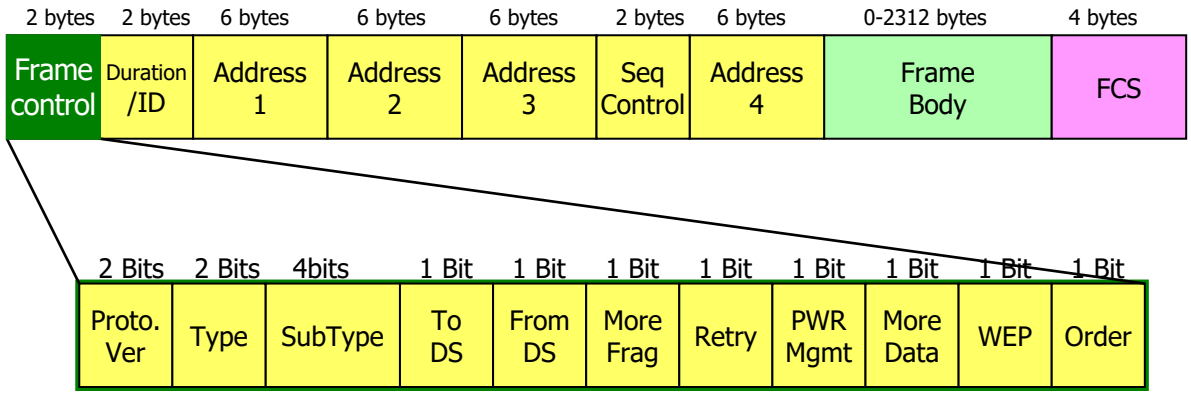
Kasetsart University, Bangkok, Thailand

Wireshark

- By regular capture,
  - Only data packet are displayed
  - No 802.11 management nor control frames
  - 802.11 packet header will be translated (by network driver) to "fake" Ethernet packet header
- With monitor mode,
  - 802.11 headers will be displayed (some work regardless of monitor mode)
  - On Linux and Mac OS X, 802.11 headers only appear in monitor mode

802.11 frame provides information about

- Frame type
- Source and destination addresses
- BSSID
- Power management
- etc.



802.11 frame does not provide

- Current operating channel (e.g. 6, 32, …)
- Channel width (e.g. 20, 40, 80 MHz)
- Frequency band (e.g. 2.4 or 5 GHz)
- Received signal strength (e.g. -56 dBm)
- Modulation technique (e.g. OFDM)
- Other RF environments

➔ … Physical Layer Information

http://wifinigel.blogspot.com/2017/05/wireshark-custom-columns-for-wireless.html

Physical Layer Information

- A captured packet contains a copy of the frame data
- prepended to each frame is a **metadata** header
  - information about how the frame was captured
- For **Wired** packet, the metadata is
  - Frame number
  - Date/Time when the packet was captured
  - Packet's length
  - Not so interesting about the physical layer (with a bit error rate of 10^{10})
- For **Wireless** packet – the physical layer is quite complex and important

Example of Important Physical Layer Info.

- Signal Strength (**RSSI**) [Signal/Noise Ratio]
- NIC captured the packet with RSSI power level (dBm)
  - < -90: signal is extremely weak (receiver lower limit)
  - ~ -67: fairly strong signal
    (Cisco -- adequate for VoWLAN)
  - > -55: very strong signal
  - > -30: locates next to the transmitter

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html

Radiotap Header

- Tries to provide those missing information about the captured frame
- For better understanding while analyzes the wireless traffic
- At the time packet being captured
  - NIC (driver) will collect the wireless status used for capturing the particular 802.11 frame
  - Present these information as a "Radiotap header" along with each corresponding captured frame
  - Obviously, it is not part of 802.11 frame

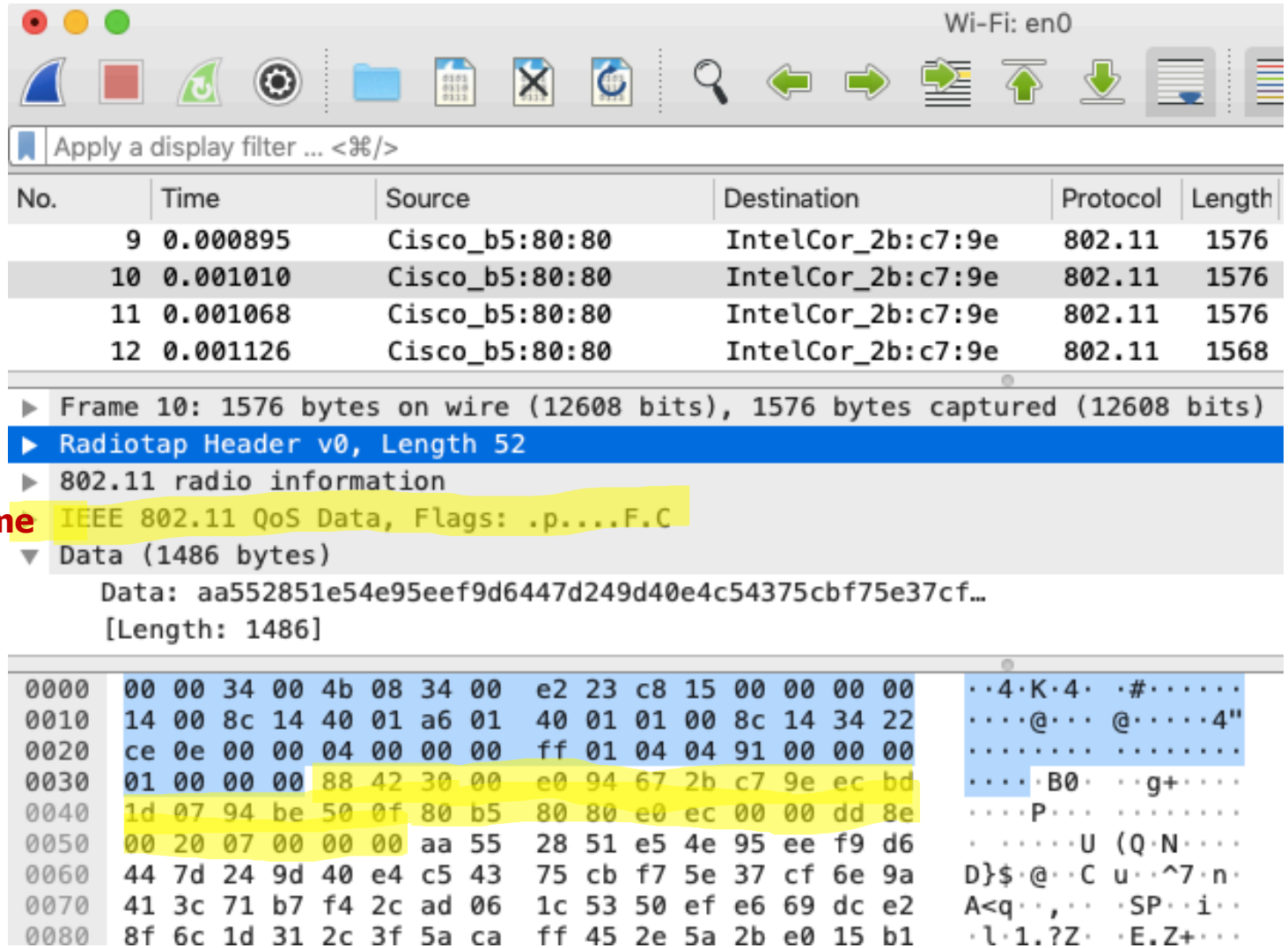
Radiotap Header

- Depends upon the wireless NIC (driver)
  - Some provide information
    ➔ "radiotap header" appears
  - Some do not provide any information
    ➔ No "radiotap header"
- Radiotap header will appear as a header that encapsulates the regular 802.11 frame
- Appear in various length (e.g. 25, 44, 52 bytes)
- Along with **Radiotap header**,
  - "**802.11 Radio Information**" are also presented

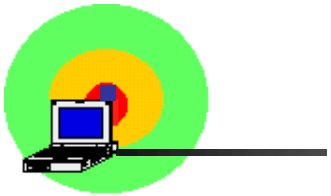
Radiotap Header

- Can be understood and presented in ”Wireshark” program or other sniffers
- De facto standard for 802.11 frame injection and reception
- http://www.radiotap.org

Example Radiotap header

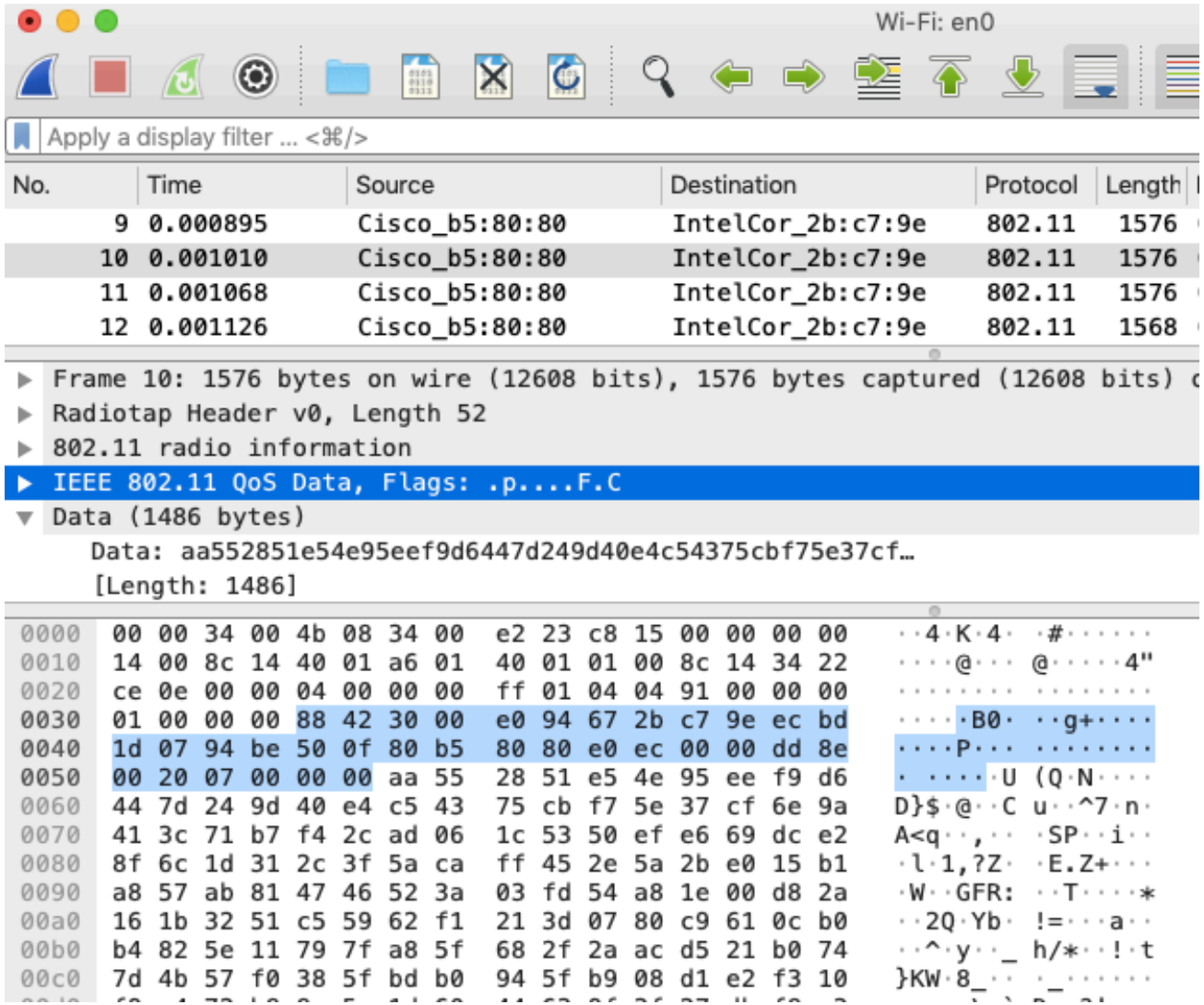


802.11 frame



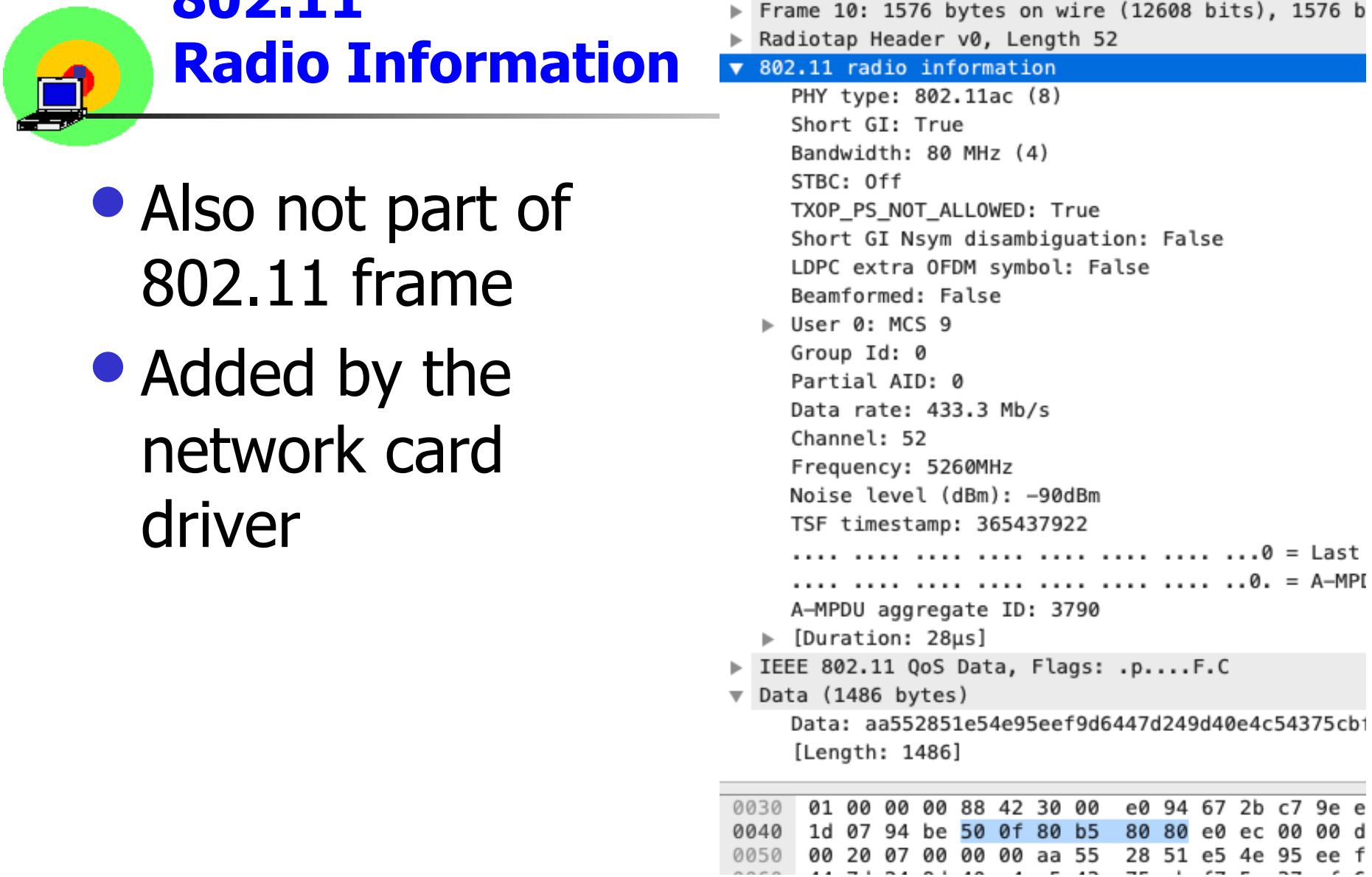
```
    10 0.001010      Cisco_b5:80:80       IntelCor_2b:c7:9e    802.11   1576 802.11
▶ Frame 10: 1576 bytes on wire (12608 bits), 1576 bytes captured (12608 bits) on int
▼ Radiotap Header v0, Length 52
    Header revision: 0
    Header pad: 0
    Header length: 52
  ▶ Present flags
    MAC timestamp: 365437922
  ▼ Flags: 0x14
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .1.. = WEP: True
      .... 0... = Fragmentation: False
      ...1 .... = FCS at end: True
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Channel frequency: 5260 [A 52]
  ▼ Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing (OFDM), 5 GHz
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
      .... .... 0... .... = 2 GHz spectrum: False
      .... ...1 .... .... = 5 GHz spectrum: True
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna noise: -90dBm
    Antenna: 1
    Channel number: 52
    Channel frequency: 5260
  ▶ Channel flags: 0x00010140, Orthogonal Frequency-Division Multiplexing (OFDM), 5
  ▶ A-MPDU status
  ▶ VHT information
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: .p....F.C
▼ Data (1486 bytes)
    Data: aa55285ac54c05eef0d6447d249d40e4c54375cbf75e37cf

0000  00 00 34 00 4b 08 34 00  e2 23 c8 15 00 00 00 00    ··4·K·4· ·#·····
```


Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length
9 0.000895 Cisco_b5:80:80 IntelCor_2b:c7:9e 802.11 1576
10 0.001010 Cisco_b5:80:80 IntelCor_2b:c7:9e 802.11 1576
11 0.001068 Cisco_b5:80:80 IntelCor_2b:c7:9e 802.11 1576
12 0.001126 Cisco_b5:80:80 IntelCor_2b:c7:9e 802.11 1568
Frame 10: 1576 bytes on wire (12608 bits), 1576 bytes captured (12608 bits)
Radiotap Header v0, Length 52
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p....F.C
Data (1486 bytes)
Data: aa552851e54e95eef9d6447d249d40e4c54375cbf75e37cf…
[Length: 1486]
0000 00 00 34 00 4b 08 34 00 e2 23 c8 15 00 00 00 00
0010 14 00 8c 14 40 01 a6 01 40 01 01 00 8c 14 34 22
0020 ce 0e 00 00 04 00 00 00 ff 01 04 04 91 00 00 00
0030 01 00 00 00 88 42 30 00 e0 94 67 2b c7 9e ec bd
0040 1d 07 94 be 50 0f 80 b5 80 80 e0 ec 00 00 dd 8e
0050 00 20 07 00 00 00 aa 55 28 51 e5 4e 95 ee f9 d6
0060 44 7d 24 9d 40 e4 c5 43 75 cb f7 5e 37 cf 6e 9a
0070 41 3c 71 b7 f4 2c ad 06 1c 53 50 ef e6 69 dc e2
0080 8f 6c 1d 31 2c 3f 5a ca ff 45 2e 5a 2b e0 15 b1
0090 a8 57 ab 81 47 46 52 3a 03 fd 54 a8 1e 00 d8 2a
00a0 16 1b 32 51 c5 59 62 f1 21 3d 07 80 c9 61 0c b0
00b0 b4 82 5e 11 79 7f a8 5f 68 2f 2a ac d5 21 b0 74
00c0 7d 4b 57 f0 38 5f bd b0 94 5f b9 08 d1 e2 f3 10

802.11 Radio Information

- Also not part of 802.11 frame
- Added by the network card driver



WLAN Standard	Band	VHT IE	HT IE	MCS	Avaiable Bandwith	Channel Type	Datarates
IEEE 802.11 b	2,4	-	-	-	20	CCK *1	1, 2, 5.5 or 11
IEEE 802.11 g	2,4	-	-	-	20	OFDM *1	6, 12, 18, 24, 36, 48 or 54
	2,4	-	x	x	20 / 40	OFDM	
IEEE 802.11 n	5	-	x	x	20 / 40	OFDM	
IEEE 802.11 a*2	5	-	-	-	20	OFDM	
IEEE 802.11 ac	5	x	-	x	20 / 40 / 80 / 160	OFDM	
IEEE 802.11 ad*3	60			x	2GHz	*3	

*1 = In an IEEE 802.11b/g mixed environment CCK-OFDM channel is used

*2 = Th IEEE 802.11h specification extends the IEEE 802.11a specification only with the techniques of DFS and TPC to be non reactive with Weatherradars

*3= The 802.11ad Directional multi-gigabit (DMG) PHY supports three distinct modulation methods:

1. Spread-spectrum, the Control PHY (MCS 0)
2. Single carrier, the Single Carrier PHY (MCS 1 to MCS 12) and the Low-Power Single Carrier PHY (MCS 25 to MCS 31)
3. OFDM, the OFDM PHY (MCS 13 to MCS 24)