Computer Networking

COMP 177 | Fall 2020 | University of the Pacific | Jeff Shafer

WiFi
IEEE 802.11

Recap

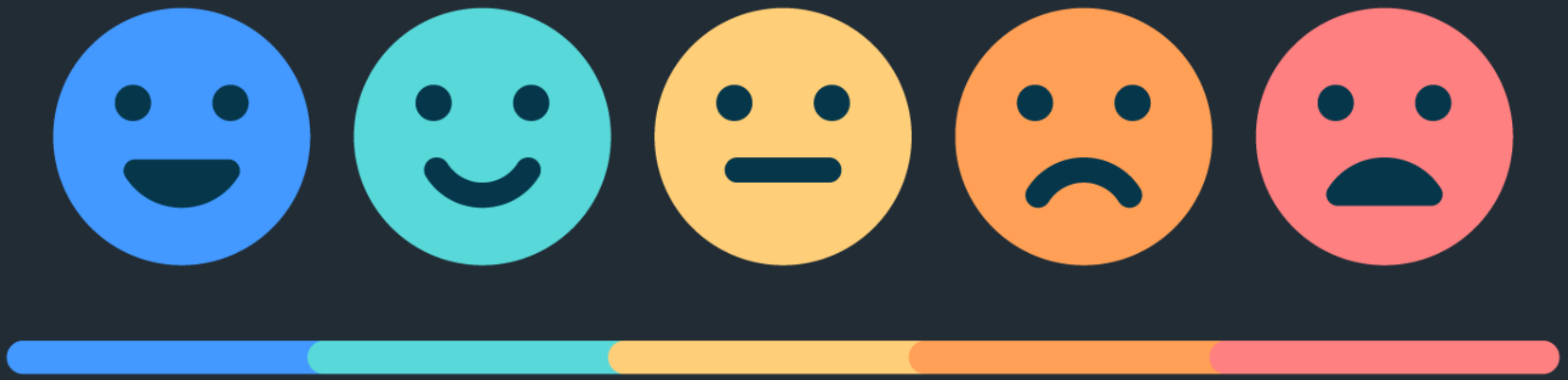
Past Topics

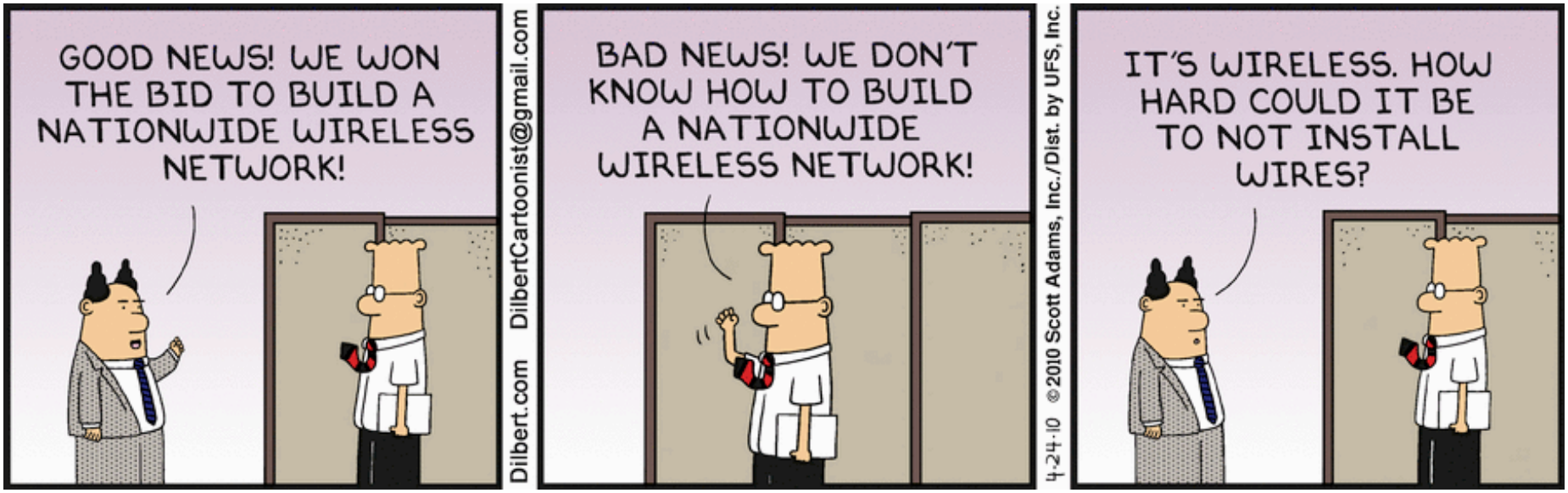
- An overview of computer networking
- Wireshark
- Ethernet

Today's Topics

- WiFi!
  - Network structure
  - Challenges
  - Packet types and standards
  - Packet format

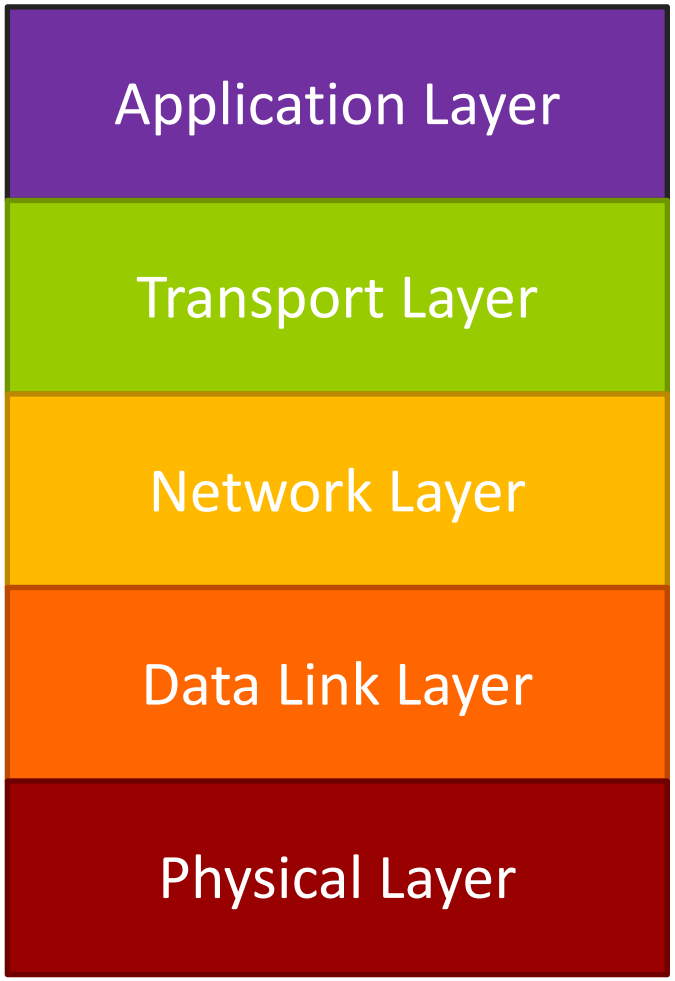
Week 3 Feedback: Class Thus Far?




GOOD NEWS! WE WON THE BID TO BUILD A NATIONWIDE WIRELESS NETWORK!
BAD NEWS! WE DON'T KNOW HOW TO BUILD A NATIONWIDE WIRELESS NETWORK!
IT'S WIRELESS. HOW HARD COULD IT BE TO NOT INSTALL WIRES?
Dilbert.com DilbertCartoonist@gmail.com
4-24-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.

Classic Network Model

(Not ISO model, but as actually implemented)



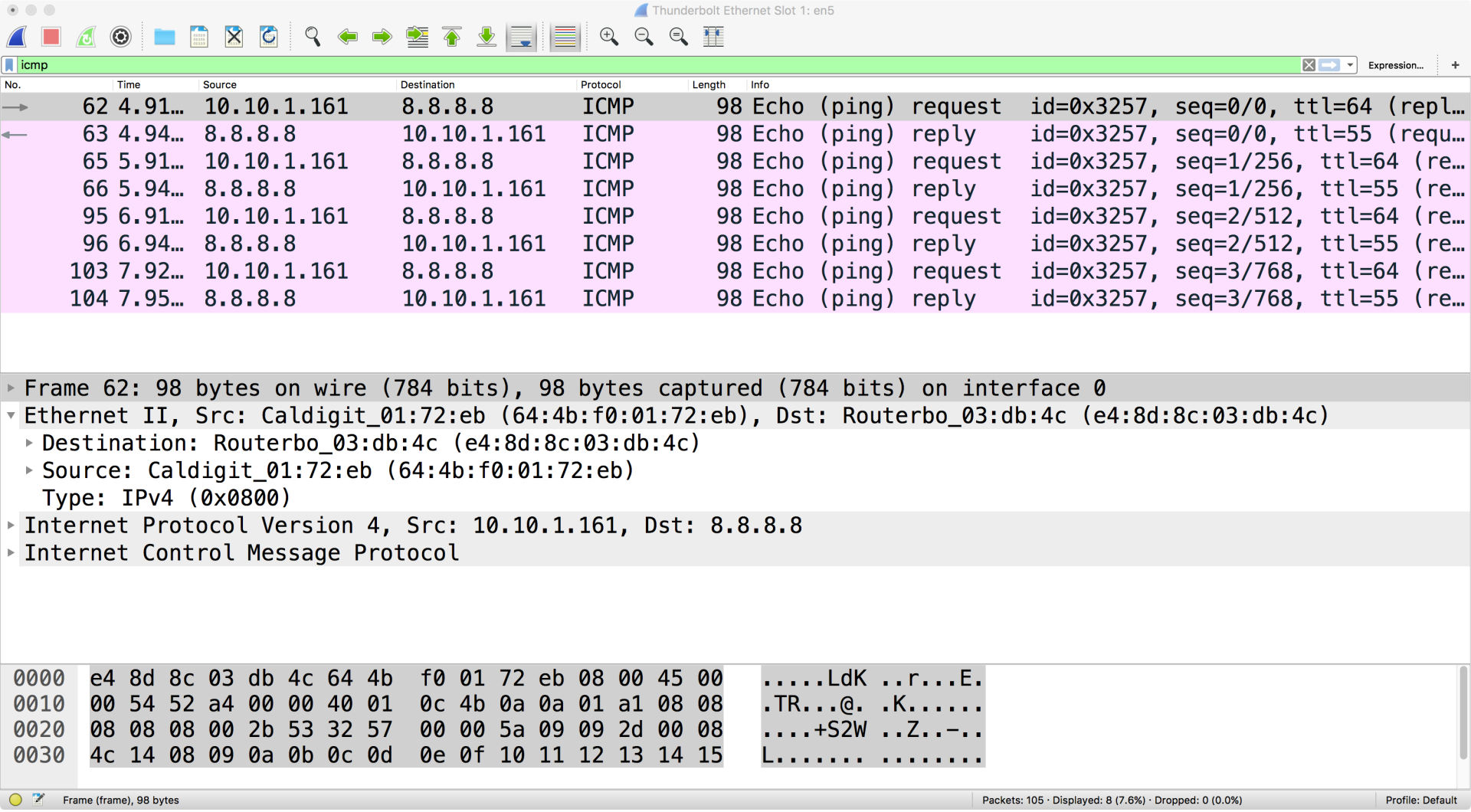
Layer 5 HTTP, ….

Layer 4 TCP, ….

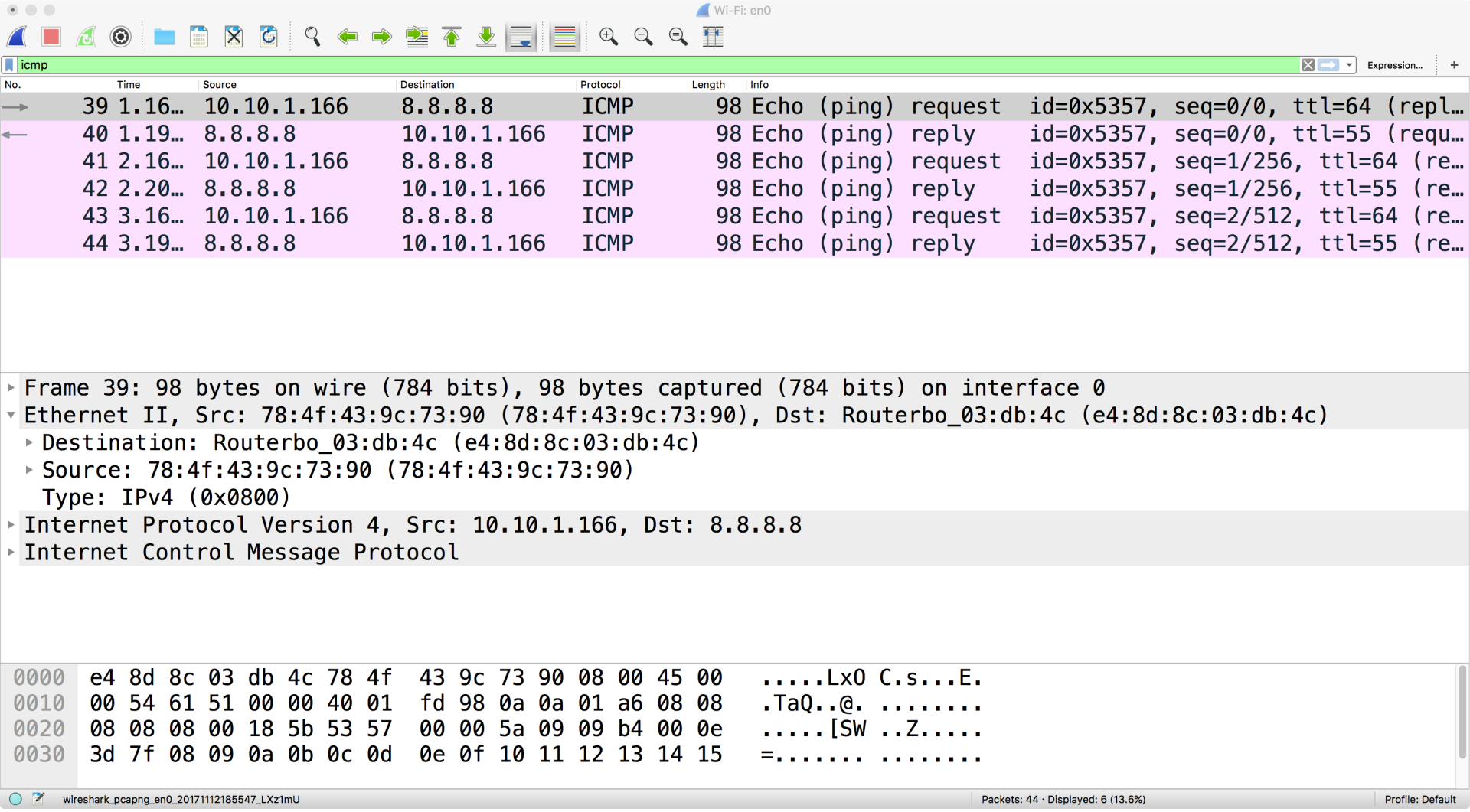
Layer 3 IP (IP addresses, routers, ….)

Layer 2 Ethernet (MAC addresses, switches, …)

Layer 1 Bits on a wire…



Wireshark capture of *wired* Ethernet



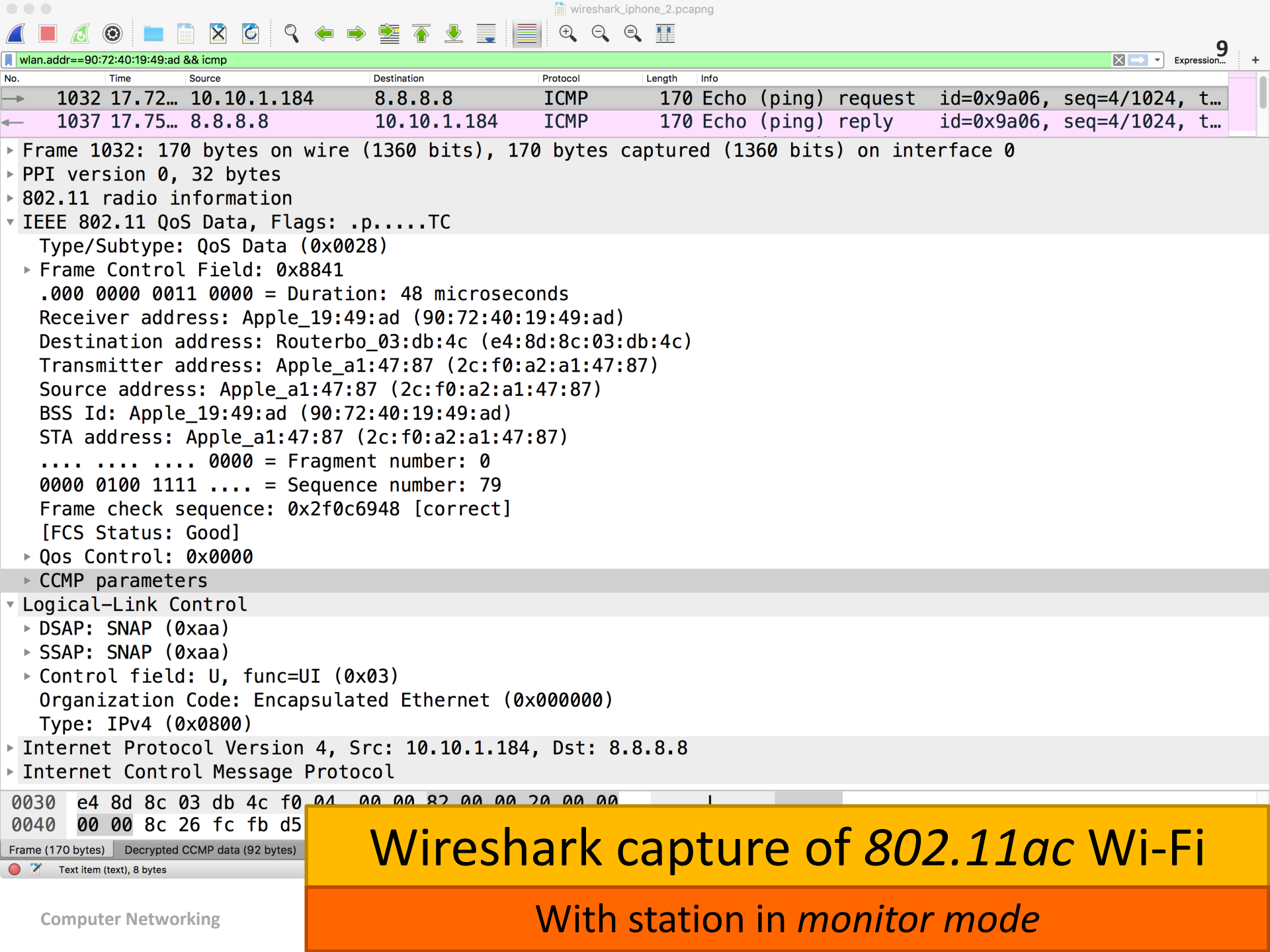
Wireshark capture of *802.11ac* Wi-Fi

Looks like wired Ethernet, so lecture over, right?

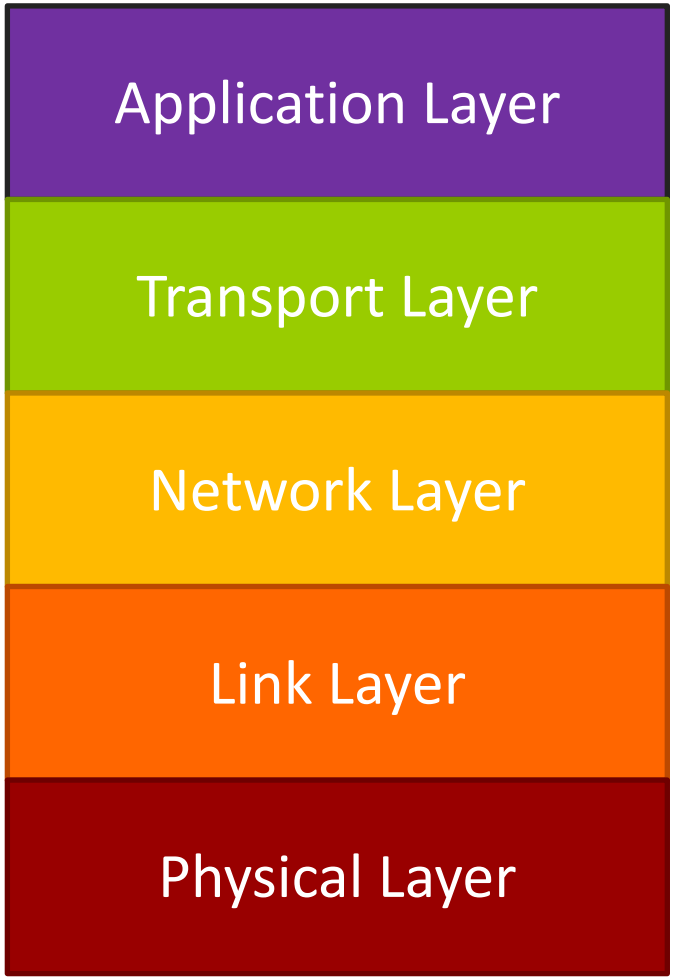
802.11

802.11 looks like Ethernet

… but only at the *network layer* and above


wireshark_iphone_2.pcapng
wlan.addr==90:72:40:19:49:ad && icmp
Expression...
9
No. Time Source Destination Protocol Length Info
1032 17.72… 10.10.1.184 8.8.8.8 ICMP 170 Echo (ping) request id=0x9a06, seq=4/1024, t…
1037 17.75… 8.8.8.8 10.10.1.184 ICMP 170 Echo (ping) reply id=0x9a06, seq=4/1024, t…
Frame 1032: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Apple_19:49:ad (90:72:40:19:49:ad)
Destination address: Routerbo_03:db:4c (e4:8d:8c:03:db:4c)
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)
STA address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
.... 0000 = Fragment number: 0
0000 0100 1111 .... = Sequence number: 79
Frame check sequence: 0x2f0c6948 [correct]
[FCS Status: Good]
Qos Control: 0x0000
CCMP parameters
Logical-Link Control
DSAP: SNAP (0xaa)
SSAP: SNAP (0xaa)
Control field: U, func=UI (0x03)
Organization Code: Encapsulated Ethernet (0x000000)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.184, Dst: 8.8.8.8
Internet Control Message Protocol
0030 e4 8d 8c 03 db 4c f0
0040 00 00 8c 26 fc fb d5
Frame (170 bytes)
Decrypted CCMP data (92 bytes)
Text item (text), 8 bytes
Wireshark capture of 802.11ac Wi-Fi
With station in monitor mode
Computer Networking

Network Model



Layer 4

Layer 3

Layer 2

Layer 1

HTTP, ….

TCP, ….

IP (IP addresses, routers, ….)

802.2 Logical Link Control (LLC)
802.11 MAC header *(identical a,b,g,n,…)*

802.11 PLCP header *(varies a,b,g,n,…)*
Physical media (DSSS, OFDM, …)

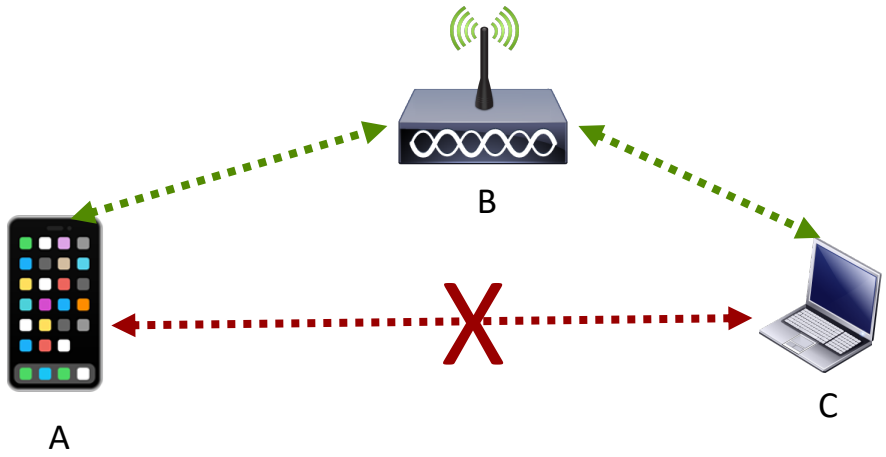
IEEE 802.11 Physical Layer

Physical Layer (PHY)

- Purpose: Transmit raw bits over a physical link
  - Copper wire, optical cable, **wireless**
- Challenges
  - Convert input bitstream into symbols/code words?
  - Frequencies to transmit on?
  - Modulation scheme?
- **Layer 1**

Physical Layer Challenges

- Stations can move
  - Changes propagation delays and signal strength
- Non-transitive reception
  - A can hear B
  - B can hear C
  - A cannot hear C
- No collision detection
  - Must detect unsuccessful transmission by absence of acknowledgement

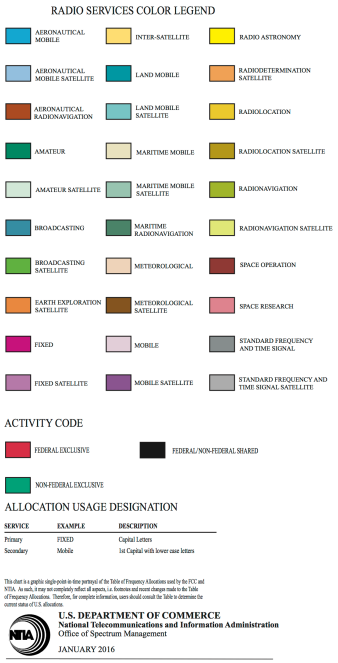


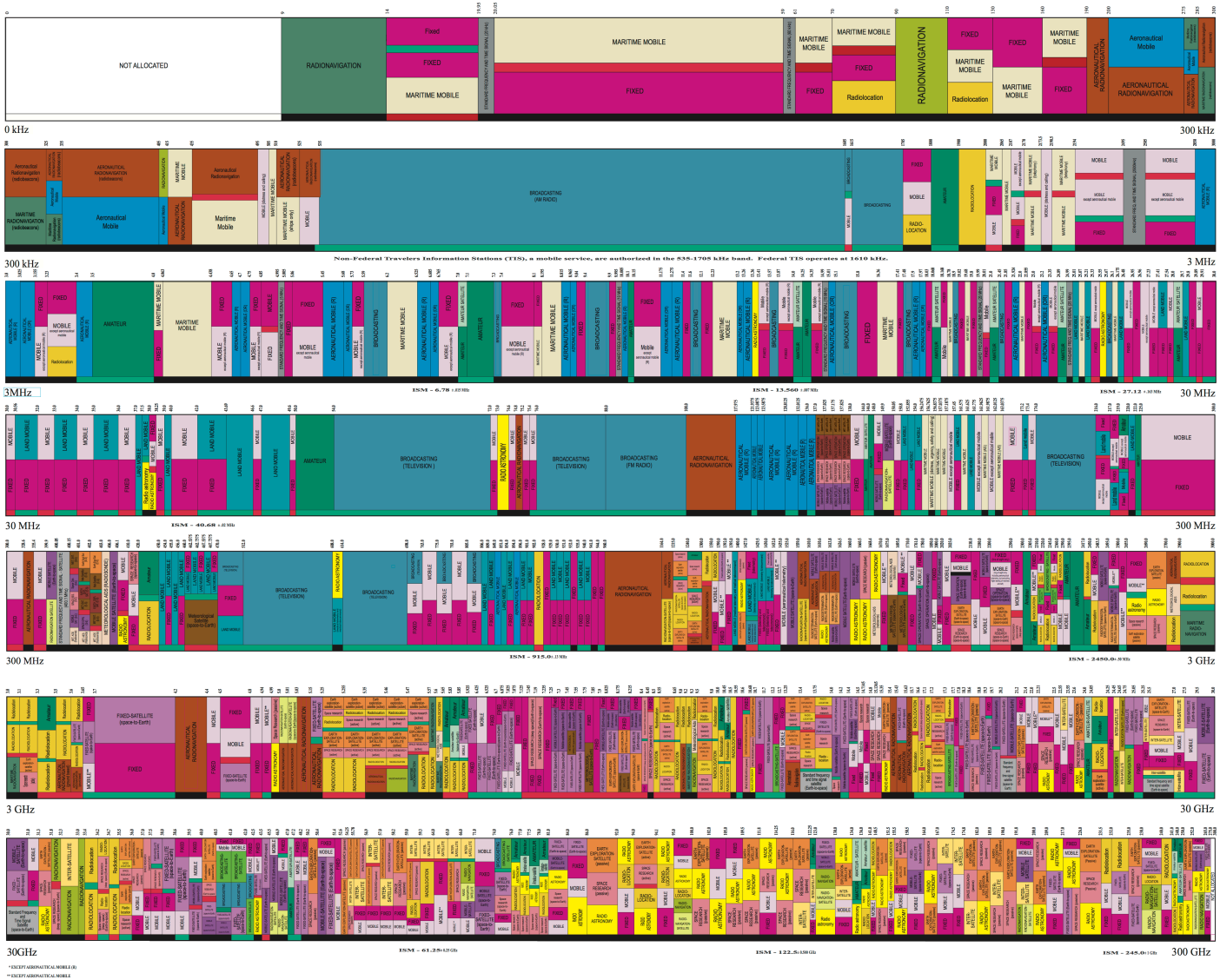
Physical Layer Challenges

- Range of network limited by transmission power
  - Limits end-to-end propagation delay
- Radio Frequency (RF) spectrum usage limited by law and treaty
  - 802.11 uses 2.4 GHz and 5 GHz bands
    - Industrial, Scientific, Medicine (ISM) bands
    - Unlicensed National Information Infrastructure (U-NII)
  - Must use spread spectrum technology to minimize interference with other devices

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM





https://www.ntia.doc.gov/page/2011/united-states-frequency-allocation-chart [Last Update: 2016]

It sure *looks* fast….

802.11 Physical Layer Standards

802.11 Protocol	Release date	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range	
							Indoor	Outdoor
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, **54**	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7						5,000 m (16,000 ft)
b	Sep 1999	2.4	22	1, 2, 5.5, **11**	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, **54**	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
n	Oct 2009	2.4/5	20	Up to **288.8**	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)
			40	Up to 600				
ac	Dec 2013	5	20	Up to **346.8**	8	MIMO-OFDM	35 m (115 ft)	
			40	Up to 800				
			80	Up to 1733.2				
			160	Up to 3466.8				

https://en.wikipedia.org/wiki/IEEE_802.11

Frequency

2.4 GHz

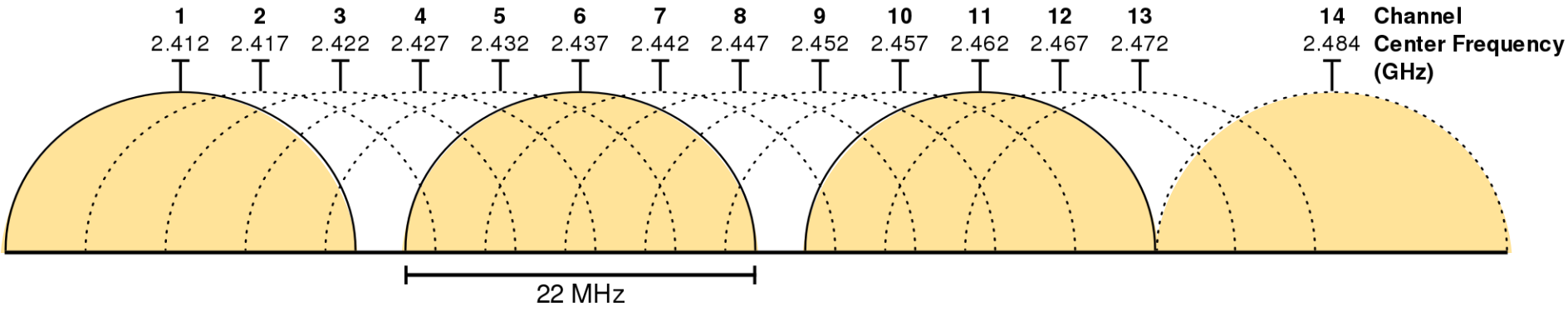
- Longer range
- Lower data rate
- Increased penetration of walls and floors
- Particularly crowded
  - Used by many other devices besides WiFi (cordless phones, Bluetooth, wireless microphones, …)
  - Subject to interferences (microwave ovens)

5 GHz

- Shorter range
- Higher data rate due to higher frequency
- Attenuated more severely by walls and floors

Each increment in **channel number** is +5MHz

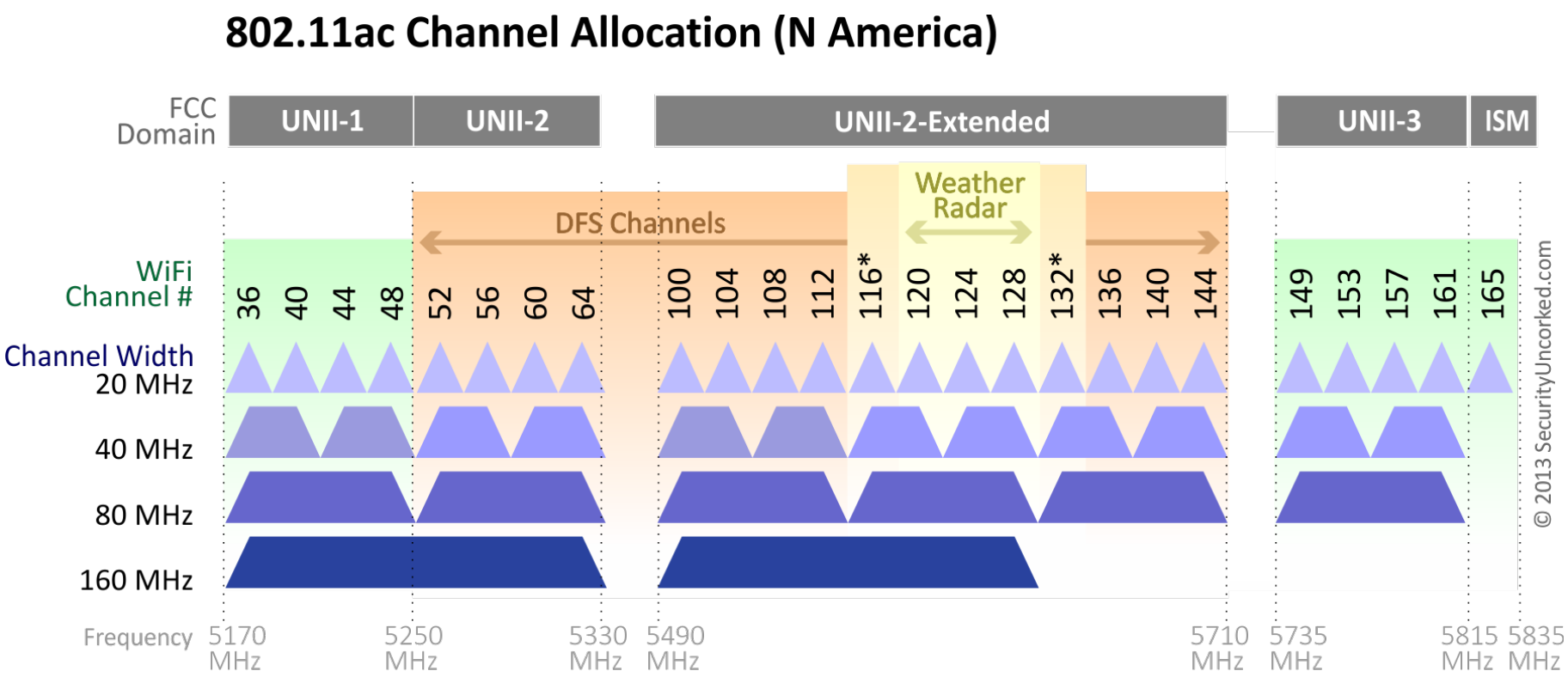
802.11 2.4 GHz Channels



2.4 GHz: Channels 1-11 valid in North America
Only 3 non-overlapping channels! (Or 4 in Japan)

https://en.wikipedia.org/wiki/List_of_WLAN_channels

802.11 5GHz Channels



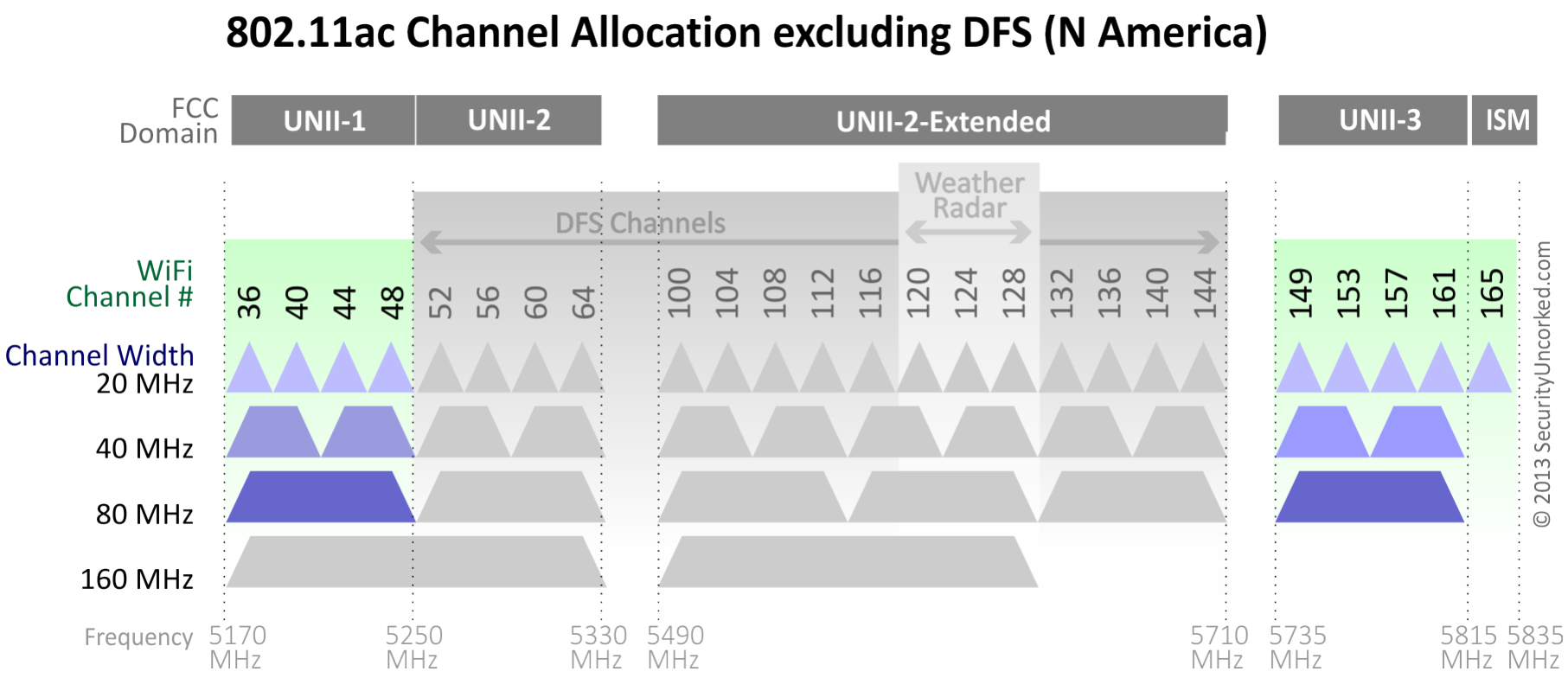
*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

http://securityuncorked.com/2013/11/the-best-damn-802-11ac-channel-allocation-graphics/

Dynamic Frequency Selection (DFS)

- **Regulatory requirement**: If your wireless device (access point, station, etc..) wants to use certain licensed 5GhZ frequencies, it must listen for **and avoid** interference
  - i.e. Your unlicensed device can only use the frequency in the *absence* of any licensed users
- Licensed users
  - Doppler weather **radar**
  - Civilian aviation **radar**
  - Military **radar**
  - Satellite **radar**

802.11 5GHz Channels



http://securityuncorked.com/2013/11/the-best-damn-802-11ac-channel-allocation-graphics/

802.11 5GHz Channels

802.11ac Channel Availability (N America)

Channel Width	Number of channels available	
	Using DFS	DFS Excluded
40 MHz	9-10*	4
80 MHz	4-5*	2
160 MHz	1	0

*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

http://securityuncorked.com/2013/11/the-best-damn-802-11ac-channel-allocation-graphics/

802.11 Physical Layer Standards

802.11 Protocol	Release date	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range	
							Indoor	Outdoor
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, **54**	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7						5,000 m (16,000 ft)
b	Sep 1999	2.4	22	1, 2, 5.5, **11**	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, **54**	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
n	Oct 2009	2.4/5	20	Up to 288.8	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)
			40	Up to 600				
ac	Dec 2013	5	20	Up to 346.8	8	MIMO-OFDM	35 m (115 ft)	
			40	Up to 800				
			80	Up to 1733.2				
			160	Up to 3466.8				

https://en.wikipedia.org/wiki/IEEE_802.11

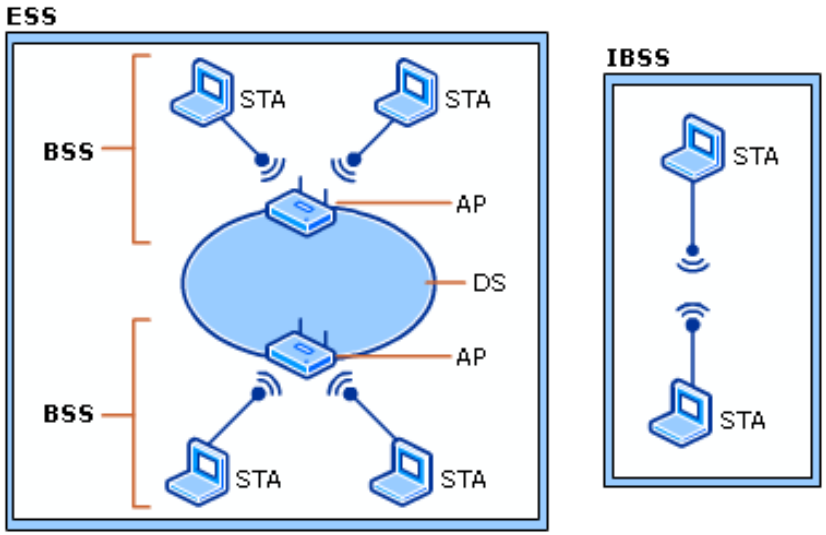
Bandwidth

- Tradeoffs
  - Smaller bandwidth (e.g. 20MHz)
    - Lower data rate
    - Lower risk of interference from APs on neighboring channels
  - Larger bandwidth (e.g. 40, 80MHz)
    - Higher data rate
    - Higher risk of interference from APs on neighboring channels
- Higher bandwidth channels (80MHz, 160MHz) difficult to use in enterprise settings due to interference

IEEE 802.11 Link Layer

Link Layer Terminology

- Station (**STA**)
  - Laptop, desktop, phone (and access point)
- Access Point (**AP**)
- Basic Service Set (**BSS**)
  - Set of stations controlled by common coordination function (decides who can transmit)
- Distribution System (**DS**)
  - Connects BSS and LANs together to form ESS
- Extended Service Set (**ESS**)



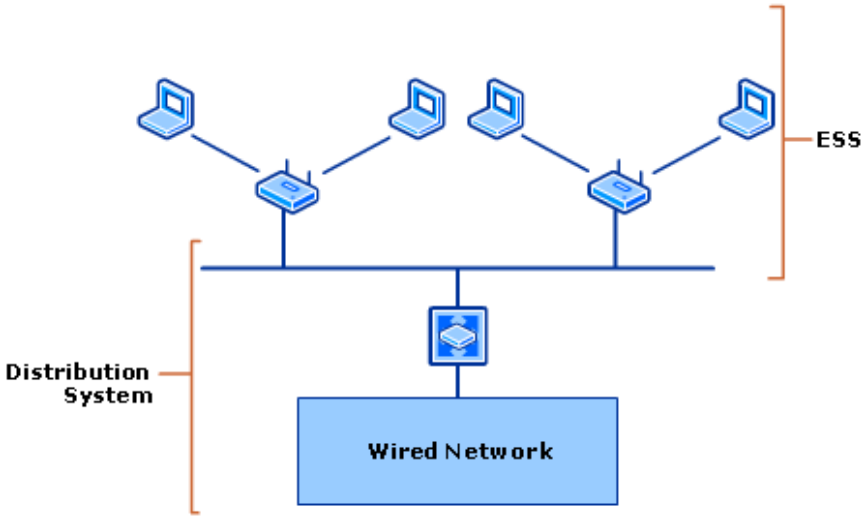
- Independent Basic Service Set (**IBSS**)
  - Ad-hoc network (no AP)

https://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx

Link Layer Terminology

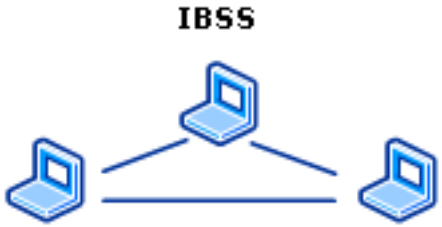
Infrastructure Mode

- One client (station) + One AP

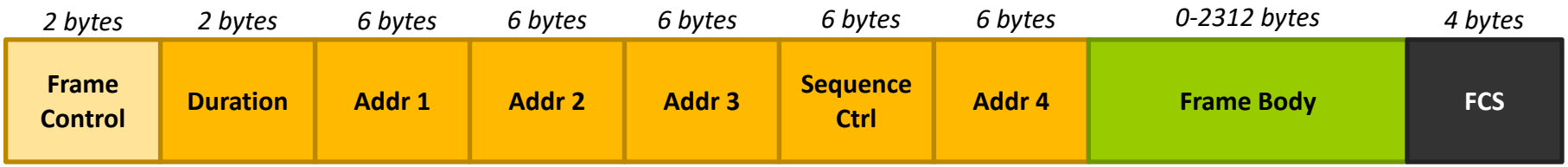


Ad-Hoc Mode

- Clients (stations) communicate directly with each other (no AP)

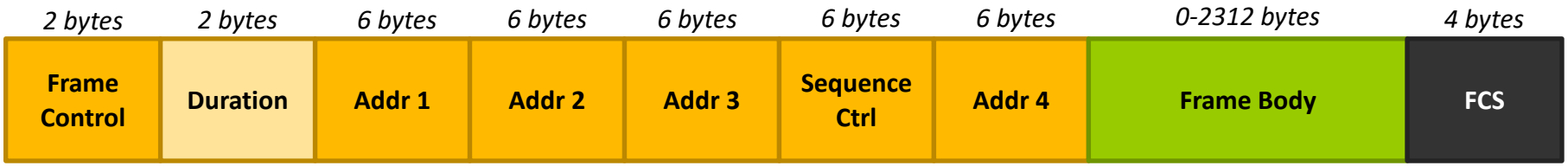


802.11 MAC Frame



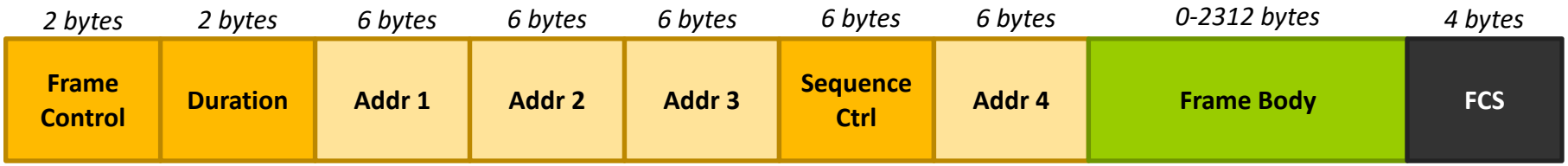
- Frame Control *(Bitfield)*
  - Protocol Version
  - Type/Subtype
  - **To DS / From DS (Distribution System, i.e. LAN)**
    - **Option 1: From STA to DS via an AP**
    - **Option 2: From DS to STA via AP**
    - ***Determines meaning of all the address fields!***
  - More Fragments
  - Power Management
  - Retry (in case ACK was not received)
  - Protected (encrypted)
  - …

802.11 MAC Frame



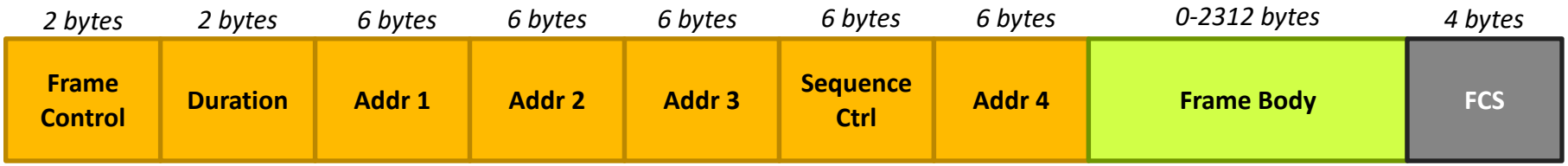
- Duration
  - Duration needed to receive next frame transmission in *microseconds*
  - i.e. Everyone else should stay quiet for this time!
- Field can also be *association ID*

802.11 MAC Frame



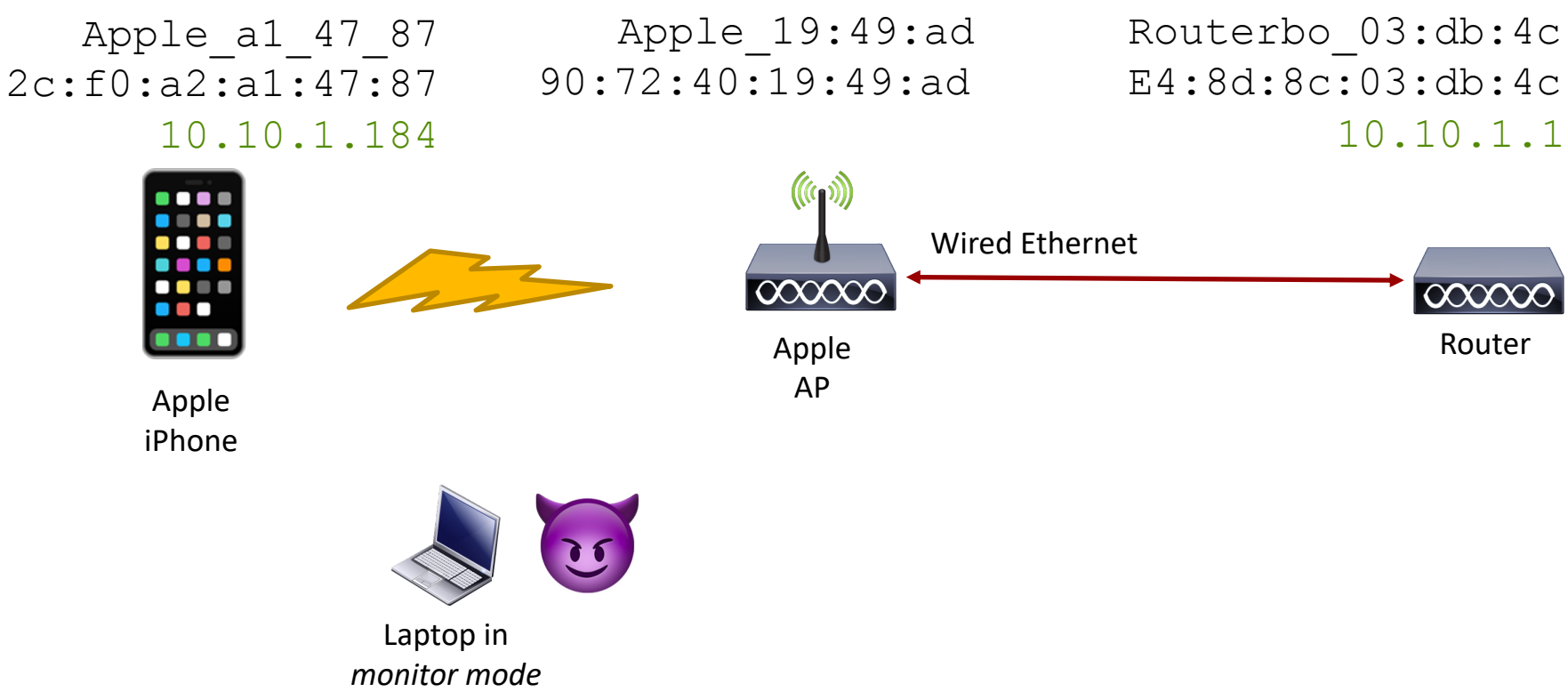
- 4 MAC address fields – will have some combination of:
  - Destination Address (DA) – Final destination to receive frame
  - Source Address (SA) – Original source that created and transmitted frame
  - Receiver Address (RA) – Address of next station on wireless medium to receive frame
  - Transmitter Address (TA) – MAC address of station that transmitted frame onto wireless medium
  - Basic Service Set Identifier (BSSID)
    - In infrastructure mode, BSSID is MAC address of access point

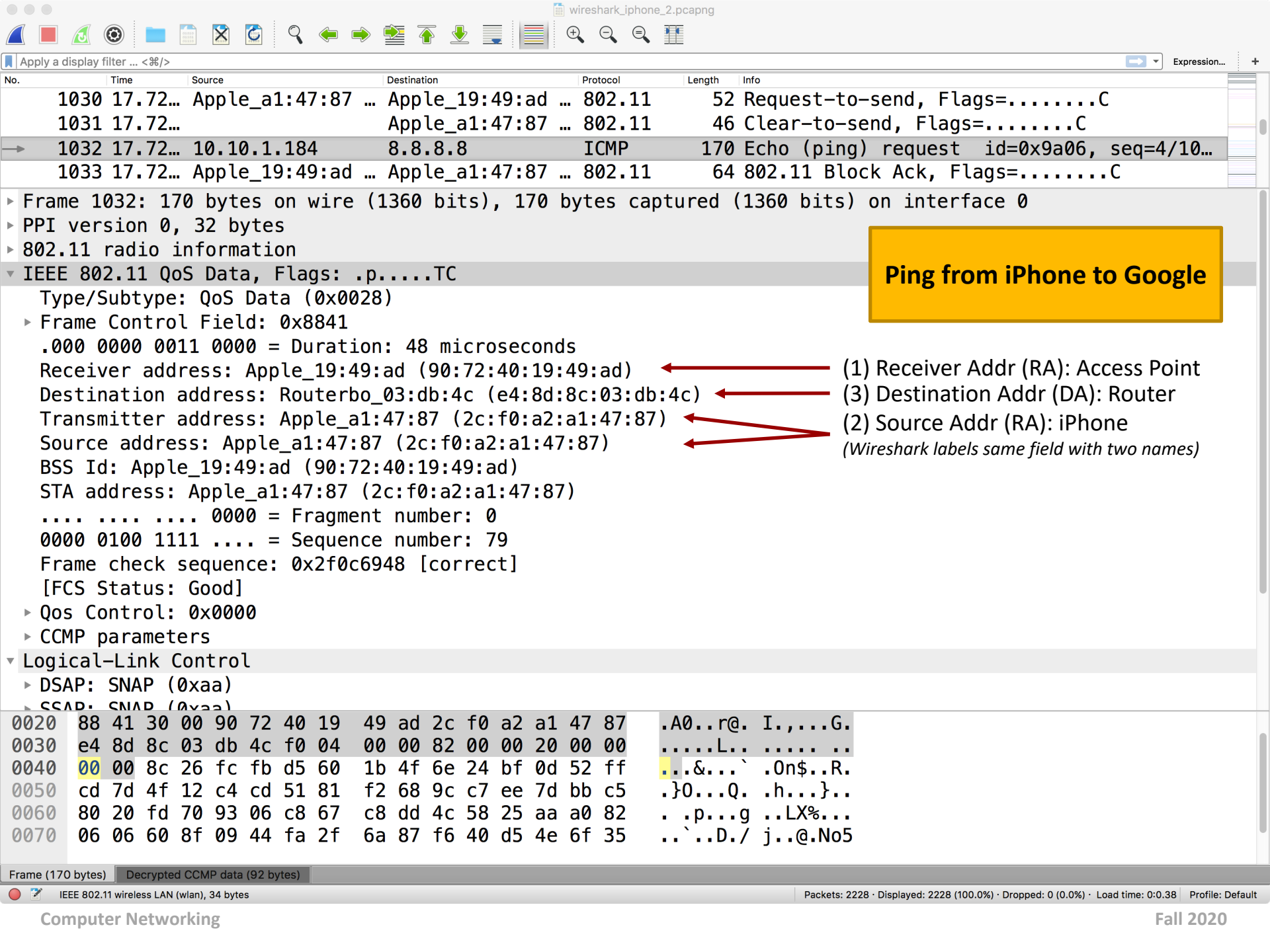
802.11 MAC Frame



- Frame Body = Payload
- FCS = Frame Check Sequence
  - Cyclic Redundancy Check (CRC) over all fields in MAC header and frame body

Example


Apple_a1_47_87
2c:f0:a2:a1:47:87
10.10.1.184
Apple_19:49:ad
90:72:40:19:49:ad
Routerbo_03:db:4c
E4:8d:8c:03:db:4c
10.10.1.1
Wired Ethernet
Apple
iPhone
Apple
AP
Router
Laptop in
monitor mode


wireshark_iphone_2.pcapng
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1030 17.72… Apple_a1:47:87 … Apple_19:49:ad … 802.11 52 Request-to-send, Flags=........C
1031 17.72… Apple_a1:47:87 … 802.11 46 Clear-to-send, Flags=........C
1032 17.72… 10.10.1.184 8.8.8.8 ICMP 170 Echo (ping) request id=0x9a06, seq=4/10…
1033 17.72… Apple_19:49:ad … Apple_a1:47:87 … 802.11 64 802.11 Block Ack, Flags=........C
Frame 1032: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Apple_19:49:ad (90:72:40:19:49:ad)
Destination address: Routerbo_03:db:4c (e4:8d:8c:03:db:4c)
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)
STA address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
.... 0000 = Fragment number: 0
0000 0100 1111 .... = Sequence number: 79
Frame check sequence: 0x2f0c6948 [correct]
[FCS Status: Good]
Qos Control: 0x0000
CCMP parameters
Logical-Link Control
DSAP: SNAP (0xaa)
0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87 .A0..r@. I.,...G.
0030 e4 8d 8c 03 db 4c f0 04 00 00 82 00 00 20 00 00 .....L.. ....
0040 00 00 8c 26 fc fb d5 60 1b 4f 6e 24 bf 0d 52 ff ...&...` .On$..R.
0050 cd 7d 4f 12 c4 cd 51 81 f2 68 9c c7 ee 7d bb c5 .}O...Q. .h...}..
0060 80 20 fd 70 93 06 c8 67 c8 dd 4c 58 25 aa a0 82 . .p...g ..LX%...
0070 06 06 60 8f 09 44 fa 2f 6a 87 f6 40 d5 4e 6f 35 ..`..D./ j..@.No5
Frame (170 bytes)
Decrypted CCMP data (92 bytes)
IEEE 802.11 wireless LAN (wlan), 34 bytes
Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38
Profile: Default
Ping from iPhone to Google
(1) Receiver Addr (RA): Access Point
(3) Destination Addr (DA): Router
(2) Source Addr (RA): iPhone
(Wireshark labels same field with two names)

wireshark_iphone_2.pcapng

Apply a display filter ... <⌘/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1030	17.72…	Apple_a1:47:87 …	Apple_19:49:ad …	802.11	52	Request-to-send, Flags=........C
1031	17.72…		Apple_a1:47:87 …	802.11	46	Clear-to-send, Flags=........C
1032	17.72…	10.10.1.184	8.8.8.8	ICMP	170	Echo (ping) request id=0x9a06, seq=4/10…
1033	17.72…	Apple_19:49:ad …	Apple_a1:47:87 …	802.11	64	802.11 Block Ack, Flags=........C

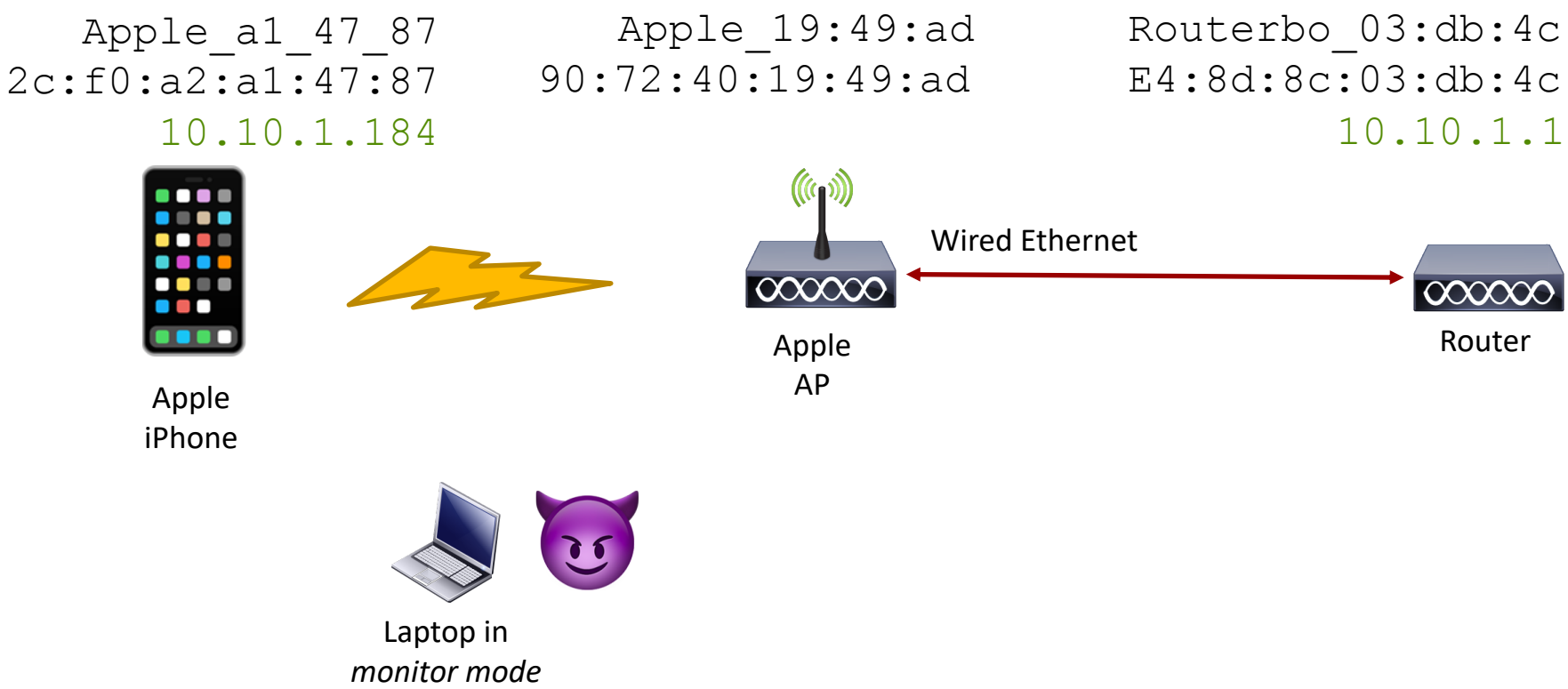
```
▸ Frame 1033: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▸ PPI version 0, 32 bytes
▸ 802.11 radio information
▾ IEEE 802.11 802.11 Block Ack, Flags: ........C
    Type/Subtype: 802.11 Block Ack (0x0019)
  ▸ Frame Control Field: 0x9400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
    Transmitter address: Apple_19:49:ad (90:72:40:19:49:ad)
    .... .10. = Block Ack Type: Compressed Block (0x2)
  ▸ Block Ack Request Control: 0x0005
  ▾ Block Ack Starting Sequence Control (SSC): 0x04f0
      .... .... .... 0000 = Fragment: 0
      0000 0100 1111 .... = Starting Sequence Number: 79
  ▸ Block Ack Bitmap: 0100000000000000
    Frame check sequence: 0x565263e4 [correct]
    [FCS Status: Good]
```

Block Acknowledgement
Sent from Access Point (. . :49:ad)
to iPhone (. . :47:87)
for sequence starting at 79

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 58 31 41 72   .. .i... ....X1Ar
0010  00 00 00 00 01 00 30 00  71 16 40 01 00 00 d2 a9   ......0. q.@.....
0020  94 00 00 00 2c f0 a2 a1  47 87 90 72 40 19 49 ad   ....,... G..r@.I.
0030  05 00 f0 04 01 00 00 00  00 00 00 00 e4 63 52 56   ........ .....cRV
```

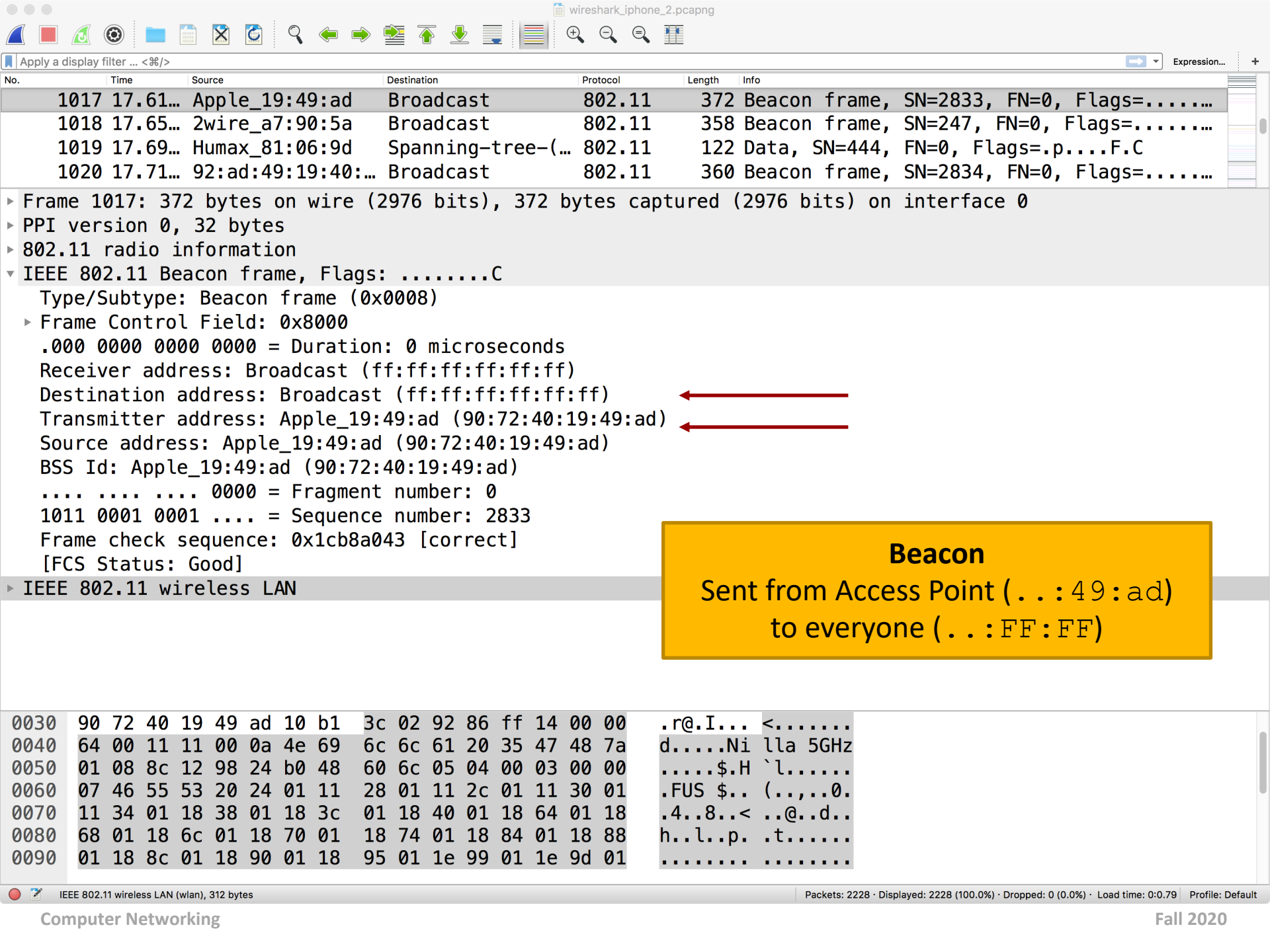
IEEE 802.11 wireless LAN (wlan), 16 bytes Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.77 Profile: Default

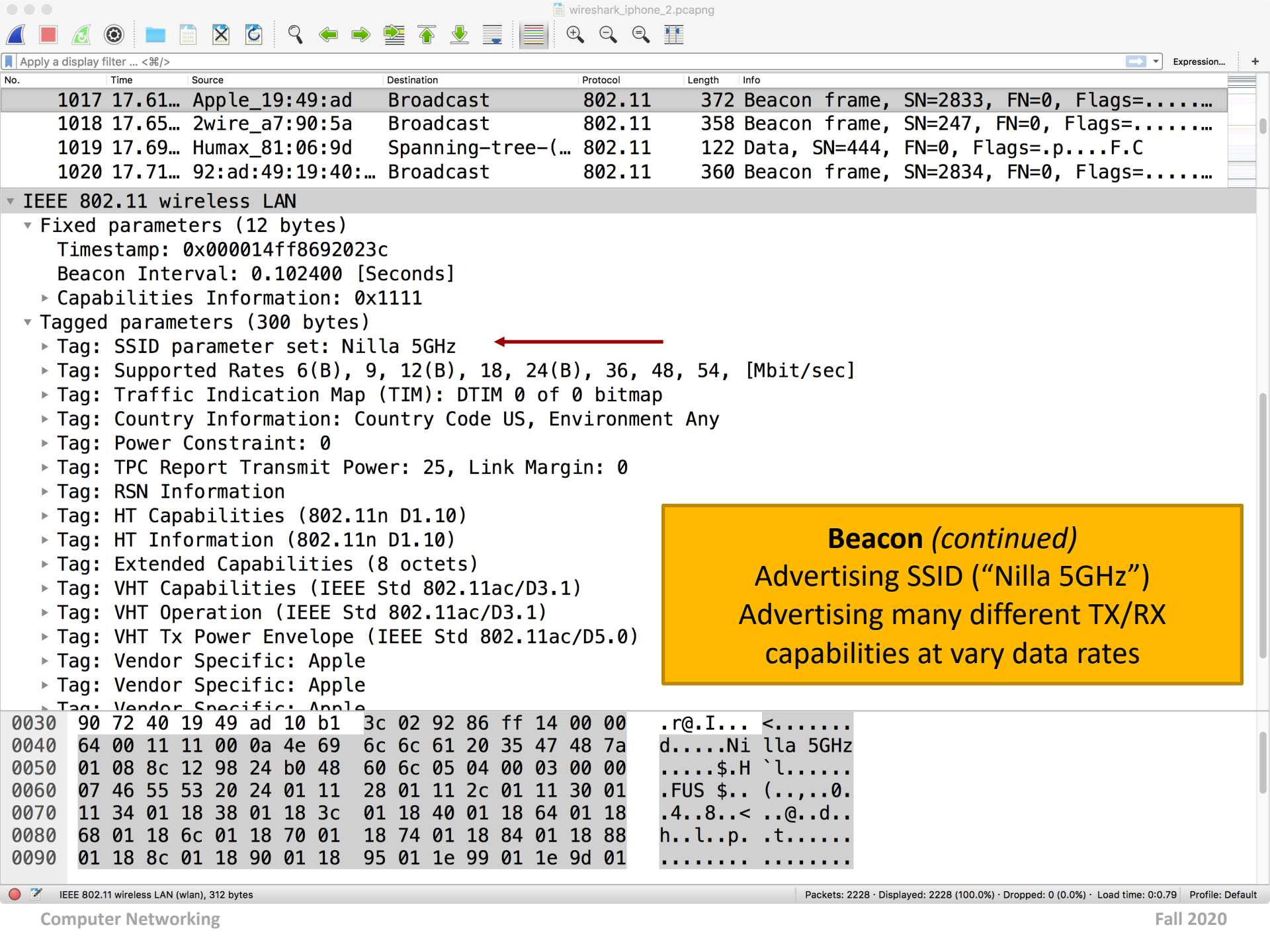
(Same) Example



Beacons and Probes

- **Beacon** Frames
  - Broadcast periodically by APs
  - Contains SSID (Service Set ID), AP address, Beacon Frame interval, supported data rates, other capabilities
- **Probe Request** Frames
  - Stations can solicit information from APs instead of waiting for beacon
  - Reply from AP sent in **Probe Response** frames


wireshark_iphone_2.pcapng
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1017 17.61… Apple_19:49:ad Broadcast 802.11 372 Beacon frame, SN=2833, FN=0, Flags=.....…
1018 17.65… 2wire_a7:90:5a Broadcast 802.11 358 Beacon frame, SN=247, FN=0, Flags=.....…
1019 17.69… Humax_81:06:9d Spanning-tree-(… 802.11 122 Data, SN=444, FN=0, Flags=.p....F.C
1020 17.71… 92:ad:49:19:40:… Broadcast 802.11 360 Beacon frame, SN=2834, FN=0, Flags=.....…
Frame 1017: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Apple_19:49:ad (90:72:40:19:49:ad)
Source address: Apple_19:49:ad (90:72:40:19:49:ad)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)
.... 0000 = Fragment number: 0
1011 0001 0001 .... = Sequence number: 2833
Frame check sequence: 0x1cb8a043 [correct]
[FCS Status: Good]
IEEE 802.11 wireless LAN
Beacon
Sent from Access Point (..:49:ad)
to everyone (..:FF:FF)
0030 90 72 40 19 49 ad 10 b1 3c 02 92 86 ff 14 00 00 .r@.I... <.......
0040 64 00 11 11 00 0a 4e 69 6c 6c 61 20 35 47 48 7a d.....Ni lla 5GHz
0050 01 08 8c 12 98 24 b0 48 60 6c 05 04 00 03 00 00 .....$.H `l......
0060 07 46 55 53 20 24 01 11 28 01 11 2c 01 11 30 01 .FUS $.. (..,..0.
0070 11 34 01 18 38 01 18 3c 01 18 40 01 18 64 01 18 .4..8..< ..@..d..
0080 68 01 18 6c 01 18 70 01 18 74 01 18 84 01 18 88 h..l..p. .t......
0090 01 18 8c 01 18 90 01 18 95 01 1e 99 01 1e 9d 01 ....
IEEE 802.11 wireless LAN (wlan), 312 bytes
Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.79
Profile: Default



Beacon *(continued)*

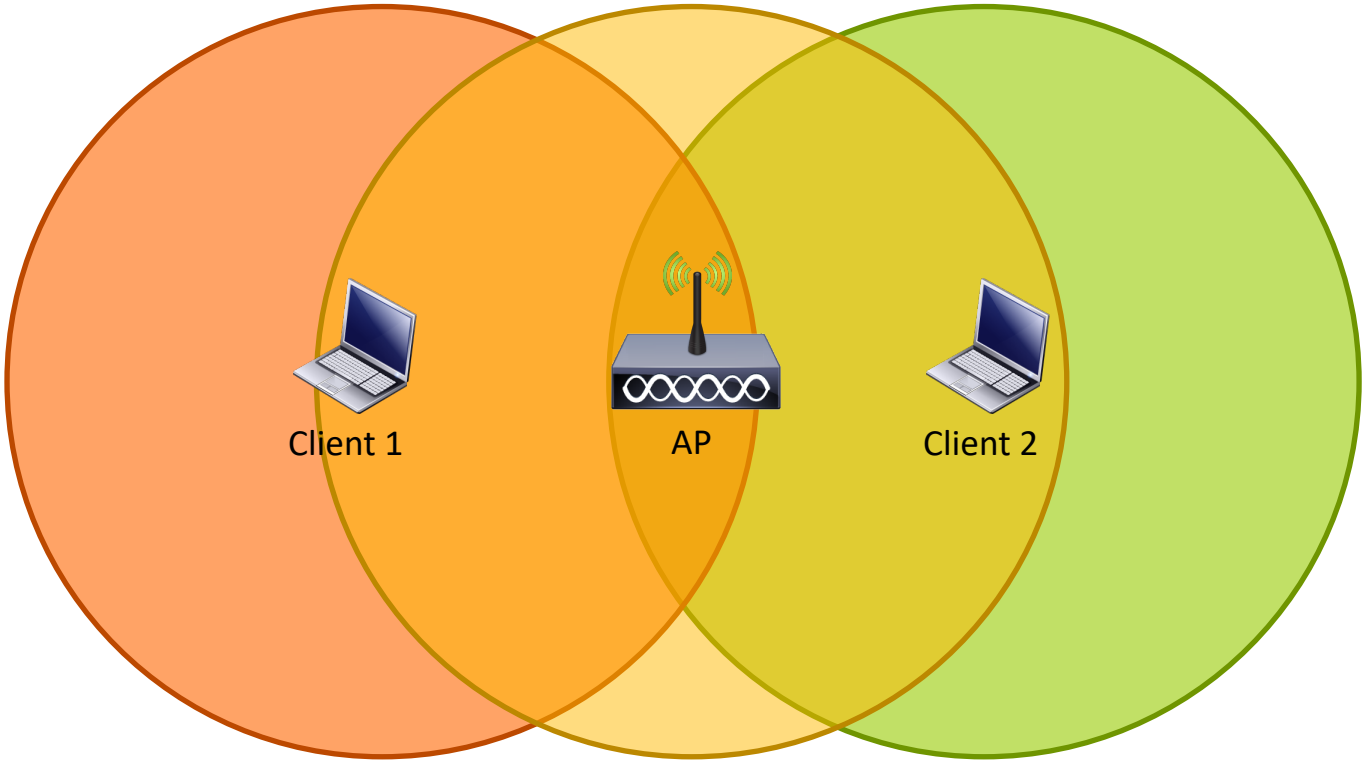
Advertising SSID (“Nilla 5GHz”)

Advertising many different TX/RX capabilities at vary data rates

Block Acknowledgements

- Phone and AP *negotiate* to enable **block acknowledgement** mode
  - Ability to send one ACK for multiple QoS data blocks
  - Introduced in 802.11e standard
  - Mandated in 802.11n and newer revisions

Hidden Node Problem



Client 1 <-> AP ✓

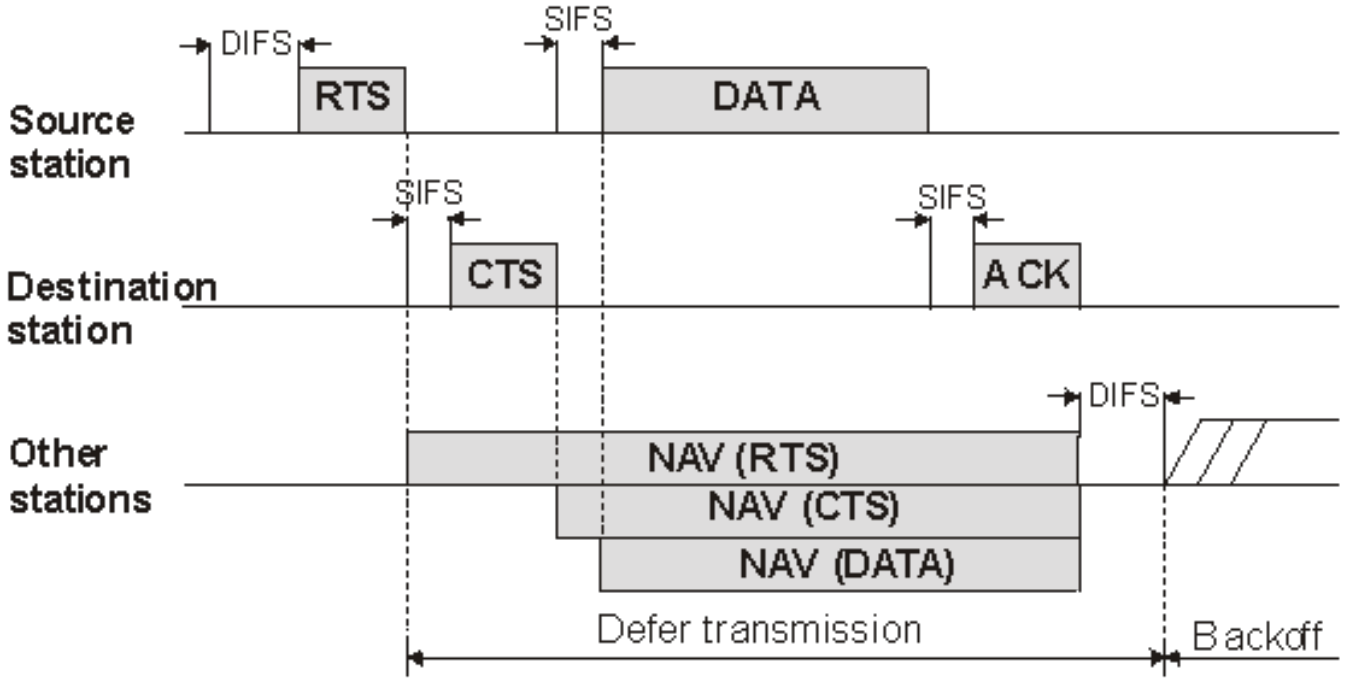
AP <-> Client 2 ✓

Client 1 <-> Client 2 🚫

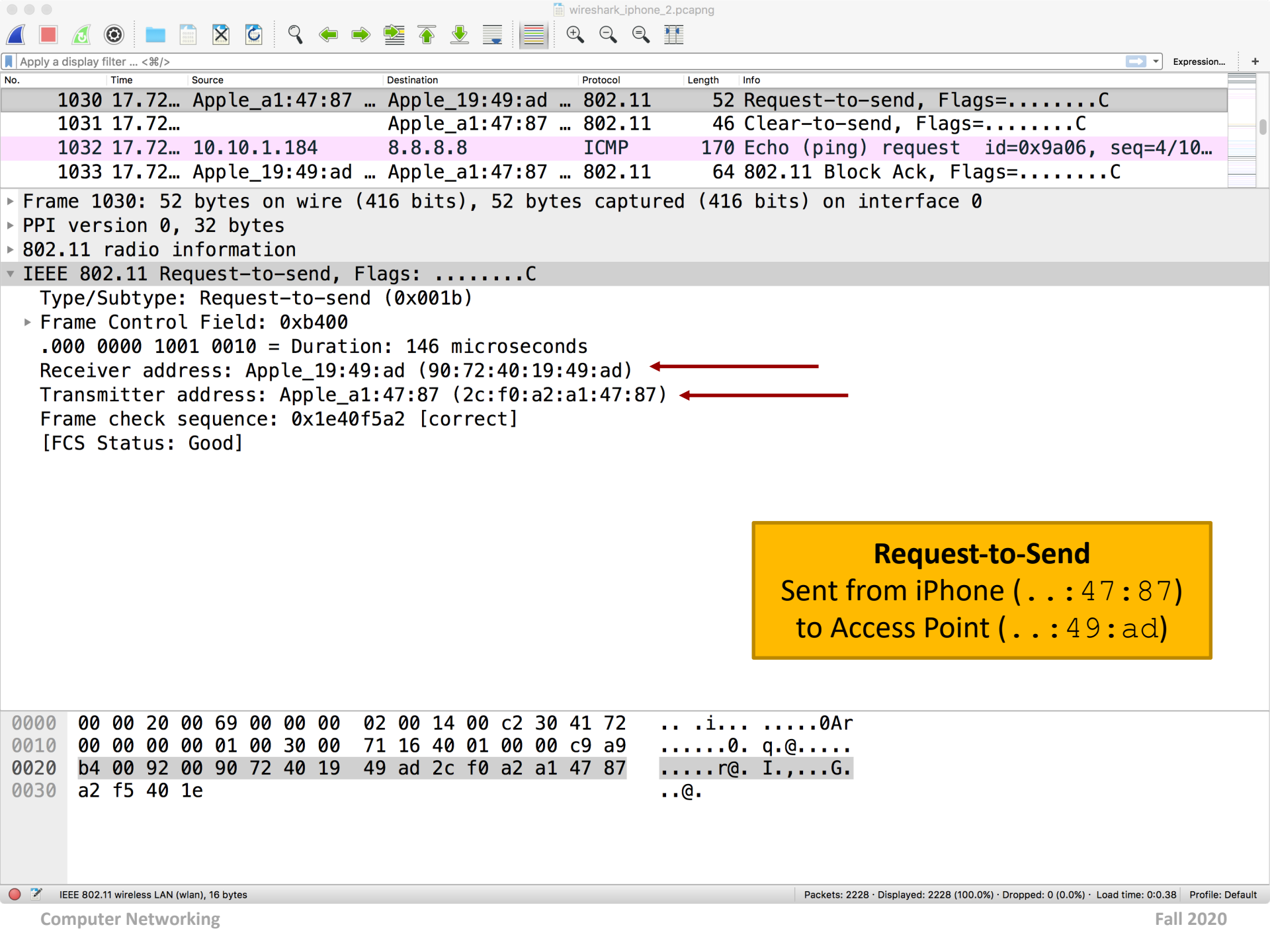
CSMA/CA, RTS/CTS

- CSMA/CA
  - Carrier Sense Multiple Access / Collision Avoidance
  - Listen for other parties transmitting
  - Channel clear? Go ahead and transmit
  - Does not solve hidden node problem
- RTS/CTS
  - Request to Send / Clear to Send

RTS/CTS



- **NAV** = Network Allocation Vector (countdown timer of imposed silence based on RTS/CTS messages that a station has overheard)
- **SIFS** = Short Inter-Frame Space (gap to detect end of frame before transmitting)
- **DIFS** = DCF Inter-Frame Space (CSMA/CA – exponential backoff from collision)



Request-to-Send
Sent from iPhone (. . :47:87)
to Access Point (. . :49:ad)

wireshark_iphone_2.pcapng

Apply a display filter ... <⌘/> Expression...

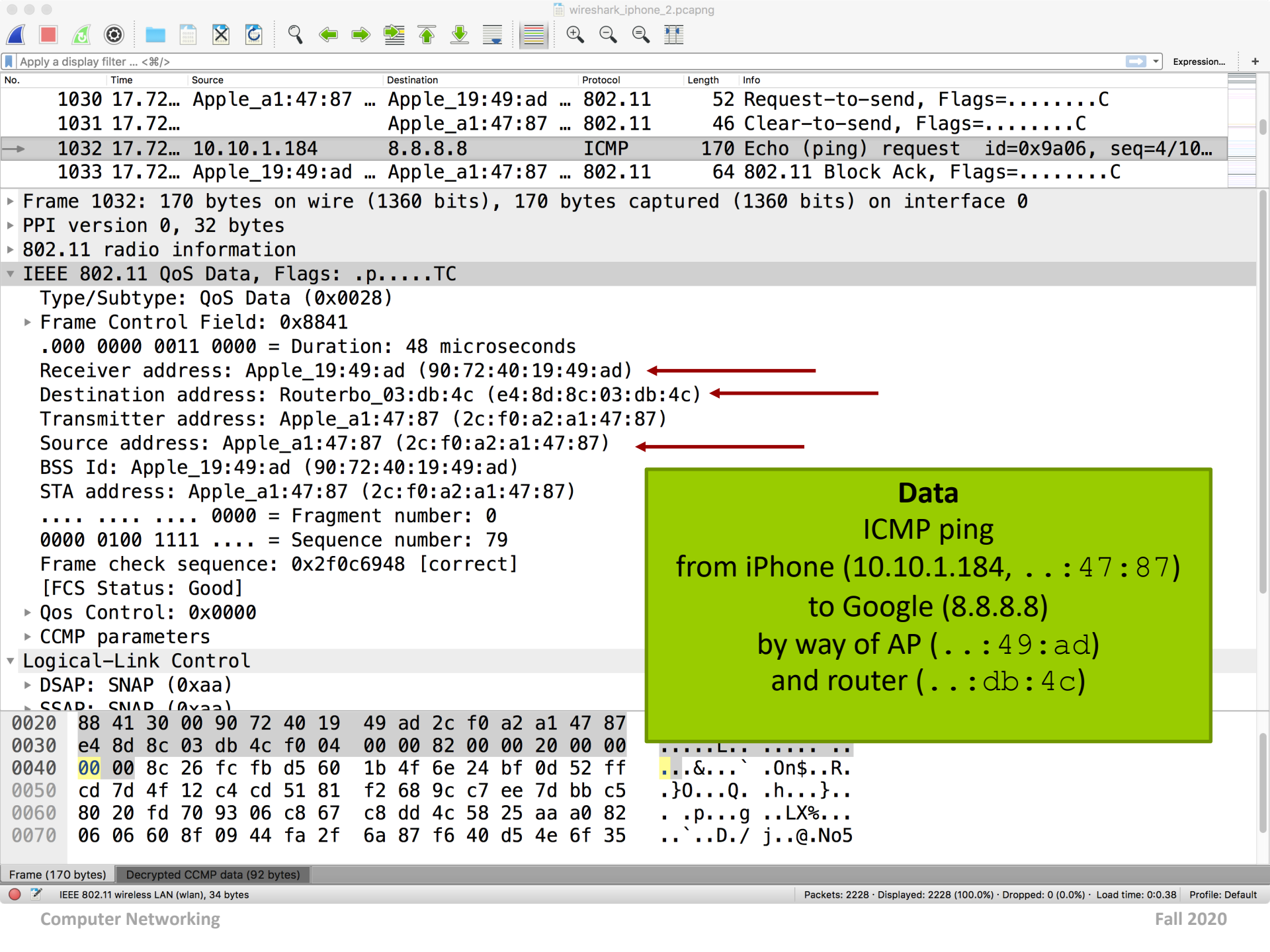
No.	Time	Source	Destination	Protocol	Length	Info
1030	17.72…	Apple_a1:47:87 …	Apple_19:49:ad …	802.11	52	Request-to-send, Flags=........C
1031	17.72…		Apple_a1:47:87 …	802.11	46	Clear-to-send, Flags=........C
1032	17.72…	10.10.1.184	8.8.8.8	ICMP	170	Echo (ping) request id=0x9a06, seq=4/10…
1033	17.72…	Apple_19:49:ad …	Apple_a1:47:87 …	802.11	64	802.11 Block Ack, Flags=........C

```
▸ Frame 1031: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
▸ PPI version 0, 32 bytes
▸ 802.11 radio information
▾ IEEE 802.11 Clear-to-send, Flags: ........C
    Type/Subtype: Clear-to-send (0x001c)
  ▸ Frame Control Field: 0xc400
    .000 0000 0101 1100 = Duration: 92 microseconds
    Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
    Frame check sequence: 0x5b319cac [correct]
    [FCS Status: Good]
```


Clear-to-Send
Sent from Access Point
to iPhone (. . :47:87)

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 ef 30 41 72   .. .i... .....0Ar
0010  00 00 00 00 01 00 30 00  71 16 40 01 00 00 d2 a9   ......0. q.@.....
0020  c4 00 5c 00 2c f0 a2 a1  47 87 ac 9c 31 5b         ..\.,... G...1[
```

IEEE 802.11 wireless LAN (wlan), 10 bytes Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38 Profile: Default


wireshark_iphone_2.pcapng
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1030 17.72… Apple_a1:47:87 … Apple_19:49:ad … 802.11 52 Request-to-send, Flags=.....C
1031 17.72… Apple_a1:47:87 … 802.11 46 Clear-to-send, Flags=.....C
1032 17.72… 10.10.1.184 8.8.8.8 ICMP 170 Echo (ping) request id=0x9a06, seq=4/10…
1033 17.72… Apple_19:49:ad … Apple_a1:47:87 … 802.11 64 802.11 Block Ack, Flags=.....C
Frame 1032: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Apple_19:49:ad (90:72:40:19:49:ad)
Destination address: Routerbo_03:db:4c (e4:8d:8c:03:db:4c)
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)
STA address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
.... 0000 = Fragment number: 0
0000 0100 1111 .... = Sequence number: 79
Frame check sequence: 0x2f0c6948 [correct]
[FCS Status: Good]
Qos Control: 0x0000
CCMP parameters
Logical-Link Control
DSAP: SNAP (0xaa)
0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87
0030 e4 8d 8c 03 db 4c f0 04 00 00 82 00 00 20 00 00
0040 00 00 8c 26 fc fb d5 60 1b 4f 6e 24 bf 0d 52 ff
0050 cd 7d 4f 12 c4 cd 51 81 f2 68 9c c7 ee 7d bb c5
0060 80 20 fd 70 93 06 c8 67 c8 dd 4c 58 25 aa a0 82
0070 06 06 60 8f 09 44 fa 2f 6a 87 f6 40 d5 4e 6f 35
Data
ICMP ping
from iPhone (10.10.1.184, . . :47:87)
to Google (8.8.8.8)
by way of AP (. . :49:ad)
and router (. . :db:4c)
Frame (170 bytes)
Decrypted CCMP data (92 bytes)
IEEE 802.11 wireless LAN (wlan), 34 bytes
Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38
Profile: Default

wireshark_iphone_2.pcapng

Apply a display filter ... <⌘/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1030	17.72…	Apple_a1:47:87 …	Apple_19:49:ad …	802.11	52	Request-to-send, Flags=........C
1031	17.72…		Apple_a1:47:87 …	802.11	46	Clear-to-send, Flags=........C
1032	17.72…	10.10.1.184	8.8.8.8	ICMP	170	Echo (ping) request id=0x9a06, seq=4/10…
1033	17.72…	Apple_19:49:ad …	Apple_a1:47:87 …	802.11	64	802.11 Block Ack, Flags=........C

```
▸ Frame 1033: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▸ PPI version 0, 32 bytes
▸ 802.11 radio information
▾ IEEE 802.11 802.11 Block Ack, Flags: ........C
    Type/Subtype: 802.11 Block Ack (0x0019)
  ▸ Frame Control Field: 0x9400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)
    Transmitter address: Apple_19:49:ad (90:72:40:19:49:ad)
    .... .10. = Block Ack Type: Compressed Block (0x2)
  ▸ Block Ack Request Control: 0x0005
  ▸ Block Ack Starting Sequence Control (SSC): 0x04f0
  ▸ Block Ack Bitmap: 0100000000000000
    Frame check sequence: 0x565263e4 [correct]
    [FCS Status: Good]
```

Acknowledgement
Sent from Access Point (. . :49:ad)
to iPhone (. . :47:87)

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 58 31 41 72   .. .i... ....X1Ar
0010  00 00 00 00 01 00 30 00  71 16 40 01 00 00 d2 a9   ......0. q.@.....
0020  94 00 00 00 2c f0 a2 a1  47 87 90 72 40 19 49 ad   ....,... G..r@.I.
0030  05 00 f0 04 01 00 00 00  00 00 00 00 e4 63 52 56   ........ .....cRV
```

IEEE 802.11 wireless LAN (wlan), 16 bytes Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38 Profile: Default

WiFi

- *WiFi* is a trademark, referring to a specific technology of transmitting data using radio waves
- WiFi trademark is owned by *WiFi Alliance*, an organization that develops and manages WiFi products
- WiFi stands for “wireless fidelity”
- WiFi Alliance tests and certifies products for
  - Interoperability
  - Security protocols
  - QoS, ...

Closing Thoughts

Recap

- Today we discussed
  - Radio transmission and WiFi
  - Structure of a WLAN
  - Access points
  - Challenges in WiFi, including collision
  - Three types of WiFi packets
  - IEEE WiFi standards
  - WiFi packet format

Next Class

- Start discussing the network layer and IPv4

Class Activity

CA.3 – WiFi & Wireshark

Due tonight at 11:59pm

Homework

Due Sept 16th at 11:59pm