

Computer Networking

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



Recap

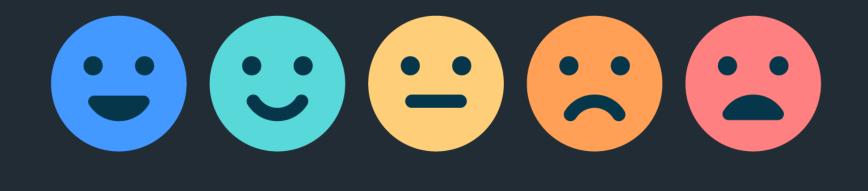
Past Topics

- An overview of computer networking
- Wireshark

Today's Topics

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

Week 3 Feedback: Class Thus Far?





Classic Network Model (Not ISO model, but as actually implemented) HTTP, **Application Layer** Layer 5 ТСР, Layer 4 Transport Layer Layer 3 **Network Layer** IP (IP addresses, routers,) Layer 2 Ethernet (MAC addresses, switches, ...) Data Link Layer Bits on a wire... **Physical Layer** Layer 1

				Τ	Thunderbolt Ethernet Slot 1:	en5					
	a 💿 🖿	🛅 🖹 🎑 🔍 🔶	♦ 🖀 🖣 🛓 📃 📗	€ Q	€, ፻፻						
icmp	· ·									Express	sion +
No.	Time	Source	Destination 8.8.8.8	Protocol ICMP	Length Info	(ning)	request	id=0x3257,	cod-0/0	++1-64 (ranl
→ ↓	63 4 . 91		10.10.1.161	ICMP	98 Echo		•	id=0x3257,			•
-		0.0.0.0 10.10.1.161	8.8.8.8	ICMP			request				
	66 5.91		8.8.8.8 10.10.1.161	ICMP	98 Echo 98 Echo			•	•	-	
		8.8.8.8 10.10.1.161	8.8.8.8	ICMP				id=0x3257,	•	-	
	95 6.91 96 6.94		8.8.8.8 10.10.1.161	ICMP			request		•		
		8.8.8.8 10.10.1.161	8.8.8.8		98 Echo			id=0x3257,			
	103 7.92		8.8.8.8 10.10.1.161	ICMP ICMP			request		•	-	
	104 / . 55	0.0.0.0	10.10.1.101	TCHE	98 Echo	(prig)	repty	id=0x3257,	Seq-3/700), [[[–]]	(16
						· · · · · ·					
		-	(784 bits), 98	-	•						
	-		_01:72:eb (64:4		-	:: Route	erbo_03:0	db:4c (e4:8d	:8c:03:db:	4c)	
			db:4c (e4:8d:8d		:4c)						
		-	o (64:4b:f0:01:7	72:eb)							
	pe: IPv4 (
			4, Src: 10.10.1	161, D	st: 8.8.8.8						
► Inte	ernet Cont	rol Message Pi	rotocol								
0000	04 9d 8c	c 03 db 4c 64 4	4b f0 01 72 eb	00 00	15 00	.LdK	~ E				
0000		2 a4 00 00 40 0				@K					
0010		3 00 2b 53 32 5				+S2W					
0020		3 09 0a 0b 0c 0			a a a = 1	+52₩					
0050	+C 1+ 00			. 12 13	14 15 1111						

🔵 🍸 Frame (frame), 98 bytes

Packets: 105 · Displayed: 8 (7.6%) · Dropped: 0 (0.0%)

Profile: Default

Wireshark capture of wired Ethernet

• • •					🚄 Wi-Fi: en0						
	<u>a</u> 💿 🖿 [🖺 🖹 🎑 🤇 🔶 🏓	, 🔨 🚡 🛓 🗐								'
📕 icmp										Exp	.pression +
No.	Time	Source	Destination	Protocol	Length Info						
>	39 1.16	10.10.1.166	8.8.8.8	ICMP	98 Echo	(ping)	request	id=0x5357,	seq=0/0,	ttl=64	(repl
←	40 1.19	8.8.8.8	10.10.1.166	ICMP	98 Echo	(ping)	reply	id=0x5357,	seq=0/0,	ttl=55	(requ
	41 2.16	10.10.1.166	8.8.8.8	ICMP	98 Echo	(ping)	request	id=0x5357,	seq=1/25/	ô, ttl=f	54 (re
	42 2.20	8.8.8.8	10.10.1.166	ICMP	98 Echo	(ping)	reply	id=0x5357,	seq=1/25/	6, ttl=5	55 (re
	43 3.16	10.10.1.166	8.8.8.8	ICMP	98 Echo	(ping)	request	id=0x5357,	•	-	
	44 3.19	8.8.8.8	10.10.1.166	ICMP	98 Echo	(ping)	•	id=0x5357,	•	-	
											,
											1
▶ Fram	ne 39 98	bytes on wire (784 hits) 98	hytes ca	ntured (78	4 hits) on inte	rface Ø			
		$\frac{1}{2} \sum_{i=1}^{n} \frac{1}{2} \sum_{i=1}^{n} \frac{1}$	•		•				. 0 0 dh	. ()	

> Frame 39: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: 78:4f:43:9c:73:90 (78:4f:43:9c:73:90), Dst: Routerbo_03:db:4c (e4:8d:8c:03:db:4c)
> Destination: Routerbo_03:db:4c (e4:8d:8c:03:db:4c)
> Source: 78:4f:43:9c:73:90 (78:4f:43:9c:73:90)
Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.10.1.166, Dst: 8.8.8.8
> Internet Control Message Protocol
0000 e4 8d 8c 03 db 4c 78 4f 43 9c 73 90 08 00 45 00Lx0 C.s...E.
0010 00 54 61 51 00 00 40 01 fd 98 0a 0a 01 a6 08 08 .TaQ..@.
0020 08 08 08 00 18 5b 53 57 00 00 5a 09 09 b4 00 0e[SW ..Z....
0030 a7f 08 09 0a 0b 0c 0d 0e of 10 11 12 13 14 15 =......

wireshark_pcapng_en0_20171112185547_LXz1mU

Packets: 44 · Displayed: 6 (13.6%)

Wireshark capture of 802.11ac Wi-Fi

Looks like wired Ethernet, so lecture over, right?

Profile: Default

802.11

802.11 looks like Ethernet

... but only at the *network layer* and above

	🛅 wireshark_iphone_2.pcapng
A = 1 A = 1	ا الله الله الله الله الله الله الله
wlan.addr==90:72:40:19:49:ad && icmp	

Expression... +

🔲 wla	an.addr==90:72:40:19:49:	ad && icmp							Exp	pression +
No.	Time	Source	Destination	Protocol	Length Info					
		10.10.1.184		ICMP					seq=4/1024,	
	1037 17.75	8.8.8.8	10.10.1.184	ICMP	170 Echo	(ping)	reply	id=0x9a06,	seq=4/1024,	t
►F	rame 1032: 1	.70 bytes on w	wire (1360 bits),	170 bytes o	captured (13	60 bits	s) on int	erface 0		
►P	PI version 0	, 32 bytes								
▶ 8	02.11 radio	information								
۳I	EEE 802.11 Q	oS Data, Flac	gs: .pTC							
	Type/Subtype	e: QoS Data (0x0028)							
►	Frame Contro	ol Field: 0x8	841							
	.000 0000 00	$011 \ 0000 = Du$	ration: 48 microse	econds						
	Receiver add	dress: Apple_	19:49:ad (90:72:40	ð:19:49:ad)						
	Destination	address: Rou	iterbo_03:db:4c (e4	4:8d:8c:03:	db:4c)					
	Transmitter	address: App	le_a1:47:87 (2c:f	ð:a2:a1:47:	87)					
	Source addre	ess: Apple_a1	.:47:87 (2c:f0:a2:a	a1:47:87)						
			90:72:40:19:49:ad							
		•• —	':87 (2c:f0:a2:a1:4	47 : 87)						
			agment number: 0							
			quence number: 79							
	Frame check	sequence: 0x	2f0c6948 [correct]]						
	[FCS Status									
►	Qos Control	: 0×0000								
	CCMP parame									
	ogical-Link									
	DSAP: SNAP									
	SSAP: SNAP									
►		ld: U, func=U								
	•	•	sulated Ethernet	(0×000000)						
	Type: IPv4									
			4, Src: 10.10.1.1	.84, Dst: 8,	.8.8.8					
►I	nternet Cont	rol Message F	rotocol							
00	30 e4 8d 8c	03 db 4c f0	01 00 00 87 00 0	0 20 00 00	I					
00	40 00 00 8c	26 fc fb d5	NA /*					0 1 1		
Fram	ne (170 bytes) Decrypt	ed CCMP data (92 bytes)	Wires	hark (captur	re o	ot 80	2.11a	C VVI-H	·
	Text item (text), 8 bytes					00				•
				14/11						
	Computer Netw	orking		With	station	in <i>m</i>	onitoi	r mode		

Network Model

	Application Layer	НТТР,
Layer 4	Transport Layer	тср,
Layer 3	Network Layer	IP (IP addresses, routers,)
Layer 2	Link Layer	802.2 Logical Link Control (LLC) 802.11 MAC header (identical a,b,g,n,)
Layer 1	Physical Layer	802.11 PLCP header (varies a,b,g,n,) Physical media (DSSS, OFDM,)

IEEE 802.11 Physical Layer

Gith

00

Physical Layer (PHY)

- Purpose: Transmit raw bits over a physical link
 - **7** Copper wire, optical cable, **wireless**
- Challenges
 - Convert input bitstream into symbols/code words?
 - **Frequencies to transmit on?**
 - Modulation scheme?
- **7** 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

13

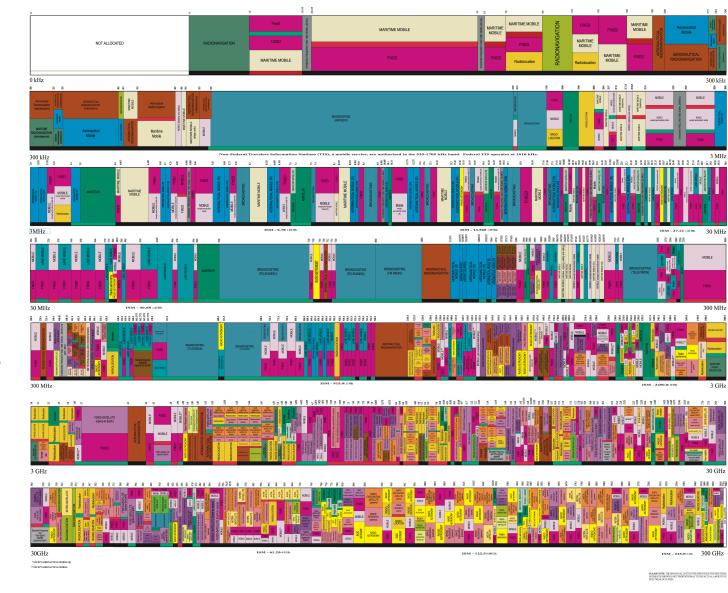
Physical Layer Challenges

- Range of network limited by transmission powerLimits end-to-end propagation delay
- Radio Frequency (RF) spectrum usage limited by law and treaty
 - **8**02.11 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]

For sole by the Superintendent of Devanteens, U.S. Government Printing Office serves bankness gauger Please and Inte (500) 1121 (200) Weshington, ICC area (200) 112-1000 Examines (2007) 113-113 (2007) 2008 (2007) Weshington, ICC area (2007) Examines (2007) 113-113 (2007) 2008 (2007) Weshington, ICC area (2007)

It sure *looks* fast....



802.11 Physical Layer Standards

802.11			Stream data rate	Stream data rate Allowable MIMO		Approximate range		
Protocol	date	date (GHz) (MHz) (Mbit/s)		streams	Modulation	Indoor	Outdoor	
	Sep	5	20	6, 9, 12, 18, 24,	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
а	1999	3.7	20	36, 48, 54	N/A	OFDIVI		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	2.4/5	20	Up to 288.8	4	MIMO-	70 m	250 m
n	2009	2.4/3	40	Up to 600	4	OFDM	(230 ft)	(820 ft)
			20	Up to 346.8				
20	Dec	5	40	Up to 800	8	MIMO-	35 m	
ac	2013	J	80	Up to 1733.2	0	OFDM	(115 ft)	
			160	Up to 3466.8				
Computer Net	working		https://en		/IEEE_802.1	1		Fall 2020

Frequency

2.4 GHz

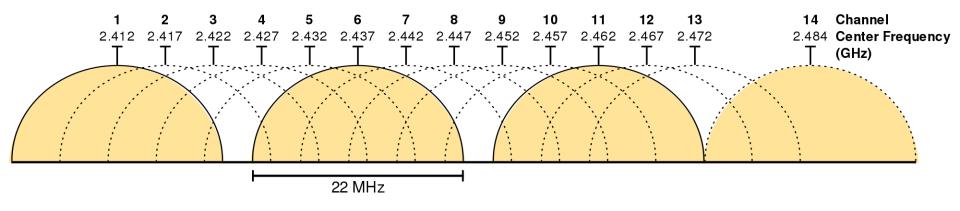
- Longer range
- Lower data rate
- Increased penetration of walls and floors
- Particularly crowded
 - Used by many other devices besides WiFi (cordless phones, Bluetooth, wireless microphones, ...)
 - Subject to interferences (microwave ovens)

5 GHz

- 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)

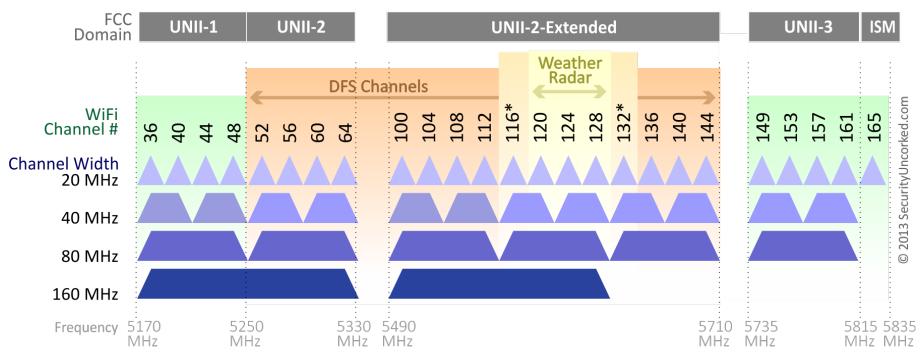
Computer Networking

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

19

802.11 5GHz Channels

802.11ac Channel Allocation (N America)



*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/ Fall 2020

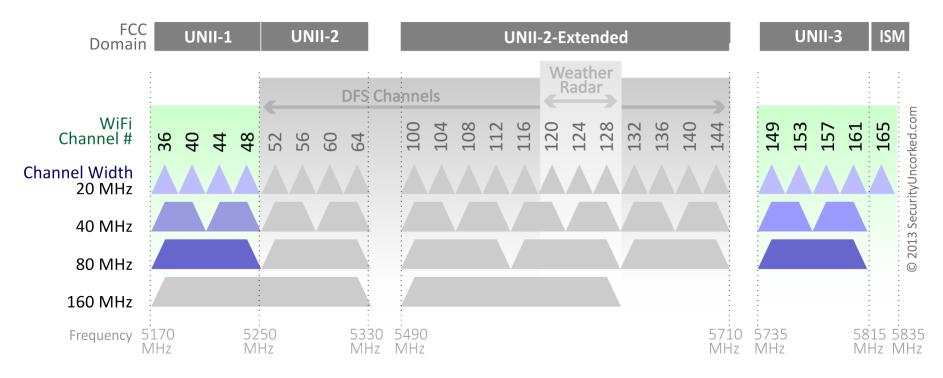
20

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 <u>and avoid</u> 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
 - **オ** Satellite radar

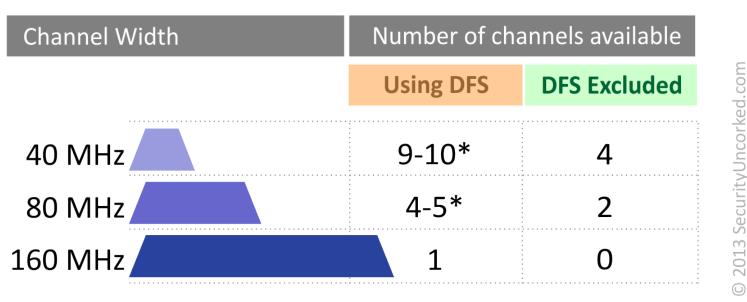
802.11 5GHz Channels

802.11ac Channel Allocation excluding DFS (N America)



802.11 5GHz Channels

802.11ac Channel Availability (N America)



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

Fall 2020

802.11 Physical Layer Standards

802.11	Release	Frequency	Bandwidth	Stream data rate	Allowable MIMO	Modulation	Approximate range		
Protocol	date (GHz) (MHz) (Mbit/s)		streams		Indoor	Outdoor			
	Sep	5	20	6, 9, 12, 18, 24,	N/A	OFDM	35 m (115 ft)	120 m (390 ft)	
а	1999	3.7	20	36, 48, 54	N/A	OFDIM		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	2.4/5	20	Up to 288.8	4	MIMO-	70 m	250 m	
n	2009	2.4/3	40	Up to 600	4	OFDM	(230 ft)	(820 ft)	
			20	Up to 346.8					
20	Dec	5	40	Up to 800	8	MIMO-	35 m		
ac	2013	J	80	Up to 1733.2	0	OFDM	(115 ft)		
			160	Up to 3466.8					
Computer Net	working		https://en	wikipedia.org/wiki	/IEEE_802.1	1		Fall 2020	

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)

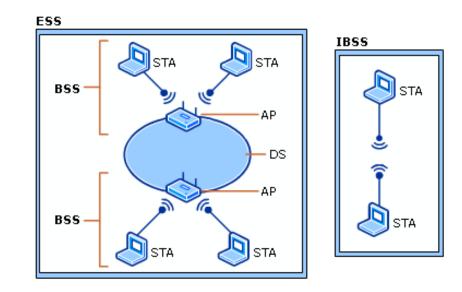
 - Higher risk of interference from APs on neighboring channels
- Higher bandwidth channels (80MHz, 160MHz) difficult to use in enterprise settings due to interference



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)

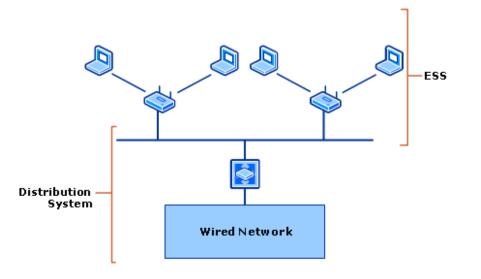


- Independent Basic Service Set (IBSS)
 - Ad-hoc network (no AP)

Link Layer Terminology

Infrastructure Mode

One client (station) + One AP



Ad-Hoc Mode

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



2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	6 bytes	6 bytes	0-2312 bytes	4 bytes
Frame Control	Duration	Addr 1	Addr 2	Addr 3	Sequence Ctrl	Addr 4	Frame Body	FCS

- → Frame Control (Bitfield)
 - Protocol Version
 - **7** 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)

7

•••

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	6 bytes	6 bytes	0-2312 bytes	4 bytes
Frame Control	Duration	Addr 1	Addr 2	Addr 3	Sequence Ctrl	Addr 4	Frame Body	FCS

Duration

- Duration needed to receive <u>next</u> frame transmission in *microseconds*
- i.e. Everyone else should stay quiet for this time!

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	6 bytes	6 bytes	0-2312 bytes	4 bytes
Frame Control	Duration	Addr 1	Addr 2	Addr 3	Sequence Ctrl	Addr 4	Frame Body	FCS

- 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

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	6 bytes	6 bytes	0-2312 bytes	4 bytes
Frame Control	Duration	Addr 1	Addr 2	Addr 3	Sequence Ctrl	Addr 4	Frame Body	FCS

Frame Body = Payload

FCS = Frame Check Sequence

Cyclic Redundancy Check (CRC) over all fields in MAC header and frame body

Example

Apple al 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







Apple iPhone



monitor mode

	ie_2.pcapng
🚄 📕 🙋 💿 🖿 🗎 🕱 🙆 🔍 🗢 🌩 警 春 👱 🜉 🗐 🔍 Q. Q	11111111111111111111111111111111111111
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	
1031 17.72 Apple_a1:47:87 802.11	
→ 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	-
Frame 1032: 170 bytes on wire (1360 bits), 170 bytes ca	ptured (1360 bits) on interface 0
PPI version 0, 32 bytes	
802.11 radio information	
IEEE 802.11 QoS Data, Flags: .pTC	Ping from iPhone to Google
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)	(1) Receiver Addr (RA): Access Point
Destination address: Routerbo_03:db:4c (e4:8d:8c:03:db	a:4c) ← (3) Destination Addr (DA): Router
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:87	
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	(Wireshark labels same field with two names)
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) 	
► DSAP: SNAP (UXdd) $ SSAP \cdot SNAP (0xaa) $	
0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87	.A0r@. 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	.}0Qh}
0060 80 20 fd 70 93 06 c8 67 c8 dd 4c 58 25 aa a0 82	pgLX%
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)

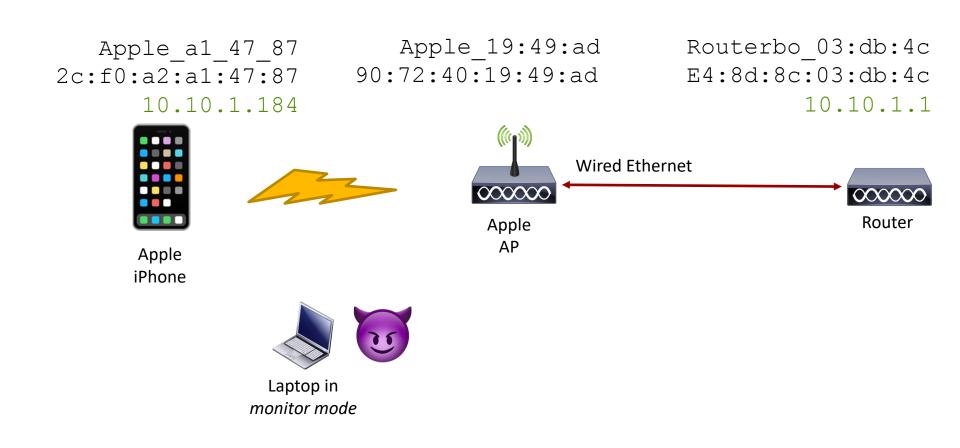
IEEE 802.11 wireless LAN (wlan), 34 bytes

Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38 Profile: Default

Computer Networking

	wireshark_iphone_2.pcapng												
📶 📕 🔬 💿 🖿 🛅 🕱 🄄 🔍 🖛 🔿 警 🚡 🛃 🧮 🗨 Q, Q, Q, III													
-	splay filter <೫/>										Expression	. +	
No.	Time ۲۵ 17 72	Source	<u>-1·17·87</u>	Destination Apple_19:		rotocol	Length Info	equest-to-ser	nd Flac	nc- (-		
	030 17.72 031 17.72		d1.4/.0/	Apple_19:				ear-to-send,			-		
	032 17.72		1.184	8.8.8.8				cho (ping) re			seg=4/10		
				Apple_a1:				02.11 Block A	•	-	•		
 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													
<pre>Type/Subtype: 802.11 Block Ack (0x0019) Frame Control Field: 0x9400 .000 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: 01000000000000</pre>													
Fra		sequence		263e4 [corre	ct]		Sent	from Acce	ess Poir ne (:47:87)):ad)		
	00 00 00 94 00 00	00 01 00	0 30 00 0 a2 a1	02001400711640014787907200000000	00 00 d2 40 19 49	a9 ad	i 0. (q.@ Gr@.I.					

(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

		vireshark_iphone_2.						
🔟 🔲 🖉 🐑 🚞 🛋 🛞	🔨 🚡 👱 📃 🖯							
📕 Apply a display filter <೫/>							Expression	+
	Destination	Protocol	Length Info					
	Broadcast	802.11			SN=2833, FN			
1018 17.65… 2wire_a7:90:5a		802.11			SN=247, FN=	· ·		
1019 17.69… Humax_81:06:9d		802.11	122 Dat	a, SN=444,	FN=0, Flags	=.pF.C	2	
1020 17.71… 92:ad:49:19:40:…	Broadcast	802.11	360 Bea	con frame,	SN=2834, FN	=0, Flags=	•••••	
 Frame 1017: 372 bytes on wire (2 PPI version 0, 32 bytes 802.11 radio information IEEE 802.11 Beacon frame, Flags: Type/Subtype: Beacon frame (0x6 Frame Control Field: 0x8000 .000 0000 0000 0000 = Duration: Receiver address: Broadcast (fr Destination address: Broadcast (fr Destination address: Apple_19:4 Source address: Apple_19:49:ad BSS Id: Apple_19:49:ad (90:72:4 0000 = Fragment 1011 0001 0001 = Sequence 	<pre>cC 0008) : 0 microseconds f:ff:ff:ff:ff:ff:ff) (ff:ff:ff:ff:ff:ff: 49:ad (90:72:40:1 (90:72:40:19:49: 40:19:49:ad) number: 0 number: 2833</pre>	ff) .9:49:ad)	ured (297	6 bits) on	interface 0			
Frame check sequence: 0x1cb8a04 [FCS Status: Good]	43 [correct]				Beacon			
IEEE 802.11 wireless LAN			Sent f	rom Acce	ess Point (.	· 49·a		
					ne (: FI			

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

		🔚 wireshark_iphone_2.pcapng
	← → 🖄 🛉 🛓	

		• • •		• • •								
Apply a display											Expression	+
No.	Time Source	40. ad	Destination	Protocol	Length	Info	fromo	CN-2022				
	17.61 Apple_19:		Broadcast	802.11			-	-	-	Flags=		
	17.65. 2wire_a7:		Broadcast	802.11			-	-	-	Flags=		
	17.69 Humax_81:		Spanning-tree-(-	-	FN=0, Fl				
) 17.71 92:ad:49:		Broadcast	802.11	300	веасоп	rrame,	SN=2834,	FIN=0,	Flags=		_
	2.11 wireless LAN											
	parameters (12 by											
	stamp: 0x000014ff											
	con Interval: 0.10	_										
	bilities Informat		1111									
	d parameters (300	-										
	SSID parameter s				-	_	_					
	Supported Rates	-				[Mbit/s	sec]					
-	Traffic Indicati	-			•							
	Country Informat		untry Code US, Env	vironme	nt Any							- 1
	Power Constraint											- 1
► Tag:	TPC Report Trans	mit Pow	er: 25, Link Marg	in: 0								- 1
	RSN Information											. 1
-	HT Capabilities						_	,				
► Tag:	HT Information (802 . 11n	D1.10)				Beaco	on (cont	tinued)		
	Extended Capabil					۸dvc	rticina	SSID ("	Nilla 9	5GH7")		
	VHT Capabilities)		Auve	i tising	, 5510 (ivina .			
	VHT Operation (I					Adver	tising ı	many di	fferer	nt TX/RX		
► Tag:	VHT Tx Power Env	elope (IEEE Std 802.11ac,	/D5.0)				· ·	_			
► Tag:	Vendor Specific:	Apple				capa	abilitie	s at var	y data	rates		
► Tag:	Vendor Specific:	Apple										- 1
	Vender Specific		~ 07 07 06 ff 1/ (00 00	ro T							
	72 40 19 49 ad 10 00 11 11 00 0a 40		c 02 92 86 ff 14 0 c 6c 61 20 35 47 4			. < Ii lla 5						
	08 8c 12 98 24 b		0 6c 05 04 00 03 0			H `l						
	46 55 53 20 24 0		3 01 11 2c 01 11 3			. (,						
	34 01 18 38 01 18		1 18 40 01 18 64 0			<@						
	01 18 6c 01 18 7					t						
	18 8c 01 18 90 0		5 01 1e 99 01 1e 9									

🔴 🎽 IEEE 802.11 wireless LAN (wlan), 312 bytes

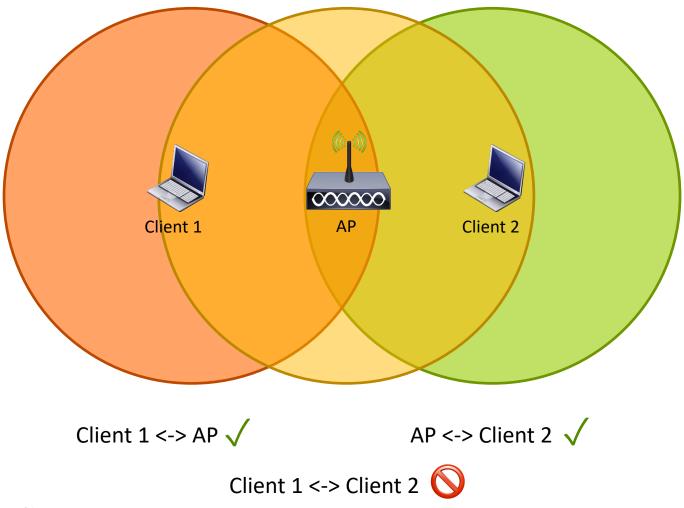
Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.79 Profile: Default

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



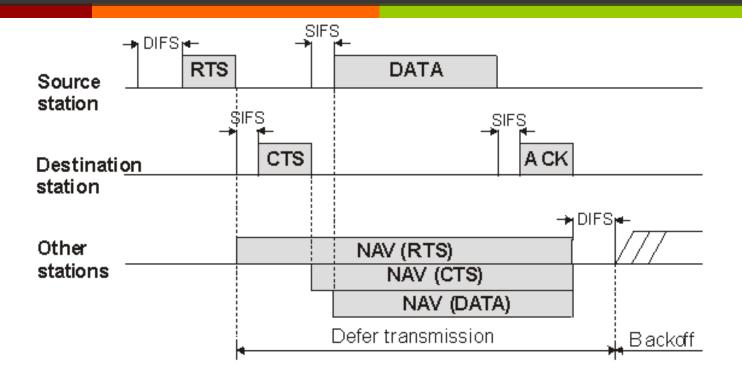
CSMA/CA, RTS/CTS

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

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)

		ſ	wireshark_iphone_2.	ie_2.pcapng	
	🖹 🖹 🍯 🤇 🔶 🏓) 😫 🗃 🛓 📃 📃		11	
Rpply a display filter <೫/>					Expression +
No. Time	Source	Destination	Protocol	Length Info	
1	. Apple_a1:47:87				
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	
 PPI version 0, 802.11 radio i IEEE 802.11 Re Type/Subtypes Frame Contro .000 0000 100 Receiver add Transmitter a 	, 32 bytes information equest-to-send, Fl : Request-to-send l Field: 0xb400 01 0010 = Duration ress: Apple_19:49 address: Apple_a1 sequence: 0x1e40f	lags:C d (0x001b) on: 146 microsecor 0:ad (90:72:40:19 L:47:87 (2c:f0:a2	onds 0:49:ad) ←		

Request-to-Send

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

0000	00	00	20	00	69	00	00	00	02	00	14	00	c2	30	41	72	i0Ar
0010	00	00	00	00	01	00	30	00	71	16	40	01	00	00	с9	a9	0. q.@
0020	b4	00	92	00	90	72	40	19	49	ad	2c	f0	a2	a1	47	87	r@. I.,G.
0030	a2	f5	40	1e													@.

	iii wireshark_iphone_2.pcapng	
🥖 📕 🙇 🔘 🖿	📄 🖹 🙆 🔍 🗢 🏓 鑒 🚡 👤 📃 🔍 Q, Q, 🏛	
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	
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	
 PPI version 0, 802.11 radio i IEEE 802.11 Cl Type/Subtype: Frame Control .000 0000 010 Receiver addi 	Information Lear-to-send, Flags:C : Clear-to-send (0x001c) l Field: 0xc400 01 1100 = Duration: 92 microseconds ress: Apple_a1:47:87 (2c:f0:a2:a1:47:87) sequence: 0x5b319cac [correct]	

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	i0Ar
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			\., G1[

IEEE 802.11 wireless LAN (wlan), 10 bytes

Computer Networking

	one_2.pcapng
📶 📕 🙍 💿 🖿 🗎 🗴 🙆 🤇 🗢 🗭 警 🖣 👱 🜉 🔍 Q, Q	2 1
Rpply a display filter <ૠ/>>	Expression +
No. Time Source Destination Protocol	Length Info
1030 17.72 Apple_a1:47:87 Apple_19:49:ad 802.13	
1031 17.72 Apple_a1:47:87 802.13	
→ 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_a1:47:87 802.13	
Frame 1032: 170 bytes on wire (1360 bits), 170 bytes ca	aptured (1360 bits) on interface 0
PPI version 0, 32 bytes	
802.11 radio information	
IEEE 802.11 QoS Data, Flags: .pTC	
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)	←
<pre>Destination address: Routerbo_03:db:4c (e4:8d:8c:03:d</pre>	Jb:4c) ←
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:8	37)
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87) 🖪	I
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)	
STA address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	Data
0000 = Fragment number: 0	
0000 0100 1111 = Sequence number: 79	ICMP ping
<pre>Frame check sequence: 0x2f0c6948 [correct]</pre>	from iPhone (10.10.1.184,: 47:87)
[FCS Status: Good]	
▶ Qos Control: 0x0000	to Google (8.8.8.8)
▶ CCMP parameters	h_{1}
	by way of AP(49:ad)
Logical-Link Control	by way of AP (:49:ad)
 Logical-Link Control DSAP: SNAP (0xaa) 	and router (:db:4c)
 Logical-Link Control DSAP: SNAP (0xaa) SSAP: SNAP (0xaa) 	
 Logical-Link Control DSAP: SNAP (0xaa) CSAP: SNAP (0xaa) 0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87 	and router (: db: 4c)
 Logical-Link Control DSAP: SNAP (0xaa) CSAP: SNAP (0yaa) 0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87 	and router (db:4c)
 Logical-Link Control DSAP: SNAP (0xaa) CSAP: 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 	and router (: db: 4c)
 Logical-Link Control DSAP: SNAP (0xaa) CSAP: 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 	and router (db:4c)

Frame (170 bytes) Decrypted CCMP data (92 bytes)

🔴 🍸 🛛 IEEE 802.11 wireless LAN (wlan), 34 bytes

Computer Networking

Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.38 Profile: Default

wireshark_iphone	_2.pcapng
⊿ ■ ⊿ ◎ ■ 🖹 🛛 🤄 ۹ 🗢 🛸 ≌ T 👱 📃 🔍 ۹ ۹	
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 captur	red (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: 010000000000000	
Frame check sequence: 0x565263e4 [correct]	
[FCS Status: Good]	
[FCS Status: GOOU]	Acknowledgement
	C C
	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	X1Ar
	0. q.@
0020 94 00 00 00 2c f0 a2 a1 47 87 90 72 40 19 49 ad	G r@ T

0020	94	00	00	00	2c	f0	a2	a1	47	87	90	72	40	19	49	ad	, Gr@.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

WiFi

48



- 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
 - **7** 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

 - 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