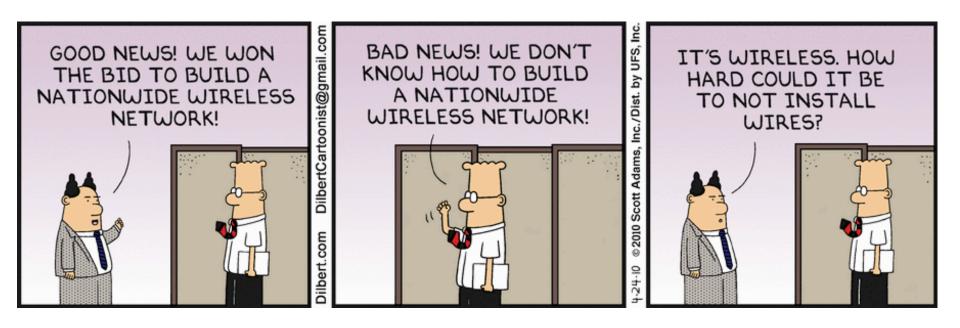


Advanced Computer Networking

CYBR 230 – Jeff Shafer – University of the Pacific





Classic Network Model

(Not ISO model, but as actually implemented)

	Application Layer	HTTP,
Layer 4	Transport Layer	ТСР,
Layer 3	Network Layer	IP (IP addresses, routers,)
Layer 2	Link Layer	Ethernet (MAC addresses, switches,)
Layer 1	Physical Layer	Bits on a wire

3

•											
	🙇 🙆 🖿 🚺	🖹 🖹 🧯 🔍 🔶 🖷) 😫 🖣 👱 📃 📕		3 0						
icmp										Expres	sion +
No.		Source	Destination 8.8.8.8	Protocol Le	09 Fcho	(ning)	raquest	id-0x2257	cog=0/0	++1-64 (ronl
→ ↓	63 4.94		10.10.1.161	ICMP		•	request	id=0x3257,			
-		10.10.1.161	8.8.8.8	ICMP	98 Echo			id=0x3257,			
							request	id=0x3257,	•	-	
	66 5 . 94		10.10.1.161	ICMP	98 Echo			id=0x3257,	•	-	
		10.10.1.161	8.8.8.8	ICMP			request	id=0x3257,	•	-	
	96 6.94		10.10.1.161	ICMP	98 Echo			id=0x3257,	•	-	
		10.10.1.161	8.8.8.8	ICMP			request	id=0x3257,		-	
	104 7.95	8.8.8.8	10.10.1.161	ICMP	98 Echo	(ping)	repty	id=0x3257,	seq=3/766	3, TTT=55	(re
		bytes on wire		•							
	•	<pre>Src: Caldigit_</pre>			•	: Route	erbo_03:c	b:4c (e4:8d)	8c:03:db:	4c)	
► Des	stination:	Routerbo_03:d	b:4c (e4:8d:8c	:03:db:4c)							
⊳ Soı	urce: Calc	ligit_01:72:eb	(64:4b:f0:01:7	2:eb)							
Тур	be: IPv4 ((0×0800)									
▶ Inte	rnet Prot	ocol Version 4	, Src: 10.10.1	.161, Dst:	8.8.8.8						
▶ Inte	rnet Cont	rol Message Pr	otocol								
		-									
2000					~~	1.117	-				
0000		03 db 4c 64 4				.LdK					
0010		a4 00 00 40 0				@k					
0020		00 2b 53 32 5				+S2W					
0030	4C 14 08	09 0a 0b 0c 0	d 0e 0f 10 11	12 13 14 .	15 L						

○ Frame (frame), 98 bytes

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

Profile: Default

Wireshark capture of wired Ethernet

•					🚄 Wi-Fi: en0						
	🗴 💿 🖿 [🗎 🖹 🧯 🔍 🔶 🏓	😤 春 Ł 📃 📕	\oplus Θ							
📕 icmp										Exp	oression +
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=1/256	5, ttl=6	4 (re
	42 2.20	8.8.8.8	10.10.1.166	ICMP	98 Echo	(ping)	reply	id=0x5357,	seq=1/250	5, ttl=5	5 (re
	43 3.16	10.10.1.166	8.8.8.8	ICMP	98 Echo	(ping)	request	id=0x5357,	seq=2/512	2, ttl=6	4 (re
	44 3.19	8.8.8.8	10.10.1.166	ICMP	98 Echo	(ping)	reply	id=0x5357,	seq=2/512	2, ttl=5	5 (re
l											
- Ener		bytes on vire (704 hitc) 00	hutes (contured (70) on into	rface A			

> 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 3d 7f 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%)

Profile: Default

Wireshark capture of *802.11ac* Wi-Fi

Looks like wired Ethernet, so lecture over, right?

802.11

6

802.11 looks like Ethernet

... but only at the network layer and above

							w w	reshark_iphone_2.pd	apng					
		0	01059 01101 01110	🗙 🙆	٩ 🤶	• 🔿 警 有	👱 📃 📃 🗨	⊖ € ፲						7
V	/lan.addr==90:7	2:40:19:	49:ad && id	cmp									Exp	pression
No.		Time	Sou	rce		Destination	Protocol	Length	Info					_
	1032	17.7	/2 10	0.10.1	.184	8.8.8.	8 ICM	P 176) Echo	(ping)	request	id=0x9a06,	seq=4/1024,	t
-	1037	17.7	/5 8.	8.8.8		10.10.	1.184 ICM	P 176) 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]

▶ Oos 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 04 00 00 82 00 00 20 00 00

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*

Advanced Computer Networking

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



IEEE 802.11 Physical Layer

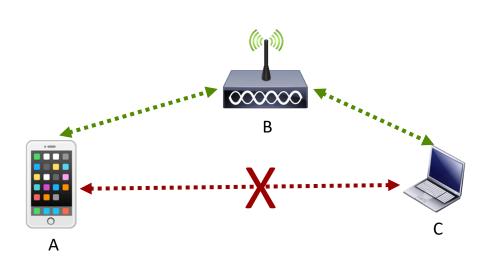
Advanced Computer Networking

Physical Layer (PHY)

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



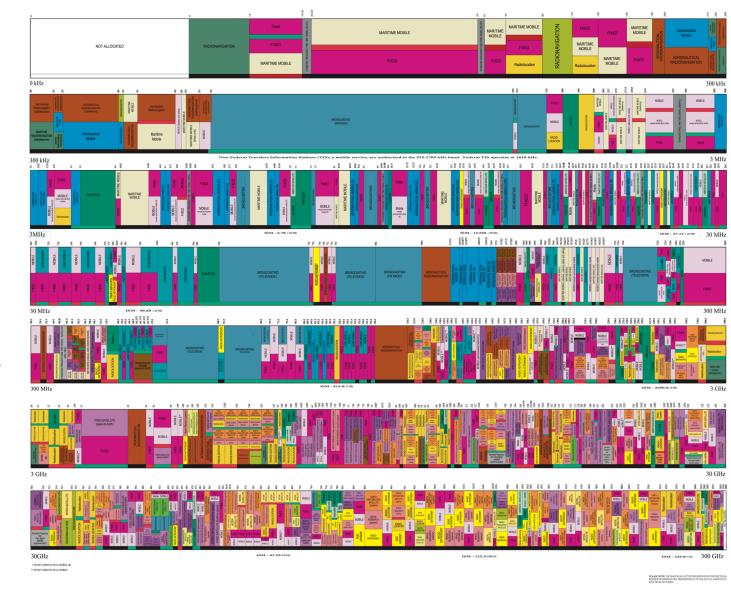
Physical Layer Challenges

- 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 Superintenders of Decements, U.S. Government Printing Different Instants beekness gave Phone tell free (964) 312-1400, Washington, DC area (202) 512-3000 Faculty (202) 113-2103 Math. Stars 10207 Beakington, DC 2000-2001

It sure *looks* fast....



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,	NI / 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	. o	MIMO-	35 m		
ac	2013	J	80	Up to 1733.2	8	OFDM	(115 ft)		
			160	Up to 3466.8					
Advanced Com	puter Netwo	orking	https://en	wikipedia.org/wiki	1		Fall 2018		

Frequency

2.4 GHz

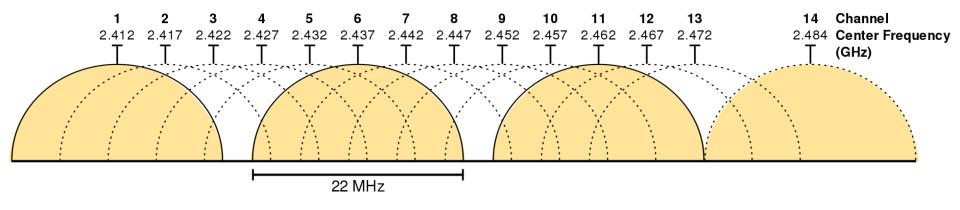
- Longer range
- Lower data rate
- Increased penetration of walls and floors
- Particularly crowded
 - Used by many other devices besides WiFi (cordless phones, Bluetooth, wireless microphones, ...)
 - Subject to interferences (microwave ovens)

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)

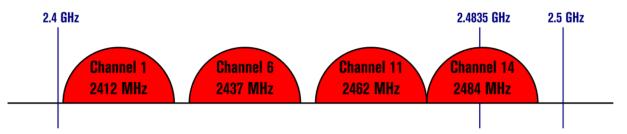
Advanced Computer Networking

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

18

Non-Overlapping Channels for 2.4 GHz WLAN

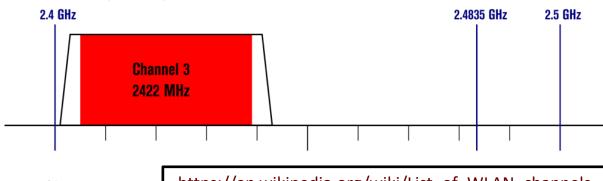
802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width - 16.25 MHz used by sub-carriers



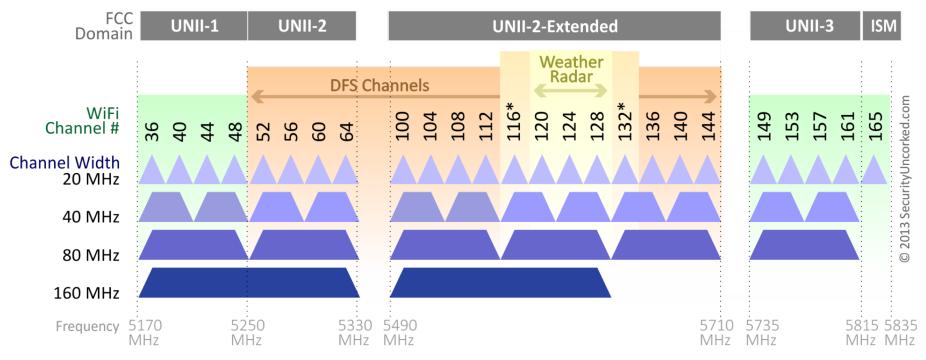
802.11n (OFDM) 40 MHz ch. width - 33.75 MHz used by sub-carriers



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

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.

Advanced Computer Networking

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

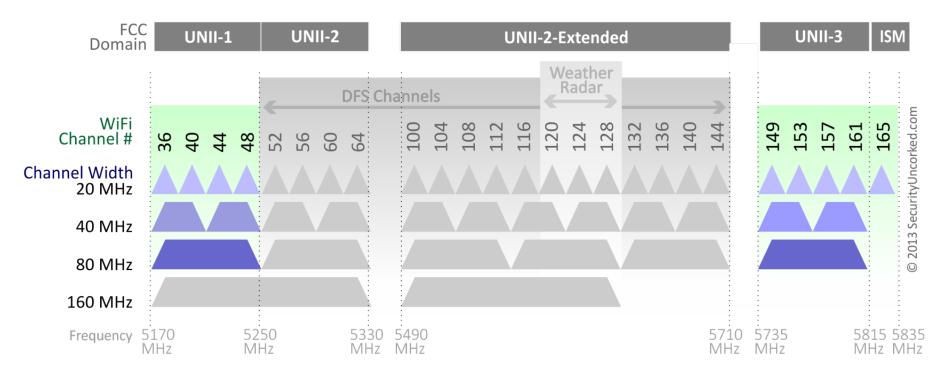
Dynamic Frequency Selection (DFS)

IEEE 802.11(h) standardized DFS

- Access point (and clients) specify a Quiet Period in the Beacon frame to silence clients
- Access point listens in Quiet Period for transmitting radar
- Radar detected?
 - AP will block further transmissions, broadcast a channel switch announcement, disassociate remaining clients, and randomly select a different channel. (If new channel is DFS-required, AP will scan for radar signals for 60 seconds before enabling beacons and accepting client associations)
- Suggestion: Avoid DFS channels (or at least verify radar interference is non-issue in your location)

802.11 5GHz Channels

802.11ac Channel Allocation excluding DFS (N America)



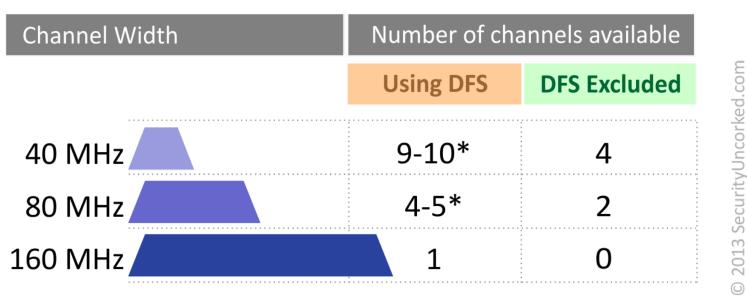
Advanced Computer Networking <u>http://securityuncorked.com/2013/11/the-best-damn-802-11ac-channel-allocation-graphics/</u>

Fall 2018

23

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.

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,	NI / 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	. o	MIMO-	35 m		
ac	2013	J	80	Up to 1733.2	8	OFDM	(115 ft)		
			160	Up to 3466.8					
Advanced Com	puter Netwo	orking	https://en	wikipedia.org/wiki	1		Fall 2018		

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

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,	NI / 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	. o	MIMO-	35 m		
ac	2013	J	80	Up to 1733.2	8	OFDM	(115 ft)		
			160	Up to 3466.8					
Advanced Com	puter Netwo	orking	https://en	wikipedia.org/wiki	1		Fall 2018		

Stream Data Rate

- Manufactures advertise gross bit rate at Layer 2
 - Megabits per second, inclusive of all signaling and control overhead, and with zero interference

802.11a	802.11b	802.11g	802.11n	802.11ac
54	11	54	288	346

- Rates in practice vary widely
 - Distance, obstructions, interference?
- Customers care about application-layer throughput

28

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,	NI / 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	. o	MIMO-	35 m		
ac	2013	J	80	Up to 1733.2	8	OFDM	(115 ft)		
			160	Up to 3466.8					
Advanced Com	puter Netwo	orking	https://en	wikipedia.org/wiki	1		Fall 2018		

MIMO

- Transmitting/Receiving more than one data signal simultaneously over the same radio channel by exploiting multipath propagation
- Added in 802.11n
- ↗ Specification: NxM system
 - N = Number of transmitter antennas
 - **M** = Number of receiver antennas

MIMO

31

Spatial multiplexing

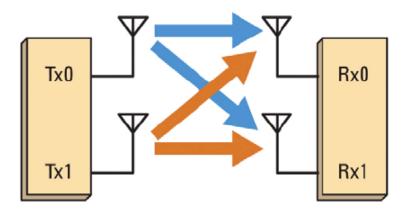
- High data rate signal is divided into multiple lowerrate streams
- Each stream is transmitted from a different transmit antenna, but in the same frequency channel
- Receiver (with multiple antennas) can separate these streams and reassemble original signal
- Limited by number of antennas at transmitter or receiver

MIMO

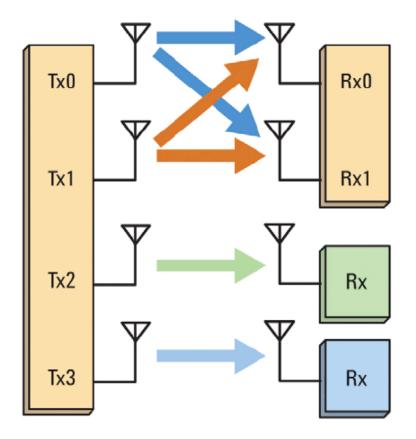
- **7** 2x2 : 1 stream
 - **7** 2 transmitting antennas
 - 2 receiving antennas
 - 1 stream of data
- **7** 2x2 : 2 streams
 - 2 transmitting antennas
 - 2 receiving antennas
 - 2 streams of data
- Cannot have 2x2 : 3 (number of streams exceeds number of antennas)

MIMO, MU-MIMO

MIM0 (2x2)



MULTI-USER MIMO 4 streams, 3 users



33

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	
2	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	F	40	Up to 800	8	MIMO-	35 m		
ac	2013	I 5 H	80	Up to 1733.2	0	OFDM	(115 ft)		
			160	Up to 3466.8					
Advanced Com	puter Netwo	orking	https://en	n.wikipedia.org/wiki	1		Fall 2018		

Modulation

DSSS

Direct Sequence Spread Spectrum

OFDM

- Orthogonal Frequency-Division Multiplexing
- MIMO-OFDM
 - Multiple Input Multiple Output Orthogonal Frequency-Division Multiplexing

Modulation and Coding Scheme (MCS)

							Data rate (ir	n Mbit/s)			
MCS index	Spatial Streams	Modulation type	Coding rate	20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns GI	400 ns GI	800 ns Gl	400 ns GI	800 ns GI	400 ns GI	800 ns Gl	400 ns Gl
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7

Added in 802.11n and 802.11ac instead of specifying data rates Index continues incrementing for multiple spatial streams

Advanced Computer Networking

https://en.wikipedia.org/wiki/IEEE 802.11ac

Modulation and Coding Scheme (MCS)

- Modulation type
 - More complex modulation = Higher data rate
 - More complex modulations require better conditions (less interference, line of sight, ...)
- Coding rate
 - How much of the data stream is used to transmit payload data (as opposed to encodings)
 - Most efficient rate is 5/6 or 83.3% of the data stream being used
- → Guard Interval (GI)
 - Short pause between packet transmission to allow for any false information to be ignored
 - Longer Guard Intervals increase reliability



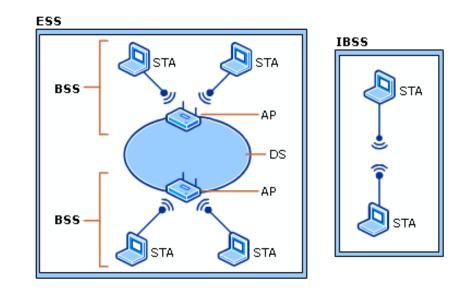
IEEE 802.11 Link Layer

38

Advanced Computer Networking

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)

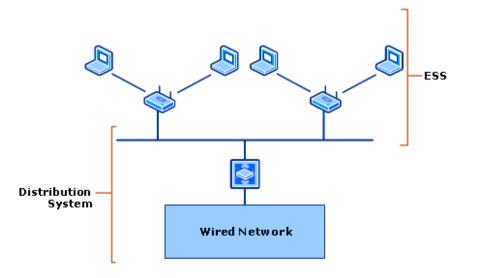


- Independent Basic Service Set (IBSS)
 - Ad-hoc network (no AP)

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
 - **オ** Type/Subtype
 - **T**o DS / From DS (Distribution System, i.e. LAN)
 - From STA to DS via an AP
 - From DS to STA via AP
 - Determines meaning of all the address fields!
 - More Fragments
 - **7** 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

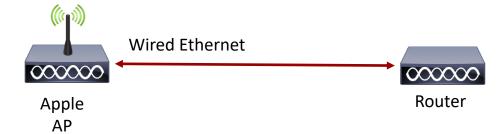
45

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



Apple iPhone







wireshark_iphone_2.pcapng	
🚄 📕 🖉 🐵 🖿 🗎 🛛 🙆 🔍 🗢 🌩 警 春 👱 🧮 🗨 🔍 Q Q 🏨	
Apply a display filter <%/>	Expression +
No. Time Source Destination Protocol Length 1030 17.72 Apple_a1:47:87 Apple_19:49:ad 802.11 52	2 Request-to-send, Flags=C
	6 Clear-to-send, Flags=C
	0 Echo (ping) request id=0x9a06, seq=4/10
	4 802.11 Block Ack, Flags=C
▶ Frame 1032: 170 bytes on wire (1360 bits), 170 bytes captured	
▶ 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:4c) <	(3) Destination Addr (DA): Router
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	(2) Source Addr (RA): iPhone
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 \dots = $ Sequence number: 79	
Frame check sequence: 0x2f0c6948 [correct] [FCS Status: Good]	
<pre>> Qos Control: 0x0000</pre>	
► CCMP parameters	
 Logical-Link Control 	
► DSAP: SNAP (0xaa)	
SCAD. CNAD (Avaa)	
	@. I.,G.
	.`.On\$R.
	Qh} .gLX%
	./ j@.No5
	i, jiienss

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

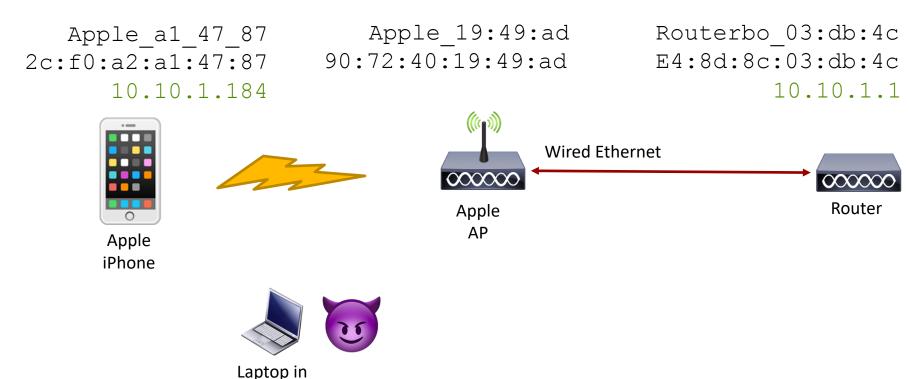
Advanced Computer Networking

wireshark_iphone_2.p	ocapng
📶 📕 🖉 💿 🖿 🖺 🗴 🗳 🍳 👄 🔿 警 🖀 🖉 📃 🗐 🔍 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	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	d (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	
\cdots	
0000 0100 1111 = Starting Sequence Number: 79	
▶ Block Ack Bitmap: 010000000000000	
Frame check sequence: 0x565263e4 [correct]	Block Acknowledgement
[FCS Status: Good]	<u> </u>
	Sent from Access Point (: 49 : ad)
	to iPhone (:47:87)
	for sequence starting at 79
	.iX1Ar
	0. q.@
	, 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

Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.77 Profile: Default

(Same) Example



monitor mode

48

Beacons and Probes

Beacon Frames

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

• • • • interstant	ne_2.pcapng
📶 📕 🔬 🐵 🖿 🗎 🗙 🙆 🔍 🖛 🌩 警 🚡 퉆 🗮 🔍 Q, Q,	. 🏥
Apply a display filter <ૠ/>>	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	. 122 Data, SN=444, FN=0, Flags=.pF.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 ca	ptured (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)	
<pre>Destination address: Broadcast (ff:ff:ff:ff:ff:ff)</pre>	
Transmitter address: Apple_19:49:ad (90:72:40:19:49:ad	d)
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]	Beacon
[FCS Status: Good]	
▹ IEEE 802.11 wireless LAN	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	dNi lla 5GHz
0050	01	0 8	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	.48<@d
0080	68	01	18	6c	01	18	70	01	18	74	01	18	84	01	18	88	hlpt
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

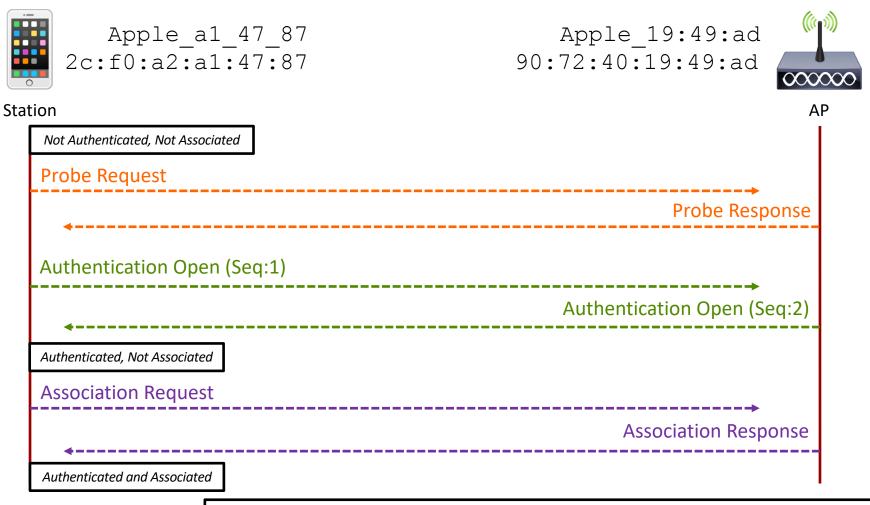
Packets: 2228 · Displayed: 2228 (100.0%) · Dropped: 0 (0.0%) · Load time: 0:0.79 Profile: Default

			wireshark_iphone_2.pcapng
🦲 🔳 🙆 🖿	🖹 🖹 🔇	🔶 🍝 🔮 春 🛓	🛃 📃 🔍 Q, Q, 🎹

		। 🛅 🖹 🎑 🤇 🔶 🍝			T						
	a display filter < %	· · · · · · · · · · · · · · · · · · ·		1 4 4	<u></u>					Expression	
No.	Time	Source	Destination	Protocol	Length	Info				Expression	
	1017 17.63	Apple_19:49:ad	Broadcast	802.11	372	Beacon	frame,	SN=2833,	, FN=0,	Flags=	
	1018 17.6	5 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, S	SN=444,	FN=0, F1	lags=.p	F.C	
	1020 17.73	92:ad:49:19:40:	Broadcast	802.11	360	Beacon	frame,	SN=2834,	, FN=0,	Flags=	
• IEE	E 802.11	vireless LAN									
	ixed param	eters (12 bytes)									
	Timestamp	: 0x000014ff8692023	c								
	Beacon In	terval: 0.102400 [S	econds]								
►	Capabilit	ies Information: 0x	1111								
• Та	agged para	meters (300 bytes)									
►	Tag: SSID	parameter set: Nil	la 5GHz 🔸 🚽		-						
		orted Rates 6(B), 9				[Mbit/s	sec]				
►	Tag: Traf	fic Indication Map	(TIM): DTIM 0 of	0 bitma	0						
►	Tag: Coun	try Information: Co	untry Code US, En	vironme	nt Any						- 1
►	Tag: Powe	r Constraint: 0									- 1
►	Tag: TPC	Report Transmit Pow	er: 25, Link Marg	in: 0							- 1
►	Tag: RSN	Information									
►	Tag: HT C	apabilities (802.11	n D1.10)					_			
►	Tag: HT I	nformation (802.11n	D1.10)		Beacon (continued)						
►	Tag: Exte	nded Capabilities (8 octets)								
		Capabilities (IEEE)	Advertising SSID ("Nilla 5GHz")						
	-	Operation (IEEE Std				Adver [®]	tising I	many di	ifferer	nt TX/RX	
		Tx Power Envelope (IEEE Std 802.11ac	/D5.0)			- hilitia	, c at var	v data	ratac	
	-	or Specific: Apple				Capa	abilitie	s at var	y Udla	rates	
		or Specific: Apple									- 1
0030) 19 49 ad 10 b1 3	c 02 92 86 ff 14 (00 00	r@ T	. <					
0040			c 6c 61 20 35 47 4			li lla 5					
0050			0 6c 05 04 00 03 (Η `l					
0060			8 01 11 2c 01 11 3			. (,.					
0070			1 18 40 01 18 64 0			<@					
0080		3 6c 01 18 70 01 1			hlp	t					
0090	01 18 8	c 01 18 90 01 18 9	5 01 1e 99 01 1e 9	9d 01							

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

Association



Advanced Computer Networking

https://documentation.meraki.com/MR/WiFi Basics and Best Practices/802.11 Association process explained

				wireshark_iphone_2.pc	apng				
	🧟 🔘 📄	🖹 🔀 🤇 🔶 🍝	2 🚯 👱 📃 🔍	Ð, Ə, Ə, 🎹					
📕 wlan.addr	==2c:f0:a2:a1:47:87							Expression	. +
No.	Time	Source	Destination		ength Info				
		Apple_a1:47:87	Broadcast	802.11	177 Probe Req				
		Apple_19:49:ad		802.11	366 Probe Res	•	•		
		Apple_a1:47:87	Apple_19:49:ad	802.11	100 Authentic	-	-		
	390 8.182		Apple_a1:47:87		46 Acknowled			C	
		bytes on wire (1	416 bits) , 177 by	tes capture	ed (1416 bits)	on inter	rface 0		
	version 0,	-							
▶ 802.	ll radio i	nformation							
▼ IEEE	802.11 Pr	obe Request, Flag	s:C						
Тур	e/Subtype:	Probe Request (0	×0004)						
► Fra	me Control	. Field: 0x4000							
.00	0 0000 000	0 0000 = Duration	: 0 microseconds						
Rec	eiver addr	ess: Broadcast (f	f:ff:ff:ff:ff:ff)						
Des	tination a	ddress: Broadcast	(ff:ff:ff:ff:ff:ff:	ff) 🗕 🗕					
Tra	nsmitter a	ddress: Apple_a1:	47:87 (2c:f0:a2:a	a1:47:87) <		_			
		s: Apple_a1:47:87							
		<pre>lcast (ff:ff:ff:ff</pre>		,					
		. 0000 = Fragment							
		00 = Sequence							
		sequence: 0x487aa6		_					
	S Status:	•					_		
		reless LAN				Probe	Request		
		eters (117 bytes)			Sent fr	om Pho	ne (:4	7 • 87)	
-	• •	arameter set: Nil	la 5GHz 🔶				•		
		ted Rates 6, 9, 1		54 [Mb-	to ev	veryone	e(:FF:	FF)	
		abilities (802.11		, ,, ,, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	الماحاتين	at af inde		:1:+:	
	•	ed Capabilities (8			WITH IIS	st of ph	<i>one</i> capab	inties.	
	0	•	b ULLELS/		(This prob	e was la	ooking for	a specific	
	ag: Interw	5	C+d 002 1122/D2 1	、	• •		0,5		
	-	pabilities (IEEE	Stu 802.11aC/D3.1)	SSID, but j	probes d	could be fo	or all Aps)	
	-	Specific: Apple	af Halman - O						
	•	Specific: Micros		_					
	ag: Vendor	Specific: Broadc	om						

wireshark_iphone_2.pc	capng
📕 📕 🙆 💿 🚞 🖹 🖄 🗳 🔍 🖛 🌩 警 🗿 💆 🧮 🔍 Q, Q, 🏢	
wlan.addr==2c:f0:a2:a1:47:87	Expression +
No. Time Source Destination Protocol 385 8.162 Apple_a1:47:87 Broadcast 802.11	177 Probe Request, SN=2276, FN=0, Flags=
386 8.163 Apple_19:49:ad Apple_a1:47:87 802.11	366 Probe Response, SN=2590, FN=0, Flags=
389 8.182 Apple_a1:47:87 Apple_19:49:ad 802.11	100 Authentication, SN=2277, FN=0, Flags=
390 8.182 App tc_d1147107 App tc_15145100 002111	46 Acknowledgement, Flags=C
Frame 386: 366 bytes on wire (2928 bits), 366 bytes captur	
PPI version 0, 32 bytes	
▶ 802.11 radio information	
IEEE 802.11 Probe Response, Flags:C	
Type/Subtype: Probe Response (0x0005)	
▷ Frame Control Field: 0x5000	
.000 0000 0011 1100 = Duration: 60 microseconds	
Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	
<pre>Destination address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)</pre>	
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 1010 0001 1110 = Sequence number: 2590	
Frame check sequence: 0xff28d2f6 [correct]	
[FCS Status: Good]	Ducho Decucione
▼ IEEE 802.11 wireless LAN	Probe Response
 Fixed parameters (12 bytes) 	Sent from AP (:49:ad)
Timestamp: 0x000014ff8601ce6a	to phone (: 47:87)
Beacon Interval: 0.102400 [Seconds]	
Capabilities Information: 0x1111	With list of AP capabilities
 Tagged parameters (294 bytes) 	•
▶ Tag: SSID parameter set: Nilla 5GHz	Phone now has list of APs and their
▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48,	
Tag: Country Information: Country Code US, Environment	capabilities and can choose which AP it
▶ Tag: Power Constraint: 0	wants to authenticate with
▶ Tag: TPC Report Transmit Power: 25, Link Margin: 0	(could gut hanticate with multiple ADe to
► Tag: RSN Information Tage UT Comphilities (202, 11, D1, 10)	(could authenticate with multiple APs to
Tag: HT Capabilities (802.11n D1.10) Frame (frame), 366 bytes	accelerate roaming. Look for
rianie (nanie), soo uytes	eraut

strongest?)

wireshark_iphone_2.	ocapng
📶 🔳 🖉 🐵 🖿 🗎 🕱 🖆 🔍 👄 🌧 警 쥼 👱 📃 📃 🔍 Q, Q, 🎚	
Wlan.addr==2c:f0:a2:a1:47:87	Expression +
No. Time Source Destination Protocol 2005 0 100 1 472007 Dwo od op other 0000 11	Length Info
385 8.162 Apple_a1:47:87 Broadcast 802.11	177 Probe Request, SN=2276, FN=0, Flags=
386 8.163 Apple_19:49:ad Apple_a1:47:87 802.11	366 Probe Response, SN=2590, FN=0, Flags=
389 8.182 Apple_a1:47:87 Apple_19:49:ad 802.11	100 Authentication, SN=2277, FN=0, Flags=
390 8.182 Apple_a1:47:87 802.11	46 Acknowledgement, Flags=C
▶ Frame 389: 100 bytes on wire (800 bits), 100 bytes capture	ed (800 bits) on interface 0
<pre>> PPI version 0, 32 bytes</pre>	
802.11 radio information	
<pre>IEEE 802.11 Authentication, Flags:C</pre>	
Type/Subtype: Authentication (0x000b)	
▶ Frame Control Field: 0xb000	
.000 0000 0011 1100 = Duration: 60 microseconds	
Receiver address: Apple_19:49:ad (90:72:40:19:49:ad)	
Destination address: Apple_19:49:ad (90:72:40:19:49:ad)	•
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)	
0000 = Fragment number: 0	
1000 1110 0101 = Sequence number: 2277	
Frame check sequence: 0x4709c80e [correct]	
[FCS Status: Good]	Open System Authentication
<pre>IEEE 802.11 wireless LAN</pre>	
Fixed parameters (6 bytes)	Sent from Phone (:47:87)
Authentication Algorithm: Open System (0)	to selected AP (:49:ad)
Authentication SEQ: 0x0001	
Status code: Successful (0x0000)	to open authentication with
 Tagged parameters (34 bytes) 	sequence 0x0001
Tag: Extended Capabilities (8 octets)	
Tag: Vendor Specific: Apple	
▶ Tag: Vendor Specific: Broadcom	

wireshark_iphone_2	pcapng
📶 📕 🖉 🞯 🖿 🛅 🖹 🙆 🔍 🗢 🔿 警 🚡 👱 🔜 🔍 Q, Q, 1	
Wlan.addr==2c:f0:a2:a1:47:87	Expression +
No. Time Source Destination Protocol 2000 0 1002 Approl_0 1002 11	Length Info
389 8.182 Apple_a1:47:87 Apple_19:49:ad 802.11	100 Authentication, SN=2277, FN=0, Flags=
390 8.182 Apple_a1:47:87 802.11	46 Acknowledgement, Flags=C
391 8.197 Apple_19:49:ad Apple_a1:47:87 802.11	77 Authentication, SN=2591, FN=0, Flags=
395 8.199… Apple_a1:47:87 Apple_19:49:ad 802.11	248 Association Request, SN=2278, FN=0, Flag
Frame 391: 77 bytes on wire (616 bits), 77 bytes captured	l (616 bits) on interface 0
PPI version 0, 32 bytes	
802.11 radio information	
IEEE 802.11 Authentication, Flags:C	
Type/Subtype: Authentication (0x000b)	
▶ Frame Control Field: 0xb000	
.000 0000 0011 1100 = Duration: 60 microseconds	
Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	
Destination address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	→
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)	
$\dots \dots $	
1010 0001 1111 = Sequence number: 2591	
Frame check sequence: 0x168dda3c [correct]	Open System Authentication
[FCS Status: Good]	
▼ IEEE 802.11 wireless LAN	Sent from AP (:49:ad)
<pre> • Fixed parameters (6 bytes) </pre>	to phone (: 47:87)
Authentication Algorithm: Open System (0)	
Authentication SEQ: 0x0002	with sequence 0x0002
Status code: Successful (0x0000)	
 Tagged parameters (11 bytes) 	Phone now has list of APs and their
	Phone now has list of APs and their
Tag: Vendor Specific: Broadcom	capabilities and can choose which AP it

wants to associate with (necessary in order to send/receive data)

Packets: 2228 · Displayed: 860 (38.6%) · Dropped: 0 (0.0%) · Load time: 0:0.182 Profile: Default

• • •	k_iphone_2.pcapng
🚄 📕 🔬 💿 🖿 🛅 🛛 🙆 🔍 🗢 🌩 警 奋 👱 📃 🗐 🔍 🔍	
wlan.addr==2c:f0:a2:a1:47:87	Expression +
No. Time Source Destination Protoco	
391 8.197 Apple_19:49:ad Apple_a1:47:87 802	, , , ,
	.11 248 Association Request, SN=2278, FN=0, Flag
396 8.199 Apple_a1:47:87 802	
	.11 222 Association Response, SN=2594, FN=0, Fla
Frame 395: 248 bytes on wire (1984 bits), 248 bytes	captured (1984 bits) on interface 0
PPI version 0, 32 bytes 802 11 radia information	
802.11 radio information	
IEEE 802.11 Association Request, Flags:C	
Type/Subtype: Association Request (0x0000) ◀ ▶ Frame Control Field: 0x0000	
.000 0000 0011 1100 = Duration: 60 microseconds	
	4)
Receiver address: Apple_19:49:ad (90:72:40:19:49:ad Destination address: Apple_19:49:ad (90:72:40:19:49	
Transmitter address: Apple_19.49.ad (90.72.40.19.49) Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47)	
Source address: Apple_a1:47:87 (2c:f0:a2:a1:47) Source address: Apple_a1:47:87 (2c:f0:a2:a1:47:87)	/.0/)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)	
0000 = Fragment number: 0	
1000 1110 0110 = Sequence number: 2278	
Frame check sequence: 0xfb4dfb5f [correct]	
[FCS Status: Good]	Association Request
▼ IEEE 802.11 wireless LAN	Sent from Phone (: 47:87)
Fixed parameters (4 bytes)	
Capabilities Information: 0x1111	to selected AP (: 49 : ad)
Listen Interval: 0x0014	
 Tagged parameters (184 bytes) 	with selected capabilities
▶ Tag: SSID parameter set: Nilla 5GHz	(encryption type, frequency, speed,)
▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 3	
► Tag: Power Capability Min: 2, Max :19	
Tag: Supported Channels	
► Tag: RSN Information	
Tag: RM Enabled Capabilities (5 octets)	
► Tag: HT Capabilities (802.11n D1.10)	
Tag: Extended Capabilities (8 octets)	
FCS Status (wlan.fcs.status)	Packets: 2228 · Displayed: 860 (38.6%) · Dropped: 0 (0.0%) · Load time: 0:0.182 Profile: Default

wirechark inhone 2 n

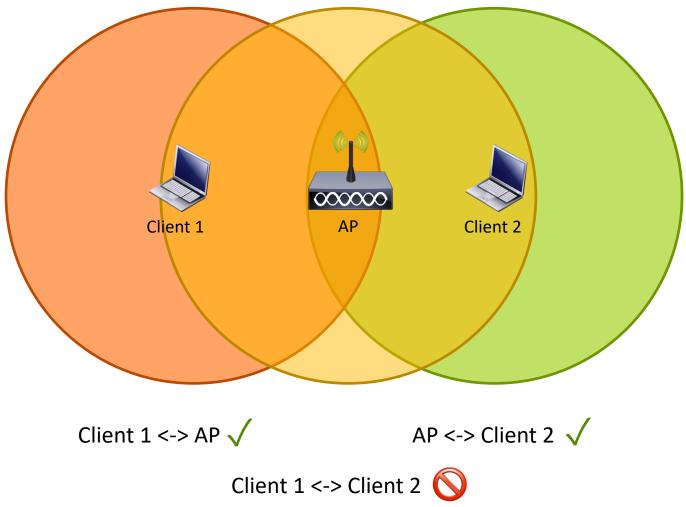
• • • •	reshark_iphone_2.pcapng
■ 🧕 💌 📄 🗋 🛛 🖸 🔍 🗢 👄 🖉 🖉 📃 📃 🔍	
wlan.addr==2c:f0:a2:a1:47:87	Expression +
	Protocol Length Info 802.11 77 Authentication, SN=2591, FN=0, Flags=
	802.11 77 Authentication, SN=2591, FN=0, Flags= 802.11 248 Association Request, SN=2278, FN=0, Flag
396 8.199 Apple_a1.47.87 Apple_a1:47:87 8	
	802.11 222 Association Response, SN=2594, FN=0, Fla
 Frame 397: 222 bytes on wire (1776 bits), 222 byte 	
PPI version 0, 32 bytes	
▶ 802.11 radio information	
IEEE 802.11 Association Response, Flags:0	C
Type/Subtype: Association Response (0x0001)	
Frame Control Field: 0x1000	
.000 0000 0011 1100 = Duration: 60 microseconds	
Receiver address: Apple_a1:47:87 (2c:f0:a2:a1:47	7:87)
<pre>Destination address: Apple_a1:47:87 (2c:f0:a2:a1</pre>	1:47:87) 🔶 🚽 🚽
Transmitter address: Apple_19:49:ad (90:72:40:19	
Source address: Apple_19:49:ad (90:72:40:19:49:a	ad)
BSS Id: Apple_19:49:ad (90:72:40:19:49:ad)	
0000 = Fragment number: 0	
1010 0010 0010 = Sequence number: 2594	
Frame check sequence: 0xd831d5c2 [correct]	Association Response
[FCS Status: Good]	Sent from AP (:49:ad)
<pre>IEEE 802.11 wireless LAN</pre>	
 Fixed parameters (6 bytes) Capabilities Information: 0x1011 	to phone (: 47 : 87)
Status code: Successful (0x0000)	with approval
00 0000 0000 0100 = Association ID: 0x0004	
 Tagged parameters (156 bytes) 	
► Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B),	Phone is now associated with AP can
 Tag: RCPI: Undecoded 	can send/receive data
► Tag: RSNI	
Tag: RM Enabled Capabilities (5 octets)	
► Tag: HT Capabilities (802.11n D1.10)	Or can it?
▶ Tag: HT Information (802.11n D1.10)	
Tag: Extended Capabilities (8 octets)	
Frame (frame), 222 bytes	Packets: 2228 · Displayed: 860 (38.6%) · Dropped: 0 (0.0%) · Load time: 0:0.182 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



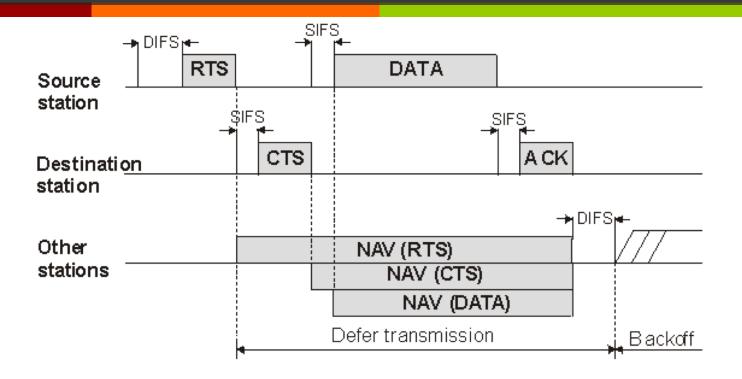
CSMA/CA, RTS/CTS

オ CSMA/CA

- **7** 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)

						wireshark_ip	hone_2.pcapng						
			ې 🧼 🖻) 😫 有 💈		$ \oplus $	2						
Apply	a display filter <郑/>>	>									— • •	Expression	+
No.	Time	Source		Destination		Protocol	Length	Info			-		
	1030 17.72		1:47:87						-	ags=	С		
	1031 17.72			Apple_a	a1:47:87 …	. 802.1	.1 46	5 Clear-to-	send, Flag	s=C		-	
	1032 17.72									id=0x9a06,		10	
	1033 17.72	Apple_1	19:49:ad	Apple_a	a1:47:87 .	. 802.1	.1 64	4 802.11 Blo	ock Ack, F	lags=	. C		
 PPI 802 IEE Ty F .(I version 0 2.11 radio EE 802.11 R ype/Subtype rame Contro 000 0000 1	0, 32 byte informati Request-to e: Reques ol Field: 001 0010 :	es ion o-send, F st-to-send 0xb400 = Duratio	Flags: nd (0x001b Lon: 146 m	C D) nicrosecond	ids		L6 bits) on	interface	0			
T F	eceiver ad ransmitter rame check FCS Status	address: sequence	Apple_a	a1:47:87 ((2c:f0:a2:a								

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													@.

$\bullet \bullet \bullet$							i wireshark	_iphone_2.pc	capng					
			i 🔀 🍯] 🤇 🔶 🗉		⊻ 📮 🔳	÷ O	0						
Apply ;	a display filter .	<೫/>											Expression	. +
No.	Time		Source		Destination		Protocol			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, F	lags=	.C		
	1032 17	/.72	10.10.	1.184	8.8.8	.8	ICM	2	170	Echo (ping) requ	est id=0x9a	06, seq=	4/10	
	1033 17	/ . 72	Apple_	19:49:ad	… Apple	_a1:47:87	802	. 11	64	802.11 Block Ack	, Flags=	C		
 PPI 802 IEE Ty Fi .0 	I versic 2.11 rac EE 802.1 ype/Sub rame Co 000 000 eceiver	on 0, dio ir 11 Cle otype: ontrol 00 010 - addr neck s	32 byt nformat ear-to- Clear- Field: 01 1100 ress: Ap sequence	tes tion -send, Fla -to-send : 0xc400 = Durati	.ags: (0x001c) ion: 92 m 47:87 (2c	C) nicrosecond c:f0:a2:a1	ds		(368	3 bits) on interfa	ace Ø			

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

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

Advanced Computer Networking

wireshark_ipho	ne_2.pcapng
🚄 📕 🖉 🐵 🖿 🖹 🛛 🗳 🔍 🗢 🔿 警 🚡 📃 📃 🔍 Q Q	
Apply a display filter <ૠ/>>	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	
1033 17.72… Apple_19:49:ad … Apple_a1:47:87 … 802.11	L 64 802.11 Block Ack, Flags=C
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>	b:4c) ←
Transmitter address: Apple_a1:47:87 (2c:f0:a2:a1:47:8	7)
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)	Data
0000 = Fragment number: 0	
0000 0100 1111 = Sequence number: 79	ICMP ping
Frame check sequence: 0x2f0c6948 [correct]	from iPhone (10.10.1.184,: 47:87)
[FCS Status: Good]	
⊳Qos Control: 0x0000	to Google (8.8.8.8)
► CCMP parameters	by way of AP (: 49:ad)
Logical-Link Control	by way of Ar (49.au)

▶ DSAP: SNAP (0xaa)

CCVD. CNIVD (UAS) 0020 88 41 30 00 90 72 40 19 49 ad 2c f0 a2 a1 47 87 e4 8d 8c 03 db 4c f0 04 00 00 82 00 00 20 00 00 0030 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 06 06 60 8f 09 44 fa 2f 6a 87 f6 40 d5 4e 6f 35 0070

and router (...: db: 4c)

...... ...&...` .On\$..R. .}0...Q. .h...}.. . .p...g ..LX%... ..`..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

Advanced Computer Networking

wireshark_iphone_2	2.pcapng
📶 📕 🖉 🐵 🖿 🖹 🛛 🙆 🔍 🗢 🌩 警 春 👱 🌉 🔲 🔍 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 10.00 10.00 10.00	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 capture	ed (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)	
<pre>10. = Block Ack Type: Compressed Block (0x2)</pre>	
Block Ack Request Control: 0x0005	
Block Ack Starting Sequence Control (SSC): 0x04f0	
▶ Block Ack Bitmap: 010000000000000	
Frame check sequence: 0x565263e4 [correct]	
[FCS Status: Good]	
	Acknowledgement
	Sent from Access Point (: 49 : ad)
	N N N N N N N N N N N N N N N N N N N
	to iPhone (: 47:87)

0000	00	00	20	00	69	00	00	00	02	00	14	00	58	31	41	72	iX1Ar
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	, 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

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



802.11 and Security

Advanced Computer Networking

Authentication and Association

802.11 network attachment process

- Authentication Station establishes its identity (MAC address) with AP
 - No password was verified!
 - ↗ No encryption!
 - This is "Open system authentication"
- Association Station chooses a specific AP to send/receive data with

So where does *security* **come into play**?

WiFi Security

- **➢** WEP − Wired Equivalent Privacy
- Used RC4 stream cipher
- ↗ Insecure, don't use! ☺

WiFi Security

- WPA WiFi Protected Access
 - → Transitional spec
 - Requires support for TKIP and RC4 stream cipher
 - オ Insecure, don't use! ☺
 - Optional support for AES-CCMP

7 WPA2

- Also known as RSN (Robust Security Network)
- Required support for AES-CCMP Use this!

IEEE 802.111, WPA2

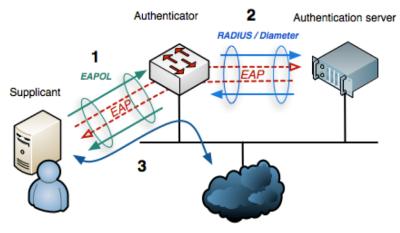
AES-CCMP?

- Advanced Encryption Standard (AES)
 - Block cipher, symmetric key encryption
- Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)
 - Operating mode for AES cipher
 - Counter Mode, Cipher Block Chaining
 - Message Authentication Code
 - Confidentiality + Integrity

IEEE 802.111, WPA2

- Extensible Authentication Protocol (EAP)
- Extensible Authentication Protocol over LAN (EAPOL)
 - Defined in IEEE 802.1X standard
 - Used in wired Ethernet (802.3) and WiFi (802.11)

- オ Terminology
 - Supplicant Client device (e.g. your laptop)
 - **オ** Authenticator − The AP
 - Authentication server –
 RADIUS server (or AP)



Internet or other LAN resources

- 4-Way Handshake
- Proven secure (in part)
 - Key secrecy and session authentication
 - Key ordering and key secrecy for group key handshake

He, Changhua & Sundararajan, Mukund & Datta, Anupam & Derek, Ante & C. Mitchell, John. (2005). *A modular correctness proof of IEEE 802.11i and TLS*. Proceedings of the ACM Conference on Computer and Communications Security.

- Pairwise Master Key (PMK)
 - Shared Secret between client and AP
 - Derived from pre-shared password in personal network
 - PBKDF2 key derivation function
 - **オ** SSID is salt
 - 4096 iterations of HMAC-SHA1
 - Derived from 802.1x authentication in enterprise network
 - RADIUS authentication server

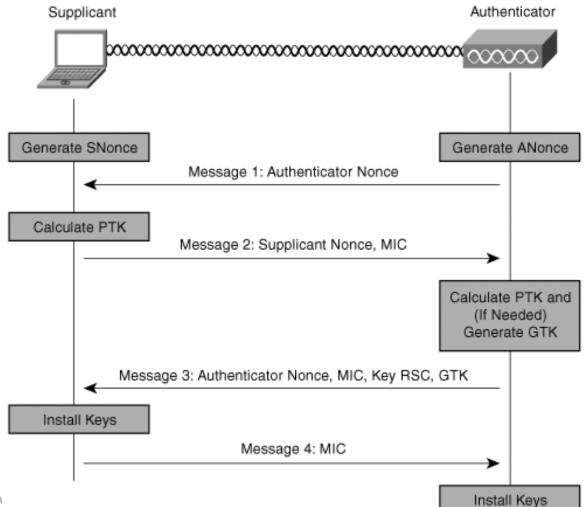
- Pairwise Transient Key (PTK) 64 bytes
 - Used as a session key (is changed periodically)
 - Derived from:
 - **PMK**
 - Authenticator Nonce (ANonce)
 - Supplicant Nonce (SNonce)
 - MAC address of authenticator
 - MAC address of supplicant

- Client never tells AP its PMK/PTK (or vice-versa)
 - Decryption only works if both parties independently calculate the same PMK/PTK
 - Protects against rogue AP impersonating real AP

76

- Keys obtained from slices of PTK
 - → Key Confirmation Key (KCK) 16 bytes of PTK
 - - Protects handshake messages
 - → Temporal Key (TK) 16 bytes of PTK
 - Protects normal data frames
 - ➤ Message Integrity Check (MIC) for TX 8 bytes of PTK
 - Message Integrity Check (MIC) for RX 8 bytes of PTK
- → Group Temporal Key (GTK)
 - Used for broadcast and multicast frames
 - Randomly generated by AP
 - **7** Rotated periodically

Authentication with EAPOL



Advanced Computer Netw

wireshark_iphone_2.pc	capng							
🚄 📕 🖉 🐵 🖿 🖺 🔀 🛇 🐥 🗭 警 春 🎐 📃 📃 🔍 Q, Q, 🏢								
wlan.addr==2c:f0:a2:a1:47:87 && eapol	Expression +							
	Length Info							
403 8.212 Apple_19:49:ad Apple_a1:47:87 EAPOL	169 Key (Message 1 of 4)							
411 8.214 Apple_a1:47:87 Apple_19:49:ad EAPOL	191 Key (Message 2 of 4)							
415 8.215 Apple_19:49:ad Apple_a1:47:87 EAPOL	225 Key (Message 3 of 4)							
419 8.217 Apple_a1:47:87 Apple_19:49:ad EAPOL	169 Key (Message 4 of 4)							
Frame 403: 169 bytes on wire (1352 bits), 169 bytes capture PRI version 0, 32 bytes	ed (1352 bits) on interface v							
PPI version 0, 32 bytes 802 11 radio information								
▶ 802.11 radio information ► 502.11 0oS Data Elago, E.C.								
 IEEE 802.11 QoS Data, Flags:F.C Logical-Link Control 								
▼ 802.1X Authentication								
Version: 802.1X-2004 (2)								
Type: Key (3)								
Length: 95								
Key Descriptor Type: EAPOL RSN Key (2)								
Key Information: 0x008a								
Key Length: 16								
Replay Counter: 0 ◀ WPA Key Nonce: e6c659db406bcfc7f096fec4e6619ffdcc3f4776b5	52ffa18 ANonce							
Key IV: 00000000000000000000000000000000000								
WPA Key RSC: 000000000000000								
WPA Key ID: 0000000000000								
WPA Key MIC: 000000000000000000000000000000000000								
WPA Key Data Length: 0 EAPOL Handshake (1 of 4)								
	Sent from AP (:49:ad)							
	to phone (: 47:87)							
	containing ANonce and replay counter r							
	Supplicant (phone) can now							
	calculate PTK							

					wireshark_iphone_2.p	capng			
📶 📕 🖉 💿 🖿 🖺 🖄 🗳 🗢 👄 🚔 🖉 🚽 📃 📃 🔍 Q, Q, 🏢									
wlan.addr==2c:		&& eapol							Expression +
No.	Time Q 717	Source	19:49:ad	Destination Apple_a1:47:87	Protocol EAPOL	Length Info	(Message 1 of 4)		[
		<u>··</u>	_19.49.au _a1:47:87	Apple_19:49:ad	EAPOL		(Message 2 of 4)		
				Apple_19:49:80 Apple_a1:47:87			(Message 3 of 4)		
				Apple_19:49:ad		•	(Message 4 of 4)		
							bits) on interface	<u>م</u>	
		-		.520 DI(3/, 191 D	yees captur	Cu (1520	bits) on interface		
	PPI version 0, 32 bytes 802.11 radio information								
			Flags:	тс					
▹ Logical		-	,						
▼ 802.1X	Authent	icatior	ı						
Versi	Version: 802.1X-2004 (2)								
Type:	Type: Key (3)								
Lengtl	n: 117								
Key De	escripto	or Type	: EAPOL RSI	N Key (2)					
⊳ Key I	nformati	ion: 0x	010a						
Key Le	Key Length: 16								
Replay	/ Counte	er: 0						C N1	
WPA Ke	ey Nonce	e: efbc	821bf790bc	830df290697cb50d	2996b05ac3d	51d4f15		SNonce	
Key I	/: 00000	0000000	00000000000	00000000000					
WPA Ke	ey RSC:	000000	00000000000						
WPA Key ID: 0000000000000									
WPA Ke	ey MIC:	932ee7	4d84bb7a91	58ea9ff2277b268a					
WPA Ke	ey Data	Length	: 22						
► WPA Ke	ey Data:	30140	100000fac0	40100000fac04010	0000fac020c		EAPOL Handsha	ake (2 of 4)	
						Se	ent from phone ((
								· /	
							to AP (: 4	19:ad)	
						contai	ining SNonce and	d renlay count	or r
						contai			
							Authenticator (A	P) can now	
							•		
							calculate	PIK	

🔴 🌋 Logical-Link Control (llc), 8 bytes

Packets: 2228 · Displayed: 6 (0.3%) · Dropped: 0 (0.0%) · Load time: 0:0.82 Profile: Default

wireshark_iphone_2.pcapng							
📶 📕 🖉 💿 🔚 🖺 🖸 🔍 👄 🔿 🙅 🜉 🚍 🔍 Q, Q, II							
wlan.addr==2c:f0:a2:a1:47:87 && eapol	Expression +						
No. Time Source Destination Protocol	Length Info						
403 8.212 Apple_19:49:ad Apple_a1:47:87 EAPOL	169 Key (Message 1 of 4)						
411 8.214 Apple_a1:47:87	191 Key (Message 2 of 4)						
415 8.215 Apple_19:49:ad Apple_a1:47:87 EAPOL	225 Key (Message 3 of 4)						
419 8.217 Apple_a1:47:87	169 Key (Message 4 of 4)						
Frame 415: 225 bytes on wire (1800 bits), 225 bytes captur	ed (1800 bits) on interface 0						
▶ PPI version 0, 32 bytes							
▶ 802.11 radio information							
IEEE 802.11 QoS Data, Flags:F.C							
▶ Logical-Link Control							
802.1X Authentication							
Version: 802.1X-2004 (2)							
Туре: Кеу (З)							
Length: 151							
Key Descriptor Type: EAPOL RSN Key (2)							
Key Information: 0x13ca							
Key Length: 16							
Replay Counter: 1							
WPA Key Nonce: e6c659db406bcfc7f096fec4e6619ffdcc3f4776b	52ffa18						
Key IV: 00000000000000000000000000000000000							
WPA Key RSC: 000000000000000							
WPA Rey RSC: 000000000000000000000000000000000000							
WPA Key MIC: bc090c1c5a594d77ec0da1dbc71ca425							
WPA Key Data Length: 56							
WPA Key Data: 4a456f56f3fd5f13995e4fe215b874bf18f6e60504							
WPA Rey Data: 484501501510511599504102150074011010000504	EAPOL Handshake (3 of 4)						
	Sent from AP (:49:ad)						
	to phone (: 47:87)						
Supplicant (phone) now knows							

🔴 🍸 Logical-Link Control (IIc), 8 bytes

Packets: 2228 · Displayed: 6 (0.3%) · Dropped: 0 (0.0%) · Load time: 0:0.82 Profile: Default

		wireshark_iphone	_2.pcapng					
🖉 📕 🖉 🔘 🖿 🛅 🗙 🖉 🔍 🖛 🗉) 😫 🐔 👱 📃 📃	\oplus \bigcirc \equiv	3					
kview wielen and wiele								
No. Time Source		Protocol	Length Info	$(M_{2}, \alpha_{2}, \alpha_{2}, \alpha_{3}, \alpha_{4}, \alpha_{5}, \alpha_{5},$				
403 8.212 Apple_19:49:ad	•• –	EAPOL	-	(Message 1 of 4)				
411 8.214 Apple_a1:47:87	•• –	EAPOL	-	(Message 2 of 4)				
415 8.215 Apple_19:49:ad	Apple_a1:47:87	EAPOL	-	(Message 3 of 4)				
419 8.217 Apple_a1:47:87	· · ·	EAPOL		(Message 4 of 4)	-			
Frame 419: 169 bytes on wire (1352 bits), 169 by	ytes capt	ured (1352	bits) on interface (0			
▶ PPI version 0, 32 bytes								
▶ 802.11 radio information								
▶ IEEE 802.11 QoS Data, Flags: .	TC							
Logical-Link Control								
<pre>* 802.1X Authentication</pre>								
Version: 802.1X-2004 (2)								
Type: Key (3)								
Length: 95								
Key Descriptor Type: EAPOL R	5N Key (2)							
▶ Key Information: 0x030a								
	Key Length: 16							
Replay Counter: 1								
WPA Key Nonce: 000000000000	000000000000000000000000000000000000000	00000000	00000000					
Key IV: 000000000000000000000	000000000000							
WPA Key RSC: 00000000000000	0							
WPA Key ID: 0000000000000								
WPA Key MIC: b89f6b76a2d88de	cc09180c881de969a							
WPA Key Data Length: 0								
				EADOL Handchak	(1 of 1)			
				EAPOL Handshak	e (4 01 4)			
			Se	ent from phone (.	.:47:87)			
				•	· · · · · · · · · · · · · · · · · · ·			
				to AP (: 4 9	ad)			
			C	and and sublem t				
			Suppli	cant and authenti	cator install PTK			
			Rea	dy to exchange er	crypted data			
			- Red	ay to exchange cr				

🔴 🌋 Logical-Link Control (llc), 8 bytes

WPA₂ Decryption

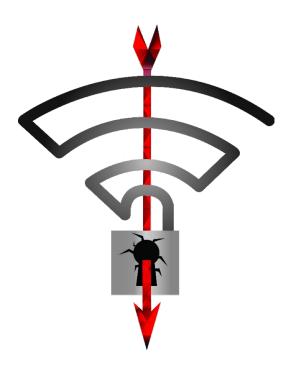
WPA2 Personal

- Every user shares the same password
- Every user shares the same Pairwise Master Key (PMK) which is derived from the password
- Each user has a *different* Pairwise Transient Key (PTK) ...
 - Image: ... but can be calculated by a party that knows the password and can observe the ANonce and Snonce handshake
- Result = Traffic can be decrypted

WPA₂ Decryption

WPA2 Enterprise (802.1x)

- **7** Each user has a *different* password
- Every user has a *different* Pairwise Master Key (PMK) which is derived from the password
- Each user has a *different* Pairwise Transient Key (PTK)
- Result = Traffic cannot be decrypted
 - Unless malicious actor can steal PMK from client or Radius server



Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse

Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven

https://www.krackattacks.com/





WPA2 KRACK

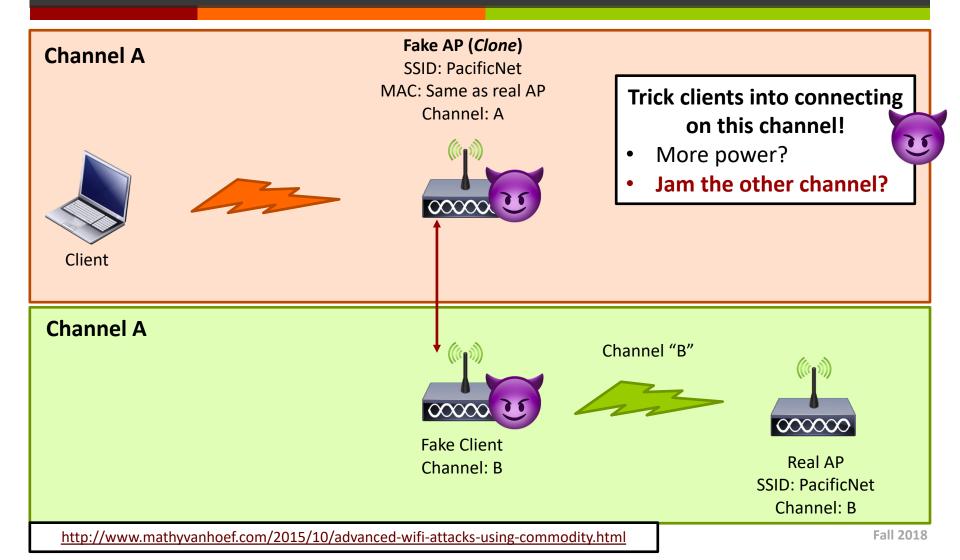
When a client joins a network, it executes the 4-way handshake to negotiate a fresh encryption key. It will install this key after receiving message 3 of the 4-way handshake. Once the key is installed, it will be used to encrypt normal data frames using an encryption protocol. However, because messages may be lost or dropped, the Access Point (AP) will retransmit message 3 if it did not receive an appropriate response as acknowledgment. As a result, the client may receive message 3 multiple times. Each time it receives this message, it will reinstall the same encryption key, and thereby reset the incremental transmit packet number (nonce) and receive replay counter used by the encryption protocol. We show that an attacker can force these nonce resets by collecting and replaying retransmissions of message 3 of the 4-way handshake. By forcing nonce reuse in this manner, the encryption protocol can be attacked, e.g., packets can be replayed, decrypted, and/or forged. The same technique can also be used to attack the group key, PeerKey, TDLS, and fast BSS transition handshake.

https://www.krackattacks.com/

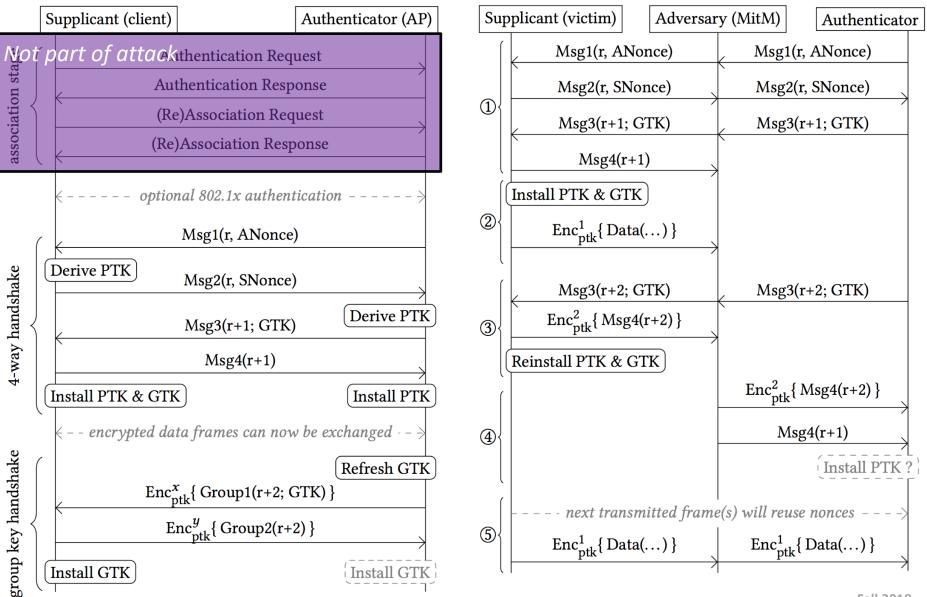
WPA2 KRACK

- Design flaw (oversight) in specification for *client* state machine
 - Does not affect APs
- Attacker obtains MiTM position between supplicant and authenticator
- Attacker uses MiTM position to trigger retransmissions of Msg3 by preventing Msg4 from arriving at the authenticator

MiTM on WiFi: *Channel-Based Attack*



Normal



WPA2 KRACK

- ✓ Same attack can be used elsewhere in 802.11
- Impact: If the attackers knows the *plaintext* (e.g. HTTP cookie) and the nonce is re-used, attacker can decrypt other frames that were encrypted with same nonce
 - Presumes a patient attacker with some knowledge of likely victim behavior
 - **Result:** TCP Hijacking attack
- Impact: Attacker does not recover password

Defense?

- Step 1: Patch your clients
- Step 2: Monitor for MiTM WiFi attacks
 - EvilAP_Defender can look for Evil Aps
 - Evil AP with a different BSSID address
 - Evil AP with the same BSSID as the legitimate AP but a different attribute (including: channel, cipher, privacy protocol, and authentication)
 - Evil AP with the same BSSID and attributes as the legitimate AP but different tagged parameter - mainly different OUI (tagged parameters are additional values sent along with the beacon frame)
 - ↗ Notify Admin (email) + DoS the malicious AP(!)
 - https://github.com/moha99sa/EvilAP_Defender/wiki

Packet Capture

92

Packet Capture

How do I capture packets from a WiFi network?

Plan "A"



Plan "A" Challenges

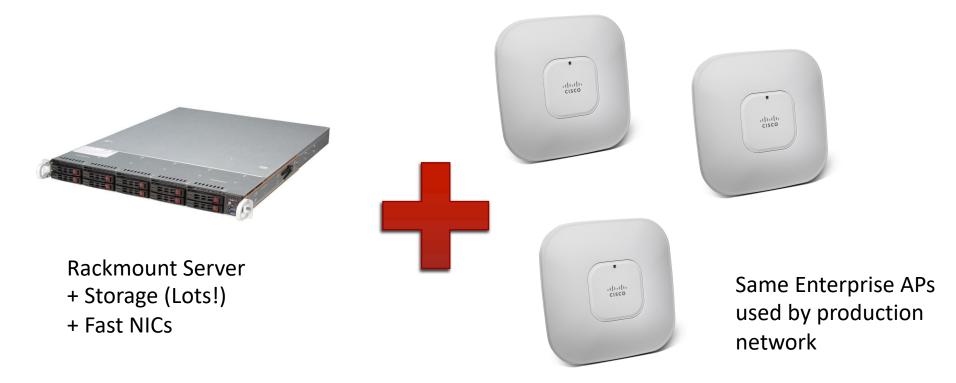
- Have to walk around the office carrying extra hardware
- USB WiFi adaptors are cheap
 - Low cost and low quality
- Hit or miss finding USB WiFi adaptors that support *monitor mode*
 - Manufacturers often use different chipsets in "same" product!
- Specifications
 - **7** Enterprise WiFi that you want to capture:
 - **7** 802.11ac
 - MU-MIMO 3x3 or more
 - **7** USB WiFi Adaptors used to monitor network:
 - 802.11a/b/g/n (ac maybe)
 - MIMO 2x2 at most (how many antennas do you see?)

95

Plan "A" Challenges

- Common problem:
 - Why don't I see my test pings in my capture?(I see plenty of beacon messages from my APs)
- Pings were sent over extended channel, or via MIMO path, or at a higher data rate than your USB WiFi adaptor supports

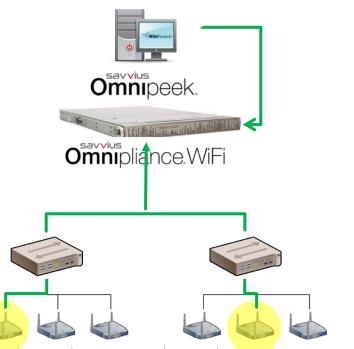
Plan "B"



- Example: Savvius Omnipliance product
 - No need to leave your desk!

How Omnipliance WiFi Works

- Using the WLAN controller UI, put the desired APs 1. in "sniffer" mode, and direct the packets to Omnipliance WiFi – packets start flowing
- Using Omnipeek, connect to Omnipliance WiFi and 2. configure your Remote Adapter capture
- Start the capture analysis (and storage) of all 3. packets from the APs begin immediately

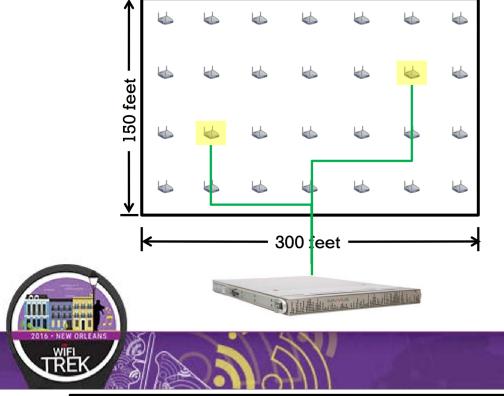




http://www.youtube.com/embed/BcWWeufQn7Q

https://www.cwnp.com/nola-ppt-pdfs/WedPresentations/Jay%20Savvius%20-%20Packet%20Capture%20and%20Analysis%20in%20the%20MU-MIMO%2011ac%20World.pdf

Highly Distributed, Multi-Campus Deployment



- Dense deployment ~ 28 APs per building floor
- 100's of building floors
- Reactive capture and analysis

https://www.cwnp.com/nola-ppt-pdfs/WedPresentations/Jay%20Savvius%20-%20Packet%20Capture%20and%20Analysis%20in%20the%20MU-MIMO%2011ac%20World.pdf

CU