SharkFest ‘16 Europe

Troubleshooting 802.11 with Monitoring Mode Finding Patterns in your pcaps

19.10.2016

Thomas Baudelet

#sf16eu

Freelance Network & Security Troubleshooter | iwaxx Sàrl

About

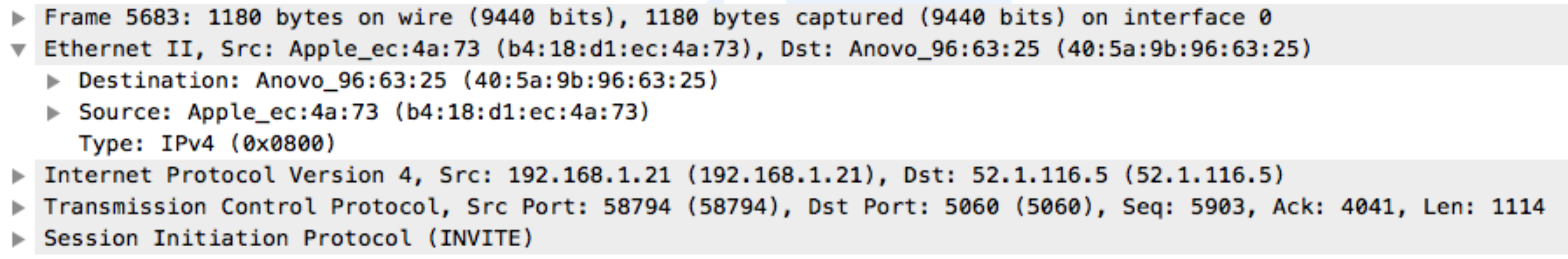
- Freelance Network & Security troubleshooter
- Professional services in Switzerland
- Wireshark trainer
  - Practical hands-on onsite trainings
  - Custom needs: proprietary protocols, Lua dissection, malware analysis
- Creator of Debookee, a macOS network analyzer
  - Includes Wireshark & Lua scripts
  - Wi-Fi Monitoring module

Wi-Fi Monitoring ≠ Promiscuous mode

Wi-Fi Monitoring

- Promiscuous mode (in case of Ethernet)
  - Not really a packet capture "mode", more an "option"
  - Capture packets destined to another layer 2 network interface
  - Available on Wire / Wireless
  - Connection state: cable plugged (!) / Wireless: associated to an AP
  - Lowest protocol seen: Ethernet (IEEE 802.3)
  - OSI model level: Data Link Layer (Mac)
  - Packets not seen: Bad FCS packets: may be dropped by the network interface before the capture library can be aware of them

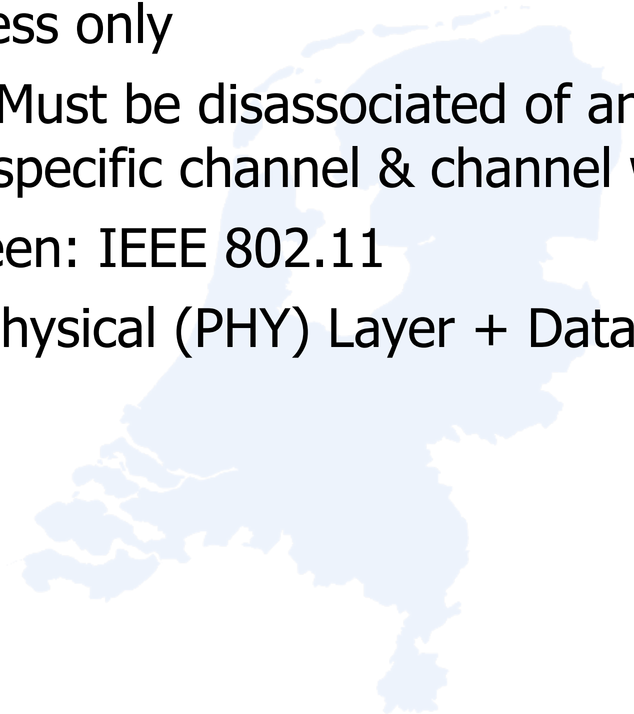
- Ethernet packet (not in Wi-Fi Monitoring mode)



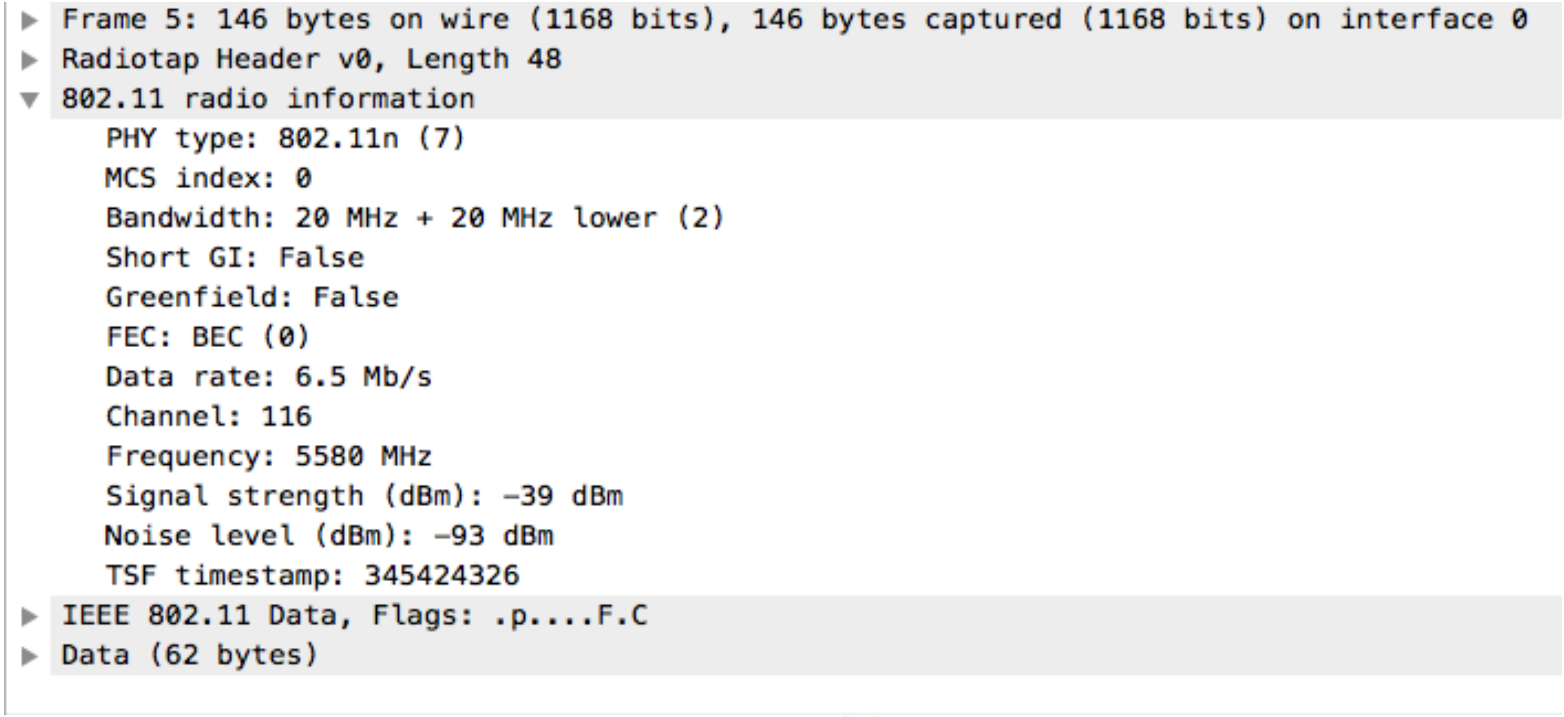
```
▶ Frame 5683: 1180 bytes on wire (9440 bits), 1180 bytes captured (9440 bits) on interface 0
▼ Ethernet II, Src: Apple_ec:4a:73 (b4:18:d1:ec:4a:73), Dst: Anovo_96:63:25 (40:5a:9b:96:63:25)
  ▶ Destination: Anovo_96:63:25 (40:5a:9b:96:63:25)
  ▶ Source: Apple_ec:4a:73 (b4:18:d1:ec:4a:73)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.1.21 (192.168.1.21), Dst: 52.1.116.5 (52.1.116.5)
▶ Transmission Control Protocol, Src Port: 58794 (58794), Dst Port: 5060 (5060), Seq: 5903, Ack: 4041, Len: 1114
▶ Session Initiation Protocol (INVITE)
```

Wi-Fi Monitoring

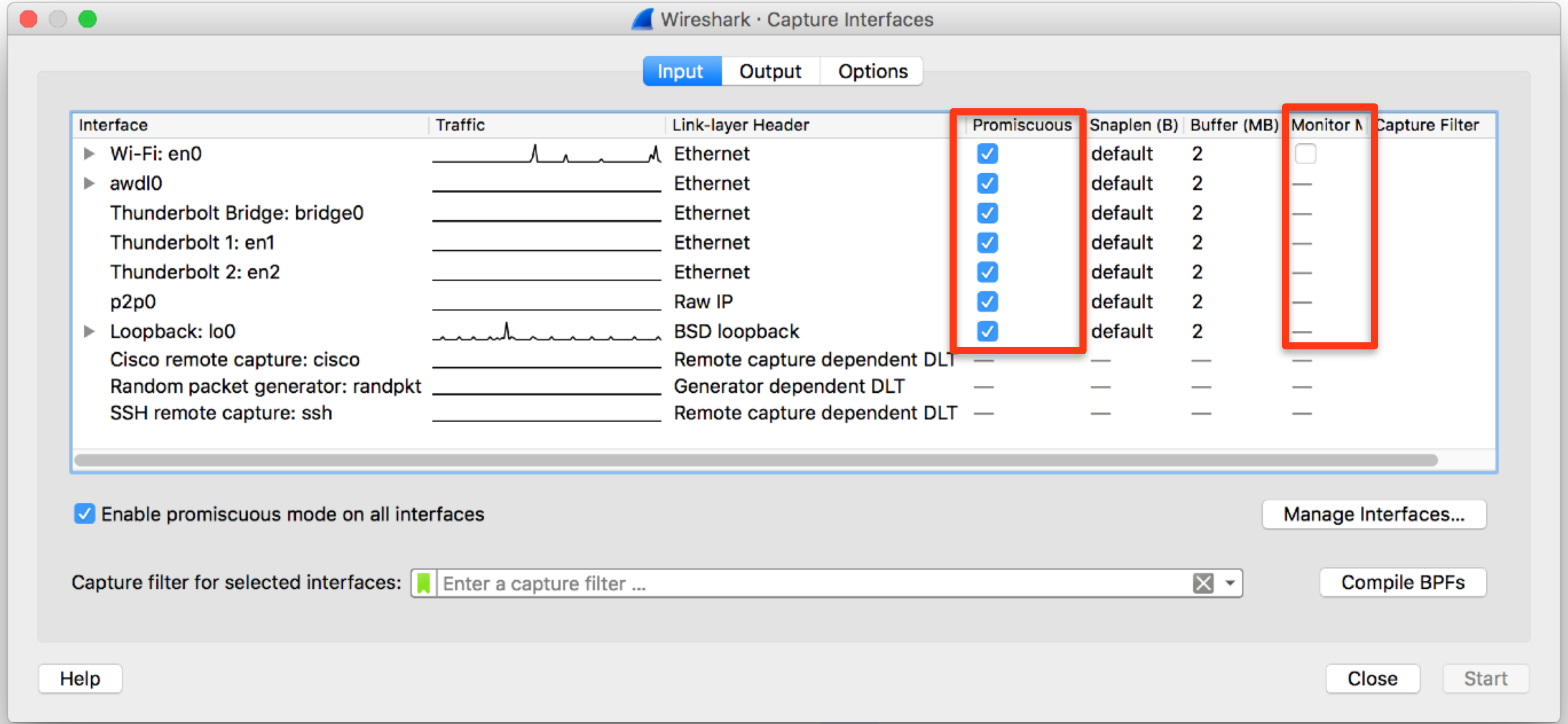
- Wi-Fi Monitoring mode
  - Available on Wireless only
  - Connection state: Must be disassociated of any network, but configured with a specific channel & channel width (20 – 80MHz)
  - Lowest protocol seen: IEEE 802.11
  - OSI model level: Physical (PHY) Layer + Data Link Layer (Mac)



- Data packet Wi-Fi Monitoring mode



```
▶ Frame 5: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
▶ Radiotap Header v0, Length 48
▼ 802.11 radio information
    PHY type: 802.11n (7)
    MCS index: 0
    Bandwidth: 20 MHz + 20 MHz lower (2)
    Short GI: False
    Greenfield: False
    FEC: BEC (0)
    Data rate: 6.5 Mb/s
    Channel: 116
    Frequency: 5580 MHz
    Signal strength (dBm): -39 dBm
    Noise level (dBm): -93 dBm
    TSF timestamp: 345424326
▶ IEEE 802.11 Data, Flags: .p....F.C
▶ Data (62 bytes)
```

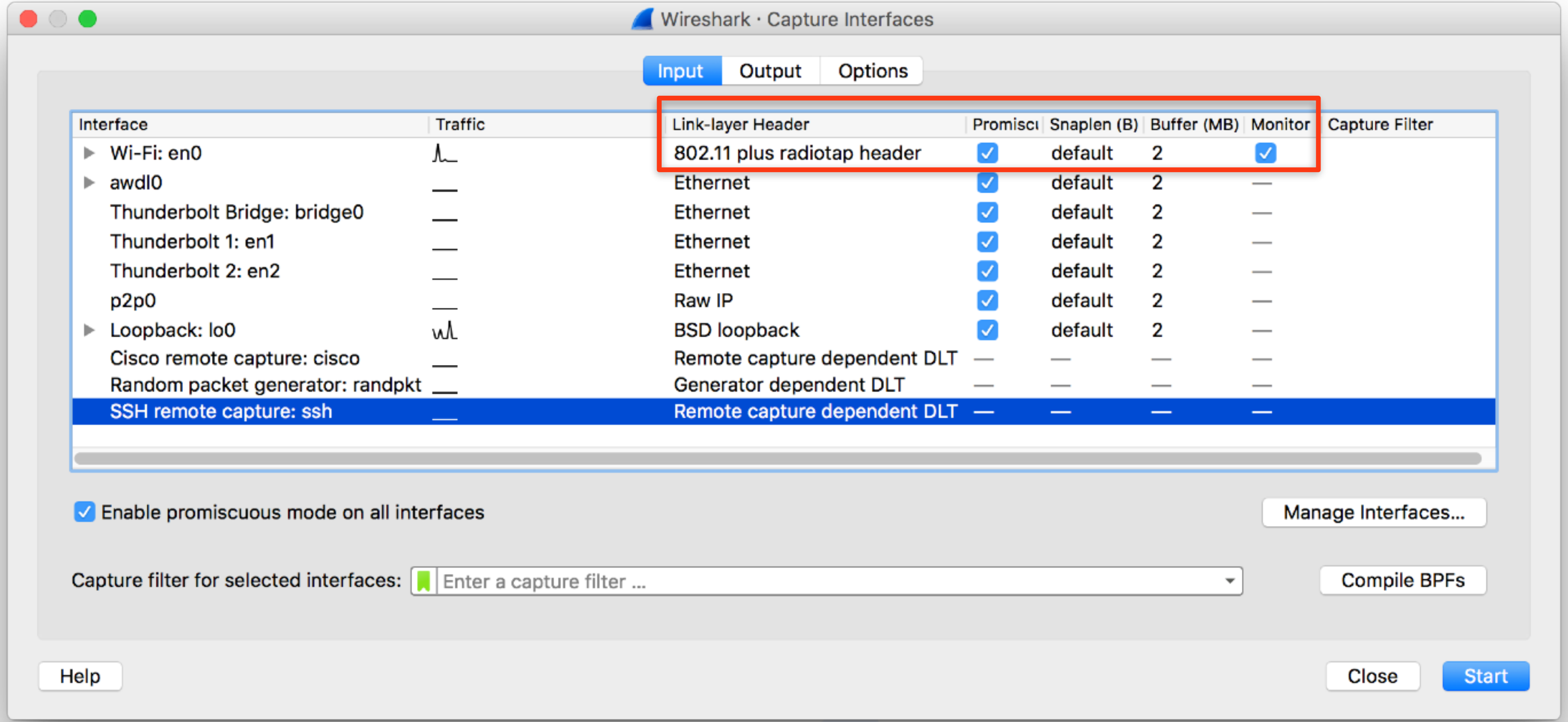


Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor M	Capture Filter
▶ Wi-Fi: en0		Ethernet	☑	default	2	☐	
▶ awdl0		Ethernet	☑	default	2	—	
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	
Thunderbolt 1: en1		Ethernet	☑	default	2	—	
Thunderbolt 2: en2		Ethernet	☑	default	2	—	
p2p0		Raw IP	☑	default	2	—	
▶ Loopback: lo0		BSD loopback	☑	default	2	—	
Cisco remote capture: cisco		Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh		Remote capture dependent DLT	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …



Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ Wi-Fi: en0		802.11 plus radiotap header	☑	default	2	☑	
▶ awdl0		Ethernet	☑	default	2	—	
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	
Thunderbolt 1: en1		Ethernet	☑	default	2	—	
Thunderbolt 2: en2		Ethernet	☑	default	2	—	
p2p0		Raw IP	☑	default	2	—	
▶ Loopback: lo0		BSD loopback	☑	default	2	—	
Cisco remote capture: cisco		Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh		Remote capture dependent DLT	—	—	—	—	

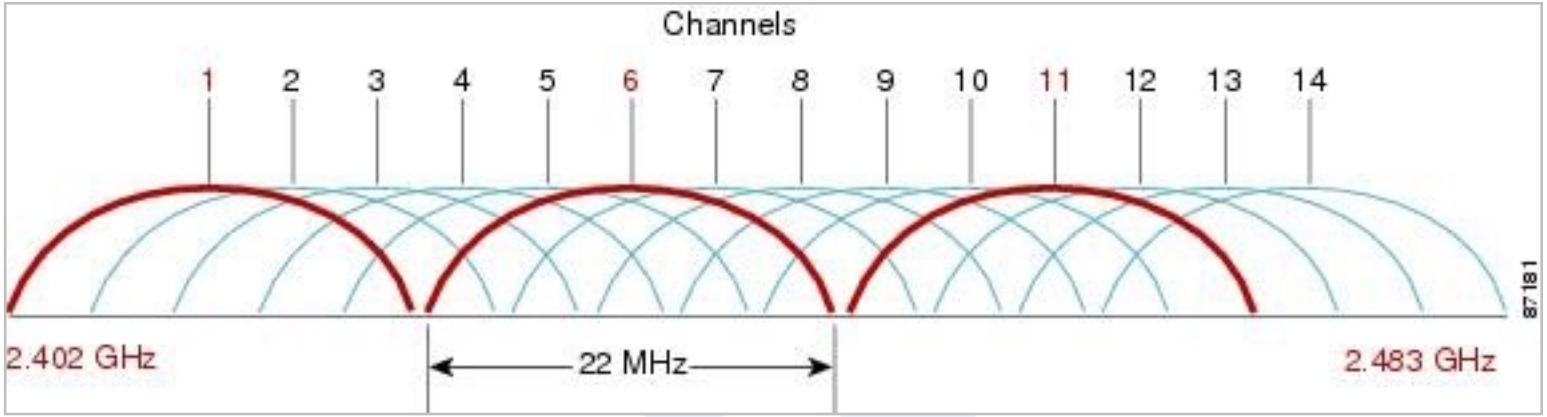
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

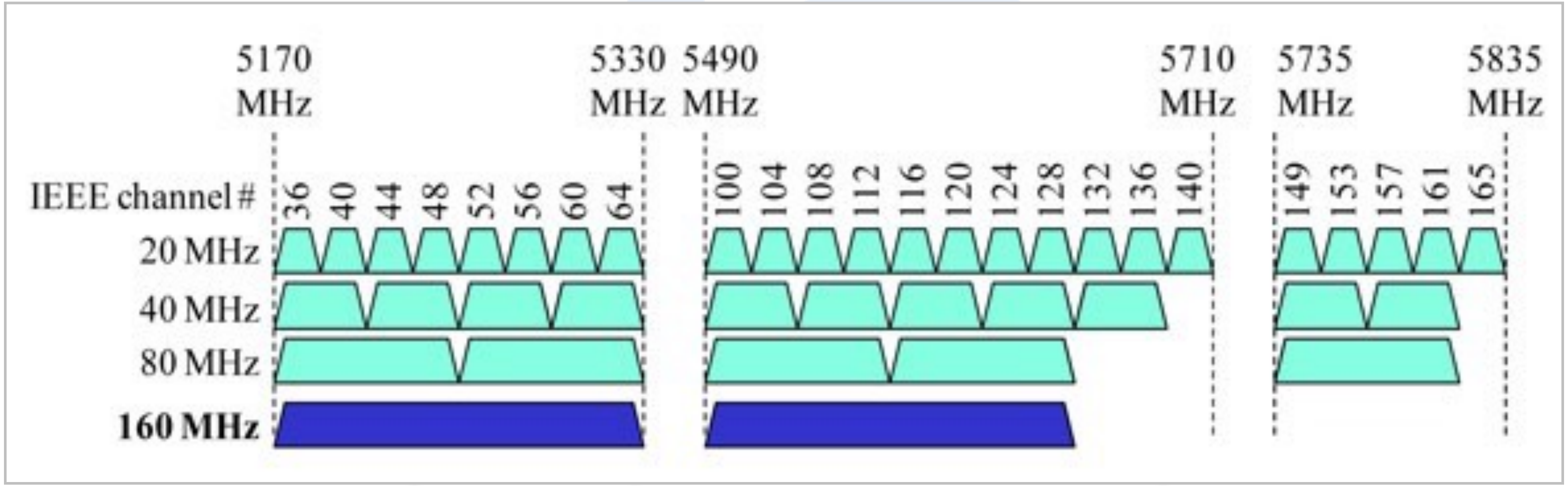
Practical theory of 802.11

- Characteristics of a Wi-Fi connection
  - Channel
    - 2.4 GHz - Channel 1 to 14 (common used: 1, 6, 11) - 802.11/b/g/ng
    - 5 GHz - Channel 36 to 165 - 802.11a/na/ac
  - Channel Width: 20, 40, 80 MHz (160 MHz soon with .11ac Wave 2)

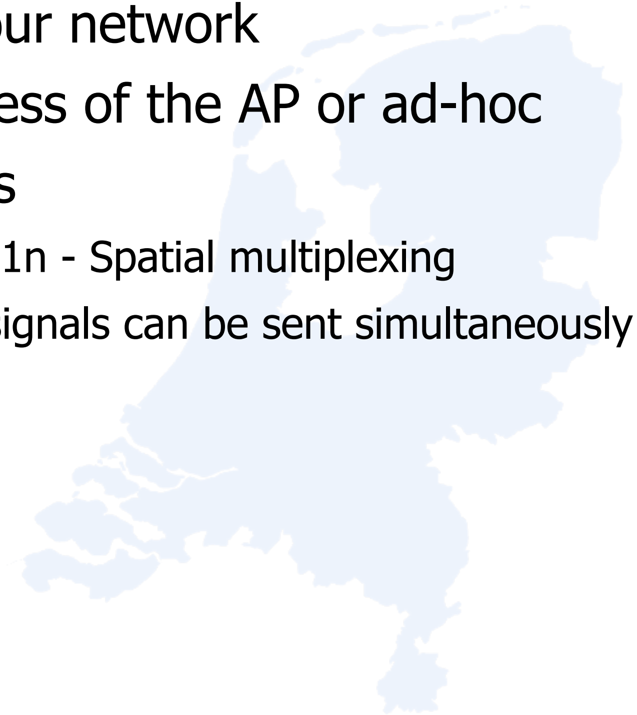
2.4 GHz


Channels
1
2
3
4
5
6
7
8
9
10
11
12
13
14
87181
2.402 GHz
22 MHz
2.483 GHz

5 GHz

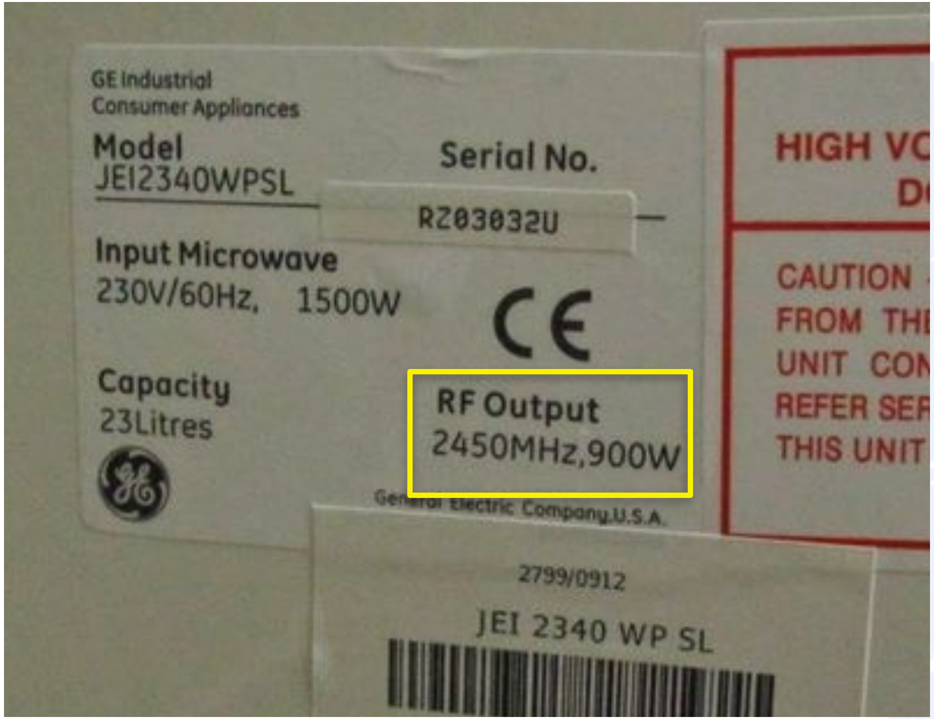

5170 MHz
5330 MHz
5490 MHz
5710 MHz
5735 MHz
5835 MHz
IEEE channel #
36
40
44
48
52
56
60
64
100
104
108
112
116
120
124
128
132
136
140
149
153
157
161
165
20 MHz
40 MHz
80 MHz
160 MHz

- Characteristics of a Wi-Fi connection
  - SSID - Name of your network
  - BSSID - MAC address of the AP or ad-hoc
  - Number of streams
    - Revolution of 802.11n - Spatial multiplexing
    - Independant data signals can be sent simultaneously by multiple TX antennas



- Characteristics of a Wi-Fi connection
  - TX Signal Power (emitted by the AP)
    - From 1dBm (1 mW) to 20 dBm (100 mW)
  - RX Signal Power (received by the Client)
    - -30 dBm (0.001 mW) - Client is touching the AP (signal divided by 100’000 directly when going out the AP)
    - -50 dBm (10 nW) - Excellent
    - -60 dBm (1 nW) - Good
    - -70 dBm (100 pW) - Time to roam
    - -80 dBm (10 pW) - Time to cable?
    - -90 dBm (1 pW - 1 billion of mW) - Common noise

- Let's buy a Microwave Oven



GE Industrial
Consumer Appliances

Model
JEI2340WPSL

Serial No.
RZ03032U

Input Microwave
230V/60Hz, 1500W

Capacity
23Litres

RF Output
2450MHz,900W

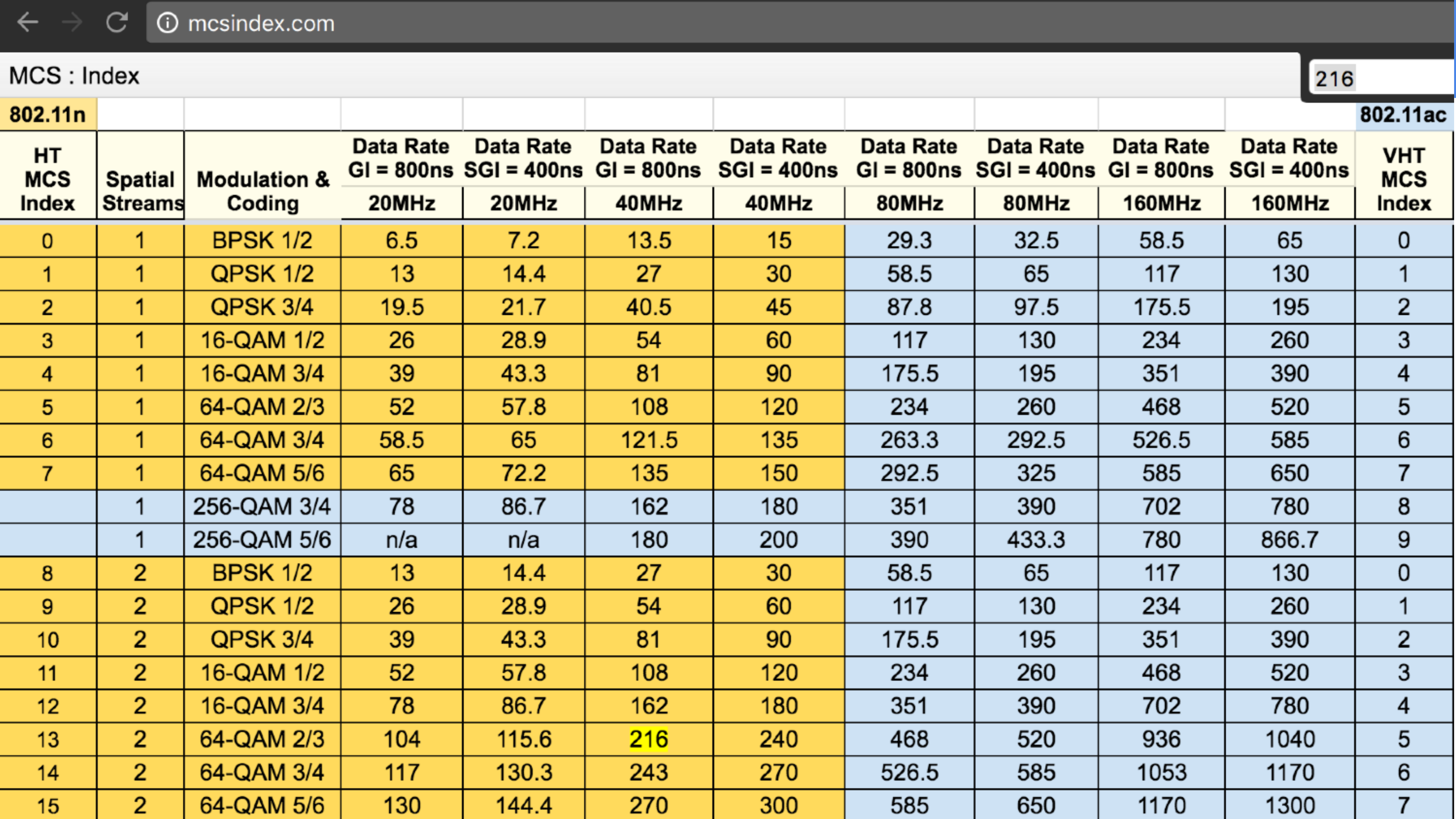
General Electric Company,U.S.A.

2799/0912
JEI 2340 WP SL

Let's compare
900kg and 1ng

Wait… Where is speed? Gimme Mb/s

- Speed is the correlation of:
  - Channel width (20, 40, 80, 160 MHz)
  - Number of streams (1-3, coming 4 they say in blogs/coffee machine)
  - Guard Interval (Short or Long - Time interval between each frames)
  - Modulation or MCS index
- Speed is set per packet, not once per connection
- Your best friend: http://mcsindex.com



MCS : Index

216

802.11n											802.11ac
HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns	VHT MCS Index
			20MHz	20MHz	40MHz	40MHz	80MHz	80MHz	160MHz	160MHz	
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26	28.9	54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9
8	2	BPSK 1/2	13	14.4	27	30	58.5	65	117	130	0
9	2	QPSK 1/2	26	28.9	54	60	117	130	234	260	1
10	2	QPSK 3/4	39	43.3	81	90	175.5	195	351	390	2
11	2	16-QAM 1/2	52	57.8	108	120	234	260	468	520	3
12	2	16-QAM 3/4	78	86.7	162	180	351	390	702	780	4
13	2	64-QAM 2/3	104	115.6	216	240	468	520	936	1040	5
14	2	64-QAM 3/4	117	130.3	243	270	526.5	585	1053	1170	6
15	2	64-QAM 5/6	130	144.4	270	300	585	650	1170	1300	7

How do I set Monitoring Mode?

Wi-Fi Monitoring

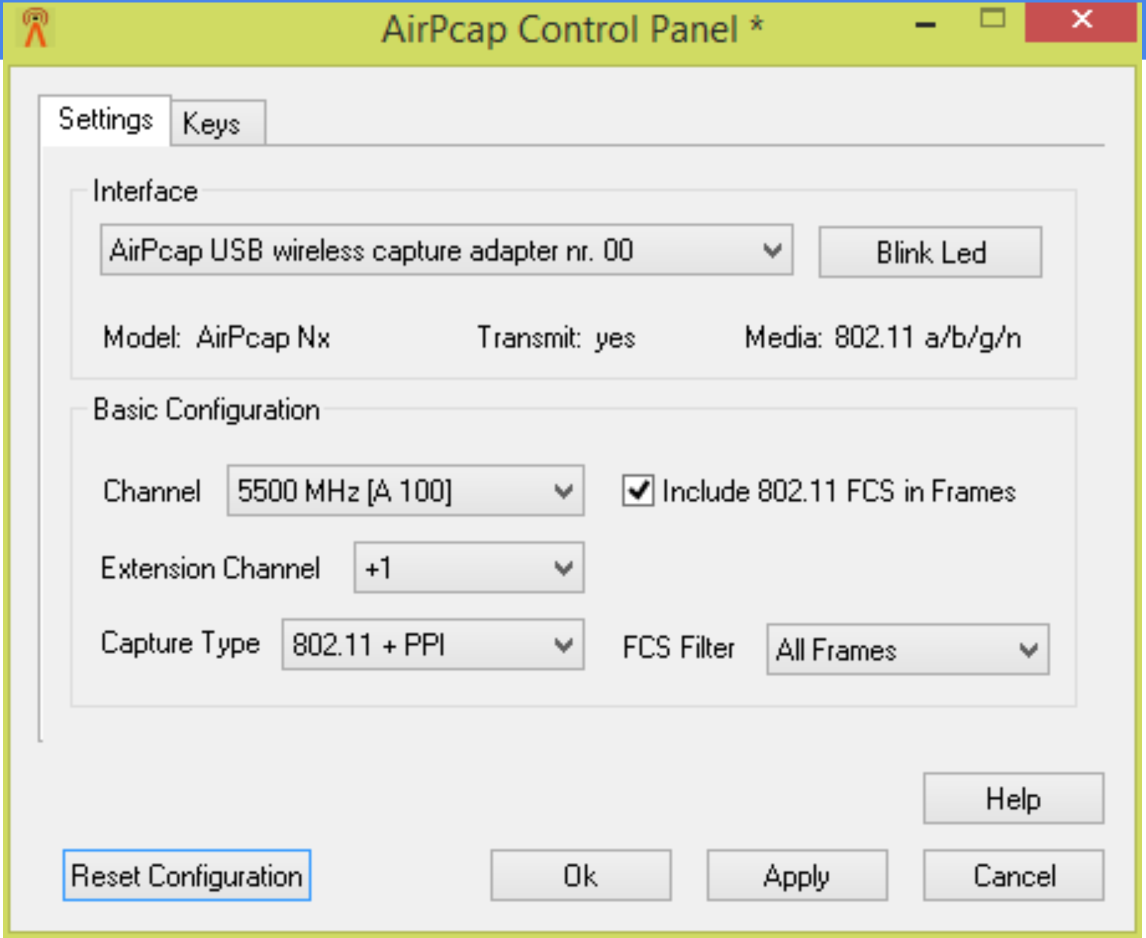
- Details for all OS: talk of Thomas d'Otreppe at SharkFest 16 US
- Linux
  - Natively with command lines or in Wireshark directly (free)
- macOS
  - Natively with command line or in Wireshark directly (free)
  - also best hardware: 802.11ac 3x3

Wi-Fi Monitoring

- Windows
  - External dongles:
    - Riverbed external Airpcap dongles: 802.11n 2x2 ($700!)

      Warning: Windows 7 + USB3 = BSOD!
    - Savvius external dongles: 802.11n 3x3 ($60) - 802.11ac 2x2 ($150)

      Works with Omnipeek only, not Wireshark or need a trick with npcap
  - Using your internal Wi-Fi interface or external dongles:
    - Acrylic Wi-Fi Professional: NDIS 6 / Airpcap drivers ($40)
    - npcap: NDIS 6 (free)
    - *Does your interface support NDIS 6? Driver support your interfaces? Support of 5GHz? Ability to configure channel bandwidth?*



Interface

AirPcap USB wireless capture adapter nr. 00

Model: AirPcap Nx

Transmit: yes

Media: 802.11 a/b/g/n

Basic Configuration

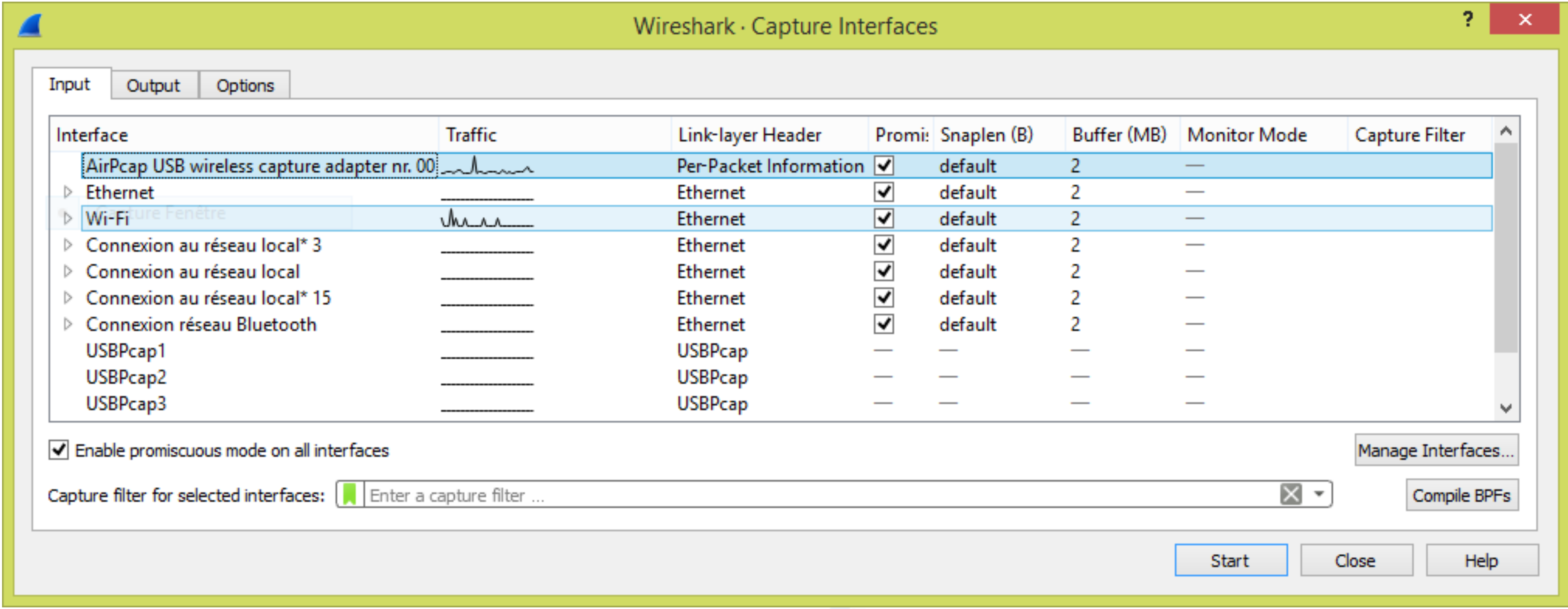
Channel: 5500 MHz [A 100]

☑ Include 802.11 FCS in Frames

Extension Channel: +1

Capture Type: 802.11 + PPI

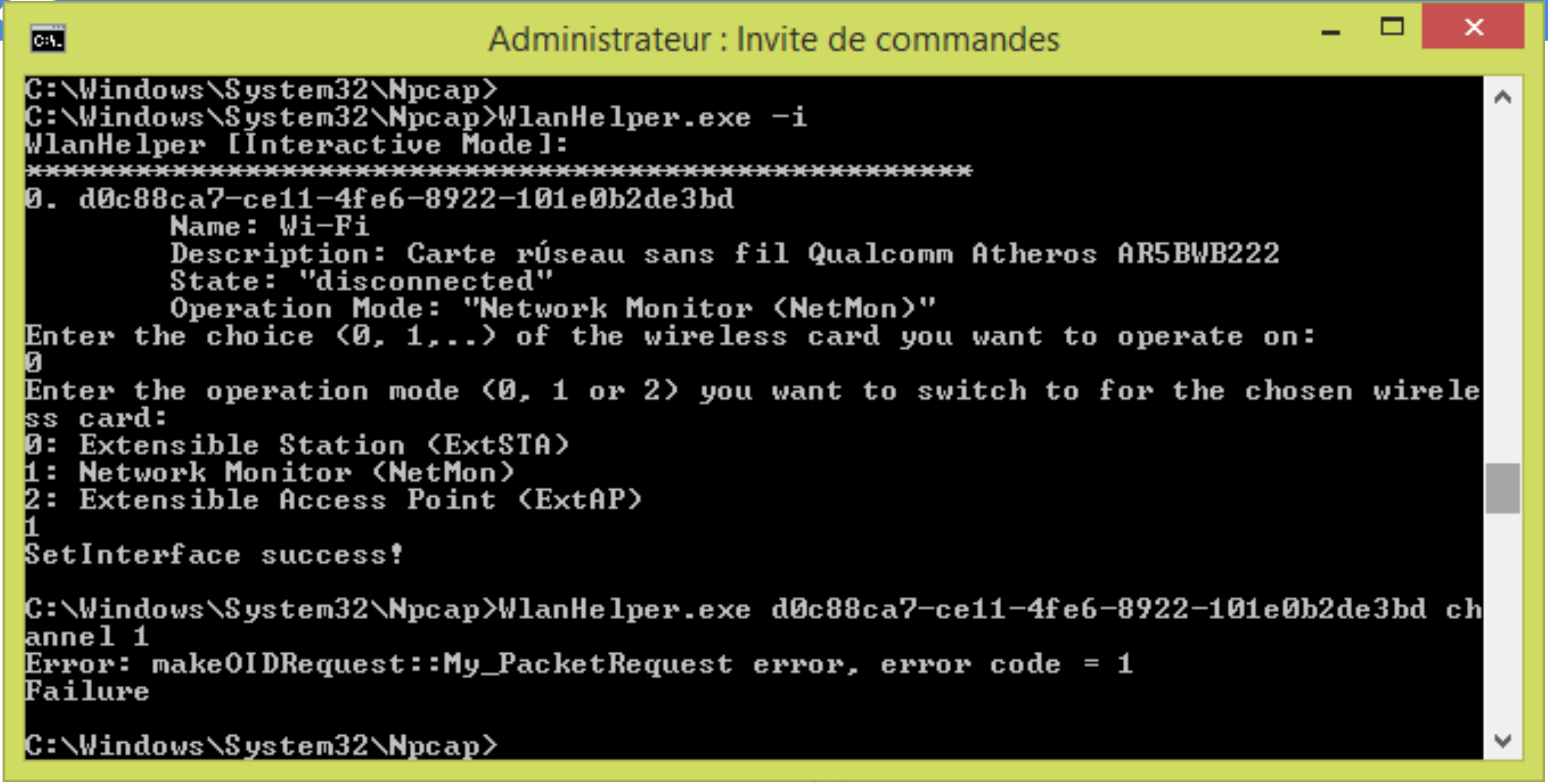
FCS Filter: All Frames



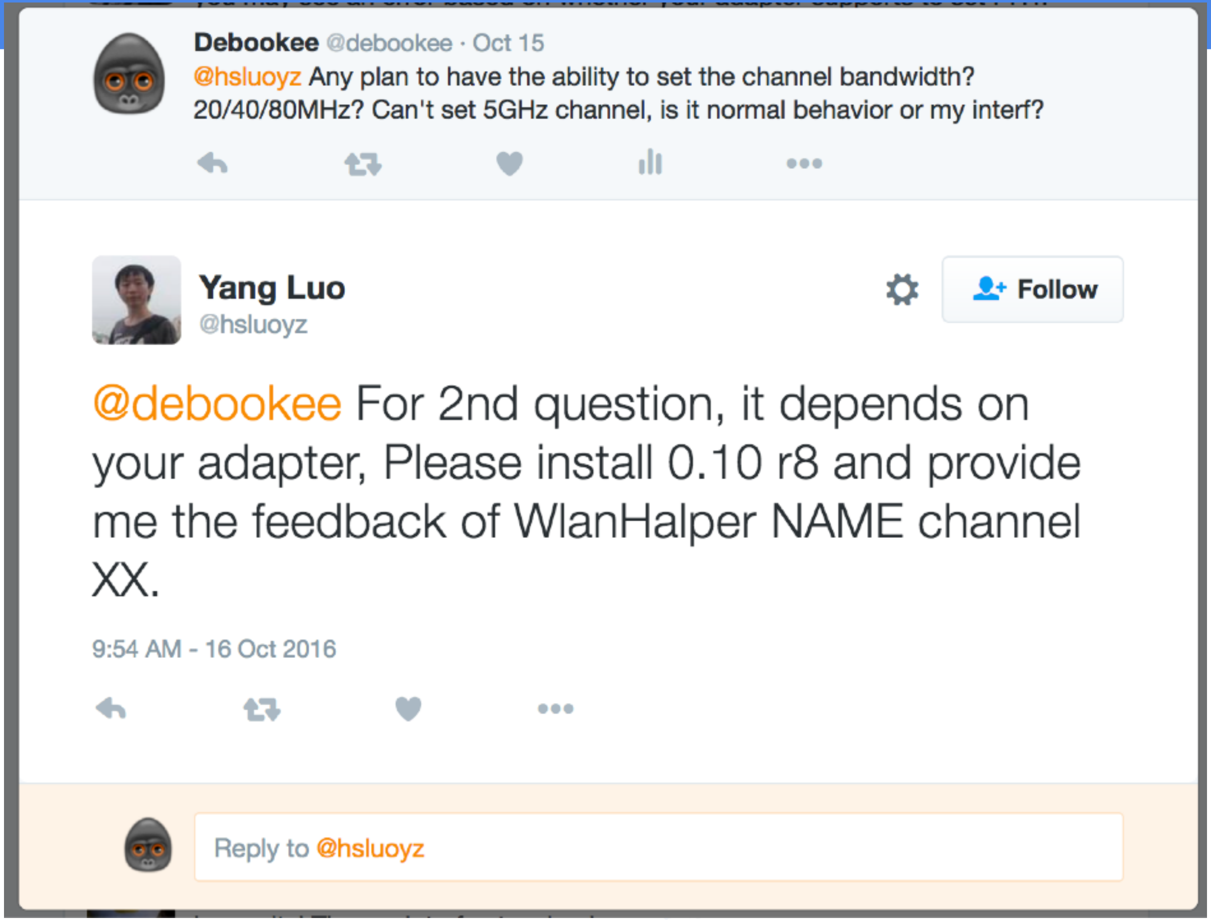
Interface	Traffic	Link-layer Header	Promi:	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
AirPcap USB wireless capture adapter nr. 00		Per-Packet Information	☑	default	2	—	
▷ Ethernet		Ethernet	☑	default	2	—	
▷ Wi-Fi		Ethernet	☑	default	2	—	
▷ Connexion au réseau local* 3		Ethernet	☑	default	2	—	
▷ Connexion au réseau local		Ethernet	☑	default	2	—	
▷ Connexion au réseau local* 15		Ethernet	☑	default	2	—	
▷ Connexion réseau Bluetooth		Ethernet	☑	default	2	—	
USBPcap1		USBPcap	—	—	—	—	
USBPcap2		USBPcap	—	—	—	—	
USBPcap3		USBPcap	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...



```
C:\Windows\System32\Npcap>
C:\Windows\System32\Npcap>WlanHelper.exe -i
WlanHelper [Interactive Mode]:
*****************************************************
0. d0c88ca7-ce11-4fe6-8922-101e0b2de3bd
        Name: Wi-Fi
        Description: Carte rúseau sans fil Qualcomm Atheros AR5BWB222
        State: "disconnected"
        Operation Mode: "Network Monitor (NetMon)"
Enter the choice (0, 1,...) of the wireless card you want to operate on:
0
Enter the operation mode (0, 1 or 2) you want to switch to for the chosen wirele
ss card:
0: Extensible Station (ExtSTA)
1: Network Monitor (NetMon)
2: Extensible Access Point (ExtAP)
1
SetInterface success!

C:\Windows\System32\Npcap>WlanHelper.exe d0c88ca7-ce11-4fe6-8922-101e0b2de3bd ch
annel 1
Error: makeOIDRequest::My_PacketRequest error, error code = 1
Failure

C:\Windows\System32\Npcap>
```



Debookee @debookee · Oct 15

@hsluoyz Any plan to have the ability to set the channel bandwidth? 20/40/80MHz? Can't set 5GHz channel, is it normal behavior or my interf?

Yang Luo
@hsluoyz

@debookee For 2nd question, it depends on your adapter, Please install 0.10 r8 and provide me the feedback of WlanHalper NAME channel XX.

9:54 AM - 16 Oct 2016

Ok, got hw, what should I do?

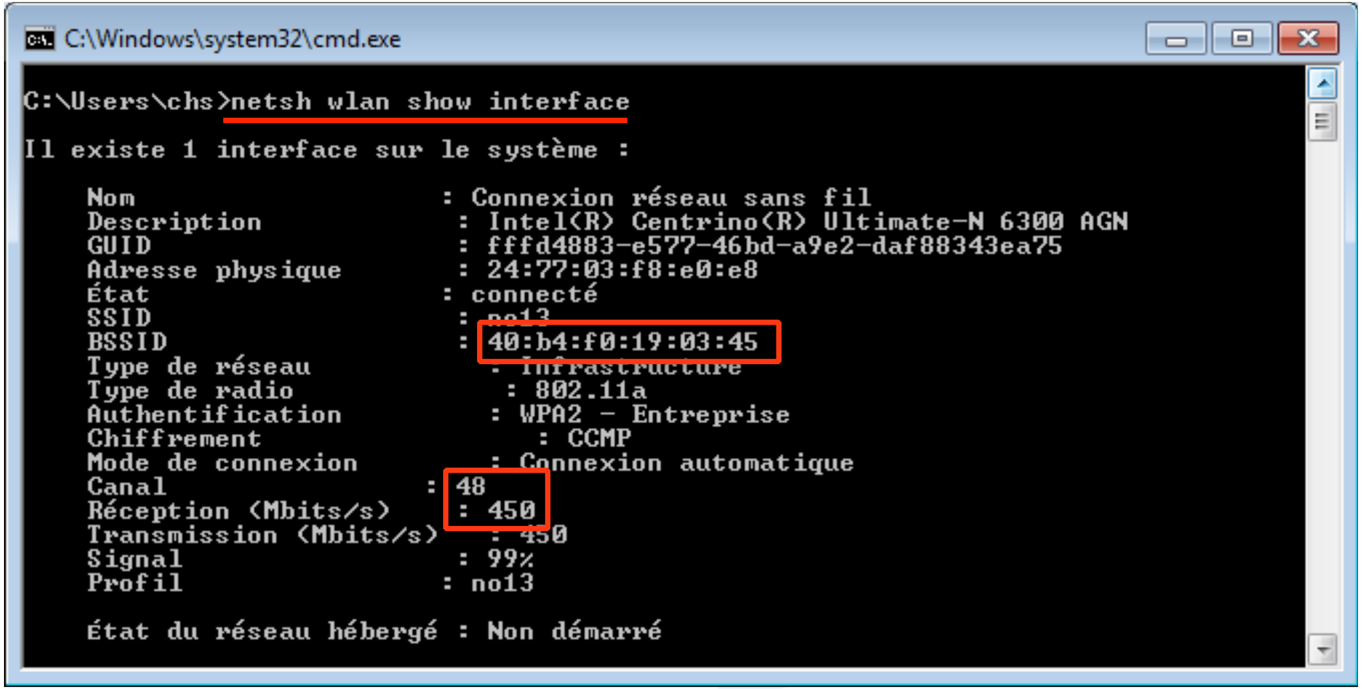
Ok, got hw, what should I do?
-> On which channel is your device?

Wi-Fi Monitoring

- A Wi-Fi scanner will help if only 1 BSSID per SSID
- If lot of APs with same SSID, must know where your device is associated

Wi-Fi Monitoring

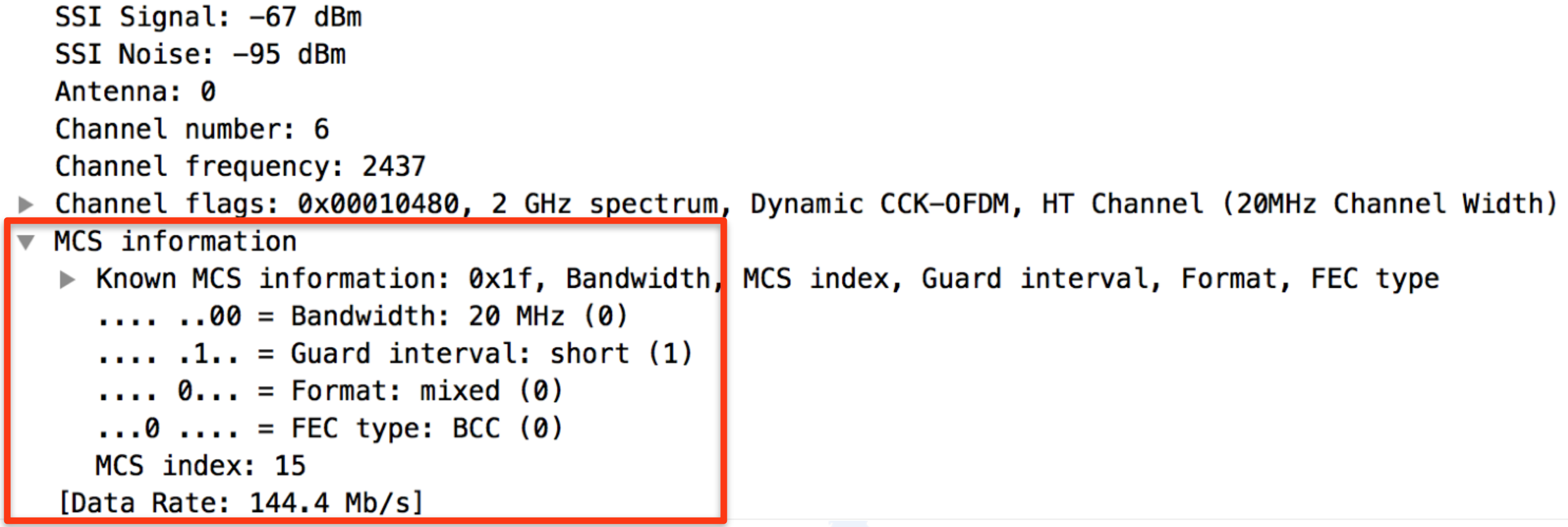
- netsh wlan show interface



```
C:\Users\chs>netsh wlan show interface

Il existe 1 interface sur le système :

    Nom                    : Connexion réseau sans fil
    Description             : Intel(R) Centrino(R) Ultimate-N 6300 AGN
    GUID                    : fffd4883-e577-46bd-a9e2-daf88343ea75
    Adresse physique        : 24:77:03:f8:e0:e8
    État                   : connecté
    SSID                    : no13
    BSSID                   : 40:b4:f0:19:03:45
    Type de réseau            : Infrastructure
    Type de radio              : 802.11a
    Authentification          : WPA2 - Entreprise
    Chiffrement                  : CCMP
    Mode de connexion         : Connexion automatique
    Canal                 : 48
    Réception (Mbits/s)     : 450
    Transmission (Mbits/s)    : 450
    Signal                  : 99%
    Profil                 : no13

    État du réseau hébergé : Non démarré
```

Back to pcap - Lab#1
Radiotap / PPI headers

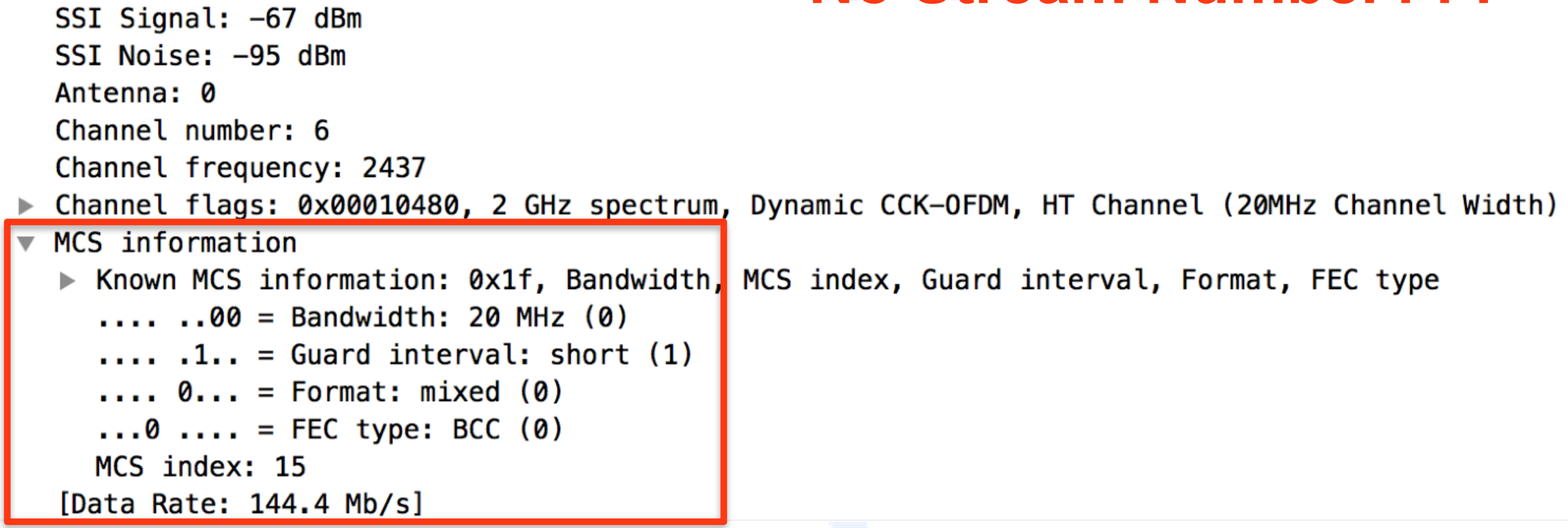
- Back to pcap



```
  SSI Signal: -67 dBm
  SSI Noise: -95 dBm
  Antenna: 0
  Channel number: 6
  Channel frequency: 2437
▶ Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)
▼ MCS information
  ▶ Known MCS information: 0x1f, Bandwidth, MCS index, Guard interval, Format, FEC type
    .... ..00 = Bandwidth: 20 MHz (0)
    .... .1.. = Guard interval: short (1)
    .... 0... = Format: mixed (0)
    ...0 .... = FEC type: BCC (0)
    MCS index: 15
  [Data Rate: 144.4 Mb/s]
```

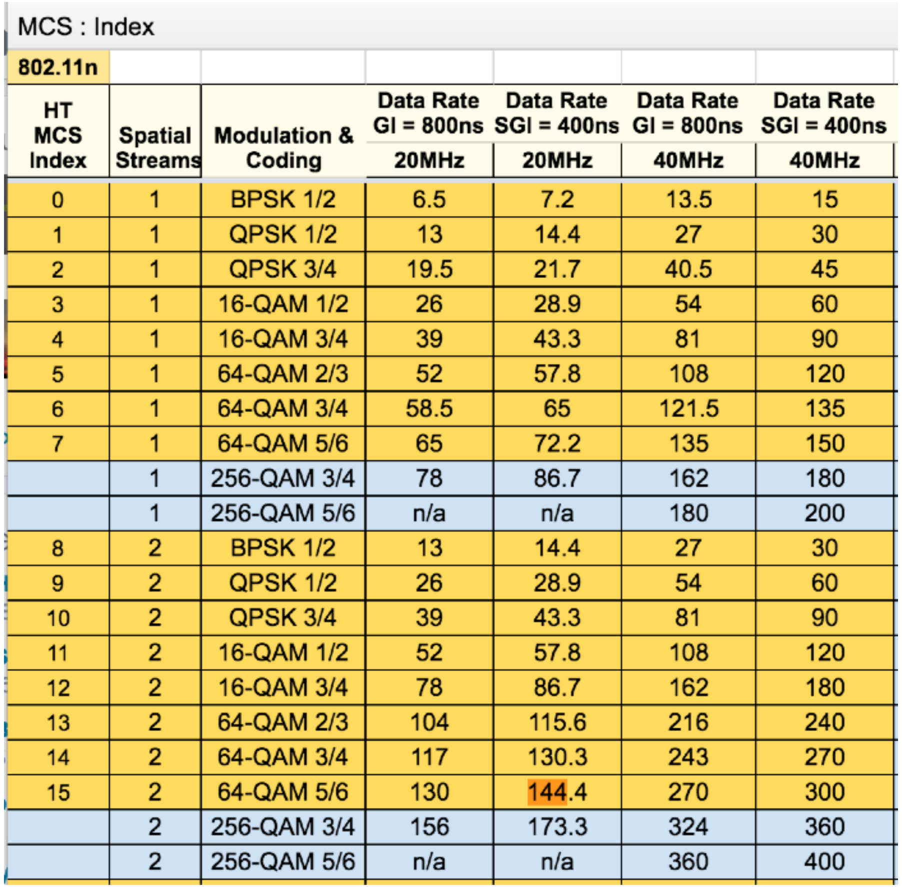
- Back to pcap

No Stream Number???



```
  SSI Signal: -67 dBm
  SSI Noise: -95 dBm
  Antenna: 0
  Channel number: 6
  Channel frequency: 2437
▶ Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)
▼ MCS information
  ▶ Known MCS information: 0x1f, Bandwidth, MCS index, Guard interval, Format, FEC type
    .... ..00 = Bandwidth: 20 MHz (0)
    .... .1.. = Guard interval: short (1)
    .... 0... = Format: mixed (0)
    ...0 .... = FEC type: BCC (0)
    MCS index: 15
   [Data Rate: 144.4 Mb/s]
```

mcsindex.com pro tip: CTRL+F is your friend

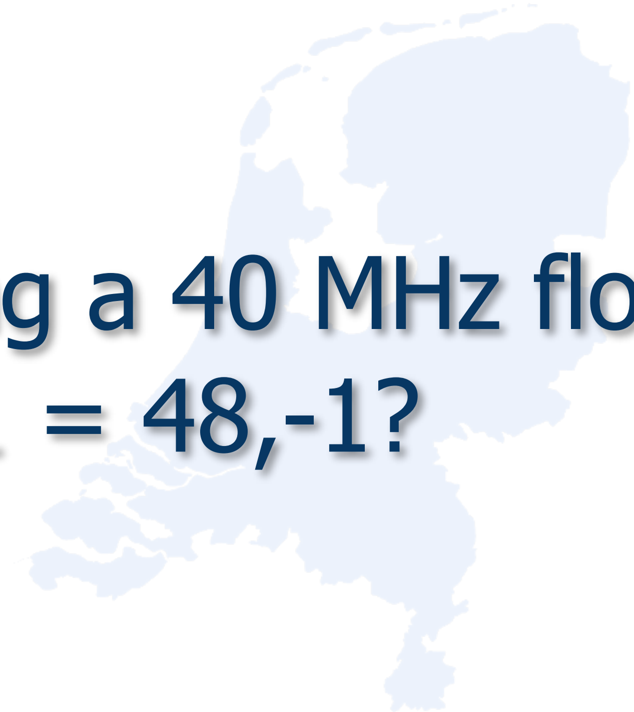


MCS : Index

802.11n

HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns	Data Rate SGI = 400ns	Data Rate GI = 800ns	Data Rate SGI = 400ns
			20MHz	20MHz	40MHz	40MHz
0	1	BPSK 1/2	6.5	7.2	13.5	15
1	1	QPSK 1/2	13	14.4	27	30
2	1	QPSK 3/4	19.5	21.7	40.5	45
3	1	16-QAM 1/2	26	28.9	54	60
4	1	16-QAM 3/4	39	43.3	81	90
5	1	64-QAM 2/3	52	57.8	108	120
6	1	64-QAM 3/4	58.5	65	121.5	135
7	1	64-QAM 5/6	65	72.2	135	150
	1	256-QAM 3/4	78	86.7	162	180
	1	256-QAM 5/6	n/a	n/a	180	200
8	2	BPSK 1/2	13	14.4	27	30
9	2	QPSK 1/2	26	28.9	54	60
10	2	QPSK 3/4	39	43.3	81	90
11	2	16-QAM 1/2	52	57.8	108	120
12	2	16-QAM 3/4	78	86.7	162	180
13	2	64-QAM 2/3	104	115.6	216	240
14	2	64-QAM 3/4	117	130.3	243	270
15	2	64-QAM 5/6	130	144.4	270	300
	2	256-QAM 3/4	156	173.3	324	360
	2	256-QAM 5/6	n/a	n/a	360	400

Lab#2
Monitoring with Airpcap dongles



Lab#3

-> Capturing a 40 MHz flow at 20 MHz?

-> Is 44,+1 = 48,-1?

Lab#4
Why don't I see any data packets?

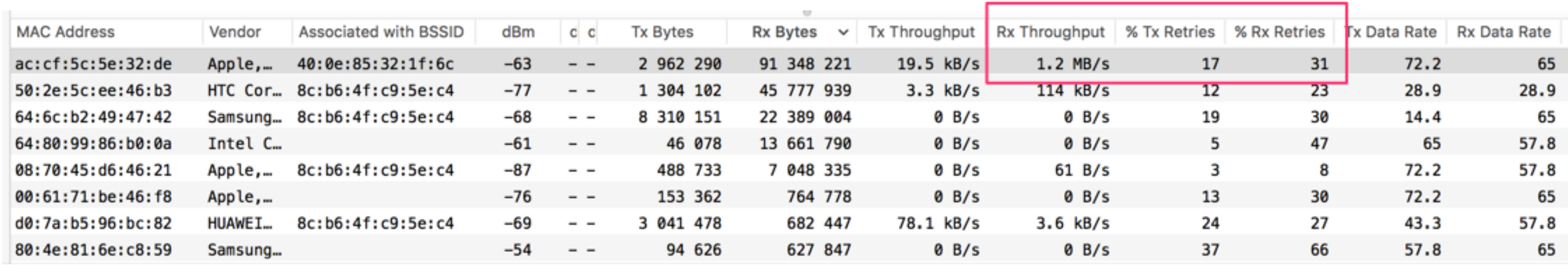
Why is my Wi-Fi slow?
Some indicators

- Is FCS a good metric in a Wi-Fi Monitoring capture?
  - NO!
  - FCS is a subjective metric of the monitoring station
  - You captured bad FCS seen by your monitoring station, not the client device
  - Lot of bad FCS if you're too close to the client
    - Radio orthogonality / Signal too strong / ???
    - Don't capture too close a client (< 2m)

- Use 802.11 Retries
  - wlan.fc.retries == 1
  - Set by the 802.11 device if previous data packet not ACKed
  - Check both Tx and Rx retries (<10-15% in a pro environment)
  - if Rx & Tx retries are high -> Check Layer 1 / Co-Channel Interferences
  - if Rx Retries >>> Tx Retries -> Power Mismatch (common with mobiles & professionnal Access Points)

- Lab#5
  - wlan.da == e0:2c:b2:3c:88:35 && wlan.fc.type == 2 - 382 pkts
  - wlan.da == e0:2c:b2:3c:88:35 && wlan.fc.type == 2 && wlan.fc.retry == 1 - 297 pkts
  - 78% Rx retries!

In Debookee



MAC Address	Vendor	Associated with BSSID	dBm	c	c	Tx Bytes	Rx Bytes	Tx Throughput	Rx Throughput	% Tx Retries	% Rx Retries	Tx Data Rate	Rx Data Rate
ac:cf:5c:5e:32:de	Apple,…	40:0e:85:32:1f:6c	-63	-	-	2 962 290	91 348 221	19.5 kB/s	1.2 MB/s	17	31	72.2	65
50:2e:5c:ee:46:b3	HTC Cor…	8c:b6:4f:c9:5e:c4	-77	-	-	1 304 102	45 777 939	3.3 kB/s	114 kB/s	12	23	28.9	28.9
64:6c:b2:49:47:42	Samsung…	8c:b6:4f:c9:5e:c4	-68	-	-	8 310 151	22 389 004	0 B/s	0 B/s	19	30	14.4	65
64:80:99:86:b0:0a	Intel C…		-61	-	-	46 078	13 661 790	0 B/s	0 B/s	5	47	65	57.8
08:70:45:d6:46:21	Apple,…	8c:b6:4f:c9:5e:c4	-87	-	-	488 733	7 048 335	0 B/s	61 B/s	3	8	72.2	57.8
00:61:71:be:46:f8	Apple,…		-76	-	-	153 362	764 778	0 B/s	0 B/s	13	30	72.2	65
d0:7a:b5:96:bc:82	HUAWEI…	8c:b6:4f:c9:5e:c4	-69	-	-	3 041 478	682 447	78.1 kB/s	3.6 kB/s	24	27	43.3	57.8
80:4e:81:6e:c8:59	Samsung…		-54	-	-	94 626	627 847	0 B/s	0 B/s	37	66	57.8	65

Why is my Wi-Fi slow? Practical theory of 802.11 #2

- What does a device before sending a packet?
  - Listen in the air for energy / ED (Energy Detection)
    - Is a microwave oven currently speaking?
    - Am I hearing bad CRC frames as noise?
  - Listen in the air for 802.11 frames / CS (Carrier Sense)
    - Save the NAV timer of heard packet (indicate when media will be freed)
  - When free, calculate a random number and wait while decreasing it
  - If media busy meanwhile, put random timer on hold
  - When random timer ends, if clear, send packet(s)
  - Wait for ACK, else resend packet with wlan.fc.retry = 1

The most important WLAN processes

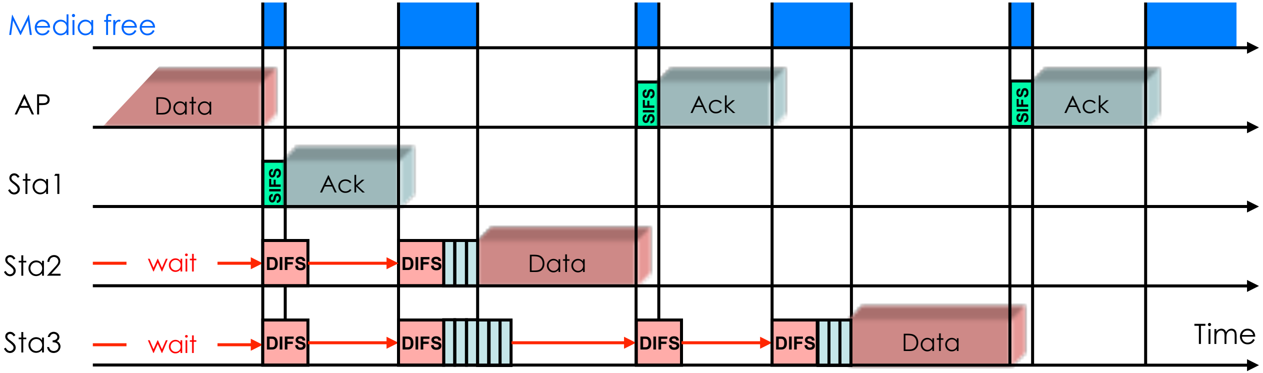
Access Control with CSMA/CA

CSMA/CA offers different Inter Frame Spaces (IFS) to control media access:

SIFS (Short Inter Frame Space) 802.11b/g = 10 µs 802.11a = 16 µs

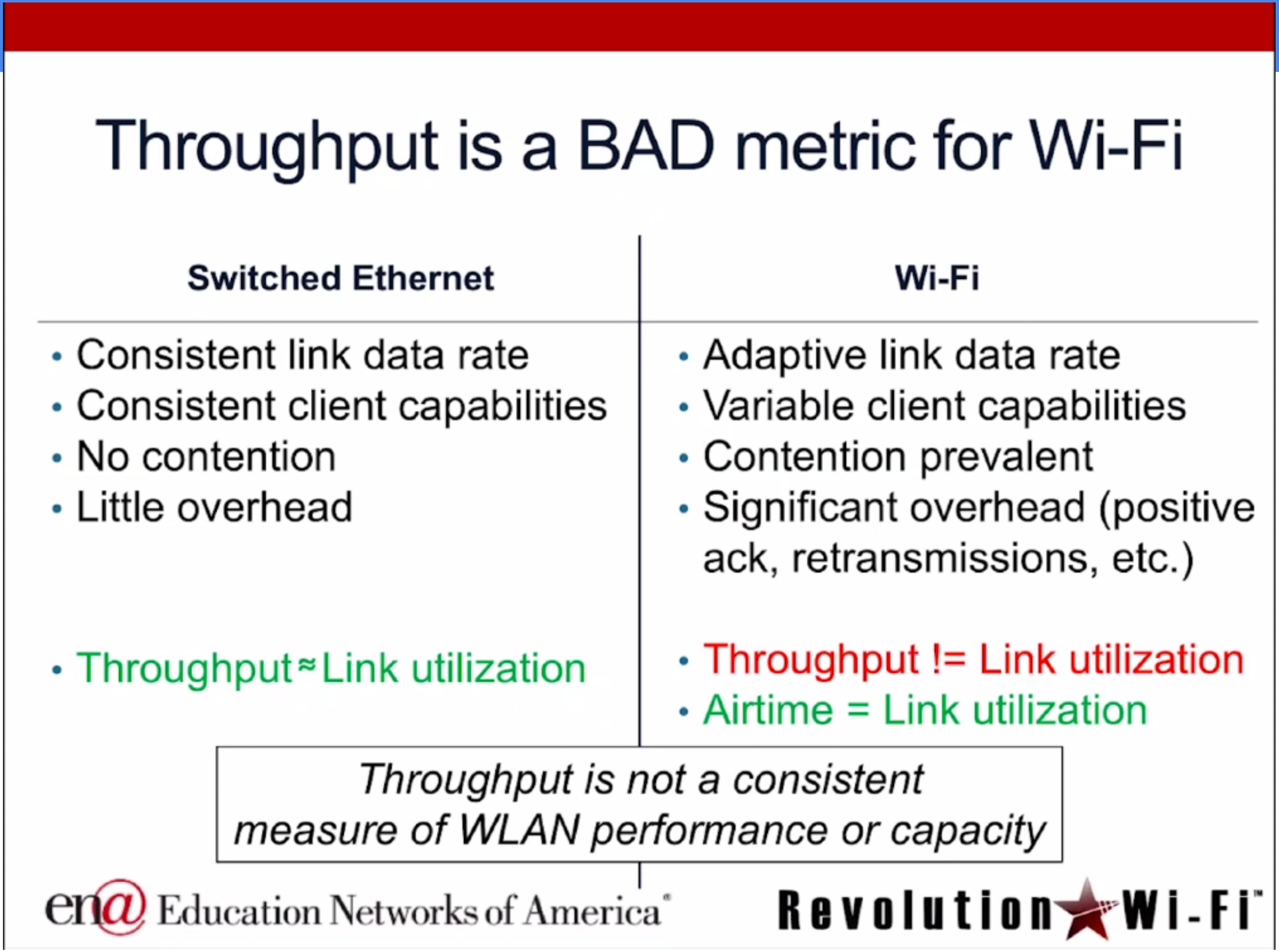
DIFS (DCF Inter Frame Space) (2x Slot time + SIFS) 802.11b=50µs 802.11g=28µs 802.11a=34µs

Slot Time 802.11b = 20 µs (max. 31x) **Short Slot Time** 802.11a/g = 9 µs (max. 15x)



- Stations can send anytime if media is free, but hold back if media is busy.
- If air becomes free, stations are waiting DIFS and a random number of Slot Times before sending
- Receiving stations verify Frame Check Sequence and if OK are sending ACK after SIFS

Forget Throughput - Think Airtime



Throughput is a BAD metric for Wi-Fi

Switched Ethernet	Wi-Fi
• Consistent link data rate	• Adaptive link data rate
• Consistent client capabilities	• Variable client capabilities
• No contention	• Contention prevalent
• Little overhead	• Significant overhead (positive ack, retransmissions, etc.)
• Throughput≈Link utilization	• Throughput != Link utilization • Airtime = Link utilization

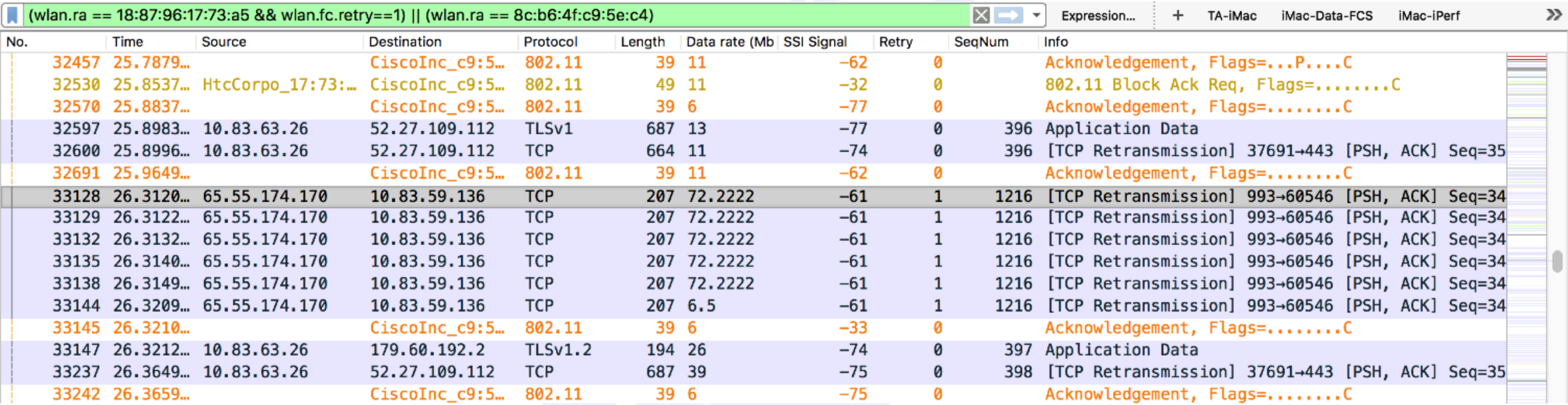
Throughput is not a consistent measure of WLAN performance or capacity

ena Education Networks of America

Revolution Wi-Fi

http://www.revolutionwifi.net/

Lab#6
Why the device doesn't ACK these valid packets?

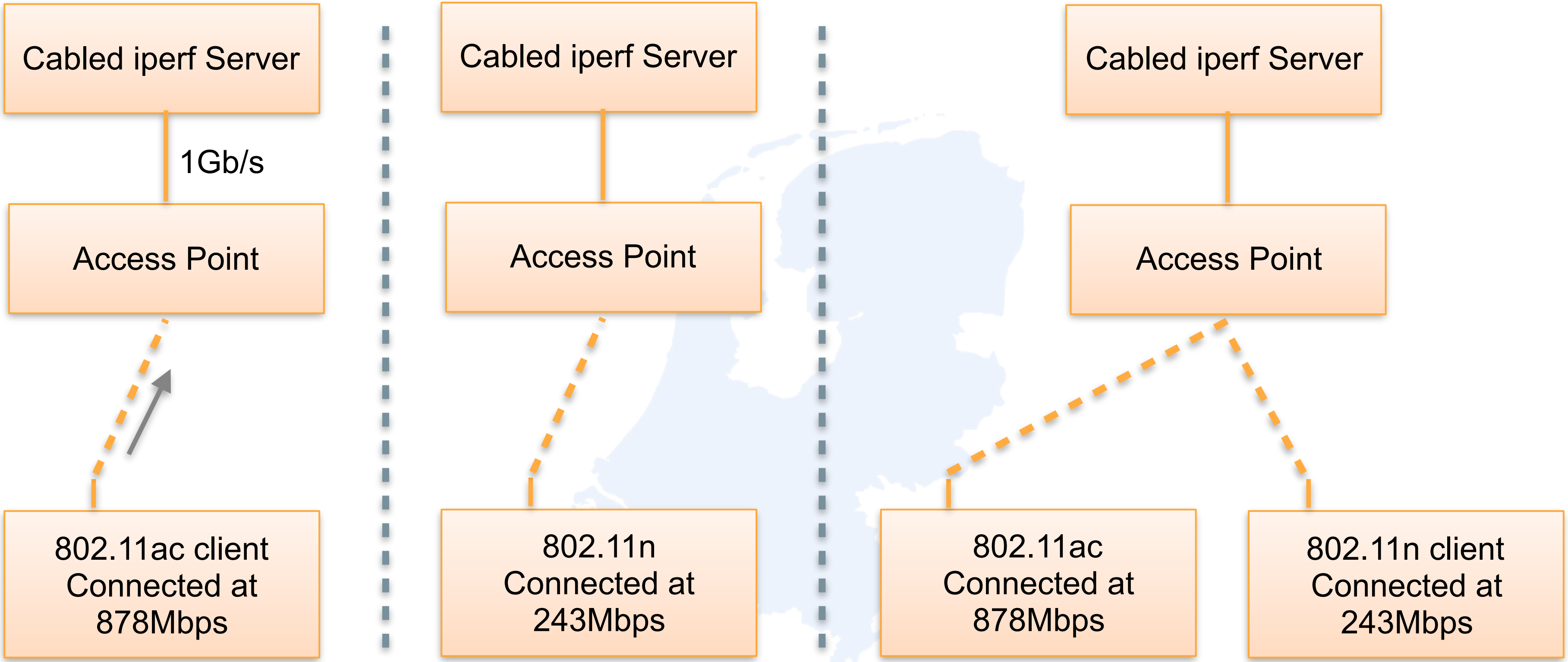


(wlan.ra == 18:87:96:17:73:a5 && wlan.fc.retry==1) || (wlan.ra == 8c:b6:4f:c9:5e:c4)

No.	Time	Source	Destination	Protocol	Length	Data rate (Mb	SSI Signal	Retry	SeqNum	Info
32457	25.7879…		CiscoInc_c9:5…	802.11	39	11	-62	0		Acknowledgement, Flags=...P....C
32530	25.8537…	HtcCorpo_17:73:…	CiscoInc_c9:5…	802.11	49	11	-32	0		802.11 Block Ack Req, Flags=........C
32570	25.8837…		CiscoInc_c9:5…	802.11	39	6	-77	0		Acknowledgement, Flags=........C
32597	25.8983…	10.83.63.26	52.27.109.112	TLSv1	687	13	-77	0	396	Application Data
32600	25.8996…	10.83.63.26	52.27.109.112	TCP	664	11	-74	0	396	[TCP Retransmission] 37691→443 [PSH, ACK] Seq=35
32691	25.9649…		CiscoInc_c9:5…	802.11	39	11	-62	0		Acknowledgement, Flags=........C
33128	26.3120…	65.55.174.170	10.83.59.136	TCP	207	72.2222	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33129	26.3122…	65.55.174.170	10.83.59.136	TCP	207	72.2222	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33132	26.3132…	65.55.174.170	10.83.59.136	TCP	207	72.2222	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33135	26.3140…	65.55.174.170	10.83.59.136	TCP	207	72.2222	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33138	26.3149…	65.55.174.170	10.83.59.136	TCP	207	72.2222	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33144	26.3209…	65.55.174.170	10.83.59.136	TCP	207	6.5	-61	1	1216	[TCP Retransmission] 993→60546 [PSH, ACK] Seq=34
33145	26.3210…		CiscoInc_c9:5…	802.11	39	6	-33	0		Acknowledgement, Flags=........C
33147	26.3212…	10.83.63.26	179.60.192.2	TLSv1.2	194	26	-74	0	397	Application Data
33237	26.3649…	10.83.63.26	52.27.109.112	TCP	687	39	-75	0	398	[TCP Retransmission] 37691→443 [PSH, ACK] Seq=35
33242	26.3659…		CiscoInc_c9:5…	802.11	39	6	-75	0		Acknowledgement, Flags=........C

Lab#7
iperf - Let see slowness in the air

3 scenarios - Alone on channel 100



Cabled iperf Server

1Gb/s

Access Point

802.11ac client Connected at 878Mbps

Upload: **536Mb/s**

Cabled iperf Server

Access Point

802.11n Connected at 243Mbps

145Mb/s

Cabled iperf Server

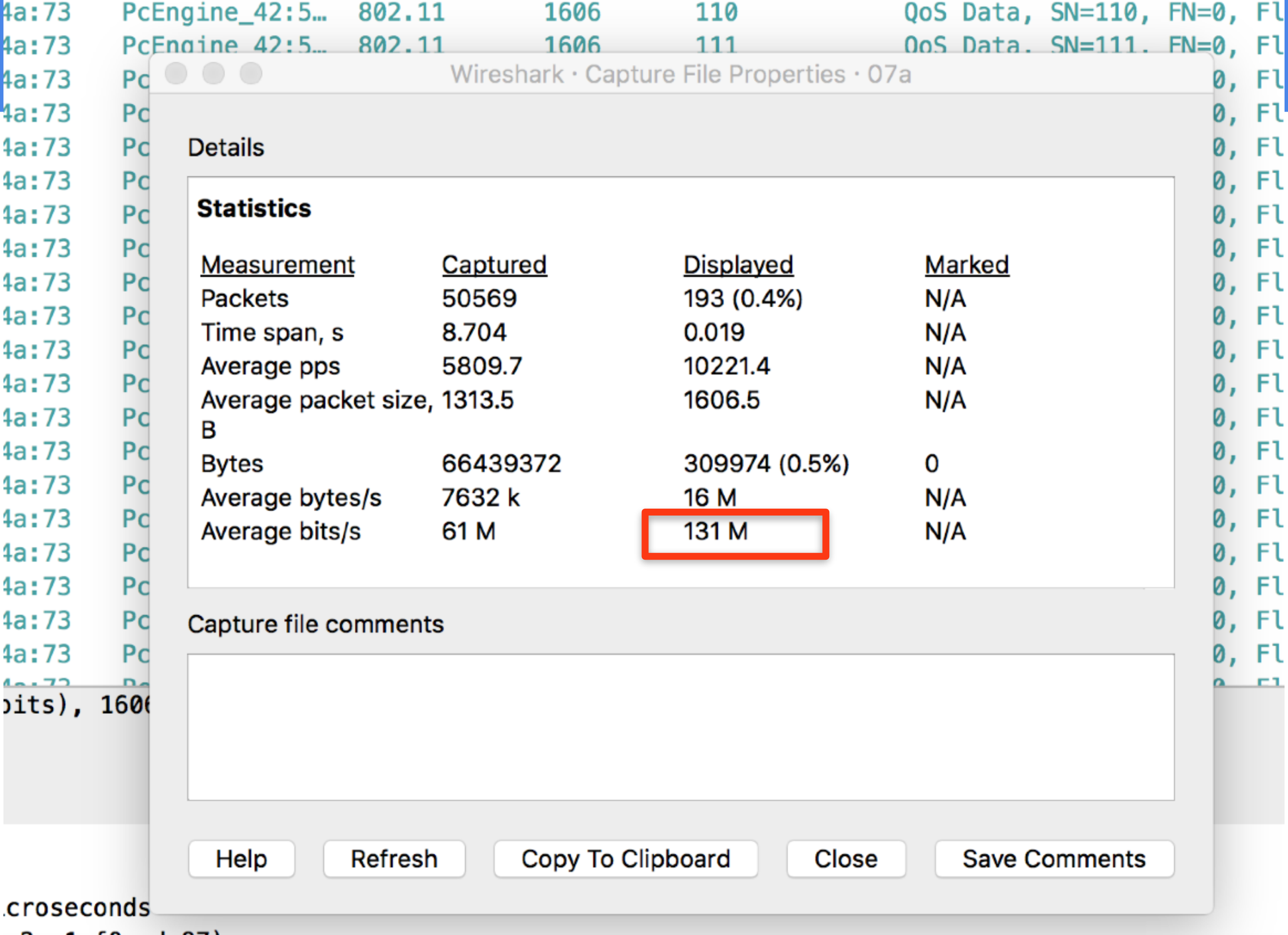
Access Point

802.11ac Connected at 878Mbps

215Mb/s

802.11n client Connected at 243Mbps

90Mb/s



```
4a:73    PcEngine_42:5…  802.11    1606    110    QoS Data, SN=110, FN=0, Fl
4a:73    PcEngine_42:5…  802.11    1606    111    QoS Data, SN=111, FN=0, Fl
```

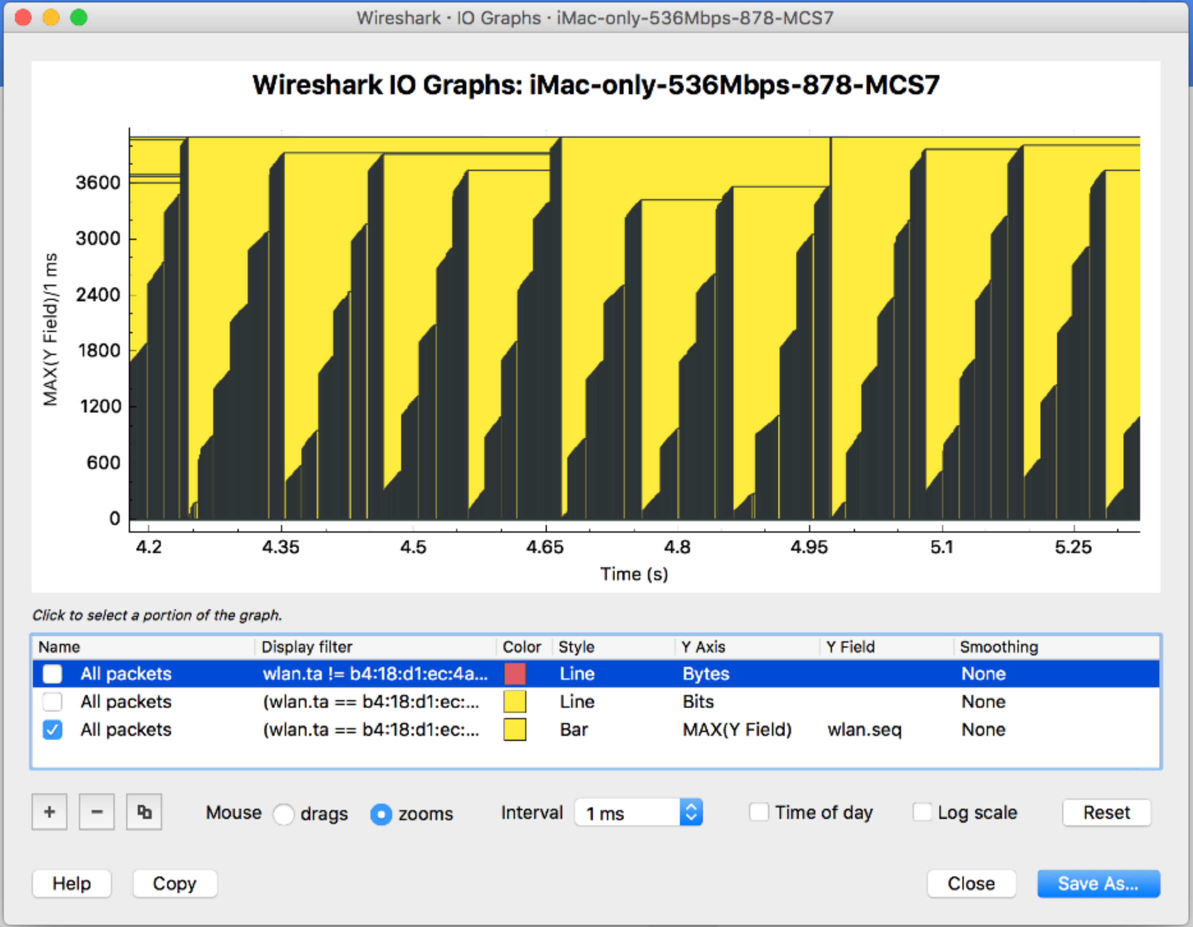
Wireshark · Capture File Properties · 07a

Details

Statistics

Measurement	Captured	Displayed	Marked
Packets	50569	193 (0.4%)	N/A
Time span, s	8.704	0.019	N/A
Average pps	5809.7	10221.4	N/A
Average packet size, B	1313.5	1606.5	N/A
Bytes	66439372	309974 (0.5%)	0
Average bytes/s	7632 k	16 M	N/A
Average bits/s	61 M	131 M	N/A

Capture file comments

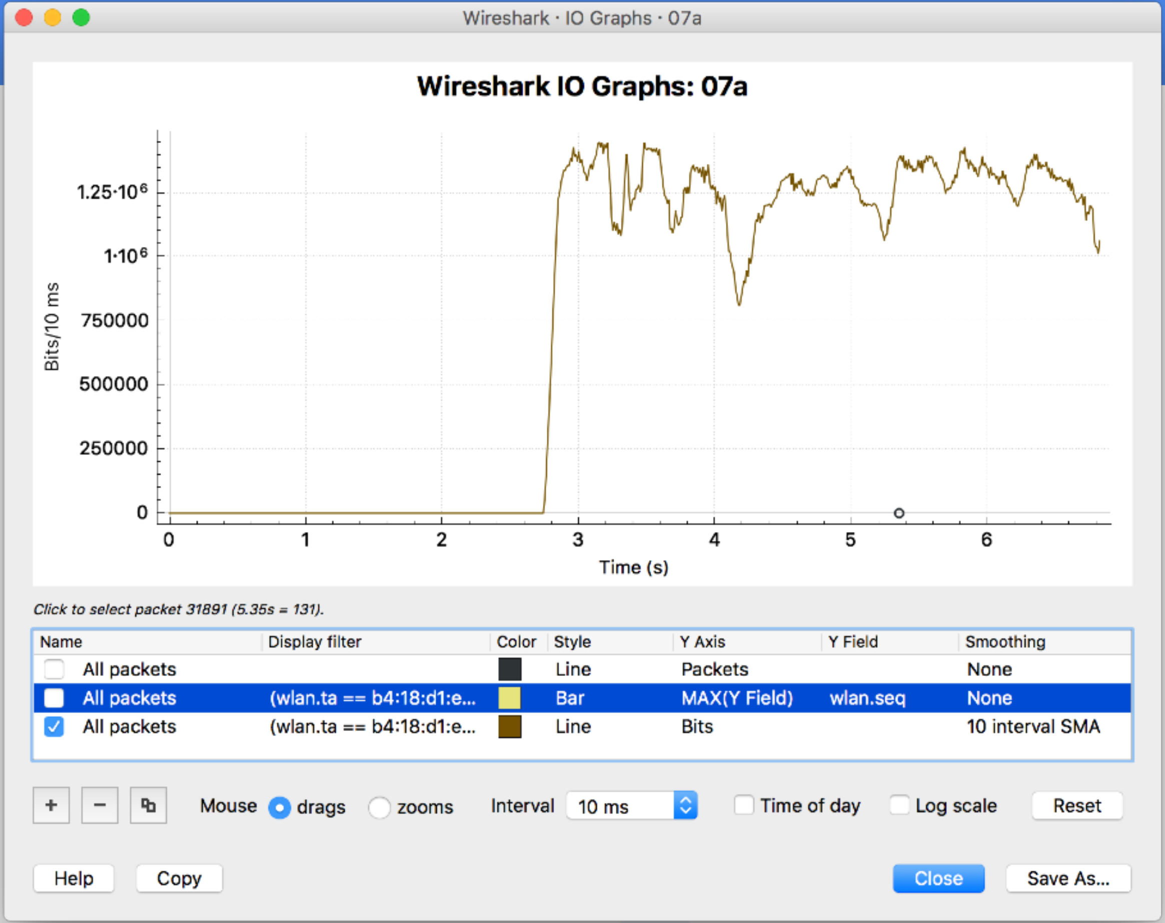


Click to select a portion of the graph.

	Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
☐	All packets	wlan.ta != b4:18:d1:ec:4a...	🟥	Line	Bytes		None
☐	All packets	(wlan.ta == b4:18:d1:ec:...	🟨	Line	Bits		None
☑	All packets	(wlan.ta == b4:18:d1:ec:...	🟨	Bar	MAX(Y Field)	wlan.seq	None

Mouse ○ drags ● zooms Interval 1 ms ☐ Time of day ☐ Log scale

- True fact: capture is dropping packet
  - We see gaps in sequence number every 18-20ms
  - Internal buffer of the laptop drops packet to reach a max of 172Mbps
  - Should increase buffer? (default 2M, to be tested)
  - Except baselining, no need to monitor data packets at such speed to troubleshoot, most troubleshooting is done with Mgt/Ctrl frames
  - See Chris Greer videos on packet losses on personal laptops



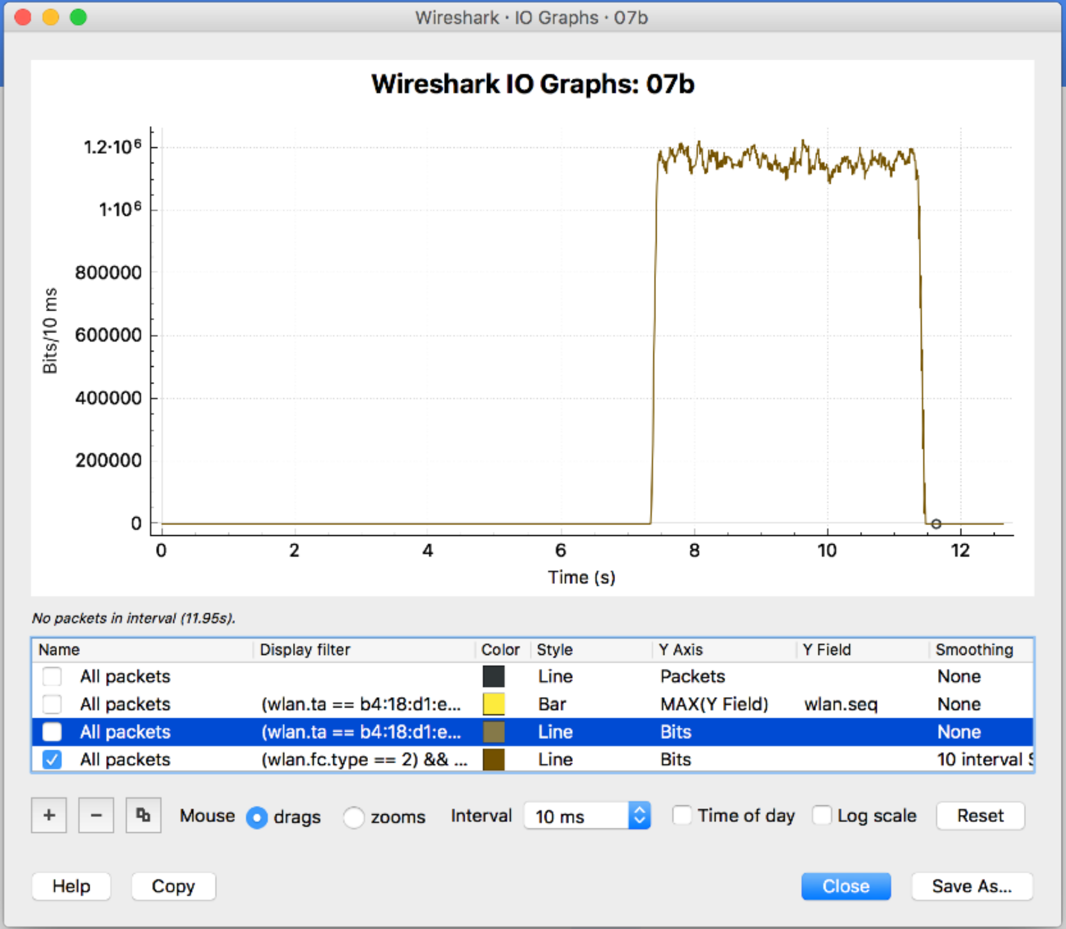
Click to select packet 31891 (5.35s = 131).

Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
□ All packets		■	Line	Packets		None
□ All packets	(wlan.ta == b4:18:d1:e...	■	Bar	MAX(Y Field)	wlan.seq	None
☑ All packets	(wlan.ta == b4:18:d1:e...	■	Line	Bits		10 interval SMA

Mouse ● drags ○ zooms Interval 10 ms □ Time of day □ Log scale

536Mb/s
Retries: 1%

145Mb/s
Retries: 1.6%

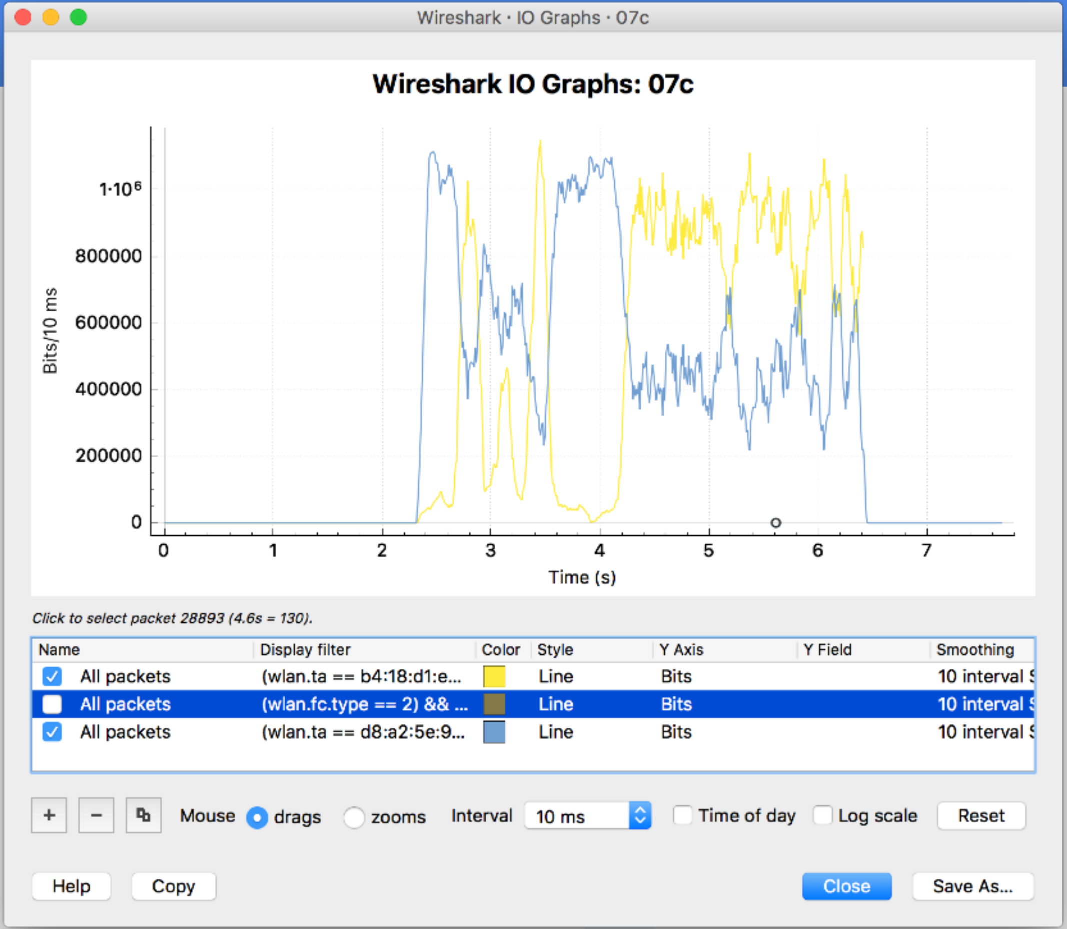


No packets in interval (11.95s).

	Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
□	All packets		■	Line	Packets		None
□	All packets	(wlan.ta == b4:18:d1:e...	🟨	Bar	MAX(Y Field)	wlan.seq	None
□	All packets	(wlan.ta == b4:18:d1:e...	🟫	Line	Bits		None
☑	All packets	(wlan.fc.type == 2) && ...	🟫	Line	Bits		10 interval S

Mouse ● drags ○ zooms Interval 10 ms □ Time of day □ Log scale

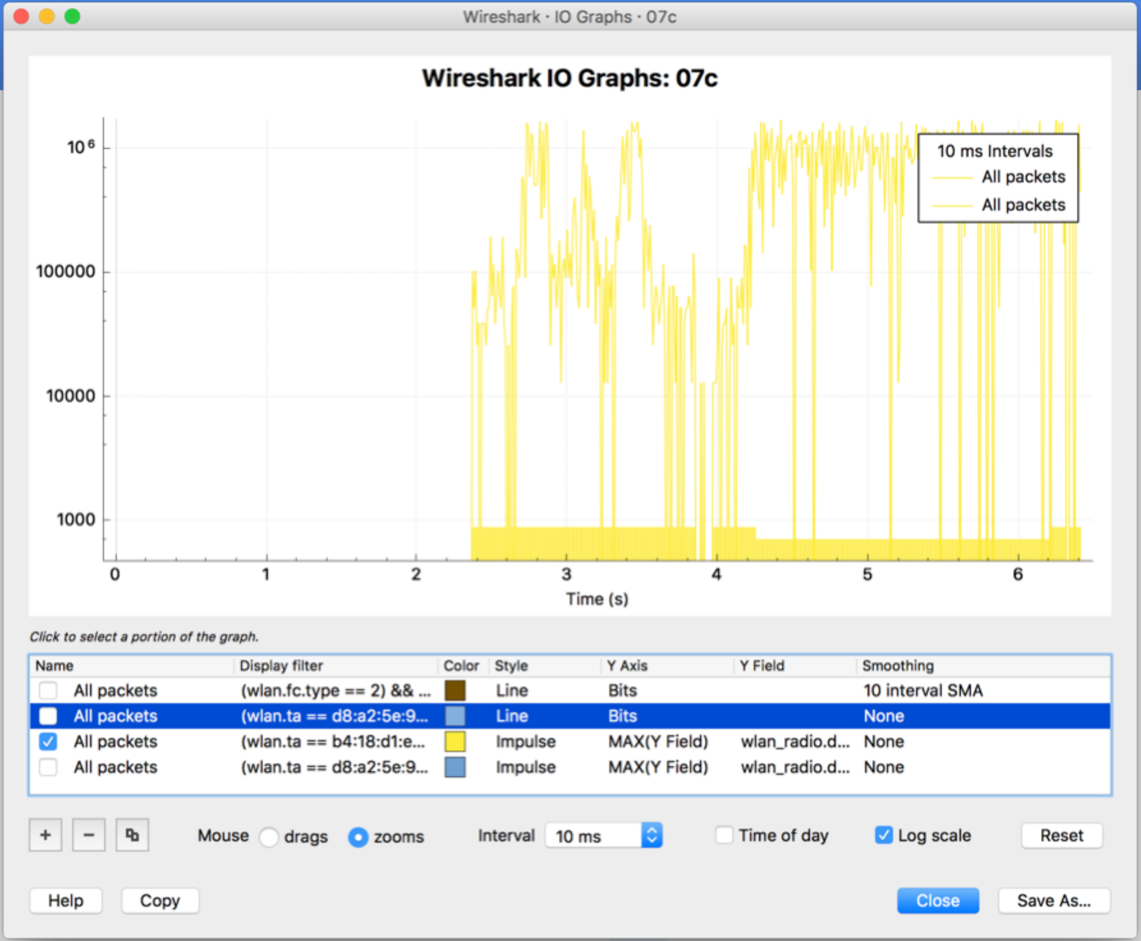
305Mb/s
Retries: 2.1%



Click to select packet 28893 (4.6s = 130).

	Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
☑	All packets	(wlan.ta == b4:18:d1:e...	🟨	Line	Bits		10 interval
□	All packets	(wlan.fc.type == 2) && ...	🟫	Line	Bits		10 interval
☑	All packets	(wlan.ta == d8:a2:5e:9...	🟦	Line	Bits		10 interval

Mouse ● drags ○ zooms Interval 10 ms □ Time of day □ Log scale Reset



Name	Display filter	Color	Style	Y Axis	Y Field	Smoothing
□ All packets	(wlan.fc.type == 2) && ...	🟫	Line	Bits		10 interval SMA
□ All packets	(wlan.ta == d8:a2:5e:9...	🟦	Line	Bits		None
☑ All packets	(wlan.ta == b4:18:d1:e...	🟨	Impulse	MAX(Y Field)	wlan_radio.d...	None
□ All packets	(wlan.ta == d8:a2:5e:9...	🟦	Impulse	MAX(Y Field)	wlan_radio.d...	None

Mouse ○ drags ● zooms Interval 10 ms □ Time of day ☑ Log scale

Some Topic

- CWNP Certification Program
  - https://www.cwnp.com

- Some Wi-Fi guys
  - https://twitter.com/KeithRParsons
  - http://www.revolutionwifi.net/revolutionwifi/
  - http://divdyn.com/blog/
  - http://wlanbook.com/twitter-ids-of-cwnp-certified-wireless-network-expert-cwne/

Thank you!

contact@iwaxx.com

twitter.com/tomlabaude