



# SharkFest '18 Europe



## IEEE802.11ac Debugging in Windows environment

New way of Debugging with Wireshark after AirPcap era.

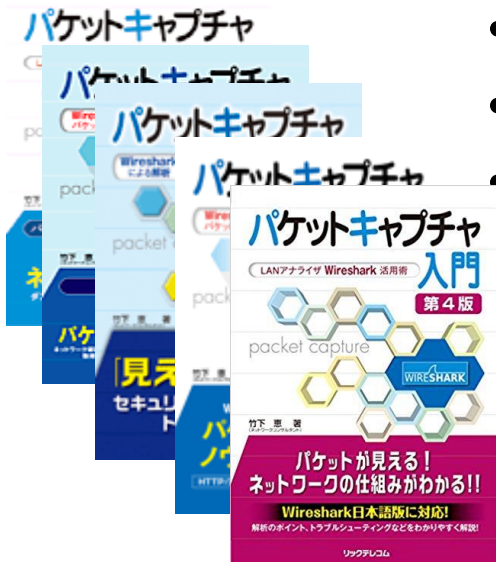
Supplemental files  
<http://www.ikeriri.ne.jp/sharkfest/>

Megumi Takeshita

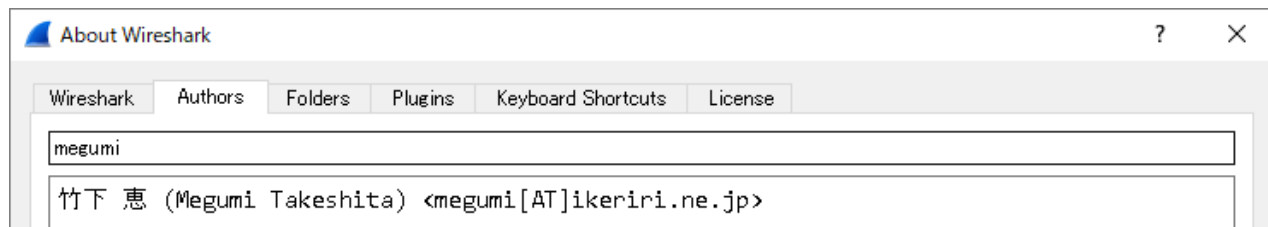
Packet Otaku  
ikeriri network service



# Megumi Takeshita, ikeriri network service



- Founder, ikeriri network service co.,ltd
- Wrote 10+ books about Wireshark
- Reseller of Riverbed Technology ( former CACE technologies ) in Japan
- Attending all Sharkfest
- Translator of QT Wireshark into Japanese



[illegible][illegible]



# Packet analysis before 11n

- Wireless packet capturing before IEEE802.11n, we used AirPcap and radiotap header to analyze and debug in Windows environment.
- AirPcap is easy to use and integrated into Wireshark.
- Radiotap header is old dissector of IEEE802.11, dissecting PHY physical information, PLCP signal (Physical Layer Convergence Protocol)

PLCP  
Preamble  
(Long/Short)

PLCP header  
(modulation,  
rate, length)

IEEE802.11  
MAC header

IEEE802.2  
LLC header

Data

FCS



# Radiotap header



▣ Radiotap Header v0, Length 20

Header revision: 0

Header pad: 0

Header length: 20

▣ Present flags

```
....0 = TSFT: Absent
....1 = Flags: Present
....1 = Rate: Present
....1 = Channel: Present
....0 = FHSS: Absent
....1 = dBm Antenna Signal: Present
....1 = dBm Antenna Noise: Present
....1 = Lock Quality: Present
....0 = TX Attenuation: Absent
....0 = dB TX Attenuation: Absent
....0 = dBm TX Power: Absent
....1 = Antenna: Present
....1 = dB Antenna Signal: Present
....0 = dB Antenna Noise: Absent
....0 = RX flags: Absent
....0 = Channel+: Absent
....0 = MCS information: Absent
....0 = A-MPDU Status: Absent
....0 = VHT information: Absent
...0 0000 00.. = Reserved: 0x00000000
..0. .... = Radiotap NS next: False
..0. .... = Vendor NS next: False
0... .... = Ext: Absent
```

▣ Flags: 0x10

```
....0 = CFP: False
....0 = Preamble: Long
....0 = WEP: False
....0 = Fragmentation: False
...1 .... = FCS at end: True
..0. .... = Data Pad: False
..0. .... = Bad FCS: False
0... .... = Short GI: False
```

Data Rate: 54.0 Mb/s

Channel frequency: 2427 [BG 4]

▣ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum

```
....0 = Turbo: False
....0 = Complementary Code Keying (CCK): False
....1 = Orthogonal Frequency-Division Multiplexing (OFDM): True
....1 = 2 GHz spectrum: True
....0 = 5 GHz spectrum: False
....0 = Passive: False
....0 = Dynamic CCK-OFDM: False
....0 = Gaussian Frequency Shift Keying (GFSK): False
...0 = GSM (900MHz): False
..0. .... = Static Turbo: False
..0. .... = Half Rate Channel (10MHz Channel width): False
0... .... = Quarter Rate Channel (5MHz Channel width): False
```

SSI Signal: -43 dBm

SSI Noise: -100 dBm

Signal Quality: 86

Antenna: 0

SSI Signal: 57 dB

## Fixed field

## Simple and easy to read

## Short display filter string

## supported by many commercial products (old style)

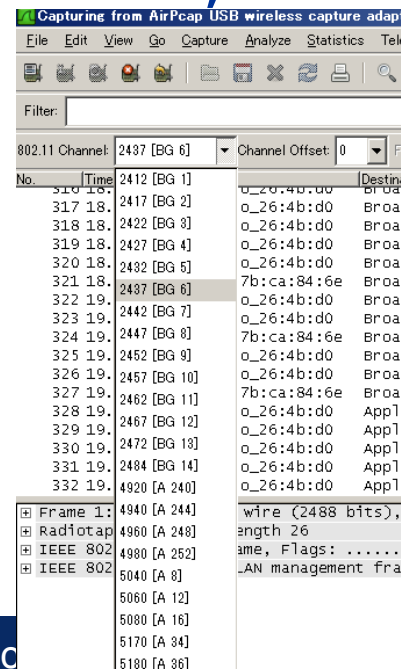
5



# AirPcap in Windows environment

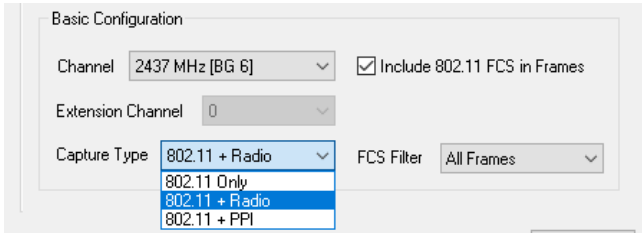
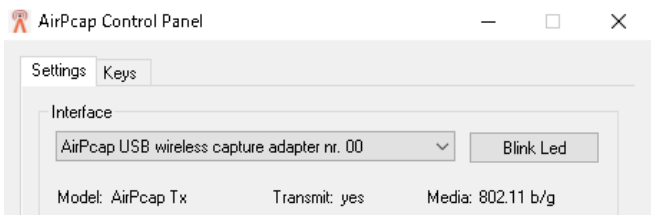


- Plug in AirPcapNX and start Wireshark, tshark, etc.
- View > Wireless toolbar to select ch, bandwidth, etc.
- Set Capture type (radiotap/ppi), etc.
- Start capturing.
- Use Wireshark / tshark to analyze
- Easy and best way until **.11n**
- AirPcap NX and TX can also transmit IEEE802.11 frames.





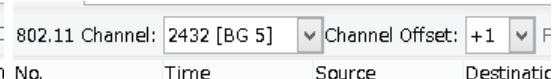
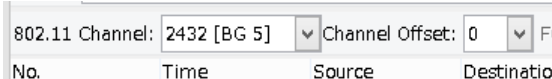
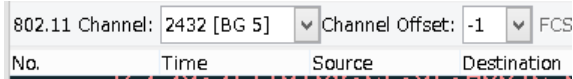
# AirPcap live demonstration in Windows10



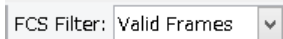
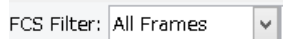
## Capture Type

802.11 Only (only L2 header)  
802.11 + Radio ( Radiotap )  
802.11 + PPI ( Per Packet Information)

Bandwidth	HT-(Offset-1)	20MHz(Offset0)	HT+(Offset+1)
Selected Channels	Primary Ch 5 + Ext. Ch 1 Ch1+5(p)(40MHz)	Primary Ch 5 Ch5(20MHz)	Primary Ch 5 + Ext. Ch 9 Ch 5(p)+9 (40MHz)



FCS settings	All frame	Capture frames FCS is valid	Capture frames FCS is invalid
--------------	-----------	--------------------------------	----------------------------------





# Linux



1. Browse WikiDevi [wikidevi.com](http://wikidevi.com) and choose good device with Linux monitor mode support
2. insmod to install driver, lsusb / lspci to check device and ifconfig / iwconfig
3. airmon-ng check kill  
airmon-ng start wlan\*  
to start monitor mode



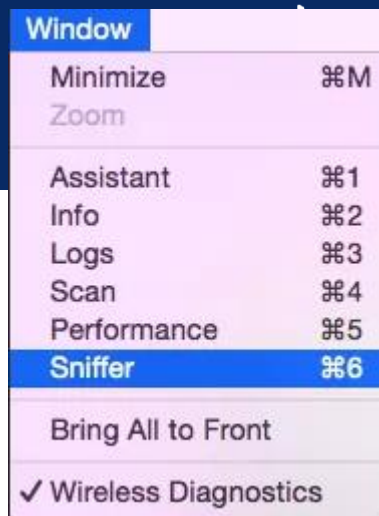
The screenshot shows the WikiDevi website interface. At the top, there's a navigation bar with links for "Not logged in", "Talk", "Contributions", and "Create account". Below this, there's a search bar and a "Log in" button. The main content area features a large yellow flower image with the text "[[...]]" next to it. To the right of the flower, there's a "Main page" tab and a "Discussion" tab. Below these, there's a "Read" button and a "View source" button. A "Search WikiDevi" input field is also present. The main content area displays a message: "Files, Images) upgraded MW to 1.30 - maybe things are slightly less broken". On the left side, there's a sidebar with links for "Main page", "Menu", "Recent changes", "Random page", "query forms", "Embedded system", "MGPC (non-PC)", "Wireless adapter", "OUI", "data/misc", "Add data", "Browse data", "Semantic search", "Search", "View XML", "Short-term conf. list", and "Contact admin". The main content area has a "Main Page" heading. Below this, there's a "Welcome to WikiDevi !" section. To the right, there's a "State of the Database" section with a list of statistics: 5743 Wireless adapters, 208 Ethernet adapters, 4997 Wireless embedded systems, and 518 Wired embedded systems. The bottom of the page features a footer with the text "#sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2".





# macOS

- Choose MacBook pro ( with monitor mode support )
- 1. Command + Space to open spotlight
  2. type Wireless Diagnostics to open Wireless Diagnostics Tool
  3. choose Sniffer in windows menu
  4. choose channel and bandwidth to start capturing
  5. You may need to enter admin pass
  6. press Stop to stop capture
  7. filename.WCAP file is the trace file
- You can open WCAP file in Wireshark and Wireshark itself can capture packets



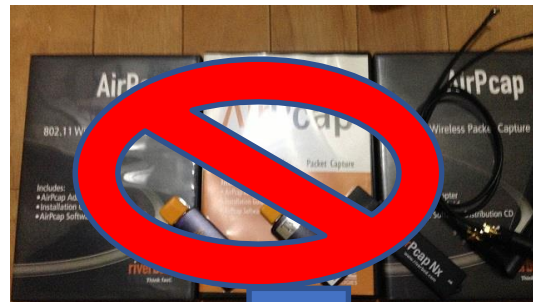
# We still need windows environments

- Windows10 PCs are still major in Japanese enterprise network, so we have to use Windows in wireless debugging and troubleshooting.
- But the time stopped at 2005 of AirPcapNX age, with IEEE802.11n 40MHz capturing, though Linux has many monitor mode driver with IEEE802.11ac with 80MHz ( thank you very much, aircrack-ng !)
- Let's talking about wireless capturing in Windows environment.





# AirPcap discontinued, then ?



- My lovely AirPcaps are go away, then what are the alternatives ?
- Off course Air magnet, Omnippeek, and other enterprise solutions in Windows at expensive price tag.
- AcrylicWiFi is a nice product, but there are some driver issues.
- EyePA is one of the best alternatives



# Eye P.A. (Eye Packet Analyzer)



この接続は次の項目を使用します(O):

- ☒ Microsoft ネットワーク用クライアント
- ☒ VMware Bridge Protocol
- ☒ Microsoft ネットワーク用ファイルとプリンター共有
- ☒ Npcap Packet Driver (NPCAP)
- ☒ QoS パケット スケジューラ
- ☒ Tarlogic NDIS Monitor Driver

Eye P.A. was just a wireless packet visualization software  
But packet capture function is added at version 2 with compatible monitor mode driver.

In version 2.0.1.2 EyePA uses Tarlogic NDIS Monitor driver, as known as Tamosoft TamoGraph



# Compatible Adapters

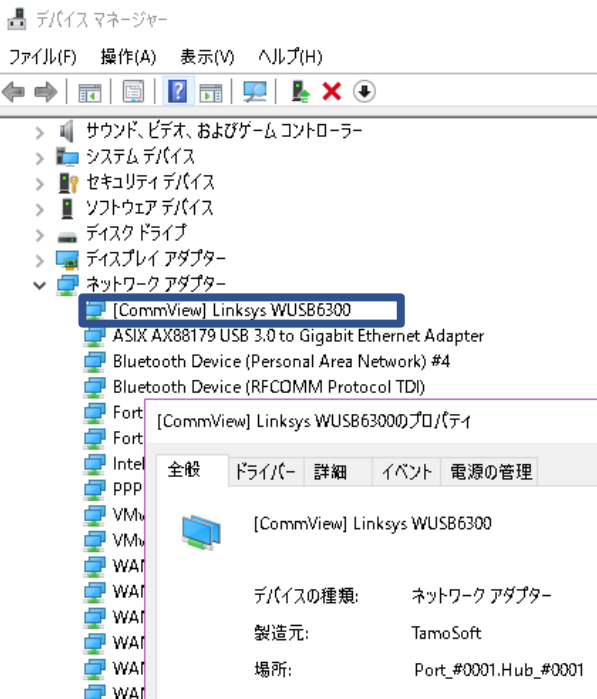


- Supported adapter:  
Linksys WUSB6300 (recommended),  
ASUS USB-AC56, ASUS USB-AC68, ALFA  
Network AWUS1900, Amped Wireless ACA1  
EnGenius EUB1200AC, D-Link DWA-182 rev  
C1, D-Link DWA-192, TRENDnet TEW-805UB,  
TP-LINK Archer T4U v2, TP-LINK Archer  
T4UH v2, Edimax EW-7822UAC, Edimax EW-  
7833UAC and AirPcap NX/TX

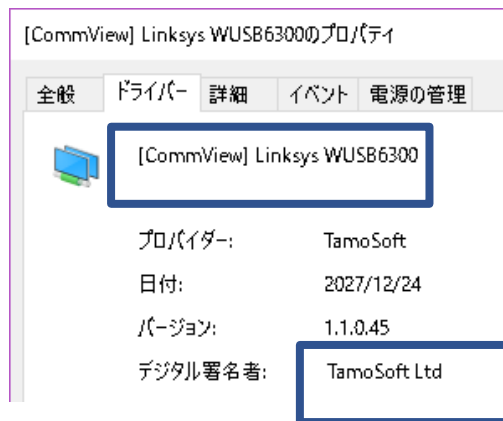




# Linksys WUSB6300 IEEE802.11abgn+ac



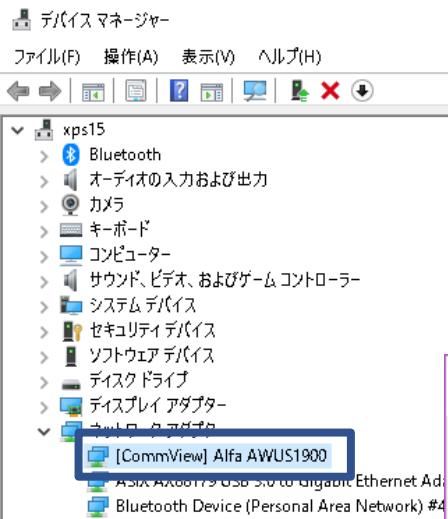
Chipset Realtek RTL8812AU  
abgn+ac, 2x2:2  
[CommView] Linksys WUSB6300



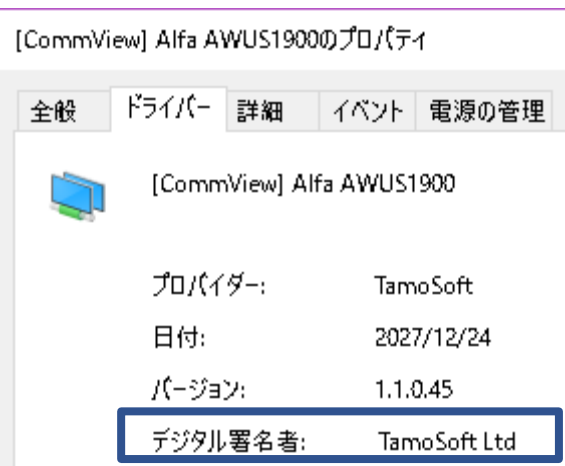
Linksys WUSB6300
Manuf/OEM/ODM SerComm
FCC approval date: 19 June 2013 (Est.) initial retail price (in USD): \$69.99 UPC: 745883598403 (UPC DB, On eBay) Country of manuf.: China
Amazon image
ASIN B00EDOG8NC (, On Amazon, On CCC) On Newegg
Interface: USB
USB 3.0 Connector: Male A Form factor tags: dongle
ID: 13b1:003f Windows: USBVID_13B1&PID_003F
FCC ID: 2A711-13B1-003F Industry Canada ID: 3839A-WUSB6300
WI1 chip1: Realtek RTL8812AU
Additional chips 5GHz Power Amplifier IC; Skyworks; SE5022T; SIGe, 5022T, AC242; 2; SPDT Switch w/ LNA; Skyworks; SKY85601; SKY, 85601, 229CU; 2; 16-pin QFN; 2.5 mm x 2.5 mm;
Probable Linux driver Realtek's vendor driver (8812au) available on Edimax's site (from the 7822UAC's prod. page) md5: fda86443df638abd9f50a9997090d58e slightly modified version (additional USB IDs added) md5: 2e345f43f5fa50ca1137655b5a5b9ab also, abperiasamy's 8812au repo on GitHub which is patched for newer kernels USB ID not yet observed in any mainline kernel / this list (see also passys)
Windows driver see Realtek's website
Antenna connector: none
abgn+ac, 2x2:2
Flags: DFS
OUI: C8:D7:19 (7 E, 9 W, 2012)

# ALFA Network AWUS 1900

## IEEE802.11abgn+ac



Chipset Realtek RTL8814AU  
abgn+ac, 4x4:3  
[CommView] Alfa AWUS1900



ALFA Network AWUS1900
FCC approval date: 28 June 2017 UPC: 4718050305209 (UPC DB, On eBay) Country of manuf.: Taiwan
Amazon image
ASIN B01MZD7Z76 (, On Amazon, On CCC)
Interface: USB
USB 3.0 Connector: Female Micro-B Form factor tags: corded (modular) adapter
ID: 0bda:8813 (1 addl. devices) Windows: USB#VID_0BDA&PID_8813
FCC ID: 2ABE78814
WI1 chip1: Realtek RTL8814AU
Probable Linux driver See this driver @ Edimax USB ID not yet observed in any mainline kernel / this list (see also passys)
Windows driver see Realtek's website
Antenna connector: RP-SMA
abgn+ac, 4x4:3
Flags: 256QAM
OUI: 00:C0:CA (5 E, 25 W, 2010)



# What is 2x2:2, 4x4:3 mean ?



Number of Transmitters

Number of Receivers

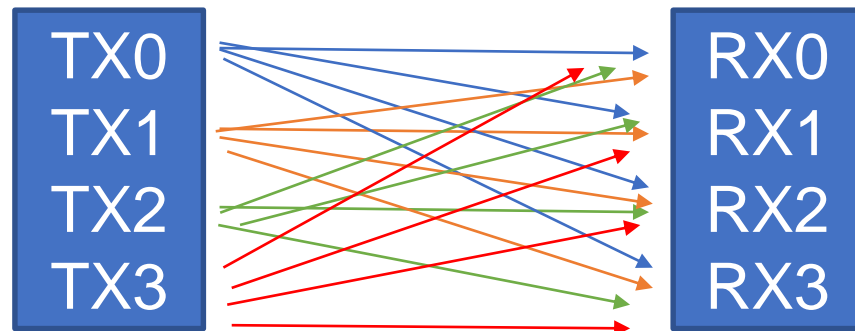
- Linksys WUSB6300

2x2:2

ALFA Network AWUS1900

4x4:3

TxR:S



Number of  
Spatial Streams

It can send multiple  
streams at a time ?  
Just a moment





# AP is just a repeater, isn't it ?



- ... I see 11ac can enlarge bandwidth to 160MHz
- But AP is just a half duplex repeater hub.  
Why AP can send multiple signals at a time ?



STBC (Space–time block coding) also as known as beam forming can send multiple channel signal at a time. So we can speed up double, triple, quadoruple in a connection.



# Single user - MIMO (Multiple Input Multiple Output)



- In IEEE802.11a/b/g, a STA/AP has one antenna to transmit traffic and one to receive from others. So easy to calculate that 1 user 1 stream 20MHz.
- In 11ac, a STA/AP has many antenna to transmit and many antenna to receive. 11AC can also send many streams at a time ( spatial stream ) to send double, triple, and quadoruple to a single user because of STBC and beam forming technologies.
- So they can enlarge the bandwidth up to 160MHz.



# 11ac capture in Windows

- Many AP supports MU-MIMO, but the capture side, we need to capture and filter a connection between an AP and a STA. Single user MIMO with multiple Spatial Stream is the first step to capture 11ac traffic.
- We have to capture at good place ( distance / direction ) such as required RSSI is  $\geq -45\text{dBm}$
- Off course aircrack-ng ( airmmon-ng and others ) and Linux is a good idea, but we want to capture in Windows environment !!



# Cisco Aironet 1702i



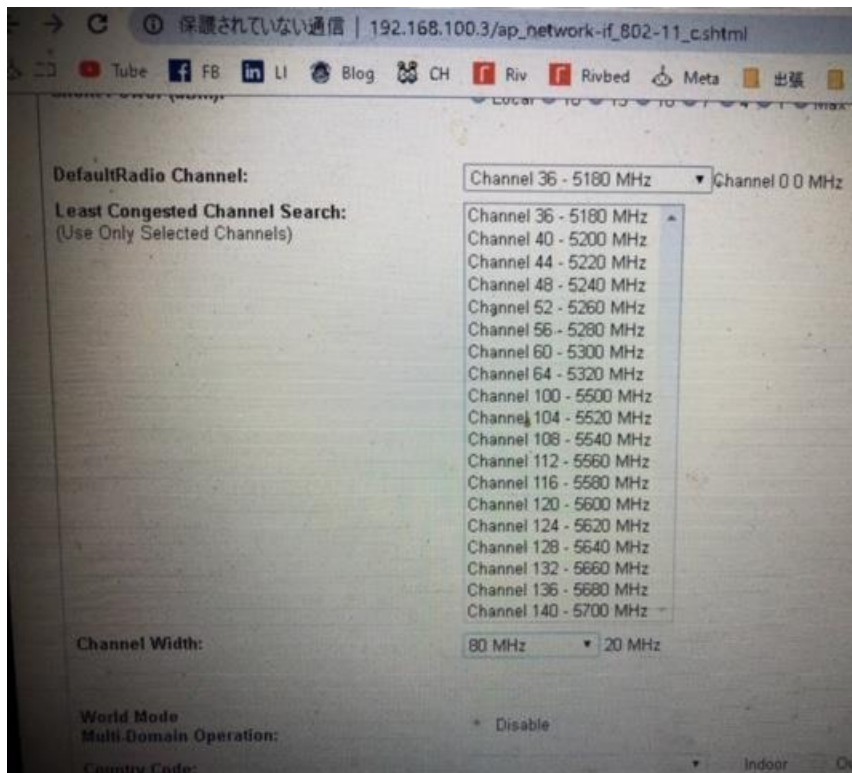
## IEEE802.11ac wave1 access point



- 3x3:2 access point MU-MIMO and 2 spatial streams
- 802.11ac beam forming
- 20/40/80 MHz channel
- Max 867Mbps at 5GHz 80MHz bandwidth
- A-MPDU/A-MSDU are supported



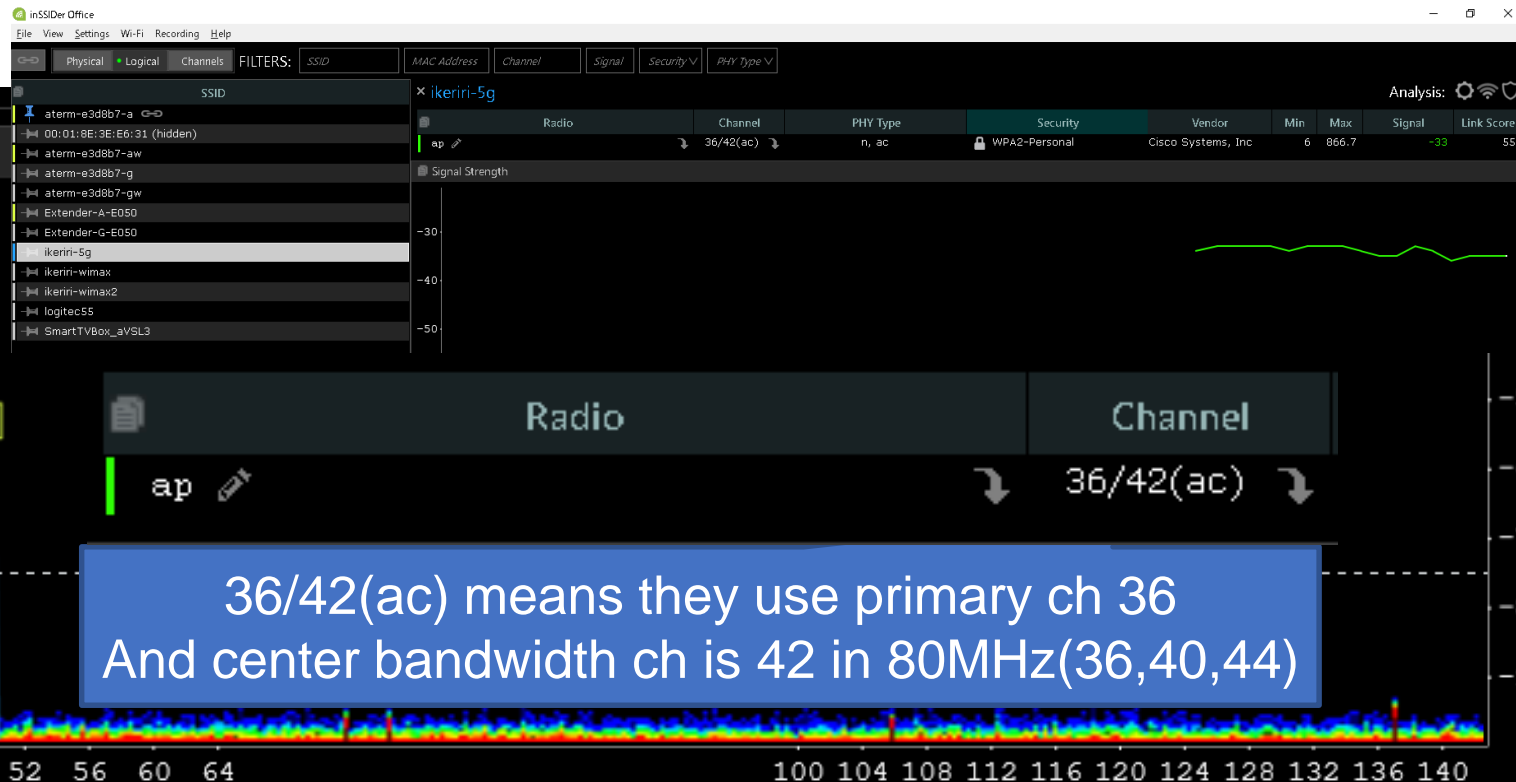
# Set up like this



- Set a fixed 80MHz bandwidth channel to 36
- Enable all MCS and beam forming, aggregation opt.
- SSID: ikeriri-5g
- WPA2-PSK passphrase: wireshark



# Check the spectrum using InSSIDer Office





# Rivet Networks Killer Wireless-AC 1535



At first I test Killer Wireless-AC 1535 in my Dell XPS ( default), the WLAN card spec:

Qualcomm Atheros QCA6174A  
Supports 20/40/80MHz at 5GHz  
2x2:2 MU-MIMO,  
Transmit Beamforming  
High-density modulation (256-QAM)  
low-density parity check (LDPC)  
maximum ratio combining (MRC)  
Rx space time block code (STBC) etc.  
But.... It failed. ( in later )

Rivet Networks Killer Wireless-AC 1535 Availability: now
FCC approval date: 28 May 2015 (Est.) release date: June 2015
Amazon image
ASIN B01724QS30 ( <a href="#">en</a> , <a href="#">On Amazon</a> , <a href="#">On CCC</a> )
Interface: NGFF
Connector: M.2 Form factor tags: 2230
ID: 168c:003e (14 addl. devices) SS: 1a56:1535 Windows: PCI\VEN_168C&DEV_003E&SUBSYS_15351A56
FCC ID: FCC-QCFA364A Industry Canada ID: 4104A-QCFA364A
WI1 chip1: Qualcomm Atheros QCA6174A
Probable Linux driver <a href="#">ath10k</a> PCI ID first seen in kernel v4.0 (2015-04-12) (see also <a href="#">passys</a> )
Windows driver Win 7/8.1/10 ( <a href="#">Bluetooth</a> )
Antenna connector: MHF4
abgn+ac, 2x2:2
Flags: MU-MIMO, bluetooth 4.1
OUI: 9C:B6:D0 (-, 1 W, 2015)



# Intel Wireless-AC 9260NGW



Then I changed the m.2 PCIe card from Killer 1535 to Intel Wireless-AC 9260NGW, the spec: Intel WCS9200 chipset Supports IEEE802.11ac w2 20/40/80/160MHz bandwidth

2x2:2 ( common in laptop PC ) MU-MIMO  
5Ghz (160Mhz bandwidth) Max Speed1.7Gbps  
May be this WLAN card is one of the newest and most advanced ( result is later.)

Intel Dual Band Wireless-AC 9260 (9260NGW)

FCC approval date: 24 July 2017

Interface: NGFF

Connector: M.2

Form factor tags: 2230

FCC ID: PD99260NG

Industry Canada ID: 1000M-9260NG

WI1 chip1: Intel WCS9200

Probable Linux driver

[iwlmwifi](#), k3.10+ ([in backports](#))

(see also [passys](#))

Antenna connector: MHF4

abgn+ac, 2x2:2

Flags: Wave2, MU-MIMO, VHT160, DFS, Bluetooth 5.0

OUI: none specified

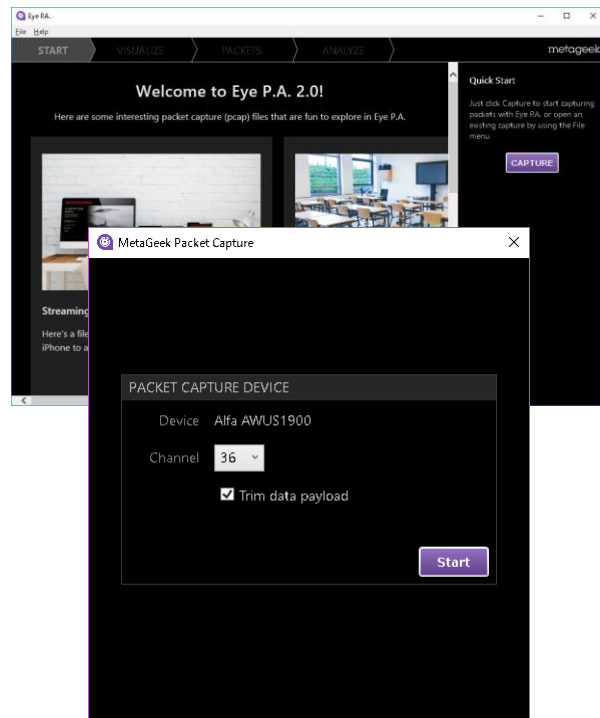




# Capture test with EyePA



1. Plug in Linksys WUSB6300 or ALFA AWUS1900 ( may be other Realtek )
2. Start up EyePA and capture at 36CH without trimming data packet ( need Administrator right )
3. Connect at SSID:ikeriri-5g (Passphrase:wireshark)
4. Ping at 1.1.1.1 or somewhere
5. Stop capture and check the pcap file





# Capture Result of 5GHz 80MHz 11ac channel using EyePA

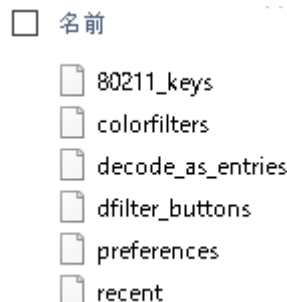
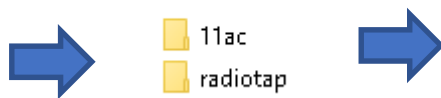
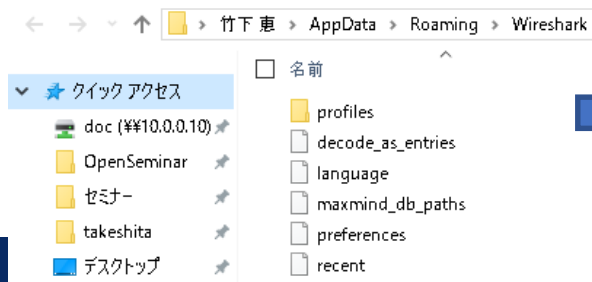
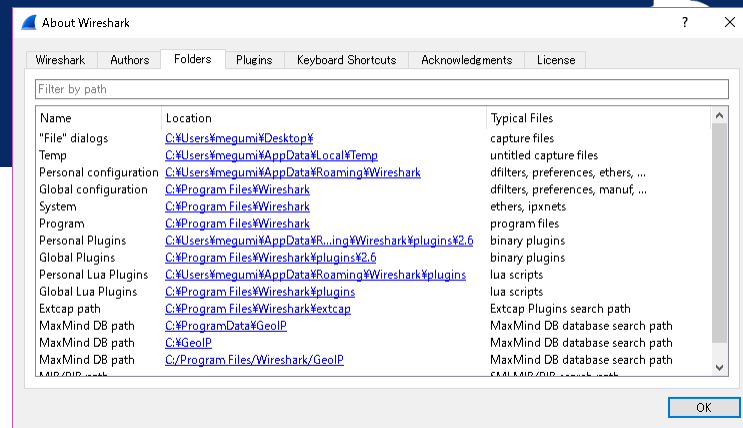


Capture Hardware / STA (AP: Cisco Aironet 1702i 5GHz 80MHz 36CH )		Rivet Networks Killer Wireless-AC 1535 2x2:2(80MHz)	Intel Wireless-AC 9260NGW 2x2:2(160MHz)
LINKSYS WUSB6300 2x2:2	Management frames	OK	OK
	Data frames	NG	NG
ALFA network AWUS1900 4x4:3	Management frames	OK	OK
	Data frames	NG	OK (only 802.11-common field without VHT PHY info)



# Open trace file 80mhz.pcapng

- Download supplemental file at <http://www.ikeriri.ne.jp/sharkfest/>
- Open 80Mhz.pcap
- Download 11ac.zip to extract and copy your personal configuration profile directory of Wireshark  
(Customized Wireshark setting, columns, coloring rules, ieee802.11keys and more )





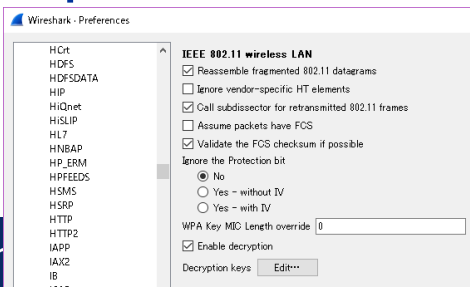
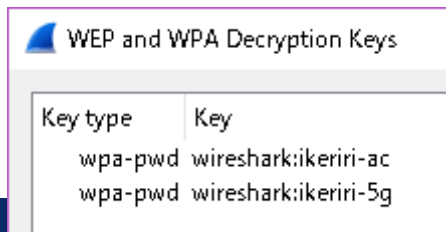
# Customizing Wireshark for dissecting 11ac (1)



- We will use PPI header for more PHY information
- Add fields as column, wlan\_radio.signal\_dbm (Signal), wlan\_radio.data\_rate (Rate), wlan\_radio.channel (Ch) and wlan.fc.type\_subtype (type/subtype)

No.	Time	Char	Signal (dBm)	Rate (Mbps)	Type/Subtype	Source	Destination	Protocol	Length	Info
6	5.104000	36	-43dBm	6	Association R..	IntelCor_a7:a1:b6	Cisco_70:18:d0	802.11	278	Assoc
7	5.120000	36	-39dBm	6	Association R..	Cisco_70:18:d0	IntelCor_a7:a1:b6	802.11	239	Assoc

- Add SSID and WPA2PSK passphrase into decryption key settings of 802.11 protocol in Wireshark preference





# Customizing Wireshark for dissecting 11ac (2)



- Create your own coloring rules, filter button, display filter and capture filter and so on.
- In this time  
Association Response (Green)  
EAPOL key exchange (Blue)  
CSMA/CA retransmit (Yellow)  
Deauthentication / Disassociation (Red)  
Weak Signal under -70dBm (Pink) note: we need -45dBm
- Let's apply 11ac profile to see trace file

Wireshark · Coloring Rules 11ac

Name	Filter
<input type="checkbox"/> アソシエーション応答	wlan.fc.type_subtype==1
<input checked="" type="checkbox"/> WPA鍵交換	eapol
<input checked="" type="checkbox"/> 再送	wlan.fc.retry==1
<input checked="" type="checkbox"/> 非認証	wlan.fc.type_subtype==12
<input checked="" type="checkbox"/> 非アソシエーション	wlan.fc.type_subtype==10
<input type="checkbox"/> 信号弱い	ppi.80211-common.dbm.antsignal <=70



# Looks nice with 11ac profile



80mhz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Char	Signal (dBm)	Rate (Mbps)	Type/Subtype	Source	Destination	Protocol	Length	Info
1	0.000000	36	-40dBm		6 Beacon frame	Cisco_70:18:d0	Broadcast	802.11	306	Beacon frame, SN=981, FN=0, Flags=....., BI=102, SSID=ikeriri-5g
2	2.896000	36	-44dBm		6 Probe Request	IntelCor_a7:a1:b6	Broadcast	802.11	110	Probe Request, SN=1309, FN=0, Flags=....., SSID=Wildcard (Broadcast)
3	2.896000	36	-39dBm		6 Probe Response	Cisco_70:18:d0	IntelCor_a7:a1:b6	802.11	300	Probe Response, SN=106, FN=0, Flags=....R..., BI=102, SSID=ikeriri-5g
4	5.104000	36	-44dBm		6 Authentication	IntelCor_a7:a1:b6	Cisco_70:18:d0	802.11	62	Authentication, SN=222, FN=0, Flags=.....
5	5.104000	36	-39dBm		6 Authentication	Cisco_70:18:d0	IntelCor_a7:a1:b6	802.11	62	Authentication, SN=1030, FN=0, Flags=.....
6	5.104000	36	-43dBm		6 Association R..	IntelCor_a7:a1:b6	Cisco_70:18:d0	802.11	278	Association Request, SN=223, FN=0, Flags=....., SSID=ikeriri-5g
7	5.120000	36	-39dBm		6 Association R..	Cisco_70:18:d0	IntelCor_a7:a1:b6	802.11	239	Association Response, SN=1031, FN=0, Flags=.....
8	5.120000	36	-39dBm		6 QoS Data	Cisco_70:18:d0	IntelCor_a7:a1:b6	EAPOL	187	Key (Message 1 of 4)
9	5.120000	36	-46dBm		6 QoS Data	IntelCor_a7:a1:b6	Cisco_70:18:d0	EAPOL	189	Key (Message 2 of 4)
...	5.136000	36	-38dBm		6 QoS Data	Cisco_70:18:d0	IntelCor_a7:a1:b6	EAPOL	221	Key (Message 3 of 4)
...	5.136000	36	-44dBm		6 QoS Data	IntelCor_a7:a1:b6	Cisco_70:18:d0	EAPOL	165	Key (Message 4 of 4)
...	5.216000	36	-39dBm		54 Data	IntelCor_a7:a1:b6	Broadcast	ARP	126	Who has 192.168.100.254? Tell 192.168.100.142
...	5.216000	36	-41dBm		780 QoS Data	Modacom_94:ea:bc	IntelCor_a7:a1:b6	ARP	128	192.168.100.254 is at 00:1d:93:94:ea:bc
...	5.868000	36	-46dBm		97.5 QoS Data	192.168.100.142	1.1.1.1	ICMP	142	Echo (ping) request id=0x0001, seq=327/18177, ttl=128 (reply in 15)
...	6.091000	36	-40dBm		867 QoS Data	1.1.1.1	192.168.100.142	ICMP	142	Echo (ping) reply id=0x0001, seq=327/18177, ttl=53 (request in 14)

<

> Frame 15: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0

> PPI version 0, 32 bytes

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags: .p....F.

> Logical-Link Control

> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.100.142

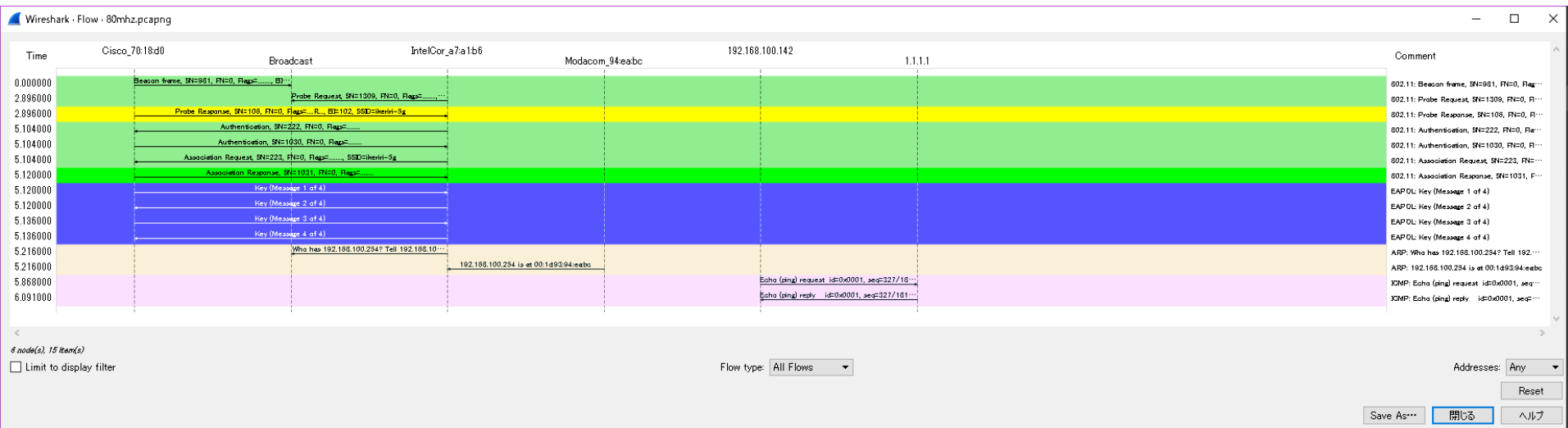
> Internet Control Message Protocol



# Visualize packet with Flow Graph



- You can also create Flow Graph from Statistics to visualize the sequence of 11ac from link up, wpa2 4 way handshake, and icmp (ping) request/response





# Check speed of #15 packet



```
> Frame 15: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface
v PPI version 0, 32 bytes
  Version: 0
  > Flags: 0x00
  Header length: 32
  DLT: 105
v 802.11-Common
  Field type: 802.11-Common (2)
  Field length: 20
  TSFT: 1808275720897148
  > Flags: 0x0000
  Rate: 867.0 Mbps
  Channel frequency: 5180 [A 36]
v Channel flags: 0x0150
  .... 1 .... = Turbo: True
  .... 0. .... = Complementary Code Keying (CCK): False
  .... 1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
  .... 0... .... = 2 GHz spectrum: False
  .... 1 .... = 5 GHz spectrum: True
  .... 0. .... = Passive: False
  .... 0.. .... = Dynamic CCK-OFDM: False
  .... 0... .... = Gaussian Frequency Shift Keying (GFSK): False
  FHSS hopset: 0x00
  FHSS pattern: 0x00
  dBm antenna signal: -40
  dBm antenna noise: -92
v 802.11 radio information
  PHY type: 802.11a (5)
  Turbo type: Dynamic turbo (2)
```

- Look inside of packet detail pane of #15 frame, and check Rate is 867Mbps, maximum rate of 80MHz bandwidth (2 spatial streams)





# Check MCS index of 11ac



We need to check MCS ( modulation code set ) table to specify MCS number, modulation, coding, bandwidth, Data rate with short/long guard interval, minimum SNR and required RSSI

802.11ac - VHT

MCS, SNR and RSSI

VHT MCS	Modulation	Coding	20MHz				40MHz				80MHz				160MHz			
			Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI
			800ns	400ns			800ns	400ns			800ns	400ns			800ns	400ns		
1 Spatial Stream																		
0	BPSK	1/2	6.5	7.2	2	-82	13.5	15	5	-79	29.3	32.5	8	-76	58.5	65	11	-73
1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76	58.5	65	11	-73	117	130	14	-70
2	QPSK	3/4	19.5	21.7	9	-77	40.5	45	12	-74	87.8	97.5	15	-71	175.5	195	18	-68
3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71	117	130	17	-68	234	260	20	-65
4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67	175.5	195	21	-64	351	390	24	-61
5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63	234	260	24	-60	468	520	27	-57
6	64-QAM	3/4	58.5	65	20	-65	121.5	135	23	-62	263.3	292.5	26	-59	526.5	585	29	-56
7	64-QAM	5/6	65	72.2	25	-64	135	150	28	-61	292.5	325	31	-58	585	650	34	-55
8	256-QAM	3/4	78	86.7	29	-59	162	180	32	-56	351	390	35	-53	702	780	38	-50
9	256-QAM	5/6			31	-57	180	200	34	-54	390	433.3	37	-51	780	866.7	40	-48
2 Spatial Streams																		
0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76	117	130	11	-73
1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71	351	390	18	-68
3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59	1053	1170	29	-56
7	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61	585	650	31	-58	1170	1300	34	-55
8	256-QAM	3/4	156	173.3	29	-59	324	360	32	-56	702	780	35	-53	1404	1560	38	-50
9	256-QAM	5/6			31	-57	360	400	34	-54	780	866.7	37	-51	1560	1733.3	40	-48
3 Spatial Streams																		
0	BPSK	1/2	19.5	21.7	2	-82	40.5	45	5	-79	87.8	97.5	8	-76	175.5	195	11	-73
1	QPSK	1/2	39	43.3	5	-79	81	90	8	-76	175.5	195	11	-73	351	390	14	-70
2	QPSK	3/4	58.5	65	9	-77	121.5	135	12	-74	263.3	292.5	15	-71	526.5	585	18	-68
3	16-QAM	1/2	78	86.7	11	-74	162	180	14	-71	351	390	17	-68	702	780	20	-65
4	16-QAM	3/4	117	130	15	-70	243	270	18	-67	526.5	585	21	-64	1053	1170	24	-61
5	64-QAM	2/3	156	173.3	18	-66	324	360	21	-63	702	780	24	-60	1404	1560	27	-57
6	64-QAM	3/4	175.5	195	20	-65	364.5	405	23	-62			26	-59	1579.5	1755	29	-56
7	64-QAM	5/6	195	216.7	25	-64	405	450	28	-61	877.5	975	31	-58	1755	1950	34	-55
8	256-QAM	3/4	234	260	29	-59	486	540	32	-56	1053	1170	35	-53	2106	2340	38	-50
9	256-QAM	5/6	260	288.9	31	-57	540	600	34	-54	1170	1300	37	-51			40	-48

(<https://www.wlanpros.com/mcs-index-charts/>)

# 2 special streams , 80MHz 867Mbps

802.11ac - VHT

MCS, SNR and RSSI

VHT MCS	Modulation	Coding	20MHz				40MHz				80MHz			
			Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI
			800ns	400ns			800ns	400ns			800ns	400ns		
2 Spatial Streams														
0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76
1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73
2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71
3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68
4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64
5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60
6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59
7	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61	585	650	31	-58
8	256-QAM	3/4	156	173.3	29	-59	324	360	32	-56	702	780	35	-53
9	256-QAM	5/6			31	-57	360	400	34	-54	780	866.7	37	-51

MCS 9, Short GI 400ns, Min SNR 37db, RSSI -51dBm



# We can capture data frame of 80MHz, MCS9, 2SS



- This time we can capture 80MHz MCS9 2SS data frame ( only 802.11-common without VHT PHY info ) in Windows environment
- Because capture hardware AWUS1900 4x4:3 and capture driver just write out 802.11-common fields in PPI header ( I hope to add more PHY info )
- Anyway we can capture 867Mbps frames !



# Check Very High Throughput information in beacon frame



80mhz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Char	Signal (dBm)	Rate (Mbps)	Type/Subtype	Source	Destination
1	0.000000	36	-40dBm	6	Beacon frame	Cisco_70:18:d0	Broadca
2	2.896000	36	-44dBm	6	Probe Request	IntelCor_a7:a1:b6	Broadca

<

> Frame 1: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on

> PPI version 0, 32 bytes

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags: .....

▼ IEEE 802.11 wireless LAN

> Fixed parameters (12 bytes)

▼ Tagged parameters (238 bytes)

- > Tag: SSID parameter set: ikeriri-5g
- > Tag: Supported Rates 6(B), 9(B), 12(B), 18(B), 24(B), 36(B), 48(B), 54
- > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
- > Tag: HT Capabilities (802.11n D1.10)
- > Tag: RSN Information
- > Tag: HT Information (802.11n D1.10)
- > Tag: Extended Capabilities (8 octets)
- > Tag: Cisco CCX1 CKIP + Device Name
- > Tag: VHT Capabilities
- > Tag: VHT Operation
- > Tag: VHT Tx Power Envelope
- > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
- > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
- > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
- > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
- > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Enabled
- > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (24)

Select #1 packet to extract  
IEEE802.11 wireless LAN  
header > Tagged parameters  
> VHT Capabilities header

Check the each field of VHT  
Capabilities



# VHT Capabilities shows AP spec



## Extract VHT Capabilities > VHT Capabilities Info

▼ VHT Capabilities Info: 0x0f8259b2

```
.....10 = Maximum MPDU Length: 11 454 (0x2)
.....00.. = Supported Channel Width Set: Neither 160MHz nor 80+80 supported (0x0)
.....1.... = Rx LDPC: Supported
.....1. .... = Short GI for 80MHz/TVHT MODE 4C: Supported
.....0. .... = Short GI for 160MHz and 80+80MHz: Not supported
.....1... .... = Tx STBC: Supported
.....001 .... = Rx STBC: 1 Spatial Stream Supported (0x1)
.....1... .... = SU Beamformer Capable: Supported
.....1 .... = SU Beamformee Capable: Supported
.....010. .... = Beamformee STS Capability: 3 (0x2)
.....010 .... = Number of Sounding Dimensions: 3 (0x2)
.....0... .... = MU Beamformer Capable: Not supported
.....0 .... = MU Beamformee Capable: Not supported
.....0. .... = TXOP PS: Not supported
.....0.. .... = +HTC-VHT Capable: Not supported
.....11 1... .... = Max A-MPDU Length Exponent: 1 048 575 (0x7)
.....11.. .... = VHT Link Adaptation: Both (can provide unsolicited feedback and respon
.....0 .... = Rx Antenna Pattern Consistency: Not supported
.....0. .... = Tx Antenna Pattern Consistency: Not supported
000.. .... = Extended NSS BW Support: 0x0
```



# Rx/Tx MCS Map



## ▼ Rx MCS Map: 0xffffa

.... ..10	= Rx 1 SS: MCS 0-9 (0x2)
.... ..10..	= Rx 2 SS: MCS 0-9 (0x2)
.... ..11 ....	= Rx 3 SS: Not Supported (0x3)
.... ..11.. ....	= Rx 4 SS: Not Supported (0x3)
.... ..11 ....	= Rx 5 SS: Not Supported (0x3)
.... 11.. ....	= Rx 6 SS: Not Supported (0x3)
..11 ....	= Rx 7 SS: Not Supported (0x3)
11.. ....	= Rx 8 SS: Not Supported (0x3)

## ▼ Tx MCS Map: 0xffffa

.... ..10	= Tx 1 SS: MCS 0-9 (0x2)
.... ..10..	= Tx 2 SS: MCS 0-9 (0x2)
.... ..11 ....	= Tx 3 SS: Not Supported (0x3)
.... ..11.. ....	= Tx 4 SS: Not Supported (0x3)
.... ..11 ....	= Tx 5 SS: Not Supported (0x3)
.... 11.. ....	= Tx 6 SS: Not Supported (0x3)
..11 ....	= Tx 7 SS: Not Supported (0x3)
11.. ....	= Tx 8 SS: Not Supported (0x3)

Extract VHT Capabilities  
> Rx/Tx MCS Map  
This AP can use 1 or 2  
spatial streams with  
MCS 0-9 in sending and  
receiving frame.



# MCS number table



VHT MCS	Modulation	Coding
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

- 11ac MCS number is simple to understand, in any bandwidth and streams, the MCS number indicates the same Modulation and Coding.
- 256QAM Modulation and 5/6 coding are used in MCS9 in AC (just 1 symbol sends 256 value =  $2^8$  8bits and send 5bits then add 1 error correction bit )



# STA's Probe Request and AP's Probe Response



Select #2/3 frames and extract IEEE802.11 wireless LAN

```
> Frame 2: 110 bytes on wire (880 bits), 110
> PPI version 0, 32 bytes
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: .....
✓ IEEE 802.11 wireless LAN
```

```
  ✓ Tagged parameters (54 bytes)
```

```
    > Tag: SSID parameter set: Wildcard SSID
    > Tag: Supported Rates 6, 9, 12, 18, 24,
    > Tag: HT Capabilities (802.11n D1.10)
```

```
  ✓ Tag: VHT Capabilities
```

```
    Tag Number: VHT Capabilities (191)
```

```
    Tag length: 12
```

```
  > VHT Capabilities Info: 0x039179f6
```

```
  > VHT Supported
```

```
  > Rx MCS Map: Supported Channel Width Set: 160MHz supported (0x1)
```

```
  > Tx MCS Map: Rx LDPC: Supported
```

```
    Short GI for 80MHz/TVHT_MODE_4C: Supported
```

```
    Short GI for 160MHz and 80+80MHz: Supported
```

```
    Rx STBC: Supported
```

```
    Rx STBC: 1 Spatial Stream Supported (0x1)
```

```
    SU Beamformer Capable: Supported
```

```
    SU Beamformee Capable: Supported
```

```
    Beamformee STS Capability: 4 (0x3)
```

> Tagged parameters

> VHT capabilities

Intel card send 11ac spec information

This STA can use 160MHz bandwidth as well as 80+80 (optional) bandwidth, but AP cannot.





# STA's Association Request and AP's Association Response



Select #6/7 frames and extract IEEE802.11 wireless LAN

Maximum MPDU Length: 11 454 (0x2)

Supported Channel Width Set: Neither 160MHz nor 80+80 supported

Rx LDPC: Supported

Short GI for 80MHz/TVHT\_MODE\_4C: Supported

Short GI for 160MHz and 80+80MHz: Not supported

Tx STBC: Supported

Rx STBC: 1 Spatial Stream Supported (0x1)

SU Beamformer Capable: Supported

SU Beamformee Capable: Supported

Beamformee STS Capability: 3 (0x2)

Number of Sounding Dimensions: 2 (0x1)

MU Beamformer Capable: Not supported

MU Beamformee Capable: Not supported

TXOP PS: Not supported

+HTC-VHT Capable: Not supported

Max A-MPDU Length Exponent: 1 048 575 (0x7)

VHT Link Adaptation: No Feedback (0x0)

Rx Antenna Pattern Consistency: Not supported

Tx Antenna Pattern Consistency: Not supported

Extended NSS BW Support: 0x0

> Tagged parameters

> VHT capabilities

STA says 160MHz or 80+80MHz but AP choose 80MHz bandwidth to associate.



# 160MHz MCS8/9 2SS in Wave 2



- 11ac has option specifications a.k.a. wave 2  
160MHz or 80+80 MHz bandwidth, MCS 8 or 9,  
256QAM, and 4 spatial streams
- In actual 80+80MHz is compli-  
-cated so many AP uses 160MHz  
( sometimes called as VHT160)  
and many laptop supports 2 spatial streams
- Finally the throughput is reached at 1.7Gbps





# 2 special streams 160MHz 1733Mbps



802.11ac - VHT

MCS, SNR and RSSI

VHT MCS	Modulation	Coding	20MHz				40MHz				80MHz				160MHz			
			Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI	Data Rate		Min. SNR	RSSI
			800ns	400ns			800ns	400ns			800ns	400ns			800ns	400ns		
2 spatial streams																		
0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76	117	130	11	-73
1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71	351	390	18	-68
3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59	1053	1170	29	-56
7	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61	585	650	31	-58	1170	1300	34	-55
8	256-QAM	3/4	156	173.3	29	-59	324	360	32	-56	702	780	35	-53	1404	1560	38	-50
9	256-QAM	5/6			31	-57	360	400	34	-54	780	866.7	37	-51	1560	1733.3	40	-48

MCS 9, Short GI, Min SNR 40db, required RSSI -48dBm

The laptop logical speed can be reached at 1.7Gbps

Netgear R7800 -100NAS (v2)  
Availability: now

Manuf/OEM/ODM Delta Networks

FCC approval date: 04 November 2015  
(Est.) release date: 04 January 2016  
Country of manuf.: China  
Series: AC2600

Amazon image

ASIN  
B0192911RA (🇺🇸, On Amazon🇯🇵, On CCC🇨🇳)  
On Newegg🇺🇸

Type: wireless router

FCC ID: PTC15100013  
PCB ID: 2976495801

Power: 12 VDC, 3.5 A  
Connector type: barrel

CPU1: Qualcomm IPQ8065 (1.7 GHz, 2 cores)  
FLA1: 128 MiB (Micron MT29F1G08ABBEAH4:E)  
RAM1: 512 MiB (Nanya NT5CC128M16IP-DI x 2)

Expansion IFS: USB 3.0, eSATA  
USB ports: 2  
SATA ports: 1  
Serial: yes

WI1 chip1: Qualcomm Atheros QCA9984  
WI1 802dot11 protocols: an+ac  
WI1 MIMO config: 4x4:4  
WI1 antenna connector: U.FL  
WI2 chip1: Qualcomm Atheros QCA9984  
WI2 802dot11 protocols: bgn  
WI2 MIMO config: 4x4:4  
WI2 antenna connector: U.FL

# Netgear R7800 Nighthawk X4S

ETH chip1: Qualcomm IPQ8065  
Switch: Qualcomm Atheros QCA8337  
LAN speed: 10/100/1000  
LAN ports: 4  
WAN speed: 10/100/1000  
WAN ports: 1

abgn+ac

Additional chips  
2.4GHz Power Amplifier Module;Skyworks;SE2623L;4;  
5GHz Power Amplifier Module;RFMD;RFPA5542;4;

Stock bootloader: U-Boot

Stock FW OS: Linux

Third party firmware supported: DD-WRT (Kong-AC) • (List), LEDE Project • (List)

Flags: Wave2, MU-MIMO, VHT160, DFS

Default IP address: <http://www.routerlogin.net>  
the IP <http://www.routerlogin.net> is used by 3 additional devices  
of which 3 are Netgear devices  
Default login user: admin  
Default login password: password  
admin:password credentials used by 381 additional devices  
of which 274 are Netgear devices

802dot11 OUI: none specified



I tried Netgear R7800  
Nighthawk X4S, supports  
abgn+ac, wave2, MU-MIMO,  
VHT160, DFS.

5GHz chipset is Qualcomm  
Atheros QCA9984 (4x4:4)

There are open source  
firmware but it is prohibited  
in Japan (radio law...)



# Netgear R7800 Nighthawk X4S and Intel Wireless-AC 9260NGW



- In November 2018, there are a few combination of AP and STA to get 1.7Gbps
- Also we cannot always get maximum logical speed because of RSSI, SNR, other radio signal, etc.
- 80+80Mhz bandwidth settings may not work ( if supported )



Home

Internet

Wireless

Attached Devices

Quality of Service

Parental Controls

ReadySHARE

Guest Network

NETGEAR Downloader (BETA)

VPN Client

Wireless Settings

Cancel Apply

WPAWPA2 Enterprise

Security Options (WPA2-PSK)

Password (Network Key): wireshark (8-63 characters or 64 hex digits)

Wireless Network (5GHz 802.11a/n/ac)

Enable SSID Broadcast

Name (SSID): ikeriri-ac

Channel: 100(DFS)

Mode: Up to 1733 Mbps

Security Options

None

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

Security

NETGEAR Downloader (BETA)

Administration

Advanced Setup

Wireless Settings

Router / AP / Bridge Mode

Port Forwarding / Port Triggering

Dynamic DNS

VPN Service

Static Routes

Remote Management

USB Settings

UPnP

IPv6

Traffic Meter

VLAN/Queue Settings

LED Control Settings

VPN Client

Help & Support

Documentation | Online Support | Router FAQ | Q&A QIP

Advanced Wireless Settings (5GHz 802.11a/n/ac)

Enable Wireless Router Radio

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period Start End Recurrence Pattern

Add a new period Edit Delete

WPS Settings

Router's PIN

Enable Router's PIN

To prevent PIN compromise, auto disable the PIN after 3 failed PIN connections, until router reboots.

In auto disabled mode, router's WPS LED will keep blinking slowly

Keep Existing Wireless Settings

Enable Implicit BEAMFORMING - Boosts

Enable MU-MIMO

Enable HT160

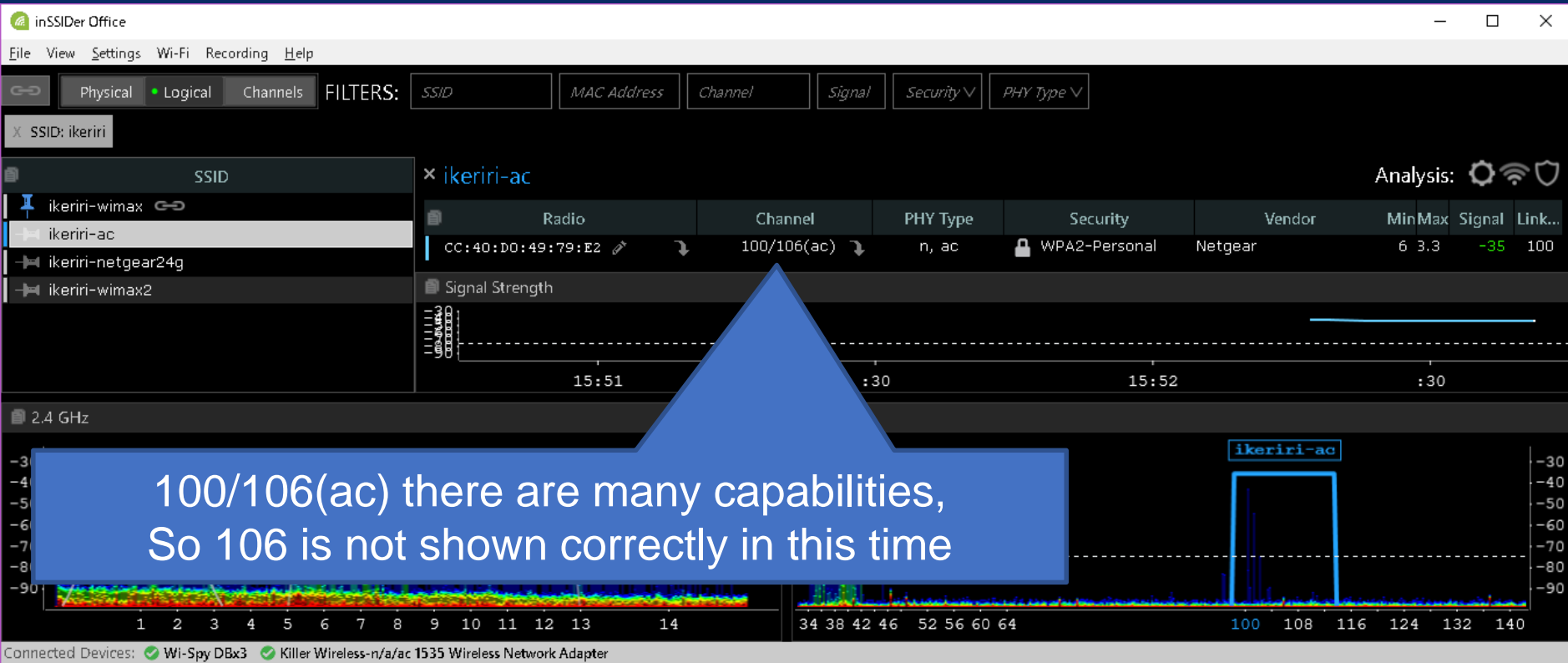
# Set up like this



- SSID: ikeriri-ac
- WPA2-PSK  
passphrase:wireshark
- Set channel (100) and mode as up to 1733Mbps
- Enable HT160 (important)
- Enable Implicit BEAMFORMING
- Enable MU-MIMO



# Check the spectrum using InSSIDer Office







# Linked up at 1.7Gbps



NETGEAR<sup>®</sup> genie<sup>™</sup>

Nighthawk(R) X4S R7800

BASIC ADVANCED

ADVANCED Home

Setup Wizard

WPS Wizard

Setup

ReadySHARE

Security

NETGEAR  
Downloader (BETA)

Administration

Advanced Setup

## Router Information

Hardware Version	R7800
Firmware Version	V1.0.2.52
GUI Language Version	V1.0.0.330
Operation Mode	Router
LAN Port	
MAC Address	CC:40:D0:49:79:E0
IP Address	192.168.1.1
DHCP Server	On

Reboot

## Internet Port

MAC Address	CC:40:D0:49:79:E1
IP Address	192.168.100.103
Connection	DHCP
IP Subnet Mask	255.255.255.0
Domain Name Server	8.8.8.8

Show Statistics

Connection Status

## Wireless Settings (2.4GHz)

Name (SSID)	ikeriri-netgear24g
Region	Japan
Channel	Auto ( 4(p) + 8(s) )
Mode	Up to 800 Mbps
Wireless AP	On
Broadcast Name	On
Wi-Fi Protected Setup	Configured

## Wireless Settings (5.0GHz)

Name (SSID)	ikeriri-ac
Region	Japan
Channel	100(p)+104+108+112 +116+120+124+128
Mode	Up to 1733 Mbps
Wireless AP	On
Broadcast Name	On
Wi-Fi Protected Setup	Configured

Help & Support Documentation | Online Support | Router FAQ | GNU GPL

Wi-Fi 6 の状態

全般

接続

IPv4 接続: インターネット

IPv6 接続: ネットワーク アクセスなし

状態: 有効

SSID: ikeriri-ac

継続時間: 00:00:07

速度: 1.7 Gbps

信号の状態:

詳細(E)... ワイヤレスのプロパティ(W)

動作状況

送信 受信

バイト: 70,002 84,464

プロパティ(P) 無効にする(D) 診断(G)

閉じる(C)

MCS 9, Short GI, Min SNR 40db, required RSSI -48dBm





# netsh wlan sh all



Open command prompt to  
type "netsh wlan sh all"

You may find receive rate  
and send rate is 1733.3Mbps

( some info is written in Japanese )

OK, let's start capturing ! Wait,  
VHT160 is not supported by  
ALFA Realtek RTL8814AU...

```
コマンドプロンプト

===== インターフェイスの表示 =====

システムに 1 インターフェイスがあります:

名前                : Wi-Fi 6
説明                : Intel(R) Wireless-AC 9260
GUID                : 6c3b344e-a6d4-46f9-a353-1b
物理アドレス       : 0c:54:15:a7:a1:b6
状態                : 接続されました
SSID                : ikeriri-ac
BSSID               : cc:40:d0:49:79:e2
ネットワークの種類 : インフラストラクチャ
無線の種類         : 802.11ac
認証                : WPA2-パーソナル
暗号                : CCMP
接続モード         : プロファイル
チャネル            : 100
受信速度 (Mbps)    : 1733.3
送信速度 (Mbps)    : 1733.3
シグナル            : 95%
プロファイル       : ikeriri-ac
```



# Open 160Mhz.pcapng in Wireshark



There are no icmp frame, but we can utilize them !

160Mhz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Signal (dBm)	Rate (Mbps)	Type/Subtype	Source	Destination	Protocol	Length	Info
1	0.000000	-28dBm	6	Beacon frame	Netgear_49:79:e2	Broadcast	802.11	368	Beacon frame, SN=2588, FN=0, Flags=....., BI=100, SSID=ikeriri-ac
2	4.649000	-37dBm	6	Probe Request	IntelCor_a7:a1:b6	Broadcast	802.11	110	Probe Request, SN=163, FN=0, Flags=....., SSID=Wildcard (Broadcast)
3	4.649000	-27dBm	6	Probe Response	Netgear_49:79:e2	IntelCor_a7:a1:b6	802.11	469	Probe Response, SN=47, FN=0, Flags=....., BI=100, SSID=ikeriri-ac
4	8.805000	-37dBm	6	Authentication	IntelCor_a7:a1:b6	Netgear_49:79:e2	802.11	62	Authentication, SN=16, FN=0, Flags=.....
5	8.805000	-29dBm	6	Authentication	Netgear_49:79:e2	IntelCor_a7:a1:b6	802.11	62	Authentication, SN=49, FN=0, Flags=.....
6	8.805000	-37dBm	6	Association R..	IntelCor_a7:a1:b6	Netgear_49:79:e2	802.11	232	Association Request, SN=17, FN=0, Flags=....., SSID=ikeriri-ac
7	8.805000	-28dBm	6	Association R..	Netgear_49:79:e2	IntelCor_a7:a1:b6	802.11	229	Association Response, SN=50, FN=0, Flags=.....
8	8.825000	-27dBm	6	QoS Data	Netgear_49:79:e2	IntelCor_a7:a1:b6	EAPOL	165	Key (Message 1 of 4)
9	8.825000	-37dBm	6	QoS Data	IntelCor_a7:a1:b6	Netgear_49:79:e2	EAPOL	189	Key (Message 2 of 4)
10	8.856000	-28dBm	6	QoS Data	Netgear_49:79:e2	IntelCor_a7:a1:b6	EAPOL	221	Key (Message 3 of 4)
11	8.856000	-38dBm	6	QoS Data	IntelCor_a7:a1:b6	Netgear_49:79:e2	EAPOL	165	Key (Message 4 of 4)
12	8.906000	-72dBm	54	QoS Data	0.0.0.0	255.255.255.255	DHCP	426	DHCP Request - Transaction ID 0x3daae13d

< >

> Frame 1: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface 0

> PPI version 0, 32 bytes

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags: .....

> IEEE 802.11 wireless LAN

```
0000 00 00 20 00 69 00 00 02 00 14 00 8c 00 00 00 .. .i... ..
0010 0f 96 0e 00 00 00 0c 00 7c 15 50 01 00 00 e4 a0 ..... |.P...
0020 80 00 00 00 ff ff ff ff ff ff cc 40 d0 49 79 e2 ..... @.Iy..
```

160Mhz.pcapng

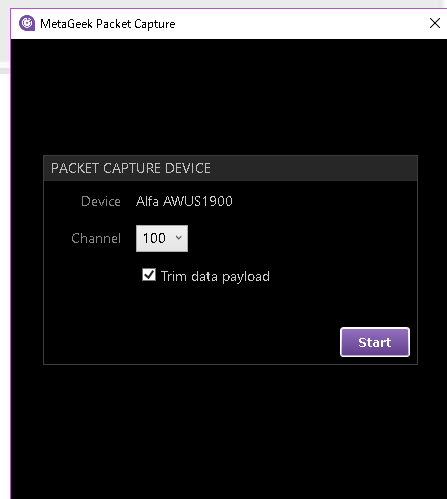
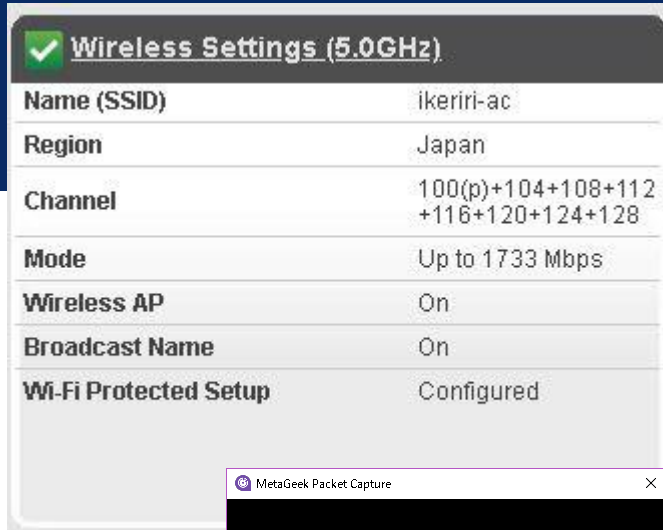
Packets: 12 · Displayed: 12 (100.0%)

Profile: 11ac



# Open 160Mhz.pcap

- We can capture beacon, probe request / response, authentication, association request / response, wpa2-psk 4way handshake, and few data frames that sent in a low rate because capture hardware and capture driver do not support 160Mhz bandwidth...
- But we can capture all connection process, all 4way handshake, deauth, disassoc, and other management frames for analysis.
- We can debug and troubleshoot !





# Select #1 beacon frame and extract VHT capabilities



Maximum MPDU Length: 11 454 (0x2)

Supported Channel Width Set: 160MHz supported (0x1)

Rx LDPC: Supported

Short GI for 80MHz/TVHT\_MODE\_4C: Supported

Short GI for 160MHz and 80+80MHz: Supported

Tx STBC: Supported

Rx STBC: 1 Spatial Stream Supported (0x1)

SU Beamformer Capable: Supported

SU Beamformee Capable: Supported

Beamformee STS Capability: 4 (0x3)

Number of Sounding Dimensions: 4 (0x3)

MU Beamformer Capable: Supported

MU Beamformee Capable: Not supported

TXOP PS: Not supported

+HTC-VHT Capable: Not supported

Max A-MPDU Length Exponent: 1 048 575 (0x7)

VHT Link Adaptation: No Feedback (0x0)

Rx Antenna Pattern Consistency: Supported

Tx Antenna Pattern Consistency: Supported

Extended NSS BW Support: 0x0

Select #1 frame and extract IEEE802.11 wireless LAN > Tagged parameters > VHT Capabilities > VHT Capabilities Info and check each field.

You can find both AP and STA support 160Mhz



# Select #2/3 probe request / probe response frame



- > Frame 2: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
  - > PPI version 0, 32 bytes
  - > 802.11 radio information
  - > IEEE 802.11 Probe Request, Flags: .....
    - ▼ IEEE 802.11 wireless LAN
      - ▼ Tagged parameters (54 bytes)
        - > Tag: SSID parameter set: Wildcard SSID
        - > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
        - > Tag: HT Capabilities (802.11n D1.10)
        - ▼ Tag: VHT Capabilities
          - Tag Number: VHT Capabilities (191)
          - Tag length: 12
          - > VHT Capabilities Info: 0x039179f6
          - > VHT Supported MCS Set
          - > Rx MCS Map: 0xffff
          - > Tx MCS Map: 0xffff
- > Frame 3: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface 0
- > PPI version 0, 32 bytes
- > 802.11 radio information
- > IEEE 802.11 Probe Response, Flags: .....
  - ▼ IEEE 802.11 wireless LAN
    - > Fixed parameters (12 bytes)
    - ▼ Tagged parameters (401 bytes)
      - > Tag: SSID parameter set: ikeriri-ac
      - > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      - > Tag: DS Parameter set: Current Channel: 100
      - > Tag: Country Information: Country Code JP, Environment Any
      - > Tag: Power Constraint: 3
      - > Tag: RM Enabled Capabilities (5 octets)
      - > Tag: HT Capabilities (802.11n D1.10)
      - > Tag: HT Information (802.11n D1.10)
      - > Tag: Extended Capabilities (8 octets)
      - ▼ Tag: VHT Capabilities
        - > Tag: VHT Operation
        - > Tag: VHT Tx Power Envelope
        - > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
        - > Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
        - > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
        - > Tag: RSN Information
        - > Tag: Vendor Specific: Microsoft Corp.: WPS
        - > Tag: Vendor Specific: Netgear

Check VHT Capabilities in  
probe request / response



# Select #6/7 association request / association response frame



```
> Frame 6: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on :
> PPI version 0, 32 bytes
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....
> IEEE 802.11 wireless LAN
  > Fixed parameters (4 bytes)
  > Tagged parameters (172 bytes)
    > Tag: SSID parameter set: ikeriri-ac
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 0, Max: 12
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Extended Capabilities (10 octets)
    > Tag: VHT Capabilities
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```

```
> Frame 7: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on :
> PPI version 0, 32 bytes
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....
> IEEE 802.11 wireless LAN
  > Fixed parameters (6 bytes)
  > Tagged parameters (167 bytes)
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: Extended Capabilities (4 octets)
    > Tag: Vendor Specific: Microsoft Corp.: WPS
    > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
```

## Check VHT Capabilities in association request / association response



# We can **partly** debug and troubleshoot 160Mhz bandwidth



Unfortunately this time we can capture 80MHz data frame at 867Mbps, cannot capture 160MHz bandwidth. Other 160MHz bandwidth WLAN card such as Atheros may be used in windows environment in the future.

But we can still capture and troubleshoot 160MHz bandwidth to look other compatible frames, such as management, control and 4way handshake frames.

## Wireshark opens the door to dissect 11ac !

# USE WIRESHARK

Thank you for attending !

どうもありがとうございました



Supplemental file

<http://www.ikeriri.ne.jp/sharkfest>



いけりり★ネットワークサービス

<http://www.ikeriri.ne.jp>