802.11

tricks & treats by @090h

802.11 basics

__init__

- Created by: NCR Corporation/AT&T
- Invention: 1991 (Wave LAN)
- Father: Vic Hayes
- Name: taken from Hi-Fi
- Frequency: 2.4GHz UHF and 5GHz SHF
- Public release: 1997
- Maximum speed: 2Mbit/s

802.11 legacy

- Date: June 1997
- Frequency: 2.4 GHz
- Bandwidth: 22 MHz
- Modulation: DSSS, FHSS
- Data rate: 1, 2 Mbit/s
- Range indoor: 20m
- Range outdoor: 100m

802.11a

- Date: September 1999
- Frequency: 5, 3.7 GHz
- Modulation: OFDM
- Bandwidth: 20 MHz
- Speed: 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
- Range indoor: 35m
- Range outdoor: 120m

802.11b

- Date: September 1999
- Frequency: 2.4 GHz
- Modulation: DSSS
- Bandwidth: 22 MHz
- Speed: 1, 2, 5.5, 11 Mbit/s
- Range indoor: 35m
- Range outdoor: 140m

802.11g

- Date: September 2003
- Frequency: 2.4 GHz
- Modulation: OFDM,DSSS
- Bandwidth: 20 MHz
- Speed: 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
- Range indoor: 38m
- Range outdoor: 140m

802.11n

- Date: October 2009
- Frequency: 2.4/5 GHz
- Modulation: OFDM
- Bandwidth: 20 MHz, 40 MHz
- Speed in Mbit/s
- [7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2]
- [15, 30, 45, 60, 90, 120, 135, 150]
- Range indoor: 70m
- Range outdoor: 250m
- MIMO: 4x4 or SISO: 1x1

802.11ac

- Date: December 2013
- Frequency: 5 GHz
- Modulation: OFDM
- Bandwidth: 20 MHz, 40 MHz, 80 MHz, 160 MHz
- Speed in Mbit/s
- [7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3]
- [15, 30, 45, 60, 90, 120, 135, 150, 180, 200]
- [32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3]
- [65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7]
- Range indoor: 35m Range outdoor: NO!
- MIMO: 8x8 streams!

802.11 1999-2016

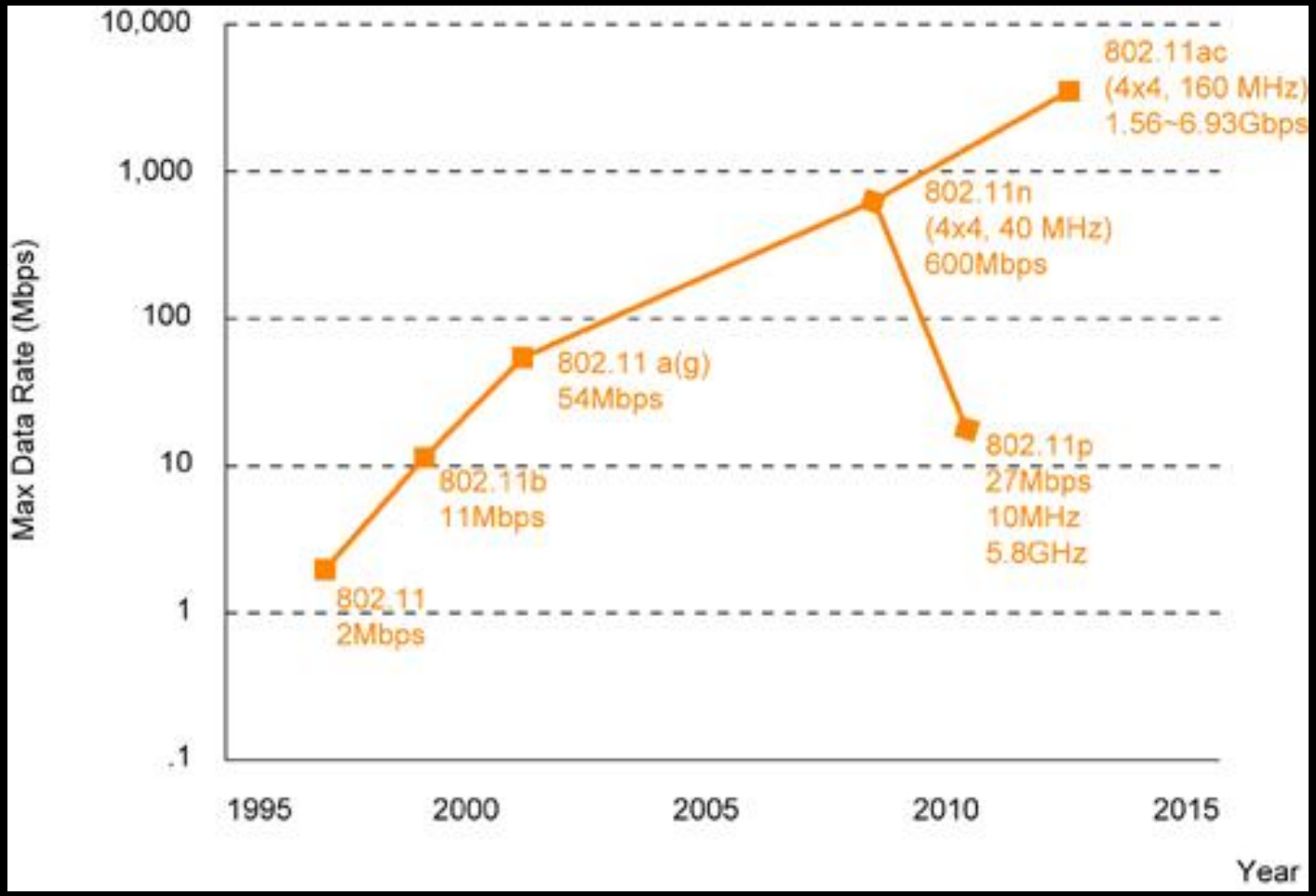
802.11 standard evolution					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

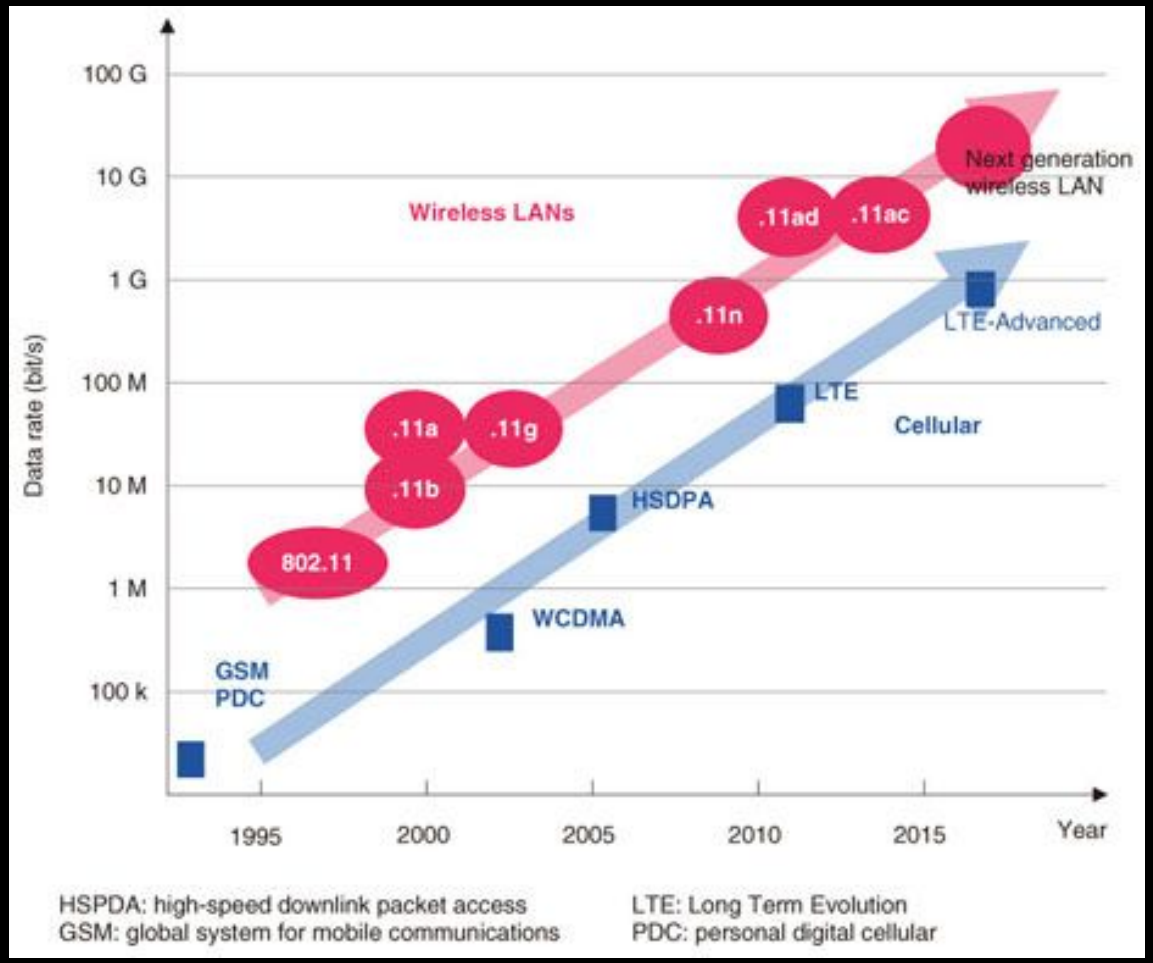
Nearest future

802.11 n/ac/ad Comparison

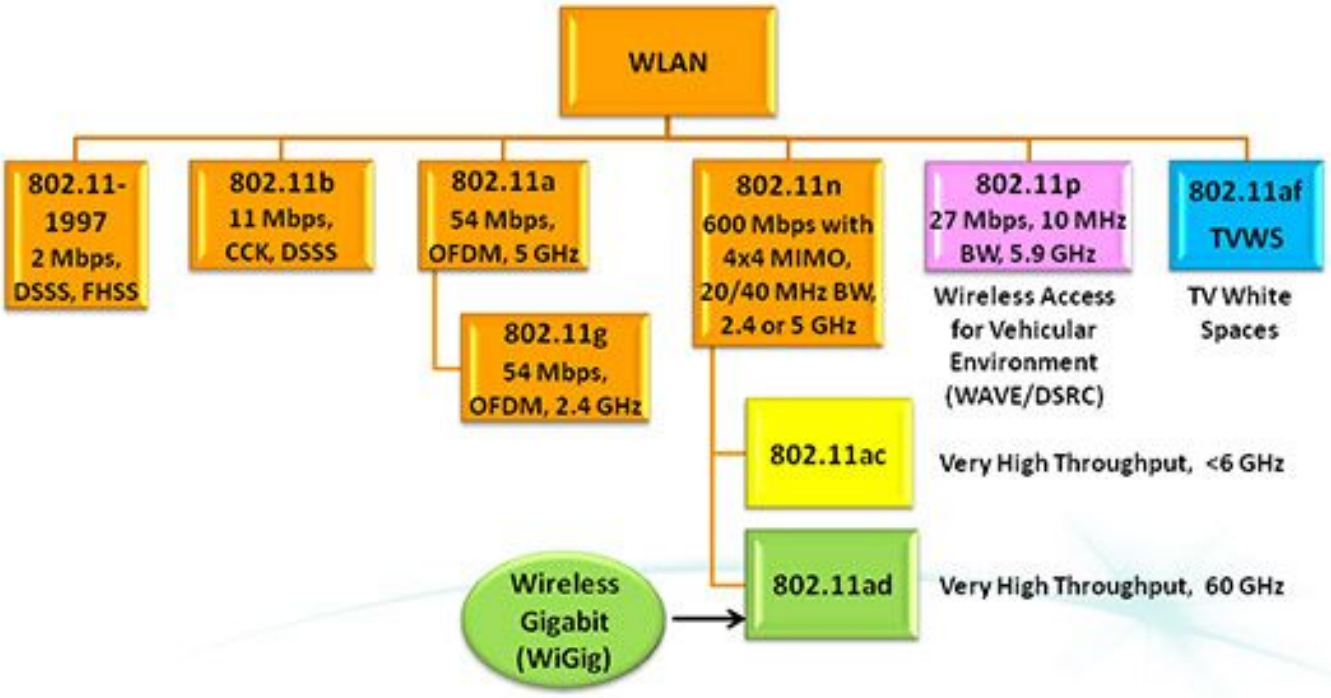
	802.11n	802.11ac	802.11ad
Throughput	600 Mbps	3.2 Gbps	Up to 7 Gbps
Coverage	Home, 70 m	Home, 30 m	Room, <5m
Freq. Band	2.4/5 GHz	5 GHz	2.4/5/60 GHz
Antennas	4 x 4 MIMO	8 x 8 MIMO	>10 x 10 MIMO
Applications	Data, Video	Video	Uncompressed Video

802.11 SPEED² EVOLUTION

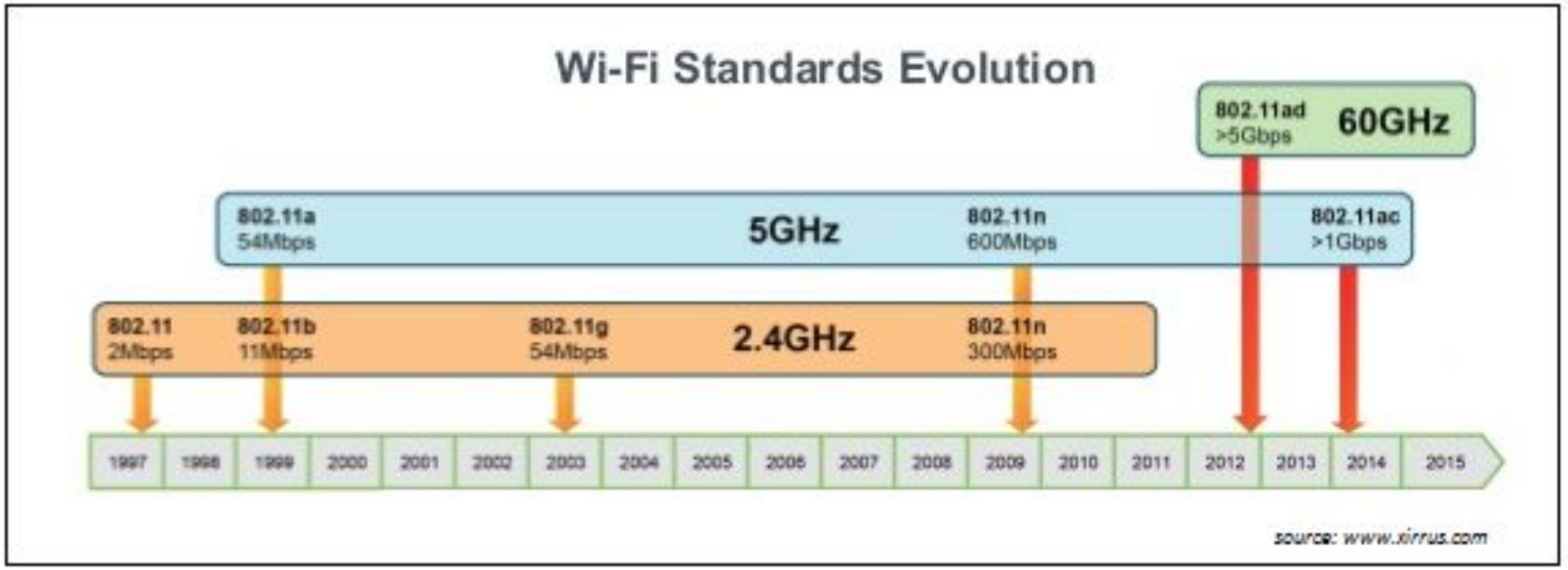



100 G
10 G
1 G
100 M
10 M
1 M
100 k
Data rate (bit/s)
Wireless LANs
802.11
.11a
.11b
.11g
.11n
.11ad
.11ac
Next generation wireless LAN
LTE-Advanced
LTE
Cellular
HSDPA
WCDMA
GSM
PDC
1995
2000
2005
2010
2015
Year
HSPDA: high-speed downlink packet access
GSM: global system for mobile communications
LTE: Long Term Evolution
PDC: personal digital cellular

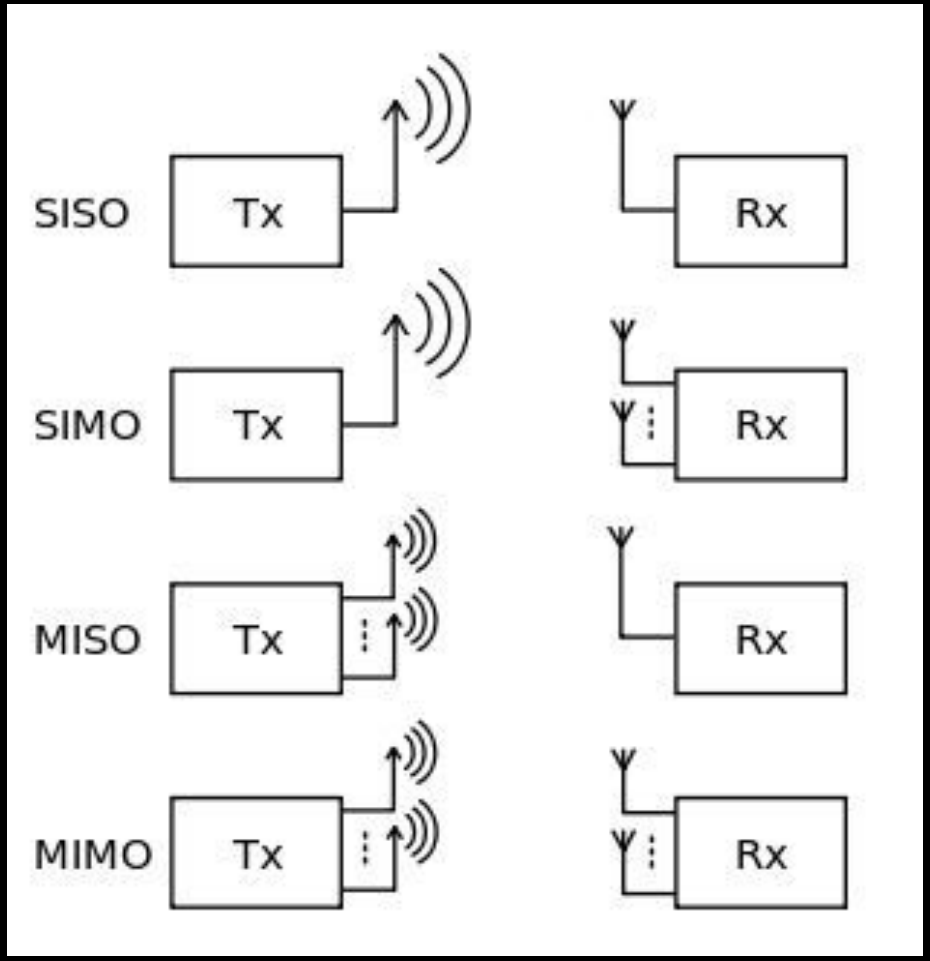
IEEE 802.11 Standards Evolution



DSRC = Dedicated Short-Range Communications


Wi-Fi Standards Evolution
802.11ad
>5Gbps
60GHz
802.11a
54Mbps
5GHz
802.11n
600Mbps
802.11ac
>1Gbps
802.11
2Mbps
802.11b
11Mbps
802.11g
54Mbps
2.4GHz
802.11n
300Mbps
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
source: www.xirrus.com

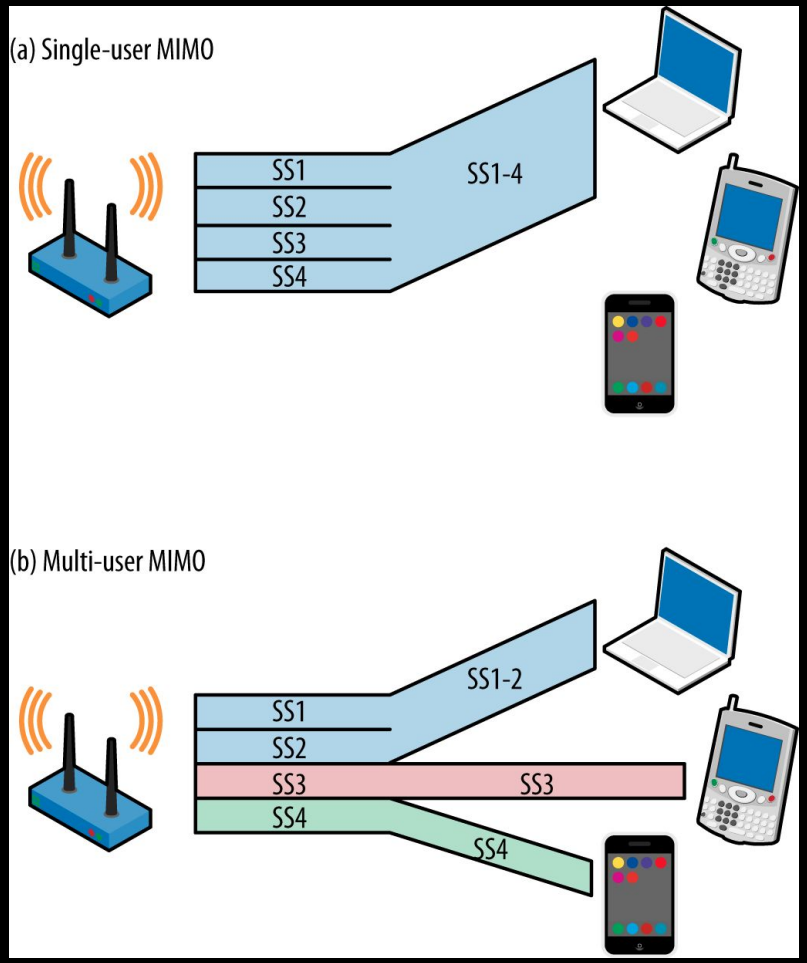
SISO/SIMO/MISO/MIMO



WTF is MIMO?

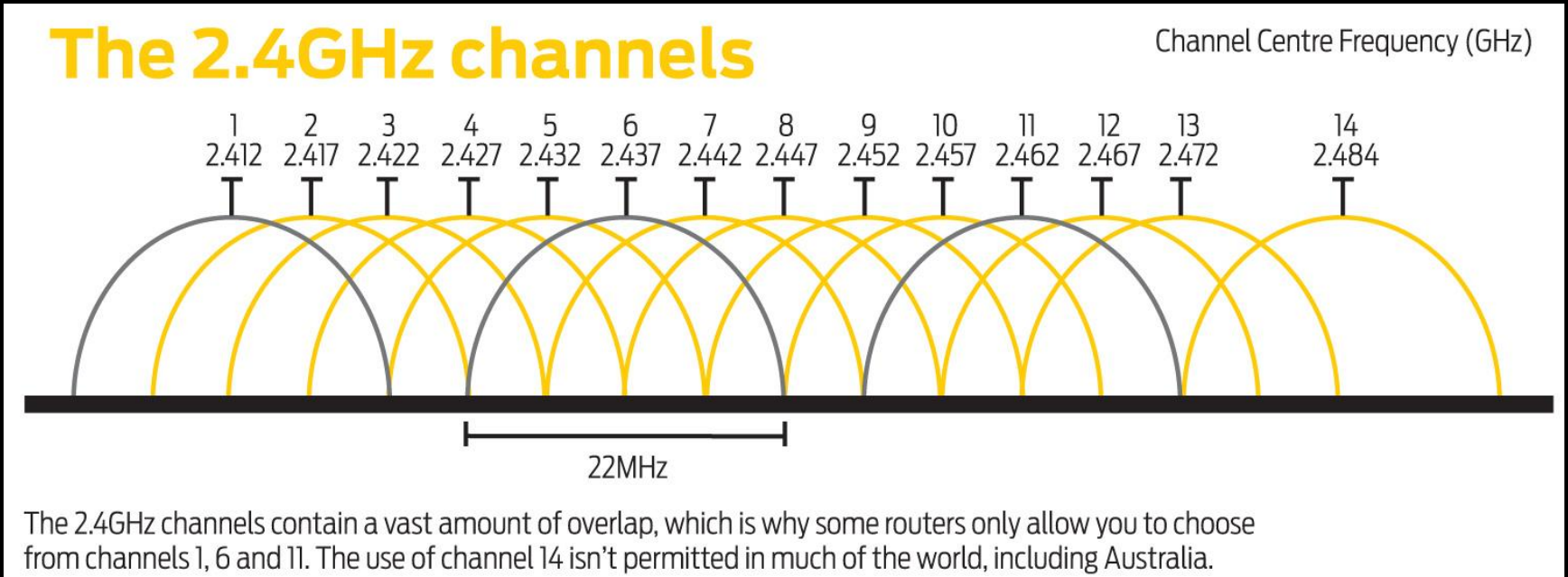

802.11n
450Mbps
SU-MIMO 802.11n
3x3, 40MHz, 150Mbps/Stream
11AC Wave 1
1.3Gbps
SU-MIMO 802.11ac
3x3, 80MHz, 433Mbps/Stream
11ac Wave 2
433Mbps
433Mbps
433Mbps
433Mbps
MU-MIMO 802.11ac
4x4, 80MHz, 433Mbps/Stream
11ac Wave 2
433Mbps
433Mbps
866Mbps
MU-MIMO 802.11ac
4x4, 80MHz, 433Mbps/Stream

MIMO vs MU-MIMO

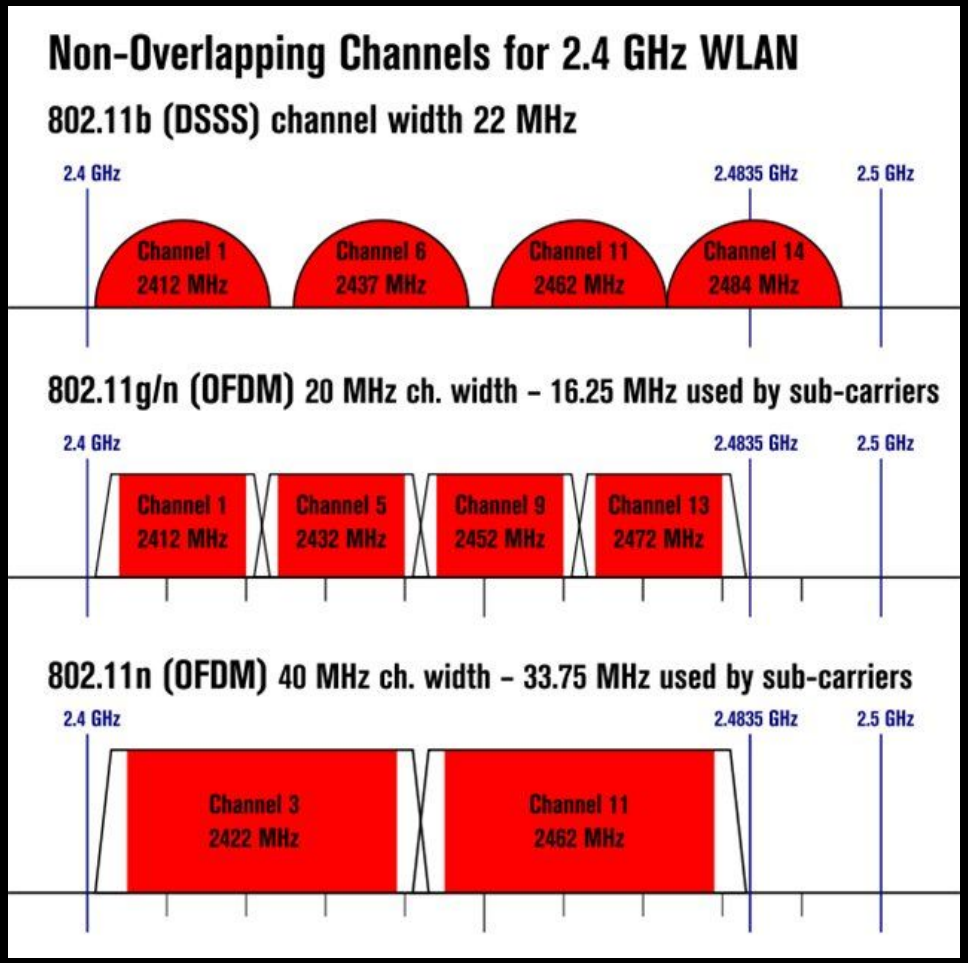


Channels and plans

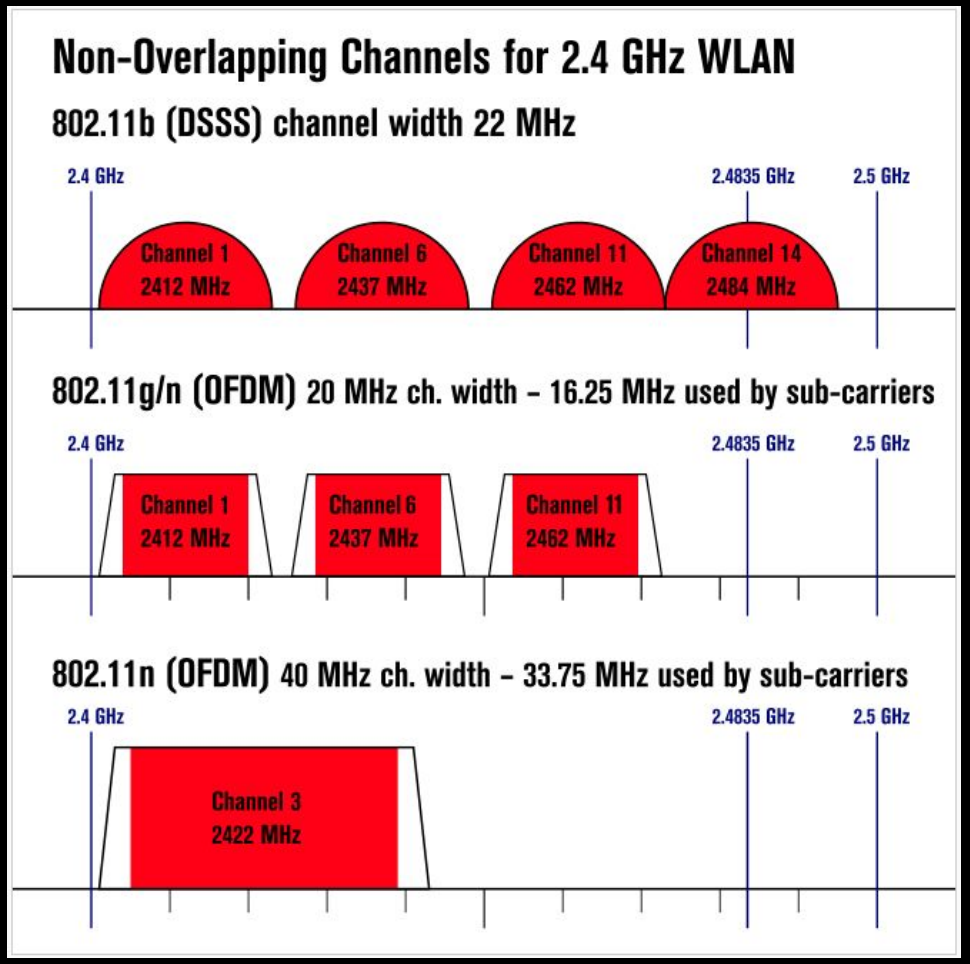
802.11b channels



2.4GHz channel plan world



2.4GHz channel plan US



Channel plans

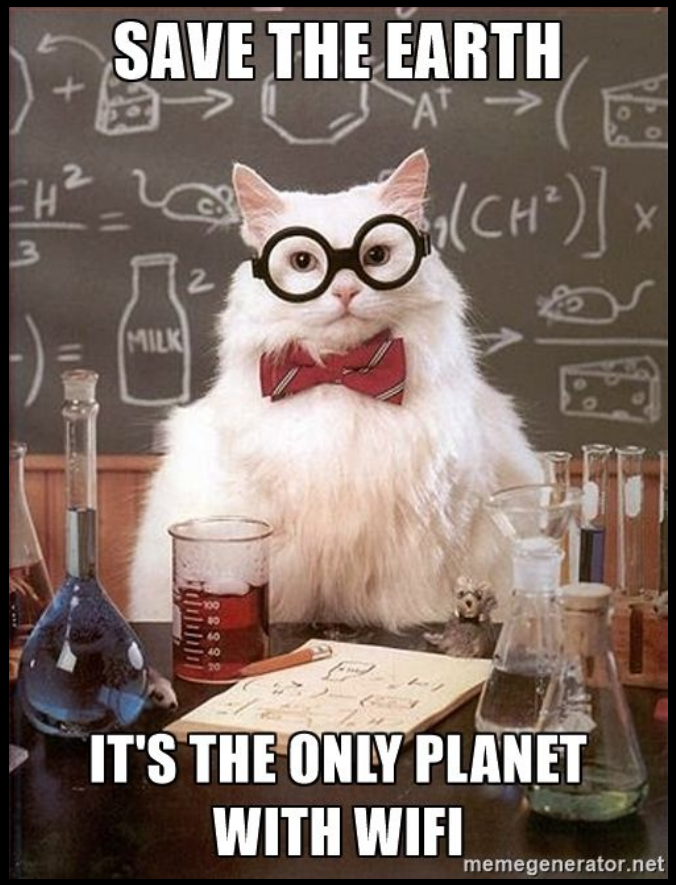
- US: 1 – 6 – 11
- JP: 1 – 5 – 9 – 13 – 14 for 802.11b
- WORLD: 1 – 5 – 9 – 13

IRL mistakes that killed 2.4GHz

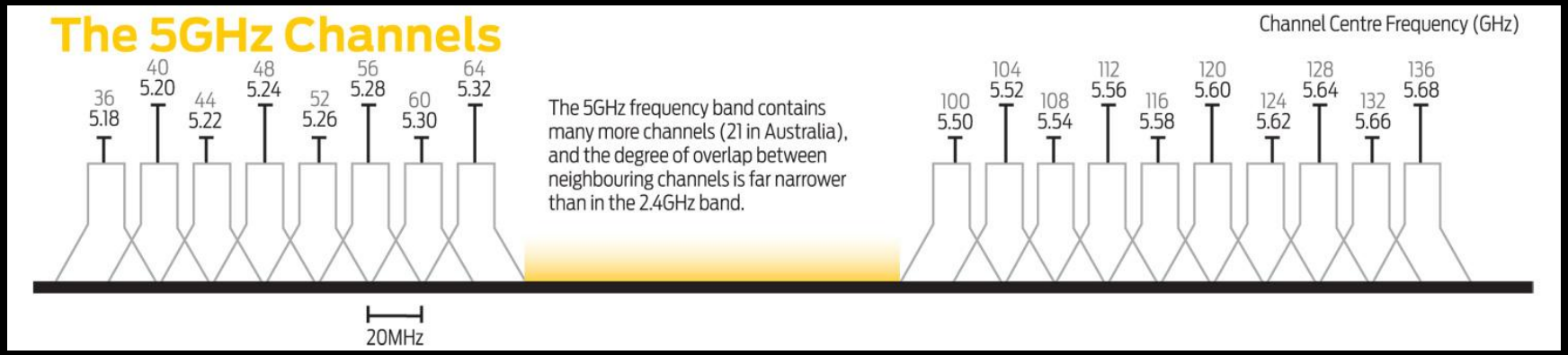
- WTF is channel plan?
- More bandwidth ~~more speed~~
- More power ~~more speed~~

Home Wi-Fi tweaks

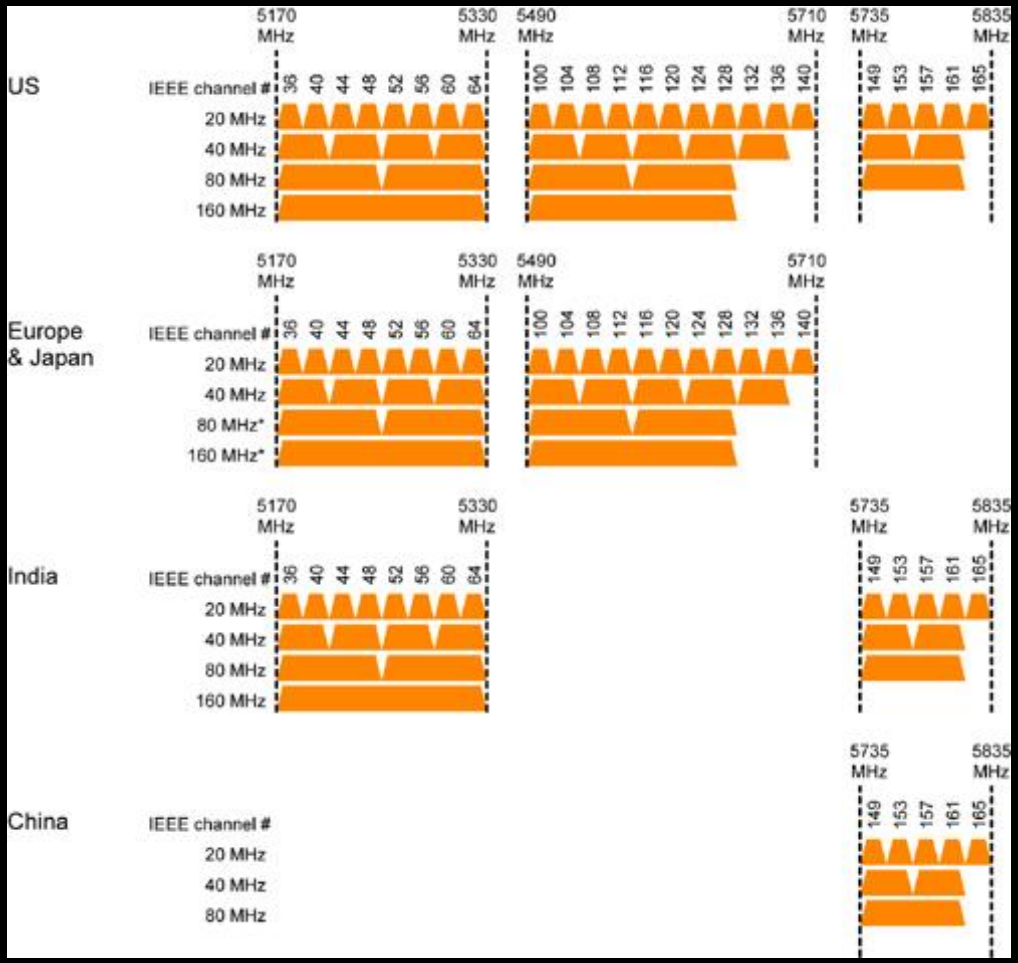
- Use ACS or set channel to most free (11 usually)
- Use 40MHz wisely
- Lower TX power if possible



5GHz channels



5GHz WORLD WIDE



Country □ RF limits □ CRDA

Allowed almost everywhere:

- Channels: 1- 11
- Signal strength (20dBm = 100mW)
- Omnidirectional antenna (6dBi)

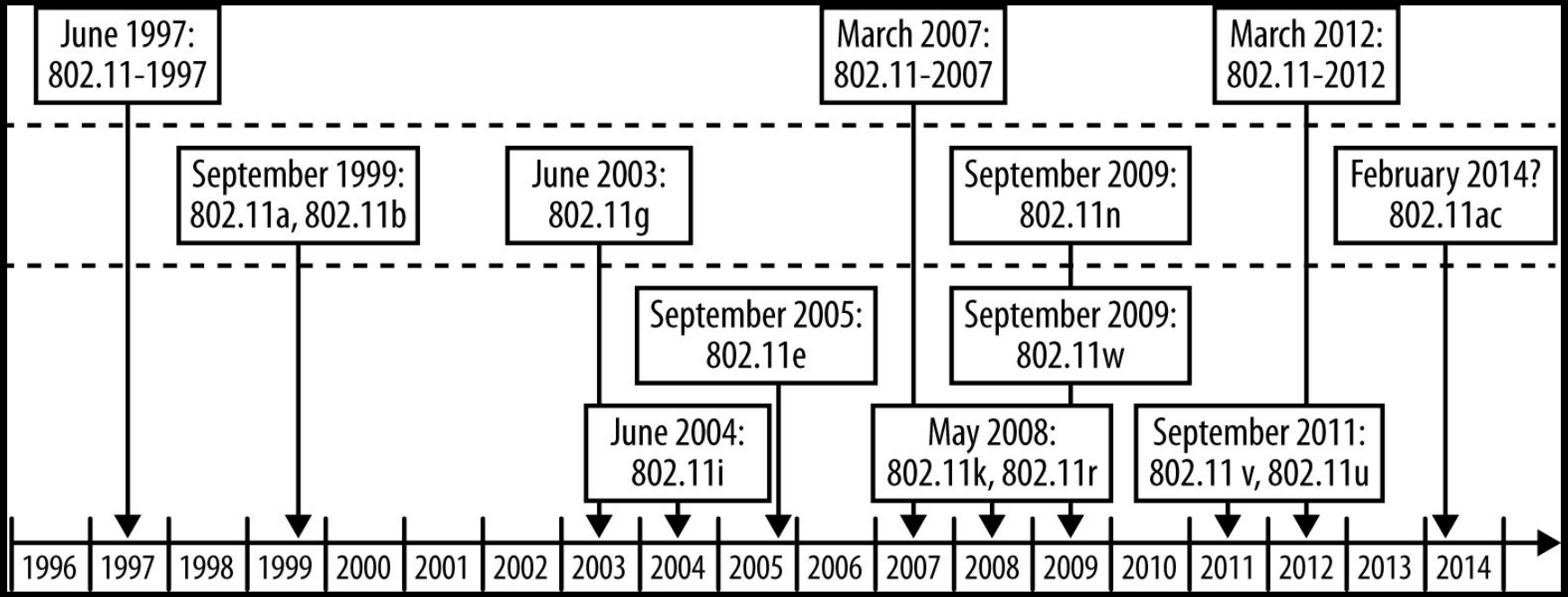
Free channel?

1. Уровень на входе приемника выше уровня среднего шума
2. На входе приемника есть реальный сигнал
3. Комбинированный = 1 + 2
4. Получение реального сигнала за фиксированный промежуток времени
5. Комбинированный = 1 + 4
6. Уровень на входе приемника выше уровня -82dBm, но меньше -62dBm. + канал занят, если уровень больше -72dBm и можно декодировать сигнал

https://wireless.wiki.kernel.org/en/users/documentation/acs

802.11 XXX

802.11 timeline



802.11i

- Security mechanisms for 802.11
- Auth, crypto
- Draft: 24 June 2004
- Released: IEEE 802.11-2007

P.S. China has WAPI
https://en.wikipedia.org/wiki/WLAN_Authentication_and_Privacy_Infrastructure

802.11e

- **Wi-Fi Multimedia (WMM), Wireless Multimedia Extensions (WME)**
- QoS for 802.11

802.11d

802.11d - is an amendment to the IEEE 802.11 specification that adds support for "additional regulatory domains".

Used to regulate:

- Channelization
- Hopping patterns

As of January 1, 2015, the U.S. Federal Communications Commission banned the use of 802.11d within the U.S.

802.11d

```
$ system_profiler SPAirPortDataType
Wi-Fi:

      Software Versions:
          CoreWLAN: 5.0 (500.35.2)
          CoreWLANKit: 4.3 (430.38.1)
          Menu Extra: 10.3 (1030.34)
          System Information: 9.0 (900.9)
          IO80211 Family: 7.3 (730.60)
          Diagnostics: 4.2 (420.71)
          AirPort Utility: 6.3.5 (635.2)
      Interfaces:
        en1:
          Card Type: AirPort Extreme  (0x14E4, 0xD6)
          Firmware Version: Broadcom BCM43xx 1.0 (5.106.98.100.24)
          MAC Address: 28:cf:da:dd:6e:6e
          Locale: RoW
          Country Code: TW
          Supported PHY Modes: 802.11 a/b/g/n
          Supported Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165
          Wake On Wireless: Supported
          AirDrop: Supported
          Status: Connected
          Current Network Information:
            HDNS:
              PHY Mode: 802.11n
              BSSID: c0:4a:00:6c:e2:a0
              Channel: 1
              Country Code: TW
              Network Type: Infrastructure
              Security: WPA2 Personal
              Signal / Noise: -37 dBm / -87 dBm
              Transmit Rate: 145
              MCS Index: 15
          Other Local Wi-Fi Networks:
            HDNS:
              PHY Mode: 802.11n
              BSSID: c0:4a:00:6c:da:42
              Channel: 1
```

802.11d in the wild

```
--
Aug 22 08:54:50 iPwn kernel[0]: en1: 802.11d country code set to 'X2'.
Aug 22 08:54:50 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 08:54:51 iPwn kernel[0]: en1: 802.11d country code set to 'US'.
Aug 22 08:54:51 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 09:30:42 iPwn kernel[0]: en1: 802.11d country code set to 'X2'.
Aug 22 09:30:42 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 09:30:43 iPwn kernel[0]: en1: 802.11d country code set to 'TW'.
Aug 22 09:30:43 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 12:38:02 iPwn kernel[0]: en1: 802.11d country code set to 'X2'.
Aug 22 12:38:02 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 12 13 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 12:38:02 iPwn kernel[0]: en1: 802.11d country code set to 'TW'.
Aug 22 12:38:02 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
--
Aug 22 13:36:57 iPwn kernel[0]: en1: 802.11d country code set to 'TW'.
Aug 22 13:36:57 iPwn kernel[0]: en1: Supported channels 1 2 3 4 5 6 7 8 9 10 11 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
```

802.11d OSX fix

- http://www.hub.ru/wiki/802.11d
- https://github.com/0x90/osx-scripts/blob/master/wifi_cc.sh

2.4GHz, 5GHz? …8(

802.11 frequency ranges:

- 900 MHz (802.11ah)
- 2.4 GHz (802.11b/g/n)
- 3.6 GHz (802.11y)
- 4.9 GHz (802.11y) Public Safety WLAN
- 5 GHz (802.11a/h/j/n/ac)
- 5.9 GHz (802.11p)
- 60 GHz (802.11ad)

802.11y

- 3.65-3.7GHz, 54Mbit/s, 4.9 GHz. US only? Public Safety WLAN 50 MHz of spectrum from 4940 MHz to 4990 MHz (WLAN channels 20–26) are in use by public safety entities in the US. Cisco 3202 4.9GHz Wireless Mobile Interface Card

802.11p

- 5.9Ghz, Wireless Access in Vehicular Environments (WAVE) 802.11p In Europe used as a basis for the ITS-G5 standard, supporting the GeoNetworking vehicle2vehicle2infrastructure communication.
- Intellectual Transport System. =^.^=

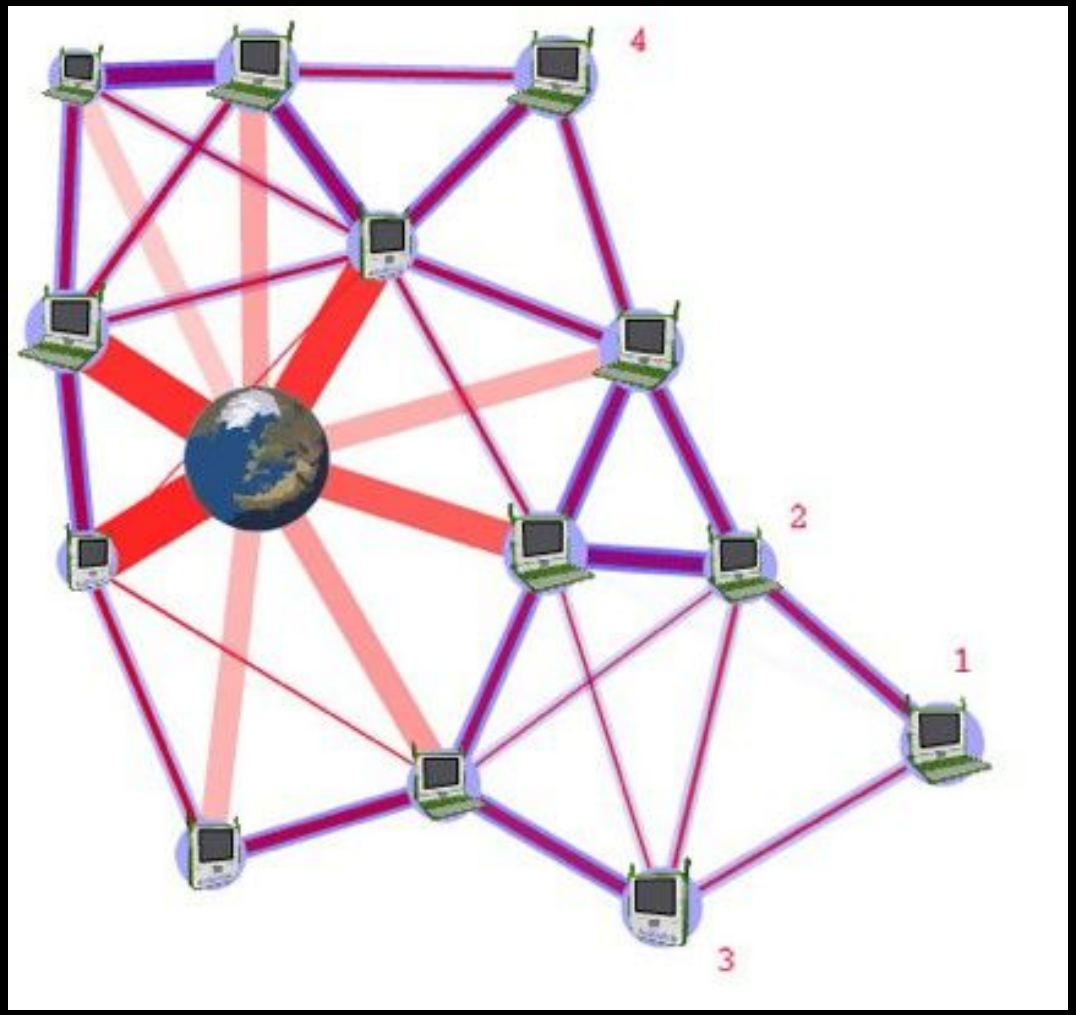
802.11ad

60 GHz,WiGig. 7Gbit/s, 10m, beamforming, wireless display/HDMI, uncompressed video

802.11ah

- 900 MHz operates in sub-gigahertz unlicensed bands.

802.11s = mesh



…and many more

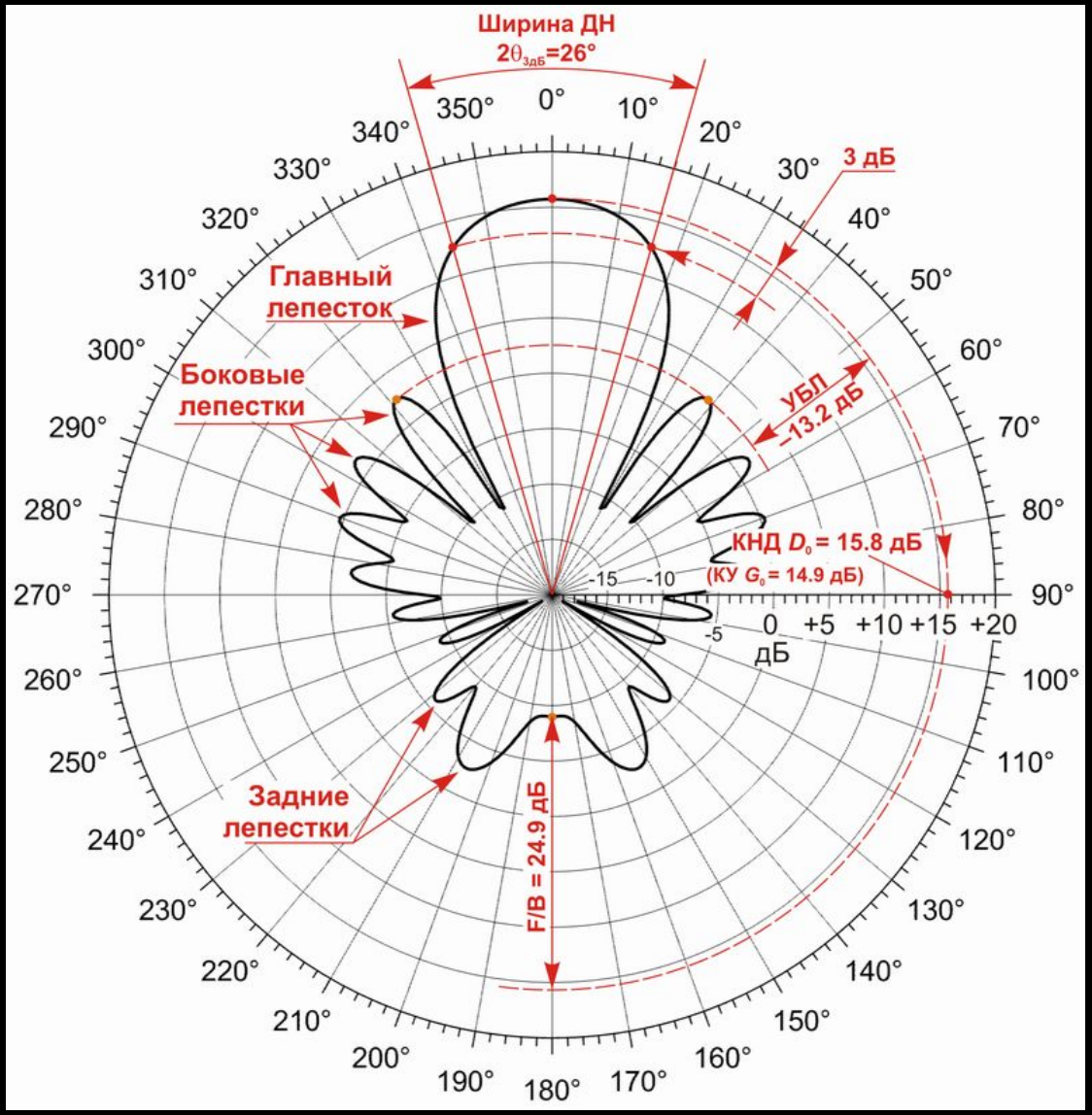
- **802.11a** — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)
- **802.11b** — улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
- **802.11c** — процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001)
- **802.11d** — интернациональные роуминговые расширения (2001)
- **802.11e** — улучшения: QoS, включение packet bursting (2005)
- **802.11F** — Inter-Access Point Protocol (2003)
- **802.11g** — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
- **802.11h** — распределённый по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
- **802.11i** — улучшенная безопасность (2004)
- **802.11j** — расширения для Японии (2004)
- **802.11k** — улучшения измерения радио ресурсов
- **802.11l** — зарезервирован
- **802.11m** — поддержание эталона; обрезки
- **802.11n** — увеличение скорости передачи данных (600 Мбит/с). 2,4--2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g . Особенно распространён на рынке в США в устройствах D-Link, Cisco и Apple (сентябрь 2009)
- **802.11o** — зарезервирован
- **802.11p** — WAVE — Wireless Access for the Vehicular Environment (Беспроводной Доступ для Транспортной Среды, такой как машины скорой помощи или пассажирский транспорт)
- **802.11q** — зарезервирован, иногда его путают с 802.1Q
- **802.11r** — быстрый роуминг
- **802.11s** — ESS Wireless mesh network[en] (Extended Service Set — Расширенный Набор Служб; Mesh Network — Ячеистая Сеть)
- **802.11T** — Wireless Performance Prediction (WPP, Предсказание Производительности Беспроводного Оборудования) — методы тестов и измерений
- **802.11u** — взаимодействие с не-802 сетями (например, сотовые сети)
- **802.11v** — управление беспроводными сетями
- **802.11x** — зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X
- **802.11y** — дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.
- **802.11w** — Protected Management Frames (Защищенные Управляющие Фреймы)
- **802.11ac** — новый стандарт IEEE. Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утвержден в январе 2014 года.
- **802.11ad** — новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с.
- **802.11as** (предположительно) — новый стандарт, использующий **резонаторно-щелевые антенны**, работающие на частоте 135 ГГц. Скорости передачи данных — до 20 Гбит/с. Коэффициент усиления антенны равен 5,68 дБ.

ANTENNA

+

= ?

Основные характеристики антенн

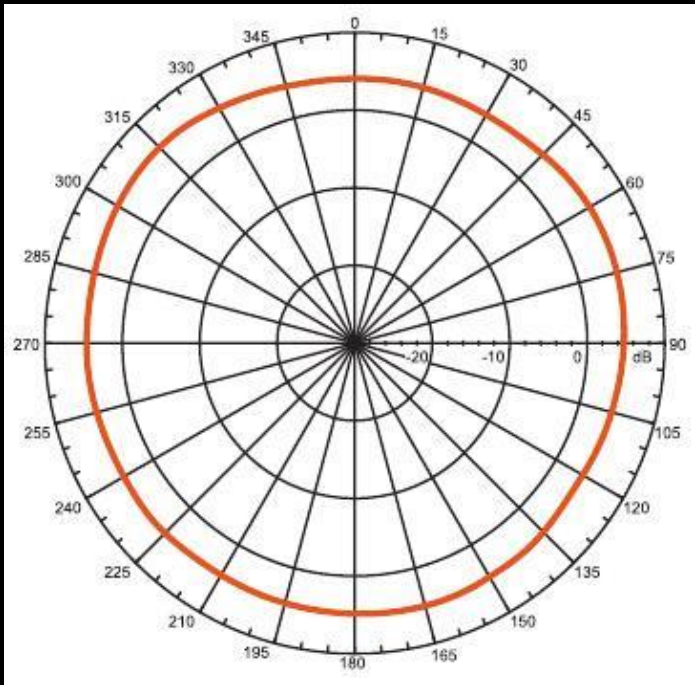


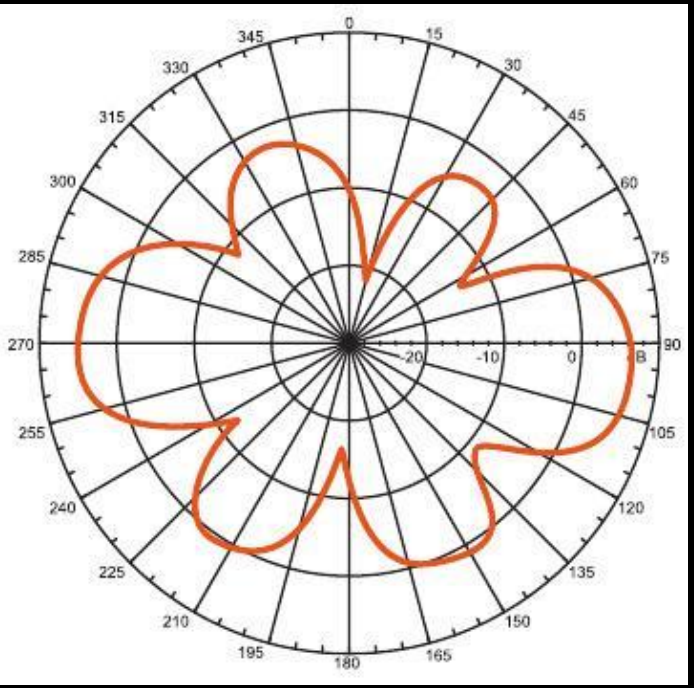
Основные Виды антенн в сетях WiFI

- Штыревые / всенаправленные – спиральные
- Волновой канал – Уда-Яги
- Панельные – патч-антенны
- Параболические – зеркальные
- Секторные – волноводно-щелевые

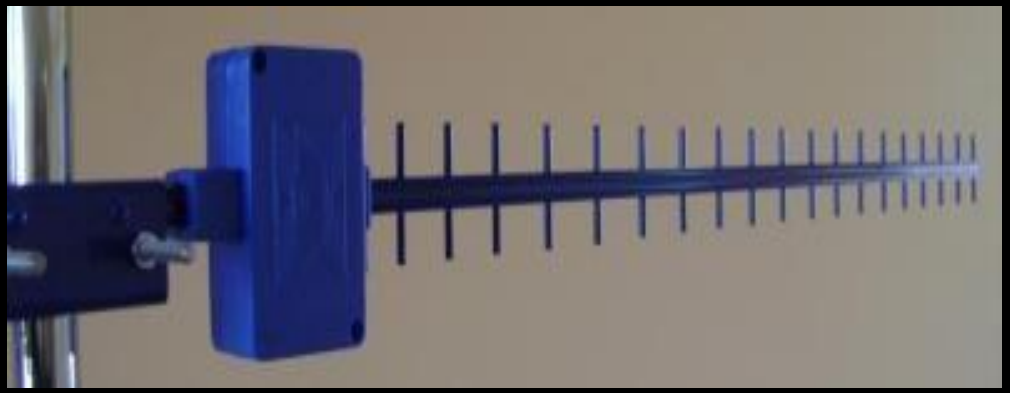
Спиральные антенны

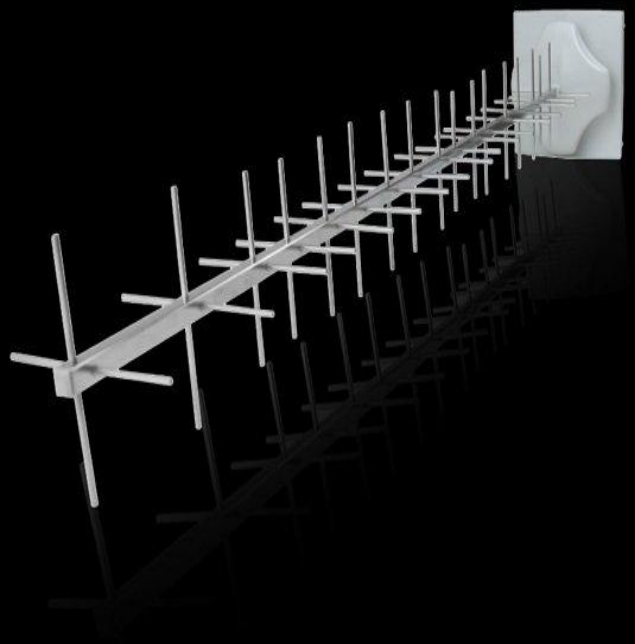
Спиральные антенны



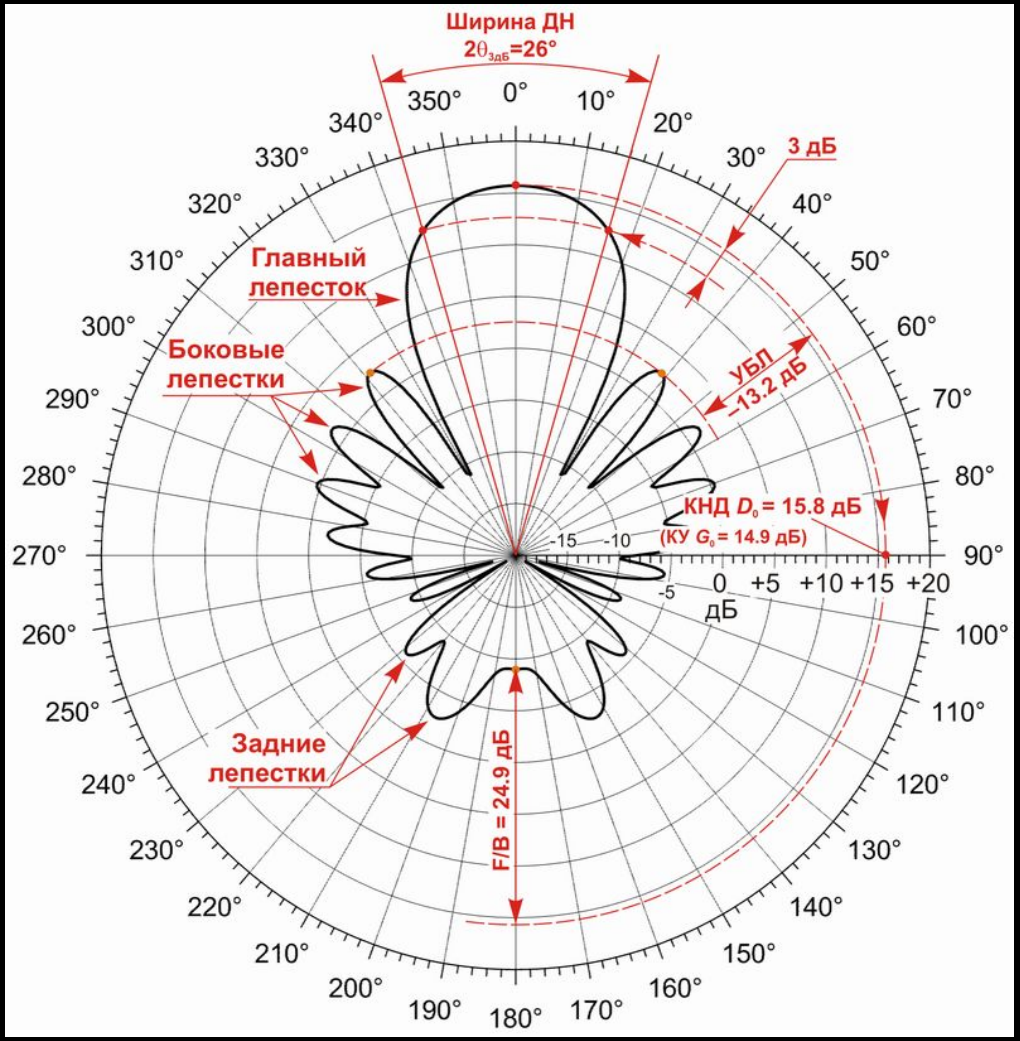


Волновой канал

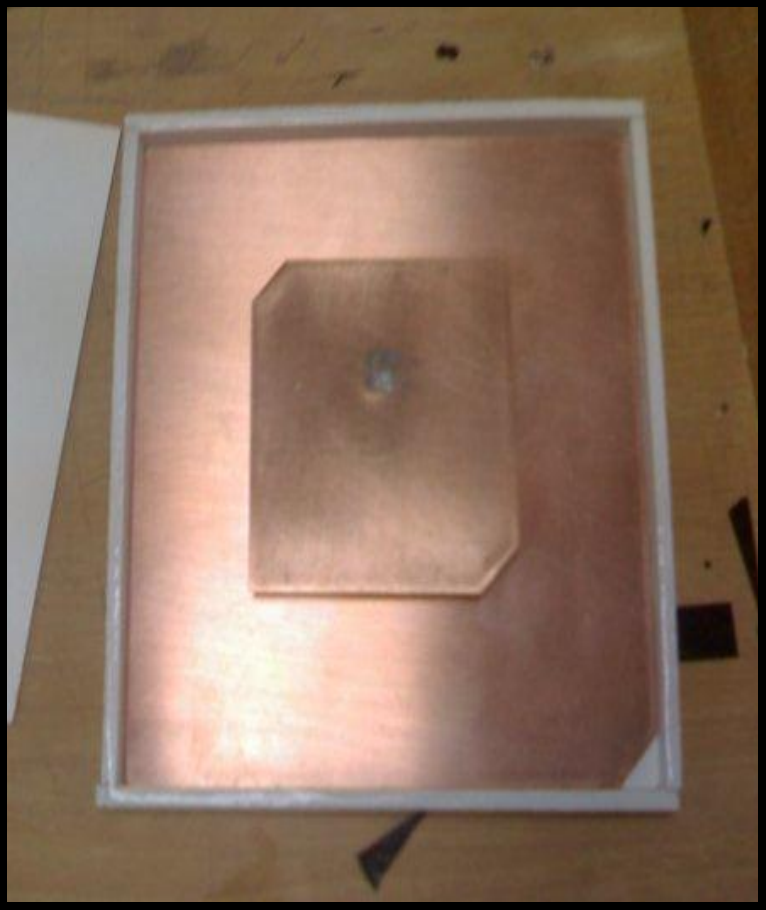




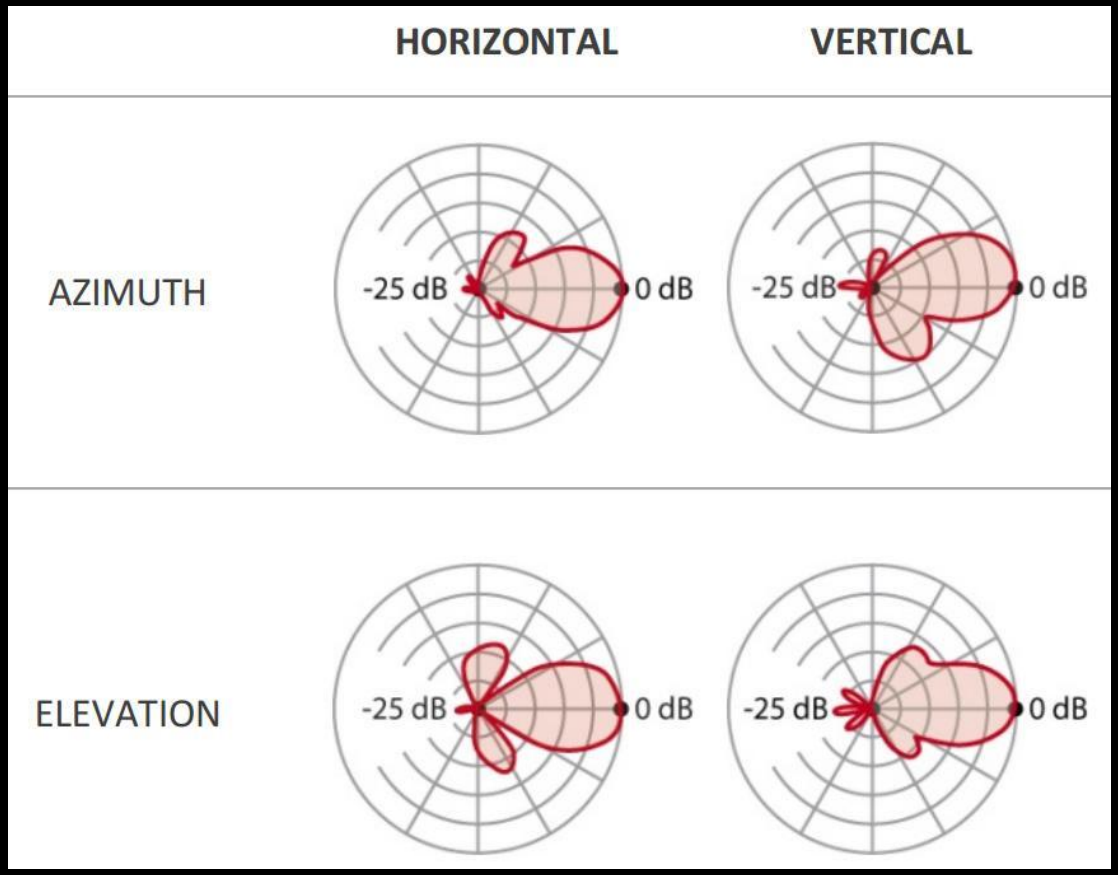
Волновой канал



Патч антенны

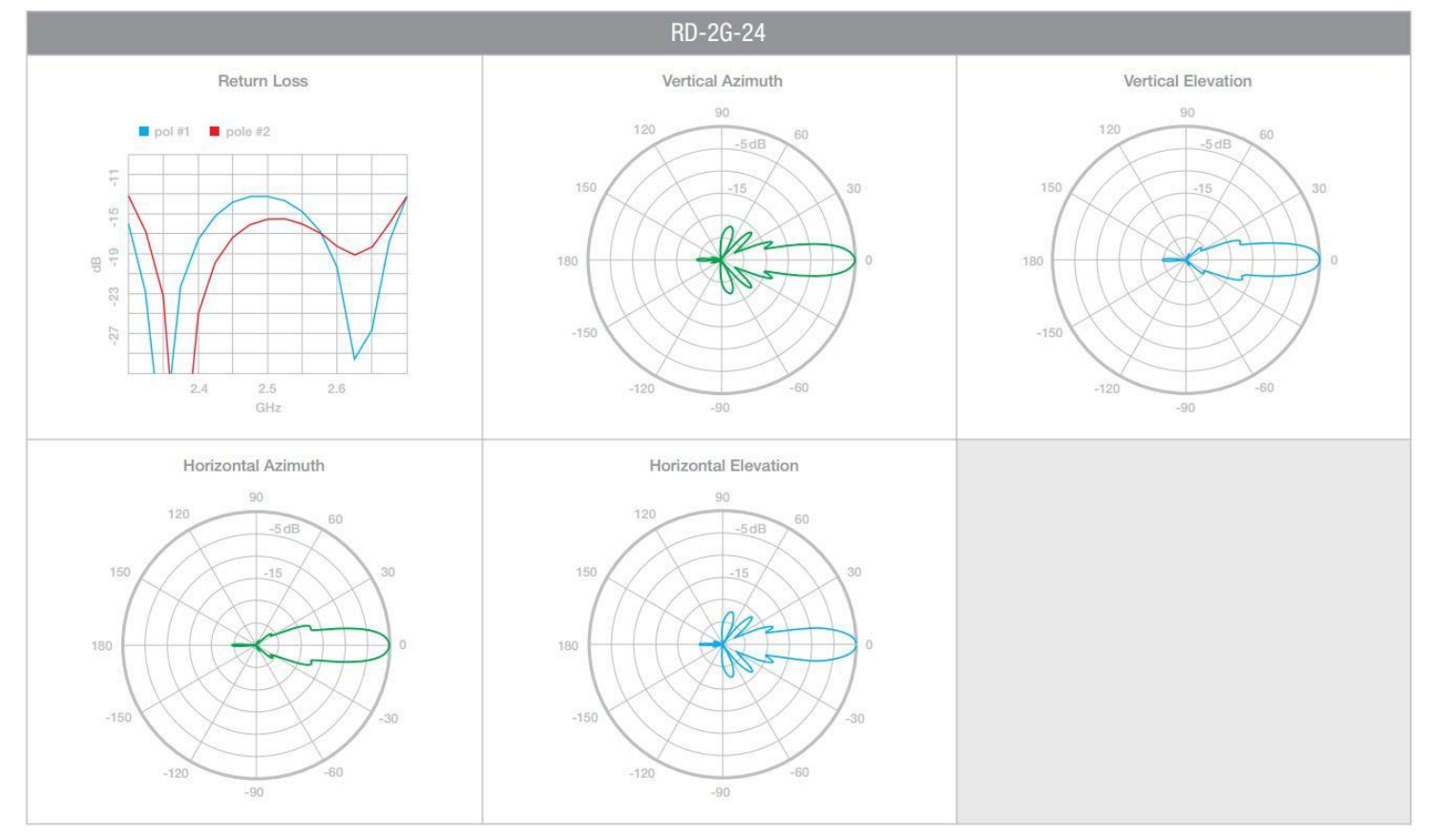


Патч антенны



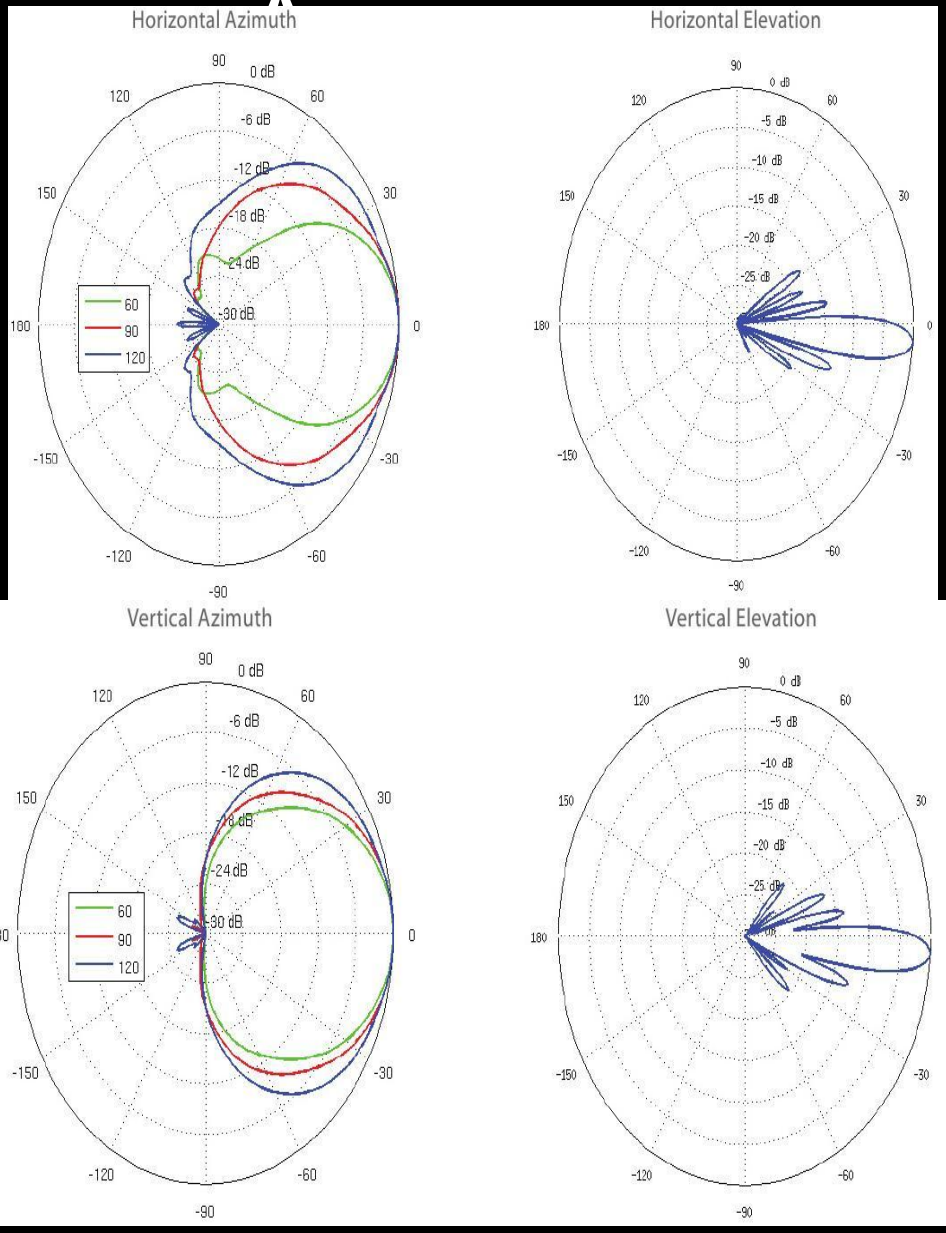
Зеркальные Антенны

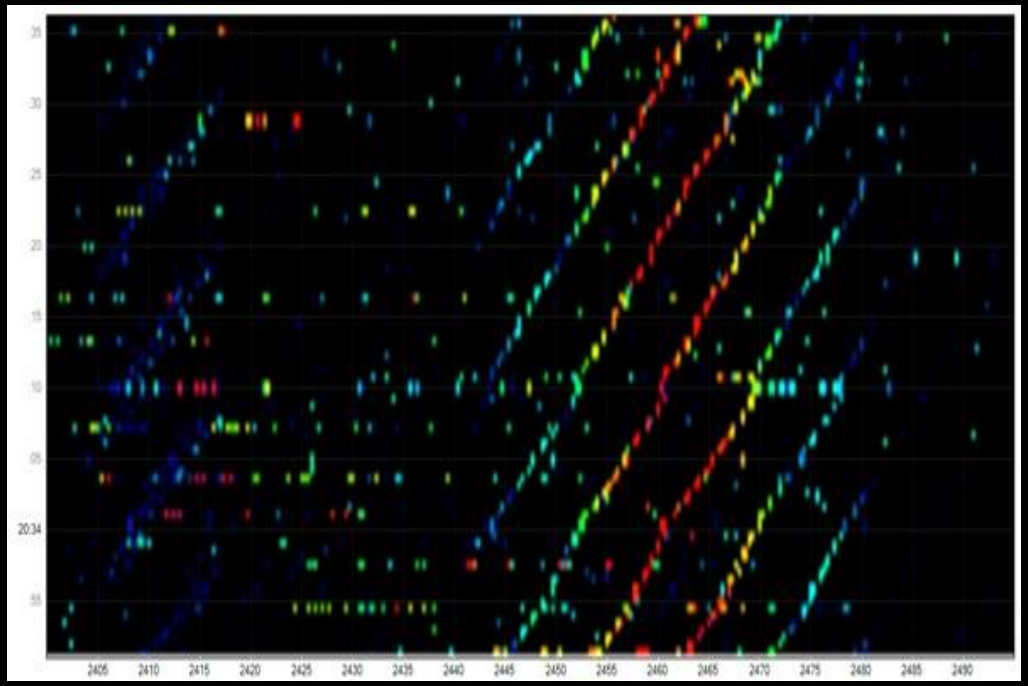
Зеркальные Антенны

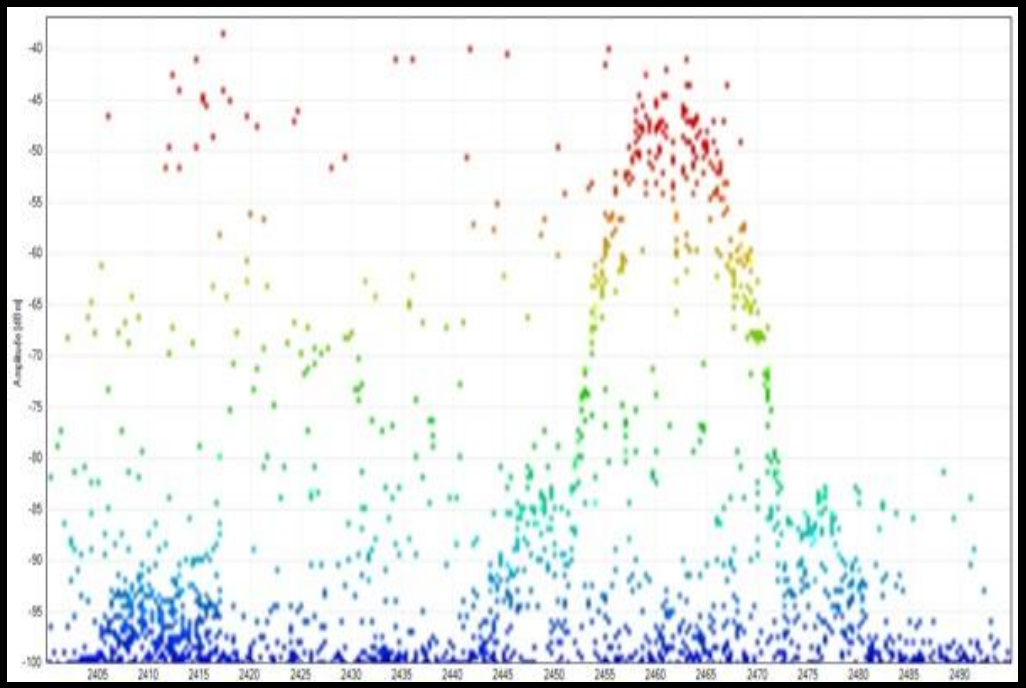


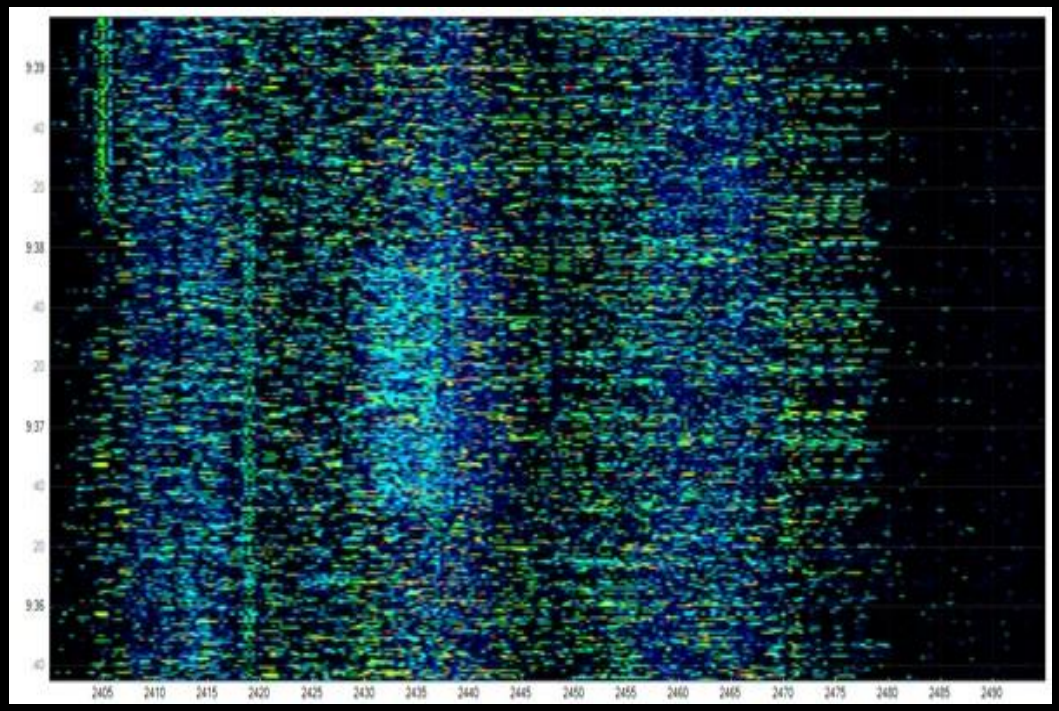
Волноводно-щелевые Антенны

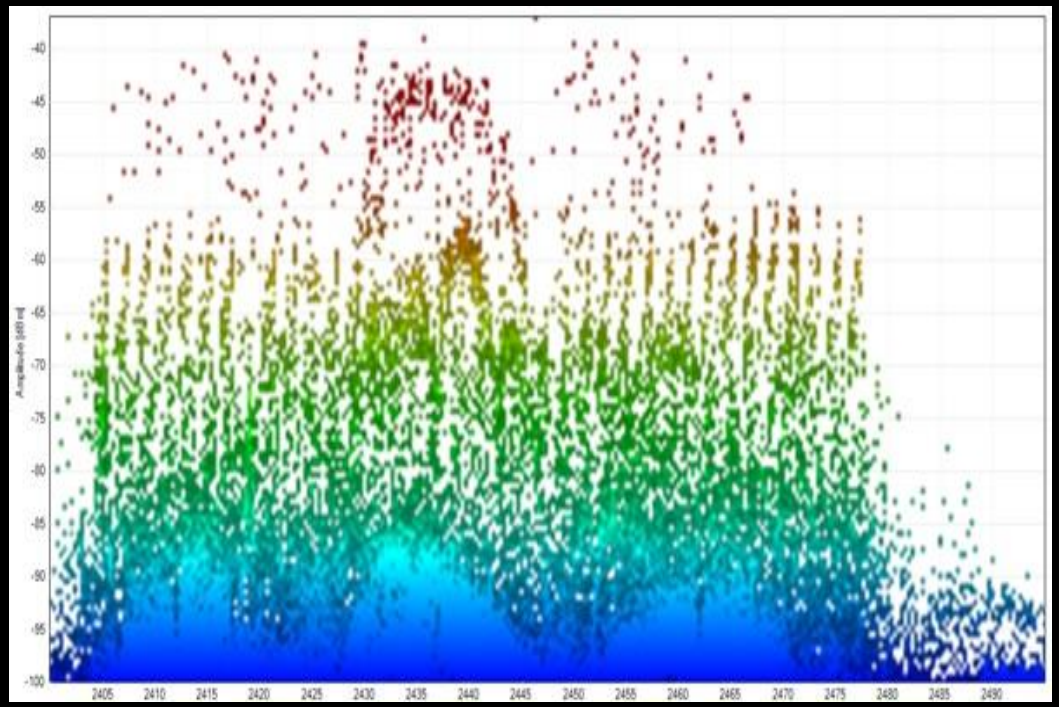
Волноводно-щелевые а




2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490


-40 -45 -50 -55 -60 -65 -70 -75 -80 -85 -90 -95 -100
2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490


9:39
9:38
9:37
9:36
2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490


-40 -45 -50 -55 -60 -65 -70 -75 -80 -85 -90 -95 -100
2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490

HARDWARE

.:MODES:.

- STA/Managed– station operating
- AP/Master – access point
- MON – passive monitor channel
- INJMON – monitor+injection (mac80211)
- AdHoc/IBSS – computers without AP
- WDS – static WDS
- Mesh – many to many

CARDS

- TP-Link TL-WN722N Atheros AR9271 (2.4 GHz)
- Alfa AWUS036H RTL8187L (2.4 GHz)
- Alfa AWUS036NHA (2.4G GHz) long range
- Alfa AWUS051NH (2.4 & 5 GHz) long range
- Ralink 3070 based cards (MediaTek now)
- Any MAC80211 can be used!

MAX POWER DREAMS?

GOOD OLD TYMES….GO TO BOLIVIA!

HACKER = NO LIMITS

```
# ifconfig wlan0 down
# iw reg set ~~BO~~ BZ
# ifconfig wlan0 up
# iwconfig wlan0 channel 13
# iwconfig wlan0 txpower 30
```

or

```
# iw phy wlan0 set txpower fixed 30mBm
```

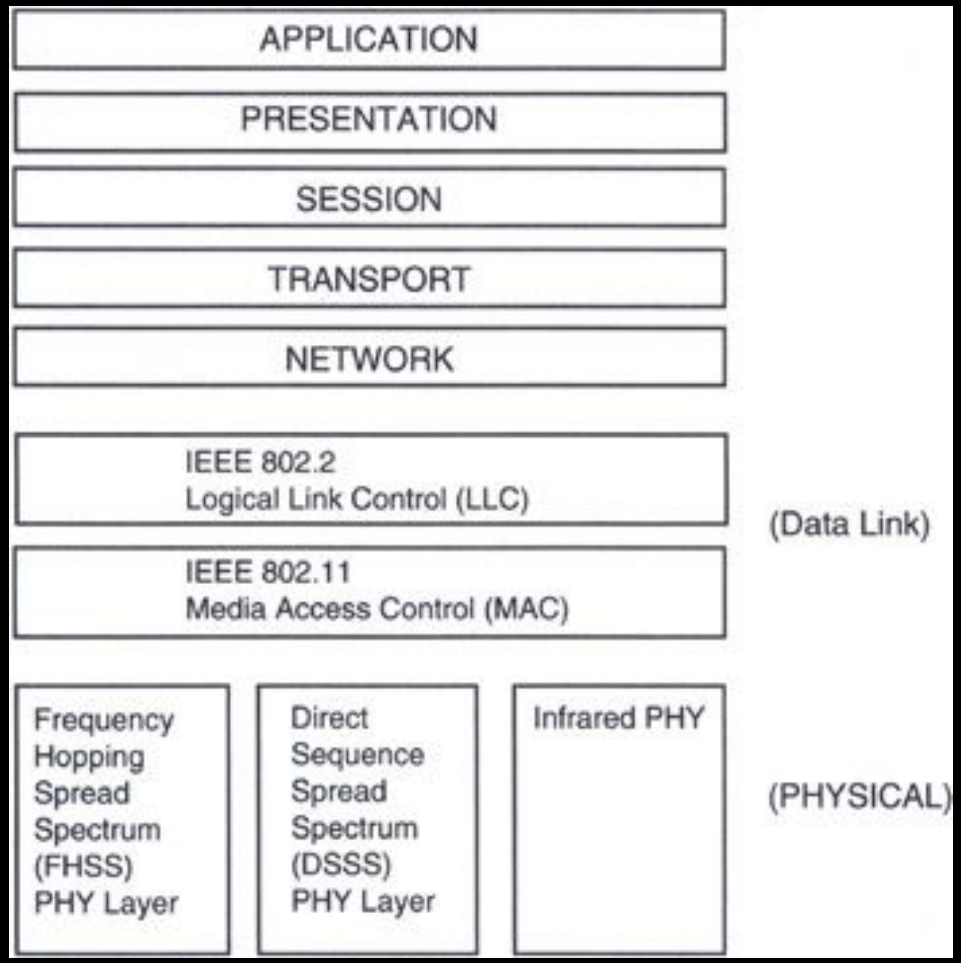
Correct way

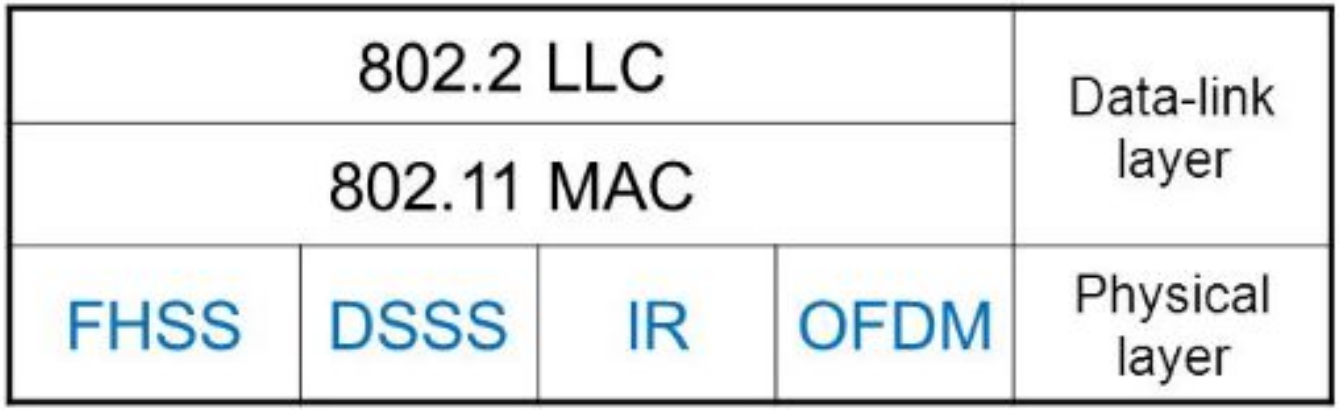
1. Patch wireless-database
2. Patch CRDA
3. PROFIT!!!!

https://github.com/0x90/kali-scripts/blob/master/wireless.sh

802.11 OSI

802.11 layer in OSI





FHSS: Frequency Hopping Spread Spectrum

DSSS: Direct Sequence Spread Spectrum

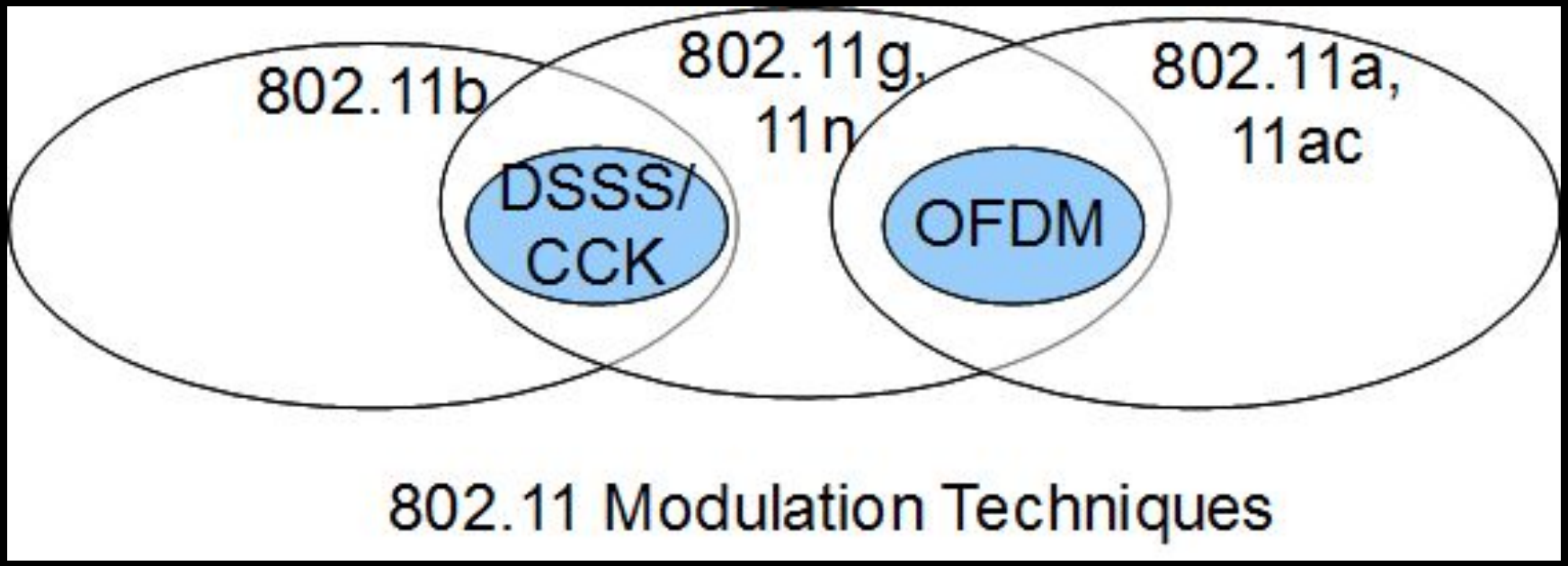
} Operate at ISM band

OFDM: Orthogonal Frequency Division Multiplexing

} Operates at U-NII band

IR: Infra Red

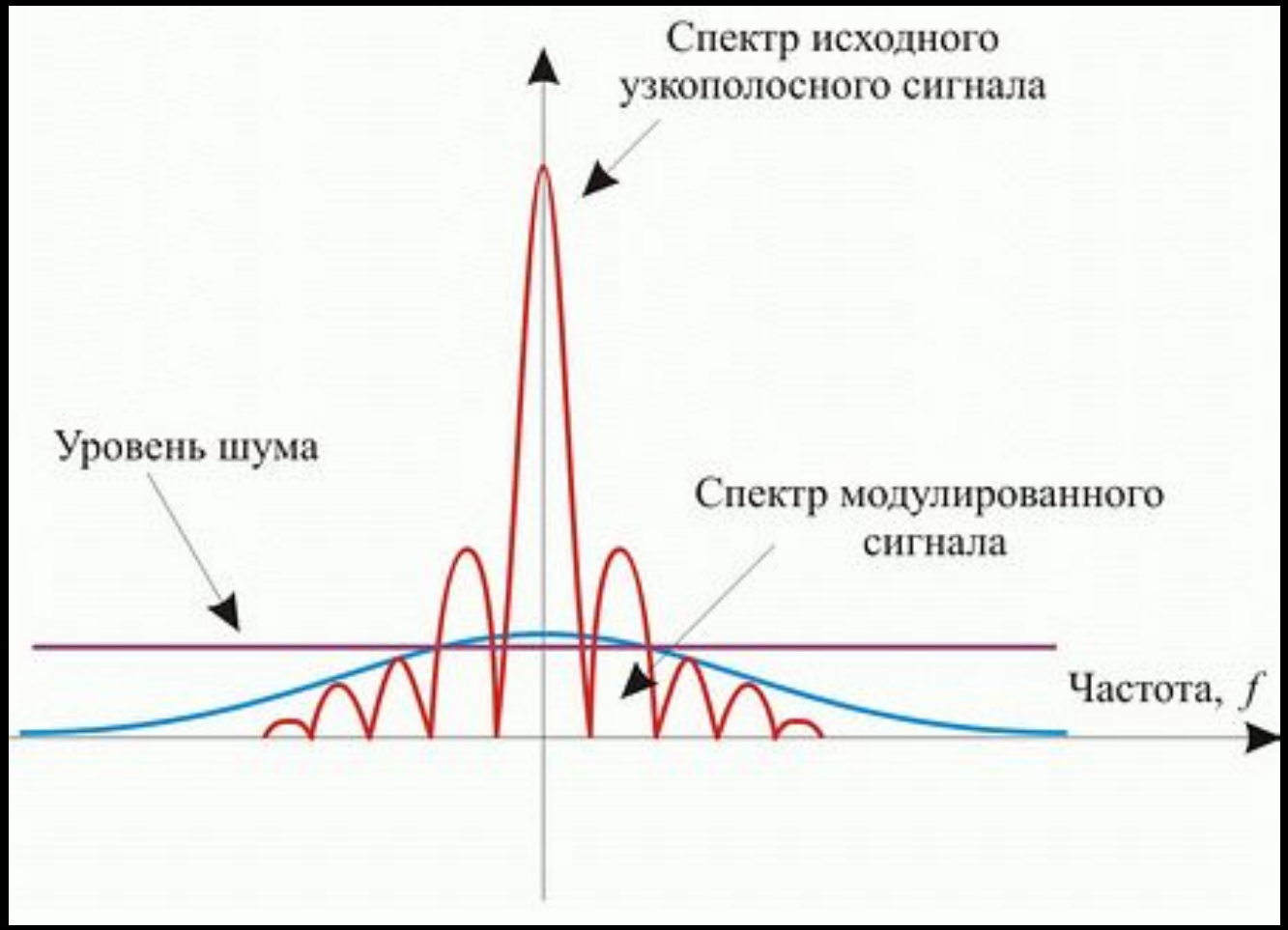
802.11 modulation



DSSS

- DSSS (direct sequence spread spectrum) - метод прямой последовательности для расширения спектра

DSSS

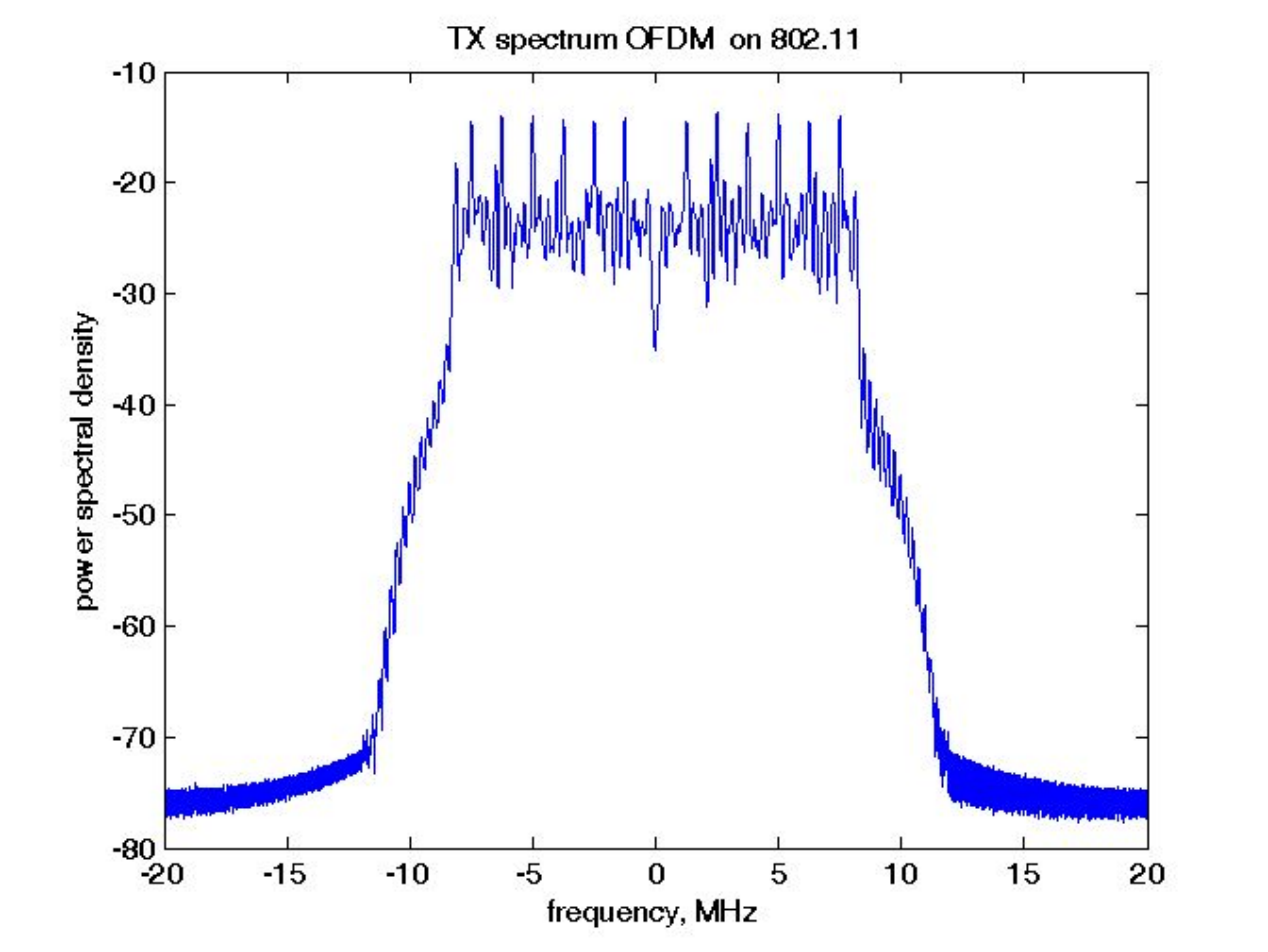

Спектр исходного
узкополосного сигнала
Уровень шума
Спектр модулированного
сигнала
Частота, f

OFDM

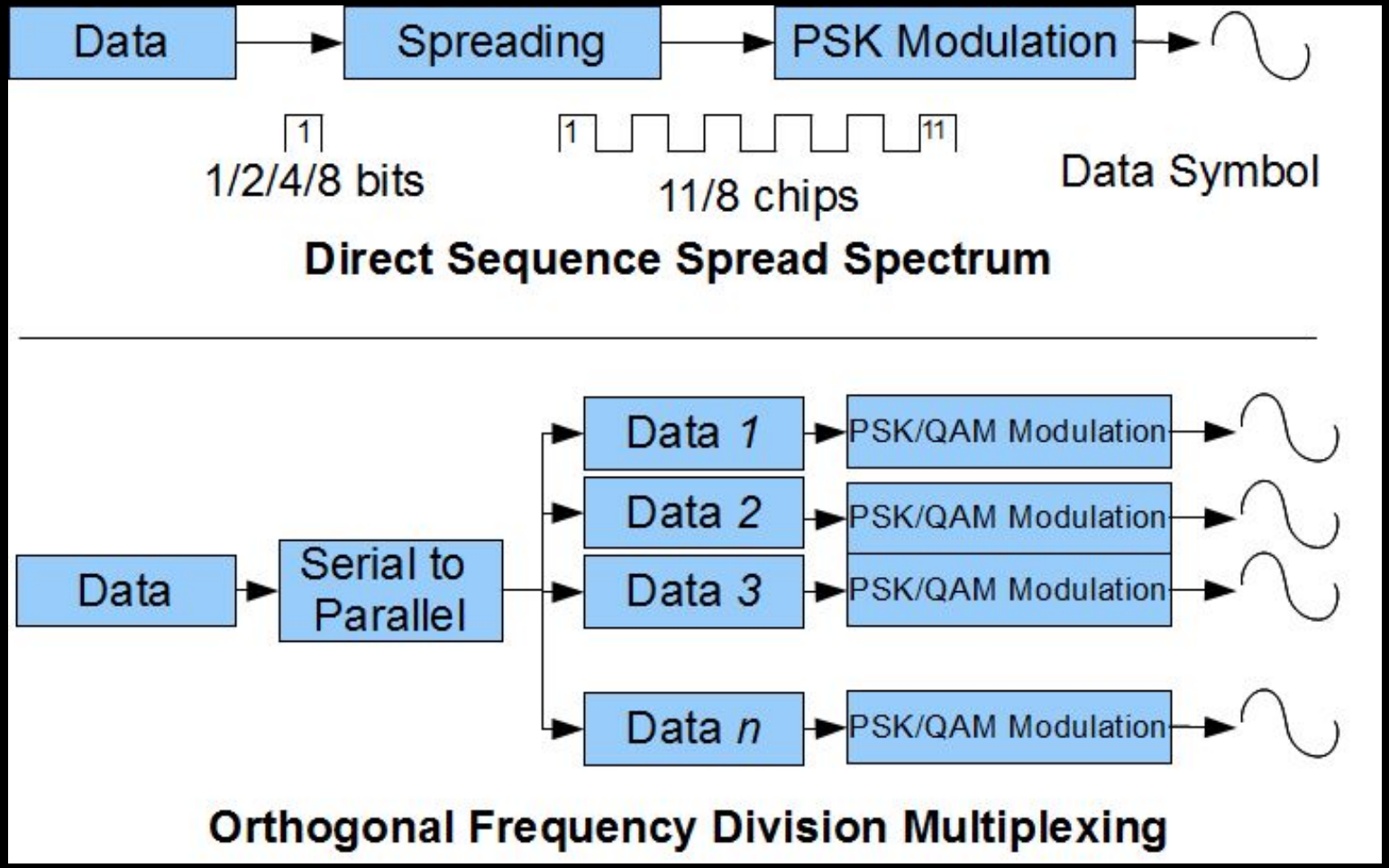
OFDM (англ. Orthogonal frequency-division multiplexing — мультиплексирование с ортогональным частотным разделением каналов) является цифровой схемой модуляции, которая использует большое количество близко расположенных ортогональных поднесущих.

Wi-Fi, WiMax, LTE

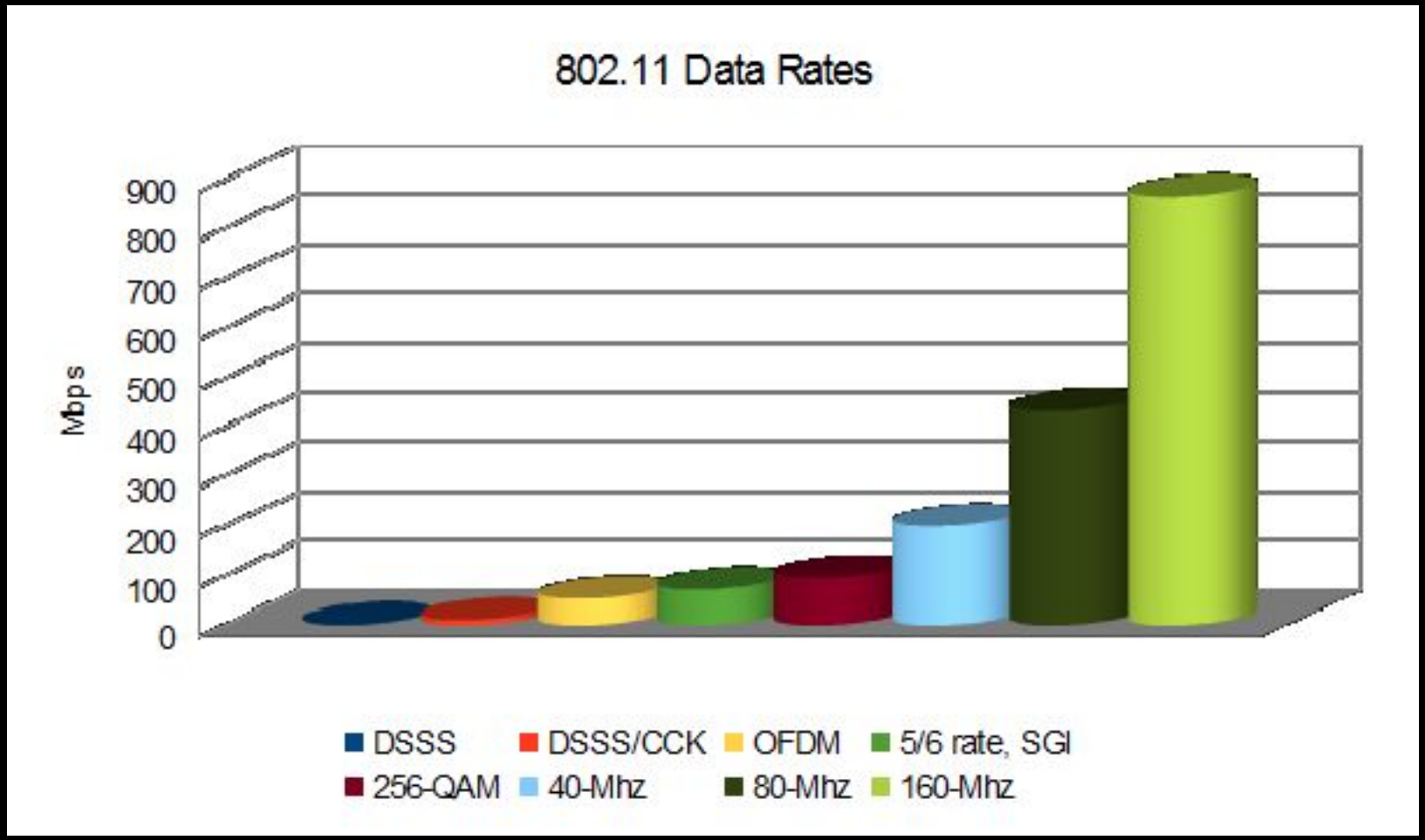
OFDM


TX spectrum OFDM on 802.11
power spectral density
frequency, MHz
-10
-20
-30
-40
-50
-60
-70
-80
-20
-15
-10
-5
0
5
10
15
20

DSSS vs OFDM


Data
Spreading
PSK Modulation
1
1/2/4/8 bits
1
11
11/8 chips
Data Symbol
Direct Sequence Spread Spectrum
Data
Serial to Parallel
Data 1
Data 2
Data 3
Data n
PSK/QAM Modulation
PSK/QAM Modulation
PSK/QAM Modulation
PSK/QAM Modulation
Orthogonal Frequency Division Multiplexing

802.11 data rates



Physical layer

- 802.11a: OFDM - Мультиплексирование с ортогональным частотным разделением каналов
- 802.11b: DSSS - Расширение спектра методом прямой последовательности
- 802.11g: Extended Rate PHY (ERP) = OFDM
- 802.11n: MIMO OFDM
- 802.11ac: MU MIMO OFDM

802.11 security

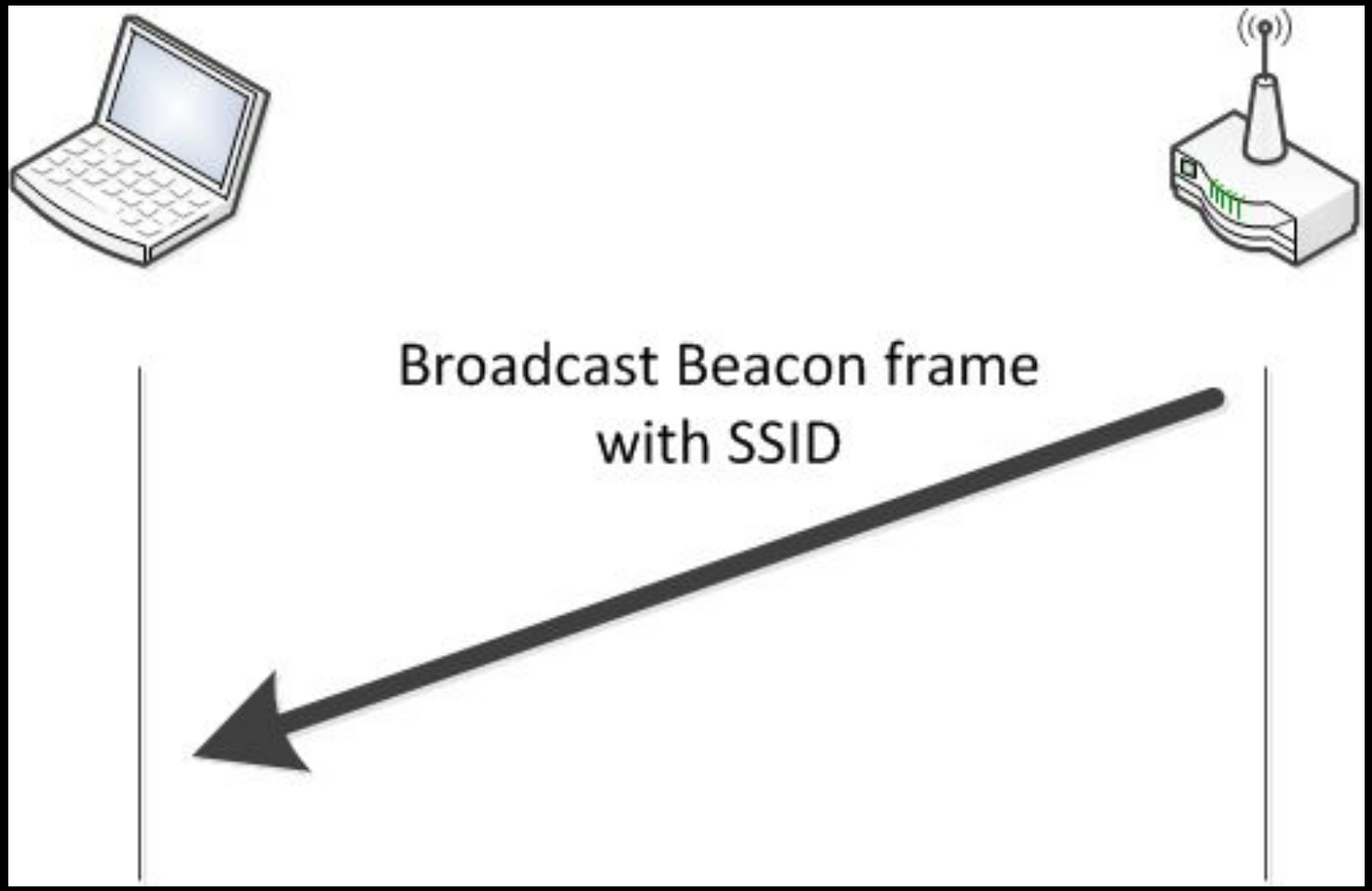
802.11 SECURITY

- Open
- WEP
- IBSS aka Ad-Hoc
- WPA
- WPA2-Personal
- WPA2-Enterprise

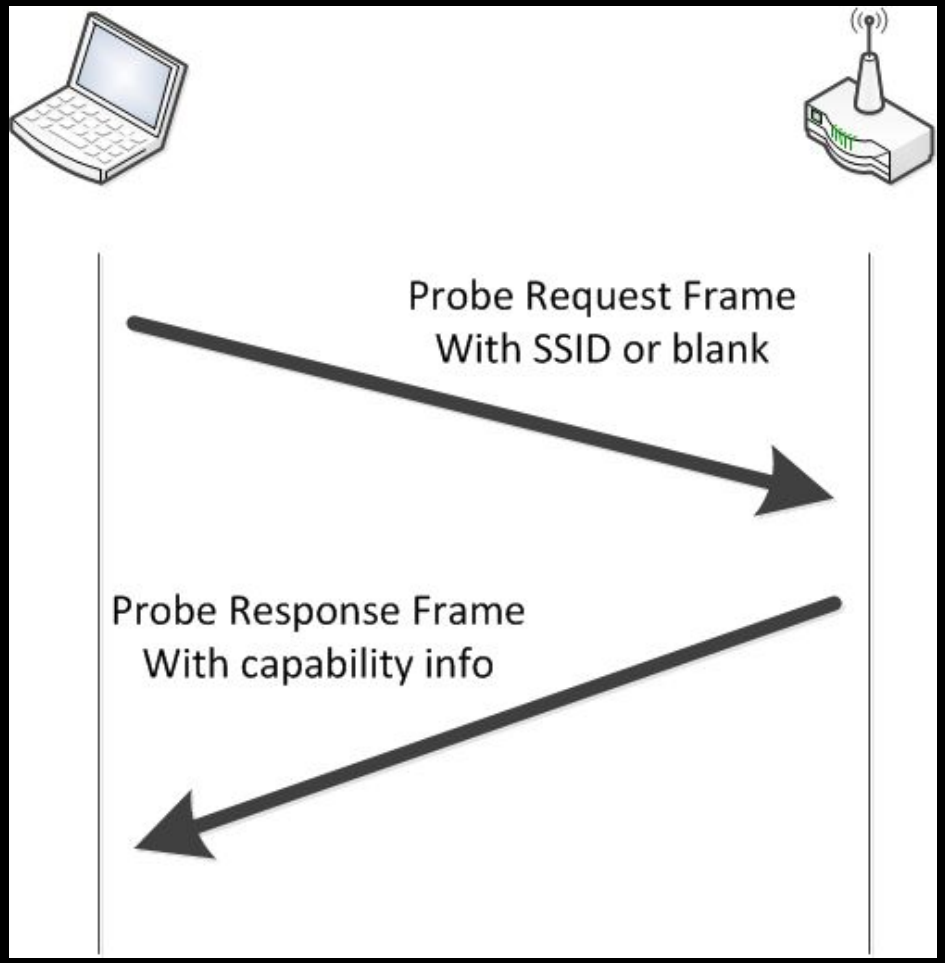
management frame types

- Authentication frame
- Deauthentication frame
- Association request frame
- Association response frame
- Disassociation frame
- Beacon frame
- Probe request frame
- Probe response frame

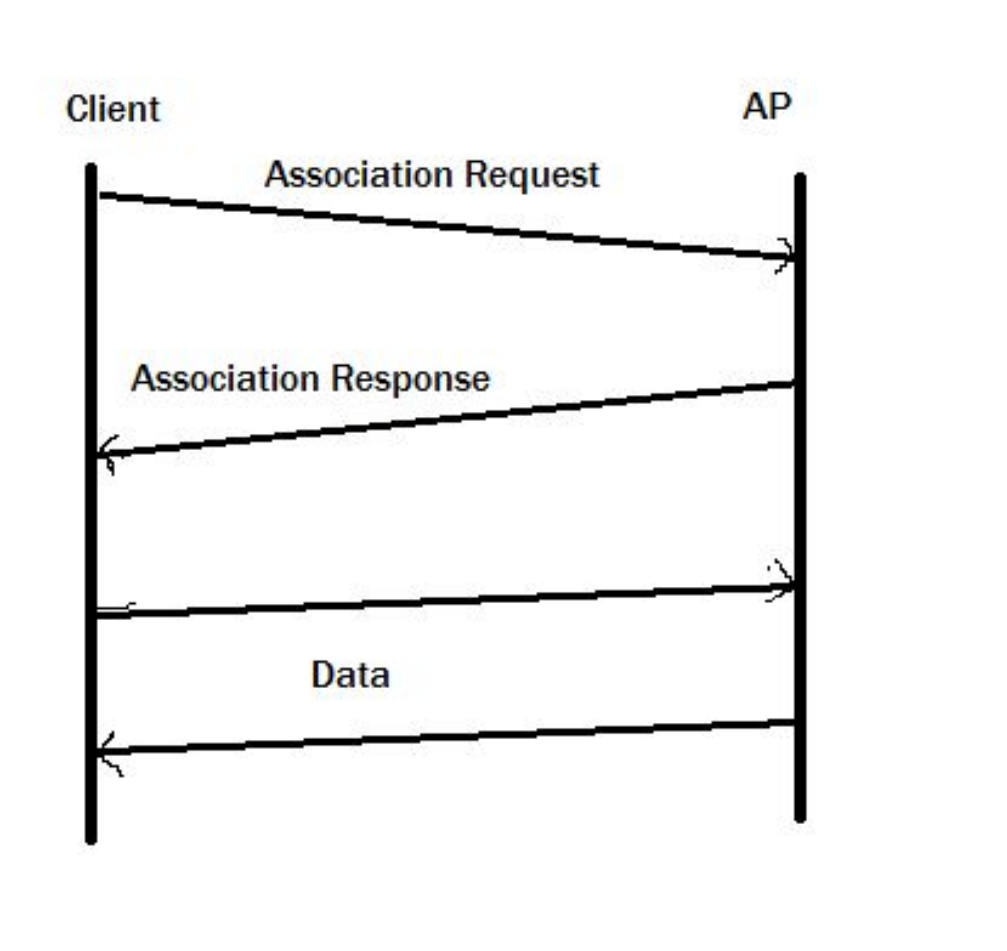
WiFi passive scan



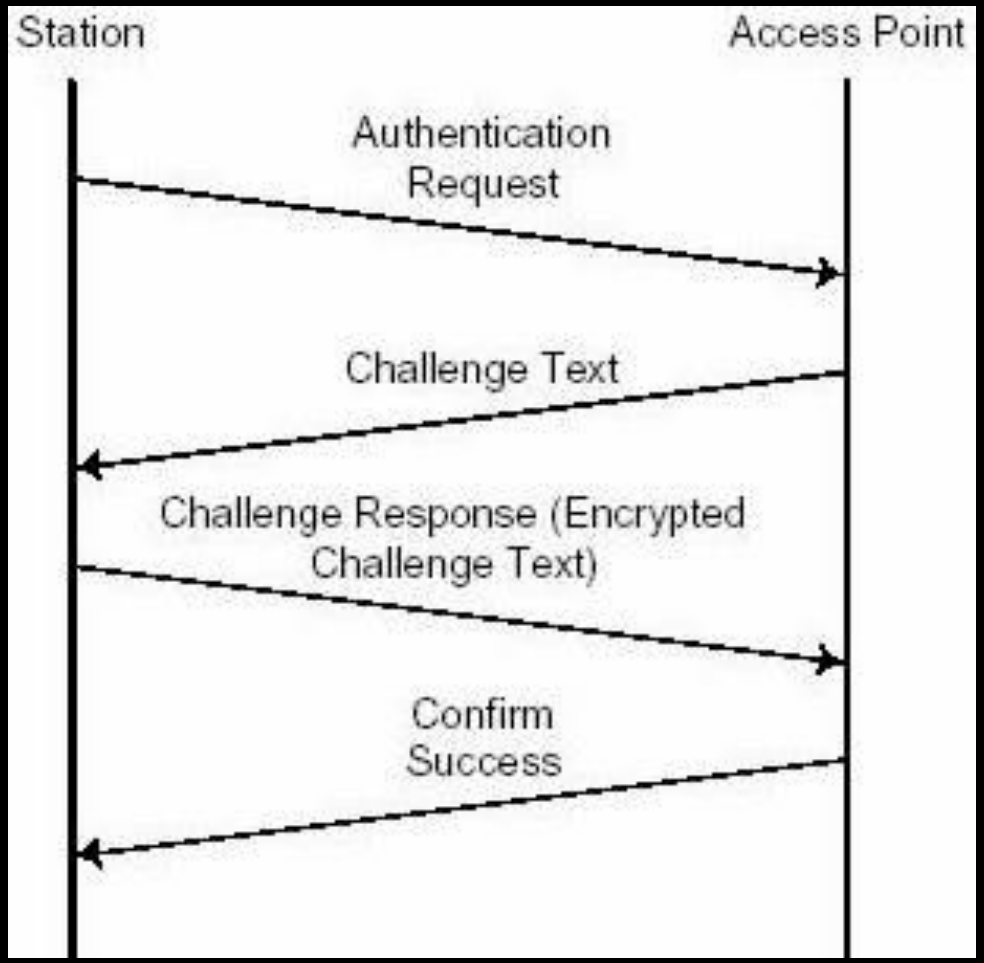
WiFi active scan



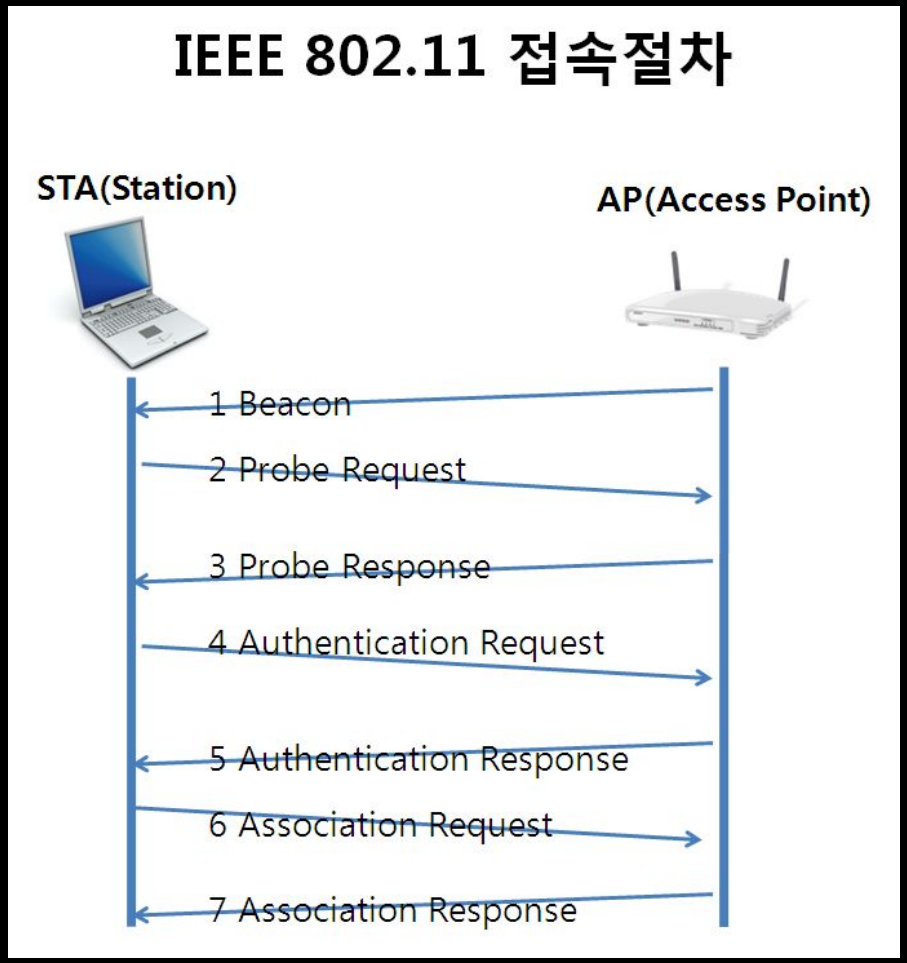
WiFi open auth



WiFi PSK auth



802.11 connection



WEP/WPA/WPA2

	802.1X Dynamic WEP	Wi-Fi Protected Access (WPA)	Wi-Fi Protected Access 2 (WPA2)
Access Control	802.1X	802.1X or preshared key	802.1X or preshared key
Authentication	EAP methods	EAP methods or preshared key	EAP methods or preshared key
Encryption	WEP	TKIP (RC4)	CCMP (AES Counter Mode)
Integrity	None	Michael MIC	CCMP (AES CBC-MAC)

WiFi authentication types

- Open Authentication to the Access Point
- Shared Key Authentication to the Access Point
- EAP Authentication to the Network
- MAC Address Authentication to the Network
- Combining MAC-Based, EAP, and Open Authentication
- Using CCKM for Authenticated Clients
- Using WPA Key Management

http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html

HACKING

What to hack?

- WiFi network (AP)
- WiFi clients

Almost like fishing and XSS.

Active and passive.

May be combined.

TOOLS

- wifite r112
- kismet, horst, aircrack-ng, mdk3, wifijammer
- pyrit, cowpatty, hashcat
- KARMA, MANA, Hostapd-WPE
- reaver, pixie-wps, WPSPIN.sh, BullyWPS,
- FruityWiFi, Snoopy-ng, modwifi
- scapy + impacket + /dev/brain + /dev/hands

RFMON

- Like promiscuous mode but at lower layer
- Used to receive ALL frames
- Used for sniff and injection
- Advice: don’t kill network-manager – free the card

airmon-ng start wlan0

airodump-ng wlan0mon

… may be use wireshark?

Radiotap

- Radiotap is a de facto standard for 802.11 frame injection and reception.
- Radiotap is pseudo layer
- http://www.radiotap.org/

WEP HACKING

WEP

- WEP = Wired Equivalent Privacy
- First WiFi crypto
- WEP = RC4 + CRC32 + XOR
- LENGTH(KEY) = 40 (1997)
- LENGTH(KEY) = 104 (2001)
- Has many bugs
- Can be hacked in 10 minutes
- Almost dead. Deprecated since 2004.

WEP weakness

- HACK RC4 = HACK WEP
- SMALL IV (init vector) = HACK
- CRC weakness
- NO AUTH, ONLY CRYPTO!

Атака на WEP

1. Направленная антенна => собираем IV с точки доступа
2. Антенна с широкой диаграммой => точка доступа + клиенты

WPA/WPA2 HACKING

WPA/WPA2 handshake catching

1. **Пассивный режим:**

Секторная антенна или всенаправленная антенна, желательно карта с MIMO

2. **Активный режим**:

Две сетевых карты: Одна мощная карта с направленной антенной для deauth, вторая карта с секторной антенной для перехвата в пассивном режиме.

HANDSHAKE CATCHING

Airodump-ng capture:

- airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w output.cap --showack wlan1mon

Pyrit capture and strip:

- pyrit -r wlan1mon -o $(date +%Y-%m-%d_%H:%M:%S)_stripped.cap stripLive

DEAUTH TO HELP

- aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 mon0
- aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 mon0
- Wifijammer.py is the best solution from the box for deauth. Launched on separate card in practice.

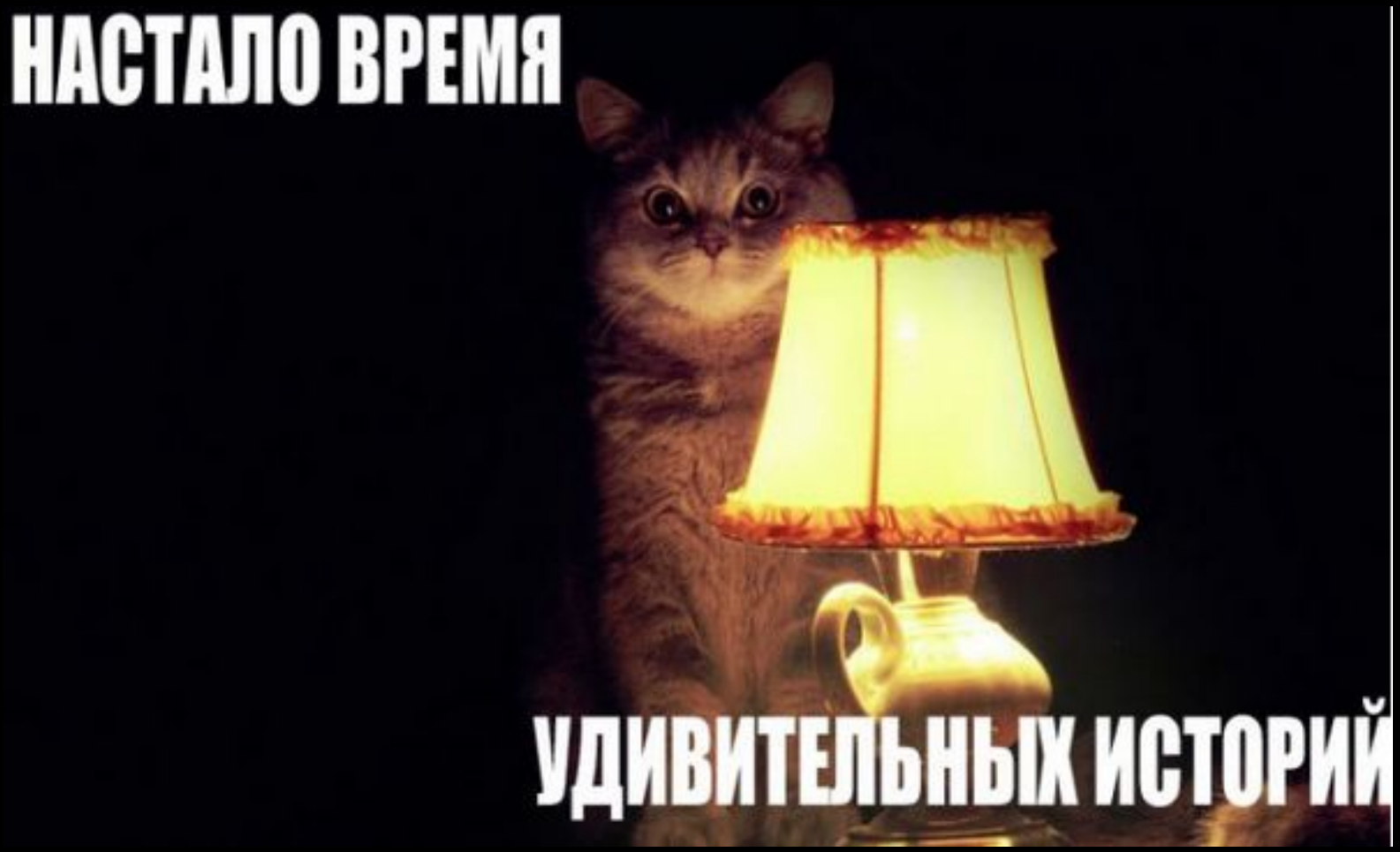
HANDSHAKE BRUTEFORCE

- Hashcat
- Pyrit
- Cowpatty
- Cloudcracker

WPA/WPA2 hacking protections?

- SSID hidden
- 802.11w
- IDS solutions arriving

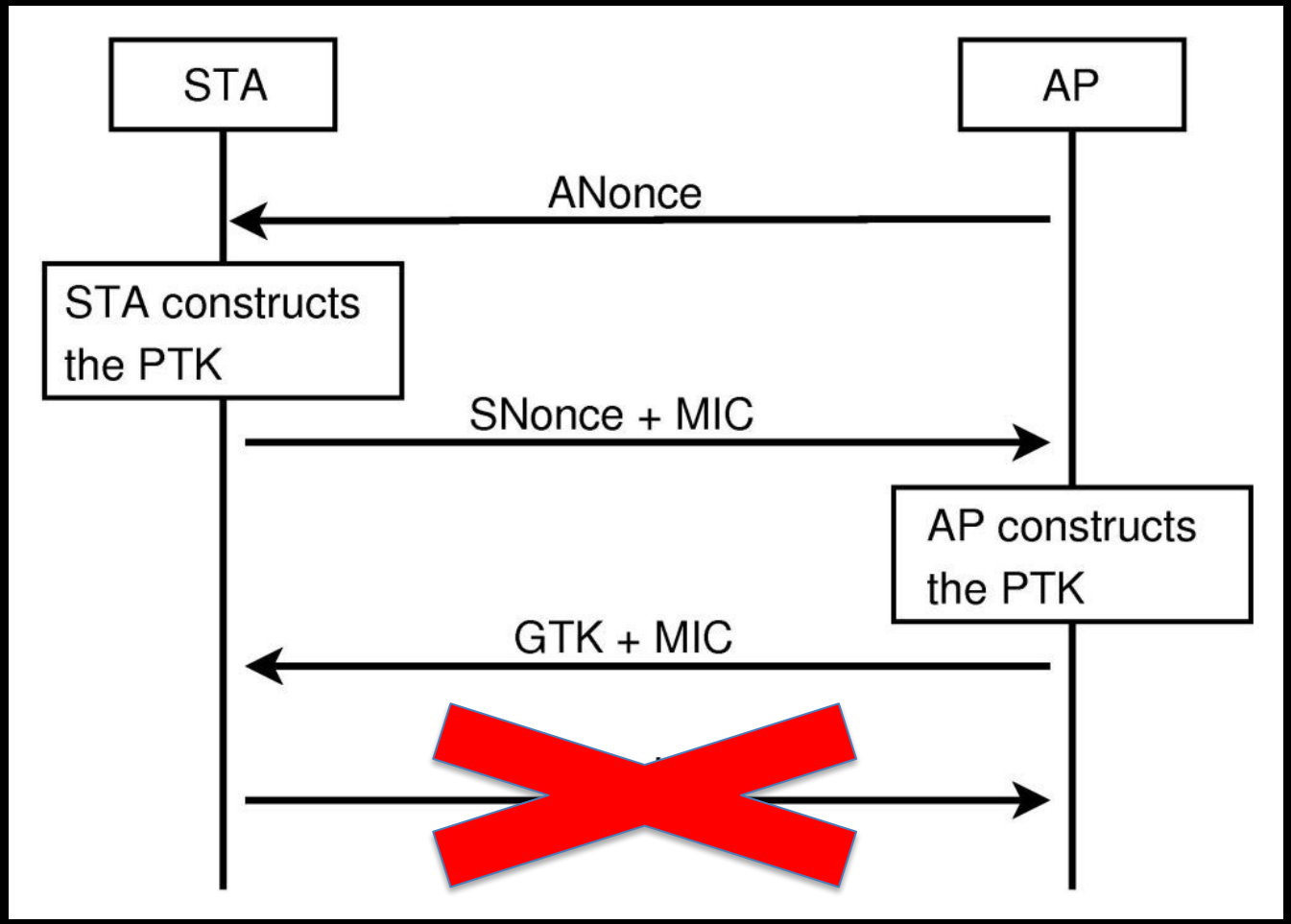
HALF HANDSHAKE STORY



Questions

- Do we REALY need all 4 frames for handshake cracking?
- What will happen if the client will try to connect to the same SSID with wrong password?

BAD/HALF HANDSHAKE



HALF HANDSHAKE TOOLS

- Pyrit --all-handshakes : Use all handshakes instead of the best one
- https://github.com/dxa4481/WPA2-HalfHandshake-Crack
- halfHandshake.py -r sampleHalfHandshake.cap -m 48d224f0d128 -s SSID_HERE

PoC thoughts

- Make custom HostAP fork
- Combine MANA and password auth with random password
- Write own access point from scratch

Lame PoC

- Hardware: TP-Link 3020/3040/3220/..
- Firmware: Custom OpenWRT based
- http://semaraks.blogspot.ru/2014/12/wispi-ver-11-for-tp-link-mr3020-mini.html
- Attack: KARMA + Randoom password @ hostapd.conf
- Cracking: pyrit --all-handshakes

ADVANCED FUTURE

- Hardware: Atheros chips
- Software: Python + Scapy + FakeAP + WiFi MAP database
- Cracking: pyrit --all-handshakes
- PWNiNiNG: setting different password for different client based on SSID database + MiTM attacks

WPS HACKING

WPS

- WPS – wireless protected setup
- Designed for connecting printers and other embedded devices
- Used by hackers to easily hack Wi-Fi

WPS HACKING WAYS

- WPS PIN brute force
- WPS PIN generation
- WPS PIN guessing

WPS BRUTE ALGO

- If the WPS Registration Protocol fails at some point, the Registrar will send a NACK message.
- If the attacker receives a NACK message after sending M4, he knows that the first half of the PIN was incorrect. See definition of R-Hash1 and R-Hash2.
- If the attacker receives a NACK message after sending M6, he knows that the second half of the PIN was incorrect.

WPS PIN brute force

- How many to brute? 8? 7? 4+3=>10^4+10^3
- Направленная антенна + подбор тракта по мощности
- Wifite, reaver-wps, bully, BullyWPSRussian.sh, ReVdK3-r2.sh

WPS PIN generation

- WPS_PIN=SOME_ALGO(MAC_ADDRESS)
- PIN = RAND(SERIAL) is not really random too
- Serial disclosure in Beacon frames at vendor specific fields
- Vulnerable vendors: ZyXELL, D-Link, Belkin, Huawei
- Reaver -W, --generate-pin Default Pin Generator [1] Belkin [2] D-Link [3] Zyxel
- Different custom pin generators https://github.com/devttys0/wps

PIXIE WPS/PIXIE DUST

- "pixie dust attack" discovered by Dominique Bongard in summer 2014
- Weak PRNG
- Pixiewps for _OFFLINE_ brute force

PIN GUESS

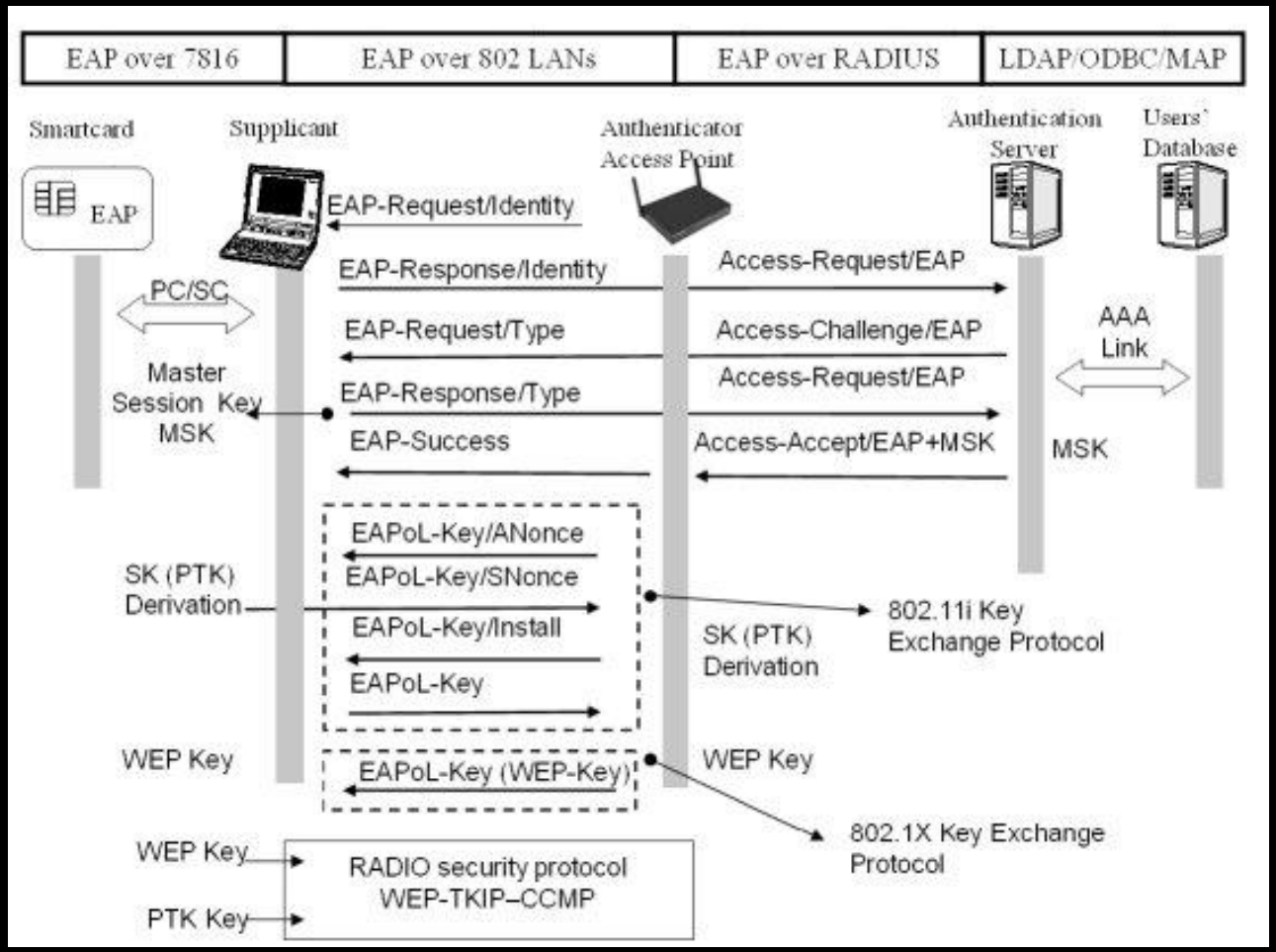
- Good PRNG @ embedded devices is a problem. E-S1 and E-S2 need to be random.
- NONCE = RAND(MAC) is not really random
- NONCE = RAND(time=01.01.1970 by default) is no really random too
- Vendors: Realtek, Ralink, Broadcom, MediaTek
- Tools: wifite fork, Pixiewps, reaver t6x fork

Protections?

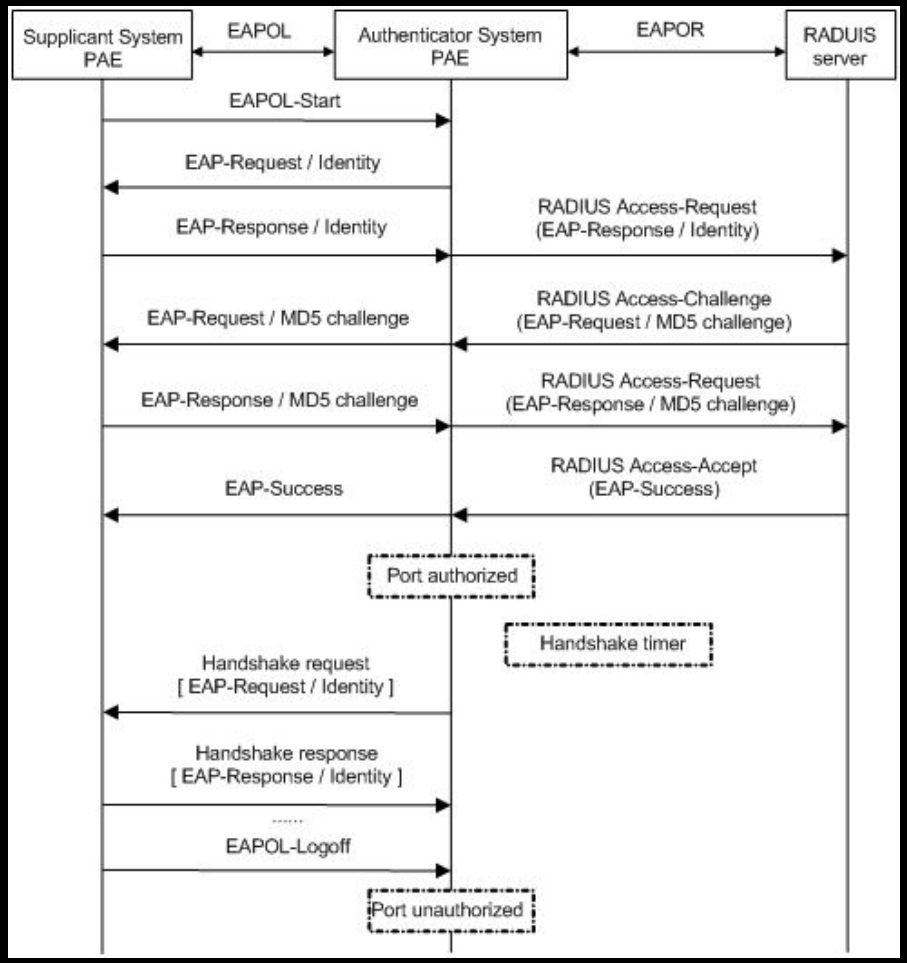
- WPS activation for 1 minute after BUTTON pressed (mgts)
- PIN from the end: 9999****
- WPS brute force timeout
- WPS brute force ban by MAC

WPA ENTERPRISE HACKING

WPA-Enterprise



EAP,EAPOL/EAPOR



WiFi + EAP

- EAP-TLS
- EAP-MD5
- EAP-SIM
- EAP-AKA
- PEAP
- LEAP
- EAP-TTLS

http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

PASSIVE Wi Fi HACKING


FREE
WiFi

Abbreviations part 1

- SSID – Service Set Identifiers (ESSID)
- BSSID – Basic service set identification (AP MAC)
- RSSI – Received Signal Strength Indication
- CINR – Carrier to Interference + Noise Ratio
- ACS – Auto Channel Selection
- WEP – Wired Equivalent Privacy
- WPA – Wi-Fi Protected Access aka Robust Secure Network (RSN)

Abbreviations part 2

- AES – Advanced Encryption Standard
- TKIP – Temporal Key Integrity Protocol
- CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- EAP – Extensible Authentication Protocol
- LEAP – Lightweight Extensible Authentication Protocol
- RADIUS – Remote Authentication Dial In User Service

Abbreviations part 3

- WPS/QSS – Wireless protected setup. WPS PIN WiFi Password
- PSK – Pre-Shared Key
- MIC – Michael message integrity code
- Authentication, Authorization, and Accounting (AAA) Key - Key information that is jointly negotiated between the Supplicant and the Authentication Server (AS). This key information is transported via a secure channel from the AS to the Authenticator. The pairwise master key (PMK) may be derived from the AAA key.
- Pairwise Master Key (PMK) – The highest order key used within the 802.11i amendment. The PMK may be derived from an Extensible Authentication Protocol (EAP) method or may be obtained directly from a Preshared key (PSK).
- Pairwise Transient Key (PTK) - A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).
- Group Master Key (GMK) - An auxiliary key that may be used to derive a group temporal key (GTK).
- Group Temporal Key (GTK) - A random value, assigned by the broadcast/multicast source, which is used to protect broadcast/multicast medium access control (MAC) protocol data units (MPDUs) from that source. The GTK may be derived from a group master key (GMK).

BOOKS

- 802.11 Wireless Networks The Definitive Guide - Matthew Gast
- 802.11n A Survival Guide – Matthew Gast
- Стандарты 802.11

Links

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

My repos

- https://github.com/0x90/kali-scripts
- https://github.com/0x90/wifi-arsenal
- https://github.com/0x90/wifi-scripts
- https://github.com/0x90/esp-arsenal

802.11 pwner in real life