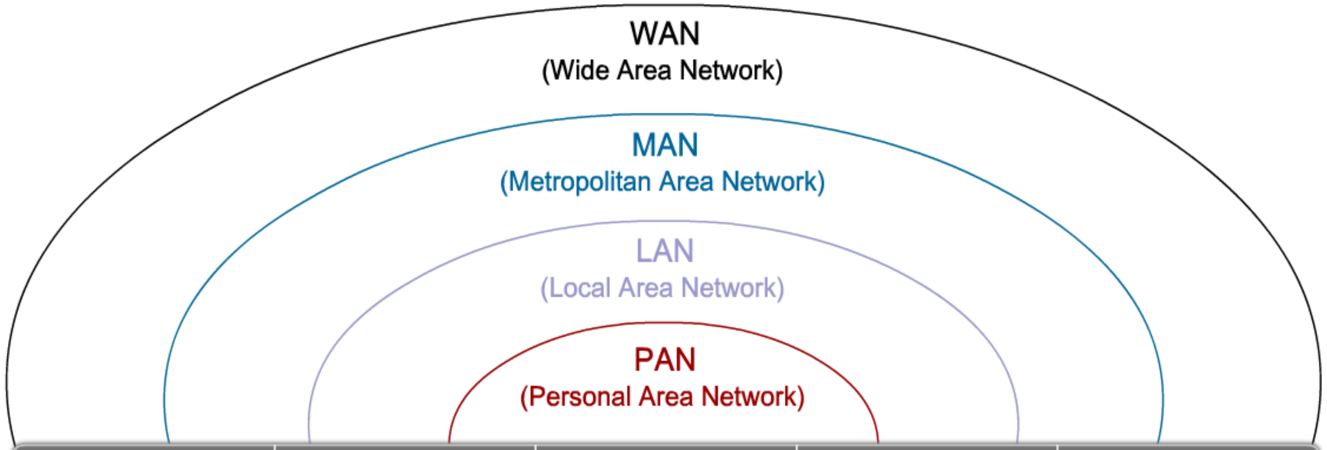
Wireless LAN 1/3

KIS FRI UNIZA

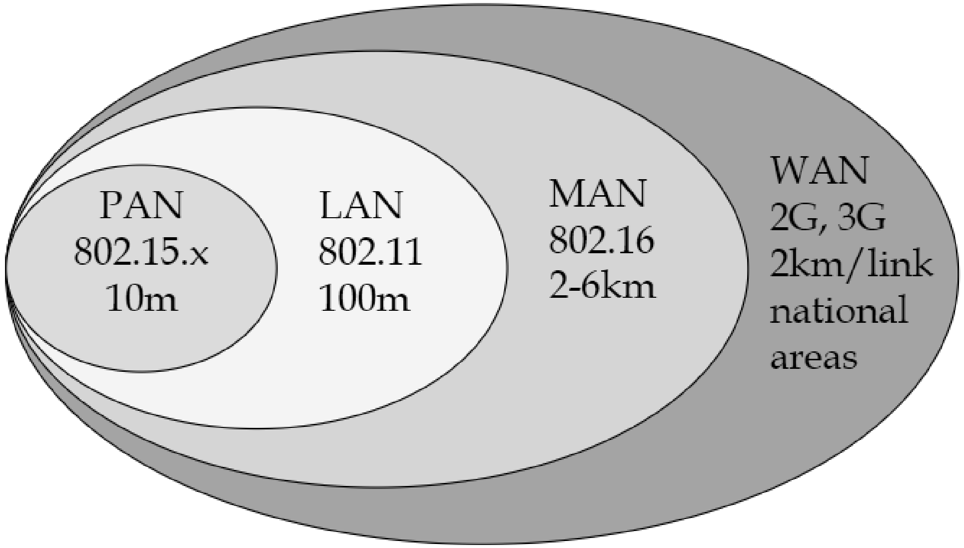
Vytvorené v rámci projektu KEGA 026TUKE-4/2021

Wireless Networks Overview

Wireless LANs



	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices



Wireless LAN (WLAN)

- A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area
- Users have the ability to move around within the area and remain connected to the network
- Through a gateway, a WLAN can also provide a connection to the wider Internet

- WLAN is based on the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standards which are the most widely used computer networks in the world
- IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of Media Access Control (MAC) and Physical layer (PHY) protocols

- WLAN is commonly called Wi-Fi, which is a trademark belonging to the Wi-Fi Alliance. WLAN certification is performed by the Wi-Fi Alliance

Wi-Fi history

- Wi-Fi was released in 1997 as 802.11 standard
- 802.11 refers to set of standards that define communication for WLAN
- It allowed 2Mbps of data transfer wirelessly between devices

- Wi-Fi uses ELM (electromagnetic) waves to communicate
- WLAN uses the Industrial, Scientific and Medical (ISM) band for WLAN operation. It shares the ISM band with other ISM band users such as Bluetooth, Near-field communication and the original intended users of the the ISM band – the Industrial/Scientific/Medical devices
- Data run typically at 2 main frequencies: 2.4GHz (802.11-1997 & 802.11b-1999) and 5GHz (802.11a-1999)

- For many years 2.4GHz frequency was popular choice as 2.4GHz Wi-Fi devices are typically less expensive and lower attenuation

Wireless Standardization Organizations

International Telecommunication Union (ITU)

- established in May 1865, specialized agency of the United Nations (from 1949)
- based in Geneva, Switzerland, the ITU's global membership includes 193 countries and around 900 business, academic institutions
- ITU Radiocommunication Sector (ITU-R) is one of the three sectors (divisions) of the ITU and is responsible for radio communications
- manages the international radio-frequency spectrum and satellite orbit resources and to develop standards for radiocommunication systems with the objective of ensuring the effective use of the spectrum

Wireless Standardization Organizations

Institute of Electrical and Electronics Engineers (IEEE)

- is a professional association for electronic engineering and electrical engineering
- established in 1963, based in New York, operations center in Piscataway, New Jersey
- more than 423,000 members in over 160 countries around the world
- IEEE 802 is a family IEEE standards for Local Area Networks (LAN), Personal Area Network (PAN), and Metropolitan Area Networks (MAN)
- The number 802 has no significance, it was simply the next number in the sequence that the IEEE used for standards projects

Wireless Standardization Organizations

Wi-Fi Alliance

- Early 802.11 products suffered from interoperability problems because IEEE had no provision for testing equipment for compliance with its standards
- Wireless Ethernet Compatibility Alliance (WECA) established in 1999 by 3Com, Aironet (acquired by Cisco), Harris Semiconductor (now Intersil), Lucent (former Alcatel-Lucent, acquired by Nokia), Nokia, and Symbol Technologies (now Zebra Technologies)
- WECA renamed itself to the Wi-Fi Alliance in 2002. It is based in Austin, Texas
- currently over 550 members
- The Wi-Fi Alliance owns and controls the "Wi-Fi Certified" logo

IEEE 802 Family of Standards

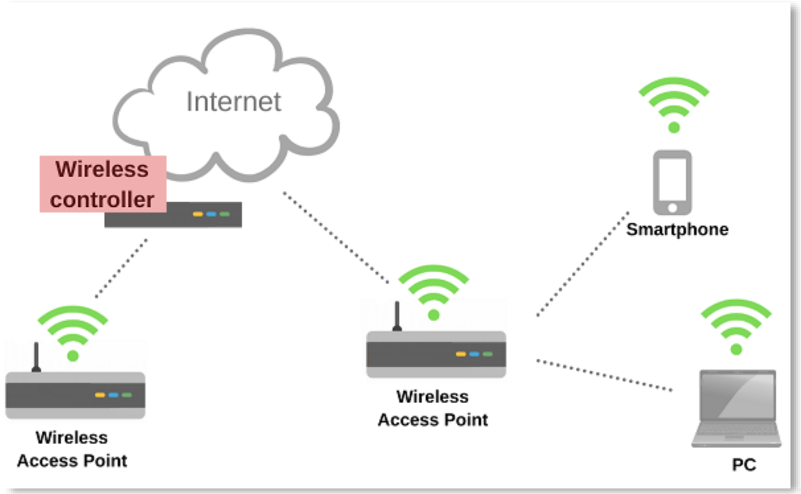
IEEE 802 Standards	
802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

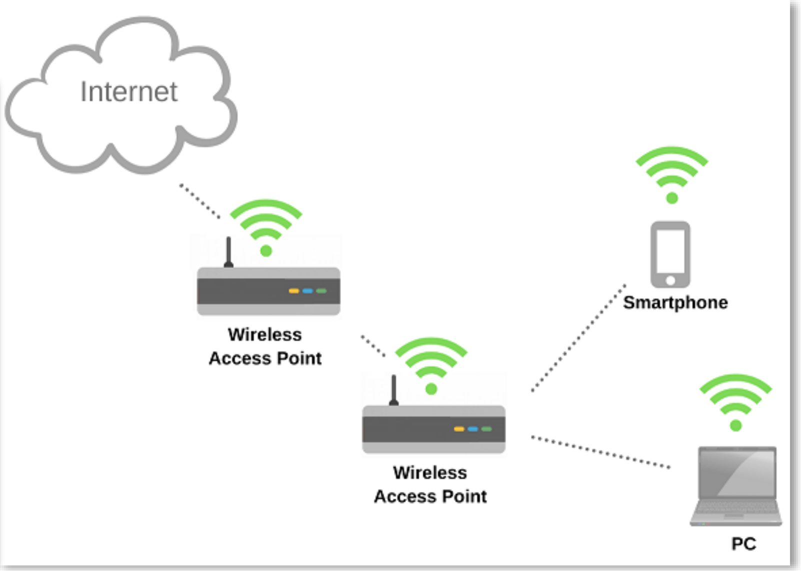
WLAN Network Topologies, Terminology and Architecture

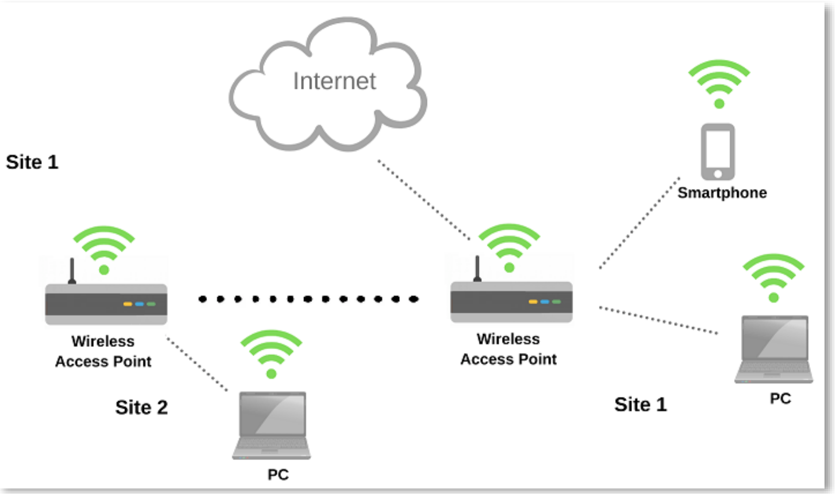
WLAN Network Topologies

Two basic modes of operation in WLAN standards commonly used:

1. **Infrastructure mode** – in this mode WLAN provides end-point connectivity to clients, end clients connect wirelessly to a WLAN master device (Access Point – AP). The AP would connect to Internet or to a network controller (typically via Ethernet)
    - Standalone or CAPWAP (Control And Provisioning of Wireless Access Points) modes
    - Client mode - APcan connect to another APas a client
    - Bridge mode using Wireless Bridge Link
2. **Ad-hoc mode** – peer to peer connections, provides a self-sufficient wireless network, one of the devices in the network would assume the role of a master, no AP







IEEE 802.11 Terminology

AP (Access Point)

- A device that provides wireless access

STA (Station)

- End devices that connect to WiFi network

BSS (Basic Service Set)

- A set of end stations controlled by a single AP

ESS (Extended Service Set)

- Two or more interconnected BSSes

IBSS (Independent Basic Service Set)

- Known as ad-hoc network without AP

BSSID

- Each BSS is identified by 6B identifier, typically AP’s MAC

SSID (Service Set ID)

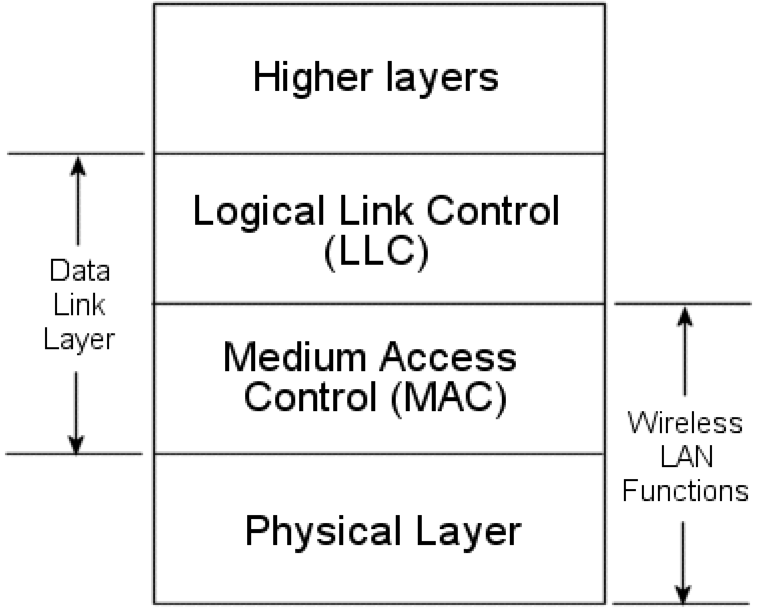
- 2B to 32B ASCI character identifier (network name), when multiple APs share the same SSID -> they form ESS and SSID is called ESSID

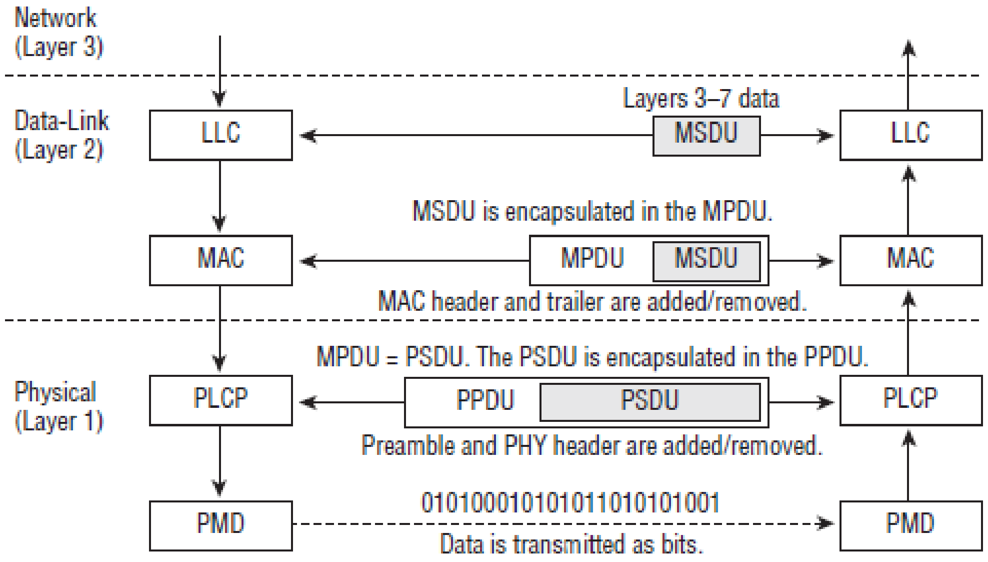
DCF (Distributed Coordination Function)

- The fundamental MAC technique (CSMA/CA) of the IEEE 802.11-based WLAN standard, DCF uses a collision avoidance (CA) mechanism to control access to the shared wireless medium (CSMA stand for Carrier Sense Multiple Access)

IEEE 802.11 Protocol Architecture

- **PHY (Physical Layer)**
  - The physical later transmits the bits of data through the channel by defining electrical, mechanical, and procedural specifications
- **MAC (Media Access Control)**
  - Allows many wireless computers, or any wireless appliances, to share the same frequency. The data needs to be transmitted at different times
- **LLC (Logical Link Control)**
  - Responsible for multiplexing of several network protocols (IPv4/IPv6, IPX, other)
  - Exchanges data between users on either end of a LAN, this is used by IEEE 802.2





PLCP - Physical Layer Convergence Procedure sublayer
PMD - Physical Medium Dependent sublayer
PPDU - PLCP Protocol Data Unit
PSDU - PLCP Service Data Unit
MPDU - MAC Protocol Data Unit
MSDU - MAC Service Data Unit

Physical Layer

IEEE 802.11 Physical Layer

Overview

- The lowest layer of the IEEE 802 reference model, includes functions as:
  - **Encoding** & **decoding** of signals
  - Bit transmission & reception - **modulation** and **transmission** techniques
  - The physical layer includes a **specification of the transmission medium**
  - Also **defines frequency bands** and antenna characteristics

IEEE 802.11 Protocol	Release Date	Frequency Band(s)	Bandwidth	Max Throughput
802.11-1997	1997	2.4	22	2 Mbps
11b	1999	2.4	22	11 Mbps
11a	1999	5	20	54 Mbps
11g	2003	2.4	20	54 Mbps
11n (Wi-Fi 4)	2009	2.4/5	20/40	600 Mbps
11ac (Wi-Fi 5)	2013	2.4/5	20/40/ 80/160	6.8 Gbps
11ax (Wi-Fi 6)	2019	2.5/5	20/40/ 80/160	10 Gbps

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11(DSSS)	BPSK	1 MSps	1
2 Mbps	11(DSSS)	QPSK	1 MSps	2
5.5 Mbps	8(CCK)	QPSK	1.375 MSps	4
11 Mbps	8(CCK)	QPSK	1.375 MSps	8

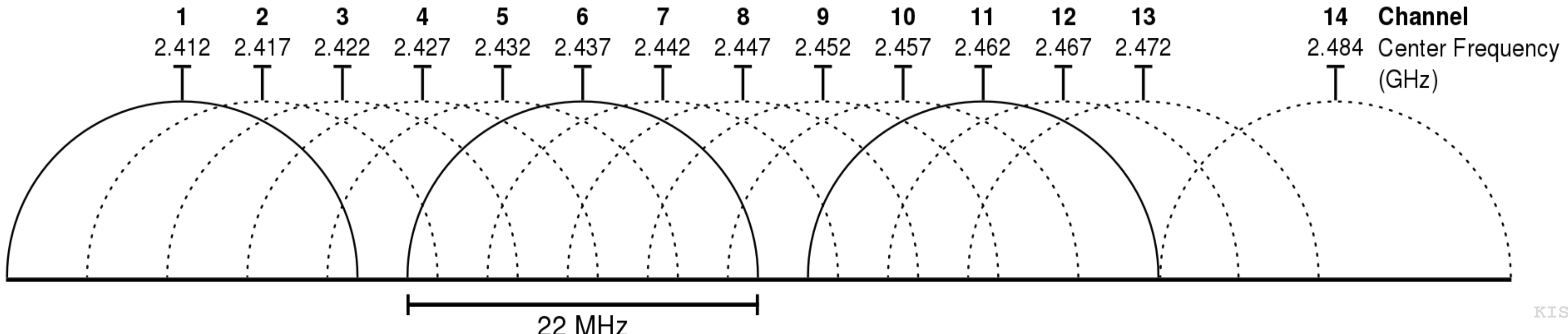
BPSK (Binary Phase Modulation)
QPSK (Quadrature Phase Modulation)
CCK (Complementary Code Keying)
DSSS (Direct Sequence Spread Spectrum) are spread spectrum modulation techniques which reduces overall signal interference during transmission due to presence of information below noise level.

IEEE 802.11 Physical Layer

WiFi 2.4GHz band

- Band covers 2,400–2,485GHz which makes it 85MHz wide
- 22MHz wide channels
- 13 channels in Europe, in Japan there are 14 channels, in the US only 11 channels
- Channels are overlapping
- The maximum transmission power in EU on 2.4GHz is 100mW or 20dBm
- 2.4GHz is also used by microwave ovens, cordless phones, baby monitors and wireless video cameras

Channel	Frequency (GHz)	Range
1	2.412	2.401 -2.423
2	2.417	2.406 - 2.428
3	2.422	2.411 - 2.433
4	2.427	2.416 - 2.438
5	2.432	2.421 - 2.443
6	2.437	2.426 - 2.448
7	2.442	2.431 - 2.453
8	2.447	2.436 - 2.458
9	2.452	2.441 - 2.463
10	2.457	2.446 - 2.468
11	2.462	2.451 - 2.473
12	2.467	2.456 - 2.478
13	2.472	2.461 - 2.483
14	2.484	2.473 - 2.495



IEEE 802.11 Physical Layer

WiFi 5GHz band

- 5GHz band is divided into 5MHz channels like the 2.4GHz band
- Only every fourth channel (36, 40, 44…) is used which provides 20MHz channel width without the overlap problems of 2.4GHz
- In Europe (or in ETSI jurisdiction) channels 36–64 are restricted for indoor use
- The maximum transmission power is 200mW (23dBm), but still doesn’t quite compensate for the 6dB attenuation due to higher frequency
- On channels 100–140 the maximum transmit power is 1W (30dBm) and the channels can be used outdoors as well (not relevant for APes, rather used for P2P links)
- The upper channels 149–165 mostly not supported yet
- 802.11n introduced the concept of combining channels
- When AP supports DFS frequencies, it will be necessary for WiFi access points to verify that any radar in proximity is not using DFS frequencies (AP startup typically delayed for a minutes due to radar detection)

<table>
<tr><td>Band</td><td colspan="4">UNII-I</td><td colspan="4">UNII-II</td><td colspan="11">UNII-II Extended</td><td colspan="4">UNII-III</td><td>ISM</td></tr>
<tr><td>20 MHz</td><td>36</td><td>40</td><td>44</td><td>48</td><td>52</td><td>56</td><td>60</td><td>64</td><td>100</td><td>104</td><td>108</td><td>112</td><td>116</td><td>120</td><td>124</td><td>128</td><td>132</td><td>136</td><td>140</td><td>149</td><td>153</td><td>157</td><td>161</td><td>165</td></tr>
<tr><td>40 MHz</td><td colspan="2">38</td><td colspan="2">46</td><td colspan="2">54</td><td colspan="2">62</td><td colspan="2">102</td><td colspan="2">110</td><td colspan="2">118</td><td colspan="2">126</td><td colspan="2">134</td><td></td><td colspan="2">151</td><td colspan="2">159</td><td></td></tr>
<tr><td>80 MHz</td><td colspan="4">42</td><td colspan="4">58</td><td colspan="4">106</td><td colspan="4">122</td><td colspan="3"></td><td colspan="4">155</td><td></td></tr>
<tr><td>160 MHz</td><td colspan="8">50</td><td colspan="8">114</td><td colspan="3"></td><td colspan="5"></td></tr>
<tr><td>Power</td><td colspan="8">23dBm (200mW)</td><td colspan="11">30dBm (1W)</td><td colspan="5">14dBm (25mW)</td></tr>
<tr><td>Notes</td><td colspan="8">Indoors</td><td colspan="5"></td><td colspan="3">WeatherRdr</td><td colspan="3"></td><td colspan="5"></td></tr>
<tr><td></td><td colspan="4"></td><td colspan="15">Dynamic Frequency Selection (DFS)</td><td colspan="5"></td></tr>
</table>

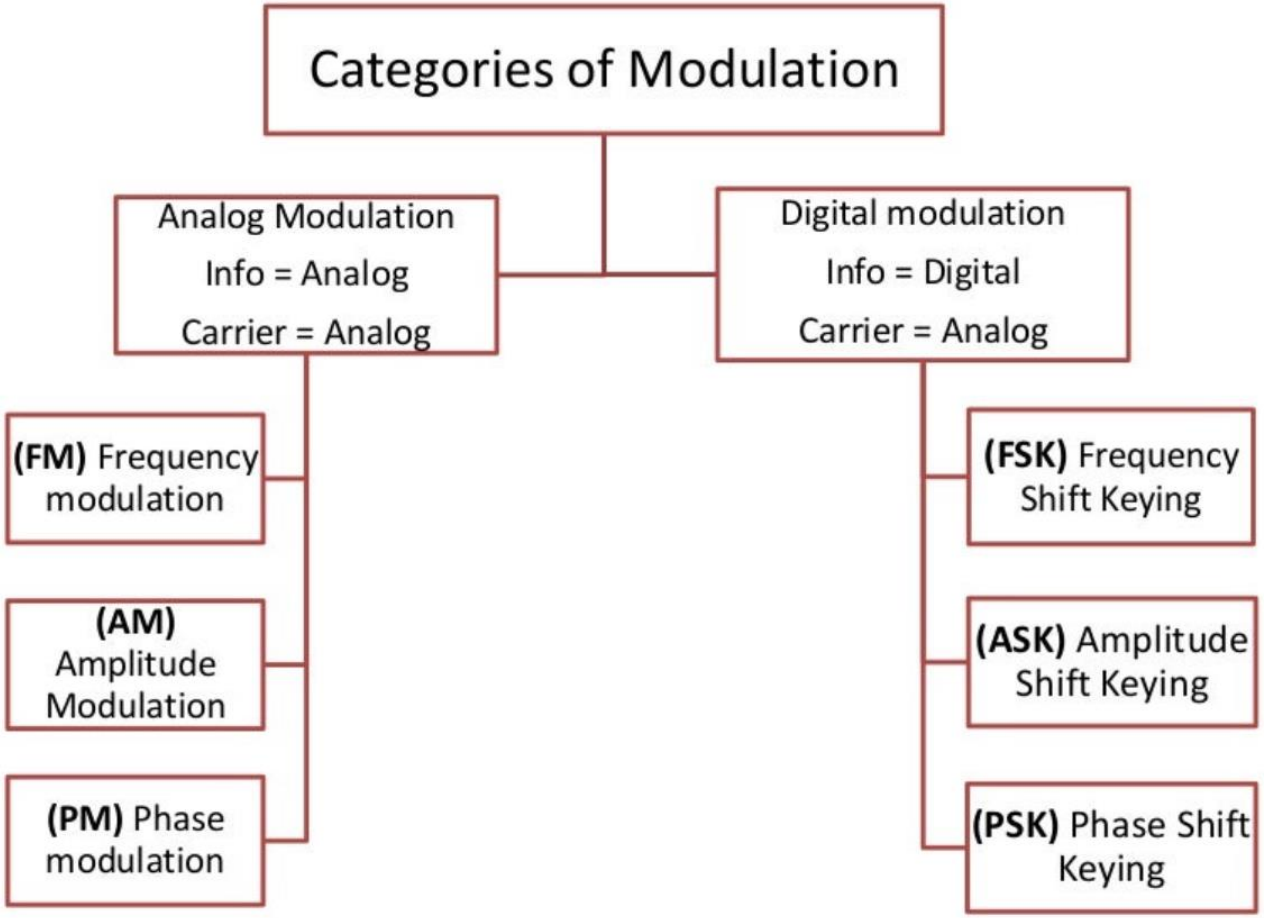
UNII - Unlicensed National Information Infrastructure

ISM - Industrial, Scientific and Medical bands

IEEE 802.11 Physical Layer

Modulation

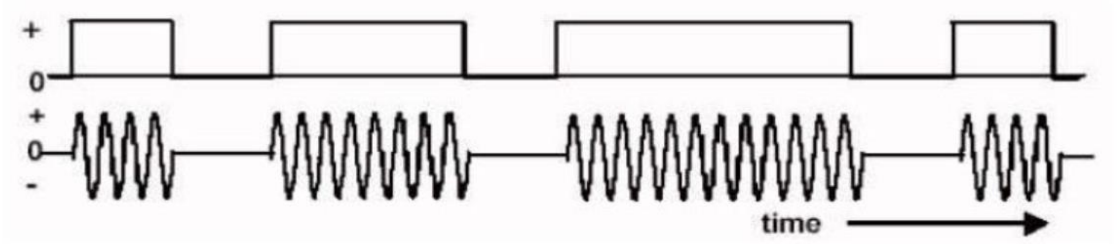
- Modulation is a process of modifying of the amplitude, frequency or phase of high frequency carrier in accordance with low frequency information signal
- The result is called modulated signal
- The carrier is typically sine wave
- Information signal may be either **analog** or **digital**



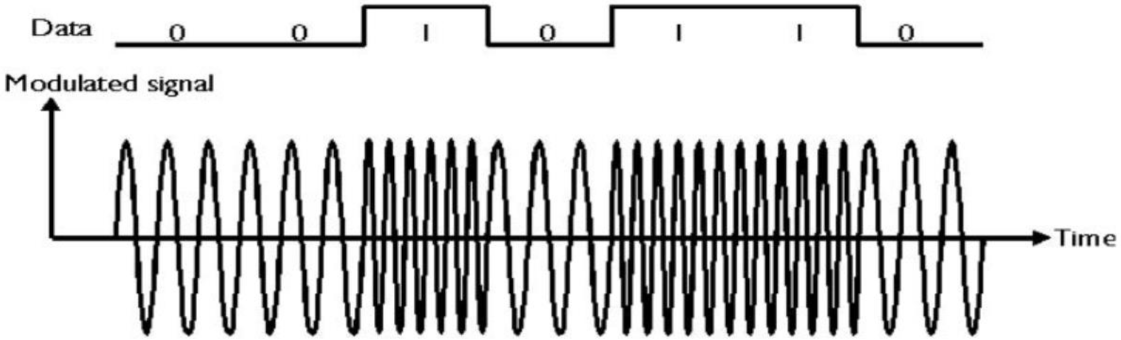
IEEE 802.11 Physical Layer

Digital Modulations

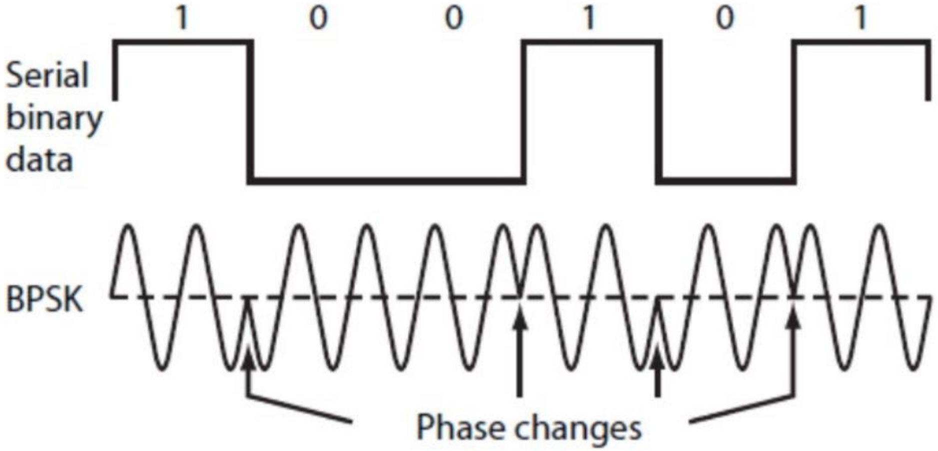
- Amplitude Shift Keying (ASK)



- Frequency Shift Keying (FSK)



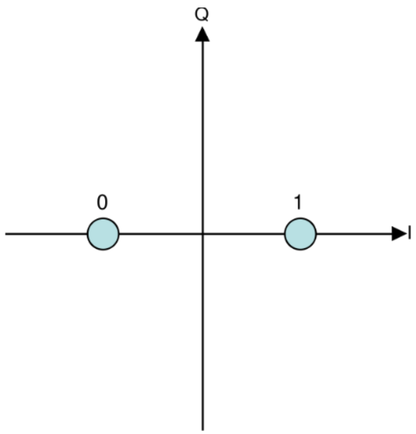
- Phase Shift Keying (PSK)

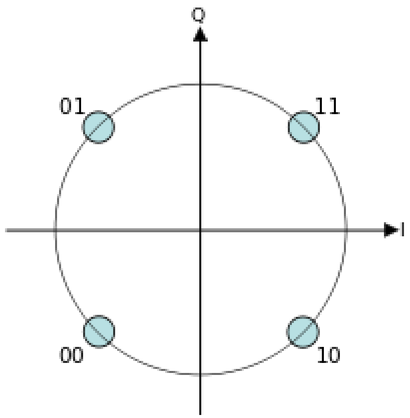


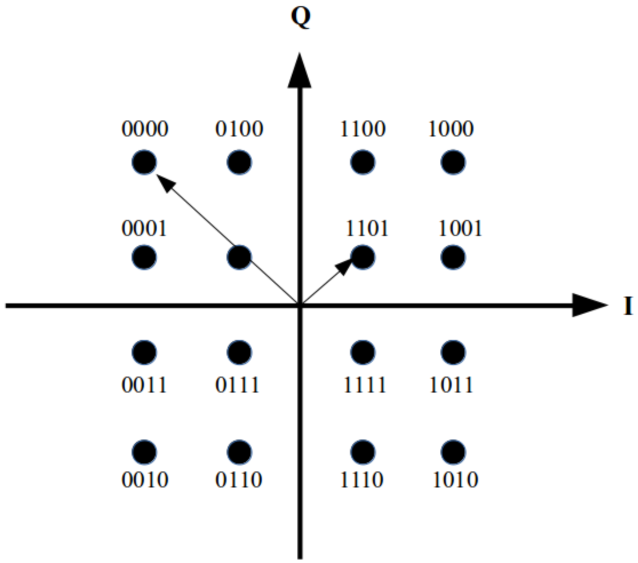
IEEE 802.11 Physical Layer

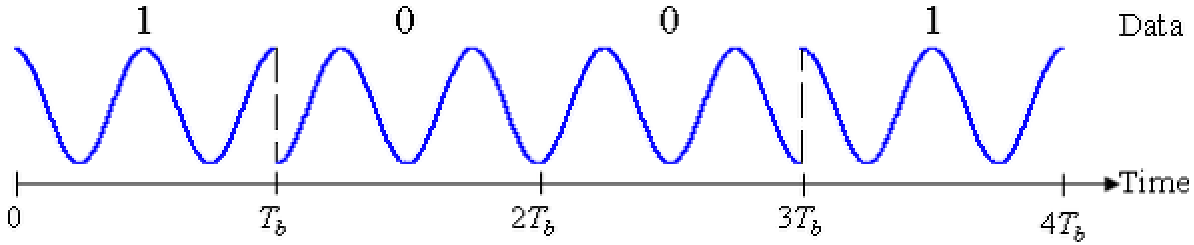
Phase Shift Keying Modulation principles

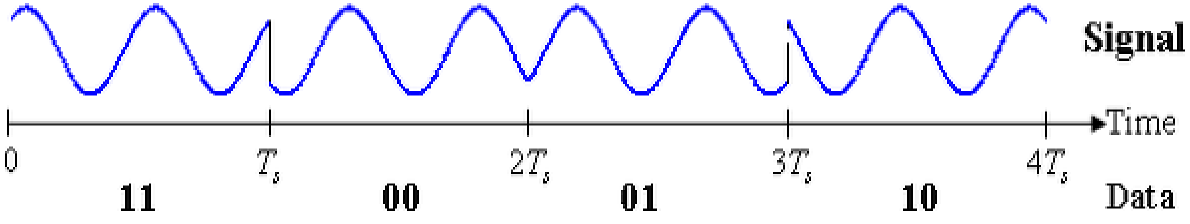
- BPSK (Binary PSK)
- QPSK (Quadrature PSK)
- QAM (Quadrature Amplitude Modulation)
  - 16-QAM, 64-QAM, 256-QAM
  - Amplitude and Phase











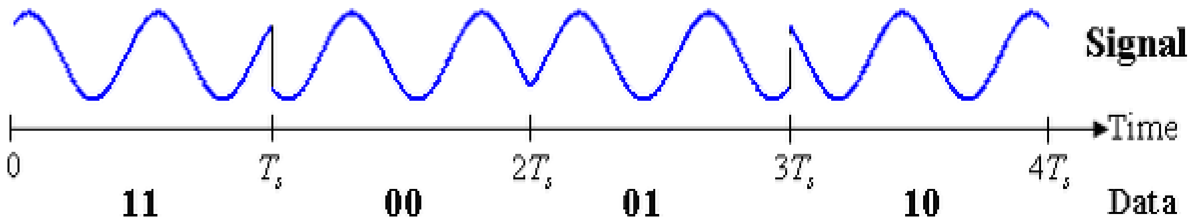
IEEE 802.11 Physical Layer

Baud (or symbol or code word) rate and bit rate

- **Baud (or symbol) rate** is the measure of the number of changes to the signal (per second) that propagate through a transmission medium
- **Bit rate** is the transmission of number of bits per second

Modulation	Bits per symbol	Symbol Rate
BPSK	1	$1.0 \times$ bit rate
QPSK	2	$1/2 \times$ bit rate
8-PSK	3	$1/3 \times$ bit rate
16-QAM	4	$1/4 \times$ bit rate
32-QAM	5	$1/5 \times$ bit rate
64-QAM	6	$1/6 \times$ bit rate

Bit_rate = Baud_rate * the_number_of_bit_per_Baud



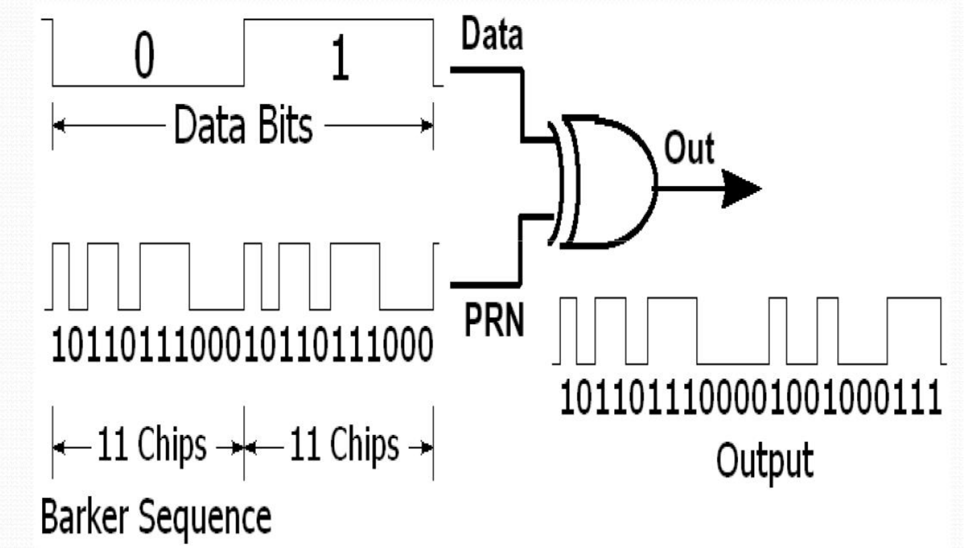
IEEE 802.11 Physical Layer

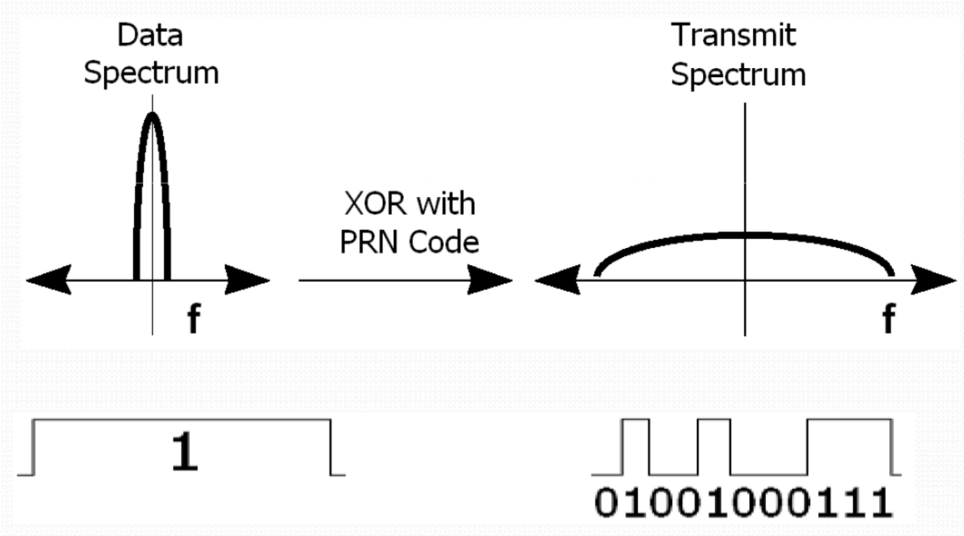
Spread Spectrum and Additional Modulation Technics

Spread spectrum technics are used to spread frequencies of a signal from its narrow band domain –> securing communication, resistance to interference

- **FHSS** – Frequency Hopping Spread Spectrum
- **DSSS** – Direct Sequence Spread Spectrum
- **CCK** - Complementary code keying
- **OFDM** – Orthogonal Frequency Division Multiplexing

Effect of PRN (Pseudo Random Numerical) sequence on transmit spectrum

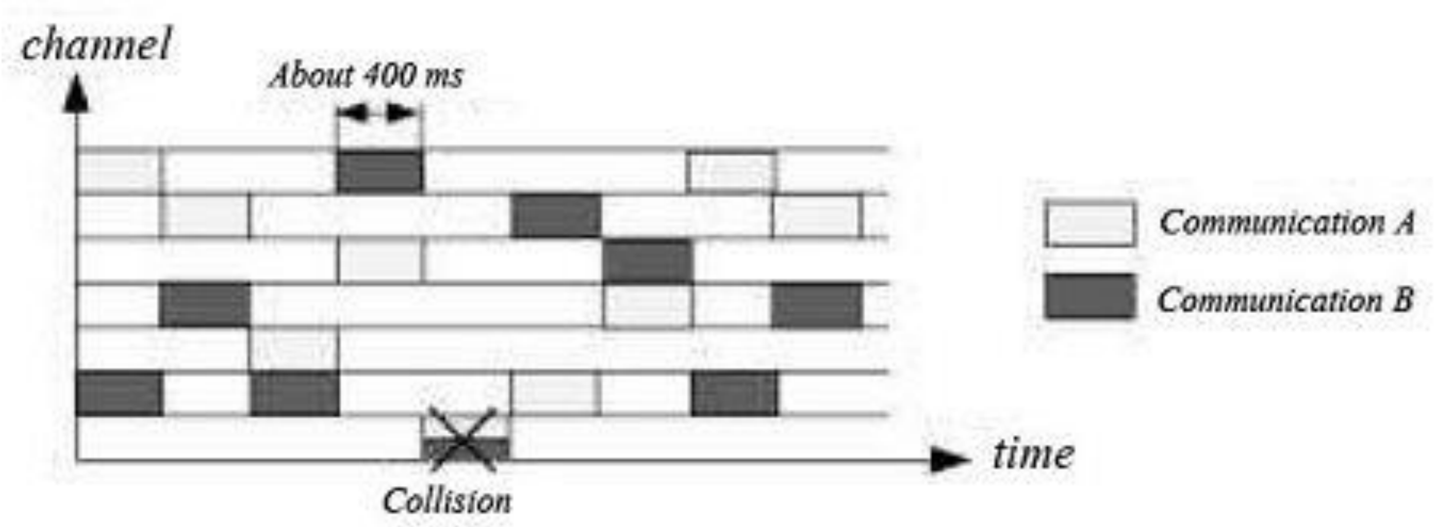




IEEE 802.11 Physical Layer

FHSS technique

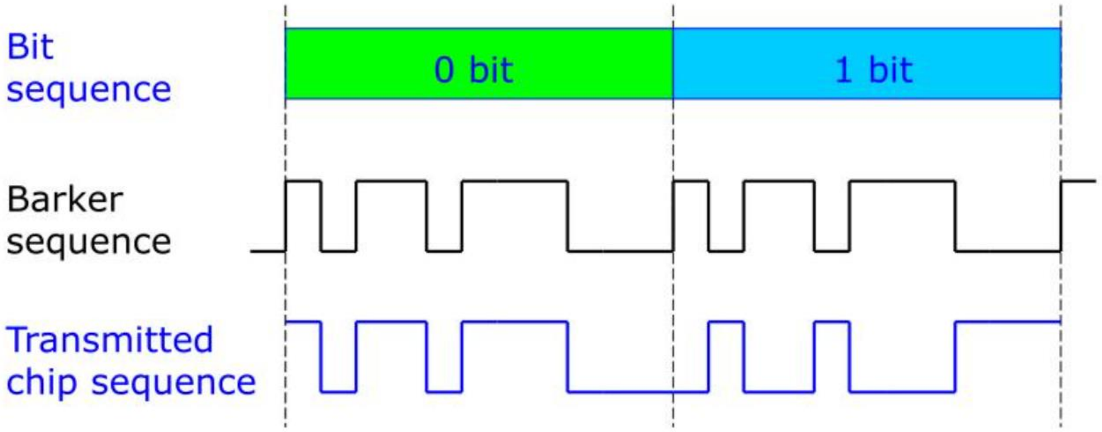
- Frequency Hopping Spread Spectrum technique is a method of transmitting signals by rapidly switching channels, using a pseudorandom sequence known to both transmitter and receiver
- Resistant technique to narrowband interference
- Difficult to intercept
- Typically, two transmitters do not transmit data over the same frequency at the same time



IEEE 802.11 Physical Layer

DSSS technique

- Direct Sequence Spread Spectrum
- Encoding with 11-chip **Barker** sequence
- Used only at 1 and 2 Mbps

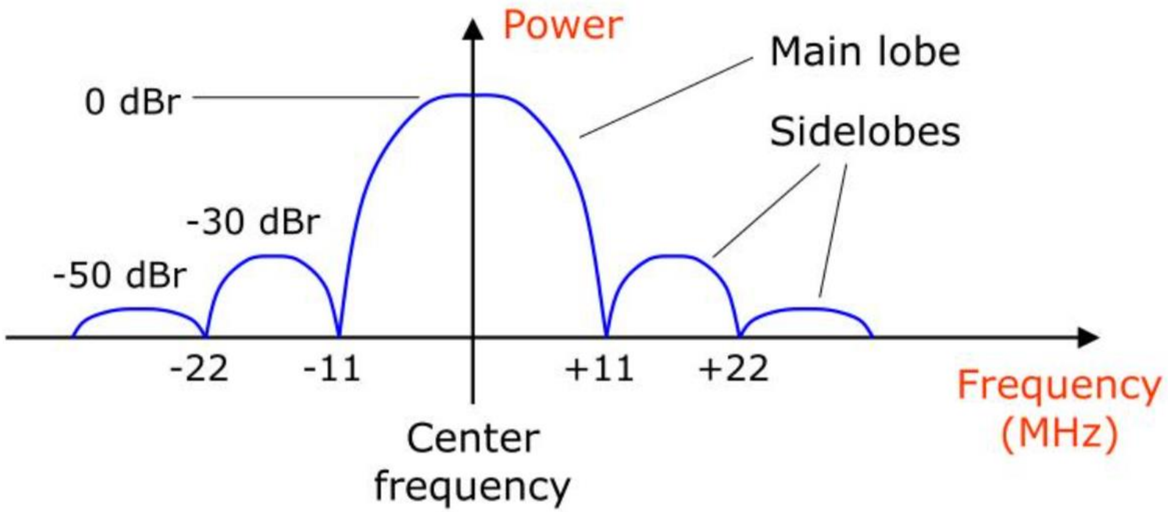


Why 1 or 2 Mbps?

- Chip rate = 11Mchip/s
- One chip duration 1/11 microsec
- Code word (or symbol) rate = 1MWord/s
- Each code word (symbol) carries 1 bit (BPSK) or 2 bits (QPSK)

- Bit rate = 1Mbps or 2Mbps

Energy spread of 11 Mchip/s sequence



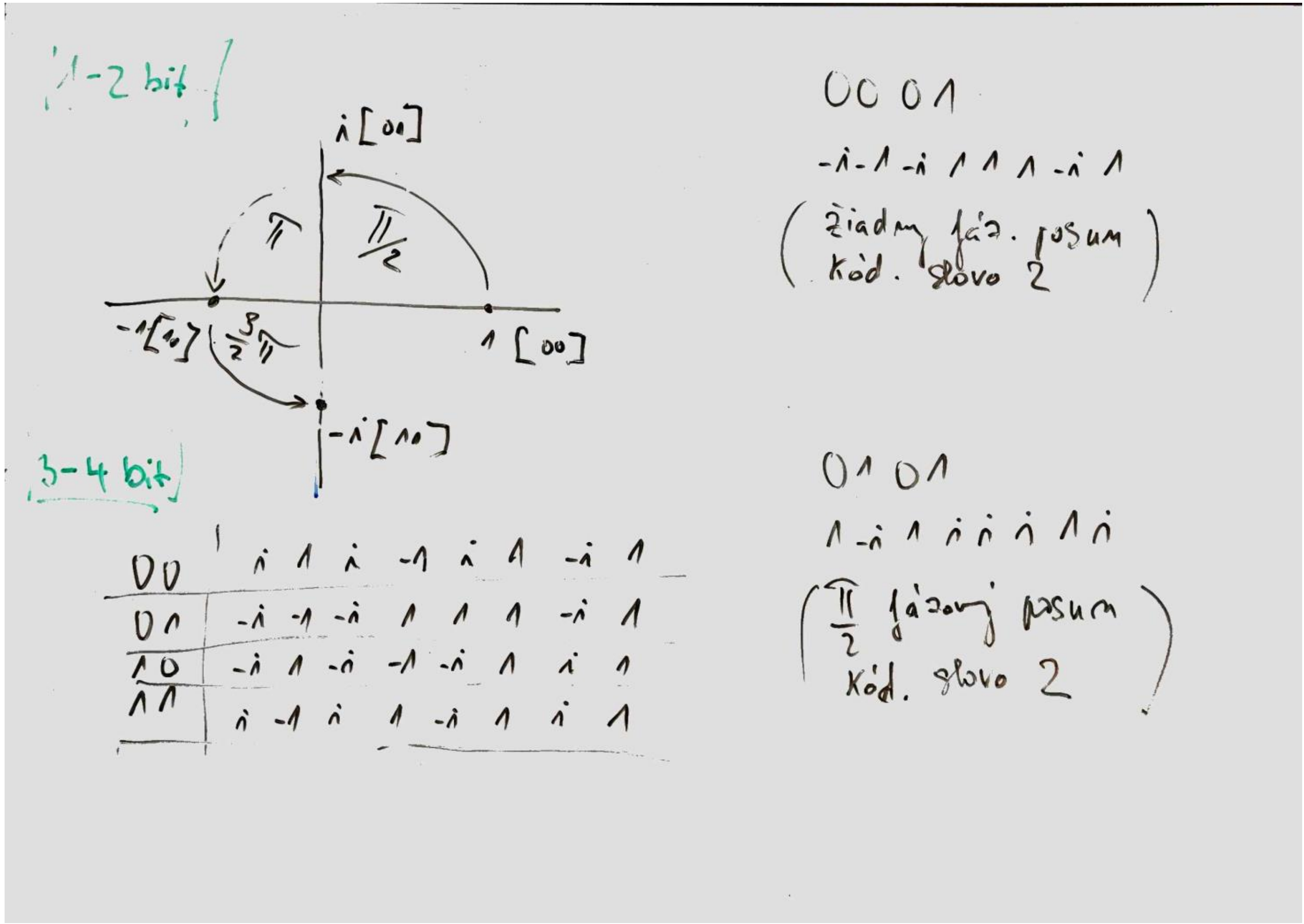
IEEE 802.11b Physical Layer

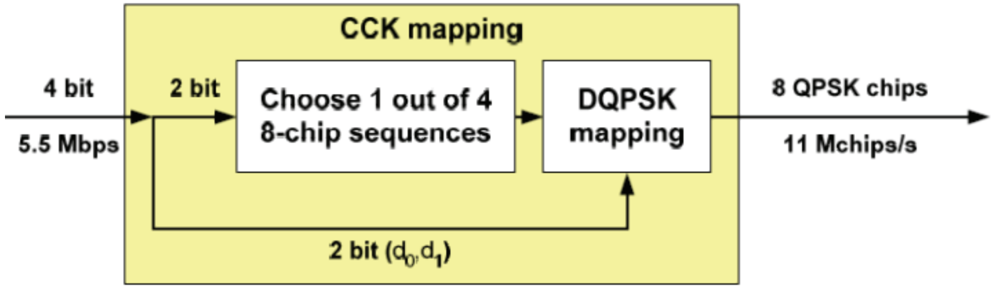
CCK technique

- Complementary Code Keying

- Set of 4 or 64 8-bit code words (symbols) used to encode data for 5.5 and 11 Mbps

- Code words have unique mathematical properties that allow them to be correctly distinguished from one another by receiver



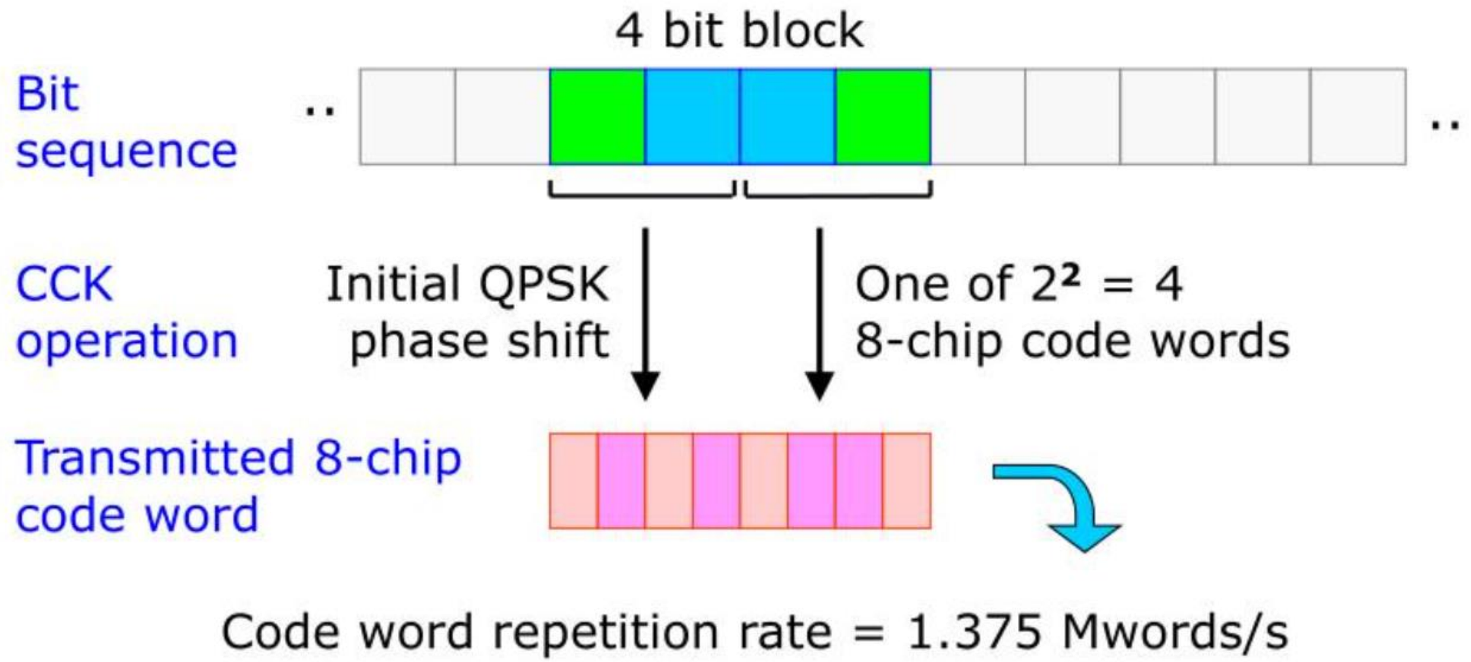


IEEE 802.11b Physical Layer

CCK technique

Why 5.5 Mbps?

- Chip rate = 11Mchip/s
- One chip duration 1/11 microsec
- Code word (symbol) rate = 11/8 MWord/s = 1.375 Mword/s
- Each code word (symbol) carries 4 bits (2 bits QPSK, 2 bits CCK chip)
- Bit rate = 5.5 Mbps

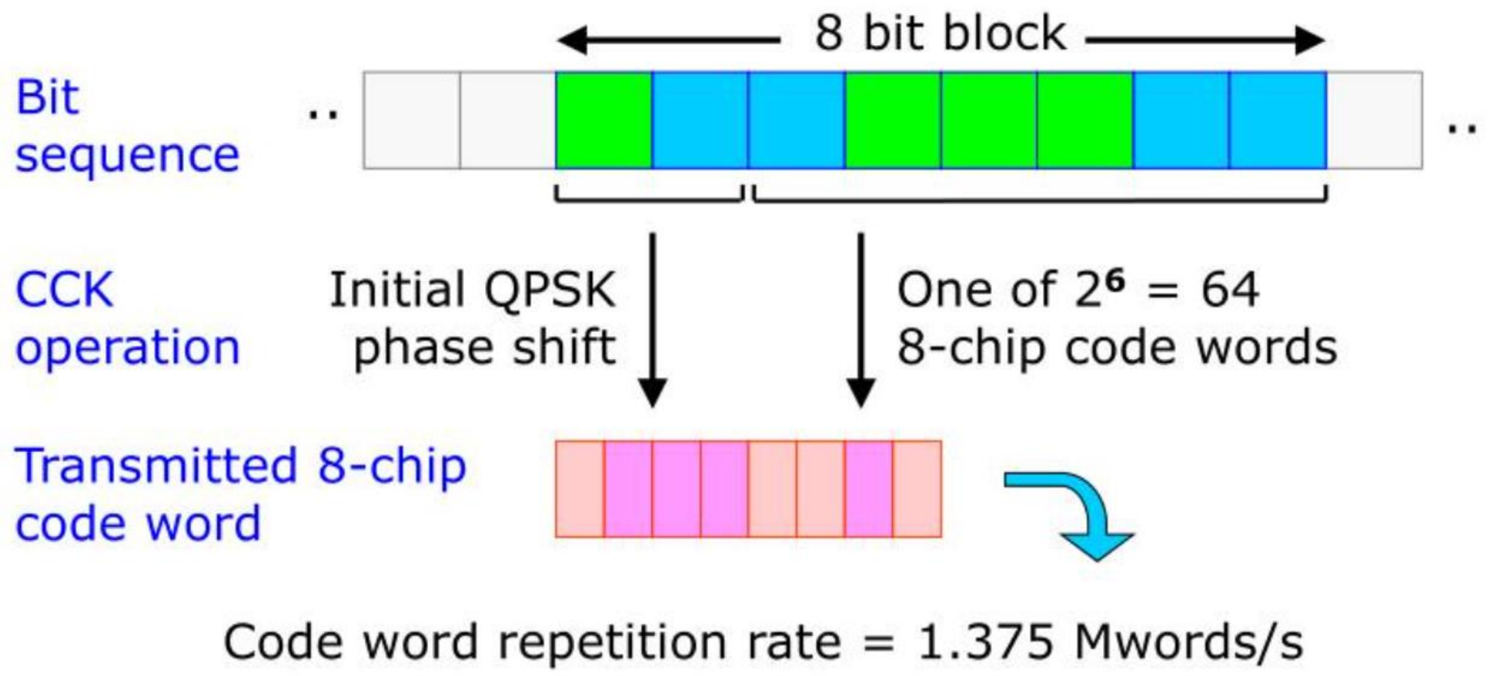


IEEE 802.11b Physical Layer

CCK technique

Why 11 Mbps?

- Chip rate = 11Mchip/s
- One chip duration 1/11 microsec
- Code word (symbol) rate = 11/8 MWord/s = 1.375 Mword/s
- Each code word (symbol) carries 8 bits (2 bits QPSK, 6 bits CCK chip)
- Bit rate = 11 Mbps



IEEE 802.11 Physical Layer

IEEE 802.11 and 802.11b summary

- **1997** – the first WLAN standard IEEE 802.11-1997 (1Mbps and 2Mbps @ 2.4GHz)
- **1999** – Extension with higher data rates IEEE 802-11b (5.5Mbps and 11Mbps @ 2.4GHz)

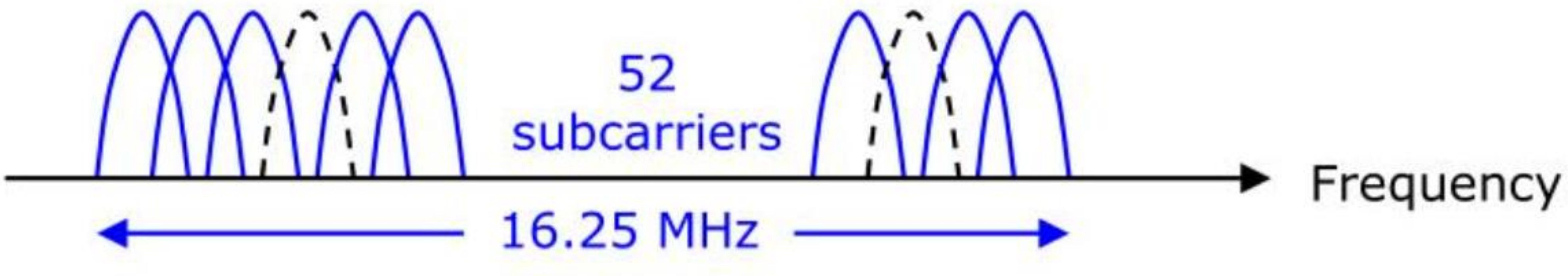
	FHSS	DSSS
Spreading	Frequency	Code
Modulation	FSK	PSK
Signal-to-Noise Ratio (SNR)	18 dB	12 dB
Frequency band	2.402 – 2.480 GHz	2.401 – 2.483 GHz
Bandwidth	79 MHz (Short term: 1 MHz for a single hop)	22 MHz (for a single sub-band)
Data rates	1 Mbps (mandatory) 2 Mbps (optional)	1 Mbps (mandatory) 2 Mbps (optional)

	Data rate	Code length	Modu-lation	Symbol rate	Bits/ Symbol
Defined in 802.11	1 Mbps	11 (Barker-Code)	BPSK	1 Msps	1
	2 Mbps	11 (Barker-Code)	QPSK	1 Msps	2
Defined in 802.11b	5.5 Mbps	8 (CCK)	QPSK	1.375 Msps	4 (2+2)
	11 Mbps	8 (CCK)	QPSK	1.375 Msps	8 (2+6)

IEEE 802.11a/g Physical Layer

OFDM technique

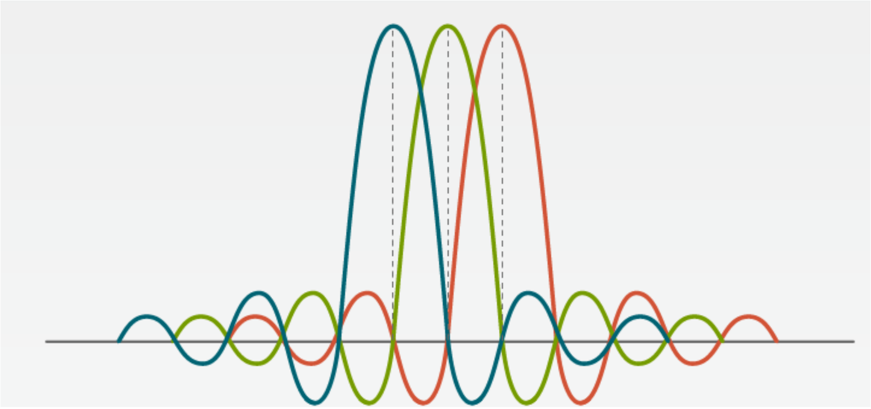
- This physical layer implementation is based on Orthogonal Frequency Division Multiplexing
- The information is carried over the radio medium using orthogonal subcarriers
- A channel (16.25 MHz wide) is divided into 52 subcarriers
- 48 data subcarriers
- 4 subcarriers serving as pilot signals
- Subcarriers are modulated using BPSK, QPSK, 16-QAM or 64-QAM using convolutional codes R=1/2, 2/3 and 3/4



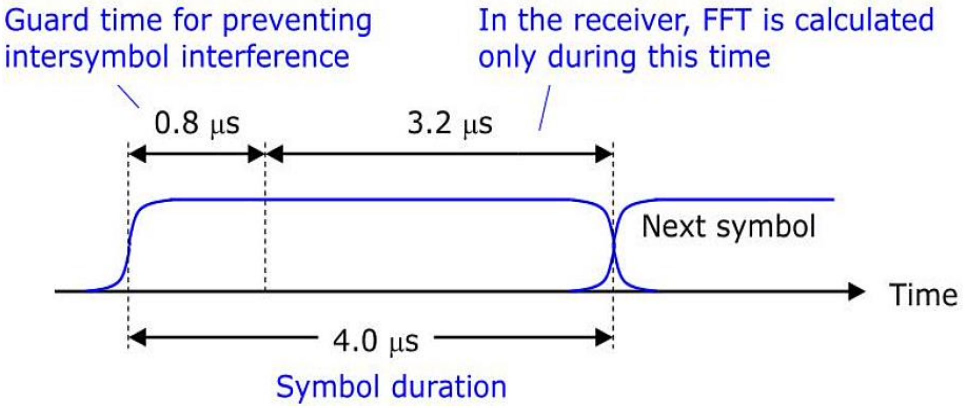
IEEE 802.11a/g Physical Layer

OFDM technique – subcarrier modulation and coding

- With OFDM, signals can overlap with each other
- While one signal is at its peak, the other signals are at their zero-point, allowing the receiver to differentiate between each signal
- It is possible to pack more data into a smaller range of frequency



Each signal peaks while other signals are at zero point



Presentation of OFDM signal in time domain

Modulation	Bit rate	Coding rate	Coded bits / symbol	Data bits / symbol
BPSK	6 Mbit/s	1/2	48	24
BPSK	9 Mbit/s	3/4	48	36
QPSK	12 Mbit/s	1/2	96	48
QPSK	18 Mbit/s	3/4	96	72
16-QAM	24 Mbit/s	1/2	192	96
16-QAM	36 Mbit/s	3/4	192	144
64-QAM	48 Mbit/s	2/3	288	192
64-QAM	54 Mbit/s	3/4	288	216

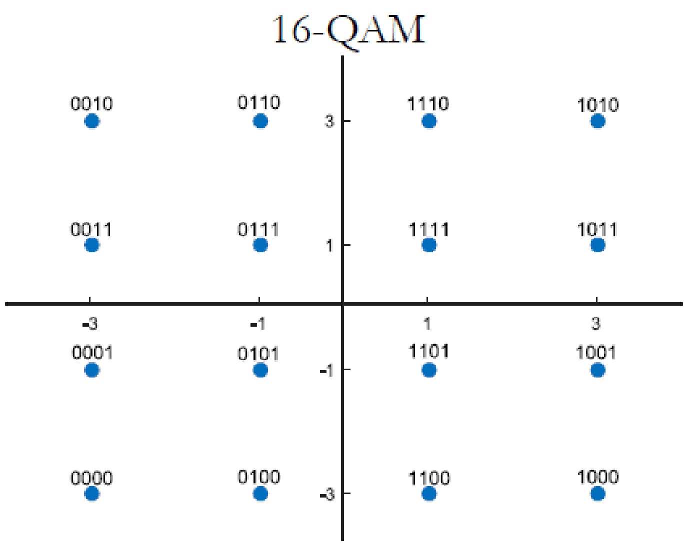
IEEE 802.11a/g Physical Layer

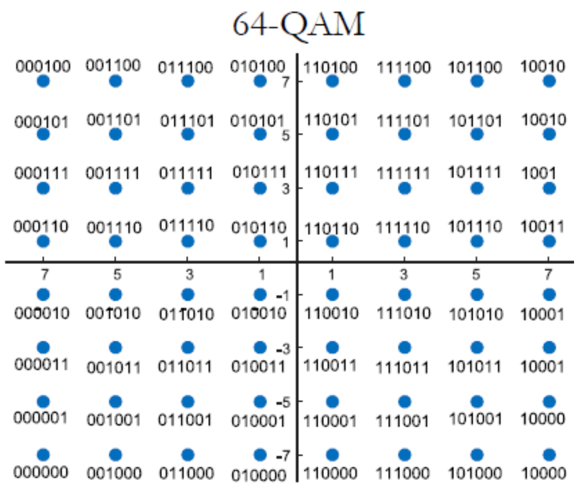
OFDM technique – data rate

Why 54 Mbps?

- Symbol duration = 4 microsecs
- Data subcarriers = 48
- Coded bits per subcarrier = 6 (64-QAM)
- Coded bits per symbol = 6*48 = 288
- Data bits per symbol 3 / 4 * 288 = 216 bits / symbol

- Bit rate = 216 bits / 4 microsecs = 54 Mbps





Note: 802.11g operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput

IEEE 802.11 Physical Layer

IEEE 802.11a and 802.11g summary

- **1999** – IEEE 802.11a (up to 54Mbps @ 5Ghz) - this standard was designed for US purposes therefore just rarely used in EU. It uses the same data link layer protocol and frame format as the original standard, just OFDM (physical layer) was added

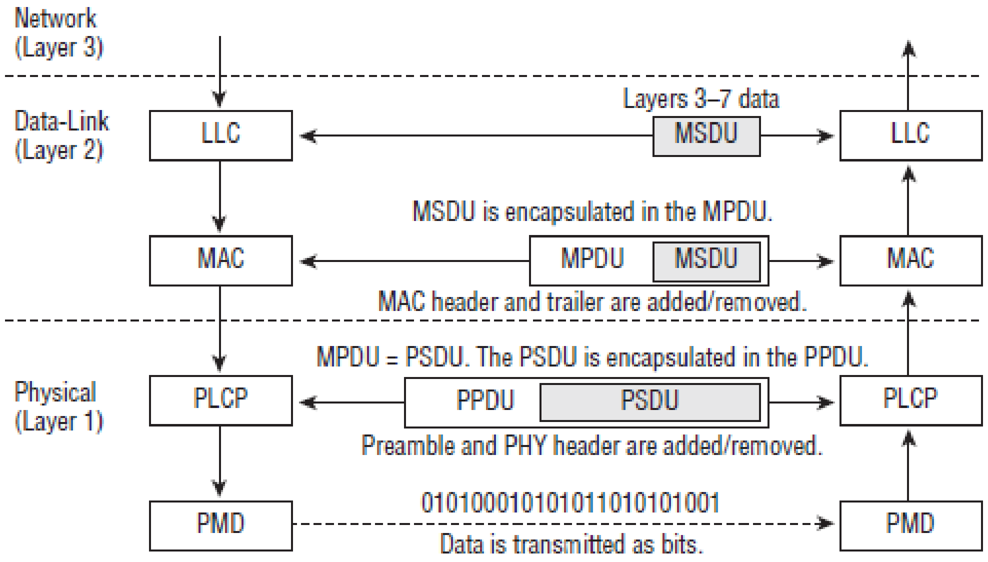
- **2003** - IEEE 802.11g - works in the 2.4 GHz band (like 802.11b) but uses the same OFDM based transmission scheme as 802.11a
- It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput
- 802.11g hardware is fully backward compatible with 802.11b hardware
- 802.11g and 802.11b stations must be able to share the same channels in the 2.4 GHz frequency band

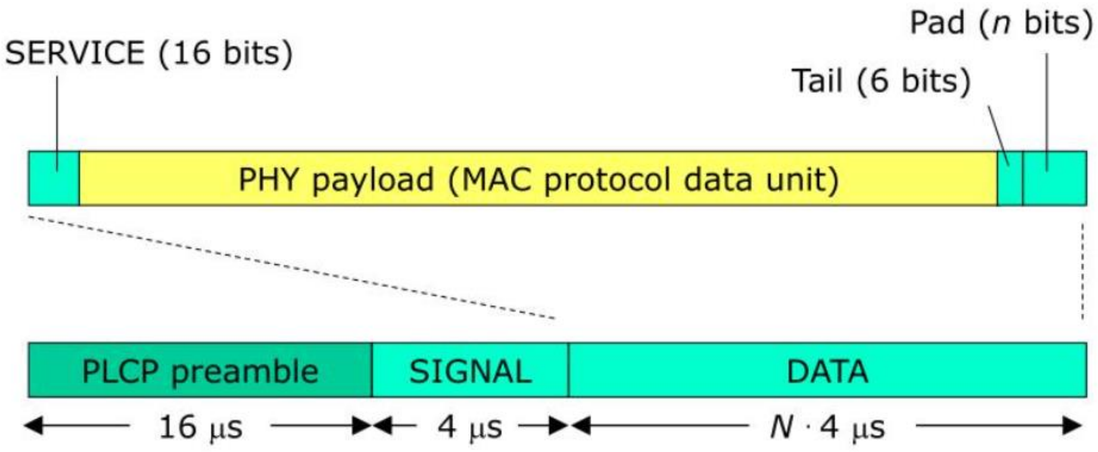
Bit-rate	802.11 Standards	DSSS or OFDM	Modulation	Bits per Symbol	Coding Rate	Mega-Symbols per second
1	b	DSSS	BPSK	1	1/11	11
2	b	DSSS	QPSK	2	1/11	11
5.5	b	DSSS	CCK	1	4/8	11
11	b	DSSS	CCK	2	4/8	11
6	a/g	OFDM	BPSK	1	1/2	12
9	a/g	OFDM	BPSK	1	3/4	12
12	a/g	OFDM	QPSK	2	1/2	12
18	a/g	OFDM	QPSK	2	3/4	12
24	a/g	OFDM	QAM-16	4	1/2	12
36	a/g	OFDM	QAM-16	4	3/4	12
48	a/g	OFDM	QAM-64	6	2/3	12
54	a/g	OFDM	QAM-64	6	3/4	12

IEEE 802.11 Physical Layer

802.11g PHY frame structure

- Preamble – 12 OFDM symbols, sync sequence of presence/absence of pulses in a series of slots
- Signal – consist of different info (PLCP header) like rate, length, parity
- Service - The service field contains control bits to help the receiver decode the frame





PLCP - Physical Layer Convergence Procedure sublayer
PMD - Physical Medium Dependent sublayer
PPDU - PLCP Protocol Data Unit
PSDU - PLCP Service Data Unit
MPDU - MAC Protocol Data Unit
MSDU - MAC Service Data Unit

IEEE 802.11 Physical Layer

IEEE 802.11 family

- **2009** – IEEE 802.11n (Wi-Fi 4) - 802.11n is an amendment that improves upon the previous 802.11 standards; its first draft of certification was published in 2006. Supports MIMO antennas. Operates on both 2.4 and 5 GHz @ 54 Mbps to 600 Mbps rates
- **2013** – IEEE 802.11ac (Wi-Fi 5) - Changes compared to 802.11n include wider channels (80 or 160 MHz versus 40 MHz), operates in the 5 GHz band, more spatial streams (up to 8 versus 4), higher-order modulation (up to 256-QAM). Wave 2 is the 2nd phase of the certification to provide higher bandwidth

IEEE Standard	Year Adopted	Frequency	Max. Data Rate
802.11a	1999	5 GHz	54 Mbps
802.11b	1999	2.4 GHz	11 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n	2009	2.4/5 GHz	600 Mbps
802.11ac	2014	5 GHz	1 Gbps
802.11ac Wave 2	2015	5 GHz	3.47 Gbps
802.11ad	2016	60 GHz	7 Gbps
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)
802.11ah	2016	2.4/5 GHz	347 Mbps
802.11ax	2019	2.4/5 GHz	10 Gbps

- **2021** – IEEE 802.11ax - the successor to 802.11ac. It's marketed as Wi-Fi 6 (2.4 GHz and 5 GHz) and Wi-Fi 6E (6 GHz). For an individual client, the maximum improvement in data rate against the predecessor (802.11ac) is only 39%, the goal was to provide 4 times the throughput-per-area. The motivation behind this goal was the deployment of WLAN in dense environments such as corporate offices and shopping malls. This is achieved by means of a technique called OFDMA, which is basically multiplexing in the frequency domain (as opposed to spatial multiplexing - OFDM – used by 802.11ac)

IEEE 802.11 Physical Layer

MCS Index

- **Modulation Code Schemes** is a metric-based index based on several parameters of a WiFi connection between the station and AP
- It depends on:
  - the modulation – the phase and amplitude modulation for bit coding
  - coding rate – how many bits transfer information and how many are used for guard / error correction
  - number of spatial streams – the number pf independent data streams used
  - channel width 20MHz, 40MHZ, 80 MHZ
  - and other parameters as well

Number of Data Subcarriers per Resource Unit ($N_{SD,U}$); *Number of Coded Bits per Subcarrier per Stream for the Resource Unit* ($N_{BPSCS,U}$); *Coding* (R); *Number of Spatial Streams* (N_{SS})

$$\text{Data Rate} = \frac{N_{SD,U} * N_{BPSCS,U} * R * N_{SS}}{T_{DFT} + T_{GI}}$$

OFDM Symbol Duration (T_{DFT}); *Guard Interval Duration* (T_{GI})

IEEE 802.11 Physical Layer

Example: MCS Index for 802.11n and 802.11ac

HT MCS	VHT MCS	Modulation	Coding	20MHz Data Rate 800ns	20MHz Data Rate 400ns	20MHz Min. SNR	20MHz RSSI	40MHz Data Rate 800ns	40MHz Data Rate 400ns	40MHz Min. SNR	40MHz RSSI	80MHz Data Rate 800ns	80MHz Data Rate 400ns	80MHz Min. SNR	80MHz RSSI	160MHz Data Rate 800ns	160MHz Data Rate 400ns	160MHz Min. SNR	160MHz RSSI
1 Spatial Stream																			
0	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	1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76	58.5	65	11	-73	117	130	14	-70
2	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	3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71	117	130	17	-68	234	260	20	-65
4	4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67	175.5	195	21	-64	351	390	24	-61
5	5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63	234	260	24	-60	468	520	27	-57
6	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	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																			
8	0	BPSK	1/2	13	14.4	2	-82	27	30	5	-79	58.5	65	8	-76	117	130	11	-73
9	1	QPSK	1/2	26	28.9	5	-79	54	60	8	-76	117	130	11	-73	234	260	14	-70
10	2	QPSK	3/4	39	43.3	9	-77	81	90	12	-74	175.5	195	15	-71	351	390	18	-68
11	3	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71	234	260	17	-68	468	520	20	-65
12	4	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67	351	390	21	-64	702	780	24	-61
13	5	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63	468	520	24	-60	936	1040	27	-57
14	6	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62	526.5	585	26	-59	1053	1170	29	-56
15	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	40	-48
3 Spatial Streams																			
16	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
17	1	QPSK	1/2	39	43.3	5	-79	81	90	8	-76	175.5	195	11	-73	351	390	14	-70
18	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
19	3	16-QAM	1/2	78	86.7	11	-74	162	180	14	-71	351	390	17	-68	702	780	20	-65
20	4	16-QAM	3/4	117	130	15	-70	243	270	18	-67	526.5	585	21	-64	1053	1170	24	-61
21	5	64-QAM	2/3	156	173.3	18	-66	324	360	21	-63	702	780	24	-60	1404	1560	27	-57
22	6	64-QAM	3/4	175.5	195	20	-65	364.5	405	23	-62			26	-59	1580	1755	29	-56
23	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

MCS Parameters

- High Throughput Modulation and Coding Scheme (HT-MCS) used by 802.11n
- Very High Throughput Modulation and Coding Scheme (VHT-MCS) used by 802.11ac
- Guard Interval - waiting time or pause between each packet transmission
- Minimum SNR and RSSI required for a specific MSC index
- Required SNR (Signal-to-Noise Ratio) [dB] SNR is defined as the ratio of signal power to the noise power (typical enterprise network background noise [dBm] will be about -120 to -90dBm; in high density WiFi network environment can be -80dBm)
- RSSI (Recieved Signal Strength Indicator) is the signal level reception
- SNR = RSSI – RF background noise

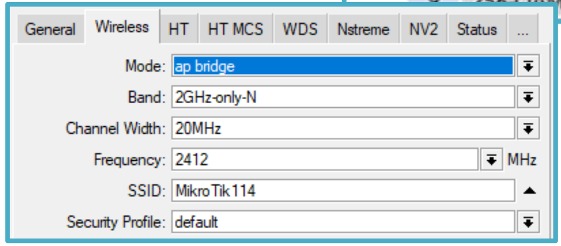
$$\mathrm{SNR_{dB}} = 10\log_{10}\left[\left(\frac{A_{\mathrm{signal}}}{A_{\mathrm{noise}}}\right)^2\right]$$

IEEE 802.11 Physical Layer

Example: Measured RSSI & SNR to MCS Index

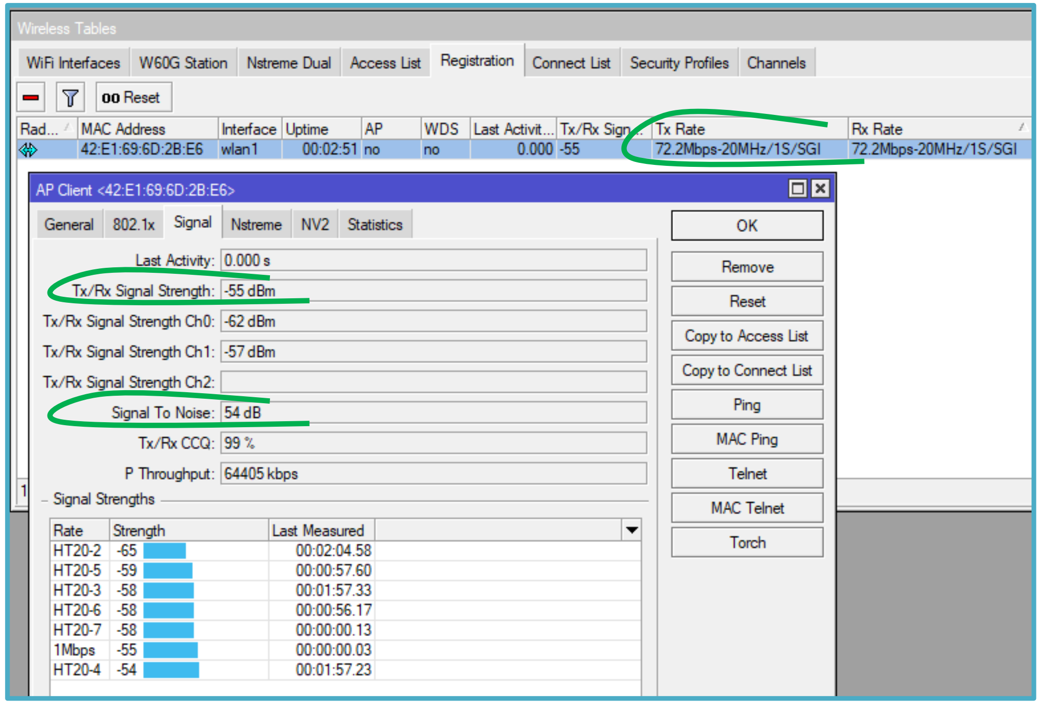
- 802.11n, 2412Mhz, 20Mhz, HT MCS
- Background noise [dBm] = RSSI [dBm] – SNR [dB]
  - -55 – 54 = -109 dBm
  - -86 – 29 = -115 dBm

HT MCS	VHT MCS	Modulation	Coding	20MHz Data Rate 800ns	20MHz Data Rate 400ns	20MHz Min. SNR	20MHz RSSI	40MHz Data Rate 800ns	40MHz Data Rate 400ns	40MHz Min. SNR	40MHz RSSI
1 Spatial Stream											
0	0	BPSK	1/2	6.5	7.2	2	-82	13.5	15	5	-79
1	1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76
2	2	QPSK	3/4	19.5	21.7	9	-77	40.5	45	12	-74
3	3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71
4	4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67
5	5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63
6	6	64-QAM	3/4	58.5	65	20	-65	121.5	135	23	-62
7	7	64-QAM	5/6	65	72.2	25	-64	135	150	28	-61
	8	256-QAM	3/4	78	86.7	29	-59	162	180	32	-56
	9	256-QAM	5/6			31	-57	180	200	34	-54

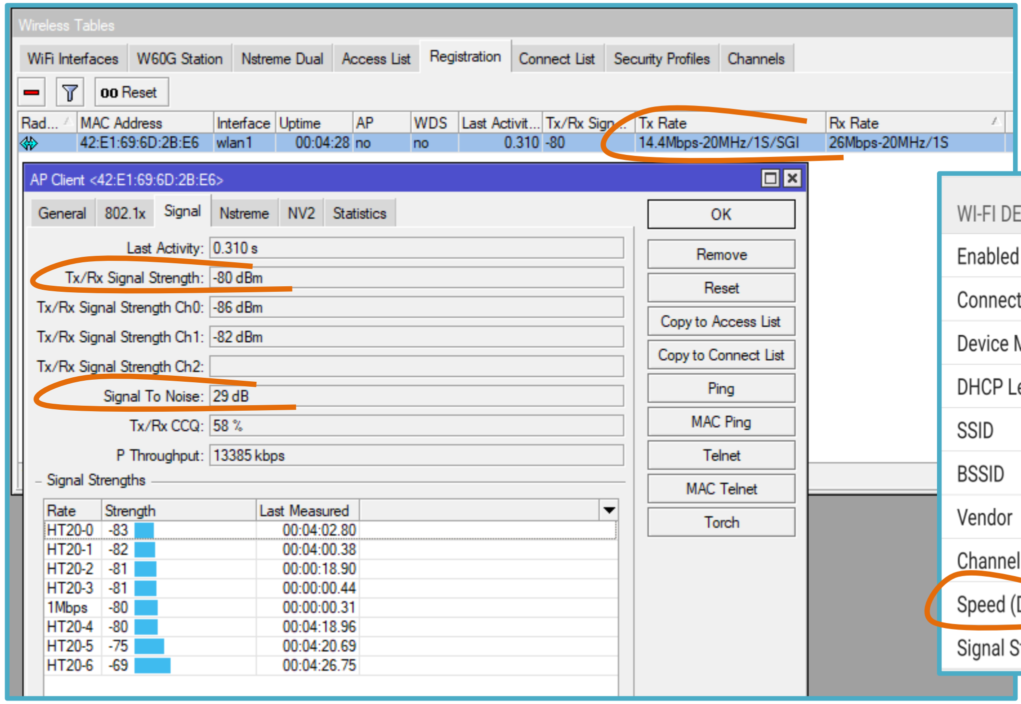


MCS provides info which rate for the current signal

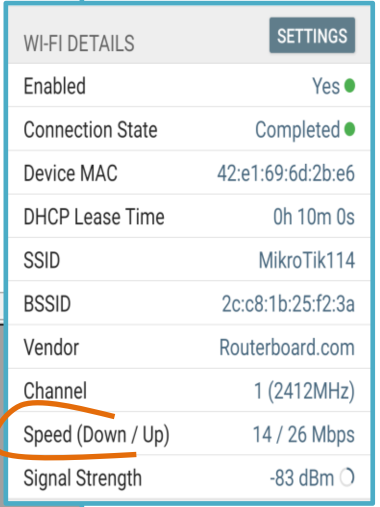
AP to mobile phone distance cca 2m, RSSI (Rx) -55dBm



AP to mobile phone distance cca 50m through walls , RSSI (Rx) -80dBm

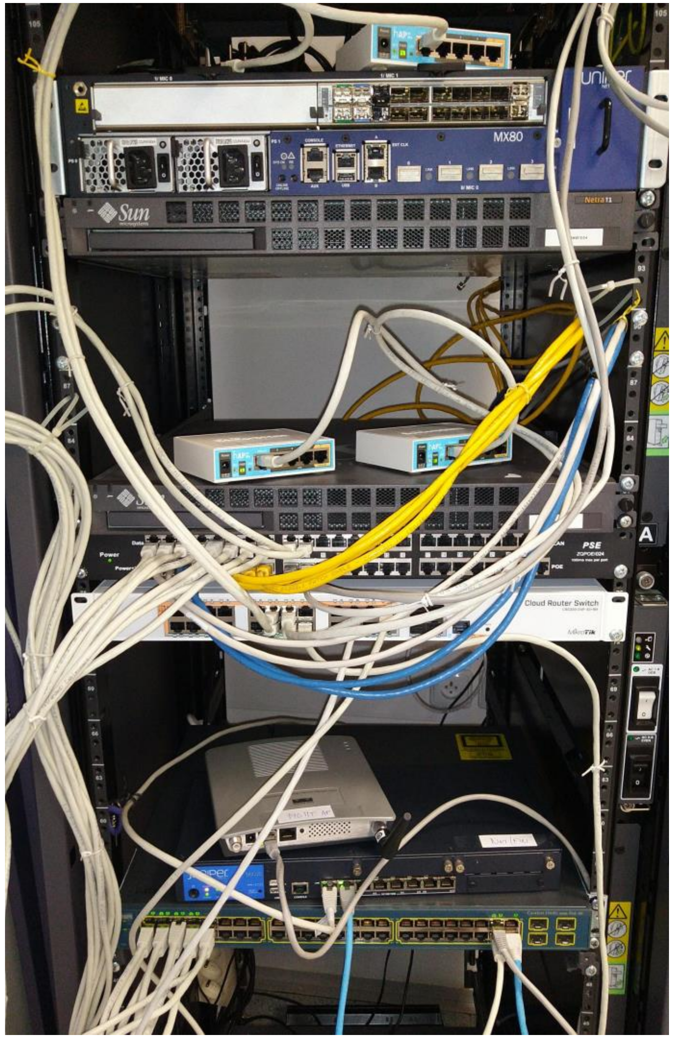


Mobile phone info

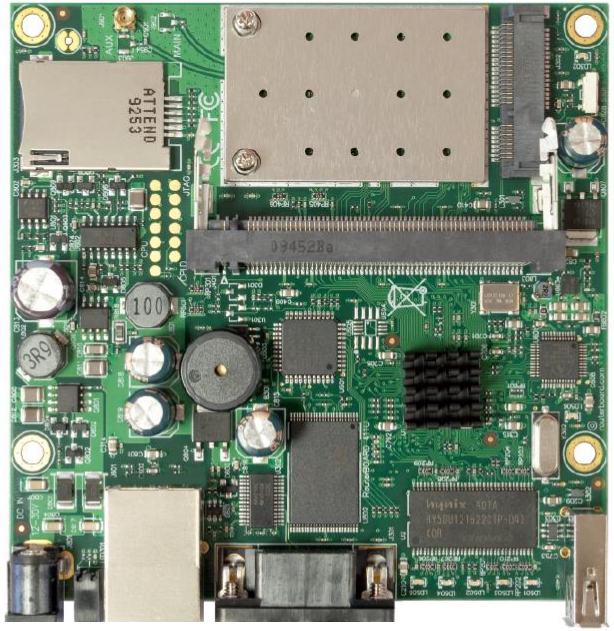


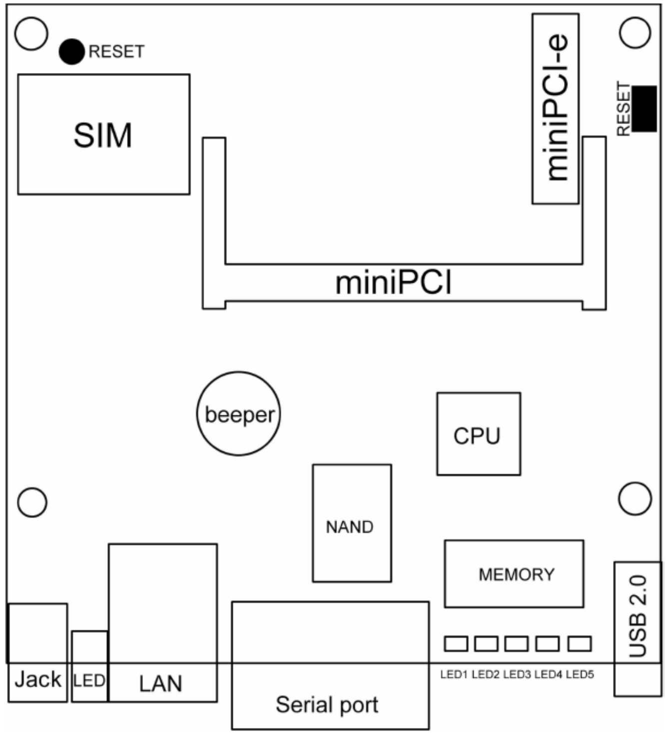
LAB Overview

LAB



Mikrotik AP





Details	
Product code	RB411UAHR
Architecture	MIPSBE
CPU	AR7161
CPU core count	1
CPU nominal frequency	680 MHz
Dimensions	105x105mm
RouterOS license	4
Size of RAM	64 MB
Storage size	64 MB
Storage type	NAND
Tested ambient temperature	-30C to 60C

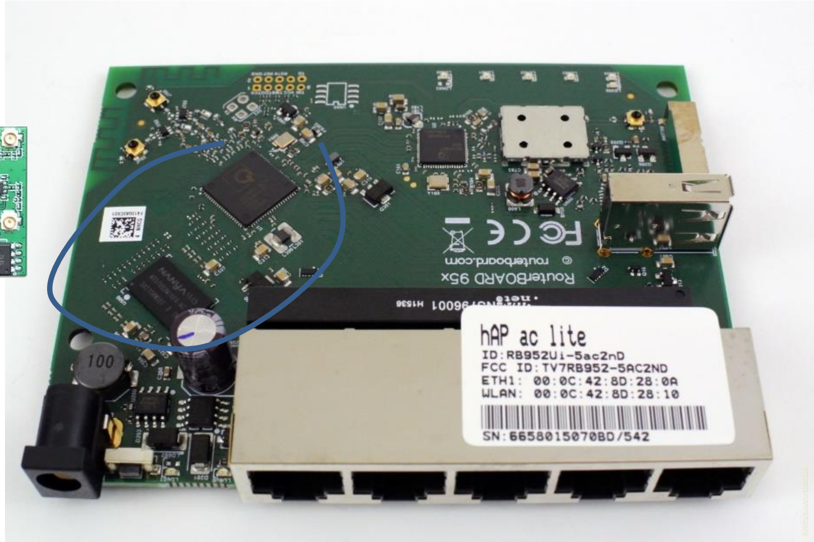
RouterBOARD 411UAHR

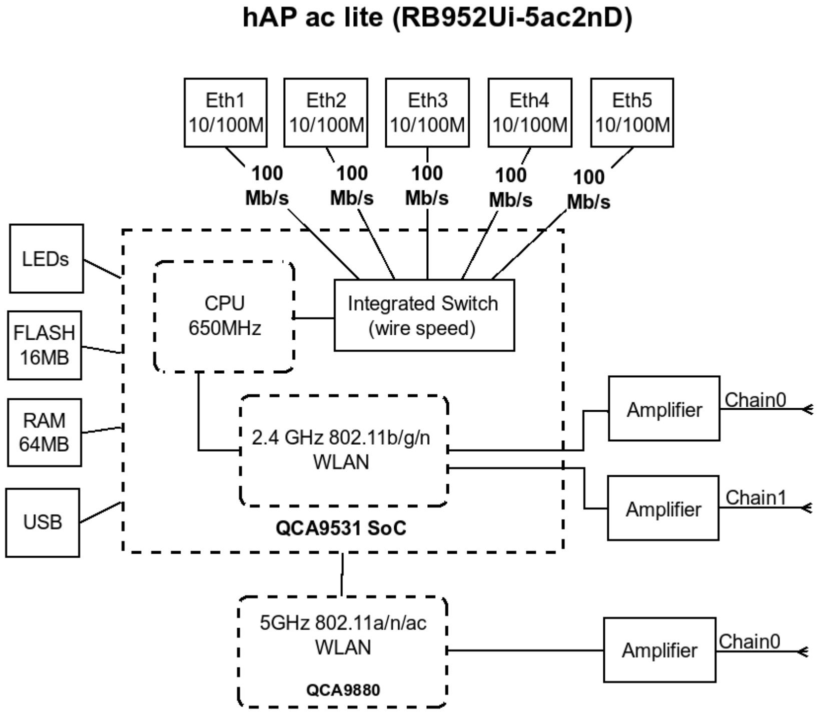
AR7161 is Atheros' first-generation high performance, cost effective and scalable wireless network processor

Mikrotik uses different types of HW (RISC) architectures: MIPS, ARM, SMIPS, TILE

Mikrotik AP

QCA9531
Qualcomm
Atheros



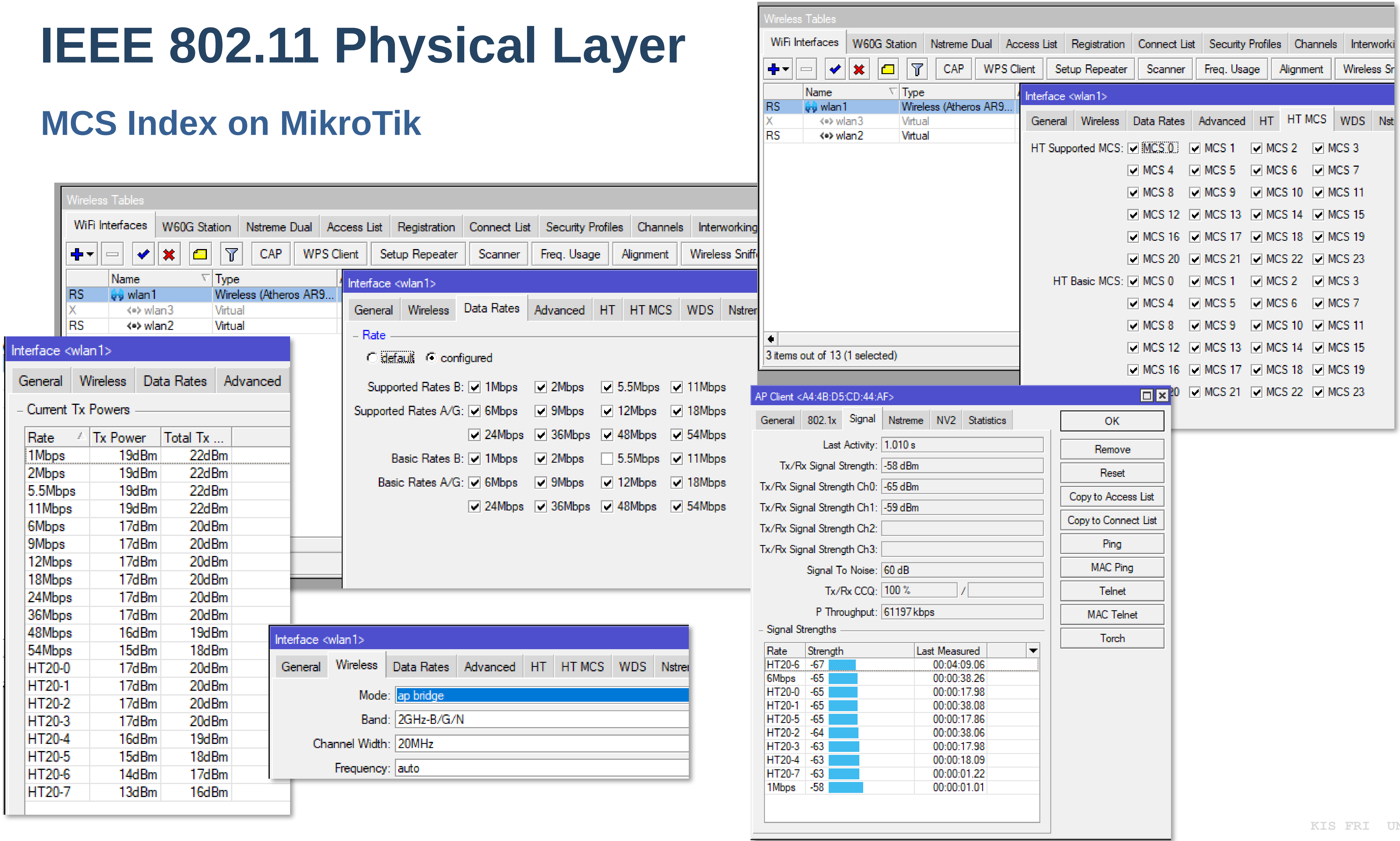


Mikrotik hAP ac lite
RouterBOARD RB952Ui-5ac2nD

650MHz MIPSBE CPU, 64MB RAM, five 10/100Mbps Ethernet ports (PoE output on port #5), dual-chain 802.11b/g/n 2.4GHz wireless, single chain 802.11a/n/ac 5GHz wireless, USB port for 3G/4G modem and a RouterOS L4 license

IEEE 802.11 Physical Layer

MCS Index on MikroTik



Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk

Vytvorené v rámci projektu KEGA 026TUKE-4/2021