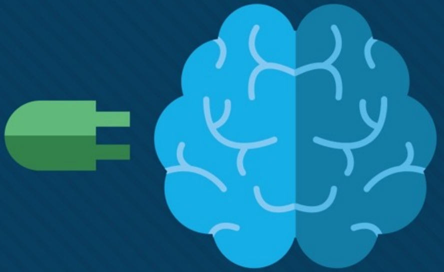


Module 12: WLAN Concepts

Switching, Routing and Wireless Essentials v7.0
(SRWE)

Module Objectives

Module Title: WLAN Concepts

Module Objective: Explain how WLANs enable network connectivity.

Topic Title	Topic Objective
Introduction to Wireless	Describe WLAN technology and standards.
Components of WLANs	Describe the components of a WLAN infrastructure.
WLAN Operation	Explain how wireless technology enables WLAN operation.
CAPWAP Operation	Explain how a WLC uses CAPWAP to manage multiple APs.
Channel Management	Describe channel management in a WLAN.
WLAN Threats	Describe threats to WLANs.
Secure WLANs	Describe WLAN security mechanisms.

12.1 Introduction to Wireless

Benefits of Wireless

- A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments.
- WLANs make mobility possible within the home and business environments.
- Wireless infrastructures adapt to rapidly changing needs and technologies.

Types of Wireless Networks

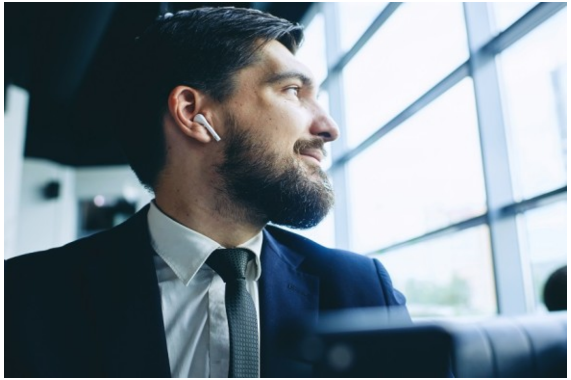
- **Wireless Personal-Area Network (WPAN)** – Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.
- **Wireless LAN (WLAN)** – Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.
- **Wireless MAN (WMAN)** – Large geographic area such as city or district. Uses specific licensed frequencies.
- **Wireless WAN (WWAN)** – Extensive geographic area for national or global communication. Uses specific licensed frequencies.

Wireless Technologies

Bluetooth – IEEE WPAN standard used for device pairing at up to 300ft (100m) distance.

- Bluetooth Low Energy (BLE) – Supports mesh topology to large scale network devices.
- Bluetooth Basic Rate/Enhanced Rate (BR/EDR) – Supports point-to-point topologies and is optimized for audio streaming.

WiMAX (Worldwide Interoperability for Microwave Access) – Alternative broadband wired internet connections. IEEE 802.16 WLAN standard for up 30 miles (50 km).



Wireless Technologies (Cont.)

Cellular Broadband – Carry both voice and data. Used by phones, automobiles, tablets, and laptops.

- Global System of Mobile (GSM) – Internationally recognized
- Code Division Multiple Access (CDMA) – Primarily used on the US.

Satellite Broadband – Uses directional satellite dish (talíř, miska) aligned with satellite in geostationary orbit. Needs clear line of site. Typically used in rural locations where cable and DSL are unavailable.

802.11 Standards

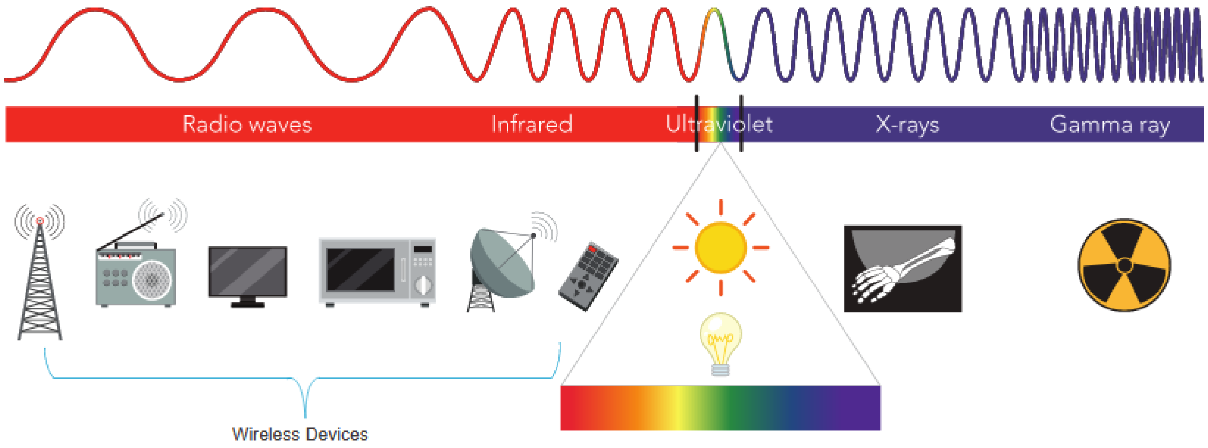
802.11 WLAN standards define how radio frequencies are used for wireless links.

IEEE Standard	Radio Frequency	Description
802.11	2.4 GHz	Data rates up to 2 Mb/s
802.11a	5 GHz	Data rates up to 54 Mb/s Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	Data rates up to 11 Mb/s Longer range than 802.11a and better able to penetrate building structures
802.11g	2.4 GHz	Data rates up to 54 Mb/s Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ac	5 GHz	Data rates 450 Mb/s – 1.3 Gb/s Supports up to eight antennas
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

Radio Frequencies

All wireless devices operate in the range of the electromagnetic spectrum. WLAN networks operate in the 2.4 and 5 GHz frequency bands.

- 2.4 GHz (UHF) – 802.11b/g/n/ax
- 5 GHz (SHF) – 802.11a/n/ac/ax



Wireless Standards Organizations

Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards:

- **International Telecommunication Union (ITU)** – Regulates the allocation of radio spectrum and satellite orbits.
- **Institute of Electrical and Electronics Engineers (IEEE)** – Specifies how a radio frequency is modulated to carry information. Maintains the standards for local and metropolitan area networks (MAN) with the IEEE 802 LAN/MAN family of standards.
- **Wi-Fi Alliance** – Promotes the growth and acceptance of WLANs. It is an association of vendors whose objective is to improve the interoperability of products that are based on the 802.11 standard

12.2 WLAN Components

Video – WLAN Components

This video will cover the following:

- Antennas
- Wireless Router
- Internet Port
- Wireless Access Point
- Autonomous and controller-based access points

Wireless NICs

To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.

If a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

Wireless Home Router

A home user typically interconnects wireless devices using a small, wireless router.

Wireless routers serve as the following:

- **Access point** – To provide wires access
- **Switch** – To interconnect wired devices
- **Router** - To provide a default gateway to other networks and the Internet

Wireless Access Point

Wireless clients use their wireless NIC to discover nearby access points (APs).

Clients then attempt to associate and authenticate with an AP.

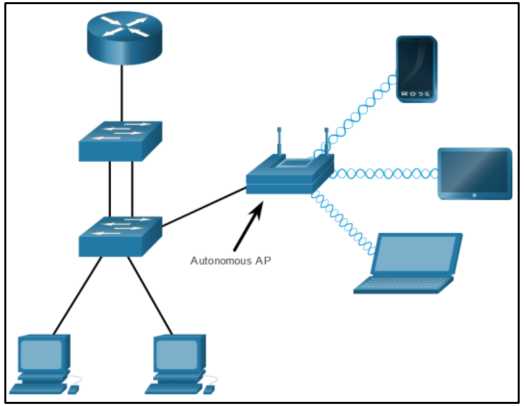
After being authenticated, wireless users have access to network resources.

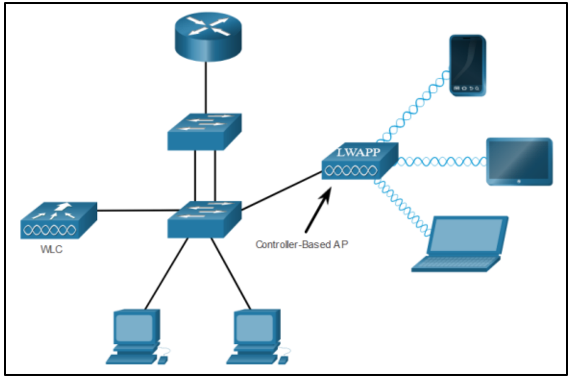
Cisco Meraki Go access points

AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

- **Autonomous APs** – Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.
- **Controller-based APs** – Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the WLC.





Wireless Antennas

Types of external antennas:

- **Omnidirectional** – Provide 360-degree coverage. Ideal in houses and office areas.
- **Directional** – Focus the radio signal in a specific direction. Examples are the Yagi and parabolic dish.
- **Multiple Input Multiple Output (MIMO)** – Uses multiple antennas (Up to eight) to increase bandwidth.

12.3 WLAN Operation

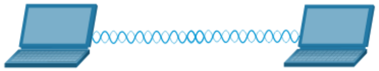
Video – WLAN Operation

This video will cover the following:

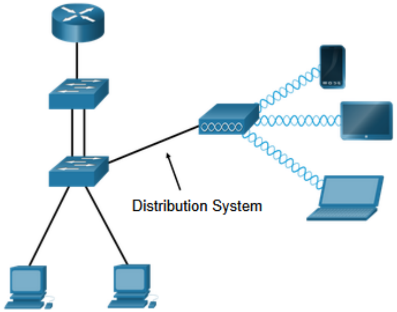
- Infrastructure Mode
- Ad hoc Mode
- Tethering
- Basic Service Set (BSS)
- Extended Service Set (ESS)
- 802.11 Frame Structure
- Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)
- Wireless Client AP Association
- Passive and Active Delivery Mode

802.11 Wireless Topology Modes

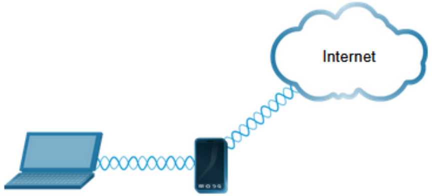
Ad hoc mode - Used to connect clients in peer-to-peer manner without an AP.



Infrastructure mode - Used to connect clients to the network using an AP.



Tethering - Variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.



BSS and ESS

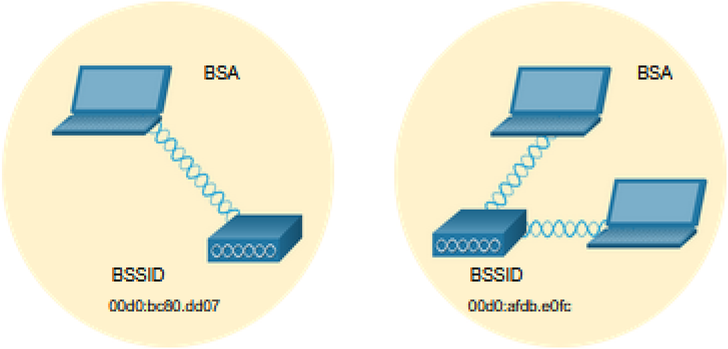
Infrastructure mode defines two topology blocks:

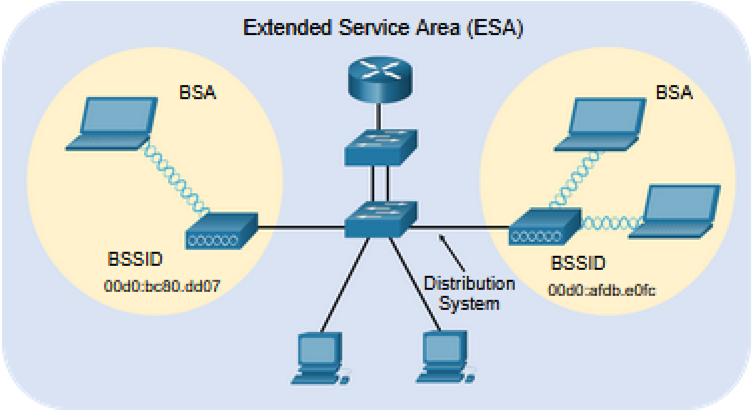
Basic Service Set (BSS)

- Uses single AP to interconnect all associated wireless clients.
- Clients in different BSSs cannot communicate.

Extended Service Set (ESS)

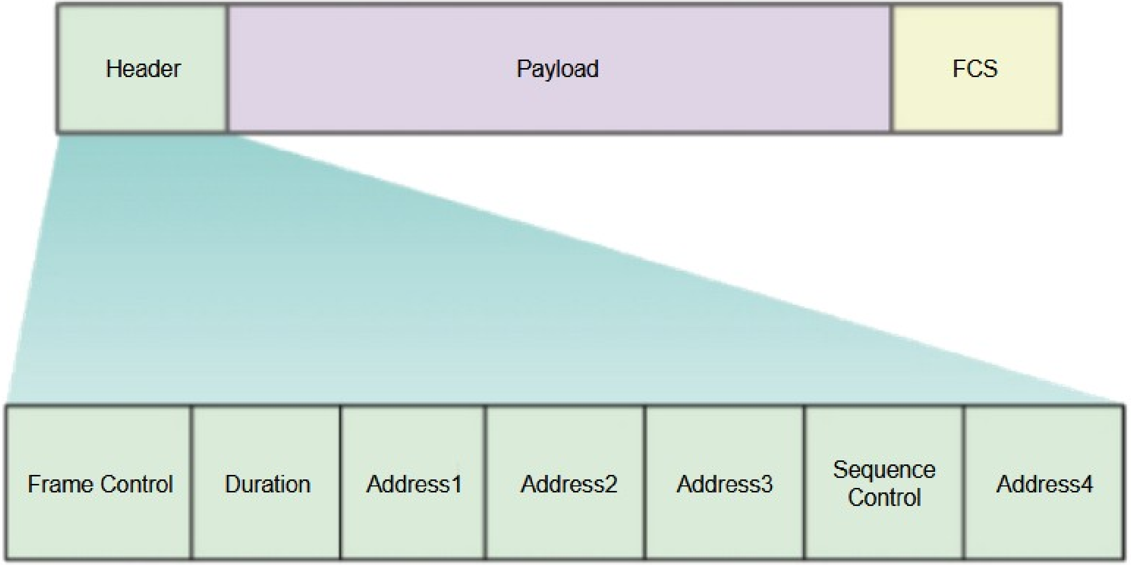
- A union of two or more BSSs interconnected by a wired distribution system.
- Clients in each BSS can communication through the ESS.



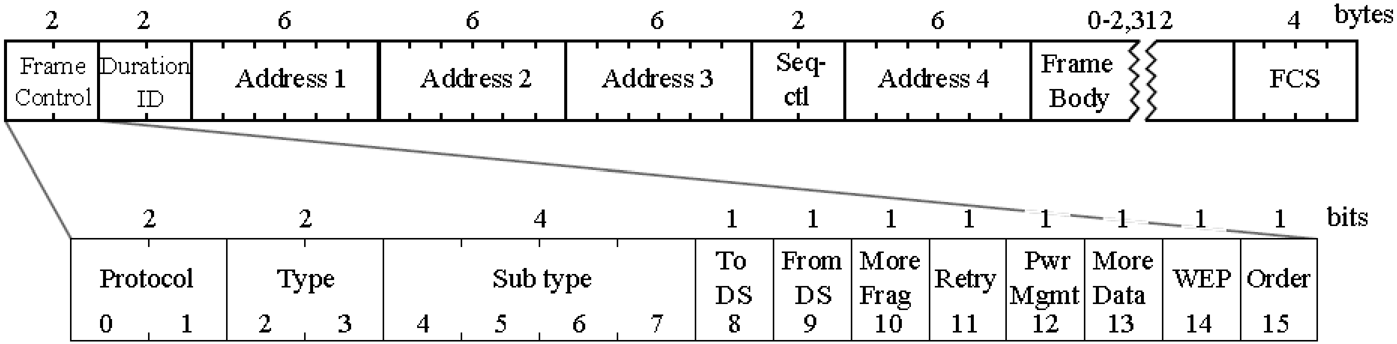


802.11 Frame Structure

The 802.11 frame format is similar to the Ethernet frame format, except that it contains more fields.



Řízení rámce 802.11

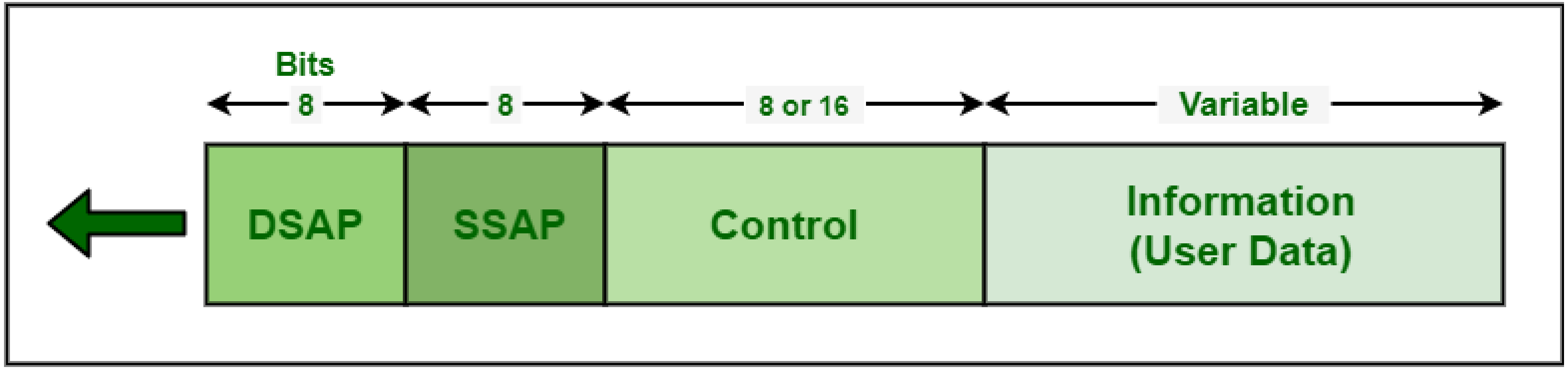


2	2	6	6	6	2	6	0-2,312	4	bytes
Frame Control	Duration ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame Body	FCS	

2	2	4	1	1	1	1	1	1	1	1	bits
Protocol	Type	Sub type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order	
0 1	2 3	4 5 6 7	8	9	10	11	12	13	14	15	

Logical Link Control (LLC)

Logical Link Control (LLC) je podvrstva, která obecně poskytuje logiku pro datové spojení, protože řídí synchronizaci, multiplexování, řízení toku a dokonce i funkce pro kontrolu chyb DLL (vrstva datového spojení). DLL je rozdělena na dvě podvrstvy, tj. Podvrstvu LLC a podvrstvu MAC (Medium Access Control).Základní model protokolů LLC je modelován podle HDLC (High-Level Data Link Control). Tyto protokoly jsou nepotvrzená služba bez připojení, služba orientovaná na připojení a potvrzená služba bez připojení. Všechny tyto protokoly používají stejný formát PDU (Protocol Data Unit):



PDU Format

Funkce vrstvy LLC

- Je zodpovědný za správu a zajištění integrity datových přenosů.
- Poskytují logiku pro datové spojení.
- Řídí také funkce synchronizace, multiplexování, kontroly chyb nebo oprav, řízení toku knihovny DLL.
- Umožňuje také vícebodovou komunikaci v celé řadě počítačových sítí.

Mechanismy vrstvy LLC

Toto pole identifikuje a určuje konkrétní PDU a také určuje různé řídicí funkce. Jedná se o 8 nebo 16bitové pole, obvykle v závislosti na identitě PDU. Používá se pro řízení toku a řešení chyb. V zásadě existují tři typy PDU. Každý PDU má jiný formát ovládacího pole.

- **Information (I)**

Obecně obsahuje 7bitové pořadové číslo (N (Send)) a také pořadové číslo (N (Received)). Slouží k přenosu dat nebo informací.

- **Supervisory (S)**

Obecně obsahuje pořadové číslo potvrzení (N (R)) a také 2bitové pole S pro tři různé formáty PDU, tj. RNR (Receive Not Ready), RR (Receive Ready) a REJ (Reject). Obvykle se používá pro řízení toku a chyb.

- **Unnumbered (U)**

Obvykle se jedná o 5bitový bit M, který se používá k označení typu PDU. Používá se pro různé protokoly PDU.

Problém near/far

- Protokol 802.11 MAC je svým konceptem podobný 802.3 v tom, že je navržen tak, aby podporoval více uživatelů na sdíleném médiu tím, že odesílatel před přístupem k médiu detekuje, zda nevysílá nějaká jiná stanice.
- U 802.3 ethernetové sítě LAN protokol protokolů vícenásobného přístupu s detekcí kolizí (CSMA/CD) reguluje, jak ethernetové stanice vytvářejí přístup k síti a jak detekují a zpracovávají kolize, ke kterým dochází, když se dvě nebo více zařízení pokouší současně komunikovat přes LAN . V síti WLAN 802.11 není detekce kolizí možná kvůli problému **near/far**.
- Problém near/far způsobuje účinek silného signálu ze zdroje blízkého signálu, který ztěžuje přijímači slabší signál z dalšího zdroje v důsledku rušení sousedního kanálu, rušení druhého kanálu, zkreslení (distorze), zachycení efekt, omezení dynamického rozsahu nebo podobně.

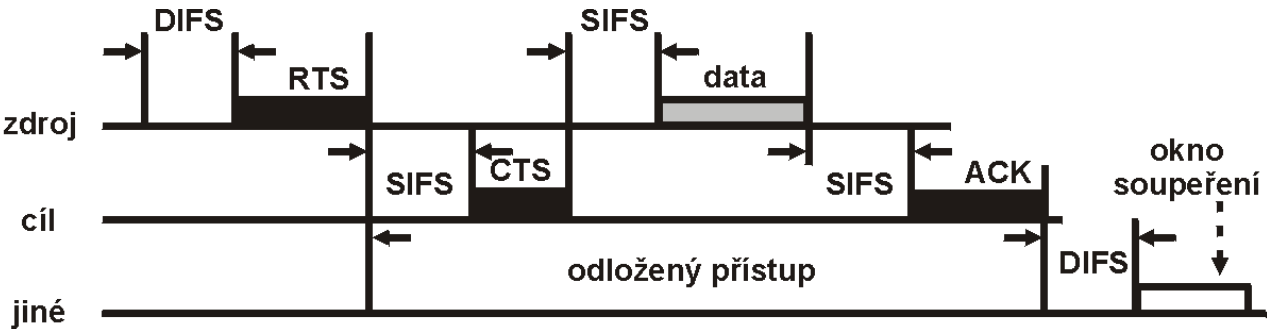
CSMA/CA

WLANs are half-duplex and a client cannot “hear” while it is sending, making it impossible to detect a collision.

WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) to determine how and when to send data. A wireless client does the following:

1. Listens to the channel to see if it is idle, i.e. no other traffic currently on the channel.
2. Sends a **ready to send** (RTS) message the AP to request dedicated access to the network.
3. Receives a **clear to send** (CTS) message from the AP granting access to send.
4. Waits a random amount of time before restarting the process if no CTS message received.
5. Transmits the data.
6. Acknowledges all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process

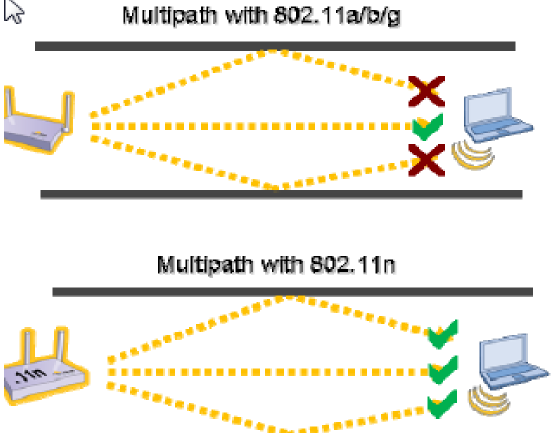
Přístupová metoda – DCF



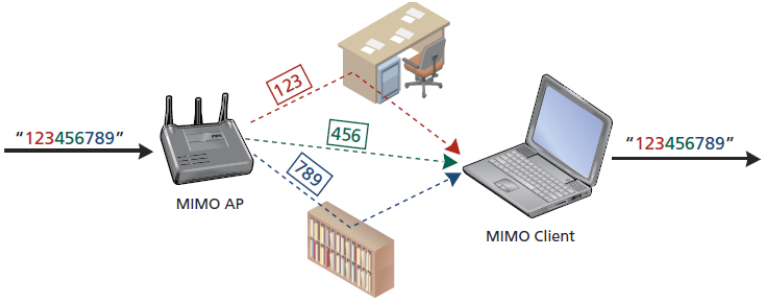
802.11n
MIMO (Multiple Input Multiple Output)

Klíčovými vlastnostmi standardu 802.11n jsou

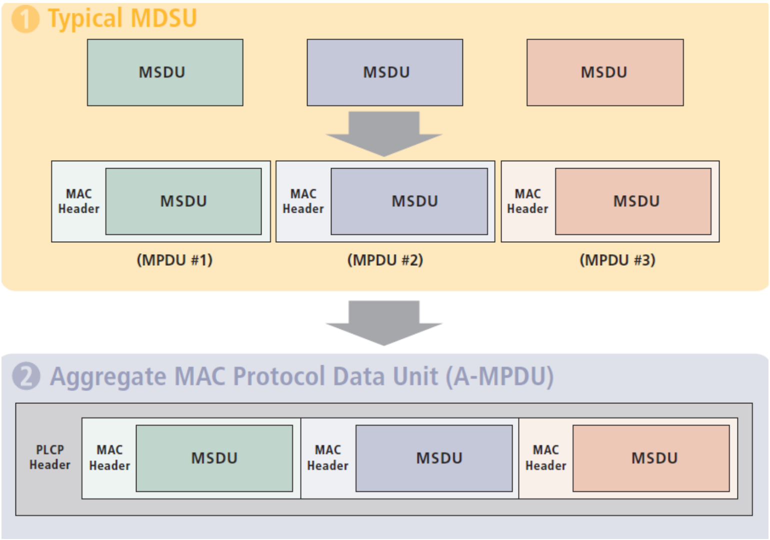
- MIMO technologie (Multiple-Input Multiple-Output)
- 40MHz kanál na fyzické vrstvě



ců na podvrstvě MAC

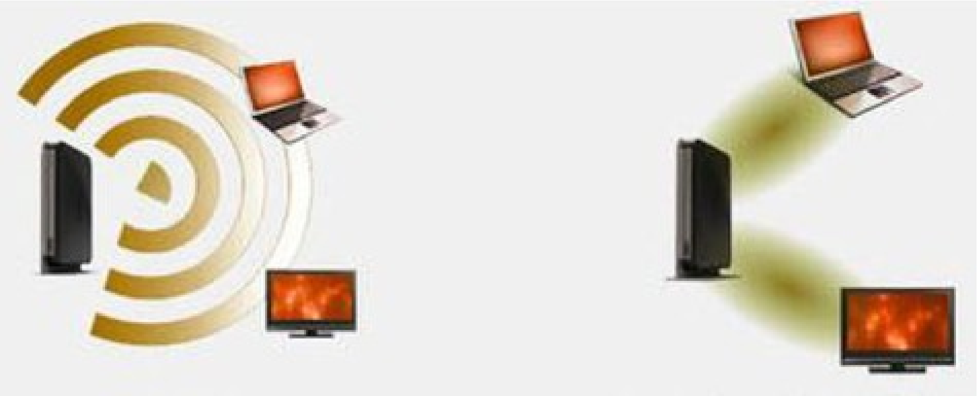


Agregace rámců

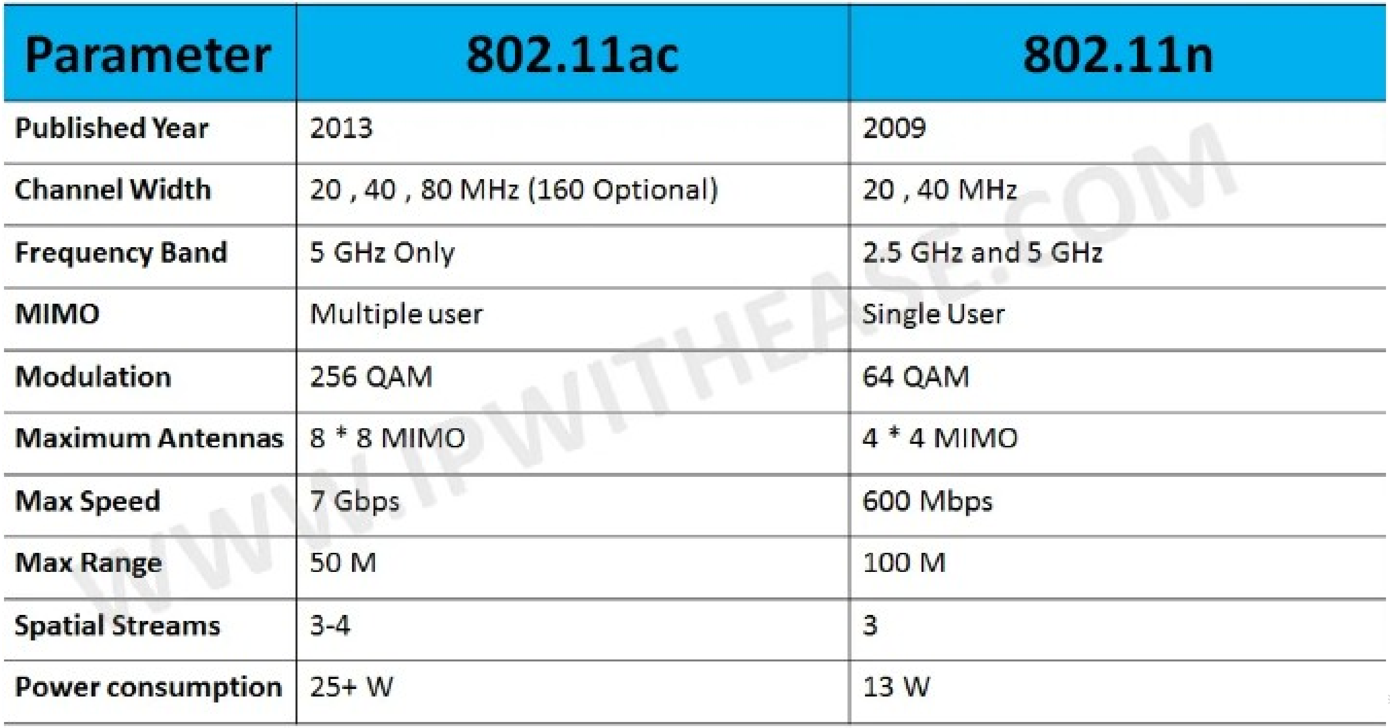


Problém: Reálná rychlost není 300 Mb/s, ale cca 130, proč?

IEEE 802.11ac (WiGig)
(návrat k pásmu 5 GHz)



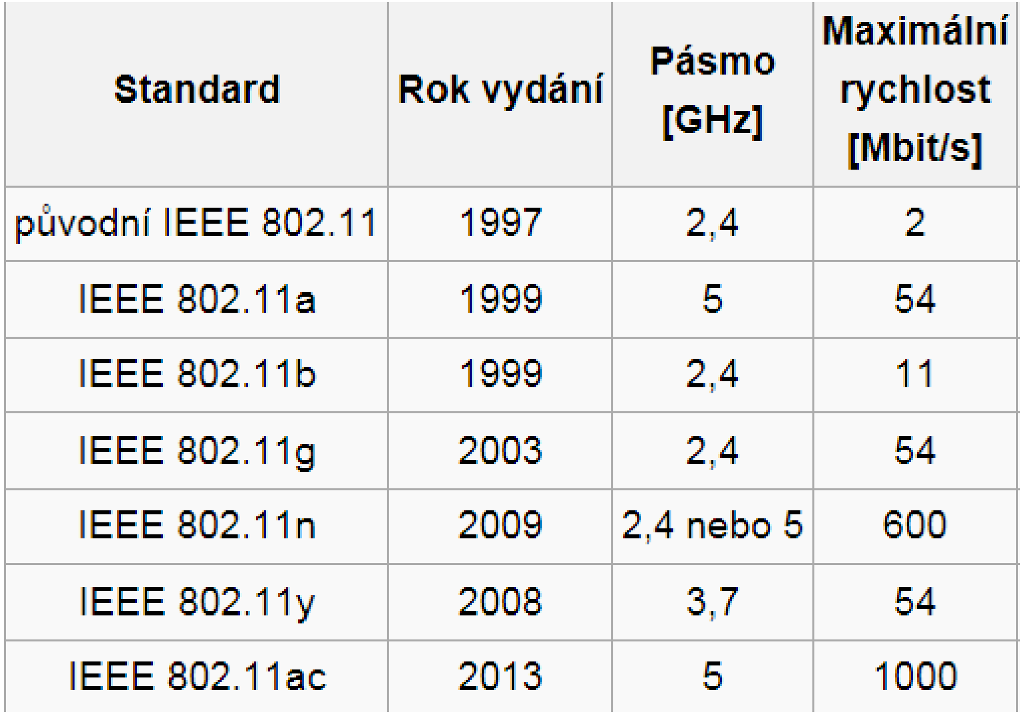
Porovnání 802.11n a 802.11ac



Parameter	802.11ac	802.11n
Published Year	2013	2009
Channel Width	20 , 40 , 80 MHz (160 Optional)	20 , 40 MHz
Frequency Band	5 GHz Only	2.5 GHz and 5 GHz
MIMO	Multiple user	Single User
Modulation	256 QAM	64 QAM
Maximum Antennas	8 * 8 MIMO	4 * 4 MIMO
Max Speed	7 Gbps	600 Mbps
Max Range	50 M	100 M
Spatial Streams	3-4	3
Power consumption	25+ W	13 W

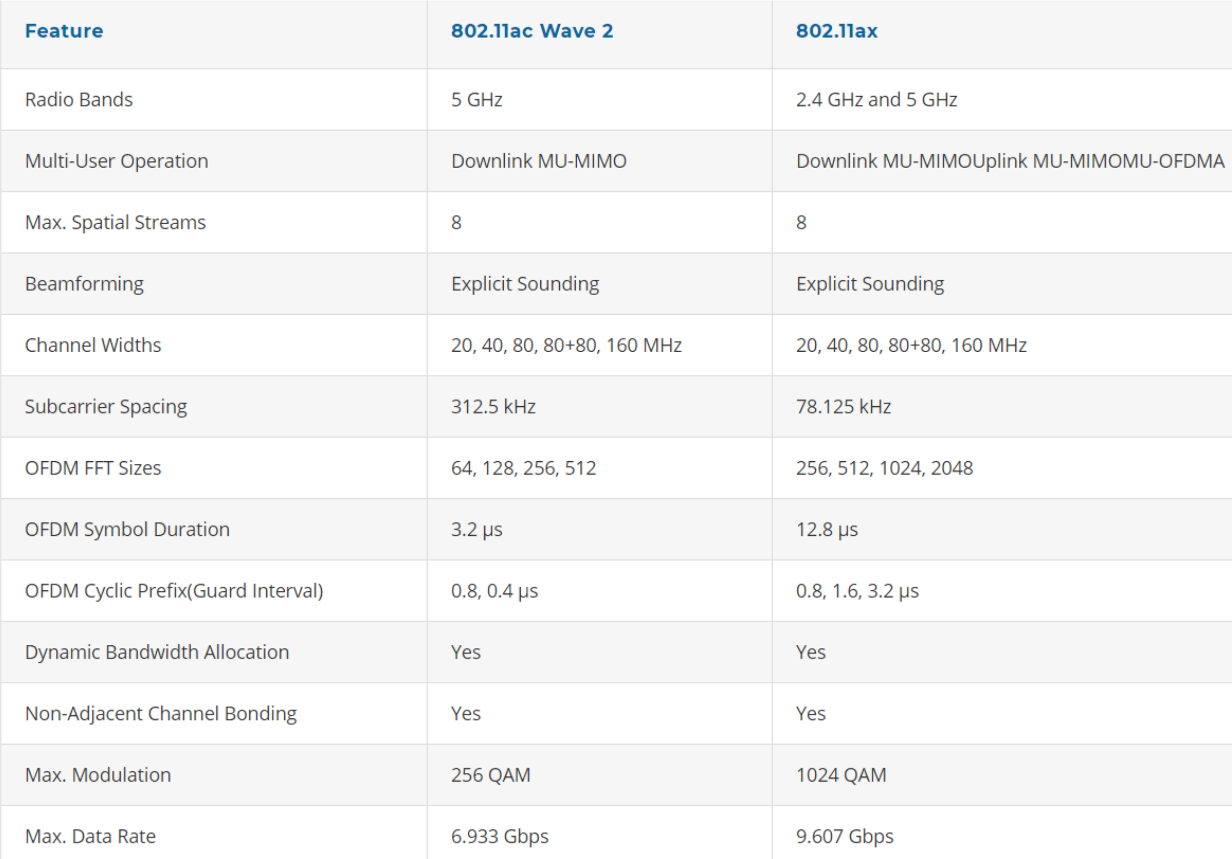
802.11ad: vyšší frekvence, ale menší dosah – co s tím?

Souhrn parametrů WiFi sítí



Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]
původní IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4 nebo 5	600
IEEE 802.11y	2008	3,7	54
IEEE 802.11ac	2013	5	1000
IEEE 802.11ad	**2014**	**2,4, 5, 60**	**7 000**

Nalezte 10 rozdílů



Feature	802.11ac Wave 2	802.11ax
Radio Bands	5 GHz	2.4 GHz and 5 GHz
Multi-User Operation	Downlink MU-MIMO	Downlink MU-MIMOUplink MU-MIMOMU-OFDMA
Max. Spatial Streams	8	8
Beamforming	Explicit Sounding	Explicit Sounding
Channel Widths	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
Subcarrier Spacing	312.5 kHz	78.125 kHz
OFDM FFT Sizes	64, 128, 256, 512	256, 512, 1024, 2048
OFDM Symbol Duration	3.2 µs	12.8 µs
OFDM Cyclic Prefix(Guard Interval)	0.8, 0.4 µs	0.8, 1.6, 3.2 µs
Dynamic Bandwidth Allocation	Yes	Yes
Non-Adjacent Channel Bonding	Yes	Yes
Max. Modulation	256 QAM	1024 QAM
Max. Data Rate	6.933 Gbps	9.607 Gbps

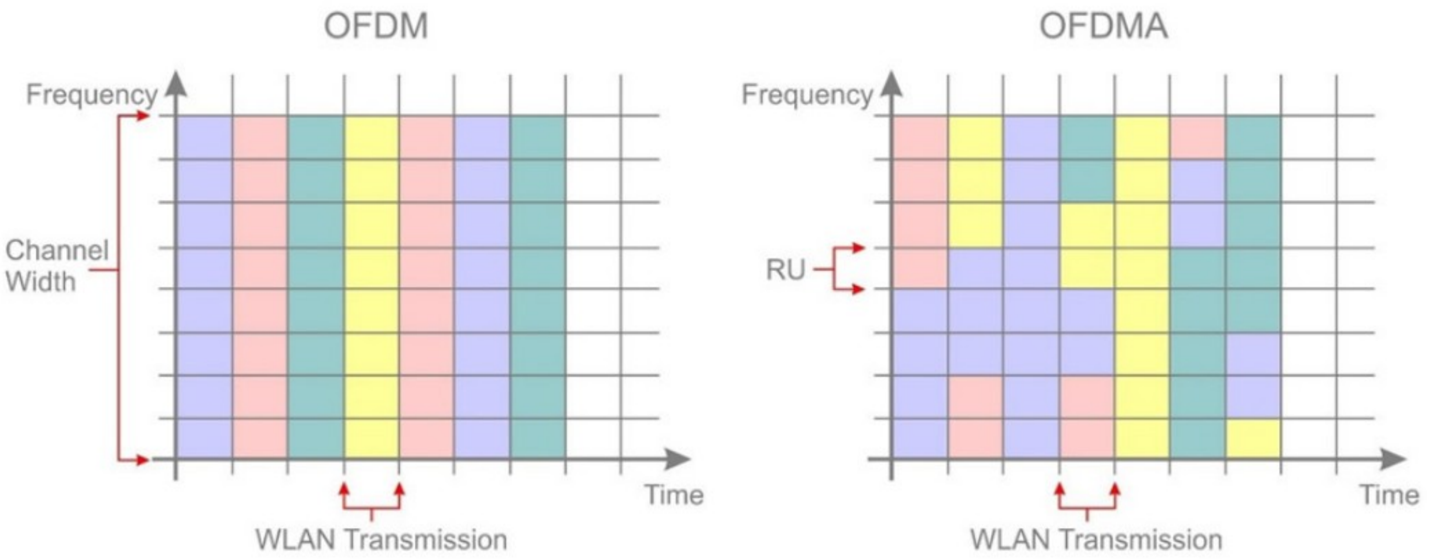
Wi-Fi 6 (dříve IEEE 802.11ax) v kostce

- Ortogonální frekvenční dělení s vícenásobným přístupem (OFDMA - Orthogonal frequency division multiple access).
- Víceuživatelský vícenásobný vstup vícenásobný výstup (MU-MIMO - Multi-user multiple input multiple output).
- Kanály 160 MHz
- Cílová doba probuzení (TWT - Target wake time).
- Režim kvadraturní amplitudové modulace 1024 (1024-QAM - 1024 quadrature amplitude modulation mode).
- beamforming.

OFDMA

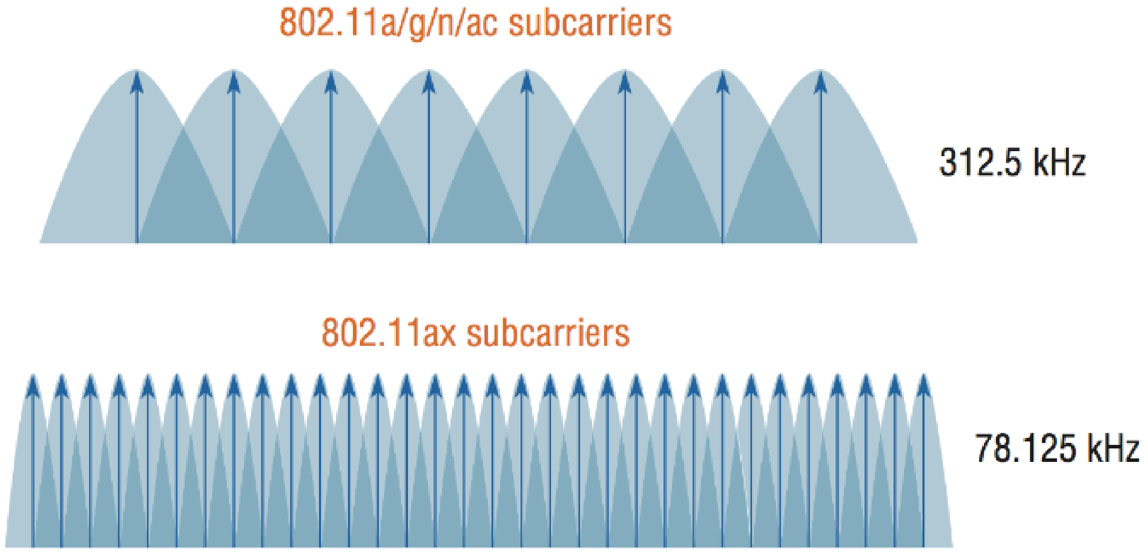
- Ortogonální frekvenční dělení s vícenásobným přístupem (OFDMA - Orthogonal frequency division multiple access): účinně sdílí kanály pro zvýšení účinnosti sítě a nižší latence pro downlink i uplink provoz v prostředí s vysokou poptávkou.

Rozdíl OFDM a OFDMA



OFDMA rozděluje kanály na menší „Resource Units“ (RU) předdefinovaného počtu subnosných a poté přiřazuje RU více klientským uživatelům.

Uzší subkanály
(nazývají se jako RU (Resouce Unit))



MU-MIMO

- Víceuživatelský vícenásobný vstup vícenásobný výstup (MU-MIMO – Multi-user multiple input multiple output): umožňuje přenos více downlinkových dat najednou a umožňuje přístupovému bodu přenášet data současně na větší počet zařízení současně

Kanály 160 MHz

- Kanály 160 MHz: zvětšuje šířku pásma a poskytuje vyšší výkon při nízké latenci.

TWT

- Cílová doba probuzení (TWT – Target wake time): výrazně zlepšuje výdrž baterie v zařízeních Wi-Fi, jako je např. internet věcí (IoT).

1024-QAM - 1024

- Režim kvadraturní amplitudové modulace 1024 (1024-QAM – 1024 – quadrature amplitude modulation mode): zvyšuje propustnost v zařízeních Wi-Fi kódováním více dat ve stejném množství spektra.

Beamforming

- Beamforming sleduje díky soustavě antén umístění bezdrátových zařízení v síti a směruje WiFi signál vždy přímo na tato zařízení. Neustále kontroluje a zohledňuje také pohyb mobilních zařízení, jako jsou mobilní telefony a tablety.
- Tato chytrá distribuce signálu cíleně zesiluje bezdrátový signál a poskytuje vysoce stabilní WiFi připojení i nejnáročnějším aplikacím, zajišťujícím např. přenos hlasu a videa ve vysokém rozlišení.

Beamforming podrobněji

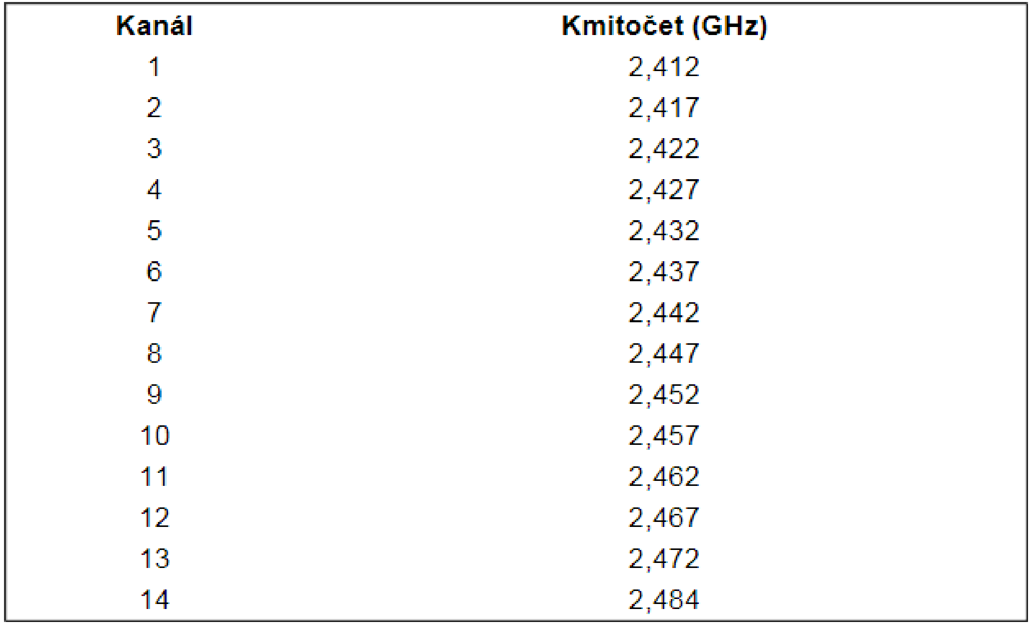
- Pokud je signál získán ze dvou směrů a v přesně stejné fázi, tak se sečtou a výsledkem je podstatně lepší příjem. Beamforming opozdí signál z druhé antény tak, že i po započtení jiné (delší) dráhy dorazí k přijímači ve stejný okamžik – tzn. jejich síla se sečte. Výsledkem je kvalitnější příjem.
- AP a klient se vzájemně kalibrují pro každý subcarrier (takže každý ze 108 subkanálů v rámci jednoho 40 MHz kanálu může mít odlišný výpočet a fázový posun).
- Beamforming ve středních vzdálenostech umožní udržet 256-QAM a 64-QAM, tedy zvýšit rychlost (a tím snížit čas obsazenosti kanálu a tím tedy celkovou kapacitu).

Airtime Fairness

- Airtime Fairness (volně přeloženo: spravedlivé přiřazování vysílacího času) s cílem vyvážit nároky jednotlivých zařízení na rychlost a přesnost.

- Kalibrované způsoby měření a algoritmy určují, jakým způsobem bude router přidělovat své vysílací kapacity a distribuovat vyčleněné Wi-Fi streamy každému zařízení, aby se plýtvalo silami v boji o šířku pásma.

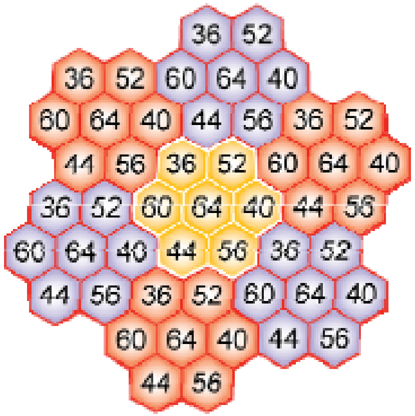
Kanály v rozmezí 2,412 - 2,484 GHz podle ČTÚ GL-12/R/2000



Kanál	Kmitočet (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

U WiFi používají USA: 11, Evropa: 13, Japonsko: 14 kanálů

Kanály by se neměly překrývat



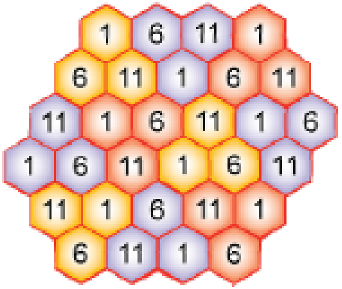
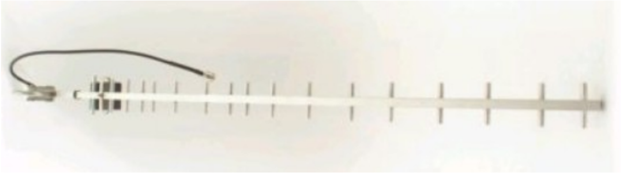


Schéma 7to1 (5 GHz, kanály 20 MHz) 3to1 (2,4 GHz, kanály 20 MHz)

Antény: směrová, sektorová, všesměrová a YAGI



Nejčastější příčiny rušení signálu

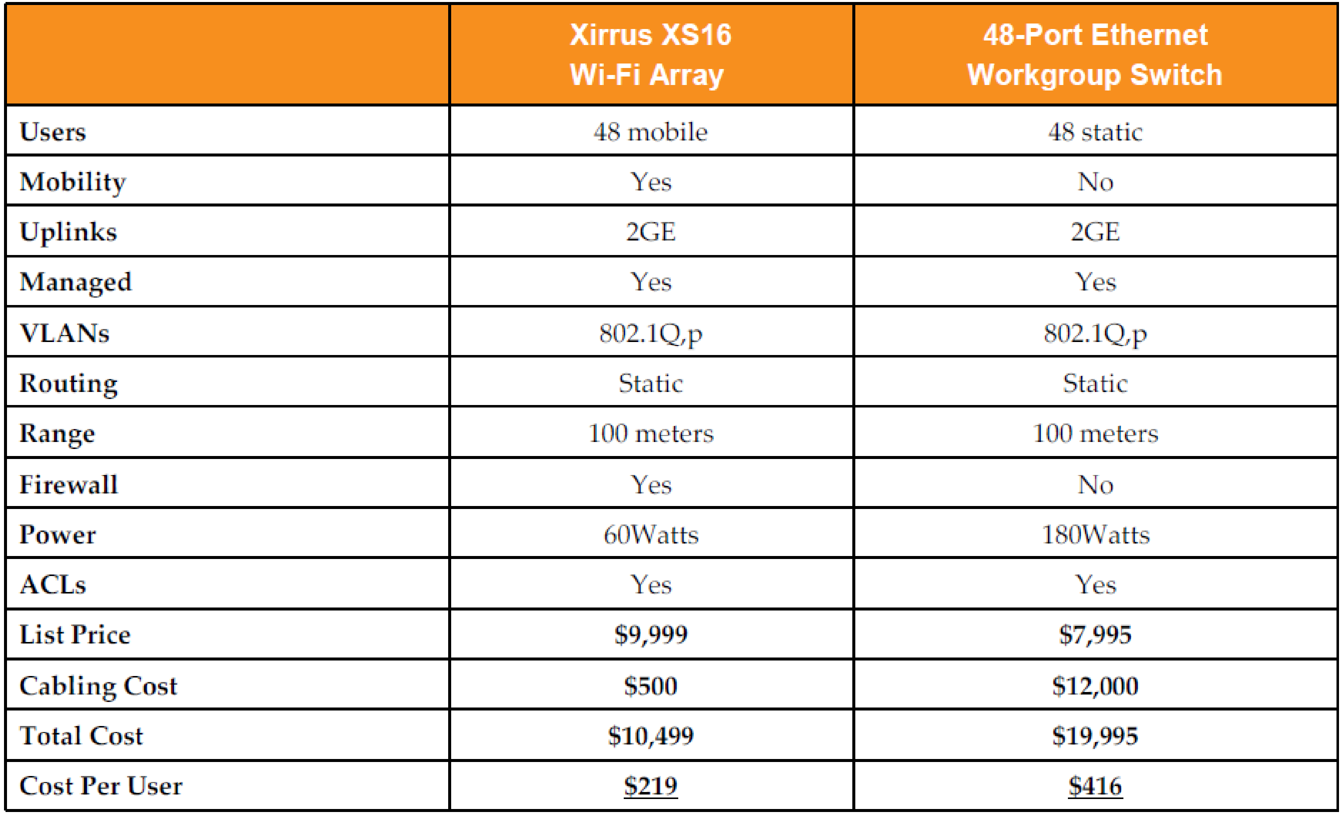
- betonové konstrukce a silné zdi
- ocelové výztuže a armatury v konstrukcích
- elektrické motory
- vysokonapěťové rozvody
- mikrovlnné trouby
- monitory
- zařízení pracující v pásmu 2,4 GHz

Co vše pracuje v pásmu 2,4 GHz?

Co vše pracuje v pásmu 2,4 GHz?
A proč?

Co vše pracuje v pásmu 2,4 GHz

Nákladová stránka: příklad



	Xirrus XS16 Wi-Fi Array	48-Port Ethernet Workgroup Switch
Users	48 mobile	48 static
Mobility	Yes	No
Uplinks	2GE	2GE
Managed	Yes	Yes
VLANs	802.1Q,p	802.1Q,p
Routing	Static	Static
Range	100 meters	100 meters
Firewall	Yes	No
Power	60Watts	180Watts
ACLs	Yes	Yes
List Price	**$9,999**	**$7,995**
Cabling Cost	**$500**	**$12,000**
Total Cost	**$10,499**	**$19,995**
Cost Per User	**$219**	**$416**

Bezpečnostní pravidla firemní WiFi sítě

- V Access Pointu (AP)zaveďte tabulku povolených MAC adres
- Zapněte WPA (Wi-Fi Protected Access), pokud už musíte mít WEP, (Wired Equivalent Privacy) tak se 128bitovým klíčem
- Pravidelně klíče měňte (např. 1x za měsíc)
- Nepovolujte DHCP a adresy přidělujte ručně
- Pokud je to možné, nastavte také tabulku povolených IP adres
- Zakažte SSID Broadcast (rozhlašování)
- Znemožněte fyzický přístup uživatelů k AP (aspoň ho dát ke stropu)
- Pravidelně kontroluje síť i logy z AP
- Omezte výkon tak, aby síť zbytečně nepřesahovala prostory vaší firmy
- Pokud chcete opravdu zajistit bezpečnost, používejte VPN (Virtuální privátní síť)

Wireshark Most Common 802.11 Filters v1.1

Filter Addresses

Addresses used for 802.11 communications

Up to 4 different MAC addresses can be used in an IEEE 802.11 frame:
- The transmitter MAC address or TA
- The receiver MAC address or RA
- The source MAC address or SA
- The destination MAC address or DA

Filters

Filter for a specific client by MAC address: Ex: wlan.addr == 00:11:22:33:44:55	**wlan.addr ==** *MAC_address*
Filter by the transmitter address (TA): Ex: wlan.ta == 00:11:22:33:44:55	**wlan.ta ==** *MAC_address*
Filter by the receiver address (RA): Ex: wlan.ra == 00:11:22:33:44:55	**wlan.ra ==** *MAC_address*
Filter by the source address (SA): Ex: wlan.sa == 00:11:22:33:44:55	**wlan.sa ==** *MAC_address*
Filter by the destination address (DA): Ex: wlan.da == 00:11:22:33:44:55	**wlan.da ==** *MAC_address*

Filter Wi-Fi Networks

BSSID vs SSID

BSSID is the MAC address of the radio transmitting in the AP
The BSSID is specific to 1 AP

SSID is the name of the global Wi-Fi network
The SSID can be used by multiple APs in a WLAN infrastructure

Filters

Filter by BSSID (by AP): Ex: wlan.bssid == 00:11:22:33:44:55	**wlan.bssid ==** *AP_radio_MAC_address*
Filter by SSID: Ex: wlan_mgt.ssid == "SemFio"	**wlan_mgt.ssid ==** *"your_SSID"*

Filter 802.11 Management Frames

Description

802.11 Management Frames are used by stations to join and leave a BSS
There is a total of 12 802.11 Management Frames:

- Association request (subtype 0x0)
- Association response (subtype 0x1)
- Reassociation request (subtype 0x2)
- Reassociation response (subtype 0x3)
- Probe request (subtype 0x4)
- Probe response (subtype 0x5)
- Beacon (subtype 0x8)
- ATIM (subtype 0x9)
- Disassociation (subtype 0xa)
- Authentication (subtype 0xb)
- Deauthentication (subtype 0xc)
- Action (subtype 0xd)

Filters

Filter for all management frames:	**wlan.fc.type == 0**
Filter for Association Requests:	**wlan.fc.type_subtype == 0**
Filter for Association Responses:	**wlan.fc.type_subtype == 1**
Filter for Reassociation Requests:	**wlan.fc.type_subtype == 2**
Filter for Resssociation Responses:	**wlan.fc.type_subtype == 3**
Filter for Probe Requests:	**wlan.fc.type_subtype == 4**
Filter for Probe Responses:	**wlan.fc.type_subtype == 5**
Filter for Beacons:	**wlan.fc.type_subtype == 8**
Filter for ATIMs:	**wlan.fc.type_subtype == 9**
Filter for Disassociations:	**wlan.fc.type_subtype == 10**
Filter for Authentications:	**wlan.fc.type_subtype == 11**
Filter for Deauthentications:	**wlan.fc.type_subtype == 12**
Filter for Actions:	**wlan.fc.type_subtype == 13**

Filter 802.11 Control Frames

Description

802.11 Control Frames assist with the delivery of data frames (type = 1)
There is a total of 8 802.11 Control Frames:

- Block ACK request (subtype 0x8)
- Block ACK (subtype 0x9)
- PS-Poll (subtype 0xa)
- Ready To Send (subtype 0xb)
- Clear To Send (subtype 0xc)
- ACK (subtype 0xd)
- CF-End (subtype 0xe)
- CF-End/CF-Ack (subtype 0xf)

Filters

Filter for all control frames:	**wlan.fc.type == 1**
Filter for Block ACK Requests:	**wlan.fc.type_subtype == 24**
Filter for Block ACKs:	**wlan.fc.type_subtype == 25**
Filter for PS-Polls:	**wlan.fc.type_subtype == 26**
Filter for Ready To Sends:	**wlan.fc.type_subtype == 27**
Filter for Clear To Sends:	**wlan.fc.type_subtype == 28**
Filter for ACKs:	**wlan.fc.type_subtype == 29**
Filter for CF-Ends:	**wlan.fc.type_subtype == 30**
Filter for CF-Ends/CF-Acks:	**wlan.fc.type_subtype == 31**

Filter 802.11 Data Frames

Description

802.11 Data Frames are mainly used to carry data (tupe = 2)
There is a total of 15 802.11 Data Frames:

- Data (subtype 0x0)
- Data+CF-Ack (subtype 0x1)
- Data+CF-Poll (subtype 0x2)
- Data+CF-Ack+CF-Poll (subtype 0x3)
- Null (subtype 0x4)
- CF-Ack (subtype 0x5)
- CF-Poll (subtype 0x6)
- CF-Ack+CF-Poll (subtype 0x7)
- QoS Data (subtype 0x8)
- QoS Data+CF-Ack (subtype 0x9)
- QoS Data+CF-Poll (subtype 0xa)
- QoS Data+CF-Ack+CF-Poll (0xb)
- QoS Null (subtype 0xc)
- QoS CF-Poll (subtype 0xe)
- QoS CF-Ack+CF-Poll (subt. 0xf)

Filters

Filter for all data frames:	**wlan.fc.type == 2**
Filter for Data:	**wlan.fc.type_subtype == 32**
Filter for Data+CF-Ack:	**wlan.fc.type_subtype == 33**
Filter for Data+CF-Poll:	**wlan.fc.type_subtype == 34**
Filter for Data+CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 35**
Filter for Null:	**wlan.fc.type_subtype == 36**
Filter for CF-Ack:	**wlan.fc.type_subtype == 37**
Filter for CF-Poll:	**wlan.fc.type_subtype == 38**
Filter for CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 39**
Filter for QoS Data:	**wlan.fc.type_subtype == 40**
Filter for QoS Data+CF-Ack:	**wlan.fc.type_subtype == 41**
Filter for QoS Data+CF-Poll:	**wlan.fc.type_subtype == 42**
Filter for QoS Data+CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 43**
Filter for QoS Null:	**wlan.fc.type_subtype == 44**
Filter for QoS CF-Poll:	**wlan.fc.type_subtype == 46**
Filter for QoS CF-Ack+CF-Poll:	**wlan.fc.type_subtype == 47**

RadioTap Header Information

Description

RadioTap Headers provide additional information (channel frequency, data rate, signal strength...) to any 802.11 frame when capturing frames.

Filters

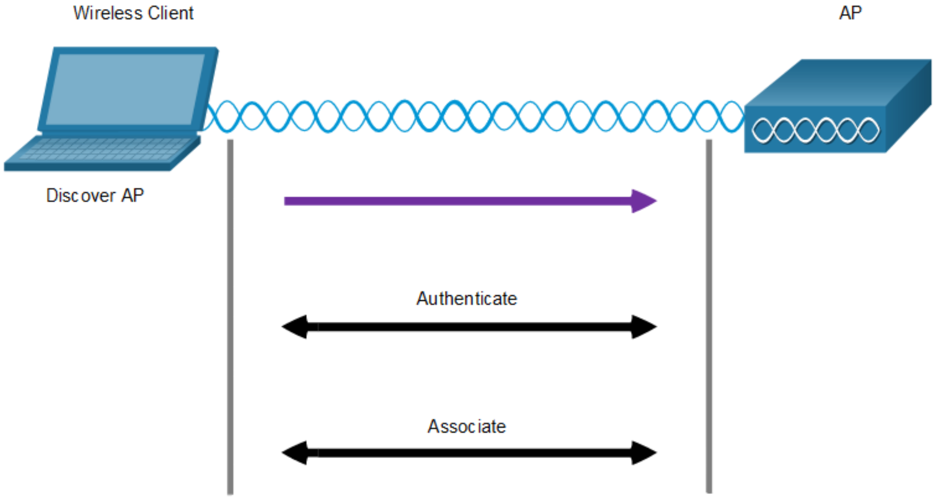
Filter a specific channel: Ex: radiotap.channel.freq == 5240	**radiotap.channel.freq ==** *frequency*
Filter a specific data rate: Ex: radiotap.datarate <= 6	**radiotap.datarate ==** *rate_in_Mbps*
Filter by signal strength (RSSI): Ex: radiotap.dbm_antsignal >= -60	**radiotap.dbm_antsignal ==** *rate_in_dBm*

Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

Wireless devices complete the following three stage process:

- Discover a wireless AP
- Authenticate with the AP
- Associate with the AP



Wireless Client and AP Association (Cont.)

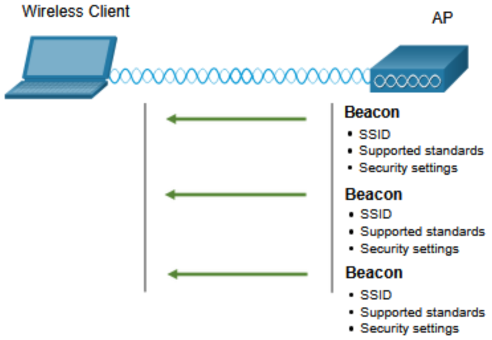
To achieve successful association, a wireless client and an AP must agree on specific parameters:

- **SSID** – The client needs to know the name of the network to connect.
- **Password** – This is required for the client to authenticate to the AP.
- **Network mode** – The 802.11 standard in use.
- **Security mode** – The security parameter settings, i.e. WEP, WPA, or WPA2.
- **Channel settings** – The frequency bands in use.

Passive and Active Discover Mode

Wireless clients connect to the AP using a passive or active scanning (probing) process.

- **Passive mode** – AP openly advertises its service by periodically sending broadcast beacon (maják) frames containing the SSID, supported standards, and security settings.
- **Active mode** – Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels.



Wireless Client

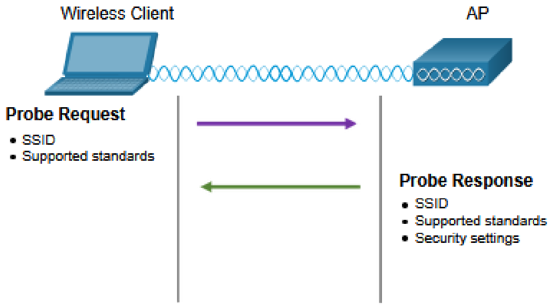
AP

Beacon
- SSID
- Supported standards
- Security settings

Beacon
- SSID
- Supported standards
- Security settings

Beacon
- SSID
- Supported standards
- Security settings

Passive mode



Wireless Client

AP

Probe Request
- SSID
- Supported standards

Probe Response
- SSID
- Supported standards
- Security settings

Active mode

12.4 CAPWAP Operation

Video – CAPWAP

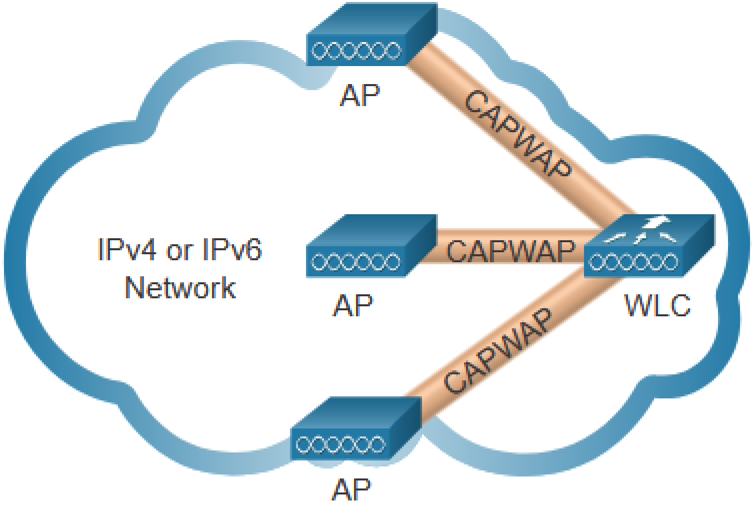
This video will cover the following:

- Control and Provisioning of Wireless Access Points (CAPWAP) function
- Split Media Access Control (MAC) Architecture
- DTLS Encryption
- Flex Connect Aps

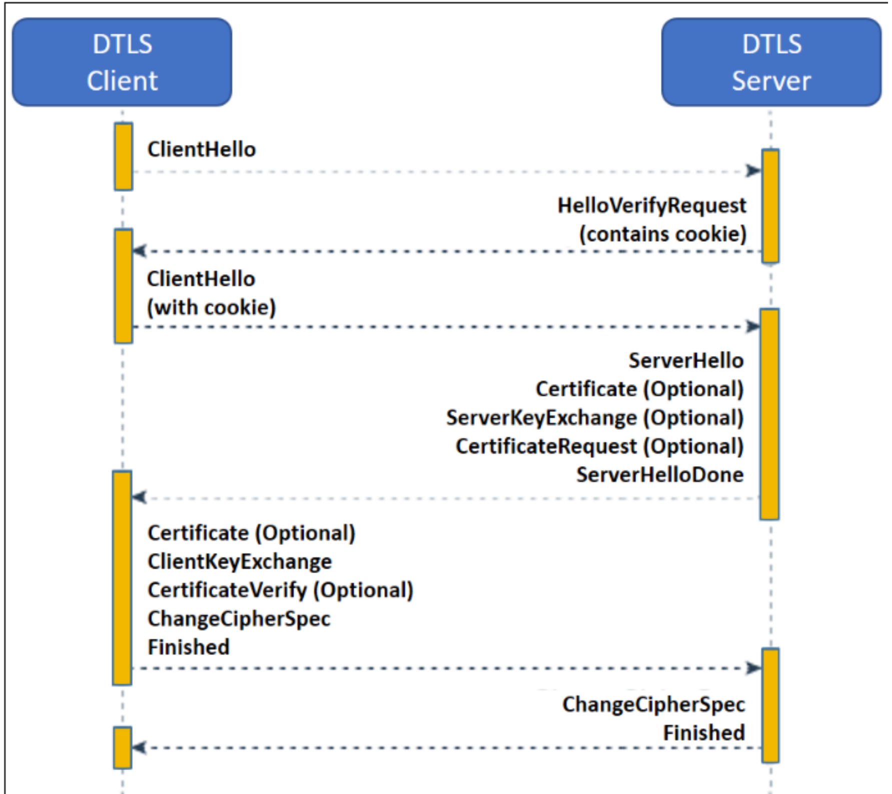
- **RFC 4564** defines the objectives for the CAPWAP protocol.
- **RFC 5418** covers the threat analysis for IEEE 802.11 deployments.
- **RFC 5415** defines the actual CAPWAP protocol specifications.

Introduction to CAPWAP

- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs.
- Based on LWAPP but adds additional security with Datagram Transport Layer Security (DLTS).
- Encapsulates and forwards WLAN client traffic between an AP and a WLC over tunnels using UDP ports 5246 and 5247.
- Operates over both IPv4 and IPv6. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.



Výměna zpráv DTLS



Split MAC Architecture

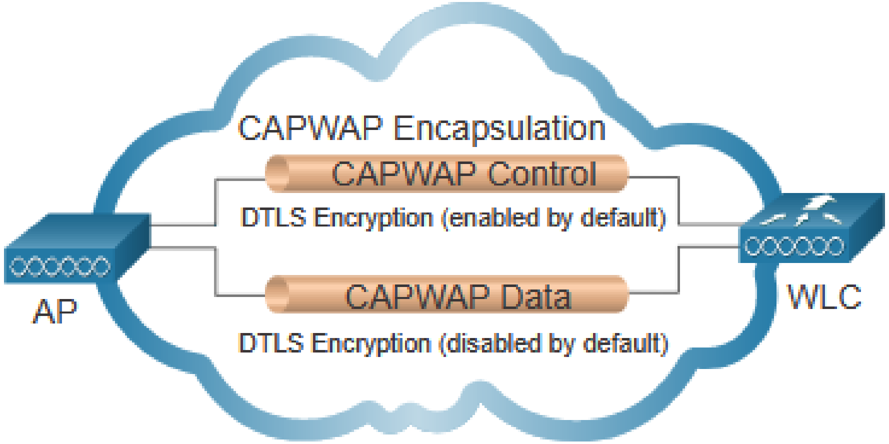
The CAPWAP split MAC concept does all the functions normally performed by individual APs and distributes them between two functional components:

- AP MAC Functions
- WLC MAC Functions

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgements and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

DTLS Encryption

- DTLS provides security between the AP and the WLC.
- It is enabled by default to secure the CAPWAP control channel and encrypt all management and control traffic between AP and WLC.
- Data encryption is disabled by default and requires a DTLS license to be installed on the WLC before it can be enabled on the AP.

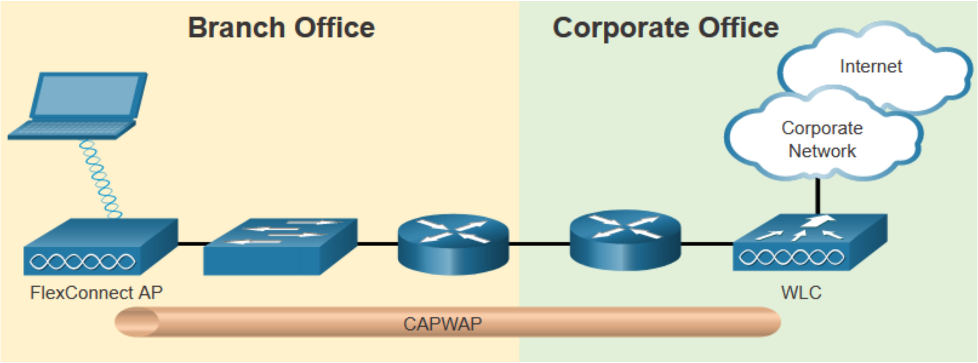

CAPWAP Encapsulation
CAPWAP Control
DTLS Encryption (enabled by default)
CAPWAP Data
DTLS Encryption (disabled by default)
AP
WLC

Flex Connect APs

FlexConnect enables the configuration and control of Aps over a WAN link.

There are two modes of option for the FlexConnect AP:

- **Connected mode** – The WLC is reachable. The FlexConnect AP has CAPWAP connectivity with the WLC through the CAPWAP tunnel. The WLC performs all CAPWAP functions.
- **Standalone mode** – The WLC is unreachable. The FlexConnect AP has lost CAPWAP connectivity with the WLC. The FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.



12.5 Channel Management

Frequency Channel Saturation

If the demand for a specific wireless channel is too high, the channel may become oversaturated, degrading the quality of the communication.

Channel saturation can be mitigated using techniques that use the channels more efficiently.

- **Direct-Sequence Spread Spectrum (DSSS)** - A modulation technique designed to spread a signal over a larger frequency band. Used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.
- **Frequency-Hopping Spread Spectrum (FHSS)** - Transmits radio signals by rapidly switching a carrier signal among many frequency channels. Sender and receiver must be synchronized to “know” which channel to jump to. Used by the original 802.11 standard.
- **Orthogonal Frequency-Division Multiplexing (OFDM)** - A subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. OFDM is used by a number of communication systems including 802.11a/g/n/ac.

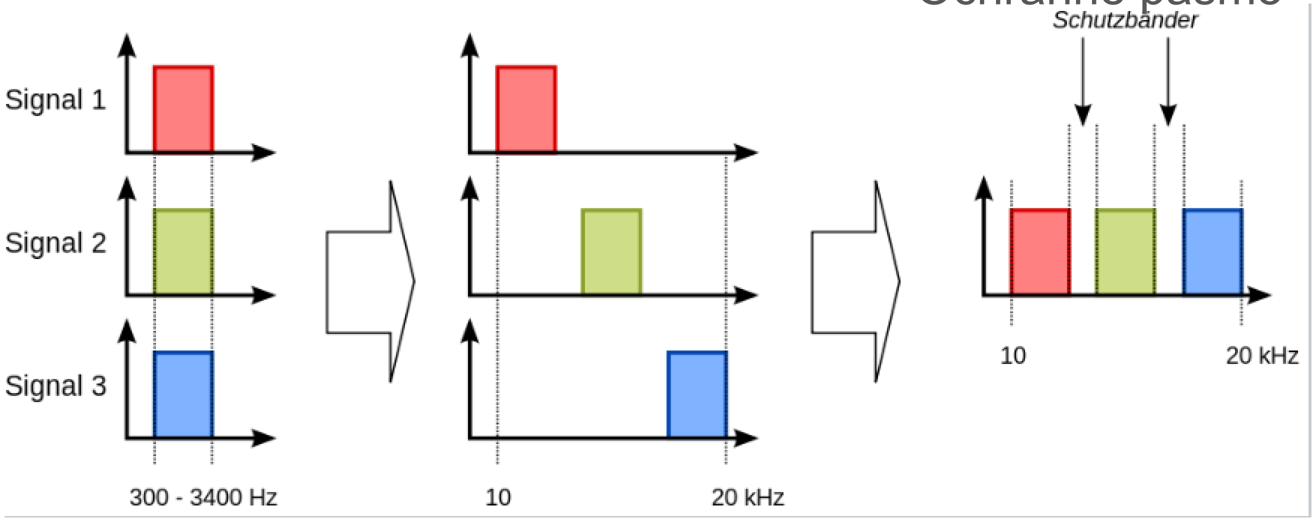
Začneme od Adama: Co je FDM (frequency-division multiplexing)

- Frekvenční multiplexování (FDM) je technika multiplexování, což znamená kombinování více než jednoho signálu na sdíleném médiu. Ve FDM jsou kombinovány signály různých frekvencí pro souběžný přenos.

- Kmitočtové spektrum každého vstupního signálu je posunuto do jiného kmitočtového pásma; přenáší se sloučené signály, které jsou na přijímací straně od sebe odděleny pomocí pásmových propustí a posunuty do původního kmitočtového pásma.

Mixování tří signálů V rámci FDM

Ochranné pásmo

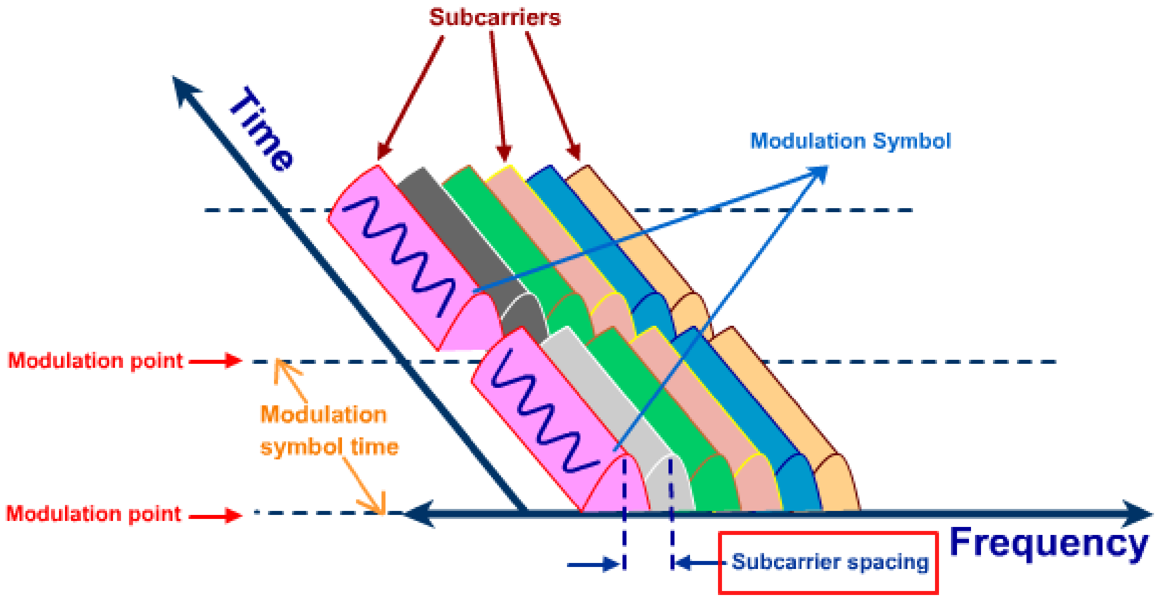


OFDM
(Orthogonal Frequency Division Multiplexing)

- **OFDM** (anglicky Orthogonal Frequency Division Multiplexing, ortogonální multiplex s frekvenčním dělením) je širokopásmová modulace využívající frekvenční dělení kanálu.

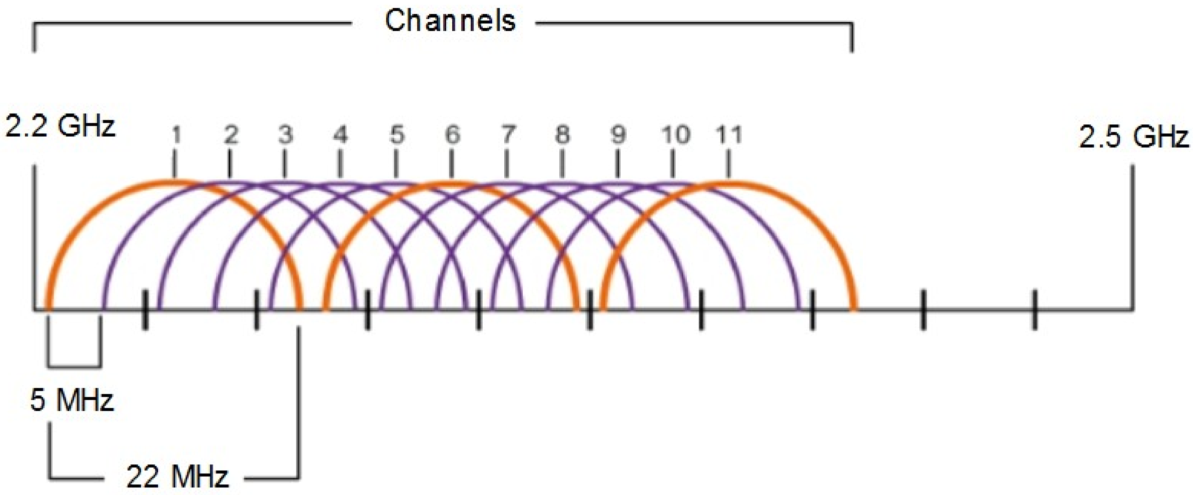
- Pracuje s tzv. rozprostřeným spektrem, kdy je signál vysílán na více vzájemně ortogonálních frekvencích , které jsou označovány jako subnosné.

Podkanály v OFDM



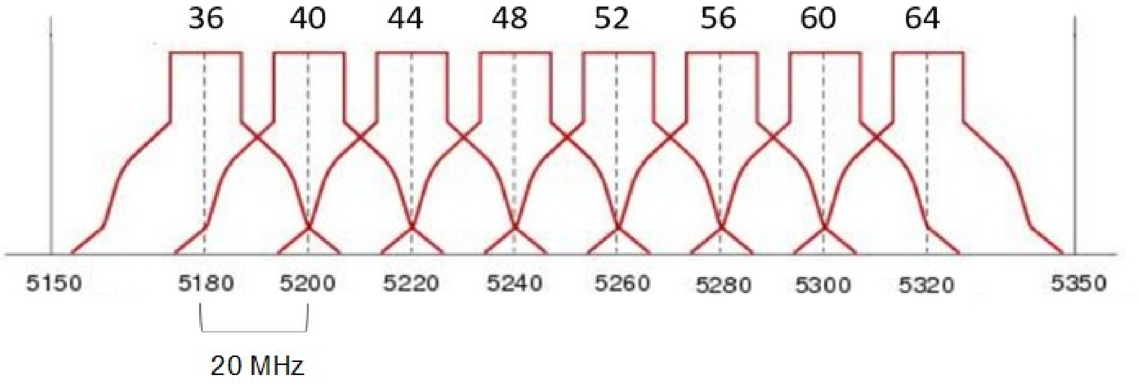
Channel Selection

- The 2.4 GHz band is subdivided into multiple channels each allotted 22 MHz bandwidth and separated from the next channel by 5 MHz.
- A best practice for 802.11b/g/n WLANs requiring multiple APs is to use non-overlapping channels such as 1, 6, and 11.

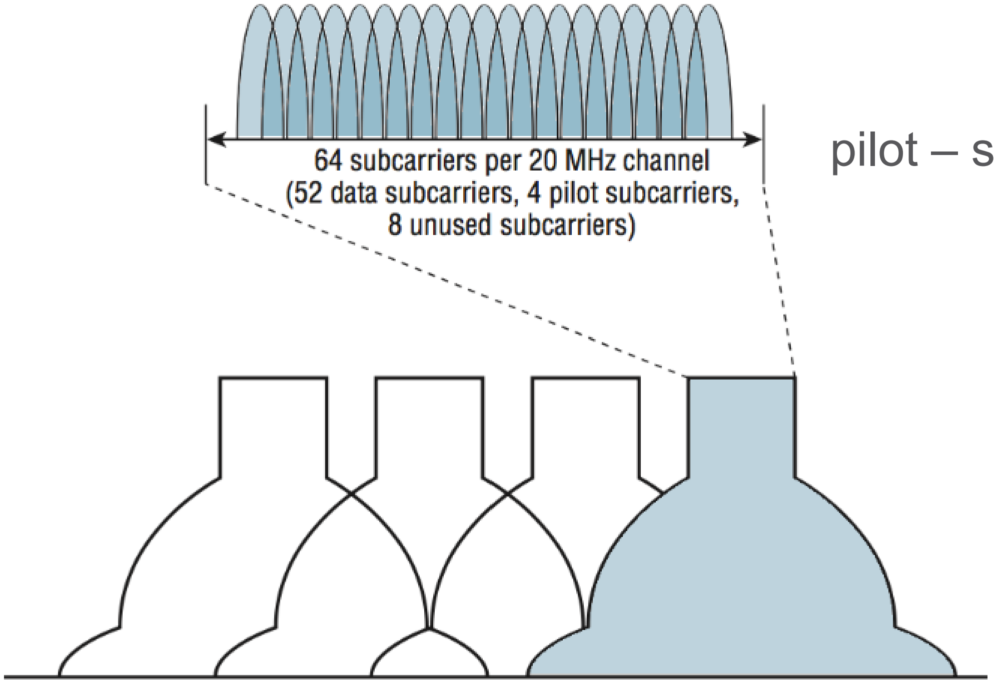


Channel Selection (Cont.)

- For the 5GHz standards 802.11a/n/ac, there are 24 channels. Each channel is separated from the next channel by 20 MHz.
- Non-overlapping channels are 36, 48, and 60.



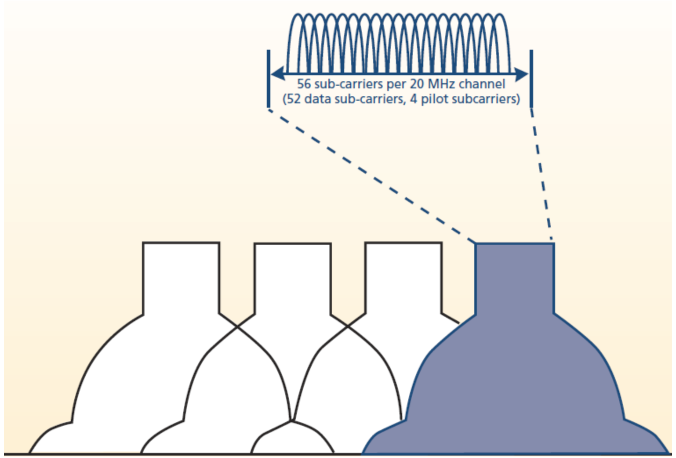
U 802.11n/ac je podkanálů 64
(Každý OFDM subcarrier je 312.5 KHz)

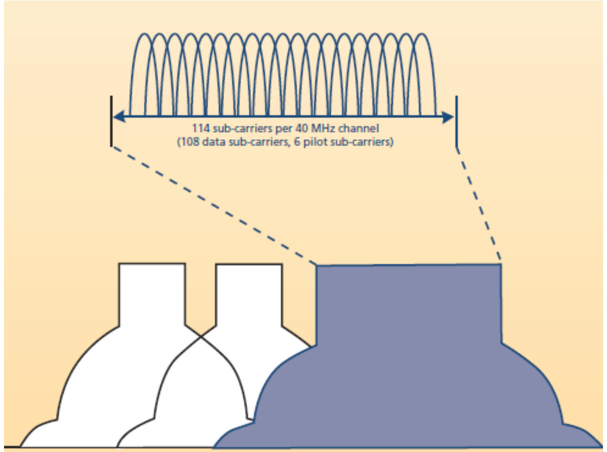


64 subcarriers per 20 MHz channel
(52 data subcarriers, 4 pilot subcarriers,
8 unused subcarriers)

pilot – synchronizace

Následovalo zrychlení OFDM z 20 na 40 MHz a zvýšení počtu subkanálů


56 sub-carriers per 20 MHz channel
(52 data sub-carriers, 4 pilot subcarriers)

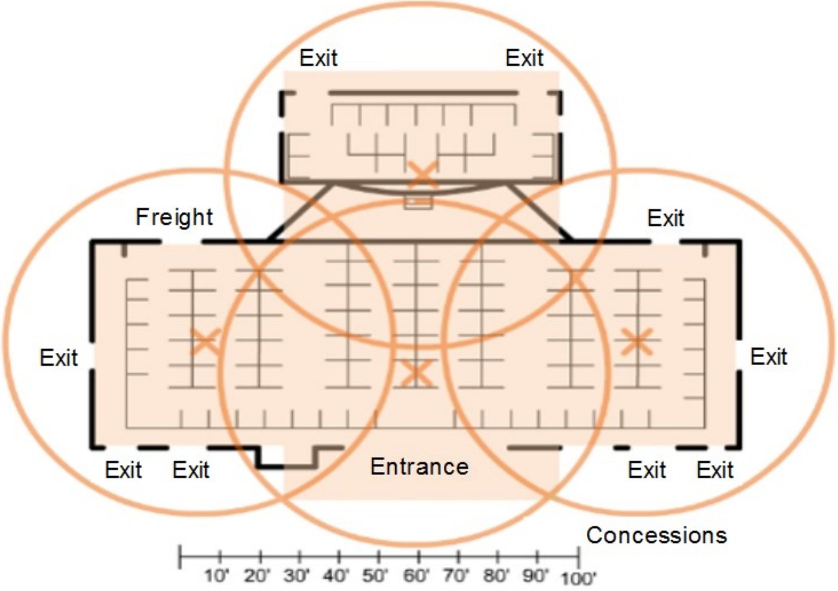

114 sub-carriers per 40 MHz channel
(108 data sub-carriers, 6 pilot sub-carriers)

Plan a WLAN Deployment

The number of users supported by a WLAN depends on the following:

- The geographical layout of the facility
- The number of bodies and devices that can fit in a space
- The data rates users expect
- The use of non-overlapping channels by multiple APs and transmit power settings

When planning the location of APs, the approximate circular coverage area is important.



12.6 WLAN Threats

Video – WLAN Threats

This video will cover the following:

- Interception of Data
- Wireless Intruders
- Denial of Service (DoS) Attacks
- Rogue APs

Wireless Security Overview

A WLAN is open to anyone within range of an AP and the appropriate credentials to associate to it.

Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including the following:

- Interception of data
- Wireless intruders
- Denial of Service (DoS) Attacks
- Rogue APs

DoS Attacks

Wireless DoS attacks can be the result of the following:

- Improperly configured devices
- A malicious user intentionally interfering with the wireless communication
- Accidental interference

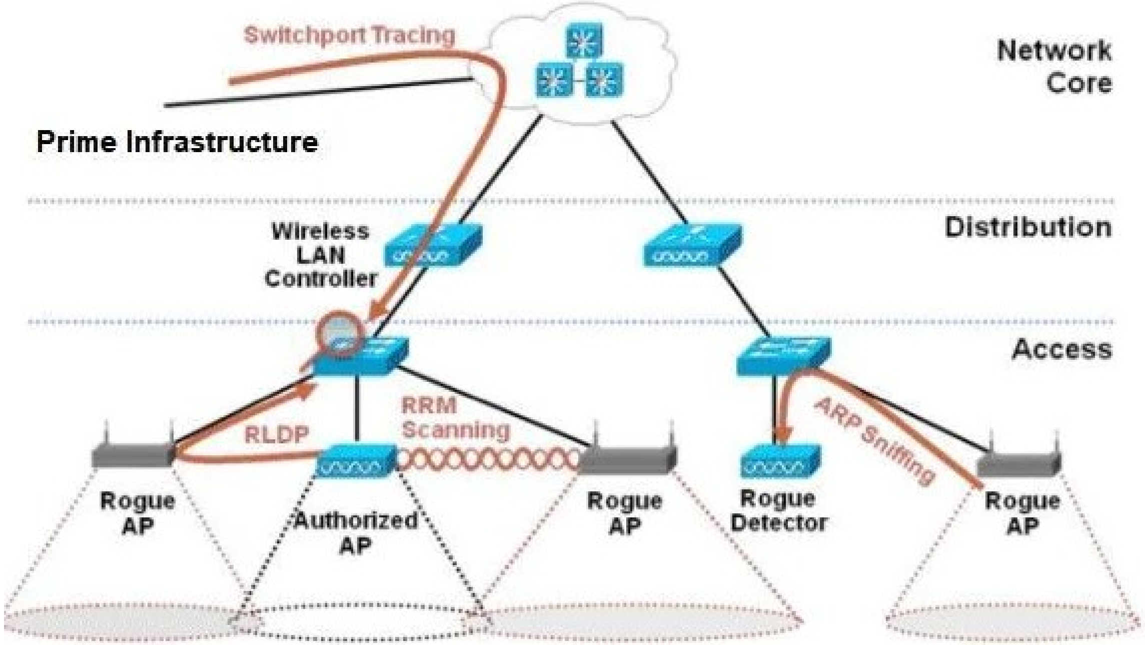
To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

Rogue Access Points

- A rogue (darebácké) AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy.
- Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.
- A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP.
- To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies and use monitoring software to actively monitor the radio spectrum for unauthorized APs.

Cisco Rogue Management

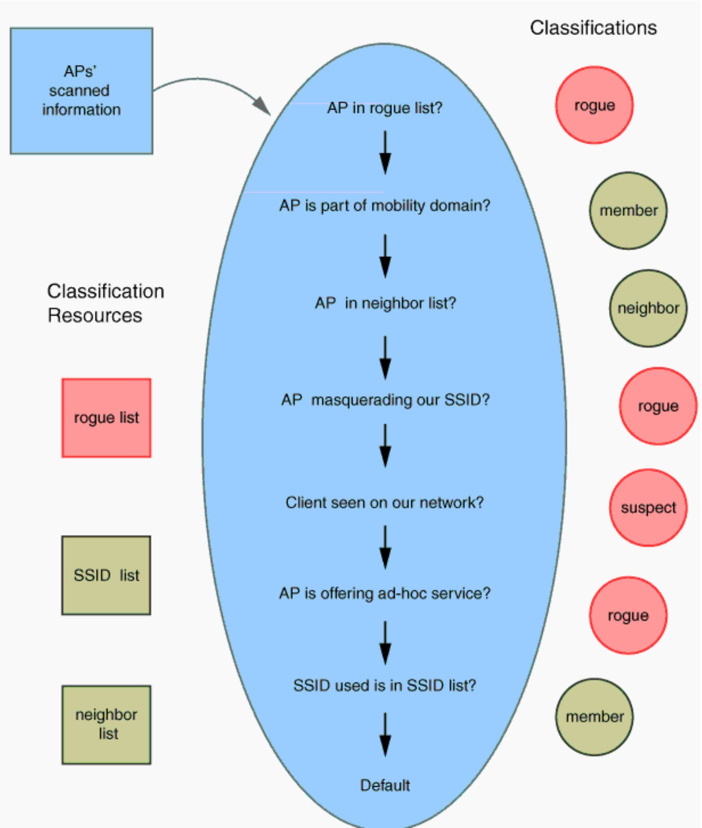
- **Detekce** - skenování pomocí správy rádiových zdrojů (RRM) se používá k detekci přítomnosti nepoctivých zařízení.
- **Klasifikace** - Rogue Location Discovery Protocol (RLDP), identifikace, zda je nepoctivé zařízení připojeno ke kabelové síti.
- **Zmírnění** - Uzavření portů přepínače, nepoctivé umístění a nepoctivé zadržení se používají ke sledování jeho fyzického umístění a zrušení hrozby nepoctivého zařízení.



Zpracování hlášení o Rogue AP

1. Řadič (controller) ověří, zda je neznámý AP v seznamu **Friendly MAC**. Pokud ano, řadič klasifikuje přístupový bod jako **Friendly**.
2. Pokud neznámý přístupový bod není v seznamu Friendly MAC, začne řadič používat pravidla klasifikace pro ty Rogue.
3. Pokud je darebák již klasifikován jako škodlivý, výstražný nebo přátelský, interní nebo externí, řadič jej automaticky neklasifikuje. Pokud je darebák klasifikován odlišně, řadič jej automaticky překlasifikuje, pouze pokud je darebák ve stavu výstrahy.
4. Řídicí jednotka použije první pravidlo na **základě priority**.
5. Pokud darebácký přístupový bod neodpovídá žádnému z nakonfigurovaných pravidel, řadič klasifikuje darebáka jako **nezařazeného**.
6. Řadič opakuje předchozí kroky pro všechny nepoctivé přístupové body.

Jiný klasifikační algoritmus



Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “**evil twin AP**” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

Defeating a MITM attack begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

12.7 Secure WLANs

Video – Secure WLANs

This video will cover the following:

- SSID Cloaking
- MAC Address Filtering
- Authentication and Encryption Systems (Open Authentication and Shared Key Authentication)

SSID Cloaking and MAC Address Filtering

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs:

SSID Cloaking

- APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must be manually configured with the SSID to connect to the network.

MAC Address Filtering

- An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

802.11 Original Authentication Methods

The best way to secure a wireless network is to use authentication and encryption systems. Two types of authentication were introduced with the original 802.11 standard:

Open system authentication

- No password required. Typically used to provide free internet access in public areas like cafes, airports, and hotels.
- Client is responsible for providing security such as through a VPN.

Shared key authentication

- Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

Shared Key Authentication Methods

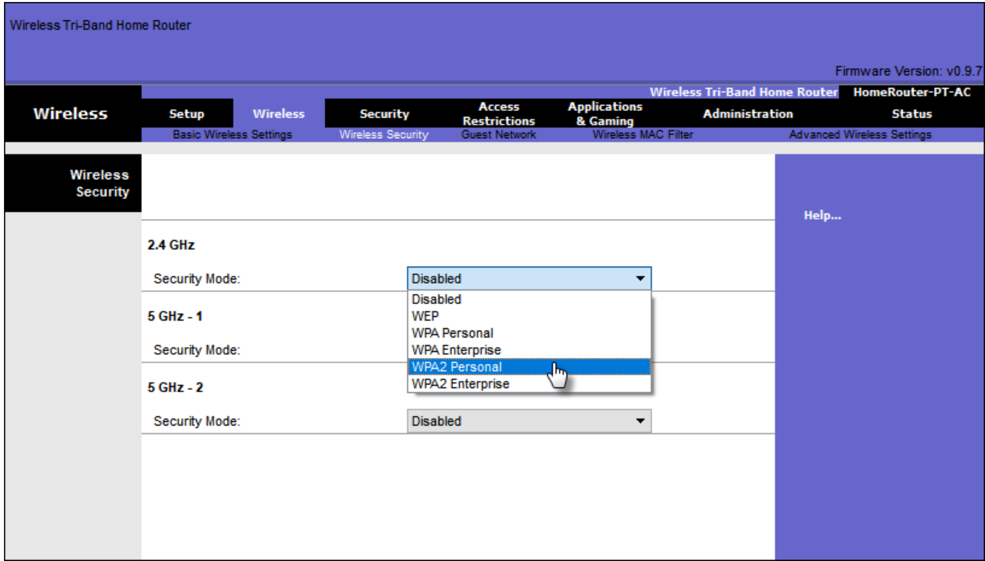
There are currently four shared key authentication techniques available, as shown in the table.

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF).

Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2, with WPA 2 having two authentication methods.

- **Personal** – Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise** – Intended for enterprise networks. Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.



2.4 GHz

Security Mode: Disabled

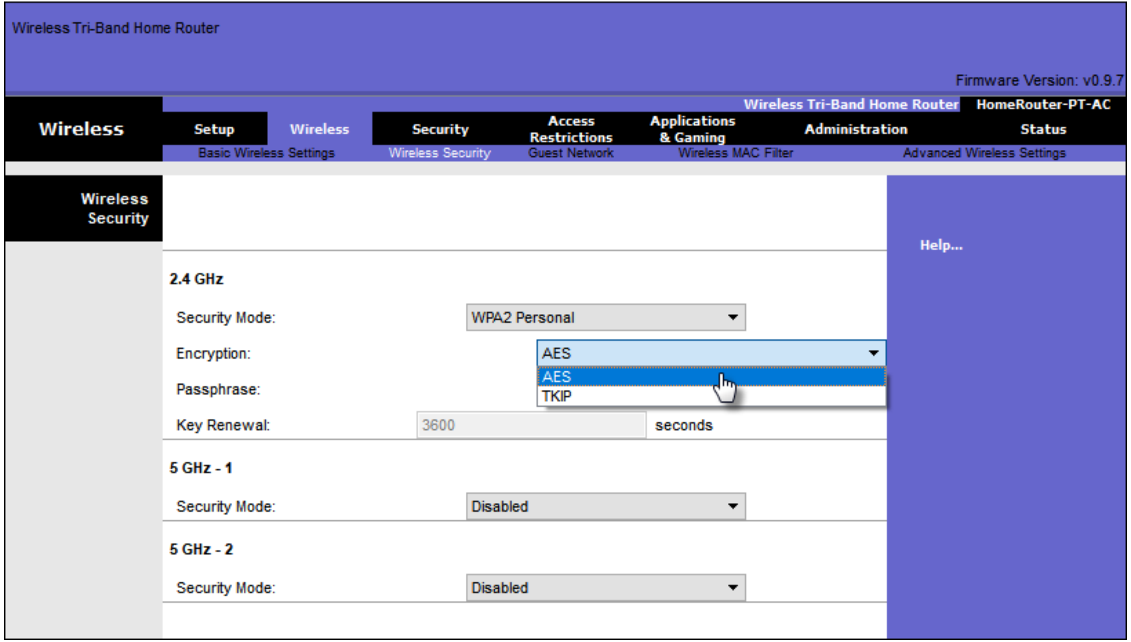
5 GHz - 1

Security Mode:

5 GHz - 2

Security Mode: Disabled

Encryption Methods



2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES (AES, TKIP)

Passphrase:

Key Renewal: 3600 seconds

5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

WPA and WPA2 include two encryption protocols:

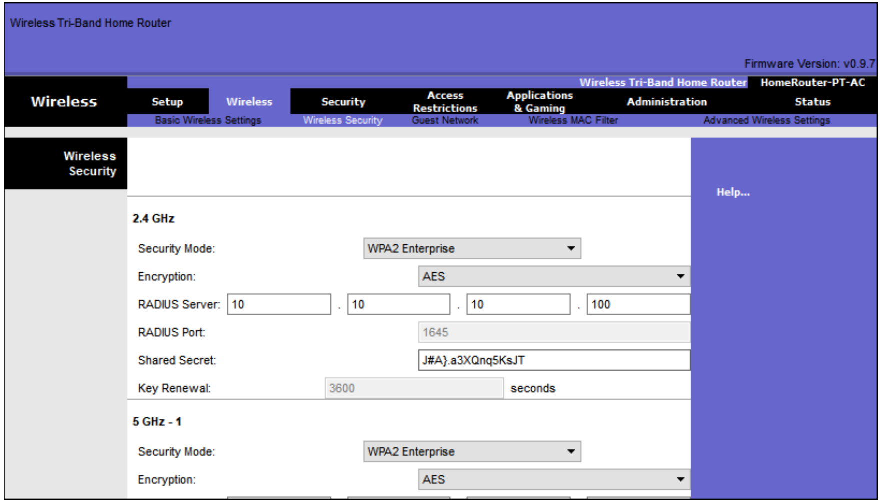
- **Temporal Key Integrity Protocol (TKIP)** – Used by WPA and provides support for legacy WLAN equipment. Makes use of WEP but encrypts the Layer 2 payload using TKIP.
- **Advanced Encryption Standard (AES)** – Used by WPA2 and uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

Authentication in the Enterprise

Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

There pieces of information are required:

- **RADIUS server IP address** – IP address of the server.
- **UDP port numbers** –UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.
- **Shared key** – Used to authenticate the AP with the RADIUS server.



2.4 GHz

Security Mode: WPA2 Enterprise

Encryption: AES

RADIUS Server: 10 . 10 . 10 . 100

RADIUS Port: 1645

Shared Secret: J#A}.a3XQnq5KsJT

Key Renewal: 3600 seconds

5 GHz - 1

Security Mode: WPA2 Enterprise

Encryption: AES

Note: User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

WPA 3

Because WPA2 is no longer considered secure, WPA3 is recommended when available. WPA3 Includes four features:

- **WPA3 – Personal :** Thwarts brute force attacks by using Simultaneous Authentication of Equals (SAE).
- **WPA3 – Enterprise :** Uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards.
- **Open Networks :** Does not use any authentication. However, uses Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.
- **IoT Onboarding :** Uses Device Provisioning Protocol (DPP) to quickly onboard IoT devices.

12.8 Module Practice and Quiz

Module 12: Osvědčené postupy

Téma 12.1

- Vysvětlete rozdíly mezi WPAN, WLAN, WMAN a WWAN.
- Proč si myslíte, že existuje tolik standardů 802.11?

Téma 12.2

- Kdy by bylo vhodné použít autonomní AP a AP založené na řadiči?
- Diskutujte o situaci, kdy je potřeba bezdrátový adaptér USB.

Téma 12.3

- Kdy by byly vhodné režimy ad hoc a režimy infrastruktury?
- Jaký je rozdíl mezi BSS a ESS?
- Diskutujte o parametrech vyjednaných mezi AP a bezdrátovým klientem pro úspěšné přidružení.

Téma 12.4

- Proč by organizace používala CAPWAP?
- Jaké možnosti poskytuje FlexConnect?

Module 12: Osvědčené postupy

Téma 12.5

- Jaké je řešení pro nasycení frekvenčního kanálu?

Téma 12.6

- Diskutujte o běžných útocích proti bezdrátovým sítím.
- Jaké jsou způsoby, jak zmírnit tyto útoky?

Téma 12.7

- Diskutujte o silných a slabých stránkách různých metod ověřování pomocí sdíleného klíče.
- Pokud je to možné, zobrazte nastavení zabezpečení bezdrátové sítě na přístupovém bodu.

Module Practice and Quiz

What did I learn in this module?

- A Wireless LANs (WLANs) are based on IEEE standards and can be classified into four main types: WPAN, WLAN, WMAN, and WWAN.
- Wireless technology uses the unlicensed radio spectrum to send and receive data. Examples of this technology are Bluetooth, WiMAX, Cellular Broadband, and Satellite Broadband.
- WLAN networks operate in the 2.4 GHz frequency band and the 5 GHz band.
- The three organizations influencing WLAN standards are the ITU-R, the IEEE, and the Wi-Fi Alliance.
- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs.
- DTLS is a protocol provides security between the AP and the WLC.
- Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate. Ranges are then split into smaller ranges called channels: DSSS, FHSS, and OFDM.
- The 802.11b/g/n standards operate in the 2.4 GHz to 2.5GHz spectrum. The 2.4 GHz band is subdivided into multiple channels. Each channel is allotted 22 MHz bandwidth and is separated from the next channel by 5 MHz.
- Wireless networks are susceptible to threats, including: data interception, wireless intruders, DoS attacks, and rogue APs.
- To keep wireless intruders out and protect data, two early security features are still available on most routers and APs: SSID cloaking and MAC address filtering.
- There are four shared key authentication techniques available: WEP, WPA, WPA2, and WPA3.