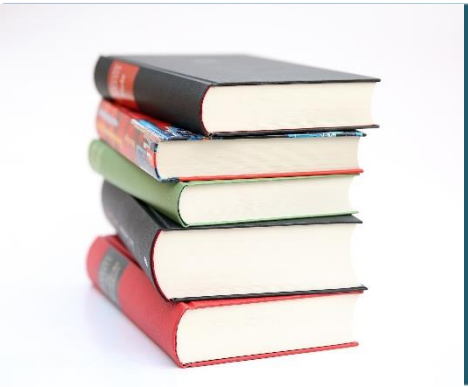
UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Prednáška 11
Wireless LAN

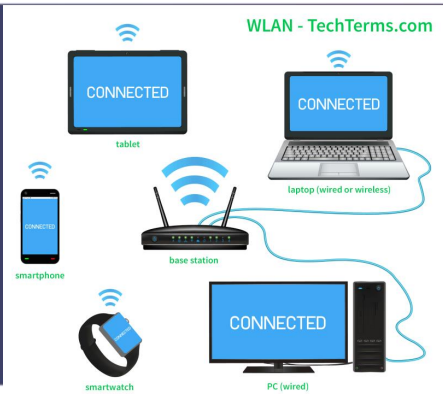
Počítačové siete 1

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.



Osnova dnešnej prednášky



WLAN

- SRWE
  - Chapter 12: WLAN Concepts (v tejto prednáške)
  - Chapter 13: WLAN Configuration (prečítať samostatne z Netacadu ! Príprava na cvičenie...)
- **Zodpovieme si tieto otázky:**
  - Aký je rozdiel medzi WPAN, WLAN, WMAN and WWAN?
  - Prečo je tak veľa štandardov pre WLAN? (802.11)
  - Kedy použiť autonómne AP a kedy controller-based?
  - Kedy je potrebný USB bezdrôtový adaptér?
- **A aj tieto:**
  - Kedy je vhodný ad-hoc model a kedy model infraštruktúry?
  - Aký je rozdiel medzi BSS a ESS?
  - Aké parametre si vymieňa AP a WLAN klient pre úspešné nadviazanie spojenia?
  - Kedy v organizácii použiť CAPWAP?
  - Čo mi prinesie FlexConnect?
  - Aké je riešenie pre saturáciu frekvenčných kanálov?
  - Čo zvažovať keď umiestňujem AP v budove?
  - Aké útoky hrozia vo WLAN a ako ich viem zmierniť?

Úvod do WLAN

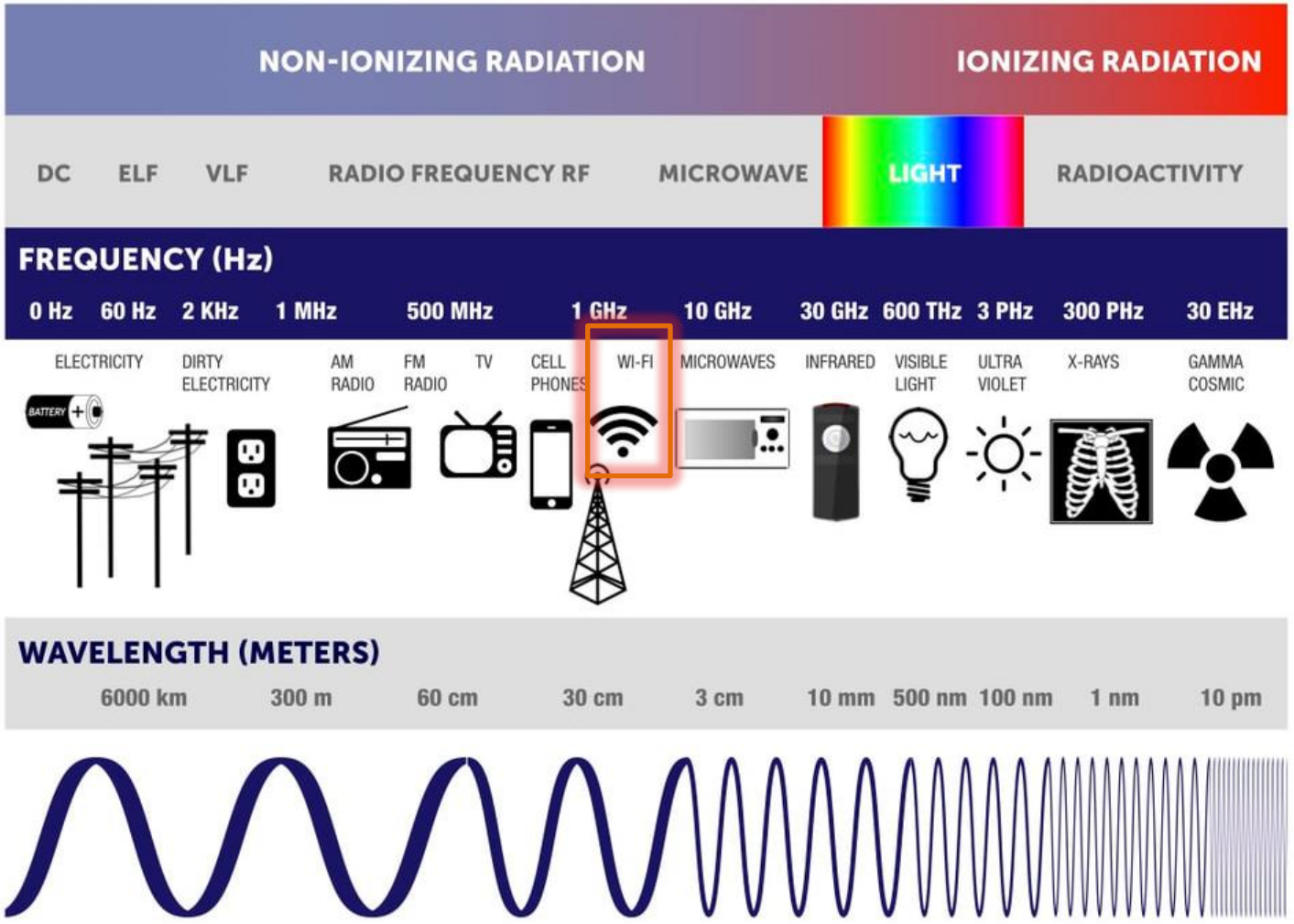
Bežne používaná

umožňuje mobilitu

prispôsobuje sa, ako sa menia potreby, a technológie

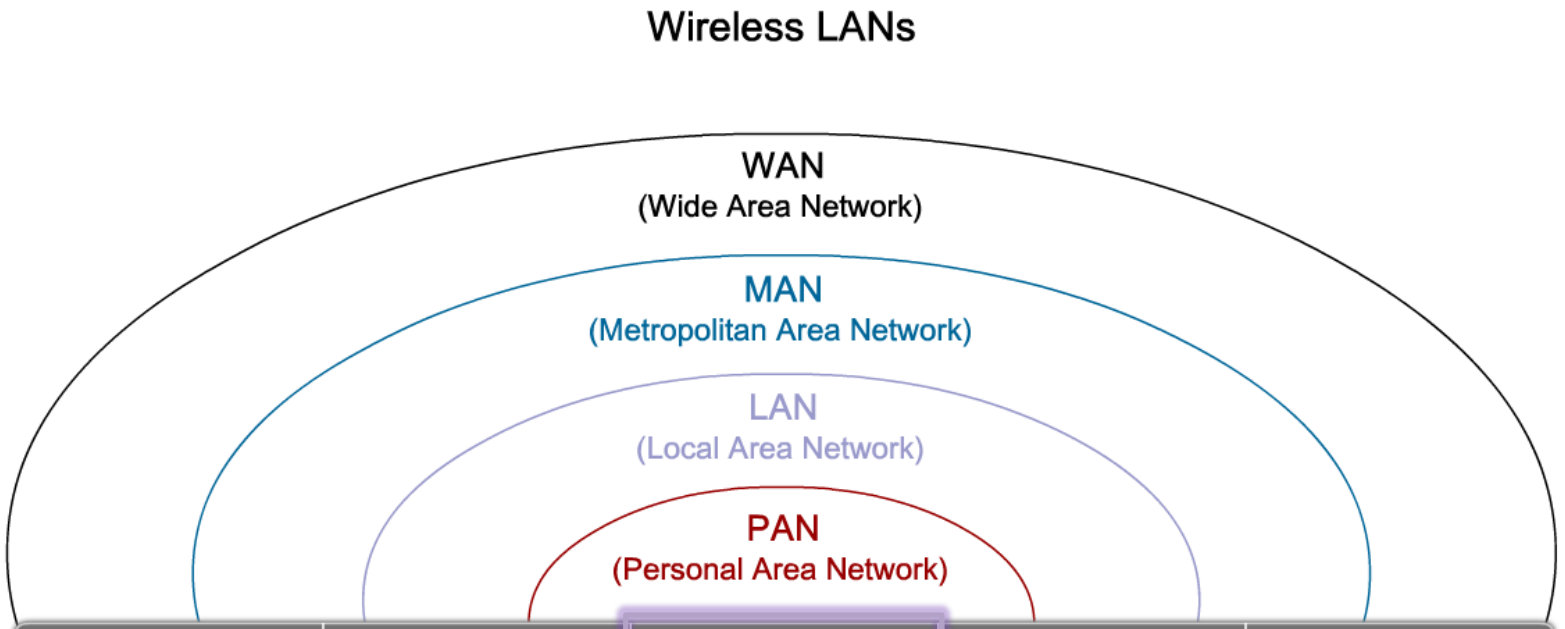
Bezrôtové technológie

- Využitie elektromagnetického vlnenia pre vysokorýchlostný prenos dát
  - „Rádiové“ vlny
  - Svetlo
    - bez svetlovodu, využívané zriedkavo
- Výhody:
  - Plošné pokrytie
  - Mobilita
  - Operatívnosť, flexibilita
  - Možnosť preklenúť pomerne veľké vzdialenosti a relatívne náročný terén



WLAN technológie (WLAN)

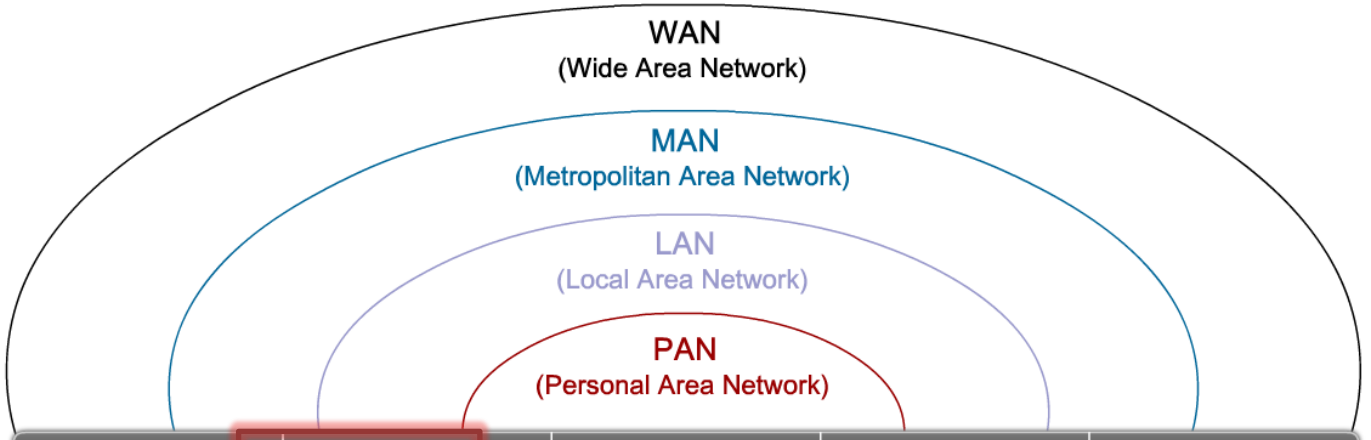
- časť **bezdrôtových** komunikačných technológií
  - poskytujú služby tradičných **LAN** sietí
  - nepatrí sem Bluetooth, GSM apod.
- najpoužívanejšie sú štandardy IEEE **802.11**



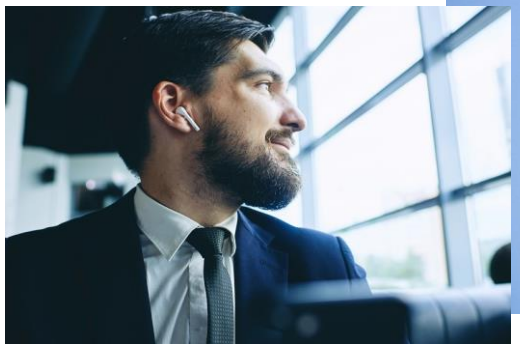
	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short 6-9 m	Medium 90 m	Medium-Long mesto	Long Národ./medzin.
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices
Frekv. pásmo	2,4 GHz	2,4 Ghz / 5 GHz		Licencované

Wireless Technologies

- **Bluetooth**
  - IEEE W**PAN** štandards
  - Pre párovanie zariadení do **100 m**
  - BLE
    - Bluetooth Low Energy
    - Podporuje **mesh** topológiu
  - BR/EDR
    - Bluetooth Basic Rate/Enhanced Rate
    - Podporuje **point-to-point** topológie
    - Optimalizované pre audio streaming
- **WiMAX**
  - Worldwide Interoperability for Microwave Access
  - Alternatíva ku **širokopásmovému** drôt. prístupu do internetu
  - IEEE 802.16 WLAN štandard, do **50 km**

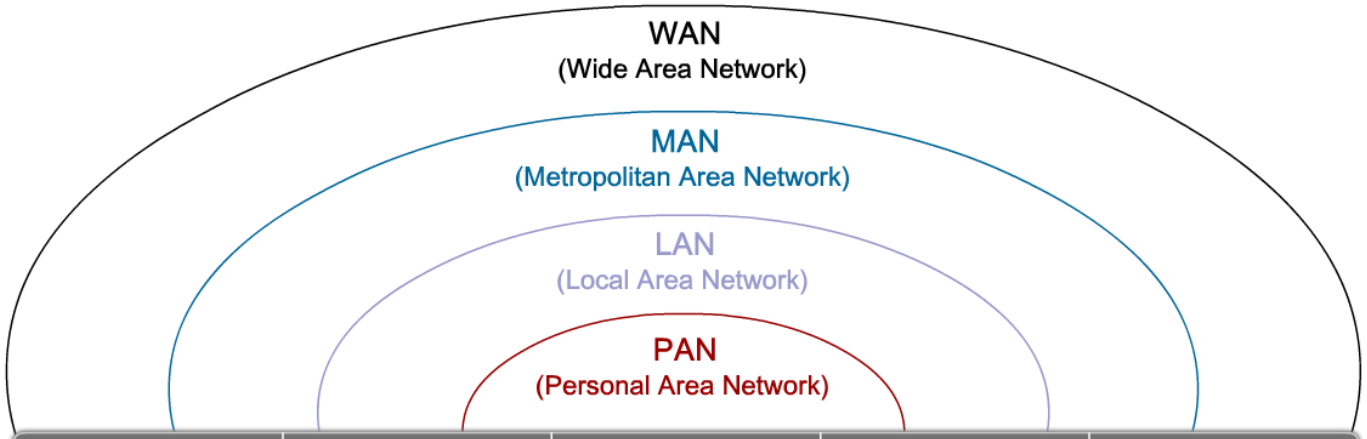


	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices



Wireless Technologies

- **Bunkové širokopásmové siete** (Cellular Broadband)
  - prenášajú aj hlas aj dáta
  - využívané telefónmi, automobilmi, tabletmi, laptopmi, ..
  - **GSM** sieť (Global System of Mobile)
- **Satelitné širokopásmové siete** (Satellite Broadband)
  - Používajú smerovú satelitnú parabolu spojenú so satelitom na geostacionárnej obežnej dráhe
  - Vyžaduje priamu viditeľnosť
  - Používané tam kde sa nedá pripojiť inak (odľahlé miesta, ...)

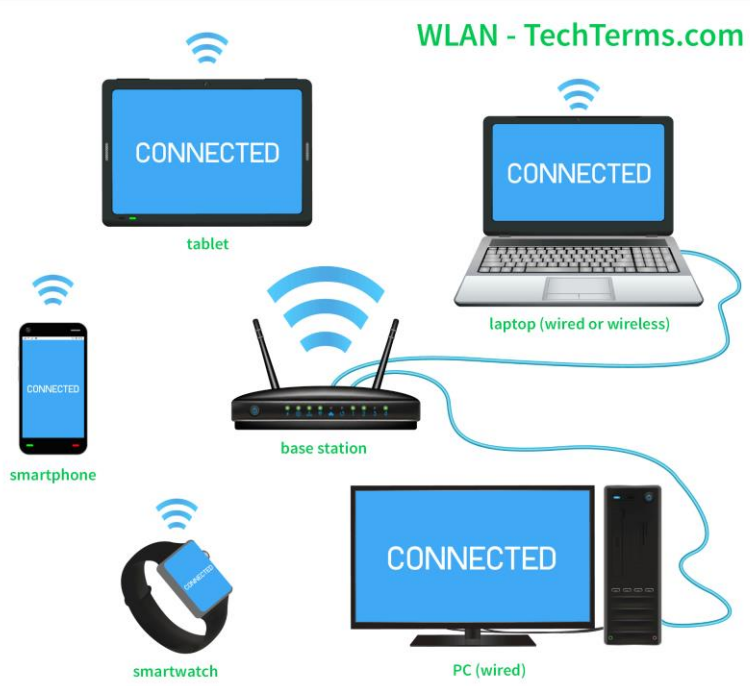


	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

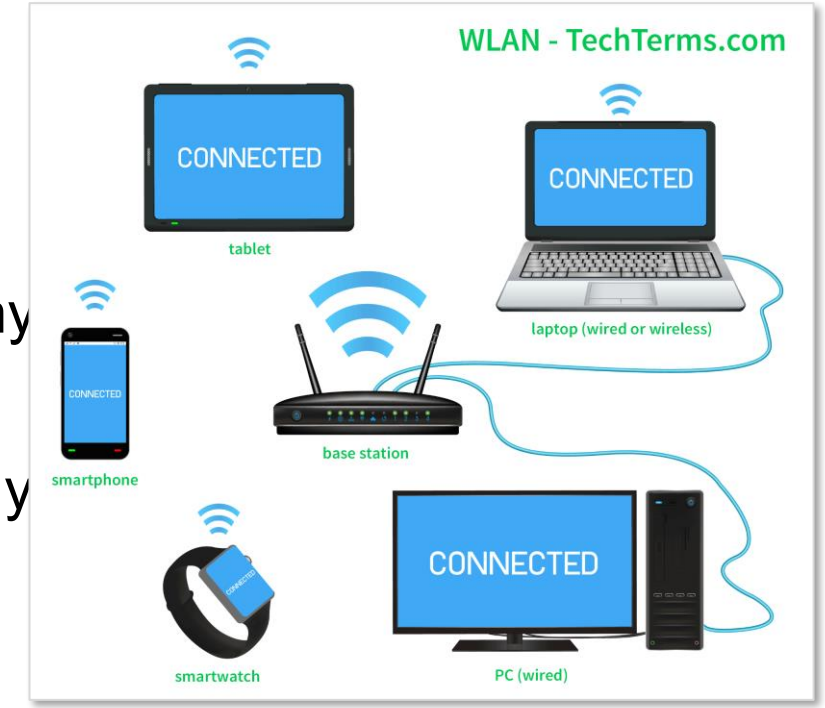
Wireless LAN technológie

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

- nie sú náhradou existujúcich „wired“ LAN sietí
  - Prenosové rýchlosti vo WLAN sieťach sú stále o rád nižšie než v LAN
    - ac už ani tak nie... (1,3 Gbps)
  - Vzájomné spojenie niektorých stavebných prvkov WLAN sietí je realizované LAN sieťou
  - WLAN siete majú voči LAN niektoré inherentné nevýhody, ktoré v LAN neexistujú alebo sú vyriešené
- Je vhodnejšie pozerať sa na WLAN
  - ako na pokračovanie a predĺženie bežných LAN sietí a v tomto zmysle ich aj nasadzovať



Wireless Standards Organizations



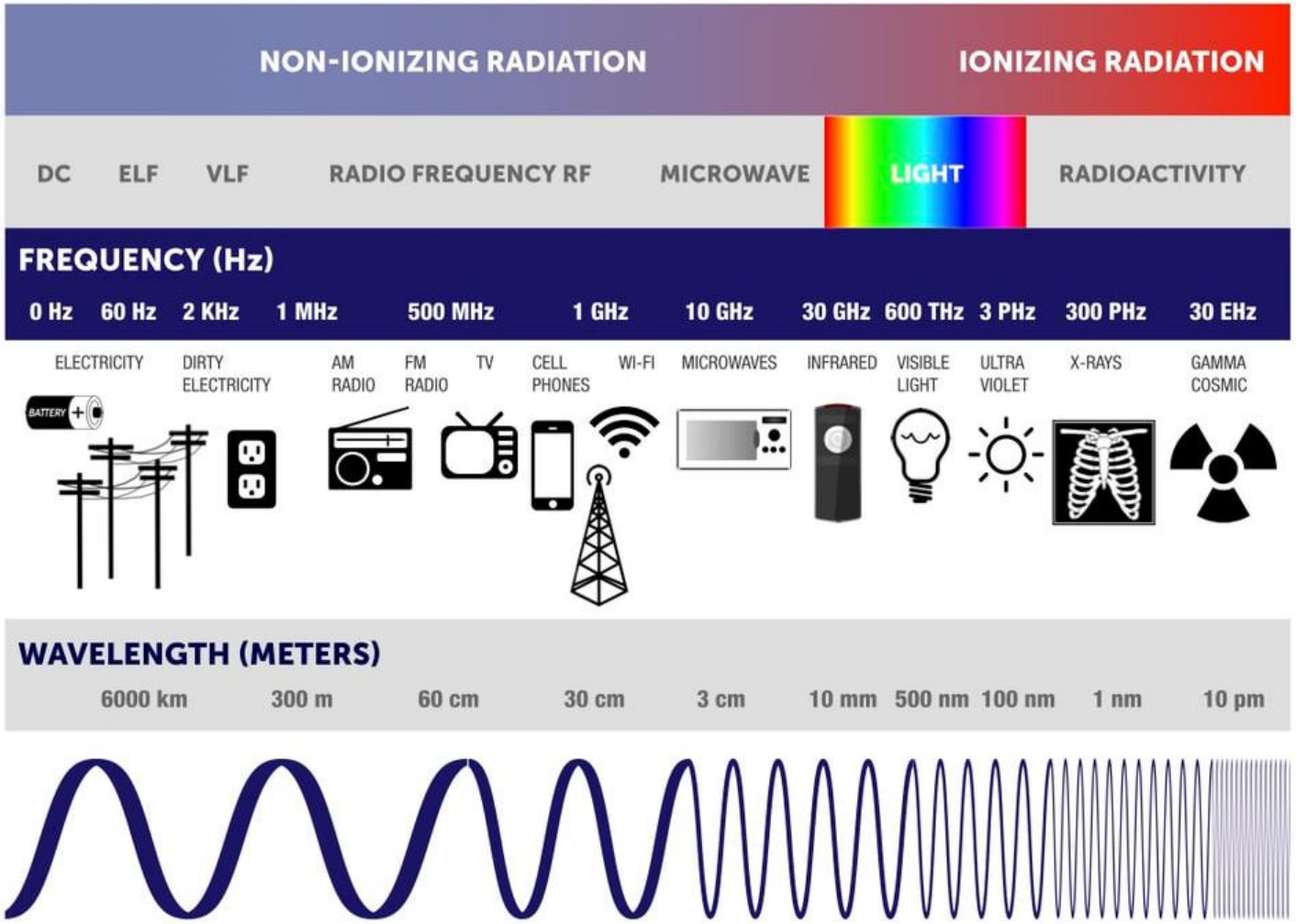
- Zabezpečenie **interoperability** medzi zariadeniami rôzny výrobcov
- Medzinárodne, tieto tri **organizácie** ovplyvňujú štandardy
  - **International Telecommunication Union (ITU)**
    - Reguluje alokované rádiové spektrum a satelitné dráhy
  - **Institute of Electrical and Electronics Engineers (IEEE)**
    - Špecifikuje ako je rádiová frekvencia modulovaná na nosný signál
    - Rodina štandardov pre LAN/MAN **802**, pre **WLAN 802.11**
      - 802.11e - prostriedky pre QoS vo WLAN
      - 802.11i - zabezpečenie WLAN sietí
  - **Wi-Fi Alliance**
    - Podporuje rast a akceptáciu sietí WLAN
    - Združenie predajcov, ktorého cieľom je zlepšiť interoperabilitu výrobkov založených na štandarde 802.11

Základné pojmy (1)

2.4 GHz (UHF) – 802.11b/g/n/ax

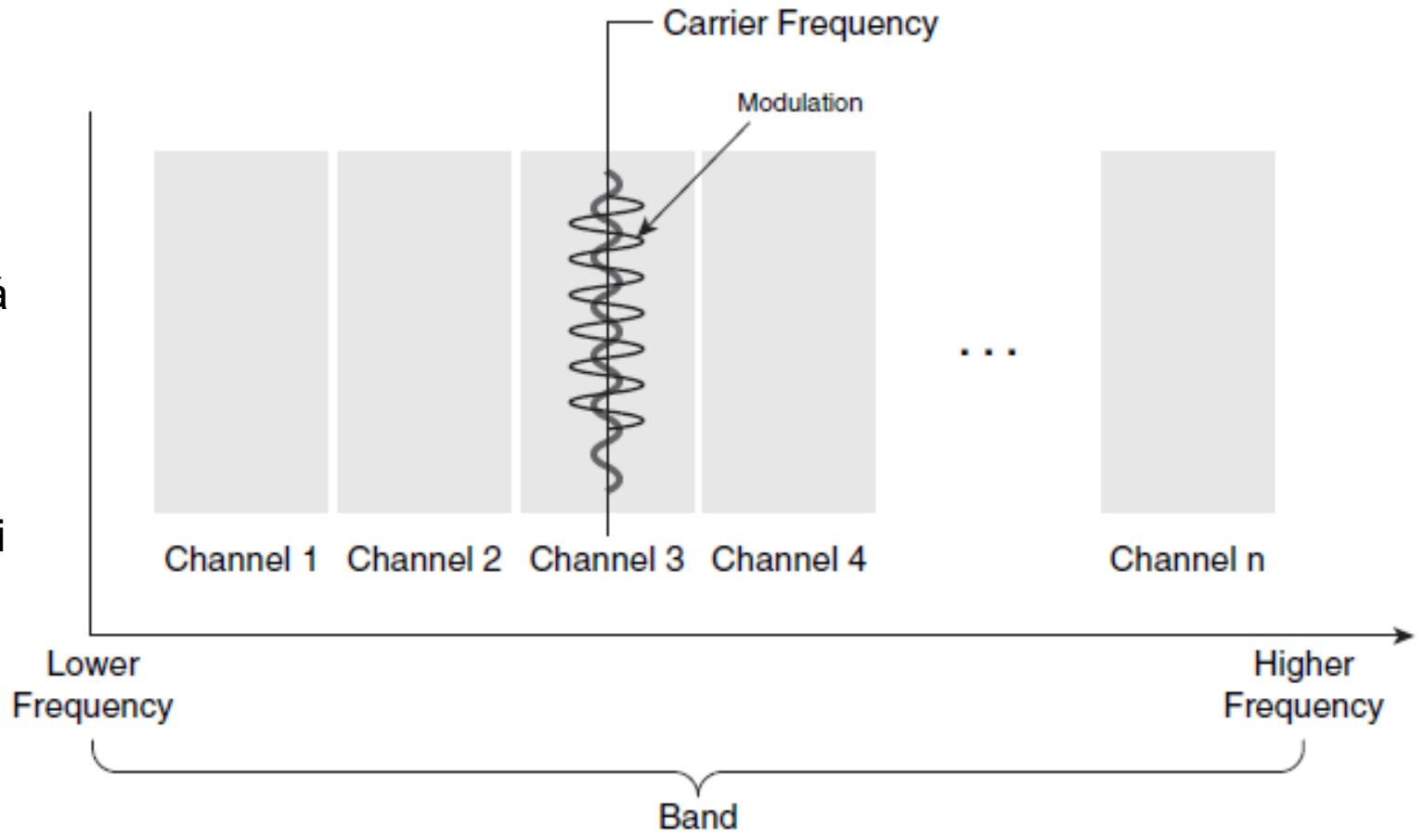
5 GHz (SHF) – 802.11a/n/ac/ax

- **Kódovanie**
  - Prevod prenášaných dát do symbolov (z jednej formy na druhú pomocou algoritmu)
    - Vhodnejších na prenos, rýchlejších, podporujúcich samosynchronizáciu, detekciu chýb, zníženie objemu a pod.
- **Šírka pásma (band)**
  - Skupina frekvencií využitá za nejakým účelom
    - Rozsah AM rádiového vysielania je od 550 MHz po 1720 MHz.
    - WiFi rozsah na 2,4GHz je od 2.412 do 2.484 GHz, pri 5GHz je rozsah použitých frekvencií 5.150 to 5.825 GHz.
- **Nosný signál (Carrier signal)**
  - Signál určitej frekvencie, vhodnej na prenos
  - Sám o seba nemá informačnú hodnotu
  - Informáciu pridávame *moduláciou*



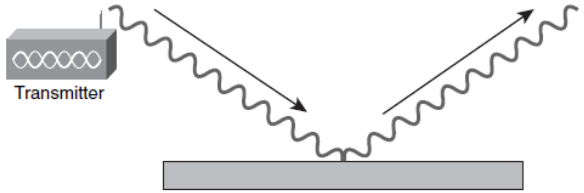
Základné pojmy (2)

- **Modulácia**
  - Zmena istej charakteristiky prenášaného signálu, ktorou bude vyjadrený prenášaný symbol počas prenosu
  - Amplitúdová, fázová, frekvenčná
- **Kanál (Channel)**
  - Kvôli tejto zmene prijímač aj vysielač síce očakávajú nosnú na určitej frekvencii ale s malými zmenami = **kanál**
- **Frekvenčná schéma**
  - Spôsob, akým vysielač obsadzuje rozsah frekvencií v danom kanáli

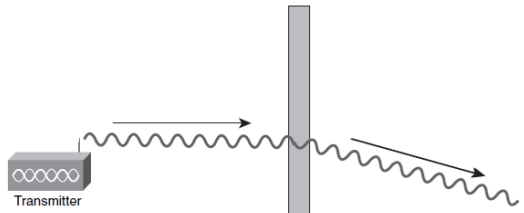


Radiofrekvenčný signál

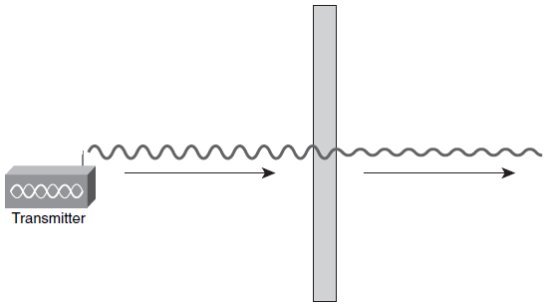
- Vplyv prostredia
  - Odraz (reflection)



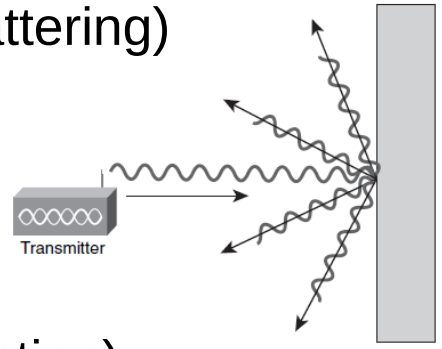
  - Lom (refraction)



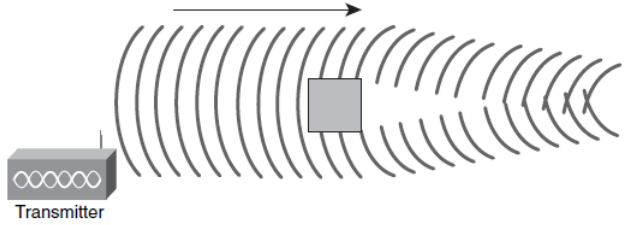
  - Absorbcia (absorbtion)

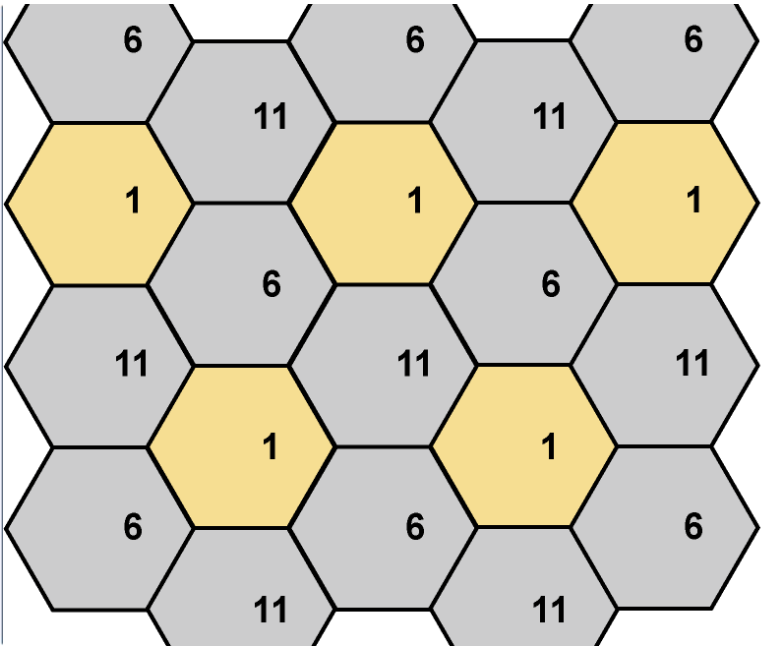


  - Rozptyl (scattering)



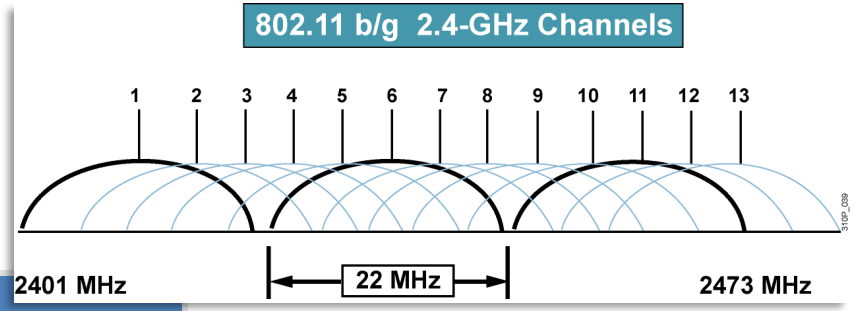
  - Ohyb (diffraction)





Manažment kanálov vo WLAN

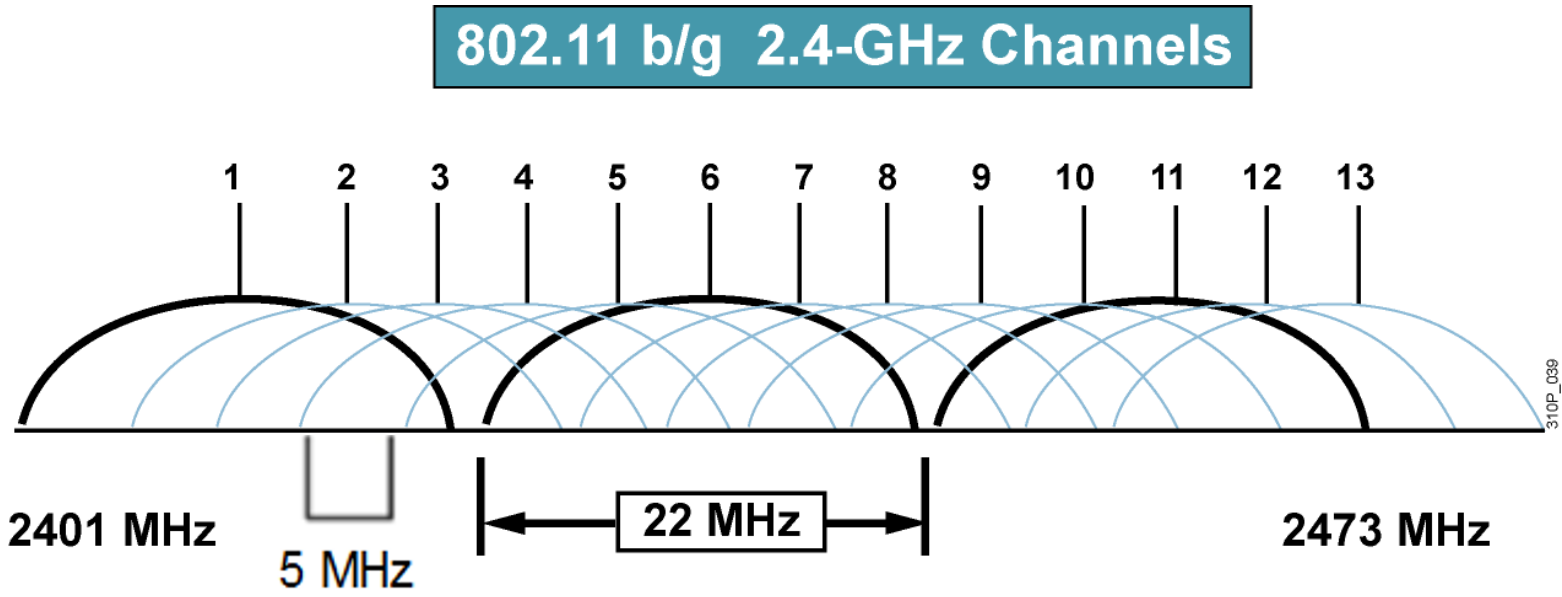
2.4-GHz Channels (b/g)



Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 2448	X	X	X
7	2442 MHz	2431 – 2453	X	X	X
8	2447 MHz	2436 – 2458	X	X	X
9	2452 MHz	2441 – 2463	X	X	X
10	2457 MHz	2446 – 2468	X	X	X
11	2462 MHz	2451 – 2473	X	X	X
12	2467 MHz	2466 – 2478		X	X
13	2472 MHz	2471 – 2483		X	X
14	2484 MHz	2473 – 2495			X

Manažment kanálov

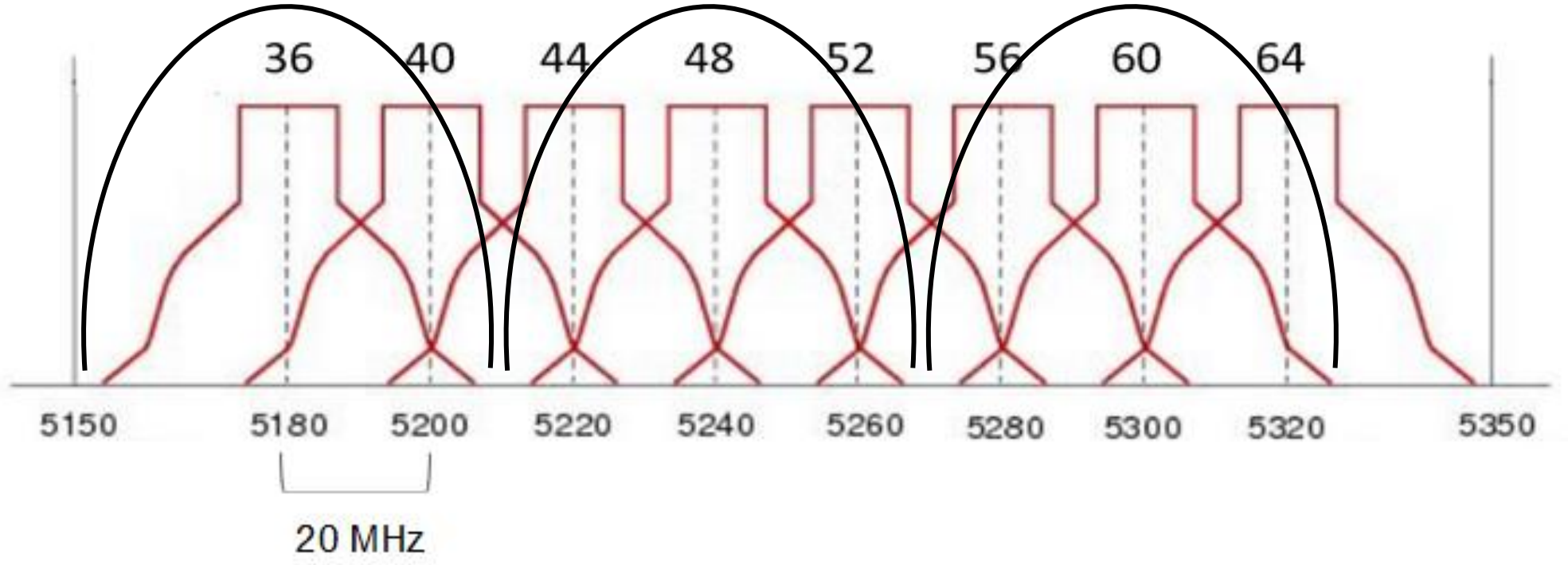
Využitie kanálov v pásme 2.4-GHz



- Každý kanál má šírku 22 MHz
- Počet kanálov:
  - Severná Amerika: 11 kanálov
  - Európa: 13 kanálov
- Sú tam 3 neprekrávajúce sa kanály: 1, 6, 11
  - Použitie ktorýchkoľvek iných, spôsobuje interferenciu
  - Na jednom území preto môžu byť bez rušenia max. 3 APs

Využitie kanálov v 5GHz

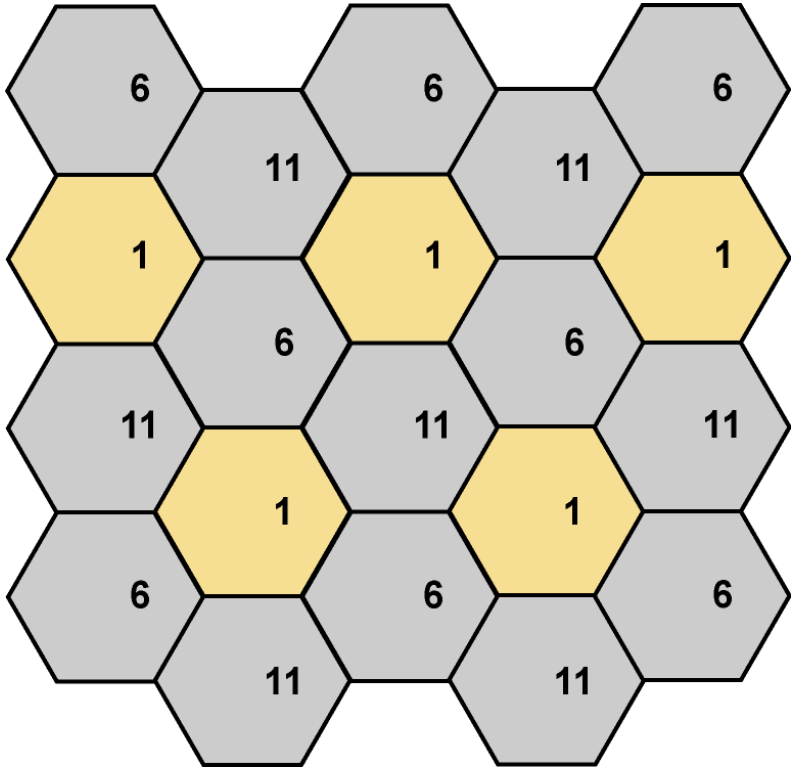
- Pre 5GHz štandardy 802.11a/n/ac je 24 kanálov
- Rozostup medzi kanálmi je 20 MHz
- Neprekrývajúce kanály sú 36, 48, and 60



Manažment kanálov

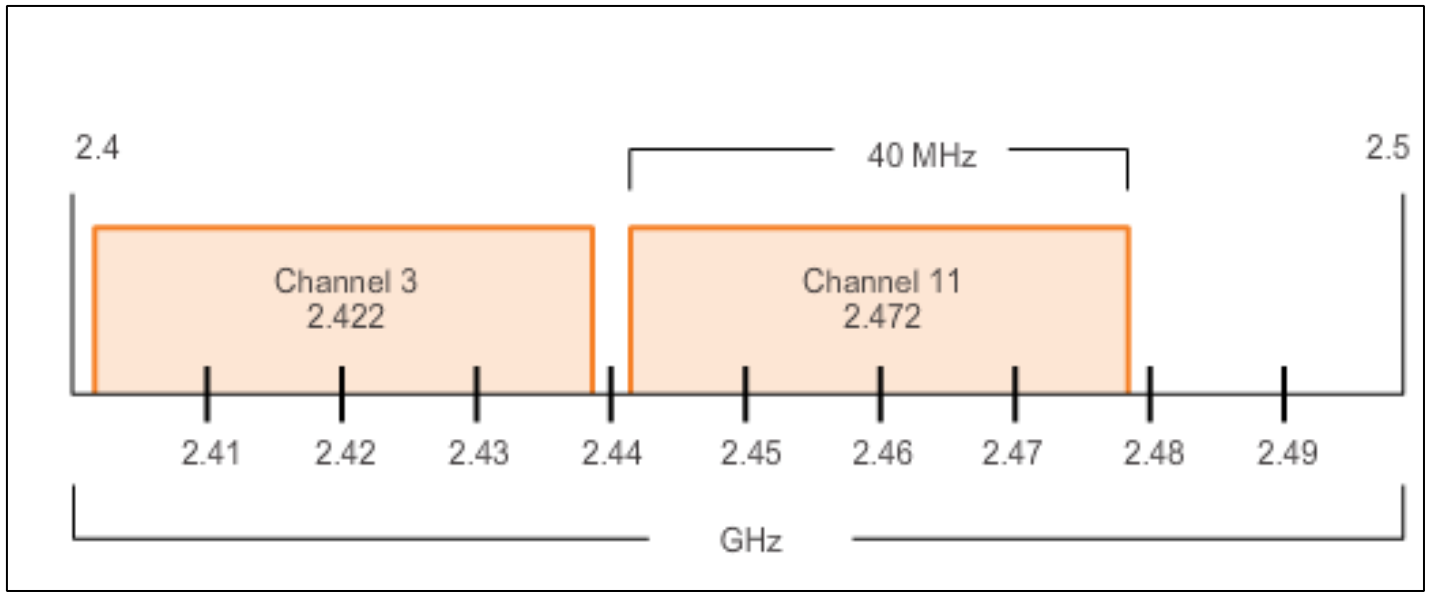
802.11b/g (2.4 GHz)

Channel Reuse



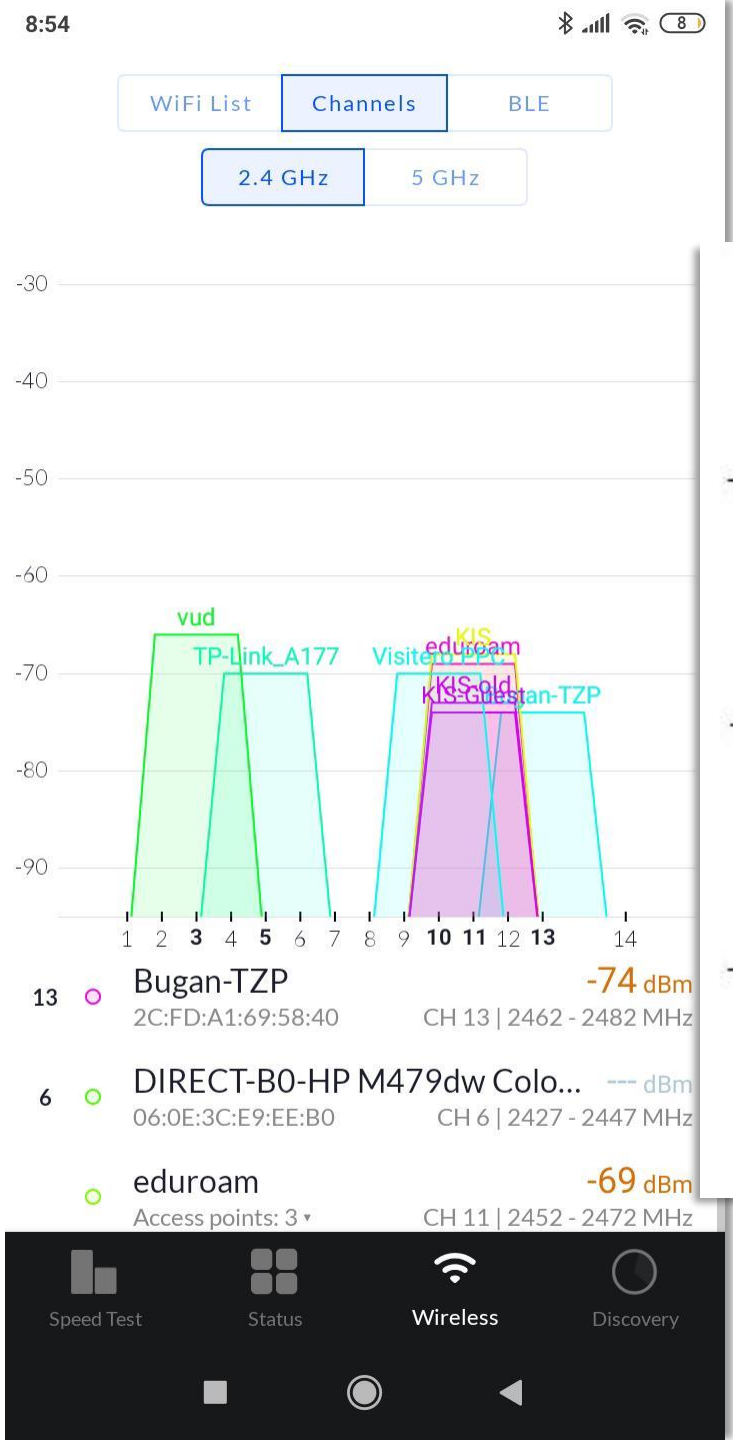
Channel bonding

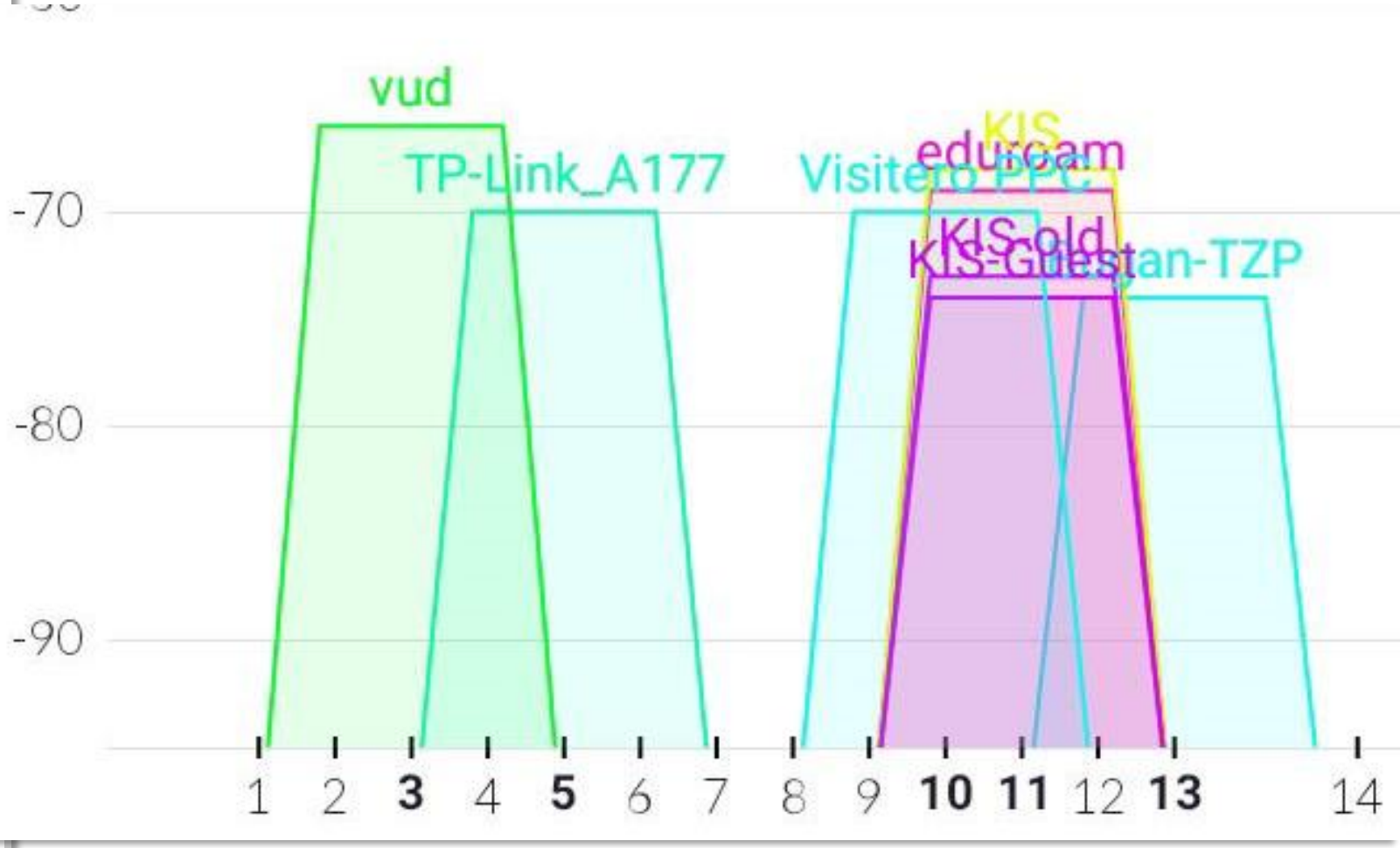
- Channel bonding kombinuje dva 20-MHz kanály do jedného 40-MHz kanála



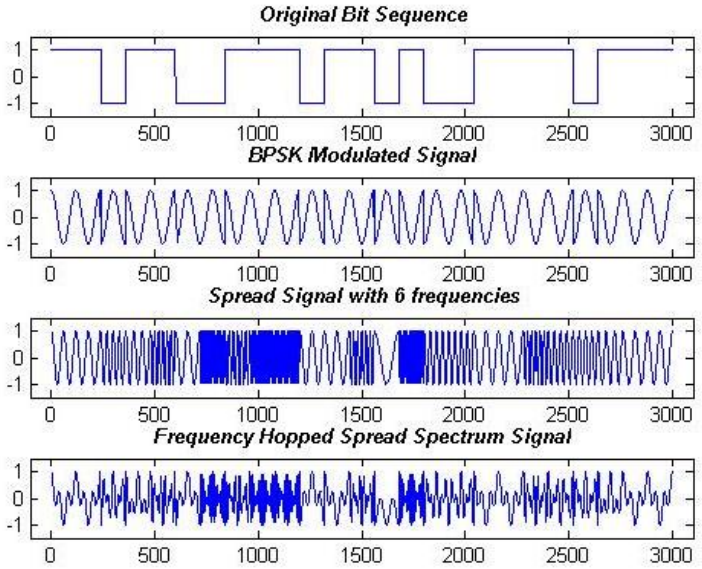
802.11n (OFDM) Channel Width 40 MHz

WLAN na FRI-KIS





Wifi Analyzers
https://play.google.com/store/search?q=wili%20anlyzer&c=apps&hl=en&gl=US



Modulačné techniky (rodiny techník)

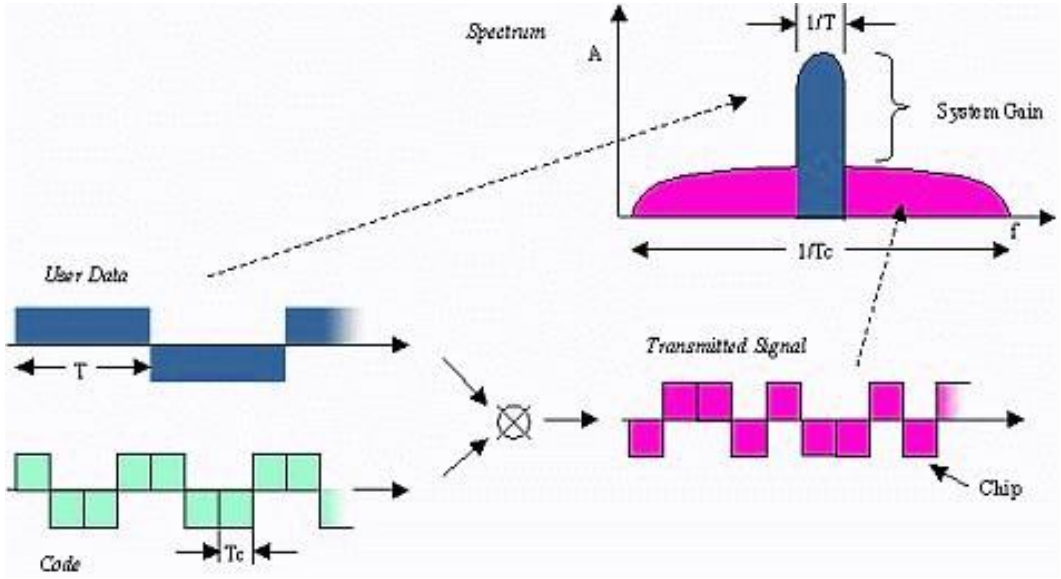
Ak je dopyt po konkrétnom bezdrôtovom kanáli príliš vysoký,
môže dôjsť k jeho nadmernému nasýteniu (oversaturation), čo by znížilo kvalitu komunikácie.

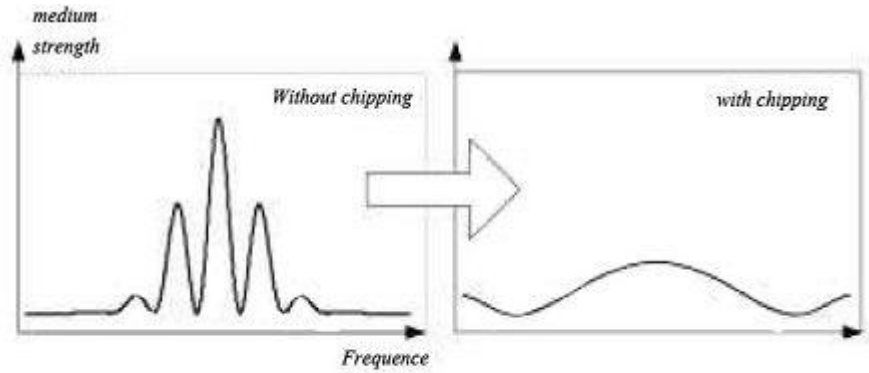
Sýtosť kanálov je možné zmierniť pomocou techník,
ktoré kanály využívajú efektívnejšie.

Direct Sequence Spread Spectrum (DSSS)

Rozprestretie spektra priamou postupnosťou

- používa sa na zariadeniach 802.11b
  - aby sa zabránilo rušeniu od iných zariadení používajúcich rovnakú frekvenciu 2,4 GHz
  - Zvyšuje odolnosť voči úzkopásmovému rušeniu
- Prenášané užitočné dáta sa kombinujú s prúdom pseudonáhodných kódov, tzv. chips (v štandarde 802.11b pripadá 8/11 chips na 1 bit)
  - Efektívne sa takto do dát pridáva šum, ktorý spôsobí rozprestrenie frekvenčného spektra
    - Zvýšenie odolnosti voči rušeniu
  - Je tu potrebná synchronizácia pri pseudonáhodnom kóde





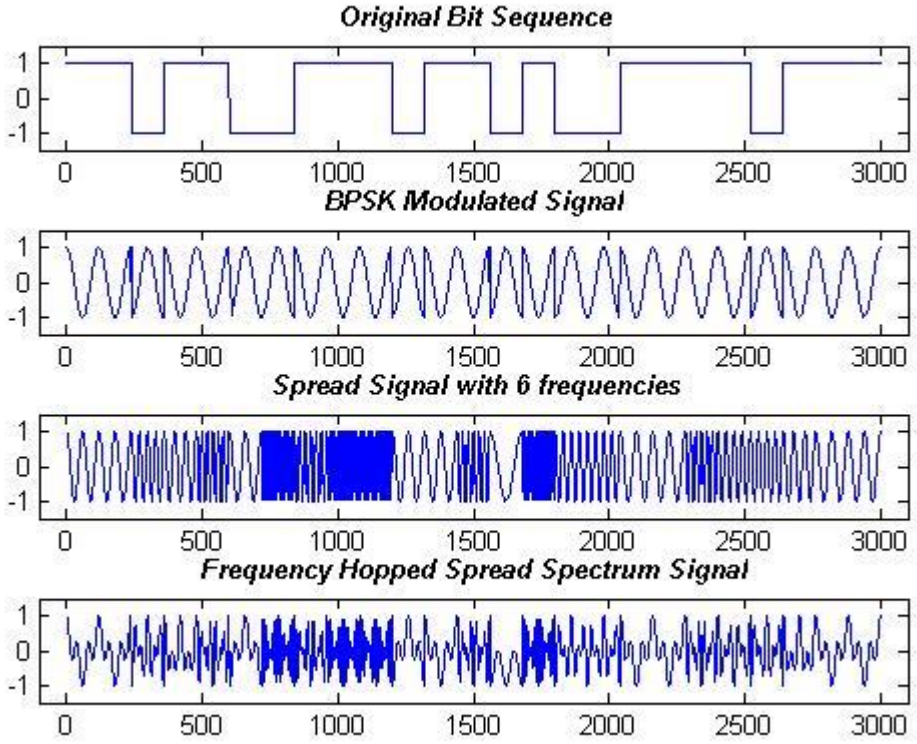
Spread spectrum due to chipping technique

Frequency Hopping Spread Spectrum (FHSS)

Rozprestretie spektra frekvenčnými skokmi

- Prenáša rádiové signály rýchlym **prepínaním** nosného signálu medzi mnohými frekvenčnými kanálmi
- Vysielač a prijímač musia byť **synchronizované**
  - aby „vedeli“, na ktorý kanál majú skočiť
  - synchronizácia pseudonáhodných generátorov
  - synchronizácia momentov prechodu medzi frekvenciami
- Používa sa v pôvodnom štandarde **802.11**

- Vysielač a prijímač prechádzajú medzi frekvenciami v danom kanáli podľa istej **pseudonáhodnej** postupnosti
  - Sekvencia obsahuje až 78 frekvencií
  - Vysielač medzi frekvenciami rýchlo skáče (hopping)
    - Získa sa lepšie rozprestretie a využitie kanála

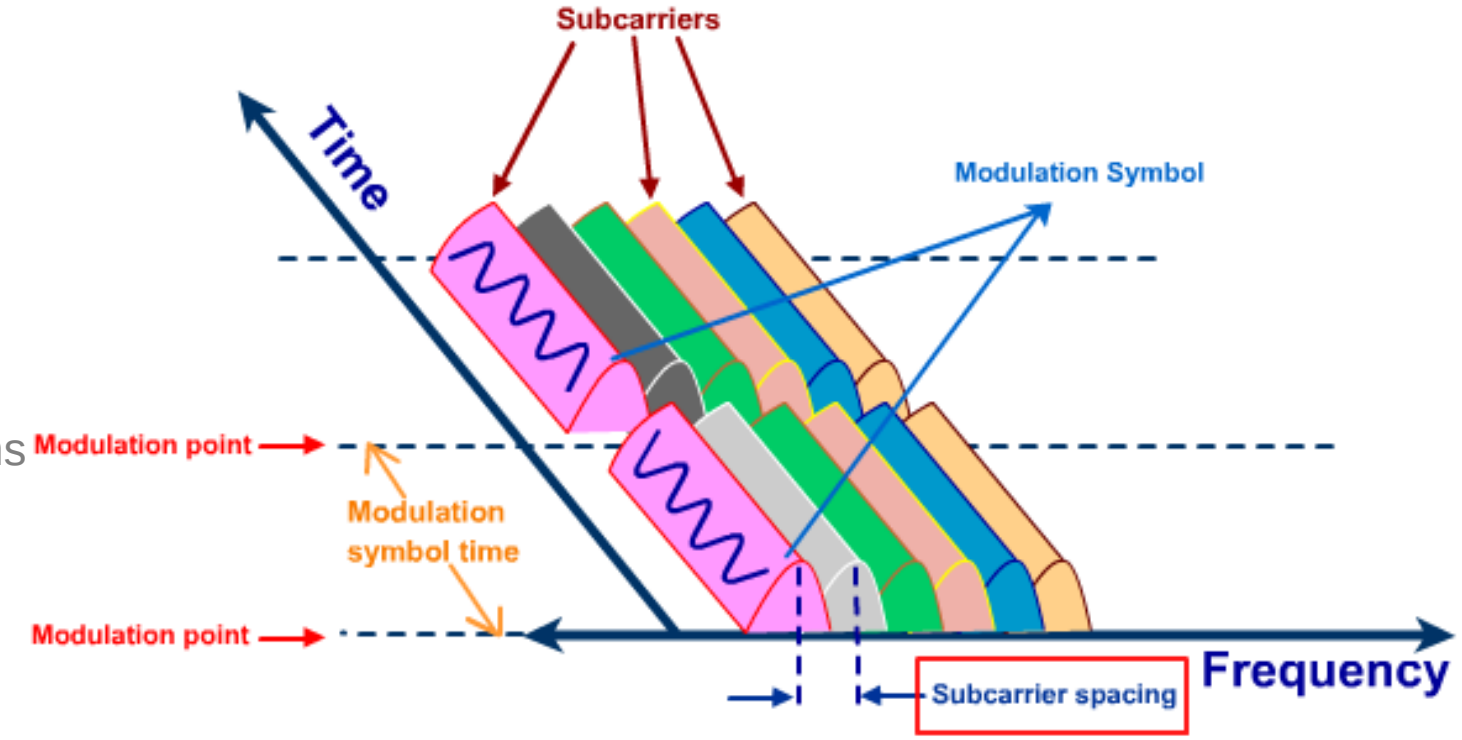


- V každom časovom **momente** sa využíva **len jedna** konkrétna frekvencia
  - Ak prenos rámca zlyhá, rámec sa prenesie znovu ale na inej frekvencii (next hop)

Orthogonal Frequency Division Multiplexing (OFDM)

Multiplex s ortogonálnym frekvenčným delením

- Podmnožina multiplexovania s frekvenčným delením
- Rodina modulačných techník, ktoré využívajú **rozdelenie kanála** na tzv. **subkanály** (na susedných frekvenciách) a simultánny prenos informácie týmito kanálmi
- Komplexná technika využívaná vo vysokorýchlostných prenosoch
- Používaná v:
  - 802.11a/g/n/ac
  - Ale aj pre:
    - DSL
    - WiMAX – 802.16
    - digital audio/video broadcast systems
    - air interface evolution of 3G Wireless systems based on 3GPP and 3GPP2



IEEE štandardy pre WLAN

IEEE WLAN štandardy

Štandard 802.11a

- Pôvodne menej známy a menej používaný štandard, z r. 1999
- Teoretická maximálna prenosová rýchlosť **54 Mbps**
  - fallback na 48, 36, 24, 18, 12, 9 a 6 Mbps
  - využíva frekvenčné pásmo **5 GHz**
- Kanály sú vzdialené od seba 5 MHz
- Kanál má šírku 20 MHz a je rozdelený na 64 podkanálov, každý o šírke 312.5 kHz, 4 podkanály sú pilotné, 12 nepoužitých
- Využíva technológiu **OFDM**
- Reálna prenosová rýchlosť: cca **25 Mbps**
- Kratší dosah
  - Väčšia absorpcia materiálom múrov
- **Nekompatibilné** s 802.11b

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	draft 6.0 (11/2020)	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

IEEE WLAN štandardy

Štandard 802.11b

- Kedysi populárny a široko nasadzovaný štandard
- Relatívna cenová dostupnosť 802.11b zariadení naštartovala boom WLAN sietí
- Teoretická maximálna prenosová rýchlosť **11 Mbps**
  - fallback na 5.5, 2 a 1 Mbps
  - využíva frekvenčné pásmo **2.4 GHz**
- Kanál má šírku 22 MHz, odstup kanálov 5 MHz, EU povoľuje použitie kanálov 1—13
- Využívané techniky **DSSS**, DBPSK, DQPSK
- Reálna prenosová rýchlosť: cca **5 Mbps**
- Väčší dosah

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps /5	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	draft 6.0 (11/2020)	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

IEEE WLAN štandardy

Štandard 802.11g

- Teoretická maximálna prenosová rýchlosť **54 Mbps**
  - Fallback na 48, 36, 24, 18, 12, 9 a 6 Mbps alebo úplne na 802.11b štandard
  - Využíva frekvenčné pásmo **2.4 GHz**
  - Používa **OFDM**
- Reálna prenosová rýchlosť: cca **27 Mbps**
- Kanály a ich odstup sú identické ako v 802.11b
- Spätne plne kompatibilný s 802.11b
  - V sieti môžu byť **kombinované** 802.11**b** a 802.11**g** prvky
  - Každý bude komunikovať na vlastnej rýchlosti
  - Celkový prenosový výkon bude o niečo znížený

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps /5	450 ft.
802.11g	2003	2.4 GHz	54 Mbps /27	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	draft 6.0 (11/2020)	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

IEEE WLAN štandardy

Štandard 802.11n

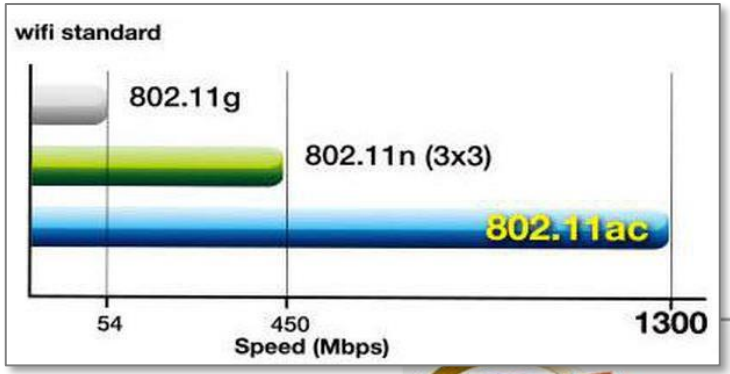
- Zatiaľ posledný štandard pre WLAN od IEEE
  - Dlhé roky draft
  - Niektorí výrobcovia predávali zariadenia založené na draft verzii 802.11n štandardu
- Vlastnosti:
  - Spätne kompatibilný s predchádzajúcimi verziami
  - Využitie viacerých antén pre vysielanie a príjem (Multiple Input Multiple Output, MIMO)
  - Pracuje na frekvenčných pásmach 2.4/5 GHz
  - Nárast teoretickej prenosovej 600 Mbps, reálna prenosová rýchlosť cca **74 Mbps**
- Dlhší dosah, cca 70 metrov

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps /5	450 ft.
802.11g	2003	2.4 GHz	54 Mbps /27	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps /230	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	draft 6.0 (11/2020)	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

IEEE WLAN štandardy

Štandard 802.11ac

- pracuje iba na frekvencii 5 GHz
- ale je spätne kompatibilný so štandardmi 802.11b/g/n aj na frekvencii 2,4 GHz
- teoretická priepustnosť je až 1 Gbps
- Rozdelený na 2 fázy
  - Wave 1 – SU MIMO (Single User)
  - Wave 2 – MU MIMO (ale iba downlink) (Multi User)
    - max 4x4, WiFi 5
    - Každý user má jeden kanál, preto zariadenie používa CSMA/CA mechanizmus na vyhnutie sa kolíziám



IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps /5	450 ft.
802.11g	2003	2.4 GHz	54 Mbps /27	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps /230	825 ft.
802.11ac	2014	5 GHz	1 Gbps /3,5	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	draft 6.0 (11/2020)	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

IEEE WLAN štandardy

Štandard 802.11ax (Wi-Fi 6)

- pracuje iba na frekvencii 5 GHz
- ale je spätne kompatibilný so štandardmi 802.11b/g/n aj na frekvencii 2,4 GHz
- teoretická priepustnosť je až 1 Gbps

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps /25	400 ft.
802.11b	1999	2.4 GHz	11 Mbps /5	450 ft.
802.11g	2003	2.4 GHz	54 Mbps /27	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps /230	825 ft.
802.11ac	2014	5 GHz	1 Gbps /3,5	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	draft 8.0 (11/2020) predic. 02/21	2.4/5 GHz	10 Gbps /9,6	1,000 ft.
802.11ay	draft 6.0 (11/2020) predic. 03/21	60 GHz	100 Gbps	300-500 m.
802.11az	draft 2.4 (10/2020) predict. 12/20	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

too old

too slow

too new

ba

...

Nová generácia?
Sľubné, ale .. malý dosah

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

If the most advanced technology a device supports is ...	Then it shall be identified as generation
802.11ax	Wi-Fi 6
802.11ac	Wi-Fi 5
802.11n	Wi-Fi 4

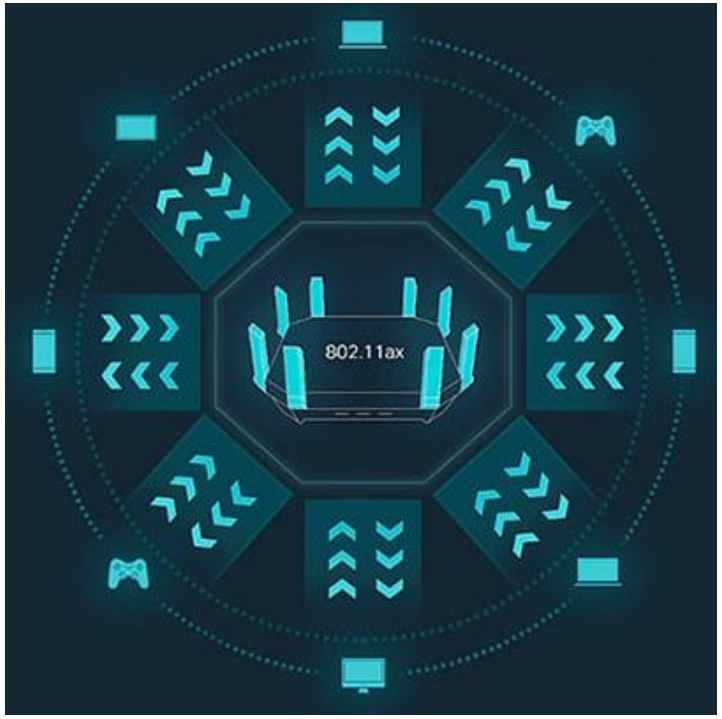
https://www.ieee802.org/11/Reports/802.11_Timelines.htm

Štandard 802.11ax (Wi-Fi 6) – **upgrade 1: MU-MIMO**

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

- MU MIMO
  - Aj pre downlink, aj uplink
  - Max 8x8
- WiFi 6

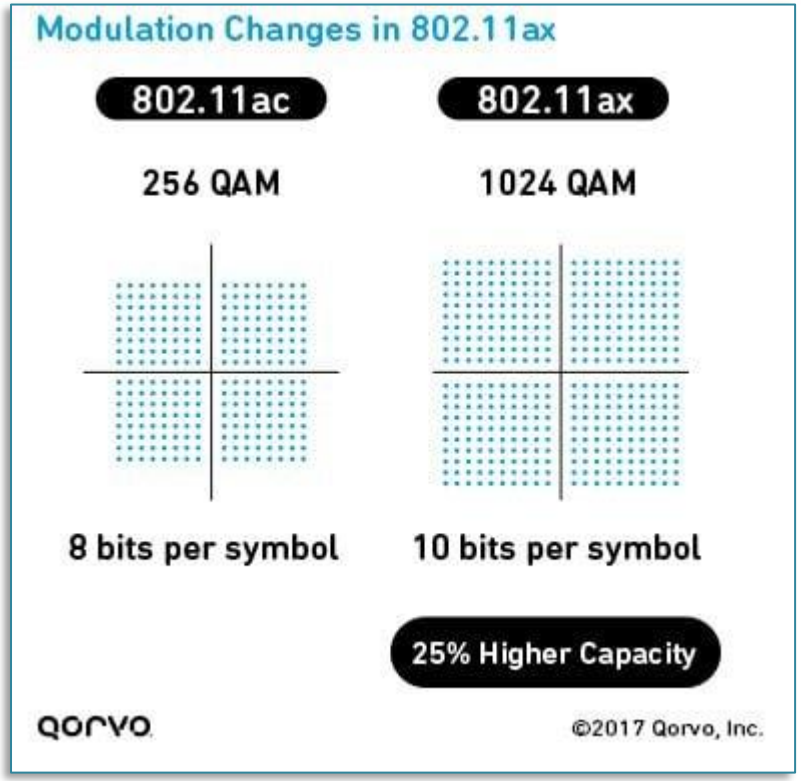


Štandard 802.11ax (Wi-Fi 6) – **upgrade 2: 1024-QAM**

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

- Čím vyšší QAM level, tým viac dát je možné obsiahnuť v signáli
- Väčšia dátová kapacita
  - O 25%
- Tým vyššia rýchlosť prenosu dát



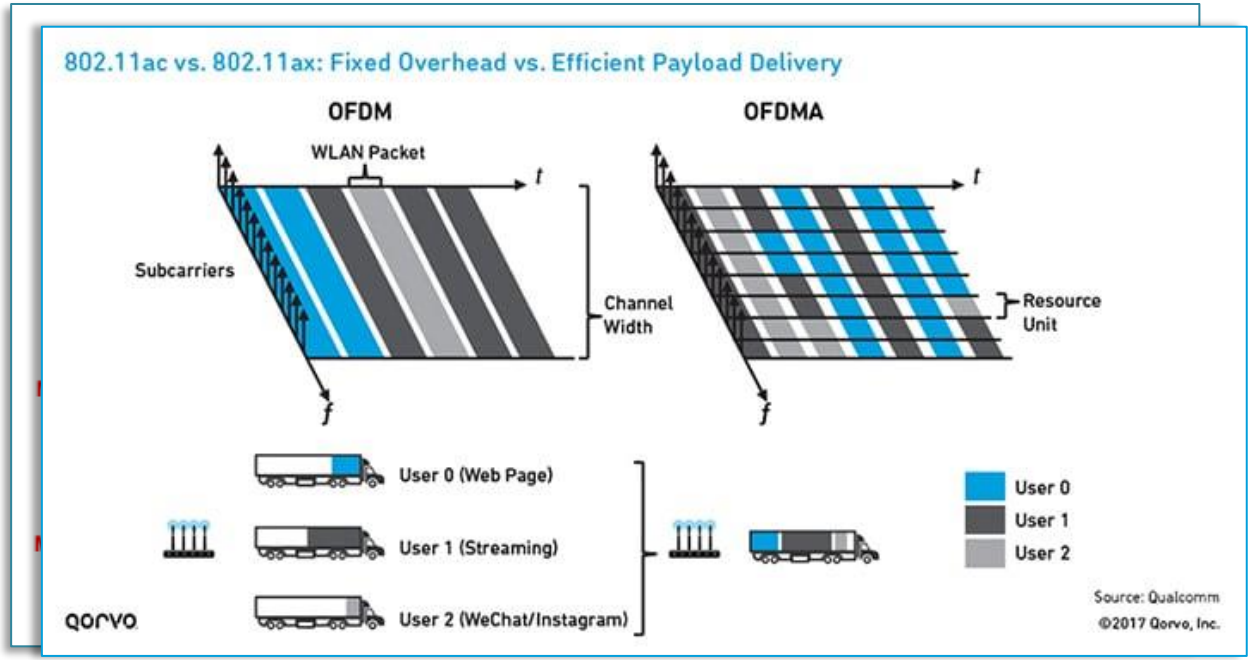
Štandard 802.11ax (Wi-Fi 6) – **upgrade 3: OFDMA**

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

Orthogonal Frequency Division Multiplexing (OFDM)

- OFDMA – technologické rozšírenie OFDM
- OFDM
  - každý user zaberá 1 kanál pri prenose dát
  - Bez ohľadu na to, koľko je to dát
  - A keď sa dáta pošlú, žiadny iný user nemôže využiť zvyšok nevyužitého pásma
- OFDMA
  - Rôzni users vedia zdieľať kanál, čím sa zníži aj response time..
  - Čím viac používateľov, tým to má väčší benefit

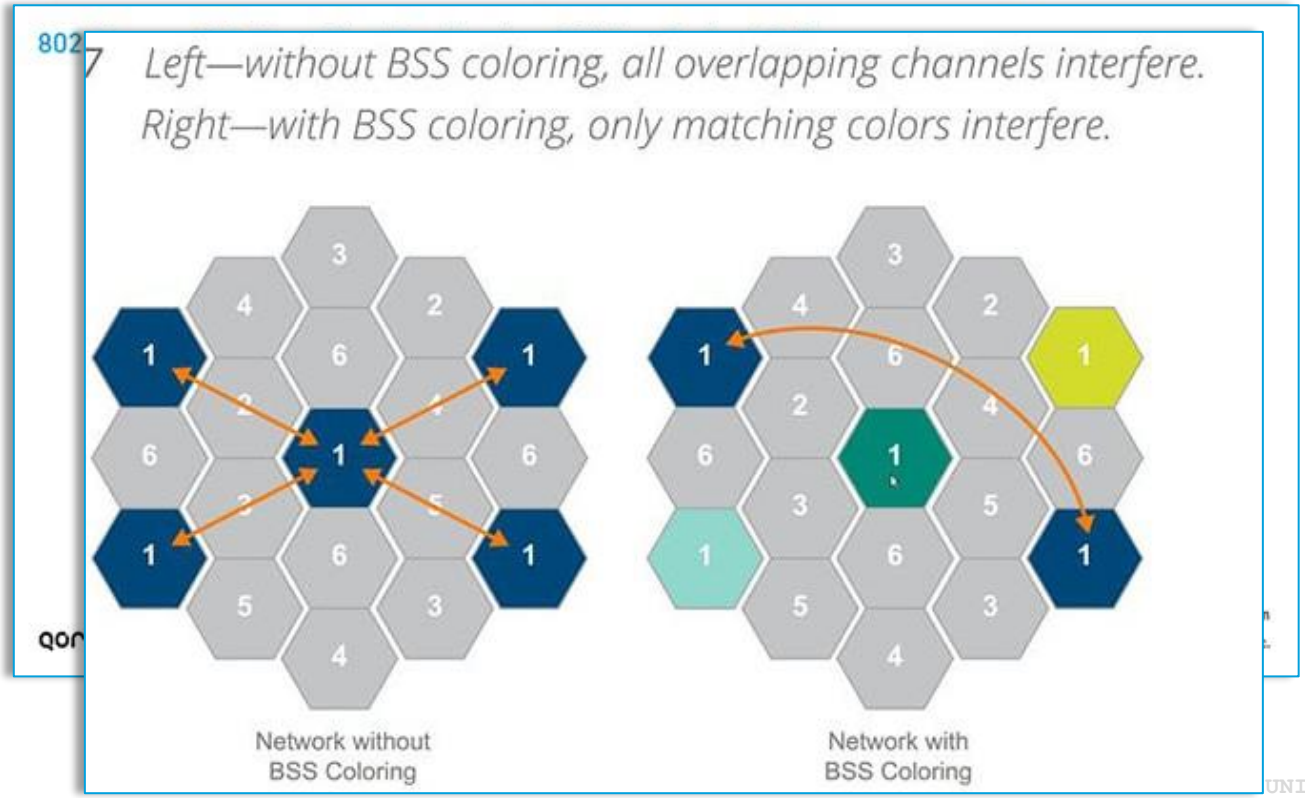


Štandard 802.11ax (Wi-Fi 6) – **upgrade 4: BSS coloring**

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

* *Depending upon number of spatial streams and channel used*

- Keďže OFDMA (Orthogonal Frequency Division Multiple Access), tak nemožno použiť CSMA/CA
  - userov v kanáli treba odlíšiť
  - Na to slúži BSS coloring
    - Individuálne sa označkuje zariadenie a následne pakety
    - A bude sa dať oddeliť komunikácia viac zariadení na jednom kanály

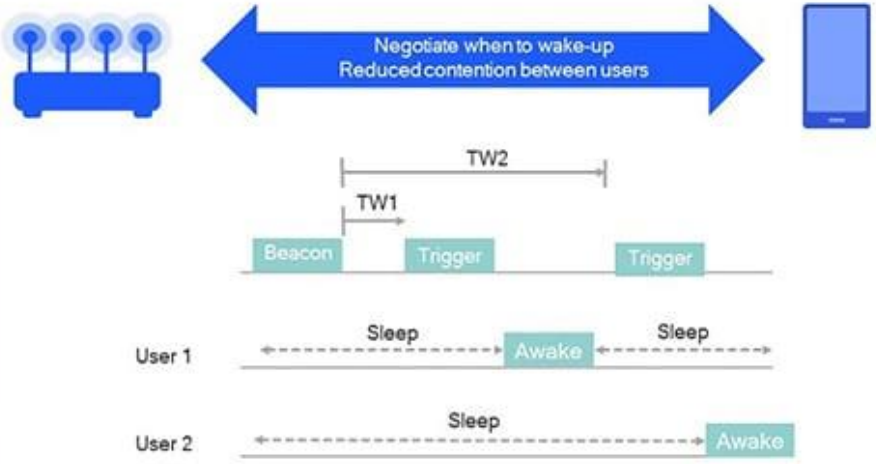


Štandard 802.11ax (Wi-Fi 6) – upgrade 5: **TWT mechanizmus**

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Channel bandwidth (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Frequency bands	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Maximum data rate	150 Mbps	3.5 Gbps*	9.6 Gbps*
Highest subcarrier modulation	64-QAM	256-QAM	1024-QAM
Spatial streams	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

** Depending upon number of spatial streams and channel used*

- Predošlé 4 funkcie riešili vysoký výkon Wi-Fi6
- Pre smart home a domáce smerovače, sa môžu objaviť aj pomalé zariadenia (2,4 GHz, 20Mhz)
- Pre ne sa implementuje TWT – Target wake-up mechanism
  - Aby sa viac zariadení nezobúdzalo naraz a nespôsobilo kolízie



WiFi aliancia

- Hoci štandard je daný, jeho implementácie sa môžu medzi výrobcami líšiť
  - Problém s interoperabilitou
  - Pomerne časté nepríjemnosti v začiatkoch WLAN sietí
- Skupina výrobcov založila skupinu WECA (Wireless Ethernet Compatibility Alliance), ktorá sa neskôr premenovala na **WiFi Alliance**
- Účelom aliancie je certifikovať interoperabilitu WLAN produktov
  - potom smú byť označené logom **WiFi Certified™**

Len na okraj...

Cisco Compatible Extensions (CCX)

- Cisco si zaviedlo vlastné rozšírenia do svojich bezdrôtových zariadení
- Spolu s tým zaviedlo aj vlastný certifikačný program CCX
  - Certifikuje spoluprácu výrobkov tretích strán s produktami Cisco

Komponenty a činnosť WLAN sietí

Nasadenie WLAN sietí predpokladá:

- Koncové zariadenia
- Zariadenia infraštruktúry

Komponenty WLAN

Bezdrôtový klient

- Koncová členská **stanica** WLAN siete
  - Jej konektivita je zabezpečená špecializovanou **bezdrôtovou sieťovou kartou** (NIC)
    - Obsahuje rádiový vysielač/prijímač
    - Existuje v rôznych vyhotoveniach s rôznymi **rozhraniami** (USB, Interný, PCMCIA)

Panda 300Mbps Wireless N **USB** Adapter

SUS **USB**-AC68 **Dual-Band**
C1900, 1300Mbps

TP-LINK TL-WN781ND 150MB Wifi **PCI Express** Adapter

Dual Band Wifi 1.73Gbps Wireless Card For Intel 9260 9260NGW 2.4G/5Ghz 802.11ac Wifi Bluetooth 5.0 Gigabit M.2 NGFF Wlan Card

802.11AC 1200Mbps Dual 5Dbi, 1200 Mbps

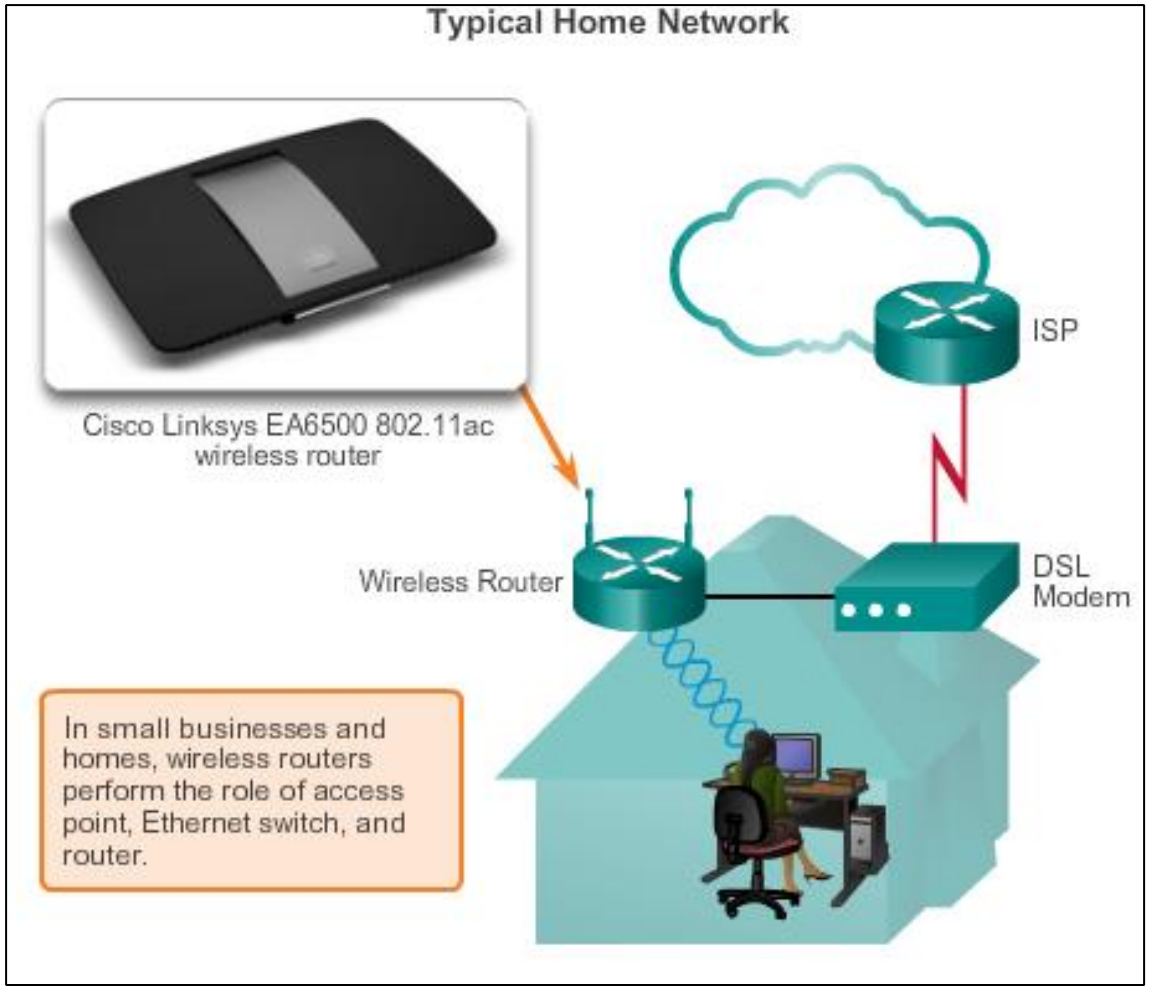
TP-Link TL-WN851N 300Mbps Wireless N **PCI** Adapter

300Mbps 802.11n MIMO Wireless LAN CardBus **PCMCIA** Adapter

Komponenty WLAN

Wireless Home Router

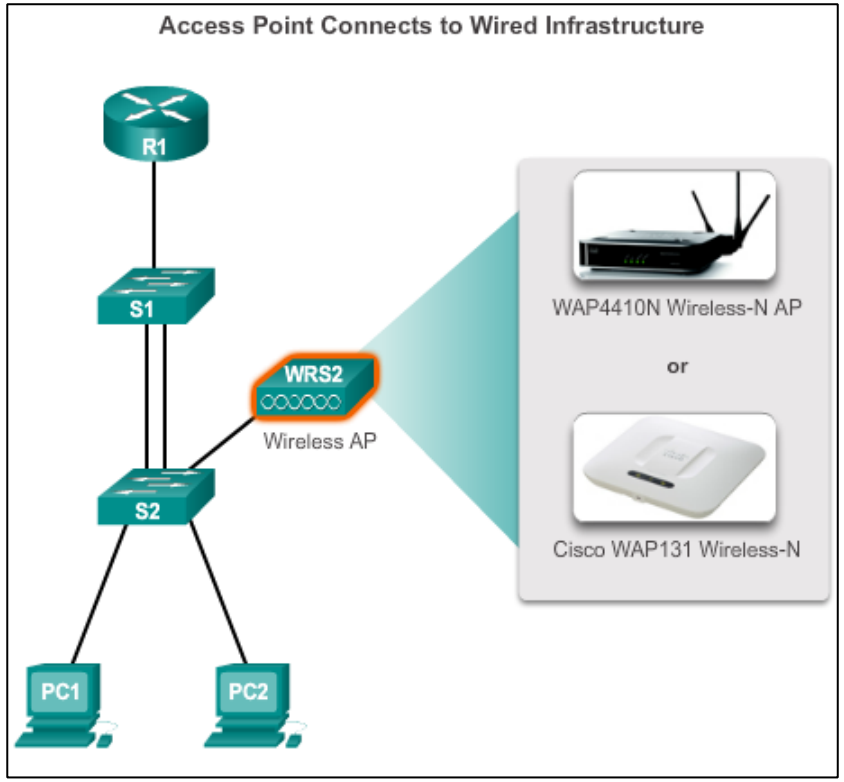
- Domáci používateľ skôr využíva **integrated wireless router**
  - Integruje v sebe viac zariadení
    - access point
      - Pre bezdrôtový prístup
    - Ethernet prepínač
      - Na káblové prepojenie zariadení
    - Smerovač (WAN rozhranie)
      - Default GW pre všetkých klientov



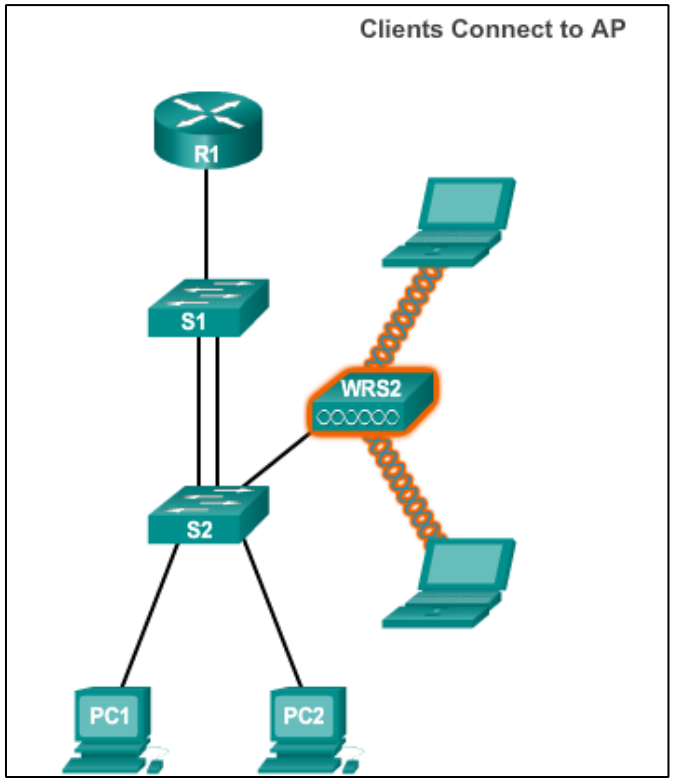
Prístupový bod – Access Point (AP)

- Typicky pripojený do siete metalickým médiom
- Zabezpečuje vzájomnú komunikáciu WLAN klientov a spojenie WLAN s LAN
- Klient sa musí s AP asociovať aby mal sieťovú službu

- Rôzne vyhotovenia pre vonkajšie/vnútorné inštalácie
- Rôzne kategórie nasadenia:
  - Autonómne APs
  - Controller-based APs

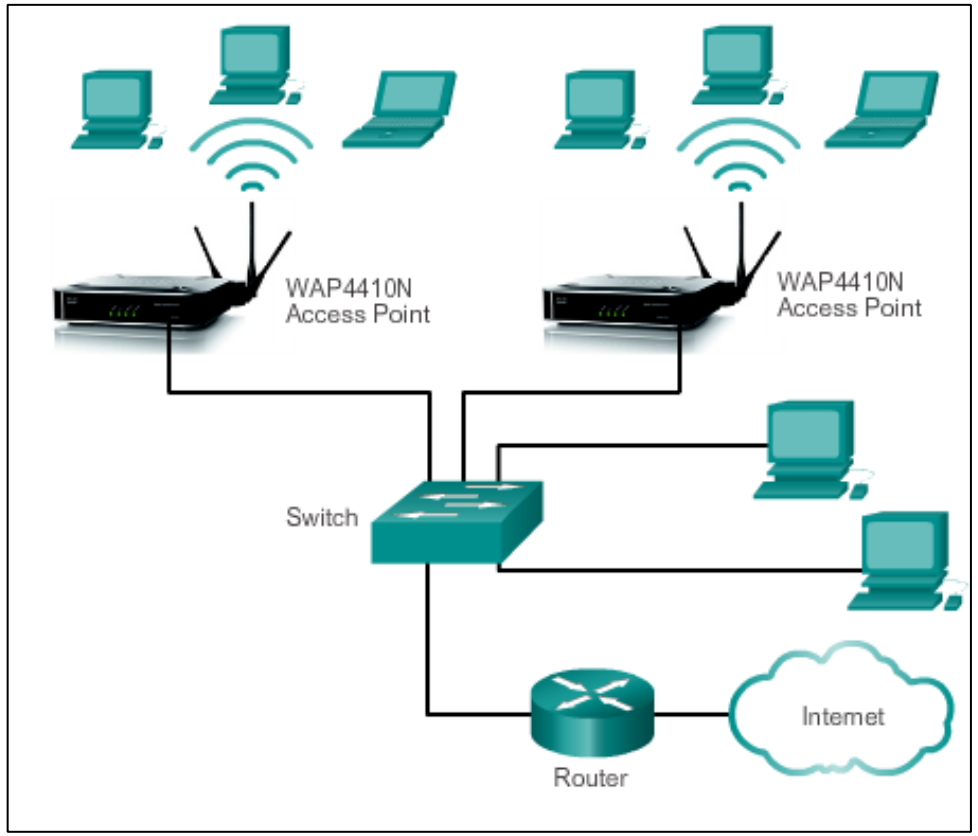


Cisco Meraki Go access points



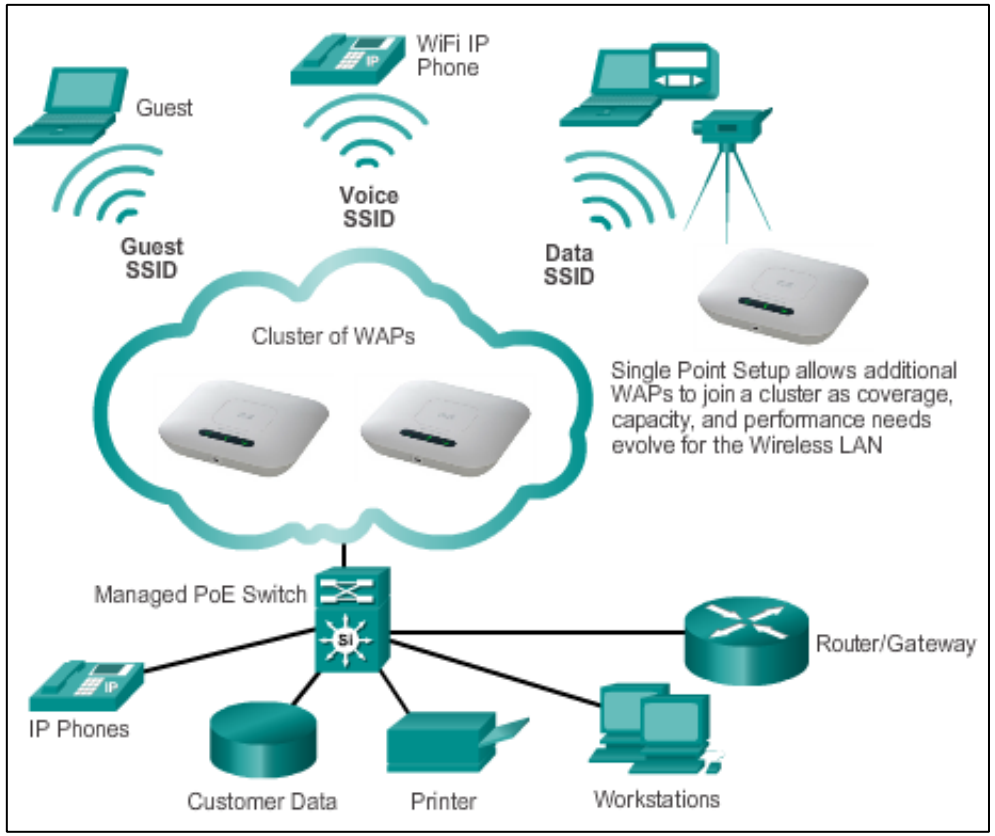
Autonómne APs

- Každé sa konfiguruje a spravuje individuálne, cez CLI, alebo GUI
- Problém ak je veľa AP



Autonómne APs

- Klastrovanie bez podpory kontroléra
  - Moderný trend
  - Viaceré AP
  - Riešené interferencie
  - Tlačíme jednotnú konfiguráciu na všetky AP v klastri
  - Riadime sieť jednotne

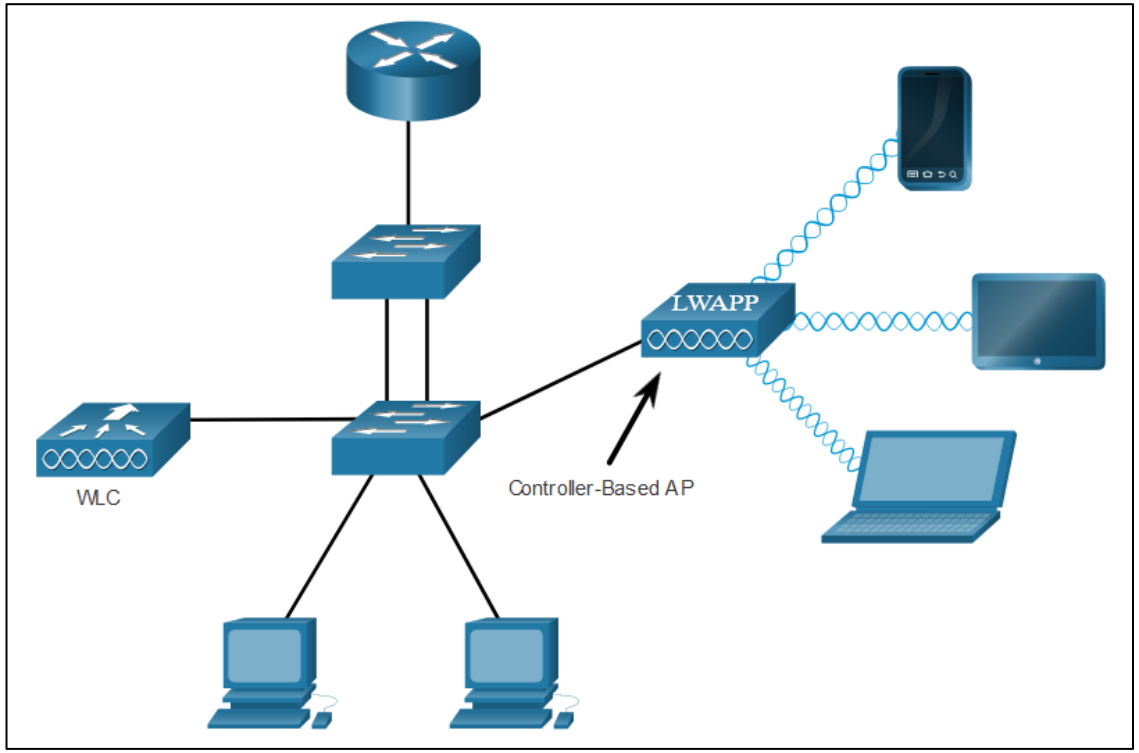


Cluster autonómnych APs

Riešenia pre veľké WLAN

Controller-base APs

- Označované aj ako lightweight
- Konfigurované a manažované z controllera
- Pre sieť s mnohými APs
- LWAPP - Lightweight Access Point Protocol
  - Pre komunikáciu APs s WLAN controllerom (WLC)



Komponenty WLAN

Bezdrôtové mosty

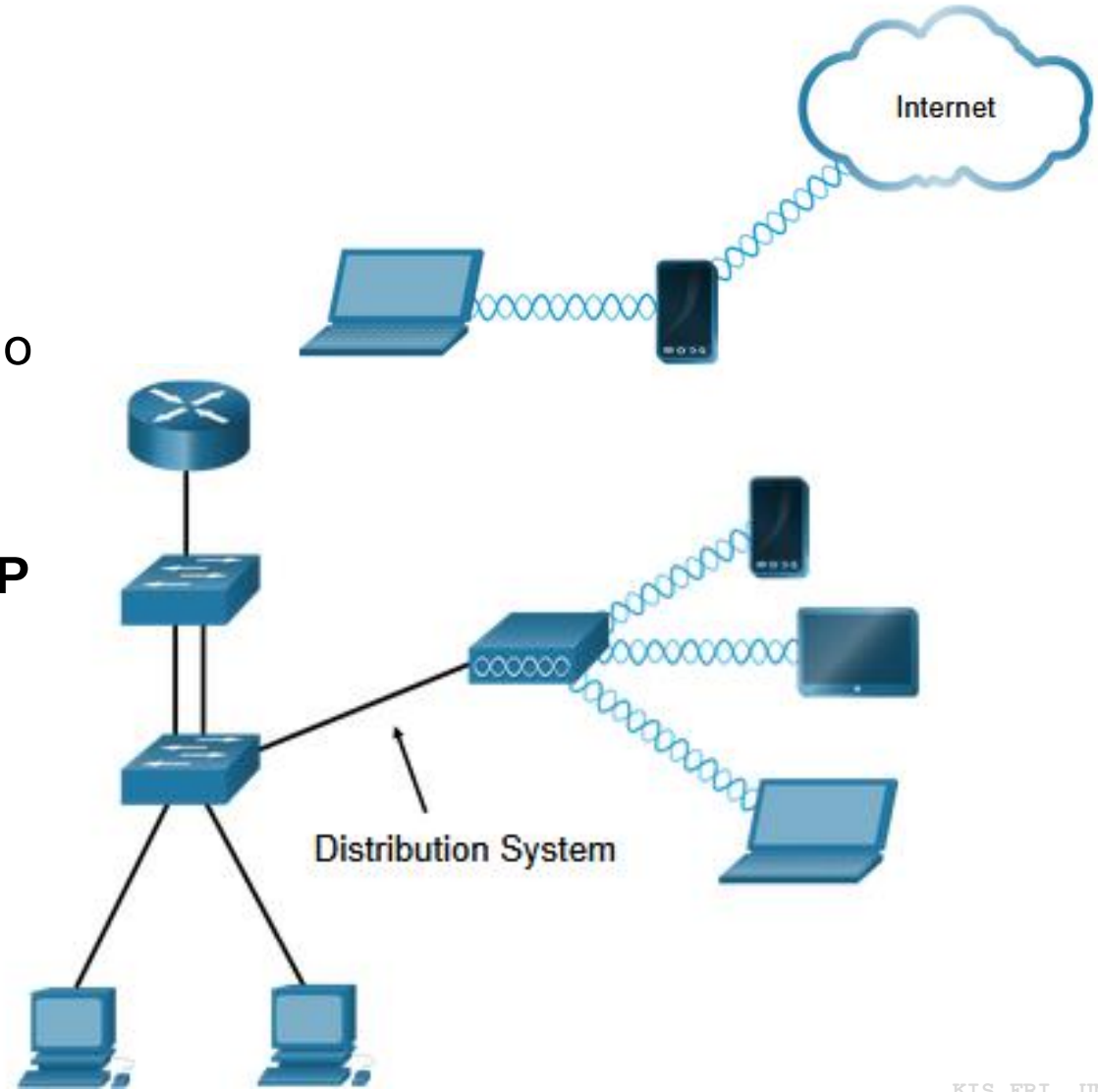
- **Most – bridge**
  - Zabezpečuje bezdrôtové **prepojenie dvoch separátnych** LAN sietí
  - Spojenia point-to-point alebo point-to-multipoint
  - Mosty častokrát používajú mierne **upravený** komunikačný **protokol** pre efektívnejšiu komunikáciu
- Opakovač – repeater
  - Zabezpečuje **zväčšenie plochy** pokrytej **signálom**
  - Jeho použitie výrazne **znižuje** efektívnu prenosovú **rýchlosť**
  - Pri využití repeaterov je potrebné **50% prekrytie** tzv. catchment area
- **Antény**
  - Rôzne druhy
    - všesmerové (domácnosti), sektorové, smerové (Yagi, parabol.)
    - MIMO (Multiple Input Multiple Output) – viacero antén (8)
  - Líšia sa použitým druhom konektora, káblom, ziskovosťou, smerovosťou...
  - Cisco zariadenia používajú konektory RP-TNC

Spôsoby prevádzky WiFi

WLAN Operation

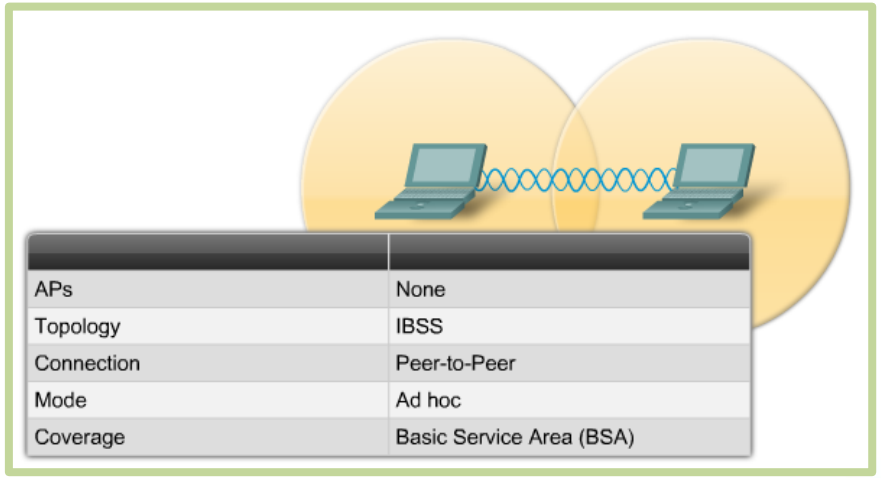
Základné topológie WLAN sietí

- **Ad hoc mód**
  - Na prepojenie klientov **peer-to-peer** bez AP
- **Tethering**
  - Variant ad hoc módu, keď mobilný smart telefón alebo tablet s bunkovým prístupom do internetu, sa použije ako osobný hotspot
- **Mód infraštruktúra**
  - Na prepojenie klientov do siete **pomocou AP**

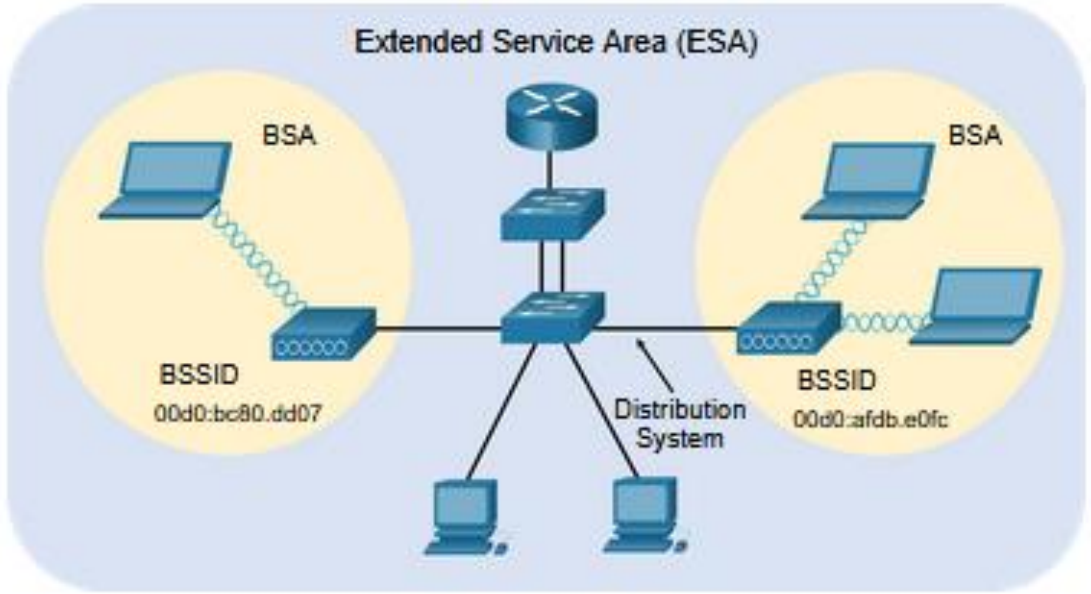


Základné topológie WLAN sietí

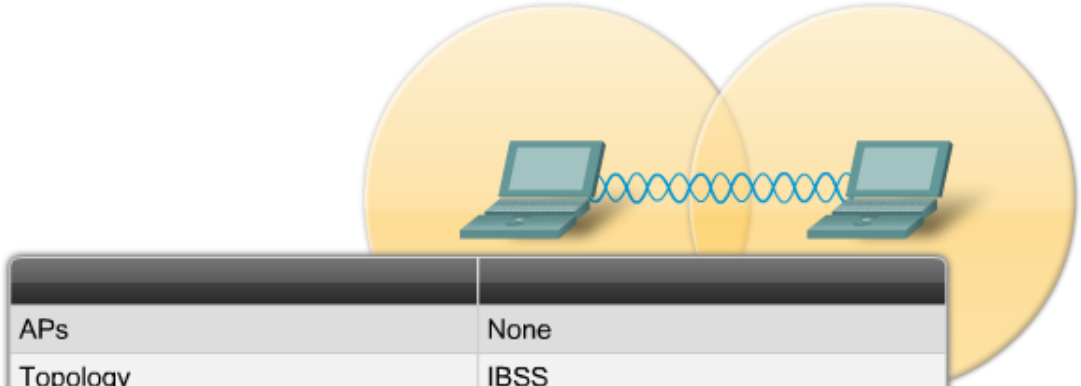
- **Ad hoc mód**
  - Na prepojenie klientov **peer-to-peer** bez AP
  - Topológia sa označuje ako IBSS (Independent Basic Service Set)
- **Tethering**
  - Variant ad hoc módu, keď mobilný smart telefón alebo tablet s bunkovým prístupom do internetu, sa použije ako osobný hotspot
- **Mód infraštruktúra**
  - Na prepojenie klientov do siete **pomocou AP**
  - Definuje 2 topologické bloky:
    - BSS (Basic Service Set)
      - Používa AP na pripojenie klientov
      - Klienti v rôznych BSS nemôžu komunikovať
    - ESS (Extended Service Set)
      - Viacero BSS prepojených tzv- distribučným systémom (káble, prepínače, ..)



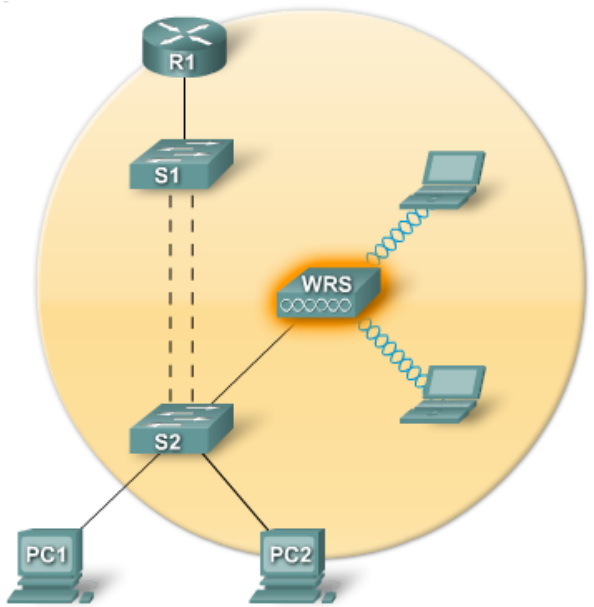
APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)



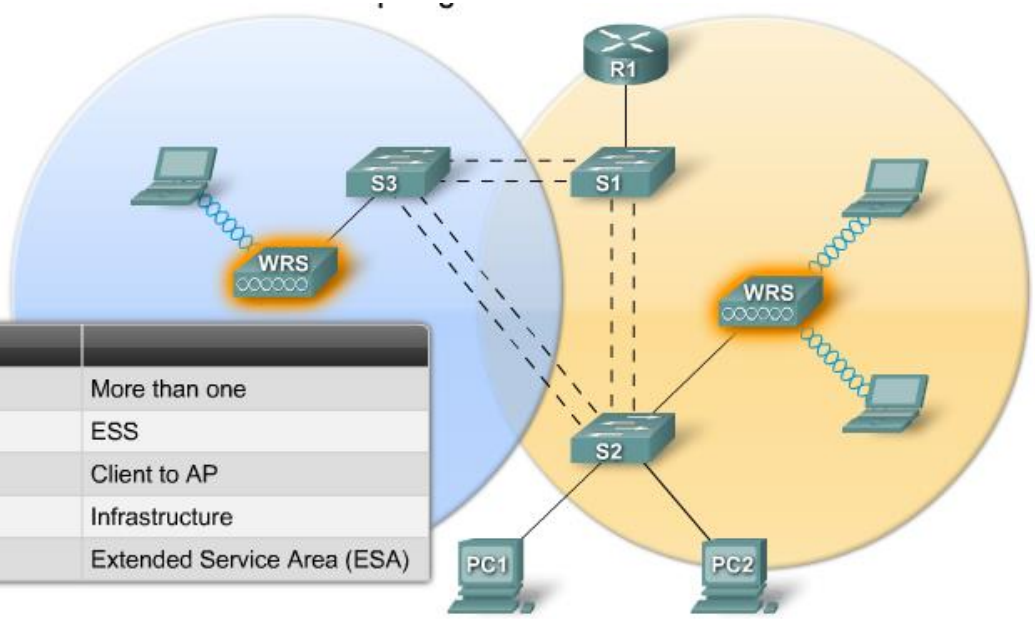
Topológie IBSS, BSS, ESS - zhrnutie



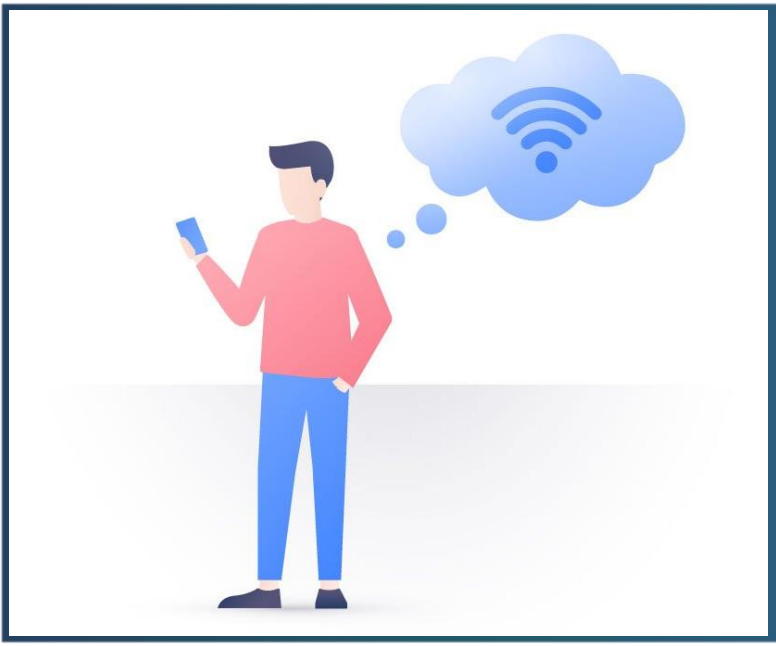
APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)



APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)



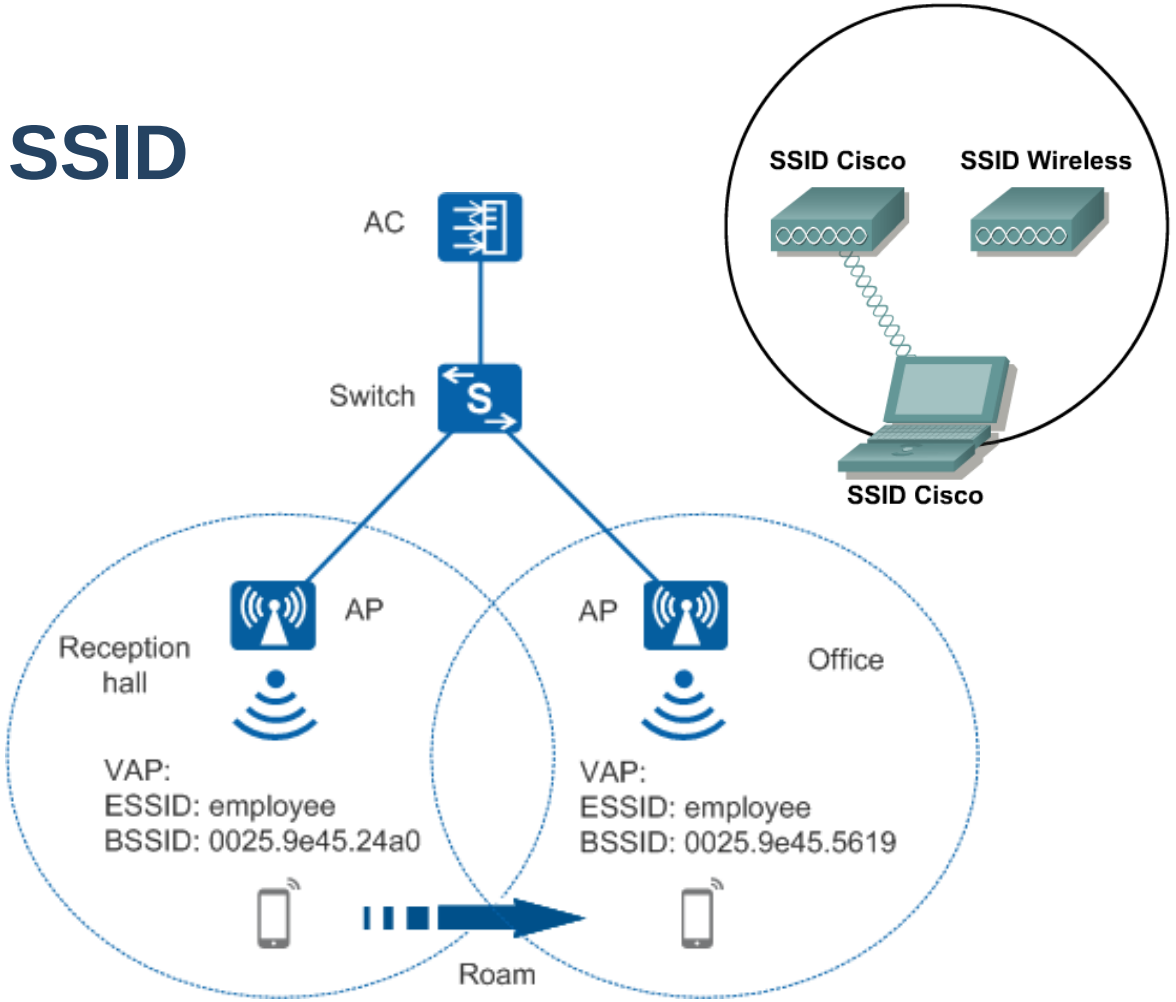
APs	More than one
Topology	ESS
Connection	Client to AP
Mode	Infrastructure
Coverage	Extended Service Area (ESA)



Wireless LAN činnosti

Identifikátor bezdrôtovej siete – SSID

- V jednom priestore môže byť dostupných niekoľko BSS alebo ESS
  - Identifikátor konkrétnej WLAN siete:
    - Service Set ID, tzv. **SSID** (resp. Extended SSID, **ESSID**)
    - SSID je základným parametrom WLAN klienta pristupujúceho k WLAN sieti
    - je **slovný názov** bezdrôtovej siete
    - AP môže SSID vysielať vo svojich tzv. beacon rámcoch
    - SSID môže byť aj skryté
- V jednej ESS sa môže klient asociovať k rôznym prístupovým bodom
  - Identifikátor konkrétneho prístupového bodu:
    - Base Service Set ID, **BSSID**
    - BSSID má formu **MAC adresy**



- Jeden AP môže navonok prezentovať niekoľko SSID
  - Každé SSID má samostatnú VLAN
  - AP využíva trunking a 802.1Q značkovanie na roztriedenie rámcov medzi SSID/VLAN

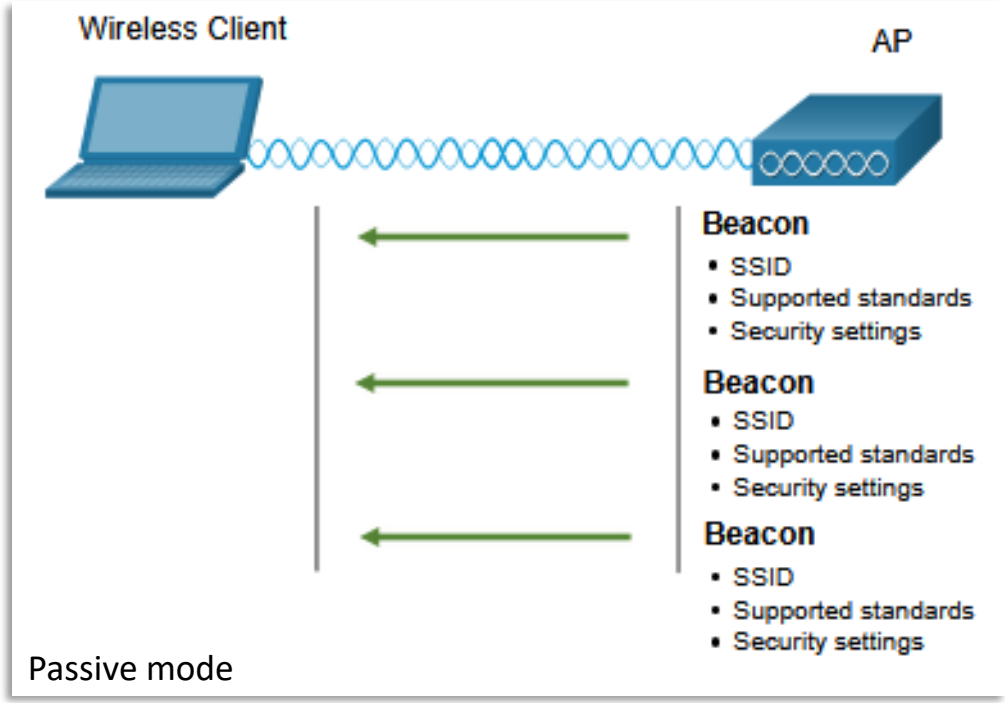
Spôsob objavenia AP klientom

Passive mode

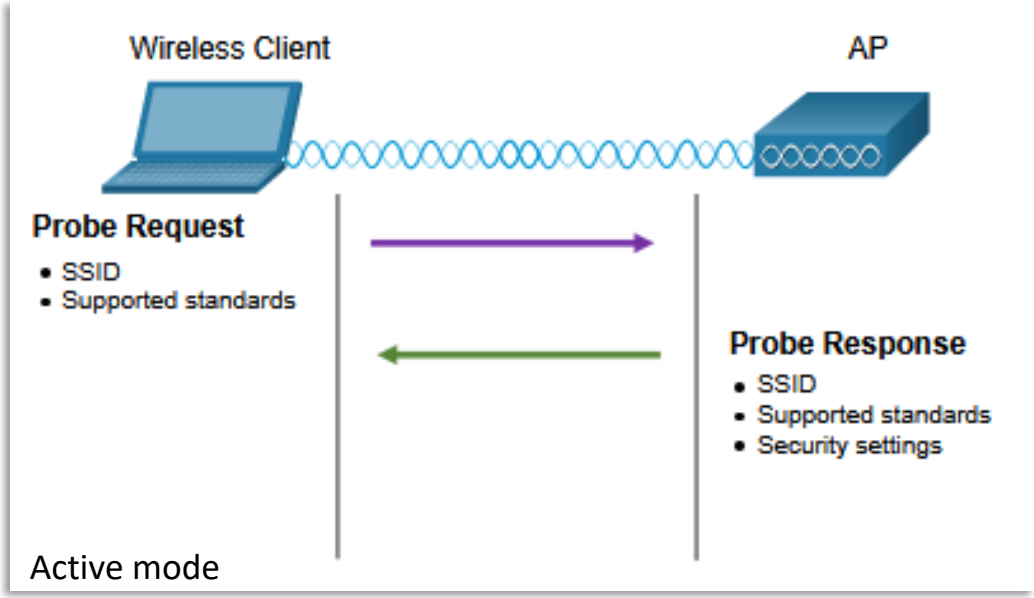
- AP ohlasuje jeho služby posielaním broadcast rámcov nazývaných beacons
- Rámce obsahujú SSID, podporované štandardy, bezpečnostné nastavenia.
- Hlavná úloha Beacons
  - Dať vedieť klientom o APs v oblasti

Active mode

- Wireless client musí vedieť meno SSID kam sa chce pripojiť
- Klient iniciuje proces poslaním PROBE požiadavky na viacerých kanáloch
  - Probe request obsahuje SSID a podporované štandardy klienta.
- Tento postup je nevyhnutný ak AP neposiela beacons



Passive mode



Active mode

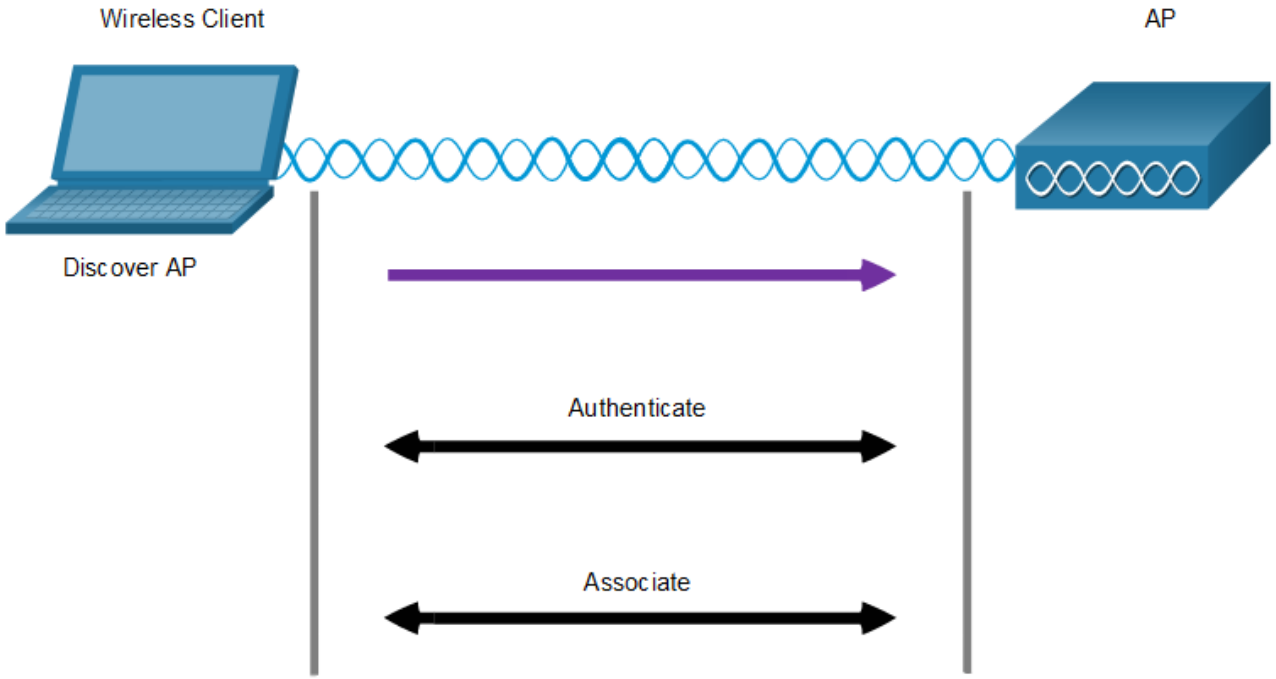
Komunikácia vo WLAN sieti

Proces prístupu klienta k WLAN má 3 fázy:

1. Objav AP
2. Autentifikuj sa voči AP (Open, Shared key)
3. Asociuj sa s AP

Stavy klienta:

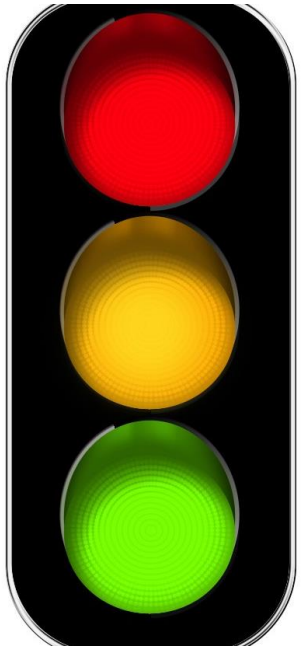
- Unauthenticated, Unassociated
  - Východzí stav
- Authenticated, Unassociated
  - Klient preukázal voči sieti svoju identitu, ale nie je trvale prihlásený k zvolenému prístupovému bodu
- Authenticated, Associated
  - Klient je prihlásený (asociovaný) ku konkrétnemu prístupovému bodu a má plnú konektivitu



Potrebná dohoda na parametroch:

- SSID
- Heslo (Shared Key)
- Network mode (802.11. štandard)
- Security mode (WEP, WPA, WPA2, ..)
- Channel settings (frekvenčné pásmo)

CSMA/CD
COLLISION DETECTION



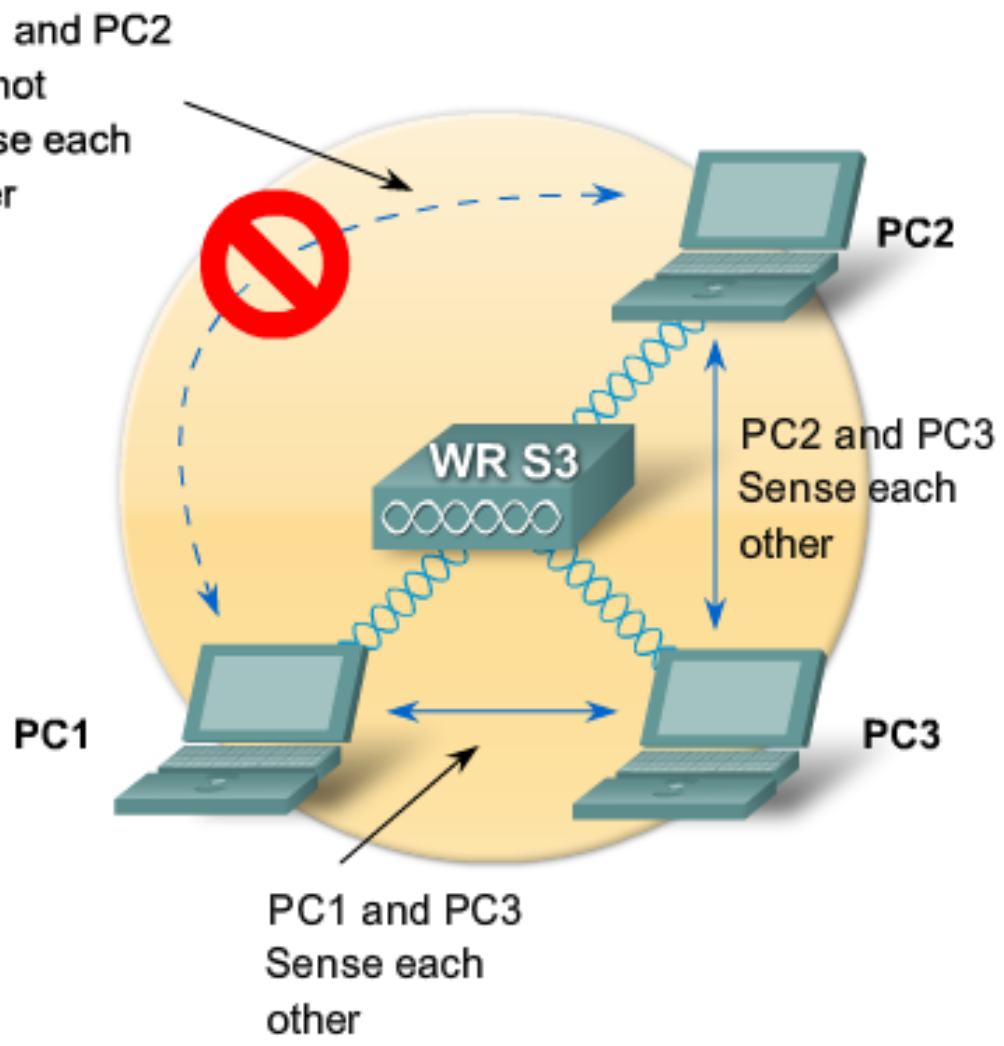
CSMA/CA
COLLISION AVOIDANCE

Komunikácia vo WLAN

CSMA/CA

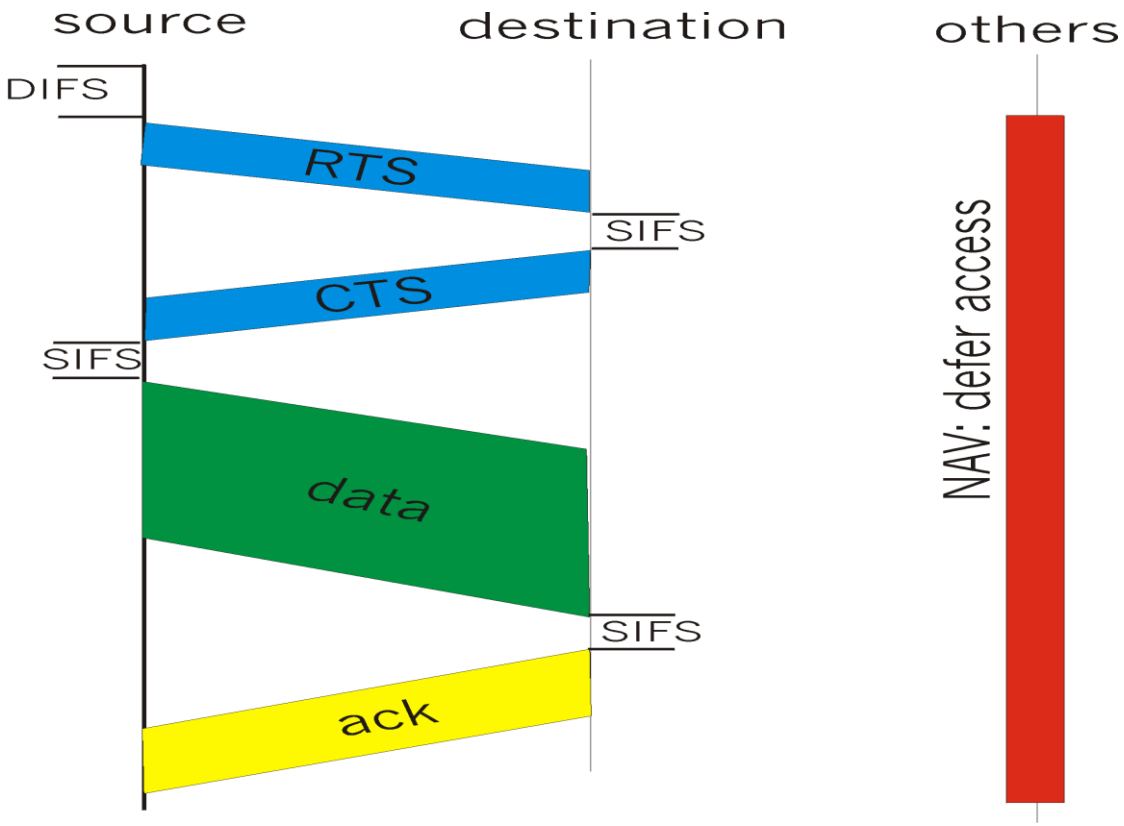
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

- Vo WLAN nemôžem použiť CSMA/CD
  - Iba CSMA – to pracuje vo WLAN dobre
    - ak som jediný čo prenáša, resp. vidím/počujem ak komunikuje niekto iný
  - Avšak CD pre WLAN nefunguje
    - Odosielajúca stanica nevie zistiť, či spôsobila kolíziu
    - Buď vysielam, alebo prijímam, neviem obe naraz na rádiu (half-duplex)
    - "Hidden node" problem
- Preto pre WLAN máme modifikáciu klasickej CSMA metódy
  - Vyhnutie sa kolíziií (CA)
    - Distribuovaná koordinačné funkcia (DCF)
    - RTS/CTS
- Prijímajúci host posiela ACK krátko po prijatí správy (Short IFS)
- Ak ACK nie je prijaté => znovu prenos



IEEE 802.11 RTS/CTS

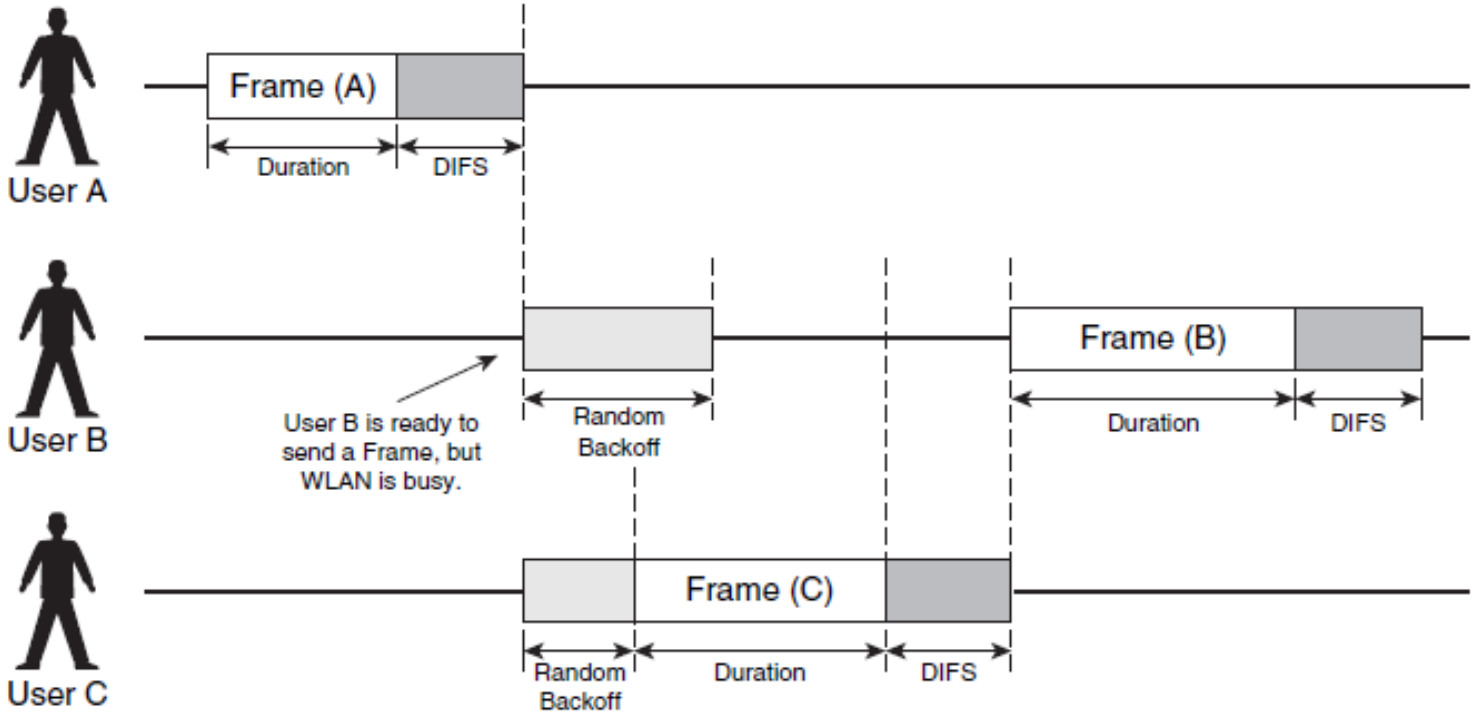
- Doplnenie CSMA/CA
- Odstraňuje problém skrytého uzla
- Request To Send (RTS)
  - Dohľadový rámec, v ktorom stanica informuje príjemcu, že mu chce poslať dáta, a informuje o potrebnom čase na tento prenos
- Clear To Send (CTS)
  - Dohľadový rámec, v ktorom príjemca potvrdzuje príjem žiadosti RTS a informuje o potrebnom zvyšnom čase na tento prenos
- Výmena inštruuje všetky uzly v dosahu odosielateľa a prijímateľa dodržať ticho a nekomunikovať



Komunikácia CSMA/CA (1.)

- Pri prenose so systémom CSMA/CA môžu nastať dve situácie
  - Nikto neprenáša (carrier sense)
    - Po poslednom rámci prenášanom v danej sieti počkaj určitú dobu,
      - tzv. DCF Interframe Space (DIFS)
        - Ak počas DIFS niekto začne vysielať – odklad prenosu
    - A prenes celý svoj rámec
      - A počkaj na potvrdenie o prijatí od príjemcu (po Short IFS)
  - Iné zariadenie prenáša rámec
    - Stanica musí počkať kým sa skončí prenos + DIFS + náhodný čas
      - Náhodný čas sa skracuje/predlžuje podľa úspešnosti prenosu
    - Ako stanica vie ako dlho potrvá prenos (rozdielna dĺžka rámca)?
      - Buď sa všetky stanice počujú navzájom
        - Fyzická detekcia aktivity kanála – pozor „hidden node problem“
      - Alebo sa využije RTS/CTS mechanizmus, v ktorom sa v správach RTS a CTS uvádza odhadované trvanie prenosu
        - Virtuálna detekcia

CSMA/CA – Distributed Coordination Function (DCF)



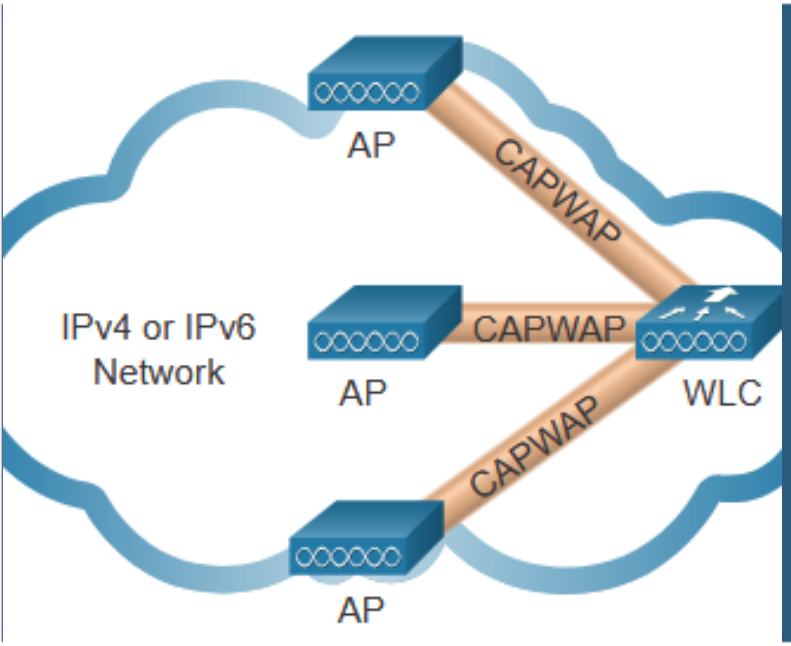
1. *A* počúva a zistí, že nikto neprenáša, prenesie rámec. Zároveň dá info o dobe trvania prenosu.
2. *B* má rámec na prenos, ale musí počkať kým skončí *A* + kým uplynie DIFS čas
3. *B* počká náhodný backoff čas kým sa pokúsi znova preniesť frame.
4. Kým B čaká, objaví sa C, ktorý chce tiež prenášať rámec. Detekuje a zistí, že nik neprenáša, *C* počká náhodný čas, ktorý je kratší ako náhodný čas B
5. C prenesie rámec a zároveň dá info o dobe trvania prenosu
6. B teraz musí počkať dobu prenosu rámca C + DIFS kým sa pokúsi preniesť svoj rámec opäť

Komunikácia CSMA/CA (2.)

- Pri prenose so systémom CSMA/CA môžu nastať dve situácie
  - Nikto neprenáša (carrier sense)
    - Po poslednom rámci prenášanom v danej sieti počkaj určitú dobu,
      - tzv. DCF Interframe Space (DIFS)
        - Ak počas DIFS niekto začne vysielať – odklad prenosu
    - A prenes celý svoj rámec
      - A počkaj na potvrdenie o prijatí od príjemcu (po Short IFS)
  - Iné zariadenie prenáša rámec
    - Stanica musí počkať kým sa skonči prenos + DIFS + náhodný čas
      - Náhodný čas sa skracuje/predlžuje podľa úspešnosti prenosu
    - Ako stanica vie ako dlho potrvá prenos (rozdielna dĺžka rámca)?
      - Buď sa všetky stanice počujú navzájom
        - Fyzická detekcia aktivity kanála – pozor „hidden node problem“
      - Alebo sa využije RTS/CTS mechanizmus, v ktorom sa v správach RTS a CTS uvádza odhadované trvanie prenosu
        - Virtuálna detekcia

Poznámky na okraj

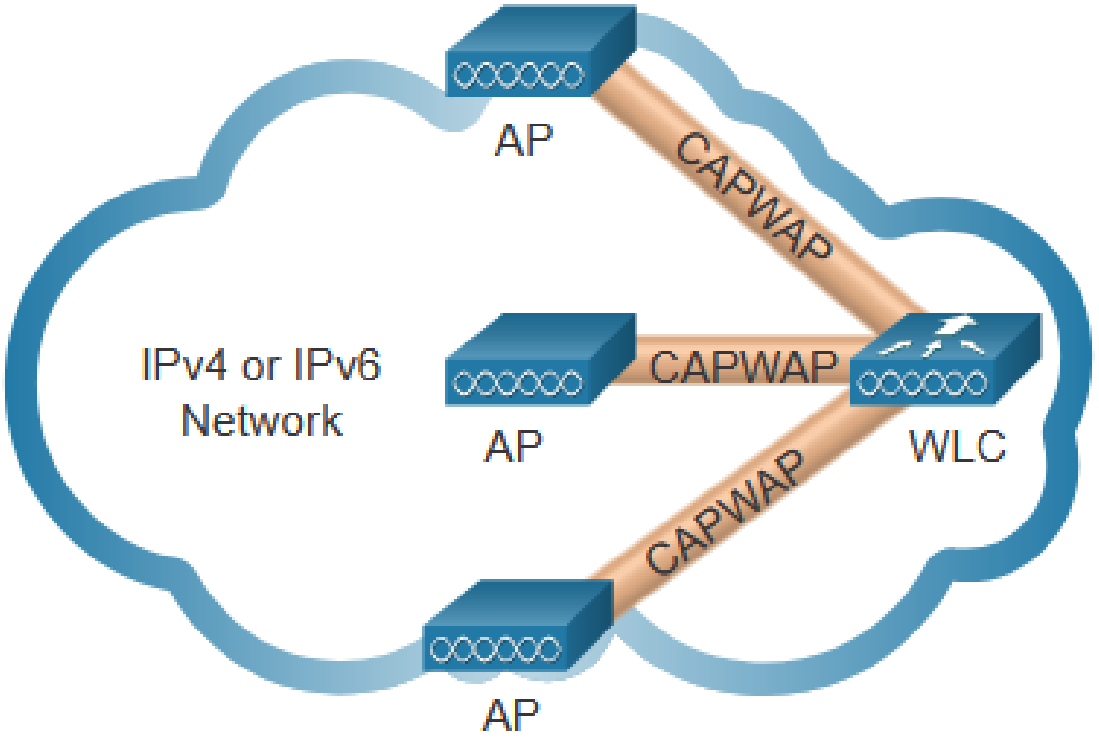
- Mosty (bridge) typicky neumožňujú bežným klientom asociovať sa
- Mosty sa asociujú vzájomne v pároch
- Vo všeobecnosti, prístupové body aj mosty sú Layer2 zariadenia a správajú sa ako prepínače
- WLAN sieť je typicky jedna broadcastová doména (t.j. jedna IP sieť)
- Niektoré pokročilejšie prístupové body dokážu obsluhovať niekoľko SSID naraz, pričom každý je zaradený do samostatnej 802.1Q VLAN



Funkcia CAPWAP protokolu

Úvod k CAPWAP

- Protokol štandardizovaný IEEE
- Umožňuje WLC manažovať viaceré APs
- Založený na LWAPP
  - Ale pridáva dodatočnú bezpečnosť s DTLS (Datagram Transport Layer Security)
  - Zapúzdruje a preposiela prevádzku WLAN klientov medzi AP a WLC cez tunel využitím UDP portov 5246 a5247
- Funguje cez IPv4 (type 17) a IPv6 (type 136)



Netacad: 12.4.1 – Video – CAPWAP

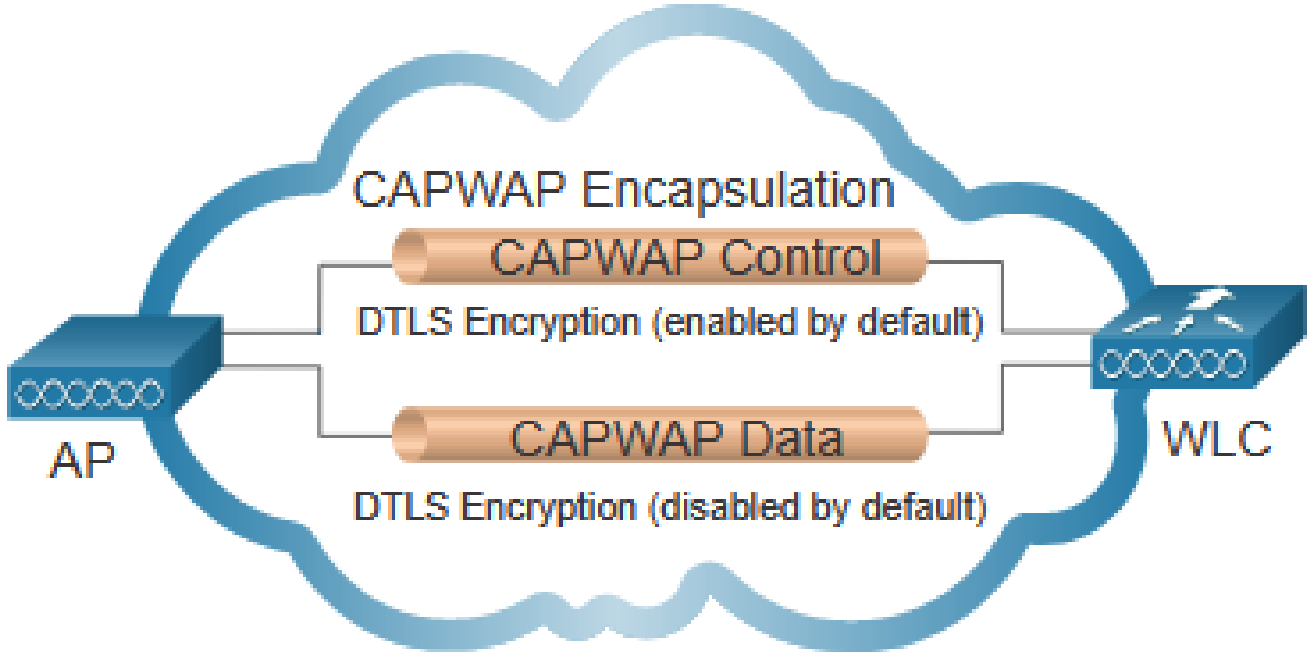
Split MAC architektúra

- Koncept CAPWAP split MAC robí všetky funkcie, ktoré bežne vykonávajú APs a distribuuje ich medzi funkčné komponenty:
  - 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

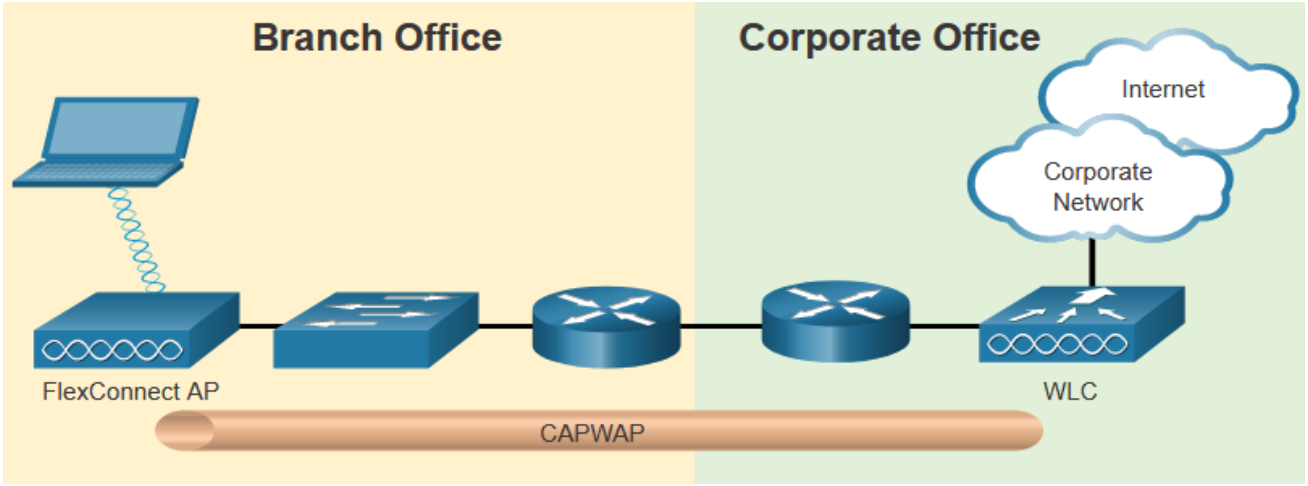
DTLS šifrovanie

- DTLS poskytuje bezpečnosť medzi AP a WLC
- Predvolene je zapnuté zabezpečenie riadiaceho kanála medzi AP a WLC



- Šifrovanie samotných dát je v predvolenom nastavení vypnuté
  - Vyžaduje si nainštalovanie licencie DTLS na WLC pred tým, ako ho bude možné povoliť na AP

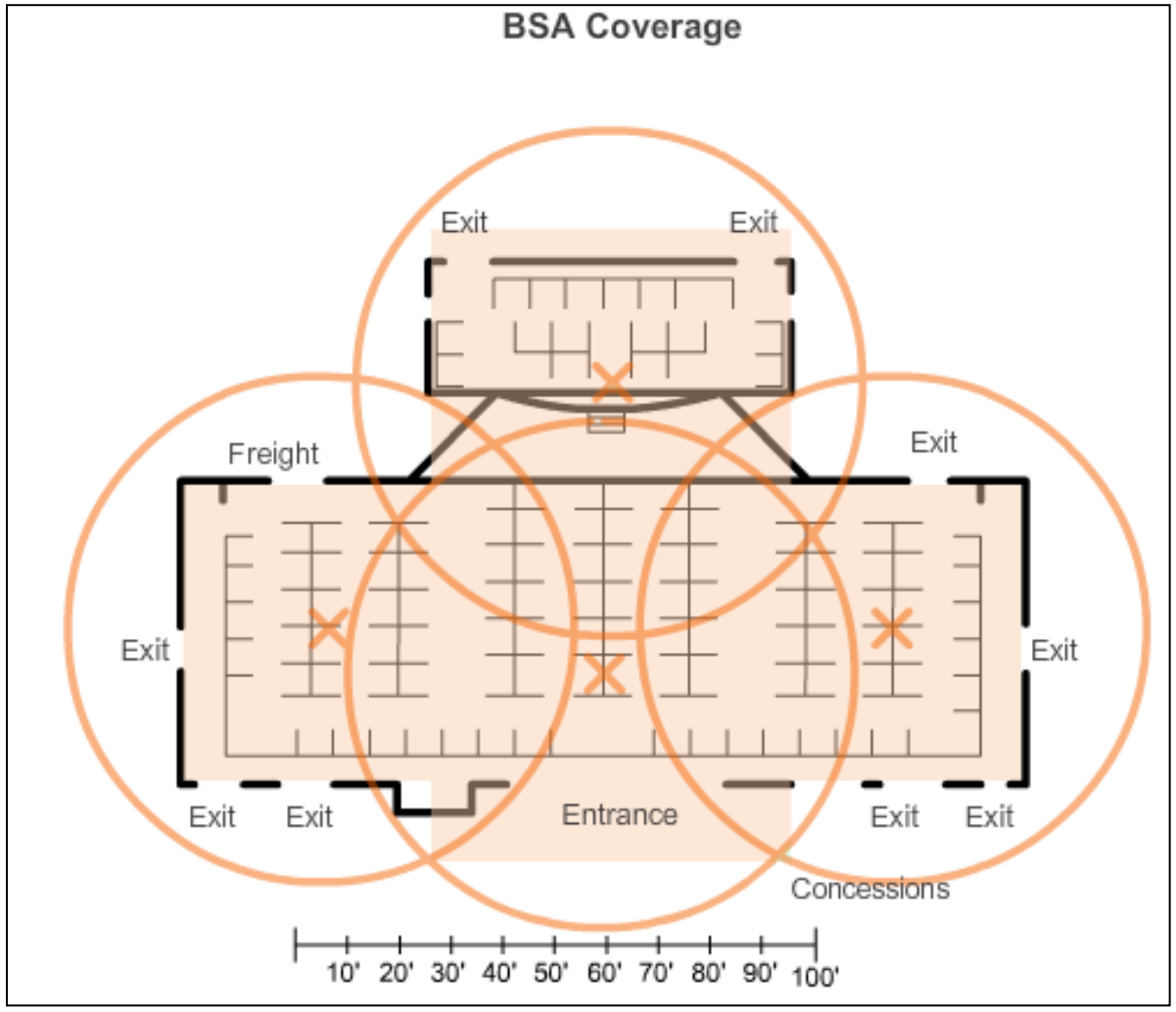
Flex Connect APs



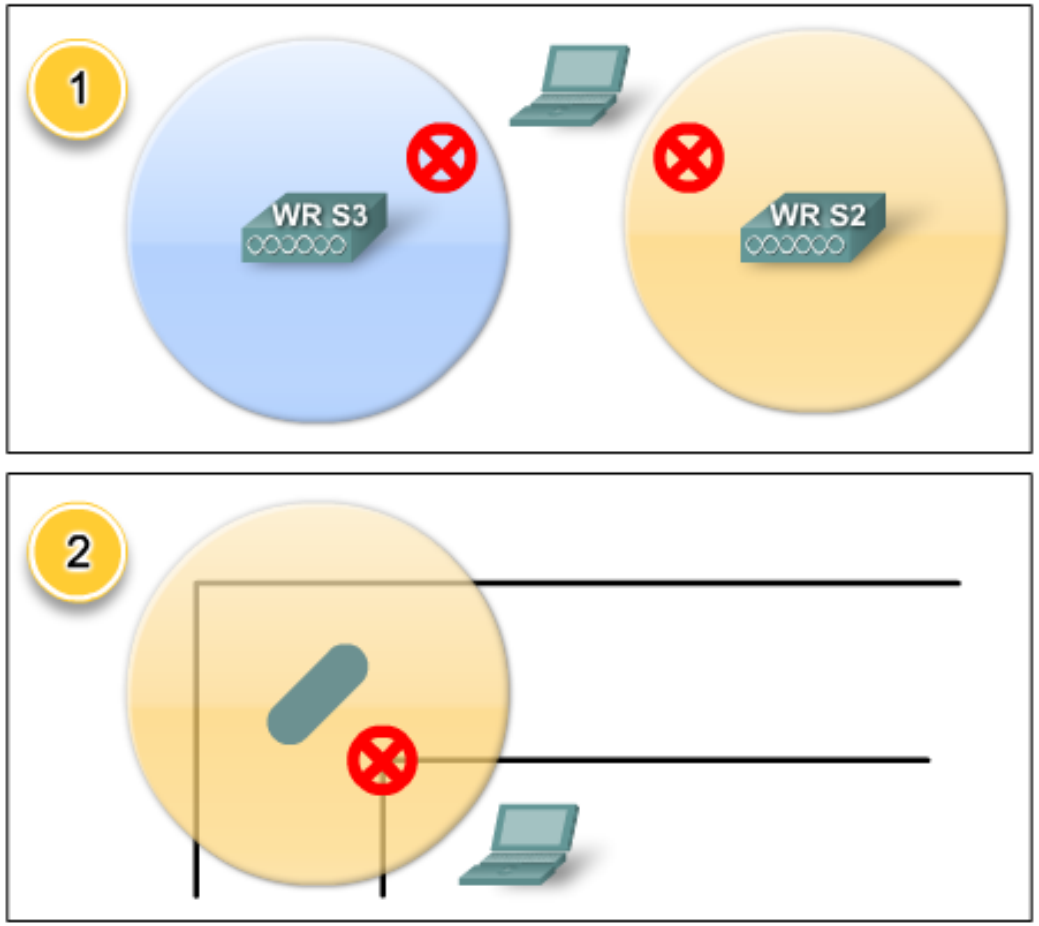
- Pre konfiguráciu a riadenie APs cez WAN linku
- Existuje v 2 módoch:
  - **Connected mód**
    - WLC je dostupné
    - FlexConnect AP má CAPWAP konektivitu s WLC cez CAPWAP tunel
    - WLC vykonáva všetky CAPWAP funkcie
  - **Standalone mód**
    - WLC je nedostupné
    - FlexConnect AP stratilo CAPWAP konektivitu s WLC
    - FlexConnect AP môže prevziať niektoré z funkcií WLC na seba lokálne, napr.:
      - prepínanie dátovej prevádzky klientov
      - vykonávanie autentifikácie klientov

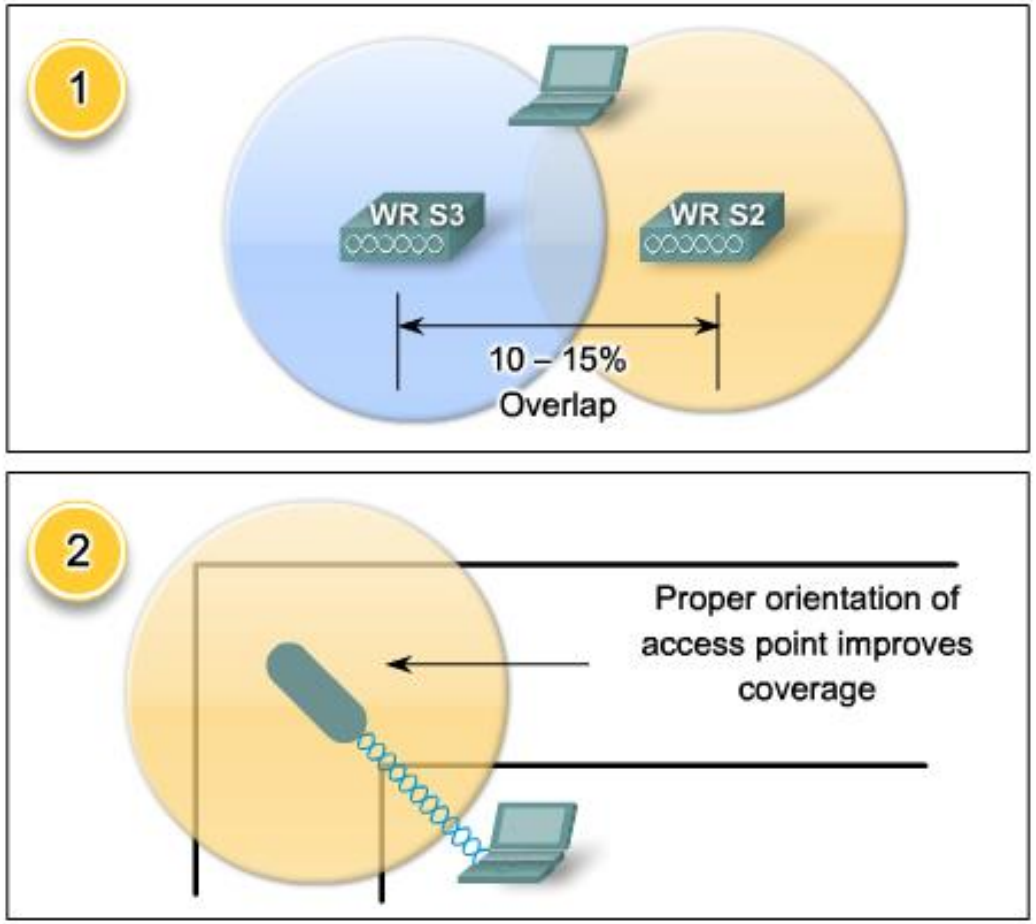
Plánovanie WLAN nasadenia

- Ber do úvahy
  - Počet používateľov
  - Následne plánovanú priepustnosť
    - Aké rýchlosti používatelia očakávajú
  - Použitie neprekrývajúcich sa kanálov viacerými APs
  - Nastavenia vysielacieho výkonu
- Pri nasadení AP zváž
  - Napojenie na kabeláž
  - Napájanie
  - Či je priestor na umiestnenie
- Extra zváž
  - Umiestni AP nad prekážky
  - Umiestni tesne pod strop v centre každej oblasti
  - Umiestni AP tam kde budú používatelia



Umiestnenie AP a nasmerovanie antény



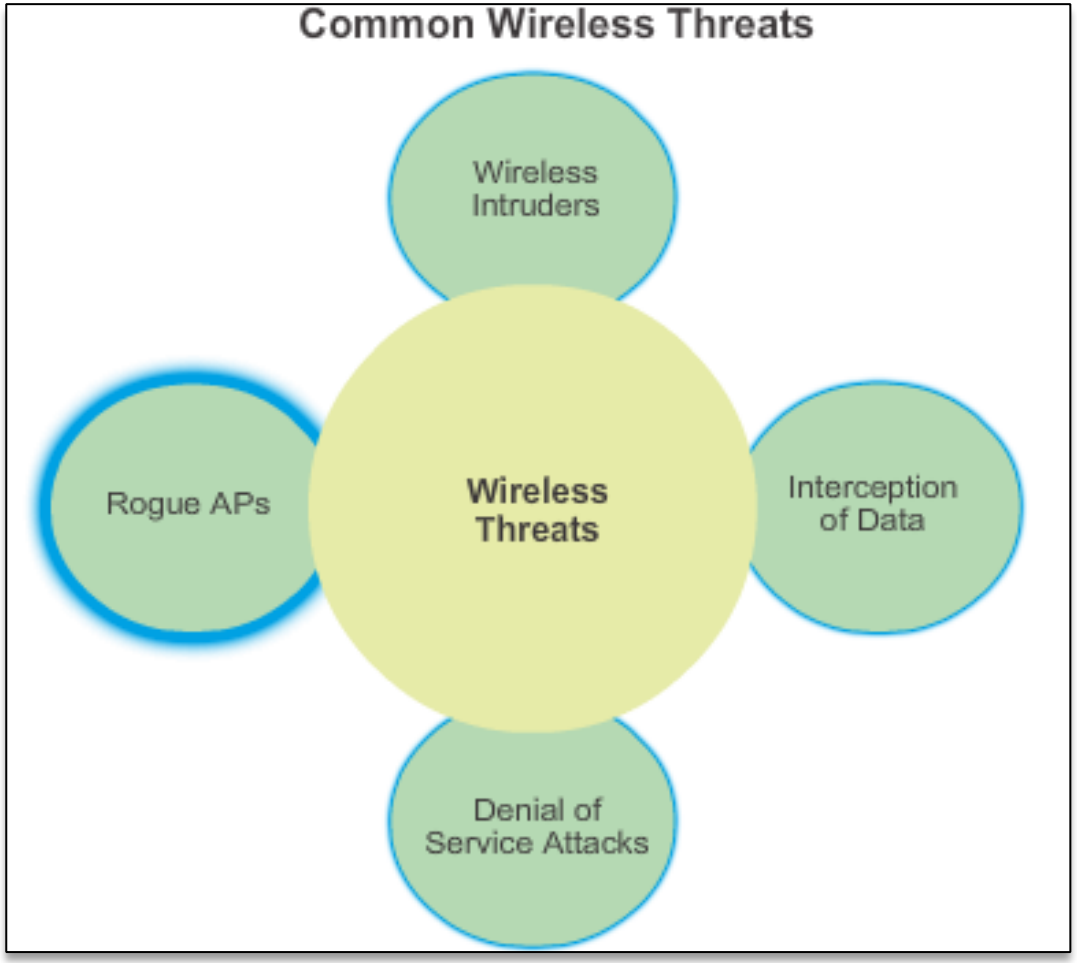


WLAN hrozby

WLAN bezpečnosť

Bezpečnosť WLAN

- WLAN je otvorená pre všetkých v dosahu AP
  - s príslušnými povereniami (credentials), ktoré je možné k nej priradiť
- Útoky
  - Úmyselné/neúmyselné
  - Zvonku, z vnútra/zamestnanci
- Osobitná náchylnosť na:
  - Odpočúvanie údajov
  - Bezdrôtových votrelcov
  - Útoky týkajúce sa odmietnutia služby (DoS)
  - Podvrhnuté APs (Rogue APs)

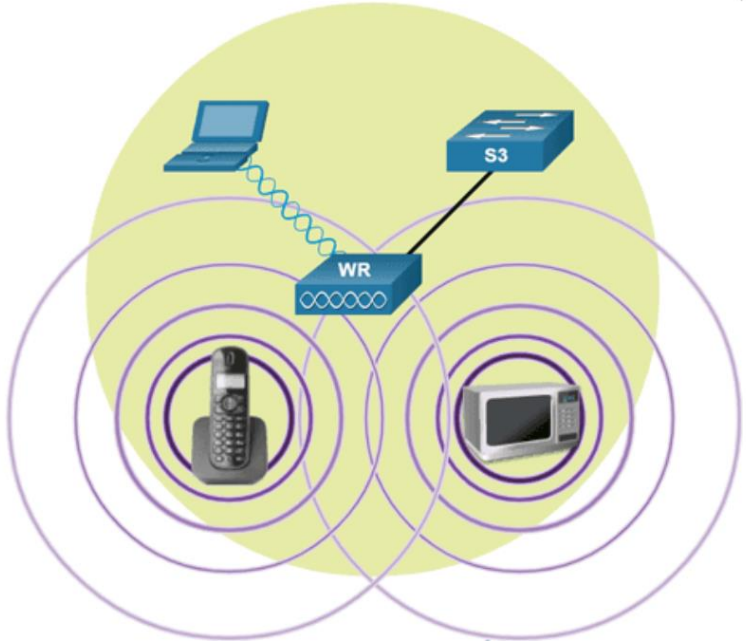


Rogue APs

Unauthorized APs installed by a well-intentioned user or willingly for malicious purpose. Use wireless management software to detect rogue APs.

DoS útok

- Bezdrôtové DoS útoky môžu byť výsledkom:
  - Nesprávne nakonfigurované zariadenia
  - Chyby v konfigurácii môžu deaktivovať WLAN
  - Zlomyseľný používateľ úmyselne zasahujúci do bezdrôtovej komunikácie
    - Zakážte bezdrôtovú sieť tam, kde žiadne legitímne zariadenie nemá prístup k médiu
- Náhodné rušenie
  - Sieť WLAN pracuje v nelicencovaných frekvenčných pásmach a je náchylná na rušenie inými bezdrôtovými zariadeniami
  - Môžu sa vyskytnúť u zariadení:
    - mikrovlnné rúry
    - bezdrôtové telefóny
    - detské vysielačky, ..



- Pásmo 2,4 GHz je náchylnejšie na rušenie ako pásmo 5 GHz
- Pre minimalizáciu DoS útoku z dôvodu nesprávne nakonfigurovaných zariadení a škodlivých útokov:
  - Zabezpečte všetky zariadenia
  - Zabezpečte silné heslá
  - Vytvárajte zálohy
  - Zabezpečte, aby boli všetky zmeny konfigurácie mimo bežného pracovného času

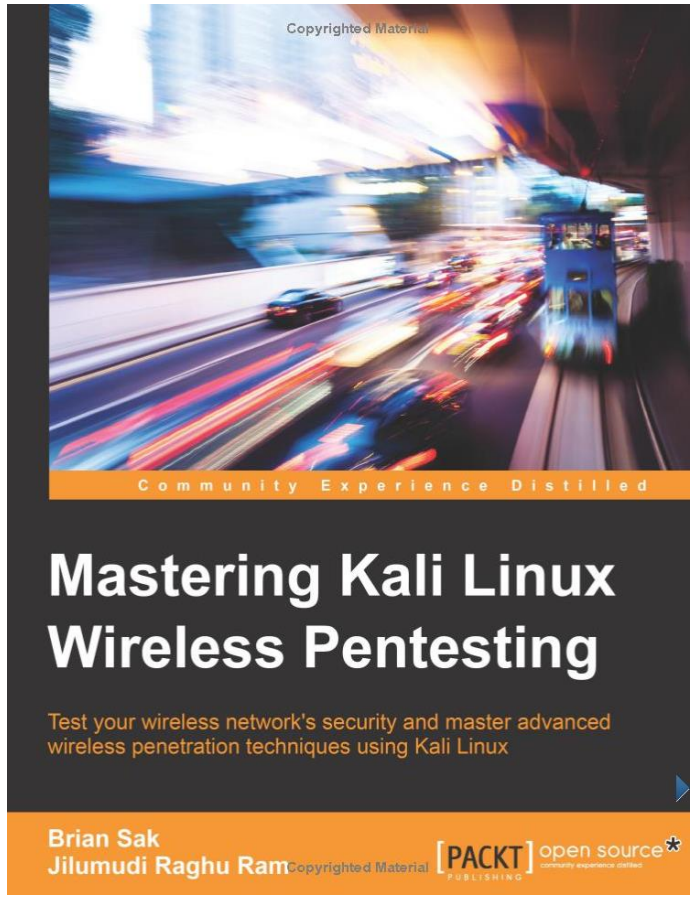
Management Frame DoS Attacks

Útok falošným odpojením (Spoofed Disconnect Attack)

- útočník pošle sekvenciu príkazov pre „diasociáciu/odpojenie“ všetkým bezdrôtovým klientom
- spôsobí odpojenie všetkých klientov
- klienti sa okamžite pokúsia znova pripojiť, čo spôsobí zahltenie

Záplava CTS rámcami (CTS flood)

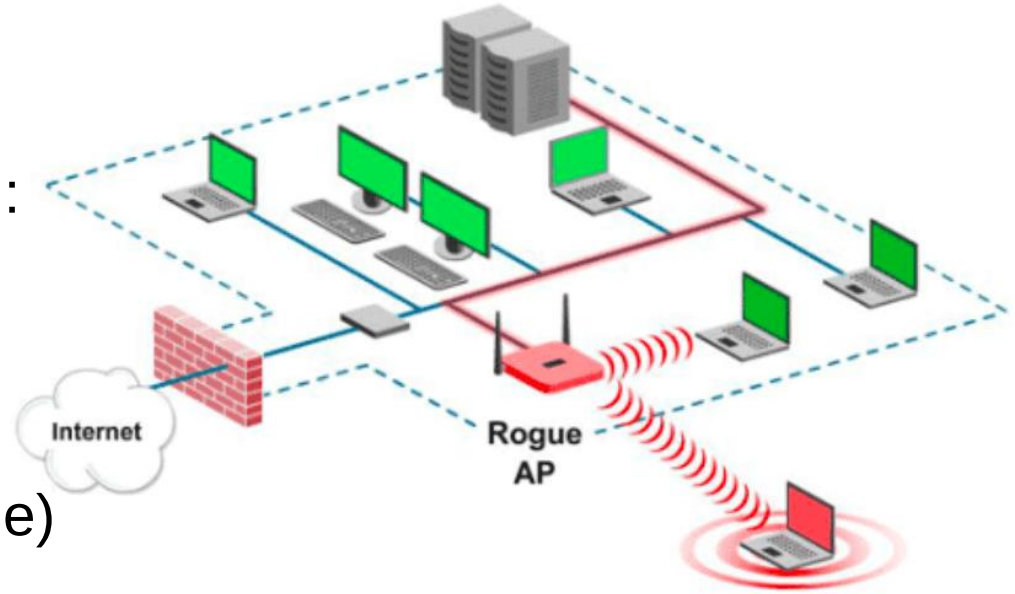
- Útočník využíva prístupovú metódu CSMA/CA na monopolizáciu šírky pásma
- Útočník opakovane zaplavuje WLAN rámcami CTS (Clear to Send) na falošný/neexistujúci STA
- Všetci bezdrôtoví klienti zdieľajúci RF médium prijímajú CTS a zadržiavajú prenosy, kým útočník neprestane vysielať rámce CTS



Podvodné AP (Rogue AP)

Podvodné môže byť AP alebo smerovač, ktorý bol:

- Pripojený k podnikovej sieti bez výslovného **oprávnenia** a proti firemnej **politike**
- Pripojený alebo povolený útočníkom
  - na **zhromažďovanie údajov** o klientoch, napr.:
    - MAC adries klientov (bezdrôtových aj drôtových)
    - zachytenie a maskovanie dátových paketov
  - pre **získanie prístupu** k sieťovým zdrojom
  - alebo spustenie **MITM** útoku (man-in-the-middle)



Obrana proti podvodným AP:

- používať **monitorovací softvér** na aktívne sledovanie rádiového spektra
  - na zistenie neoprávnených prístupových bodov

Man-in-the-Middle Attack (MITM)

- Hacker sa umiestni medzi dve legitímne entity
  - aby mohol čítať alebo upravovať údaje, ktoré prechádzajú medzi oboma stranami
- Útok „**Zlého dvojčaťa**“ (Evil twin AP)
  - Útočník zavedie **podvodné** AP
  - a nakonfiguruje ho na **rovnaké SSID** ako legitímny AP
- Ohniskom tohto útoku sú lokality ponúkajúce **bezplatné a otvorené Wi-Fi** pripojenie na internet
  - Letiská
  - Kaviarne, reštaurácie
- Klienti, ktorí sa nachádzajú v blízkosti podvodného AP, nájdu **silnejší signál** a pravdepodobne sa spoja so zlým dvojčaťom

- Dáta od klienta sa potom odosielajú podvodnému AP, ktorý zachytáva údaje a preposiela ich legitímnemu AP
- Spätná prevádzka z legitímneho AP sa odošle nečestnému AP, zachytí sa a potom sa odovzdá nič netušiacemu klientovi (STA)

Obrana proti MITM:

- identifikovať legitímne zariadenia vo WLAN
  - Používať autentifikáciu používateľov
- Následne monitorovať nelegitímne zariadenia a prenos

Zabezpečenie WLAN

Authentication and Encryption Systems

Open Authentication and Shared Key Authentication

SSID Cloaking

MAC Address Filtering

Bezpečnosť WLAN sietí

- Zabezpečiť WLAN siete tak zahŕňa viaceré aspekty:
  - Autentifikácia používateľov, autentifikácia siete
  - Dôvernosť prenášaných dát
  - Ochrana proti neoprávnenému rozširovaniu siete
  - Ochrana aktívnych prvkov siete
- Podobne ako pri LAN sieti, ani WLAN pri svojom vybudovaní nie je bez dodatočnej konfigurácie nijako významne zabezpečená
- „Bezdrôtovosť“ útokov mnohokrát veľmi komplikuje vystopovanie útoku a odrádza nasadenie WLAN

SSID Cloaking, MAC Address Filtering

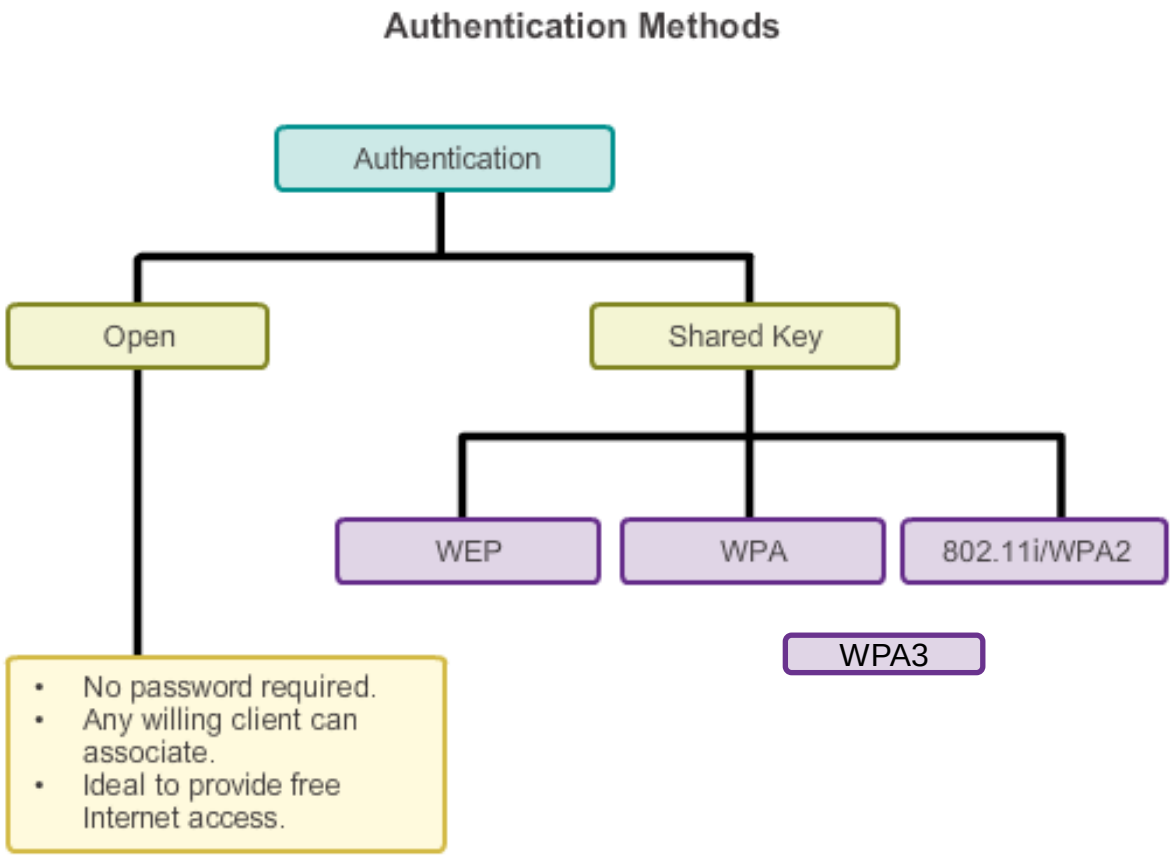
Na riešenie hrozieb, zabránenie prístupu bezdrôtových útočníkov a ochranu údajov, je možné použiť dve (historicky staré) bezpečnostné funkcie, ktoré sú stále k dispozícii na väčšine smerovačov a prístupových bodov:

- **Maskovanie SSID**
  - Zakázať posielanie SSID v beacon rámcoch
  - Bezdrôtoví klienti musia byť na pripojenie k sieti manuálne nakonfigurovaní so správnym SSID
- **Filtrovanie MAC adries**
  - Manuálne povoliť alebo zakázať klientom bezdrôtový prístup na základe ich fyzickej MAC adresy

Zabezpečenie WLAN

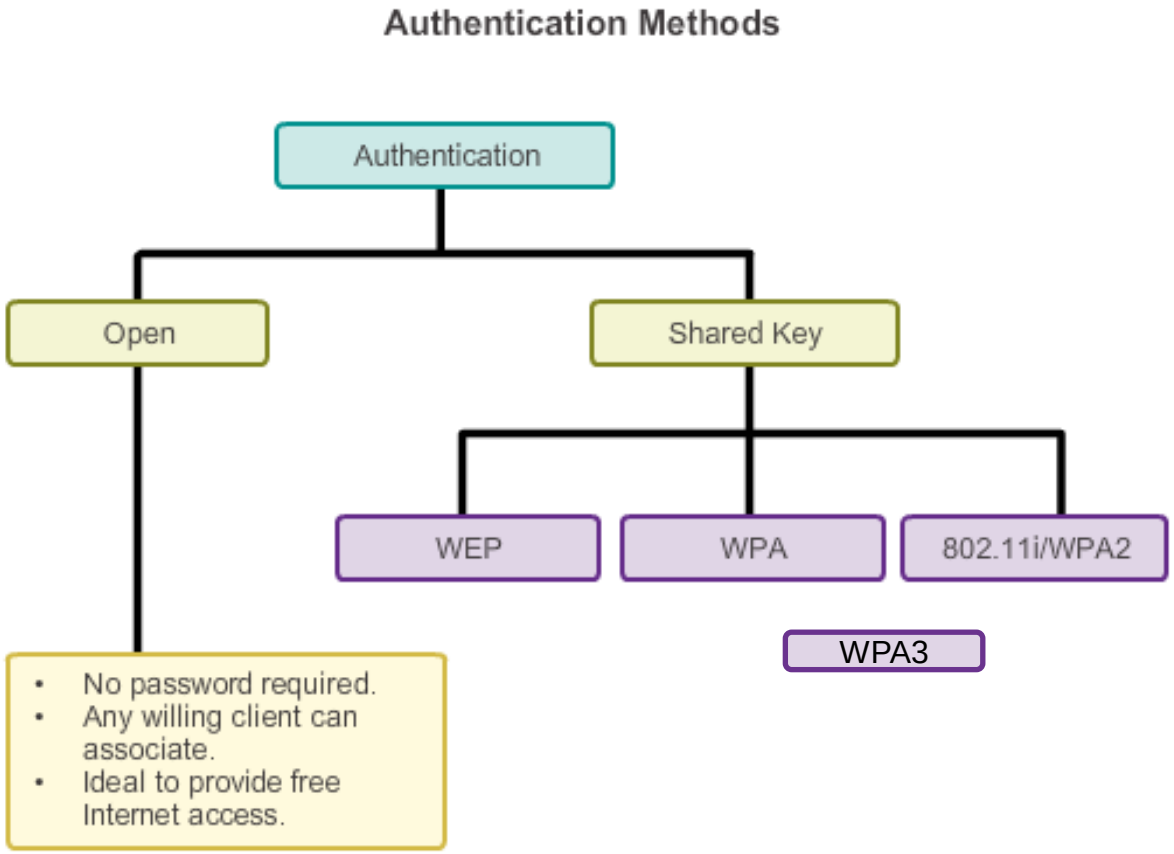
Autentifikácia používateľov

Autentifikácia používateľov



- Pôvodný štandard 802.11 obsahuje jednoduchú podporu pre autentifikáciu používateľov:
- Dva režimy autentifikácie:
  - **Open System**
    - Autentifikácia sa nevykonáva, resp. klient žiada a dostane
    - Klient by si v tomto prípade mal riešiť bezpečnosť napr. použitím VPN
  - **Shared Key**
    - Prístupový bod posiela klientovi výzvu (challenge), klient ju pomocou hesla zašifruje a posiela nazad na prístupový bod. Ak prístupový bod s pomocou toho istého hesla dokáže prijatú odpoveď správne dešifrovať, klienta autentifikuje.
- Heslo používané v režime Shared Key sa následne používa aj pre šifrovanie prenášaných dát

Shared key

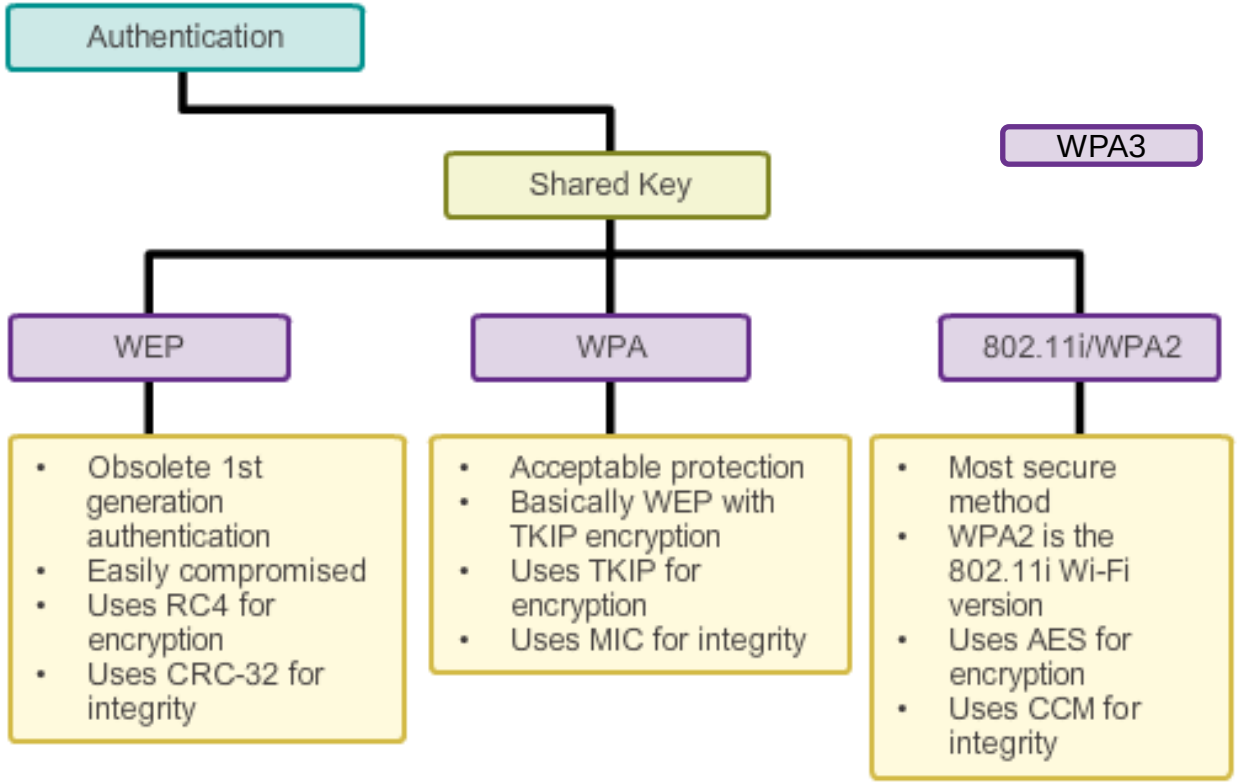


Tento základný algoritmus má podstatné chyby:

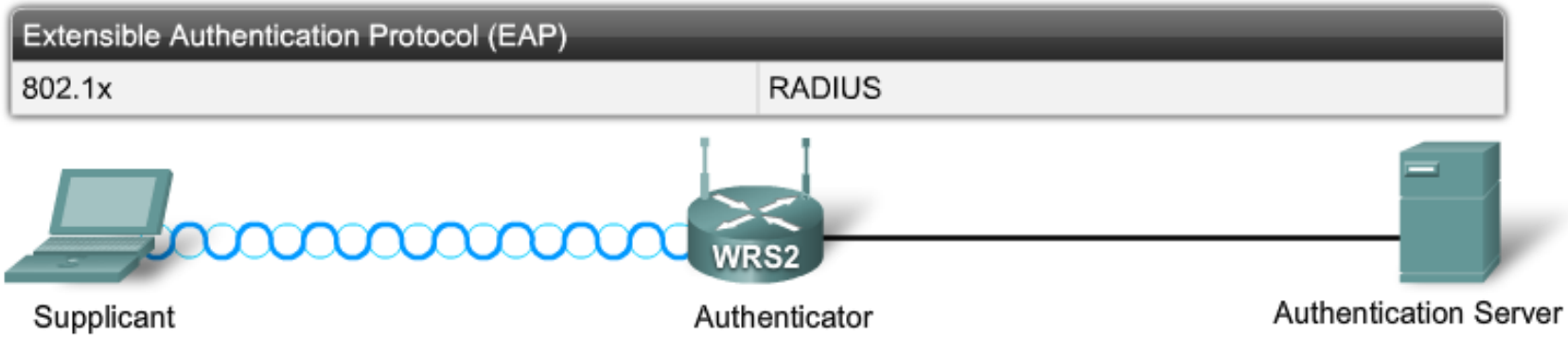
- Identický kľúč pre autentifikáciu a následné šifrovanie prenášaných dát
- Po prvotnom úspechu sa autentifikácia neopakuje
- V autentifikačných paketoch sa prenášajú dešifrovateľné dáta
- Dáta sú v autentifikačných paketoch šifrované triviálne: heslo XOR challenge
  - Z toho plynie: (heslo XOR challenge) XOR challenge = heslo

Autentifikácia používateľov

- Použitím Shared Key autentifikácie hrozí zhoršenie celkovej bezpečnosti
  - Útočníkovi stačí pri prihlasovaní sa klienta odchytiť autentifikačný dialóg a bez väčšej námahy získa heslo
- Tento nedostatok je riešený niekoľkými spôsobmi:
  - **EAP**
    (Extensible Authentication Protocol)
  - **WPA2**
    (Štandard 802.11i)
    - Vyvinuté na používanie s 802.1x (RADIUS)



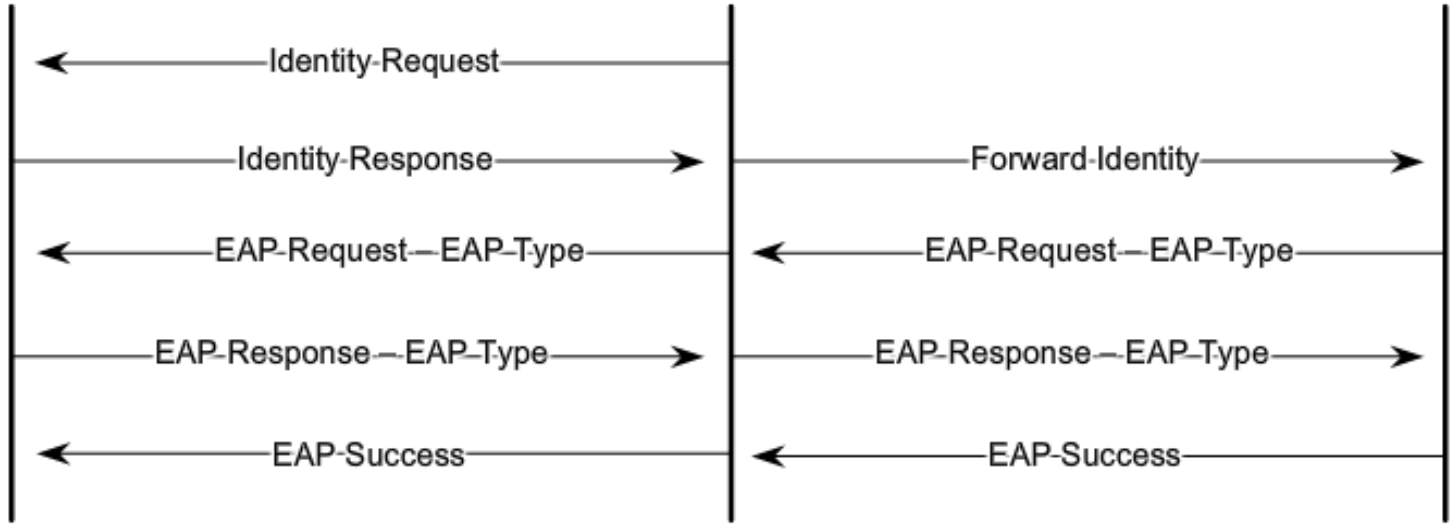
Protokol EAP



RFC 3748

Generický protokol (framework) pre prenos rôznych druhov autentifikačných dialógov medzi

- klientom (tzv. **supplicant**)
- a bodom vyžadujúcim autentifikáciu (tzv. **authenticator**)

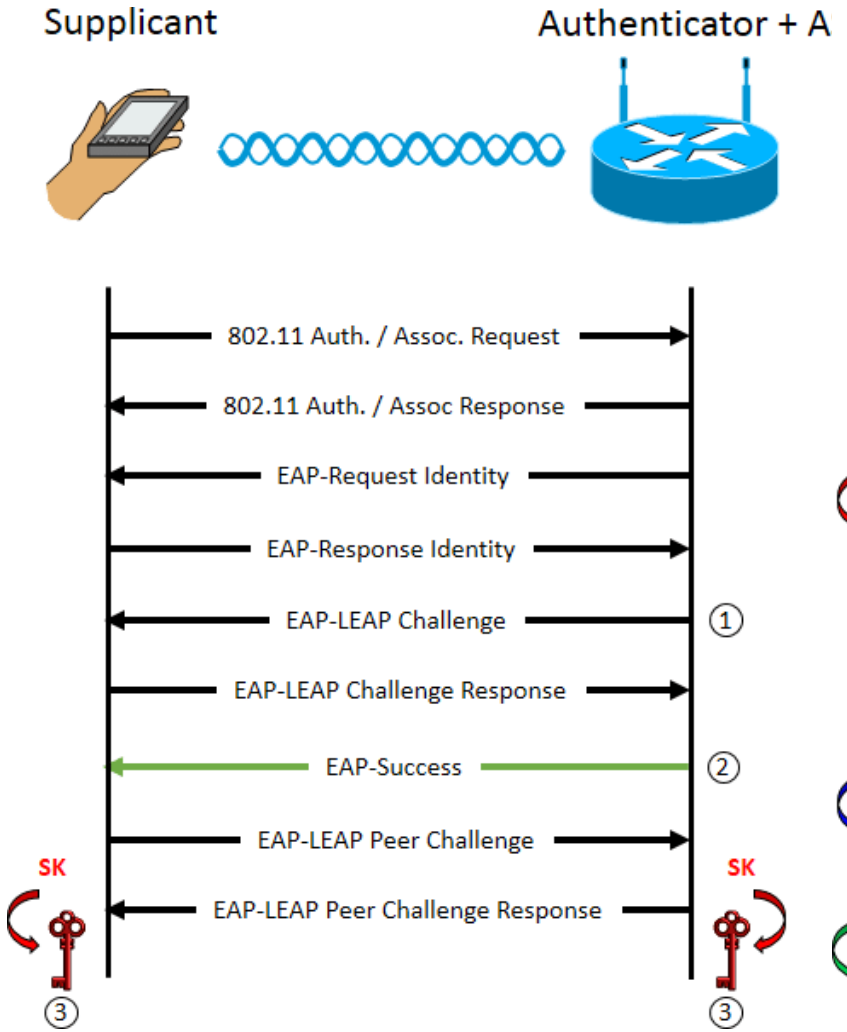


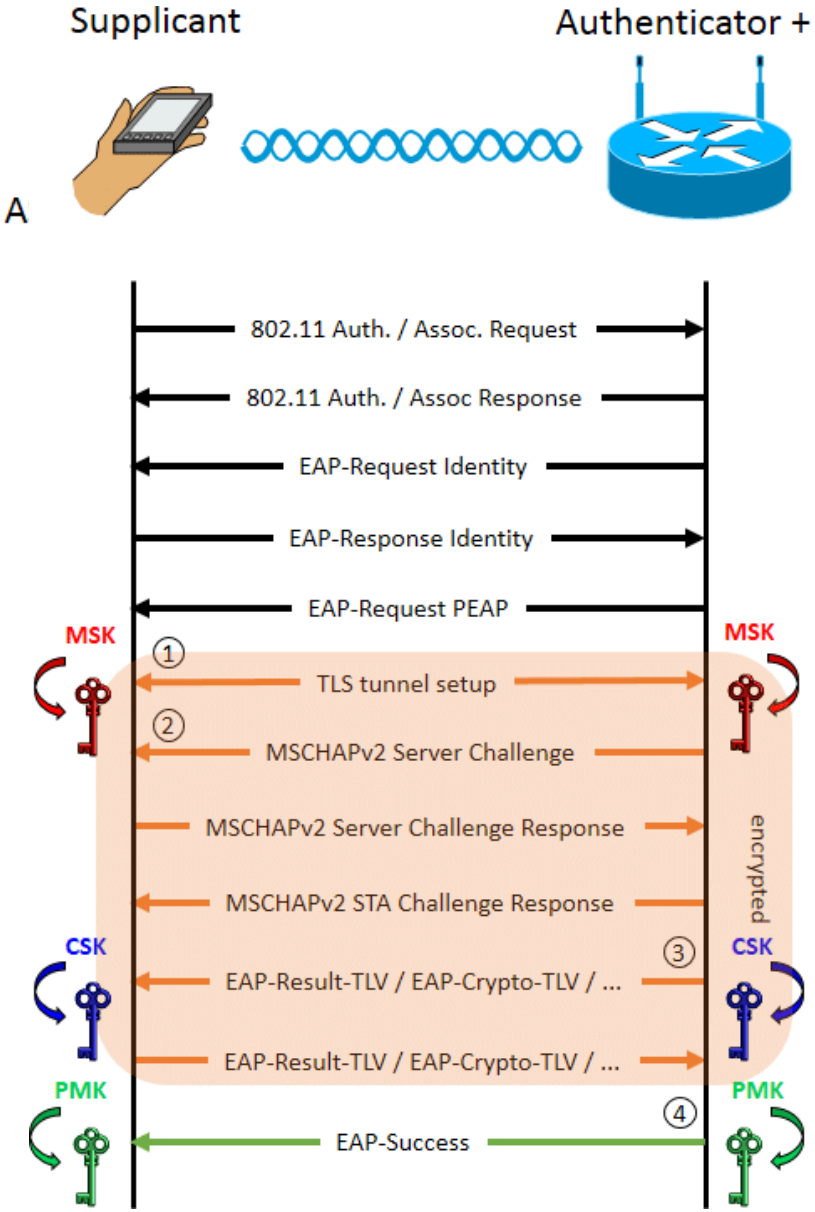
- Poskytuje základný formát dátových štruktúr, ktoré sú využiteľné pre ľubovoľný druh autentifikácie
- Nie je to konkrétny spôsob autentifikácie
- Výhodou je, že authenticator nemusí konkrétnemu typu autentifikácie rozumieť, len prenáša dialóg medzi supplicantom a autentizačným serverom

Autentifikačné metódy nad EAP

V súčasnosti používané metódy nad EAP:

1. **LEAP (Lightweight EAP)**
   - Cisco implementácia challenge-response protokolu. Overenie použitím mena a hesla.
2. **PEAP (Protected EAP)**
   - Dvojfázová overovacia schéma.
   - V prvej fáze sa pomocou TLS protokolu vybuduje bezpečné šifrované spojenie medzi supplicantom a autentifikačným serverom, pričom sa overí autenticita servera (TLS certifikát).
   - V druhej fáze sa voliteľným ďalším spôsobom overí autenticita klienta





Autentifikácia používateľov

V súčasnosti používané metódy nad EAP:

3. EAP-Transport Layer Security (EAP-TLS)
   - Vzájomné overenie klienta i servera. Medzi serverom a klientom sa vybuduje bezpečné spojenie a overí sa identita klienta i servera.
   - Vyžaduje si certifikáty pre klienta i server.

- Existuje množstvo ďalších metód, nie všetky sú používané
- Pre multi-vendor prostredia je vhodná metóda PEAP alebo EAP-TLS

Prehľad autentifikačných metód nad EAP

802.1X EAP Types Feature / Benefit	**MD5** Message Digest 5	**TLS** Transport Level Security	**TTLS** Tunneled Transport Level Security	**PEAP** Protected Transport Level Security	**FAST** Flexible Authentication via Secure Tunneling	**LEAP** Lightweight Extensible Authentication Protocol
Client-side certificate required	no	yes	no	no	no (PAC)	no
Server-side certificate required	no	yes	yes	yes	no (PAC)	no
WEP key management	no	yes	yes	yes	yes	yes
Rogue AP detection	no	no	no	no	yes	yes
Provider	MS	MS	Funk	MS	Cisco	Cisco
Authentication Attributes	One way	Mutual	Mutual	Mutual	Mutual	Mutual
Deployment Difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate	Moderate
Wi-Fi Security	Poor	Very High	High	High	High	High when strong passwords are used.

Autentifikácia siete

- Tak, ako je potrebné autentifikovať používateľa, je potrebné autentifikovať aj sieť
  - Je veľmi jednoduché tajne umiestniť do priestoru prístupový bod so silným signálom a rovnakým SSID, ktorý na seba stiahne klientov - **Rogue AP**
- Pre autentifikáciu siete sú vhodné EAP metódy, kde sa server preukazuje svojím certifikátom (PEAP, EAP-TLS, EAP-TTLS...)
- Kameňom úrazu sú používateľské návyky
  - Ak sa používateľovi objaví upozornenie, že certifikát servera nie je platný, spravidla len bezmyšlienkovito hlášku odklikne

Zabezpečenie WLAN

Zabezpečenie prenášaných dát

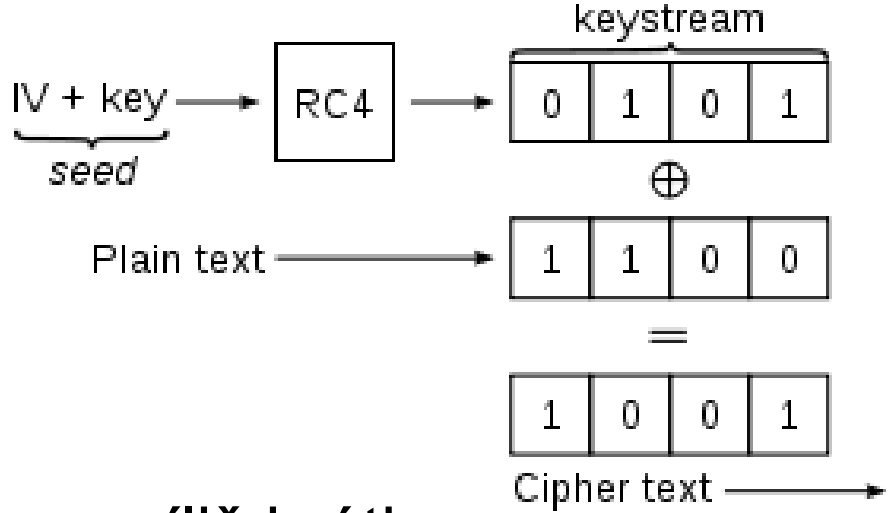
Dôvernosť prenášaných dát

- Treba si uvedomiť
  - Pasívne odpočúvanie nemožno detegovať vôbec
  - Rádiový signál nemožno ľahko ohraničiť
  - Pri WLAN je potrebné akceptovať, že prevádzka bude odpočúvaná, a zamerať sa na to, aby jej zachytením útočník nič nezískal
- Vhodné riešenie: šifrovanie prenášaných dát
- Štandard 802.11b/g obsahuje klasickú implementáciu šifrovania obsahu s názvom Wired Equivalent Privacy (WEP)

Šifrovanie dát - WEP

- **Wired Equivalent Privacy (WEP)**
  - Symetrická šifra využívajúca algoritmus RC4
  - Štandard pôvodne uvažoval WEP 64 (40-bitový kľúč + 24 bit IV vektor)
    - neskôr nárast na 104-bitový kľúč (proprietárne implementácie i viac), t.j. WEP 128
  - Kľúč je identický s kľúčom pre voliteľnú autentifikáciu
  - Kľúč je statický

Šifrovanie dát - WEP

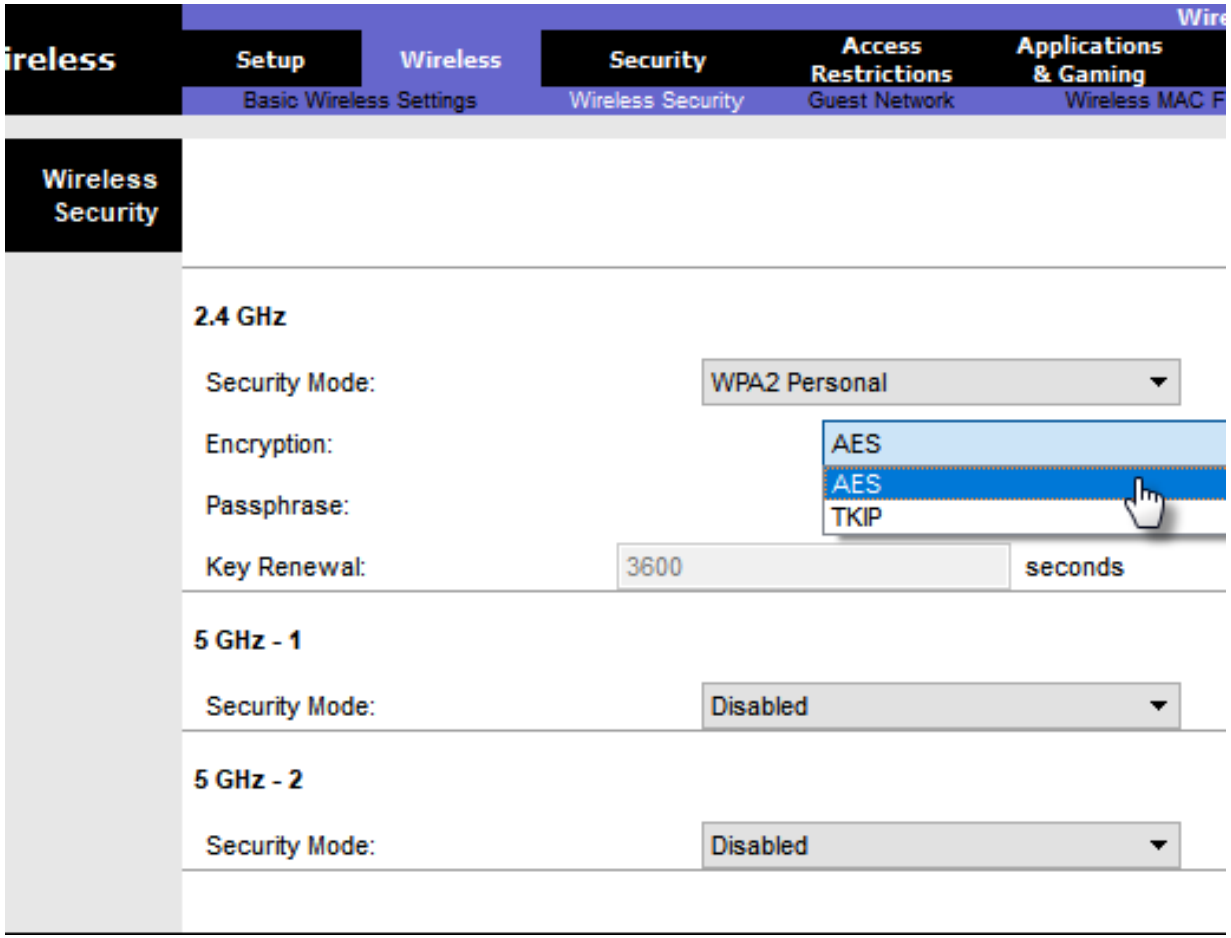


- Pre WEP boli vyvinuté mnohé spôsoby bezpečnostných útokov
  - https://www.aircrack-ng.org/
- 40-bitový kľúč je pre dnešný výpočtový výkon príliš krátky
  - Inicializačný vektor (24 bitov)
    - pre generátor pseudonáhodných čísel v RC4 algoritme sa posiela v každom rámci ako plaintext
- Dlhšie kľúče používané niektorými výrobcami: 64, 128, 152, 256
- Existuje séria slabých inicializačných vektorov, ktoré zo zašifrovaného obsahu dovoľujú zistiť hodnotu niektorých bajtov kľúča

Náhrada WEP: WPA

WiFi Protected Access (WPA)

- Šifrovanie sa realizuje pomocou algoritmu RC4 so 128-bitovým kľúčom a 48-bitovým inicializačným vektorom
- Kľúč je dynamicky priebežne aktualizovaný pomocou protokolu **TKIP**
  - Temporary Key Integrity Protocol
- Každý rámec je šifrovaný iným kľúčom (odvodeným od základného kľúča)
- Rámec môže niesť kontrolný súčet, ktorý je takisto šifrovaný (MIC – algoritmus Michael)



- WPA aj WPA2 poskytuje 2 šifrovacie protokoly (pre L2 payload):
  - TKIP
  - AES

Šifrovanie dát – náhrada WEP: WPA2

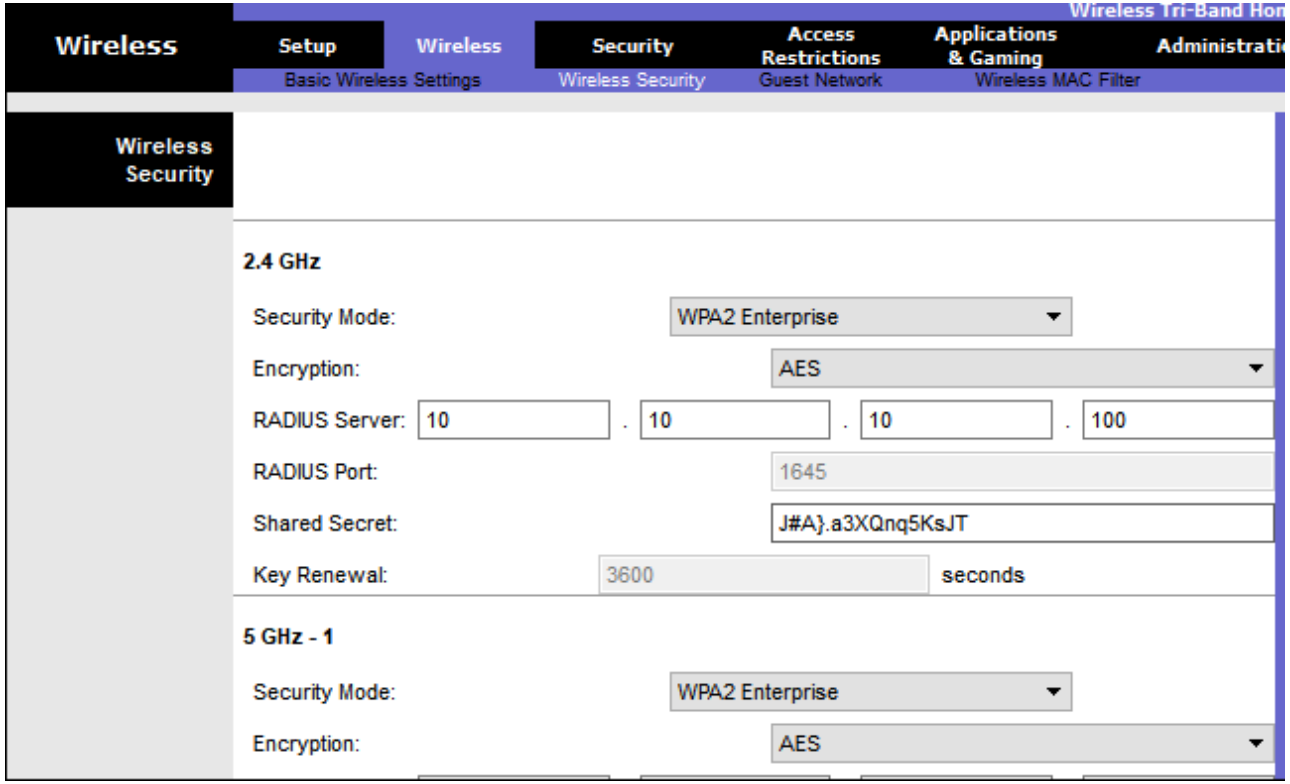
- **WiFi Protected Access 2 (WPA2)**
  - Štandardizovaná v **802.11i** (používaná od r. 2000)
  - Využíva šifrovací algoritmus **AES** (Rijndael)
    - Advanced Encryption Standard
  - Namiesto TKIP využíva protokol **CCMP** (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)
  - V súčasnosti nie sú voči WPA2 známe efektívne spôsoby útokov
  - Na rozdiel od WPA si nasadenie WPA2 spravidla vyžiada výmenu bezdrôtových komponentov, pretože z výkonových dôvodov je potrebné AES implementovať hardvérovo

Autentifikácia v organizácii (Enterprise)

Voľba: **Enterprise security mode** vyžaduje **AAA** server: Authentication, Authorization, and Accounting (AAA) RADIUS server.

Potrebné je definovať tieto 3 informácie:

- **RADIUS server IP address**
- **UDP port numbers**
  - Zväčša: 1812 for RADIUS Authentication, 1813 for RADIUS Accounting
  - Ale môže byť aj: 1645 a 1646
- **Shared key**
  - Pre autentifikáciu AP s RADIUS serverom



Autentifikácia a autorizácia používateľov je riešená pomocou **802.1X štandardu**, ktorý poskytuje **centralizovanú**, server-based autentifikáciu používateľov.

Náhrada WPA2: WPA3

- V januári **2018** Aliancia Wi-Fi oznámila WPA3 ako náhradu za WPA2.
  - WPA3 Specification ver 3.0, posl. update 14.12.2020 https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf
- Certifikácia sa začala v júni 2018.
- Využíva ekvivalentnú 192-bitovú kryptografickú silu v režime WPA3-**Enterprise**
  - **AES-256** v režime GCM s **SHA-384** ako HMAC
  - a stále nariaďuje použitie protokolu **CCMP-128** (AES-128 v režime CCM)
    - ako minimálny šifrovací algoritmus v režime WPA3-**Personal**
- Nahrádza výmenu vopred zdieľaných kľúčov simultánnym overovaním rovnocenných údajov, ako je definované v IEEE 802.11-2016, t.j.:
  - bezpečnejšia počiatočná výmena kľúčov v osobnom režime
- Zmierňuje problémy so zabezpečením, ktoré spôsobujú slabé heslá, a zjednodušuje proces nastavovania zariadení bez zobrazovacieho rozhrania
- Ochrana riadiacich rámcov uvedená v IEEE 802.11w je vo WPA3 špecifikácii vynútená
- Avšak ešte to nie je ono....
  - Už boli nájdené zraniteľnosti aj pre WPA3, pre skalných:
    - https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/
    - https://papers.mathyvanhoef.com/dragonblood.pdf)

WPA3™

Specification

Version 3.0

WPA 3

WPA3 zahŕňa 4 funkcionality:

- **WPA3 – Personal :** používa SAE
  - Bráni útokom hrubou silou simultánnym overovaním rovnocenných údajov - Simultaneous Authentication of Equals (SAE).
- **WPA3 – Enterprise :** používa 802.1X/EAP autentifikáciu
  - Vyžaduje si to však použitie 192-bitového šifrovacieho balíka a eliminuje miešanie bezpečnostných protokolov pre predchádzajúce štandardy 802.11.
- **Open Networks :** nepoužíva žiadnu autentifikáciu, šifruje s OWE
  - Používa ale: Opportunistic Wireless Encryption (OWE) na šifrovanie celej bezdrôtovej prevádzky.
- **IoT Onboarding :** používa DPP
  - Používa Device Provisioning Protocol (DPP) na rýchle pripojenie IoT zariadení.

Autentifikačné metódy so zdieľaným kľúčom

V súčasnosti dostupné metódy – SÚHRN:

Authentication Method	Description
Wired Equivalent Privacy (WEP)	Pôvodná špecifikácia 802.11 navrhnutá na zabezpečenie údajov pomocou metódy šifrovania Rivest Cipher 4 (**RC4**) so **statickým kľúčom**. **WEP** sa už **neodporúča** a nikdy by sa nemalo používať.
Wi-Fi Protected Access (WPA)	Štandard Wi-Fi Alliance, ktorý používa **WEP**, ale zabezpečuje dáta oveľa silnejším šifrovacím algoritmom Temporal Key Integrity Protocol (TKIP). **TKIP** mení kľúč pre každý paket, takže je oveľa ťažšie hacknúť ho.
WPA2	Na šifrovanie používa Advanced Encryption Standard (AES). **AES** je v súčasnosti považovaný za **najsilnejší šifrovací** protokol.
WPA3	Toto je ďalšia generácia zabezpečenia Wi-Fi. Všetky zariadenia s podporou WPA3 používajú najnovšie bezpečnostné metódy, nepovoľujú zastarané staršie protokoly a vyžadujú použitie chránených riadiacich rámcov - Protected Management Frames (PMF).

Ochrana proti neoprávnenému rozširovaniu siete

- Útočník mimo kancelárie resp. budovy sa môže pokúsiť asociovať sa s našimi prístupovými bodmi, alebo môže nastražiť vlastný prístupový bod
- Používatelia môžu kvôli vlastnému pohodliu doniesť vlastný prístupový bod, zapojiť ho do siete a nechať ho pracovať so štandardnými nastaveniami
- Riešenie nie je triviálne a spočíva v mnohých zabezpečeniach:
  - Zoznam povolených MAC adries klientov
  - Autentifikácia
  - Prístupové body umožňujúce priebežnú sondáž siete a ohlásenie neautorizovaných prístupových bodov

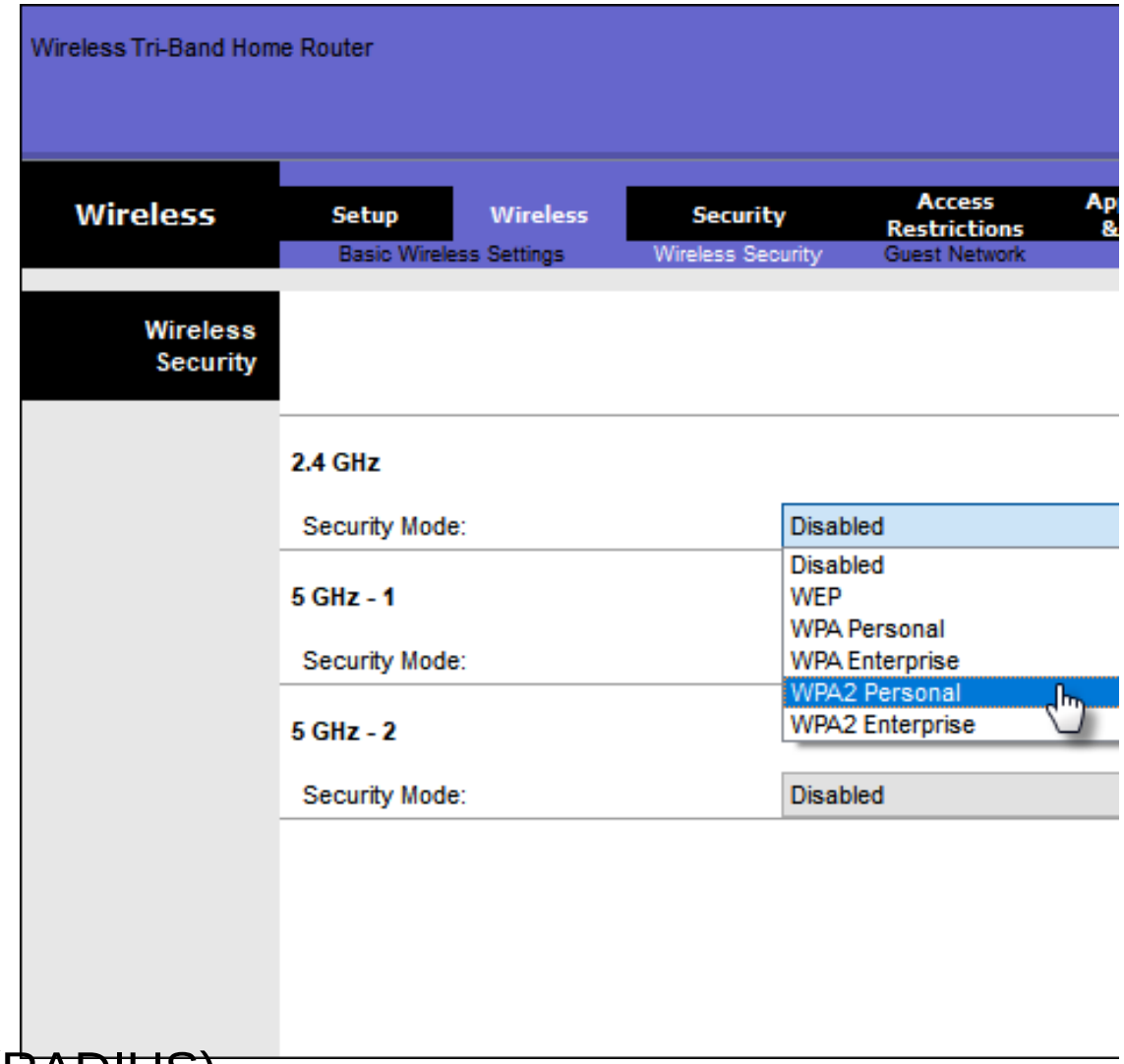
Methods for controlling wireless LAN access:

1. SSID broadcasts from access points are off
2. MAC Address filtering is enabled
3. WPA2 Security implemented

CAUTION: Neither items 1 or 2 are considered valid security measures

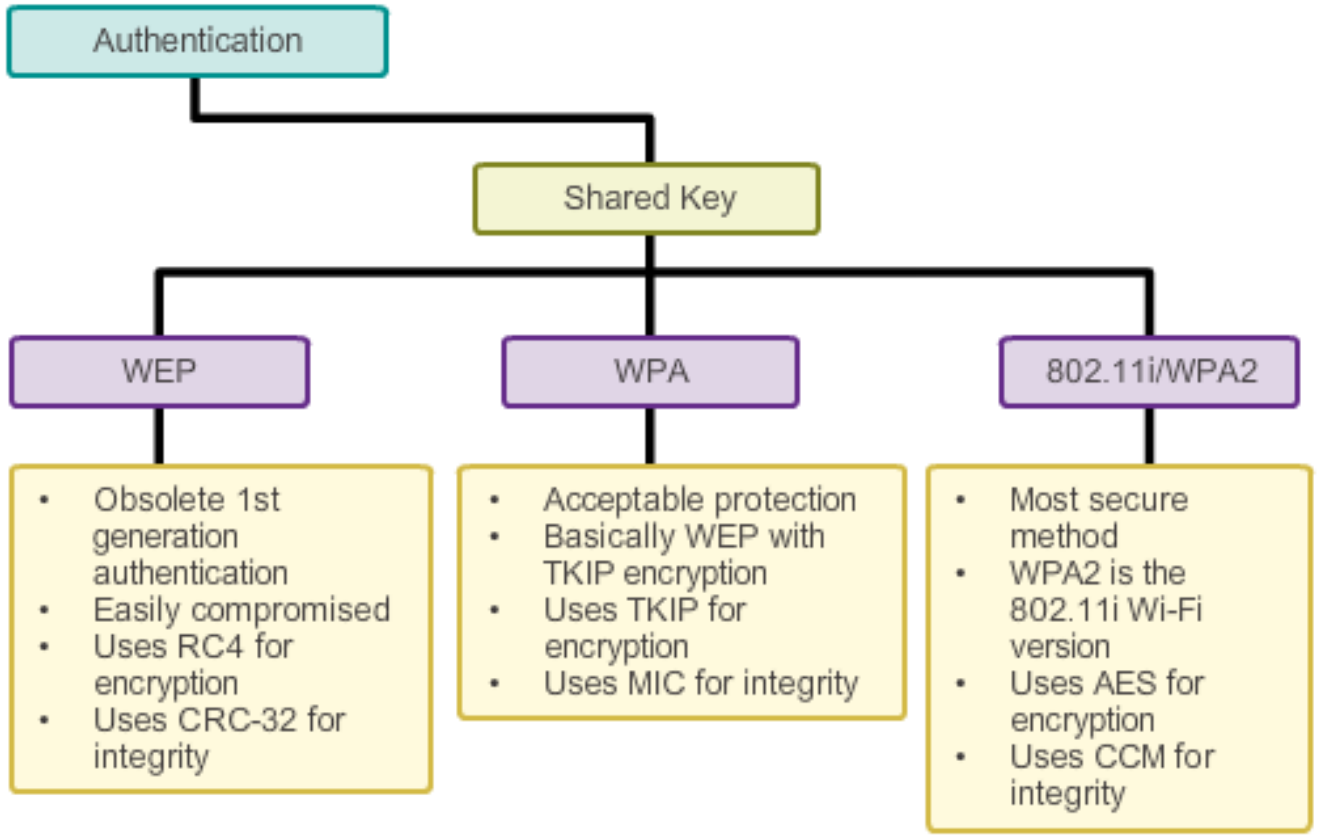
Autentifikácia na domácom wifi smerovači

- Zväčša je pre WPA a WPA2 na výber z dvoch typov autentifikácie:
- **Personal**
  - Určené pre domáce siete alebo siete malých kancelárií alebo pre overených používateľov, ktorí používajú zdieľaný kľúč (PSK). Nevyžaduje sa žiadny špeciálny autentifikačný server.
- **Enterprise**
  - Vyžaduje autentifikačný server – Remote Authentication Dial-In User Service (RADIUS).
  - Poskytuje dodatočnú bezpečnosť.
  - Používatelia sa musia overiť pomocou štandardu 802.1X, ktorý na overenie používa protokol EAP (Extensible Authentication Protocol).



Ochrana aktívnych prvkov siete

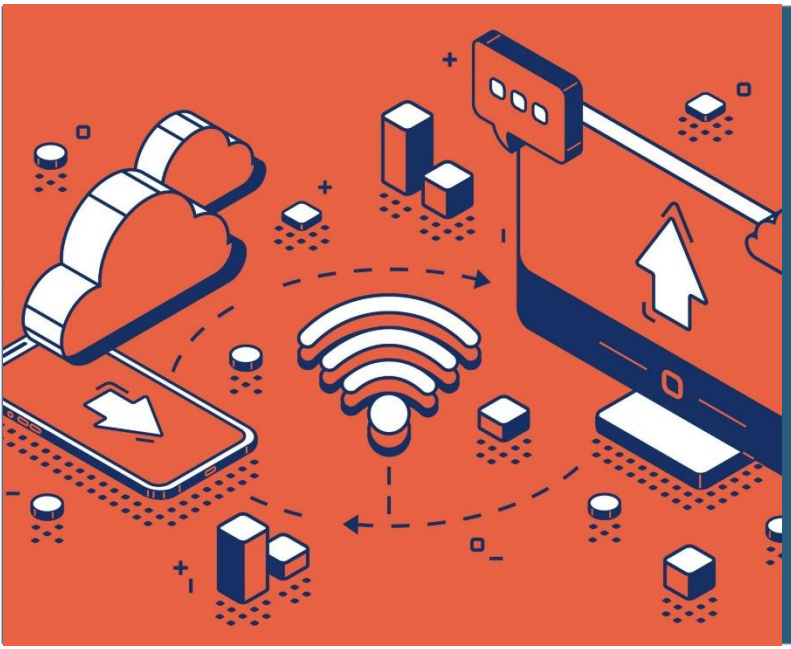
- Ochrana aktívnych prvkov cez zabezpečenie prístupu k ich administračnému rozhraniu
  - Prístupové body a mosty sú manažovateľné zariadenia a umožňujú vzdialenú konfiguráciu
- Veľmi často je možné stretnúť sa s nasadeným aktívnym prvkom siete s nezmenenými heslami od výrobcu
- Je zásadne potrebné
  - Zmeniť prístupové mená a heslá
  - Pokiaľ je to možné, obmedziť rozsah IP adries, z ktorých môže byť zariadenie riadené
- Sebalepšie zariadenie nebude prínosom k bezpečnosti, ak nie je adekvátne nakonfigurované



Zhrnutie metód

Odporúčanie zabezpečenia WiFi

1. Zapnite šifrovanie.
   - Najlepšie možné je WPA2
   - Ďalšou možnou alternatívou je WPA
   - V prípade, že predchádzajúce šifrovania sa nedajú použiť (do siete sa budú pripájať zariadenia, ktoré ich nepodporujú), zapnite aspoň WEP, aj jednoduché šifrovanie
2. Zmeňte prednastavené prístupové heslá na prístupové body a WiFi smerovače.
   - Tieto heslá sú útočníkom známe a dajú sa ľahko zneužiť pre prístup do siete.
3. Zmeňte prednastavené meno siete (SSID).
   - Útočníci poznajú väčšinu prednastavených mien sietí a vyvodia si z toho, že daná sieť nie je dostatočne zabezpečená.
   - Nastavte ich tak, aby jednotlivý užívatelia mohli ľahko identifikovať, ku ktorému prístupovému bodu sa chcú pripojiť.
   - Nepoužívajte názvy firmy, alebo mená, ktoré by boli pre útočníkov veľmi nápadne (napríklad OMEGA-SKLAD).
4. Vypnite zdieľanie tlačiarní a súborov v sieti, ak ich nepotrebujete.
   - Znemožníte tak prístup k údajom prípadnému útočníkovi, ktorý prelomí prístupový bod.
5. Umiestnite prístupové body tak, aby ich signál pokrýval len územie, kde to je nevyhnutne potrebné.
   - Používajte radšej sektorové antény na pokrytie miestností a umiestnite ich do rohov.
   - Niektoré prístupové body umožňujú nastaviť silu vyžarovaného signálu.
   - Nastavte ich len na takú silu, aby bolo možne na ne sa pripojiť len z bezpečnej vzdialenosti (vnútro budov).
6. Medzi bezdrôtovú sieť a lokálnu sieť umiestnite firewall
   - .. na ktorom povolíte len nevyhnutné služby (WEB, MAIL).
   - Toto znemožní útočníkom prístup do siete a dovolí im len „bezpečné služby“.



Diagnostika

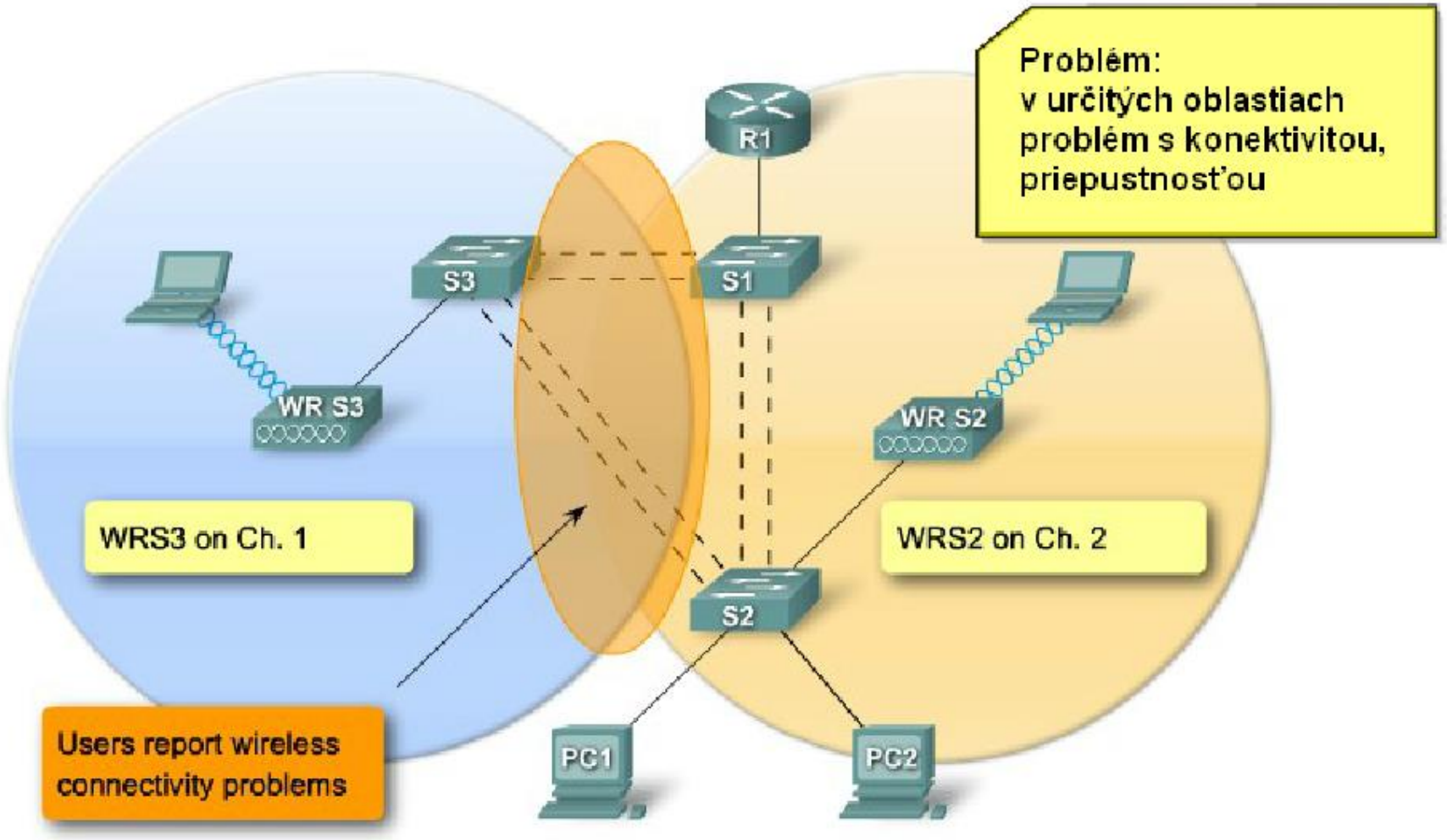
Diagnostické prístupy

Je viacero diagnostických postupov:

- **Bottom-up** – Začni na Layer 1 a postupuj smerom nahor.
- **Top-down** – Začni na najvyššej vrstve a postupuj dole.
- **Divide-and-conquer** – začni v strede, napr. Ping
  - Ak ping nejde postupuj dole
  - Ak ping úspech, pokračuj hore

Riešenie problémov

- Vykonávaj upgrade firmware



UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Ďakujem za pozornosť

Obsahom bola téma WLAN.

Chapter 12: WLAN Concepts (bolo v tejto prednáške).
Chapter 13: WLAN Configuration
(bude na cvičení, prečítať z Netacadu samostatne, ako príprava)

Vyjadrite svoj názor na prednášku tohto týždňa (alebo cvičenie).

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.