



Wireless LAN



M4, CCNA, v5

Pavel Segeč

Katedra informačných sietí

Fakulta riadenia a informatiky, ŽU

Wireless technológie

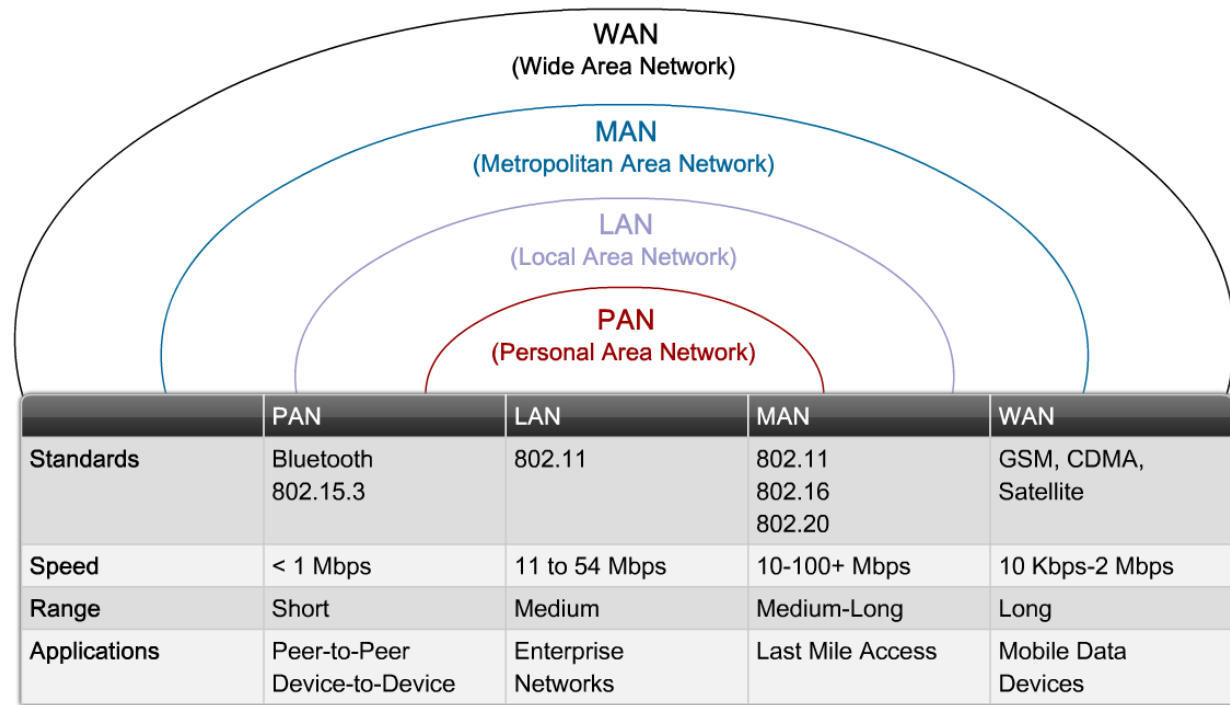
- Využitie elektromagnetického vlnenia pre vysokorýchlostný prenos dát
 - „Rádiové“ vlny
 - Svetlo (bez svetlovodu, využívané zriedkavo)
- Výhody:
 - Plošné pokrytie
 - Mobilita
 - Operatívnosť, flexibilita
 - Možnosť preklenúť pomerne veľké vzdialenosti a relatívne náročný terén

Wireless technológie

■

WLAN technológie

Wireless LANs



- Wireless LAN (WLAN) technológie sú tá časť bezdrôtových komunikačných technológií, ktoré poskytujú služby tradičných LAN sietí
 - Nepatrí sem Bluetooth, GSM apod.
- V súčasnosti sú v oblasti WLAN najpoužívanéjšie štandardy IEEE 802.11

Wireless LAN technológie

- WLAN nie sú náhradou existujúcich „wired“ LAN sietí
 - Prenosové rýchlosti vo WLAN sieťach sú stále o rád nižšie než v LAN
 - 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 pozerat' sa na WLAN
 - ako na pokračovanie a predĺženie bežných LAN sietí a v tomto zmysle ich aj nasadzovať

Porovnanie LAN a WLAN

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

Základné pojmy

- **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

■ Modulácia

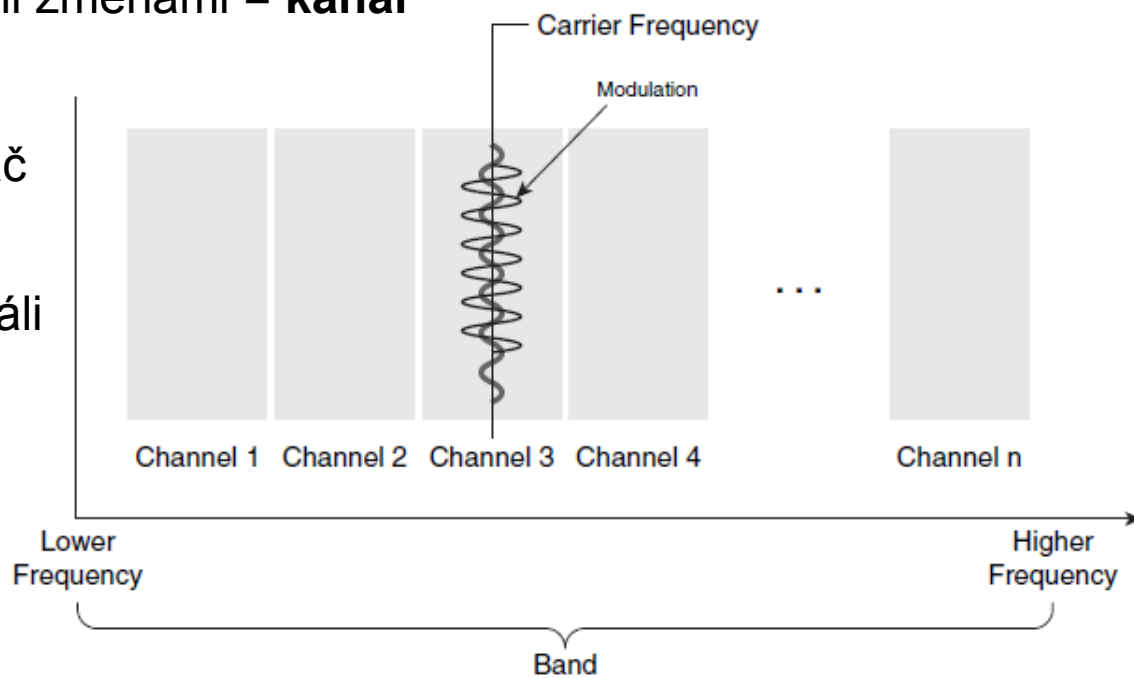
- Zmena istej charakteristiky prenášaného signálu, ktorou bude vyjadrený prenášaný symbol počas prenosu
- Amplitúdová, fázová, frekvenčná

■ Kanál (Channel)

- Kvôli tejto zmene prijímač aj vysielač síce očakávajú nosnú na určitej frekvencii ale s malými zmenami = **kanál**

■ Frekvenčná schéma

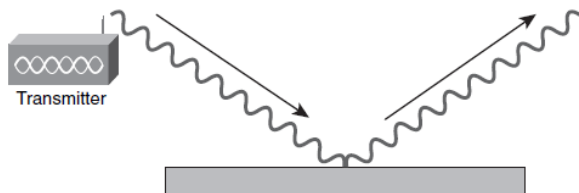
- Spôsob, akým vysielač obsadzuje rozsah frekvencií v danom kanáli



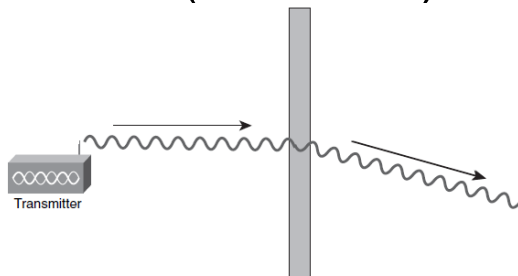
Radiofrekvenčný signál

- Vplyv prostredia

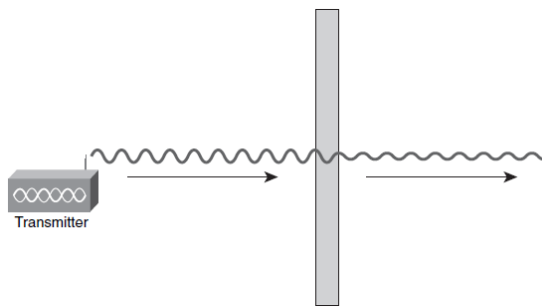
- Odraz (reflection)



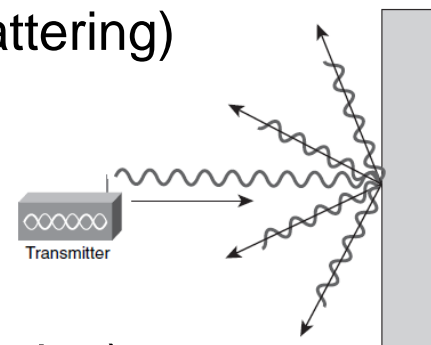
- Lom (refraction)



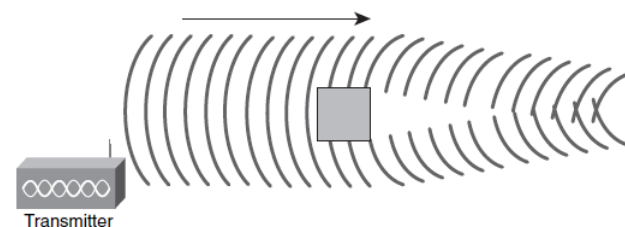
- Absorbcia (absorbction)



- Rozptyl (scattering)



- Ohyb (diffraction)



Prenosové modulačné techniky

■ Frequency Hopping Spread Spectrum (FHSS):

- Vysielač a prijímač prechádzajú medzi frekvenciami v danom kanáli podľa istej pseudonáhodnej postupnosti
 - Sekvencia obsahuje až 78 frekvencií
- V každom časovom momente sa využíva len jedna konkrétna frekvencia
 - Ak prenos rámca zlyhá, rámec sa prenesie znovu ale na inej frekvencii (next hop)
- Nevyhnutná je synchronizácia pseudonáhodných generátorov a momentov prechodu medzi frekvenciami

Prenosové modulačné techniky

- **Direct Sequence Spread Spectrum (DSSS):**
 - 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 spektra
 - Takisto ako pri FHSS, aj tu je potrebná synchronizácia pri pseudonáhodnom kóde
 - DSSS je **využívaná v súčasných WLAN sieťach**

Prenosové modulačné techniky

■ Orthogonal Frequency Division Multiplexing (OFDM)

- Rodina modulačných techník, ktoré využívajú rozdelenie kanála na tzv. subkanály a simultánny prenos informácie týmito kanálmi
- Komplexná technika využívaná vo vysokorýchlostných prenosoch (802.11a/g, DSL apod.)

Štandardy IEEE

- **Institute of Electrical and Electrical Engineers**

- Štandardizačná organizácia v oblasti WLAN sietí

- Štandardy IEEE týkajúce sa WLAN sietí:

- 802.11a – 54 Mbps, 5 GHz
 - 802.11b – 11 Mbps, 2.4 GHz
 - 802.11g – 54 Mbps, 2.4 GHz
 - 802.11n – 248 Mbps, 2.4 GHz a 5GHz

 - 802.11ac – rozšírenie n, dualband 2,4/5GHz 1,3Gbps na 5Ghz, 450Mbps na 2,4GHz(Wave 2)
 - 802.11ad – WiGig, triband 2,4/5/60GHz, 7Gbps,
 - 802.11af – superWifi, 54 and 790 MHz (TV spektrum|, 426,7Mbps

 - 802.11e – prostriedky pre QoS vo WLAN
 - 802.11i – zabezpečenie WLAN sietí

802.11 wireless štandardy - zhrnutie

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11 a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11 a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11 a/b/g/n/ac

Štandard 802.11a

- Pôvodne menej známy a menej používaný štandard, v súčasnosti naberá na popularite
- 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

Štandard 802.11b

- Veľmi populárny a široko nasadzovaný štandard
- Relatívna cenová dostupnosť 802.11b zariadení naštartovala súčasný 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

Štandard 802.11g

- Späťne plne kompatibilný s 802.11b
- 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
- V sieti môžu byť kombinované 802.11b a 802.11g prvky
 - Každý bude komunikovať na vlastnej rýchlosti
 - Celkový prenosový výkon bude o niečo znížený

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:
 - Späťne 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 rýchlosti na 248 Mbps (niektoré správy tvrdia dokonca o 600 Mbps), reálna prenosová rýchlosť cca 74 Mbps
- Dlhší dosah, cca 70 metrov

WiFi aliancia



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

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



[p://www.cisco.com/go/ciscocompatible/wirele](http://www.cisco.com/go/ciscocompatible/wirele)

Komponenty a činnosť WLAN sietí



Nasadenie WLAN sietí predpokladá:

- Koncové zariadenia
- Zariadenia infraštruktúry

Komponenty WLAN

Bezdrôtový klient

- WLAN klient
 - Koncová členská stanica WLAN siete
 - Konektivita klienta je zabezpečená špecializovanou bezdrôtovou sieťovou kartou
 - Existujú rôzne vyhotovenia bezdrôtových sieťových kariet s rôznymi rozhraniami



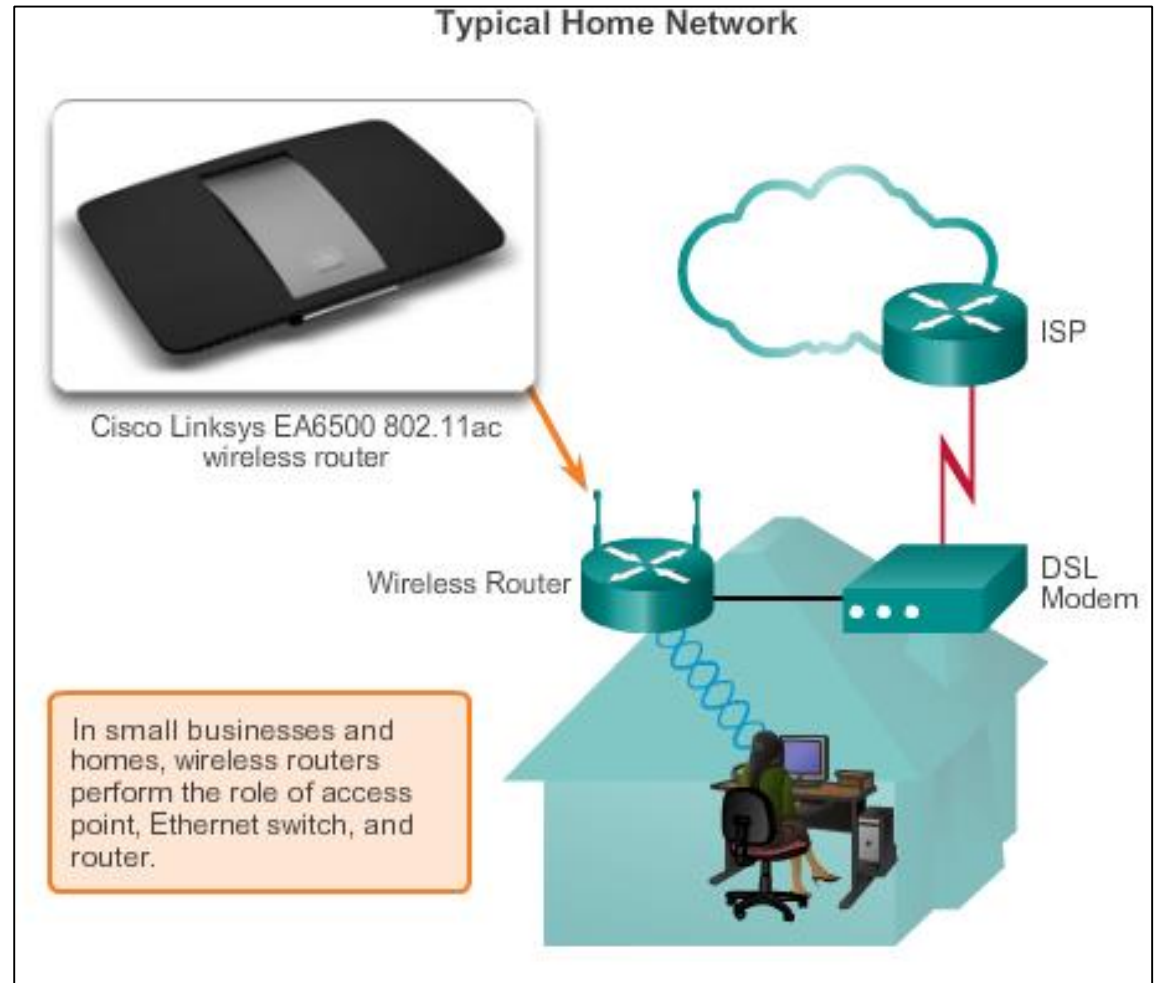
Komponenty WLAN

Wireless Home Router

- Domáci používateľ skôr využíva integrated wireless router.
 - Integrácia viac zariadení

Napr.

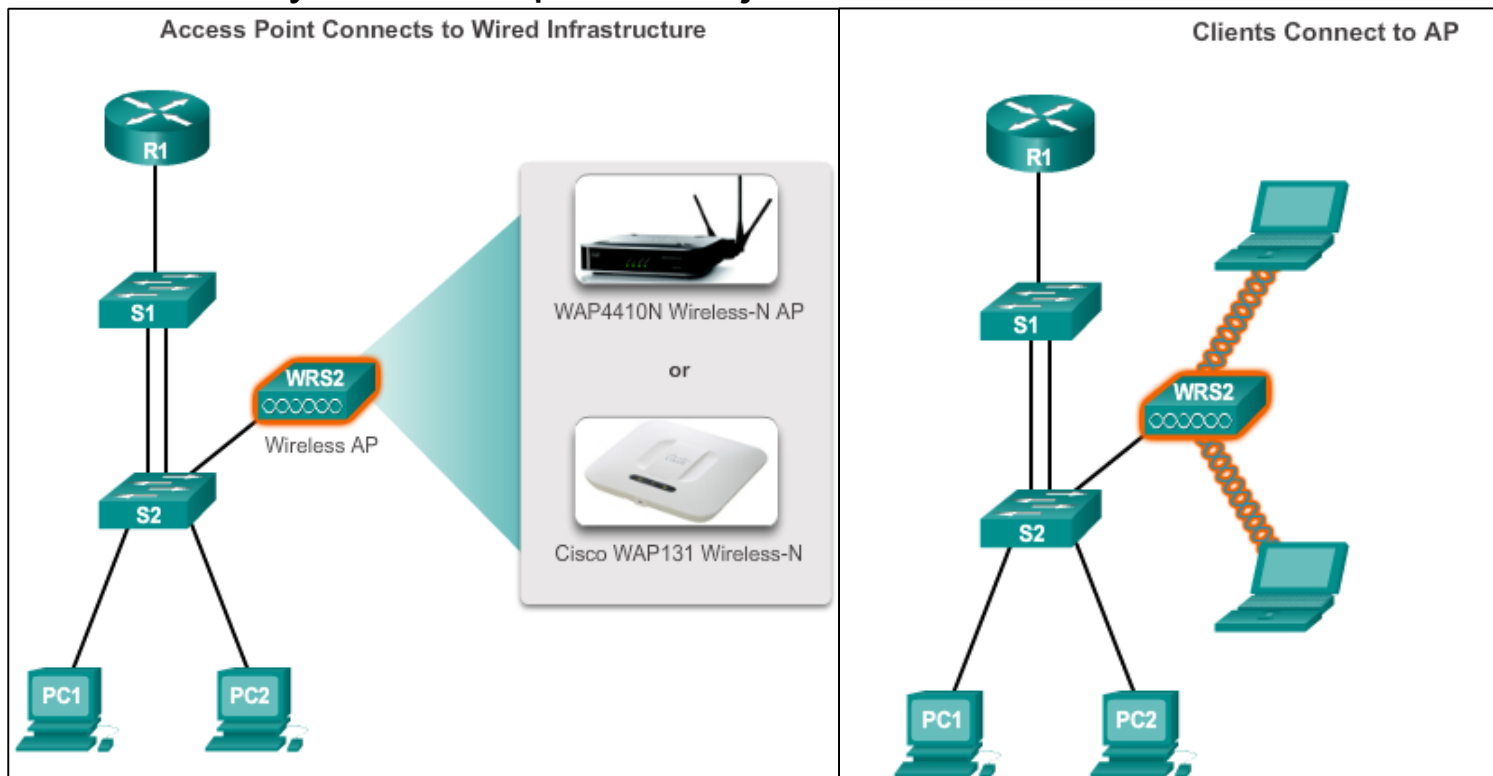
- access point
- Ethernet prepínač
- Smerovač (wan rozhranie)



Komponenty WLAN

Prístupový bod

- Prístupový bod – access point (AP):
 - Typicky pripojený do siete metalickým médiom
 - Zabezpečuje vzájomnú komunikáciu WLAN klientov a spojenie WLAN s LAN
 - Rôzne vyhotovenia pre vonkajšie/vnútorne inštalácie



Riešenia pre malé siete

Cisco Small Business Autonomous APs



Cisco WAP4410N

- Intro-level small business AP
- Configured using a GUI
- Powered using AC or PoE



Cisco WAP121 and WAP321

- Mid-level small business APs
- Configured and managed using a GUI or CLI
- Supports clustering with Single PointSetup
- Powered using AC or PoE

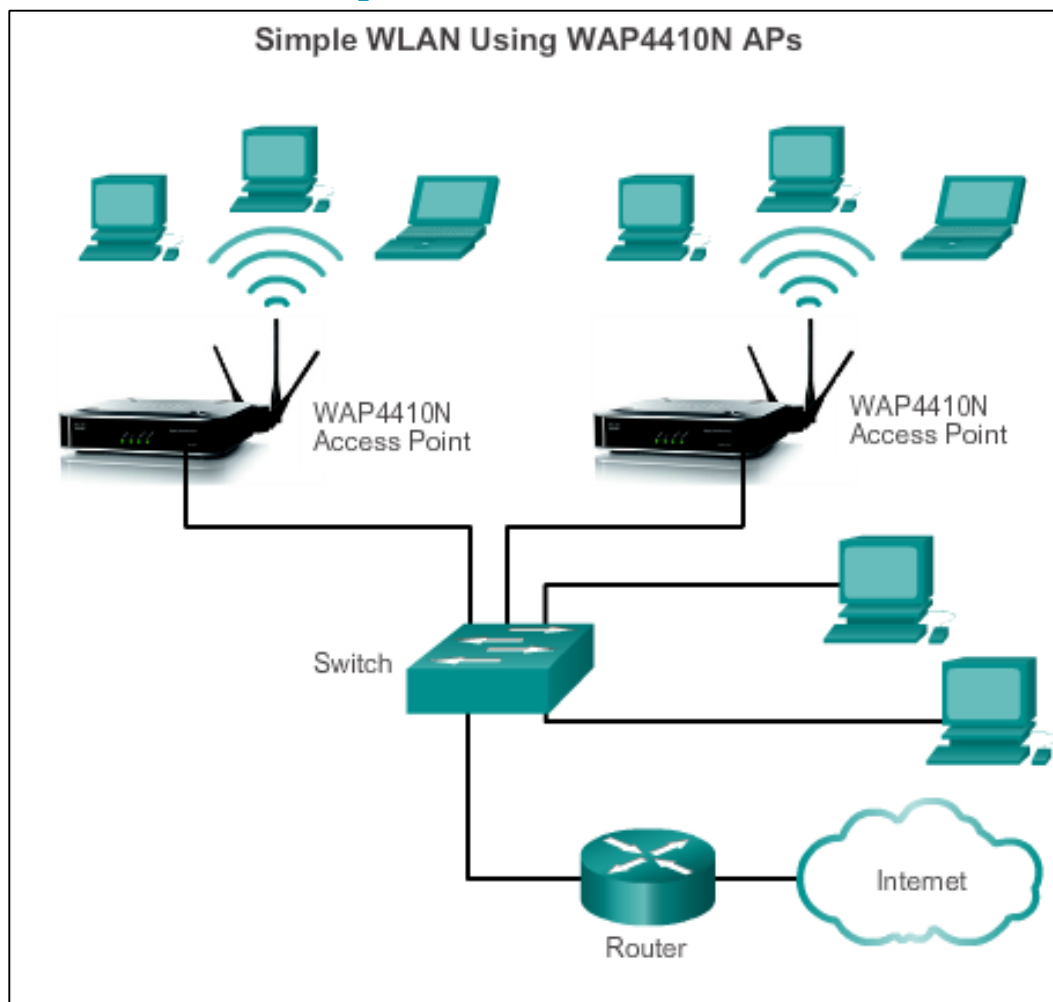


Cisco AP541N

- Mid-level small business APs
- Configured using a GUI
- Supports controller-less clustering technology
- Powered using AC or PoE

Komponenty WLAN

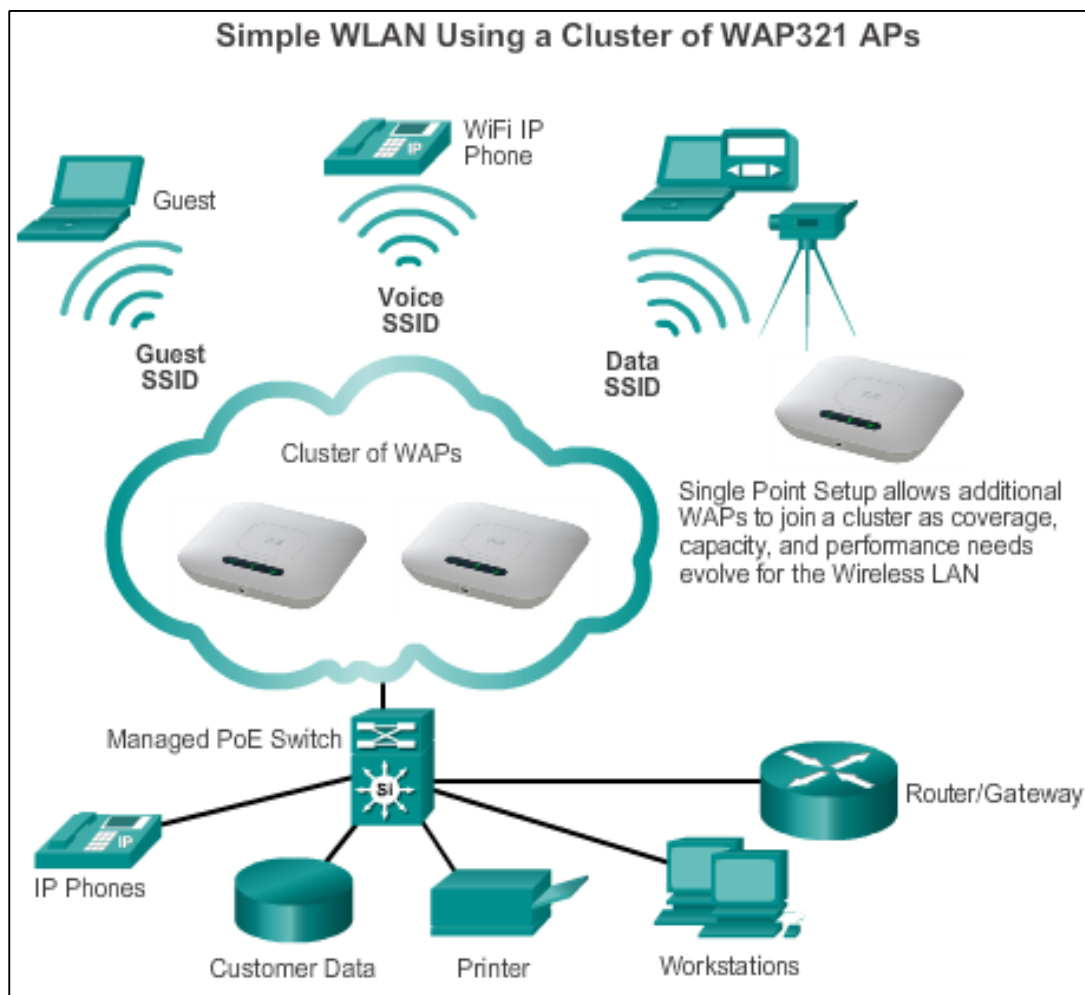
Riešenia pre malé siete



- Autonómne AP
 - Každé sa konfiguruje a spravuje individuálne.
 - Problém ak je veľa AP

Komponenty WLAN

Riešenia pre malé siete



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

Components of WLANs

Large Wireless Deployment Solutions

- For larger organizations with many APs, Cisco provides controller-based managed solutions, including the Cisco Meraki Cloud Managed Architecture and the Cisco Unified Wireless Network Architecture.
- Cisco Meraki cloud architecture is a management solution used to simplify the wireless deployment. Using this architecture, APs are centrally managed from a controller in the cloud.



Components of WLANs

Large Wireless Deployment Solutions (cont.)

Controller-Based Wireless APs



Cisco Aironet 1600, 2600, and 3600 Series
Robust controller-based APs



Cisco Aironet 600 Series OfficeExtend
Used to extend 802.11n wireless coverage to the home teleworking environment



Cisco 1552 Series Outdoor Rugged APs
Robust outdoor controller-based AP

Components of WLANs

Large Wireless Deployment Solutions (cont.)

Controllers for Small and Medium-Sized Businesses



Cisco Virtual Controller



Cisco Wireless Controller on the
Cisco Services Ready Engine
(SRE)



Cisco Wireless Controller on the
Cisco Services Ready Engine
(SRE)

Komponenty WLAN

Bezdrôtové mosty

- Most – bridge:
 - Zabezpečuje bezdrôtové prepojenie dvoch separátnych LAN sietí
 - Spojenia point-to-point alebo point-to-multipoint
 - Mosty často používajú mierne upravený komunikačný protokol pre efektívnejšiu komunikáciu



Ďalšie komponenty WLAN sietí

- 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, sektorové, smerové
 - Líšia sa použitým druhom konektora, káblom, ziskovosťou, smerovosťou...
 - Cisco zariadenia používajú konektory RP-TNC





Spôsoby prevádzky WiFi



Základné topológie WLAN sietí

- **Independent Basic Service Set (IBSS):**

- Sieť tvorená výlučne WLAN klientmi bez centrálného prvku
- Často nazývaná aj **Ad-hoc** sieť,
- alebo v poslednej dobe **Tethering** (mbt hotspot)

- **Basic Service Set (BSS):**

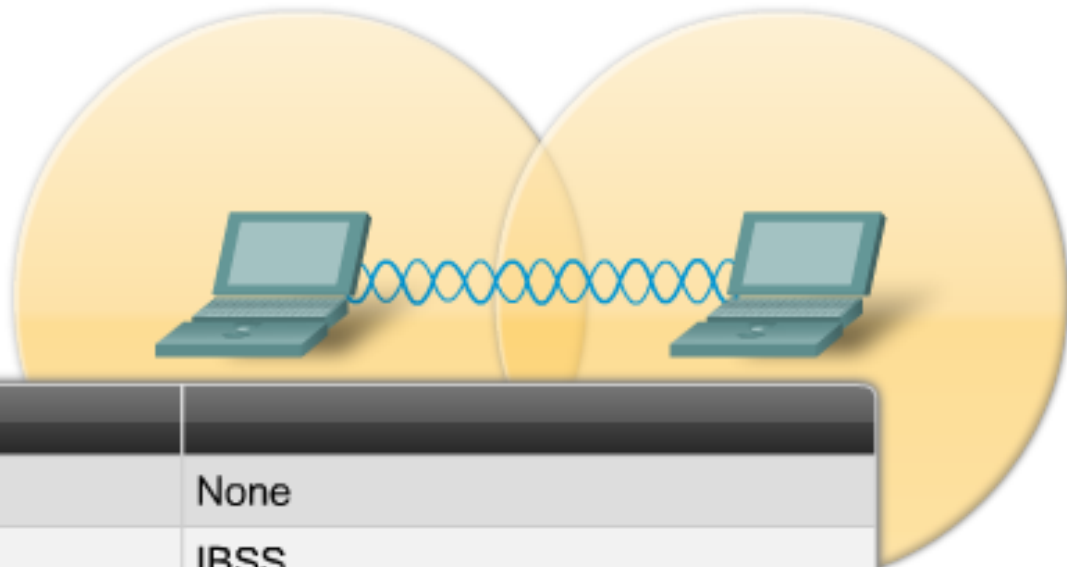
- WLAN sieť tvorená prístupovým bodom a klientami
- Nazývaná aj Infrastructure (Infra-BSS)
 - Mode infrastructure

- **Extended Service Set (ESS):**

- WLAN sieť skladajúca sa z niekoľkých BSS sietí, prepojených tzv. distribučným systémom
 - Mode infrastructure

Základné topológie WLAN sietí

Ad-hoc mód - IBSS

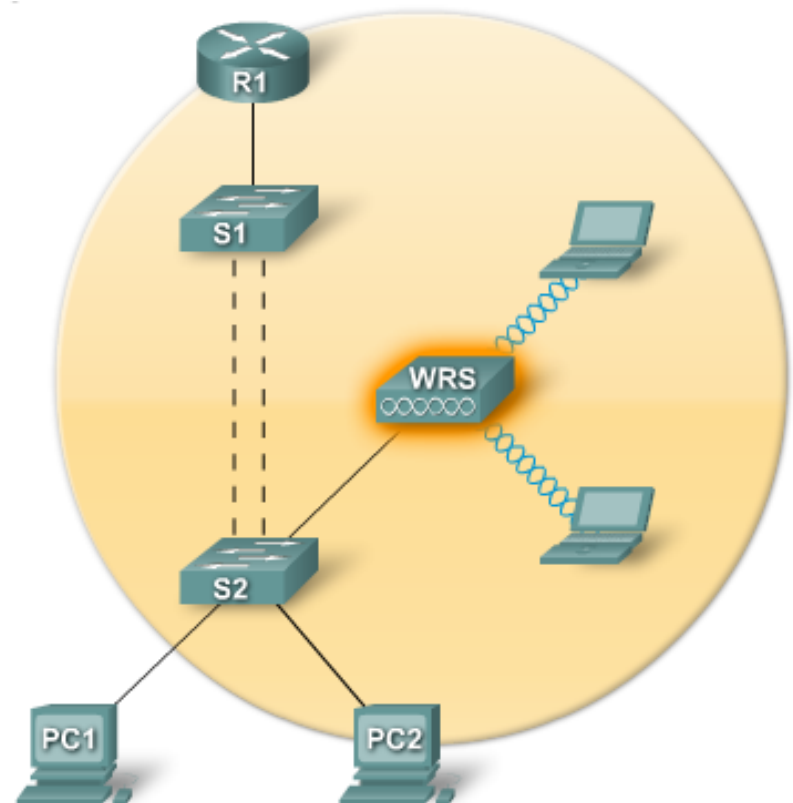


APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

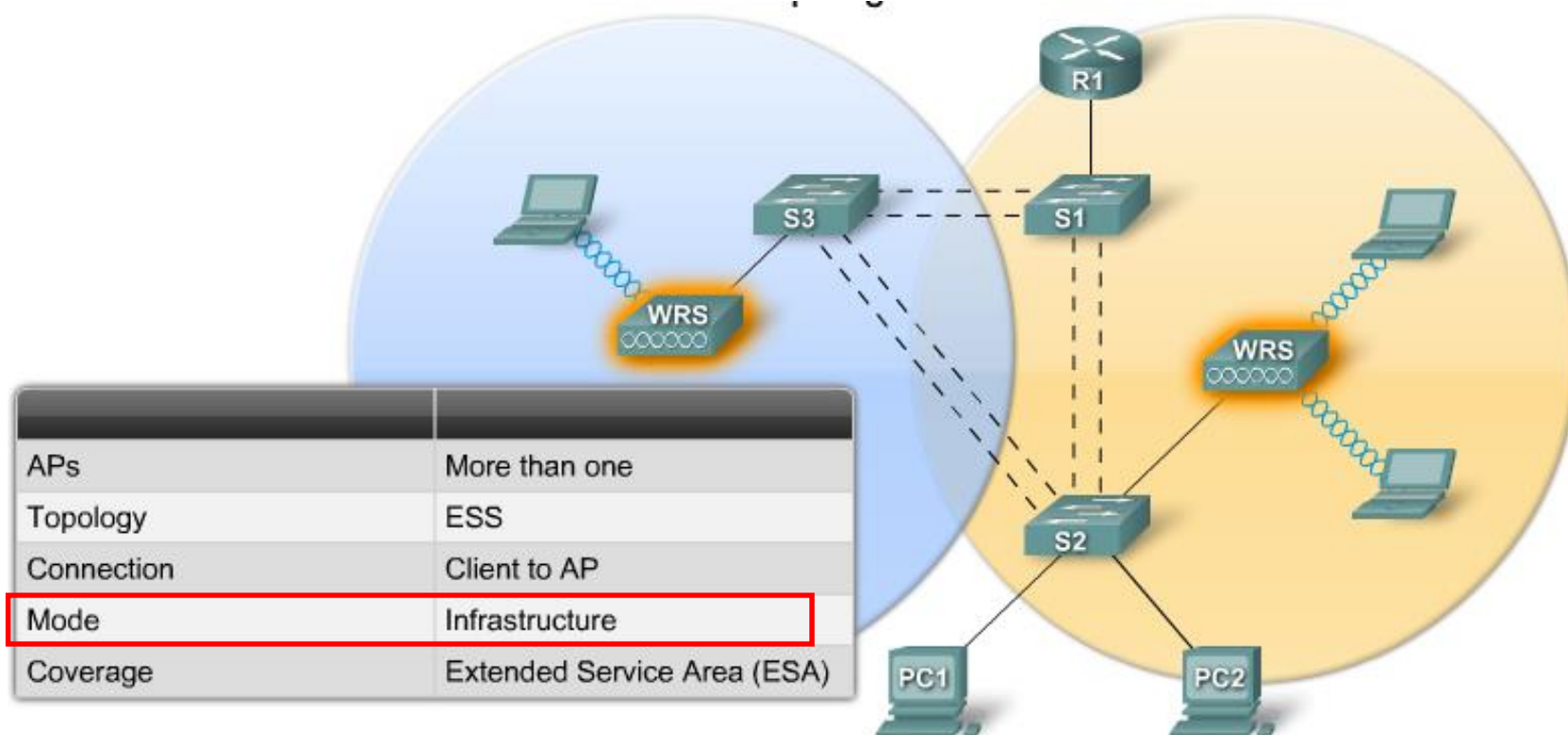
Základné topológie WLAN sietí

Mód infraštruktúra – Basic Service Set

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



Mód infraštruktúra – Extended Service Set





Wireless LAN činnosti

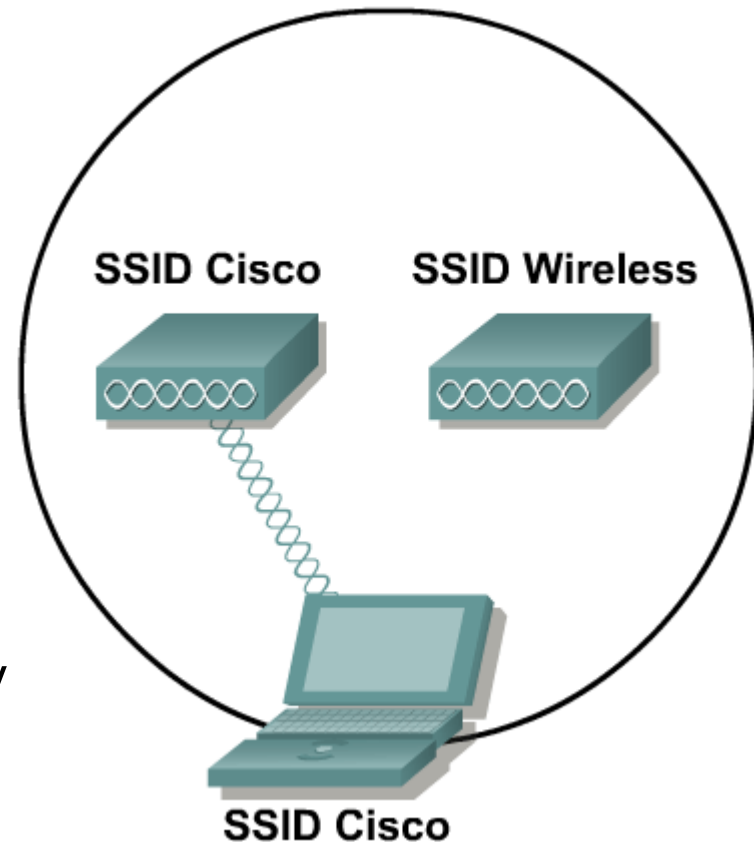


Základné formy WLAN sietí

- 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 prístupujúceho k WLAN sieti
- 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**

Identifikátor bezdrôtovej siete – SSID

- SSID (Service Set ID) je slovný názov bezdrôtovej siete
 - AP môže SSID vysielat' vo svojich tzv. beacon rámcoch
 - SSID môže byť aj skryté
- 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 objavenie AP klientom

Passive mode

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

Komunikácia vo WLAN sieti

- Proces prístupu klienta k bezdrôtovej sieti má 3 fázy:
 - 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
 - Autentifikácia
 - Open,
 - Shared Key

Komunikácia vo WLAN sieti – CSMA/CA

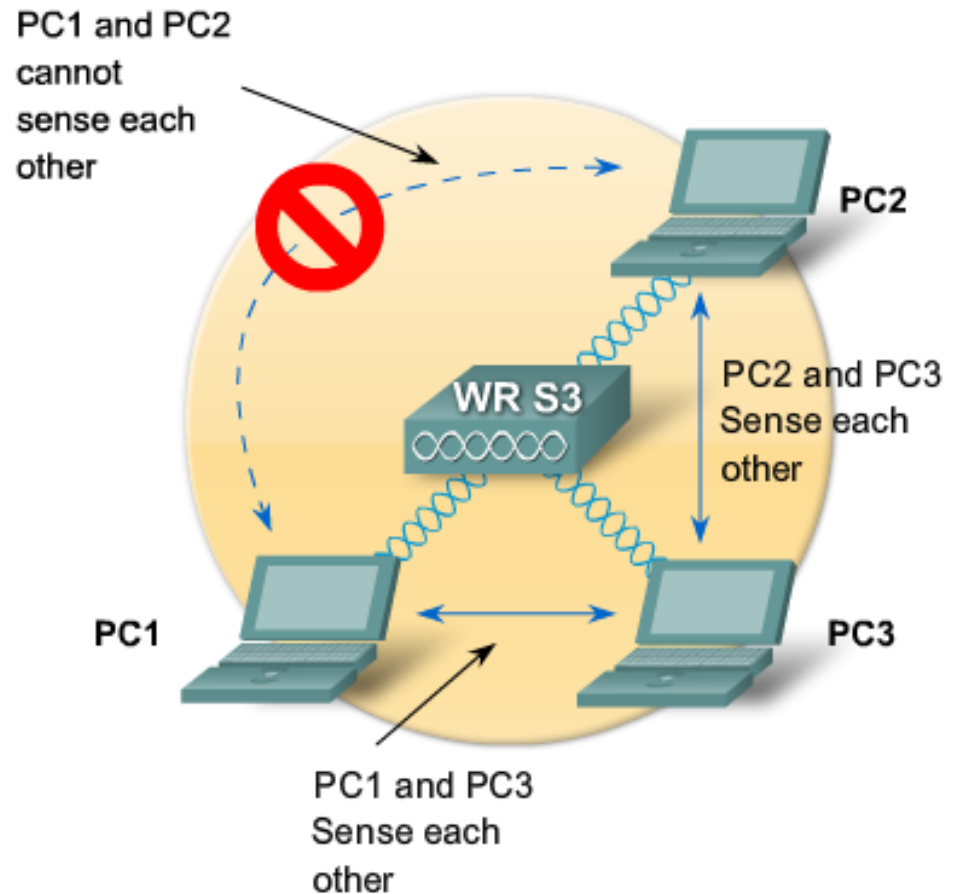
- WLAN klienti sa vzájomne musia počuť („vidieť“)
 - dáta si prenášajú výlučne prostredníctvom prístupového bodu
- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance (DCF - Distributed Coordination Function)
 - Vo WLAN nemôžem použiť CSMA/CD
 - CSMA pracuje dobre (ak som jediný čo prenáša, resp. vidím ak komunikuje niekto iný)
 - Avšak CD nefunguje - Odosielajúca stanica nevie zistiť, či spôsobila kolíziu
 - Problém na rádiu aj vysielat' aj prijímať
 - “Hidden node” problem
 - Preto pre WiFi máme modifikáciu klasickej CSMA metódy
 - Vyhnutie sa kolízií
 - Distribuovaná koordinačná funkcia (DCF)
 - RTS/CTS
 - Prijímajúci host posiela ACK krátko po prijatí správy (Short IFS)
 - Ak ACK nie je prijaté = znovu prenos

Hidden node problém

The Hidden Node Problem:

- PC1 and PC2 reach WRS3
- PC1 and PC2 cannot reach each other
- PC1 does not detect PC2 activity on the channel
- PC1 sends data while PC2 is transmitting
- A collision occurs

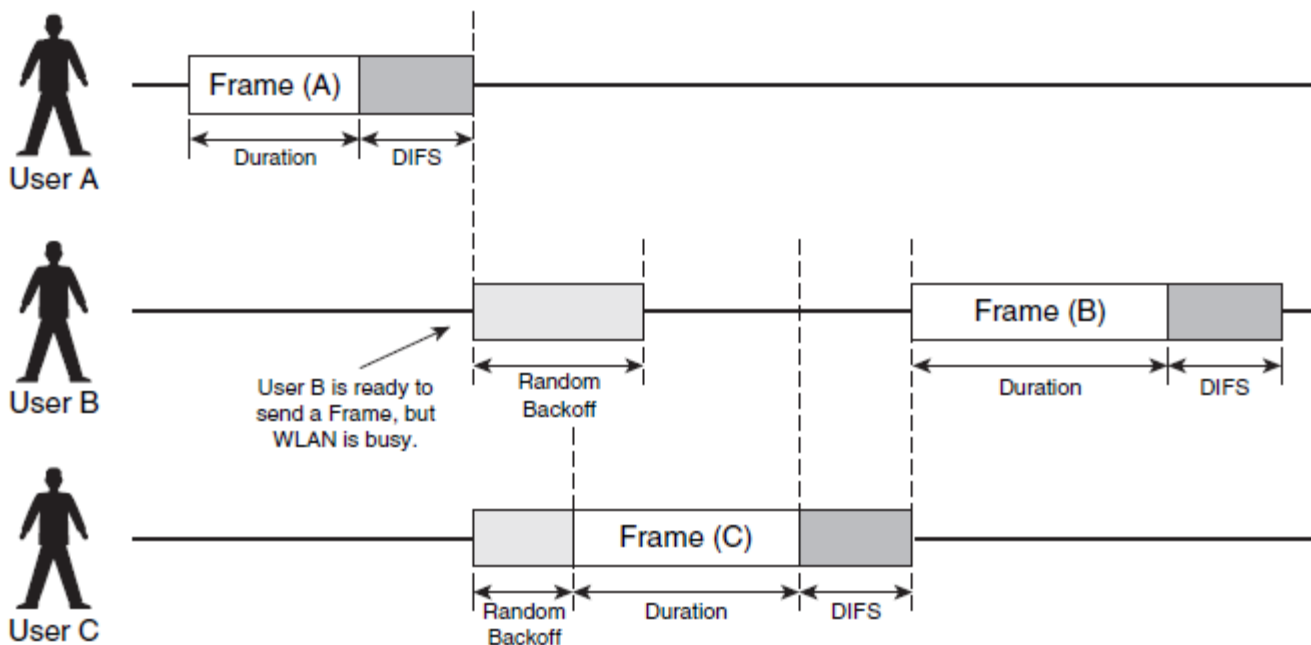
PC3 is sensed by both PC1 and PC2, so there are no collisions involving PC3.



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 vysielat' – 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 + random

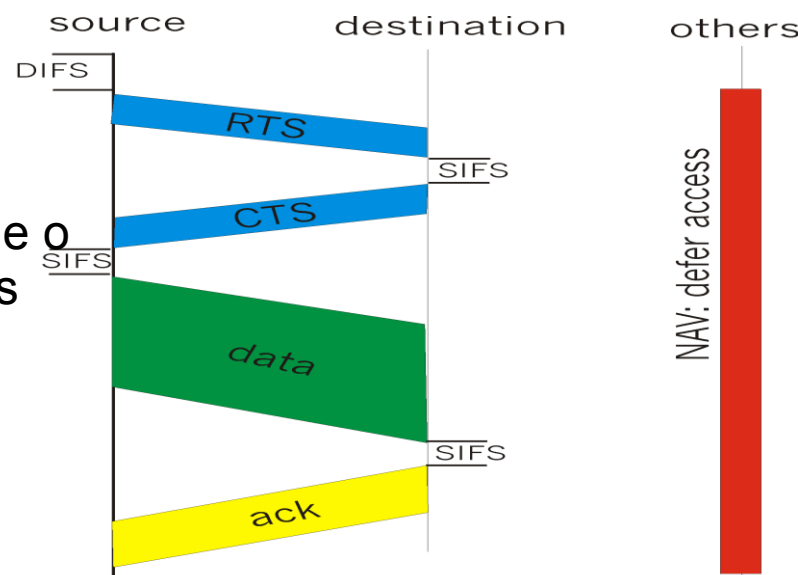
3. B počká náhodný backoff čas kým sa pokúsi znova preniesť frame.
4. Kým B čaká, objaví sa C, ktorý chce tiež prenášať rámec. Detekuje a zistí, že nik neprenáša, C počká náhodný čas, ktorý je kratší ako náhodný čas B
5. C prenesie rámec a zároveň dá info o dobe trvania prenosu
6. B teraz musí počkať 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 vysielat' – 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

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 vysielateľa a prijímateľa dodržať ticho a nekomunikovať



Komunikácia vo WLAN sieti

- 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

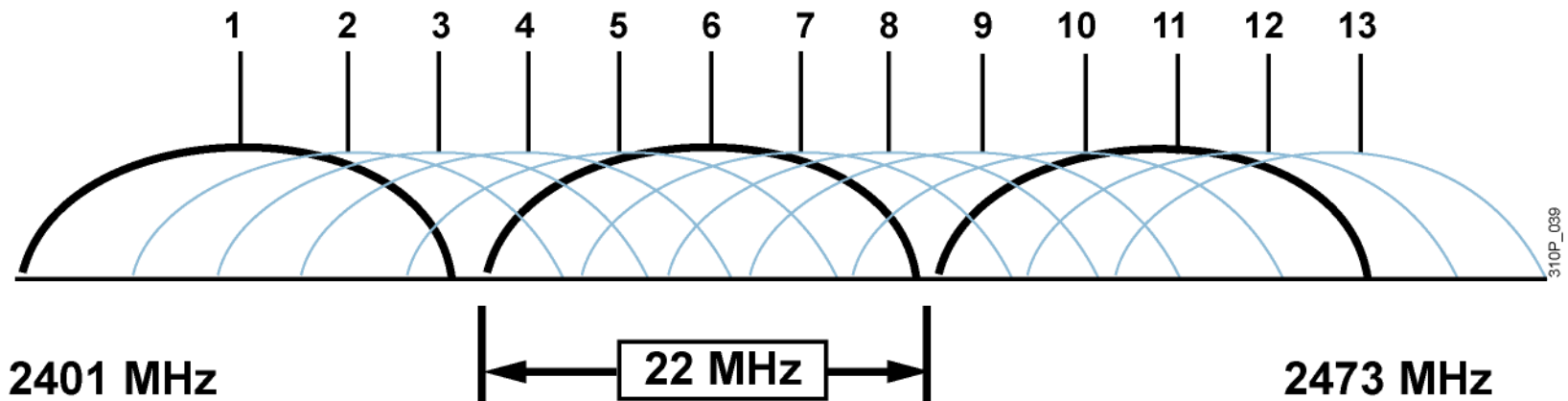
Manažment kanálov

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

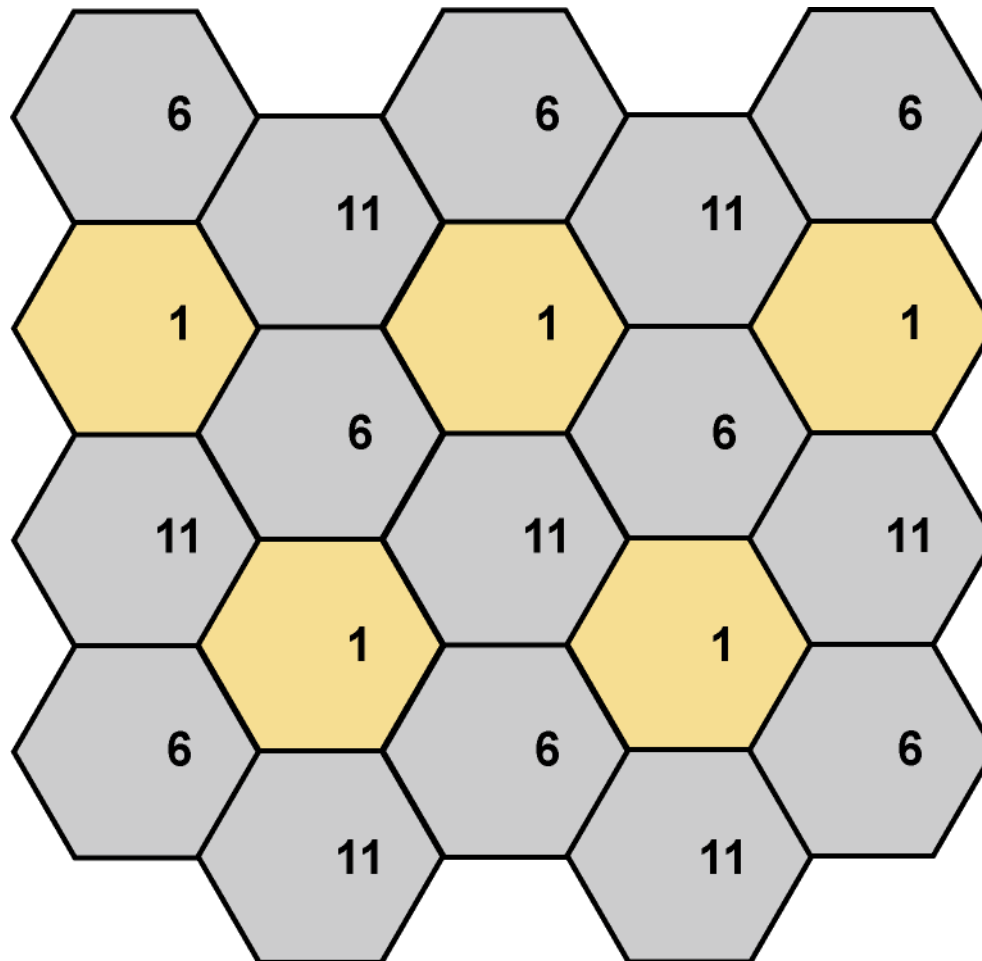
2.4-GHz Channel Use

802.11 b/g 2.4-GHz Channels

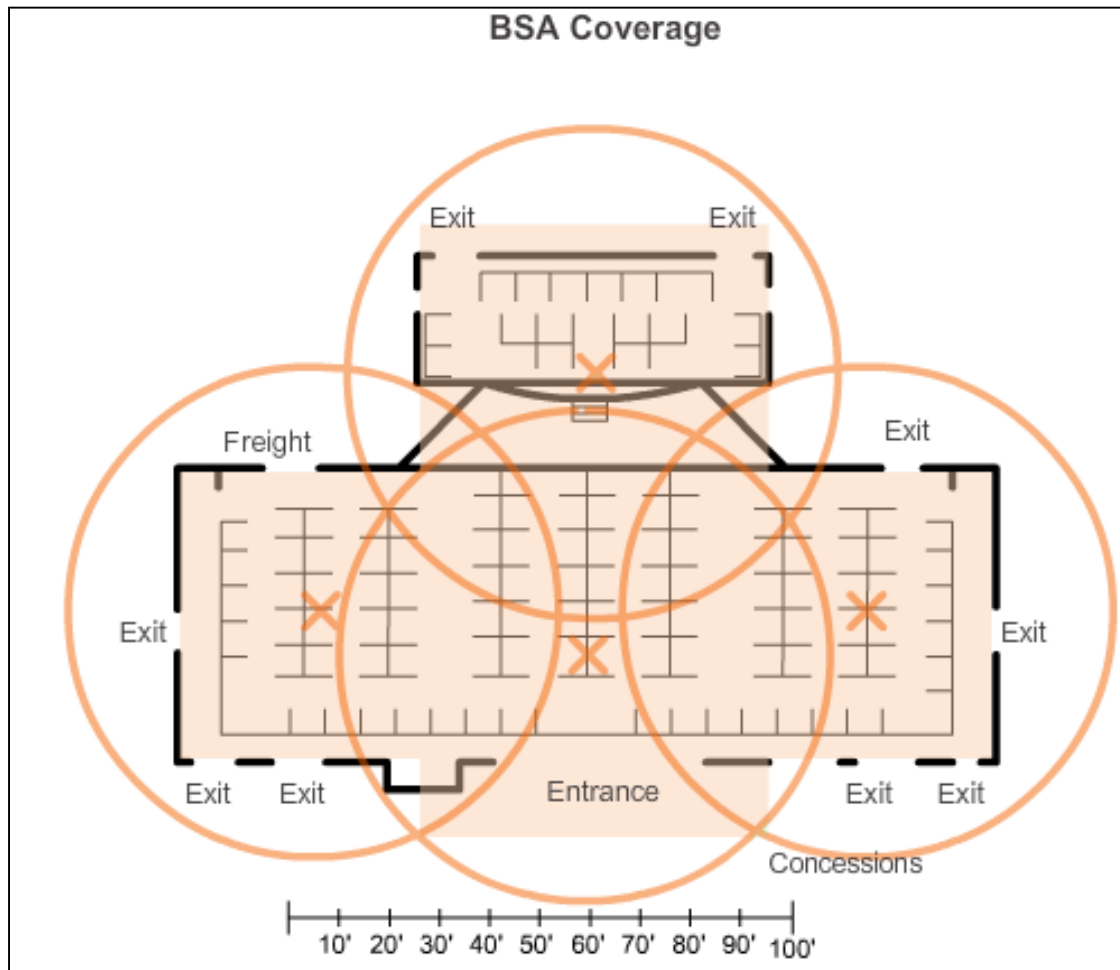


- Each channel is 22 MHz wide.
- North America: 11 channels
- Europe: 13 channels
- There are three nonoverlapping channels: 1, 6, 11.
- Using any other channels will cause interference.
- Three access points can occupy the same area.

802.11b/g (2.4 GHz) Channel Reuse



Plánovanie WLAN nasadenia



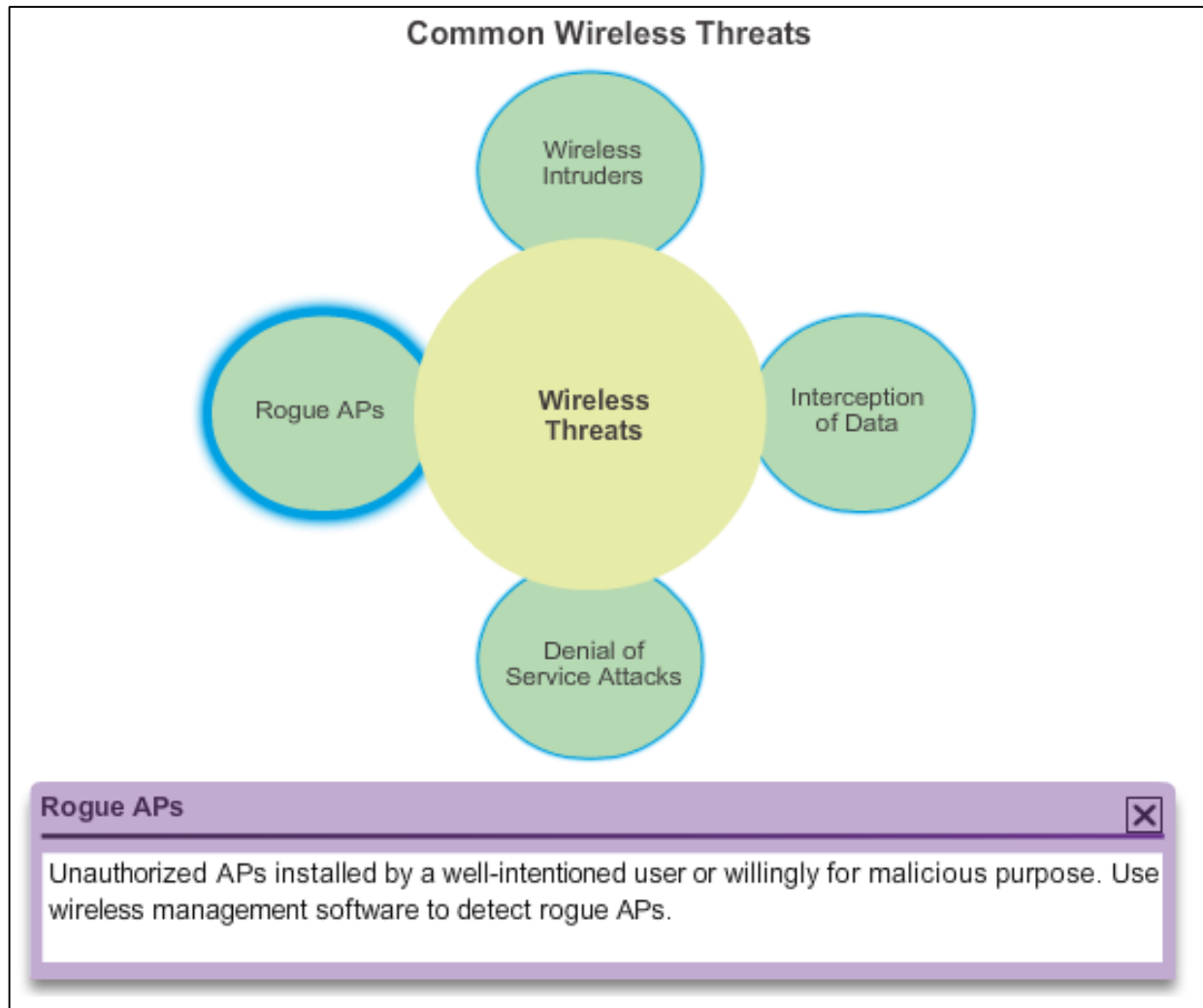
- Ber do úvahy
 - Počet používateľov
 - Následne plánovanú priepustnosť
- Pri nasadení AP zvaž
 - Napojenie na kabeláž
 - Napájanie
 - Či je priestor na umiestnenie
- Extra zvaž
 - Umiestni AP nad prekážky
 - Umiestni tesne pod strop v centra každej oblasti
 - Umiestni AP tam kde budú používatelia



WLAN bezpečnost'



Securing Wireless



WLAN Threats

DoS Attack

Wireless DoS attacks can be the result of:

- Improperly configured devices.
- Configuration errors can disable the WLAN.
- A malicious user intentionally interfering with the wireless communication. Disable the wireless network where no legitimate device can access the medium.

Accidental interference

- WLANs operate in the unlicensed frequency bands and are prone to interference from other wireless devices.
- May occur from such devices as microwave ovens, cordless phones, baby monitors, and more.
- 2.4 GHz band is more prone to interference than the 5 GHz band.

Management Frame DoS Attacks

A spoofed disconnect attack

- Occurs when an attacker sends a series of “disassociate” commands to all wireless clients.
- Cause all clients to disconnect.
- The wireless clients immediately try to re-associate, which creates a burst of traffic.

A CTS flood

- An attacker takes advantage of the CSMA/CA contention method to monopolize the bandwidth.
- The attacker repeatedly floods Clear to Send (CTS) frames to a bogus STA.
- All wireless clients sharing the RF medium receive the CTS and withhold transmissions until the attacker stops transmitting the CTS frames.

Rogue Access Points

A rogue AP is an AP or wireless router that has been:

- Connected to a corporate network without explicit authorization and against corporate policy.
- Connected or enabled by an attacker to capture client data, such as the MAC addresses of clients (both wireless and wired), or to capture and disguise data packets, to gain access to network resources, or to launch man-in-the-middle (MITM) attacks.
- To prevent the installation of rogue APs, organizations must use monitoring software to actively monitor the radio spectrum for unauthorized APs.

Man-in-the-Middle Attack

“Evil twin AP” attack:

- A popular wireless MITM attack where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.
- Locations offering free Wi-Fi, such as airports, cafes, and restaurants, are hotbeds for this type of attack due to the open authentication.
- Connecting wireless clients would see two APs offering wireless access. Those near the rogue AP find the stronger signal and most likely associate with the evil twin AP. User traffic is now sent to the rogue AP, which in turn captures the data and forwards it to the legitimate AP.
- Return traffic from the legitimate AP is sent to the rogue AP, captured, and then forwarded to the unsuspecting STA.

Bezpečnosť WLAN sietí

- Zabezpečiť WLAN siete tak zahŕňa viaceré aspekty:
 - Autentifikácia používateľov, autentifikácia siete
 - Dôvernoscť 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



Autentifikácia používateľov



Autentifikácia používateľov

- Pôvodný štandard 802.11b obsahuje jednoduchú podporu pre autentifikáciu používateľov
- Dva režimy autentifikácie:
 - **Open System**
 - Autentifikácia sa nevykonáva, resp. klient žiada a dostane
 - **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 prijať odpoveď správne dešifrovať, klienta autentifikuje.
- Heslo používané v režime Shared Key sa následne používa aj pre šifrovanie prenášaných dát

Autentifikácia používateľov

- 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

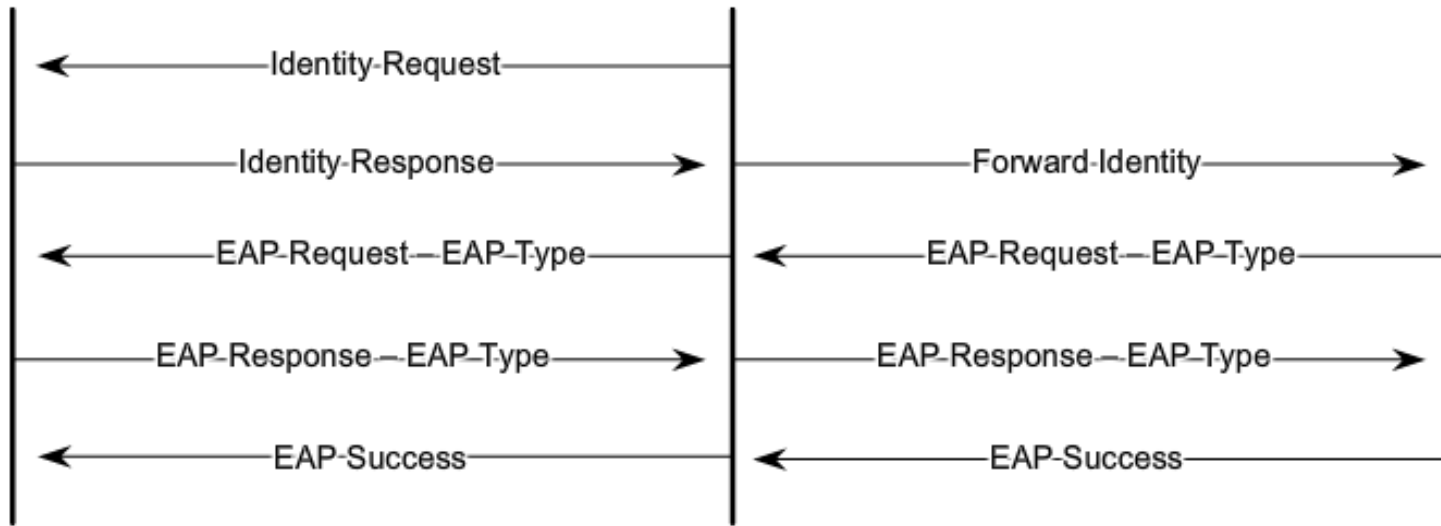
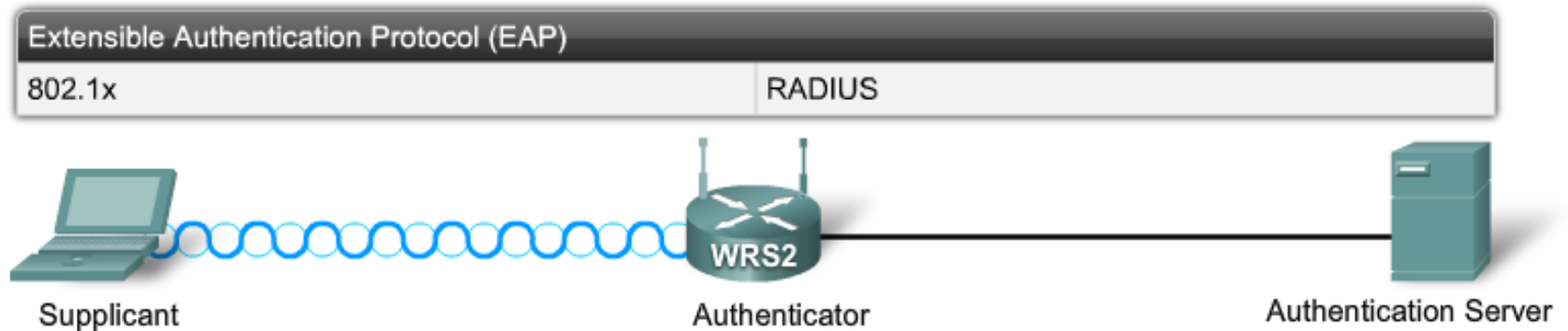
Autentifikácia používateľov

- 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:
 - **Extensible Authentication Protocol (EAP)**
 - **Štandard 802.11i (WPA2)**
 - Vyvinuté na používanie s 802.1x (RADIUS)

Autentifikácia používateľov

- EAP – Extensible Authentication Protocol, 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

EAP



Autentifikácia používateľov

- V súčasnosti používané metódy nad EAP:
 - **LEAP (Lightweight EAP)**
 - Cisco implementácia challenge-response protokolu. Overenie použitím mena a hesla.
 - **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:
 - 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



Autentifikácia siete



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 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
 - 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
 - Existuje séria slabých inicializačných vektorov, ktoré zo zašifrovaného obsahu dovoľujú zistiť hodnotu niektorých bajtov kľúča

Šifrovanie dát – 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 byť niest' kontrolný súčet, ktorý je takisto šifrovaný (MIC – algoritmus Michael)

Šifrovanie dát – náhrada WEP – WPA2

■ **WiFi Protected Access 2 (WPA2)**

- Štandardizovaná v **802.11i**
- Využíva šifrovací algoritmus AES (Rijndael)
 - Advanced Encryption Standard
- Namiesto TKIP využíva protokol CCMP
- 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

Authenticating a Home User

- WPA and WPA2 support two types of authentication:
- **Personal**
 - Intended for home or small office networks, or authenticated users who use a pre-shared key (PSK).
 - No special authentication server is required.
- **Enterprise**
 - Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server.
 - Provides additional security.
 - Users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

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

Ochrana aktívnych prvkov siete

- Ochrana aktívnych prvkov cez zabezpečenie prístupu k ich administráčnemu 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

Odporúčanie zabezpečenia WiFi

- 1. Zapnite šifrovanie.
 - Najlepšie možné je WPA2, ďalšou možnou alternatívou je WPA, v prípade, že predchádzajúce šifrovanie sa nedajú použiť (do siete sa budú pripájať zariadenia, ktoré ich nepodporujú), zapnite aspoň WEP, aj jednoduché šifrovanie je lepšie ako nezabezpečená sieť.
- 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 vyvodí sa z toho, že daná sieť nie je dostatočne zabezpečená. Nastavte ich tak, aby jednotliví užívatelia mohli ľahko identifikovať, ku ktorému prístupovému bodu sa chcú pripojiť. Nepoužívajte názvy firmy, alebo mená, ktoré by boli pre útočníkov veľmi nápadné (napríklad OMEGA-SKLAD).
- 4. Vypnite zdieľanie tlačiarň a súborov v sieti, ak ich nepotrebuje.
 - Znemožní 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 možné 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“.



Konfigurácia WLAN



Postup

- Step 1: Verify local wired operation—DHCP and Internet access
- Step 2: Install the access point
- Step 3: Configure the access point—SSID (no security yet)
- Step 4: Install one wireless client (no security yet)
- Step 5: Verify wireless network operation
- Step 6: Configure wireless security—WPA2 with PSK
- Step 7: Verify wireless network operation

Konfigurácia Wifi na Linksys

<http://nil.uniza.sk/wireless/hardware/konfiguracia-ap-cisco-linksys-wrt54g2>

The screenshot shows the 'Basic Wireless Settings' page in a Windows Internet Explorer browser. The page has a purple header with the Linksys logo and a navigation bar with 'Setup', 'Wireless', and 'Security' tabs. The 'Wireless' tab is selected, and the 'Basic Wireless Settings' sub-tab is active. The main content area contains settings for Network Mode, Network Name (SSID), Radio Band, Wide Channel, Standard Channel, and SSID Broadcast. Numbered annotations (1-6) point to specific elements: 1 points to the 'Wireless' tab; 2 points to the 'Basic Wireless Settings' sub-tab; 3 points to the 'Network Mode' dropdown menu; 4 points to the 'Network Name (SSID)' text box; 5 points to the 'Radio Band', 'Wide Channel', and 'Standard Channel' dropdowns; 6 points to the 'SSID Broadcast' radio buttons. Yellow callout boxes provide additional instructions for steps 3, 4, 5, and 6.

1 Select network mode:

- MixedBG-Mixed
- Wireless-B Only
- Wireless-G Only
- Wireless-N Only
- Disabled

2 Change default SSID.

3 Set RF Channels.

4 Select SSID Broadcast option.

5 Save Settings Cancel Changes

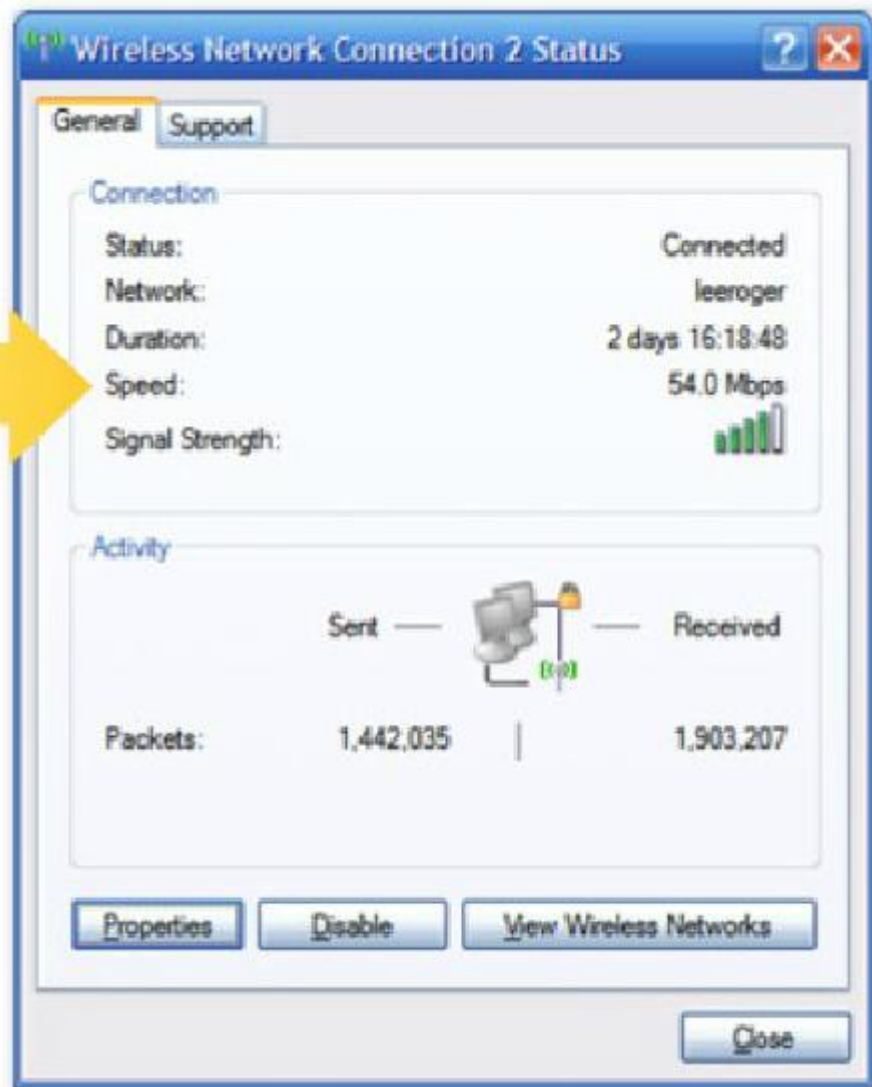
Značenie – napr. Linksys

- PSK or PSK2 with TKIP is the same as WPA
- PSK or PSK2 with AES is the same as WPA2
- PSK2, without an encryption method specified, is the same as WPA2
- PSK
 - Personal
 - Enterprise
 - Potrebuje AAA server, napr. RADIUS

Konfigurácia Wifi na NIC



Double-click





Diagnostika



Diagnostické prístupy

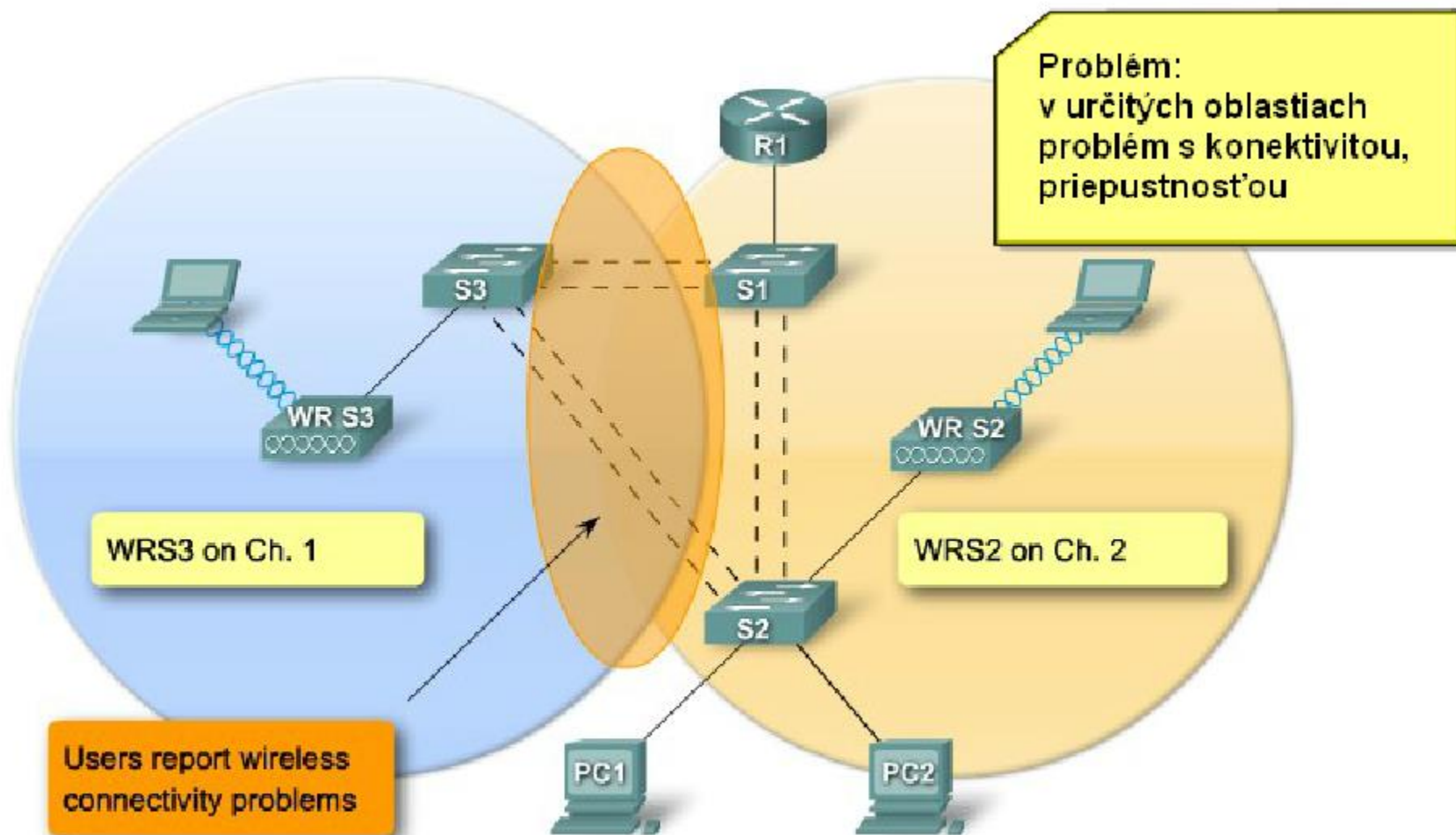
Je viacero diagnostických postupov:

- **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

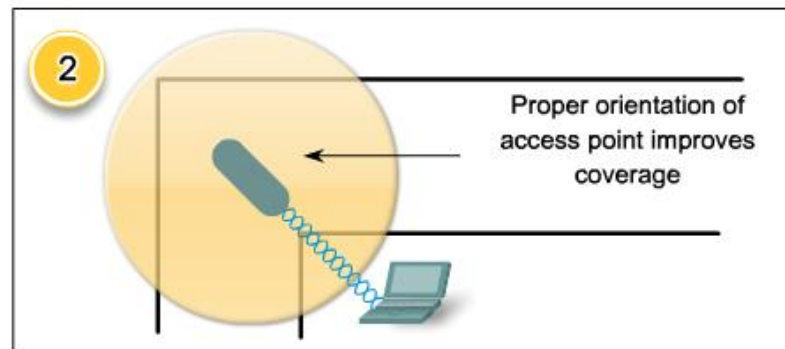
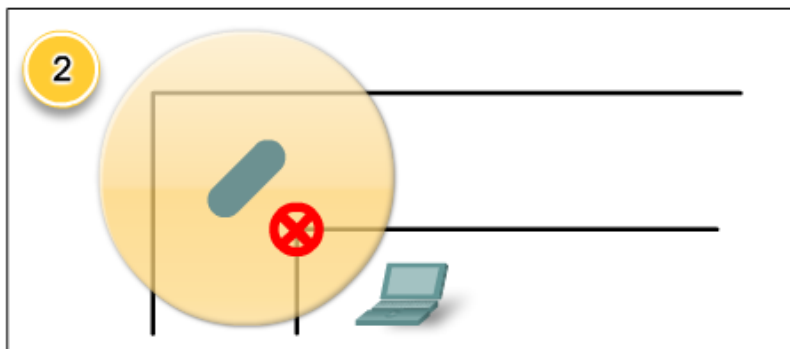
Riešenie problémov

- Vykonávaj upgrade firmware

Riešenie problémov



Umiestnenie AP a nasmerovanie antény



KONIEC