Wireless LAN

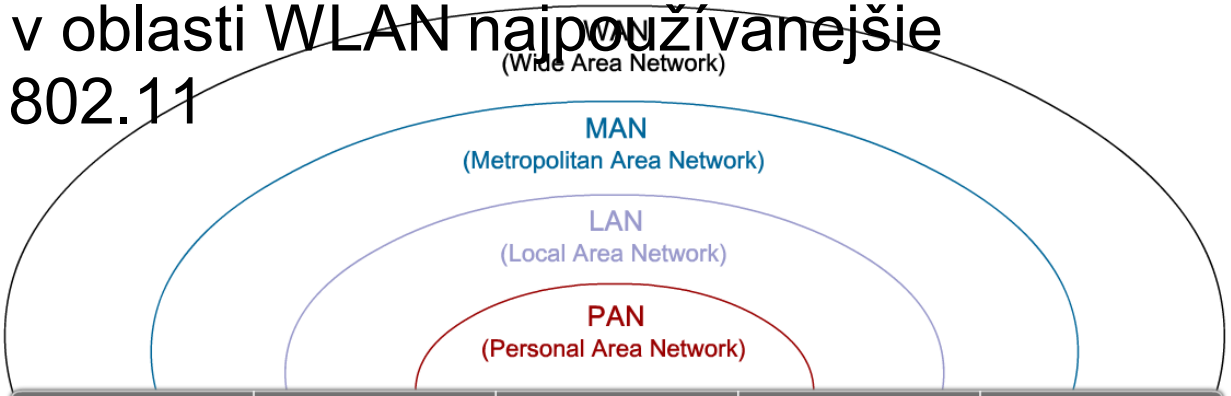
CCNA Exploration Semester 3 - Chapter 7

Wireless technológie

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

Wireless LAN technológie

- 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 najpoužívanejšie 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	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

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 pozerať 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

Modulačné, kódovacie a frekvenčné schémy

- 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.
- Modulácia
  - zmena istej charakteristiky prenášaného signálu, ktorou bude vyjadrený prenášaný symbol počas prenosu
- Frekvenčná schéma
  - spôsob, akým vysielač obsadzuje rozsah frekvencií v danom kanáli
- V terminológii sa mnohokrát nedostatočne rozlišuje medzi kódovaním a moduláciou

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

Wireless štandardy - zhrnutie

	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		Unconfirmed Possibly 2.4 and 5 GHz bands
Channels*	Up to 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps	Speculated to be 248 Mbps for two MIMO streams
Range	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Release Date	October 1999	October 1999	June 2003		Expected in 2008
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed		Very good data rates, improved range
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band		

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

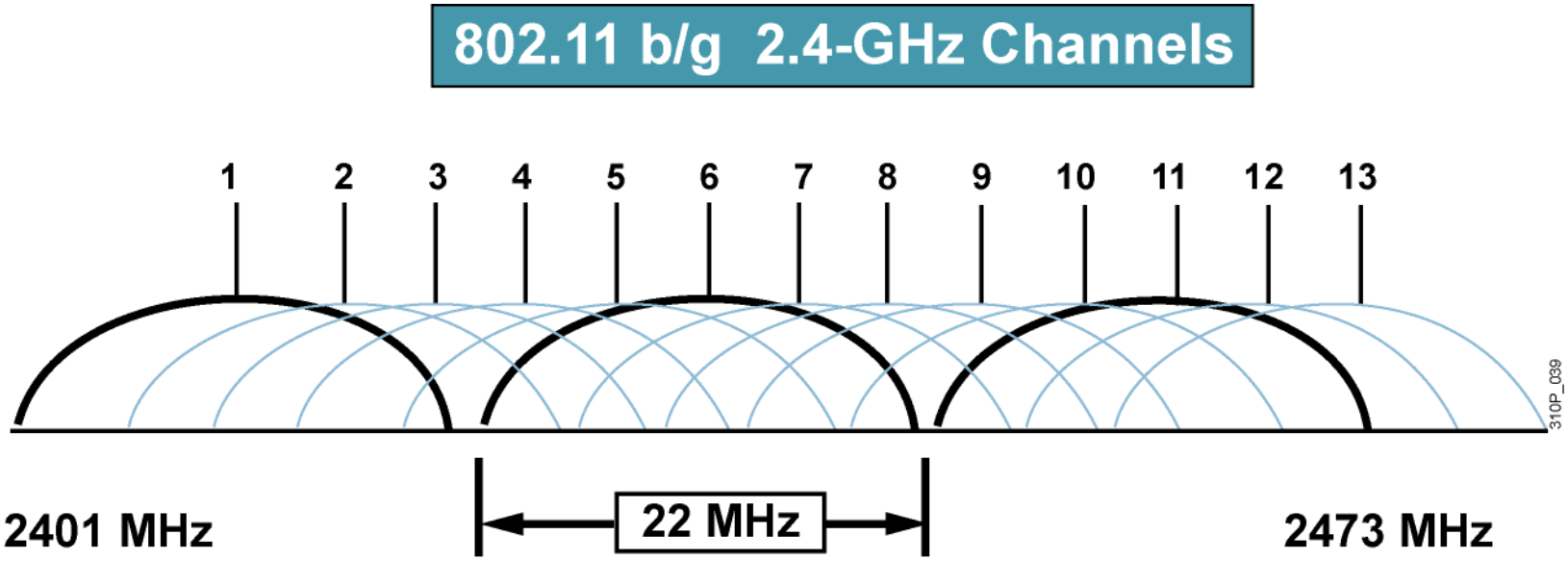
Štandard 802.11g

- Spätne 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

2.4-GHz Channels (b/g)

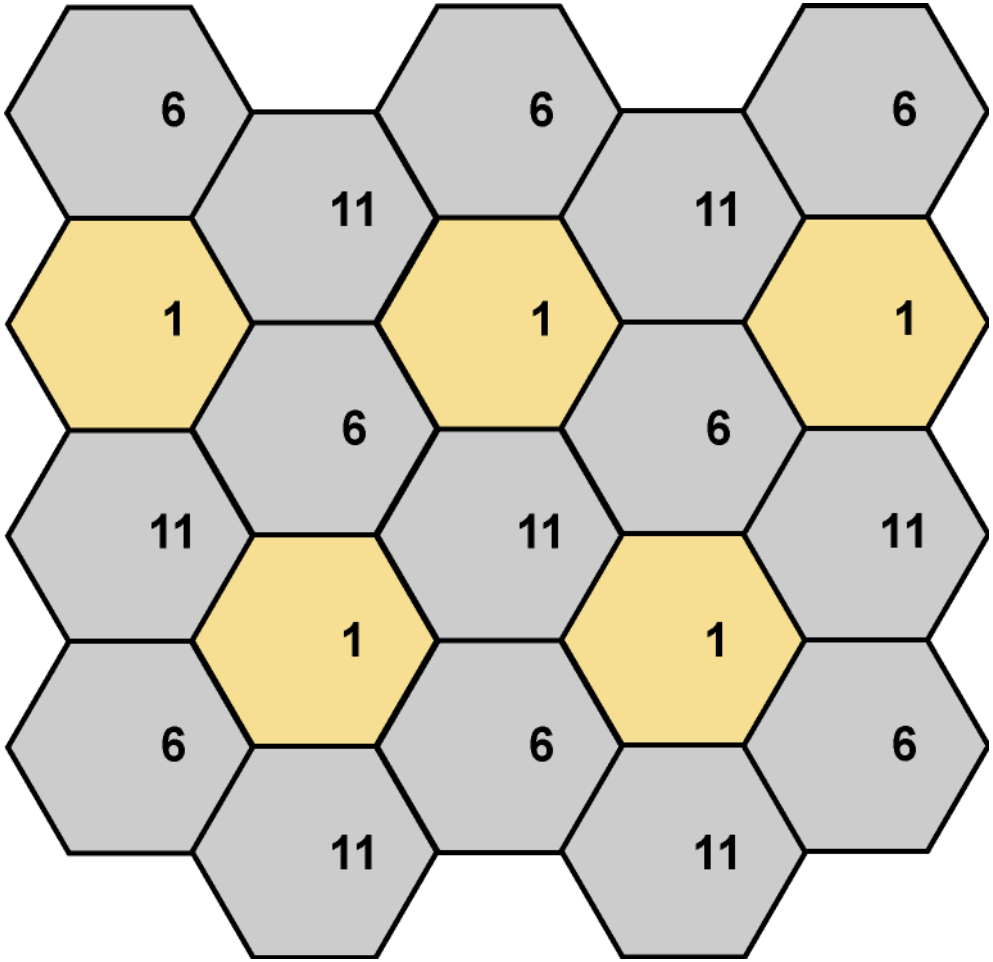
Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 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



- 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



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 rýchlosti na 248 Mbps (niektoré správy tvrdia dokonca o 600 Mbps), reálna prenosová rýchlosť cca 74 Mbps
- Finálne schválenie štandardu sa očakáva až v roku 2009
- 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 zotrvávajú 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™**

Iné organizácie

- ITU-R
  - Prideľuje a riadi RF spektrum
- ETSI

Komponenty a činnosť WLAN sietí

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

Prístupový bod

- Prístupový bod – access point (AP):
  - Zabezpečuje vzájomnú komunikáciu WLAN klientov a spojenie WLAN s LAN
  - Podľa vyhotovenia môže byť integrovaný aj s ďalšími zariadeniami, spravidla so smerovačmi
  - Rôzne vyhotovenia pre vonkajšie/vnútorné inštalácie

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

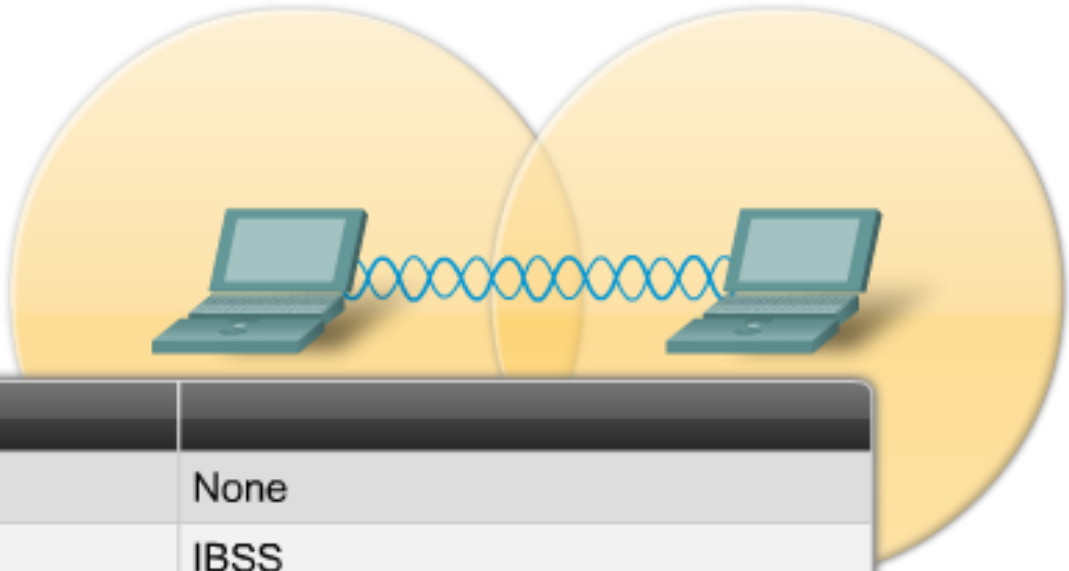
Ďalšie komponenty WLAN sietí

- 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

Základné formy WLAN sietí

- **Independent Basic Service Set (IBSS):**
  - Sieť tvorená výlučne WLAN klientmi bez centrálneho prvku
  - Často nazývaná aj **Ad-hoc** sieť
    - Mode ad-hoc
- **Basic Service Set (BSS):**
  - WLAN sieť tvorená prístupovým bodom a klientami
  - Nazývaná aj Infrastructure (Infra-BSS)
    - Mode infrasctructure
- **Extended Service Set (ESS):**
  - WLAN sieť skladajúca sa z niekoľkých BSS sietí, prepojených tzv. distribučným systémom
    - Mode infrasctructure

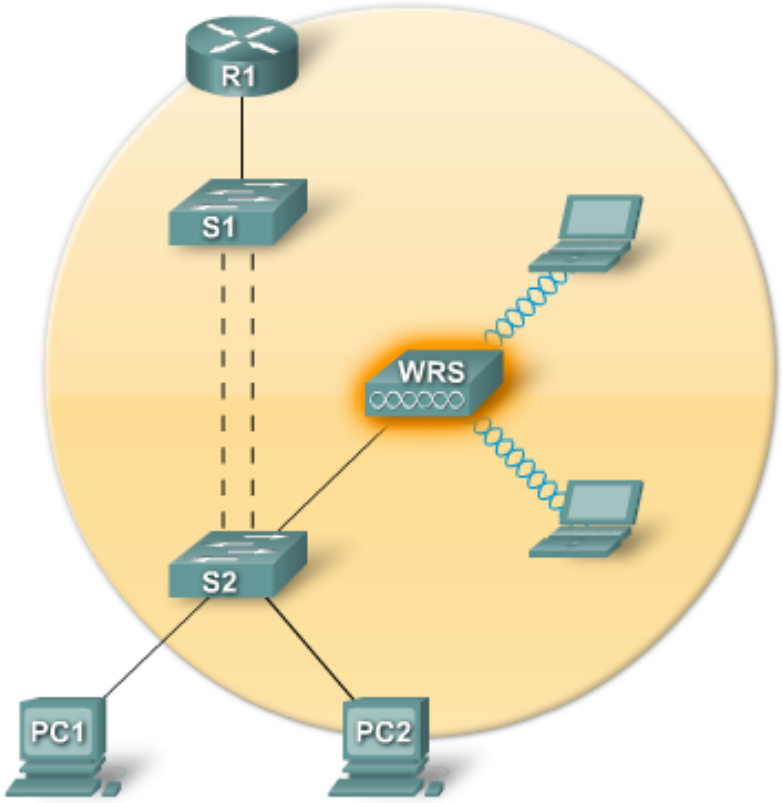
Základné formy WLAN sietí – Ad-hoc - IBSS



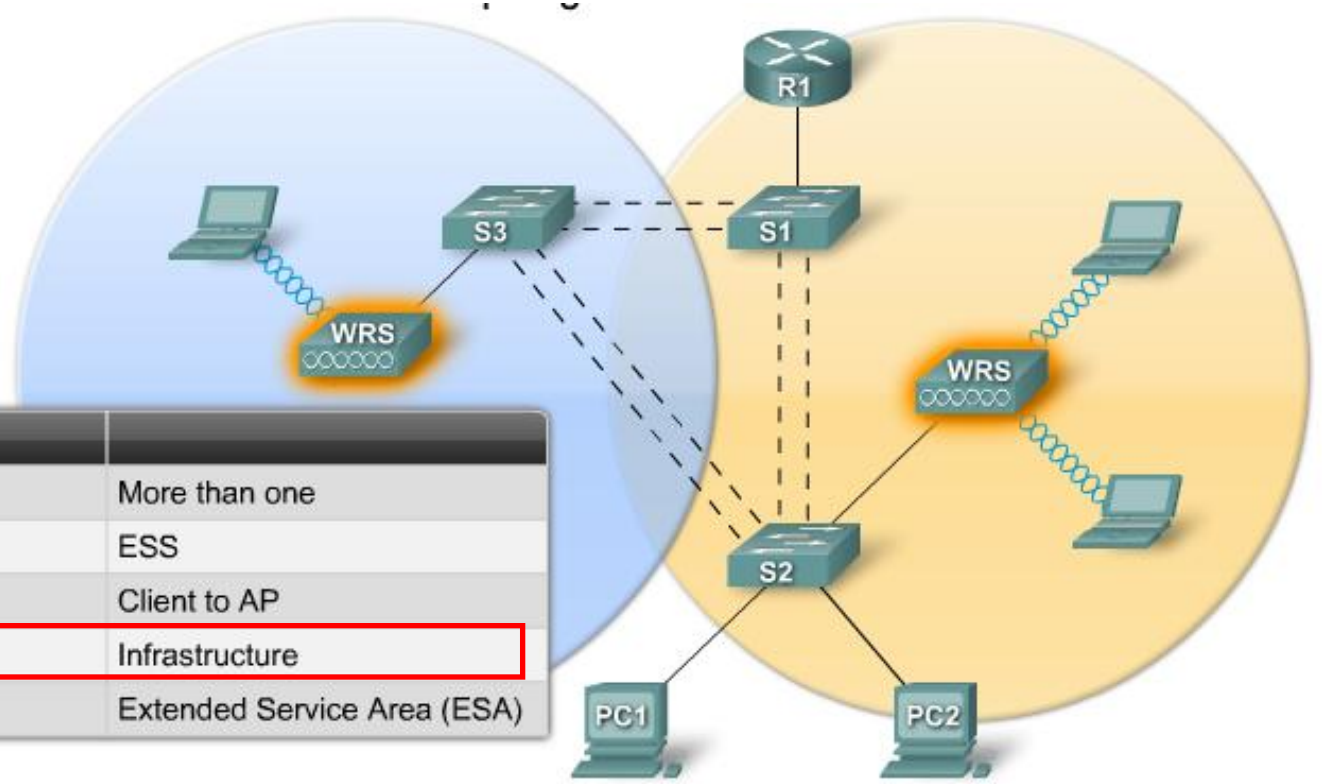
APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Základné formy WLAN sietí – BSS

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



Základné formy WLAN sietí – ESS



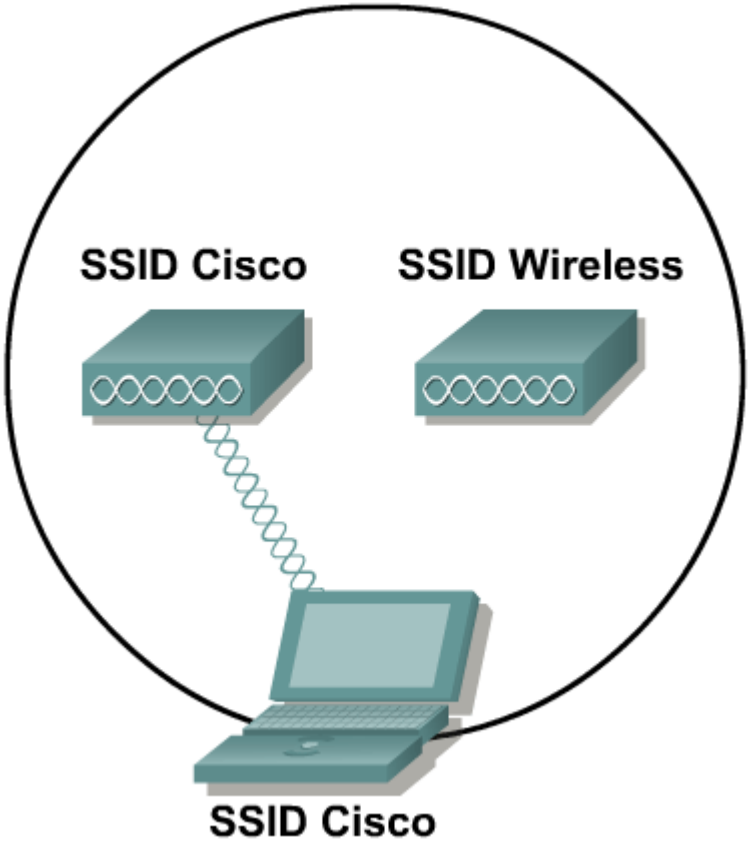
APs	More than one
Topology	ESS
Connection	Client to AP
Mode	Infrastructure
Coverage	Extended Service Area (ESA)

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 pristupujúceho 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

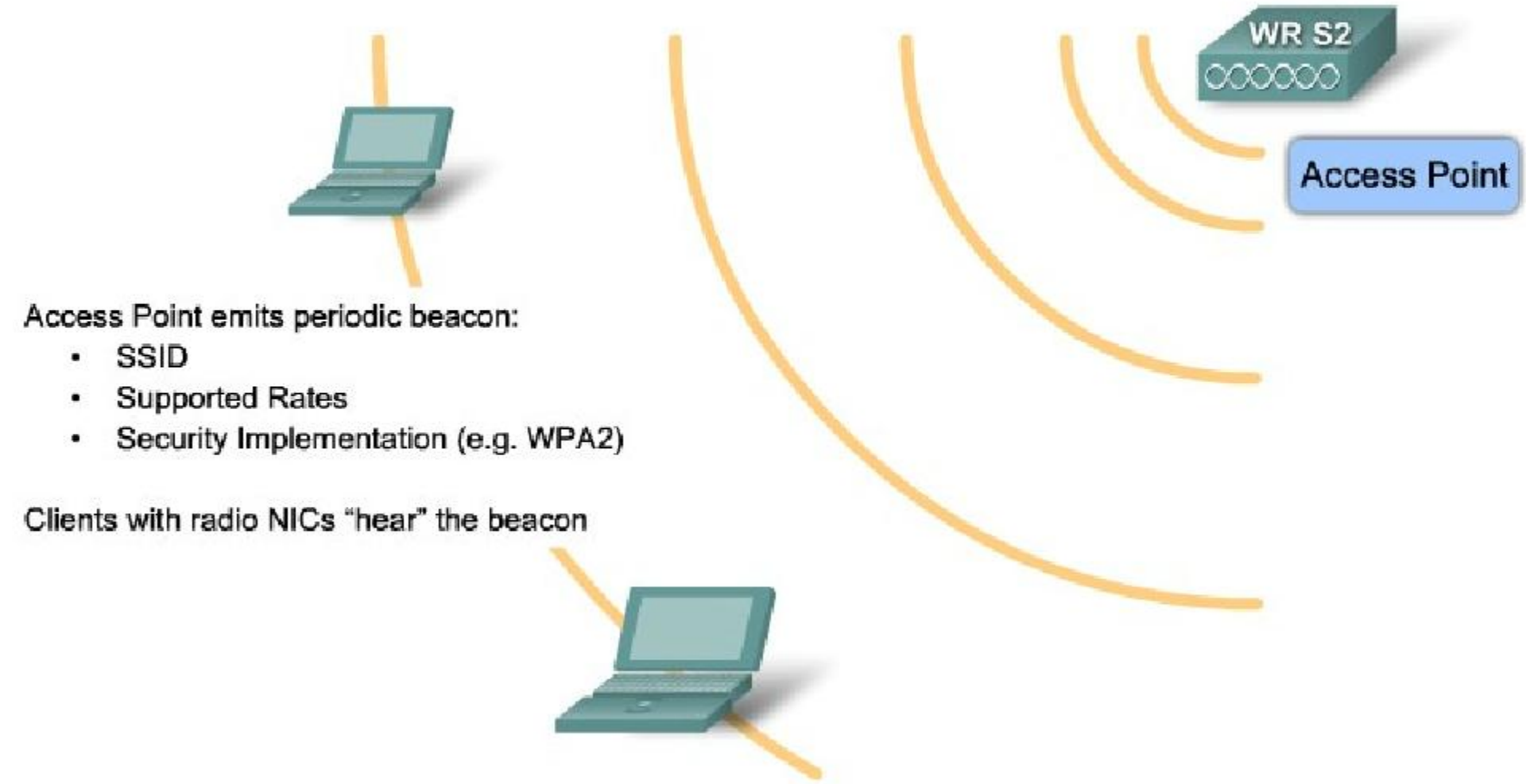
- SSID (Service Set ID) je slovný názov bezdrôtovej siete
- AP môže SSID vysielať vo svojich tzv. beacon rámcoch
  - SSID môže byť aj skryté
- Klient musí pri prihlasovaní sa do siete SSID poznať
- Jeden AP môže navonok prezentovať niekoľko SSID
  - Každé SSID má samostatnú VLAN
  - AP využíva trunking a 802.1Q značkovanie na roztriedenie rámcov medzi SSID/VLAN



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

Komunikácia vo WLAN sieti



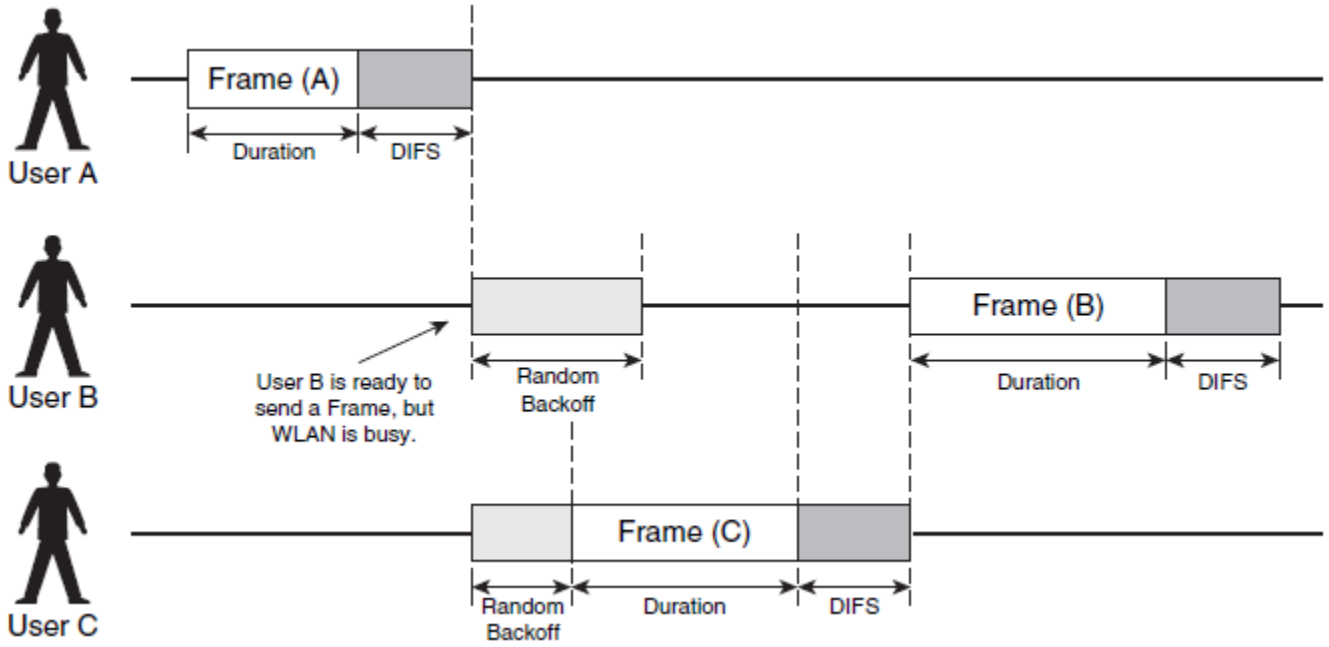
Komunikácia vo WLAN sieti

- WLAN klienti sa vzájomne musia počuť („vidieť“), ale dáta si prenášajú výlučne prostredníctvom prístupového bodu
- Požiadavka, aby sa WLAN klienti vzájomne počuli, vychádza z použitej metódy prístupu na zdieľané médium CSMA/CA
- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
  - Vo WLAN nemôžem použiť CSMA/CD
    - Odosielajúca stanica nevie zistiť, že spôsobila kolíziu keď vysiela
  - Modifikácia klasickej CSMA metódy
  - Pred prenosom počúvaj, ak nik neprenáša chvíľu počkaj a začni prenos

CSMA/CA

- Pri prenose so systémom CSMA/CA môžu nastať dve situácie
  - Nikto neprenáša
    - Po poslednom rámci prenášanom v danej sieti musí nasledovať tichá doba, tzv. DCF Interframe Space (DIFS)
      - Ak počas DIFS niekto začne vysielať – odklad prenosu
      - Inak po uplynutí DIFS môže stanica odvysielať svoj rámec a čaká na potvrdenie o prijatí
  - Iné zariadenie prenáša rámec
    - Stanica musí počkať kým skončí prenos + DIFS + náhodný čas
    - Ako stanica vie ako dlho potrvá prenos (rozdielna dĺžka rámca)?
      - Buď sa všetky stanice počujú navzájom
      - Alebo sa využije RTS/CTS mechanizmus, v ktorom sa v správach RTS a CTS uvádza odhadované trvanie prenosu

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

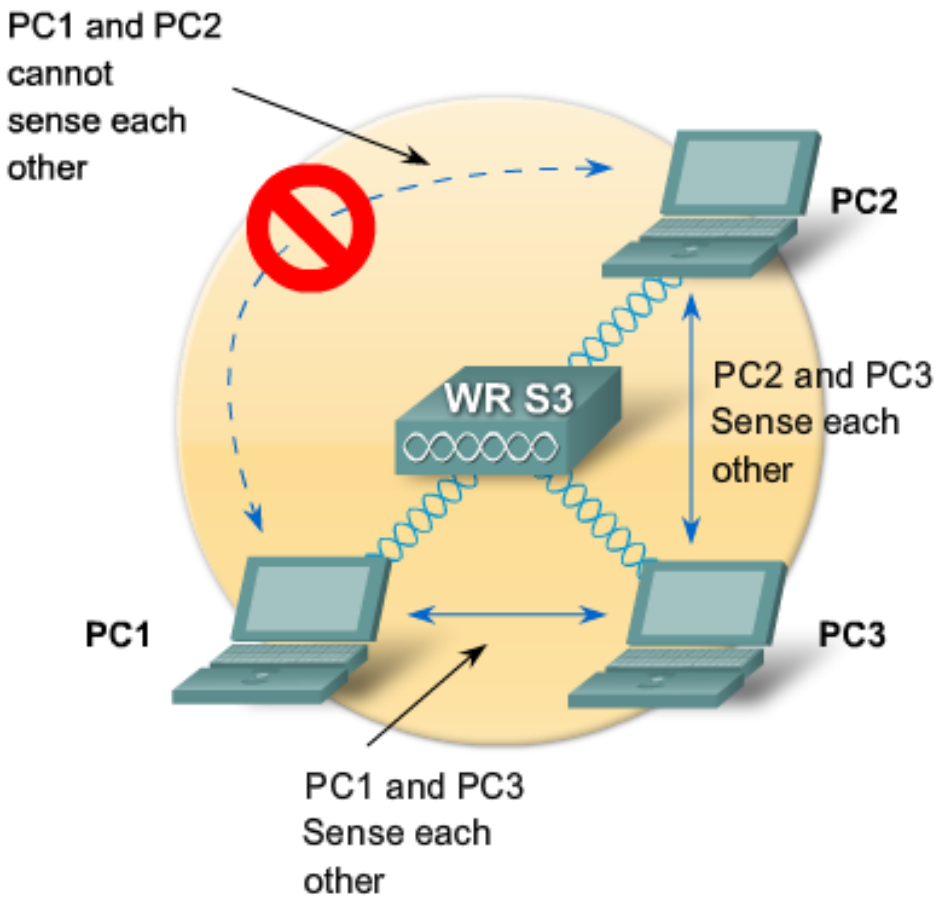
3. *B* počká náhodný backoff čas kým sa pokúsi znova preniesť frame.
4. Kým B čaká, objaví sa C, ktorý chce tiež prenášať rámec. Detekuje a zistí, že nik neprenáša, *C* počká náhodný čas, ktorý je kratší ako náhodný čas B
5. C prenesie rámec a zároveň dá info o dobe trvania prenosu
6. B teraz musí počkať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

Hidden node problem

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.



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

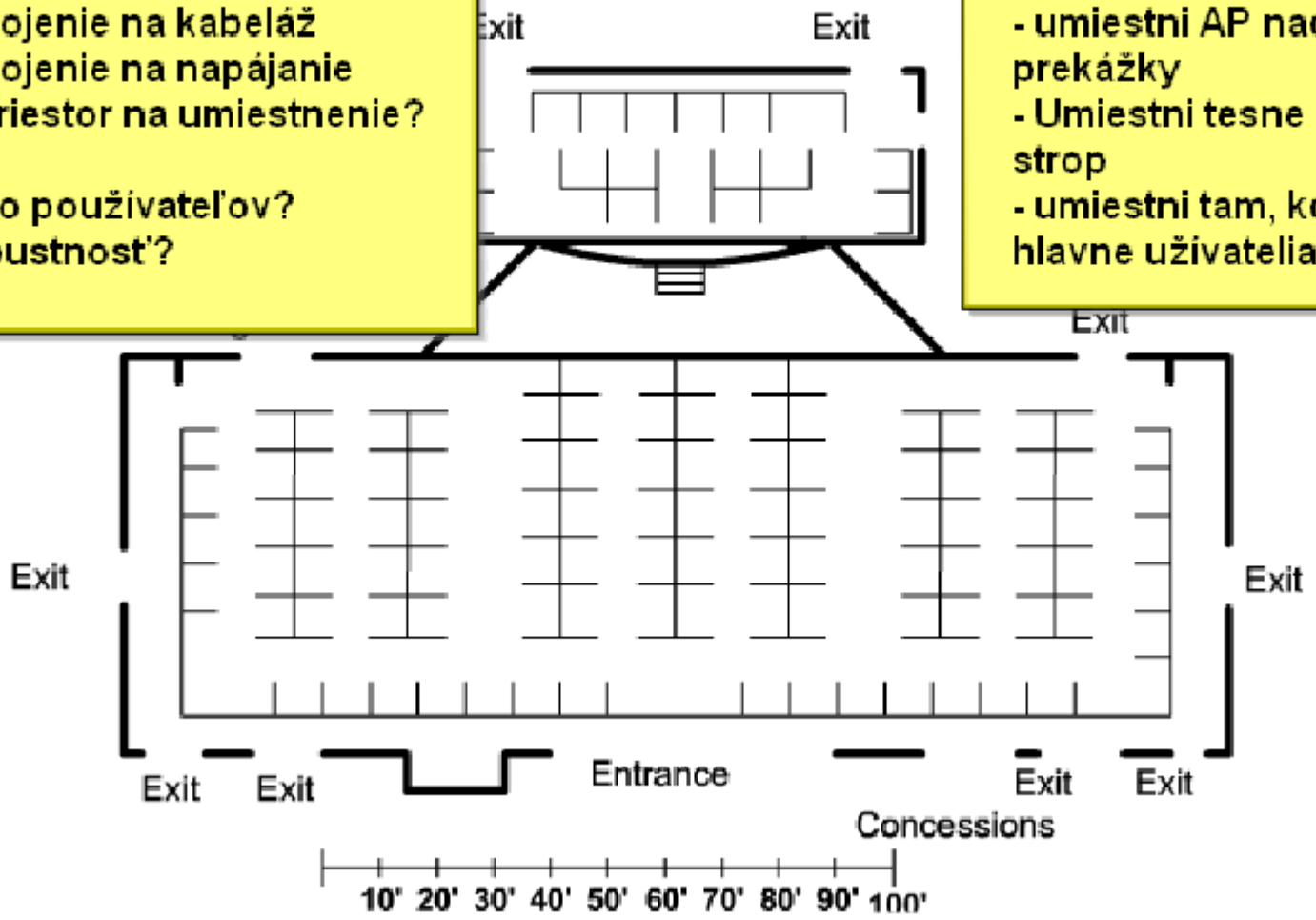
- Mosty (bridge) typicky neumožňujú bežným klientom asociovať sa
- Mosty sa asociujú vzájomne v pároch
- Vo všeobecnosti, prístupové body aj mosty sú Layer2 zariadenia a správajú sa ako prepínače
- WLAN sieť je typicky jedna broadcastová doména (t.j. jedna IP sieť)
- Niektoré pokročilejšie prístupové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

Plánovanie WLAN

Zváž pri umiestňovaní AP
- napojenie na kabeláž
- napojenie na napájanie
- je priestor na umiestnenie?

Koľko používateľov?
Priepustnosť?

Extra zváž:
- umiestni AP nad prekážky
- Umiestni tesne pod strop
- umiestni tam, kde budú hlavne uživatelia



WLAN bezpečnosť

Bezpečnosť WLAN sietí

- Bezpečnosť WLAN sietí 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

Autentifikácia používateľov

Bezpečnosť WLAN sietí
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 prijatú odpoveď správne dešifrovať, klienta autentifikuje.
- Heslo používané v režime Shared Key sa následne používa aj pre šifrovanie prenášaných dát

Bezpečnosť WLAN sietí
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

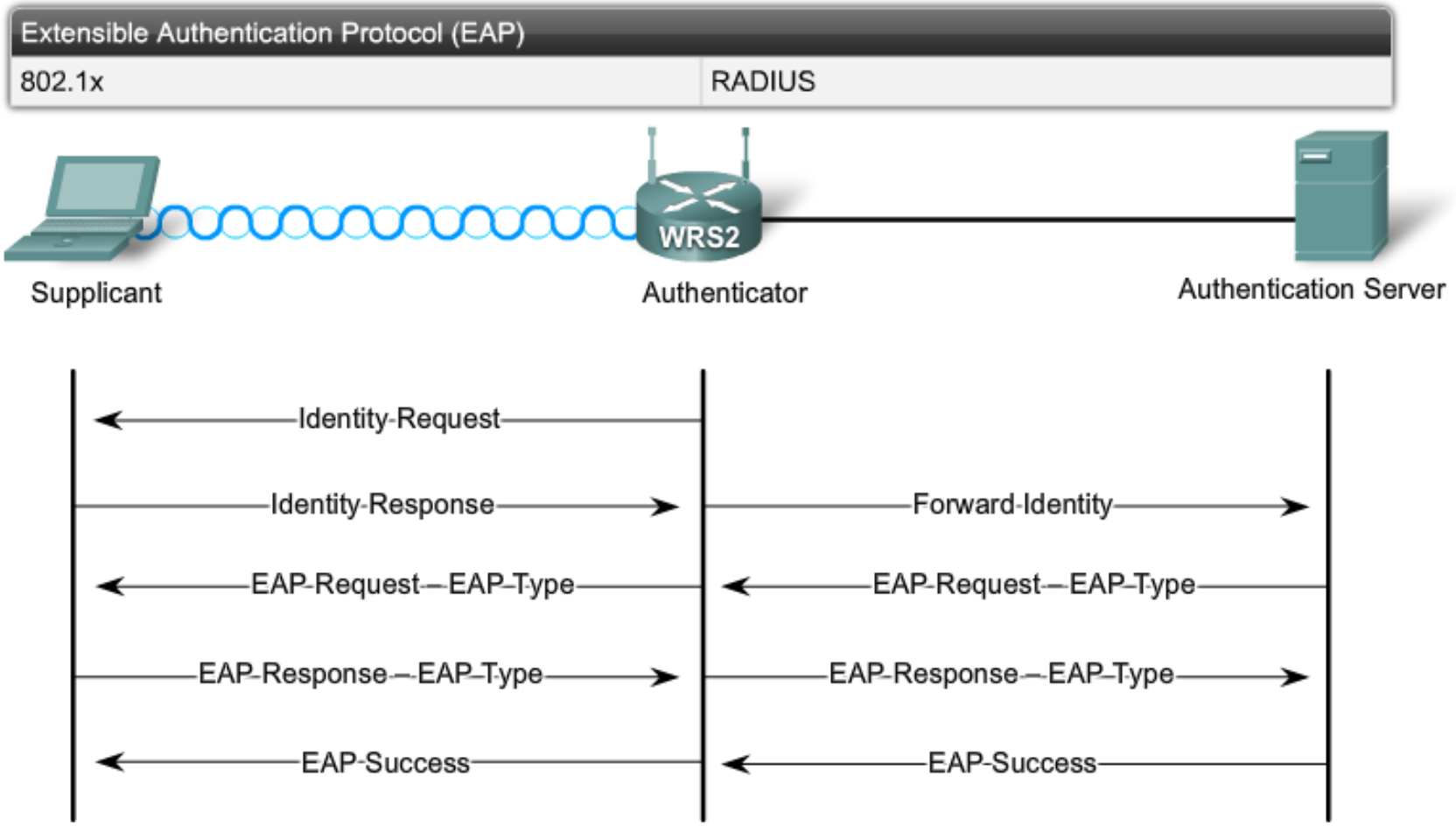
Bezpečnosť WLAN sietí
Autentifikácia používateľov

- 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)

Bezpečnosť WLAN sietí
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


Extensible Authentication Protocol (EAP)
802.1x
RADIUS
WRS2
Supplicant
Authenticator
Authentication Server
Identity-Request
Identity-Response
Forward-Identity
EAP-Request—EAP-Type
EAP-Request—EAP-Type
EAP-Response—EAP-Type
EAP-Response—EAP-Type
EAP-Success
EAP-Success

Bezpečnosť WLAN sietí
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.

Bezpečnosť WLAN
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

Bezpečnosť WLAN sietí
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

Bezpečnosť WLAN sietí
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 niesť 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

Bezpečnosť WLAN sietí
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

Bezpečnosť WLAN sietí
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

Odporúčanie zabezpečenia WiFi

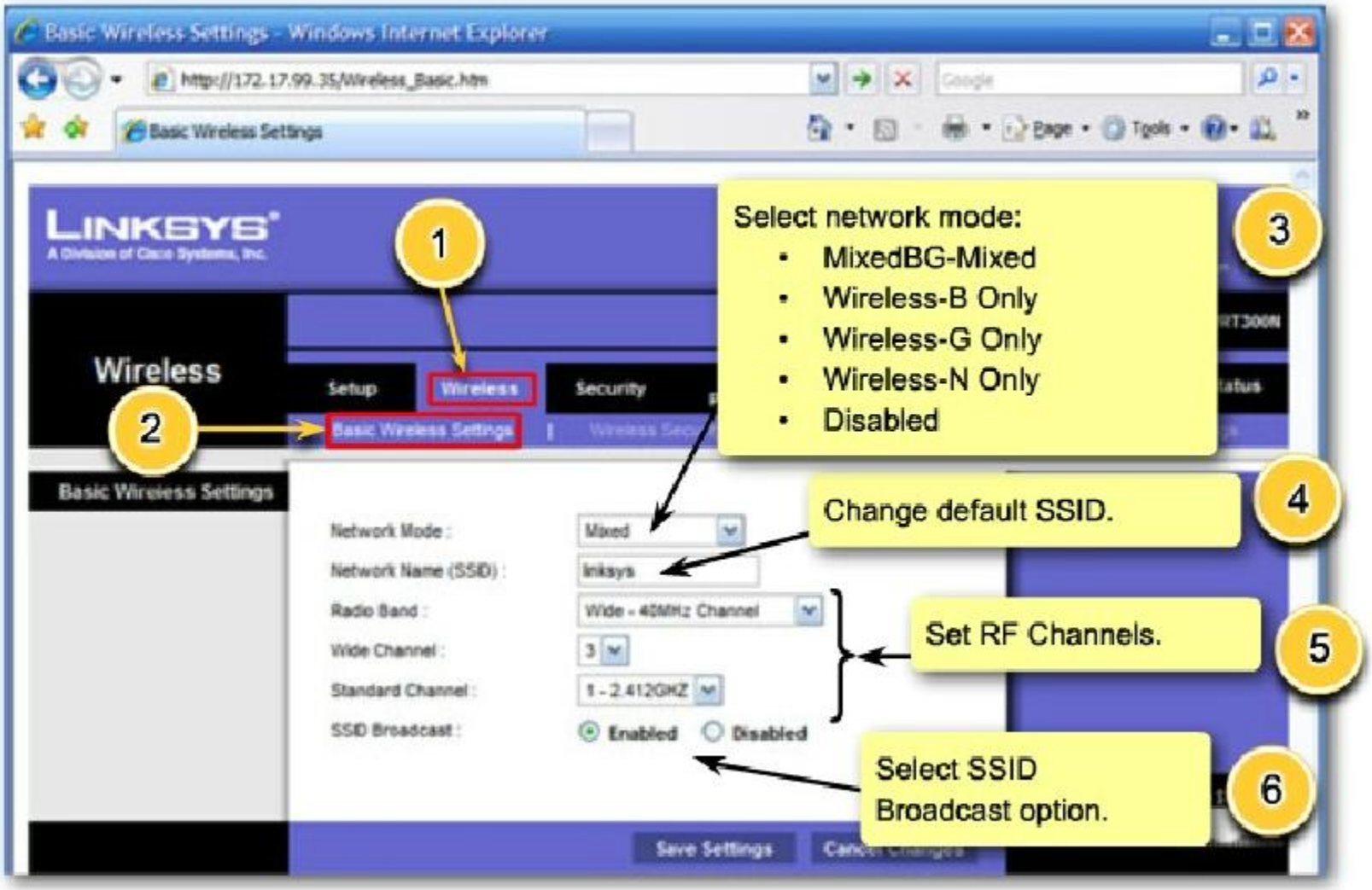
- 1. Zapnite šifrovanie.
  - Najlepšie možné je WPA2, ďalšou možnou alternatívou je WPA, v prípade, že predchádzajúce šifrovania sa nedajú použiť (do siete sa budú pripájať zariadenia, ktoré ich nepodporujú), zapnite aspoň WEP, aj jednoduché šifrovanie je lepšie ako nezabezpečená sieť.
- 2. Zmeňte prednastavené 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 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“.

Konfigurácia WLAN

- 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

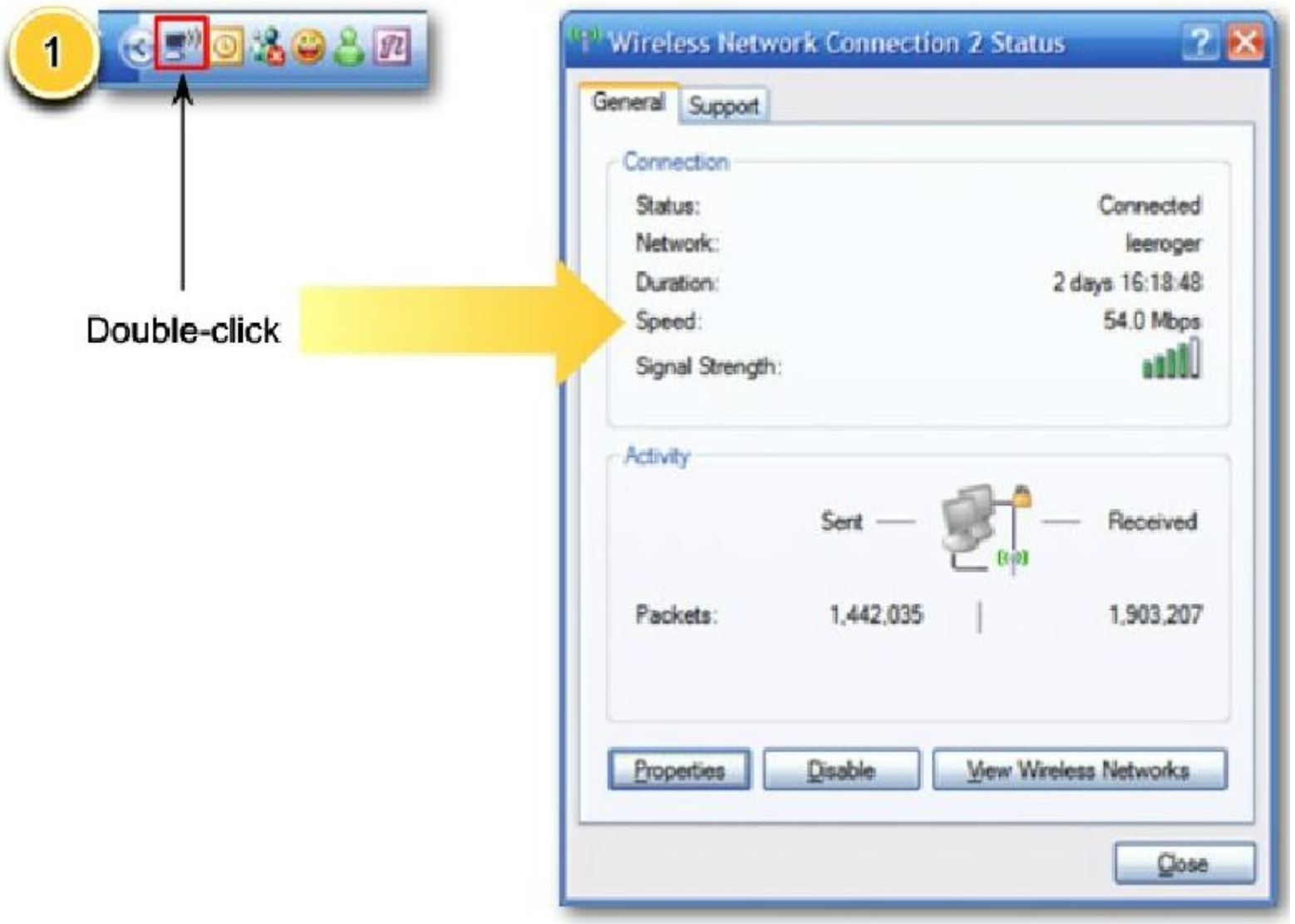
http://nil.uniza.sk/wireless/hardware/konfiguracia-ap-cisco-linksys-wrt54g2



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

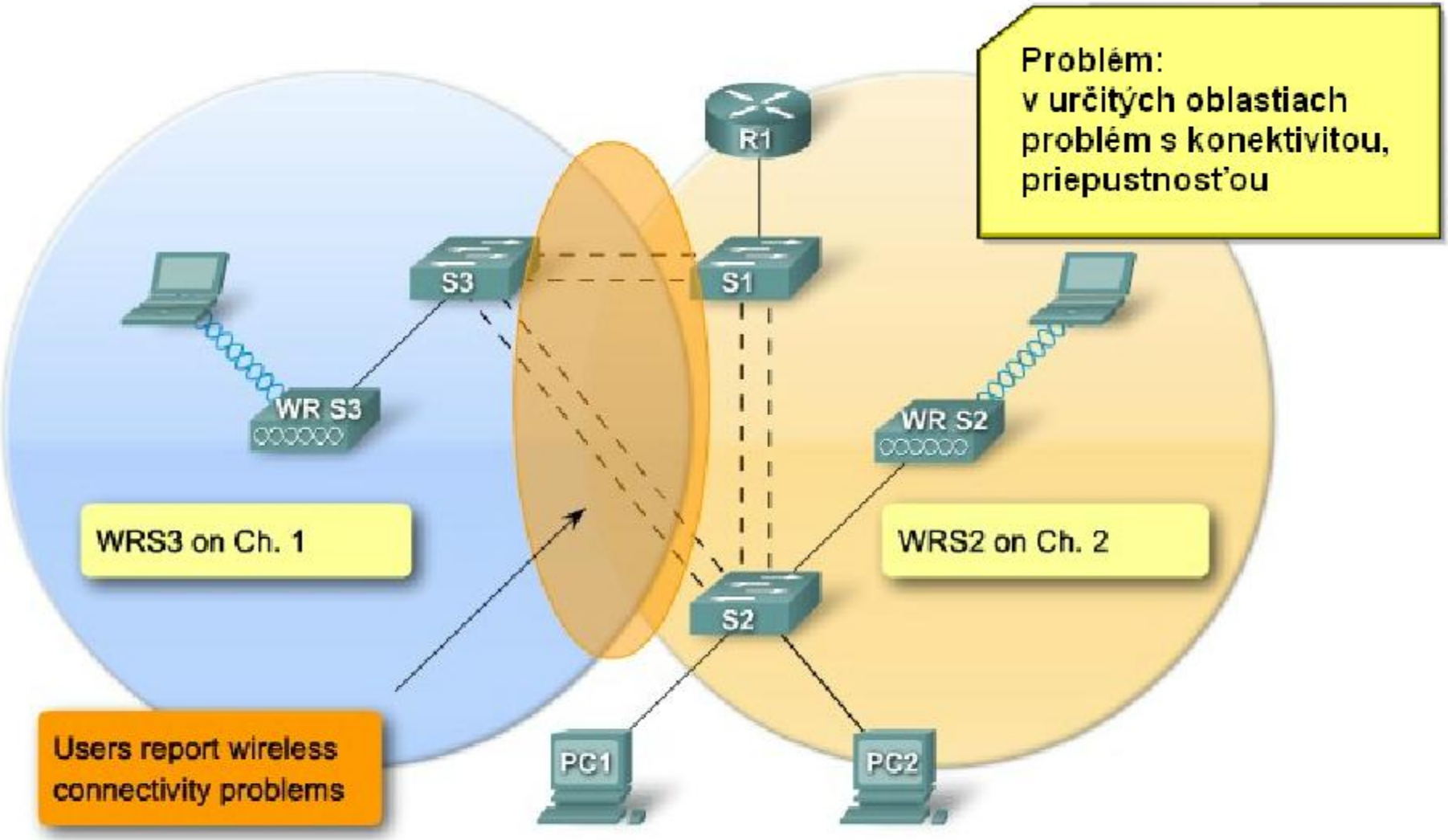


Diagnostika

Riešenie problémov

- Vykonávaj upgrade firmware

Riešenie problémov



Umiestnenie AP a nasmerovanie antény