Bezdrátové sítě

Šárka Vavrečková

Ústav informatiky, FPF SU Opava
http://vavreckova.zam.slu.cz/hwkom.html

Poslední aktualizace: 7. května 2015

Bezdrátové technologie

jsou technologie vedení signálu „vzduchem“, bez podpory metalického nebo optického kabelu. Rozlišujeme

- rádiová – rádiové vlny o určité frekvenci (Wi-Fi, WiMAX)
- sonická – ultrazvuk, verbální komunikace
- optická – laser, IR, ostatní (mávání vlajkou, blikání, posunková řeč apod.)

Dělení:

- *fixní* – sice bezdrátové, ale při pohybu připojeného zařízení se buď silně zhoršuje signál nebo se dokonce odpojí,
- *mobilní* – připojené zařízení se může volně pohybovat, i vyšší rychlostí.

Wi-Fi

Princip

- rádiový signál v *bezlicenčním pásmu* 2,4 GHz nebo 5 GHz
- kolizní metoda CSMA/CA (protokol na MAC)
  - CS – Carrier Sense (naslouchá na médiu)
  - MA – Multiple Access (na médium přistupuje více stanic)
  - CA – with Collision Avoidance (když chce stanice vysílat a nasloucháním zjistí, že nikdo jiný nevysílá, informuje ostatní uzly o úmyslu vysílat)
- half duplex
- standardizována jako IEEE 802.11, o certifikaci se stará Wi-Fi Alliance

Možnosti řešení sítě:

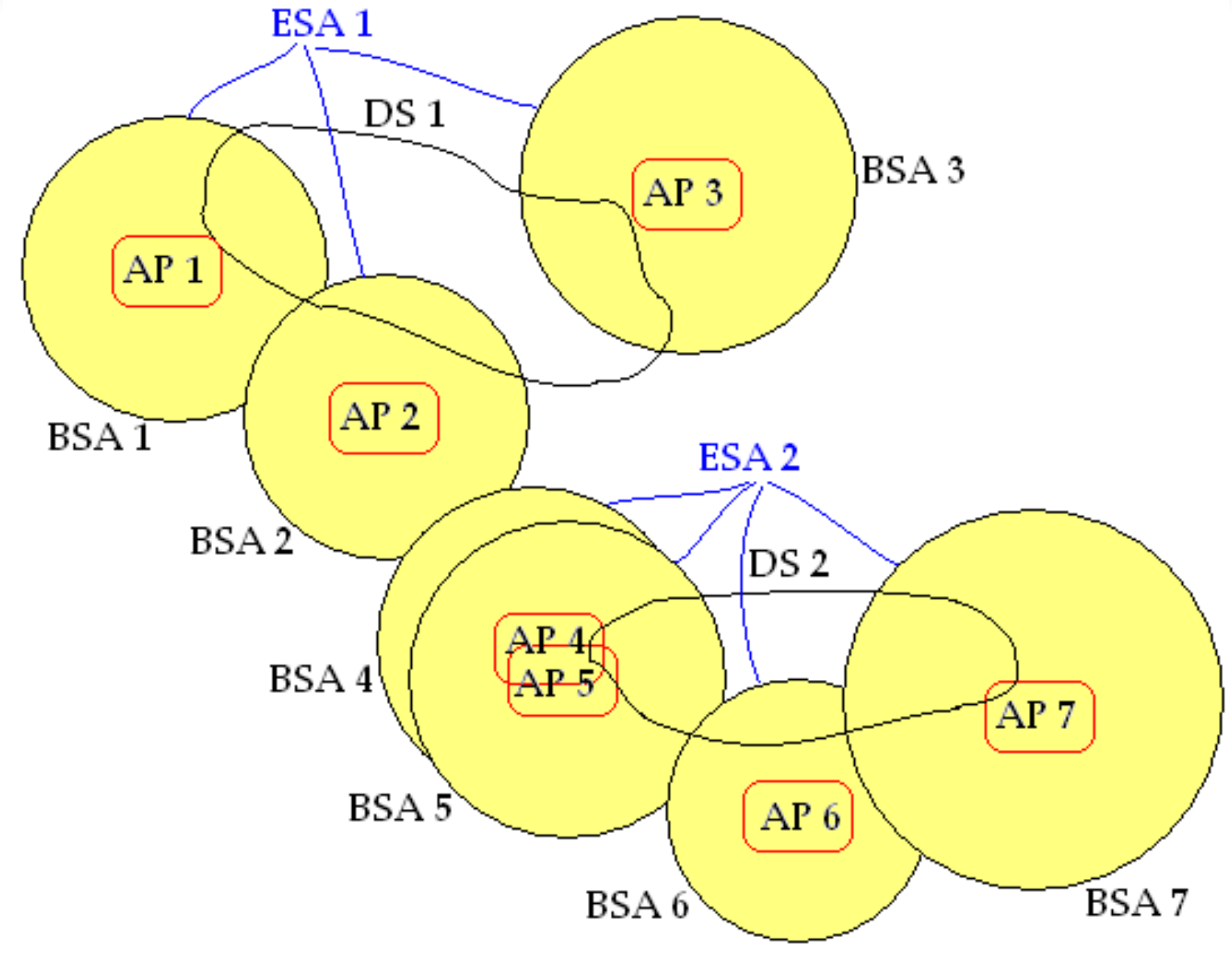
- *ad-hoc řešení*: každá komunikující stanice je vybavena Wi-Fi síťovou kartou, komunikují spolu přímo (pro sítě o pár počítačích),
- *infrastruktura*: existuje *přístupový bod* (AC – Access Point), přes který jde veškerá komunikace (point-to-multipoint), žádné dvě stanice spolu nekomunikují přímo.

Struktura sítě

- přístupový bod (AP)
- BSA (Basic Service Area) = základní oblast služeb, buňka

Distribuční systém (DS – Distribution system)

- více propojených přístupových bodů
- oblast pokrytá signálem = *rozšířená oblast služeb* (ESA – Extended Service Area)


ESA 1
DS 1
AP 3
BSA 3
AP 1
AP 2
BSA 1
BSA 2
ESA 2
DS 2
AP 4
AP 5
BSA 4
AP 7
BSA 5
AP 6
BSA 6
BSA 7

Služby přístupového bodu

- *autentizace* – AP zjišťuje informace o stanici a rozhoduje, zda jí dovolí přístup do sítě
- *asociace* (přidružení) – vzniká vazba mezi AP a stanicí, stanice je asociována k buňce daného AP
- *de-asociace* – zrušení této vazby

Identifikační kódy

SSID (Service Set IDentifier)

- řetězec 0–32 oktetů
- AP obvykle vysílá své SSID *v rámcích beacon* v intervalech několika sekund v otevřené formě
- SSID se vysílá v otevřené formě i při přidružování stanic do sítě
- „název sítě“, společné pro všechny stanice v ESA

BSSID (Basic Service Set ID)

- v rámci BSA, 6 oktetů, obvykle MAC přístupového bodu nebo u ad-hoc sítě náhodný řetězec

ESSID (Extended SSID)

- totéž co SSID, v ESA (případně může být stejný jako BSSID)

Režimy Wi-fi zařízení

Gateway (brána)

- propojení ven ze sítě, NAT server

Wi-fi router (směrovač)

- vidí na síťovou vrstvu, umí směrovat podle IP adres
- NAT, firewall, DHCP server, obvykle i brána
- obsahuje funkčnost AP

Access Point (AP)

- na 2. vrstvě, neběží NAT, připojuje se k Wi-fi routeru
- funguje jako switch (nebo bridge), jehož jeden port je bezdrátový

Režimy Wi-fi zařízení

AP klient (Station)

- připojuje se k jinému AP (bezdrátově)
- zařízení jsou k němu připojena drátem
- pouze distribuce signálu jiného AP

Repeater (opakovač)

- pouze přeposílá signál na fyzické vrstvě
- žádné směrování ani přepínání

Režimy Wi-fi zařízení

WDS (Wireless Distribution System)

- chceme distribuovat spojení „ven“ na další mezilehlé prvky, chceme plynule přecházet mezi AP v WDS
- značné snížení přenosové rychlosti
- není standardizováno

WISP

- bezdrátová komunikace bude představovat WAN port (máme poskytovatele Internetu přes Wi-fi)
- ostatní (fyzické) porty LAN, WAN: k nim se chová jako switch na 2. vrstvě

Fyzická vrstva Wi-Fi

- IEEE 802.11b – frekvence 2,4 GHz, rychlost až 11 Mb/s, modulace DSSS
- IEEE 802.11a – frekvence 5 GHz, rychlost až 54 Mb/s, modulace OFDM
- IEEE 802.11g – frekvence 2,4 GHz, rychlost až 54 Mb/s, OFDM
- IEEE 802.11n – frekvence 2,4 nebo 5 GHz, rychlost až 600 Mb/s (spíše značně nižší), OFDM+MIMO
- IEEE 802.11ac – frekvence 5 GHz, s jednou anténou (jeden stream) až 433 Mb/s, osm antén až 3,47 Gb/s, OFDM+MIMO

Modulace: podle 802.11b *DSSS* (Direct Sequence Spread Spectrum, rozprostřené spektrum), podle 802.11a/g *OFDM*. Starší (původní 802.11): také FHSS (2,4 GHz) a DFIr (infračervené záření, 300–428 GHz).

Fyzická vrstva Wi-Fi

IEEE 802.11n

- modulace typu OFDM, konkrétně až 64-QAM
- může pracovat v obou pásmech (2,4 GHz i 5 GHz), ale záleží na zařízení, zda ano, a jestli v obou pásmech zároveň
- kanál o šířce obvykle 40 MHz
- více antén, kombinace signálu pomocí MIMO
- jedna anténa: IEEE 802.11n Lite

Fyzická vrstva Wi-Fi

IEEE 802.11ac

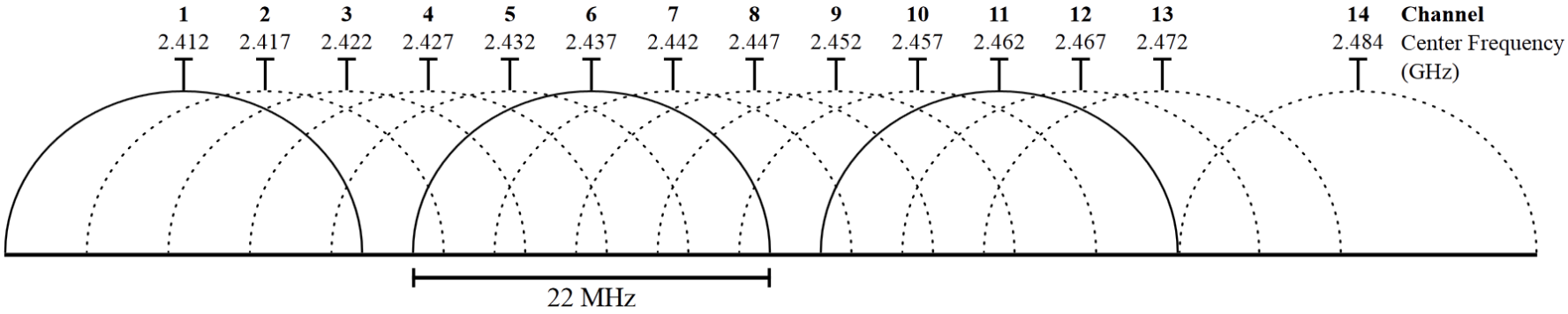
- pouze na frekvencích kolem 5 GHz
- podpora až 8 antén s MIMO, MU-MIMO (paralelní komunikace s více zařízeními)
- MU-MIMO: při 8 anténách až 4 klientská zařízení
- šířka kanálu typicky 80 MHz nebo 160 MHz
- typická rychlost kolem 1 Gb/s
- modulace – základní OFDM, subnosné pak QAM, postupné zvyšování efektivity
  - 802.11g: 16-QAM (jeden symbol = 4 bity, $2^4 = 16$ možností pro hodnotu symbolu),
  - 802.11n: 64-QAM (jeden symbol = 8 bitů),
  - 802.11ac: 256-QAM (16 bitů)

Fyzická vrstva Wi-Fi

IEEE 802.11ac – proč je rychlejší a má lepší propustnost

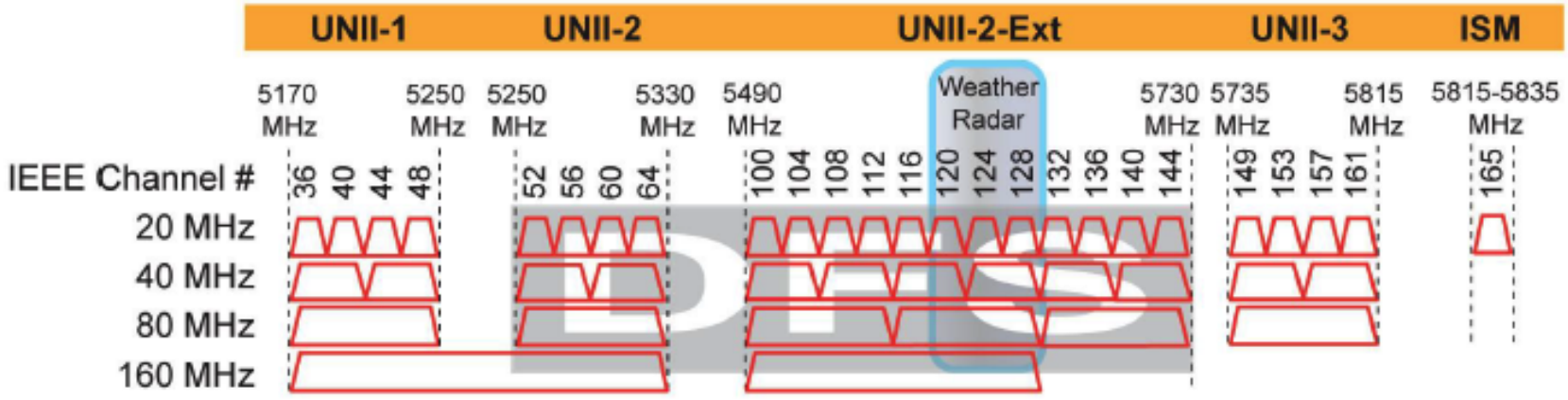
- pásmo 5 GHz – nezarušené (ani „nepočítačovými zařízeními“ – DECT telefony, mikrovlnné trouby, dětské chůvičky)
- větší šířka pásma, větší počet kanálů, při přibližně dvojnásobné frekvenci se data přenášejí cca dvakrát rychleji
- Beam-forming:
  - počítá s tím, že signál se odráží od překážek, láme se, dorazí s určitým časovým posunem,
  - tj. při spolupráci více antén na vyslání téhož signálu (od každé se signál odrazí jinak) každá anténa vyšle signál *se stanoveným zpožděním*,
  - cílové zařízení tyto signály (z různých odrazů) zkompletuje do výsledného signálu

IEEE 802.11b



- zařízení vysílající na sousedních kanálech se navzájem ruší
- zařízení zabírá celkem 5 kanálů (1 plus 2 na každé straně), v reálu vytváří šum do ještě větší vzdálenosti ve spektru
- teoreticky 3 kanály max. vzdálené bez vzájemného rušení, realita horší (šum i dál)
- vyšší standardy: zařízení vysílá ve více kanálech zároveň

IEEE 802.11ac



Šířka kanálu	Možná čísla kanálů
20 MHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 161, 165, 169
40 MHz	38, 46, 54, 62, 102, 110, 118, 126, 134, 142, 151, 159
80 MHz	42, 58, 106, 122, 138, 155
160 MHz	50, 114

Podvrstva MAC

- pro IEEE 802.11a/b/g stejná, odlišná je MAC pro IEEE 802.11n, ac (za účelem dalšího zvýšení rychlosti)
- přidružení stanice k přístupovému bodu, autentizace, přenos dat, přenosové režimy
- časový multiplex, poloviční duplex (sloty jsou využívány vždy jen v jednom směru)

Podvrstva MAC

MAC rámce

1. Datový rámec (Data Frame)
2. Řídící rámec (Control Frame)
   - vyjednání vysílacího času, ACK – potvrzení přijatých rámců
3. Rámec pro správu (Management Frame)
   - beacon rámec (AP se ohlašuje)
   - probe, probe response (zjišťování přítomnosti uzlů sítě a jejich možností)
   - association request, association response (žádost o asociaci od stanice, odpověď)
   - re-association request, response (přechod k jinému AP ve stejné ESS)
   - diassociation
   - authentication (žádost o autentizaci uzlu), de-authentication

Podvrstva MAC

Struktura MAC rámce

- Frame Control
  - například verze protokolu, příznak opakovaného přenosu, zda je/není použito WEP, příznak, zda budou následovat ještě další rámce, příznaky To DS a From DS, atd.
- adresy

To DS/From DS, adresy

- síť ad-hoc:
  - oba příznaky = 0 (odesílatel i příjemce jsou uzel)
  - addr1 = MAC příjemce (Destination Address)
  - addr2 = MAC odesílatele (Source Address)

Podvrstva MAC

Struktura MAC rámce

- Frame Control
  - například verze protokolu, příznak opakovaného přenosu, zda je/není použito WEP, příznak, zda budou následovat ještě další rámce, příznaky To DS a From DS, atd.
- adresy

To DS/From DS, adresy

- infrastruktura, přenos od AP ke stanici:
  - To DS=0 (příjemce je uzel), From DS=1 (odesílatel je AP/DS)
  - addr1 = MAC příjemce (stanice)
  - addr2 = BSSID (MAC AP), fyzický odesílatel
  - adr3 = MAC odesílatele (stanice), logický odesílatel

Podvrstva MAC

Struktura MAC rámce

- Frame Control
  - například verze protokolu, příznak opakovaného přenosu, zda je/není použito WEP, příznak, zda budou následovat ještě další rámce, příznaky To DS a From DS, atd.
- adresy

To DS/From DS, adresy

- infrastruktura, přenos k AP:
  - To DS=1 (příjemce je AP/DS), From DS=0
  - addr1 = BSSID AP (fyzický příjemce)
  - addr2 = MAC odesílatele
  - addr3 = logický příjemce (MAC)

Podvrstva MAC

Struktura MAC rámce

- Frame Control
  - například verze protokolu, příznak opakovaného přenosu, zda je/není použito WEP, příznak, zda budou následovat ještě další rámce, příznaky To DS a From DS, atd.
- adresy

To DS/From DS, adresy

- infrastruktura, přes DS:
  - To DS=From DS= 1
  - addr1 = MAC (BSSID) přijímajícího AP
  - addr2 = MAC (BSSID) odesílajícího AP
  - addr3 = DA (MAC logického příjemce)
  - addr4 = SA (MAC logického odesílatele)

AAA

(autentizace, autorizace, účtování – accounting)

- *autentizace* = ověřování a potvrzování totožnosti komunikujících stran, buď otevřená nebo podle autentizačního klíče
- *autorizace* = určení konkrétních přístupových oprávnění (ACL, politiky), po autorizaci je stanice *přidružena* k přístupovému bodu
- *účtování* = zaznamenávání všech činností provedených uživatelem v systému a případné následné reakce

Šifrování = základ

Typy šifrování

1. symetrické – 1 klíč pro šifrování i dešifrování
2. asymetrické – 2 klíče (soukromý a veřejný)
3. hybridní

Potřebujeme:

- šifrovací algoritmus
- „proměnné“ složky postupu – obvykle šifrovací klíč

Šifrování = základ

Symetrické šifrování

- odesílatel zašifruje data pomocí klíče, odešle
- příjemce dešifruje data pomocí téhož klíče
- výhoda: rychlost šifrování a dešifrování
- problém: jak bezpečně distribuovat klíč – nutnost zabezpečeného kanálu pro přenos klíče

Například: DES, AES, RC4

Šifrování = základ

Asymetrické šifrování

- princip: jednocestná funkce
- pro tutéž komunikaci existují dva klíče – veřejný a soukromý, ten soukromý má pouze jeden účastník komunikace
- soukromý klíč vlastní příjemce
- odesílatel šifruje veřejným klíčem, příjemce dešifruje soukromým
- výhoda: veřejný klíč lze poslat nezabezpečeným kanálem
- nevýhoda: výpočetně (časově) náročné

Například: RSA, PGP, digitální podpisy

Šifrování = základ

Hybridní šifrování

- kombinace obou
- první stupeň = symetrické šifrování (odesílatel zašifruje data pomocí symetrického klíče)
- druhý stupeň = asymetrické šifrování (symetrický klíč zašifruje asymetricky veřejným klíčem příjemce)
- odešle
  - data šifrovaná symetricky (velký objem $\Rightarrow$ výhoda rychlosti symetrie)
  - symetrický klíč šifrovaný asymetricky (malý objem $\Rightarrow$ rychlost není tak nutná)
- komunikace obvykle bývá delší, proto je výhodné poslat šifrované symetrické klíče pouze jednou (v obou směrech) $\Rightarrow$ relace

Metody autentizace

- WEP – zastaralý, dávno prolomen
- WPA – používá stejné klíče jako WEP, ale dynamicky je mění (protokol TKIP), autentizace pomocí RADIUS Serveru (přihlašování jménem a heslem) nebo klíče PSK (Pre-Shared Key)
- WPA2 – šifrování AES
- zjednodušená autentizace WPS

Další přídavné mechanismy, například IEEE 802.1

WEP (Wired Equivalent Privacy)

Šifrování

- stejné šifrování pro autentizaci i přenos dat – možnosti:
  - bez šifrování (plně otevřená síť)
  - symetrická šifra RC4, 40bitový *statický* klíč + 24bitový *proměnný* inicializační vektor = 64bitový RC4 klíč
  - symetrická šifra RC4, 104bitový *statický* klíč + 24bitový *proměnný* inicializační vektor = 128bitový RC4 klíč

  IV (inicializační) vektor se mění pro každý paket $\Rightarrow$ příjemce musí mít možnost IV vektor zjistit
  - teoreticky může existovat sdílený algoritmus pro generování IV vektoru
  - prakticky ve WEP: IV vektor je součástí *nešifrované* hlavičky WEP paketu!!! (hned první prvek uvnitř MAC rámce)

WEP (Wired Equivalent Privacy)

Autentizace

1. žádost o připojení
2. přístupový bod odešle žadateli (stanici) náhodně vygenerovaný řetězec
3. stanice i přístupový bod tuto sekvenci zašifrují
4. stanice odešle zašifrovaný řetězec
5. přístupový bod porovná

WEP (Wired Equivalent Privacy)

Autentizace

1. žádost o připojení
2. přístupový bod odešle žadateli (stanici) náhodně vygenerovaný řetězec
3. stanice i přístupový bod tuto sekvenci zašifrují
4. stanice odešle zašifrovaný řetězec
5. přístupový bod porovná

Výhody a nevýhody

- výhoda: kompatibilita, transparentní pro aplikace (je na L2)
- kontrola integrity pomocí kontrolního součtu CRC-32
- nevýhoda: téměř nulová bezpečnost, i když lepší než „bez“
- nástroj Aircrack dokáže odposlechnout klíč během několika minut

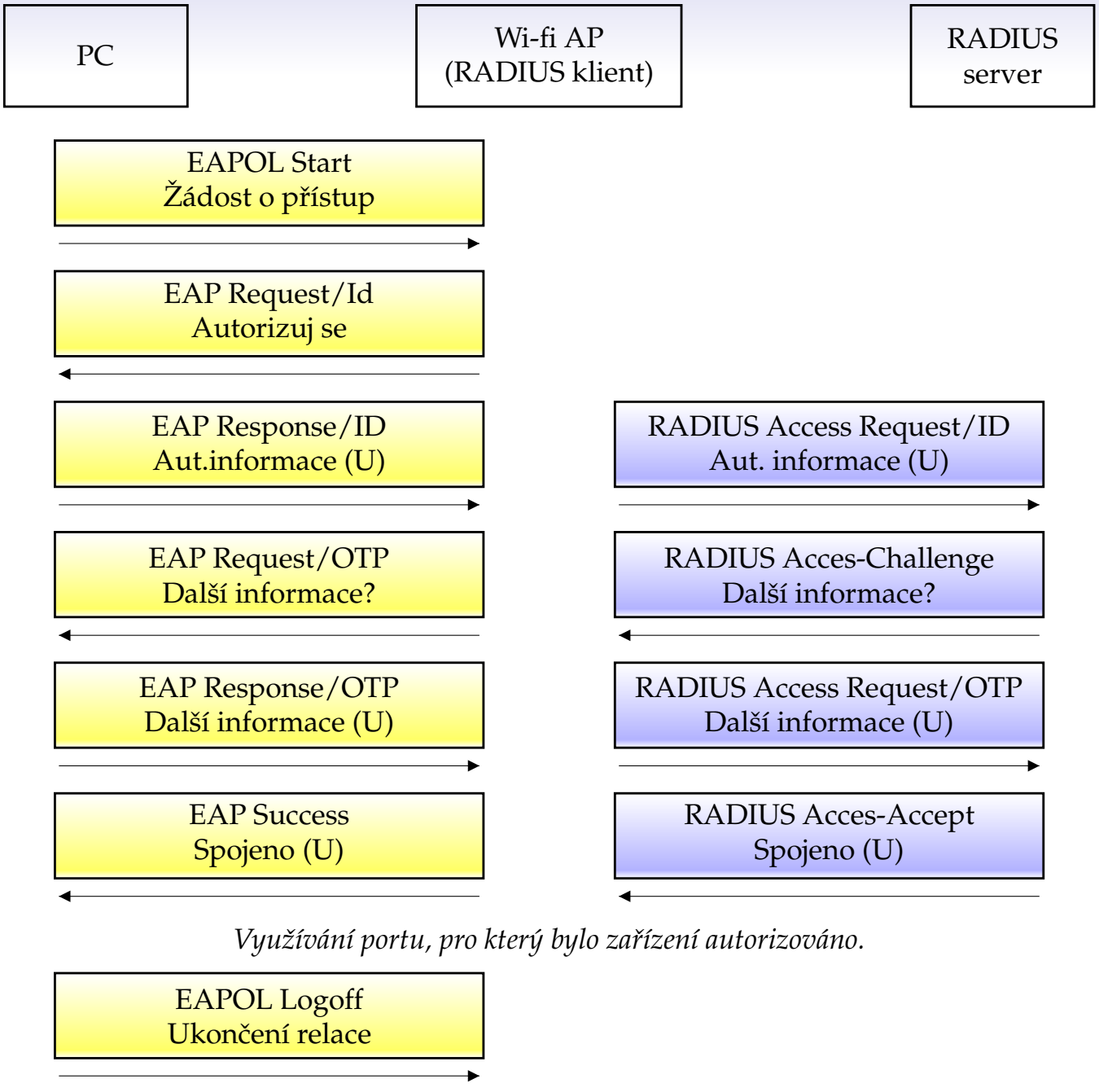
IEEE 802.1X

- mechanismus autentizace uživatelů, distribuce klíčů a zajištění integrity zpráv
- autentizační server (například RADIUS – Remote Authentication Dial-In User Service)
- RADIUS: struktura typu klient-server
  - RADIUS server
  - klienty = přístupové servery (autentizátoři)
- volně dostupný SW: FreeRADIUS, DaloRADIUS

RADIUS – komunikace

- uživatel požádá o připojení,
- přístupový server si vyžádá přihlašovací jméno a heslo,
- přístupový server odešle RADIUS serveru (přes lokální nebo rozlehlou síť) žádost o připojení (RADIUS Access Request),
- RADIUS server ověří platnost přihlašovacího jména a hesla (dostal je v zašifrované podobě),
- podle výsledku ověření odešle přístupovému serveru souhlas nebo odmítnutí (RADIUS Access Accept/Deny).

Na stanici musí běžet klientská aplikace (je běžně součástí operačních systémů).



Využívání portu, pro který bylo zařízení autorizováno.

RADIUS – komunikace

Šifrování: obvykle některá z metod EAP

- EAP-TLS (Microsoft) – v kombinaci s protokolem TLS a mechanismem PKI, certifikáty X.509 (místo jména a hesla), dostupný na většině verzí Windows, MacOS X
- LEAP (Cisco) – dynamické klíče WEP jednorázové pro každou relaci, relace je časově omezená (několik minut), oboustranná autentizace
- EAP-MD5 – ze jména a hesla vytvoří MD5 hash, používá pouze statické klíče WEP, nejméně bezpečná možnost
- další – EAP-TTLS, EAP-PSK, EAP-IKEv2, atd.

EAP lze zapouzdřovat, například PEAP stanovuje zapouzdření (jakéhokoliv) EAP do zabezpečeného tunelu.

WPA (Wi-Fi Protected Access)

Princip

- dočasné řešení, které vzniklo před dokončením standardu IEEE 802.11i (WPA2)
- „ořezání“ připravovaného WPA2 na pouze ty prvky, které nevyžadovaly změny v hardwaru
- šifrování podobně jako u WEP (RC4), ale IV vektor je 48bitový, klíč 128bitový
- podpora šifrování: protokol TKIP (Temporal Key Integrity Protocol) pro dynamickou správu šifrovacích klíčů (celý klíč se mění pro každý paket)

WPA (Wi-Fi Protected Access)

Integrita zpráv

- *mechanismus MIC* (Message-Integrity Check, taky Michael) pro kontrolu integrity zpráv (def. v TKIP)
- na konec šifrované části rámce před kontrolní součet se přidá 64 kontrolních bitů (MIC) vytvořených z
  - cílové a zdrojové MAC adresy,
  - dat,
  - pořadového čísla paketu a náhodné hodnoty (příp. priority)

  vpodstatě digitální podpis paketu

WPA (Wi-Fi Protected Access)

Varianty

1. WPA-Enterprise (pro firemní užití) – používá se v kombinaci s IEEE 802.1X – RADIUS
2. WPA-Personal (domácnosti, SOHO segment; také WPA-PSK) – autentizace s provádí jen pomocí sdíleného klíče PSK

WPA-PSK (Pre-Shared Key)

- není nutné mít speciální autentizační uzel v síti, stačí běžná infrastrukturní síť
- uživatel zadává heslo 8-63 ASCII znaků (nebo 64 hex. číslic)

WPA2 (IEEE 802.11i)

- místo TKIP používá protokol CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
- šifrování: místo slabé RC4 používá 128bitové šifrování AES, MIC pole je také o délce 64bitů
- varianty: WPA2-Enterprise, WPA2-PSK (Personal)

Autentizace WPS (W-Fi Protected Setup)

Více možností – PBC, PIN, NFC, atd.

Tlačítko WPS (PBC – Push Button)

1. na AP zmáčkneme tlačítko „WPS“ (nebo QSS nebo podobně – hardwarové nebo „softwarové“ tlačítko)
2. po několik desítek sekund AP skenuje okolí a hledá nové stanice
3. stejné tlačítko zmáčkneme na zařízení, které chceme připojit (lednička, televize apod.)
4. AP detekuje nové zařízení, automaticky provede autentizaci a asociaci

Riziko: několik desítek sekund je síť prakticky bez ochrany

Autentizace WPS (W-Fi Protected Setup)

WPS přes PIN

1. na připojovaném zařízení zjistíme PIN (v administraci zařízení nebo na nálepce)
2. PIN zadáme v administraci AP
3. zařízení si opět vše automaticky vyjedná s AP, případně může být třeba zadat přístupové údaje

Riziko:

- AP s podporou tohoto typu WPS naslouchá neustále
- PIN je 8místné číslo, poslední číslice je kontrolním součtem
- pokud PIN zadáme špatně, AP vrací informaci, která polovina PINu je špatně!

Zabezpečení Wi-Fi sítí

Blokování vysílání SSID

- AP standardně vysílá své SSID, ale nemusí, pak síť není běžným způsobem viditelná
- dá se snadno překonat

Filtrování MAC adres

- whitelist nebo blacklist
- také se dá překonat

Změna přednastavených přístupových údajů

- přihlašovací údaje, případně SSID

Monitorování WLAN

- NetStumbler – identifikuje přístupové body, dá se použít pro zjištění neautorizovaných přístupových bodů nebo možných zdrojů rušení vlastní sítě
- Wireshark (dříve Ethereal) – analyzátor LAN sítí, ať už „drátových“ nebo bezdrátových
- AirSnort – monitoring sítě
- Kismet – monitoring sítě, IDS (Intrusion Detection System)

Antény

- signál se šíří *kolmo na anténu* všemi směry
- vysokofrekvenční zářič, měli bychom zkontrolovat sílu signálu (zdraví, rušení okolních sítí)
- zarušení $\rightarrow$ špatný signál, „padání“ přístupového bodu
- řešení: domluva se sousedy, volba kanálů, přechod na IEEE 802.11a
- naopak – slabý signál (příliš velká oblast) $\rightarrow$ pořídíme Wi-Fi router, který dokáže pracovat v režimu opakovače–zesilovače

MIMO

(Multiple Input Multiple Output)

= využití více antén a hlavně algoritmus pro kombinování přijatého signálu z těchto antén

- prakticky se počítá s omezením na 4 antény pro vnitřní oblast budov a 16 antén pro použití venku
- pracuje na fyzické vrstvě, a tedy jeho konkrétní implementace hodně souvisí s IEEE 802.11a/b/g/n
- často u 802.11n, kde slouží také ke zvýšení přenosové kapacity v důsledku paralelního vysílání
- MU-MIMO (Multi-User MIMO): možnost komunikovat s několika klienty zároveň (různé antény)

Wi-fi 4. generace

- místo překrývajících se buněk *blankety*, centralizovaná síť
- jeden blanket přes všechny AP, všechny na stejném kanálu, AP jsou připojeny kabelem
- obrazně: tyto AP fungují jako antény vzhledem k centrálnímu prvku, podobně jako v klasické 802.11n antény v MIMO režimu vzhledem k jednomu AP
- AP nefungují samostatně, veškerá obdržená data přeposílají centrálnímu prvku
- kompatibilní s IEEE 802.11a/b/g/n
- čím víc AP, tím lepší pokrytí, propustnost, rychlost
- kvalitní zabezpečení