Bezdrátové sítě IEEE 802.11b/g

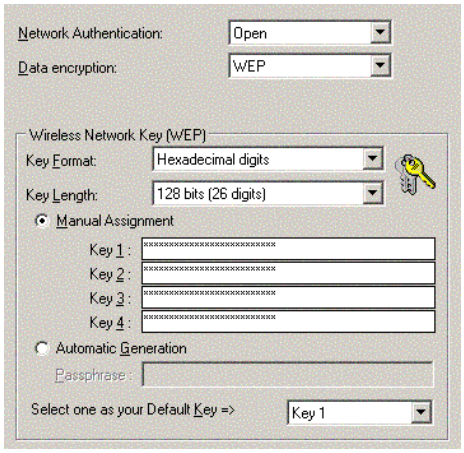
Zpracoval: Jan Dohnal
Ročník: 3.
Předmět: 32PD
Vedoucí úlohy: Ing. Vaněk

1. Zadání

1. Seznamte se s WiFi adaptérem WL-167g a access pointem WL-500gx.
2. Proveďte nastavení adaptéru a access pointu dle návodu.
3. Vytvořte seznam dostupných sítí (SSID, síla signálu , šifrování , kanál,…)
3. Navažte spojení s WiFi kamerou, zhodnoťe kvalitu přenášeného obrazu.
4. Změřte přenosové rychlosti při stahování souboru z FTP – klient v režimu 802.11g
5. Změřte přenosové rychlosti pro stahování souboru z FTP – klient 802.11b
6. Změřte zpoždění paketů pomocí programu PING mezi
   - PC a Access Pointem
   - PC a FTP serverem

2. Měření

Hlavním úkolem měření bylo zprovoznit síťové spojení mezi adaptérem ASUS WL-167g a AP což se podařilo rychle. Konfigurace adaptéru spočívala v nastavení WiFi parametrů, jako je SSID, WEP šifrování (tento adaptér bohužel nepodporuje WPA protokol). Při hledání dostupných sítí jsme zjistili, že adaptér není nijak zvláště výkonný. Podařilo se nám zaznamenat 3 různé sítě:

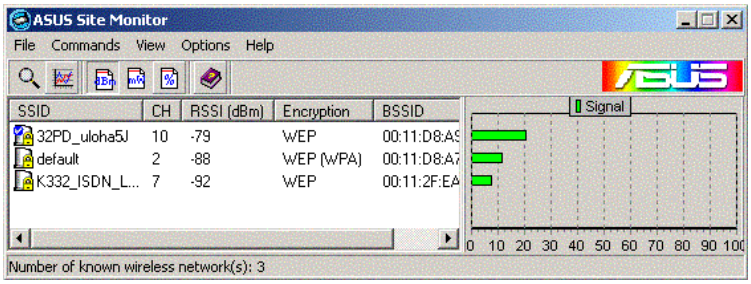


Po úspěšném spárování s AP stačilo již nastavit pouze síťové parametry IP:

IP adresa 10.0.0.55
maska 255.255.255.0
GW, DNS: 10.0.0.1

Nastavení AccessPointu bylo o něco složitější. Vzhledem k tomu, že funguje jako router mezi WiFi a LAN konfiguruje se pomocí síťového protokolu HTTP. Nastavení opět probíhalo ve dvou úrovních. Nejdříve IP routeru s následujícím nastavení:

adresa 10.0.0.33
maska 255.255.255.0
GW, DNS: 10.0.0.1



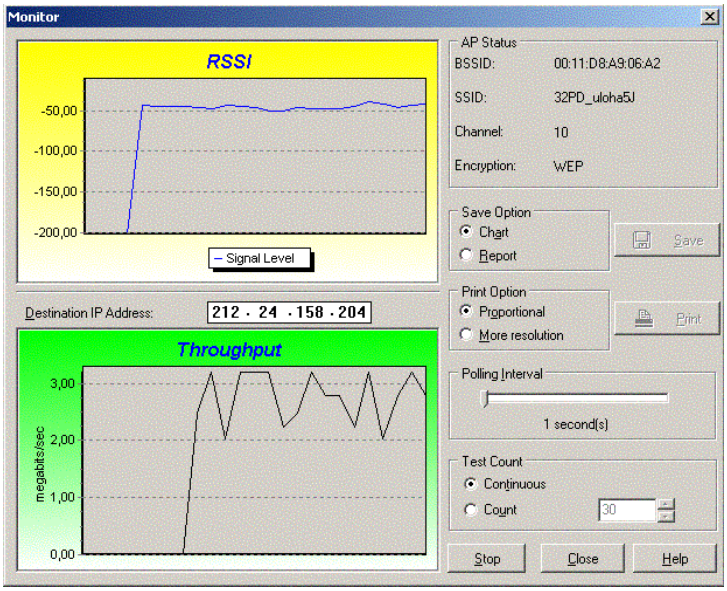
a pak WiFi:

SSID: 32PD_uloha5J
Channel 10
Network Autentication: Shared
WEP Pre-Shared Key: 01234567890123456789012345

Následné měření rychlosti přenosu jsme měřili pomocí programu ASUS Site Monitor a přenášli jsme soubory o velikosti okolo 4,5MB (připojení bylo dostatečně rychlé, tzn. cca 3,2Mb/s).

Nakonec jsme se připojili na WiFi kameru a zjistili z úhlu záběru polohu kamery.

Pomocí programu PING jsme sledovali rychlost odezvy v rámci sítě WiFi. Po počátečních problémech způsobenými zřejmě špatnou odezvou Windows na změnu konfigurace.



Používané přístroje

adaptér Asus WL-167g pro připojení do bezdrátové sítě 802.11b/g
Access Point - Asus WL-500gx
WiFi kamera Vivotek IP3136

3. Závěr

Úkolem měření bylo seznámení s WiFi technologií což se celkem dobře povedlo, zjistili jsme jaké jsou standardy a jaké reálné přenosové rychlosti. Také jsme zjistili problémy se zabezpečením WiFi sítí. Cvičení bylo úspěšné.

4. Použité zdroje

Úloha 5J - popis Wi-Fi - http://www.comtel.cz/files/download.php?id=1738 (jako příloha)

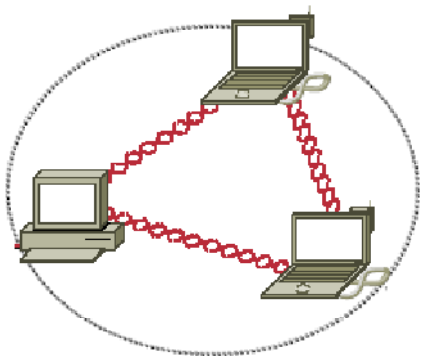
Velmi stručný a řadu důležitých věcí zcela opomíjející úvod do problematiky bezdrátových sítí dle standardu IEEE 802.11

Standardem pro bezdrátové sítě jsou dokumenty pracovní skupiny IEEE 802.11. Slupina 802.11 je podskupinou výboru IEEE 802 pro LAN a MAN. Standard 802.11 byl přijat v červenci 1997 a definuje:

- přístupovou metodu k médiu bezdrátových sítí,
- specifikaci fyzické vrstvy (PHY) modelu RM-OSI

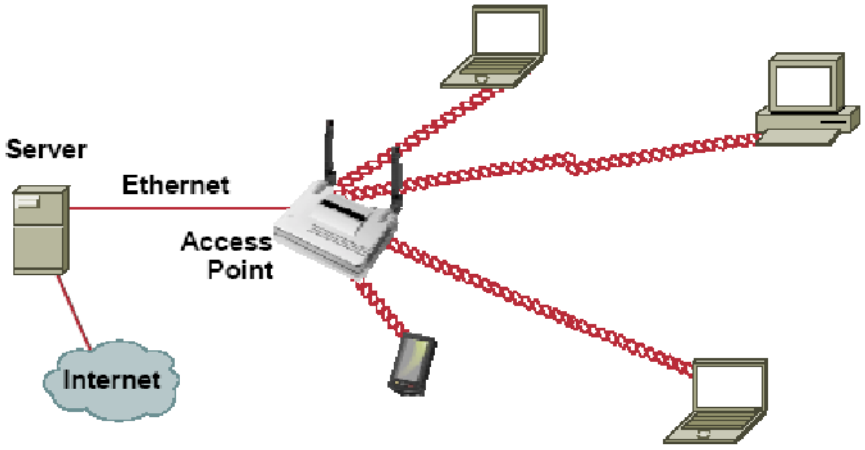
Topologie sítě

Základním prvkem sítě je bezdrátový uzel. Dva a více uzlů, které se navzájem uznaly a navázaly spolu komunikaci, tvoří Basic Service Set (BSS), který má svůj vlastní identifikátor, tzv. BSSID. Jednotlivé uzly spolu komunikují přímo, systémem peer-to-peer. Takto vytvořená síť se nazývá Ad-Hoc. Tento způsob je zejména vhodný pro vybudování menších počítačových sítí. Po nákupu síťových adaptérů a konfiguraci klientů je síť možno okamžitě provozovat. Klienti jsou mobilní v rámci dosahu pokrytí.



Ad-Hoc režim

Pro větší sítě je nutné mít v tzv. přístupový bod (Access Point – AP). Potom BSS operuje v tzv. Infrastructure mode. Přístupový bod řídí veškerý provoz v bezdrátové síti a zároveň zpravidla tvoří můstek do běžné sítě na bázi strukturované kabeláže. Veškerá komunikace mezi účastníky bezdrátové sítě jde vždy prostřednictvím přístupového bodu.



Režim Infrasctructure

V praxi nastává situace, kdy je velikost jedné buňky BSS nedostatečná. Tato velikost je v Infrastructure mode daná dosahem AP. V takovém případě připojíme jednotlivé AP na společný distribuční systém, zpravidla to bývá síť Ethernet, a získáme tak Extended Service Set (ESS), který má své ESS ID a je tvořen jednotlivými překrývajícími se BSS. Tím je možné pokrýt signálem velký prostor a umožnit uživatelům volný pohyb v celé oblasti, tj. roaming

Fyzická vrstva

Standard 802.11 definuje v základu 3 fyzické vrstvy:

- rádiový přenos
  - FHSS – Frequency Hopped Spread Spektrum
  - DSSS – Direct Sequence Spread Spectrum
- přenos v IR pásmu infračervený přenosu.

Později byl rozšířen o technologie ortogonálního frekvenčního multiplexu a technologii HR/DSSS. Vzhledem k nevýhodám IR přenosu (nutná přímá viditelnost, malý dosah, atp..), se tento způsob prakticky nerozšířil, a dnes je nejvyužívanější technika přímo rozprostřeného spektra DSSS / OFDM.

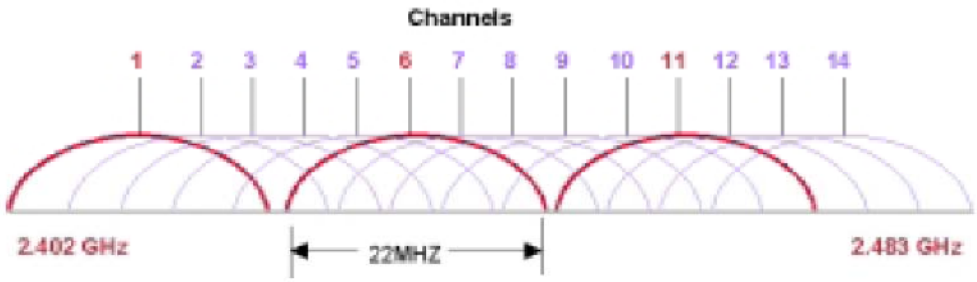
V České republice je umožněn provoz v bezlicenčním pásmu ISM (Industrial Scientific Medical Band) 2,400–2,4835 GHz generální licencí GL-12/R/2000, vydanou Českým telekomunikačním úřadem. Maximální povolený vyzářený výkon EIRP je 100mW.

DSSS

Technika přímo rozprostřeného spektra (DSSS, Direct Sequence Spread Spektrum) předpokládá, že každý jednotlivý bit, určený k přenosu, je nejprve nahrazen určitou sekvencí bitů, a skutečně přenášena (modulována na nosný signál) je pak až tato sekvence bitů.

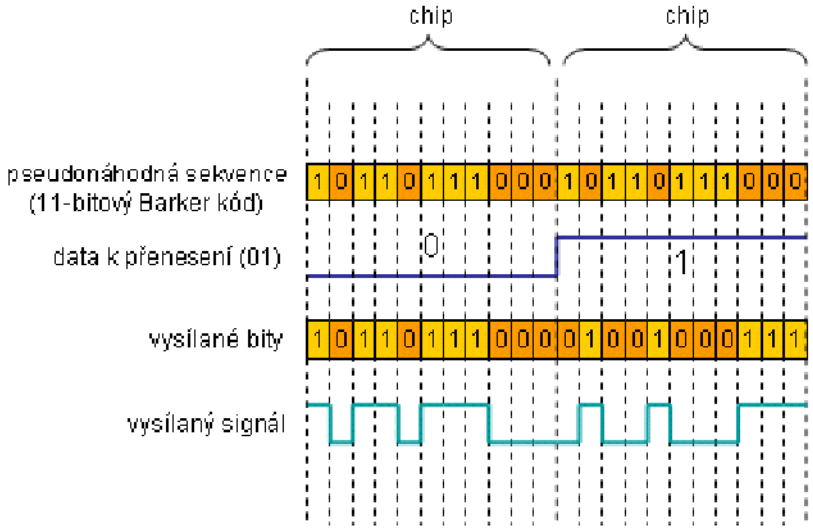
DSSS dělí pásmo (2,412GHz - 2,484 GHz) na 14 kanálů. Šířka jednoho kanálu je 22Mhz, ale rozdíl mezi frekvencemi je pouze 5Mhz, tzn. že vedle sebe ležící kanály se překrývají. Pouze 3 se nepřekrývají vůbec (kanály 1, 6 a 11). Vysílač komunikuje s přijímačem na jednom

předem zvoleném kanále (frekvenci). Pásmo 2,4Ghz však není ve všech zemích stejné, a tak je v různých zemích povoleno vyžívat pouze některé kanály (např. v ČR je možno využít kanály 1-13).



Kanály při použití DSSS

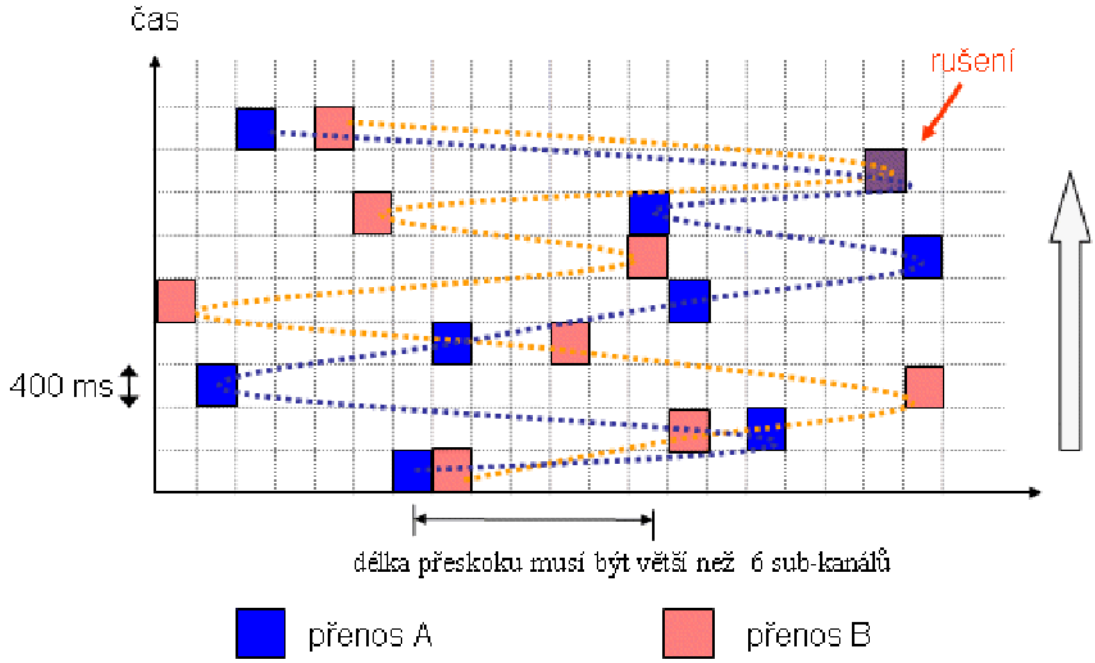
Standard 802.11 pro přenosové rychlosti 1 Mb/s a 2 Mb/s počítá s tím, že každý bit je nahrazen 11-bitovou sekvencí bitů (tzv. Barterovým kódem), označovanou také jako tzv. chip. Jde o umělé zavedení redundance (nadbytečnosti), podobné tomu, které se při datových přenosech někdy používá pro zajištění větší spolehlivosti přenosů. Zde je ale důvod pro zavedení takovéto redundance jiný - signál je zde rozprostřen do větší části spektra, je méně citlivý vůči rušení (což opět zvyšuje spolehlivost přenosu), a ostatním uživatelům se jeví jako náhodný šum (k tomu je zapotřebí, aby příslušná sekvence bitů, alias chip, byla volena alespoň pseudonáhodně).



Systém modulace je závislý na použité přenosové rychlosti. Technologie DSSS umožňuje přenosy rychlostmi 1/2/5,5/11 Mb/s. Pro rychlost 1 Mb/s je signál modulován na nosnou frekvenci pomocí BPSK (Binary Phase Shift Keying). Pro rychlost 2 Mb/s se použije čtyřstavovou fázovou modulací QPSK (Quaternary Phase Shift Keying). Rychlosti 11 a 5,5 Mb/s (definované v 802.11b) používají modulace CCK (Complimentary Code Keying) vyvinuté firmami Lucent Technologies a Harris Semiconductor. 802.11b. Kromě kódování CCK nabízí standard 802.11b alternativně kódování PBCC (Packet Binary Convolutional Coding), které poskytuje, za cenu složitějšího dekódéru, poněkud lepší výsledky.

FHSS

Princip této techniky je následující: nosný signál s namodulovanými daty je vysílán na určité frekvenci (resp. v úzkém frekvenčním pásmu, sub-kanálu, v případě 802.11 o šířce 1 MHz) jen po velmi krátkou dobu (t<400 ms), a poté "přeskočí" a pokračuje na jiné frekvenci podle předem známého schématu.. Dostupné pásmo (zhruba 83,5Mhz) je rozděleno na 79 kanálů o šířce 1 Mhz, zbylé pásmo slouží jako "ochranné" proti interferencím ze sousedních frekvenčních pásem. Přenosová rychlost je definována ve dvou úrovních, zaručená je 1 Mb/s a při dobrých přenosových podmínkách je možné přejít na 2 Mb/s. Výhodou je možnost existence více nerušících se sítí vedle sebe (prakticky až 15 na rozdíl od 3 u DSSS). Nevýhodou je menší odolnost proti rušení a malá přenosová rychlost. Dnes se již prakticky nepoužívá, všechny novější standardy b/g/h používají DSSS.



OFDM

Nový standard 802.11g přinesl technologii ortogonálního frekvenčního multiplexu i do pásma 2,4 Ghz (původně jej vyžíval standard. 802.11a v pásmu 5GHz). Maximální rychlost byla zvýšena až na 54Mb/s. Princip je takový, že tu část frekvenčního spektra, kterou má tato technika k dispozici, rozděluje na menší části (sub-kanály), po kterých přenáší samostatné nosné signály (sub-nosné). Na každý takovýto (sub) nosný signál pak mohou být samostatně namodulována konkrétní data, čímž vzniká nezávislý přenosový kanál. Lze si tedy představit, že "celková" data, určená k přenosu, jsou průběžně rozkládána do jednotlivých dílčích přenosových kanálů, přičemž toto rozdělování může být adaptivní a sledovat to, jaké jsou v daném okamžiku přenosové schopnosti daného dílčího kanálu (jak se v něm projevuje event. rušení atd.) - momentálně nejméně zarušené dílčí kanály mohou být využívány intenzivněji (s vyšší přenosovou rychlostí) než ty dílčí kanály, které právě vykazují zhoršené přenosové vlastnosti. Základní přenosovou rychlostí 802.11g při kódování FEC (Forvard Error Correction) a při modulaci BPSK, je 6 Mb/s. Použití alternativního kódování FEC s vyšší efektivitou při modulaci BPSK poskytuje 9 Mb/s. Vyšších rychlostí dosahují režimy, opírající

se o čtyřstavovou QPSK (12 a 18 Mb/s), o šestnáctistavovou 16-QAM (24 a 36 Mb/s) a o čtyřiašedesátistavovou 64-QAM (48 a 54 Mb/s).

Obdobná technika frekvenčního multiplexu je využívána např. u technologie ADSL. Ve všech případech umožňuje maximalizovat využití přenosových schopností daného média i v situaci, když část přenosového spektra má různé vlastnosti a tyto se v čase mění.

Princip OFDM názorně předvádí např. tutoriál Andrew McCormicka *(Java applet)*.

Linková vrstva

Nejdůležitější částí z této oblasti je podvrstva MAC - Media Acces Control, neboli ovládání přístupu k médiu. MAC podvrstva slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením a také vytváří podporu ad-hoc i infrastrukturního zapojení sítě.

Koordinace přístupu k médiu

Ve většině počítačových sítí používáme sdílené přenosové médium - tzn. že počítač připojený do sítě musí "soupeřit" o přenosové médium (ať už se jedná o kabel, nebo vzduch v případě bezdrátových přenosů) s ostatními PC připojenými do sítě. Aby nevznikali kolize a rušení na společném médiu, je nutné přístup nějakým způsobem koordinovat. Například u klasického ethernetu se používá technologie označovaná jako CSMA/CD - Carrier Sense Multiple Acces / Collision Detection - Vícenásobný přístup k médiu s nasloucháním nosné a s detekcí kolizí.

Standard 802.11 pro bezdrátové sítě předpokládá 2 funkce pro koordinaci přístupu k médiu:

- DCF - Distributed Coordination Function - funkce distribuované koordinace
- PCF - Point Coordination Function - funkce koordinace jedním bodem

DCF je základem standardního přístupového mechanismu CSMA/CA, který je v bezdrátových sítích WiFi nejpoužívanější. PCF (vhodný např. pro real-time aplikace) se v současné době prakticky nevyžívá.

CSMA/CA

U klasického ethernetu může každá stanice slyšet vysílání jiné stanice, a tak detekovat kolizi. U bezdrátových sítí však toto neplatí, stanice je schopná detekovat volné médium ve svém okolí, to však neznamená, že to je volné u příjímače. Např. stanice komunikující prostřednictvím AP svoje vysílání navzájem nemusí vůbec slyšet. Toto se nazývá problém "skrytého uzlu".

Proto se u bezdrátových sítí používá protokol CSMA/CA (Carrier Sense Multiple Acces / Collision Avoidance - Vícenásobný přístup k médiu s nasloucháním nosné a předcházením kolizí), který minimalizuje vznik kolizí a interferencí.

K tomu používá CSMA/CA čtyři speciální rámce:

- RTS - Request to send

- CTS - Clear to send
- ACK - Acknowledge
- NAV - Network allocation vector

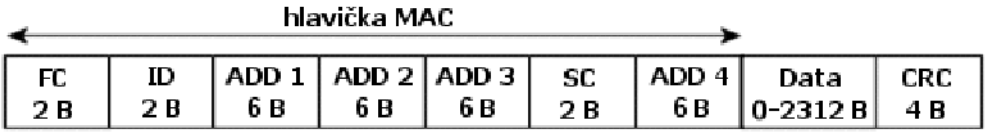
K mechanismu přecházení kolizí se přidává ještě kladné potvrzování. To znamená, že stanice nejprve naslouchá, a pokud je médium volné, počká ještě určený čas (DIFS,Distributed Inter Frame Space) a teprve pak začne vysílat. Přijímací stanice zkontroluje kontrolní CRC součet přijatého paketu a odešle potvrzení ACK. Přijetí potvrzení znamená pro odesílající stanici, že nedošlo ke kolizi. Pokud potvrzení nepřijde, stanice opakuje vysílání.

Vlastní "naslouchání" probíhá pomocí dvou speciálních rámců - RTS a CTS. Stanice, která chce vysílat, pošle nejdříve krátký řídící paket (RTS, Request To Send), který obsahuje kromě zdroje a cíle i trvání následujícího přenosu. Cílová stanice odpoví jiným řídícím paketem (CTS, Clear To Send), který rovněž obsahuje dobu trvání následujícího přenosu. Stanice slyšící RTS a/nebo CTS paket si nastaví indikátor virtuálního naslouchání, tzv. NAV (Network Allocation Vector) na dobu trvání přenosu. Jinými slovy bude po tuto dobu brát médium jako obsazené. Snižuje se tak pravděpodobnost kolize ze strany ostatních stanic v lokalitě příjemce pouze na dobu vysílání RTS, protože pak už zachytí paket CTS a budou brát médium jako obsazené. Takový mechanismus je efektivní pouze pro delší pakety, proto standard umožňuje také přenos bez RTS/CTS mechanismu. Tato možnost je volitelně nastavitelná na stanici (RTS Treshold). Multicasty ani broadcasty se nepotvrzují.

Formát rámce

Rámec se sestává z MAC hlavičky (MAC header), která obsahuje informace o přenášených datech, a těla rámce, jenž obsahuje vlastní data a kontrolní součet (CRC).

Struktura rámce



MAC rámec obsahuje:

- Frame Control (FC) - informace o verzi protokolu a typu rámce (řídící, datový nebo kontrolní rámec)
- Duration/ID (ID)
  - Station ID je identifikátor stanice používaný pro funkci úspory energie.
  - Duration Value - délka trvání rmce používaná pro výpočet rezervace přenosového média pomocí Network Allocation Vector (NAV)
- Address field 1-4 - čtyři adresní pole obsahující adresy zdroje, cíle, přenašeče a přijímače v závislosti na poli Frame Control.
- Sequence control (SC) - používá se pro defragmentaci a likvidaci duplikátních rámců.
- CRC (někdy také FCS) - obsahuje 32-bitový kontrolní součet (CRC), který se počítá ze všech dat v MAC hlavičce a datového pole

Struktura pole Frame Control

Protocol 8 b	Type 2 b	Subtype 4 b	To DS 1 b	From DS 1 b	More Frag 1 b	Retry 1 b	Pw Mgt 1 b	More Data 1 b	WEP 1 b	Order 1 b

- Protocol version - verze standardu 802.11
- Type, Subtype - indikuje obsah rámce - řídící (management), ovládací (control) a datový (data); subtypy pak RTS, CTS, ACK, atd...
- To DS je nastaveno na 1, pokud je rámec posílán do distribučního systému.
- From DS je nastaveno na 1, pokud je rámec přijímán od distribučního systému.
- More Fragment je nastaveno na 1, pokud byl přenášený rámec rozdělen na více částí přenášených samostatně.
- Retry oznamuje, že jde o znovuvysílání již vysílané části rámce. Přijímač tak poznává duplicitu rámce.
- Power management je režim úspory energie, v němž se bude stanice nacházet po přenesení rámce.
- More data oznamuje, že je ve vyrovnávací paměti pro tuto stanici uloženo více dat.
- WEP indikuje, že tělo rámce je šuifrováno algoritmem WEP
- Order indikuje, že rámec je odesílán službou Strict-Ordering, tedy nebude dále zpracováván.

Některé důležité kontrolní rámce

Struktura rámce RTS:

Frame Control (2B)	Duration (2B)	Receiving Addres (6B)	Transmitting Addres (6B)	FCS (4B)

Struktura rámce CTS:

Frame Control (2B)	Duration (2B)	Receiving Addres (6B)	FCS (4B)

Struktura rámce ACK

Frame Control (2B)	Duration (2B)	RA (6B)	FCS (4B)

Některé důležité řídící rámce

Struktura rámce Beacon:

Timestamp (8B)	Beacon Interval (2B)	Capability information (2B)	SSID (2-34B)	Supported rates (3-10B)	FH Parameter Set (7B)	DS Parameter Set (3B)	CF Parameter Set (8B)	IBSS Parameter Set (4B)	TIM (6-256B)

Všechny elementy krom prvních tří patří do skupiny tzv. *informačních elementů*, jejichž zákl. struktura je následující:

ElementID (1B)	Length (1B)	Information (max. 255B)

Délky informačních elementů jsou uváděny včetně polí ElementID a Length

- FH Parameter Set - slouží k synchronizaci zařízení využívajících technologii FHSS
- DS Paremeter Set - podobě jako předchozí, ale pro zařízení vyžívající DSSS
- CF Parameter Set - je přítomný u zařízení používajících PCF
- IBSS Parameter Set - je přítomný u zařízení vyžívajících IBSS
- TIM - je přítomný v rámcích vygenerovaných AP

Struktura rámce Probe Request:

SSID (2-34B)	Supported rates (3-10B)

Struktura rámce Probe Response:

Timestamp (8B)	Beacon Interval (2B)	Capability information (2B)	SSID (2-34B)	Supported rates (3-10B)	FH Parameter Set (7B)	DS Parameter Set (3B)	CF Parameter Set (8B)	IBSS Parameter Set (4B)

Zabezpeční Wi-Fi

Na téma zabezpečení bezdrátových sítí existují celé knihy, proto zde budou zmíněny pouze nejdůležitější postupy a metody.

Autentizace IEEE 802.11 (POZOR nezaměňovat s 802.11**i** !)

Standard 802.11 specifikuje dvě možné metody autentizace (ověření "totožnosti" uživatele) na linkové vrstvě:

- **open-system** autentizace
- **shared key** autentizace

Open-system autentizace

Tento typ autentizace je jako jediný vyžadovaný ve standardu 802.11 pro všechny zařízení. Bohužel však nepředstavuje téměř žádnou úroveň zabezpečení. Klient je totiž autentizován pouze na základě informací jím zaslaných, které nejsou ověřovány. Tzn. že AP vždy autentizuje každého klienta.

Shared key autentizace

Autentizace pomoci sdíleného klíče je ve standardu vyžadována pro všechna zařízení s podporou WEP. Zatímco u open-system autentizace pouze klient odeslal žádost *Authentication request* a AP mu ihned odpověděl zprávou *Authentication succes*, zde je proces poněkud komplikovanější. Klient, který se chce připojit k síti, nejprve vyšle žádost o autentizaci (*Authentication request*). Přístupový bod mu odpoví náhodně vygenerovaným textem (*Authentication challenge*, nebo též *challenge text*). Klient tento text zašifruje algoritmem RC4 (stejným způsobem jako při použití WEPu) a pošle jej zpět (*Authentication response*). AP si tento text dešifruje a zkontroluje, zda souhlasí s vyslaným. Pokud ano, data od klienta jsou dále propouštěna do sítě a klient je informován o úspěšném přihlášení. Bohužel však tento typ autentizace přináší řadubezpečnostích rizik. Tím, že se posílá jeden text (náhodné číslo, *challenge text*) nejprve jako plain text, a nazpět již zašifrované, může tak útočník odposlouchávající náš přenos získat hodnotné informace - dvojici nezašifrovaného a zašifrovaného textu, ze kterého již pak jednoduchým způsobem získá použitý klíč (díky slabinám algoritmu RC4).

Formát autentizačních zpráv

Algorithm Num	Transaction Seq.	Status Code	Challenge Text

Význam jednotlivých polí:

- **Algorithm Number** (2B) - označuje číslo použité autentifikace:
  - 0 - open-system
  - 1 - shared key
- **Transaction Seq.** (2B) - indikuje kde se právě nacházíme v autentizační sekvenci. První zpráva se označuje 1, druhá 2, atd...
- **Status code** (2B) - posílá se v poslední zprávě jako indikace úspěchu/neúspěchu autentizačního požadavku.

  Může nabývat následujících hodnot:

Hodnota	Význam
0	Úspěch
1	Nespecifikovaná chyba
2-9	Rezervováno
10	Nejsou podporovány všechny požadované funkce z Capability Information field
11	Reasociace byla odmítnuta kvůli nemožnosti potvrdit současnou asociaci

12	Asociace byla odmítnuta kvůli důvodu mimo tento standard
13	Odpovídající stanice nepodporuje specifikovaný autentifikační protokol
14	Byl přijat autentizační rámec s "Transaction sequence" jiným než je očekáván
15	Autentizace odmítnuta kvůli špatné odpvědi (challenge failure)
16	Autentizace odmítnuta kvůli vypršení časového limitu při čekání na další rámec v pořadí
17	Asociace odmítnuta protože AP není schopno obsloužit další stanice
18	Asociace odmítnuta protože stanice nepodporuje všechny vyžadované přenosové rychlosti
19-65535	Rezervováno

Challenge Text (3B - 255B) - je používán pouze u shared key autentizace

SSID

SSID (Service Set ID), kterým se označují přístupové body (Access Point, AP), představuje nejnižší stupeň bezpečnosti pro komunikaci ve WLAN. SSID je logický identifikátor dané bezdrátové podsítě. Může být manuálně nakonfigurován na stanici, dokáže informaci o něm přístupový bod pravidelně vysílat, či může být vysílání SSID vypnuto a klient se na něj sám dotáže (probe). Vysílání SSID se doporučuje vypnout, aby se pro vetřelce přístup do sítě stal obtížnější - nebudou moci SSID snadno odposlechnout.

Filtrování MAC adres

Některé přístupové body umožňují omezit přístup do sítě podle MAC adres. MAC (Media Access Control) adresa je celosvětově jednoznačný identifikátor většiny síťového zařízení, který používá mnoho síťových protokolů druhé vrstvy. MAC adresa má 48 bitů a nejčastěji se zapisuje jako šestice dvou hexadecimálních čísel, tedy ve tvaru xx:xx:xx:xx:xx:xx. První tři dvojice určují výrobce zařízení. MAC adresa příjemce a odesílatele je součástí každého ethernetového rámce Ke zjištění MAC adresy cílového počítače z jeho IP adresy se používá protokol ARP.

Filtrování MAC přináší totiž několik problémů - mezi ty základní patří distribuce seznamu MAC adres a možnost falšovat MAC adresu. Každý přístupový bod si totiž musí udržovat vlastní databázi povolených MAC adres. Ve chvíli, kdy spravujeme několik přístupových bodů ke kterým se nepřipojuje více jak několik desítek klientů, je možné toto dělat standardní cestou - a to přes webové konfigurační rozhraní AP (některé AP ani jinou možnost nepodporují), kde se přidávají/ubírají jednotlivé MAC adresy. V případě větší sítě by se však toto stalo noční můrou správce sítě. Některé AP toto můžou řešit uploadem seznamu pomocí TFTP (Trivial FTP), avšak ten sám o sobě není zabezpečený. MAC adresa jako taková, bývá obvykle v nějaké flash paměti v zařízení. V dnešní době je tato paměť přepisovatelná, tzn. MAC adresa se dá změnit. Útočník tak může zkusit nastavit MAC adresu, a doufat že se "trefí" do povoleného rozsahu, nebo může odposlouchávat komunikaci na síti a odchytit si jednu z povolených MAC adres, kterou později použije.

WEP

Protokol WEP (*Wired Equivalent Privacy*) pracuje jako volitelný doplněk k 802.11b pro řízení přístupu k síti a zabezpečení přenášených dat. WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč. Klíč je stejný pro všechny uživatele dané sítě (sdílený klíč) a klienti jej využívají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu. Ve skutečnosti se tedy ověřuje totožnost síťové karty, nikoli samotného uživatele. Autentizace ve WEP pracuje pouze jednostranně, nikoli vzájemně. Šifrování přenášených dat se provádí 64-bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (*Initialization Vector*) o délce 24 bitů. IV se posílá v otevřené formě a mění se s každým paketem, takže výsledná šifra je jedinečná pro každý jednotlivý paket. WEP používá šifrovací algoritmus RC4. Existuje i silnější zabezpečení ve formě 128-bitového šifrování (sdílený klíč má délku 104 bitů, vektor poté 24 bitů). Hlavní problémy WEPu spočívají především ve statických klíčích (nijak neřeší automatickou distribuci nových klíčů, a tak si ho v případě změny musí každý uživatel sám ručně znovu nastavit), a ve slabém inicializačním vektoru (posílá se "vzduchem" nezakódovaný a ještě se jeho kombinace poměrně "brzy" vyčerpají - jedná se "pouze" o 2^{24} možností). Bezpečnost sítě s WEP je možno narušit snadno odposlechem. K získání WEP klíče stačí odchytat pouze několik set tisíc paketů a pomocí volně dostupných nástrojů (*Airsnort, WEPcrack ,Kismet*) je to již otázka několika málo minut, než útočník získá klíč…

IEEE 802.1x

802.1x (*Port-Based Network Access Control*, 2001) je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. 802.1x má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. Je založený na protokolu EAP (*Extensible Authentication Protocol*, RFC 2284). Ověřování provádí přístupový bod na základě výzvy klienta pomocí externího autentizačního systému (např. Kerberos, nebo RADIUS).

Obecný postup autentizace podle 802.1x:
1) přístupový server k síti (Network Acces Server - NAS), tj. switch nebo bezdrátový přístupový bod, vyšle klientovi na základě detekce jeho přítomnosti zprávu EAP REQUEST-ID.
2) klient odpoví zprávou EAP RESPONSE-ID, která obsahuje identifikační údaje uživatele; přístupový server zapouzdří celou zprávu EAP RESPONSE-ID do paketu RADIUS ACCESS_REQUEST a vyšle ji serveru RADIUS.
3) server RADIUS odpoví zprávou obsahujícím povolení/zákaz přístupu pro daného klienta do sítě: RADIUS ACCESS_ACCEPT/DENY, která v sobě obsahuje informaci EAP SUCCESS/FAILURE, jíž přístupový server přepošle klientovi;
4) v případě povolení (SUCCESS) je příslušný port přístupu do sítě (přes nějž autentizační komunikace probíhala) otevřen pro data daného uživatele, který je na základě úspěšného výše popsaného procesu považován za autentizovaného.

802.1x používá k šifrování dat v další komunikaci pro každou autentizovanou stanici dynamické klíče. Tyto klíče jsou známy pouze dané stanici, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí. Dynamické klíče 802.1x omezují možnosti útočníků. Už se ovšem prokázalo, že ani 802.1x

není dostatečně odolný vůči některým typům útoků (session hijacking , man-in-the-middle attack).

WPA

Zkratka WPA označuje WiFi Protected Area, a jedná se o jakousi předzvěst standardu 802.11i. WPA byl přijat WiFi Aliancí, což je sdružení, které se stará o interoperabilitu jednotlivých zařízení a mezi jeho činnosti patří také udělování certifikátu "WiFi". Díky tomu, že se jedná o "uznaný standard", začínají se již prodávat zařízení s podporou WPA.

WPA používá pro šifrování komunikace protokol TKIP - Temporal Key Integrity Protocol - ten využívá stejný šifrovací algoritmus jako WEP (tedy RC-4), ale s klíčem délky 128 bitů. Na rozdíl od WEPu obsahuje tzv. dynamické dočasné klíče - TKIP pracuje s automatickým klíčovým mechanismem, jenž mění dočasný klíč každých 10 000 paketů. Další výhodou TKIP je MIC - Message Integrity Check - kontrola integrity zpráv. MIC je podstatně lepší než dosud užívaný jednoduchý kontrolní součet CRC.

IEEE 802.11i

Autentizaci a zabezpečení v sítích Wi-Fi komplexně řeší až nový standard 802.11i. Problém autentizace je vyřešen zakomponováním standardu 802.1x. Zabezpečení dat se děje pomocí protokolu TKIP (Tempoval Integrity Protocol). Ten vylepšuje WEP o dynamickou změnu klíčů kontrolu integrity přenášených zpráv (MIC – Message Integrity Check).

K protokolu TKIP, který může pracovat s minimálními požadavky na softwarový upgrade na stávajících zařízeních s hardwarem pro WEP, se přidal nový protokol CCMP (Counter-mode-CBC[1]-MAC[2] Protocol), zaručující silnější šifrování díky využití AES (Advanced Encryption Standard) právě v režimu CCM (kombinuje režim CTR, Counter Mode, pro utajení a CBC-MAC pro autentizaci a integritu).

K vlastnímu šifrování se používá algoritmus AES (Advanced Encryption Standard). Velikost šifrovacího klíče AES může být zvolena jako 128,192 nebo 256 bitů, a samozřejmě platí, že čím delší klíč, tím více poskytuje bezpečnosti ale zároveň potřebuje tím vyšší výpočetní výkon. V protokolu TKIP nahradí AES starý a nevyhovující algoritmus RC-4. Zatímco dříve stačilo útočníkovi odposlechnout dostatečný objem zpráv, aby mohl zlomit klíč WEP, a jedinou obranou bylo manuálně klíče včas změnit, než k tomu dojde, s 802.11i se mění šifrovací klíče automaticky.

Výkonnost 802.11g vs. 802.11b

Výkonnost sítě 802.11g závisí velmi na tom, zda podporuje také 802.11b klienty. Protože klienti 802.11b nerozumí modulaci OFDM (chápou ji jako šum) obsahuje 802.11g ochranný mechanizmus pro koexistenci 802.11b a 802.11g klientů v jedné síti. Jedná se o mechanizmus RTS/CTS, původně vyvinutý jako doplněk k naslouchání nosné podle CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pro řešení problému skrytého uzlu ve WiFi. Ten se v tomto případě spustí v okamžiku přidružení klienta 802.11b k síti 802.11g.

---

[1] CBC – Cipher Block Chaining
[2] MAC – Message Authentication Code

Mechanizmus RTS/CTS zamezí současnému vysílání (kolizím) klientů 802.11g a b, ale za cenu dost vysoké režie. Pokud dojde ke kolizi, musí si klienti zvolit náhodně dlouhou dobu čekání (*back off*), než se znovu pokusí vysílat. Tuto dobu si volí výběrem jednoho z časových úseků. U 802.11bi jich je k dispozici 31 o délce 0-20 µs, u 802.11g (po vzoru 802.11a) pouze 15 o délce 0-9µs. To znamená, že 802.11g bez klientů 802.11b bude mít kratší dobu čekání a lepší výkonnost zejména s rostoucím počtem uživatelů připojených k síti. Pokud se budou v jedné síti nacházet klienti také 802.11b, pak 802.11g přejde na režim 802.11b s delší dobou čekání.

V síti pouze s klienty 802.11g je výkonnost sítě prakticky shodná s výkonností 802.11a (samozřejmě s tím rozdílem, že se pracuje v jiném kmitočtovém pásmu), tedy kolem 25 Mbit/s. S přítomností klientů 801.11b se reálná propustnost sítě snižuje až trojnásobně (na 8 Mbit/s), což je sice více než u tradiční 802.11b (5-6Mb/s) ale rozhodně ne o moc.

Stručné shrnutí standardů skupiny 802.11

802.11 – Původní standard pro WLAN. Pásmo 2,4GHz. Maximální přenosová rychlost 2Mb/s. Přijato v roce 1997.

802.11a – Pásmo 5GHz. Maximální rychlost 54Mb/s. Modulace OFDM. V Evropě je zakázána. Přijat v roce 1999.

802.11b – Pásmo 2,4GHz. Maximální přenosová rychlost 11Mb/s. Přijato v roce 1999.

802.11c - řeší práci komunikačních mostů v rámci podvrstvy MAC (Media Access Control) 802.11

802.11d - mezinárodní harmonizace. Se vznikem standardu 802.11 se ukázalo, že je potřeba mezinárodní kooperace a harmonizace. Problémy způsobovaly různé možnosti vyžití např. pásma 5Ghz (v některých státech je možné využívat pouze část jeho sp

802.11e – MAC Enhancements for Quality of Service – doplněk 802.11a/b/g na podporu kvality služby (QoS), která je potřeba pro interaktivní provoz, např. pro přenos hlasu po WLAN (VoWLAN). Zatím nepřijato.

802.11f - Inter Access Point Protocol (IAPP) - vylepšuje mechanismus předávání stanic (roaming) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu.

802.11g – rychlejší verze Wi-Fi v pásmu 2,4 GHz, zpětně slučitelná s 802.11b, s rychlostí 54 Mbit/s na fyzické vrstvě. Modulace OFDM. Přijat v roce 2003. Vysílací výkon je vzhledem k práci ve stejném pásmu je upraven stejnou generální licencí ČTÚ jako pro IEEE 802.11b. Dosah je mírně větší nebo stejný jako u 802.11b, avšak na hranici dosahu již rychlost klesá více než u "b" zařízení

802.11h – doplněk 802.11a pro použití v Evropě podle požadavků ITU-T, ETSI a CEPT pro harmonizaci využití spektra 5 GHz; s mechanismy pro minimalizaci rušení s jinými systémy: DFS (Dynamic Frequency Selection) a TPC (Transmit Power Control). Přijato v roce 2003.

802.11i – doplněk 802.11a/b/g pro autentizaci uživatele i přístupového bodu, utajení a integritu dat. Přijato v roce 2004.

Pokud jste dočetli tento výklad až sem , jistě bez problémů absolvujete čtvrteční cvičení i kontrolní test. ☺