TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií

Studijní program: B2612 – Elektrotechnika a informatika
Studijní obor: Elektronické informační a řídící systémy

Využití WiFi ve výuce

Bakalářská práce

Autor: **Lukáš Švejzdral**
Vedoucí práce: Ing. Miloš Hernych
Konzultant: Ing. Zbyněk Mader, Ph.D.

V Liberci 3. 1. 2011

Prohlášení

Byl(a) jsem seznámen(a) s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom(a) toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum

V Liberci 3.1.2011

Podpis

Anotace

Tato práce se zabývá problematikou bezdrátových sítí. Shrnuje technologie použité při bezdrátovém připojení. Pomocí dostupné literatury a rešerší výukových materiálů popisuje standard IEEE 802.11, který je klíčový pro bezdrátovou komunikaci. Na základě těchto informací a analýzy dostupných komerčních prvků obsahuje návrh a realizaci sady úloh pro předmět Komunikační technika. Sady úloh budou realizovány na platformě společnosti MikroTik. A to konkrétně na softwarovém produktu RouterOS a hardwarovém řešení Routerboard. Výsledkem práce bude popis standardu 802.11, technologie WiFi, seznámení s produkty společnosti MikroTik a sada úloh s pedagogickou dokumentací.

Klíčová slova

Bezdrátové sítě, IEEE 802.11, WiFi, Access Point, Mikrotik, RouterOS, Routerboard.

Annotation

This work focuses on matters of wireless networks. It summarizes technologies used for wireless networks. Using aviable literature and educational materials, describes standard IEEE 802.11, which is the key standard for wireless communication. Using these information and an analysis of commercially aviable products, contains plan and realization of a set of tasks for lecture Communication technology . Set of tasks will be realized using platform from company MikroTik, concretely on software product called RouterOS and hardware solution called RouterBoard. The goal of this work will be description of standard 802.11 and WiFi technology, familiarization with products from MikroTik and realizations of given taks with pedagogical documentation.

Keywords

Wireless network, IEEE802.11, WiFi, Access Point, Mikrotik, RouterOs, RouterBoard.

Obsah

1 Úvod

Bezdrátové sítě jsou v dnešní době velmi skloňovaným pojmem a nejsou již jen výhradou velkých firem, podnikových sítí či poskytovatelů internetu. Dnes se setkáváme s pojmem bezdrátové sítě velmi často taktéž v osobní sféře. Tyto technologie umožňují uživatelům úplnou volnost připojení i v místech, kde by kabelové sítě byly jen těžko použitelné. Pod pojmem bezdrátové sítě se neskrývá jen notoricky známá technologie WiFi (Wireless Fidelity – bezdrátové spojení), ale i mnoho dalších používaných technologií například Bluetooth, CDMA atd.

Tato bakalářská práce se zabývá převážně technologií WiFi potažmo standardem 802.11, který svým vydáním v roce 1997 odstartoval technologický rozvoj tohoto odvětví. A je klíčovým prvkem bezdrátové komunikace, díky vzájemné kompatibilitě výrobků od různých výrobců bylo umožněno masové šíření WiFi prvků a s tím spojený mohutný rozvoj bezdrátových sítí. Dalším důvodem tak masového šíření WiFi je použití bezlicenčního pásma ISM (Industrial Scientific and Medical) neboli pásmo vyhrazené pro průmyslové, vědecké a lékařské potřeby. To znamená, že sítě WiFi při dodržení pravidel nastavených regulačním úřadem může provozovat každý. Jak již bylo zmíněno bezdrátové sítě založené na standardu 802.11 jsou jen podmnožinou bezdrátových sítí využívající přenos pomocí rádiových vln. Na podobném principu pracují například sítě mobilních operátorů, rádiové a televizní vysílaní. Ty však oproti pásmu ISM potřebují pro své fungování licenci vydanou příslušným regulačním úřadem.

WiFi nabízí svým uživatelům nespočet výhod, které spolu s použitím bezlicenčního pásma přispěly k rozšíření WiFi sítí. Mezi zásadní patří mobilita, flexibilita a jednoduchost výstavby bezdrátové sítě bez nutnosti pokládky kabelů, stavebních úprav nebo nutnosti upravovat infrastrukturu budovy. Přes kterou je poté možnost velmi jednoduše sdílet data a především přístup k internetu. Avšak s nástupem bezdrátových sítí se objevily i problémy v podobě zabezpečení bezdrátových sítí. Díky přístupnosti přenosového média je bezdrátová síť zranitelnější, než sítě kabelové. A proto je nutné zabezpečení bezdrátových sítí věnovat větší pozornost.

Cílem a přínosem této práce je popsat teoretické zásady pro tvorbu bezdrátové sítě. Seznámit se s principy fungování bezdrátových sítí a následně jejich správy a zabezpečení. Taktéž by měla pomoci při výstavbě vlastní bezdrátové sítě na konkrétním hardwarovém řešení. První kapitola je věnována typům sítí, dále pak způsobu přenosu a přehledu norem standardu 802.11. V druhé kapitole se věnuji hardwarovým komponentám WiFi sítí. Je zde uveden přehled komponentů, které se využívají při stavbě WiFi sítí. Následující kapitola se snaží přiblížit správu sítě a popisuji zde nejpoužívanější služby a funkce přístupových bodů. Čtvrtá kapitola je věnována zabezpečení bezdrátových sítí. Práce je zakončena sestavením praktických úloh, které by měly

sloužit jako návod pro sestavení a zabezpečení bezdrátové sítě pomocí komerčně dostupných WiFi prvků v případě této práce od společnosti Mikrotik. Jedním z bodů zadání bakalářské práce bylo vypracování rešerše výuky problematiky bezdrátových sítí na jiných školách v ČR. V rámci splnění tohoto bodu jsem si obstaral studijní materiály týkající se bezdrátových sítí ze tří škol a to SPŠSE Liberec, VUT Brno a ČVUT. Studijní materiály se povětšinou věnovaly pouze obecným popisem bezdrátových sítí, tedy typům přenosů a popisem standardu 802.11 a taktéž otázkou zabezpečení. Ale ani v jednom případě neobsahovaly cvičení, návod či postup jak řešit konkrétní úlohy. Z tohoto usuzuji, že studenti mají dobré teoretické znalosti bezdrátových sítí, které však nejsou podložené praktickou částí, v níž by mohli teoretické znalosti převést do praxe. Právě proto jsem se v této práci zaměřil na sestavení ukázkových úloh, které budou sloužit jako doplněk výuky v předmětu "Komunikační technika". Díky nim si budou moci studenti v praxi vyzkoušet sestavit bezdrátovou síť, spravovat a konfigurovat bezdrátové zařízení a taktéž budou mít možnost porovnat teoretické hodnoty z praxí, například co se přenosových rychlostí bezdrátových sítí týče. Kde se od sebe výsledky mohou velice lišit v závislosti na zarušení prostředí, délce spoje nebo použité technologii. A získají tak přehled o možnostech dnešních bezdrátových sítí. To považuji za hlavní přínos této práce.

2 Počítačové sítě

Pod pojmem počítačová síť se rozumí spojení dvou a více počítačů za účelem sdílení svých prostředků a umožňuje komunikaci uživatelů podle určených pravidel.

2.1 Typy sítí

Počítačové sítě lze rozdělit podle mnoha hledisek. Nejpoužívanějším je rozdělení dle rozlehlosti a účelu sítě: **LAN, MAN, WAN a PAN**. Dále lze počítačové sítě rozdělit, podle hlediska vzájemného vztahu stanic, na sítě typu **peer-to-peer** a **serverové sítě.** A v neposlední řadě dělení podle způsobu propojení na sítě metalické, optické a bezdrátové.

2.1.1 LAN (Local Area Network)

LAN označuje počítačovou síť, která pokrývá malé geografické území (např. domácnosti, malé firmy). Přenosové rychlosti jsou vysoké, řádově Gbit/s.

Mezi sítě LAN patří

- Ethernet, Fast Ethernet, Gigabit Ethernet (IEEE 802.3)
- ARCNET
- Token Bus (IEEE 802.4)
- Token ring (IEEE 802.5)
- IsoEthernet (IEEE 802.9)
- Bezdrátové sítě (WiFi, IEEE 802.11)
- 100VG-AnyLAN (IEEE 802.12)
- Fiber distributed data interface (FDDI) (ISO/IEC 9314, ANSI X3.x)

2.1.2 WAN (Wide Area Network)

Rozlehlé sítě umožňují komunikaci na velké vzdálenosti. Bývají obvykle veřejné, ale existují i soukromé WAN sítě. Typicky pracují prostřednictvím komunikace se spojením, které nepoužívají sdílený přenosový prostředek. Přenosové rychlosti se velmi liší podle typu sítě. Začínají na desítkách Kbit/s, ale dosahují i rychlostí řádu Gbit/s. Příkladem takové sítě může být Internet [1].

Mezi sítě WAN patří

- Integrated Services Digital Network (ISDN)
- X.25
- Frame Relay
- Switched Multimegabit Data Service (SMDS)
- Asynchronous Transfer Mode (ATM)
- WiMAX (IEEE 802.16d)

2.1.3 MAN (Metropolitan Area Network)

Metropolitní sítě umožňují rozšíření působnosti lokálních sítí jejich prodloužením, zvýšením počtu připojených stanic a zvýšením rychlosti. Rychlost MAN sítí bývá vysoká a svým charakterem se řadí k sítím LAN. Sítě mohou být jak soukromé, tak veřejné, které provozovatel pronajímá různým uživatelům [1].

Mezi sítě MAN patří

- protokol Distributed Queue Dual Bus (DQDB) (IEEE 802.6)

2.1.4 PAN (Personal Area Network)

PAN je počítačová síť tvořená komunikujícími zařízeními jako mobilní telefon, PDA, laptop, které jsou v blízkosti jedné osoby. Dosah takové osobní sítě je většinou jen několik metrů. Používá se ke komunikaci mezi samotnými zařízeními nebo k připojení k okolním sítím nebo k internetu [1].

Mezi sítě PAN patří

- Bluetooth
- ZigBee
- IrDA

2.1.5 Sítě typu Klient – server

Server poskytuje služby stanicím – klientům. Serverů může být více typů podle poskytovaných služeb (souborový server, tiskový server, poštovní server, www server, ftp server atd.) [1].

2.1.6 Sítě typu Peer to peer

Peer-to-peer (doslova rovný s rovným), P2P nebo klient-klient je označení architektury počítačových sítí ve které spolu komunikují přímo jednotliví klienti. Všechny uzly sítě jsou si rovnocenné a působí současně jako klienti i servery pro jiné klienty [1].

Obr. 1: síť typu klient-server

Obr. 2: síť typu peer-to-peer

2.2 Bezdrátová síťová komunikace

Bezdrátová komunikace spočívá ve spojení dvou a více subjektů jiným způsobem, než mechanicky (kabelem). Existuje více přenosových technik v zásadě však lze říci, že v praxi se uplatnily pouze dva způsoby bezdrátové komunikace a to optická (infračervené záření, laser) a pomocí rádiových vln. V následujícím přehledu jsou tyto metody popsány blíže.

2.2.1 Přehled přenosových technik

Infračervené záření

IrDA (Infrared Data Association) je organizace definující standardy komunikačních protokolů pro infračervená záření. Tato technologie byla vytvořena pro snadnou komunikaci mobilních zařízení na krátkou vzdálenost řadově cm, mezi kterými musí být přímá viditelnost [1].

Laser

Pro komunikaci pomocí laseru se využívají dvojsměrné teleskopy s rychlými optickými transceivery, které pracují až s přenosy do 2,5 Gbit/s. Stejně jako u předchozí technologie i zde je potřeba přímé viditelnosti mezi optickými jednotkami. Použitelná vzdálenost se počítá v řádech jednotek km.

Rádiové frekvence

Technologie přenosu pomocí rádiových vln patří mezi nejrozšířenější způsoby. U této technologie není dán požadavek na přímou viditelnost a komunikace může probíhat na velké vzdálenosti.

2.2.2 Přehled bezdrátové rádiové technologie

Dostupné rádiové frekvence

Bezdrátové sítě využívající přenos po rádiových vlnách pracují ve stanovených frekvencích. Používání radiofrekvenčních pásem podléhá regulaci, v České republice toto reguluje ČTÚ (Český telekomunikační úřad). Bezdrátové sítě pracují v bezlicenčních pásmech, která jsou uvolněná pro komerční použití, a proto na jejich provoz není potřeba licence. V případě bezdrátových sítích jsou to frekvence:

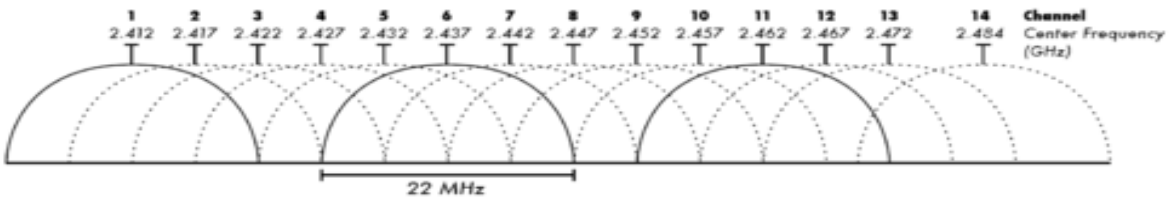
- 2.4 GHz v pásmu 2,412-2,484 GHz
- 5 GHz v pásmu 5,15-5,825 GHz

Bezlicenční pásmo 2,4 GHz se dělí na 14 kanálů s odstupem 5 MHz a šířkou 22 MHz od frekvence 2,412 po 2,484 GHz. S maximálním vyzářeným výkonem 100 mW. V některých zemích však určité kanály nejsou k dispozici, zaleží na místních podmínkách a hospodaření s kmitočtovým pásmem, taktéž každá země definuje regulaci vysílacích výkonů záření v každém frekvenčním rozsahu [1]. Přehled použitelných kanálů je uveden v tabulce.

Tab. 1: Seznam použitelných kanálů

Kanál č.	Rozsah frekvencí	USA	Evropa	Japonsko
1	2401-2423	x	x	x
2	2406-2428	x	x	x
3	2411-2433	x	x	x
4	2416-2438	x	x	x
5	2421-2443	x	x	x
6	2426-2448	x	x	x
7	2431-2453	x	x	x
8	2436-2458	x	x	x
9	2441-2463	x	x	x
10	2446-2468	x	x	x
11	2451-2473	x	x	x
12	2456-2478	-	x	x
13	2461-2483	-	x	x
14	2466-2488	-	-	x

Z tabulky je vidět, že Evropa se řídí konvencí ETSI a má tedy k dispozici 13 kanálů, avšak jelikož technologie rozprostřeného spektra (DSSS) používá vysílání v rozsahu 22 MHz pouze tři kanály se nepřekrývají. Aby mezi kanály nedocházelo k rušení a interferenci musí být nastaveny 5 kanálů od sebe [2].



Obr. 3:Rozdělení kanálů

Pásmo 5 GHz se dělí na tři frekvenční subpásma:

- "nízké" (5.15 - 5.25 GHz) max. výkon 200 mW, určené pouze pro vysílání uvnitř budov.
- "střední" (5.25 - 5.35 GHz) max. výkon 200 mW, určené pouze pro vysílání uvnitř budov.
- "vysoké" (5.725 - 5.825 GHz)max. výkon 1 W. Pouze venkovní použití s použitím regulace výkonu.

Ale stejně tak jako v pásmu 2,4 GHz ani v pásmu 5 GHz nejsou k dispozici všechny kanály a záleží na konkrétních licenčních podmínkách v dané zemi. Pro Evropu platí konvence ETSI, která určuje pásmo od 5.470 GHz po 5.725 GHz, kde se nachází 11 nepřekrývajících se kanálů [3].

2.2.3 Rozprostřené spektrum

Technologie rozprostřeného spektra se používá pro dosažení rychlých datových přenosů v pásmu ISM. Tradiční rádiové technologie se soustředí na vměstnání co největšího počtu signálů do relativně úzkého pásma. Rozprostřené spektrum oproti tomu používá matematické funkce pro rozptýlení síly signálu do širokého frekvenčního bloku. Používaní rozprostřeného spektra ovšem nepřináší žádnou zvláštní odolnost proti zarušení. Systémy s rozprostřeným spektrem mohou být rušeny dalšími podobnými systémy, ale i interferencemi a také provozem klasických vysílačů pracujících s úzkým rádiovým pásmem. Aby se tedy alespoň z části předešlo problémům s rušením, předepisují regulační orgány omezení týkající se maximálního vyzářeného výkonu [2].

Typy rozprostřeného spektra

DSSS (Direct Sequence Spread Spectrum)

Technika přímo rozprostřeného spektra předpokládá, že každý jednotlivý bit určený k přenosu je nejprve nahrazen určitou sekvencí bitů a namodulováním na nosný signál je pak přenášena až tato sekvence bitů. Například standard 802.11 pro přenosové rychlosti 1 Mbps a 2 Mbps počítá s tím, že každý bit je nahrazen 11-bitovou sekvencí bitů (tzv. Barkerovým kódem), označovanou také jako tzv. chip. Jde tedy vlastně o umělé zavedení redundance (nadbytečnosti) podobné tomu, které se při datových přenos někdy používá pro zajištění větší spolehlivosti přenosů (jde o tzv. samoopravné kódy umožňující příjemci opravit část eventuelních chyb při přenosech). Zde je ale důvod pro zavedení takovéto redundance jiný - signál je zde rozprostřen do větší části spektra, je méně citlivý vůči rušení [3].

FHSS (Frequency Hopping Spread Spectrum)

Podstata systému FHSS spočívá v tom, že vstupní datová posloupnost je vysílána na několika frekvencích. Tyto frekvence jsou měněny podle pseudonáhodné posloupnosti, která musí být známa jak na vysílací straně, tak i na přijímací a v obou zařízeních musí být tato posloupnost synchronizována. Velká výhoda systémů, které pracují podle FHSS je, že jsou odolné vůči rušení. Nevýhodou pak, že tyto systémy dosahují malých přenosových rychlostí [4].

OFDM (Orthogonal Frequency Division Multiplexing)

Systémy s ortogonálním frekvenčním multiplexem rozdělí přenosové pásmo na velké množství úzkých kanálů, data se v každém kanálu přenášejí relativně pomalu a signál je tak mnohem robustnější. Ve výsledku je ale rychlost přenosu dána součtem všech kanálů [2].

MIMO (Multiple Input, Multiple Output)
Technologie Mimo funguje na principu vysílání několika datovými cestami najednou (použití více antén). Technologie MIMO vyniká vysokou přenosovou rychlostí a vzdáleností přenosu.

2.3 Model OSI pro 802.11

OSI (Open System Interconnection) je sedmivrstvý model, který popisuje strukturu sítě a průběh komunikace od nejnižší vrstvy (fyzická vrstva) po nejvyšší (aplikační vrstva). Model OSI je hierarchický. Základní síťové funkce, jako jsou stanovení přenosového média či dekódování rádiových signálů, probíhá na nižších vrstvách. Vyšší vrstvy řídí způsob předávání transakcí a definují pravidla pro konkrétní síťové aplikace. Ne všechny normy, či protokoly musejí využít všech vrstev OSI [5].

Vrstvy OSI

1. Fyzická vrstva (physical layer) – komunikace na nejnižší hardwarové úrovni
2. Spojová vrstva (data-link layer) – kódování a přenos informací
3. Síťová vrstva (network layer) – obsluha přenosových tras a zpráv
4. Transportní vrstva (transport layer) – řízení doručování informací a kvality přenosu
5. Relační vrstva (session layer) – udržování a koordinace komunikace
6. Prezentační vrstva (presentation layer) – formátování, konverze a zobrazování přenesených dat
7. Aplikační vrstva (application layer) – přenos informací mezi programy

Standard 802.11 definuje jako vlastní pouze dvě nejnižší vrstvy OSI, tedy fyzickou a spojovou vrstvu. Všechny ostatní nechává nedotčené [2].

Spojová vrstva	LLC					
	IEEE 802.11 MAC					
Fyzická vrstva	IEEE 802.11 IR	IEEE 802.11 DSSS	IEEE 802.11 FHSS	IEEE 802.11a OFDM	IEEE 802.11b HR-DSSS	IEEE 802.11g OFDM

Obr. 4: Referenční model ISO/OSI pro WiFi

2.3.1 Fyzická vrstva

Fyzická vrstva je nejnižší vrstvou v referenčním modelu OSI. Realizuje samotné vysílání a příjem dat bezdrátovým prostředím. V případě standardů 802.11 jsou na fyzické vrstvě definovány přenosové mechanismy DSSS, FHSS, OFDM [4].

Struktura vrstvy v modelu 802.11 je rozdělena do dvou podvrstev:

- **PLCP** (Physical Layer Convergence Procedure) – v této podvrstvě se k datovým rámcům MAC (Medium Access Control) podvrstvy přikládají informace o použitém přenosovém mechanismu a modulaci. Díky této podvrstvě je přenášený datový rámec nezávislý na typu fyzické vrstvy. Do této podvrstvy je implementována rovněž funkce CCA (Clear Channel Assessment), která poskytuje odezvu pro MAC vrstvu o připravenosti přenosového média [4].
- **PMD** (Physical Medium Dependent) – tato podvrstva je zodpovědná za přenos dat mezi jednotlivými vysílači a přijímači. Z podvrstvy PLCP jsou data v závislosti na použitém přenosovém mechanismu ve vysílači vysílána do bezdrátového prostředí, kde jsou na straně přijímače pomocí PMD přijímána a předávána podvrstvě PLCP [4].

2.3.2 Spojová vrstva

Důležitou vrstvou bezdrátové sítě 802.11 je podvrstva spojové vrstvy MAC (Medium Access Control) nebo také vrstva řízení přístupu k médiu. MAC podvrstva slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením [2].

Pro robustnost podvrstvy MAC jsou důležité dvě hlavní vlastnosti.

- CRC (Cyclic Redundancy Check) – cyklický kontrolní součet
- Fragmentace paketů

Každý přenášený paket je opatřen kontrolním součtem CRC (Cyclic Redundancy Check), díky tomu je možné poznat zda (ne)byl během přenosu poškozen. Další vlastností je fragmentace paketů, která rozděluje přenášené pakety do menších celků a přenáší je postupně. Tím se šetří čas v případě, že by bylo nutné paket přenést znovu. Navíc pravděpodobnost poškození paketu narůstá s jeho velikostí [2].

Formát MAC rámce

Rámec má dvě hlavní části a to hlavičku sestávající se z informací o přenášených datech a tělo rámce obsahujícího samotná data a kontrolní součet.

Rámec obsahuje:

- Frame Control (FC) - informace o verzi protokolu a typu rámce.
- Duration/ID(ID) - délka trvání rámce pro výpočet rezervace přenosového média.
- Address field - jsou 4 adresní pole obsahující adresy zdroje, cíle, přenašeče a příjmače.
- Sequence Control- se používá pro odstranění duplicitních rámců.

FC 2 bajty	ID 2bajty	ADD1 6 bajtů	ADD2 6 bajtů	ADD3 6 bajtů	SC 2 bajty	ADD4 6 bajtů	DATA 0-2312 bajtů	CRC 4 bajty

2.4 Přístupové metody

2.4.1 CSDMA/CA

Protokol CSDMA/CA (Collision Avoidance – Předcházení kolizí) používá mechanismus předcházení kolizím s potvrzením. Stanice naslouchá, jestli je médium volné, pokud ano počká určený čas (DIFS - Distributed Inter Frame Space) a pak začne vysílat. Poté přijící stanice zkontroluje CRC (Cyclic redundancy check) přijatého paketu a odešle potvrzení ACK, to značí přijetí paketu. Pokud stanice paket ACK nedostane vysílání se opakuje, dokud nevyčerpá určitý počet pokusů [2].

2.4.2 RTS/CTS

Metoda RTS/CTS (Request to Send / Clear to Send) je mechanismus, který slouží jako ochrana před problémem skrytého uzlu. Stanice, která chce vysílat nejdříve pošle řídící paket RTS (Ready to send), ten obsahuje adresu příjemce, cíle a dobu po kterou bude vysílat. Cílová stanice odpoví řídícím paketem CTS (Clear to send), který rovněž obsahuje dobu přenosu. Na základě těchto řídících paketů si jednotlivé stanice nastaví NAV (Network allocation vector) indikátor virtuálního nastavení. Po tuto dobu bude stanice brát médium jako obsazené. Použitím tohoto mechanismu se riziko kolize velice snižuje, avšak implementace tohoto mechanismu je nepovinná [2].

2.5 Stavba bezdrátové sítě

2.5.1 Komponenty sítě

Standard 802.11 obsahuje čtyři hlavní druhy fyzických komponent.

- Distribuční systém
- Přístupový bod (Access point)
- Bezdrátové médium
- Stanice, klient

Obr. 5: Komponenty sítě

Distribuční systém

Pokud je v síti více přístupových bodů, komunikují spolu právě přes distribuční systém. Distribuční systém je logická komponenta, která směruje data na určitou stanici. Většinou je systém řešen jako síťový most (bridge) s distribučním médiem, kterým jsou informace přenášeny. Médium je většinou ethernetový kabel [2].

Přístupový bod

Představuje přemostění mezi kabelovou a bezdrátovou sítí dále nabízí další funkce jako je routování, směrování portů a v neposlední řadě také zabezpečení bezdrátové sítě [2]. Bližší popis je uveden v kapitole 3.

Bezdrátové médium

Je nosičem dat mezi stanicemi. Bezdrátovým médiem normy 802.11se rozumí dvě rádiové frekvence (2,4 a 5 GHz) a málo využívanou infračervenou fyzickou vrstvu [2].

Stanice

Stanicí se rozumí obecně jakékoliv zařízení v síti (počítač, notebook, pda) [2].

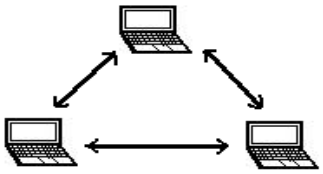
2.5.2 Topologie bezdrátové sítě

Základním stavebním blokem 802.11 sítě se označuje jako Basic Service Set (BSS), jedná se o základní soubor služeb. Je tvořen skupinou stanic, které spolu navzájem komunikují. Stanice jsou omezeny průnikem dosahů svých vysilačů a takové území se nazývá Basic Service Area (BSA). Pokud se stanice nachází v rámci pokrytí BSA, je schopna komunikovat s dalšími stanicemi.

Existují dva hlavní typy sítí podle toho, jak probíhá komunikace v rámci BSA.

Ad-hoc

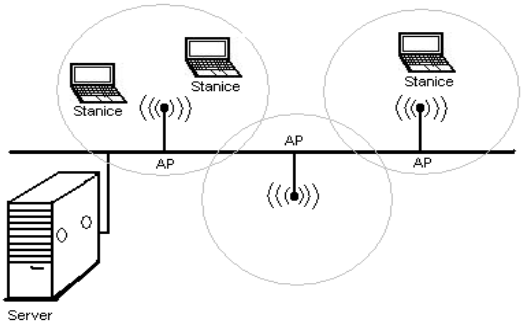
V sítích Ad-hoc spolu stanice komunikují přímo, nezávisle na prostředníkovi. Stanice musí být ve vzájemném rádiovém dosahu. Z tohoto důvodu nejsou sítě ad-hoc vhodné pro rozsáhlejší prostory a členitější sítě slouží pro spojení několika stanic vzdálených pár metrů na krátký čas [2].



Obr. 6: Ad-hoc síť

Infrastrukturní sítě

Přístupový bod je schopen komunikovat i s více než jednou stanicí. Proto spolu mohou komunikovat stanice i mezi sebou, právě díky propojení přes přístupový bod. V tomto případě je rozdíl od ad-hoc sítě takový, že data putují dvěma skoky. Nejdříve na přístupový bod a pak z něj [2].



Obr. 7: Infrastrukturní síť

V infrastrukturní síti může tedy fungovat každá stanice, která je v oblasti pokrytí a je schopna komunikovat s přístupovým bodem. Tato síť má sice větší nároky na spojovací kapacitu (větší počet skoků), ale ad-hoc má zase větší nároky na klientskou stanici a musí neustále udržovat spojení s každou stanicí, s níž právě komunikuje. V infrastrukturní síti stačí udržovat pouze jedno spojení a přístupový bod může ukládat data pro stanici, která přešla do úsporného režimu [2].

2.6 STANDARD 802.11

802.11 je standard s dalšími doplňky pro lokální bezdrátové sítě (*Wireless LAN*, WLAN) vyvíjený 11. pracovní skupinou IEEE od roku 1990. Jejím úkolem bylo vypracovat bezdrátovou alternativu k drátovému ethernetu, která by pracovala v bezlicenčním pásmu ISM. Vývoj standardu trval celých 7 let a teprve v roce 1997 přišel první standard 802.11, který měl však oproti ethernetu velmi omezenou přenosovou rychlost 1 až 2 Mbit/s, proto se dále pracovalo na zdokonalení standardu, které by přineslo zvětšení přenosové rychlosti. To přišlo o dva roky později v podobě standardů 802.11a a 802.11b [4].

2.6.1 Přehled základních standardů 802.11

IEEE 802.11b

Doplněk IEEE 802.11b vznikl v roce 1999 a poskytuje vyšší přenosové rychlosti v pásmu 2,4 GHz, a to až 11 Mbit/s. Pro jejich dosažení využívá nový způsob kódování, tzv. doplňkové kódové klíčování (CCK) s použitím DSSS na fyzické vrstvě. Doplněk specifikuje, že podle momentálního rušení prostředí se dynamicky mění rychlost: 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s či 1 Mbit/s [4].

IEEE 802.11g

Doplněk IEEE 802.11g je obdobou IEEE 802.11a s tím rozdílem, že je specifikován pro pásmo 2,4 GHz, stejně jako IEEE 802.11b. Pro dosažení vyšší rychlosti až do 54 Mbit/s se používá na fyzické vrstvě OFDM a navíc se používá DSSS pro zpětnou kompatibilitu s IEEE 802.11b. Doplněk byl schválen v roce 2003 [4].

IEEE 802.11a

Doplněk IEEE 802.11a byl schválen v roce 1999, a na rozdíl od IEEE 802.11b pracuje v pásmu 5 GHz s výrazně vyšší přenosovou rychlostí - 54 Mbit/s. Pro její dosažení se poprvé v paketových komunikacích používá OFDM. Výhoda IEEE 802.11a oproti původnímu standardu není pouze ve vyšší rychlosti, ale také v použitém kmitočtu, protože kmitočtové pásmo 5 GHz je méně vytížené než pásmo 2,4 GHz a poskytuje více kanálů pro komunikaci [4].

IEEE 802.11n

IEEE 802.11n je standard, který si klade za cíl upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou *Media Access Control* (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s. Maximální fyzická (L1) rychlost může být až 600 Mbit/s při MAC (L2) rychlosti až 400Mbit, to v konfiguraci 4X4 MIMO. V roce 2008 se masověji prodávají zařízení 802.11n Draft 2.0, typicky s konfigurací 2X2 nebo max. 3X3 MIMO. Reálná přenosová rychlost (L4) zatím do 200Mbit/s [1].

Tab. 2: Přehled norem 802.11

standard	Rok vydání	Pásmo [GHz]	Max. rychlost [Mbit/s]	Reálná rychlost [Mbit/s]	modulace
IEEE 802.11	1997	2,4	2	1	DSSS a FHSS
IEEE 802.11a	1999	5	54	30	OFDM
IEEE 802.11b	1999	2,4	11	6	DSSS
IEEE 802.11g	2003	2,4	54	20	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	70	MIMO

2.6.2 Přehled doplňujících standardů 802.11

IEEE 802.11c

Tento doplněk řeší práci komunikačních mostů v rámci podvrstvy MAC a doplňuje mezinárodní normu IS 10038 (IEEE 802.1d) o transparentních mostech. Doplněk byl schválen v roce 1998 [4].

IEEE 802.11h

Připravovaný doplněk IEEE 802.11h vylepšuje řízení využití kmitočtového spektra (výběr kanálu a řízení vysílacího výkonu) a doplňuje 802.11a. Evropští regulátoři požadují pro schválení produktů 802.11a použití dynamického výběru kanálu (Dynamic Channel Selection, pro venkovní i vnitřní komunikaci) a řízení vysílacího výkonu (Transmit Power Control) u zařízení pracujících na kmitočtu 5 GHz. IEEE 802.11h má právě tyto možnosti doplnit do normy 802.11a. Tyto doplňky se budou tedy týkat pouze pásma 5 GHz, nikoli 2,4 GHz [4].

IEEE 802.11e

Doplňuje podporu pro kvalitu služeb QoS pro zajištění přenosu hovorového signálu, obrazu apod. IEEE 802.11e doplňuje sítě definované IEEE 802.11a/b/g a nahrazuje stávající metody pro přístup k médiu. Doplněk navíc zajišťuje zpětnou kompatibilitu se zařízeními, které nejsou podporou pro QoS vybaveny [4].

IEEE 802.11f

Doplněk IEEE 802.11f vylepšuje mechanismus předávání stanic (*Roaming*) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu. Protokol IAPP (*Inter-Access Point Protocol*) umožňuje spolupráci přístupových bodů od různých výrobců. Doplněk byl schválen v roce 2003 [4].

IEEE 802.11i

Doplňuje lepší zabezpečení IEEE 802.11 sítí. Místo WEP (Wired Equivalent Privacy) používá nový způsob šifrování AES (Advanced Encryption Standard). Doplněk byl schválen v roce 2004 [4].

2.6.3 WiFi

WiFi(Wireless Fidelity) je globální nezisková průmyslová asociace, zabývající se kompatibilitou produktů použitých pro bezdrátovou komunikaci na standardu 802.11 a sdružuje více jak 300 výrobců a vývojářů WiFi technologií. WiFi Alliance testuje výrobky a těm, které splňují dané požadavky, dává certifikaci a svolení k používání loga na jejich zařízeních a propagačních materiálech.

To tedy znamená, že právo honosit se označením WiFi (resp. Wi-Fi Certified) nemají automaticky všechny produkty, které vychází ze standardů IEEE 802.11. Jsou to jen ty, které jejich výrobci přihlásí do příslušného testování a tím úspěšně projdou. Spolu se získáním příslušného loga pak jsou takovéto produkty také zařazeny do oficiální databáze WiFi produktů, kde si je může kdokoli vyhledat (i po internetu, na adrese http://www.wi-fi.org/) a přesvědčit se, zda se eventuelně nějaký produkt neohání označením WiFi, aniž by na to měl právo [3].

Obr. 8: Logo WiFi

3 Hardware pro bezdrátové sítě

3.1 Přístupový bod (Access point)

Přístupový bod slouží pro směrování provozu mezi jednotlivými bezdrátovými klienty a kabelovými sítěmi. Přístupový bod je obvykle realizován malým jednoúčelovým zařízením, ale s potřebnou softwarovou výbavou se jím může stát i jakýkoliv počítač s bezdrátovým WiFi zařízením. Některá z těchto jednoúčelových zařízení využívají jako základ operační systém Linux [5].

Obr. 9: Access Point

3.1.1 Součásti přístupového bodu

Radiostanice

Každý přístupový bod obsahuje radiostanici, která určuje, kterou normu 802.11 zařízení podporuje. Tato radiostanice zpravidla bývá pevnou součástí přístupového bodu, někteří výrobci však umožňují radiostanici vyměnit nebo rozšířit přístupový bod o další radiostanice díky přídavnému slotu miniPCI [5].

Komunikační porty

Přístupový bod obsahuje několik ethernetových portů pro připojení ke kabelové síti. Port, který slouží k připojení konektivity nebo k přístupu do sítě se nazývá WAN, pro přístup do lokální sítě slouží porty označené jako LAN [5].

Antény

Součástí přístupového bodu je jedna nebo několik antén, tyto antény jsou zpravidla externí a lze je vyměnit za jiné (silnější). Připojením externí antény lze zvětšit dosah sítě až v extrémních případech až na několik km [5].

2.1.2 Role přístupového bodu

Přístupové body vystupují v několika různých rolích, které jsou dány nejen požadavky na strukturu sítě, ale i schopnostmi těchto zařízení. I když jsou schopnosti bezdrátových zařízení snadno rozšiřitelné pomocí změny softwarového vybavení, většina výrobců ji neumožňuje. Naopak hardwarově identická zařízení se mohou cenově několikanásobně lišit jen díky existenci jednoduchého softwarového doplňku [1].

bridge – bezdrátová síť je součástí sítě LAN

- bridge odděluje síťový provoz, ale propouští lokální broadcasty
- není nutné konfigurovat

router – bezdrátová síť je samostatnou podsítí

- router odděluje síťový provoz a nepropouští lokální broadcasty
- vyžaduje konfiguraci IP adres zařízení a nastavení směrování

3.1.3 Režimy přístupového bodu

Access Point

jedná se o základní režim, který umožňuje bezdrátovou komunikaci mezi bezdrátovým klientem a Access Pointem. Uživatelé (klienti) se do bezdrátové sítě připojují v režimu infrastruktury.

Wireless klient

Access point se chová jako klient a připojuje se na jiné AP.

Wireless bridge

jedná se o režim pro vytváření přímých spojů (bezdrátových mostů).

Repeter

režim používaný pro rozšíření bezdrátové sítě. Zařízení přijímá požadovaný tok dat a odesílá jej dál.

3.1.4 Funkce přístupového bodu

- Administrace přístupu
- Firewall
- Šifrování WEP/WPA/WPA2
- DHCP/NAT
- Překlad portů

Bližší popis jednotlivých funkcí je popsán v kapitole 4 (správa sítě) a 5 (bezpečnost sítě).

3.2 Bezdrátový síťový adaptér (Klient)

Slouží k připojení do bezdrátové sítě.

3.2.1 Druhy síťových adaptérů

Síťové adaptéry dělíme podle několika kritérií, první z nich je způsob připojení k PC (USB, PCI, PCMCIA), dále pak dle podpory jednotlivých standardů 802.11abgn.

Obr. 10: Druhy bezdrátových klientů

3.3 Antény

Základní funkcí antény je zvýšení dosahu signálu. Prvky WiFi jsou navrženy tak, aby se anténa dala vyměnit a použít tak anténu podle konkrétní aplikace, a tím zvýšit dosah sítě až na několik kilometrů [5].

3.3.1 Vlastnosti antén

Šířka frekvenčního pásma (bandwidth) – určuje pracovní frekvenci antény.

Zisk (gain) – Popisuje stupeň směrovosti antény. Zisk se měří v dBi a jedná se poměr výkonu antény vůči anténě izotropní. Taktéž se používá dBm, což je poměrná jednotka vztažena k jednomu miliwattu [5].

Úhel vyzařování (beam width) – úhel vyzařování se vyjadřuje ve stupních a určuje oblast kde je signál maximální [5].

Polarizace (polarization) – polarizace antény může být buď vertikální, nebo horizontální. Polarizace antén na každém konci musí být stejná. Jinak dochází vytváření signálového šumu a ztrátám anténního zisku [5].

3.3.2 Typy antén

Výběr antény závisí vždy na jejím použití. Od malých antén pro vnitřní použití pro pokrytí v okruhu desítek metrů, až po antény větších rozměrů k venkovnímu použití a na velké vzdálenosti.

Všesměrové antény

Vyzařují signál do všech směrů stejně. Pokrývají tedy velkou oblast a jsou vhodné pro plošné pokrytí signálem. Většinou jsou trubicového tvaru a umísťují se vertikálně. Nevýhodou je pak poměrně malý zisk.

Sektorové antény

Směrové antény vyzařují signál do jednoho směru, z pravidla úhel vyzařování nepřekračuje 180 stupňů a jsou tedy vhodné k pokrytí určité konkrétní oblasti. Dosahují taktéž většího zisku než antény všesměrové [5].

Yagi antény

Yagi antény jsou primárně určeny na delší spoje řádově km při spojení bod-bod. Vyzařovací úhel se pohybuje od 15 do 60 stupňů. Ziskovost yagi antén je vysoká [5].

Panelové antény

Panelové antény se řadí mezi směrové a vyzařovací úhel u těchto antén dosahuje až 90 stupňů.

Parabolické antény

Parabolické mohou být tvořeny mřížkou nebo pevnou konstrukcí, vyznačují se velmi vysokým ziskem a vysokou směrovostí, proto se používají pro dálkové spoje typu bod-bod [5].

Obr. 11: Druhy antén

3.4 Konektory a kabely

Kabely jsou v bezdrátových sítí použity k propojení antény s přístupovým bodem. Používají se koaxiální kabely určené pro práci v pásmu GHz. Na výběru kabelu závisí, protože při použití nevhodného kabelu dochází k velkému útlumu signálu. Čím delší kabel použijeme, tím je útlum větší, proto se koaxiální kabely vedou co možná nejkratší cestou bez velkých ohybů [5].

Podobně jako kabely tak i konektory představují ztrátu signálu. Používají se konektory typu SMA TNC a N. Typ konektoru musí také odpovídat konektoru dané antény a mít opačnou polaritu [5].

4 Správa sítě

4.1 Konfigurace přístupového bodu

Přístupový bod umožňuje správu a konfiguraci sítě pomocí jeho konfiguračního softwaru.

4.1.1 Možnosti konfigurace přístupového bodu

Klientský software
Jedná se o aplikace zpravidla určené pro platformu Windows, které nastavení provedou přes průvodce.

SNMP (Simple Network Management Protocol)

Webové rozhraní
Patří mezi nejrozšířenější způsoby konfigurace přístupových bodů. Konfigurace probíhá přes webové rozhraní implementované v přístupovém bodě.

Telnet

Používá se pro dálkovou správu.

4.1.2 Přístup k internetu

Hlavní funkcí přístupového bodu je sdílení dat a přístupu na internet. Pro přístup do sítě je nutná autorizace a konfigurace a existuje několik možností:

- Automatické získání IP adresy (DHCP klient) - přístupový bod si vyžádá IP adresu od nadřazeného serveru.
- Statická IP Adresa – IP adresy se zadají do přístupového bodu ručně, adresy přidělí poskytovatel
- PPPoE (Point-to-Point Protocol over Ethernet – používá se pro vytáčené spojení údaje nám poskytne poskytovatel.

4.1.3 Veřejné a privátní IP adresy

IP adresa slouží k jednoznačné identifikaci počítače v síti. Veřejné adresy přiděluje ISP (poskytovatel) a slouží pro identifikaci na internetu je tedy viditelná pro všechny (vnější síť). Oproti tomu privátní adresy se používají k identifikaci počítače v lokální síti (vnitřní síť) a nejsou z internetu viditelné. Privátní adresy se začali používat z důvodu nedostatku adres veřejných a nejčastěji tedy síť funguje tak, že za jednu adresu veřejnou se schová lokální síť. K tomuto účelu slouží funkce NAT. Přístupový bod tak předává internetové pakety počítačům na lokální síti. Všechny počítače jsou pak připojeny přes jednu veřejnou IP adresu [5].

4.2 Služby a funkce přístupového bodu

4.2.1 DHCP server

DHCP protokol umožňuje prostřednictvím jediného DHCP serveru nastavit všem stanicím sadu parametrů nutných pro komunikaci v sítích používajících rodinu protokolů TCP/IP včetně parametrů doplňujících a uživatelsky definovaných. Významným způsobem tak zjednodušuje a centralizuje správu počítačové sítě [1].

4.2.2 NAT

Překlad síťových adres je funkce, která umožňuje překládání adres. Což znamená, že adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě (např. Internetu), adresu překládanou si uloží do tabulky pod náhodným portem, při odpovědi si v tabulce vyhledá port a pošle pakety na IP adresu přiřazenou k danému portu[1].

4.2.3 Firewall

Firewall chrání počítač před vnějším napadením a nežádoucím průnikům do sítě z internetu. Tuto činnost vykonává blokováním prostředků, které využívají specifické internetové a síťové aplikace [5].

4.2.4 Přesměrování portů

Přesměrování portů (Port forwarding) představuje možnost jak na vnitřní síti provozovat služby dostupné z internetu. Přesměrování portů umožní vybrat jeden nebo více počítačů a jeden nebo více specifických portů, které budou k dispozici pro vnější síť (internet), zatímco zbývající část vnitřní sítě zůstane chráněna[5].

4.2.5 Filtrování

Řada přístupových bodů nabízí možnost filtrování služeb a přístupu na internet. Filtry slouží k blokování určitých serverů, omezení přístupu na základě klíčových slov nebo zdrojové domény, omezit přístup na internet v určitých hodinách a také na určité porty [5].

4.2.6 VPN (Virtual Private Network)

VPN umožňuje počítačům připojeným k internetu bezpečně přistupovat k prostředkům privátní (vnitřní) sítě. K privátní síti přistupují počítače prostřednictvím nedůvěryhodné transportní sítě nejčastěji internetu, přičemž dochází k šifrování všech dat přenášených ze vzdáleného počítače na privátní síť [5].

5 Bezpečnost bezdrátových sítí

Bezpečnosti bezdrátových sítí je nutné věnovat velkou pozornost, jelikož jsou daleko zranitelnější než sítě kabelové. Signál se šíří volně vzduchem a není omezen překážkami v podobě zdí nebo plotů. A útočníkovi tak stačí velmi málo, aby mohl síť nabourat. V podstatě jakýkoli bezdrátový klient s vhodným softwarem, který je volně dostupný na internetu, je potencionální zbraň k nabourání bezdrátové sítě. Typy zabezpečení pro bezdrátové sítě se vyvíjeli postupně s tím, jak stoupali technologické možnosti jejich prolomení. Proto s pohledu dnešních možností počítačů a kapacity výpočetního výkonu jsou starší typy zabezpečení nevyhovující, jelikož se dají snadno prolomit. Uživatelé taktéž často doplácejí na svoji neznalost a spustí bezdrátové zařízení bez jakéhokoli zabezpečení a vystavují se tak riziku napadení sítě.

Bezpečnost bezdrátových sítí můžeme rozdělit do dvou hlavních skupin:

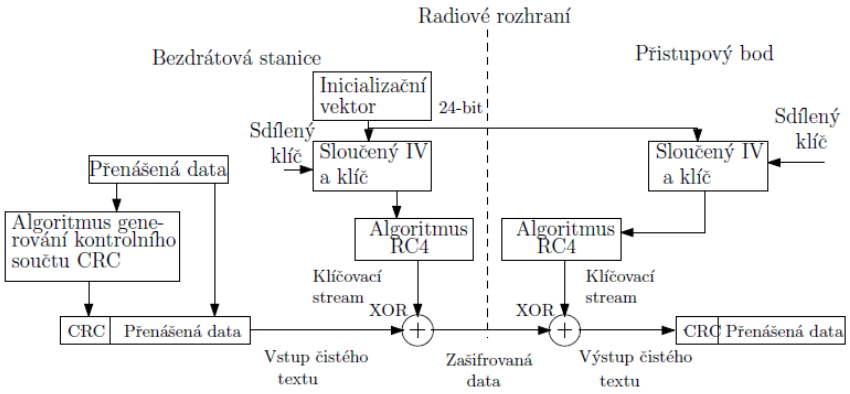
- šifrování - zabezpečení přenášených dat před odposlechem
- autorizace - řízení přístupu oprávněných uživatelů

5.1 Šifrování

5.1.1 WEP (Wired Equivalent Privacy)

WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč. Nejčastější (a nejslabší) 40-bitový klíč pro ověření totožnosti (autentizaci) 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. V závislosti na výrobci může nabízet silnější zabezpečení ve formě 128-bitového šifrování (sdílený klíč má délku 104 bitů, vektor poté 24 bitů).

Bezpečnost sítě s WEP je možno narušit snadno jak mechanicky (krádeží jednoho z koncových zařízení s příslušnou WiFi kartou), tak odposlechem [10].



Obr. 12: algoritmus RC4

5.1.2 WPA (WiFi Protected Access)

WPA je nový bezpečnostní mechanismus ratifikovaný WiFi Aliancí. A vznikl jako reakce na nedostatky zabezpečení pomocí WEP. Obsahuje nástroje šifrování TKIP (Tempoval Key Integrity Protocol) a řízení přístupu (802.1x).

TKIP využívá stejného algoritmu šifrování jako WEP, používá standardně 128 bitový klíč a dočasné dynamické klíče, které pomocí automatického mechanizmu mění každých 10 000 paketů. Dále TKIP obsahuje vylepšenou funkci kontroly integrity MIC (Massage integrity Code) a vylepšená pravidla generování inicializačního vektoru včetně sekvenčních pravidel [2].

WPA představuje řešení všech známých problémů protokolu WEP.

5.1.3 WPA2

V roce 2004 byl schválen dodatek 802.11i , který je známější pod označením WPA2. Zásadní rozdíl od WPA je použití nové blokové šifry AES (Advanced Encryption Standard), na rozdíl od původní RC4. Bloková šifra AES využívá symetrického klíce o délce 128, 192 nebo 256 bitu. Tato metoda šifruje data postupně v blocích s pevnou délkou 128 bitu. Šifra se vyznačuje vysokou rychlostí šifrování [9].

5.2 Autentizace

Autentizace neboli řízení přístupu do sítě je realizováno jako zabránění nepovolaným osobám vstupu do bezdrátové sítě. Klientské stanice bezdrátové sítě musí zažádat o autentizaci do sítě, zatímco síť se vůči stanicím autentizovat nemusí. Z tohoto pohledu má přístupový bod privilegované postavení jako součást síťové architektury [2].

802.11 specifikuje dvě metody pro autentizaci:

- Open-system autentizace
- Shared-key autentizace

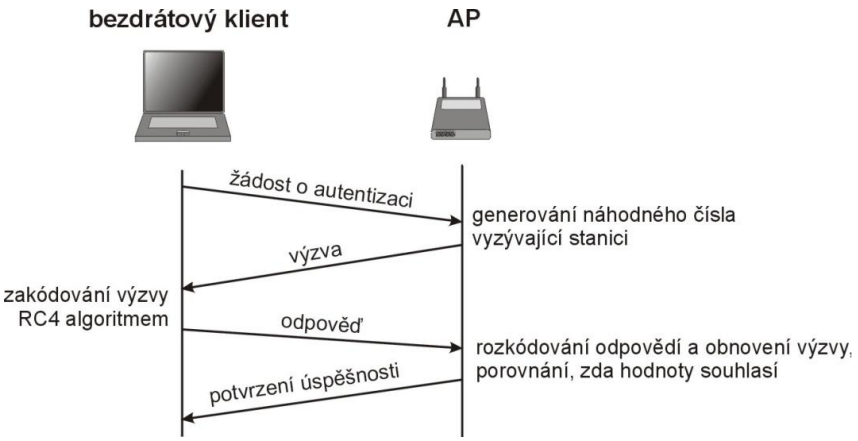
5.2.1 Open-system autentizace

Tato metoda autentizace spočívá v tom, že přístupový bod přijme klientské zařízení na základě údajů, které mu poskytne, aniž by je ověřoval. Klient posílá svojí identifikaci v podobě SSID (Service Set Identifier). U přístupových bodů se doporučuje SSID vypnout, a to z toho důvodu, že přístupový bod, který SSID vysílá, může každá stanice přijmout a použít pro neoprávněný přístup do sítě [2].

5.2.2 Shared-key autentizace

Autentizace se sdíleným klíčem. Princip této autentizace je, že každé zařízení, které chce přistupovat do sítě, se musí prokázat přístupovým klíčem. Přístupový bod ověří platnost tohoto klíče a pak zařízení autentizuje. Ověření probíhá tak, že přístupový bod odešle náhodné číslo, bezdrátový klient toto číslo zakóduje algoritmem RC4 s pomocí přístupového klíče a odešle zpět přístupovému bodu, který je dekóduje. Pokud se dekódované číslo rovná odeslanému číslu, je klient autentizován.

Standard 802.11 vyžaduje, aby každé zařízení s implementovaným WEP zabezpečením bylo také schopno užívat autentizaci se sdíleným klíčem [2].



Obr. 13: Autorizace Sdíleným klíčem (shared-key)

5.2.3 Filtrování adres

Administrátor má možnost v nastavení přístupového bodu určit seznam MAC adres, jimž je zakázán/ povolen přístup do bezdrátové sítě. MAC adresa je unikátní adresa každého síťového zařízení a slouží k jeho jednoznačné identifikaci.

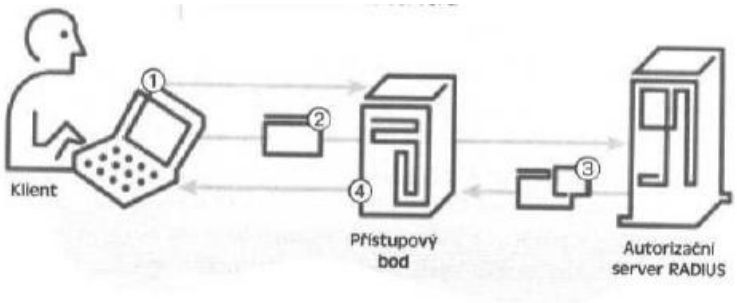
Nevýhodou tohoto řešení je, že MAC adresa je uložena v programové paměti přístroje a lze ji tedy měnit a tím filtrování obejít. Z tohoto důvodu se používá druhá možnost, kdy seznam obsahuje povolené MAC adresy a pro případné útočníky je těžší zjistit povolenou MAC adresu než si náhodně upravit MAC adresu z adres, která má přístup zakázán [2]. Filtrování adres samo osobě není dostačující zabezpečení, a proto je vhodné jej použít s některým způsobem šifrování.

5.2.4 802.1x, EAP (Extensible Authentication Protocol)

IEEE 802.1× (Port-Based Network Access Control, 2001) je obecný bezpečnostní rámec pro všechny typy LAN zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Ověřování se u WLAN realizuje na úrovni portů přístupového bodu WLAN (protokol ale není specifický pro bezdrátové sítě). 802.1× má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele [2].

Je založený na protokolu Extensible Authentication Protocol (EAP, RFC 2284), který byl původně vyvinut pro PPP LCP (Point-to-Point Protocol Link Control Protocol). Jedná se o mechanizmus přenosu EAP paketů prostřednictvím spojové vrstvy LAN (typu 802): zprávy EAP se zapouzdřují do rámců 802.1×. Proto se 802.1× označuje jako EAPOL (Extensible Authentication Protocol over LANs) [2].

Ověřování ve WLAN provádí přístupový bod pro klienty na základě jejich výzvy pomocí seznamu nebo externího autentizačního systému (serveru Kerberos nebo RADIUS, Remote Authentication Dial In User Service). Pouze ověřený uživatel má možnost přístupu k bezdrátové síti[2].



Obr. 14 : Autentizace podle 802.1x

6 Použití konkrétního řešení

Jak již bylo řečeno v úvodu práce hardwarových řešení pro WiFi sítě je nespočet a většina firem má ucelenou řadu modelů pro různé aplikace. Avšak většina komerčně dostupných prvků má omezené možnosti konfigurace, které se soustředí spíše na domácí použití, a proto jsou jejich možnosti nastavení omezeny pro co největší jednoduchost. Proto mi nepřišly vhodné k použití pro ukázkové úlohy, na kterých by si studenti měli ukázat fungování bezdrátových sítí. Hledal jsem řešení, které by mělo ucelené ovládání, a přesto mělo více možností nastavení. Proto jsem vybral řešení, které se v domácím použití často nevyskytuje, přesto je velice používané poskytovateli internetu pro stavbu WiFi sítí v rámci metropolitních sítí. Toto řešení nabízí společnost Mikrotik a jedná se o software RouterOS a hardware Routerboard. Tyto produkty se zaměřují především na možnost vybudování inteligentní lokální sítě, takovéto sítě se vyznačují jednoduchou obsluhou s možností široké nabídky nastavení. Mezi nejpoužívanější funkce se řadí rating, firewalling, omezování rychlosti, bezdrátové spoje, skriptování, tunelování.

6.1 Mikrotik

Společnost byla založena v roce 1995 k vývoji a prodeji bezdrátových systémů zejména pro ISP (poskytovatele internetu). Původně byl tento software vyvíjen pro dřívější Sovětský svaz. Následné zkušenosti s PC přivedly vývojáře k vybudování routovacího software MikroTik v2 PC, který přinesl výraznou stabilitu, ovladatelnost a flexibilitu pro všechny typy komunikačních periférií a kompatibilitu routovacích systémů založených na standardu PC. Nyní poskytuje bezdrátové systémy pro internetovou konektivitu v mnoha zemích po celém světě. Společnost se nachází v Lotyšsku. MikroTik je známý zejména díky svému operačnímu systému MikroTik RouterOS, ale nabízí také jiné produkty a řešení [1].

Sídlo společnosti:	Aizkraukles iela 23, Riga, LV-1006 LATVIA
Web:	www.mikrotik.com
Email:	sales@mikrotik.com

6.2 RouterOS

RouterOS je routerový operační systém založen na bázi Linux OS, vhodný zejména pro bezdrátové spoje a jako bezpečný HW firewall popřípadě router se snadnou GUI konfigurací. Komunikace s tímto OS se v současnosti provádí zejména přes GUI Winbox, ssh, telnet, sériovou konzoli, Mac-telnet (specifický protokol komunikující po 2. síťové vrstvě na správu OS bez zavedení IP adres. Dnes je tento OS zejména uplatňován u kvalitních bezdrátových spojů 802.11a, 802.11b/g a 802.11n [1].

6.2.1 Praktické použití

- Bezpečnostní Firewall (pravidla typu iptables)
- Omezující Firewall (QoS)
- VPN Tunel Server/Klient s podporou protokolů PPP, PPTP, L2TP, OVPN, EoIP, IPs
- WiFi zařízení v režimech AP, Klient, WDS, Nstreeme (Podpora protokolů 802.11abgn)
- Kompletní Hotspotové řešení pro hotely, letiště, kavárny
- Proxy server
- Bridge
- Router s podporou dynamických protokolů (RIP, OSPF, BGP, MME)
- Syslog
- TrafficMonitor Server

6.2.2 Licence

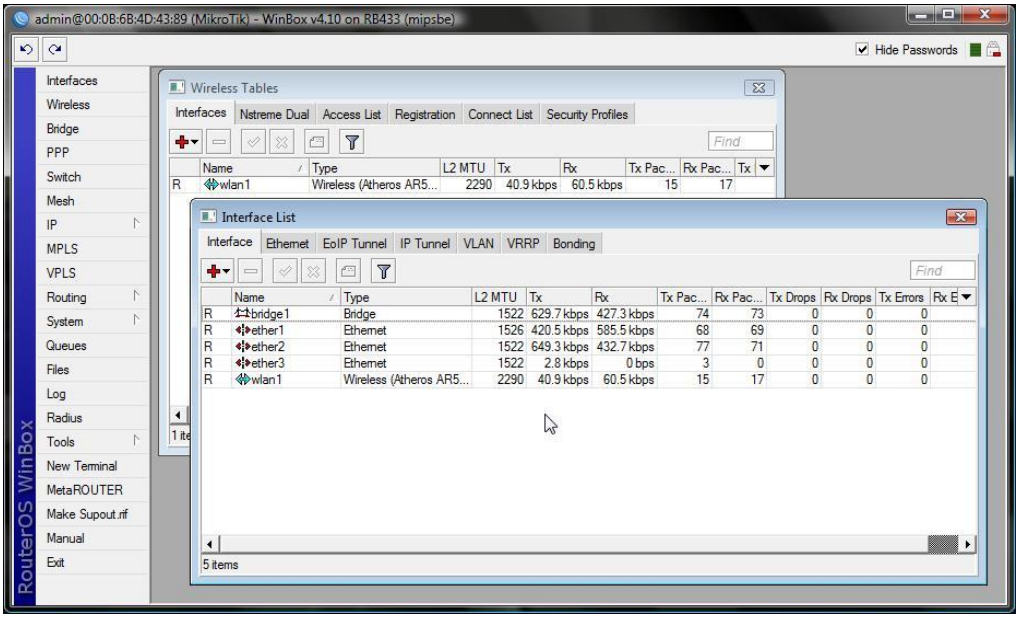
Funkce systému RouterOS jsou omezeny zakoupenou licencí. Poslední tři licence si můžeme zakoupit pro běžný hardware. První tři jsou určené buď k distribuci s různými zařízeními nebo k vyzkoušení. Ceny licencí se pohybují od 560 Kč za L4 po 3000 Kč za licenci L6. Licence jsou časově neomezeny.

Tab. 3: Přehled licencí RouterOS

Vlastnost	**Licence**	L1 (Free)	L2 (Demo)	L3 (WISP CPE)	L4 (WISP)	L5 (WISP)	L6 (Controller)
Aktualizace		Ne	Ne	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Podpora		Ne	Ne	Ne	15 dní	30 dní	30 dní
WiFi AP		24h	Ne	Ne	Ano	Ano	Ano
WiFi klient		24h	Ne	Ano	Ano	Ano	Ano
Směr. protokoly		24h	Ne	Ano	Ano	Ano	Ano

6.2.3 Konfigurace

Konfigurace softwaru RouterOs lze provést několika způsoby (GUI, telnet, ssh), ale nejpřehlednější možností pro začátečníky je použití grafického rozhraní, ke kterému se přistupuje přes aplikaci Winbox. Po přihlášení se spustí okno z GUI rozhraním, přes které je možno RouterOS spravovat. Podrobnějšímu popisu nastavení se věnuji ve vypracovaných úlohách, které jsou obsaženy v příloze.



Obr. 15: GUI rozhraní RouterOS

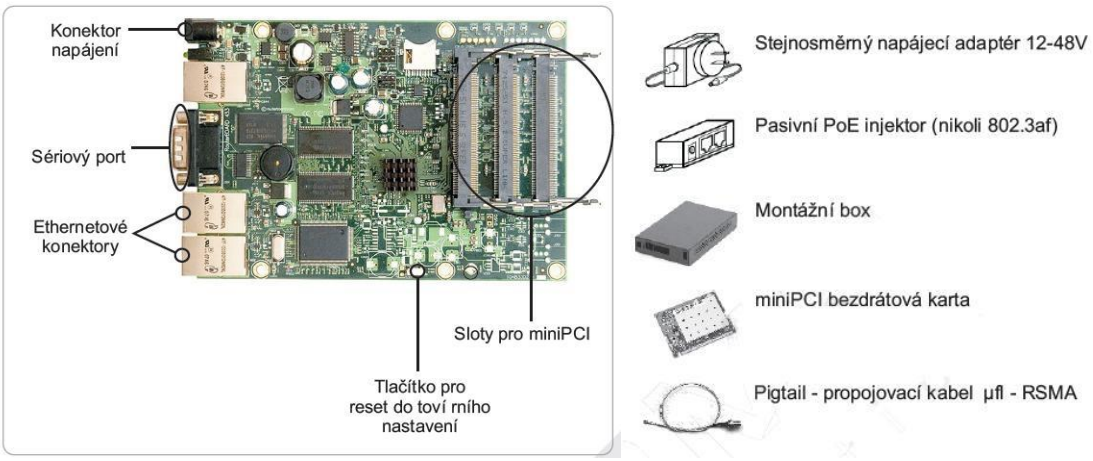
6.3 RouterBoard

Firma Mikrotik dodává ucelenou řadu produktů, které mohou sloužit jako bezdrátový AP, firewall nebo směrovač. Jednotlivé modely se od sebe odlišují počtem ethernetových konektorů, výkonem procesoru, počtem slotů miniPCI, popřípadě dalšími prvky rozšíření jako jsou sloty pro SD karty, konektivitu USB a podobně a v neposlední řadě také dodávanou licencí. Základní přehled produktů je uveden v tabulce.

Tab. 4: Přehled verzí Routerboard

RB 1xx	Dnes je již nevyrábí a maximálně se dají nakoupit skladové zásoby. Jedná se o nejslabší řadu RB od Mikrotiku určenou převážně ke klientům. Modely se dají osadit až třemi WiFi kartami a obsahují až tři ethernet porty (model 150 jich měl 5). Tato řada byla nahrazena modely 411, případně 433.
RB 3xx	Dnes se již také nedá sehnat, ale je stále součástí mnoha páteřních spojů a najdeme ho také u množství klientů, kteří potřebovali připojit více než jen pár počítačů.
RB 4xx	Nová řada nahrazující modely z řad 1×x a 3×x. Přináší především rychlejší procesor a více paměti. V této řadě můžeme najít jak modely určené pro domácí použití, tak pro nasazení na středně zatížené spoje.
RB 6xx	Pro páteřní spoje o několika desítkách uživatelů je řada 6×x jako stvořená a s možností rozšíření je možné tyto karty osadit až osmi WiFi kartami.
RB 10xx	Nejvýkonnější řada a také s patřičnou cenou. Hodí se především v kombinaci s 1 Gbit/s ethernetem. RB této řady můžeme umístit do racků.

Cena těchto zařízení se pohybuje od 2500 Kč do 6000 Kč, záleží na typu a přesné konfiguraci. K ceně je nutné připočítat cenu miniPCI karty, která se pohybuje okolo 1000 Kč a taktéž cenu zdroje a krytu RouterBoardu.



Obr. 16: Routerboard a příslušenství

6.3.1 Specifikace Routerboard 433

Použití	Vysoce výkonné AP/Router
Procesor	Atheros AR7130 300MHz
Paměť	RAM64MB DDR SDRAM
Ethernet	porty3x 10/100 Auto-MDI/X
Rozšíření	3x miniPCIPaměť64MB NAND
Napájení	(konektor)10-28V DC; přepěťová ochrana
PoE	10-28V DC
Software	RouterOs Level4

6.3.2 Sestavení a připravení hardwaru

Pro praktickou část této práce bylo nutné sestavit dva přístupové body. Jako základ jsem zvolil Routerboard řady 433, který svým výkonem a vybaveností plně dostačuje pro zvolené úlohy. Pro kompletní sestavení jsem použil originálního příslušenství a Routerboard umístil do plechového montážního boxu. Jako miniPCI kartu jsem zvolil model CM-09 s chipsetem Atheros AR5213. Ten podporuje normy 802.11a/b/g a podporuje nejnovější standardy v šifrování přenosu 802.1x, WPA, WPA-PSK, AES-CCM & TKIP, WEP kódování. Napájení zařízení jsem vyřešil standardním napaječem 24V. Díky tomu, že jedna z úloh vyžadovala mobilitu zařízení pro měření v otevřeném prostoru, vytvořil jsem redukci, kdy Routerboard mohl být napájen pomocí 12 V baterie. Jako anténa byla použita 3,5 dBi všesměrová dipólová anténa. Zařízení pracovalo s operačním systém RouterOs verze 4.10. Na kterém byly taktéž sestaveny veškeré úlohy.

7 Praktické úlohy

Praktická část této bakalářské práce se skládá ze sestavení pěti ukázkových úloh pro použití softwaru RouterOs. Úlohy jsou navržené pro základní pochopení práce se softwarem RouterOs a seznámení se základními funkcemi tohoto systému. Takto navržené úlohy by měli postačit k vytvoření bezdrátové sítě s použitím zabezpečení a posléze pro správu softwaru RouterOs. Úlohy pouze nastiňují možnosti tohoto systému, kterých existuje celá řada a vždy záleží na konkrétní úloze, které má zařízení plnit. Proto zde nepopisuji veškeré funkce, pro hlubší pochopení práce s RouterOS doporučuji navštívit domovské stránky společnosti *wiki.mikrotik.com* , kde je uvedena celá řada postupů a návodů. Taktéž je možnost navštívit kurzy ovládání RouterOS, které pořádá společnost i4wifi (*http://www.skoleni-mikrotik.cz/*).

Pro sestavení úloh se nejdříve bylo nutné seznámit se systémem RouterOS. Nejvíce informací jsem čerpal z právě již zmíněné stránky *wiki.mikrotik.com*, kterou jsem použil jako „odrazový můstek“. Zde jsem se seznámil se základními funkcemi systému RouterOs. Dalším velice přínosným zdrojem informací mi byl server *www.ispforum.cz,* kde se nachází obsáhlé fórum věnované systému RouterOS. Fórum slouží jako diskusní místnost pro lokální poskytovatele internetu, kteří využívají RouterOS. Fórum obsahuje logicky rozdělené sekce s návody, typy a hotovými skripty pro RouterOs.

Úlohy jsou navržené tak, aby je studenti mohli zároveň použít jako příručku pro nastavení RouterOS. Pomocí těchto úloh by měl být student schopen ovládat základní nastavení systému RouterOS, které postačuje pro sestavení funkční bezdrátové sítě. Jako hardware jsem použil dva RouterBoardy řady 433. Z nichž jeden vždy plnil úlohu přístupového bodu a druhý úlohu klienta.

7.1 Popis úloh

Úloha 1 – Domácí brána

V první úloze se věnuji nastavení RouterOS, do funkce domácí brány. To znamená, že zařízení Routerboard vystupuje jako klasický Access point, kdy konektivita je přivedena pomocí ethernetové sítě na port1, porty 2 a 3 slouží jako přístup do lokální sítě s automatickým přidělením adres z DHCP serveru. Veškerý vnitřní provoz je maskován za výchozí IP adresu domácí brány pomocí funkce NAT. Dále je použita bezdrátová část zařízení, která slouží jako přístupový bod. Bezdrátová část je zabezpečena šifrováním WPA2.

Úloha 2 – NAT klient

Úloha 2 slouží k nastavení zařízení do režimu klient. Které je hojně používáno k připojení klienta k bezdrátové síti. K připojení konektivity slouží bezdrátová část, s pevně nastavenou IP adresou a určeným zabezpečením od ISP (poskytovatel internetu). Pro přístup do lokální sítě slouží ethernet port 1 až 3 s automatickým přidělením adres z DHCP serveru. Veškerý vnitřní provoz je maskován pomocí funkce NAT za adresu určenou poskytovatelem.

Úloha 3 – Řízení datových toků

Úloha 3 se zaměřuje na řízení datových toků v síti, v tomto případě omezení rychlostí jednotlivých klientů. Využívá integrovanou funkci systému RouterOS „Queues“, pomocí které lze nastavit omezení rychlosti a nastavení priorit konkrétních klientů.

Úloha 4 – Bandwidth test

Úloha 4 se zaměřuje na test propustnosti pásma v režimech 802.11abg. Využívá integrovanou funkci systému RouterOS „Bandwidth test“, pomocí které lze změřit reálnou průchodnost dat mezi dvěma zařízeními.

Úloha 5 – HotSpot

Úloha 5 se zaměřuje na vytvoření vlastního HotSpotu, tedy přístupového bodu se specifickými požadavky na přihlášení, registraci a dobu užívání. Nejčastěji se s ním setkáme v restauracích, hotelech, a internetových kavárnách. Kde k přístupu na internet dojde, až po registraci či zadání přístupových údajů přes webové rozhraní.

7.2 Shrnutí úloh

První tři úlohy jsou určeny pro vytvoření domácí bezdrátové sítě, kde jako Access point slouží RouterBoard řady 433, jedná se o klasickou síť podle standardu 802.11. Dále je zde rozebráno omezení jednotlivých klientů, tato funkce se může hodit v případě připojení více uživatelů k internetu, kdy máme možnost pomocí integrované funkce systému RouterOS omezovat jednotlivé klienty podle potřeby. Čtvrtá úloha mi přišla velice zajímavá z pohledu studenta, kde si díky integrované funkci bandwidth test, může vyzkoušet reálnou propustnost dat při různých režimech bezdrátové sítě. Úloha se zabývá měřením propustnosti pásma v režimech 802.11a, 802.11b, 802.11g, 802.11a turbo. A ukazuje rozdíl mezi teoretickými a reálně dosaženými přenosovými rychlostmi. V rámci této úlohy jsem se zúčastnil pokusu, kdy studenti měřili rychlosti v podzemní štole Josef a naměřené výsledky srovnávali s hodnotami naměřenými ve volném prostranství. Pátá úloha nastiňuje možnosti nasazení systému RouterOs ve veřejných prostorách (internetová kavárna, letiště, restaurace, hotel), kdy zařízení funguje jako HotSpot a k přístupu na internet je nutné přihlášení.

8 Závěr

V předložené bakalářské práci se zabývám obecnými principy, tvorby, správy a realizací bezdrátových sítí. Především pak sítí založených na standardu 802.11. Tato práce, tedy její praktická část, by měla sloužit jako doplněk výuky předmětu Komunikační technika. Kde by se studenti z pomocí mnou vytvořených úloh měli seznámit s praktickým návrhem bezdrátové sítě na platformě společnosti Mikrotik. Práci jsem rozdělil do jednotlivých ucelených kapitol, kde se nejdříve v teoretické části snažím shrnut a popsat nejdůležitější termíny, které se v rámci bezdrátové komunikace vyskytují. V další kapitole popisuji hardware určený pro bezdrátové sítě a jeho základní funkce. V kapitole nazvané správa sítě shrnuji metody přístupu a nastavení přístupového bodu, taktéž jsou zde popsány nejčastěji využívané funkce a služby přístupových bodů. Teoretickou část zakončuji shrnutím možností zabezpečení bezdrátové sítě. Kde popisuji nejčastěji používané metody zabezpečení.

Pro vypracování praktické části bylo nutné se nejdříve seznámit se systémem RouterOs, díky tomu, že systém je tak obsáhlý neexistuje ucelená příručka, která by popisovala veškeré funkce systému. A proto bylo nutné hledat na alternativních zdrojích, jako jsou fóra, odborné články, návody. Z tohoto důvodu mi tato část zabrala nejvíce času. Po základním seznámení jsem sestavil sadu úloh, které by měly být dostačující pro vytvoření fungující bezdrátové sítě.

V praktické části práce se věnuji zdůvodnění výběru řešení od společnosti Mikrotik a jeho popisu. Práci zakončuji popisem mnou vytvořených úloh.

Seznam literatury

[1] Wikipedie otevřená encyklopedie [online]. URL: < www.wikipedie.cz >.

[2] ZANDL, P. *Bezdrátové síte WiFi: praktický pruvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

[3] Jiří Peterka. earchiv.cz [online].2007. URL: < www.earchiv.cz >.

[4] Access server [online].URL: < http://access.feld.cvut.cz >.

[5] BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi sít.* Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.

[6] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z.* Praha : Computer Press, 2008. 432 s., ISBN: 80-251-1287-0.

[7] ISPForum poskytovatelů internetu [online]. URL: < www.ispforum.cz >

[8] Oficiální forum pro Mikrotik [online]. URL: < wiki.mikrotik.com >

[9] bezpečnost WiFi Wep-WPA-WPA2 [online]. URL: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf >

[10] Rita Pužmanová. Lupa.cz [online]. 2002. URL: < http://www.lupa.cz/clanky/bezpecnost-wlan-podle-ieee/ >

Seznam obrázků

Seznam tabulek

Zdroj obrázků

Obrázek 1,2,16 – vytvořeny pomocí grafického editoru

Obrázek 3 – převzat z portálu www.lupa.cz

Obrázek 4 – převzat z portálu http://access.feld.cvut.cz

Obrázek 5, 6, 7, 12, 13, 14 – převzat z publikace ZANDL, P. *Bezdrátové sítě WiFi: praktický pruvodce*.

Obrázek 8 – převzat z www.earchiv.cz

Obrázek 9, 10, 11 – převzat z portálu www.czc.cz

Tabulka 3 a 4 převzata z portálu www.root.cz

Přílohy

ÚLOHA 1 – Domácí brána

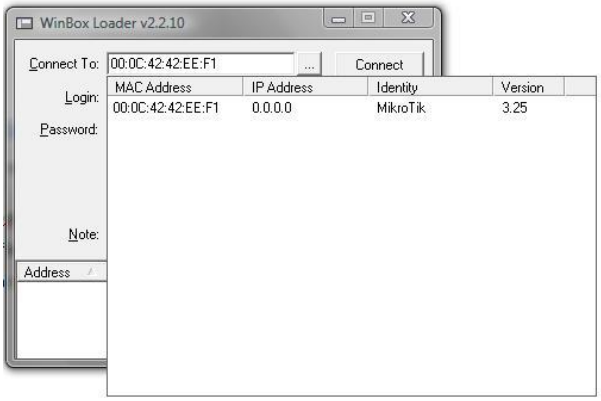
V první úloze se seznámíme se základním nastavením software RouterOS, jakož to domácí brány.

Zadání úlohy

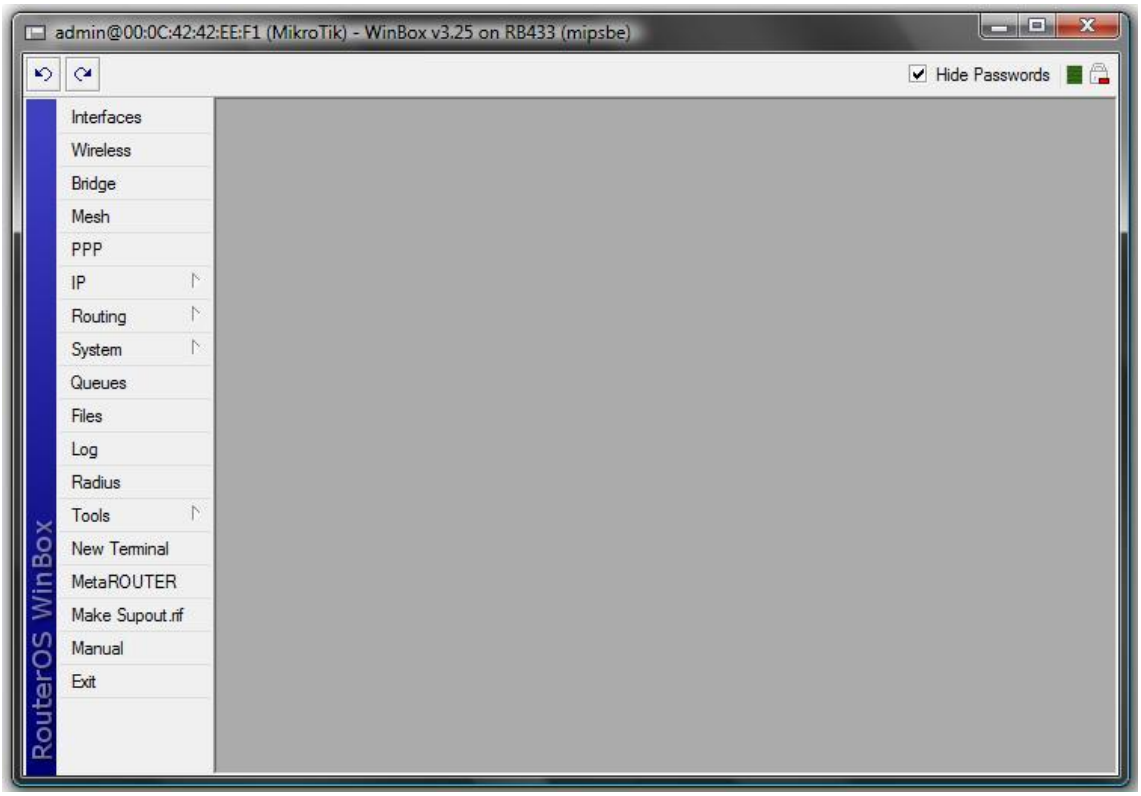
Nastavení zařízení do režimu domácí brána. Pro připojení konektivity bude použit ethernet1, s automatickým přidělením IP adresy z nadřazeného dhcp serveru. Pro připojení do domácí sítě bude použit ethernet2 a ethernet3 s nastavením dhcp serveru. Veškerý vnitřní provoz bude maskován za výchozí IP adresu domácí brány. Dále bude použita wifi část zařízení, která bude sloužit jako přístupový bod. Wifi část bude zabezpečena šifrováním WPA2.

1. Ethernet1 – dhcp klient
2. Ethernet2,3 – dhcp server
3. Wifi – přístupový bod, zabezpečení WPA2
4. NAT – překlad adres

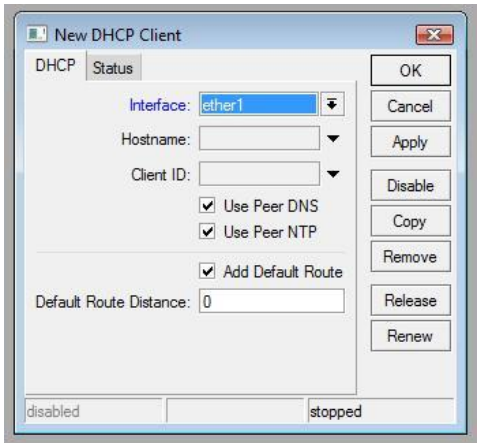
Pro konfiguraci softwaru RouterOS použijeme utilitu Winbox , pro připojení rozklikneme nabídku *Connect To:*
kde se zobrazí dostupné zařízení připojené v síti. Vybrané zařízení vybereme a spojíme se tlačítkem *Connect.*
Login je defaultně nastaven na Admin a heslo není žádné.



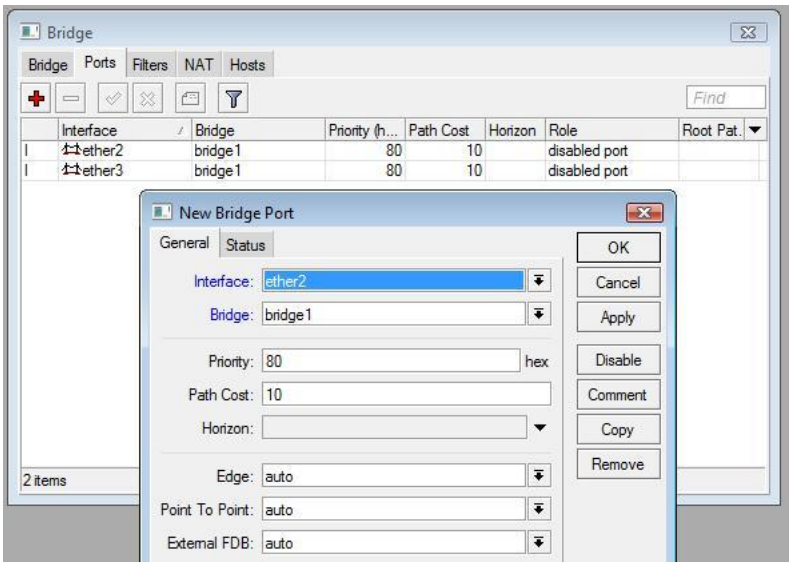
Poté se zobrazí GUI softwaru RouterOS.



1. Pro nastavení dhcp klienta pro ethernet1 postupujeme následovně ***IP-Dhcp klient-add*** Jako interface vybereme rozhraní ethernet1 a potvrdíme tlačítkem Apply.

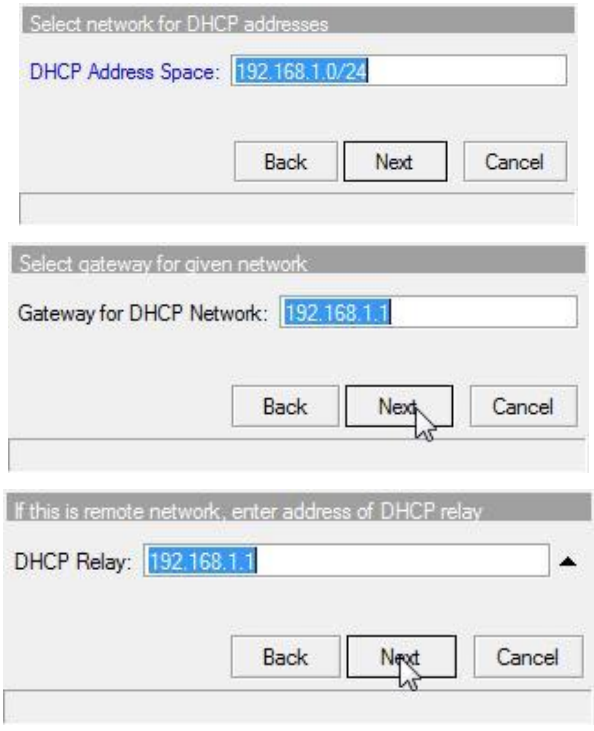


2. Porty Ethernet1 ,ethernet2 a wifi slouží ke stejnému účelu, proto se spojí do síťového mostu. Postupujeme následovně ***Bridge-add***. Kde vytvoříme bridge1, dále musíme určit, které porty mostu náleží, to provedeme následovně záložka ***ports-add*** a do bridge1 přidáme postupně porty Ethernet2, 3 a wifi.

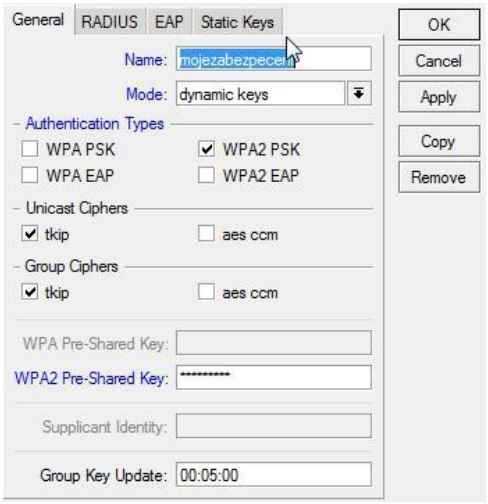


Následně můžeme nastavit DHCP server pro automatické přidělování adres. Postupujeme v nabídce ***IP-Dhcp server- dhcp setup***. Jako intefaces vybereme Bridge1, dále nastavíme adresní rozsah vnitřní sítě, nejčastěji 192.166.1.0/24. Číslo za lomítkem odpovídá masce sítě. Přehled neveřejných rozsahů a použitých masek viz tab. Jako poslední vyplníme DNS server který je stejný jako výchozí brána v našem případě 192.168.1.1

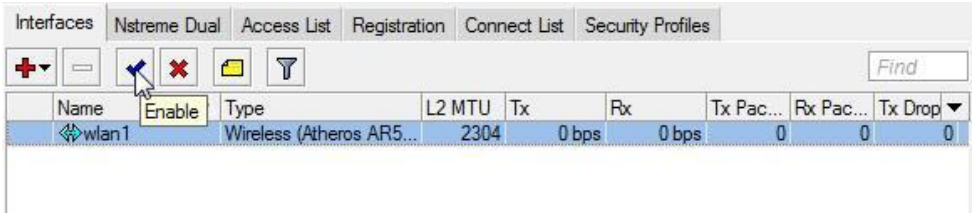
10.X.X.X 172.16.X.X 192.168.X.X	255.255.255.0 - /24 255.255.255.192 - /26 255.255.255.240 - /28 255.255.255.255 - /32



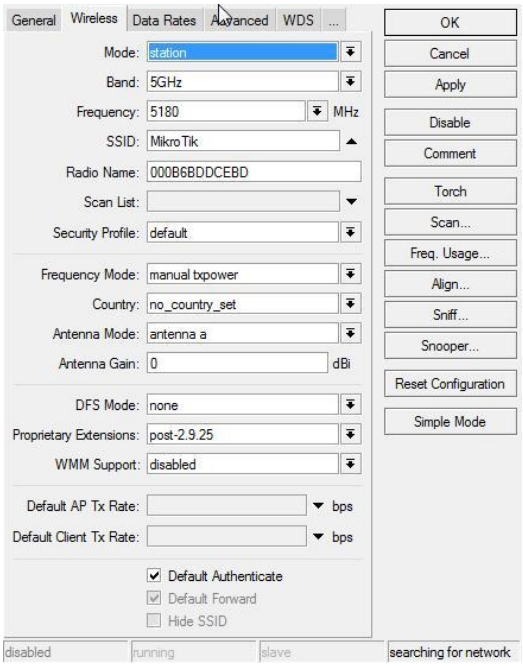
3. Pro nastavení wifi části postupujeme následovně v menu ***Wireless-Serity Profiles-add*** přidáme nový zabezpečovací profil název je libovolný. V položce Authentication Types vybereme WPA2 PSK a v položce WPA2 Pre-Shared Key: zvolíme heslo zabezpečení. Heslo musí obsahovat minimálně 8 znaků.



Potvrdíme nastavení pomocí Apply a přejdeme zpět do nabídky ***Wireless-Interfaces***. Kde povolíme wifi modul pomocí výběru modulu a stiskem tlačítka enable.



Dále rozklikneme vybraný wifi modul a v záložce v postranní liště přepneme na Advenced mode a přejdeme do záložky ***Wireless.***



Pro nastavení wifi modulu do režimu přístupového bodu určíme následující položky.

Mode: Ap bridge – určuje pracovní mód wifi modulu v našem případě přístupový bod.

Band: 2,4GHz B/G – určuje pracovní pásmo.

Frequency: určuje pracovní kanál. Pro zjištění nejlepší volby kanálu je možno použít funkci Freq. Usage, která ukáže reálnou zátěž na všech kanálech, vybíráme kanál z co nejmenší zátěží.

SSID: určuje název sítě. Výběr je libovolný. Pomocí tlačítka Hide SSID je možno vysílaní SSID potlačit.

Security Profile: vybereme námi nastavený profil.

Country: Czech republic - výběrem dané země se zakáží nepovolené kanály a nastaví max. vysílací výkony.

4. Jako poslední je potřeba nastavit pravidla routování. Postujeme následovně v nabídce ***IP-Firewall-NAT-Add*** přidáme pravidlo směrování. V záložce Generel zvolíme Chain: Srcnat a Out.Intefaces: Ethernet1. Dále v záložce Action zvolíme Action: Maquerade.

ÚLOHA 2 – NAT klient

Druhá úloha je obdobná první úloze s rozdílem, připojení konektivity pomocí wifi části. Tedy režim klient.

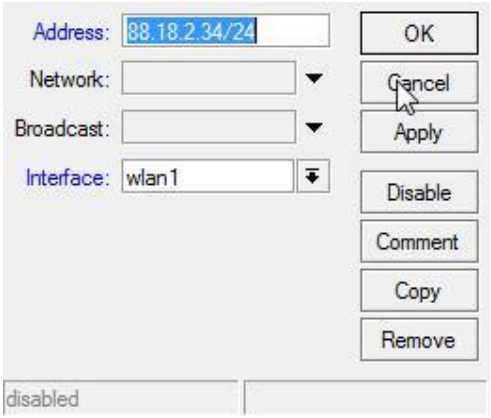
Zadání úlohy

Nastavení zařízení do režimu NAT klient. Pro připojení konektivity bude použita wifi část s pevně určenou IP adresou a daným zabezpečím od poskytovatele. Pro připojení do domácí sítě budou použity rozhraní ethernet1-3 nastavením dhcp serveru. Veškerý vnitřní provoz bude maskován za výchozí IP adresu NAT klienta.

1. Wifi – pevná ip, klient, zapezčení WEP
2. Ethernet1-3 – dhcp server
3. NAT – překlad adres

1. Nejdříve nastavíme pevnou adresu části wifi. Adresu nám určí poskytovatel. Postupujeme ***IP-Adresess-Add***

   Zvolíme adresu a za lomítkem masku sítě a adresu pomocí nabídky Interface: přidělíme wifi modulu. Položky network a broadcast se vyplní automaticky.



Pro nastavení wifi části postupujeme následovně v menu ***Wireless-Serity Profiles-add*** přidáme nový zabezpečovací profil název je libovolný. V položce Mode vybereme Static key required a v záložce Static keys vyplníme klíče zabezpečení. Klíče nám určí poskytovatel. Potvrdíme nastavení pomocí Apply a přejdeme zpět do nabídky ***Wireless-Interfaces***. Kde povolíme wifi modul pomocí výběru modulu a stiskem tlačítka enable. Dále rozklikneme vybraný wifi modul a v záložce v postranní liště přepneme na Advenced mode a přejdeme do záložky ***Wireless.***

Pro nastavení wifi modulu do režimu klienta určíme následující položky.

Mode: Station – určuje pracovní mód wifi modulu v našem případě klient.

Band: 2,4GHz B/G – určuje pracovní pásmo.

Frequency: určuje pracovní kanál. V módu klient nevyplňujeme.

SSID: určuje název sítě ke které se připojujeme, tedy název sítě poskytovatele. Můžeme vyplňit ručně nebo pomocí funkce Scan, kdy se nám zobrazí dostupné sítě.

Security Profile: vybereme námi nastavený profil.

Country: Czech republic - výběrem dané země se zakáží nepovolené kanály a nastaví max. vysílací výkony

2. Porty Ethernet1 ,ethernet2 a ethernet3 slouží ke stejnému účelu, proto se spojí do síťového mostu. Postupujeme následovně ***Bridge-add***. Kde vytvoříme bridge1, dále musíme určit, které porty mostu náleží to provedeme následovně záložka ***ports-add*** do bridge1 přidáme postupně porty Ethernet1,2,3.

   Následně můžeme nastavit DHCP server pro automatické přidělování adres. Postupujeme v nabídce ***IP-Dhcp server- dhcp setup***. Jako intefaces vybereme Bridge1, dále nastavíme adresní rozsah vnitřní sítě, nejčastěji 192.166.1.0/24. Číslo za lomítkem odpovídá masce sítě. Jako poslední vyplníme DNS server který je stejný jako výchozí brána v našem případě 192.168.1.1.

3. Jako poslední je potřeba nastavit pravidla routování. Postujeme následovně v nabídce ***IP-Firewall-NAT-Add*** přidáme pravidlo směrování. V záložce Generel zvolíme Chain: Srcnat a Out.Intefaces: Ethernet1. Dále v záložce Action zvolíme Action: Maquerade.

ÚLOHA 3 – Řízení datových toků

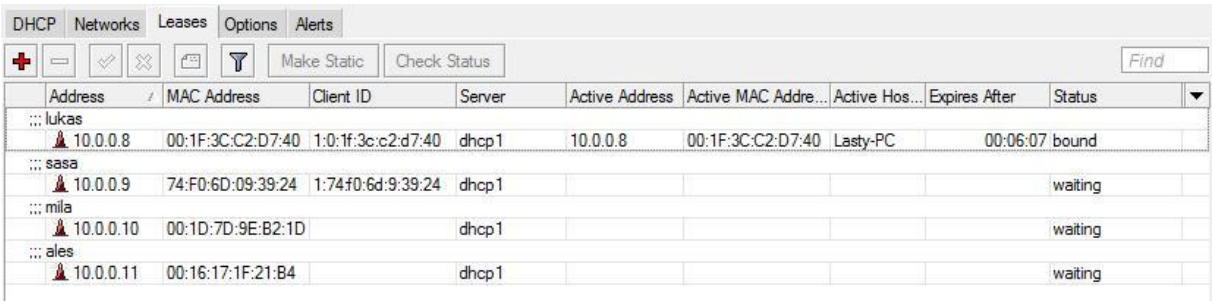
Třetí úloha je zaměřena na řízeních datových toků, v našem případě omezení rychlosti u jednotlivých klientů.

Zadání úlohy

Pomocí integrovaného nástroje pro řízení datových toků Queues, nastavte jednotlivým klientům různé povolené rychlosti Tx-Rx.

1. Nastavení dhcp serveru
2. Omezení rychlosti

1. Omezení rychlosti se vztahuje vždy ke konkrétní IP adresu, či rozsahu adres, v našem případě, tedy nejdříve musíme zajistit statické rozdělování ip adres klientům, aby klient pokaždé dostal přidělenou stejnou ip adresu. K statickému přidělení ip adres využijeme funkci Dhcp serveru, která zajišťuje přidělení adresy podle Mac adresy zařízení. Postupujeme následovně, v nabídce
   IP-DHCP server zvolíme záložku Leases. Zde vidíme připojené klienty z přidělenou ip adresou. Pomocí tlačítka Make Static, se adresa uloží do paměti a od této chvíle klient dostává stále stejnou ip adresu.

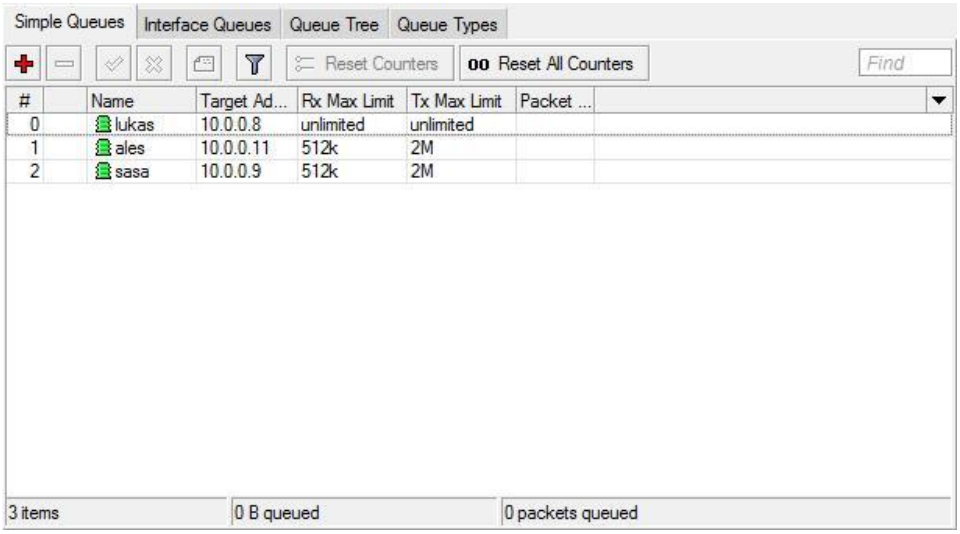


2. Nyní můžeme přistoupit k nastavení omezení rychlosti. V nabídce ***Queues*** klikneme na záložku Simple Queues a přidáme nového klienta. Pro správnou funkci je nutné vyplnit následující položky.

Name: slouží pro pojmenování klienta.

Target address: určuje cílovou adresu klienta, nastavíme konkrétní adresu klienta nebo celý rozsah adres.

Max limit: určuje maximální rychlosti klienta Tx-Rx.



ÚLOHA 4 – Bandwidth Test

Čtvrtá úloha je zaměřena na test propustnosti pásma v režimech 802.11a, 802.11b, 802.11g, 802.11a turbo.

Zadání úlohy

Pomocí integrované funkce Bandwidth test. Změřte propustnost pásma v režimech 802.11a, 802.11b, 802.11g, 802.11a turbo. Mezi dvěma zařízeními RouterBoard 433.

1. RouterBoard 1 - režim přístupový bod
2. RouterBoard2 - režim klient
3. Bandwidth test

1. Nejdříve nastavíme pevnou adresu části wifi. Vybereme jakoukoli adresu z neveřejného rozsahu. Postupujeme ***IP-Adresess-Add z***volíme adresu a za lomítkem masku sítě a adresu pomocí nabídky Interface: přidělíme wifi modulu. Položky network a broadcast se vyplní automaticky.

   Pro nastavení wifi části postupujeme následovně ***Wireless-Interfaces***. Kde povolíme wifi modul pomocí výběru modulu a stiskem tlačítka enable. Dále rozklikneme vybraný wifi

modul a v záložce v postranní liště přepneme na Advenced mode a přejdeme do záložky ***Wireless.***

Pro nastavení wifi modulu do režimu přístupového bodu následující položky.

Mode: Ap Bridge– určuje pracovní mód wifi modulu v našem případě přístupový bod.

Band: měníme v závislosti na testovaném pásmu – určuje pracovní pásmo.

Frequency: určuje pracovní kanál. Zvolíme libovolně.

SSID: určuje název sítě zvolíme libovolné.

Country: Czech republic - výběrem dané země se zakáží nepovolené kanály a nastaví max. vysílací výkony

2. Přihlásíme se pomocí utility WinBox k Routrerboardu 2 a nastavíme pevnou adresu části wifi. Vybereme další možnou adresu z rozsahu nastaveného na RouterBoardu 1. Postupujeme ***IP-Adresess-Add*** Zvolíme adresu a za lomítkem masku sítě a adresu pomocí nabídky Interface: přidělíme wifi modulu. Položky network a broadcast se vyplní automaticky.

   Pro nastavení wifi části postupujeme následovně ***Wireless-Interfaces***. Kde povolíme wifi modul pomocí výběru modulu a stiskem tlačítka enable. Dále rozklikneme vybraný wifi modul a v záložce v postranní liště přepneme na Advenced mode a přejdeme do záložky ***Wireless.***

   Pro nastavení wifi modulu do režimu klienta určíme následující položky.

   Mode: Station – určuje pracovní mód wifi modulu v našem případě klient.

   Band: měníme v závislosti na testovaném pásmu – určuje pracovní pásmo.

   Frequency: určuje pracovní kanál. V módu klient nevyplňujeme.

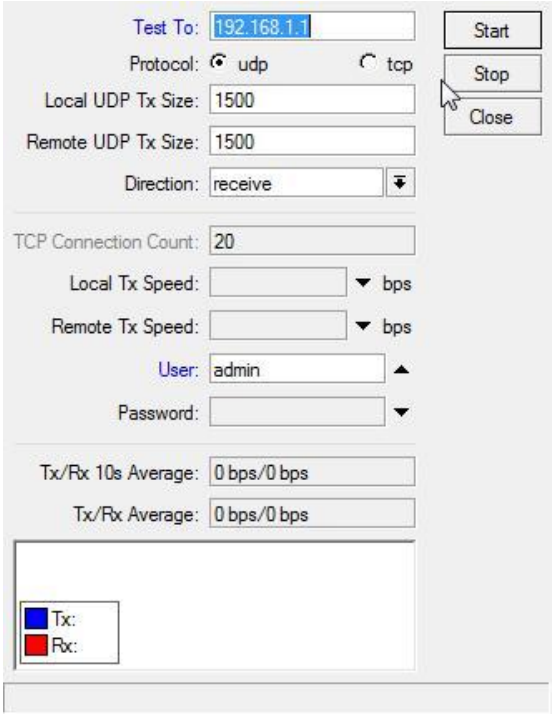
   SSID: určuje název sítě ke které se připojujeme, tedy název sítě na RouterBoardu1. Můžeme vyplňit ručně nebo pomocí funkce Scan, kdy se nám zobrazí dostupné sítě.

   Country: Czech republic - výběrem dané země se zakáží nepovolené kanály a nastaví max. vysílací výkony

   Po potvrzení nastavení dojde k propojení, to označuje písmeno „R“ u wifi modulu.

3. Máme vytvořený aktivní spoj a můžeme začít měřit jeho maximální propustnost. Využijeme obsaženou funkci Bandwidth Test. ***Tools- Bandwidth Test***. Zadáme ip adresu RouterBoardu1, dále vybereme protokol na kterém chceme spoj měřit a v položce

Direction: vybereme směr dat . Dále musíme vyplnit přihlašovací údaje do testovaného routerBoardu1. Test spustíme tlačítkem Start.



Po odečtení hodnot z grafu, změníme pracovní mód zařízení v položce **Band:** pracovní pásmo a postup 3 opakujeme.

ÚLOHA 5 – Vytvoření HotSpotu

Pátá úloha je zaměřena na vytvoření vlastního HotSpotu, tedy přístupového bodu se specifickými požadavky na přihlášení, registraci a dobu užívaní. Nejčastěji se s ním setkáme v restauracích, hotelech a věřejných prostranství.

Zadání úlohy

Vytvoření vlastního HotSpotu, kdy k připojení k internetu dojde pouze po registraci uživatele přes webové rozhraní.

1. Wifi – režim, pracovní pásmo
2. HotSpot

1. Pro nastavení wifi části postupujeme následovně ***Wireless-Interfaces***. Kde povolíme wifi modul pomocí výběru modulu a stiskem tlačítka enable. Dále rozklikneme vybraný wifi modul a v záložce v postranní liště přepneme na Advenced mode a přejdeme do záložky ***Wireless.***

   Pro nastavení wifi modulu do režimu přístupového bodu následující položky.

Mode: Ap Bridge

Band: libovolné – určuje pracovní pásmo.

Frequency: určuje pracovní kanál. Zvolíme libovolně.

SSID: určuje název zvolíme libovolné.

Country: Czech republic - výběrem dané země se zakáží nepovolené kanály a nastaví max. vysílací výkony

2. Pro nastavení samotného Hotspotu využijeme integrovaného průvodce v nabídce ***IP-Hotspot***. Kde spustíme průvodcem přes nabídku Hotspot setup. Pro spuštění Hotspotu je nutné vyplnit následující údaje.

   Hotspot interface: určuje rozhraní pro které bude Hotspot vytvořen.

   Local address network: určuje síť pro kterou bude Hotspot aktivní.

   Address Poll: určuje rozsah adres pro který bude Hotspot aktivní.

   Select Certificate: způsob ověřovaní v našem případě vybereme none.

   DNS server: vyplníme adresu DNS serveru.

   Name Hotspot user: zvolíme uživatelské jméno nutné k přihlášení k Hotspotu.

   Password Hotspot user: zvolíme uživatelské heslo nutné k přihlášení k Hotspotu.

   Pokud máme nastaven Dhcp server údaje budou přednastavené.