MESHovaní na platformě mikrotik

MESHing on the Mikrotik platform

Bc. Martin Ohnůtek

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin OHNŮTEK**
Osobní číslo:	**A09425**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**MESHování na platformě Mikrotik**

Zásady pro vypracování:

1. **Zpracujte literární rešení na dané téma.**
2. **Aplikujte doporučení 802.11s na firemní bezdrátové síti.**
3. **Odzkoušejte a vyhodnoťte provoz doporučení 802.11s v zarušeném prostředí v pásmu 2,4 a 5 GHz.**
4. **Vyhodnoťte výsledky testů mezi nezarušeným a zarušeným prostředím.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Mikrotik. Manual: The Dude [online]. 2011 [cit. 2012-02-07]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:The_Dude**
2. **MikroTik RouterOS v3.0 Reference manual [online]. 2007 [cit. 2012-02-07]. Dostupné z: http://www.mikrotik.com/testdocs/ros/3.0/refman3.0.pdf**
3. **BIGELOW, J. S. Mistrovství v počítačových sítích. Brno : Computer Press, 2004. 990 s. ISBN 80-251-0178-9.**
4. **i4wifi. Návod k obsluze [online]. 2011 [cit. 2012-02-07]. Dostupný z: http://i4wifi.cz/img.asp?attid=74453**
5. **BARTOŠEK, J. – HAVÍČEK, P. Směrovací protokol Mesh (802.11s) na platformě Mikrotik [online]. 2009 [cit. 2012-02-07]. Dostupný z: http://wh.cs.vsb.cz/sps/images/b/b3/Mesh-Mikrotik.pdf**
6. **KABELOVÁ, A. – DOSTÁLEK, L. Velký průvodce protokoly TCP/IP a systémem DNS. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.**
7. **AKYILDIZ, I. F. – WANG, X. Wireless Mesh Networks. Chichester: John Wiley & Sons LTD, 2009. 301 s. ISBN 978-0-470-03256-5.**

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **28. května 2012**

Ve Zlíně dne 24. února 2012

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je vytvořit funkční síťové MESHové propojení na platformě mikrotik. Testovat chování MESH sítě na této platformě, dále zjistit chování funkčního MESHového propojení v praxi, zjistit datové propusti v pásmu 2,4 GHz a 5GHz, nastavit jednoduchý monitoring MESH sítě.

Klíčová slova: Mikrotik,The Dude, MESH, Winbox, RouterOS

ABSTRACT

The aim of this thesis was to create a functional MESH network connection based on Mikrotik platform. Verify the MESH network behavior on this platform using functional MESH network in practice, determine the data transfer rates in the 2.4 GHz and 5GHy frequency bands and set up a simple MESH network monitoring.

Key words: Mikrotik,The Dude, MESH, Winbox, RouterOS

Rád bych poděkoval mému vedoucímu práce, kterým je Ing. Miroslav Matýsek za jeho rady, připomínky a pomoc při řešení této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Na fakultě aplikované informatiky se procesy výuky neustále vyvíjejí a předmět počítačové sítě jistě nezůstává pozadu. Tento předmět je jeden z nejdůležitějších předmětů v oboru informačních technologií. Cílem předmětu je studenta naučit základům počítačové sítě. Obor informačních technologií jde neustále vpřed a vyvíjí se každým dnem. Od prvotních náznaků samotné počítačové sítě již bylo učiněno hodně kroků ke zdokonalení vlastností samotných sítí.

Jednou z nových a zajímavých technologií je programovací platforma MIKROTIK. V dnešní době představuje jedinečnou technologii, která dokáže profesionálně spravovat počítačovou síť a to s minimálními náklady. Spolehlivost zařízení MIKROTIK je srovnatelné s velkými výrobci v tomto odvětví. Nastavitelnost funkcí tohoto výrobce dosahuje profesionálních kvalit a využitelnost v oboru je široká. Tato platforma je převážně určena pro uživatele bezdrátových technologií, nicméně již dnes vyrábějí kvalitní drátové zařízení, které mohou sloužit jako servery pro správu sítě.

Právě díky platformě MIKROTIK můžeme odsimulovat funkčnost protokolu MESH. K této simulaci byly použity čtyři zařízení mikrotik, jedno tvoří vstupní bránu pro internet, další zařízení je zařízení, které má spravuje chod MESH sítě a další dvě použitá zařízení v podstatě tvoří mosty, přes které se tento signál šíří. V případě výpadku jednoho vysílače se automaticky notebook přihlásí k jinému, přičemž uživatel nepozná výpadek vysílače a může danou síť využívat dále. V podstatě stejný princip funguje u mobilních sítí, kdy mobilní telefon se automaticky přihlašuje k vysílači, který má lepší signál.

Pro sledování jednotlivých pokusů v MESH síti byl použit notebook, na kterém byl nainstalován sledovací software THE DUDE, dále sledování a další testy byly prováděny v aplikaci WINBOX, pro testování byl používán reálný provoz sítě, například streamování videa v síti nebo stahování velkých souborů.

I TEORETICKÁ ČÁST

1 POČÍTAČOVÉ SÍTĚ

Počítač připojený k síti, který nabízí své prostředky, se nazývá server. Počítač s přístupem k těmto prostředkům se označuje jako pracovní stanice nebo klient. Servery jsou obvykle nejvýkonnějšími počítači v síti, protože výkon potřebují k obsluze mnoha požadavků jiných počítačů, které sdílejí jejich prostředky. Pracovní stanice nebo klient, jsou naproti tomu obvykle počítače, které jsou levnější a méně výkonné Počítač může být zpravidla serverem nebo pracovní stanicí, avšak jen zřídka obojím (toto oddělení velmi zjednodušme správu a administraci sítě). Malé sítě s relativně malým množstvím uživatelů mohou využívat síť peer-to-peer, ve které každý počítač může sdílet informace. Všechny počítače v síti musí být samozřejmě fyzicky propojeny a taková propojení jsou většinou zajišťována pomocí adaptérů NIC (network rozhraní card) a měděných kabelů, či alternativním propojením, jako je například optické vlákno nebo bezdrátové připojení [1].

1.1 Rozlehlost sítí

Počítačové sítě obvykle spadají podle své velikosti a funkce do jedné ze tří skupin. Místní síť LAN (Local Area Network) je základní klasifikací kterékoli počítačové sítě. Architektura LAN může být jednoduchá (dva počítače propojené kabelem) až složitá (stovky propojených počítačů a periferních zařízeni v celé obchodní společnosti). Rozlišující vlastností sítě LAN je to, že je omezena na určitou geografickou oblast, jako je jedna budova nebo oddělení (většinou umístěné v oblasti s průměrem 5 km). Pokud jsou počítače propojené mezi několika budovami ve velkém městě, sítě se někdy označují jako metropolitní sítě (MAN - Metropolitan Area Network, obvykle 5-50 km). V porovnání s tím nemá rozlehlá síť (WAN - Wide Area Network) žádné geografické omezení. Ve většině případů je síť WAN tvořena z většího počtu propojených sítí LAN - pravděpodobně nejzákladnější sítí WAN je Internet [1].

1.2 Síťový hardware

Síťový hardware má obrovský vliv na rychlost, kvalitu a celkový výkon sítě. Patří do něj rozbočovače, opakovače, mosty, směrovače, brány, síťové karty a kabely.

1.2.1 Opakovače

Jak elektrické signály cestují kabely, degradují a jsou zkreslovány. Tento efekt se nazývá útlum. Jak narůstá délka kabelu, efekt útlumu se zhoršuje. Je-li kabel příliš dlouhý, útlum nakonec znemožní rozpoznatelnost signálu a vzniknou tak datové chyby v síti. Instalace opakovačů umožňuje, aby signály cestovaly dále pomocí obnovení signálu sítě a jejich novým odesláním na další úsek kabelů. Aktivní rozbočovače často slouží jako aktivní opakovače, avšak samotné opakovače mohou být potřeba pro příliš dlouhé kabelové vedení [1].

1.2.2 Rozbočovače

Jednoduše řečeno je rozbočovač centrálním spojovacím zařízením, které propojuje počítače v hvězdicové topografii. Variaci rozbočovače je MAU (Multistation Access Unit) používaný k propojení počítačů v topologii Token Ring. Rozbočovače jsou v moderních sítích standardním zařízením i a dělí se na pasivní nebo aktivní. Pasivní rozbočovač vůbec nezpracovává data - jde o propojovací panel. Naproti tomu obnovují aktivní rozbočovače (někdy nazývané opakovače) data, aby udržely příslušnou sílu signálu. Některé rozbočovače mají také schopnost zpracovávat další úkoly, jako je přemostění, směrování a přepínání. Systémy založené na rozbočovačích jsou všestranné a nabízejí oproti systémům bez využití rozbočovačů několik výhod. Narušeni kabelu v obyčejné sběrnicové topologii například způsobí vypnutí sítě. Při použití rozbočovačů však narušení jakéhokoli kabelu připojeného k rozbočovači ovlivní pouze omezenou část sítě [1].

1.2.3 Mosty

Mosty nabízí zatížené síti více funkcí. Most muže fungovat jako opakovač k prodloužení efektivní délky síťového kabelu. Most však má větší „inteligenci" a může rozdělit síť pro izolování nadměrného provozu nebo problematických dat. Pokud například svazek z jednoho či dvou počítačů (nebo jednoho odděleni) zaplavuje síť daty a zpomaluje tak její činnost, muže most tyto počítače (nebo oddělení) izolovat umístěním do jejich vlastní části kabelu. Místo rozlišováni mezi protokoly mohou mosty jednoduše odesílat všechny protokoly po síti. Protože všechny protokoly procházejí mosty, je na jednotlivých počítačích, aby stanovily, které protokoly mohou byt rozpoznány. Mosty mohou

propojovat také různá fyzická médiu, jako je kabel s kroucenou dvojlinkou a tenký koaxiální kabel [1].

1.2.4 Směrovače a kombinace směrovače s mostem

Když pracujete ve složitějších síťových prostředích, která používají různé segmenty sítě - každý s jinými protokoly a architekturami - most je často pro rychlou a efektivní komunikaci mezi jednotlivými segmenty nedostatečný. Taková složitá síť vyžaduje propracovaná zařízení, která znají adresy každého segmentu, stanovují nejlepší cestu pro odesílání dat a filtrují data vysílaná na místní segmenty. Tento typ zařízení se nazývá směrovač. Stejně jako most mohou směrovače filtrovat a izolovat data posílaná sítí a mohou také připojovat segmenty sítě. Směrovače mohou navíc přepínat a směrovat pakety přes více sítí. Činí tak vyměňováním informací o určitém protokolu mezi samostatnými sítěmi. Směrovače mají přístup k více informacím o paketech než most a používají tyto informace ke zdokonalení přenosu paketu. Směrovače se používají ve složitých sítích, protože poskytují lepší správu přenosu dat. Směrovače mohou například sdílet informace o stavu a směrování a používat tyto informace k překlenutí pomalých nebo špatně fungujících připojení [1].

1.2.5 Brány

Brána funguje jako výkonný překladač určený pro připojení radikálně odlišných sítí. Ačkoli je pomalejší než most nebo směrovač, může brána provádět složitější funkce, jako je překlad mezi sítěmi, které hovoří různými jazyky (za pomoci technik, jako je převod protokolu a šířky pásma). Brány umožňuji komunikaci mezi zcela odlišnými architekturami a prostředími. Efektivně přetvářejí pakety a převádějí data pocházející z jednoho typu sítě do jiného tak, že každý z nich rozumí datům toho druhého. Brána přetváří informace, aby vyhovovaly požadavkům cílového systému, a změní formát zprávy tak, aby se přizpůsobil aplikaci přijímající přenášená data. Ve většině případů jsou brány úkolově specifické, což znamená, že jsou vyhrazena určitému typu přenosu. Často vyznačují podle svého úkolu (tj. Windows NT Server-to-SNA Brána) [1].

1.2.6 Síťové karty

Síťová karta (NIC, také známá jako adaptér LAN) funguje jako rozhraní mezi samostatným počítačem (serverem nebo klientem) a síťovými kabely. Uvnitř musí karta NIC identifikovat počítač v síti a načíst do vyrovnávací paměti data mezi počítačem a kabelem. Při odesílání dat musí karta NIC převést data z paralelních bajtů na sériové bity (poté znovu zpět během přijímání). Na straně sítě musí karta NIC vygenerovat elektrické signály, které cestují prostřednictvím sítě, řídit přístup k síti a vytvořit fyzické připojení ke kabelu. Každý počítač v síti musí mít alespoň jeden nainstalovaný port NIC. Moderní karty NIC zvyšují efektivní propustnost pomocí pokročilých technik *spolupráce adapterů,* jako je například *odolnost vůči chybám adaptéru* (AFT - adapter fault tolerance) poskytující automatickou redundanci vašemu adaptéru. Pokud primární adaptér selže, přejímá jeho funkce sekundární. *Adaptivní vyvážení zatížení* umožňuje vyvážení toku přenosu dat mezi dvěma až čtyřmi adaptéry [1].

1.2.7 Kabeláž

Sítě všech velikostí a konfigurací jsou založeny na fyzické kabeláži, která spojuje všechny počítače a další hardware dohromady. Kabeláž (také označovaná jako síťové médium) přichází v mnoha různých konfiguracích, avšak mezi běžné typy kabelů používaných pro běžné sítě patří nestíněná kroucená dvojlinka (UTP - Unshielded Twisted Pair), koaxiální kabel, stíněná kroucená dvojlinka (STP - Shielded Twisted Pair) a optický kabel (FO – Fiber Optic). Jsou známy tři hlavní parametry, které by kabel měl splňovat.

- Odolnost vůči *přeslechu* (elektřina probíhá mezi páry drátů ve stejném kabelu).
- Odolnost vůči narušení z vnějšku elektrického pole (šum vytvářený elektrickými motory, převaděči a vysílači)
- Snadnost instalace,

Toto jsou důležité aspekty, protože kabely odolné vůči přeslechu a narušení mohou běžet déle a podporovat vyšší hodnoty přenosu dat. Například koaxiální kabely a kabely STP mají ve vnější vrstvě tenkou kovovou fólii, která nabízí dobrou odolnost vůči elektrickému šumu, avšak fólie navíc vytváří větší, tlustší kabel, který lze hůře protáhnout instalačními trubkami a zdmi během instalace. Kabel UTP je tenčí a jeho instalace je snazší, nabízí však

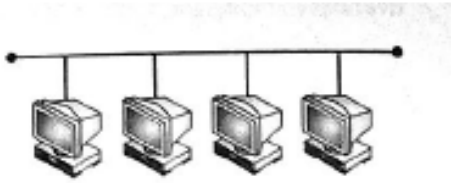
menší odolnost vůči elektrickému šumu. Oproti tomu nese optický kabel místo elektrických impulsů světelné signály, takže je odolný vůči přerušení dodávky elektřiny. To optickému kabelu umožňuje přenášet signály rychleji a dále, než je tomu u jakéhokoli jiného kabelu. Optický kabel je bohužel mnohem dražší než jiné typy kabelů a správná instalace vyžaduje specializované nástroje a zkušenosti [1].

1.3 Topologie sítě

Termín „topologie“ označuje způsob, jakým jsou počítače a další zařízení v síti propojeny. Konkrétní typ kabelu, který použijete, stanovuje topologii vaší sítě. Nemůžete nainstalovat určitý typ kabelu za použití libovolné topologie. Pro instalaci každého konkrétního typu kabelu je nutné použít správnou topologii. Třemi hlavními topologiemi sítě LAN jsou sběrnicová, hvězdicová a kruhová. Ukážeme si sedm nejčastějších topologií - sběrnicová, hvězdicová, hybridní, hierarchická, hvězdicová, kruhová, vícecestná a bezdrátová [1].

1.3.1 Sběrnicová topologie

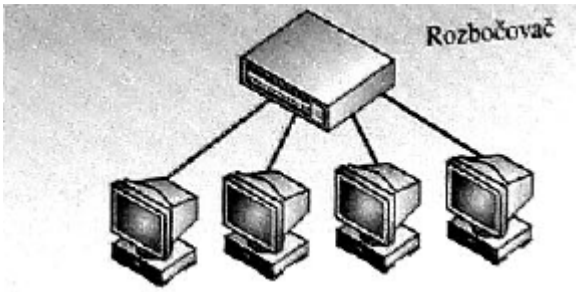
Zvolíte-li pro svou síť sběrnicovou topologii, počítače a jiná zařízení jsou propojeny v jedné linii a každý systém je kabelem spojen s dalším systémem. Tato konfigurace se často označuje jako uzavřený cyklus. Všechny signály přenášené systémy v síti procházejí podél sběrnice v obou směrech všemi systémy, než dosáhnou svého cíle. Sběrnicová topologie má vždy dva otevřené konce, jak ukazuje obrázek 1. Dva konce sběrnice musí být zakončeny elektrickými rezistory tak, že se signály neodrážejí zpět do opačného směru, což by vedlo k interferenci s novějšími přenášenými signály. Chybějící zakončení u jednoho z konců může zabránit správné komunikaci počítačů připojených k dané sběrnici [1].



Obr. 1. Sběrnicová topologie [1].

1.3.2 Hvězdicová topologie

Hvězdicová topologie používá centrální zařízení nazývané rozbočovač nebo koncentrátor. Každý počítač je připojen k rozbočovači samostatným kabelem, jak ukazuje obrázek 2. Hvězdicová topologie používá kabely kroucené dvojlinky, jako je lOBaseT a lOOBaseT. Hvězdicovou topologii používá většina sítí Ethernet LAN a mnoho sítí LAN používajících jiné protokoly. I když je každý počítač připojen k rozbočovači samostatným kabelem, rozbočovač šíří všechny signály vstupující kterýmkoli z jeho portů do všech dalších portů. Tímto způsobem jsou všechny signály odesílané každým z počítačů v síti přijaty všemi zbývajícími počítači [1].



Obr. 2. Hvězdicová topologie [1].

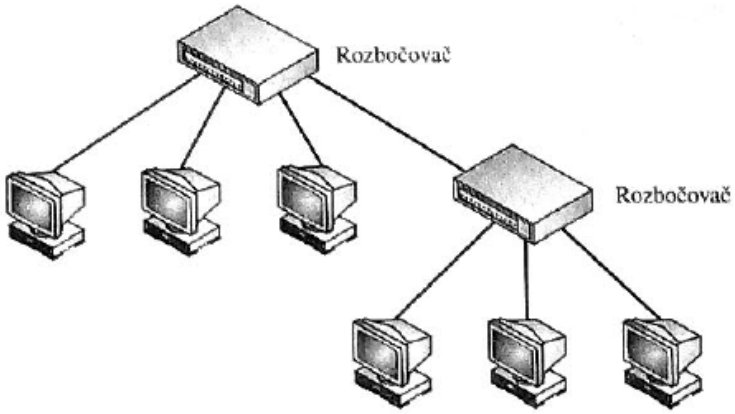
1.3.3 Hvězdicová a sběrnicová topologie

Hvězdicová a sběrnicová topologie, kterou můžete použít k rozšíření velikosti sítě LAN o více než jednu hvězdici. Síť LAN rozšíříte spojením několika hvězdicových sítí se samostatným segmentem sběrnicového kabelu pro vzájemné propojení jejich rozbočovačů. Každý rozbočovač odesílá příchozí data prostřednictvím sběrnicového portu a zároveň i hvězdicovým portem, což umožňuje všem počítačům v síti LAN komunikovat mezi sebou. Tato topologie byla původně určena pro rozšíření 10BaseT Ethernet, avšak kvůli snížení výkonu sítě způsobeného pomalostí koaxiálních sběrnicových sítí se v dnešní době používá jen zřídka [1].

1.3.4 Hierarchická hvězdicová topologie

Když potřebujete rozšířit síť z kapacity původního rozbočovače, implementujete hierarchickou hvězdicovou topologii (známá jako stromová topologie), jak ukazuje obrázek 3. Pro rozšíření hvězdicové sítě jednoduše připojíte původní rozbočovač

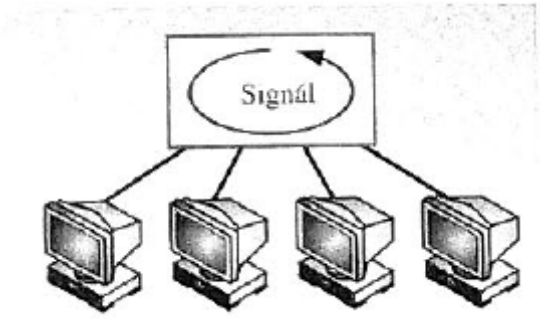
k druhému rozbočovači pomocí standardního kabelu připojeného ke speciálnímu portu, který je označován jako vzestupný port a slouží tomuto účelu. Data, která dorazí k jednomu z rozbočovačů, jsou předána oběma rozbočovačům stejně jako počítačům připojeným k síti. Protokol používaný síti LAN stanovuje počet rozbočovačů, které může jedna síť LAN podporovat. Sítě Fast Ethernet mohou například většinou podporovat jen dva rozbočovače [1].



Obr. 3. Hierarchická hvězdicová topologie [1].

1.3.5 Kruhová topologie

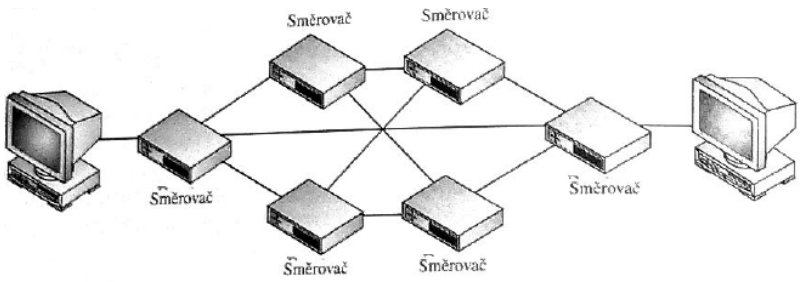
Kruhová topologie se podobá sběrnicové topologii v tom, že každý počítač je propojený s dalším počítačem. Místo ukončeni obou konců jsou však tyto spojeny dohromady ve formě kruhu, jak je vidět na obrázku 4. Toto propojení způsobuje, že signály cestují cyklicky od jednoho počítače k dalšímu a nakonec se vrátí k počátečnímu bodu. Ve většině případů je kruhová topologie striktně logickou konstrukcí, a ne fyzickou, protože kabely se v kruhové topologii připojují k rozbočovači a tvoří spíše hvězdici. V kruhové topologii můžete použít několik různých typů kabelů. Sítě FDDI (Fiber Distributed Data Rozhraní) používají kruhovou topologii s optickým kabelem, zatímco sítě Token Ring používají kroucené dvojlinky [1].



Obr. 4. Kruhová topologie [1].

1.3.6 Vícecestná topologie

Použití vícecestné topologie v síti LAN není praktické. Každý počítač má vyhrazené připojení ke každému počítači ve vícecestné LAN síti. Tato topologie je praktická pouze ve dvouuzlové síti. Vícecestná síť se třemi, či více počítači by vyžadovala samostatnou kartu NIC pro každý další počítač v síti. Například sedmiuzlová síť by vyžadovala, aby každý počítač měl nainstalováno šest karet NIC. Ačkoliv je použití této topologie v síti LAN nepraktické poskytuje výbornou odolnost proti chybám. Jedno chybné místo může ovlivnit jen jeden počítač, ne celou LAN síť [1].

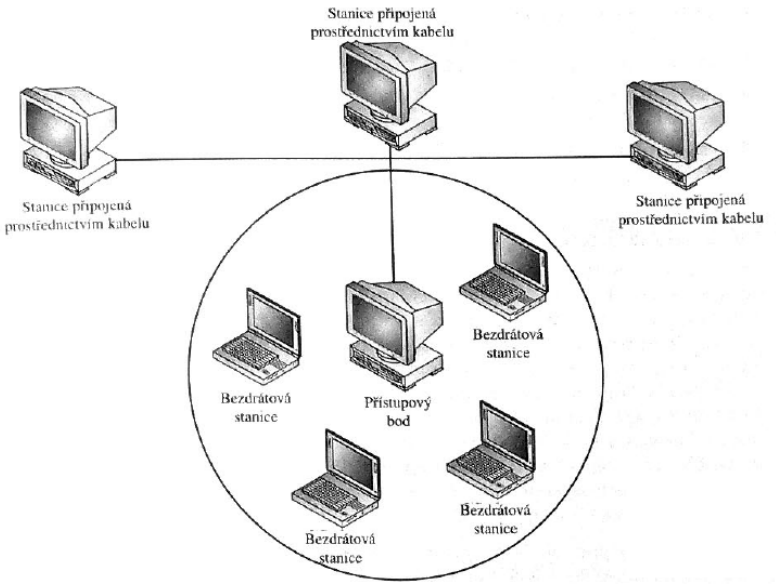


Obr. 5. Vícecestná topologie[1].

1.3.7 Bezdrátová topologie

Ačkoli termín „topologie“ obvykle označuje uspořádání kabelů v síti, nemusí tomu tak být vždy. Bezdrátové sítě používají to, co se označuje jako nevázaná média, která jsou formou rádiových nebo světelných vln tvořících určité vzorky, které mohou počítače používat ke vzájemné komunikaci. Existují dvě základní bezdrátové topologie, infrastrukturní a ad-hoc. Infrastrukturní síť se skládá z bezdrátově zařízených počítačů, které komunikují se sítí

prostřednictvím bezdrátových vysílačů (místa přístupu k síti), které jsou připojeny k síti standardními kabely, jak je vidět na obrázku 6. V této topologii nekomunikují počítače vzájemně mezi sebou, ale se sítí přes bezdrátové vysílače. Tato topologie je nejvhodnější pro rozsáhlé sítě s několika bezdrátovými počítači, které spolu nepotřebují komunikovat, jako jsou například přenosné počítače cestujícího obchodního zástupce. Tyto typy uživatelů obvykle nepotřebují komunikovat s ostatními pracovními stanicemi v síti, ale bezdrátové přípojem používají spíše pro přístup k serverům a prostředkům sítě. Topologie ad-hoc se skládá ze skupiny počítačů, které jsou vybaveny bezdrátovými kartami NIC a jsou schopné komunikovat mezi sebou. Nevýhodou obou těchto bezdrátových topologií je to, že počítače musí zůstat v komunikační oblasti bezdrátové technologie. Tato topologie je vhodnější pro domácí či menší kancelářské sítě, kde není instalace kabelů [1].

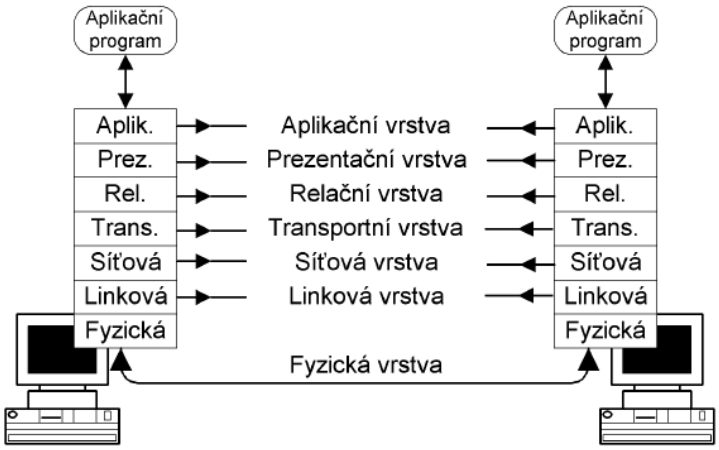


Obr. 6. Bezdrátová topologie [1].

1.4 Referenční model OSI

Účelem referenčního modelu bylo definovat strukturu, která stanovuje logické úkoly komunikace požadované pro přemisťování informací mezi počítačovými systémy Základním předpokladem modelu OSI (Open Systems Interconnection) je definovat a seskupit logické funkce toku informací mezi systémy, aniž by se pokoušel popisovat detaily každé z funkcí. Proto byl vyvinut model se sedmi vrstvami, v němž každá vrstva zastupuje skupinu souvisejících logických funkcí. Podrobnosti každé vrstvy jsou

ponechány na vývojářích systému, model definuje celkovou funkci každé vrstvy a vzájemný vztah s vyššími a nižšími vrstvami [2].



Obr. 7. Sedmivrstvá architektura ISO OSI [2].

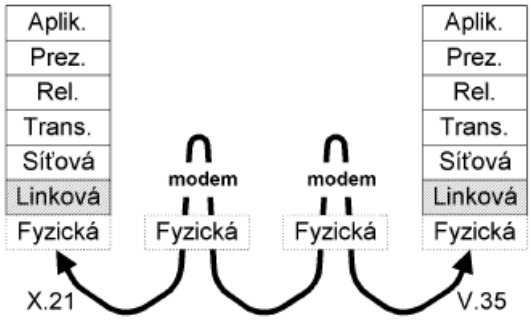
1.4.1 Fyzická vrstva

Fyzická vrstva popisuje elektrické či optické signály používané při komunikaci mezi počítači. Na fyzické vrstvě je vytvořen tzv. fyzický okruh. Na fyzický okruh mezi dva počítače bývají často vkládána další zařízení, např. modemy, které modulují signál na telefonní vedení atp. [2].

1.4.2 Fyzická vrstva

Linková vrstva zajišťuje v případě sériových linek výměnu dat mezi sousedními počítači a v případě lokálních sítí výměnu dat v rámci lokální sítě. Základní jednotkou pro přenos dat je na linkové vrstvě datový rámec. Datový rámec se skládá ze záhlaví (Header), přenášených dat (Payload) a zápatí (Trailer). Datový rámec nese v záhlaví linkovou adresu příjemce, linkovou adresu odesílatele a další řídící informace. V zápatí nese mj. obvykle kontrolní součet z přenášených dat. Pomocí něho lze zjistit, zdali nedošlo při přenosu k porušení dat. V přenášených datech je pak zpravidla nesen paket síťové vrstvy. Z obr. 8 je vidět, že na fyzické vrstvě mohou být pro každý konec spojení použity jiné protokoly. V našem případě jeden konec používá protokol X.21 a druhý konec používá protokol V.35.

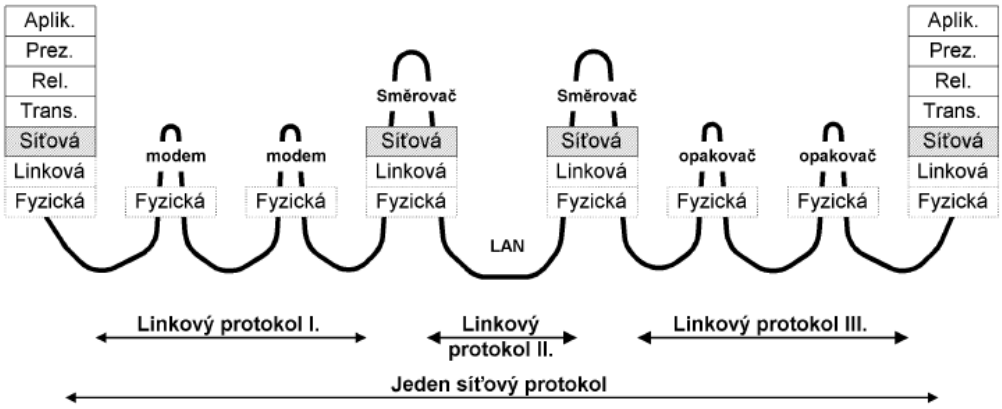
Tento fakt neplatí jen pro sériové linky, ale i pro lokální sítě. U lokálních sítí se ale spíše setkáváme s komplikovanějším případem, kdy mezi oba konce spojení je vložen např. přepínač (Switch), který konvertuje linkové rámce jednoho linkového protokolu na rámce jiného linkového protokolu (např. Ethernet na FDDI), což má pochopitelně za následek i použití jiných protokolů na fyzické vrstvě [2].



Obr. 8. Komunikace na linkové vrstvě [2].

1.4.3 Síťová vrstva

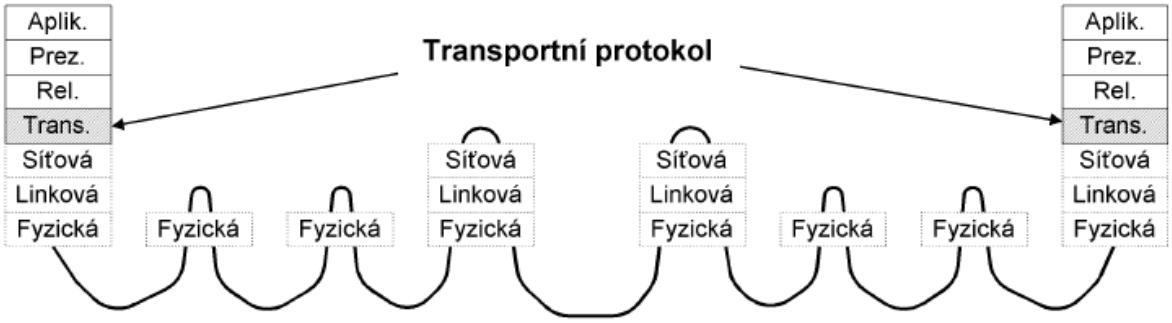
Síťová vrstva zabezpečuje přenos dat mezi vzdálenými počítači WAN. Základní jednotkou přenosu je síťový paket, který se balí do datového rámce. Síťový paket se také skládá ze záhlaví a datového pole. Se zápatím se u síťových protokolů setkáváme jen zřídka. V rozsáhlých sítích (WAN) mezi počítači leží zpravidla jeden nebo více směrovačů. Mezi sousedními směrovači je na linkové vrstvě vždy přímé spojení. Směrovač vybalí síťový paket z datového rámce (jednoho linkového protokolu) a před odesláním do jiné linky jej opět zabalí do jiného datového rámce (obecně jiného linkového protokolu). Síťovou vrstvu příliš nezajímá, jaké jednotlivé linkové protokoly byly na cestě mezi oběma konci spojení použity. Na síťové vrstvě je jednoznačně v celé WAN adresováno síťové rozhraní. Síťovým rozhraním může být např. karta pro Ethernet [2].



Obr. 9. Komunikace na síťové vrstvě [2].

1.4.4 Transportní vrstva

Síťová vrstva zabezpečí spojení mezi vzdálenými počítači, takže transportní vrstvě se jeví jakoby žádné modemy, opakovače, mosty či směrovače na cestě nebyly. Transportní vrstva se zcela spoléhá na služby nižších vrstev. Také předpokládá, že spojení mezi počítači je zajištěno, proto se bez zbytečných starostí může věnovat spojení mezi aplikacemi na vzdálených počítačích. Mezi dvěma počítači může být několik transportních spojení současně, jedno např. pro virtuální terminál a druhé pro elektronickou poštu. Z hlediska síťové vrstvy jsou pakety adresovány adresou počítače (resp. jeho síťového rozhraní). Z hlediska transportní vrstvy jsou adresovány jednotlivé aplikace. Aplikace jsou jednoznačně adresovány v rámci jednoho počítače. Jednotkou přenosu je transportní paket, který se opět skládá ze záhlaví a datové části. Transportní paket se přenáší v datové části síťového paketu [2].



Obr. 10. Spojení na transportní vrstvě [2].

1.4.5 Relační vrstva

Relační vrstva zabezpečuje výměnu dat mezi aplikacemi, tj. provádí tzv. checkpoint, synchronizaci transakcí (commit), korektní uzavírání souborů atd. Dobře představitelnou relací je např. sdílení síťového disku. Disk může být sdílen po určitou dobu, avšak pracuje se s ním jen zřídka. Vždy, když je např. třeba pracovat se souborem na síťovém disku, tak se naváže na dobu od otevření souboru až po jeho uzavření spojení na transportní vrstvě. Avšak relace na relační vrstvě existuje po celou dobu sdílení disku. Základní jednotkou je relační paket, který se opět vkládá do transportního paketu. V literatuře se můžeme často sekat s obrázkem, jak se relační paket skládá z relačního záhlaví a relačních dat a celý relační paket se vkládá do transportního paketu. Od transportní vrstvy výše tomu tak být nemusí. Informace relační vrstvy mohou být přenášeny uvnitř dat. Ještě markantnější je tato situace u prezentační vrstvy, která data např. zašifruje, takže změní celý obsah paketu [2].

1.4.6 Prezentační vrstva

Prezentační vrstva je zodpovědná za reprezentaci a zabezpečení dat. Reprezentace dat může být na různých počítačích různá. Např. se jedná o problém, zdali je nejvyšší bit v bajtu zcela vlevo nebo vpravo atp. Zabezpečením se rozumí šifrování, zabezpečení integrity dat, digitální podepisování atd. [2].

1.4.7 Prezentační vrstva

Aplikační vrstva předepisuje v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů. Např. protokol Virtuální terminál popisuje, jak mají být data formátována, ale i dialog mezi oběma konci spojení [2].

Aplikační	X.400, FTAM, CMIP
Prezentační	X.226, X.216, ASN.1
Relační	X.225, X.215
Transportní	TP 0-4, TP nespoj.
Síťová	X.25, X.75, ISDN
Linková	HDLC, LAPB, ISDN
Fyzická	V.24, V.35, X.21, ISDN

Obr. 11. Některé protokoly z rodiny protokolů ISO OSI [2].

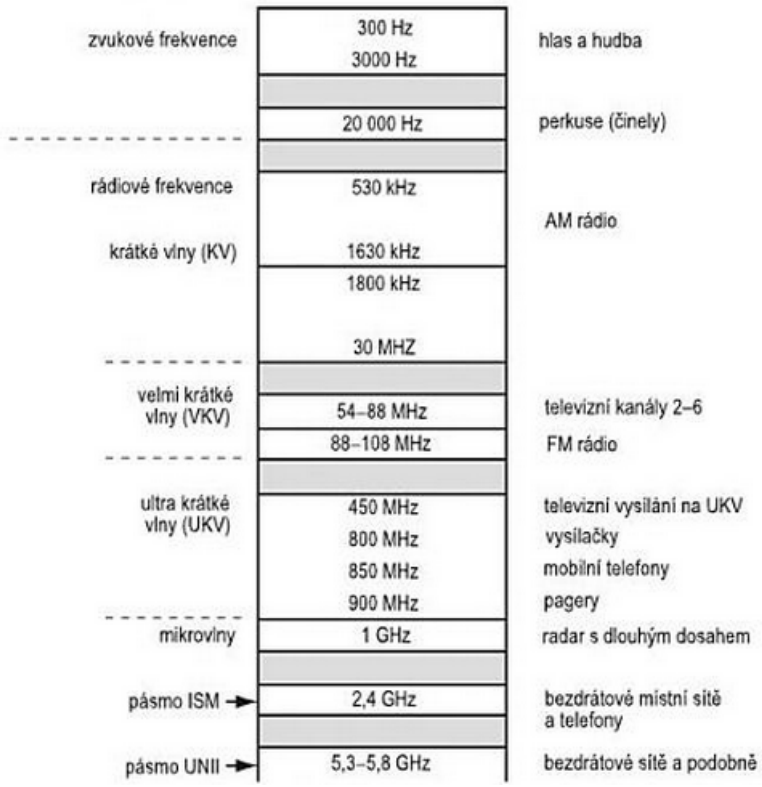
2 BEZDRÁTOVÉ SÍTĚ A IEEE 802.11

Bezdrátové sítě neboli WLAN (Wireless LAN) jsou stále oblíbenější nástroje pro rozšíření sítí na místa, kam se s klasickou kabeláží dostanete jen špatně anebo vůbec. Žádosti o poskytnutí konektivity pro bezdrátové sítě nebo o instalaci sítě jsou u správců sítí a počítačových firem na denním pořádku. Bezdrátové sítě vyrůstají všude tam, kde požadavky pro síť jsou převážně bezdrátového charakteru, nejčastěji připojenými zařízeními jsou notebooky, tablety, smartphony a další bezdrátová zařízení v moderně se rozvíjejících společnostech, které kráčí s dobou. Veškeré standardy pro bezdrátovou komunikaci jsou popsány ve standardu IEEE 802.11. Sítě standardu 802.11 se označují jako Wi-Fi, což je zkratka pro wireless fidelity [3].

2.1 Základy bezdrátových sítí

Pojďme se v rychlosti podívat, jak bezdrátové *sítě* fungují. Bezdrátové sítě data vysílají a přijímají na rádiových frekvencích, tak trochu jako všechna rádiová zařízení. Jediný rozdíl je v modulaci a samotné frekvenci, která je asi 25* vyšší než frekvence rádiového vysílání v pásmu I;M. Bezdrátová zařízení jsou všude kolem nás - od klasického rádia přes televizi až po mobilní telefony; bezdrátové technologie zkrátka používáme každý den. Pro bezdrátové sítě bychom, ale měli vědět něco víc o tom, jak bezdrátové vysílání a příjem funguje. Přenos informací vzduchem (nebo vakuem) se děje pomocí elektromagnetického pole neboli rádiových vln, na které se obsah v podobě zvuku, obrázků nebo dat namodeluje. Elektromagnetické pole je něco jako trojrozměrné vlnky na rybníce - Siří se všemi směry, odráží se od stěn a dalších objektů a nechávají se ovlivnit médiem, kterým zrovna procházejí. Od kovových předmětů se odráží úplně, stejně jako voda od pevných objektů (například přehrady). Jinými předměty, které nejsou příliš silné a neobsahují příliš mnoho železa, rádiové vlny projdou. Při průchodu ale ztratí na síle, dochází k takzvanému útlumu. Jestli si dokážete představit vlnu na rybníce porostlém rákosím, máte docela dobrou představu i o šíření rádiových vln skrz sádrokarton nebo zděnou stěnu či podlahu. Rádiové vysílání většinou probíhá na určité základní frekvenci, které se říká *nosná.* Nosné frekvence jsou národními i mezinárodními zákony rozdělené do *pásem.* Jednotlivá pásma slouží konkrétním službám, například rádiu a televizi, rádiovému vysílání státní správy nebo soukromému rádiovému vysílání. Vysílání v některých pásmech vyžaduje licenci, která může být udělená pro konkrétní frekvenci, nebo může pokrývat celé pásmo. Mezi

licencovaná pásma patří rádio a televize, firemní vysílačky, vysílačky státní správy a většina mikrovlnných spojů. Provoz na jiných pásmech se obejde bez licencí, jen musíte používat schválený vysílač s omezeným výkonem. Sem patří rádio, Family Radio Service (FRS) a samozřejmě i bezdrátové místní sítě typu 802.11 Wi-Fi [3].

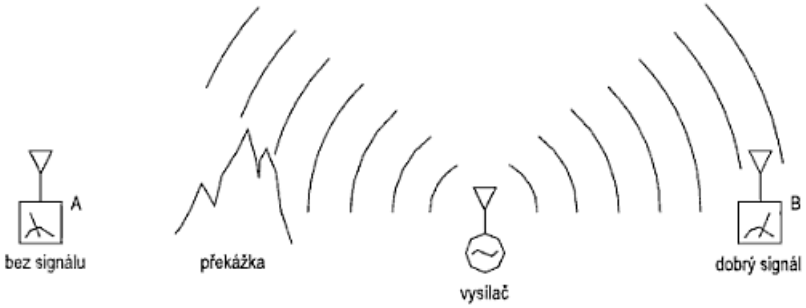


Obr. 12. Běžná rádiofrekvenční pásma [3].

2.1.1 Modulace

Informace přenášená po rádiových vlnách se na nosnou frekvenci přidává takzvanou modulací. Existuje široké spektrum modulací, většina z nich jsou jednoduché variace na amplitudovou nebo frekvenční/fázovou modulaci, někdy s více nosnými. Nejjednodušším příkladem amplitudové modulace je AM (Amplitude modulation) rádlo, u kterého se amplituda zvukového signálu přenáší jednoduše jako změny v intenzitě vysílaného signálu. Naproti tomu u vysílání FM (Frequency modulation) se v závislosti na zvukovém signálu mění frekvence vysílaného signálu. Bezdrátové sítě své vysokorychlostní data na nosný RF (Radio frequency) signál modulují pomocí několika různých variant těchto základních modulačních metod. Mezi oblíbená modulační schémata patří například skokové změny nosné frekvence mezi několika předem vybranými frekvencemi a současné kódováním dat pomocí změn amplitudy i fáze signálu. Tato modulační metoda se až na skákání mezi

frekvencemi podobá modulaci používané u vysokorychlostních modemů. Další modulační technika vysílaný signál digitálně rozptyluje v rámci celé šířky pásma kanálu. Technika skokových změn nosné frekvence a technika digitálního rozmístění signálu se formálně označují jako rozptýlené spektrum [3].



Obr. 13. Přímá viditelnost – rádiové vlny s vysokou frekvencí se nedostanou přes překážky [3].

2.1.2 Antény

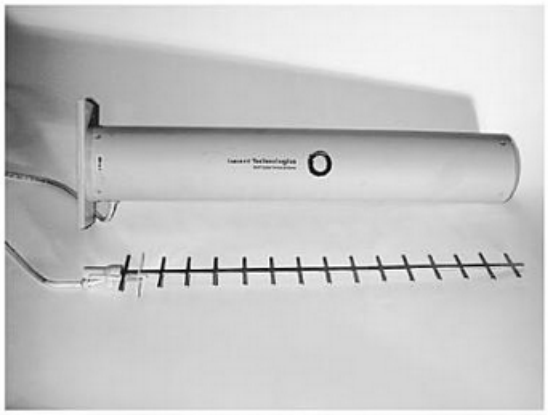
Antény molům být směrové nebo všesměrové. Jako všesměrové se označují antény, které vysílají ve všech směrech stejně. Skutečně všesměrová je ale pouze teoretická jednobodová takzvaná izotropní anténa. Ta by po připojení ke zdroji vysílání veškerou elektrickou energií přeměnila na elektromagnetickou energii a rádiově vlny vyslala na všechny strany. Totéž by provedla i na příjmu, takže ve výsledku by ve všech směrech trojrozměrného prostoru vysílala i přijímala stejné množství energie. Skutečné antény se s touto anténou poměřují a výsledek se udává v decibelech nad nebo pod izotropní anténou, dBi. Dokonalá izotropní anténa by měla 0 dBi [3].

Kvůli optimalizaci přenosu bezdrátového síťového signálu se předpokládá, že většina síťových zařízení bude zhruba paralelní se zemí, například podlahou budovy. Dá se vyrobit anténa, která bude do stran vysílat lépe než nahoru a dolů. Když u takové antény přeměříte sílu signálu přijatého ze stran (vodorovně), dostanete vyšší číslo, než byste dostali u izotropní antény [3].

Tomuto typu antén se běžně říká ziskové antény. Když někdo mluví o všesměrové anténě, většinou má na mysli ziskovou anténu s rovnoměrným ziskem ve všech vodorovných směrech (360°). Tento vodorovný zisk je na úkor zisku v jiných směrech. Všesměrové

antény mají většinou zisk 5-6 dBi. ale dají se postavit i antény s větším ziskem, na úkor zisku v ostatních směrech [3].

Naproti tomu směrové antény mají zisk napřený jedním směrem, vodorovně i svisle. Mezi nejběžnější směrové antény patří Yagi antény a paraboly. Každá z nich vysílá mnohem soustředěnější elektromagneticky signál, který už by se skoro dal označit za paprsek energie. Směr, do kterého se soustředí většina signálu, se označuje jako beamwidtb. Směrové antény pro naše frekvenční pásmo se většinou pohybuji v rozmezí 12-15 dBi, ale parabolické antény se mohou dostat až na dvojnásobek, kolem 25-30 dBi [3].



Obr. 14. Yagi anténa a její kryt [3].

2.1.3 Rozptylování spektra a techniky rozptylování spektra

Rozptylování spektra má v bezdrátových sítích řadu výhod, už z principu je například nenáročné na výkon a odolné proti náhodnému rušení. Na jednu skupinu frekvencí se díky němu vejde větší počet zařízení, stačí frekvence měnit v jiných Časech. Při současném stavu elektroniky jsou i složité RF obvody malé a cenově dostupné [3].

Pro rozptylování spektra existuje několik standardů. Nejčastěji se používají techniky direct sequence spread spectrum (DSSS), quadroture frequency division multiplexing (QFDM) a frequency bopping spread spectrum (FHSS). Systém DSSS se používá pro IEEE 802.11b (Wi-Fi) na frekvenci 2,4 GHz a nabízí propustnost 2-11 Mb/s. Pro standardy 802.11a a 802.11g na frekvencích 2,4 GHz a 5 GHz se používá technika QFDM, která maximální rychlostní limit posouvá na 54 MB/s. FHSS se používá pro Bluetooth a některé starší vybavení standardu 802.11, obojí na frekvenci 2,4 GHz [3].

K přijetí signálu s rozptýleným spektrem je potřeba znát jednotlivé nosné frekvence a přesné pořadí, ve kterém je vysílač bude střídat. Navíc musí existovat ještě nějaký způsob synchronizace začátku posloupnosti. Každý systém, který odpovídá mezinárodním standardům, používá nějakou kompatibilní metodu pro vypočet posloupnosti vysílacích frekvencí a sestavení přijatého signálu [3].

2.1.4 Odolnost proti rušení

Vysílání s rozptýleným spektrem je už z principu tolerantní k náhodnému rušení. Pokud je v libovolném okamžiku na některé z nosných frekvencí přítomny rušivý signál, kódování dat umožní snadnou rekonstrukci původních informací. Běžně se to stává u rušení čistým šumem - jedna konkrétní nosná frekvence může být na okamžik zrušená šumem, ale je nepravděpodobné, že by se nedala použít ani v dalším kole [3].

Pokud je nějaká frekvence rušená neustále a je tudíž nepoužitelná, ideální bezdrátová karta by si toho všimla a jednoduše se jí vyhýbala, takže by snížila datový tok. Tento způsob obcházení rušení je naneštěstí zakázaný předpisy pro rozptylování spektra, ale přesto se některé bezdrátové technologie s dlouhodobým rušením vypořádají lépe než jiné [3].

Rušení a vzdálenost snižují rychlost přenosu dat po bezdrátové síti. Standardy s tím naštěstí počítají a umožňují rychlost snižovat postupně. Někteří výrobci bezdrátových zařízení navíc nabízejí pokročilé techniky zpracování signálu, které snižují ztráty způsobené vícenásobným příjmem. Technika OFDM (Orthogonal Frequency Division Multiplexing) je proti vícenásobnému příjmu odolnější sama od sebe [3].

2.2 IEEE 802.11

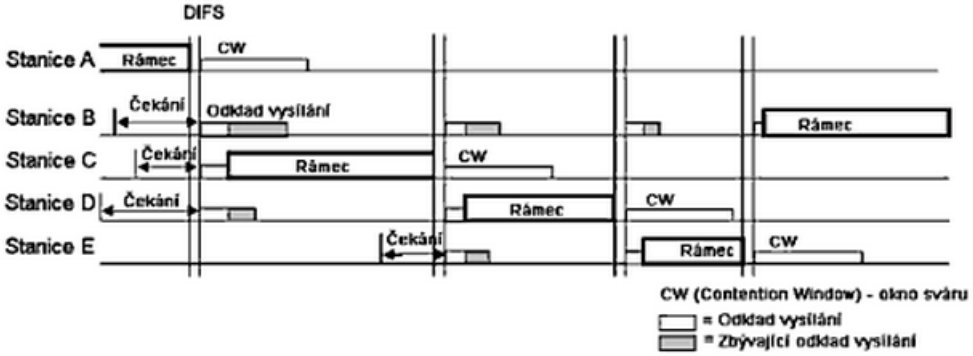
2.2.1 Media Access Control podvrstva linkové vrstvy Wi-Fi

Standard 802.11 definuje dva přístupové metody k médiu - DCF (Disiributed Coordination Function - Funkce rozložené koordinace) a PCF (Point Coordination Function - Funkce bodové koordinace) [4].

Základ všech tří standardů (802.1 a, b, g) tvoří metoda DCF, která je založena na CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - mnohonásobné metodě přístupu s nasloucháním nosné a zabráněním kolizí) a volitelné na RTS/CTS (Request To

Send / Clear To Send). Klient naslouchá sdílené médium, zda nevysílá jiný uživatel sítě. Teprve pokud tomu tak není, začne vysílat, a tím se lze vyhnout většině kolizí. To by ovšem vyžadovalo, aby měli všichni klienti v Čase přesné informace o všech ostatních klientech, což u většiny venkovních bezdrátových sítí nelze s ohledem na konečnou rychlost šíření zajistit. Proto se používá RTS/CTS metoda, kde je každé vysílání zahájeno žádostí (RTS), vysílání je potvrzeno ze strany centrálního bodu (CTS) a tím je zabráněno ostatním ve vysílání. Vše je pak potvrzeno potvrzovacím rámcem ACK. Takto se minimalizuje ztrátovost rámců paketů, ovšem za cenu zvýšené režie provozu. Pro ochranu před kolizemi používá DCF dále dvě techniky. Je to vkládání mezery mezi vysílanými rámci (IFS – InterFrame Space) a odklad vysílání (backoff). Interval DIFS (DCF IFS) odpovídá době povinného čekání po zjištění volného vysílacího kanálu, než může stanice sama začít vysílat. Pokud v této době začne vysílat jiná stanice, musí se vysílání odložit. Interval odkladu si každá stanice generuje sama z intervalu mezi nulou a velikostí tzv. okna potenciální kolize (C\\\ Content Window). Velikost okna potenciální kolize se pří každé kolizi zdvojnásobuje (exponential backoff). Jakmile interval odkladu odezní a médium je volné, může stanice začít vysílat. Příjemce po obdržení rámce čeká po dobu SIFS (Short IFS) a pak vyšle potvrzení přijetí paketu. Mechanizmus je naznačen na obrázku 15. Jeden z problémů, kromě kolizí a absence QoS, je stav, kdy jeden klient „získá“ právo přístupu k médiu. Není stanovený časový limit, kdy musí komunikaci ukončit. Pokud má nízkou rychlost připojení (1 Mb/s), bude mu trvat podstatné déle, než rámec odešle. Tím se zpomaluje celá komunikace a celý přenos dat od všech klientů [4].

Druhou metodu PCF lze použít pouze v infrastrukturní konfiguraci sítě. Tato funkce je volitelná a je velmi zřídka implementována. Přístupové body posílají tzv. „beacon“ rámce v pevně stanovených intervalech (obvykle 0,1 s), které specifikují parametry PCF. Dobu mezi těmito rámci PCF dělí na dva časové úseky, v jednom se používá DCF metoda, tento bývá označován jako CP (Contention Period), ve druhém přístupový bod posílá klientům signál, který klient má právo dále vysílat. Tento úsek je označován jako CFP (Contention Free Period). Ostatní klienti mají zakázáno snažit se o vysílání. Toto je vhodné pro aplikace v reálném čase. Bohužel PCF není dostatečné podporována a má značné limity, protože není stanoven nástroj předání informace o prioritách rámců [4].



Obr. 15. DCF [4].

2.2.2 802.11a – norma pro pásmo 5GHz

Standard označovaný jako 802.11a byl schválen v roce 1999. Využívá bezlicenční pásmo 5 GHz. Jedná se konkrétně o pásmo 5.470-5,725 GHz, kde je k dispozici 11 kanálů s odstupem 20 MHz. Vyzářeny výkon je omezen na 1W e.i.r.p. (equivalent Isotropically radiated power - střední ekvivalentní izotropický vyzářený výkon). Tato hodnota odpovídá nejvyššímu výkonu, pokud je použita regulace výkonu. Pokud zařízení umožňuje automatickou regulaci výkonu nejméně o 3dB, platí limit 1W, ale jinak je výkon omezen na 500 mW e.i.r.p. Teoretická rychlost je 54 Mb/s, skutečná rychlost pak závisí na mnoha parametrech konkrétní rádiové trasy, průměrné se pohybuje v rozsahu 30-36 MB/s. Standard podporuje rychlosti 54, 48, 36. 2-1, 18. 12, 9 a 6 Mb/s a v případě zhoršující se kvality spoje se přenosová rychlost patřičné snižuje, případně naopak při lepších podmínkách se při zvyšující se kvalitě spoje rychlost zvyšuje [4].

Pro dosažení těchto rychlostí se používá ortogonální multiplex s kmitočtovým dělením (OFDM). OFDM je rychlý multiplex, ovšem na druhou stranu jej není možné použít na větší vzdálenosti a v členitém terénu, kde vykazuje horší výsledky než DSSS, které je použito u IEEE 802.11b. Jako skutečnou modulaci lze použít jakýkoliv typ modulace včetně BPSK (Binary Phase-shift keying), QPSK (Quadrature Phase Shift Keying), 16-QAM či 64-QAM (Quadrature amplitude modulation) [4].

2.2.3 802.11b – norma pro pásmo 2,4GHz

Tento standard patří mezi základní nejrozšířenější standardy z rodiny IEEE 802.11. Wi-Fi 802.11b pracuje v bezlicenčním pásmu 2,4 GHz. Toto pásmo bylo ČTU (Český

telekomunikační úřad) schváleno k bezlicenčnímu využití v roce 2000. K dispozici je 13 kanálů, a to od 2,412 GHz do 2,172 GHz, s odstupem 5 MHz. Bohužel jeden kanál má šířku ideálně 20 MHz (až 24 MHz), z čehož můžeme usoudit, že jednotlivé kanály se překrývají. V praxi existují tedy pouze tři kanály, které se nepřekrývají. Vyzářený výkon je omezen na 100 mW e.i.r.p [4].

Norma 802.11b dosahuje rychlosti až 11 Mb/s pomocí tzv. doplňkového klíčového kódování (CCK. Complementary Code Keying) v rámci DSSS modulace na fyzické vrstvě. DSSS je modulace používající matematické kódování. Signál je rozprostřen do širšího spektra, tím je zavedena redundance, která vede ke zvýšení spolehlivosti přenosu dat [4].

Při zhoršení parametrů rychlost přenosu klesá z 11 Mb/s na 5,5 Mb/s, 2 Mb/s, případně až na l Mb/s. Poměrně značnou část teoretické kapacity tvoří režie — 30 až 40%, takže průměrná skutečná rychlost se pak pohybuje kolem 5-6 Mb/s [4].

2.2.4 802.11g – zvýšení přenosové rychlosti v pásmu 2,4GHz

V roce 2003 byla přijata norma pod označením IEEE 802.11g. Hlavní důvodem pro vznik této normy byla nedostatečná rychlost normy IEEE 802.11b. Wi-Fi 802.11g pracuje ve stejném pásmu se stejnými kanály jako 802.11b a je s ní zpětně kompatibilní [4].

Maximální rychlost podle standardu je 54 Mb/s. Aby bylo možné dosáhnout vyšší rychlosti a zároveň kompatibility, používá norma 802.11g DSSS modulaci pro kompatibilitu a OFDM pro dosažení vysoké rychlosti. V podstatě spojuje metody ze standardů 802.11a a 802.11b. Podporované rychlosti jsou závislé na použité modulaci. Dostupné podporované rychlosti pomocí OFDM jsou následující: 54, 48, 36 a 24 Mb/s s pomocí 16-QAM, 18 a 12 Mb/s s pomocí QPSK, 9 a 6 Mb/s s využitím BPSK. Další rychlosti jsou v souladu s 802.11b a používají DSSS (Direct-Sequence Spread Spectrum): 1, 5,5, 2 a 1 Mb/s [4].

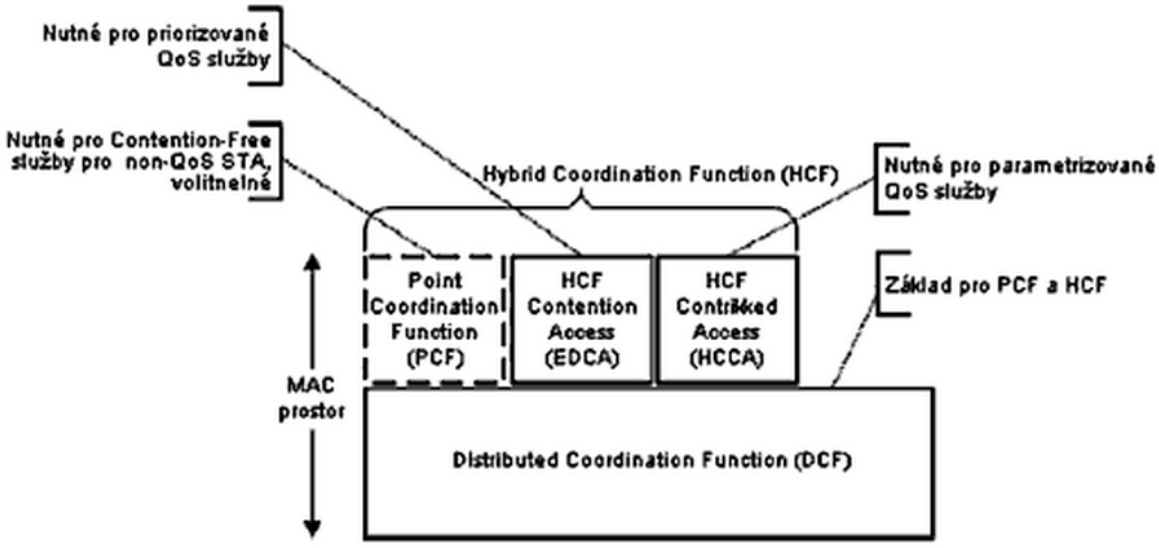
Skutečná rychlost opět závisí na parametrech rádiové trasy a pohybuje se do 30 Mb/s. Zde navíc záleží i na tom, zda do sítě nejsou připojeni i klienti s pomocí standardu 802.11b, jelikož se tím snižuje výkonnost systému a tím i podstatné přenosová rychlost. Systém je nucen přejít na systém požadavků o vysílání, aby se předešlo kolizím na fyzické vrstvě [4].

2.2.5 802.11e – sledování provozu a priorit v síti

Standard IEEE 802.11e, dokončený v září 2005, představuje doplněk pro IEEE 802.11. Doplňuje podporu pro kvalitu služeb (QoS - Quality of Service) a opravuje chyby v podvrstvě MAC (Media Access Control) pro podporu všech fyzických vrstev používaných v IEEE 802.11 sítích. Standard je důležitý pro aplikace citlivé na koncové zpoždění, kolísání zpoždění a šířku pásma, jako je například přenos hlasu (VoIP. Voice over WLAN, VoWLAN, VoWi-Fi, VoFi) nebo přenos videa [4].

Mezi hlavní funkce patří mapování QoS, kde se sleduje provoz a určuje se, s jakou prioritou má být daná část přenesena, dále se sleduje řízení přístupu k médiu, kde se stanoví, zda je možné požadavkům vyhovět, a naposled přidělování síťových prostředku, které se realizuje bud rezervací, nebo upřednostněním provozu [4].

IEEE 802.11e vylepšuje MAC metody DCF (Distributed Coordination Function) a PCF novou hybridní koordinační funkcí HCF (Hybrid Coordination Function). HCF má dvě metody přístupu k médiu, podobné původním metodám. Jedná se o HCCA (HCF Controlled Channel Access) a EDCA (Enhanced DCF vylepšená DCF přístupová metoda ke kanálům). Obě definují třídy provozu (TC, Traffic Classes). Architektura MAC vrstvy standardu je zobrazena na obrázku 16 [4].



Obr. 16. IEEE 802.11e MAC architektura [4].

2.2.6 802.11c – bezdrátové přemostění

IEEE 802.11c je WiFi standard věnující se přemosťování v bezdrátových zařízeních. Jde o hotový standard doplňující standard IEEE 802.1D, který přidává požadavky na přemosťování Media Access Control (MAC), což je podvrstva linkové vrstvy. Standard IEEE 802.1D upravuje základní LAN standard pro 802.11 rámce. Zejména dodává do klauzule 2.5 Support of the Internal Sublayer Service podklauzuli, která pokrývá přemosťovací operace v rámci 802.11 MAC podvrstvy [5].

2.2.7 802.11d – globální harmonizační standard

IEEE 802.11d je Wi-Fi standard často nazývaný také jako globální harmonizační standard. Je používaný v zemích, kde nejsou povoleny systémy používající jiné dodatky k IEEE 802.11 standardu. Definuje požadavky na fyzickou vrstvu k uspokojení regulačních domén nepokrytých existujícími standardy. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu. Specifikace eliminuje nutnost vývoje a výroby specifických produktů pro různé země [5].

Zapnutím podpory pro IEEE 802.11d v přístupovém bodě způsobí, že zařízení začne vysílat do celé sítě (broadcastovat) ISO kód země ve které se nachází jako součást svých beacon paketů a požadavků na odpověď. Pokud je zapnut, klient přizpůsobí své frekvence, vyzařovací výkon a propustnost. Standard je tak vhodný pro systémy, které chtějí poskytovat globální roaming [5].

2.2.8 802.11h – dynamický výběr kanálu

IEEE 802.11h je WiFi standard doplňující IEEE 802.11a, který je navržen s ohledem na evropské podmínky, aby bylo možné sítě využívat mimo budovy. Řeší například problémy s rušením od ostatních zařízení pracujících na 5 GHz frekvenci. Na tomto pásmu pracují například radary nebo některé satelitní systémy. V podstatě mají bezdrátová zařízení v případě, že detekovaly rušení omezit vysílací výkon nebo uvolnit kanál, na kterém toto rušení rozpoznaly. Tento standard upravuje fyzickou vrstvu a podčást linkové vrstvy, takzvanou Media Access Control (MAC) podvrstvu. Dynamickým výběrem kanálu přináší také lepší pokrytí jednotlivých kanálů [5].

2.2.9 802.11n – vylepšení pro vyšší datovou propustnost

Norma 802.11n je nově schválenou normou, používá modulaci OFDM a je tedy zcela legální zařízení podporující novou normu provozovat v rámci všeobecného oprávnění tak jako 802.11a/b/g. Rychlost, kterou zařízení komunikují v normě 802.11n určují tzv. Modulační a kódová schémata MSC. Těchto je definováno celkem 31 a také záleží na šířce pásma, kterou zařízení používá. Standardní šířka pásma u Wi-Fi je 20 MHz, což je jeden kanál. Nová norma umožňuje 40 MHz šířku pásma tedy 2 sousedící kanály. Proto se u zařízení používajících tuto normu objevuje i možnost volby, zda se má k takzvanému řídícímu kanálu připojit nižší nebo vyšší kanál [6].

MSC 8-15 přidává technologii MIMO (Multiple Input Multiple Output) – více vstupů více výstupů, tedy. U těchto schémat konkrétně 2 antény (označováno jako MIMO 2x2). Není to tak, že jedna anténa vysílá a druhá přijímá, ale vždy vysílají a přijímají obě antény [6].

MIMO 3x3 tedy schémata MSC16-23 používá mnoho typů domácích směrovačů, avšak v současné době není příliš znát reálné zvýšení rychlosti a i u těchto směrerů se běžně udává max. teoretická rychlost 300 Mbps, přestože schématu MSC23 odpovídá maximální rychlost 450 Mbps [6].

MIMO 4x4 (MCS24-31). U kódového schématu MSC31 lze dosáhnout max. teoretické rychlosti 600 Mbps, což je strop normy 802.11n [6].

2.2.10 802.11s – Samoorganizující se bezdrátové sítě. (ESS Mesh Networking)

Mesh sítě jsou aplikací sítí typu peer-to-peer do bezdrátového světa, tedy aplikací myšlenky rovnosti a nezávislosti jednotlivých síťových prvků. Zatímco klasická bezdrátová síť je vystavěna tak, že k přístupovému bodu se uživatelé připojují klientským adaptérem, mesh síť tento rozdíl stírá. V mesh síti nejsou přístupové body (pánové) ani klienti (sluhové) - v mesh síti jsou si zařízení rovna (proto taky spojení peer-to-peer) a libovolné mesh síťové zařízení je schopné poskytnout stejnou sadu služeb jako jakékoliv jiné zařízení kdekoliv [7].

Pokud chcete praktický příklad, ukážeme si to na mobilní síti. V mobilní síti máte základnovou stanici BTS (base transceiver station) a k ní je připojený mobilní terminál.

Každý mobil, který chce volat, musí být v dosahu BTS. V mesh síti si signál mezi sebou předávají jednotlivé mesh adaptéry, takže k tomu, abyste se připojil do Internetu, stačí připojit se k mesh adaptéru, jenž má připojení do Internetu - a to klidné i přes jiné mesh adaptéry - vůbec nemusíte být v oblasti pokryté tím připojeným adaptérem, stačí mít možnost přes ostatní mesh adaptéry k tomu cílovému adaptéru „dohopsat“ [7].

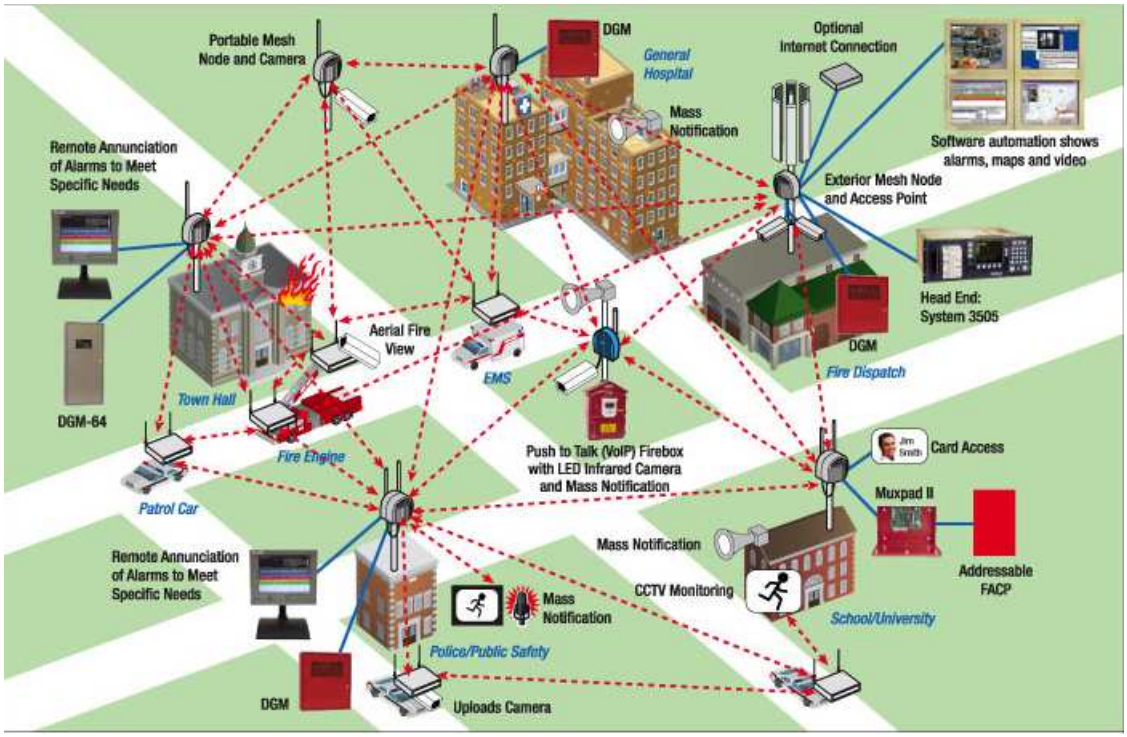
Mesh sítě jsou tedy založeny na takzvaném „ad hoc peer to peer routingu" na směrování provozu mezi rovnocennými adaptéry podle potřeby [7].

U bezdrátových sítí se „mešování“ ujímá především u WiFi, kde také dává značný smysl. Mnoho zařízení připojených do WiFi sítě potřebuje relativně malou šířku pásma, ale nenachází se v dosahu sítě. Mešování signálu z jednoho zařízení na druhé až do Internetu je tedy velmi zajímavá funkce [7].

Mesh sítě mají své výhody:

1) Zastupitelnost - při výpadku (nebo zničení) jednoho prvku mesh sítě ho může jakýkoliv jiný prvek nahradit.
2) Úsporu pásma - v mesh sítích je potřeba méně pásma. Na první pohled to vypadá nesmyslně, jenže je to tak - spojení v mesh síti se sestaví jen tehdy, když je potřeba a na dobu, po kterou je potřeba. V jiných sítích bývá sestavené celou dobu, co jsou zařízení zapojena, protože připojování a odpojování ručně řídí obsluha.
3) Nízké náklady na výstavbu a údržbu - taková síť se jednoduše staví a jednoduše udržuje, protože o všechno základní nastavení se stará směrovací protokol.
4) Zvýšení dosahu sítě díky většímu počtu adaptérů, které mohou předávat signál

Mesh sítě mají jako hlavní nevýhodu fakt, že směrování v nich musí být velmi dobře promyšlené. Kromě toho jsou také náročnější na odběr energie, což muže být u mobilních zařízení problém - nicméně to řeší fakt, že předávání signálu může být v economy módu vypnuto. A do třetice mají problémy se zabezpečením. Mesh síť v případě WiFi znamená používat adaptéry v ad-hoc režimu, tedy nabízet všem dalším vlastně plný přístup k počítači. V takovém případě je nutné kvalitně nastavit zabezpečení počítače, případně se samotný software mesh sítě musí s touto nástrahou vypořádat [7].



Obr. 17. Příklad MESH sítě.

2.2.11 Další neuvedené IEEE standardy

IEEE 802.11f – Komunikace mezi bezdrátovými přístupovými body (2003) Stažen v březnu 2006.

IEEE 802.11i – Vylepšený autentizační a šifrovací algoritmus (WPA2) (2004)

IEEE 802.11j – Dodatek pro Japonsko; nová frekvenční pásma pro multimedia (2004)

IEEE 802.11k – Vylepšení správy rádio zdrojů pro vysoké frekvence. (Navazuje na IEEE 802.11j)

IEEE 802.11l – (rezervováno a nebude použito)

IEEE 802.11m – Správa standardu: přenosové metody a drobné úpravy.

IEEE 802.11o – (rezervováno a nebude použito)

IEEE 802.11p – Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)

IEEE 802.11q – (rezervováno a nebude použito, aby se nepletlo s 802.1Q)

IEEE 802.11r – Rychlé přesuny mezi přístupovými body (roaming) (2008)

IEEE 802.11T – Předpověď bezdrátového výkonu – testovací metody

IEEE 802.11u – Spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi)

IEEE 802.11v – Správa bezdrátových sítí (konfigurace klientských zařízení během připojení)

IEEE 802.11w – Chráněné servisní rámce

IEEE 802.11x – (rezervováno a nebude použito)

IEEE 802.11y – Pro běh ve frekvenčním pásmu 3650 – 3700 MHz (veřejné pásmo v USA)

3 MIKROTIK

Mikrotiky jsou velmi populární u poskytovatelů bezdrátového připojení a ohlasy od uživatelů jsou většinu kladné. Tento seriál bych rád věnoval jejích konfiguraci. Úvodní článek ale bude především o seznámení s možnostmi na této platformě, samotnou konfiguraci si necháme na příští díly.

Často nesprávně se Mikrotikem označuje samotný hardware, ve skutečnosti je to pouze název firmy, která vyvíjí Router OS a RouterBOARDy. Firma vznikla v roce 1995 a sídlo má v Lotyšsku. Vývoji bezdrátových technologií se věnuje již od svého vzniku a za posledních několik let si našla množství příznivců i odpůrců.

RouterBOARD je deska s několika miniPCI sloty, ethernet porty a RS232 konektorem, na které je nejčastěji nahrán tzv. RouterOS a dohromady tvoří velmi výkonný a propracovaný směrovač.

Router OS (ROS) je operační systém využívaný právě na RouterBOARDech. Umožňuje provozovat mnoho věcí od FTP serveru po dynamické směrování. Možnosti jsou opravdu široké a konfiguraci celého zařízení je rychlá a jednoduchá.

Modely RouterBOARDů se liší především výkonem, licencí ROS a možnostmi rozšíření. V neposlední řadě to je také spotřeba a velikost celého zařízení. Některé modely se dají dále rozšiřovat o další miniPCI sloty a ethernetové porty. Největším rozdílem je ale rychlost CPU, která je největším limitem pro připojení klientů na RB [8].

3.1 Mikrotik RouterOS

Základem sítě Internet je protokol TCP/IP. K němu dále patří nespojový protokol UDP a protokol pro diagnostiku ICMP. V souvislosti se svým rozšířením pak Internet vytlačil protokoly, dříve hojně používané v lokálních sítích, jako je NetBEUI či IPX/SPX. Z nichž první jmenovaný neměl ani možnost pracovat ve směrovaných sítích. A právě směrování sítí je hlavním posláním Mikrotik RouterOS. Abychom mohli obsluhovat RouterOS, je nutné mít alespoň základní znalost sítí, síťového modelu ISO/OSI a TCP/IP [8].

MikroTik RouterOS používá až na výjimky zkrácený zápis masky sítě (např. 192.168.1.50/24), uvádím jednoduchou tabulku pro rozsah, kterou byste měli mít v hlavě [8].

255.255.0.0	/16	
255.255.255.0	/24	(prostor "C" – 256 IP adres)
255.255.255.128	/25	
255.255.255.192	/26	
255.255.255.224	/27	
255.255.255.240	/28	
255.255.255.248	/29	
255.255.255.252	/30	
255.255.255.255	/32	(1 IP adresa)

Obr. 18. Příklad IP adres při zadávání do Mikrotiku.

3.1.1 Inicializace RouterOS

Ve chvíli, kdy se vám RouterOS dostane do rukou, je v defaultním nastavení. Při každém startu systému je provedena inicializace a každý podporovaný hardware je okamžitě připraven k použití. V defaultním nastavení jsou všechny zařízení zakázány. Prvotní nastavení je nutné provést přes příkazovou řádku. K té můžete přistupovat přes sériové rozhraní nebo přímo přes konzoli (monitor+klávesnice). Příkazová řádka umožňuje kompletní administraci RouterOS. Ovládání je velmi intuitivní (nedá se mu upřít podobnost s konzolí produktů Cisco) a je vybavena bohatou nápovědou, která se dá kdykoliv vyvolat napsáním otazníku „?“. Přesto předpokládáme, že většině začínajících uživatelů bude bližší grafické rozhraní WinBox. Abyste ho mohli použít, musíte nastavit IP adresu a povolit síťové rozhraní (rozhraní), přes který se k RouterOS připojujete. Pro tyto účely je RouterOS vybaven jednoduchým průvodcem, který spustíte po přilogování k systému (jméno „admin“, prázdné heslo) příkazem / setup, případně dnes lze winbox spustit ještě druhým způsobem a to tím že po připojení k RouterOS lze ve Winboxu načíst MAC adresu daného zařízení, přes kterou se lze připojit do RouterOS [8].

3.1.2 Nastavení rozhraní

V menu interfaces najdete všechny rozpoznané síťové adaptéry (metalické i bezdrátové). Také jsou zde zobrazeny virtuální adaptéry (mosty, IP tunely, virtuální AP). Můžete nastavit vlastní názvy rozhraní, které se poté budou zobrazovat ve všech ostatních nastaveních, velikost MTU, režim ARP, u ethernetových karet rychlost a duplex (10/100 Mbps, full/half duplex, autodetekce), u bezdrátových karet parametry bezdrátové sítě

(SSID, frekvenci, zabezpečení, rychlost atd..). Pod tlačítkem Settings naleznete volbu Wireless Tables, což je tabulka autorizovaných MAC adres pro bezdrátové sítě [8].

3.1.3 Statické směrování

Směrování slouží k určování cest paketů v sítích TCP/IP. V menu ip – routes můžete zadávat statické cesty. Kromě toho zde vidíte dynamické cesty, které se automaticky tvoří ze zadaných IP adres. Jednou ze základních položek je defaultní brána, kterou vytvoříte přidáním statické cesty s Destination 0.0.0.0/0 a vyplněním políčka brána [8].

3.1.4 DNS

Mikrotik RouterOS pro svou práci DNS (Domain Name System) nepotřebuje. Má ovšem zabudován interní DNS server, který je schopen odpovídat na požadavky překladu doménových názvů. K tomu potřebuje mít nastaven nadřazený doménový server. Zodpovězené dotazy si uchovává ve vyrovnávací paměti, čímž zrychluje vyřizování požadavků. Nastavení naleznete v ip – ns – settings. Můžete zde dále zadat statické záznamy, které nebudou překládány, ale přesměrovány dle nastavení statického záznamu [8].

3.1.5 Synchronizace času pres NTP

Přestože na samotný chod směrovače to nemá vliv, je vhodné na něm zajistit aktuální čas. Co například s logovacími soubory, pokud mají zaznamenávané události špatný čas? Pokud používáme funkci system – scheduler, nemá ani smysl o správně nastaveném systémovém čase polemizovat. Ruční nastavení systémového času můžeme provést přes menu system – time. Abychom však pokaždé nemuseli správný čas korigovat ručně, využijeme k tomu automatickou synchronizaci času přes protokol NTP (Network Time Protocol). RouterOS umí s NTP pracovat jako klient i jako server pro ostatní stanice v síti. Veškeré volby naleznete v system – ntp client a system – ntp server. Pro nastavení NTP klienta potřebujeme znát IP adresu serveru, podle kterého provádíme synchronizace [8].

3.1.6 Nastavení DHCP (klient i server)

Mikrotik RouterOS může obsluhovat dynamické přidělování IP adres. Konfigurace DHCP (Dynamic Host Configuration Protocol) serveru sestává z několika kroků: Nejprve je třeba definovat rozsah přidělovaných adres, který lze nastavit v ip – pool. Po přidání položky zvolte název a rozsah požadovaných adres, který můžete zadat ve tvaru např. 192.168.1.100-192.168.1.150, popř. pomocí tlačítka […] můžete přidat jednotlivé IP adresy či více rozsahů. Ostatní nastavení se provádí v ip – dhcp server. Na záložce DHCP definujete nastavení serveru, který adresy přiděluje. Po přidání položky zvolte název, rozhraní, na kterém mají být adresy přidělovány, expirační dobu a rozsah IP adres, který jste definovali v ip – pool. Pokud nechcete přidělovat dynamické IP adresy ale pouze statické, můžete zvolit static-only. DHCP server bude přidělovat pouze adresy definované na záložce Leases. Na záložce Networks nastavíte údaje přidělované DHCP serverem – brána, maska sítě, DNS servery, doménu a servery WINS (Windows Internet Naming Service). Pomocí položky Address nastavíte, jakým IP adresám se mají údaje přidělovat. Na záložce Leases vidíte přidělené IP adresy, popř. jak bylo řečeno výše, můžete zde nastavit statické záznamy i mimo rozsah adres definovaných v ip – pool. Mikrotik RouterOS může pracovat i jako DHCP klient. Nastavení naleznete v ip – dhcp client. Nastavení je jednoduché, klienta pouze zapnete a nastavíte rozhraní, na kterém má být DHCP klient aktivní [8].

3.1.7 Nastavení source NAT

Ve chvíli, kdy jste zprovoznili směrovač pro privátní síť a vnitřní počítače mohou na Internet, většinou potřebujete namapovat některé vnější porty na vnitřní počítače. Mimo jiných případů i tento pokrývá destination NAT (Network Address Translation). Naleznete ho, podobně jako source NAT, v ip – firewall – destination nat. Nastavení není složité [8].

Na záložce general:

Src. address – zdrojová adresa, zde můžete nastavit, že se na daný mapovaný port půjde přihlásit pouze z jedné IP adresy, po př. rozsahu

In. Rozhraní – příchozí rozhraní, můžete ponechat all

Dst. Address – cílová adresa, jedná se o VNĚJŠÍ adresu směrovače, tedy adresu, na kterou se budou hlásit vnější uživatelé. Pokud se jedná pouze o jednu adresu, musí mít masku /32.

Dst. Port – port, na kterém budou požadavky přijímány, může být odlišný od portu vnitřní IP adresy, na kterou se budou požadavky směrovat

Protocol – protokol, na který se má pravidlo aplikovat. Pokud chcete definovat jednotlivé porty, musíte zvolit protokol tcp

Na záložce action:

Action – typ akce, v našem případě to bude nat

To Dst. Addresses – cílové adresy ve vnitřní síti, zadejte do obou políček cílovou adresu

To Dst. Ports – cílový port vnitřní IP adresy

3.1.8 Základní práce s paketovým firewallem

Mikrotik RouterOS disponuje pokročilým firewallem, který umožňuje pracovat s pakety procházející směrovačem. Pravidla pro práci s pakety můžete nastavit v ip – firewall, záložka Filter Rules.

Pravidla ve Filter Rules, jsou rozdělena do tří základních skupin, tzv. Filter Chains:

Input – pravidla aplikující se na pakety, které přichází některým rozhranním a končí na směrovači. Mohou to být např. pingy, administrační pakety (WinBox, ssh) atd…

Forward – pravidla pro pakety, které prochází směrovačem, na tyto pakety se neuplatňují pravidla uvedené v Input či Output

Output – pravidla pro pakety, které vznikly na směrovači a odcházejí některým rozhranním. Mohou to být odpovědi na ping, komunikace s WinBoxem, ssh atd…

Můžete si (např. z důvodu přehlednosti) definovat vlastní Filter Chain. Pokud budete chtít jejich aplikaci, musíte v některém z defaultních Filter Chains definovat pravidlo, které přesměruje datový tok do vašeho Filter Chain. Nastavení takového pravidla naleznete níže.

Pravidlo může být aplikováno na základě následujících podmínek:

Src. address – zdrojová adresa

Src. port – zdrojový port

In. Rozhraní – příchozí rozhraní paketu

Dst. Address – cílová adresa

Dst. Port – cílový port

Out. rozhraní – odchozí rozhraní paketu

Protocol – protokol, na jehož pakety bude pravidlo aplikováno

Content – textový řetězec, který musí paket obsahovat

Flow – značka, kterou paket obdržel při značkování paketů (mangling), značkování paketů je popsané v sekci Bandwidth management

Connection – stejně jako flow

P2P – zahrnutí paketů některého (všech) z vý měnných systémů P2P

Src. MAC Address – zdrojová MAC adresa

TOS – Type of service, typ služby

Limit count, Limit burst, Limit time – omezení funkčnosti pravidla na určitý počet hitů za stanovený čas

S paketem vybraným dle podmínek můžete provést následující akce:

Accept – paket je akceptován a puštěn dál

Drop – paket je zahozen, není generováno chybové hlášení

Reject – paket je odmítnut, směrovač vygeneruje chybové hlášení ICMP

Passthrough – není aplikována žádná akce, pravidlo se chová, jako by bylo vypnuto. Může být použito pro počítání paketů

Jump – provede skok do určeného Chainu

Return – vrátí se do předchozího Chainu [8]

3.1.9 Bandwidth management

MikroTik RouterOS disponuje širokými možnostmi omezování a řízení datových toků. Od omezování jednotlivých IP adres po upřednostňování jednotlivých protokolů, portů, omezování skupin IP adres (sdílené linky).

Omezování se provádí pomocí Queues. Mikrotik rozeznává dva typy Queues: Simple queues a Queue tree. Simple queues se používají pro jednoduché a rychlé nastavení omezení. Jdou použít pouze pro omezení jednotlivých IP adres, popřípadě skupin definovaných síťovou maskou. Queue tree se dají použít pro pokročilé řízení provozu. Základem jejich fungování je označování paketů, tzv. mangling, který se nastavuje v ip – firewall – mangle. Označování paketů je podobné jako zadávání pravidel ve firewallu. Paket se označí na základě daných podmínek. Značkou (flow, connection) se rozumí textový řetězec, kterým je paket označen v rámci směrovače. Pomocí značky můžete s paketem pracovat v různých nastaveních včetně větveného stromu. Můžete označit všechny pakety, které mají cílový port 80 (http) a upřednostnit před ostatními pakety [8].

3.1.10 Diagnostické utility RouterOS

Všechny naleznete v menu tools:

Ping - Základní utilita pro ověření dostupnosti vzdálené IP adresy

Ping MAC - Ověření vzdáleného síťového zařízení na základě MAC adresy, funguje pouze mezi systémy Mikrotik

Traceroute - Na základě zadané IP adresy zobrazí směrovače po cestě k ní

Bandwidth test - Měření propustnosti k jinému RouterOS nebo Windows stanici s běžícím programem Bandwidth tester, ke stažení:

Btest server - Zapíná bandwidth server pro vzdálené klienty, opačný případ předchozí utility

Packet Sniffer - Utilita pro odchytávání paketů, možnost zobrazení ve WinBoxu nebo přesměrování na jiný stroj

Torch Monitorování - aktuálního provozu s možnostmi zobrazování dle kritérií (zdrojová IP adresa, port, protokol, cílová adresa)

Mac Server - Nastavení služby mac telnet, obdoba klasického telnetu běžícího na základě mac adres, pouze pro mikrotik, k dispozici klient pro windows

Ping Speed - Orientační výpočet rychlosti linky na základě příkazu ping

Flood ping - Odeslání velkého počtu pingů o dané velikosti

Netwatch Monitoring - dostupnosti IP adres v síti, možnost spuštění libovolného skriptu při událostech UP/DOWN [8]

3.1.11 Lokální a vzdálené logování událostí

Seznam událostí, které RouterOS dovoluje logovat, naleznete pod menu system – logging. U každé z událostí máte možnost nastavit čtyři druhy zacházení se vzniklým záznamem:

None - Ignoruje jakoukoliv událost

Memory - Zaznamená událost do paměti, která je pak přístupná přes menu Log. Záznam událostí je při každém rebootu smazán

Disk - Zaznamenává události na CF. Tato možnost se striktně nedoporučuje vzhledem k omezenému množství zápisů na CF. Snižujete tak její životnost

Remote - Logování událostí na vzdálený Syslog server. Tím může být například Linuxový Syslog (spuštěný s volbou „-r“) nebo některá z Windows alternativ. Windows Syslog server přímo od Mikrotiku [8]

3.1.12 Export, import a zálohování konfigurace

Konfigurace routeru může být kompletně zálohována pomocí funkce /systém backup save name <název_souboru>. Pokud není zadán název souboru, RouterOS vygeneruje název z data a času vytvoření zálohy. Záloha může být také vytvořena ve WinBoxu ve files – backup. Obnova se může provést buď /system backup load name <název_souboru>, nebo o pět z WinBoxu files – restore poté co kliknete na příslušný soubor zálohy. RouterOS poté vyžaduje restart. Pokud provádíte obnovu zálohy na stejném stroji, obnova se provede v plném rozsahu. Pokud obnovu provádíte na jiném stroji, s největší pravděpodobností se neobnoví správně rozhraní, které pak musíte dokonfigurovat ručně [8].

3.1.13 Export, import a zálohování konfigurace

Mikrotik RouterOS je možné (v případě, že vám to umožňuje licence) upgradovat či downgradovat na libovolnou minoritní verzi. Downgrade doporučujeme používat pouze v případě, kdy jste si jisti, že daná vyšší verze obsahuje chybu, která v nižší verzi nebyla. Upgrade i downgrade se provádí podobně, kopírováním příslušných balíčků na směrovač. V případě upgrade stačí pouze provést reboot, buď pomocí příkazu, nebo za pomocí Ctrl+Alt+Delete na konzoli. Downgrade se musí provést ručně příkazem /system package downgrade. V obou případech zůstane na směrovači zachována konfigurace. Avšak i přes vysokou spolehlivost tohoto procesu se doporučuje provést zálohu konfigurace [8].

3.1.14 Reset do defaultního nastavení

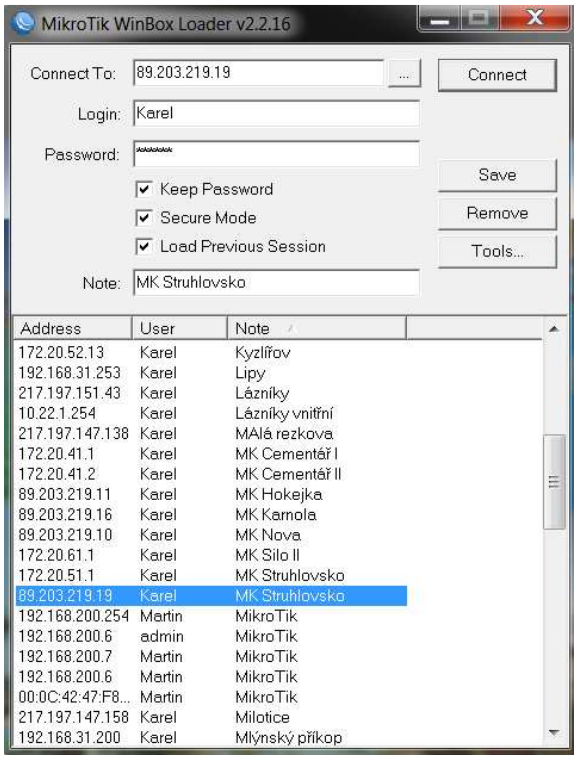
Reset provede výmaz všech nastavení a uvedení RouterOS do defaultního stavu, kdy nejsou zaktivovány ani žádné síťové rozhraní. Proto jej provádějte, pokud máte přístup k lokální administraci, tedy přes klávesnici nebo sériové rozhraní.

Příkaz:

/ system reset [8]

3.2 Winbox

Winbox je konzole, přes kterou přistupujeme k směrovačům Mikrotik. Díky této konzoli lze jednotlivá zařízení používající RouterOS konfigurovat a spravovat. Nabízí grafické rozhraní GUI. Funkce Winboxu se snaží přiblížit co nejvíce běžně používaným funkcím, které umožňuje správa RouterOS přes konzoli. Většina běžných a konfigurovatelných funkcí, které jsou v RouterOS správcovatelná a lze je díky grafické nástavbě Winbox použít jsou popsána v předchozím výkladu, kde jsme se seznamovali s Mikrotikem.



Obr. 19. Winbox.

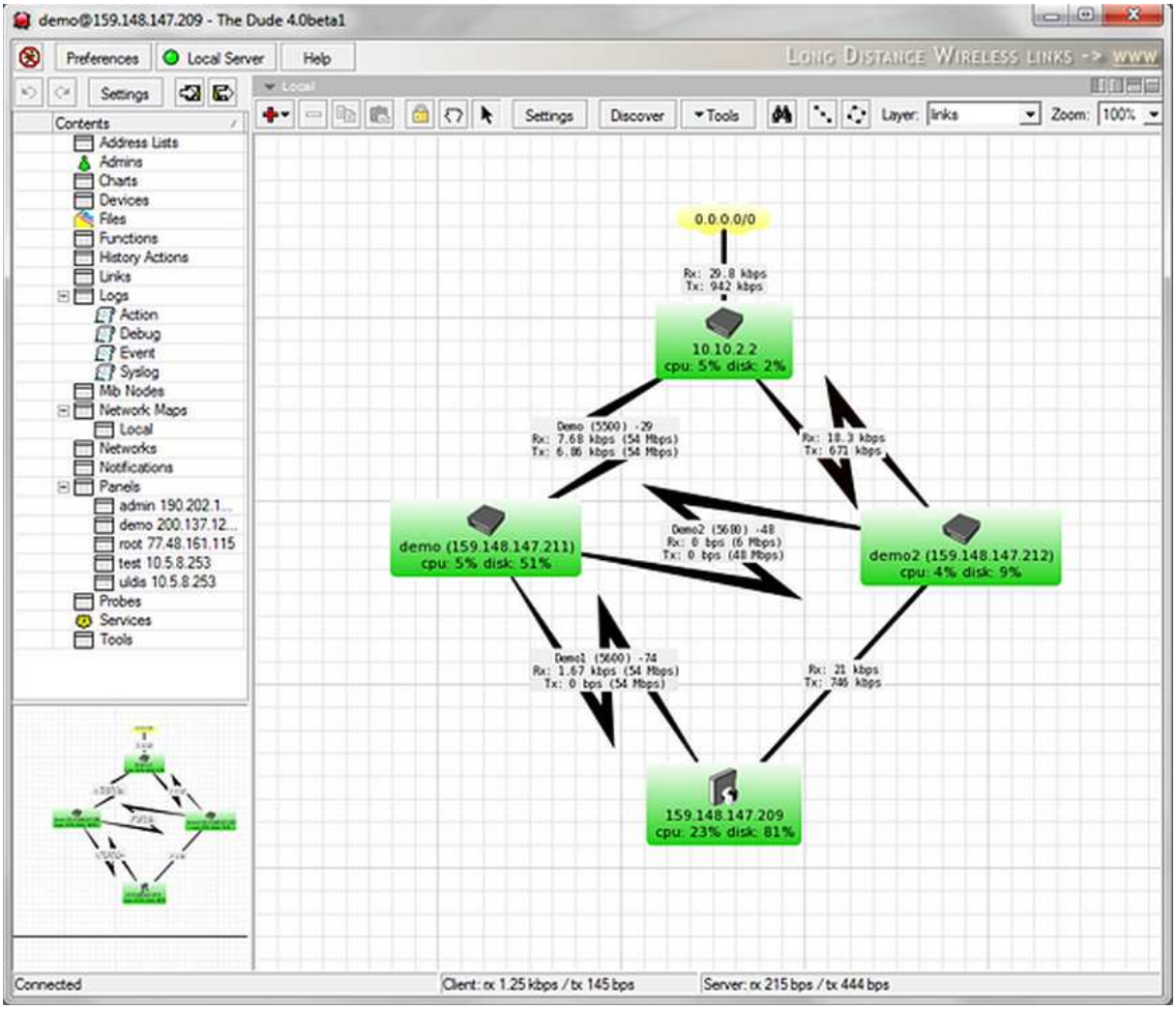
Na obrázku 19 lze vidět okno Winboxu, do řádku Connect To zadáváme IP adresu zařízení, v případě, že IP adresu neznáme a jsme k zařízení fyzicky připojení a chceme jej konfigurovat, tak rozklikneme rozšířenou nabídku vedle této záložky, kde se nám zobrazí síťová MAC adresa připojeného zařízení v síti, na základě které se do daného zařízení dostaneme, abychom jej mohli konfigurovat.

Každé zařízení má defaultní nastavení s přihlašovacími údaji jako login: Admin a password zůstává prázdné. Na obrázku 19 vidíme již změněné údaje loginu. Každý nový login lze uložit a vytvořit tím tabulku loginů pro rychlejší správu. Tlačítkem Save nový login uložíme, tlačítkem Remove smažeme. Pod položkou tools se skrývá nabídka, která nám může smazat celý seznam adres, případně importovat, či exportovat seznam do souboru a vytvořit tak efektivní zálohu přihlašovacích údajů k zařízením ve své síti.

3.3 The Dude

The Dude je bezplatná Aplikace od společnosti Mikrotik, která vylepšuje správu síťového prostředí. Lze do ní zaznamenat graficky veškerá zařízení v síti, kreslit podsítě, monitorovat jednotlivé služby na svých zařízeních a v případě, že některá služba má problém, tak vás tento program upozorní na tento problém. Nejen, že můžete sledovat

samotná zařízení, můžete je taktéž řídit. Díky této aplikaci lze provést hromadné upgrady RouterOS, konfigurovat RouterOS přímo s The Dude.



Obr. 20. Spuštěný program Dude s příkladem sledování sítě.

Jak již bylo řečeno, tak program The Dude slouží převážně pro monitoring RouterOS sítě, nejčastější používané funkce jsou ping, díky této funkcí víme, zdali je síť v pořádku a všechna zařízení jsou připojena. Dále měření propustnosti sítě a zaznamenávání toků v čase, neméně důležitou funkcí je sledování zátěže CPU jednotlivých Mikrotiků, jelikož každá ze sledovacích funkcí má vliv na CPU mikrotiku, tudíž je potřeba sledovat zatížení těchto strojů, pakliže je zatížení CPU vysoké, mikrotik se začíná stávat nespolehlivým a má tendence se zaseknout. Většinou se nastavuje automatický watchdog, ale někdy v praxi nepomáhá.

II PRAKTICKÁ ČÁST

4 HARDWARE

V této části si ukážeme použitý hardware a schémata jednotlivých zapojení, na kterých bylo prováděno testování.

4.1 Použitý HW pro testování

4.1.1 Kroucená dvojlinka – kabeláž UTP s konektorem RJ45

V současné době existují dva typy kroucené dvojlinky.UTP, jehož použití je velmi rozšířeno u většiny síti LAN, a STP, který se používá v prostředích náchylných k elektromagnetické interferenci. Kroucená dvojlinka se skládá z osmi samostatných zapouzdřených měděných vodičů. Těchto osm vodičů je uspořádáno do čtyř párů a každý pár je barevně odlišen podle standardu 568. Vodiče jsou krouceny v různých úrovních, aby se předešlo vzájemnému rušení i vlivům z vnějších zdrojů.

Organizace TIA (Telecommunications Industry Association) a EIA (Electronics Industry Association) vyvinuly standard TIA/EIA-568, který definuje různé úrovně (označované jako kategorie) kabelů UTP. Čím vyšší je hodnocení kategorie, tím efektivněji a rychleji může kabel data přenášet. Rozdíl mezi kategoriemi spočívá v těsnosti kroucených párů linek. S výjimkou protokolů 100BaseT4 a 1OOBaseVG-AnyLAN používají sítě Ethernet v kabelu UTP obvykle pouze dva ze čtyř párů linek — jeden pro přijímání a jeden pro odesílání dat. I když nemusí být použity všechny čtyři páry linek, nemůžete zbylé dva páry použít pro jinou aplikaci, jako je například telekomunikační provoz. Posílání signálů prostřednictvím dvou nevyužitých párů linek by pravděpodobně vedlo ke zvýšení zatížení linek, čímž vzrůstá riziko potenciální ztráty dat a ohrožení signálu [1].

Obr. 21. Příklad UTP s RJ45.

4.1.2 1 x Mikrotik RB411AH

RouterBoard RB411AH narozdíl od RB411A zvyšuje takt procesoru na 680 MHz a tím i zvyšuje propustnost. RB411AH je ideální pro použití jako AP nebo jako klientská jednotka

funkce: statické přidělování adres a směrování, router advertisement daemon (pro autokonfiguraci adres), dynamické směrování: BGP+, OSPFv3, a RIPng protokoly, firewall (filter, mangle, address lists), DNS, 6in4 (SIT) tunely, telnet, ping, traceroute, web proxy, nástroje sniffer a fetch

Specifikace:

Název	**Hodnota**
Operační mód:	AP, Client, Bridge, WDS
DHCP:	ano
Regulace výkonu:	ano - po 1dB
LAN port:	1x 10/100 Mbit/s
Výchozí jméno:	admin
Napájení:	JACK + POE (10-28 V)
Provozní teplota:	-20 až 60 °C
Rozměry:	105 x 105 mm
Rozhraní:	LAN, WiFI
Procesor:	Atheros AR7130 680 MHz
RAM:	64 MB DDR SDRAM
NAND:	64 MB
Sloty:	1x miniPCI
Hmotnost:	0.09 Kg

I/O Control:	1x serial port DB9 RS-232C
LED indikace:	ano
OS:	Mikrotik - RouterOS Level 4
Podpora IPv6:	Plná

Obr. 22. RB411AH.

4.1.3 2 x Mikrotik RB433

MikroTik RouterBOARD RB433 3xLAN 3x miniPCI. Skvělá platforma pro zprovoznění bezdrátové technologie.

funkce: statické přidělování adres a směrování, router advertisement daemon (pro autokonfiguraci adres), dynamické směrování: BGP+, OSPFv3, a RIPng protokoly, firewall (filter, mangle, address lists), DNS, 6in4 (SIT) tunely, telnet, ping, traceroute, web proxy, nástroje sniffer a fetch

Specifikace:

Název	**Hodnota**
Operační mód:	AP, Client, Bridge, WDS
DHCP:	ano
Regulace výkonu:	ano - po 1dB
LAN port:	3 x RJ45 10/100 Mbps MDI/MDI-X
Výchozí jméno:	admin
Napájení:	JACK + POE (16-28 V)
Provozní teplota:	-20 až 60 °C
Rozměry:	150 x 105 mm
Rozhraní:	LAN, WiFI
Procesor:	MIPS 300 MHz
RAM:	64 MB SDRAM
NAND:	64MB
Sloty:	3x miniPCI
Hmotnost:	0.3 Kg
I/O Control:	1x serial port RS-232
LED indikace:	ano
OS:	Mikrotik - RouterOS Level 4
Podpora IPv6:	Plná

Obr. 23. RB433.

4.1.4 1 x Mikrotik RB750G

RouterBoard RB750G konstrukčně vychází ze směrovače RB750. Oproti němu má rychlejší procesor (680 MHz), novější verzi RouterOS Mikrotik (v4) a plně gigabitové porty. Stejně jako RB750 je dodáván včetně krytu a zdroje. RouterBoard je možné napájet nejen pomocí klasického konektoru jack, ale také přes **PoE** (k tomu je určený **PORT 1**, ostatní porty POE napájení nepodporují).

funkce: statické přidělování adres a směrování, router advertisement daemon (pro autokonfiguraci adres), dynamické směrování: BGP+, OSPFv3, a RIPng protokoly, firewall (filter, mangle, address lists), DNS, 6in4 (SIT) tunely, telnet, ping, traceroute, web proxy, nástroje sniffer a fetch

Specifikace:

Název	**Hodnota**
DHCP:	ano
LAN port:	5 x RJ45 10/100/1000 Mbps MDI/MDI-X
Výchozí jméno:	admin
Napájení:	JACK + POE (10-28 V)

Provozní teplota:	-20 až 60 °C
Rozměry:	113 x 89 x 28 mm
Rozhraní:	LAN
Procesor:	Atheros AR7161 680MHz
RAM:	32 MB SDRAM
NAND:	64MB
Hmotnost:	0.142 Kg
LED indikace:	ano
OS:	Mikrotik - RouterOS v3 Level 4
Podpora IPv6:	Plná

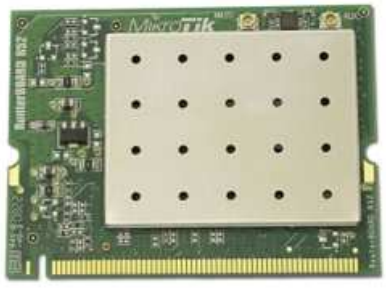
Obr. 24. RB750G.

4.1.5 3 x R52 miniPCI bezdrátová karta

Bezdrátová karta podporuje pro pásmo 2,4 i 5GHz podporují systémy Mikrotik i StarV3.

Specifikace:

Název	**Hodnota**
Operační mód:	AP, Client, Ad-HOC
Frekvence:	2.4, 5 GHz
Přenosová rychlost:	54 Mbps
Normy:	802.11a/b/g
Chipset:	Atheros AR5414
Výstup na ext. anténu:	2 x U-FL male
Regulace výkonu:	ano (Mikrotik, STAR-OS, StarV3)
Max. výstupní výkon:	a: 17, b: 19, g: 18 dBm
Citlivost:	-95 (1 mbps) až -71 (54 mbps) dBm
Modulace:	DSSS, OFDM
Šifrování:	WEP 64/128, WPA, WPA2, 802.1X
Shoda:	FCC, CE
Provozní teplota:	0 - 50 °C
Rozhraní:	miniPCI
Podporované OS:	MikroTik RouterOS, Windows, Linux
Spotřeba:	max.: 1320 mW
Hmotnost:	0,012



Obr. 25. R52 miniPCI bezdrátová karta.

4.1.6 Další použitá zařízení pro testování

1 x Notebook Lenovo Ideapad s205

1 x Notebook Asus F3KA

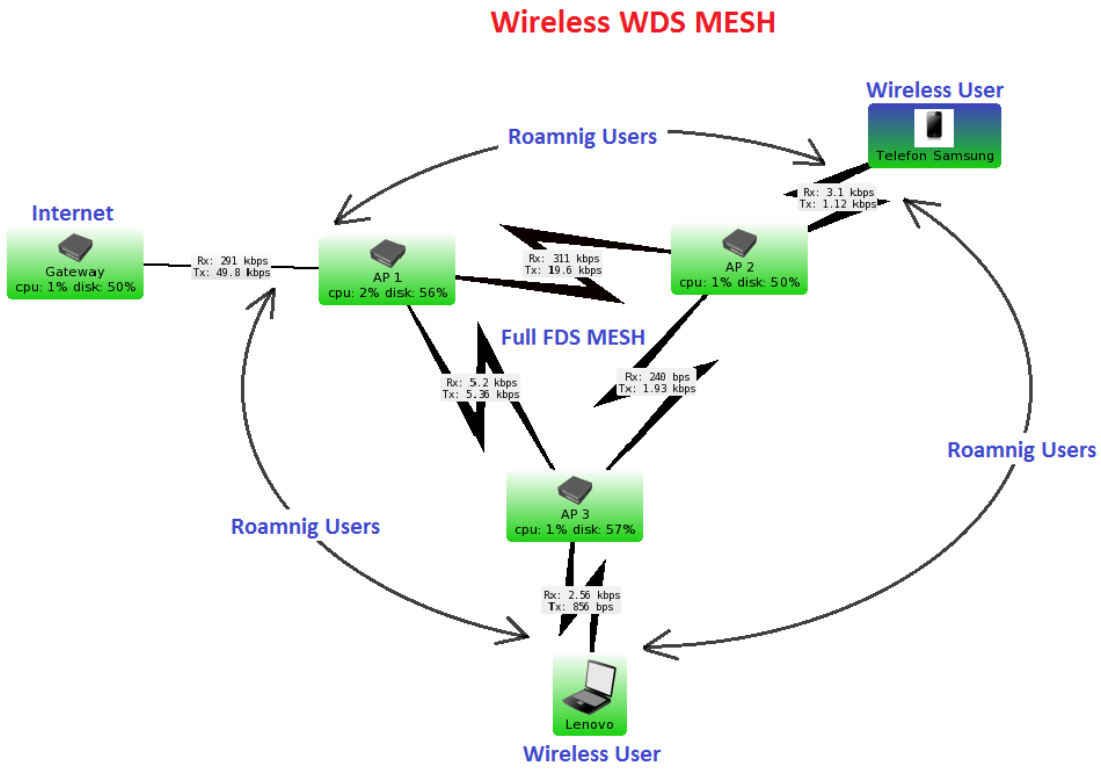
1 x Mobilní telefon Samsung Galaxy Ace

3 x 5dBi anténa

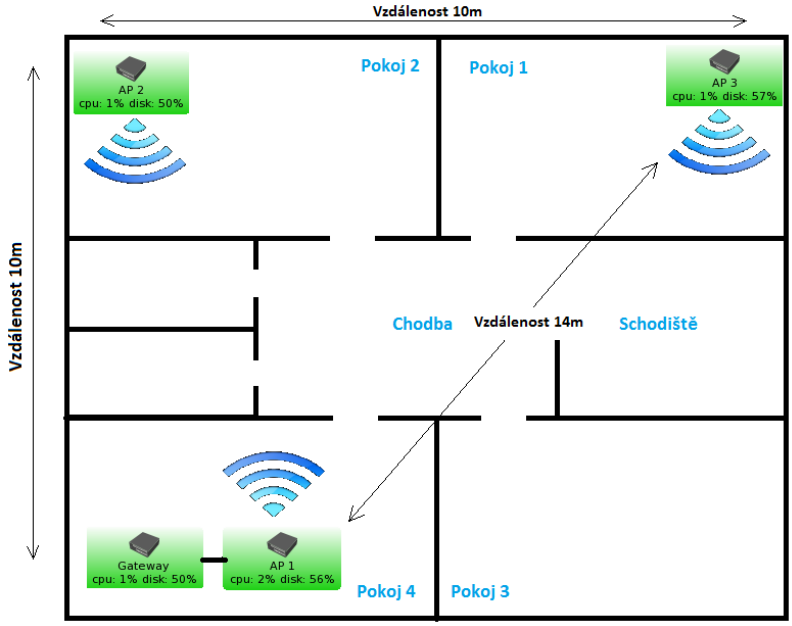
1 x Cisco USB 802.11a,b,g,n bezdrátový adaptér – označení Linksys AE1000

4.2 Schéma zapojení pro testování provozu

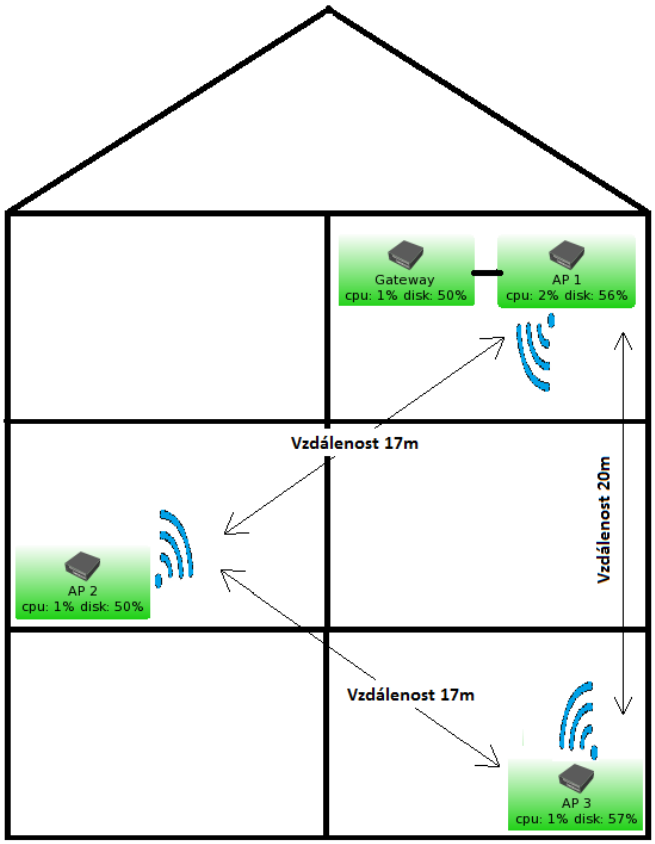
Jak již bylo zmíněno, tak MESH síť se v podstatě chová jako mobilní síť, v případě výpadku jednoho AP (Access point) se automaticky všechna připojená zařízení v síti připojí na funkční jednotky, pakliže jsou v signálovém dosahu. Uživatelé využívají tzv. roaming v síti. Pro testování sítě byla použita struktura na obrázku 26. Testovací provoz byl prováděn ve velkém rodinném domě (sídlo společnosti), využitelnost tohoto řešení je nejen v hotelích, velkých firmách, kde je kladem důraz na spolehlivost sítě nebo venkovních řešeních za předpokladu, že v dané lokalitě nebude Wi-Fi síť zarušena . První série testů byla prováděna v rámci jednoho patra, přičemž vysílače byly rozmístěny v různých pokojích, vzdáleny od sebe od 10m do 14m viz. obrázek 27. Tyto testy měly ověřit kolísání rychlosti a stabilitu sítě, funkčnost MESH sítě, přepojování na další AP v síti. Druhá série testů byla prováděna v rámci pater domu, přičemž byl kladen důraz na minimální frekvenční obsazenost sítě v rámci jednoho frekvenčního pásma a to z důvodu především zarušení. Testy, které se v rámci tohoto pokusu dělaly, byly stejné jako v prvním případě, nicméně uvážíme-li vzdálenosti jednotlivých AP od řídícího AP, tak hlavní prioritou této zkoušky bylo dokázat, že lze signál šířit jednotlivými přeskoky v MESH síti sériově aniž by kvalita signálu a datová propust zakolísala. Šíření v rámci pater viz. obrázek 28.



Obr. 26. Wireless WDS MESH.



Obr. 27. Test v rámci patra.



Obr. 28. Test v rámci pater domu

5 NASTAVENÍ MIKROTIKU A TESTOVÁNÍ MESH SÍTĚ

V této části diplomové práce se seznámíme se základním nastavením Mikrotiku, provedeme nastavení WDS (wireless distribution systém) MESH sítě a provedeme testovaní naší MESH sítě.

5.1 Nastavení MESH na Mikrotiku

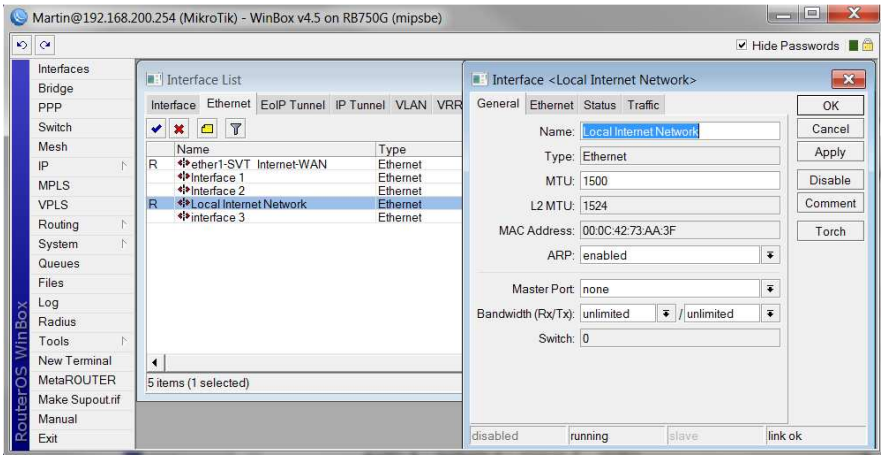
5.1.1 Nastavení v RB750G (brána)

Nejprve na RB750G vytvoříme lokální síť. MESH síti v této lokální síti přidělíme IP adresu, která bude tvořit brána pro MESH síť. Díky tomuto statickému přidělení IP adresy lze díky funkci Queues omezovat a řídit tok dat v MESH síti.

Postup:

Po otevření programu winbox nejprve pojmenujeme rozhraní, všechny rozhraní, kterým daný mikrotik disponuje se načtou automaticky.

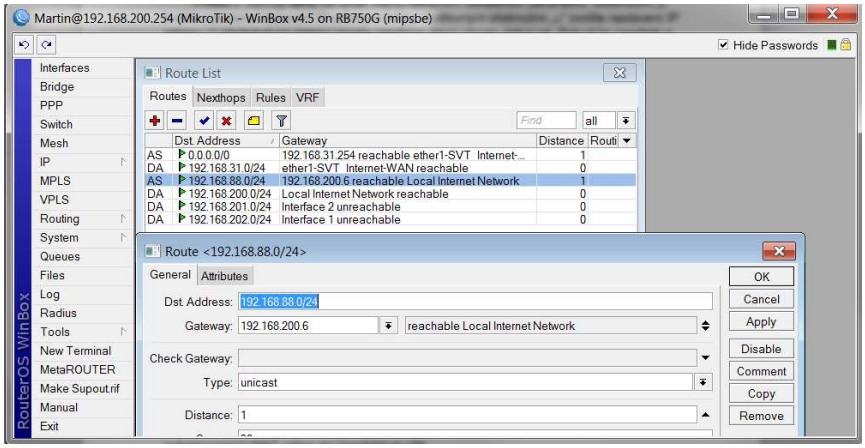
Rozhranís -> rozklikneme příslušný rozhraní -> General -> Name (v našem případě Local Internet Network, viz. obrázek 29)



Obr. 29. Rozhranís.

Dále nastavíme statické cesty, díky kterým lze do sítě MESH přistupovat. Předpokládá se, že v Mikrotiku již je vytvořena defaultní brána 0.0.0.0/0.

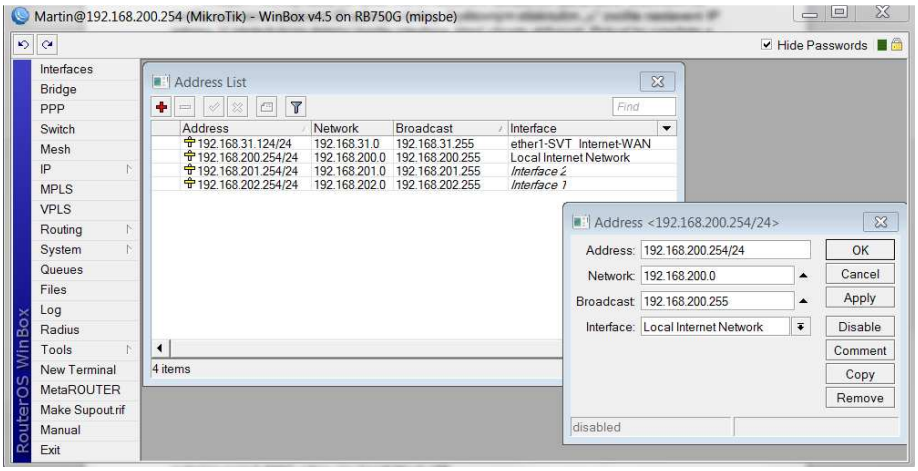
Založka IP -> Routes -> + -> General -> Dst. Address (zde zadáme naši cílovou síť) -> Getaway (zde zadáme IP adresu, ze které do sítě budeme přistupovat, postup viz. obrázek 30)



Obr. 30. Statické cesty.

Dále je potřeba pro inicializaci sítě nastavit Address List.

Záložka IP -> Addresses -> + -> a vyplnit viz. obrázek 31, to znamená zadat adresový rozsah sítě, broadcast, rozhraní, který přísluší dané síti a síťovou adresu AP1. Poté, co se vytvoří adresové rozsahy jednotlivých sítí, tak si můžete všimnout, že v předchozí záložce Routes přibudou další záznamy. Nezapomeňte správně v záložce Addresses nastavit rozhraní na jednotlivých záznamech, které budete přidávat. Např. dle obrázku 31 pro adresu 192.168.200.254/24 je rozhraní Local Internet Network.

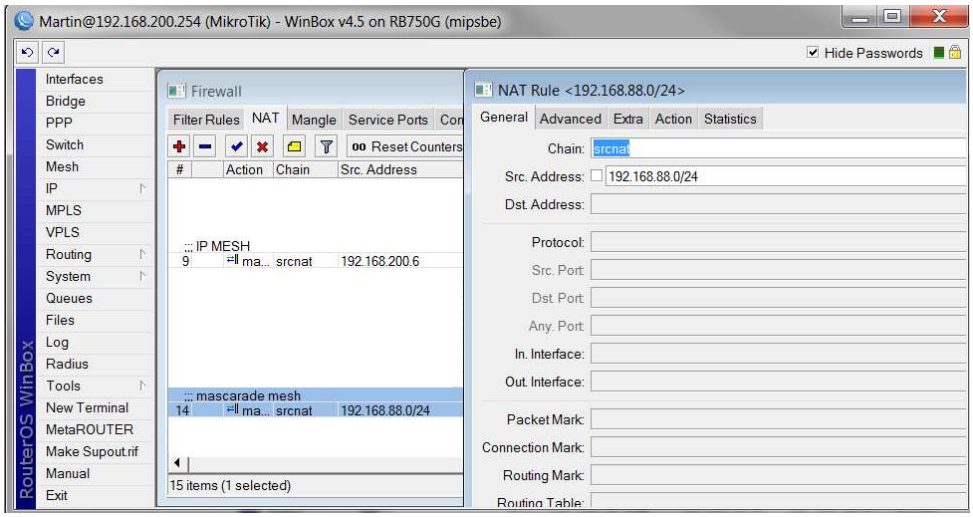


Obr. 31. Addresses.

Dále je potřeba nastavit pokročilejší pravidla a to jsou pravidla firewallu. Ve firewallu je potřeba povolit komunikaci IP adresy, která tvoří bránu pro MESH síť, dále je potřeba

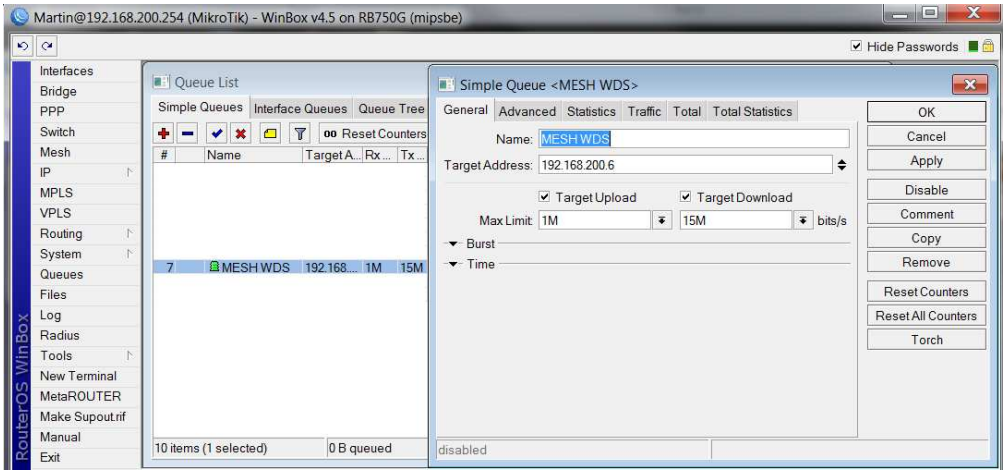
povolit komunikaci pro všechny IP adresy v MESH síti. Na obrázku 32 vidíte naši bráně pod adresou 192.168.200.6 a všechny adresy v MESH síti pod 192.168.88.0/24 .

IP -> Firewall ->NAT -> + -> záložka General, v ní zadáme Chain, většinou na srcnat, druhá možnost se používá v případě směrování veřejné IP adresy, dále zadáme Src. Address, pro bránu 192.168.200.6, pro IP adresy MESH sítě 192.168.88.0/24, nesmíme zapomenout na záložku Action, kde v obou případech zadáme masquerade, toto pravidlo říká, ať se všechny vnitřní IP adresy schovají za adresu poskytovatele.



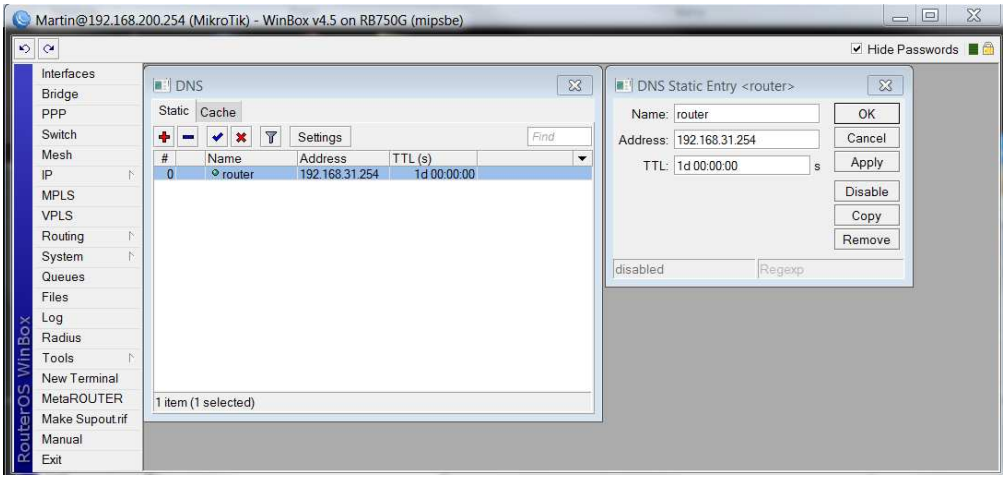
Obr. 32. Firewall.

Dále nastavíme v záložce Queues omezení pro naši MESH síť, klikneme na přidej, vyplníme Name, v záložce Target Address zadáme naší IP adresu, tedy 192.168.200.6 a nastavíme Target Upload, Target Download, viz. obrázek 33.



Obr. 33. Queues.

Jako poslední přidáme server DNS v záložce IP -> DNS -> + -> vyplníme Name, Address, což je v tomto případě adresa DNS serveru.



Obr. 34. DNS.

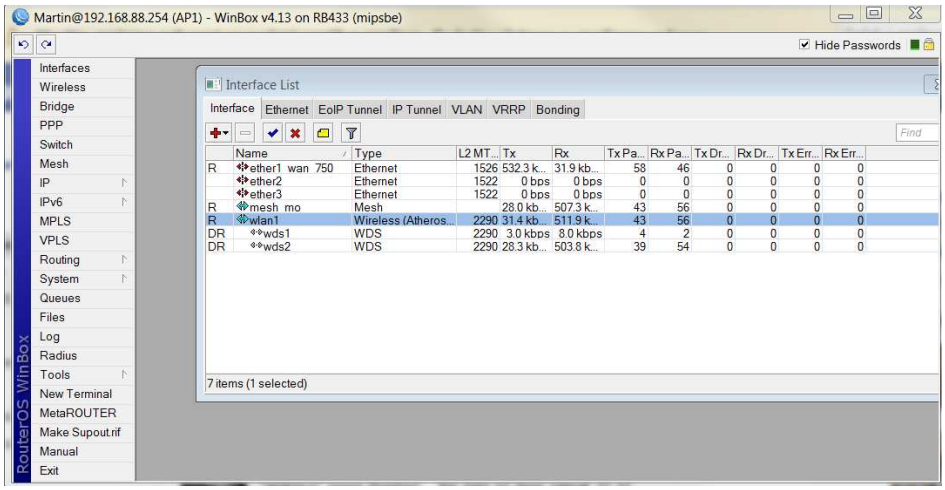
RB750G je v tuto chvíli připraven plnit dle našeho schématu úlohu brány (Gateway).

5.1.2 Nastavení v RB433 (AP1 – řídící AP MESH sítě)

RB433 v našem případě taktéž dle schématu AP1 představuje řídící AP celé MESH sítě. V případě výpadku tohoto AP naše MESH síť nespadne, ale nebude možné se připojit k internetu, řešit by se tento problém dalo přivedením konektivity do jednoho ze zbylých AP, které by tvořilo tzv. záložní internetovou jednotku a tím zvýšit spolehlivost celé sítě. Připojení k internetu bude ztraceno z důvodu, že na AP1 je nastaveno dynamické přidělování IP adresy. V případě výpadku AP1 nelze dynamicky přidělit IP adresu, síťové zařízení zůstane připojeno na funkčním vysílači, nicméně nebude možné pracovat v síti, dokud se řídící jednotka neopraví.

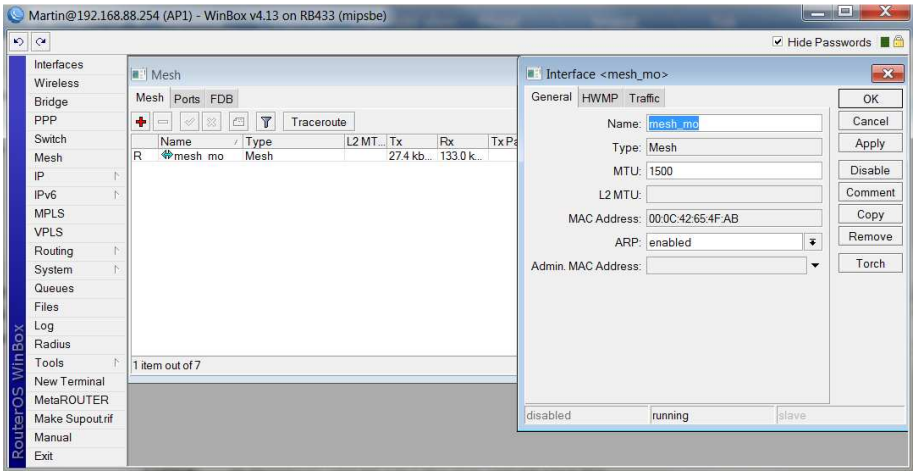
Postup nastavení RB433 – řídící AP:

Postup je stejný jako u RB750G. To znamená, že v první řadě pojmenujeme všechny rozhranís, která nám RB433 nabízí, navíc zde nalezne rozhraní pro bezdrátovou kartu R52. Dle obrázku 35 můžeme vidět, že v rozhranís je jedno navíc, které není automatickou součástí RB433 a tím je mesh_mo. Tento rozhraní nám představuje naší MESH síť a vytvoříme jej ručně.



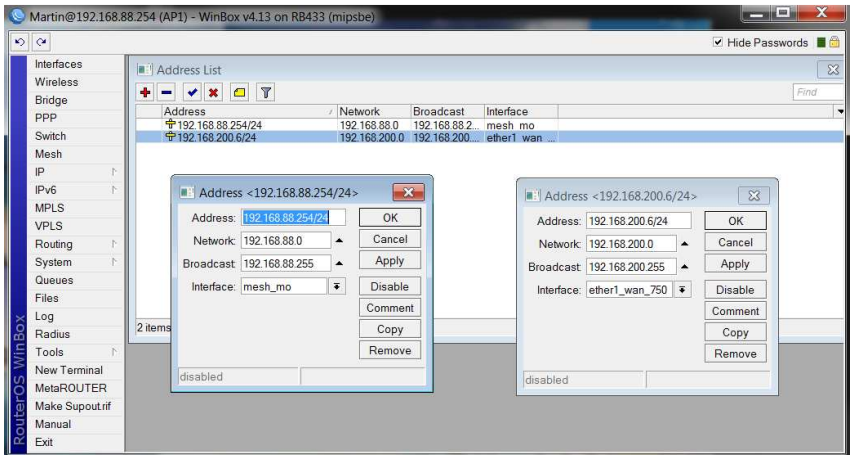
Obr. 35. Rozhranís RB433.

Rozhraní mesh_mo vytvoříme v záložce Mesh -> + -> General -> Name , v tuto chvíli máme přidán rozhraní mesh_mo.



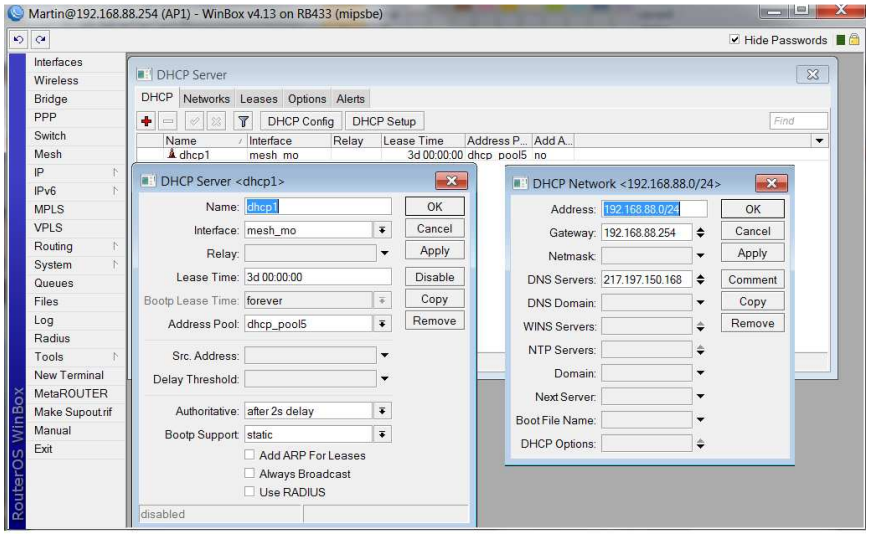
Obr. 36. Vytvoření MESH na RB433.

Další postup je podobný jako u RB750G, musíme na záložce IP -> routes přidat cestu 0.0.0.0/0, kde výchozí brána pro tuto cestu bude adresa 192.168.200.254. V záložce IP -> Addresses přidáme dva nové záznamy, to znamená IP adresu našeho AP1, spolu s rozsahem sítě a IP adresu naší brány, přes kterou přistupujeme ven., viz. obrázek 37. Důležité v tomto případě je nastavit správně rozhraní.



Obr. 37. Adrresses na RB433.

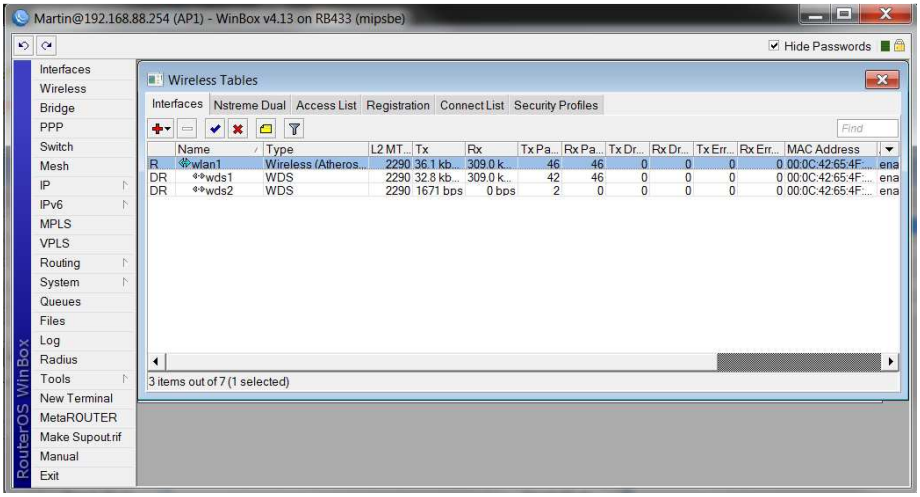
Dále v RB433 rozběhneme DHCP Server a to tak, že v záložce IP -> DHCP Server -> DHCP -> + -> Name (pojmenuj server) -> záložka rozhraní vybereme mesh_mo potvrdíme nastavení a zavřeme, dále se posuneme na záložku network, kde nastavíme rozsahy našeho DHCP serveru.



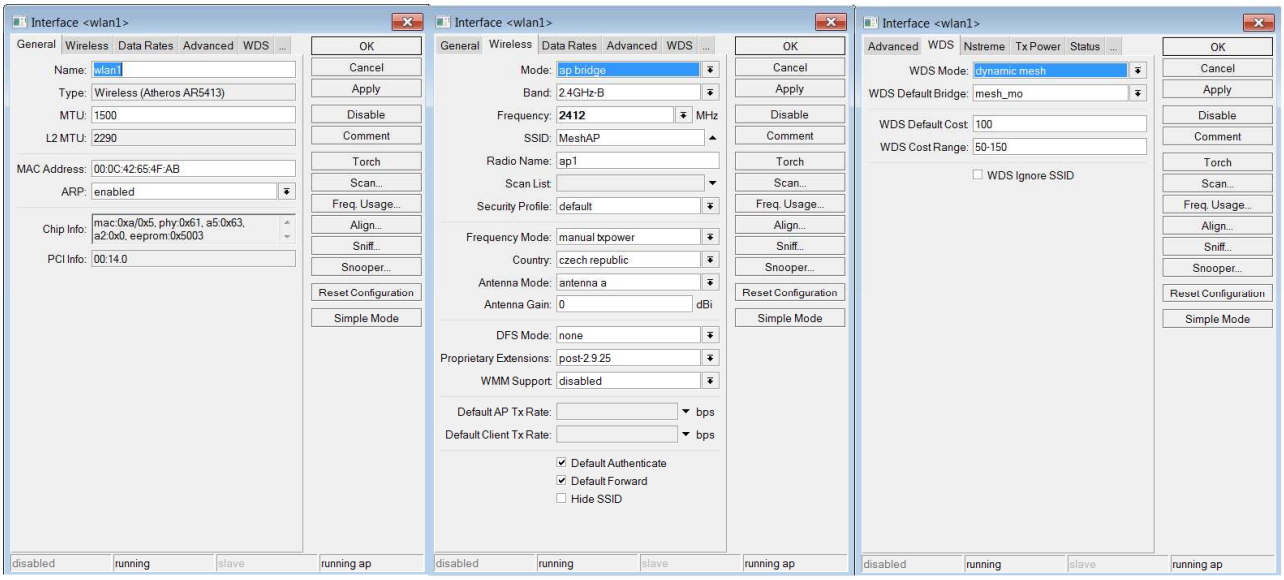
Obr. 38. DHCP server na RB433.

V neposlední řadě musíme správně nastavit bezdrátovou kartu. To uděláme následovně, záložka Wireless-> zde by měla být vidět naše bezdrátová karta. Kartu otevřeme a budeme postupně nastavovat jednotlivé záložky, general, zde nastavíme jméno rozhraní, v záložce wireless nastavíme mode na ap bridge, pásmo na 2,4 GHz, případně 5GHz, pakli-že testy chcete provádět v pásmu 5GHz, nastavíme SSID sítě, v našem případě se jmenuje MeshAP, můžeme dát jméno našemu vysílači pro snadnější přehled při testech, nazvali jsme jej ap1, důležité je nastavit country, což je země vysílání, přejdeme na další záložku a

tou je WDS, kde nastavíme WDS Mode na dynamic mesh a WDS Deafault Bridge na mesh_mo. Všechna nastavení jsou popsána na obrázku 40, na obrázku 39 vidíte, že když správně nastavíte MESH i na ostatních radiích, tak se v zobrazených bezdrátových rozhraních objeví funkční režim WDS MESH.



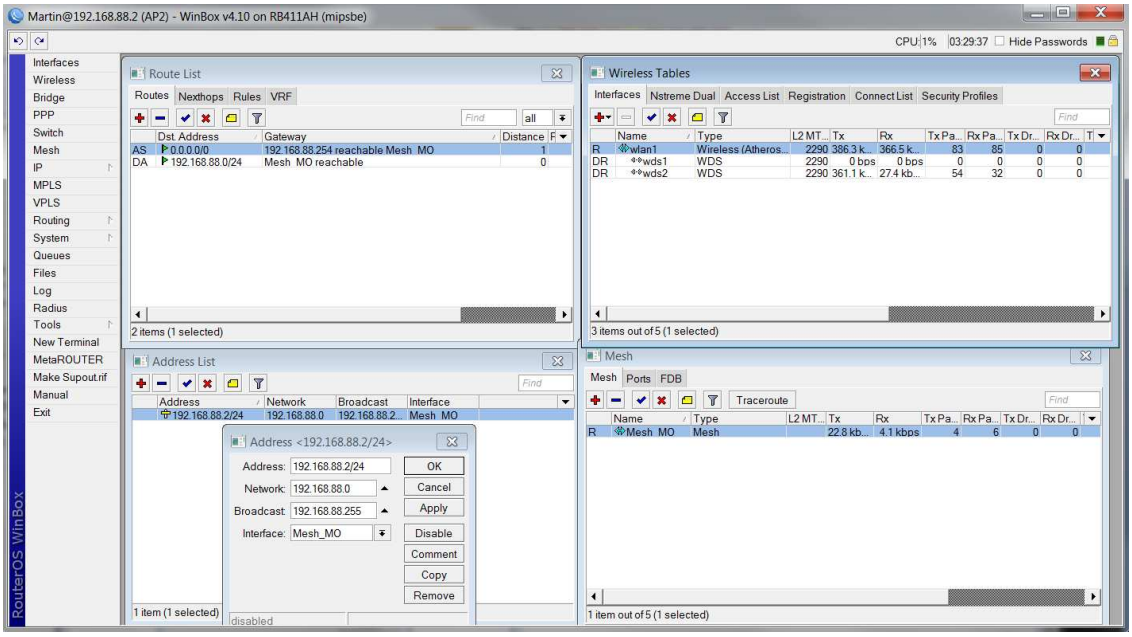
Obr. 39. Wireless Tables na RB433.



Obr. 40. Nastavení wireless rozhraní RB433.

5.1.3 Nastavení ostatních AP v síti (v našem případě RB433 – AP3 a RB411AH - AP2)

Nastavení zbývajících AP jsou v podstatě stejná jako v případě nastavení RB433 řídícího rádia, jediným rozdílem je, že se nenastavuje DHCP server. V záložce wireless je natavení taktéž stejné jako v popisovaném postupu u řídícího AP1 RB433. Nastavení dalších AP viz. obrázek 41. Každé nové AP bude mít jinou IP adresu, je třeba na to brát ohled v Addresses .



Obr. 41. Nastavení ostatních AP (AP2 a AP3).

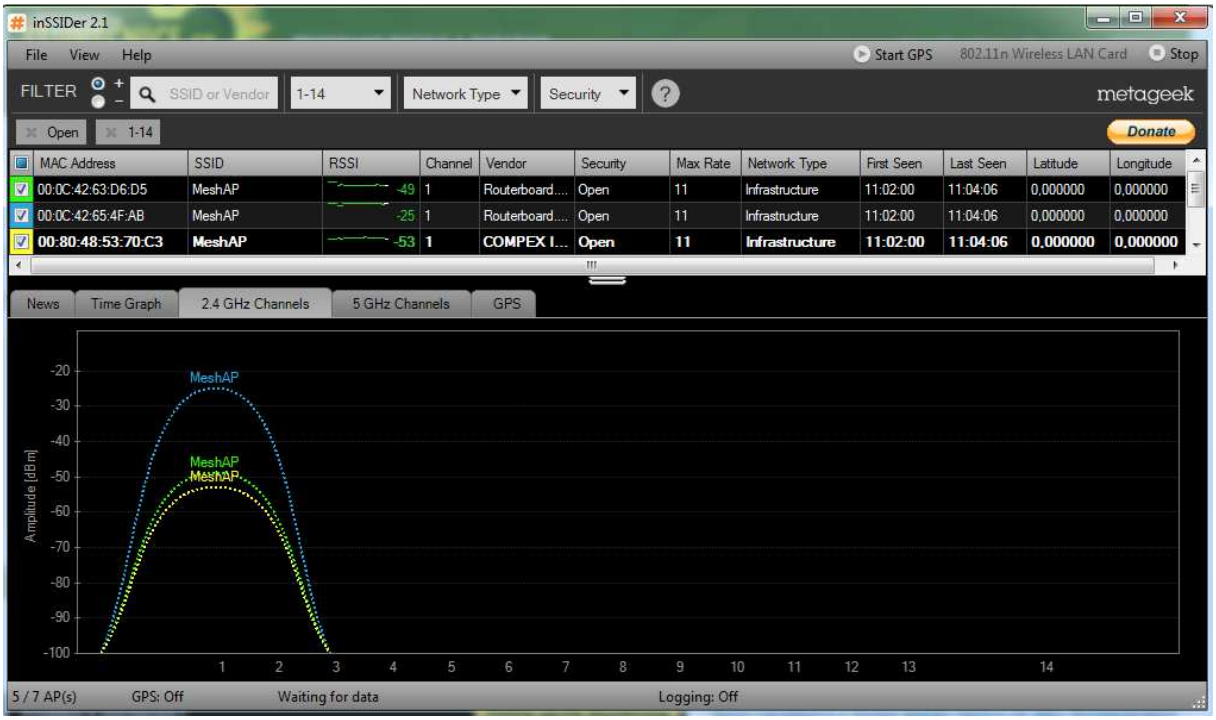
5.2 Testy prováděné v MESH síti

Dle schémat, podle kterých byl vytvořen testovací provoz MESH sítě, byly prováděny následující testy: test, zdali všechny AP opravdu vysílají na stejné frekvenci a splňují charakteristiku MESH sítě, test spolehlivosti MESH, test reakce klientské jednotky na změnu AP pomocí pingu

5.2.1 Test vysílání AP na stejné frekvenci

V tomto testu ověříme, zdali všechny AP ve Wi-Fi síti opravdu vysílají na stejné frekvenci. Pro tento test bylo zvoleno pásmo 2,4 GHz kanál 1. Na obrázku 42 byl tento test proveden v programu inSSIDer 2.1, kde můžete vidět, že podmínka vysílání na stejné frekvenci je

splněna. Modré znázornění na obrázku 42 představuje AP1, zelené znázornění představuje AP2 a poslední žluté označení představuje AP3.



Obr. 42. Test vysílání AP na stejné frekvenci.

Pro lepší orientaci:

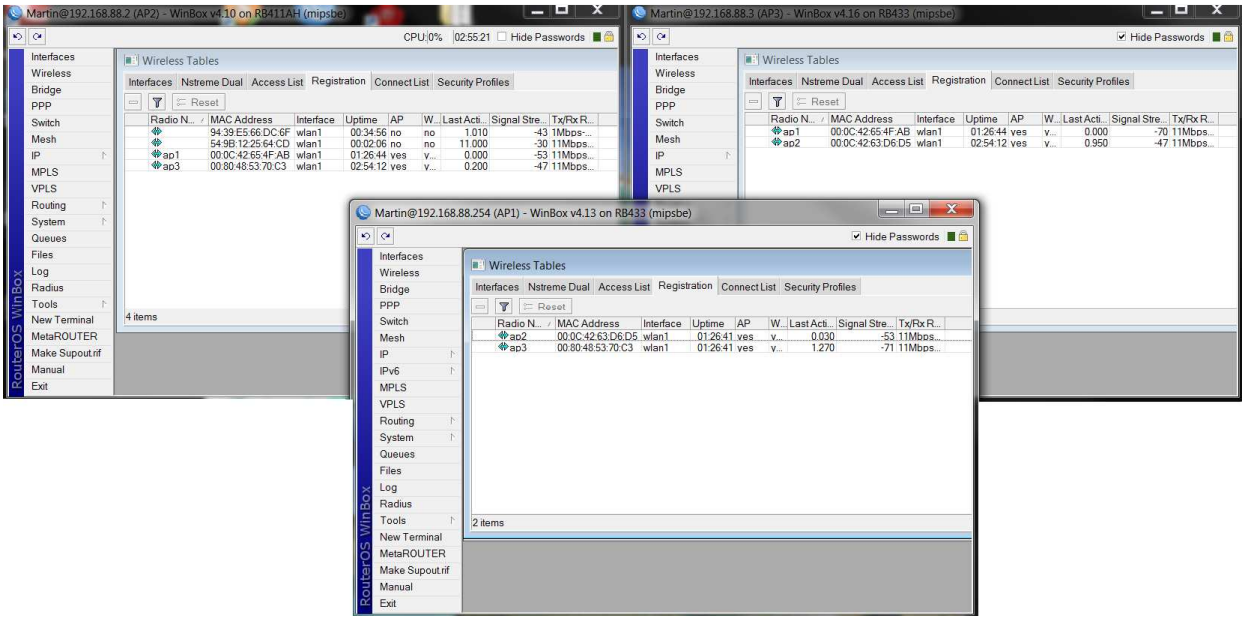
AP1 – MAC adresa: 00:0C:42:65:4F:AB

AP2 – MAC adresa: 00:0C:42:63:D6:D5

AP3 – MAC adresa: 00:80:48:53:70:C3

5.2.2 Test spolehlivosti Wifi MESH sítě

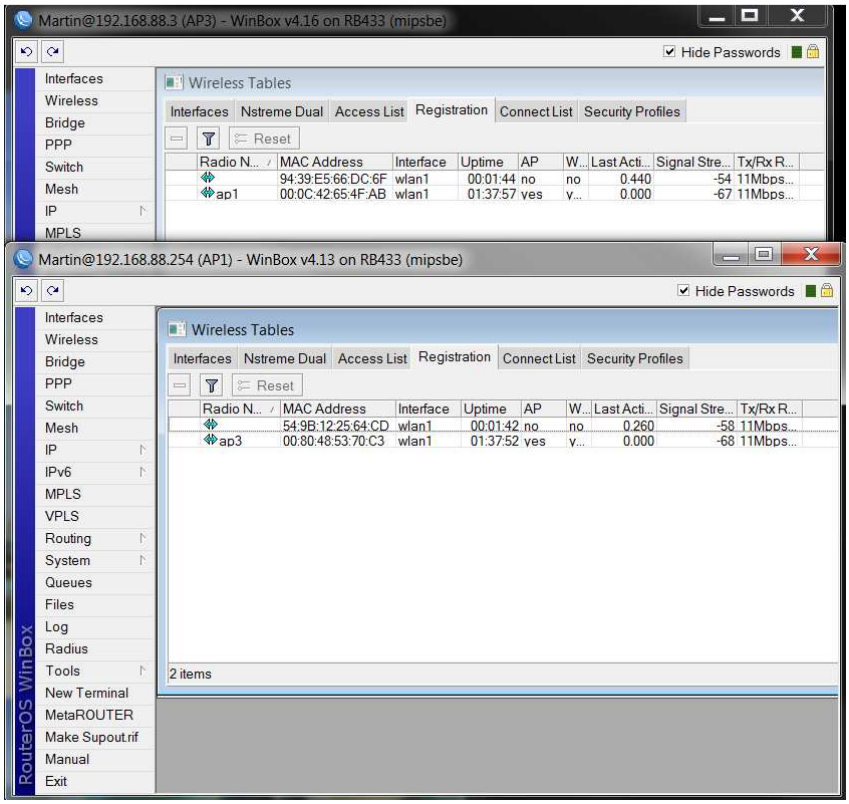
V tomto testu zkontrolujeme podmínku automatického přepojování jednotlivých koncových klientských jednotek (v našem případě notebook Lenovo a smartphone Samsung Galaxy Ace). Budeme simulovat výpadek bodu AP2. V tuto chvíli jsou veškerá zařízení přihlášena na vysílači AP2 viz. obrázek 43.



Obr. 43. Zařízení v registration na AP2.

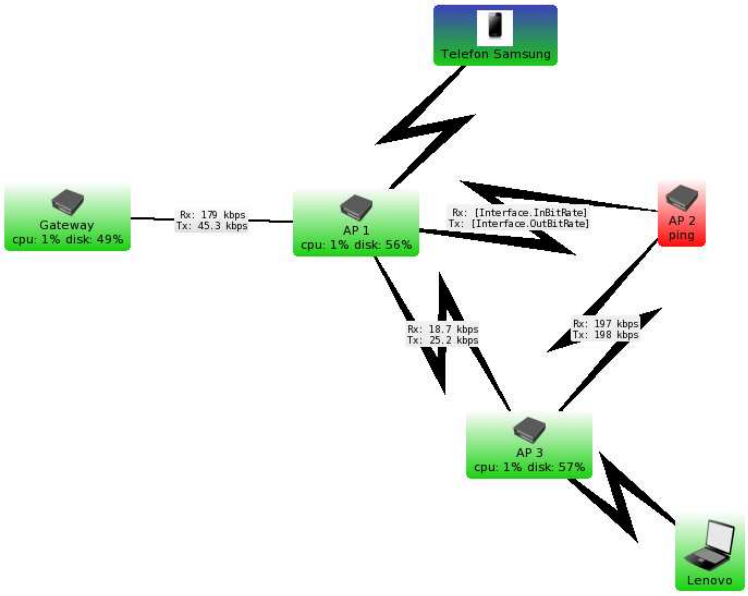
Mac adresa notebooku Lenovo: 94:39:E5:66:DC:6F

Mac adresa smarphonu Samsung Galaxy Ace: 54:9B:12:25:64:CD



Obr. 44. Přeregistrování klientů na zbylé vysílací AP.

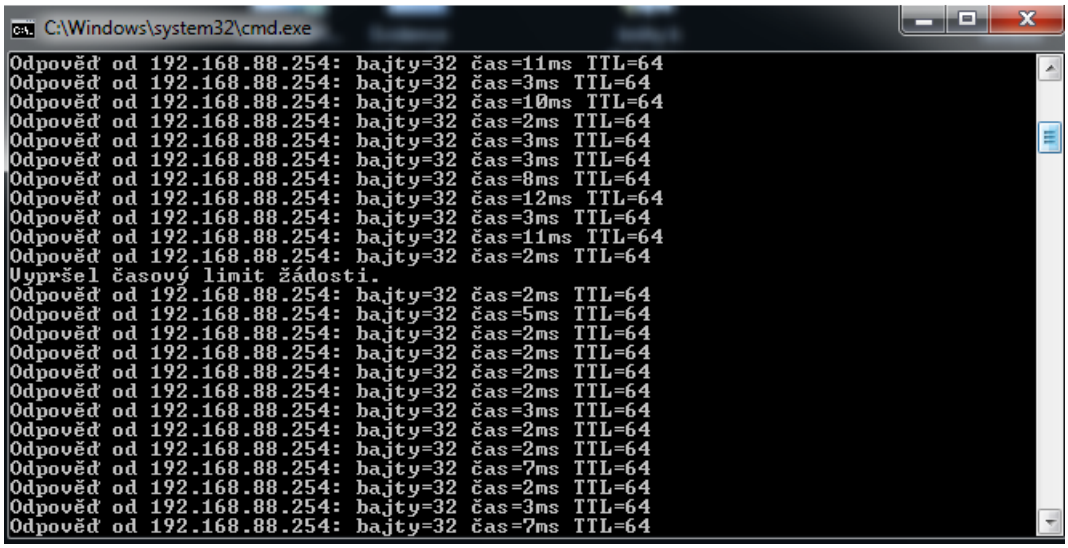
Na obrázku 44 lze vidět, že notebook Lenovo se přeregistroval na AP3 a mobilní telefon se přihlásil k AP1, které v tuto chvíli vysílají. Ve sledovacím programu The Dude lze vidět na základě monitoringu sítě, že AP2 je opravdu neaktivní, ale síť je funkční a vysílá viz. obrázek 45.



Obr. 45. Stav sítě při výpadku AP2.

5.2.3 Test reakce klientské jednotky na změnu AP pomocí pingu

Tento test měl odhalit rychlost přepojení notebooku Lenovo na jiné AP v případě výpadku AP, na kterém byl připojen. Rychlost přepojení na základě měření pingu můžete vidět na obrázku 46. Jak vidíte, tak vypadl jediný packet, což jako výsledek testu hodnotím velmi pozitivně, což této technologii přidává na praktické použitelnosti.



Obr. 46. Rychlost změny AP.

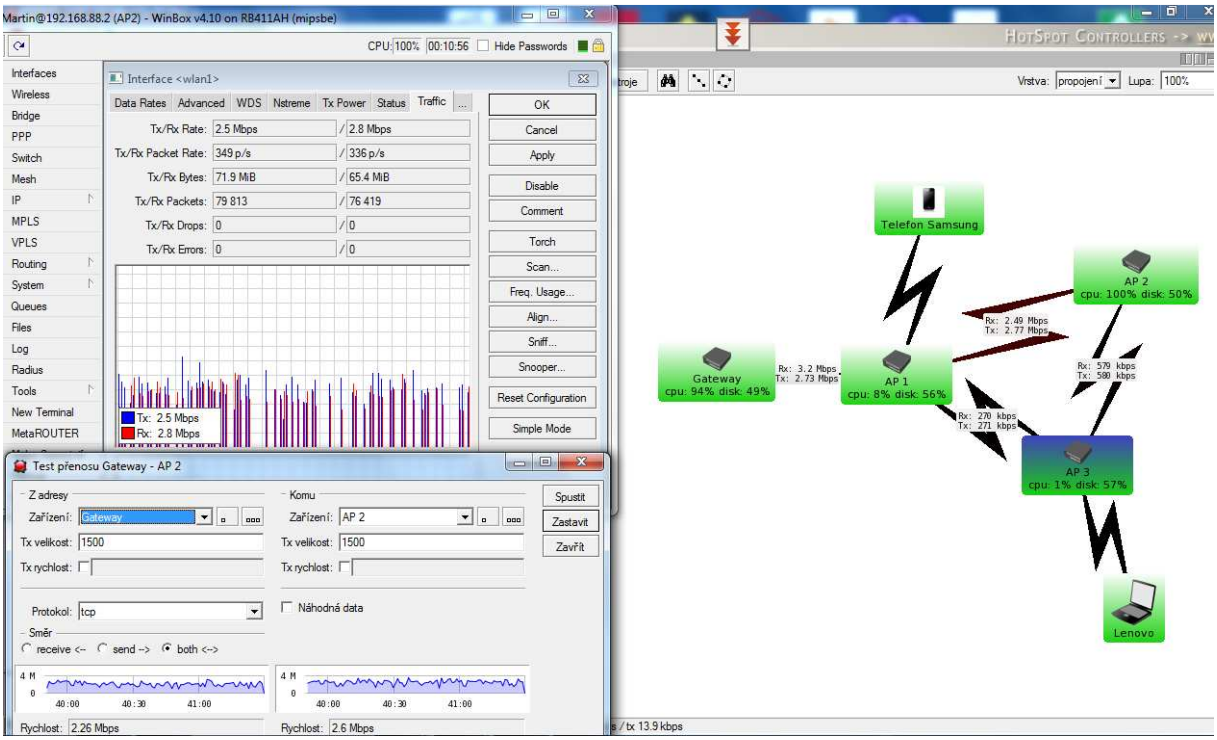
5.3 Testy prováděné na jednotlivých zapojeních dle rozmístění AP v domě

V této části diplomové práce se zaměřím na test propustnosti mezi jednotlivými AP na základě zapojení v rámci jednoho patra a zapojení v rámci rozmístění AP v rámci zbytku domu a to v pásmu 2,4GHz. Jako poslední pro pásmo 2,4GHz provedu test rychlosti připojení a provozu na koncovém zařízení, kdy toto zařízení bude připojeno na posledním AP3 a bude se na něm spuštěn stream videa z internetu. Pro pásmo 5GHz je nachystán test propustnosti mezi AP v rámci patra domu v nezarušeném prostředí. Poslední test, který jsme v pásmu 5GHz prováděli, byl vliv rušení jiné sítě na MESH síť.

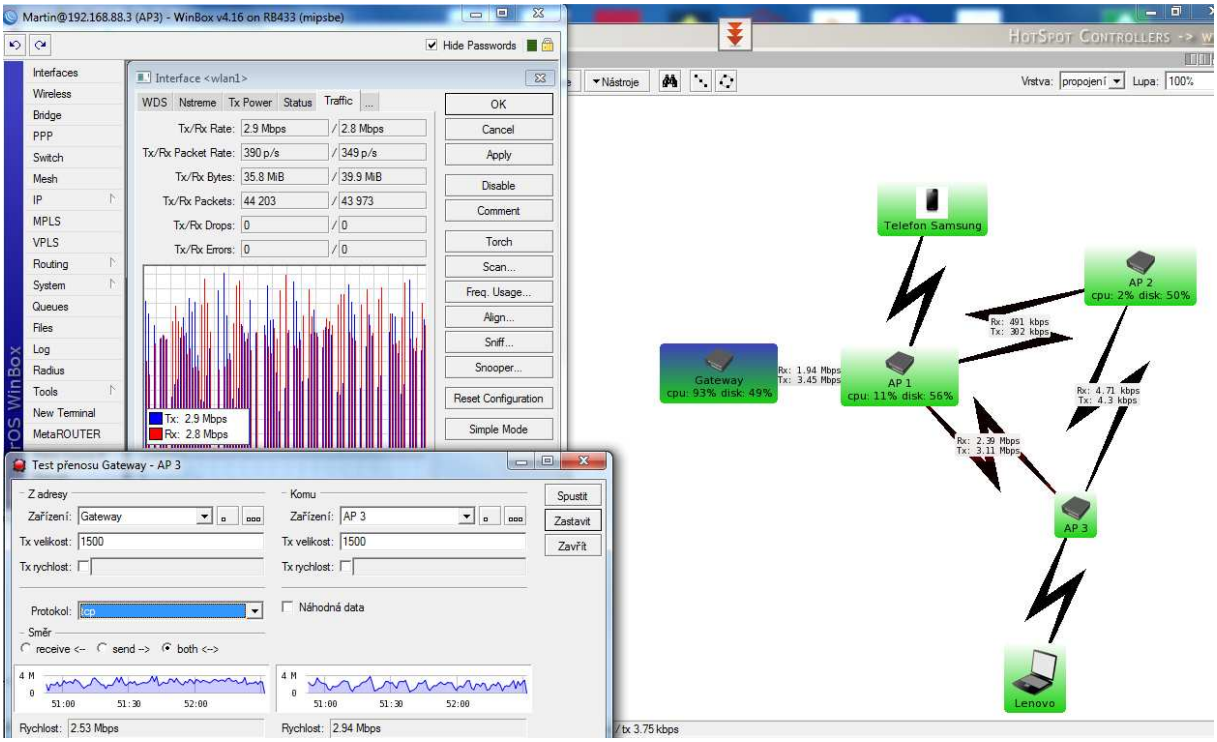
Schéma zapojení naleznete na obrázku 27 a 28.

5.3.1 Test propusti mezi AP v rámci patra domu

V tomto režimu jsme testovali datovou propust MESH sítě a to konkrétně směrem k AP2 a AP3. Data byla odesílána z hlavní Brána, přičemž na obrázku 47 a 48 je vidět vytíženost sítě, rychlost na lince, zatížení CPU, provoz na jednotlivých AP. K testu byly použity aplikace Winbox a The Dude. Testování bylo prováděno na protokolu TCP/IP a byla měřen jak upload, tak i download zároveň.



Obr. 47. Test propustnosti směrem k AP2.

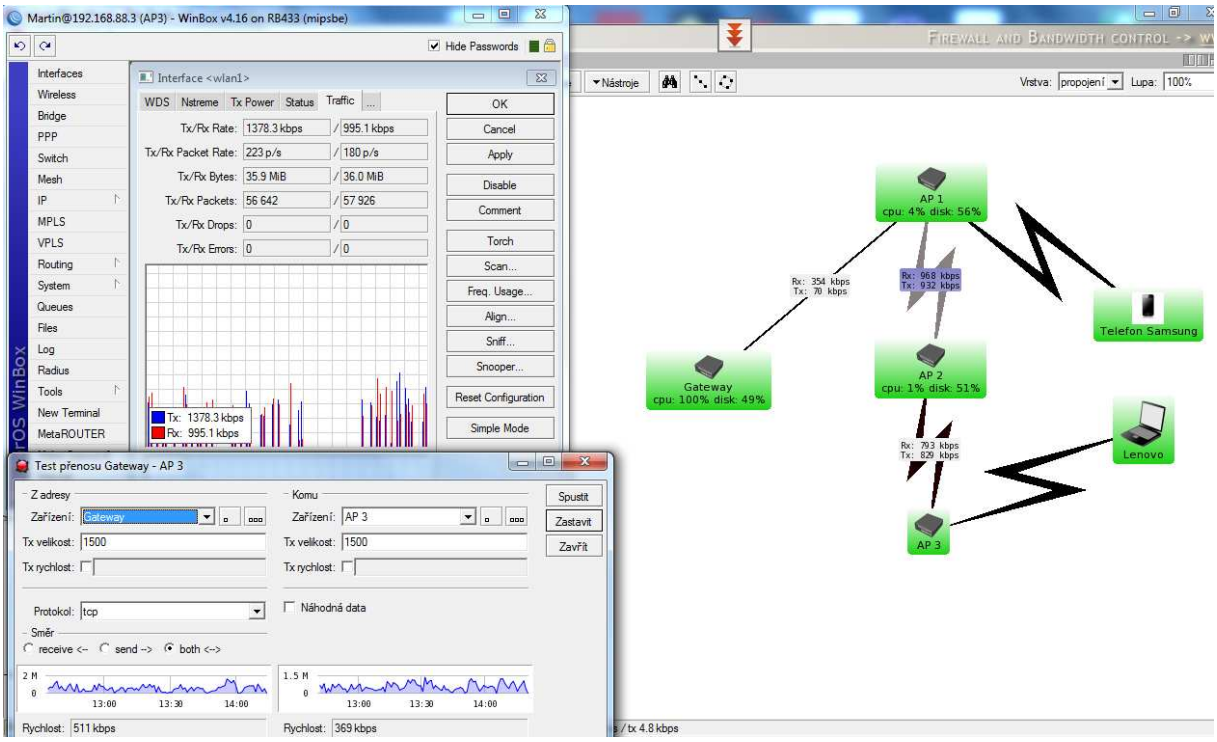


Obr. 48. Test propustnosti směrem k AP3.

Jak je vidět, tak rychlost na bezdrátové síti MESH v režimu 2,4GHz, nepřesáhla rychlost 3Mbit/s, spojení bylo stabilní, výpadek na základě vytíženosti procesorů jednotlivých zařízení nebyl zaznamenán.

5.3.2 Test propusti mezi AP v rámci celého domu

V tomto režimu byla AP rozmístěna na základě schématu z obrázku 28. Cílem bylo dokázat, že komunikace bude probíhat sériově, jako by jednotlivá AP byla zapojena postupně za sebou. Bylo potřeba taktéž zjistit, jak sem MESH síť bude chovat v případě horších signálu mezi jednotlivými AP a jaké budou rychlosti v síti. Veškeré testování viz. obrázek 49.



Obr. 49. Test propustnosti směrem k AP3, kdy jsou AP v sérii.

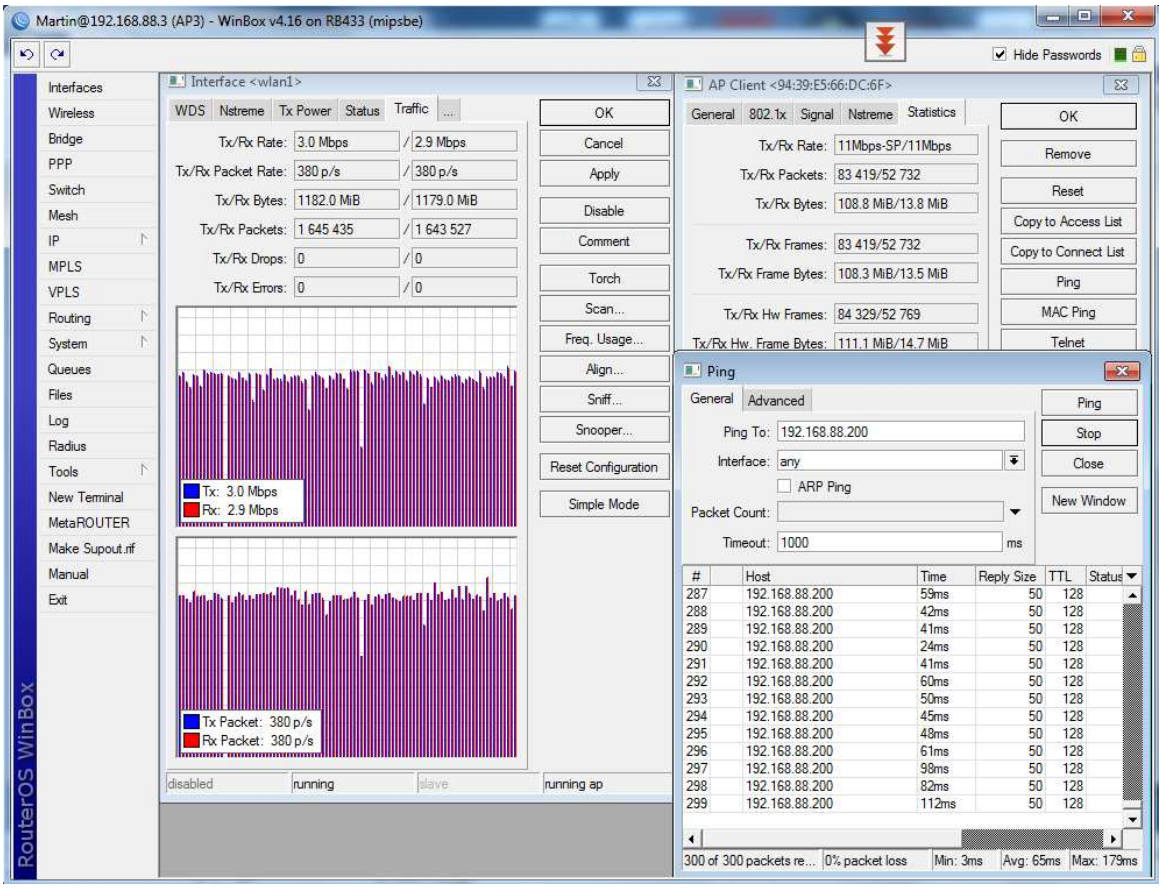
Jak můžete na první pohled vidět, tak se tento test dost výrazně liší od testu předchozího. Díky tomu, že mezi jednotlivými patry v testovaném objektu jsou železobetonové stropy a AP byla od sebe výrazněji vzdálena než v případě předchozího testování, tak nám klesla celková propust sítě. Tak jak se dalo očekávat, tak komunikace opravdu probíhala sériově, to znamená, že nebylo možno uzavřít v MESH síti trojúhelník mezi jednotlivými AP, jelikož AP1 a AP3 nešlo na základě slabého signálu spojit. Veškerá komunikace striktně probíhala přes AP2. Pakliže chceme zajistit kvalitní výkon a stabilitu MESH sítě, je lepší

samotnou MESH síť stavět tak, aby hustota AP v síti byla co největší s ohledem na vysílací výkon jednotlivých AP, tak zaručíme, že každý vysílací bod bude vzdálen od dalšího vysílacího bodu přesně tak, aby nedocházelo k poklesům signálu a zároveň klesání datového toku v síti.

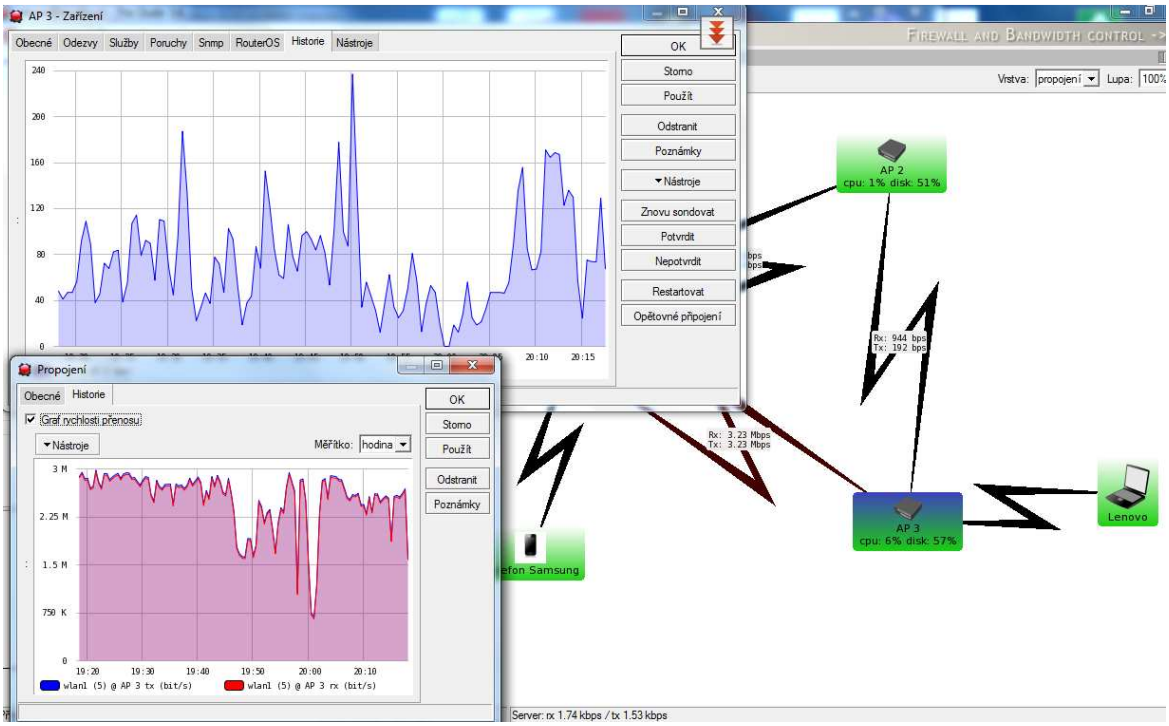
5.3.3 Test provozu na koncovém zařízení

V této části jsem prováděl test, kterým jsem měřil a zaznamenával zatížení sítě reálným provozem na notebooku Lenovo. K testu bylo zvoleno 2 hodinové video a poté ještě 1 hodinové video. Obě tato videa se přehrávaly v prohlížeči ve formátu 720p, což představuje HD formát. Test byl prováděn 1h, přičemž se měřil tok dat na koncové zařízení, ping na koncové zařízení, provoz na lince zaznamenaný v 1 hodinovém grafu, vytíženost CPU na koncovém AP3.

Výsledek testu viz obrázek 50 a 51.



Obr. 50. Naměřené výsledky na koncovém zařízení.

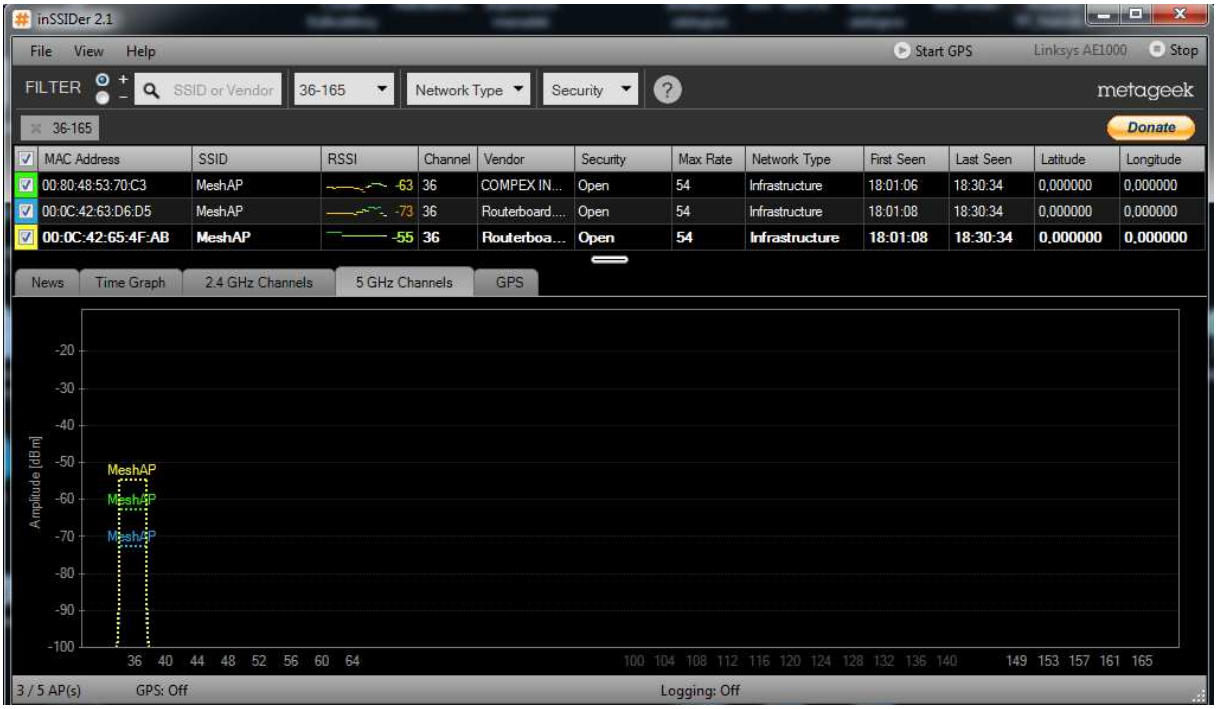


Obr. 51. Graf provozu sítě, graf zatížené CPU.

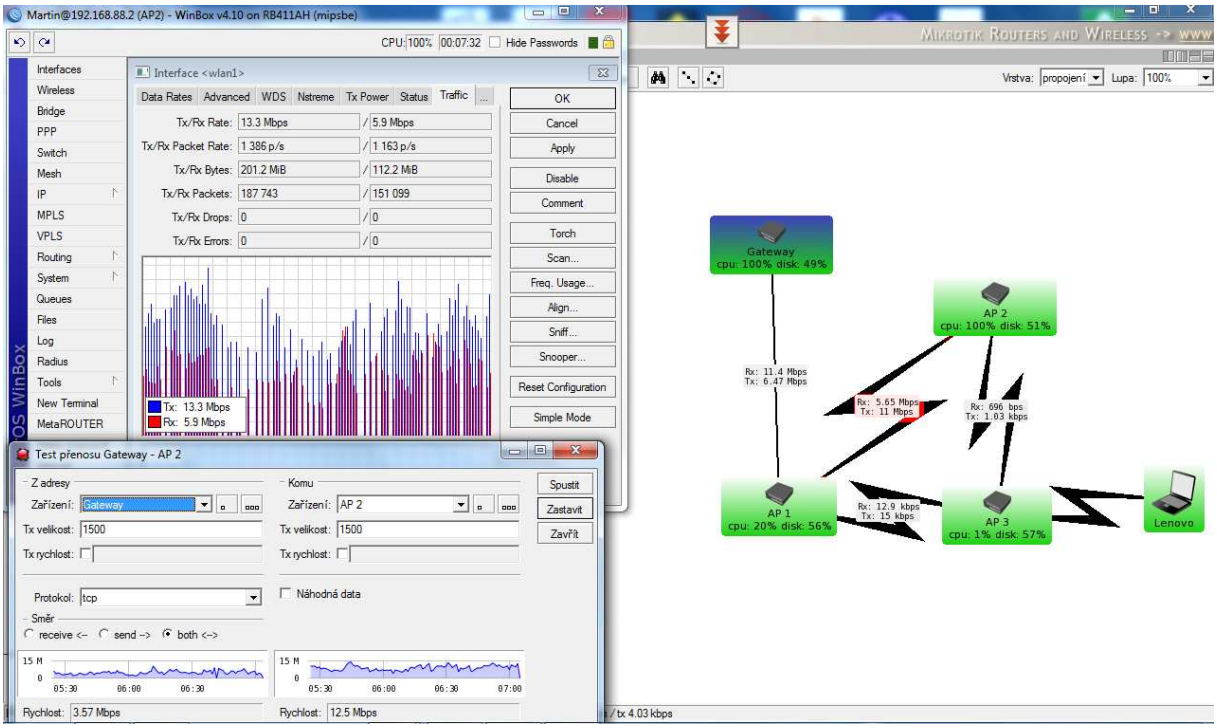
Jak je vidět, tak test dopadl úspěšně. Na obrázku 50 se stabilní vytížení linky dle hodnot na rozhraní pohybovalo kolem 3Mbit/s, přenos probíhal v pásmu 2,4GHz a ping se v našem případě pohyboval do 100ms. Obrázek 51 nám ve spodní části červeným grafem ukazuje vytížení sítě v hodinovém grafu. Test začal v 19:15 5.5.2012 a skončil v 19:15 5.5.2012. Jak si můžete v červeném grafu všimnout, tak načítání dvouhodinového videa skončilo po 45min, kdy je v červeném grafu jasně patrné zakolísání provozu sítě, to byla přesně chvíle, kdy docházelo v prohlížeči ke změně videa, poté je křivka opět stabilní ke 3Mbit/s. V druhém grafu, který je reprezentován modrou křivkou, je zaznamenáno průměrný ping v ms. Jak si můžeme všimnout, tak se ping pohyboval opravdu během celé hodiny v průměru do 100ms, občasné výkyvu jsou přisuzovány chvilkovým zhoršením kvality vysílacího signálu. Poslední důležitý údaj, který nás zajímal, bylo vytížení CPU, které se pohybovalo na AP3 do 6% nominálního výkonu, který je 300MHz.

5.3.4 Test v rámci jednoho patra pro pásmo 5 GHz

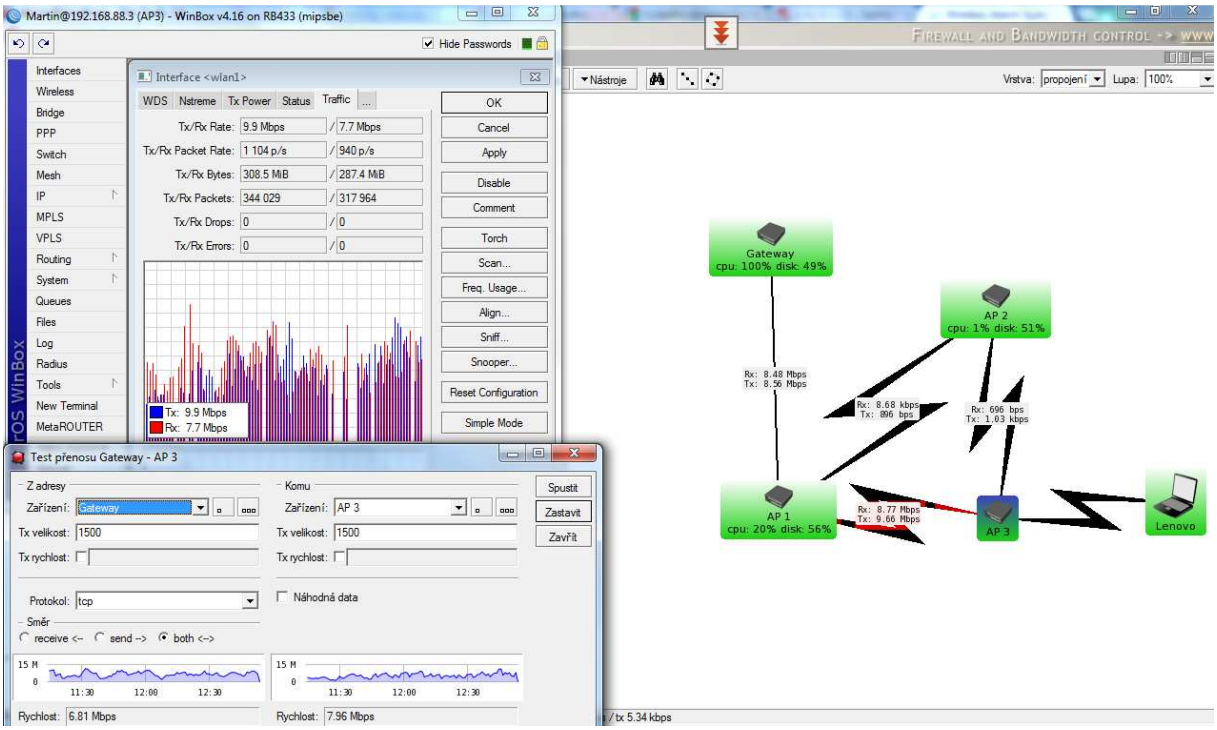
Pro testování bylo zvoleno pásmo 5GHz, kdy nebylo detekováno žádné zarušení. K síti byl opět připojen notebook Lenovo, tentokrát využíval 5 GHz bezdrátový USB adaptér. V rámci testu se zjišťovaly přenosové rychlosti mezi jednotlivými AP, měřil se jak upload, tak i download zároveň. Pro generování datového toku se využíval Brána (RB750G). Cílem bylo zjistit, zda pásmo 5GHz je vhodným řešením pro MESH indor síť, zároveň výsledkem testu mělo být zhodnocení, zdali přenosová kapacita sítě je vhodnějším řešením než u testu pro pásmo 2,4GHz. Na obrázku 52 lze vidět opět splněnou podmínku, že všechny AP vysílají na stejné frekvenci v pásmu 5GHz, najdete zde úrovně signálů a kanál, ve kterém v pásmu 5GHz vysílají. Výsledky testu jsou zobrazeny na obrázcích 53, kde probíhalo měření rychlosti přenosu směrem k AP2 a 54, kde probíhalo měření rychlosti směrem k AP3.



Obr. 52. Síť MeshAP v pásmu 5GHz.



Obr. 53. Naměřené výsledky na koncovém zařízení AP2.

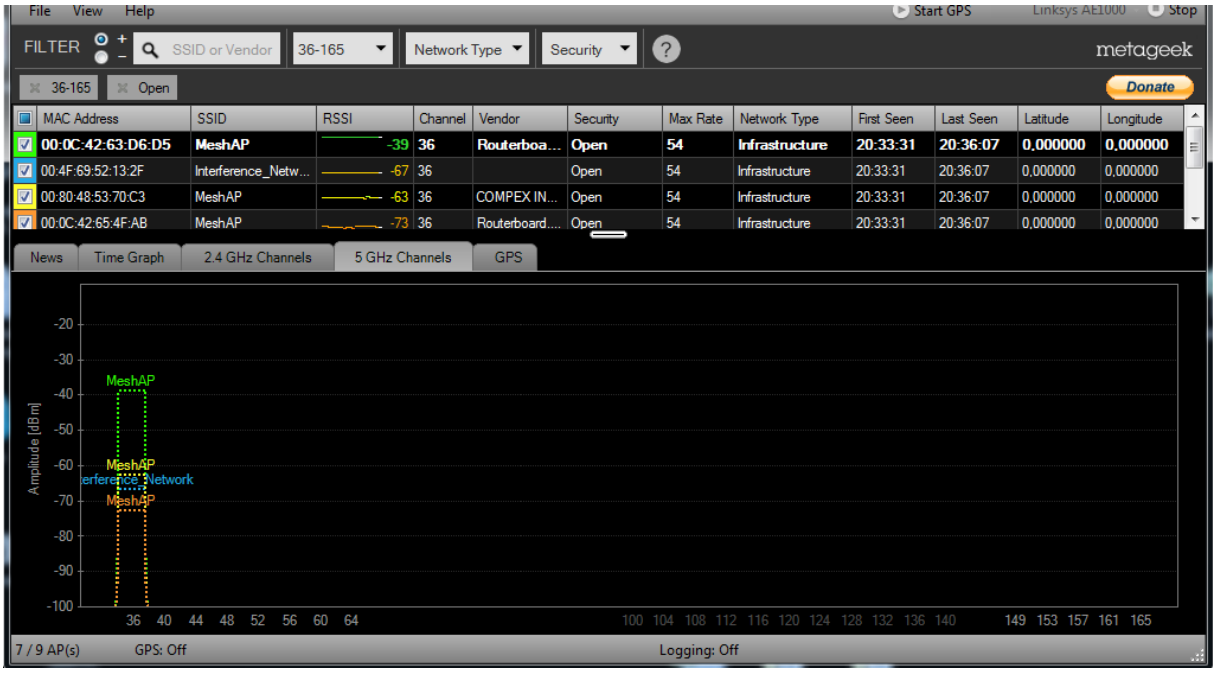


Obr. 54. Naměřené výsledky na koncovém zařízení AP3.

Jak můžeme vidět, tak komunikace, která probíhala v pásmu 5GHz prokázala mnohem lepší výsledky, než komunikace, která v předchozím testu probíhala v pásmu 2,4GHz. Rychlosti mezi jednotlivými AP byly vyšší a tudíž pásmo 5GHz je vhodnější pro budování sítí, kde je požadavkem vyšší datová propust. Samozřejmě výsledky hodně ovlivňovala kvalita signálu mezi jednotlivými AP. Tak jak platilo v pásmu 2,4GHz, tak platí i v pásmu 5GHz, čím horší je kvalita signálu na jednotlivých vysílačích, tím horší je výsledná kvalita přenosových rychlostí v samotné síti.

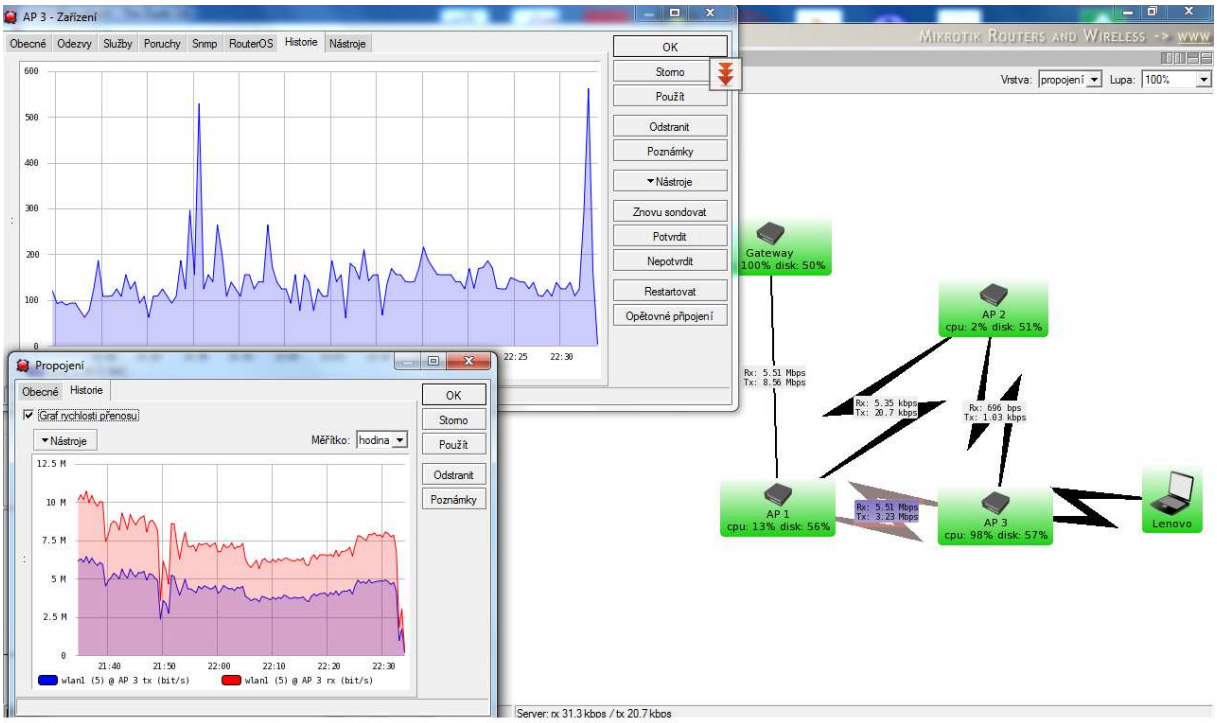
5.3.5 Test pro pásmo 5 GHz – zarušené prostředí

Cílem testu bylo v rámci patra ověřit chování sítě v pásmu 5GHz v případě vlivu jiného AP, které vůči naší MeshAP vysílalo na stejné frekvenci. Název této sítě lze vidět na obrázku 55, kdy k potřebám testu byla tato síť pojmenována jako interference network. Na základě rušení se měřil přenos k nejvzdálenějšímu AP3, které dle předpokladů má být tímto zarušením nejvíce ovlivněno, měřil se ping k AP3, tento test byl prováděn jednu hodinu a výsledky byly zaznamenány do grafu. Jako poslední byl zvolen test, kde se měřila průměrná rychlost a doba stahování souboru do koncového přístroje Lenovo a ping ke koncovému přístroji Lenovo, notebook Lenovo byl v tomto testu připojen k vysílacímu AP 3.



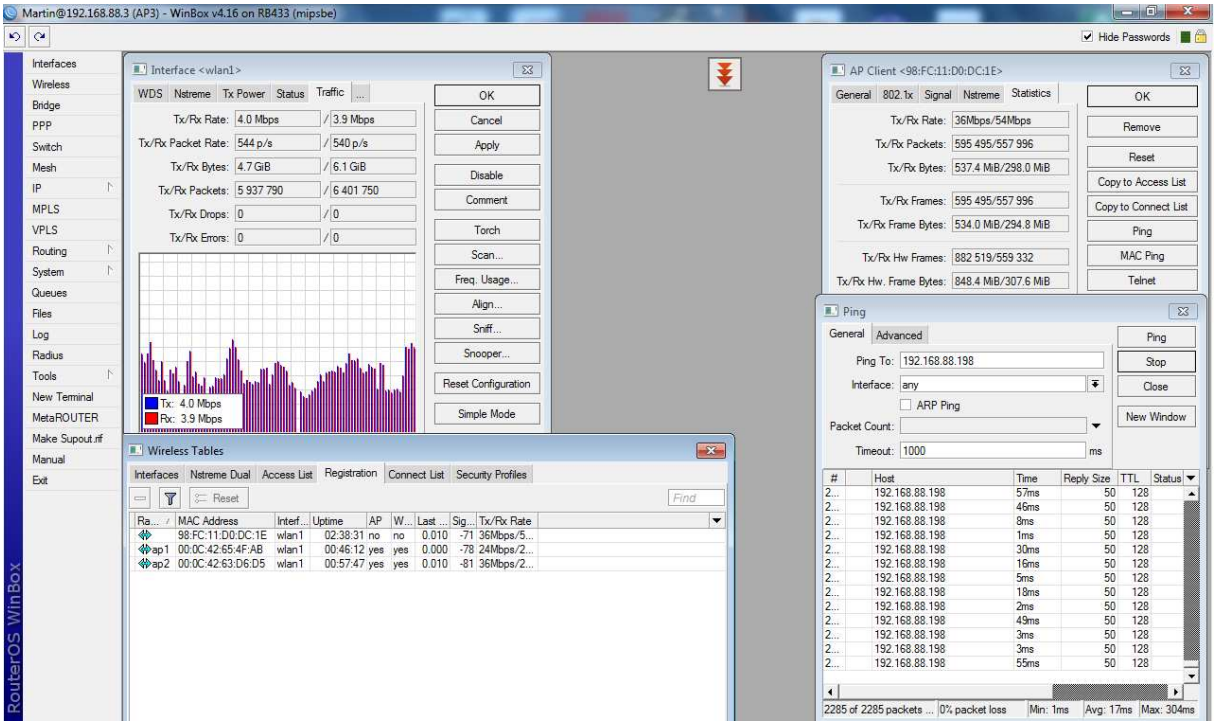
Obr. 55. Interference network.

Jak si můžeme z obrázku všimnout, tak oranžová křivka nám v tuto chvíli dle MAC adresy představuje AP1 (MAC 00:0C:42:65:4F:AB) , což je naše řídící AP v sítí MeshAP, které je jednoznačně pro naše účely záměrně zarušeno sítí interference network (MAC vysílacího AP 00:4F:69:52:13:2F), která je na obrázku 55 zobrazena modrou křivkou.

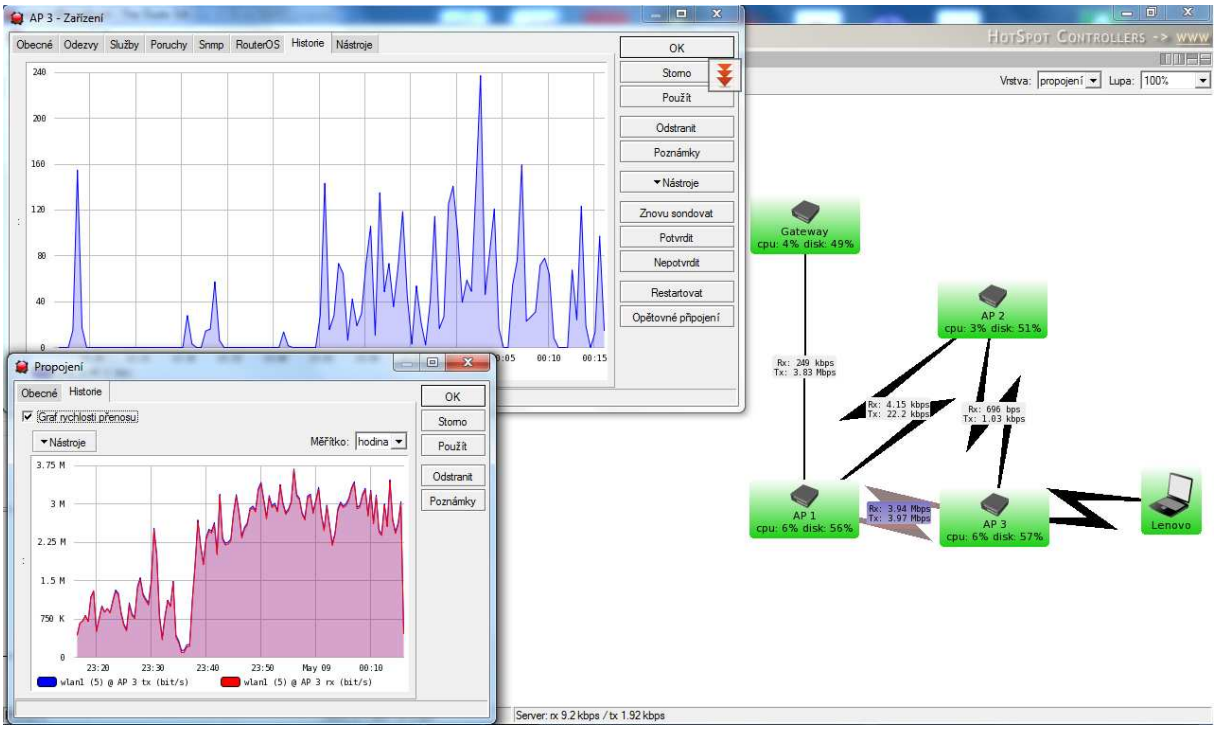


Obr. 56. Ping a rychlost linky na AP3.

Na obrázku 56 naleznete výsledek hodinového zatěžování sítě v zarušeném prostředí směrem k vysílači AP3, pro generování datového toku opět byla použita Brána (RB750G). Horní graf na obrázku 56 představuje ping, spodní graf představuje datovou propust uploadu a downloadu zároveň, modrá upload, červená download. Jak je vidět, tak interference v síti se nijak neprojevila na kvalitě přenosu mezi AP1 a AP3 a lze říci, že MESH síť si zachovává kvalitní parametry při vysokém datovém toku v zarušeném prostředí.



Obr. 57. Zarušené pásmo 5GHz – vývoj měření ve Winbox pro Lenovo při stahování 1,4GB souboru



Obr. 58. Zarušené pásmo 5GHz – vývoj měření The Dude pro Lenovo pro stahování 1,4GB souboru – hodinový interval.

Jak si lze všimnout z obrázku 58, tak našemu stahovanému souboru o velikosti 1,4GB chvíli trvalo, než se download ustálil na konstantní průměrné hodnotně. Download se pohyboval okolo 4Mbit/s a ping byl v rámci normy. Lze říci, že reálný provoz a větší vliv rušení na spojení mezi notebookem Lenovo a AP3 přispěl k nižší výsledné rychlosti downloadu oproti teoretické maximální testované propusti v síti MESH viz. obrázek 56. I tak lze říci, že rychlost 4Mbit/s v 5GHz pásmu při vlivu rušícího elementu vykazuje pozitivní výsledky a na základě pozorování bylo zjištěno, že síť hledá nejlepší možnou cestu ke koncovému klientovi, aby byla kvalita a stabilita sítě co nejoptimálnější.

ZÁVĚR

Hlavním cílem práce bylo navrhnout zapojení MESH sítě, nastavit zařízení mikrotik k použití v této navrhnuté MESH síti a otestovat funkčnosti protokolu MESH a otestovat chování sítě v provozu.

Úvod této práce se věnuje základům počítačových sítí, kde se postupně rozebírá hardware, který se v dnešních sítích používá, jsou zde probírány topologie sítí, které dnes můžeme používat při tvorbě vlastní sítě, jako poslední ze základů je zde rozebírán referenční model OSI. V další části teoretické přípravy se věnuji bezdrátovým sítím a protokolům, které jsou používány v těchto sítích. První část práce je ukončena rozebíráním samotného HW zařízení mikrotik a programy, které s tímto HW spolupracují, což je program Winbox a The Dude.

Druhá část práce se věnuje návrhu samotné bezdrátové sítě, možnosti zapojení pro jednotlivá testování, rozebírá samotná zařízení, která se použila k výstavbě sítě podrobně, s hardwarového hlediska, dále je v této části podrobně popsáno nastavení jednotlivých síťových prvků. Část poslední se věnuje praktickému testování MESH technologie v provozu, byly zde dělány testy, které ověřili spolehlivost MESH sítě, ověřili, zdali se je splněna podmínka vysílání na jedné frekvenci všech AP v MESH síti, ověřili reakční rychlost na výpadek AP. Další testy byly prováděny při reálném stremování videa z internetu, byl zde kladen důraz na použitelnost a nasazení tohoto síťového řešení v praxi. Poslední fáze testování se věnula pásmu 5GHz a použitelnosti při zarušení frekvenčního pásma. V této části byla testována datová propust, kdy není detekováno žádné rušení a v další části se prováděly opět testy na datovou propust, ale tentokrát při zarušení. Po vyhodnocení veškerých testů, jak pro pásmo 2,4GHz, tak i pro pásmo 5GHz, bylo zjištěno, že síť MESH vyhovuje firemním požadavkům a lze jí nasadit jako LAN, případně MAN řešení.

CONCLUSION

The main objective of this thesis was to design a MESH network connection, set MikroTik equipment for use in the proposed MESH network and finally test MESH protocol functionality and network traffic behavior.

The theoretical part deals with the basics of computer networks, where today's networking hardware and common network topologies are analyzed including the OSI reference model. Next section describes the wireless networks and protocols that are used in these networks. Finally, the MikroTik hardware device and cooperating software applications Winbox and The Dude are discussed.

The practical part deals with design of wireless network, possibilities of connection setup for each test, analyzing equipment used to build the network in detail from hardware perspective and finally detailed settings of the individual network elements. The last section is devoted to practical testing of operational MESH technology, where tests were done to verify the reliability of MESH network, check of the MESH network in its principal and reaction time in the event of AP failure. Further tests were made in real conditions using video stream from the Internet, the emphasis was on applicability and deployment of this network solution in practice. Last set of tests was made in 5GHz frequency band with regard to its usability when the frequency band is jammed. Data transfer rates are recorded in situations where either no interference is detected, or interference jamming is applied. After evaluating of all tests for both the 2.4 GHz and 5 GHz band, it was found that the MESH network meets the company requirements and can be deployed as a LAN or MAN solution.

SEZNAM POUŽITÉ LITERATURY

[1] **BIGELOW, Stephen J.** *Mistrovství v počítačových sítích.* Praha : Computer press, 2003. ISBN 80-251-0178-9.

[2] **DOSTÁLEK, Libor a KABELOVÁ, Alena.** *Velký průvodce protokoly TCP/IP a systémem DNS.* Praha : Computer Press, 2000. ISBN 80-7226-323-4.

[3] **TRULOVE, James.** *Sítě LAN.* Praha : Grada *Publishing*, a.s., 2009. ISBN 978-80-247-2098-2.

[4] **ZELINKA, Tomáš a SVITEK, Miroslav.** Telekomunikační *řešení pro informační systémy síťových odvětví.* Praha : Grada Publishing, a.s., 2009. 978-80-247-3232-9.

[5] IEEE 802.11. *Wi-Fi Wireless LAN.* [Online] GNU Free *Documentation* License, 11. 4 2012. [Citace: 2012. 5 2.] Dostupné z: http://wi-fi.unas.cz/ieee-802-11.php

[6] **SIMANDL, Martin.** IEEE 802.11n — Jak na rychlé Wi-Fi doma i venku. *PCTuning.* [Online] ,17. 3 2010. [Citace: 3. 5 2012.] Dostupné z: http://pctuning.tyden.cz/

[7] **ZANDL, Patrik.** *Bezdrátové* sítě *WiFi Praktický průvodce.* Praha : Computer Press, 2003. ISBN 80-7226-632-2.

[8] Seznámení s *Mikrotik RouterOS. WiFi hardware.* [Online] , 2. 2 2009. [Citace: 3. 5 2012.] Dostupné z: http://www.wifihw.cz/

[9] **ŠTRAUCH, Adam.** Mikrotik: *seznámení* s Wi-Fi *krabičkou*. *ROOT.CZ.* [Online] Internet Info, s.r.o., 7. 11 2008. [Citace: 3. 5 2012.] Dostupné z: http://www.root.cz/

[10] **BARTOEK, J. a HAVLÍČEK, P.** *Směrovací* protokol MESH (802.11s) na Platformě Mikrotik. *WikiHosting.* [Online] wh.cs.vsb.cz, 1. 5 2009. [Citace: 5. 5 2012.] Dostupné z: whwh.cs.vsb.cz

[11] **AKYILDIZ, Ian a WANG, Xudong.** *Wireless Mesh Networks.* Chichester : Jonh Wiley & Sons LTD, 2009. ISBN 978-0-470-03256-5.

[12] i4wifi. *Návod k obsluze* Platforma *RouterBoard s přeinstalovaným RouterIS Mikrotik.* [Online] i4wifi, 1. 1 2011. [Citace: 5. 5 2012.] Dostupné z: http://i4wifi.cz/img.asp?attid=74453

[13] Manual: The Dude. *Mikrotik.* [Online] Mikrotik, 17. 11 2011. [Citace: 5. 5 2012.] Dostupné z: http://wiki.mikrotik.com/wiki/Manual:The_Dude

[14] MikroTik RouterOS v3.0 manual. *Mikrotik.* [Online] Mikrotik, 1. 1 2007. [Citace: 5. 5 2012.] Dostupné z: http://www.mikrotik.com/testdocs/ros/3.0/refman3.0.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AFT	Adapter fault tolerance
AM	Amplitude modulation
AP	Access Point
ARP	Address Resolution Protocol
BGP	Border Brána Protokol
BPSK	Binary Phase-shift keying
CP	Contention Period
CSMA/ CA	Carrier Sense Multiple Access with Collision Avoidance
DCF	Disiributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSSS	Direct sequence spread spektrum
EIA	Electronics Industry Association
FDDI	Fiber Distributed Data Rozhraní
FHSS	Frequency bopping spread spektrum
FM	Frequency modulation
FO	Fiber Optic
FRS	Family Radio Service
IP	Internet Protocol
LAN	Local Area Network lokální síť
MAC	Media Access Control
MAU	Multistation Access Unit
MAN	Metropolitan Area Network
MTU	Maximum transmission unit

NAT	Network Address Translation
NIC	Network rozhraní card
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
PCF	Point Coordination Function - Funkce bodové koordinace
QAM	Quadrature amplitude modulation
QFDM	Quadroture frequency division multiplexing
QPSK	Quadrature Phase Shift Keying
RF	Radio frequency
RIP	Routing Information Protocol
SSID	Service Set Identifier
STP	Shielded Twisted Pair
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
WAN	Wide Area Network
WDS	Wireless Distribution Systém
Wi-Fi	Wireless Fidenlity
WINS	Windows Internet Naming Service

SEZNAM OBRÁZKŮ