

Renovace počítačové sítě ZŠ a MŠ Kanice

Bakalářská práce

Vedoucí práce:

Ing. Jiří Balej

Martin Kučera

Brno 2015

Rád bych poděkoval svému vedoucímu práce, panu Ing. Jiřímu Balejovi, za cenné rady, připomínky a čas strávený kontrolou a metodickým vedením při zpracování závěrečné práce.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Renovace počítačové sítě ZŠ a MŠ Kanice** vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací*.

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmetná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 21. května 2015

Abstract

Kučera, M. Renovation of a network ZŠ a MŠ Kanice. Brno: Mendel University, 2015.

The object of this bachelor thesis is a renovation of computer network at Elementary School in Kanice. The task is to move the ICT classrooms and network elements to the new floor. Another task is to lay out and create a wireless communication between buildings of the Elementary School. Final task of this thesis will be to create Wi-Fi for students, which will have a limited speed capacity. This thesis ends with the economical evaluation of the entire project.

Keywords

Wireless communication, MikroTik, Wi-Fi, security, computer network.

Abstrakt

Kučera, M. Renovace počítačové sítě ZŠ a MŠ Kanice. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2015.

Tahle bakalářská práce se zabývá renovací sítě v ZŠ a MŠ Kanice. Úkolem je přesunutí ICT učebny a síťových prvků do nového patra. Dalším úkolem je navržení bezdrátové komunikace mezi budovami ZŠ a MŠ. Na závěr vytvoříme Wi-Fi síť pro studenty, která bude mít omezenou rychlostní kapacitu. Práce je zakončena ekonomickým zhodnocením celého projektu.

Klíčová slova

Bezdrátová komunikace, MikroTik, Wi-Fi, zabezpečení, počítačová síť.

Obsah

1	Úvod a cíl práce	14
1.1	Úvod.....	14
1.2	Cíl práce.....	14
2	Přehled literatury	16
2.1	Literatura v oblasti LAN sítě	16
2.2	Literatura v oblasti bezdrátové komunikace.....	16
2.3	Internetové stránky.....	17
3	Teoretický úvod	18
3.1	Rozdělení sítě.....	18
3.1.1	Podle velikosti	18
3.1.2	Dělení podle úlohy prvků.....	18
3.2	Přenosová média	18
3.2.1	Metalické kabely.....	19
3.2.2	Optické vlákno.....	19
3.2.3	Bezdrátová komunikace.....	19
3.3	Síťové modely.....	20
3.3.1	Referenční model ISO/OSI.....	20
3.3.2	Topologie sítě	21
3.3.3	Aplikační služby.....	21
3.4	Bezpečnost sítě.....	22
3.4.1	Základní pojmy.....	22
3.4.2	Častá rizika.....	22
3.4.3	Firewall	23
3.5	Aktivní síťové prvky.....	23
3.5.1	HUB.....	23
3.5.2	Bridge.....	24
3.5.3	Switch	24

3.5.4	Router	24
3.6	Windows Server.....	24
3.6.1	Edice rodiny Windows server 2012 R2	24
3.6.2	Adresářová služba (AD – Active Directory)	25
3.7	Bezdrátový přenos v pásmech 5 GHz	25
3.7.1	Podmínky využívání radiových kmitočtů 2,4 – 66 GHz.....	25
3.7.2	CSMA	26
3.7.3	TDMA	27
3.7.4	Protokoly	27
3.7.5	Polarizace	29
3.7.6	Zabezpečení.....	29
3.8	EoIP tunel	30
4	Současný stav sítě	31
4.1	Struktura sítě	31
4.1.1	ICT učebna	31
4.1.2	Ostatní místnosti s výpočetní technikou.....	31
4.1.3	Wi-Fi síť	32
4.1.4	Aktuální síťové prvky	33
4.2	Současný stav v mateřské škole	33
4.3	Zabezpečení sítě.....	34
4.4	Konektivita k síti Internet.....	34
5	Návrh řešení – implementace	36
5.1	Přemístění ICT učebny	36
5.2	Návrh 5 GHz přenosu.....	37
5.2.1	MikroTik SXT Lite 5	37
5.2.2	Podmínky využití pásma 5 GHz.	37
5.2.3	Nastavení vysílače.....	38
5.2.4	Nastavení přijímače.....	41
5.2.5	Testování	43
5.3	Návrh Wi-Fi sítě	48
5.3.1	MikroTik 951Ui-2HnD.....	48
5.3.2	Nastavení AP	48

5.3.3	Testování Wi-Fi.....	52
5.4	Závěrečné testování celé sítě.....	54
6	Ekonomické zhodnocení projektu	56
7	Závěr	57
8	Reference	58
A	Fyzický nákres staré sítě	62
B	Fyzický nákres nové sítě	64
C	Přenosová rychlost při šířce pásma 40 MHz.	68
D	Nastavení hlavního routeru.	69

Seznam obrázků

Obr. 1	Referenční model ISO/OSI.....	20
Obr. 2	Firewall hlídající provoz.	23
Obr. 3	Technické parametry stanic.	26
Obr. 4	Záložka Nstreme na MikroTik SXT Lite 5.	29
Obr. 5	Nastavení hesla pro WPA i WPA2 na MikroTiku.	30
Obr. 6	Současná topologie sítě.....	32
Obr. 7	Active Directory běžící na Windows server 2012.	34
Obr. 8	Návrh sítě z hlediska topologie.....	36
Obr. 9	Scan sítě 5180 až 5865 MHz.....	38
Obr. 10	Vymazání defaultní konfigurace.	39
Obr. 11	Spojení rozhraní v Bridge.	39
Obr. 12	Wireless nastavení na vysílači.	40
Obr. 13	Vyzařovací výkon TX.	41
Obr. 14	Wireless nastavení na přijímači.....	42
Obr. 15	Status konektivity.....	43
Obr. 16	Bandwidth test s protokolem 802.11n.....	44
Obr. 17	Omezení rychlosti na 90 Mbps.	45
Obr. 18	latence bez zátěže.	45
Obr. 19	Bandwidth test s protokolem Nstreme	46
Obr. 20	Bandwidth test s protokolem Nv2	46
Obr. 21	Latence při maximální zátěži u protokolu Nv2.	47
Obr. 22	Vytvoření EoIP tunelu.	49

Obr. 23	Omezení rychlosti.....	50
Obr. 24	Firewall rules	50
Obr. 25	Vysílací rozhraní.	51
Obr. 26	Přemostění rozhraní.....	51
Obr. 27	Plánovač vypínání a zapínání rozhraní wlan2.	52
Obr. 28	Testování Wi-Fi studenti.....	53
Obr. 29	Měření rychlosti ve Wi-Fi síti Studenti.....	53
Obr. 30	Přechod mezi přístupovými body.....	54
Obr. 31	Monitoring sítě při toku dat.....	55
Obr. 32	Fyzický nákres staré sítě - přízemí	62
Obr. 33	Fyzický nákres staré sítě - 1.patro	63
Obr. 34	Fyzický nákres nové sítě - přízemí.....	64
Obr. 35	Fyzický nákres nové sítě - 1.patro.....	65
Obr. 36	Fyzický nákres nové sítě - 2.patro.....	66
Obr. 37	Fyzický nákres nové sítě - školka	67
Obr. 38	Bandwidth test s protokolem 802.11n a s šířkou pásma 40 MHz.....	68
Obr. 39	Nastavení bridge u hlavního routeru.....	69
Obr. 40	Nastavení DHCP, Addresses a NTP serveru na hlavním routeru.	69
Obr. 41	NAT na hlavním routeru.....	70
Obr. 42	Prostředí RouterOS v programu Winbox.	70

Seznam tabulek

Tab. 1	Standardy IEE 802.11	20
Tab. 2	Technické parametry RB 951UI-2HnD.....	33
Tab. 3	Technické parametry SXT Lite 5	37
Tab. 4	Výsledky testování jednotlivých protokolů.....	47
Tab. 5	Celková cena za projekt.....	56

1 Úvod a cíl práce

1.1 Úvod

V dnešní době je ve školách nezbytnou součástí i počítačová síť. Moderní komunikační technologie zajišťují organizacím značné výhody. Jen minimum organizací nevyužívá počítačové sítě. Výjimkou není ani ZŠ a MŠ Kanice. Tato krásná škola leží asi 6 km od Brna a navštěvuje ji asi 170 studentů všech kategorií.

První počítače dostala škola kolem roku 2000 a každým rokem přibýval počet zařízení. Po pár letech se vedení školy rozhodlo otevřít učebnu informatiky. Od té doby se počítačová síť rozšiřuje a téměř v každé učebně najdeme PC, který slouží k vyhledávání informací pro kantory i žáky.

Poskytovatelem Internetu se stala místní firma TS-Hydro s.r.o, která se zabývá internetovým připojením od roku 2003 a ZŠ Kanice byla jedním z prvních zákazníků. Jelikož majitelé firmy jsou jejími bývalými žáky, pomohli vybudovat moderní komunikační infrastrukturu počítačové sítě a škola díky tomu nemusela platit drahé externí specialisty.

V roce 2011 se otevřela nově zbudovaná mateřská škola, která stojí asi 30 metrů od budovy ZŠ. Dalším důležitým projektem je rekonstrukce 2. patra, který má být v provozu od 1.9. 2015. Díky zapojení školy do projektu *EU peníze školám*¹ dostala škola v roce 2013 peníze na přebudování nové počítačové infrastruktury.

1.2 Cíl práce

Cílem bakalářské práce je zprovoznit a rozšířit počítačovou síť. Prvním krokem bude přemístit učebnu ICT a síťové prvky do serverovny. Hlavním úkolem je propojení ZŠ a MŠ pomocí dvoubodového bezdrátového spoje. Dalším cílem je vytvoření Wi-Fi sítě pro studenty a učitele. Studenti budou mít omezené přenosové rychlosti, aby nenarušovali běh sítě. Také nebudou mít přístup do školní sítě. Síť musí splňovat současné a budoucí požadavky. V závěru práce provedeme ekonomické zhodnocení celého projektu.

Nová infrastruktura byla zhotovena v loňském roce během prázdnin, ale z důvodu dostavby druhého patra síť není zcela v provozu. Zprostředkování WIFI je velice důležité pro zaměstnance, kteří využívají notebooky k práci. Jako hlavní cíl práce bude dobře fungující point-to-point spoj na 5 GHz frekvenci. Celá síť bude fungovat na platformách MikroTik. Tento výrobce patří několik let mezi špičku v bezdrátových komunikacích a v posledních letech i oblastech vnitřních zařízení. MikroTik využívá vlastní operační systém RouterOS. Tento operační systém nabízí širokou škálu možností nastavení.

RouterOS poskytuje funkce pro detailní testování, což je pro tuto práci velice důležité. Správné zapojení je dobrým předpokladem kvalitně fungující sítě. Je po-

¹ Peníze školám: <http://www.op-vk.cz/cs/eu-penize-skolam/eu-penize-zakladnim-skolam/>

třeba podrobně nastudovat bezdrátovou komunikaci, kde se nachází množství způsobu spojení.

Zabezpečení sítě je v dnešní době nezbytnou součástí. Z důvodu neoprávněného přístupu je potřeba nastavit na každém zařízení heslo. U bezdrátové komunikace musíme zavést šifrování, kde existuje několik různých standardů.

2 Přehled literatury

Článků a dostupné literatury týkající se návrhu sítě je nespočetné množství. Literatura vybraná pro tuto bakalářskou práci poskytuje dostatečné informace k sestavení lokální počítačové sítě. Na základě analýzy prostředí místní školy v Kanicích bude navržena LAN síť jak z funkčního a výkonnostního hlediska, tak i z pohledu finančních nákladů potřebných na výstavbu a údržbu této sítě.

2.1 Literatura v oblasti LAN sítě

K oprášení znalostí komunikačních sítí nám pomůže kniha „Moderní komunikační sítě od A do Z“ (Pužmanová, 2006), která popisuje principy síťové komunikace, přenosové prostředky, technologie bezdrátových a optických sítí. Důležitou vlastností každé LAN sítě je stabilita. Základem je správné zapojení a instalace. V tomto směru nám pomůže kniha „Sítě LAN: hardware, instalace a zapojení“ (Trulove, 2009). Seznámení s MikroTik RouterOS nám pomůže anglická literatura „Learn RouterOS“ (Burgess, 2009), která popisuje software MikroTiků a práci s Winboxem. Tento program je zdarma a slouží ke konfiguraci síťových prvků značky MikroTik.

Síťové protokoly nám popisuje „Velký průvodce protokoly TCP/IP a systémem DNS“ (Kabelová a Dostálek, 2008). Tato kniha se zabývá rozlišením základních protokolů, manipulací s adresami IPv4/IPv6 a také aplikačními protokoly FTP, HTTP, SMTP, POP3 aj. Kniha mimo jiné popisuje práci s programy nmap a Wireshark, který slouží k monitorování sítě. Bakalářská práce „Renovace sítě a počítačových učeben na SOŠ Podyji“ (Šupola, 2014) má velice podobný návrh řešení ohledně výměny prvků v síti. Práce se ovšem nezabývá bezdrátovou komunikací. K tomuto tématu nám poslouží bakalářská práce „Mapování a analýza WiFi sítě Österreich institutu v Brně“ (Šturma, 2014).

2.2 Literatura v oblasti bezdrátové komunikace

V oblasti bezdrátové komunikace nám poskytne základní znalosti kniha „Vytváříme domácí bezdrátovou síť“ (Horák, 2011). Zde se dozvíme hlavně o vysílání na frekvenci 2,4 GHz, kterou budeme používat pro Wi-Fi. Kniha popisuje mimo jiné nastavení počítačů k připojení k přístupovému bodu, rady pro výběr hardwaru a zabezpečení bezdrátové domácí sítě. Pro bezdrátový přenos mezi budovami nám pomůže diplomová práce „Bezdrátové sítě v zarušených prostředích“ (Skipala, 2011). Tato práce využívá platformu Mikrotik na 5 GHz bezdrátový přenos. Pro podrobné informace můžeme použít přednáškový materiál „Moderní bezdrátová komunikace“ (Slanina, 2010). Tato skripta detailně popisují historii bezdrátové komunikace, anténní systémy a mobilní komunikační systémy.

2.3 Internetové stránky

Internetová síť je největší databází informací na světě. Informace ale nemusí být vždy pravdivé. Proto je dobré si zdroj víckrát ověřit než se publikuje. Neocenitelnou pomůckou na internetu jsou stránky výrobců, kde můžeme najít manuály ke každému hardwaru. Také zde můžeme najít pravidelnou aktualizaci softwaru (firmwaru) a řešení často se vyskytujících problémů. Litevská společnost MikroTik² nabízí na svém webu školení MikroTik Academy. Mezi další výrobce patří i společnost Cisco Systems, Inc³, která patří mezi největší počítačové firmy dnešní doby. Dalším zdrojem informací mohou být diskuzní fóra, kde uživatelé přispívají svými zkušenostmi a snaží se vyřešit problém dotazujícího. Nejedná se ale o věrohodný zdroj.

² <http://www.mikrotik.com/>

³ <http://www.cisco.com/>

3 Teoretický úvod

Počítačová síť je označení pro technické prostředky, které jsou spojeny pomocí síťových prvků a uživatelských stanic. Účelem je sdílení informací, hardwaru a konektivity k síti Internet. Každý síťový prvek musí být propojen kabeláží nebo bezdrátovým spojením. Počítačovou síť můžeme dělit podle určitých kritérií.

3.1 Rozdělení sítě

3.1.1 Podle velikosti

- PAN (Personal area network) – osobní síť.
- LAN (Local area network) – lokální počítačová síť nebo místní síť.
- MAN (Metropolitan area network) – metropolitní síť propojující lokální sítě.
- WAN (Wide area network) – rozlehlá síť, která spojuje LAN a MAN sítě.

3.1.2 Dělení podle úlohy prvků

1. Peer-to-peer (rovný s rovným). Jedná se o síť, ve které spolu komunikují jednotliví klienti (uživatelé). Data a prostředky se nacházejí na jednotlivých počítačích, které jsou zapojeny v síti. Toto uspořádání má řadu nevýhod. Počítače musí být neustále zapnuty a při větším množství zařízení je těžké mít přehled o všech sdílených prostředcích. Peer-to-peer spoje jsou často cílem tradičních útoků jako například DoS útoky, viry nebo spamy. (Pužmanová, 2006).
2. Client-server. Rozděluje připojené stroje na klienty a servery, kteří komunikují přes počítačovou síť. Všechna data a prostředky jsou uloženy na serveru. Klientské počítače už zpravidla žádnou službu neposkytují. Přenosová kapacita se dělí mezi připojené klienty. Server navíc může přidělovat klientům oprávnění k jednotlivým prostředkům. Pokud dojde k výpadku serveru, nemůžou být požadavky klientů splněny. (Pužmanová, 2006).

3.2 Přenosová média

Z hlediska funkčnosti dělíme přenosová média do tří základních skupin. První skupinou jsou *metalické kabely*, které využívají pro přenos elektromagnetické vlnění. *Optické vlákno* je druhá skupina, která pro šíření informací využívá světelné paprsky. Poslední skupinou je *bezdrátová komunikace*, kde využíváme vlnění na určité frekvenci.

3.2.1 Metalické kabely

Jedná se o nejběžnější přenosové medium. Informace se přenášejí na principu elektromagnetického signálu. V oblasti počítačových sítí se využívají dva typy kabelů. Jedná se o koaxiální kabel a o kroucenou dvojlinku.

1. Koaxiální kabel

Koaxiální kabel je asymetrický elektrický kabel, který se skládá ze 4 vrstev. První vrstva, nazývaná vnitřní vodič, bývá zhotovena z mědi. Izolační vrstva mezi vnitřním a vnějším vodičem je označována jako dielektrikum. Další vrstvou je vnější vodič, který bývá zhotoven z hliníkové nebo měděné folie. Poslední vrstvou koaxiálního kabelu je plášť. (Šupola, 2014).

2. Kroucená dvojlinka

Symetrický druh kabelu, jenž je tvořen páry vodičů, které jsou pravidelně zkrouceny. Jedná se v současnosti o nejpoužívanější metalický kabel. Kroucená dvojlinka je použitelná pouze pro vytváření dvoubodových spojů a navíc je omezena jen na maximální vzdálenost 100m. (Trulove,2009).

3.2.2 Optické vlákno

Optická vlákna jsou široce využívána pro přenos informací prostřednictvím světla na velké vzdálenosti při vyšších přenosových rychlostech dat. Odolávají elektromagnetické interferenci a přeslechům. Principem funkčnosti je převod elektrického signálu na světelný, který provádí LED (Light Emitting Diode) dioda nebo laserová dioda. Téměř vždy potřebujeme duplexní spoj, proto musíme mít dvojici vláken – pro každý směr jedno. Rozlišujeme dva typy optických vláken:

- **Mnohovidová vlákna** – Využívají se pro komunikaci na krátké vzdálenosti. Buzení pomocí LED, u gigabitového Ethernetu pomocí laseru. Levnější varianta oproti jednovidovým vláknům.
- **Jednovidové vlákna** - Tato vlákna se používají pro spojení na velké vzdálenosti. Tento druh vlákna má úzké jádro a vlivem toho se paprsek šíří vláknem rovnoběžně, nedochází zde k odrazu mezi oběma skly. (Kabelová, 2002)

3.2.3 Bezdrátová komunikace

Bezdrátová komunikace spočívá ve spojení dvou subjektů jinak než mechanickým kabelem. Může se jednat o komunikaci optickou (světelnou), radiovou a sonickou (zvuk). Aktuálně se zatím nejvíce osvědčil přenos pomocí radiového signálu. Je to proto, že optické spoje lze využít pouze na krátké vzdálenosti. U optické komunikace se setkáváme s laserovým světlem nebo světlem infračerveným. U radiové komunikace se využívá rádiových vln, které vysílají na určité frekvenci. Sonická komunikace pracuje na principu přenosu zvukových signálů.

Nejpoužívanějším standardem v bezdrátových komunikacích LAN v ČR je WI-FI (Wireless Fidelity), které dodržují normy IEEE 802.11. Původně bylo WI-FI určeno jako náhrada za metalické rozvody sítě, avšak díky bezplatnosti frekvenci

2,4 GHz se stalo oblíbeným způsobem přístupu k Internetu. Mezi hlavní výhody WI-FI patří snadná instalace, nízká cena a velké množství výrobků. Z toho vyplývá hlavní nevýhoda, a to je rušení. Ve 2,4 GHz pásmu je v Evropě k dispozici celkem třináct kanálů, které se navzájem překrývají, takže ve skutečnosti lze použít tři nepřekrývající se kanály.

Pásmo 5 GHz se stalo u nás novou bezplatnou frekvencí v roce 2005 a přineslo do bezdrátových komunikací obrovský posun. Rozsah pásma je značně větší a není hlavně ovlivněn zařízeními pracujícími v pásmu 2,4 GHz. Tím je zaručena vyšší přenosová rychlost a stabilita.

IEEE 802.11 je Wi-Fi standard s dalšími doplňky značící se písmenem na konci. Tento standard zahrnuje několik typů modulací pro vysílání radiových signálů. IEEE 802.11

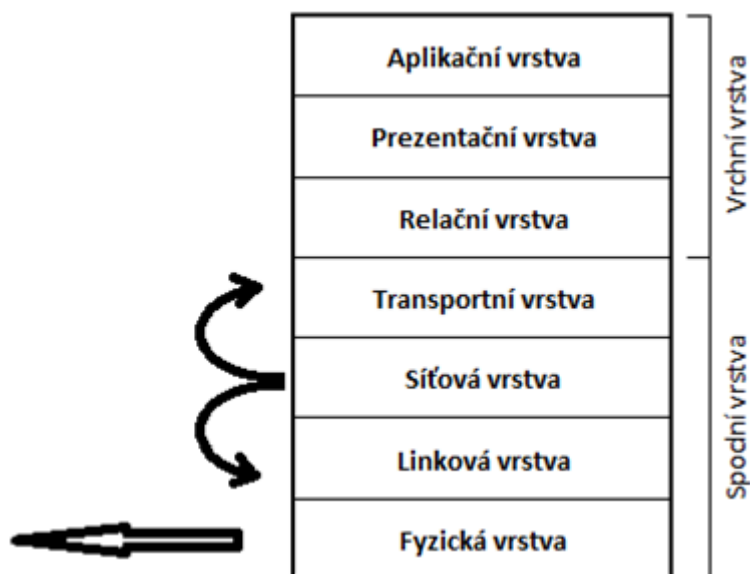
Tab. 1 Standardy IEEE 802.11

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Modulační techniky
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11y	2008	3,7	54	
IEEE 802.11ac	2013	5	1000	MU-MIMO OFDM
IEEE 802.11ad	2014	2,4, 5 a 60	7000	

3.3 Síťové modely

3.3.1 Referenční model ISO/OSI

Jedná se o teoretický model, který byl vytvořen za účelem sjednocení komunikace mezi různými produkty výrobců. Je založen na sedmi referenčních vrstvách, které se dělí na horní a spodní vrstvy, přičemž horní vrstva je uživateli nejbližší. Horní vrstvy se zabývají aplikačními prvky, zato spodní vrstvy jsou implementovány nejen v hardwaru, ale i v softwaru. V rodině protokolů TCP/IP jsou použity pouze čtyři vrstvy (aplikační vrstva, transportní vrstva, síťová vrstva a síťové rozhraní).



Obr. 1 Referenční model ISO/OSI

3.3.2 Topologie sítě

Topologie sítě se zabývá rozmístěním a propojením jednotlivých prvků v síti. Základní typy topologií jsou:

- **Sběrníková topologie** – zastaralá technologie. Má řadu nevýhod, jako je omezení délky kabeláže, malý výkon sítě při zátěži a složitá diagnostika závad. Výhodou sběrníkové topologie je nízká pořizovací cena a jednoduchý způsob zapojení.
- **Kruhová topologie** – vzniká spojením dvou konců dohromady. Má komplikovanou diagnostiku závady a na trase má více přenosových uzlů. Výhodou jsou nižší náklady na vybudování sítě.
- **Hvězdicová topologie** – jedná se o nejpoužívanější topologii. Každý počítač je připojen do centrálního prvku (Switch, Hub). Musí se ovšem použít hodně kabeláže a při výpadku centrálního prvku vypadne celá síť.
- **Stromová topologie** – propojení více hvězdicových sítí.
- **Mesh topologie** – topologie sítě, ve které jsou některé uzly přímo propojeny s více než jedním dalším uzlem v síti.

3.3.3 Aplikační služby

- **HTTP (Hypertext Transfer Protocol)** – protokol sloužící pro komunikaci mezi WWW servery a jejich klienty. Používá obvykle TCP port 80. Pomocí rozšíření služby MIME umí přenášet jakýkoliv soubor. Pro bezpečný režim se používá HTTPS, kde jsou data šifrována.
- **NTP (Network Time Protocol)** – tento protokol slouží k synchronizaci času. Zajišťuje, aby všechny prvky v síti měly stejný čas.

- **SMTP (Simple Mail Transfer Protocol)** – poštovní protokol pro vzájemnou komunikaci mezi přepravci elektronické pošty. Používá TCP port 25. Patří mezi jedny z nejstarších aplikačních služeb.
- **DHCP (Dynamic Host Configuration Protocol)** – Protokol, který umožňuje prostřednictvím DHCP serveru nastavit stanicím IP adresu, masku, bránu, DNS atd. Patří do rodiny TCP/IP.
- **DNS (Domain Name Server)** – hlavním úkolem DNS jsou převody doménových jmen a IP adres uzlů sítě. Později přibral i další funkce (např. IP telefonii). Používá TCP port 53.

3.4 Bezpečnost sítě

Bezpečnost sítě se stala nezbytnou součástí každého informačního systému. Zabezpečení sítě se skládá z předpisů a politik, které obsahují shrnutí bezpečnostních požadavků pro řešení informační bezpečnosti na různých úrovních, od fyzické až po počítačovou a komunikační bezpečnost. Cílem je zabránit neoprávněnému přístupu či sledování, zneužití a modifikaci citlivých dat. (Loveček, 2006)

3.4.1 Základní pojmy

3. Autentizace

Jedná se o proces, který ověří identitu subjektu. Negarantuje přístupová práva do zdrojů systému.

4. Autorizace

Subjekt je důvěryhodný a získal souhlas s provedením určité činnosti.

5. Hrozba

Určité zranitelné místo, které vytváří možnost průniku do systému a porušit důvěryhodnost a integritu aktiv.

6. Nepopíratelnost

Vyloučení možnosti popřít dřívější provedení nějaké operace. (Wikipedia, 2014).

7. Útok

Uskutečnění hrozby. Úmyslně cílí na zranitelné místo za účelem způsobení škod.

8. Riziko

Je pravděpodobnost využití zranitelného místa, pokud existuje nějaká hrozba (Hanáček, Staudek, 2000)

3.4.2 Častá rizika

- Zastaralý hardware a software.

- Vlastní zařízení zaměstnanců
- Neloajální zaměstnanci.
- Špatně nastavené procesy

3.4.3 Firewall

Jedná se o hardwarové nebo softwarové zařízení, které slouží k zabezpečení síťového provozu zpravidla mezi internetem a lokální sítí. Principem funkčnosti je kontrolovat provoz podle daných pravidel. Firewally rozdělujeme nejčastěji do následujících kategorií:

- Paketové filtry
- Stavový firewall
- Aplikační proxy



Obr. 2 Firewall hlídající provoz.

Zdroj: <http://www.gocit.vn/bai-viet/firewall-how-to-dynamically-manage-firewall-in-rhelcentos-7-0/>

3.5 Aktivní síťové prvky

Aktivní síťové prvky slouží ke vzájemnému propojení v počítačových sítích. Jedná se o prvky, které působí aktivně na přenášený signál.

3.5.1 HUB

Síťový prvek, který je známý také jako *rozbočovač*. Pracuje na první vrstvě modelu ISO/OSI a je základním stavebním prvkem v topologii Star. Tento aktivní prvek se chová jako opakovač. Všechna data, která přijdou na jeden z portů, tak zkopíruje na ostatní porty. To má za následek zbytečné přetěžování segmentů. Nástupcem rozbočovače (HUB) se stal Switch.

3.5.2 Bridge

Bridge (most) funguje na druhé vrstvě v modelu ISO/OSI. Principem činnosti je oddělený provoz dvou segmentů sítě, kde si v paměti sestaví tabulku s MAC adresami a porty. Pokud se dvě komunikující zařízení nachází v jednom segmentu, bridge rámce do jiných segmentů neodešle.

3.5.3 Switch

Switch (přepínač) je speciální aktivní prvek vyvinutý jako nástupce HUBu. Důvody pro jeho návrh a realizaci byly čistě technické, protože HUB nesplňoval zátěž stále náročnějšího datového toku a stával se tedy oním slabým článkem v síti. Bylo nutno vytvořit prvek, který nebude síť brzdit v přenosu, toku dat a bude ji částečně umět řídit svým jistým interním systémem. Switch jako i HUB má porty, konektory, do kterých připojíte kabely. Při aktivitě v síti „posbírá“ SWITCH všechny potřebné informace – MAC adresy (Media Access Control) a čísla portů, které jsou mu dostupné a vytvoří si CAM tabulku (Content Addressable Memory table). Pokud se chce počítač spojit s druhým počítačem, „podívá“ se switch do CAM tabulky a najde cestu. Vytvoří spojení pouze mezi dvěma konektory a nezatěžuje zbytečně další konektory, které obsluhuje. (Spurná, 2010).

3.5.4 Router

Router (Směrovač) je zařízení, které řídí chod paketů. Patří mezi nejinteligentnější prvky sítě. Pracuje na třetí vrstvě v modelu ISO/OSI. Hlavním úkolem routeru je směrování datagramů k cíli na základě IP adresy, která je uvedena v hlavičce paketu. Fyzicky tedy propojuje sítě, které jsou mezi sebou logicky odděleny. Směrovače lze vidět v kombinaci i s dalšími prvky, jako například v kombinaci se switchem, nebo s integrovaným firewallem (brána zabezpečení). (Jirovský, 2001)

3.6 Windows Server

Windows server je operační systém od firmy Microsoft. Je určen pro použití jako server v počítačové síti. V současnosti je nejnovější verze Windows Server 2012 R2, která se rozděluje do několika edic.

3.6.1 Edice rodiny Windows server 2012 R2

- **Edice Windows Server 2012 R2 Datacenter** – pro vysoce virtualizovaná privátní cloudová prostředí.
- **Edice Windows Server 2012 R2 Standard** – pro lehce nebo zcela nevirtualizovaná prostředí.
- **Edice Windows Server 2012 R2 Essentials** – malé firmy s maximálně 25 uživateli na serverech až se dvěma procesory.

- **Edice Windows Server 2012 R2 Foundation** – malé firmy s maximálně 15 uživateli na serverech s jedním procesorem

3.6.2 Adresářová služba (AD – Active Directory)

Služba Active Directory je vlastně adresářová služba, která je součástí systému Windows Server. Tato služba zahrnuje adresář (Directory) a je to vlastně databáze s hierarchickou strukturou, ve které jsou uloženy informace o distribuovaných prostředcích, o službách. Prostřednictvím nich jsou tyto informace užitečné a lehce dostupné. Adresář se však liší od klasické relační databáze. Je totiž navržen tak, aby vyhovoval častému čtení, vyhledávání a jen k občasnému záznamu. Přístup k záznamům můžeme libovolně omezovat pomocí ACL (Access Control List). V podstatě všechny verze systému Windows Server a to začátkem systému Windows 2000 podporují službu Active Directory. (Staněk, 2009).

Služby, které využívají službu Active Directory, se nazývají domény služby Active Directory. Data jsou uložena na jediném úložišti a tím jeho údržba nevyžaduje velký rozsah správy. Využití fyzických a logických struktur umožňuje měnit velikost adresáře tak, aby nejlépe splňoval požadavky růstu firmy nebo podniku. (Staněk, 2009).

3.7 Bezdrátový přenos v pásmech 5 GHz

3.7.1 Podmínky využívání radiových kmitočtů 2,4 – 66 GHz

Pravidla bezdrátové komunikace určuje Český telekomunikační úřad. Na stránkách ČTÚ⁴ se dozvíme aktuální informace o provozu jednotlivých kmitočtů. Podmínky provozu v pásmech 2,4 až 66 GHz jsou definovány všeobecným oprávněním č. VO-R/12/09.2010-12. (viz obrázek č. 1). Po nedodržování pravidel může ČTÚ udělit pokutu. Informace ze seminářů k problematice sítí RLAN pořádaných ČTÚ jsou dostupné na jejich webu. V této bakalářské práci nás zajímá provoz na frekvencích 2,4 a 5 GHz.

⁴ <https://www.ctu.cz/>

Ozn.	Kmitočtové pásmo	Vyzářený výkon	Maximální spektrální hustota e.i.r.p.	Další podmínky
a	2400,0–2483,5 MHz	100 mW e.i.r.p. ²⁾	10 mW/1 MHz	systémy s technikou DSSS ⁵⁾ nebo OFDM ³⁾
			100 mW/100 kHz	systémy s technikou FHSS ⁶⁾
b	5150–5250 MHz	200 mW střední e.i.r.p. ^{2), 7)}	10 mW/MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz)	pouze pro použití uvnitř budovy ⁸⁾
c	5250–5350 MHz	200 mW střední e.i.r.p. ^{2), 7)}	10 mW/MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz)	pouze pro použití uvnitř budovy ⁸⁾
d	5470–5725 MHz	1 W střední e.i.r.p. ^{2), 7)}	50 mW/MHz (střední spektrální hustota v libovolném úseku širokém 1 MHz)	—
e	17,1–17,3 GHz	100 mW střední e.i.r.p. ⁷⁾	—	—
f	57–66 GHz	40 dBm střední e.i.r.p. ⁷⁾	13 dBm/MHz (střední spektrální hustota)	Stále venkovní instalace jsou vyloučeny

- c) stanice musí dodržet maximální vyzářený výkon e.i.r.p. a maximální střední spektrální hustotu při libovolné kombinaci výstupního výkonu vysílače a použité antény;
- d) stanice nesmějí být provozovány s přidavnými zesilovači vysokofrekvenčního výkonu a s převaděči;
- e) stanice v pásmech c a d musí být vybaveny automatickou regulací výkonu, která průměrně poskytuje činitel potlačení rušení alespoň 3 dB oproti maximálnímu povolenému výstupnímu výkonu uvedených systémů. Není-li automatická regulace výkonu použita, snižuje se maximální povolený střední e.i.r.p. a odpovídající mez střední hustoty e.i.r.p. pro pásma c a d o 3 dB;
- f) v pásmech c, d a f musí být použity techniky přístupu ke spektru a zmírnění rušení, které poskytují přinejmenším rovnocenný účinek jako techniky popsané v harmonizovaných normách⁹⁾. Technologie potlačení rušení v pásmech c a d musí vyrovnávat pravděpodobnost výběru konkrétního kanálu ze všech dostupných kanálů, aby se v průměru zajistilo rovnoměrné rozprostření zátěže spektra a aby byl zajištěn provoz slučitelný se systémy rádiového určování;
- g) stanice jsou provozovány na sdílených kmitočtech;
- h) provoz stanice nemá zajištěnu ochranu proti rušení způsobenému vysílacími rádiovými stanicemi jiné radiokomunikační služby provozovanými na základě individuálního oprávnění k využívání rádiových kmitočtů nebo jinými stanicemi pro širokopásmový

Obr. 3 Technické parametry stanic.

Zdroj: http://www.ctu.cz/cs/download/ooop/rok_2010/vo-r_12-09_2010-12.pdf

3.7.2 CSMA

Jedná se o metodu náhodného přístupu k médiu, kde každá stanice před vlastním vysláním kontroluje přítomnost signálu v médiu, zda není sdílené médium již využívané k přenosu jinou stanicí. Může nastat situace, kdy během krátkého intervalu chtějí dvě stanice po sobě zahájit vysílání. Jestliže je tento interval kratší než doba šíření signálu po médiu, druhá stanice pak nemůže v daném okamžiku zaznamenat, že médium je již obsazené a začne také vysílat, čímž způsobí kolizi. (Ručka, 2007).

V CSMA je nemožné zcela zabránit kolizím, avšak existují způsoby, jak se s nimi vypořádat. Existují metody, které předcházejí kolizím:

9. Metoda CSMA/CA

Uzel naslouchá aktivitě sítě a hledá nosný signál, který indikuje aktivitu na síti. Pokud uzel neslyší nosný signál a chce něco přenést, pošle RTS signál na síť. Jestliže se očekává přenos do určitého uzlu, čeká vysílací stanice na CTS signál. Pokud CTS signál není přijat, vysílací stanice předpokládá kolizi a celou akci v náhodných intervalech opakuje. Přijatý signál CTS znamená zahájení vysílání paketů na určitý uzel. Jedná-li se o zprávy, nečeká se na CTS signál. (Ručka, 2007).

10. Metoda CSMA/CD

Nejrozšířenějším představitelem metody CSMA/CD je klasický Ethernet. V průběhu odesílání rámce si tato stanice sama zjišťuje, zda její signál nekoliduje se signálem jiné stanice, která začala vysílat ve stejné době. Tato vlastnost se nazývá detekce kolizí (Collision Detection – odtud zkratka CD). (Ručka, 2007).

Pro síť WLAN jsou definovány dva typy koordinačních funkcí, distribuované a centralizované.

- **Distribuovaná koordinační funkce** (DCF – Distributed Coordination Function) je specifikována v standardu 802.11 a lze ji využít v BSS, ESS i IBSS. V tomto případě se využívá náhodná přístupová metoda a stanice soutěží o přístup k médiu.
- **Centralizovaná koordinační funkce** (Point Coordination Function) představuje přístupovou metodu bez soutěžení. U této přístupové metody se přístupový bod pravidelně dotazuje všech stanic a zjišťuje, zda nemají data k vysílání.

3.7.3 TDMA

TDMA (Time Division Multiple Access) je přístupová metoda k médiu pro sdílené síť. V TDMA uživatelé využívají stejný rádiový přenosový kanál. Tento kanál je ale rozdělen v čase na jednotlivé časové díly (timesloty), jejichž určitý počet formuje TDMA rámec opakující se pravidelně v čase. Z důvodu sdílení frekvenčního kanálu více uživatelů není telefonní hovor nebo přenos dat souvislý, daný uživatel má kanál přidělen jen po dobu trvání přiděleného časového dílu. (Kokešová, 2006).

3.7.4 Protokoly

1. IEEE 802.11n

Protokol 802.11n patří do rodiny Wi-Fi standardů IEEE 802.11. Standard 802.11 je označován jako původní a jelikož byl postupem času pomalý a nevyhovující, vzniklo označení 802.11x. Tímto výrazem se označuje celá skupina upravujících doplňků označená písmeny. Mezi starší standardy patří 802.11b a 802.11g. Aktuálně jde u některých přenosových médiích využívat standard

802.11ac. Současným nejpoužívanějším standardem je 802.11n, který byl schválen v roce 2009. Vznikl jako reakce zajistit odpovídající datovou propustnost pro dnešní stále náročnější aplikace. Jde o technologicky vylepšený standard využívající funkcionality:

- MIMO (Multiple-Input Multiple- Output)
- Šířka pásma až 40 MHz.
- Využívá prostorový multiplexing.
- Shlukování rámců na podvrstvě MAC.

Maximální teoretické rychlosti dosažitelné ve standardu 802.11n za použití čtyř antén jsou na hranici 600 Mbps. Reálná rychlost, kterou lze dosáhnout pomocí čtyř antén bývá na úrovni cca. 400 Mbps. Oproti předchozím standardům je zde vidět velký rychlostní skok. 802.11n si však zachovává kompatibilitu se staršími standardy 802.11a/b/g. I zde platí pravidlo nejpomalejšího klienta, který způsobí zpomalení rychlosti celého vysílače. (Vágner, 2011).

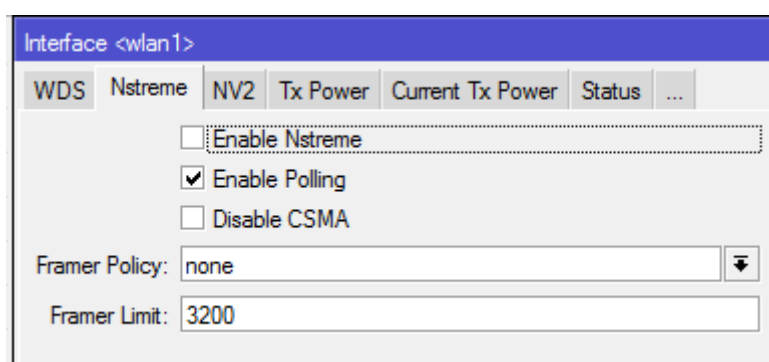
1.1. MIMO

Technologie MIMO je jedno z hlavních vylepšení od původních 802.11. Tato technologie zavádí do klasického modelu komunikace inovaci v rámci používání více antén a tedy více jednotlivých toků, které se šíří prostorem a odráží se od překážek.

2. Nstreme

Tento proprietární protokol vytvořila firma MikroTik. Nstreme se využívá pro bezdrátové přenosy na vylepšení spojů bod-bod a spojů bod-multibod. Protokol lze využívat pouze pro spoje na platformě MikroTik.

Nstreme standardně využívá přístupovou metodu polling. Přístupný bod se postupně dotazuje klientů, zda mají nějaká data k vysílání. Tím odpadá problém skrytého uzlu a taktéž zařízení nemusí detekovat, zda je medium obsazené. (Skipala, 2011). Nstreme obsahuje ještě vylepšení, které upravuje velikosti přenášených rámců s funkcí best-fit. Ten pracuje tak, že čeká, až se naplní rámec a poté jej odešle. (Vágner, 2011). RouterOS umožňuje vypnout CSMA, což má za následek úplnou změnu z CSMA/CA na polling. Vypnutím CSMA se karta zbavuje povinnosti poslouchat médium před vysláním, což může silně negativně ovlivnit soužití s jinými sítěmi na stejné frekvenci. (Skipala, 2011). Bohužel Nstreme používá hodně skrytých technik (nepublikovatelných).



Obr. 4 Záložka Nstream na MikroTik SXT Lite 5.

3. Nv2

Nejnovějším protokolem z rodiny MikroTik je Nv2 (Nstream version 2). Tento protokol rozšiřuje původní Nstream a přidává podporu časového multiplexu TDMA. (Vágner, 2011). TDMA řeší problém skrytého uzlu a zlepšuje využití přenosového kanálu, což má za důsledek zlepšení propustnosti a latence, a to zejména v sítích point-to-manypoint. Nv2 je určený pro karty Atheros 802.11. Maximální limit u protokolu Nv2 je 511 klientů. (MikroTik, 2015). Bohužel Nv2 také používá hodně skrytých technik (nepublikovatelných).

3.7.5 Polarizace

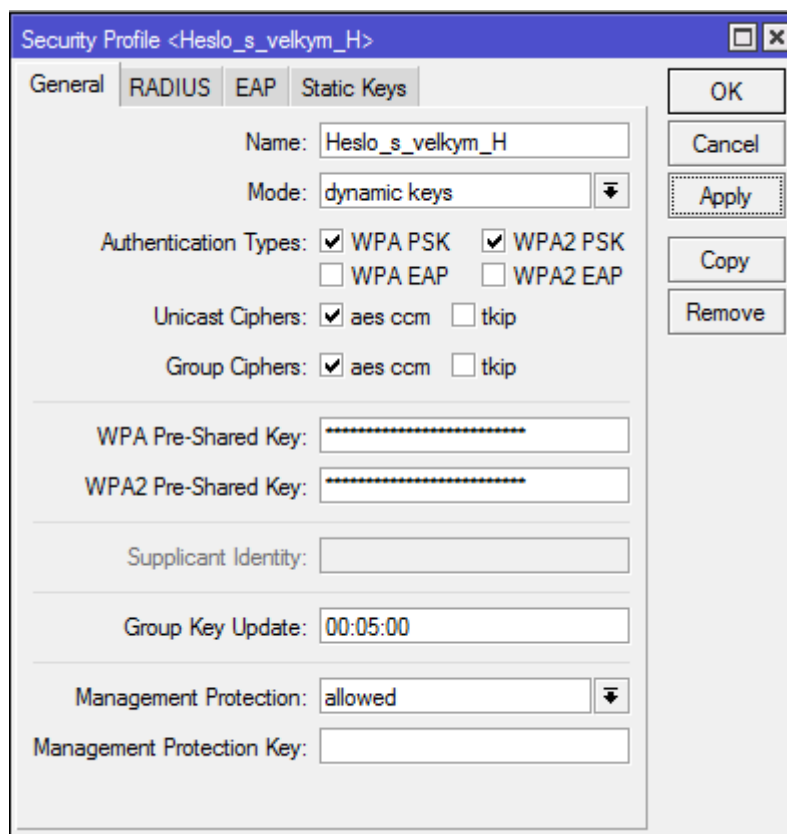
Při vysílání signálu do prostoru může anténa usměrnit signál do jedné ze dvou rovin (vertikální/horizontální). (Skipala, 2011). Pokud jednopolarizační vysílač má vertikální polarizaci a přijímač horizontální pozici, tak v ideálním stavu je útlum nekonečný. V reálném prostředí antény nemají nekonečný útlum. Aktuálně výrobci vyrábí dvoupolarizační antény, takže stanice proti sobě mohou být ve vertikálním i horizontálním stavu.

3.7.6 Zabezpečení

Důležitou funkcí při nasazování bezdrátové sítě je výběr vhodného typu zabezpečení. Mezi nejběžnější typy zabezpečení patří WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access) a WPA2 (WiFi Protected Access 2). První ze zmiňovaných patří mezi nejslabší typ zabezpečení, který jde za pomocí speciálního softwaru do pár minut prolomit. Tuto problematiku a detailní vysvětlení popisuje Fogie (2002). V roce 2003 byl tento standard nahrazen WPA, který lépe odolává útokům. Nejlepší aktuální zabezpečení nabízí nejnovější standard WPA2, který nabízí dva režimy. Režim Personal využívá přednastaveného klíče. Druhý režim, nazývaný Enterprise, je zodpovědný za dynamickou distribuci klíčů. (Skovajsa, 2012)

WPA2 je povinně implementováno od 13. března 2006 do zařízení, která chtějí nést certifikaci Wi-Fi. WPA2 povinně integruje prvky z 802.11i a přidává k TKIP nový algoritmus CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), který je založený na AES, jenž je považovaný za bezpečný. Systém AES využívá symetrickou šifru a stejný klíč pro šifrování i dešifro-

vání. Klíče mohou mít délku 128, 192 a 256 bitů. Metoda šifruje data postupně po blocích o pevné délce 128 bitů. (Pužmanová, 2005). Některé zařízení umožňuje nastavit WPA i WPA2.



Obr. 5 Nastavení hesla pro WPA i WPA2 na MikroTiku.

3.8 EoIP tunel

EoIP tunel je technologie důvěrně známá ze zařízení společnosti MikroTik. EoIP (Ethernet over IP) je tunelovací nešifrovaný protokol postavený na zapouzdření Ethernet rámce do standardního GRE protokolu (Generic Routing Encapsulation). EoIP samotný je stavěn primárně pro tunelování L2 provozu (přenáší navíc proti GRE Ethernet hlavičku a MAC adresy). (Havel, 2015).

4 Současný stav sítě

Základní škola v Kanicích se nachází asi 7 km od Brna. Tato škola byla otevřena 4. února 1961 pro děti nejen z obce Kanice, ale i pro okolní vesnice. (ZSKANICE, 2015). Škola prošla během své existence několika stavebními úpravami. Jedná se o budovu o třech patrech. První počítačová síť, která vznikla kolem roku 2000, rozšiřovala svoji působnost až do nynějších dob.

4.1 Struktura sítě

Poslední rok probíhala na Základní škole v Kanicích renovace sítě. Díky dotacím z Evropské unie najala škola firmu na vybudování nové síťové infrastruktury. Téměř do každé místnosti byly instalovány ethernetové zásuvky. Veškerá kabeláž vede ve zdech, takže nikdo ze studentů nemá přístup k nějakému poškození. Přenosovým médiem se stal kabel UTP kategorie 5e s konektory RJ45. V současnosti je vzhledem k síťovým prvkům využíván standard Fast Ethernet s přenosovou rychlostí 100/100 Mbps s možností budoucího zavedení na standard Gigabit Ethernet.

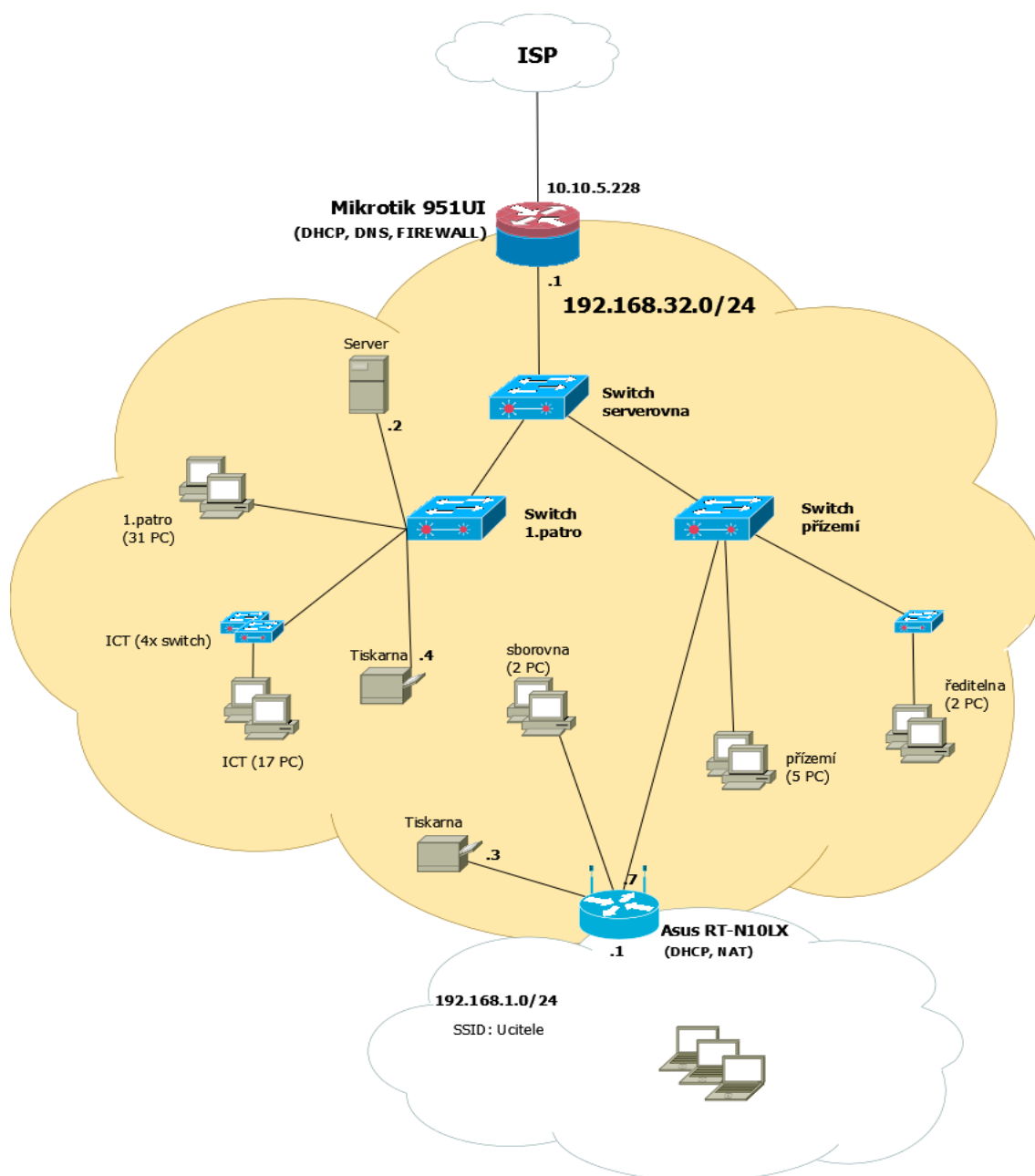
Nově vybudované druhé patro obsahuje místnost serverovnu. Tato místnost má omezený vstup a tím se zajistí větší bezpečnost provozu. V novém patře je také vybudovaná místnost pro výpočetní techniku, která bude přesunuta z prvního patra.

4.1.1 ICT učebna

Ve škole se nachází pouze jedna učebna pro výpočetní techniku. Tato učebna prochází často inovací. Poslední proběhla loni, když jeden z rodičů daroval škole vyřazené stolní počítače. Tyto počítače běžící na operačním systému Windows 7 s dvoujádrovým procesorem AMD, operační pamětí 4 GB a s diskovým prostorem 300 GB jsou velkým posunem vpřed oproti minulým zařízením. Nezbytnou součástí výukového programu je využití dataprojektoru BenQ TW523P. Současná učebna se nachází v 1. patře a jedná se přetvořenou třídu na učebnu ICT, takže jsou switche volně položeny na lavicích, což z hlediska bezpečnosti není správné.

4.1.2 Ostatní místnosti s výpočetní technikou

Učebny a kabinety většinou disponují výpočetní technikou. Bohužel počítače, které tam najdeme, nejsou příliš výkonné. Proto zaměstnanci školy kladou důraz na vybudování Wi-Fi sítě, aby si mohli využívat vlastní notebooky. Současná Wi-Fi síť nevyhovuje podmínkám školy.



Obr. 6 Současná topologie sítě.

4.1.3 Wi-Fi síť

Bezdrátová síť existuje ve škole pouze ve sborovně, kde si na vlastní náklady koupili učitelé Wi-Fi router Asus RT-N10LX, který má dosah jen ve sborovně. Nastavení routeru neumožňuje vysílat dvě SSID zároveň, takže přístup na Wi-Fi mají pouze učitelé. Jako zabezpečení se využívá standard WPA.

4.1.4 Aktuální síťové prvky

Hraničním bodem v lokální síti ZŠ je RB951UI-2HnD. Tento router má dostatečný výkon pro řízení celé sítě a běží na něm DHCP, DNS, NAT a Firewall.

Tab. 2 Technické parametry RB 951UI-2HnD

CPU	600 MHz
core	1
RAM	128 MB
OS	RouterOS
porty	5
wireless	Yes
POE	Yes

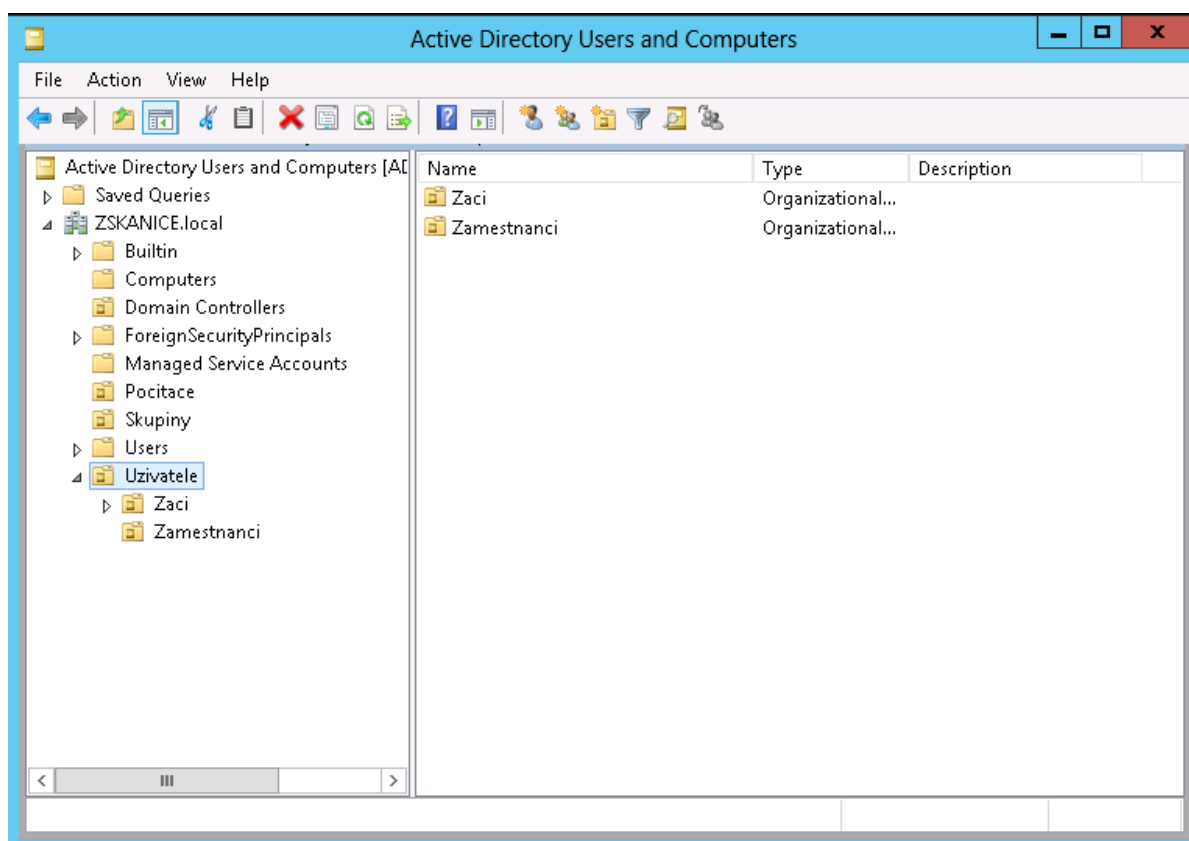
Zdroj: <http://routerboard.com/RB951Ui-2HnD>

Nejčastěji se vyskytujícím síťovým prvkem v síti je switch. Celkový počet zařízení je jedenáct. Sedm switchů typu Zyxel ES-105A slouží v učebnách k připojení více zařízení. Tři switche TP-Link TL-SF1016D jsou upevněny ve zdi v každém patře. Poslední switch typu TP-Link TL-SF1048 je umístěn v racku. Žádný ze switchů neumožňuje management.

Přístup do studentských a zaměstnaneckých počítačů spravuje Windows server 2012 R2 Standard. Každý počítač je přihlášen do domény ZSKANICE.local a pomocí služby Active Directory má každý student a zaměstnanec svoje přihlašovací údaje. Na serveru jsou nainstalované také různé programové aplikace, které využívají učitelé k výuce.

4.2 Současný stav v mateřské škole

Tento nově vybudovaný objekt byl otevřen v roce 2011. Školka má vybudovanou síťovou infrastrukturu, ale není zapojena. Veškerá kabeláž je přivedena na malou půdu. V místnostech jsou ethernetové zásuvky. Chybí pouze konektivita do školní sítě včetně Internetu.



Obr. 7 Active Directory běžící na Windows server 2012.

4.3 Zabezpečení sítě

Zabezpečení sítě bylo na programu minulý rok. Síť postrádala téměř jakékoli zabezpečení. S instalací serveru se každý počítač ve škole přihlásil do domény, takže veškerý přístup je řízený pomocí AD běžící na serveru (viz Obr. č. 7). Lokální účty počítačových stanic jsou zaheslovány, takže už žádný student nemá práva administrátora. Dalším důležitým krokem bylo nastavit zaheslování BIOSu, kde mohl útočník změnit pořadí bootování a na PC spustit libovolné médium jako např. Live OS, který by mu umožnil administrátorská práva k samotnému PC. Na žádost vedení školy se zprostředkovalo blokování stránek. Nová aplikace i-bezpecne.cz zabraňuje přístup na určité internetové stránky. Aplikace obsahuje seznam více než 1 300 000 vytipovaných nevhodných stránek, dělených do kategorií. Seznam si ovšem může každý administrátor libovolně upravovat. Tato aplikace je nasazena na hraničním prvku sítě. Škola využívá antivirovou ochranu AVG, kterou každý rok platí a je tedy na všech počítačích nainstalovaná.

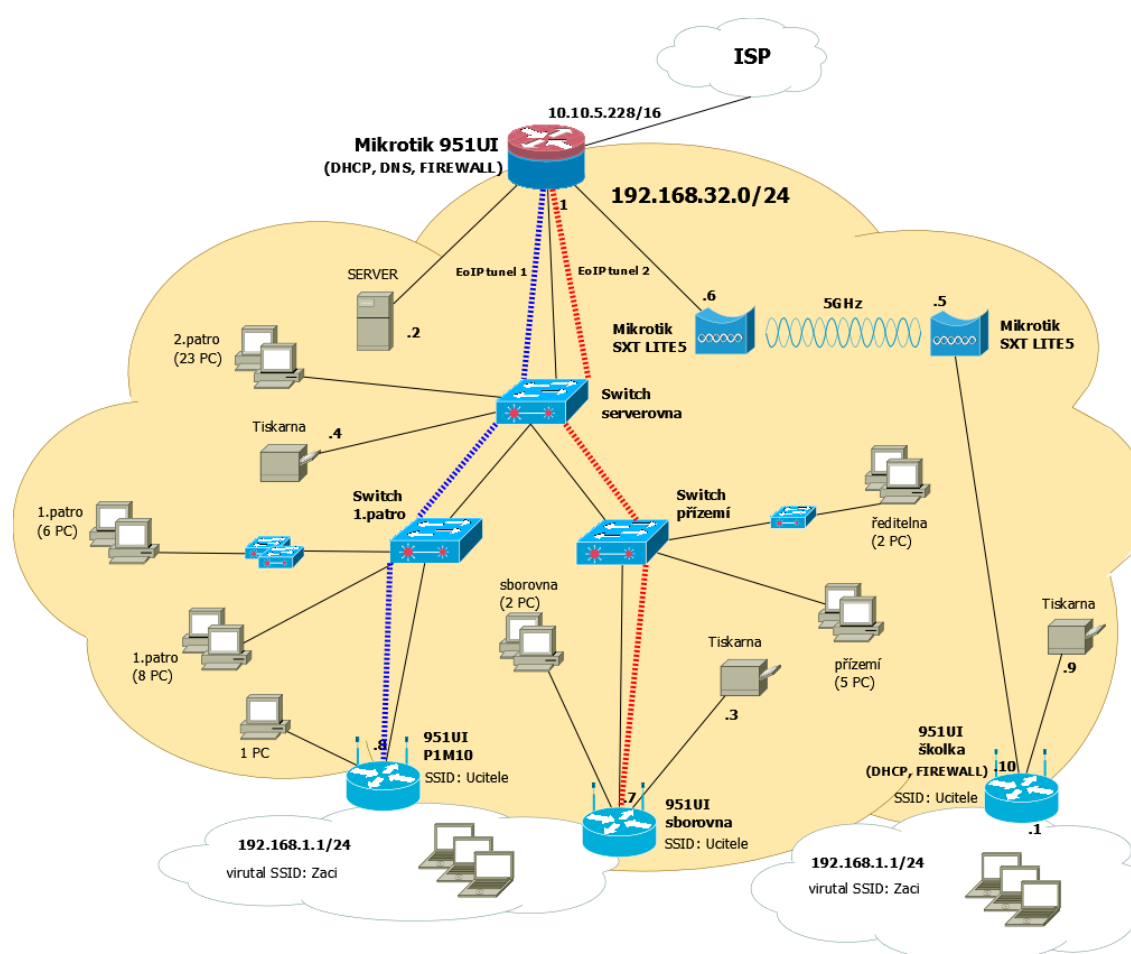
4.4 Konektivita k síti Internet

Konektivitu k síti Internet poskytuje firma TS-Hydro s.r.o, která je společně s mobilními operátory jediným poskytovatelem internetu v okolí. Firma je připoje-

na na páteřní linku v Brně a přes bezdrátový 10 GHz spoj o kapacitě 200 Mbps poskytuje nejlepší možné připojení. Internet ve vesnici je rozveden pomocí venkovních UTP kabelů s duplexní kapacitou 100 Mbps. Jedná se o sdílené připojení, takže rychlost Internetu je nestabilní, ale reálně se pohybuje rychlost kolem 40/40 Mbps. Tato rychlost je pro využití školy naprosto dostačující.

5 Návrh řešení – implementace

V úvodu návrhu řešení je třeba si ujasnit cíle. Musíme přemístit veškerý technologický materiál do nové učebny a serverovny tak, aby vše fungovalo stejně jako předtím. Důležitým bodem práce bude návrh bezdrátového spoje na frekvenci 5 GHz. Posledním krokem bude vybudování Wi-Fi sítě pro studenty a učitele. Na bezproblémový přechod mezi AP budeme využívat EoIP tunely. Návrh sítě z pohledu topologie můžeme vidět na obrázku č. 8.



Obr. 8 Návrh sítě z hlediska topologie.

5.1 Přemístění ICT učebny

Jako první krok zvolíme zprovoznění počítačové sítě v budově ZŠ a přemístění ICT učebny do nově připravené místnosti. Server se nachází v učebně ICT, kde je ve zdi přimontován malý rack, který lze zamykat. Toto zařízení se přenesse do serverovny a připojí k hlavnímu routeru (bráně) a příslušný port na MikroTiku popíšeme.

Další krokem je přemístění veškeré technologie do nové ICT učebny. V nové učebně jsou vybudované zásuvky ethernetové i elektrické. Počítače a síťovou tiskárnu otestujeme, zda komunikují s lokální sítí.

5.2 Návrh 5 GHz přenosu

Pro bezdrátovou komunikaci mezi budovou ZŠ a MŠ využijeme přenos v pásmu 5 GHz. Lze použít i jiné frekvence, ale frekvence 2,4 GHz je příliš rušená a pásmo 10 GHz je pro přenos na několik desítek metrů zbytečně nákladné.

5.2.1 MikroTik SXT Lite 5

Výrobců pro 5 GHz přenos je spousta, ale mezi špičku patří výrobci MikroTik a Ubiquiti Networks. Z důvodu využití MikroTiku jako hlavního routeru a také kvůli mé zkušenosti s RouterOS jsem si vybral MikroTik SXT Lite 5. Parametry antény jsou naprosto dostačující pro bezdrátový přenos mezi školou a školkou. Cena jednoho zařízení je 1405 Kč.

Tab. 3 Technické parametry SXT Lite 5

CPU	600 MHz
core	1
RAM	64 MB
OS	RouterOS
porty	1
POE	Yes
Zesílení DBI	16dB
Wireless standards	802.11 a/n

Zdroj: <http://routerboard.com/RBSXT5nDr2>

5.2.2 Podmínky využití pásma 5 GHz.

Podmínky využití bezdrátových přenosů jsou popsány v kapitole 3.2.3 Bezdrátová komunikace. Pro 5 GHz pásmo pro venkovní využití platí:

- Lze použít frekvence 5470 – 5725 MHz.
- Maximální vyzařovací výkon u zařízení s automatickou regulací výkonu je 1W (30dBm).
- Maximální vyzařovací výkon u zařízení bez automatické regulace výkonu je 501mW (27dBm).
- Aktivovat funkci DFS, která vyhodnotí přítomnost meteoradarů.
- Zvolit zemi Czech Republic z důvodu správné aktivace DFS a povolení kanálů.

Z praxe je ovšem známo, že provozovatelé tyto podmínky nedodržují. Dle průzkumu ČTÚ dodrželo správné požadavky pouze 28% provozovatelů. Dalším důležitým bodem je morální legislativa. Je zbytečné používat vysoký výkon na krátké vzdálenosti. Přenosová rychlost se nám nezmění a navíc rušíme ostatní provozovatele. Proto je ve městech velice těžké najít volnou frekvenci. V posledních letech je na 5 GHz pásmech dovoleno využívat šířku pásma 40 MHz. Pokud bydlíme na samotě u lesa, není problém tuto šířku pásma využít, ale jestliže provozujeme bezdrátový přenos ve městě a použijeme všesměrovou anténu s vysokým výkonem a šířkou pásma 40 MHz, jedná se o bezohlednost.

	Address	SSID	Channel	Signa...	Noise...	Signa...	Radio Name	RouterOS...
APRNWB	D4:CA:6D:E1:FF:ED	Nonko1	5220/20/an	-78	-111	33	K_Ko	6.4
ARTB	00:0C:42:CD:E5:D9	Def_2a	5260/20/an	-77	-111	34	Omni147	
ARTB	00:0C:42:CC:70:4B	Hidrazin	5280/20/an	-88	-111	23	156	
APRWB	D4:CA:6D:AB:82:66	Nonko2	5320/20/an	-72	-111	39	K_Ko	6.15
APRWB	00:0C:42:C3:45:BD	Def_1	5580/20/an	-77	-115	38	K_omni	5.24
APRWB	02:0C:42:C3:45:BD	Def_2	5580/20/an	-79	-115	36	K_omni	5.24
APRWB	4C:5E:0C:68:57:65	DumDum	5600/20/an	-76	-116	40	Dum	6.19
RTB	00:C0:CA:1D:A5:7C	Ko6	5620/20/a	-87	-115	28	K_Ko	
APRWB	00:0C:42:CD:10:AD	Reloaded	5640/20/an	-87	-117	30	K_Byt_SXT	6.23
APRW	00:27:22:34:2B:62	Rodeo	5660/20/an	-80	-117	37	NanoStation M5	2.9.31

Obr. 9 Scan sítí 5180 až 5865 MHz.

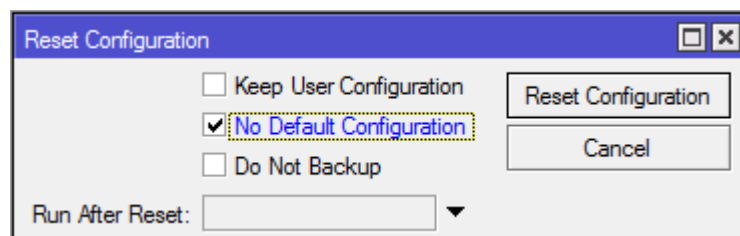
Na obrázku č. 9 je scan sítí na SXT Lite 5. MikroTik umí vysílat i na zakázaných kmitočtech 5725 – 5865. Podle jednoho webu ⁵ se projednává rozšíření pásma až do kmitočtů 5,9 GHz. Zatím toto pásmo využívají dopravní systémy.

5.2.3 Nastavení vysílače.

Koupenou anténu namontujeme na střechu na stožár a namíříme na stožár umístěný na mateřské škole. Ve škole ze serverovny je připraven „husí krk“, který je přiveden pod střechu. Tímto „husím krkem“ protáhneme UTP kabel. Na oba konce nalisujeme konektory RJ-45 a připojíme do SXT Lite 5. Anténa bude napájena přes PoE (Power over Ethernet).

⁵ <http://i4wifi.blog.cz/1410/planovane-rozsireni-pasma-5-ghz-od-ctu-a-budoucnost-10-ghz>

Na konfiguraci zařízení MikroTiku stáhneme Winbox, který je dostupný na webových stránkách výrobce. Před nastavením zařízení vymažeme aktuální konfiguraci kvůli čistému nastavení.



Obr. 10 Vymazání defaultní konfigurace.

Máme čistou konfiguraci MikroTiku. Můžeme nahrát nejnovější firmware, který je dostupný na webových stránkách výrobce. Není to ovšem nezbytně nutné. Popíšeme si nastavení vysílače v několika krocích:

1. *Addresses*

IP adresa jednoznačně identifikuje síťové rozhraní. V našem případě se bude jednat o adresu 192.168.32.6/24. Lomítko 24 určuje masku podsítě.

2. *Identity*

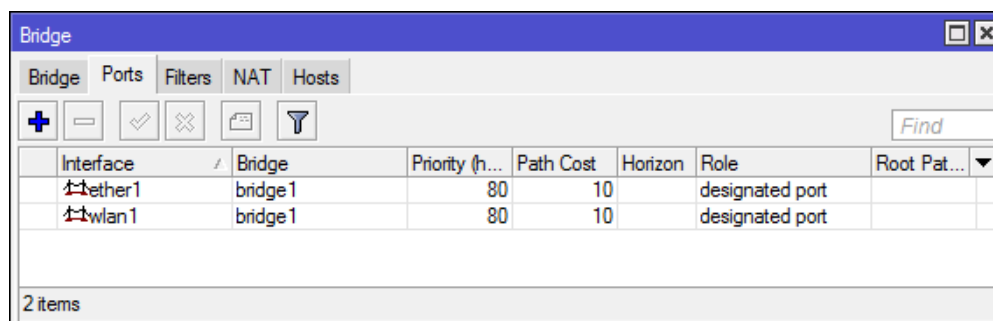
Je třeba si pojmenovat MikroTik, tak abychom věděli, které zařízení nastavujeme. (Např. Skola_vysilac).

3. *Password*

Nezbytnou součástí je nastavení hesla do MikroTiku. Mělo by se jednat alespoň o 8 znaků, i když to MikroTik nevyžaduje.

4. *Bridge*

Přemostění slouží ke spojení dvou fyzických sítí na vrstvě L2. Následně jsou veškeré přijaté pakety na jedno rozhraní automaticky zaslány na rozhraní druhé. Tento proces probíhá transparentně, tudíž bez jakéhokoli meziskoku. Vytvoříme tedy bridge a záložce ports přidáme rozhraní ether1 a wlan1.



Obr. 11 Spojení rozhraní v Bridge.

5. Watchdog

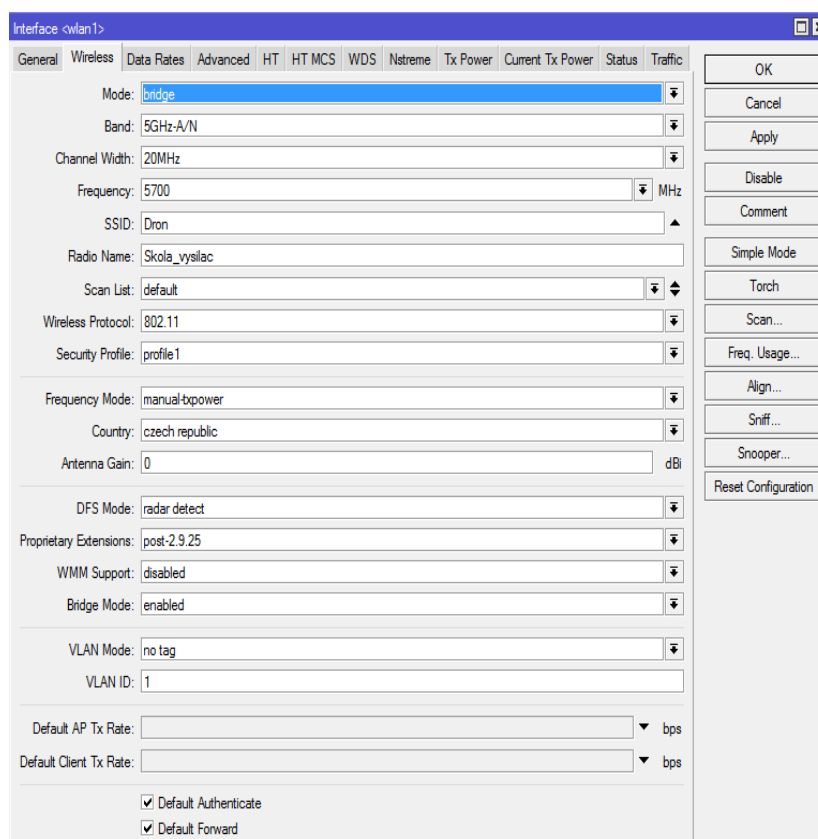
Watchdog sleduje funkce prvku. Např. neustále posílá ping na zvolenou adresu a při delším výpadku pingu restartuje zařízení.

6. Security Profiles

Nutností je nastavit typ šifrování. V kapitole 3.7.6 jsou popsány standardy, které lze využít. My využijeme typ zabezpečení WPA2.

7. Wireless

Nejdůležitější částí konfigurace je nastavení bezdrátové komunikace. Musíme mít na zřeteli všechny všeobecné podmínky pro provoz.



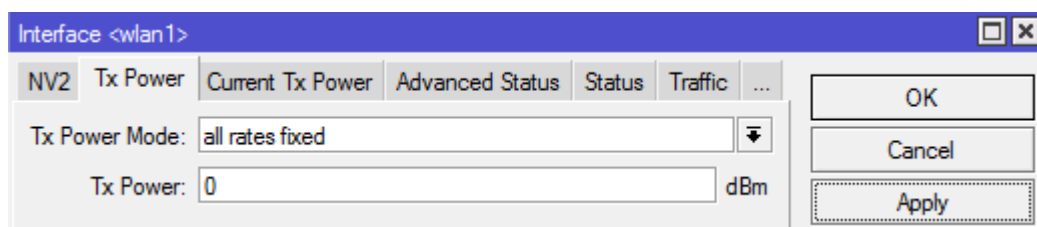
Obr. 12 Wireless nastavení na vysílaču.

8.1. Wireless

8.1.1. *Mode* – Je nastavený mode bridge, protože AP bridge požaduje vyšší verzi licence, která se dá koupit, ale v našem případě je nepotřebná z důvodu spojení point-to-point.

8.1.2. *Band* – Nastavení frekvenčního bezdrátového pásma a Wi-Fi standardu.

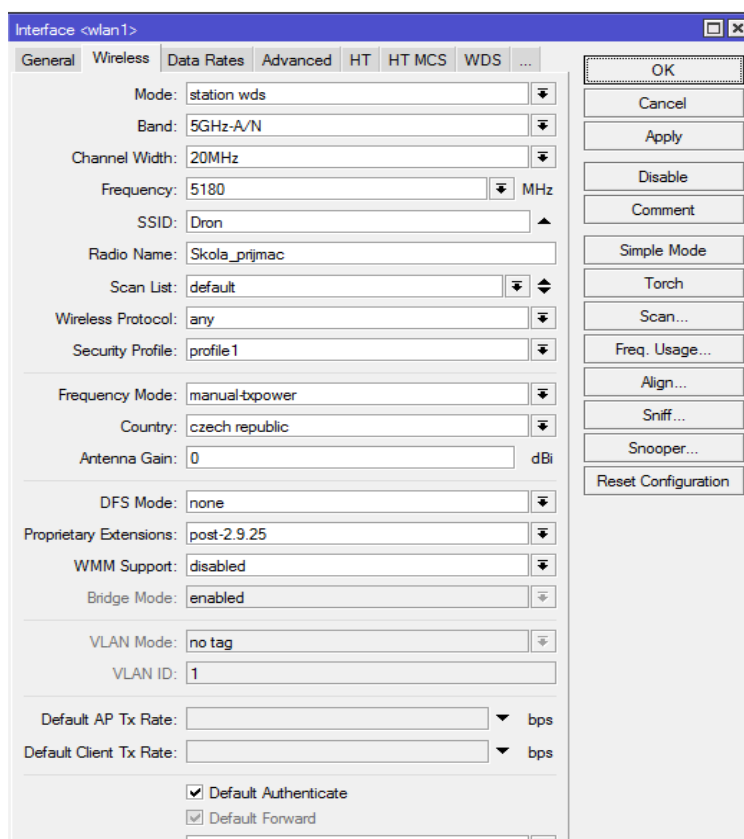
- 8.1.3. *Channel Width* – Šířka pásma nám bude stačit 20 MHz z důvodu nepotřebné vyšší rychlosti ve mateřské škole.
 - 8.1.4. *Frequency* – Nastavení vysílacího kmitočtu. Řídit se podle vysílacích podmínek viz kapitola 5.2.2.
 - 8.1.5. *SSID* – Název sítě, která bude vysílána wlan1 rozhraním.
 - 8.1.6. *Security Profile* – Nastavení zabezpečení sítě. Viz kapitola 3.7.6.
 - 8.1.7. *Wireless Protocol* – Výběr protokolu. Viz kapitola 3.7.4.
 - 8.1.8. *Country* – Poloha instalace, jejíž pravidla budou v nastavení aplikována.
 - 8.1.9. *Antenna Gain* – Hodnota = zisk antény – útlum pigtailu (propojovací kabel mezi bezdrátovou kartou a anténní konektor). (Šturma, 2014)
 - 8.1.10. *DFS Mode* – nastavíme na radar detect. Tato funkce detekuje signál meteorradaru. V případě detekce automaticky vypne vysílání na dané frekvenci.
- 8.2. *HT* – V této záložce je potřeba, aby zde byla zapnuta polarizace vertikální i horizontální. Viz kapitola 3.7.5.
 - 8.3. *WDS* – V manuálu MikroTiku doporučují pro budování bezdrátových mostů použít jejich proprietární protokol WDS.
 - 8.4. *TX Power* – Vzhledem ke vzdálenosti nastavíme vyzařovací výkon na 0 dBm.



Obr. 13 Vyzařovací výkon TX.

5.2.4 Nastavení přijímače.

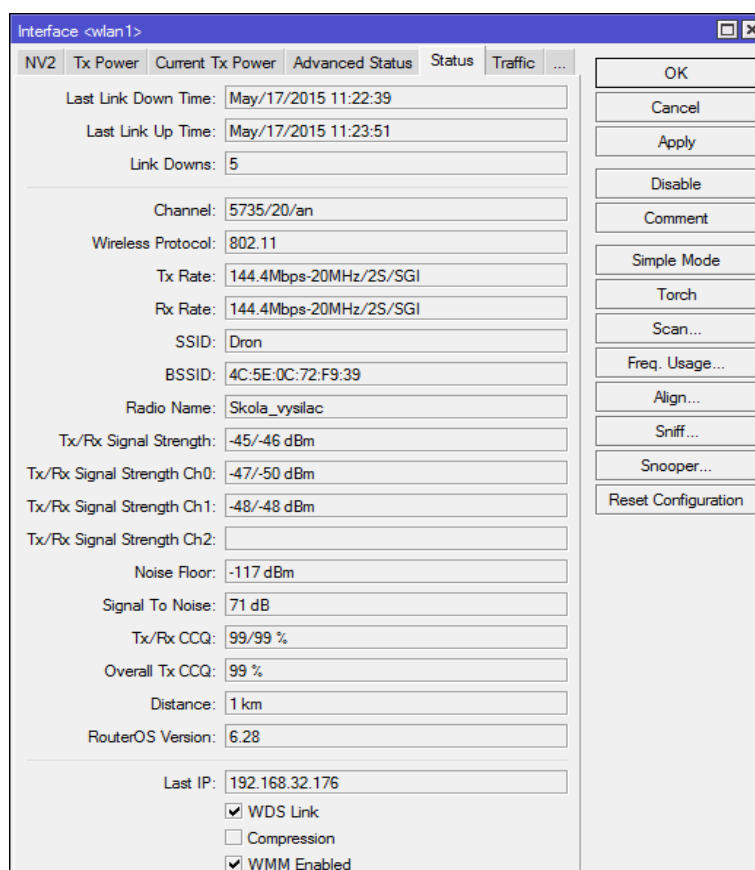
U nastavení přijímače budeme postupovat obdobně jako u vysílače. Opět si vymažeme konfiguraci MikroTiku a začneme nastavovat jednotlivé body. IP adresu nastavíme staticky na 192.168.32.5/24 a nastavíme název antény (např. skolka_prijimac). Krok 3-6 nastavíme totožně jak u vysílače.



Obr. 14 Wireless nastavení na přijímaču.

Nastavení wireless nastavujeme podle toho, co jsme nastavili na vysílači. Mode Station WDS znamená, že se jedná o klienta s funkcí WDS. I když je Wireless Protocol 802.11, tak na klientovi použijeme any. Důvodem je, že pokud změníme Wireless Protocol na vysílači, automaticky se klient přizpůsobí.

Opět zkontrolujeme polarizaci v záložce HT a také nastavíme WDS. Vyzařovací výkon TX snížíme na 0 dBm stejně jako u vysílače. Po potvrzení veškeré konfigurace se antény spojí. Na obrázku č. 15 je status konektivity mezi oběma zařízeními.



Obr. 15 Status konektivity.

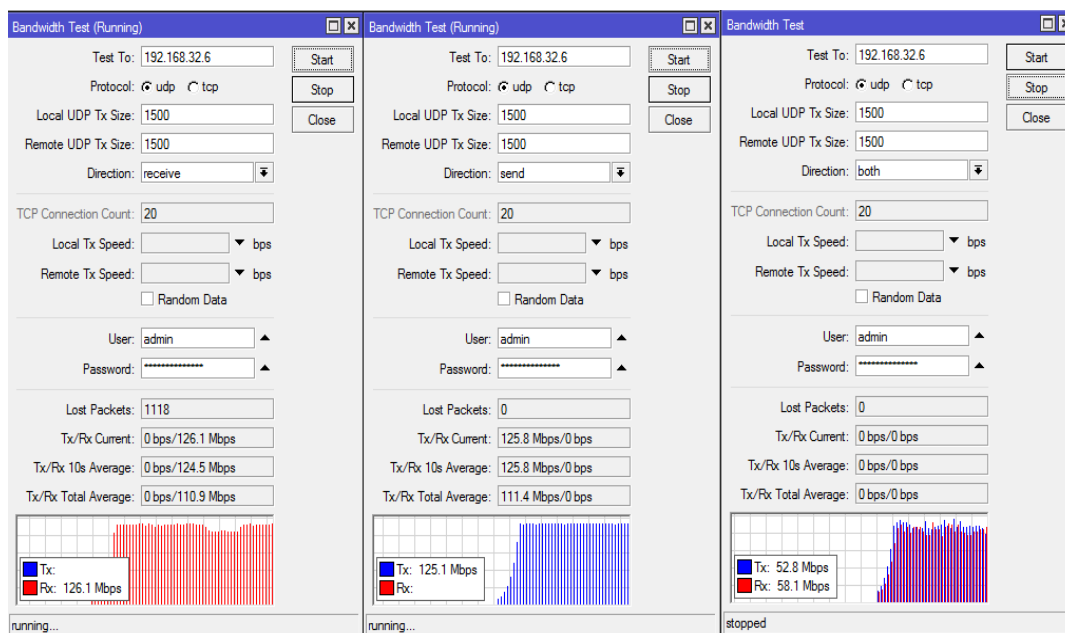
Podle obrázku č. 15 vidíme:

9. *Channel* – Frekvence, na které zařízení mezi sebou komunikují.
10. *Tx, Rx Rate* – Maximální teoretická rychlost.
11. *BSSID* – MAC adresa vysílače.
12. *Tx/Rx Signal Strength* – Síla signálu je i po úplném snížení výkonu ideální.
13. *Signal To Noise* – síla signálu k síle šumu v určené šířce pásma.
14. *Tx, Rx CCQ* – Ukazatel kvality signálu.
15. *RouterOS Verssion* – Verze firmwaru.

5.2.5 Testování

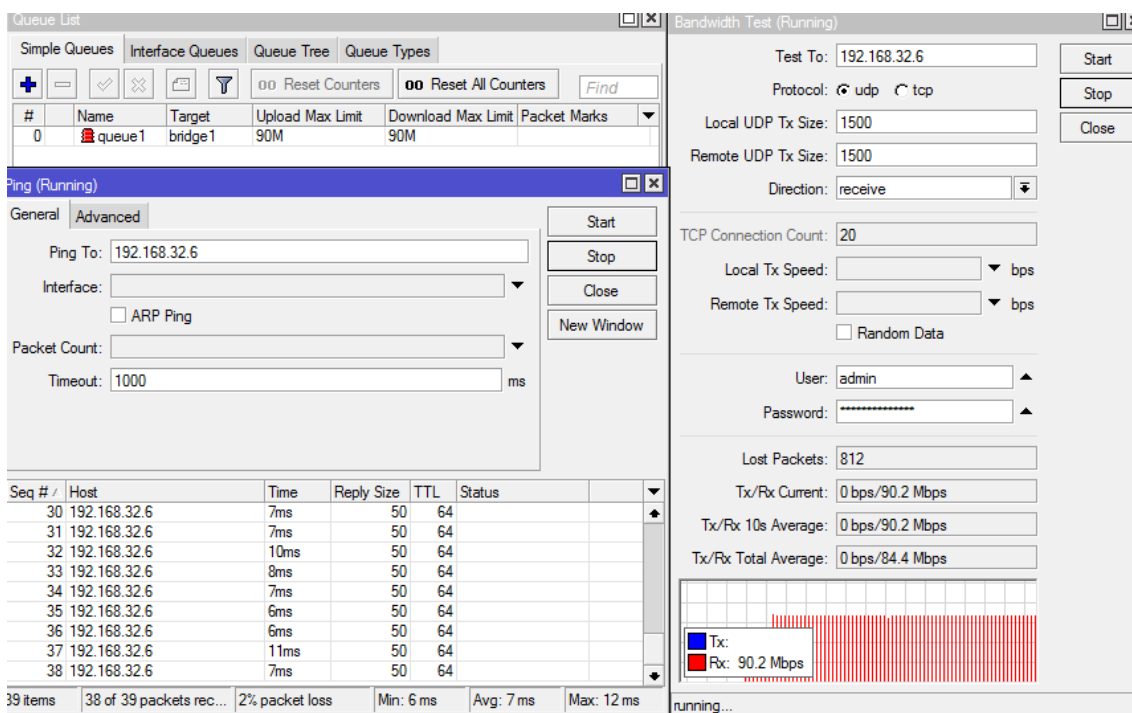
Ačkoliv teoretické výsledky vypadaly dobře, je třeba otestovat síť z praktického pohledu. MikroTik má funkci bandwidth test, která otestuje reálnou prostupnost dvoubodového spoje. Pro zjištění latence lze použít v RouterOS nástroj ping nebo příkazový řádek v systémech Windows. Budeme také testovat bezdrátové protokoly, které jsou popsány v kapitole 3.7.4.

1. Testování protokolu 802.11n



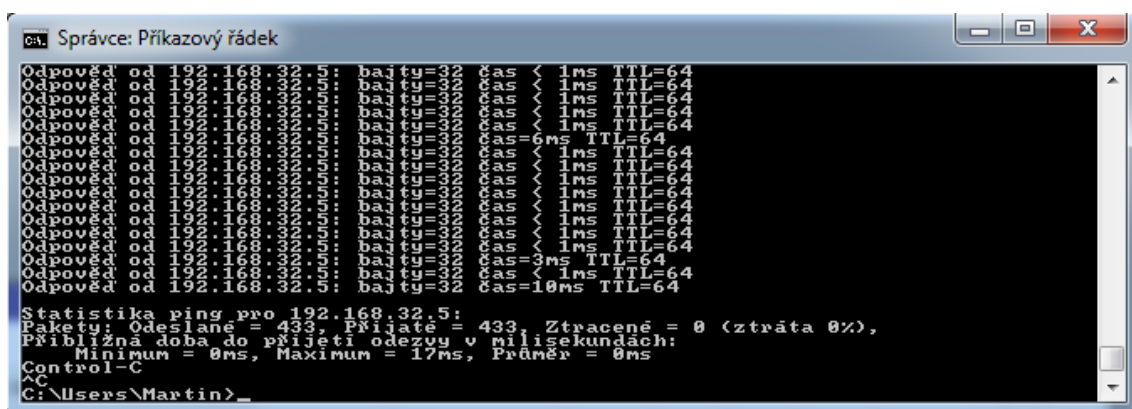
Obr. 16 Bandwidth test s protokolem 802.11n.

Protokol 802.11n je popsán v kapitole 3.7.4. Dle testu vidíme, že prostupnost se blíží teoretické rychlosti. Spoj dokáže přenášet 125 Mbps half duplex. Latence při takto zatíženém spoji jde do vysokých čísel a dochází k velké ztrátovosti. To ovšem není nic neobvyklého. Zkusíme tedy omezit rychlost přenosu a sledovat latenci.



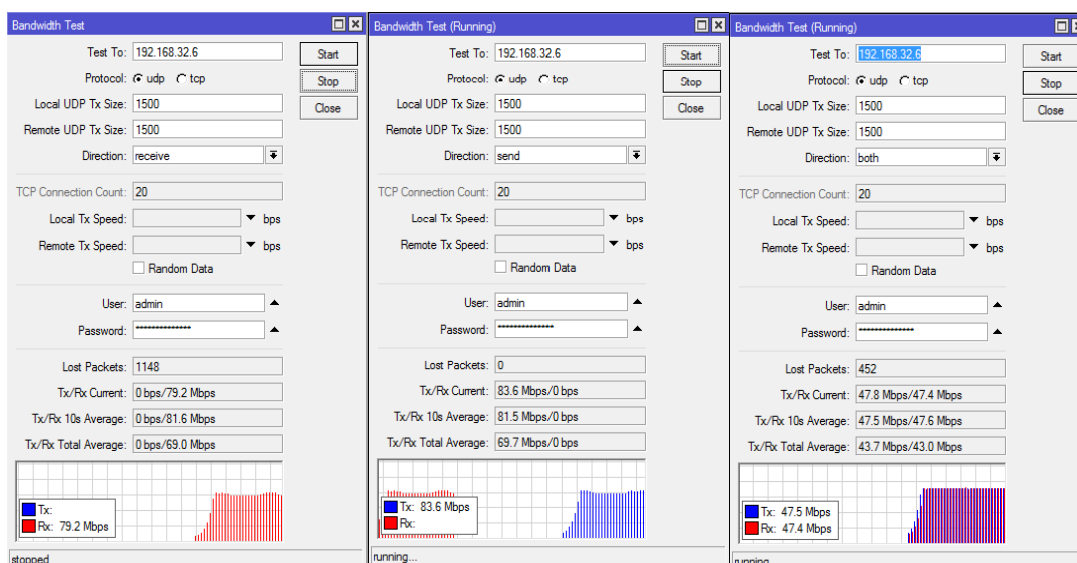
Obr. 17 Omezení rychlosti na 90 Mbps.

Dle obrázku č. 17 můžeme vidět, že při omezení rychlosti je odezva stabilní. Omezení ovšem nemusíme nastavovat, protože rychlostní omezení nám dělá standard Fast Ethernet, který má maximální přenosovou rychlost 100 Mbps. Pokud by se ve školce využívala bezdrátová linka full duplexně, tak by bylo vhodné nastavit nějaké omezení. Dle mého názoru je to v našem případě zbytečné. Na obrázku č. 18 je vidět, že bez zátěže je latence spoje minimální.



Obr. 18 latence bez zátěže.

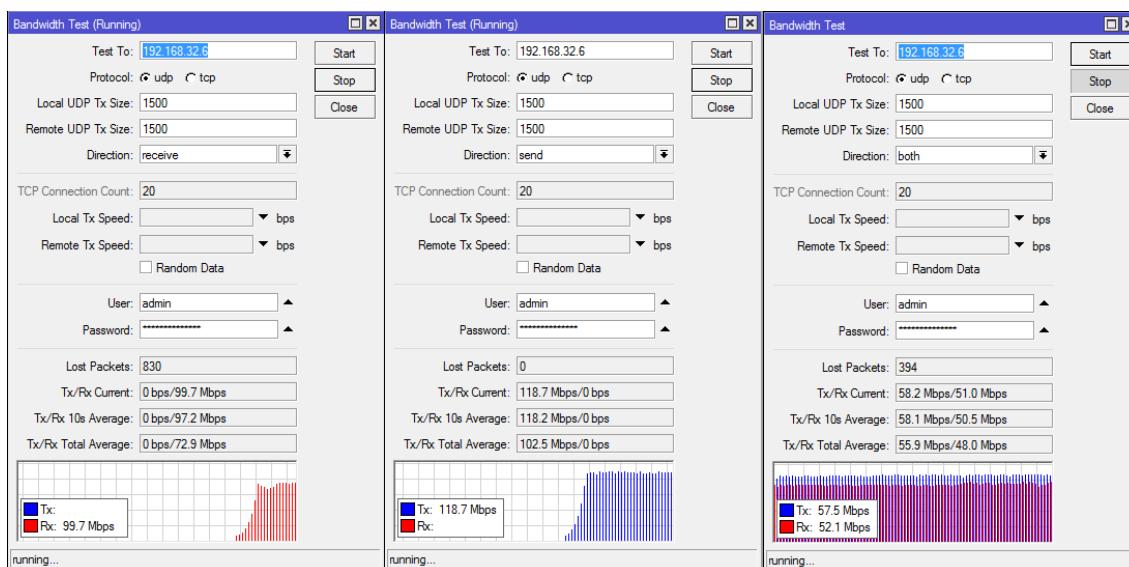
2. Testování protokolu Nstereme



Obr. 19 Bandwidth test s protokolem Nstereme

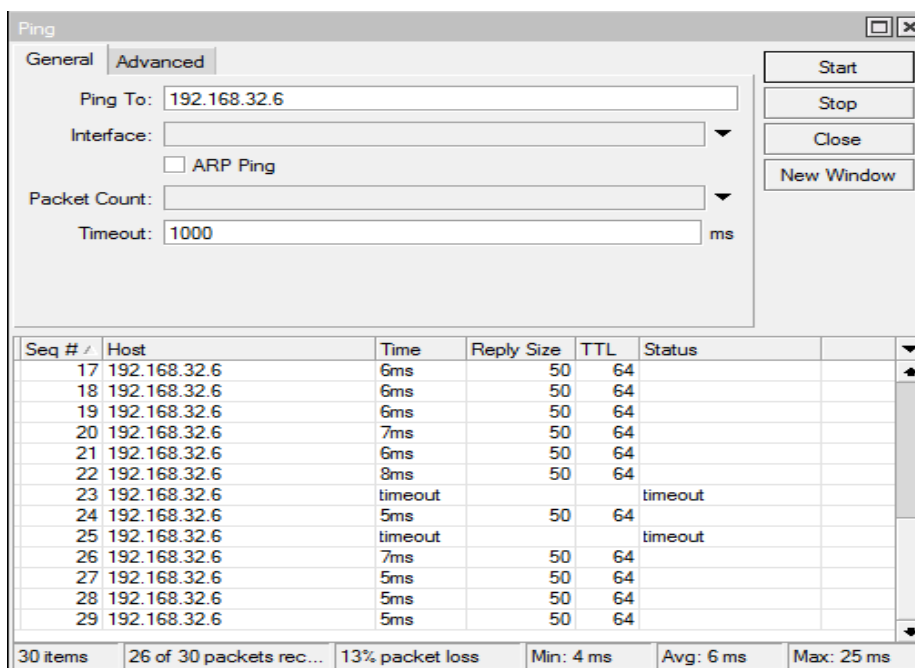
Protokol Nstereme je popsán v kapitole 3.7.4. Testování s protokolem Nstereme snížilo přenosové rychlosti o čtvrtinu. Nutno ovšem podotknout, že při maximální zátěži vypadal ping méně než u protokolu 802.11. Také lze upozorovat, že ve full duplexním zatížení se přenosová rychlost zvýšila na 94 Mbps. Latence bez zátěže je 0 ms se ztrátou 0 %.

1. Testování protokolu Nv2



Obr. 20 Bandwidth test s protokolem Nv2

Protokol Nv2 je pokračováním protokolu Nstreme. (viz kapitola 3.7.4). Dle testování dopadl Nv2 výborně. Přenosová rychlost sice nedosahuje stejných rychlostí jako u protokolu 802.11n, ale při full duplexní zátěži je ping stabilnější (viz obr 21). Latence bez zátěže je 2 ms se ztrátou 0 %.



Obr. 21 Latence při maximální zátěži u protokolu Nv2.

Otestovali jsme všechny tři protokoly. Podle tabulky č. 4 vidíme přehled výsledků testovacích protokolů.

Tab. 4 Výsledky testování jednotlivých protokolů.

Protokol	přenosové rychlosti			ztrátovost pingu při zátěži [%]	průměrná odezva [ms]	ztrátovost pingu bez zátěže [%]	průměrná odezva [ms]
	Rx [Mbps]	Tx [Mbps]	both [Mbps]				
802.11n	126	125	53/58	10%	22 ms	0%	0 ms
Nstreme	79	84	48/47	4%	20 ms	0%	0 ms
Nv2	100	118	58/52	5%	10 ms	0%	3 ms

Nejlépe dle výsledku dopadl protokol Nv2. I když nedosahuje stejné maximální přenosové rychlosti jako u protokolu 802.11n, tak při full duplexní zátěži je stabilnější. Sice má bez zátěže vyšší ping o 2 ms, ale to nijak neovlivní výsledek. Pro náš bezdrátový přenos využijeme protokol Nv2.

5.3 Návrh Wi-Fi sítě

Ve škole se nenachází Wi-Fi, která by stačila potřebám školy. Podmínkou vedení školy je vybrat tři zařízení do 5000 Kč. Studenti budou mít svoji Wi-Fi, která bude omezena rychlostí a nebude zasahovat do sítě školy. Naopak učitelé budou mít neomezené rychlosti a přístup do sítě školy.

5.3.1 MikroTik 951Ui-2HnD

Výrobců pro šíření bezdrátové komunikace na frekvenci 2,4 GHz je nespočetné množství. MikroTik 951Ui splňuje všechny předpoklady pro splnění podmínek školy. MikroTik poskytuje funkce, které žádné jiné zařízení v této cenové kategorii nemá. Cena jednoho zařízení je 1460 Kč, což splňuje při nákupu tří zařízení limit 5000 Kč.

5.3.2 Nastavení AP

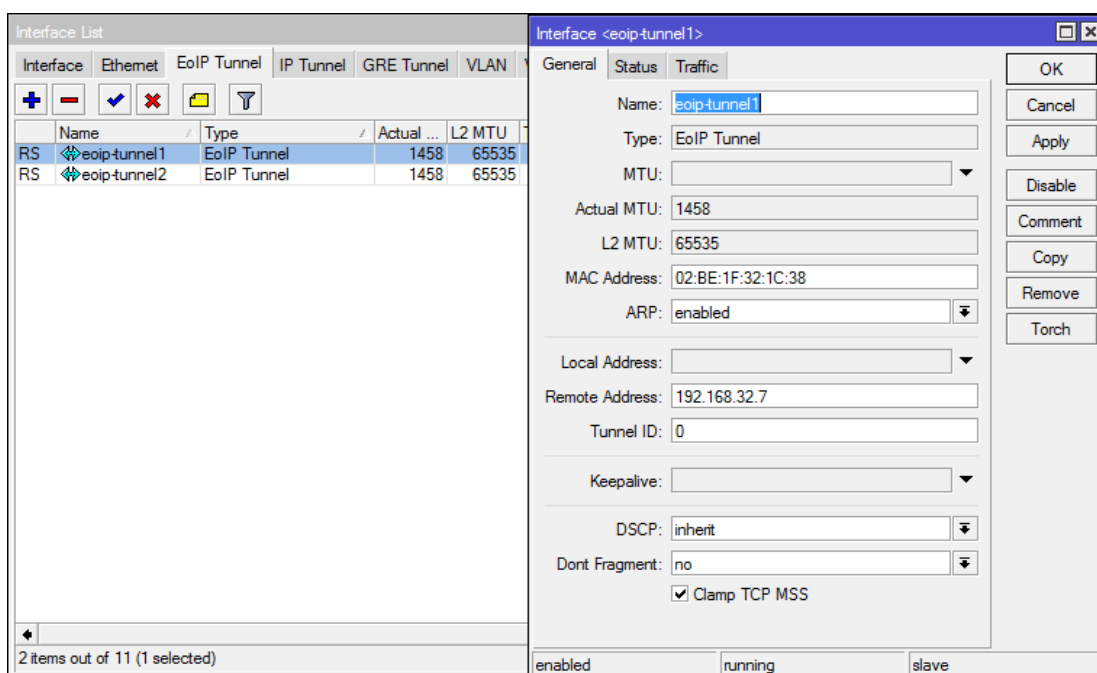
Prvotně je důležité uvědomit si, jaké funkce AP má mít. Z důvodu nasazení značky MikroTik můžeme zajistit bezdrátový roaming. Jeho nasazení je vysvětleno v bakalářské práci Michala Šturmy. (Šturma, 2014). Nutno ovšem podotknout, že aby bezproblémové přepojení fungovalo, musíme nastavit totožné SSID a síťové zabezpečení. Naopak parametr BSSID musí být rozdílný, aby byl klient schopen rozeznat přístupové body. (Šturma, 2014). Kvůli absenci VLAN ve školní síti bude potřeba vytvořit EoIP tunely, který budou řídit toky dat a přidělování adres. EoIP tunel je popsán v kapitole 3.8.

2. Nastavení routeru.

Na hlavním routeru musíme nastavit:

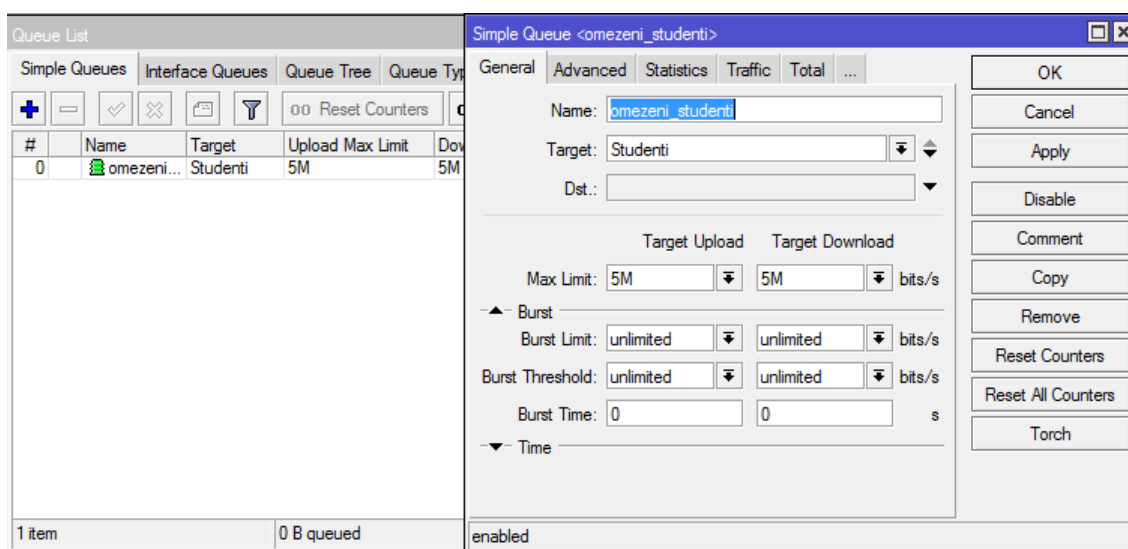
- DHCP s rozsahem 192.168.1.100 – 192.168.1.240
- Vytvořit dva EoIP tunely
- Vytvořit bridge studenti, do kterého budou přidány rozhraní obou EoIP tunelů.
- Omezit rychlost pro bridge studenti.
- Nastavit pravidla ve firewallu pro síť studenti.

2.1.1. EoIP tunnel – V Interface je záložka EoIP tunnel. Přidáme EoIP tunel a označíme si jeho ID, podle kterého bude rozpoznáván a IP adresu zařízení, kam tunel povede.



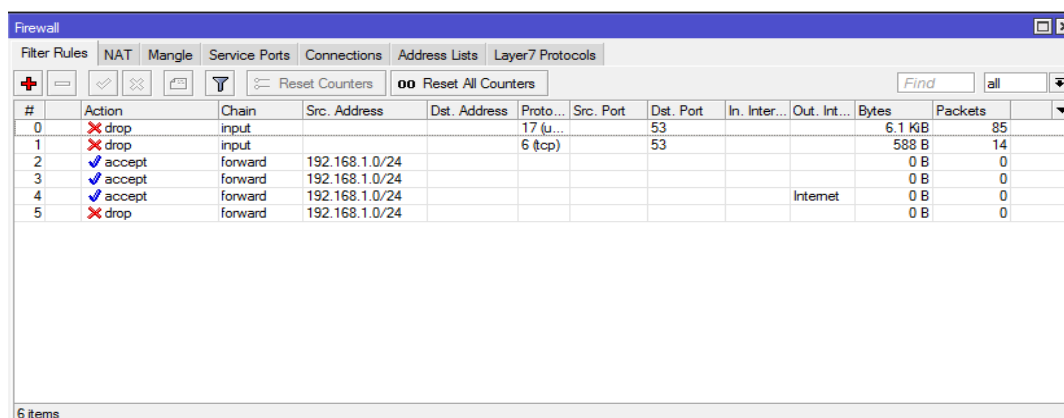
Obr. 22 Vytvoření EoIP tunelu.

- 2.1.2. *Bridge* – Vytvoříme bridge s názvem studenti. Do tohoto bridge přidáme rozhraní obou tunelů. Pro bridge studenti nastavíme IP adresu na 192.168.1.1.
- 2.1.3. *DHCP* – V položce pool si vytvoříme rozsah adresy 192.168.1.100 – 192.168.1.240. Poté přidáme další DHCP server, jehož rozhraní je bridge studenti.
- 2.1.4. *Queues* – Jedná se o funkci MikroTiku, která omezí přenos dat. Nastavíme si pro rozhraní bridge studenti omezení 5 Mbps. (viz Obr. 23).



Obr. 23 Omezení rychlosti.

2.1.5. *Firewall* – Ve Firewallu nastavíme pravidla pro oddělení studentské sítě od lokální. Také musí nastavit NAT. Tam nastavíme maškarádu, která zprostředkovává přístup do Internetu studentům.



Obr. 24 Firewall pravidla

3. Nastavení vysílacích AP

Obě vysílací AP, které budou v budově ZŠ, mají téměř stejnou konfiguraci. Rozdílná konfigurace bude v názvu zařízení, ID EoIP tunelu a v IP adrese.

3.1.1. *Addresses, Identity* – Nastavíme si statickou IP adresu a název zařízení.

3.1.2. *EoIP* – Vytvoříme si EoIP tunel, který podle ID bude spojen s tunelem na hlavním routeru.

3.1.3. *Wireless* – V nastavení bezdrátové komunikace si vytvoříme dvě vysílací sítě. První bude SSID Ucitele na rozhraní wlan1. Tato síť

bude přístupná do školní sítě a nebude nijak omezena. Druhé SSID Studenti bude virtuální rozhraní wlan2. Sít' bude mít omezení rychlostní i přístupová. Tato omezení jsme nastavovali na hlavním routeru.

Name	Type	L2 MTU	Tx	Fx	Tx Packet (p/s)	Fx Packet (p/s)	MAC Address	AR
wlan1_Ucitele	Wireless (Atheros AR9...)	1600	0 bps	0 bps	0	0	0 4C:5E:0C:AB:0A:76	enable
wlan2_studenti	VirtualAP	1600	0 bps	0 bps	0	0	0 02:0C:42:8B:55:FF	enable

Obr. 25 Vysílací rozhraní.

3.1.4. *Bridge* – Zde přemostíme rozhraní EoIP tunel do rozhraní wlan2 a tím se všechna pravidla vytvořená na hlavním routeru aplikují do vysílací sítě Studenti. Druhý bridge s názvem SIT, slouží pro přemostění do vnitřní sítě školy.

Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Pat...
eoip-tunnel1	Studenti	80	10		designated port	
wlan2_studenti	Studenti	80	10		designated port	
ether1_privod	Siti	80	10		designated port	
wlan1_Ucitele	Siti	80	10		disabled port	

Obr. 26 Přemostění rozhraní.

3.1.5. *Scheduler* – Neboli plánovač. Z důvodu omezení využívání Wi-Fi v hodinách nastavíme zapnutí a vypnutí Wi-Fi pouze na přestávky. Učitelská Wi-Fi bude v provozu nonstop.

Name	Start Date	Start Time	Interval	On Event	Owner	Run Count	Next Run
Disable 2	May/09/2015	07:45:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 07:45:00
Disable 4	May/09/2015	08:41:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 08:41:00
Disable 6	May/09/2015	09:41:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 09:41:00
Disable 8	May/09/2015	10:41:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 10:41:00
Disable 10	May/09/2015	12:01:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 12:01:00
Disable 12	May/09/2015	13:01:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 13:01:00
Disable 14	May/09/2015	13:54:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 13:54:00
Disable 16	May/09/2015	19:00:00	1d 00:00:00	interface wirel...	admin	0	May/09/2015 19:00:00
Enable 1	May/09/2015	07:00:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 07:00:00
Enable 3	May/09/2015	08:29:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 08:29:00
Enable 5	May/09/2015	09:24:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 09:24:00
Enable 7	May/09/2015	10:24:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 10:24:00
Enable 9	May/09/2015	11:24:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 11:24:00
Enable 11	May/09/2015	12:44:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 12:44:00
Enable 13	May/09/2015	13:44:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 13:44:00
Enable 15	May/09/2015	14:34:00	1d 00:00:00	interface wirel...	admin	0	May/10/2015 14:34:00

Obr. 27 Plánovač vypínání a zapínání rozhraní wlan2.

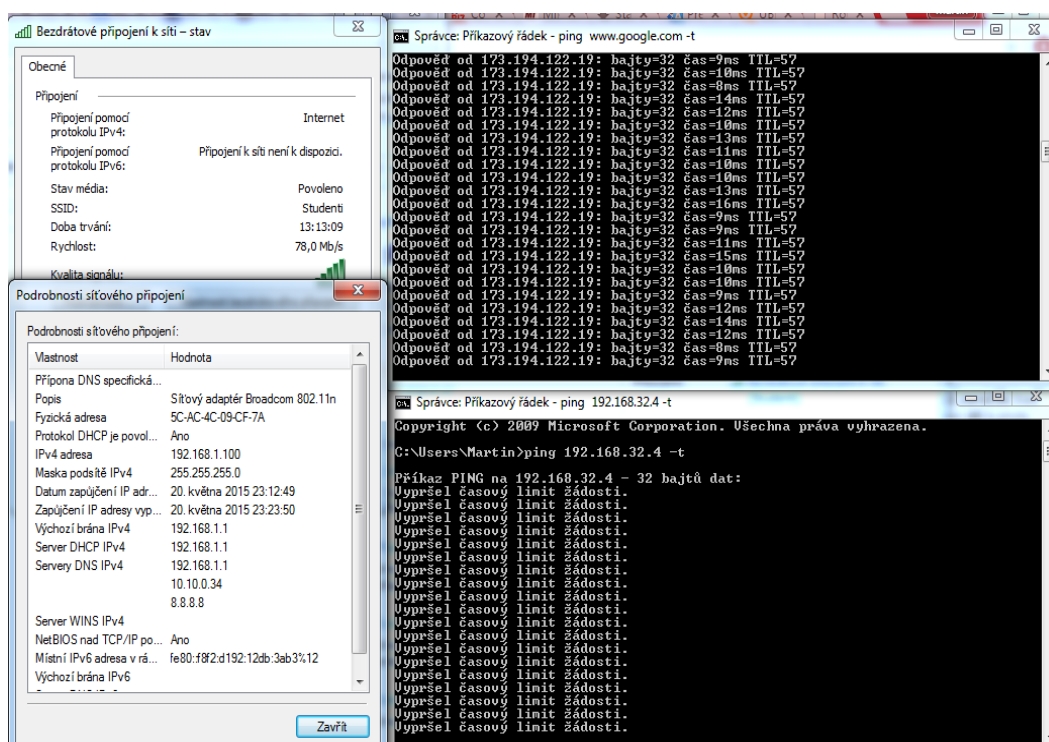
3.1.6. *NTP client* – slouží k synchronizaci času. Na hlavním routeru je nastaven NTP server, který zajišťuje, aby zařízení v síti měla stejný čas.

4. Nastavení AP ve školce

Školka je daleko od školy, takže je zde bezdrátový roaming zbytečný, a proto na tomto přístupovém bodě nebude využíván EoIP tunel. Z toho vyplývá, že všechny pravidla nastavená na hlavním routeru pro EoIP tunel použijeme na přístupovém bodě ve školce. Nastavíme zde DHCP s rozsahem 192.168.1.100-192.168.1.240. Ve Firewallu přidáme pravidla k oddělení sítě a NAT. Poslední odlišná věc bude nastavení omezení rychlosti. Tato nastavení se budou lišit od AP ve škole.

5.3.3 Testování Wi-Fi

Po nastavení a přemístění AP zařízení na připravené místo můžeme začít s testováním. Počítač nascanuje obě vysílací SSID. Po připojení na SSID Ucitela je počítač připojen s IP adresou vnitřní sítě a s přístupem na server.



Obr. 28 Testování Wi-Fi studenti

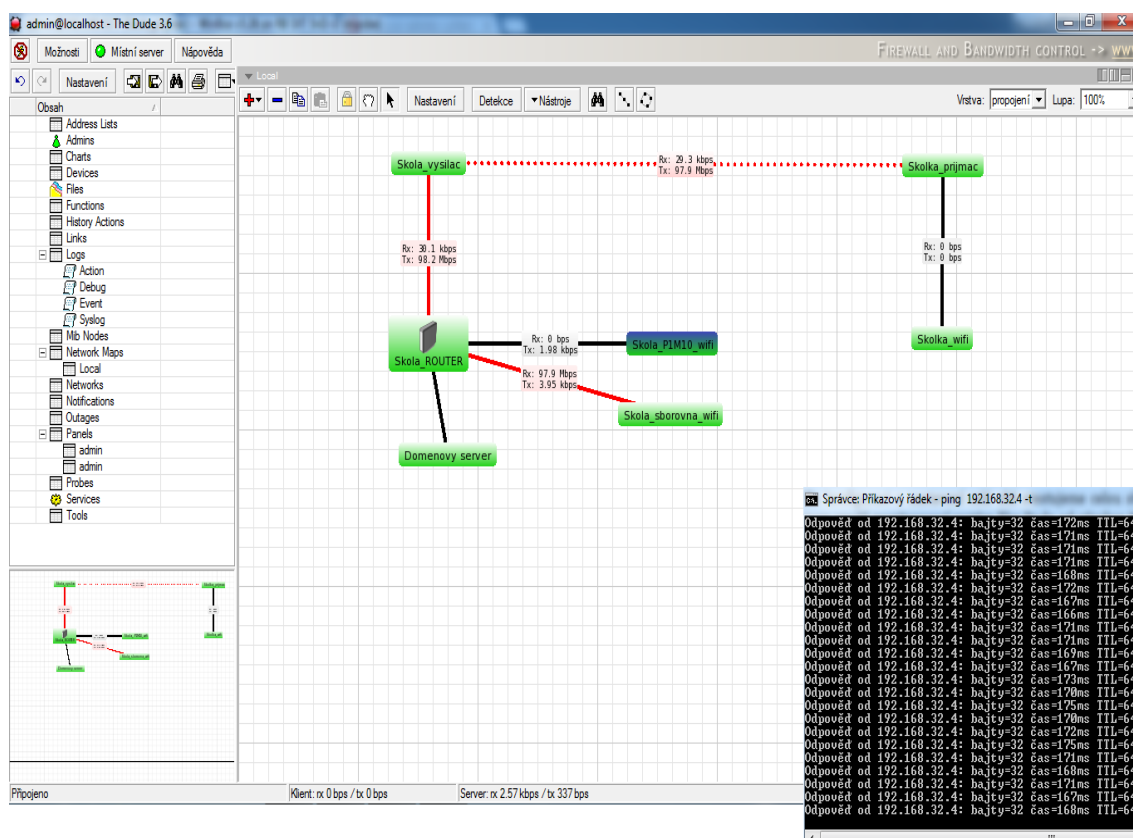
Podle obrázku č. 28 můžeme vidět, že se úspěšně podařilo připojit na Wi-Fi Studenti. Wi-Fi síť nepropustí ping na žádné školní zařízení kromě hlavního routeru. Odezva pingu je měřena při měření rychlosti. Rychlost přenosu dat je omezen na 5 Mbps. (viz obrázek č. 29).



Obr. 29 Měření rychlosti Internetu ve Wi-Fi síti Studenti.

Zdroj: <http://speedtest.net>

Přechod mezi přístupovými body musí být plynulý. Z tohoto důvodu byly vytvořeny EoIP tunely. Dle obrázku č. 29 vidíme výpadek pingu při změně přístupového bodu. Je z důvodu změny BSSID. Můžeme tedy říct, že nasazení bezdrátového roamingu proběhl úspěšně



Obr. 31 Monitoring sítě při toku dat.

Dle obrázku č. 31 vidíme odesílání dat ze školky do sborovny. Vysoký ping, ač stabilní, je způsoben využitím standardu Fast Ethernet. Tyto testy provedeme na více místech. Po ukončení úspěšných testů můžeme říct, že síť je připravena k provozu.

6 Ekonomické zhodnocení projektu

Závěrem projektu musíme zhodnotit práci po finanční stránce. Rozpočet školy na tento projekt byl 20000 Kč. Pro bezdrátové síť na frekvenci 5 GHz byly využity prvky MikroTik SXT Lite 5. Dále bylo nutné pořídit příslušenství pro fyzickou instalaci antén (konektory, kabeláž, pásky). Zdroj napětí a PoE adaptér je součástí krabice SXT. Pro Wi-Fi síť na frekvenci 2,4 GHz byly využity prvky MikroTik RB 951Ui-2HnD. U tohoto prvku nebylo potřeba žádného příslušenství. Veškerá práce byla provedena autorem práce. Jedná se o odhad zpracování cen firmou.

Tab. 5 Celková cena za projekt.

Název položky	Cena/ks	Množství	Cena celkem
MikroTik RB951Ui - 2HnD	1 520 Kč	3 ks	4560 Kč vč. DPH
MikroTik SXT Lite 5	1 440 Kč	2 ks	2880 Kč vč. DPH
Kabeláž	10 Kč/ m	20m	200 Kč vč. DPH
konektory	4 Kč	5 ks	20 Kč vč. DPH
	celkem za prvky		7660 Kč vč. DPH
Návrh konfigurace	300 Kč	6 h	1800 Kč vč. DPH
Instalace zařízení	300 Kč	3 h	900 Kč vč. DPH
Konfigurace zařízení	300 Kč	6 h	1800 Kč vč. DPH
Závěrečné testování	300 Kč	5 h	1500 Kč vč. DPH
Výjezd	300 Kč	1 h	300 Kč vč. DPH
	celkem za práci		6300 Kč vč. DPH
	Celková cena		13960 Kč vč. DPH

Vzhledem k tomu, že vybudování nové počítačové infrastruktury je z dotací EU, celková cena je pro školu přívětivá. Na zařízení a instalaci má škola záruku 2 roky.

7 Závěr

Cílem této bakalářské práce bylo dokončit budování nové počítačové infrastruktury. Práce včetně pokládání nové kabeláže cizí firmou trvala s přestávkami celkem rok. Tato práce přinese zlepšení podmínek nejen pro výuku, ale i pro práci zaměstnanců. Cela síť je zdokumentovaná nejen z logické topologie sítě, ale vytvořil jsem i nákresy sítě z fyzického pohledu. (viz. přílohy). Realizace projektu probíhala mimo školní výuku. Celkově jsme splnili všechny požadavky vedení školy. ICT učebna byla do nově vzniklé třídy přemístěna během víkendu. Mezi základní školou a mateřskou školou byl realizován bezdrátový spoj, který je dle testů více než dostačující. Závěrečným požadavkem bylo vytvoření Wi-Fi sítě, která proběhla úspěšně a Wi-Fi síť pokrývá 95 % objektu. Z ekonomického hlediska jsme měli rezervu téměř 7000 Kč. Možná se zbývající peníze investují do výpočetní techniky, která je dle mého názoru zastaralá, ale to není v mé kompetenci.

Zcela určitě je ve školní síti co zlepšovat. Pokud se síť bude dále rozšiřovat, je na uvážení, zda nepoužívat VLAN. K tomu by se musely dokoupit nové přepínače a vybudovat nový návrh sítě. Dalším určitě významným krokem do budoucna může být přechod ze standardu Fast Ethernet na standard Gigabit Ethernet. Kabeláž i zásuvky jsou na to připraveny, takže stačí pouze vyměnit síťové prvky. Dalším možným budoucím krokem může být využití certifikátu pro bezdrátovou komunikaci. Také jsem doporučil vedení školy o přidělení veřejné IP adresy pro hlavní router. Z důvodu absence síťového technika musím často jezdit do školy z důvodu vytváření nových účtů na serveru. Pokud by hlavní router měl veřejnou IP adresu, tak lze nastavit v NAT přesměrování adres a z domu se připojit přes vzdálenou plochu na Windows Server 2012. Všechny inovace jsou pouze otázkou peněz, které ve školství dlouhodobě nejsou.

8 Reference

- BURGESS, Dennis. *Learn RouterOS*. Lexington: Dennis Burgess, 2009, 391 s. ISBN 978-0-557-09271-0.
- FOGIE, Seth a Cyrus PEIKARI. *Windows Internet security: protecting your critical data*. Upper Saddle River, NJ: Prentice Hall, c2002, xix, 370 p. ISBN 0130428310.
- GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika. 2., přeprac. a aktualiz. vyd.* Praha: Grada, 2009, 496 s. Expert (Grada). ISBN 978-80-247-2615-1.
- HANÁČEK, PETR A JAN STAUDEK. Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií. [online]. Soubor ve formátu PDF. 2000 [cit. 2015-05-13].
- HAVEL, František: *Linux: EoIP tunel proti MikroTik*. [cit. 2015-05-13]. Dostupné z: <http://havel.mojeservery.cz/linux-eoip-tunel-proti-mikrotik/>
- HORÁK, Jaroslav. *Vytváříme domácí bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2011, 293 s. ISBN 978-80-251-2977-7.
- JANZA, Čeněk. *Návrh postupu pro ověření odolnosti podnikové LAN proti síťovým útokům*. Brno, 2014. Bakalářská práce. Mendelova univerzita v Brně. Provozně ekonomická fakulta. Vedoucí práce Ludmila Kunderová.
- JIROVSKÝ, Václav. *Vademecum správce sítě*. 1. vyd. Praha: Grada, 2001, 428 s. ISBN 80-7169-745-1.
- KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.
- KOKEŠOVÁ, Nikol. *Reálná prostupnost zařízení pracujících na standardu 802.11n*. [cit. 2015-05-16]. Brno, 2011. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Petr Münster.
- LOVEČEK, T. Bezpečnostná it politika ako jeden zo základných dokumentov organizácie [online], aktualizácia 19. 04. 2006, [2015-05-12], Security Revue. Dostupné na adrese: <http://www.securityrevue.com/article/2006/04/bezpecnostna-it-politika-ako-jeden-zo-zakladnych-dokumentov-organizacie/>
- MAČALA, Pavel. *Implementace zásad skupin pro doménu Microsoft Server ve společnosti Kovárna VIVA a.s* [cit. 2015-05-10]. Zlín, 2012. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky. Vedoucí práce Petr Šilhavý.
- MIKROTIK. manual:NV2. [online]. 2015 [cit. 2015-05-16]. Dostupné z: <http://wiki.MikroTik.com/wiki/Manual:Nv2>

- MIKROTIK. manual:Interface/EoIP. [online]. Dostupné z:
<http://wiki.mikrotik.com/wiki/Manual:Interface/EoIP>
- PLZÁK, Jan. *Migrace operačních systémů a jejich služeb malé podnikové sítě*. [cit. 2015-05-12]. Zlín, 2014. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky. Vedoucí práce Jiří Korbel.
- PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualiz. vyd. Brno: Computer Press, 2006, 430 s. ISBN 80-251-1278-0.
- PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.
- RUČKA, Tomáš. *Simulace přístupové metody CSMA*. [cit. 2015-05-15]. Praha, 2007. Bakalářská práce. České vysoké učení technické v Praze. Fakulta elektrotechnická. Vedoucí práce Jiří Douša.
- SKIPALA, Ondřej. *Bezdrátové sítě v zarušených prostředích*. Brno, 2011. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká.
- SKOVAJSA, T. *Bezpečnost WiFi sítí* [online]. 2012 [cit. 2015-05-10]. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Ing. Mgr. et Mgr. Zdeněk Říha, Ph.D.
- SLANINA, Martin. *Moderní bezdrátová komunikace: přednášky*. Vyd. 1. V Brně: Vysoké učení technické v Brně, Fakulta elektrotechniky a informatiky, Ústav radioelektroniky, 2010, 169 s. ISBN 978-80-214-4156
- SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. Vyd. 1. Kralice na Hané: Computer Media, c2010, 180 s. ISBN 9788074020360.
- STANEK, William R. *Active Directory: kapesní rádce administrátora*. [cit. 2015-05-12]. Vyd. 1. Brno: Computer Press, 2009, 352 s. Microsoft (Computer Press). ISBN 978-80-251-2555-7.
- STANEK, William R. *Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]*. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0.
- ŠTURMA, Michal. *Mapování a analýza WiFi sítě Österreich institutu v Brně*. [cit. 2015-05-17]. Brno, 2014. Bakalářská práce. Mendelova univerzita v Brně. Provozně ekonomická fakulta. Vedoucí práce Martin Pokorný.
- ŠUPOLA, Martin. *Renovace sítě a počítačových učeben na SOŠ Podyji*. Brno, 2014. Bakalářská práce. Mendelova univerzita v Brně. Provozně ekonomická fakulta. Vedoucí práce Jiří Balej.
- TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení*. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.
- VÁGNER, Adam. *Reálná prostupnost zařízení pracujících na standardu 802.11n*. [cit. 2015-05-16]. Brno, 2011. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Petr Münster.

VÁLKO, Martinl. *Prístupové mechanizmy pre vysokorychlostnú sieť s kruhovou topológiou*. [cit. 2015-05-16]. Bratislava, 2011. Diplomová práce. Slovenská technická univerzita v Bratislave. Fakulta informatiky a informačných technológií. Vedoucí práce Ivan Kotuliak.

WIKIPEDIA: *Twisted pair*. [online]. [cit. 2015-05-09]. Dostupné z:

http://en.wikipedia.org/wiki/Twisted_pair

WIKIPEDIA: Informační bezpečnost [online]. [cit. 2015-05-12]. Dostupné z:

http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_bezpe%C4%8Dnost

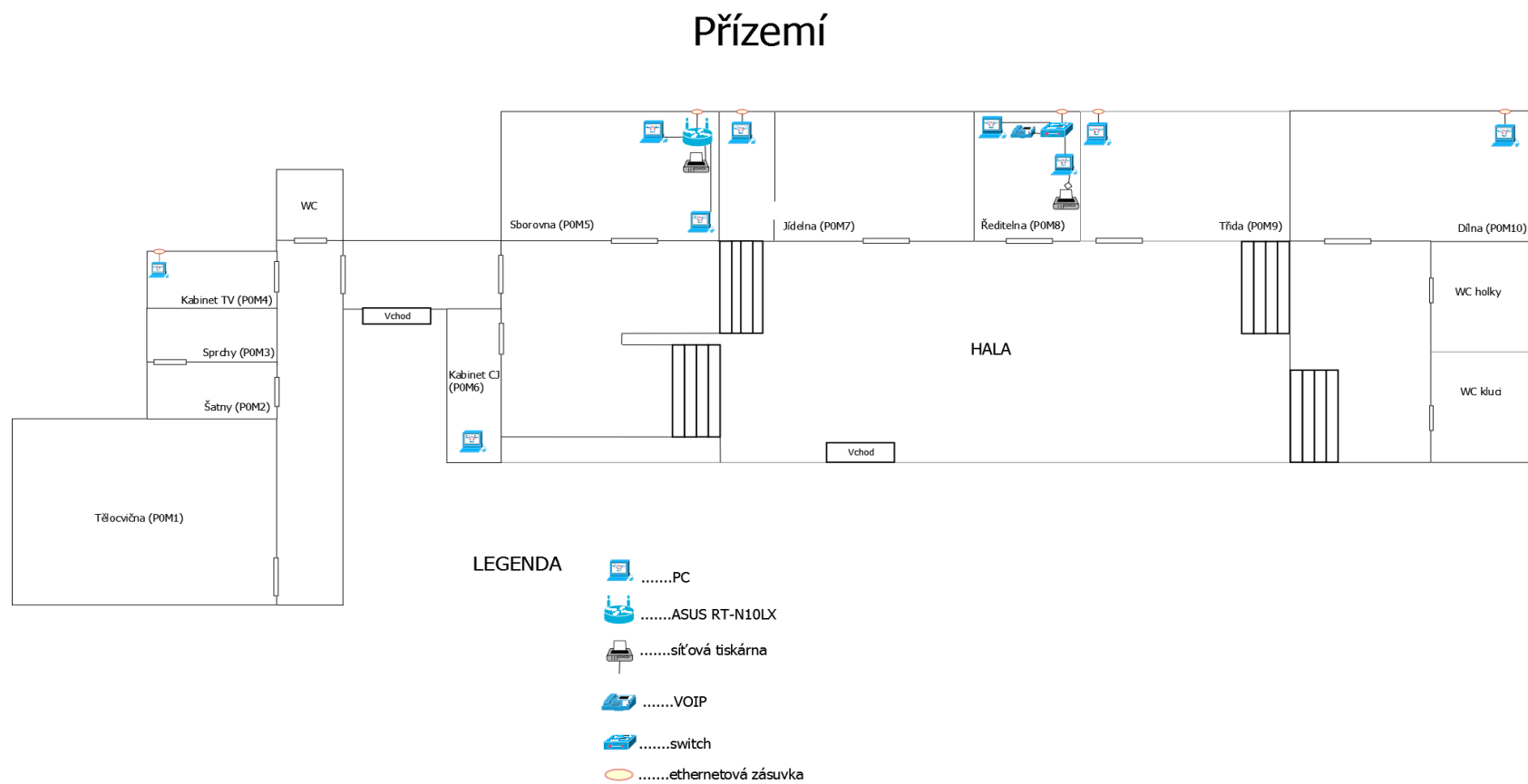
ZEMÁNEK, Jakub. *Stavba a správa sítě, aneb, Cesta do hlubin internetu*. Vyd. 1. Kralice na Hané: Computer Media, 2004. ISBN 80-866-8626-4.

ZSKANICE: *Historie* [online]. [cit. 2015-05-13]. Dostupné z:

<http://www.zskanice.cz/historie/>

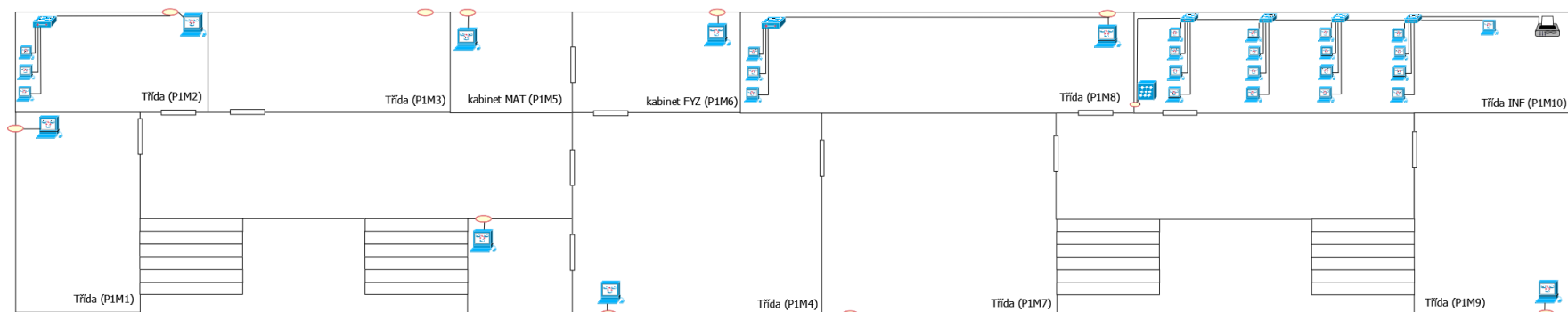
Přílohy

A Fyzický nákres staré sítě



Obr. 32 Fyzický nákres staré sítě – přízemí

1.patro



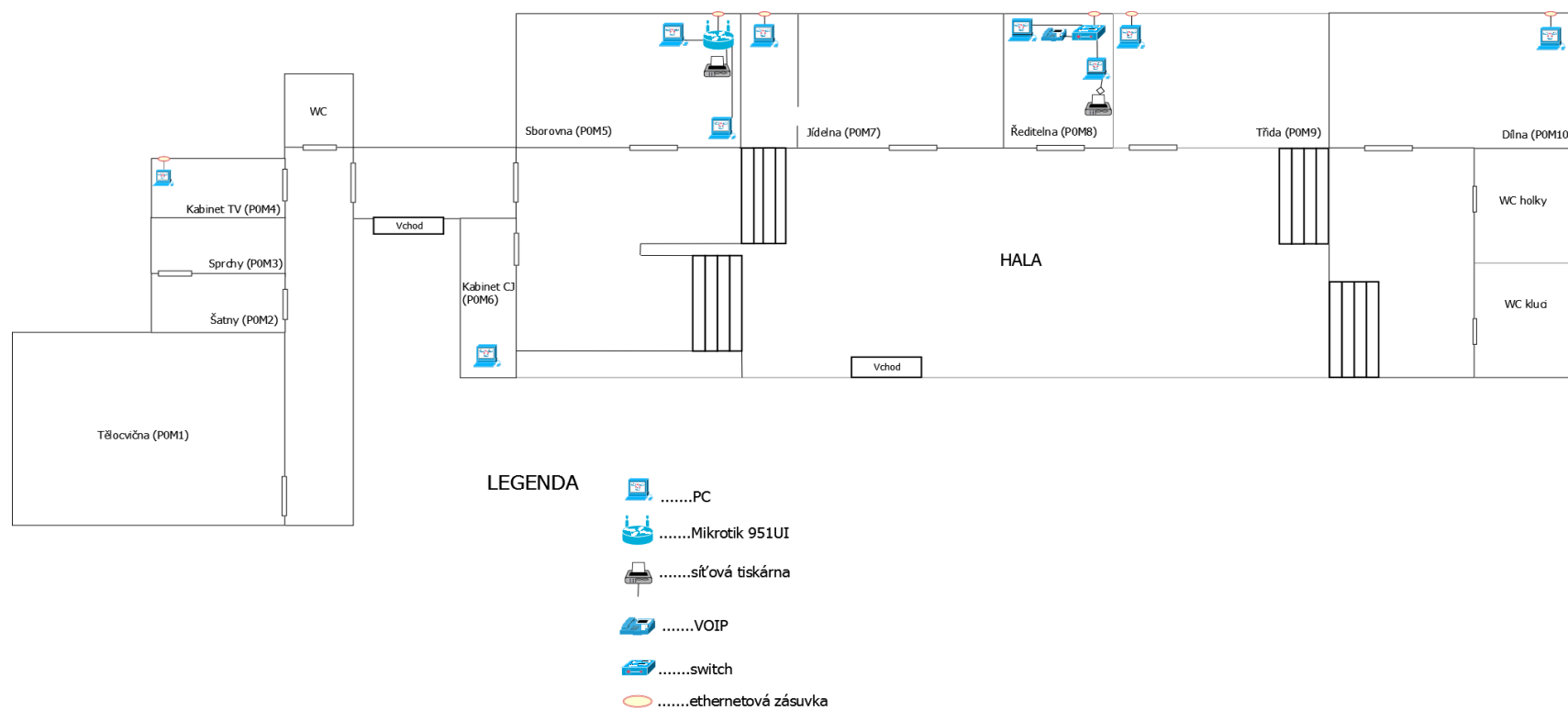
LEGENDA

- PC
- RACK
- síťová tiskárna
- switch
- ethernetová zásuvka

Obr. 33 Fyzický nákres staré sítě – 1.patro

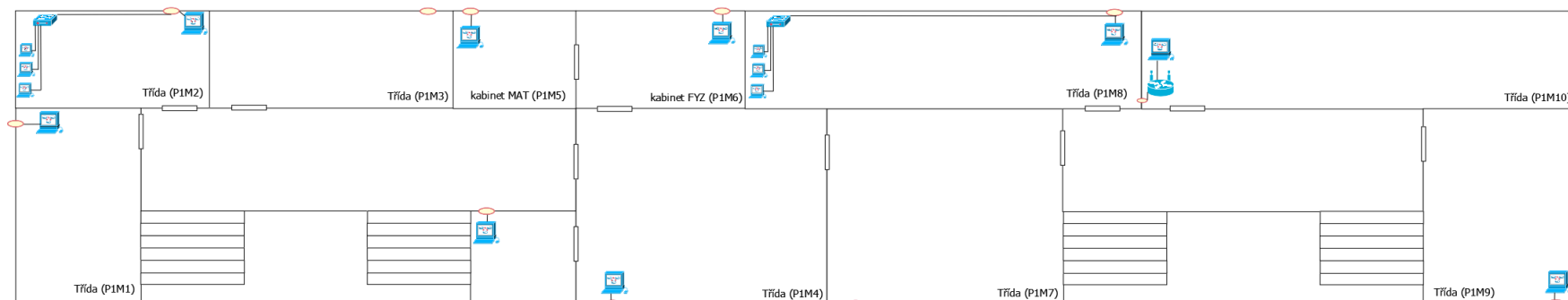
B Fyzický náskres nové sítě

Přízemí








Obr. 34 Fyzický náskres nove sítě – přízemí

1.patro

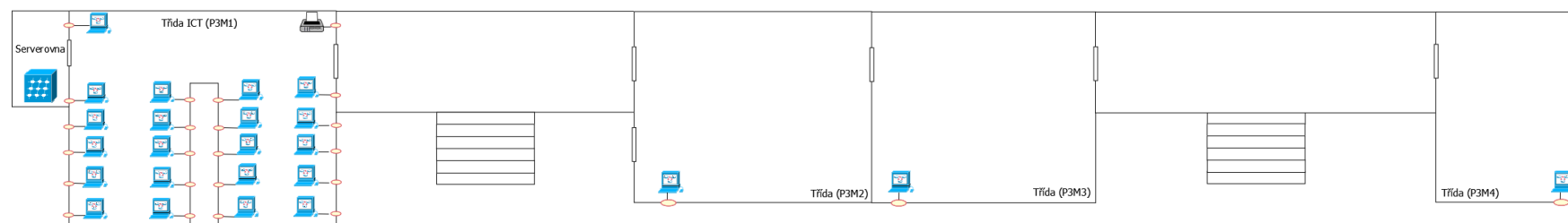


LEGENDA





- PC
- RACK
- síťová tiskárna
- switch
- ethernetová zásuvka
- Mikrotik 951UI

Obr. 35 Fyzický náčrt nové sítě – 1.patro

2.patro



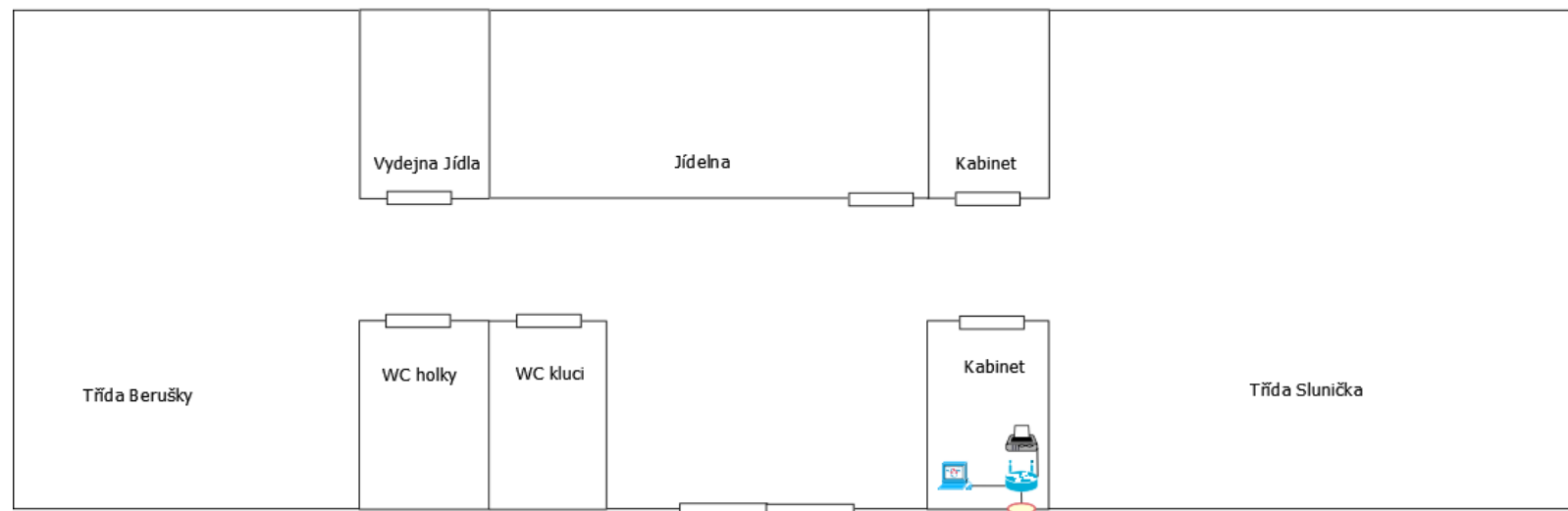
LEGENDA

- PC
- RACK
- síťová tiskárna
- ethernetová zásuvka

Obr. 36

Fyzický náskres nové sítě – 2.patro

Školka

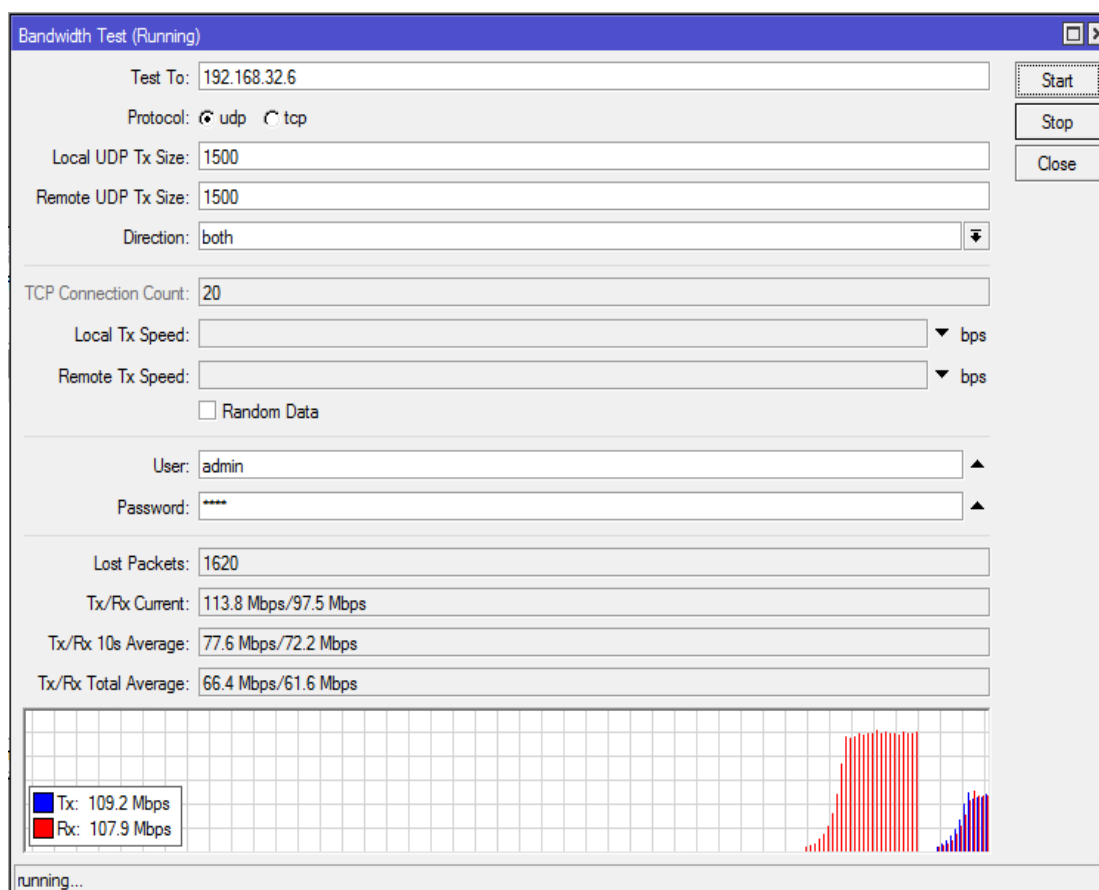


LEGENDA

-PC
-Mikrotik 951UI
-síťová tiskárna
-ethernetová zásuvka

Obr. 37 Fyzický náčrt nové sítě – školka

C Přenosová rychlost při šířce pásma 40 MHz.



Obr. 38 Bandwidth test s protokolem 802.11n a s šířkou pásma 40 MHz.

D Nastavení hlavního routeru.

The screenshot shows two windows from Mikrotik WinBox. The top window is the 'Bridge' configuration window, displaying a table of bridge statistics. The bottom window is the 'Bridge' configuration window showing interface settings for various ports.

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	MAC Address	Proto...
SIT	Bridge	1598	150.1 kbps	859.9 kbps	95	121	D4:CA:6D:A4:22:62	rstp
Studenti	Bridge	65535	35.2 kbps	571.1 kbps	59	73	02:07:1F:AD:16:66	rstp
Internet	Bridge	1600	843.6 kbps	133.3 kbps	111	164	D4:CA:6D:A4:22:5E	rstp

Interface	Bridge	Priority (n...)	Path Cost	Horizon	Role	Root Pat...
oeip-tunnel1	Studenti	80	10		designated port	
oeip-tunnel2	Studenti	80	10		root port	10
ether1_WAN	internet	80	10		root port	1110
ether2_server	SIT	80	10		designated port	
ether3_switch	SIT	80	10		root port	10
ether4_SXT_Vysilac	SIT	80	10		designated port	
ether5	SIT	80	10		disabled port	
wlan1	SIT	80	10		designated port	

Obr. 39 Nastavení bridge u hlavního routeru.

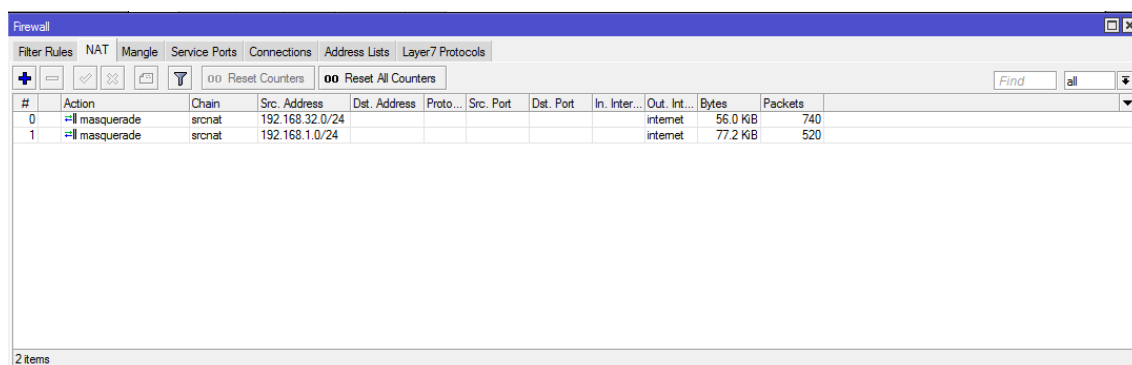
The screenshot shows three windows from Mikrotik WinBox. The top window is the 'DHCP Server' configuration window. The middle window is the 'Address List' window. The bottom window is the 'NTP Server' configuration window.

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
Studenti	Studenti		00:10:00	Studenti	no
dhcp1	SIT		00:10:00	dhcp-pool	no

Address	Network	Interface
192.168.32.1/24	192.168.32.0	SIT
192.168.1.1/24	192.168.1.0	Student
10.10.5.228/16	10.10.0.0	internet

NTP Client	NTP Server
<input checked="" type="checkbox"/> Enabled Mode: unicast Primary NTP Server: 10.10.1.14 Secondary NTP Server: 195.113.144.201 Dynamic Servers:	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Prioicast <input type="checkbox"/> Multicast <input checked="" type="checkbox"/> Anycast broadcast Addresses:

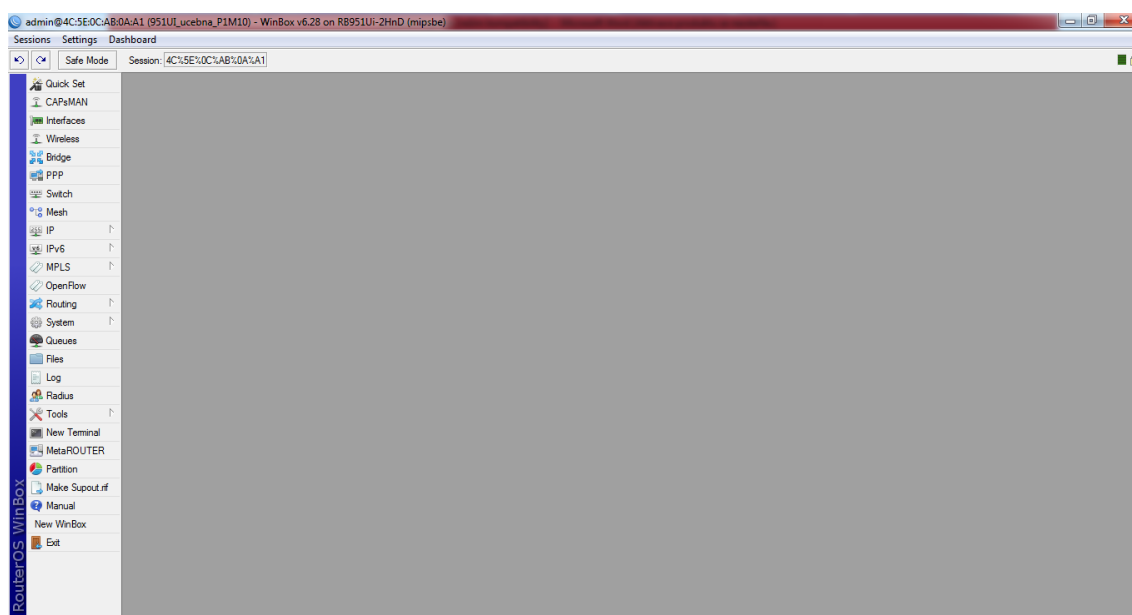
Obr. 40 Nastavení DHCP, Addresses a NTP serveru na hlavním routeru.



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active, and the 'NAT' sub-tab is selected. The main area displays a table of NAT rules. Two rules are visible, both named 'masquerade' and using the 'srcnat' chain. Rule 0 has a source address of 192.168.32.0/24 and shows 56.0 KB of bytes and 740 packets. Rule 1 has a source address of 192.168.1.0/24 and shows 77.2 KB of bytes and 520 packets. The table has columns for #, Action, Chain, Src. Address, Dst. Address, Proto., Src. Port, Dst. Port, In. Inter., Out. Int., Bytes, and Packets.

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	Bytes	Packets
0	masquerade	srcnat	192.168.32.0/24						internet	56.0 KB	740
1	masquerade	srcnat	192.168.1.0/24						internet	77.2 KB	520

Obr. 41 NAT na hlavním routeru.



Obr. 42 Prostředí RouterOS v programu Winbox.