Návrh a realizace bezdrátové sítě připojené do Internetu v oblasti obce Trnava

Proposal and realization of wireless network connected to Internet in the area of municipality Trnava

Bc. Roman Kalivoda

Diplomová práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav automatizace a řídicí techniky
akademický rok: 2006/2007

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Roman KALIVODA**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Automatické řízení a informatika**
Téma práce:	**Návrh a realizace bezdrátové sítě připojené do Internetu v oblasti obce Trnava.**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Navrhněte a realizujte bezdrátovou síť připojenou do Internetu v Trnavě.**
3. **Vyhodnoťte dostupnost, průchodnost, zarušení a stabilitu bezdrátové sítě.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. ZANDL, P. Bezdrátové sítě WiFi: Praktický průvodce. 1. vydání. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2
2. BARKEN, L. Wi-Fi: Jak zabezpečit bezdrátovou síť. 1. vydání. Brno: Computer Press, 2004. 173 s. ISBN 80-251-0346-3
3. FIEDLER, P.; BRADÁČ, Z. Zabezpečení bezdrátových sítí WiFi (IEEE 802.11b, g) [online]. 7.10.2004 [cit. 2006-6-11].
Dostupné z http://www.odbornecasopisy.cz/automa/2004/au100426.htm
4. Podrobné informace k provozu bezdrátových sítí v pásmech 5 GHz [online]. 17.11.2004 [cit. 2006-6-11].
Dostupné z http://www.i4shop.net/cz/iObchod/WebInfo.asp?Id=136

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav aplikované informatiky

Datum zadání diplomové práce: **13. února 2007**

Termín odevzdání diplomové práce: **24. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá návrhem a realizací bezdrátové sítě připojené k Internetu v oblasti obce Trnava. Protože je v dnešní době vysokorychlostní Internet v domácnosti pro většinu obyvatel samozřejmostí, snahou je vytvořit takový projekt, který vyřeší stávající problém téměř nulové možnosti vysokorychlostního připojení v této lokalitě a nahradí tak nedostačující a drahé nabídky mobilních operátorů.

Z důvodu složité geomorfologie celé oblasti musí být síť pečlivě navržena tak, aby byla signálem pokryta téměř všechna osídlená místa. Zároveň je nutné docílit toho, aby poruchovost byla co nejnižší a síť mohla nabízet zajímavé a atraktivní možnosti pro všechny zájemce. Také je potřeba zajistit, aby celkový projekt nebyl ztrátový a přitom mohl nabízet dobré vyhlídky do budoucna.

Klíčová slova:

Wi-Fi, Internet, ethernet, model OSI, TCP/IP protokol.

ABSTRACT

The goal of this thesis is proposal and realization of wireless network connected to Internet in the area of municipality Trnava. Nowadays is high-speed Internet for most of inhabitants matter of fact and on that ground the endeavour is to create project, which will solve existing problem of practically zero possibilities of high-speed connection in this locality and which will substitute deficient and expensive offers of mobile operator.

By the reason of complicated geomorphology must be network proposed careful to coverage of settled places. Simultaneously must be attained a low failure rate and the net could offer interesting and attractive potentialities for every users. It is necessary to avoid loss-making project and prepare conditions for advancement in the future.

Keywords:

Wi-Fi, Internet, ethernet, model OSI, TCP/IP protocol.

Chtěl bych poděkovat vedoucímu diplomové práce Ing. Miroslavu Matýskovi, Ph.D. za velmi užitečné rady a poznámky při vývoji tohoto projektu.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně, 23. 05. 2007 …….

Roman Kalivoda

OBSAH

ÚVOD

Dnešní moderní svět si asi těžko dokážeme představit bez výpočetní techniky, která nám každý den usnadňuje práci a komunikaci mezi lidmi. Nejen že se každý setkává s počítačem v zaměstnání a ve škole, ale osobní počítač se stal téměř pro všechny samozřejmostí i v domácnosti. Ale samotný počítač by pro nás neměl až takový význam, kdyby nebyl připojen k celosvětové počítačové síti - Internetu. Internet je jedním z nejvýznamnějších prvků při práci s počítačem. Můžeme zde najít nepřeberné množství informací a zábavy. Potřebná data můžeme vyhledat velmi jednoduše a rychle. Internet by ale nemohl existovat bez jedné velmi důležité věci a tou jsou počítačové sítě. Pod tímto pojmem si můžeme představit spojení klasické – tedy kabelové, nebo bezdrátové radiofrekvenční spojení bez potřeby pevné kabeláže.

Bezdrátové sítě dle normy 802.11a/b/g spojované se zkratkou Wi-Fi (Wireless Fidenlity) jsou jen dalším logickým stupněm ve vývoji telekomunikací. Fixní spoje budou v budoucnu dostávat čím dále tím méně prostoru a důraz bude kladen především na jednoduchost a mobilitu.

Zhruba před dvěma lety se Wi-Fi dočkalo mohutného rozmachu, který souvisel s rozjezdem výroby levných čipů pro bezdrátové sítě v Asii a Číně. Do této doby bezdrátové prvky prodávaly pouze drahé renomované značky jako Cisco, Intel, 3Com nebo Nokia. Jeden z prvních cenově dostupných čipů, který se začal vyrábět ve velkém, byl dnes již legendární čip Atmel. Byl použitelný pro access pointy, PCI a PCMCIA karty i USB klienty a prakticky odstartoval celosvětovou Wi-Fi mánii.

I. TEORETICKÁ ČÁST

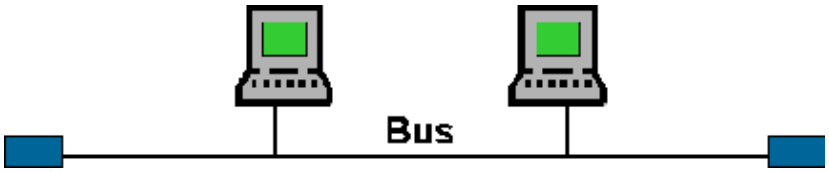
1 POČÍTAČOVÉ SÍTĚ

1.1 Topologie a komunikace

1.1.1 Základní topologie

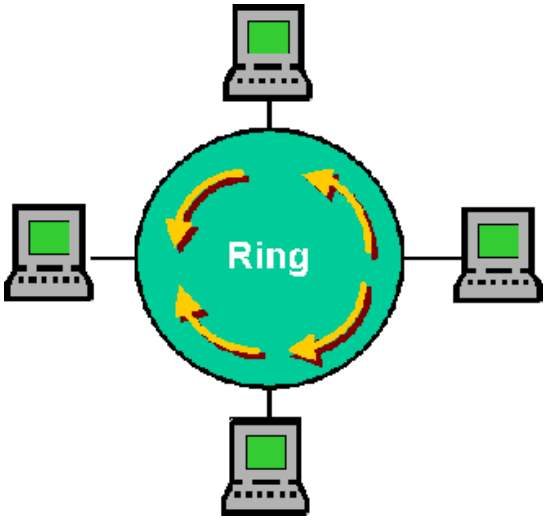
Základními topologiemi počítačových sítí LAN (Local Area Network) jsou:

sběrnice (bus) – tuto topologii používá Ethernet realizovaný koaxiálním kabelem. Existují dvě specifikace, 10Base-2 a 10Base-5, rozdíl je dán typem použitého kabelu a jeho délkou. Protože jde o přežitek nehodný dnešní doby, můžeme konstatovat, že tato topologie má několik nevýhod (např. obtížnou identifikaci příčin závad, topologickou omezenost počtu uzlů i vzdáleností mezi nimi, striktní sdílení pásma bez možnosti významněji ovlivnit tuto vlastnost použitím aktivních prvků atd.) a jedinou výhodu, kterou je cena řešení.



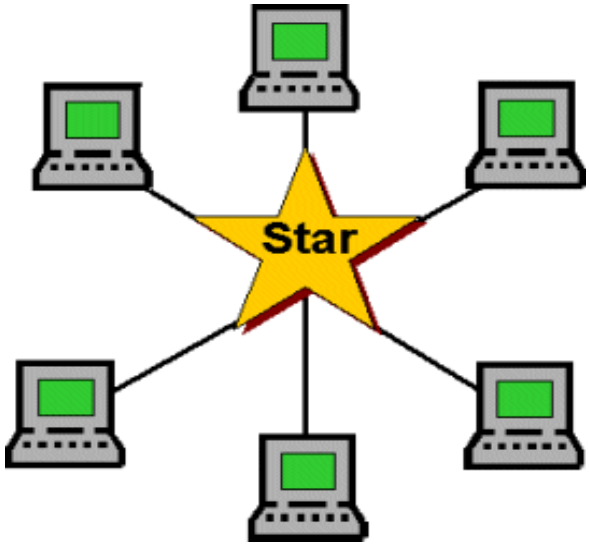
Obr. 1. Topologie sběrnice

kruh (ring) – tato topologie je založena na tom, že vysílací část jednoho uzlu je zapojena do přijímací části uzlu následujícího; typickými technologiemi používajícími topologii kruhu jsou Token Ring a FDDI. Jak Token Ring tak FDDI používají kruh logicky, ale fyzicky je topologie tvořena hvězdou s centrálním prvkem.



Obr. 2. Topologie kruh

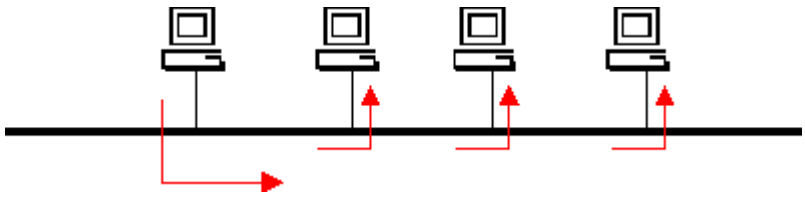
hvězda (star) – tato topologie představuje současný trend vytváření počítačových sítí. Spoje od koncových přípojných uzlů jsou vedeny do centrálního uzlu, kde je prvek realizující propojení koncových uzlů. Při obecném pohledu na topologii lze vidět, že struktura je vhodná nejen pro sítě (Ethernet, Token Ring, FDDI, ATM), ale i pro telefonní ústředny; prvek spojující uzly je pak v místě s označením **Star** (viz. obr. 3.).



Obr. 3. Topologie hvězda

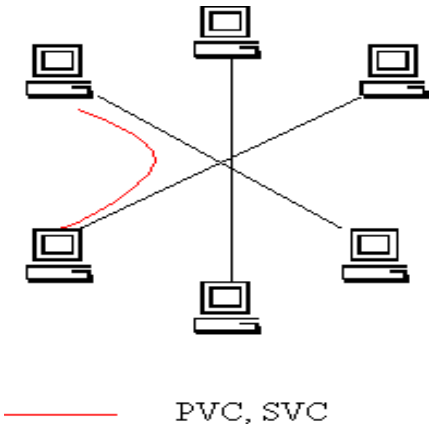
1.1.2 Charakter komunikace

Charakterem komunikace mohou být sítě spojové a nespojové (správněji nazývané jako sítě s navazováním spojení a bez navazování spojení – v angl. terminologii with connection a connectionless). U spojových sítí je před zahájením přenosu nutné navázat spojení, tzn. uzly se musí domluvit s aktivními prvky a koncovými uzly, které následně vytvoří virtuální kanál, prostřednictvím něhož jsou přenášena data. U nespojových sítí se žádné spojení nenavazuje.



Obr. 4. Nespojové sítě

Příkladem nespojových technologií jsou technologie založené na broadcastu, tzn. všesměrovém vysílání – např. Ethernet, Token Ring, FDDI. Rámec se dostane ke všem uzlům a příslušný uzel rozhoduje, zda je adresátem nebo ne.



Obr. 5. Spojové sítě

Příkladem spojových technologií je ATM. Zde musí před komunikací příslušných uzlů dojít k vytvoření trvalého spojení (PVC) nebo dočasného spojení (SVC). Pro stávající aplikace, které byly připraveny pro nespojové technologie, je nutné řešit komunikační princip prostřednictvím přidaných mechanismů typu Broadcast and Unknown Server (BUS). Určitým hybridem obou technologií může být přepínání nespojových technologií, kde sice nedochází k vytváření virtuálních spojů, ale zároveň jsou unicastové pakety posílány pouze příslušnému uzlu.

1.2 Principy komunikace, média, rozsah

1.2.1 Princip komunikace

Základní principy jsou stochastický a deterministický.

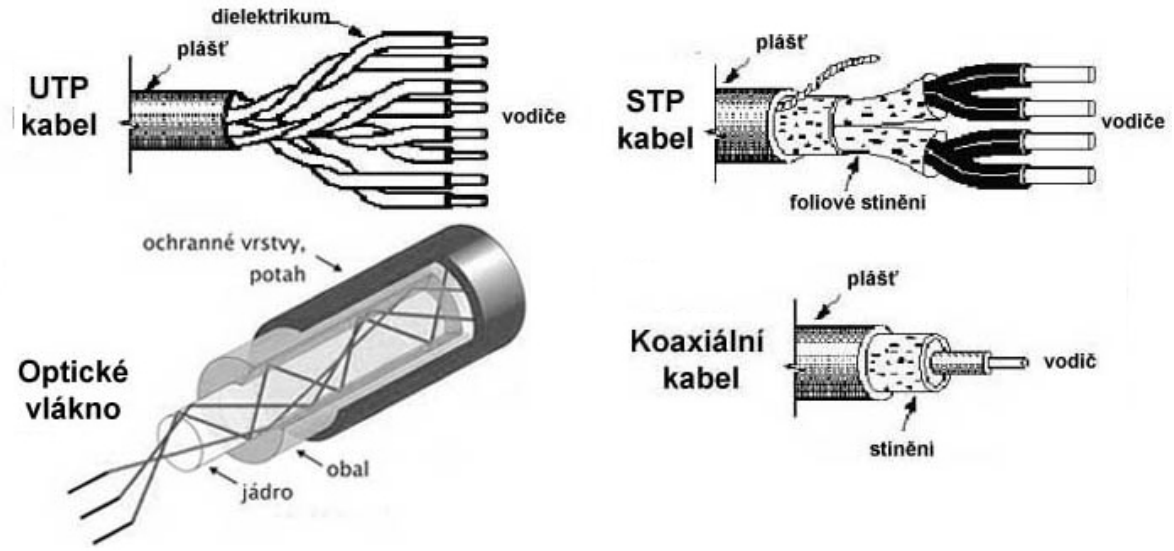
Stochastické metody jsou založeny na náhodném přístupu k médiu. Typickým představitelem technologie používající stochastickou metodu je Ethernet. Při stochastickém přístupu se jednotlivé uzly pokoušejí komunikovat bez jakéhokoliv pořadí. Žádný uzel tak nemá garantováno, že se mu podaří přenést určité množství dat za určitou dobu.

Deterministické metody jsou založeny na řízení přístupu k médiu. K řízení je používána metoda předávání speciálního paketu - peška (token). Typickým představitelem technologie používající deterministickou metodu je Token Ring. Velice zjednodušený náhled na funkci Token Ringu lze popsat následovně : po síti je přenášen paket nazývaný token. Uzel, který potřebuje komunikovat, musí počkat až k němu „token" dorazí. Pak má příležitost změnit příznak, doplnit hlavičku, naplnit datové pole a odeslat data cílovému uzlu. Ten po obdržení datového paketu zkontroluje kontrolní součty, nastaví příslušné

příznakové bity a pošle paket dále. Paket posléze dorazí k tomu uzlu, který data poslal. Tento uzel si prohlédne příznaky a předá je vyšším vrstvám. Vygeneruje prázdný paket (token) a odešle jej. Token je pak předáván mezi uzly na síti až dorazí k prvnímu uzlu, který má připravena data – a zde se historie opakuje. Ze znalosti maximální velikosti paketu a počtu uzlů na kruhu lze vypočítat maximální dobu, za kterou se uzlu podaří odeslat příslušné množství dat. Technologie je tedy logicky složitější a tím i dražší než Ethernet.

1.2.2 Použité přenosové médium

V současné době je v LAN nejpoužívanějším přenosovým médiem **kroucená dvojlinka** označovaný jako UTP (Unshelded Twisted Pair). Základním parametrem tohoto kabelu je impedance 100 ohmů. V Evropě je ovšem používanější stíněná modifikace tohoto kabelu – stínění je prováděno na úrovni celého svazku, jedná se tedy o ochrannou fólii pod plastovým obalem kabelu. Označení je pro tuto modifikaci do jisté míry závislé na výrobci. Někteří výrobci jej označují jako STP (Shielded Twisted Pair) nebo FTP (Foiled Twisted Pair). Napříč označení je nutné si uvědomit, že tyto moderní kabely mají impedanci stejnou jako UTP kabely. Tyto kabely nejsou shodné s klasickými STP kabely, které mají impedanci 150 ohm a mají zpravidla stíněné jednotlivé páry. UTP kabely lze používat pro celé spektrum současně používaných technologií – Ethernet Fast Ethernet, Gigabit Ethernet, Token Ring i ATM. Topologií, která je krouceným dvoupárem vytvořena je hvězda. Běžné označení pro sítě tvořené kroucenou dvojlinkou je **strukturovaná kabeláž**.



Obr. 6. Přenosová média

Ještě v nedávné době byl nejpoužívanějším přenosovým médiem v Ethernet LAN sítích **koaxiální kabel**. Výhodou byla cena a jednoduchost provedení. Nevýhodami jsou náchylnost k poruchovosti a technologická omezení (počet uzlů, rychlost).

V LAN sítích se pro překlenutí delších vzdáleností používají optické kabely. Pro kratší vzdálenosti (cca 260 m až 2 km v závislosti na technologii) multimodové (neboli mnohovidové) pro větší vzdálenosti singlemodové (neboli jednovidové). Stejně tak jako UTP kabely, lze i optické kabely použít pro celé spektrum aktuálních technologií. Optické kabely se používají i pro spojování budov tam, kde je nutné realizovat spoj venkovním prostředím a to i na poměrně krátké vzdálenosti. Optické kabely totiž zajistí galvanické oddělení potenciálů a nezpůsobí zničení infrastruktury při náhodném úderu blesku. Typickou topologií tvořenou optickým kabelem je hvězda.

Jsou místa kde nelze použít spojení optikou. Důvodem může být např. přílišná nákladnost položení kabelu nebo dokonce nemožnost položení kabelů. V tom případě jsou používány bezdrátové technologie. Ty byly časem rozvinuté tak, že jsou používány jako alternativa lokálních sítí založených na kabelových systémech. Nevýhodou jsou prozatím cena a relativně nízká rychlost. To ale naopak nečiní překážky pro použití bezdrátových sítí pro připojování k Internetu - zde se daří dosahovat více než zajímavého poměru cena/výkon.

Pro velké vzdálenosti se používají pronajaté datové okruhy jejichž provoz zajišťuje některý z poskytovatelů připojení (běžně telekomunikační operátor).

1.2.3 Rozsah

Sítě mohou být rozličně rozsáhlé - některé mají pouze několik uzlů v jedné místnosti, jiné mají velké skupiny rozmístěné po celém světě.

Pro sítě se podle rozsahu používá několik označení :

Local Area Network – **LAN** – běžně síť v jedné nebo několika sousedních budovách. V rámci budovy se používá strukturovaná kabeláž kombinují UTP kabely a optické kabely. Pro spojování budov se používají optické kabely nebo bezdrátové spoje.

Metropolitan Area Network – **MAN** – je označení pro síť většího rozsahu pokrývající např. území velkého podniku nebo města. Velmi zjednodušeně lze říci, že MAN je LAN s velkým počtem budov nebo několik LAN spojených vysokorychlostní páteří.

Wide Area Network – **WAN** – je síť tvořená větším či menším počtem vzájemně vzdálených LAN. Lokální sítě jsou spojovány většinou pronajatými datovými okruhy. Použité aktivní prvky (dnes již téměř výhradně směrovače) umožňují nejen přenos dat, ale ve stále větší míře i spojování telefonních ústředen.

1.3 Fyzická a linková vrstva ISO OSI

Pravděpodobně nejznámější metodu popisu komunikačních systémů představuje sedmivrstvá architektonická struktura, nazývaná **referenční model OSI**. Znalost této architektury je základním předpokladem pro pochopení funkce počítačových sítí, přenosu dat a návazných technologií.

Existují určité příměry usnadňující pochopení funkce datových přenosů. Tím nejoblíbenějším je srovnání s poštou. Srovnání s poštou dělí vrstvy na dvě části :

5 až 7 - *uživatelská část*

a 1 až 3 - *síťová část.*

Uživatelská část odpovídá v poštovní analogii psaní dopisu a splnění konvencí používaným pro doručení dopisů. Síťová část je v poštovní analogii přirovnávána ke službám zajišťujícím přenos dopisu mezi sběrnou schránkou do schránky domovní.

Mezi těmito částmi je 4. vrstva, která je chápána jako rozhraní mezi uživatelskou částí a síťovými službami. Lze ji přirovnat k přepážkové službě, kde se rozhoduje zda dopis půjde standardní službou, expres, letecky, jako balíček, stylem dopisu v láhvi atd.

Tabulka I. Vrstvy modelu OSI

7. aplikační
6. presentační
5. relační
4. transportní
3. síťová
2. linková
1. fyzická

Zatímco první čtyři vrstvy jsou poměrně exaktně definovány, zbylé tři vrstvy nemusí být striktně použity tak, jak jsou definovány podle tohoto modelu. (Příkladem kdy nejsou v modelu použity všechny vrstvy je např. IP protokol).

Teoreticky každá vrstva přidává zepředu k balíku dat hlavičku s údaji této vrstvy a na závěr kontrolní součet nebo informaci o ukončení dat vrstvy. Paket si pak lze představit následovně:

Obr. 7. Ukázka paketu

Velikost celého balíku i jeho režijní části je značně závislá na použité přenosové technologii, použitých protokolech a typu aplikace. Např. Ethernet umožňuje variabilitu v délce rámce 64 až 1518 byte, samotná hlavička tohoto protokolu je min. **xy** byte. Pokud je pro přenos použit protokol IP, představuje IP hlavička velikost min. 20 byte. Hlavička protokolu TCP má velikost min. 24 byte.

1.3.1 Fyzická vrstva

Fyzická vrstva (Physical Layer) specifikuje bitový přenos z jednoho zařízení na druhé prostřednictvím fyzického média. Samotné fyzické médium není součástí vrstvy, v OSI modelu je pod touto vrstvou. Fyzická vrstva zajišťuje synchronizaci (synchronní vs. asynchronní komunikace) a multiplexing – několik logických spojení lze realizovat jedním fyzickým médiem. Datové jednotky přenášené fyzickou vrstvou jsou **bity**. Tato vrstva je závislá technologicky (Ethernet, Token Ring, ATM, FDDI, ...), ale protokolově (IP, IPX, Vines IP, XNS, ...) je nezávislá. Prvky pracující na této vrstvě jsou opakovače a rozbočovače.

1.3.2 Linková vrstva

Linková vrstva (Data Link Layer) zajišťuje přístup ke sdílenému médiu a adresaci na fyzickém spojení – tj. v jednom síťovém segmentu. K adresaci jsou používány fyzické neboli MAC (Media Access Control) adresy. MAC adresa je 48 bitová adresa a je svázána se síťovým adaptérem připojujícím zařízení do sítě (např. 00-00-64-65-73-74). První tři oktety znamenají výrobce, další oktety zajišťují unikátnost MAC adresy.

Tabulka II. Formát hlavičky linkové vrstvy

Úvodní sekvence	Cílová adresa	Zdrojová adresa	...

Úvodní sekvence je často řazena do informace fyzické vrstvy. Cílová adresa (destination address) a zdrojová adresa (source address) jsou velmi významné součásti hlavičky linkové vrtsvy. Lze je nalézt téměř u všech síťových technologií (např. ArcNet, Ethernet, Token Ring, FDDI). Další části paketu jsou tvořeny zbývajícími údaji hlavičky, hlavičkami vyšších vrstev, přenášenými daty a údaji o ukončení příslušné vrstvy. V závislosti na hodnotě prvního bitu prvního oktetu adresy určení se adresy (a tím i pakety) dělí na Unicastové a NonUnicastové. **Unicastové** adresy slouží pro komunikaci s konkrétním uzlem, adresa určení odpovídá MAC adrese tohoto uzlu sítě (nebo MAC adrese směrovače). **NonUnicastové** adresy slouží pro komunikaci s určitou skupinou uzlů. Datové jednotky přenášené linkovou vrstvou jsou **rámce** (frame). Tato vrstva je znovu závislá technologicky, ale nezávislá protokolově. Prvky pracující na této vrstvě jsou můstky a přepínače.

1.4 Síťová a vyšší vrstvy referenčního modelu ISO OSI

1.4.1 Síťová vrstva

Síťová vrstva (Network Layer) zajišťuje adresaci v rámci síťového prostředí s více fyzickými segmenty. Používá logické adresy a prostřednictvím nich přenos dat z jednoho zařízení na druhé i z jedné sítě do jiné. Adresa zařízení má **dvě části** – část označující **síť** do níž zařízení patří (poštovní analogie – město + PSČ) a část označující konkrétní **uzel** (poštovní analogie např. ulice + číslo popisné). Konkrétním příkladem protokolu třetí vrstvy OSI je protokol IP. Dalším příkladem je IPX. Sítě jsou spojeny zařízeními pracujícími na této vrstvě. Jsou nazývány směrovače (routery) a mají přehled o okolních částech sítě. Síťová vrstva pak používá nejlepší cestu z jedné sítě do druhé – to je dáno buď konfigurací cest nebo použitím směrovacích protokolů.

Datové jednotky přenášené síťovou vrstvou jsou **pakety** (packet). Síťová vrstva je opět technologicky nezávislá, ale je závislá protokolově. Technologická nezávislost je dána tím, že pro každou požadovanou technologii je ve směrovači příslušný adaptér.

1.4.2 Transportní (přenosová) vrstva

Účelem transportní vrstvy (Transport Layer) je zajistit spolehlivost a kvalitu přenosu jakou požadují vyšší vrstvy. Principielně nabízí tato vrstva spojově orientované (connection - oriented) služby a nespojové (connectionless) služby.

Spojově orientované služby zajišťují spolehlivý přenos navázáním virtuálního spojení, výměnou informací o průběhu přenosu (potvrzováním příjmu rámců) a ukončení spojení. Na základě potvrzování je vysílající uzel schopen zopakovat ztracené nebo opožděné rámce. Konkrétním představitelem tohoto typu protokolů jsou SPX nebo TCP.

Nespojové služby slouží k jednoduchému odeslání dat. Na této vrstvě neexistuje mechanismus kontroly spolehlivosti. Je ji nutno zajistit mechanismy vyšších vrstev. Typickým představitelem tohoto typu protokolů je UDP.

1.4.3 Relační vrstva

Relační vrstva (Session Layer) zajišťuje pravidla pro navazování a ukončování datových přenosů mezi uzly na síti. Dále zajišťuje služby typu překlad jmen na adresy nebo bezpečnost přístupu. Poměrně zajímavou funkcí této vrstvy je synchronizace datových přenosů. Příkladem protokolů spojové vrstvy jsou např. Network File System (NFS), Structured Query Language (SQL), Remote Procedure Call (RPC) a další. Datové jednotky přenášené spojovou vrstvou jsou TPDU (Session Layer Protocol Data Unit).

1.4.4 Presentační vrstva

Presentační vrstva (Presentation Layer) je zodpovědná za formátování a syntaxi dat. Různé systémy používají různé kódy pro presentaci znakových řetězců, čísel s plovoucí čárkou, apod. Presentační vrstva tedy zajišťuje převod datových struktur mezi syntaxí používanou na příslušném systému a syntaxí obecnou. Další funkcí presentační vrstvy je konverze přenášených dat do formátu srozumitelného pro přijímající zařízení. Příkladem pro tyto operace jsou např. šifrování /dešifrování a komprese/dekomprese dat, které mohou být realizovány touto vrstvou.

1.4.5 Aplikační vrstva

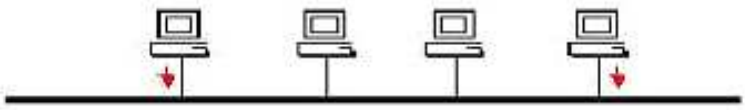
Aplikační vrstva (Application Layer) představuje okno, prostřednictvím kterého mohou uživatelé nebo aplikace vidět výsledky služeb zajišťovaných všemi předcházejícími vrstvami. Jde o vrstvu nejbližší uživateli, která na rozdíl od ostatních nezajišťuje služby pro vyšší vrstvu (žádnou již nemá). Příklady funkcí zajišťovaných touto vrstvou jsou souborové přenosy, sdílení zdrojů, přístup k databázím, prohlížení webových stránek, ovládání programů, apod. Datové jednotky přenášené aplikační vrstvou jsou APDU (Application Layer Protocol Data Unit).

1.5 Ethernet

V současné době je nejpoužívanější síťovou technologií Ethernet. Tato technologie je, nezávisle na tom zda jde klasický 10 Megabitový Ethernet nebo jeho rychlejší mutace (Fast Ethernet, Gigabit Ethernet a Ten Gigabit Ethernet), založena na velice jednoduchém principu, nazývaném CSMA/CD.

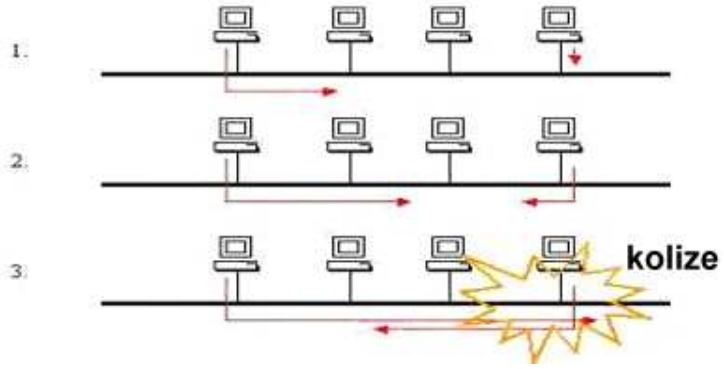
Na strukturovaném kabelovém systému lze používat rozličné síťové technologie založené na rozdílných přenosových metodách - např. Ethernet, Token Ring, CDDI, ATM.

CSMA (Carrier Sense Multiple Access) - stanice připravená vysílat data si „poslechne“ zda přenosové médium (kabel) nepoužívá jiná stanice. V případě, že ano, stanice zkouší přístup později až do té doby dokud není médium volné. V okamžiku kdy se médium uvolní začne stanice vysílat svá data.



Obr. 8. CSMA

CD (Collision Detection) - stanice během vysílání sleduje zda je na médiu signál odpovídající vysílaným úrovním (tedy aby se např. v okamžiku kdy vysílá signál 0 nevyskytl signál 1). Případ kdy dojde k interakci signálů více stanic se nazývá kolize. V případě detekce kolize stanice generuje signál JAM a obě (všechny) stanice které v daném okamžiku vysílaly generují náhodnou hodnotu času po níž se pokusí vysílání zopakovat.



Obr. 9. Detekce kolize

Fáze 1- stanice vlevo si poslechla na drátu zda někdo vysílá, zjistila, že ne a začala sama posílat data; v okamžiku kdy ještě signál nedorazil ke stanici vpravo si tato stanice ověřila stav média, zjistila, že je možnost zahájit vysílání.

Fáze 2 – obě stanice posílají data.

Fáze 3 – stanice vpravo zjistila kolizi a generuje signál JAM, všechny vysílající stanice zastavují vysílání a generují náhodné číslo.

Díky této jednoduchosti bylo dosaženo nízké ceny síťových adaptérů a aktivních prvků a tím i značného rozšíření Ethernetu. Jednoduchost řešení ovšem přináší i jednu významnou nevýhodu – s narůstajícím počtem uzlů narůstá počet kolizí a tím klesá teoretická propustnost sítě. Soubor uzlů jejichž vzájemná činnost může vygenerovat kolizi se nazývá **kolizní doména**. Logicky lze odvodit, že kolizní doména by měla být co nejmenší. Používané aktivní prvky mají ke kolizní doméně rozdílný vztah. Některé kolizní doménu rozšiřují, některé kolizní domény oddělují. Jejich volbou lze proto propustnost sítě ovlivnit.

Vedle pojmu kolizní doména existuje pojem **broadcastová doména**. Na počítačové síti se vyskytují principielně dva typy paketů – tzv. unicasty a nonunicasty. Unicasty jsou pakety které mají konkrétního adresáta vyjádřeného regulérní síťovou adresou. Nonunicasty používají skupinovou adresu a jsou určené buď všem uživatelům sítě (broadcasty) nebo vybrané skupině uživatelů (multicasty). Problém je v tom, že nonunicastu se musí počítač věnovat i když není určen pro něj. S nárůstem počtu uzlů v broadcastové doméně narůstá i množství nonunicastů. Z tohoto důvodu je nutné udržet velikost broadcastové domény v rozumné velikosti. Používané aktivní prvky mají k broadcastové doméně rozdílný vztah a proto lze jejich volbou propustnost sítě ovlivnit.

Formát paketu

Jak již bylo zmíněno, všechny rychlostní modifikace Ethernetu používají stejnou komunikační metodu CSMA/CD. Používají však i stejný formát a velikost paketu. Ethernetový paket je definován na 1. a 2. vrstvě OSI. Základní částí paketu je hlavička linkové vrstvy, která je následována daty (včetně hlaviček vyšších vrstev). Hlavičky jsou principielně 4 typů a jsou vzájemně nekompatibilní. Tyto typy jsou :

-Ethernet_II

-Ethernet_802.3

-Ethernet_802.2

-Ethernet_SNAP

Tabulka III. Nejjednodušší formát – Ethernet_II

Preamble	Adresa určení (DA)	Zdroj. adresa (SA)	Typ paketu	Data	CRC
8 byte	6 byte	6 byte	2 byte	46 až 1500 byte	4 byte

Každý paket je uvozen preambulí, která slouží k synchronizaci vysílající stanice a přijímajících stanic. Následuje adresa určení (MAC) a zdrojová adresa (MAC), číslo označující typ paketu, datová část a kontrolní součet. **Typ paketu** obsahuje číslo větší než 0x05DC. Jako příklad může být použit např. číslo 0800 označují IP paket nebo 8137 označují Novell IPX paket. Ostatní čísla lze najít např. v RFC např. 1700.

Používaná média

Ethernet je dnes nejčastěji standardizován v těchto verzích:

Fast Ethernet s přenosovou kapacitou 100 Mbit/s

100Base-TX -Používá jako přenosové médium kroucená dvojlinka (stíněná nebo nestíněná) s impedancí 100 ohm (min. Cat 5). Délka kabelu mezi uzlem a aktivním prvkem může být max. 100 m.

100Base-T4 -Používá jako přenosové médium kroucená dvojlinka (stíněná nebo nestíněná) s impedancí 100 ohm (min. Cat 3). Délka kabelu mezi uzlem a aktivním prvkem může být max. 100 m. Používá všechny 4 páry kabelu. Technologie ale není příliš rozšířena.

100Base-FX -Používá jako přenosové médium multimodový optický kabel. Délka kabelu mezi uzly může být v případě plně duplexního provozu max. 2 km; v příp. poloviční duplexu je vzdálenost ovlivněna zapojením sítě. Existuje i modifikace používající singlemodový optický kabel.

Gigabit Ethernet s přenosovou kapacitou 1000 Mbit/s

1000Base-SX -Používá jako přenosové médium multimodový optický kabel. Délka kabelu mezi uzlem aaktivním prvkem je ovlivněna parametry kabelu.

1000Base-LX -Používá jako přenosové médium ultimodový nebo singlemodový optický kabel. Délka kabelu mezi uzlem a aktivním prvkem je ovlivněna typem a parametry kabelu [1].

Ten Gigabit Ethernet

10GBase-T - Ethernet s rychlostí 10 Gbit/s. Využívá 4 páry S/FTP (jednotlivé páry stíněné metalickou fólií + metalický oplet kolem všech párů dohromady) kabeláže kategorie 6A (Category 6 Augmented - šířka pásma 500 MHz), je definován do vzdálenosti 100 metrů. V současné době (rok 2007) je ve vývoji nestíněná varianta UTP kabeláže kategorie 6A [5].

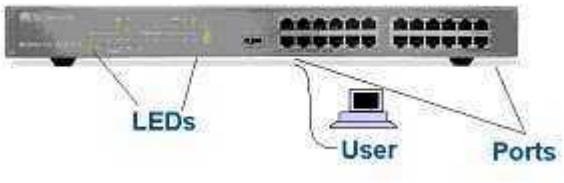
1.6 Aktivní prvky, fyzická a linková vrstva

Podle počtu uzlů použitých v počítačové síti a v závislosti na její topologii by měly být voleny aktivní prvky. Protože je zřejmý celosvětový příklon k technologii Ethernet a tato technologie je v mnoha společnostech zvolena za standard, bude popis prvků zaměřen převážně na ni (i když v některých případech je popis obecný). V LAN sítích jsou používány následující typy aktivních prvků. V tomto přehledu jsou rozděleny z pohledu sedmivrstvého modelu OSI.

1.6.1 Fyzická vrstva

Opakovač (repeater) – aktivní prvek zajišťující spojení dvou a více segmentů sítě tím, že signál obdržený na jednom portu zopakuje do ostatních portů přičemž signál přečasuje, tj. obnoví ostré vzestupné a sestupné hrany.

Rozbočovač (hub, koncentrátor) – multiportový opakovač vybavený UTP porty typu RJ45 nebo Telco, případně rozšiřujícím portem jiného typu (coax, FO, AUI); rozbočovač rozšiřuje kolizní i broadcastovou doménu; vedle klasických rozbočovačů používajících jednu rychlost (ať již 10 Mbit/s nebo 100 Mbit/s) existují dvojrychlostní rozbočovače (dual speed hub) – ty mají dvě sběrnice a port se automaticky přepne na jednu z nich v závislosti na tom jakou rychlost používá připojované zařízení; dvourychlostní rozbočovače se dnes již vyrábějí převážně v provedení s integrovaným přepínačem zajišťujícím spojení obou sběrnic.



Obr. 10. Rozbočovač

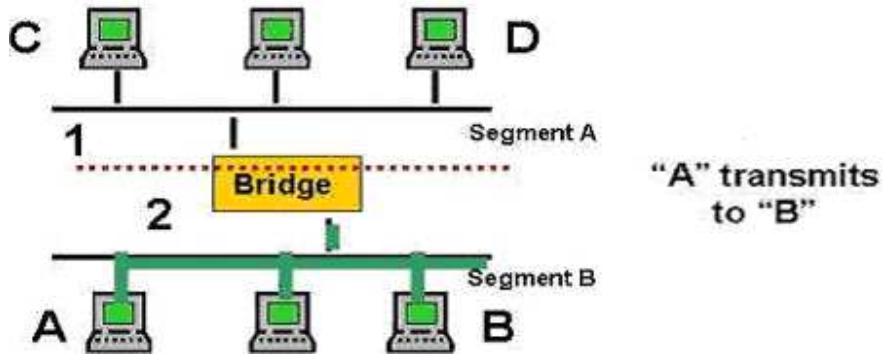
Počet opakovačů nebo rozbočovačů spojených za sebou je omezen. U technologie 100Base-X se vyskytují dva typy Class I a Class II. Typ Class I umožňuje vzájemné spojení maximálně dvou rozbočovačů, Class II spojování rozbočovačů dokonce neumožňuje. Pravidlo je naštěstí eliminováno přepínači takže je potřeba se pouze vyvarovat propojování rozbočovačů a volit vhodný návrh sítě.

Převodník (Media Converter) – je zařízení, které zajišťuje konverzi (převod) signálu z jednoho typu média do jiného. Rozdíl mezi opakovačem a převodníkem je v tom, že převodník na rozdíl od opakovače neprovádí přečasování signálu. Převodníky jsou dostupné v pevné konfiguraci nebo modulární, spravovatelné i nespravovatelné, připravené pro určitou technologii nebo universální. Jsou používány tam, kde je potřeba určitý počet portů definovaného typu a řešení na primárních aktivních prvcích je příliš nákladné (např. konverze z multimodové optiky na singlemodovou optiku nebo z UPT na optiku).

1.6.2 Linková vrstva

Můstek (bridge) – dvouportové zařízení které odděluje provoz dvou segmentů sítě na základě učení se fyzických (MAC) adres uzlů na obou portech, na základě těchto adres můstek buď data na druhou stranu propouští nebo nepropouští; můstek pracuje na druhé vrstvě modelu OSI (linková vrstva) a proto je protokolově nezávislý, je však závislý na

používané síťové technologii (přenosové metodě); můstek odděluje kolizní domény, ale rozšiřuje broadcastovou doménu; filtrační schopnost platí s jedním omezením – vztahuje se pouze na Unicast pakety, NonUnicast pakety (Multicast, Broadcast) jsou propouštěny.

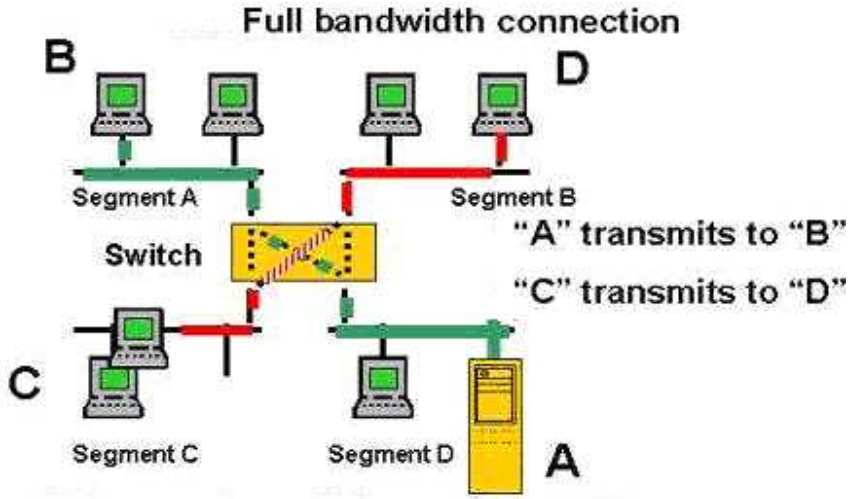


Obr. 11. Princip můstku

1. A posílá paket stanici B, můstek se dívá do tabulky zda má zavedenu MAC adresu vysílajícího, tedy A. V této fázi nemá, proto zavede MAC adresu A do tabulky s portem 2. Další krok můstku je pohled do tabulky zda je zavedena adresa stanice B. V případě, že není (a to v první fázi není) provede můstek tzv. flooding, tj. zkopíruje paket na všechny porty kromě toho na němž paket přijal.

2. B odpovídá A. Můstek se dívá do tabulky zda má B zaveden - nemá, zavádí jej tedy do tabulky s portem 2. Dále se dívá do tabulky na adresu A. Tuto adresu nachází na portu 2, tj. na stejném portu jako je vysílající stanice B. Paket tedy není kopírován do zbývajících portů. Při vysílání stanic C a D je princip stejný.

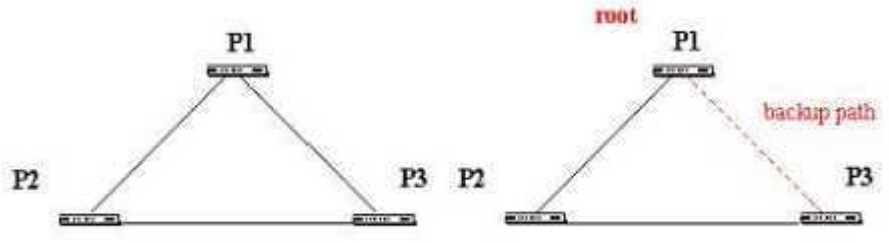
Přepínač (switch) – vysokorychlostní multiportový můstek který přináší nové významné vlastnosti. Umožňuje totiž paralelní komunikace mezi různými porty (tzn. např. dvojice portů 2-3, 5-9, 6-4, atd. mohou komunikovat současně), dále umožňuje aplikaci vysokorychlostních portů a pomocí inteligentního používání vyrovnávacích pamětí rozdělit provoz vysokorychlostního portu do několika portů s nižší rychlostí. Vedle standardního poloviční duplexního provozu přináší teoreticky dvakrát rychlejší plně duplexní provoz. Přepínač odděluje kolizní domény, ale rozšiřuje broadcastovou doménu (v případě nonunicatového paketu se chová jako rozbočovač – tj. pošle tento paket na všechny porty).



Obr. 12. Princip přepínače

Smyčky a mechanismus STP

Na základě obrázku si lze představit, že teoreticky stačí jeden NonUnicast k tomu aby zahltil síť. Přijde např. na některý z přípojných portů přepínače P1. Ten jej pošle na všechny ostatní porty včetně těch na něž jsou připojeny P2 i P3. P2 jej pošle na všechny porty mimo toho, na kterém jej přijal. Tím se paket dostává na P3 – ten jej posílá na P1, odtud jde na P2 a zase na P3, atd. Nekonečné kolečko je hotové. Původní paket od stanice připojené na P1 je ovšem šířen i druhou stranou, tj. z P1 na P3, z P3 na P2 a z P2 na P1, atd. Jedinou cestou na druhé vrstvě OSI jak se vyhnout těmto nekonečným přeposíláním paketů je zabránit vytváření smyček. Toho se dá dosáhnout pečlivým návrhem, realizací a rozvojem sítě nebo automatizovaným mechanismem nazývaným Spanning Tree Protocol (STP). Můstky a přepínače tento protokol používají.



Obr. 13. Smyčky

Hlavní význam STP je v tom, že uzavře redundantní cesty, ale zároveň umožní jejich opětovné otevření při selhání primární trasy (např. přerušením kabelu nebo výpadkem některého prvku po cestě).

Topologie je řízena prostřednictvím priorit. Každé zařízení může teoreticky být tzv. „root“, od kterého je topologie stavěna. Jako „root“ je voleno zařízení s nejnižší prioritou, případně s nižší MAC adresou. V závislosti na cenách (prioritách) jednotlivých linek jsou některé z nich vybrány jako funkční, ostatní jsou v záložním stavu.

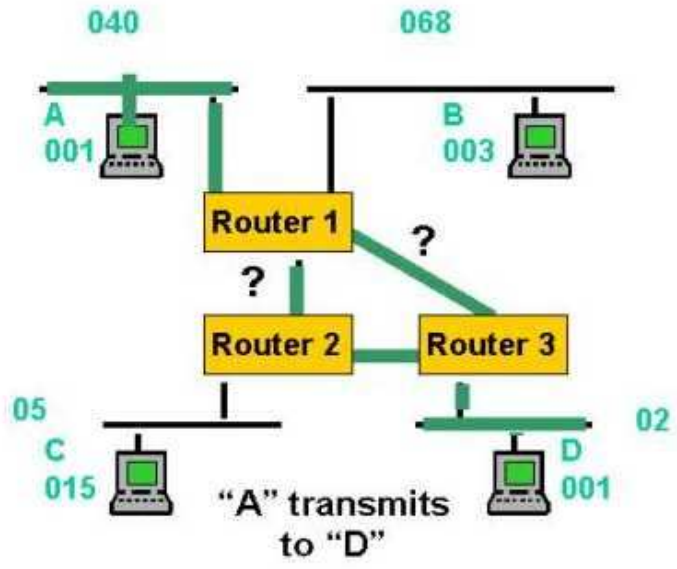
Určitou nevýhodou STP je poměrně dlouhá konvergence sítě v případě výpadku primární trasy nebo prvku, který je aktuálně zvolen jako „root“.

1.7 Aktivní prvky, síťová vrstva

Směrovač (router) – dvou nebo více portové zařízení které pracuje na podobném principu jako můstek; rozdíl je v tom, že směrovač pracuje na třetí vrstvě modelu OSI (**síťová vrstva**) – pracuje tedy s logickými adresami a je protokolově závislý, ale relativně nezávislý na použité síťové technologii (pro každou technologii musí mít patřičný adaptér); směrovače jsou v LAN sítích používány převážně pro spojení rozdílných technologií (např. Ethernet a Token Ring) a pro oddělení broadcastových domén (samozřejmě oddělují i kolizní domény) – tuto oblast však opouštějí neboť jsou zda nahrazovány směrovacími přepínači; vedle použití v sítích LAN našly směrovače důležité uplatnění ve WAN sítích, kde jsou používány pro připojování vzdálených lokalit

Můstek (přepínač) pracuje s jednou tabulkou a to s tabulkou kde jsou relace mezi MAC adresou a portem zařízení. Směrovač pracuje se dvěmi tabulkami. V první je relace mezi MAC adresou, logickou adresou a portem (tabulka obsahuje údaje pouze o přímo připojených uzlech). V druhé tabulce je seznam sítí (částí logických adres) s portem kudy je na danou síť nejlepší cesta.

Lze si představit, že kompletní adresa je interpretována dvěma čísly oddělenými tečkou ve formátu síť.uzel (např. 040.001). Část sítě musí být unikátní z globálního hlediska tzv. intersítě (neboli propojení několika lokálních sítí - subsítí). Pokud bude mít pardubická síť logickou adresu 040, žádná jiná lokalita spojená s Pardubicemi nemůže tuto adresu použít. Libovolný prvek může použít adresu uzlu 001, pak však tuto adresu uzlu nesmí použít žádný jiný prvek v dané lokalitě, ale v jiné lokalitě ji může použít bez problému – celková adresa 040.001 je totiž jiná než 02.001.



Obr. 14. Princip směrovačů

Směrovač Router 1 ví, že se k prvku D dostane dvěma cestami. Jedna z nich je výhodnější a proto používá ji. Existují však i mechanismy pro rozložení zátěže a používání všech dostupných cest (např. ECMP – Equal Cost Mlti Path).

Směrovací přepínač (routing switch) – jde o relativně nový typ zařízení pracující s rychlostmi obvyklými pro druhou vrstvu i s informacemi třetí vrstvy, zajišťuje tedy směrování při rychlosti přepínání – tím nahrazuje pomalé směrovače v oddělení broadcastových domén; směrovače vytlačuje do použití pro spojení rozdílných technologií, do prostředí se speciálními protokoly (Banyan Vines, DECNet, …) a do WAN komunikací

Výhody směrovacích přepínačů:

Nejmodernějším trendem pro centra počítačových sítí je tzv. přepínání na 3 vrstvě OSI (Layer 3 Switching). Jedná se o vlastně o směrování prováděné hardwarově. Důvod pro zavádění této technologie je následující - před několika lety se pro rozdělení sítí do více skupin používaly směrovače (tzv. colapsed backbone architektura). Při stále narůstajícím zatížení sítí přestaly směrovače vyhovovat (nízký výkon za vysoké ceny, velké zpoždění paketů při průchodu směrovačem). V té době přišly na svět výkonné přepínače. Začaly jimi být nahrazovány centrální směrovače, ale správci sítí si společně s dodavateli velice záhy ověřili slabinu přepínačů – přenášejí broadcasty a tudíž se sítě s vysokým počtem stanic začínají zahlcovat. Směrovače proto znovu našly uplatnění v propojování segmentů sítí postavených na přepínačích (tzv. virtuálních sítí). Protože jsou však směrovače drahé a technologický rozvoj postoupil značně dopředu, začali výrobci hledat cesty jak řešení

maximálně zlevnit. Jako jedna z nejschůdnějších se ukázala cesta integrace směrování do přepínačů, tedy tzv. Layer 3 Switching. V podstatě se jedná o obdobu přepínání na druhé vrstvě – zde je přepínání na základě tabulky MAC adres; na třetí vrstvě je přepínání také řešeno hardwarově a rozhodovací algoritmy jsou rozšířeny o další tabulku – tabulku logických adres (převážně IP, časem i IPX). Definice směrovacího přepínače (Routing Switch), tak jak jej zavedla firma která tento pojem začala používat jako první, tedy Bay Networks, hovoří o několika základních atributech:

-přepínání na 3. vrstvě je implementováno v hardware;

-směrování a přepínání jsou stejně rychlé;

-zařízení zajišťuje libovolnou kombinaci přepínání i směrování na každém portu;

-průchodnost při zvýšeném zatížení, implementaci filtrů nebo použití QoS zůstane zachována;

-zařízení rozhoduje o každém paketu;

-zařízení umožňuje provozovánív standardních směrovacích protokolů (RIP, OSPF);

Všechna zařízení by měla být připojena na UPS, zajistí se tím ochrana proti výpadku napájení, ale i ochrana proti poruchám napájecí sítě (např. přepětí) a tím i možné poruše.

1.8 IPv4 protokoly a model OSI

Protokoly třídy TCP/IP byly vyvinuty na začátku 70-tých let pro potřeby amerického ministerstva obrany (DoD – Department of Defense) a jeho síť ARPANET (Advanced Research Project Agency´s NET). Tato síť byla navržena jako experimentální WAN s přepínáním paketů. Protože byl experiment úspěšný, došlo v dalších letech k rozvoji a vylaďování protokolového stacku a jeho adaptaci pro použitelnost i v LAN.

Začátkem 80-tých let byl TCP/IP implementován jako integrální součást Berkley UNIXu verze 4.2. V roce 1983 byl protokol TCP/IP přijat americkou armádou jako standard pro síťové komunikace. IP protokol získal takovou oblibu a je v něm spatřována budoucnost kvůli těmto důvodům:

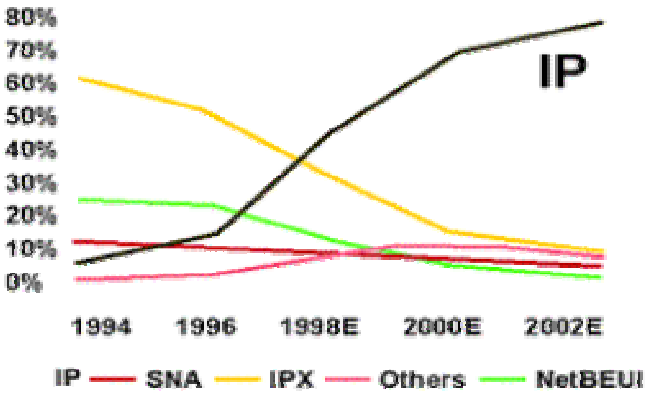
-IP protokol není proprietární (na rozdíl od např. IPX, DecNET, SNA, …) a není uzavřený, je vyvíjen a rozvíjen na základě široké spolupráce výrobců a uživatelů;

-není monolitický, ale je definovatelný na základě modelu OSI;

-zajišťuje interoperabilitu mezi různými platformami (PC, Workstation, Mini, Mainframe; Unix, Windows, Mac) a výrobci (IBM, HP, Sun, PC, …);

-jsou na něm založeny aplikace typu klient/server (např. SAP R/3);

-jsou na něm založeny webové technologie a Internet.



Obr. 15. Dominance protokolu IP

Poněkud matoucí může být to, že občas je o protokolu psáno jako o protokolu IP a někdy jako o TCP/IP.

Tabulka IV. Popis IP protokolu ve vztahu k referenčnímu modelu OSI

OSI	IP	
7. aplikační	Application (5-7) TCP	Application (5-7) UDP
6. presentační		
5. relační		
4. transportní	Transport (4)	
3. síťová	Internet (3)	
2. linková	Interface (1 a 2)	
1. fyzická		

Vrstva **Interface** není tímto modelem popsána. Zajišťuje protokolům IP funkčnost pro enkapsulaci datagramů a jejich přenos specifickým médiem (včetně relace mezi IP a MAC adresou).

Vrstva **Internet** používá protokol nazývaný Internetwork Protocol – zkratka **IP** a jeho prostřednictvím zajišťuje :

-služby doručení datagramů bez závislosti na fyzické médium (vrstvu Interface);

-adresní mechanismus;

-směrovací schéma pro přenos dat.

Vrstva **Transport** zajišťuje spolehlivý přenos dat mezi dvěma koncovými uzly. Míra spolehlivosti odpovídá požadavkům aplikace. Pro přenos dat jsou používány dva typy protokolů – Trasmission Control Protocol známý zkratkou jako **TCP** a User Datagram Protocol - **UDP**.

Vrstva **Application** zahrnuje protokoly specifikující procedury pro uživatele (přihlašování se k serverům, přenos souborů, …). Procedury (aplikace) jsou rozděleny podle použitého protokolu vrstvy Transport. Jsou jimi protokoly UDP a TCP.

Část protokolového stacku podle 3. vrstvy OSI

Jak již bylo popsáno v předchozí části, protokol 3. vrstvy OSI (síťové) je Internetwork Protocol (IP) a jeho úkolem je zajistit adresaci a bezspojovou přepravu datagramů v rámci síťového prostředí; IP protokol má jako všechny ostatní protokoly 3. vrstvy OSI přesně definovanou adresní strukturu, kde každá adresa musí být unikátní.

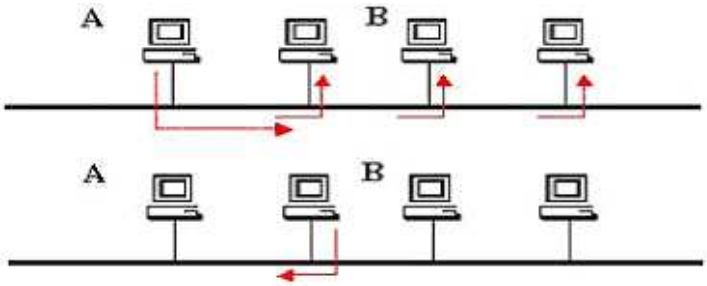
V současné době je používána verze IPv4. Ta byla připravena pro přenos dat a má v moderních sítích řadu omezení, které je nutno řešit podpůrnými mechanismy a protokoly. Je připravena nová verze nazývaná IPng (IP new generation) nebo IPv6 IP version 6. I když má řadu výhod a integrované důležité mechanismy (např. podporu QoS 4 bitovým polem pro priority) k jeho masovému rozšíření zatím nedošlo a zdá se, že jen tak hned nedojde.

1.9 ARP – protokol a mechanismus zjišťování MAC adresy

Komunikační mechanismus podle referenčního modelu OSI vyžaduje vyplnění údajů hlaviček všech vrstev. Z tohoto důvodu potřebujeme k IP adrese zjistit MAC adresu. Mechanismus zjišťování MAC adresy pro IP protokol se nazývá ARP (Address Resolution Protocol). Předpokládejme, že stanice A má IP adresu 192.168.1.21 a chce komunikovat s adresou 192.168.1.1. Mohou nastat dva případy. Stanice spolu nedávno komunikovaly a uzel má MAC adresu uloženu v tzv. ARP Cache. ARP Cache je paměťový segment v němž

je držena tabulka s relacemi IP adresa, MAC adresa. Důvodem je snížení množství požadavků na zjišťování MAC adres. Údaj je v ARP Cache je však držen omezenou dobu.

Stanice si tedy v první fázi zkontroluje zda má v ARP Cache MAC adresu dané IP adresy. Pokud ne, musí si MAC adresu zjistit.



Obr. 16. ARP

1. stanice A odesílá **ARP Request**, zdrojovou adresou je její MAC adresa a adresou určení je broadcast; zdrojová adresa i adresa určení protokolu IP odpovídají konkrétním hodnotám

2. všechny uzly se musí broadcastu věnovat a porovnat svoji IP adresu s adresou určení, ten uzel jehož IP adresa odpovídá adrese z požadavku posílá tzv. **ARP Response**, tedy odpověď s vyplněnou svojí MAC adresou. Další vzájemné komunikace obou uzlů probíhají prostřednictvím Unicastů.

ARP není IP protokol v pravém slova smyslu protože nemá IP hlavičku – tím nemůže ani opustit logickou síť neboť nemůže projít přes směrovač.

1.10 Základy směrování v IP prostředí

Stanice v rámci jedné logické sítě komunikují přímo (s použitím mechanismu ARP). Pokud však chce komunikovat stanice z jedné sítě (např. 192.168.1.x) s uzlem z jiné sítě (např. 192.168.2.x), je potřeba sítě propojit zařízením pracujícím na 3. vrstvě OSI, tzv směrovačem.

Směrovače si udržují přehled o tom, za kterým rozhraním je která síť. Tyto informace jsou do zařízení zadány staticky nebo je používán určitý mechanismus pro jejich dynamickou výměnu (to znamená, že směrovače si vzájemně předávají informace o sítích o kterých vědí). Dynamických směrovacích protokolů poměrně široká škála. Jejich použití je vhodné pro různé velikosti sítí a aplikace je rozdílně komplikovaná. Jedná se např. o protokoly RIP, OSPF, BGP, EGP, IGRP atd..

Tabulka V. Příklad směrovací tabulky (routing table)

Cílová síť Destination Network	Následující směrovač Next Hop Router	Metrika Metric (Hops)
192.168.1.0	Direct Port 1	0
192.168.2.0	Direct Port 2	0
192.168.3.0	192.168.2.3	1
192.168.4.0	192.168.2.3	2

V závislosti na implemenatci mohou být součástí směrovací tabulky i masky cílových sítí a typ protokolu pomocí něhož směrovač o síti ví. Speciálním typem statické cesty je tzv. **Default Route**, používaná pro všechny neznámé sítě. Ta má tvar samých nul, tedy adresa 0.0.0.0 s maskou 0.0.0.0. U standardních pracovních stanic, které si nedrží tabulky s cestami do jiných sítí je potřeba zajistit mechanismus podobný mechanismu Default Route. Tento mechanismus se nazývá **odchozí brána;** neboli **Default Gateway.**

Nyní bude popsán mechanismus, kterým je realizován přenos dat mezi uzly v různých sítích (tedy z jedné logické sítě do druhé). Předpokládá se, že stanice **A**, která je v síti 192.168.1.x potřebuje komunikovat s uzlem **B** umístěným v síti 192.168.2.x. Mezi sítěmi jsou dva směrovače **R1** a **R2**. Uzel A ví, že má poslat paket do jiné sítě. K tomu má nastavenu tzv. odchozí bránu - směrovač R1. Paket tedy vyplní následujícím způsobem:

L2 - zdrojová adresa – vlastní MAC (A), cílová adresa – MAC směrovače R1

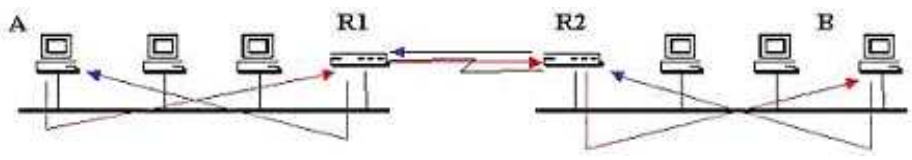
L3 - zdrojová adresa – vlastní IP adresa (A), cílová adresa – IP adresa uzlu B

Paket přijde na směrovač R1. Ten z IP adresy určí adresu sítě pro kterou je paket určen a na základě znalosti cest jej pošle na příslušný směrovač (v tomto případě R2). Směrovač R2 připraví a odešle paket s následujícími parametry:

L2 - zdrojová adresa – vlastní MAC (R2), cílová adresa – MAC uzlu B

L3 - zdrojová adresa – IP adresa A, cílová adresa – IP adresa uzlu B

Lze vidět, že při průchodu paketu se mění údaje 2. vrstvy, ale údaje 3. vrstvy jsou beze změny.



Obr. 17. Směrování

Pokud se má paket vrátit, musí mít i druhá strana správně vyplněnu Default Gateway. Mechanismus je analogický.

1.11 UDP protokol

UDP je nespojový (connectionless) protokol, nepřináší vlastnosti spolehlivosti přenosu, řízení toku nebo funkcí opravy chyb. Jde o jednoduchý interface mezi protokoly vyšší vrstvy a IP protokolem. Hlavička protokolu UDP obsahu menší množství informací než hlavička TCP a tím má tento protokol menší režii.

1.12 Adresace v IP sítích,

1.12.1 Základní principy

Adresace v počítačových sítích, nezávisle na typu protokolu, musí zajistit unikátnost adresy uzlu v rámci celé sítě. Tento problém je řešen logickým rozdělením adres na část **adresy sítě** a **adresy uzlu** (jde o jakousi analogii telefonních čísel, kde je koncový uzel jednoznačně určen dvojicí číslo předvolby a číslo koncové stanice).

Nejdůležitějším protokolem se společně s rozvojem Internetu stal protokol IP. Nejde pouze o jeden protokol, ale o celou sadu protokolů. Jak již bylo uvedeno výše, tuto sadu lze popsat na základě sedmivrstvého modelu OSI. Z těchto mnoha protokolů lze zmínit ten, jež dal celé sadě jméno – Internetwork Protokol (IP). Jde o protokol 3. vrstvy OSI (síťové) a jeho úkolem je zajistit adresaci a bezspojovou přepravu datagramů v rámci síťového prostředí.

V IP prostředí je konkrétní vyjádření adresy ve formátu 4 jednobytových čísel oddělených tečkami. Vypadá tedy následovně – **x.x.x.x** (např. 192.168.1.3). Rozdělení na část adresy sítě a adresy uzlu není úplně triviální jako u některých jiných protokolů (např. IPX, DECNet, Vines IP, …). Východiskem jsou nejvyšší bity prvního oktetu. Podle nich se adresy dělí do několika tříd z nichž nejvýznamnější jsou A, B a C. V následující tabulce znamená *s* část sítě a *u* část uzlů, přičemž nuly v adrese sítí sice nejsou striktně zakázány, ale jejich použití se nedoporučuje – na síti se může vyskytnou zařízení, které je nepodporuje.

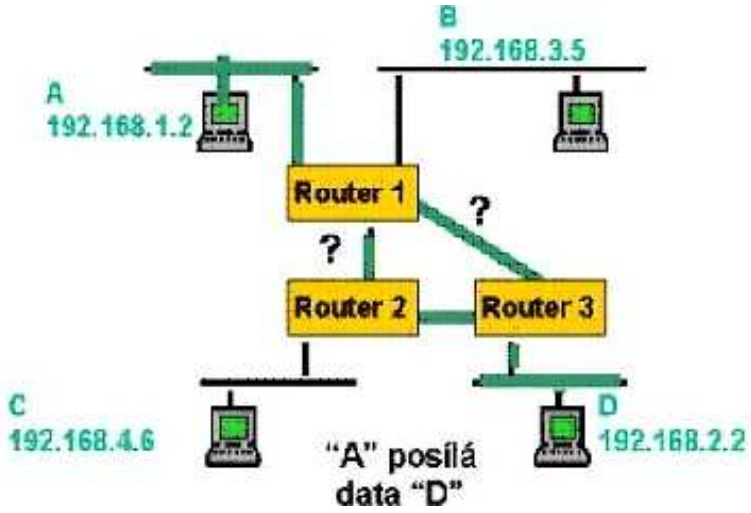
Tabulka VI. Třídy adres

Třída	Nejvyš.bit	Formát	Rozsah	Počet sítí	Počet uzlů
A	0	s.u.u.u	1..x.x.x až 126.x.x.x	126	16.777.214
B	10	s.s.u.u	128.0.x.x až 191.254.x.x	16.384	65.534
C	110	s.s.s.u	192.0.0.x až 223.254.254.x	2.097.150	254
D	111	s.s.s.u	224.0.0.x až 239.254.254.254	Pro multicast aplikace	

V adrese uzlu se nula stejně tak jako číslo 255 vyskytnout nesmí. Adresní prostor 127 je rezervován pro „loopback“.

Aby situace nebyla tak jednoduchá byl definován pojem maska IP sítě, který problematiku lehce komplikuje.

Příklad IP sítě je na obrázku. Jsou dány 4 lokální sítě spojené pomocí směrovačů. V každé LAN musí být unikátní adresní rozsah. V příkladu je část sítě zvýrazněna.



Obr. 18. Příklad IP sítě

Zařízení spojující jednotlivé sítě, nazývané směrovače (router) ví za kterým rozhraním je příslušná síť. Znalost je dána buď prostřednictvím staticky konfigurovaných informací nebo prostřednictvím dynamických informací předávaných některým ze směrovacích protokolů – např. RIP, OSPF, BGP, …. Unikátnost adresy pak zajišťuje správné doručení paketu od A k D. Pokud by došlo k chybné konfiguraci a např. síť s uzlem C měla nastavenu shodný rozsah se sítí s uzlem D, bude docházet ke zmatení směrovačů a síť nebude fungovat korektně.

To co platí v malé WAN síti se projevuje i v globální síti Internetu. Musí být zajištěna unikátnost adres. To ovšem vede k tomu, že všechny sítě k Internetu připojené by měly mít vlastní rozsah. Pomocí kalkulátoru lze velice rychle dojít ke konečnému počtu sítí a uzlů,

které mohou být připojené. Východiska z této situace jsou dvě. Tím prvním byla definice IP protokolu v 6, která přináší kromě mnoha vylepšení především v oblasti bezpečnosti a priorit i významné zvětšení počtu sítí a uzlů. Jde ale o významný zásah spojený s rozsáhlými investicemi. Zejména z tohoto důvodu získalo větší význam druhé východisko řešící problematika podstatně levněji – jde o privátní adresní rozsahy.

1.12.2 Masky sítě

Masky zajišťují mechanismus, jak jednu síť rozdělit do logických podsítí. Například třída A – je připravena pro 126 sítí, každá s 16.777.214 uzly. Bez maskování má k dispozici jednu ohromnou broadcastovou doménu. S použitím masek se může síť rozdělit do mnoha podsítí. Část sítě přidaná maskou se nazývá **subnet**.

Princip masek vychází z předpokladu, že tam, kde je v binárním vyjádření masky jednička, tam je síť. Tam kde je nula, je uzel. Následně jsou uvedeny nejprve přirozené masky jednotlivých rozsahů:

Tabulka VII. Třídy masek

Třída	Přirozená maska	Binární vyjádření masky
Třída A	255.0.0.0	11111111.00000000. 00000000. 00000000
Třída B	255.255.0.0	11111111. 11111111. 00000000. 00000000
Třída C	255.255.255.0	11111111. 11111111. 11111111. 00000000

Pomocí masek je možné oblast sítě roztáhnout na úkor oblasti uzlů. Viz. další příklad:

Tabulka VIII. Typ maskování

	Dekadické vyjádření	Binární vyjádření
Adresa	10.1.1.1	00001010.00000001.00000001.00000001
Maska	255.255.0.0	11111111.11111111.00000000.00000000

Jedná se o nejjednodušší typ maskování, tedy maskování vyšší třídy přirozenou maskou nižší třídy. V tomto případě „Áčko Béčkem“. Adresa sítě je v tomto případě 10.1, adresa uzlu je 1.1.

1.12.3 Privátní adresní rozsahy

Síť připojená k Internetu nemusí nutně být přímo adresovatelná z Internetu. Ve většině případů je to dokonce nežádoucí neboť přímá adresovatelnost znamená i možnost přímé

dosažitelnosti. Řešením je tedy to, že vnitřní síť (intranet) používá určitý rozsah, který je skrytý pomocí Proxy nebo NAT služby.

V březnu 1994 vytvořen dokument RFC 1597 (který byl nahrazen dokumenty RFC 1627 a posléze RFC 1918) upravující privátní adresní prostory. V každé třídě (A, B i C) je pro tyto účely vyhrazena část adres. Zmíněný dokument dělí sítě podle požadovaných komunikací do tří kategorií, které dále dělí na privátní (private) a veřejné (public). Základním rozdílem je možnost přímé komunikace ven ze sítě a naopak (tj. z venku do sítě).

Tabulka IX. Privátní rozsahy

Třída	Rozsah	Množství adresních prostorů
C	192.168.0.x až 192.168.254.x	254
B	172.16.x.x až 172.31.x.x	16
A	10.x.x.x	1

[1]

2 WI-FI BEZDRÁTOVÉ SÍTĚ

Wi-Fi (wireless fidelity-bezdrátová věrnost), je název organizace Wi-Fi Alliance označující určitý bezdrátový standard neboli protokol používaný k bezdrátové komunikaci. Wi-Fi Aliance je nezisková organizace, která certifikuje interoperabilitu bezdrátových zařízení odpovídajících standardu 802.11 a následně podporovat a vylepšovat i tento standard.

2.1 Bezdrátová spektra

Na rozdíl od řady jiných bezdrátových standardů běží 802.11 na „volné" části radiového spektra. To znamená, že (oproti komunikaci mobilních telefonů) pro vysílání a komunikaci pomocí 802.11 (neboli Wi-fi) není zapotřebí žádná licence. Volnými částmi rádiového spektra, které využívá 802.11, jsou pásma 2,4 GHz a také 5 GHz. Tato volná spektra využívá mnoho domácích zařízení, jako např. mikrovlnné trouby a bezdrátové domácí telefony [2].

Třebaže se běžně označuje za pásmo 2,4 GHz, skutečné spektrum sahá od 2,4000 GHz až do 2,4835 GHz. V případě 5GHz spektra se ve skutečnosti jedná o pásmo 5,150 – 5,250 GHz; 5,250 – 5,350 GHz a 5,470 – 5,725GHz [3].

Skutečnost, že tyto frekvence byly vyhrazeny pro nelicencované použití, má jeden velmi významný dopad: Jejich použití je laciné. Tato „volná" spektra tak získávají neférovou konkurenční výhodu oproti jiným spektrům, za něž se musí platit.

2.2 Standard 802.11 a jeho varianty

Obecně lze říci, že standard 802.11 má za cíl specifikovat způsob, jakým počítače využívají právě popsaná volná spektra 2,4 GHz a 5 GHz. (Když jsou počítače spojené, pak tvoří *místní síť* – Local Area Network neboli LAN. Jestliže jsou spojené bezdrátově, označuje se příslušná síť za bezdrátovou LAN – Wireless LAN neboli WLAN.)

2.2.1 Standard 802.11 b

Většina zařízení Wi-fi, která se v současné době používají, podporuje právě 802.11b. Technologie se ale rychle vylepšuje a tak nastupuje 802.11g. Standard 802.11b využívá spektrum 2,4 GHz a má teoretickou propustnost 11 megabitů za sekundu (11Mb/s). Dále využívá technologii Direct Sequence Spread Spectrum (DSSS), která minimalizuje

interference s dalšími zařízeními vysílajícími ve spektru 2,4 GHz. Rychlost 11 Mb/s je srovnatelná s rychlostí 10 Mb/s standardní kabelové ethernetové sítě 10BASE-T. Z různých důvodů však připojení Wi-Fi jen velmi výjimečně dosahuje svého teoretického maxima (např. šifrování nebo slabý signál zpomalují 802.11b).

2.2.2 Standardy 802.11a a 802.11g

Standardy 802.11a a 802.11g jsou odlišnými variantami 802.11, které lze považovat za chytřejší a mladší bratry 802.11b. Standard 802.11a využívá k přenosu 5GHz pásmo, čímž se minimalizuje možnost interference s řadou existujících zařízení pracujících na frekvenci 2,4 GHz (mikrovlnné trouby, otvírače garážových dveří atd.) a slibuje teoretickou propustnost až na úrovni 24 Mb/s.

Ještě novější než 802.11a je standard 802.11g fungující na spektru o frekvenci 2,4 GHz a chlubící se propustností až 54 Mb/s. Jinými slovy tyto standardy nabízejí rychlosti výrazně vyšší, než 802.11b.

Standard 802.11a zavádí určitou nekompatibilitu s 802.11b. Někteří výrobci však nabízejí vybavení 802.11a, které jsou zpětně kompatibilní se zařízeními 802.11b. (A vyrábějí také chipsety s kompletní podporou všech tří standardů.) Hlavní výhodou 802.11a je to, že trpí méně poruchami od ostatních zařízení. Přechod na 802.11a má své výhody i nevýhody, ale přechod na 802.11g není nic náročného – systémy 802.11g jsou zpětně kompatibilní s 802.11b a přitom rychlejší. Tato zpětná kompatibilita zařízení 802.11g je požadavkem pro certifikaci Wi-Fi.

2.2.3 Standard 802.11i

Organizace IEEE vyvíjí nový bezpečnostní standard pro 802.11 nazvaný 802.11i. Aliance Wi-Fi uvolnila podmnožinu standardu 802.11i, kterou označuje za „Wi-Fi Protected Access“ neboli WPA. Produkty, které úspěšně absolvují testování aliance Wi-Fi vyžadované k naplnění standardu 802.11i, získají certifikaci „Wi-Fi Protecte Access”. Ta zajišťuje silnější úroveň šifrování a ověřování, než je vestavěná v aktuálních standardech Wi-Fi. To znamená, že sítě Wi-Fi budou lépe chráněny před neoprávněným přístupem a dalšími bezpečnostními problémy. WPA má nahradit šifrování WEP vestavěné do aktuálních zařízení Wi-Fi.[2]

2.3 Zabezpečení přenosu dat ve standardu 802.11

Pakety fyzické vrstvy jsou především zabezpečeny:

-CRC kontrolním součtem,

-ACK paketem potvrzujícím správné přijetí předchozího paketu.

V celé normě 802.11 je použito CSMA/CA řízení přístupu k médiu. Minimalizaci kolizí zabezpečují 3 základní kontrolní pakety:

-RTS (request to send) - tento paket vysílá stanice ještě před samotným počátkem přenosu, mimo jiné obsahuje i předpokládanou dobu přenosu;

-CTC (clear to send) - tento paket vysílá stanice, která předtím obdržela paket RTS a je připravena pro příjem informace;

-ACK (acknowledge) - tento paket vysílá stanice po úspěšném přijetí informace se správným CRC součtem.

Registr NAV (Network Alocation Vector) - ostatní stanice v síti si do tohoto registru zapisují dobu, po kterou nemají vysílat (zjistí pomocí odposlechu RTS).

V sítích na bázi ethernetu vše funguje bez problémů, tj. všechny stanice se vždy navzájem slyší. V 802.11 se může objevit "problém skrytého uzlu", tj. pokud spolu komunikují stanice A (řídí komunikaci), B a C (klienti), přičemž B a C se navzájem "neslyší". Pokud totiž stanice B vyšle RTS paket, stanice C ho nezachytí a nemůže si správně nastavit registr NAV, takže dochází ve zvýšené míře ke kolizím. To je důvod, proč při „outdoor” použití 802.11 se ziskovými směrovými anténami nepřipojujeme na jedno AP více než cca 10 klientů současně, i když teoretické možnosti AP jsou vyšší.

2.4 Aktivní prvky

V síti se nachází tzv. access pointy (přístupové body) a jejich klienti. Přístupový bod si lze představit jako "elektrickou zásuvku" a klienty pak jako "elektrické spotřebiče". Pokud se bere na vědomí toto přirovnání, nemůže dojít při stavbě sítě k omylům, jakými jsou např. snaha spárovat dva klienty nebo propojit dva přístupové body. Z tohoto obecného pravidla existují výjimky v podobě režimu WDS u přístupových bodů a režimu "ad-hoc" u klientů. Tyto dva režimy jsou však pro budování rozsáhlejších sítí téměř nepoužitelné.

Přístupové body jsou z 99% samostatné jednotky s vlastním napájením, které v bezdrátové síti zastávají funkci ether. switche či HUBu. Často mají výstup na externí anténu a v naprosté většině případů jsou vybaveny konektorem RJ45 pro propojení se stávající 100/10 mbps ethernetovou sítí. Kromě konektoru RJ45 se občas lze setkat i s konektory USB či RS232, které však slouží pouze pro správu a konfiguraci přístupového bodu. U moderních access pointů se často nachází i paralelní porty LPT či USB 2.0 porty pro připojení a sdílení tiskáren, externích disků a webových kamer.

Klientské adaptéry se nejčastěji vyrábějí v provedení PCMCIA (CardBus), PCI nebo USB. Slouží pro připojení klientských PC k access pointu, ale lze je propojit i navzájem (režim ad-hoc). Režim ad-hoc se však nedoporučuje používat, protože takto propojená klientská zařízení neumožňují kontrolovat sílu přijímaného signálu a vytvořená spojení jsou dost nestabilní.

PCMCIA bezdrátové karty slouží pro připojení notebooků, dříve však byly z důvodů nedostatku PCI karet používány pomocí redukce i do stolních PC. Při výběru je důležité kontrolovat, zda má kupovaná PCMCIA karta výstup na externí anténu - bez něho totiž nebudeme moci plnohodnotně měřit sílu signálu v dané lokalitě. Nejčastěji se používá konektor typu "MC card" (Dlink, Orinoco, Compex, Dell), méně často pak reverzní MMCX (Zcomax).

PCI karty se objevily na trhu záhy po PCMCIA kartách. Naprostá většina z nich má výstup na externí anténu pomocí reverzního SMA konektoru a disponuje rozhraním PCI 2.1. Pouze nejnovější PCI karty standardu 802.11g jsou pouze pro sběrnici PCI 2.2 a nebudou tak fungovat ve starých počítačích. Čipy používané v PCI kartách jsou většinou naprosto totožné s těmi v PCMCIA kartách.

USB adaptéry jsou nejlevnější a nejmenší zařízení, která dokáží připojit počítač do bezdrátové sítě. Bohužel však v naprosté většině případů nejsou vybaveny žádným konektorem pro připojení externí antény a své použití tak najdou pouze v kancelářském a domácím prostředí.

2.4.1 Režim WDS a ad-hoc:

Režim WDS (Wireless Distribution System) je nadstavba nad původní normu 802.11, která umožňuje bezdrátové propojení dvou access pointů. Takto lze propojit až 6 zařízení,

přičemž všechna tato zařízení pracují na stejném kanálu a o přenosovou rychlost se dělí rovným dílem. Z toho vyplývá, že použití tohoto režimu je krajně nevhodné v rozsáhlých sítích, kde již tak jsou problémy s přenosovou rychlostí. Pokud jsou totiž zapojeny pouze dva přístupové body do režimu WDS, sníží se maximální rychlost komunikace na polovinu, tj. u 802.11b na cca 3 mbps. Pokud se na každý z těchto access pointů připojí pět klientů, budou přenášet data maximálně rychlostí 300 kbps, což již začíná být nepoužitelné i pro běžné připojení k internetu.

Režim ad-hoc slouží k propojení více klientských zařízení bez nutnosti přístupového bodu. V principu pak celá síť pracuje tak, že první spuštěný klient vytvoří jakýsi imaginární access point, který pak řídí další komunikaci všech ostatních klientů, kteří však komunikují navzájem přímo, tj. bez toho jednoho "hlavního" klienta. Nevýhody jsou zjevné - při vypnutí „hlavního“ počítače se na malý okamžik síť rozpadne, a to až do doby, než se funkce „hlavního“ PC ujme další klient (většinou zcela náhodně). Velkou nevýhodou této sítě je nemožnost jakkoliv měřit sílu přijímaného signálu a také slabé zabezpečení (WEP šifrování je dnes již překonané). Ad-hoc sítě jsou velice nestabilní, objevují se zde velké latence paketů a velké výkyvy dosahovaných rychlostí.

2.5 Antény

Anténa je zařízení schopné střídavou vysokofrekvenční energii (přivedenou k jejím vstupním svorkám kabelem z vysílače) vyzářit do prostoru, tedy vytvořit v prostoru vysokofrekvenční elektromagnetické pole o určité intenzitě (při vysílání). Antény pracují recipročně. To znamená, že jsou-li umístěny do prostředí vysokofrekvenčního elektromagnetického pole, může se z jejich svorek odebírat energie, jejíž velikost je intenzitě tohoto pole úměrná. To je využíváno v režimu příjmu. Obecně se anténa chová jako rezonanční obvod, naladěný na kmitočet (kmitočtové pásmo), na kterém se přenos vysokofrekvenčních signálů uskutečňuje.

2.5.1 Polarizace

Při bezdrátovém přenosu informací používáme dva typy polarizace elektromagnetického vlnění, lineární a kruhovou. Lineární polarizace se v praxi používá dvojí - horizontální a vertikální. Kruhová polarizace může být pravotočivá nebo levotočivá. Rovina polarizace vyzářeného vlnění je dána výhradně konstrukčním uspořádáním antény. Má-li být zajištěn

optimální provoz datového spoje, musí být obě stanice vybaveny stejným (z hlediska polarizace) druhem antény. Nouzově lze provozovat některé kombinace, při nichž nejsou ztráty zisku velké.

2.5.2 Typy antén

Všesměrové antény jsou nejčastěji tvořeny leptaným plošným spojem uvnitř plastové trubky (v případě levnějších typů) nebo důmyslnou soustavou navzájem sfázovaných zářičů (dražší typy). Zisk těchto antén se pohybuje do 10 dBd. Všesměrové antény mohou mít jak vertikální (častěji), tak horizontální polarizaci. Zkonstruovat všesměrovou anténu s horizontální polarizací je však dražší a složitější. Proto je tato polarizace méně rozšířená.

Sektorové antény se používají tam, kde je třeba vykrýt větší souvislý prostor, ale přitom je zbytečné nasadit nízkoziskovou všesměrovou anténu. Nejlevnější sektorové antény mívají vyzařovací úhel cca 30 stupňů, kvalitnější a dražší antény složené z více sfázovaných zářičů pokrývají až 180 stupňů. Opět lze sehnat sektorové antény jak s horizontální, tak i s vertikální polarizací.

Směrové antény se vyrábějí buď v provedení YAGI nebo jako parabolické reflektory. YAGI antény jsou dlouhé tyče s mnoha sfázovanými půlvlnnými dipóly, které navzájem rezonují a zesilují přijímaný či vysílaný signál. Výhodou YAGI antén jsou kompaktní rozměry a nižší cena. Naopak nevýhodou jsou horší mechanické a fyzikální vlastnosti - antény často v zimě namrzají.

Parabolické reflektory jsou tvořeny zářičem (dipól, malá YAGI anténa, plechovka) a parabolickým reflektorem (síto, plná parabola). Zářič ozařuje parabolickou plochu, která vlnění soustředí do úzkého paprsku. Tyto antény mohou mít zisk i 30 dBd a vyzařovací úhel menší než 10 stupňů.

Velký rozdíl je mezi parabolickou anténou s mřížovým reflektorem a plným (lisovaným) reflektorem. Tzv. „síto“ má mnohem větší postraní a zadní vyzařování a nedosahuje zdaleka kvalit plného hliníkového reflektoru.

Samostatnou skupinou jsou směrové antény s kruhovou polarizací. Jsou to "šroubovice" s vyzařovacím úhlem cca 30 stupňů, jejichž hlavní výhoda spočívá ve schopnosti přijímat jak horizontální, tak vertikální polarizaci. Používají se v lokalitách s mnoha odrazy, kde

může docházet k přepolarizování signálu (panelová sídliště, šikmé ulice atd.). Naopak jsou silně nevhodné pro point-to-point spoje - dokáží spolehlivě zarušit vše kolem sebe.

Obr. 19. Typy antén (všesměrová, sektorová, směrová)

2.6 Výkony, limity ČTU a GL č. 12/R/2000

Dosah jakéhokoliv rádiového spojení je založen na jediném principu - úroveň signálu, který vyjde z výstupu vysílače, může po cestě poklesnout jen natolik, aby byla na vstupu přijímače vyšší, než je jeho citlivost (tedy schopnost ho ještě zpracovat). Úroveň signálu naštěstí nemusí po cestě jen klesat, např. zisk antén je téměř vždy kladný a proto signál „zesilují“. U Wi-Fi je plánování bezdrátových spojů omezeno důležitým faktem - úroveň vysílaného signálu na výstupu z antény nesmí přesáhnout určitou maximální hodnotu. Ta je stanovena Českým telekomunikačním úřadem (ČTÚ) v tzv. Generální licenci č. GL-12/R/2000. Generální licence užívá poměrně složité pojmy, ale pro další výpočty stačí pouze vyjít z toho, že by neměla být překročena hodnota +20 dBm. Jednotka dBm je vztažena k výkonu 1 miliwatt, tj. pokud má zařízení výkon 1 mW, rovná se to výkonu 0 dBm; 17 dBm odpovídá výkonu 50 mW a 20 dBm pak výkonu 100 mW neboli maximální hodnotě povolené ČTU.

2.6.1 Jednotka decibel

Aby se úrovně, zisky a útlumy snadno počítaly, používají se decibely (dB). Je to bezrozměrná jednotka (podobně jako procento), která umožňuje používat místo pojmu „změna na X procent původní hodnoty“ (tedy násobení) pojem „změna o Y dB“ (tedy sčítání). Kladná hodnota v dB znamená poměr větší než jedna, záporná hodnota v dB znamená poměr menší než jedna. Při vyjadřování úbytku (útlumu) nebo přírůstku (zisku) znamená 0 dB žádný útlum a žádný zisk, tedy poměr 1:1, tj. v obou případech je na výstupu stejná úroveň jako na vstupu. Vyjadřujeme-li v dB i absolutní úroveň (sílu) signálu, pak jsou to vždy dB vztažené k nějaké (dohodnuté, standardní) hodnotě. Tedy 0 dB signálu neznamená žádný signál, ale naopak přesně tu samou úroveň, na které jsme se

předem domluvili a ke které vše vztahujeme. Úroveň signálu vyjádřená v dB může být i záporná - je-li signál menší, než ta vztažná hodnota. Je třeba mít vždy na paměti, že dB vždy vyjadřuje pouze poměr.

2.6.2 Zisk antény vyjadřovaný v dB

Zisk antény (v dB) je vyjádřením poměru. Do antén není přiváděna žádná dodatečná energie (pouze VF signál z karty či access pointu) a tak se tam signál nemůže nijak zesílit (myšleno v absolutních jednotkách). Anténa, která má kladný zisk, je vždy anténa nějakým způsobem směrová, tj. soustředí svoji vysílací/přijímací schopnost jen do určitého směru, zatímco jiný směr se stává „hluchým“. Zisk antény je pak vyjádřením poměru, kolikrát je ten určitý preferovaný směr antény zvýhodněn oproti situaci, kdyby se anténa chovala ve všech směrech stejně (tj. její tzv. vyzařovací diagram by byl ideální koule). I všesměrová anténa má zisk, je totiž všesměrová jen v jedné rovině a její vyzařovací diagram je placka. Při porovnávání antén se dále můžete setkat s jednotkami dBi a dBd - dBi je vztaženo k výkonu izotropního zářiče a dBd k výkonu půlvlnného dipólu. Pokud je tedy anténa se ziskem 9 dBd, znamená to, že je cca 3 x výkonnější, než půlvlnný dipól (každé 3 dB jsou dvojnásobek/polovina). Pro stejnou anténu je velikost zisku v dBi o 2,16 dB větší než údaj v dBd. Snad také proto většina výrobců uvádí velikost zisku svých antén v dBi.

2.6.3 Útlumy koaxiálních kabelů

Koaxiální kabel má vždy pouze útlum, tj. k výpočtům nám přispívá zápornými dB. Útlum kabelu je přímo úměrný jeho délce, takže se klidně může pro každý typ kabelu vyjádřit v dB/m, tuto tabulkovou hodnotu pak v každém jednotlivém konkrétním případě vynásobit délkou kabelu a výslednou hodnotu použít do celkového výpočtu.

2.6.4 Útlum prostředí a Fresnelova zóna

Útlum trasy (tj. kolik se ztratí signálu při přenosu vzduchem na určitou vzdálenost) lze také teoreticky vypočítat. V praxi bude útlum souhlasit s teorií (nebo se k ní aspoň blížit) v případě, že mezi oběma konci trasy (anténami) je přímá optická viditelnost (vůbec žádné překážky), a to nejen v přímce, musí být volná (bez překážek) i v tzv. Fresnelově zóně.

Jednou z nutných podmínek v pásmu 2,4GHz je přímá viditelnost mezi přijímací a vysílací anténou. Není to však podmínka postačující. Pro kvalitní přenos musí být volná (bez

překážek) ještě tzv. Fresnelova zóna, tedy určitý prostor kolem spojnice těchto dvou bodů (podobný doutníku, odborněji také elipsoid). V prostoru této zóny by se neměla vyskytovat žádná překážka, ani by do ní neměla třeba částečně zasahovat (např. střecha nějakého domu). Průměr Fresnelovy zóny v jejím nejširším místě (což je v polovině celkové délky trasy) lze vypočítat, ale často postačí stručná přehledová tabulka. Je sestavena pro různé celkové délky trasy:

Tabulka X. Rozměry Fresnelovy zóny

100 m	200 m	400 m	500 m	700 m	1000 m	1500 m	2000 m	3000 m
1,8 m	2,5 m	3,6 m	4,0 m	4,7 m	5,6 m	6,9 m	8,0 m	9,8 m

Protože je to elipsoid, je počáteční nárůst průměru poměrně strmý. Např. trasa 1 km dlouhá (maximální průměr zóny 5,6m) má již po prvních 100 metrech průměr zóny 3,4m. Pokud je tedy anténa nainstalována na střechu domu na 1,5m vysoký stožár a ve vzdálenosti 100m je stejně vysoký dům, zasahuje už jeho střecha do Fresnelovy zóny. Narušená Fresnelova zóna většinou nemá za následek příliš podstatné snížení úrovně signálu. Spíše se projeví jako nárůst rušivých odrazů, což snižuje kvalitu přenášeného datového toku (ztrátovost paketů, vyšší latence). Pokud není volných alespoň 60% průměru zóny, dochází již k výrazné degradaci kvality spoje [4].

II. PRAKTICKÁ ČÁST

3 ÚVOD K PROJEKTU

3.1 Smysl celého projektu

V dnešní době je vysokorychlostní internet v domácnosti pro většinu obyvatel již samozřejmostí. Například poskytovatelé ADSL slibují téměř stoprocentní dostupnost. Bohužel existují stále oblasti, kde ADSL není k dispozici a nebo místa, kde sice dostupné je, ale kvůli zastaralé technologii a ústřednám nenabízí takové možnosti, jako je tomu jinde.

Podobná situace je v okolí obce Trnava. Oblast, která čítá téměř 1500 obyvatel, neměla ještě nedávno žádnou možnost vysokorychlostního připojení k internetu. Jedinou šancí bylo připojení pomocí telefonní linky (vytáčené připojení), nebo některého z mobilních operátorů. Tyto varianty byly však velmi drahé a rychlost příliš pomalá. Proto sílil tlak obyvatel na vedení obce, aby byl vypracován projekt na vysokorychlostní internet. Záhy byly osloveny firmy Telefonica O2 a Avonet. Jednání bohužel skončila neúspěšně, protože od zástupců firmy Telefonica O2 bylo oznámeno, že připojení pomocí linky ADSL bude dostupné nejdříve do dvou let. Naopak firmou Avonet byli vysláni technici k důkladnému prozkoumání terénu a všech zásadních podmínek pro bezdrátové připojení. Závěrem bylo usneseno, že tato oblast je geomorfologicky značně složitá, a proto jakýkoliv projekt bezdrátového internetu by byl velmi obtížně realizovatelný a náklady na provedení příliš vysoké. Následně byl projekt firmou Avonet zamítnut. Poslední šancí bylo tedy najít podporu v soukromém sektoru.

3.2 Počátky realizace

Z pořízených detailních fotografií bylo zjištěno, že existuje přímá viditelnost do obce Veselá, což je zhruba vzdálenost 8 km vzdušnou čarou. Následně došlo k dohodě se soukromým podnikatelem Zdeňkem Hrbáčkem a na základě ní bylo možno získat konektivitu. Nejdříve ale musel být vypracován seznam uchazečů. Kvůli vysokým nákladům na realizaci bylo potřeba zajistit co nejvíce zájemců, aby nebyl celkový projekt ztrátový. Obrovský zájem obyvatel předčil všechna očekávání a proto mohla být zahájena realizace.

4 KONEKTIVITA A PÁTEŘNÍ SÍŤ

4.1 Poskytovatel Internetu

Jak již bylo zmíněno, konektivita je poskytována soukromým podnikatelem Zdeňkem Hrbáčkem. Hlavní spoj Veselá - Trnava navazuje na již vybudovanou soukromou trasu ze Želechovic u Zlína, kde hlavním poskytovatelem Internetu je společnost Avonet. Bohužel zatím nejsou k dispozici žádné veřejné IP adresy, což je značná nevýhoda pro správu sítě z Internetu. V současné době se ale pracuje na nové konektivitě přímo od společnosti Avonet, která má nový spoj přímo v obci Veselá.

4.2 Hlavní spoj

4.2.1 Použitý hardware

Důležitým faktorem byl výběr antén. Poměrem cena/kvalita byly nakonec zvoleny antény **PAR24 – PRO 2x PACK**.

Obr. 20. Anténa PAR24 – PRO

Je to anténa určená pro pásmo 5 GHz. Parabola má průměr 380 mm a činitelem směrování (zisk) do 24 dBi. Anténa nemá žádný kelímkový ozařovač. Součástí je i plně nastavitelný držák proveden tak, že na něj lze připevnit montážní krabici a veškerou elektroniku umístit dovnitř krabice. Při tomto postupu vznikne kompaktní zařízení. Při dodržení platných legislativních postupů je tedy možné celé zařízení vyhlásit za radiový spoj s vestavěnou

anténou. Narozdíl od dřívějších antén, zcela odpadá problém při nastavování směru díky kvalitnímu provedení držáku. Anténu je také velmi snadné sestavit.

Tabulka XI. Specifikace antény PAR24 - PRO

Zisk:	až 23,5 dBi
Frekvenční pásmo:	5,0 - 5,95 GHz
Polarizace:	horizontální nebo vertikální dle polohy zářiče
PSV:	lepší než 1,5 (pro 5.3 až 5.9 GHz)
Vyzař. úhel :	8,8° (-3dB)
Typ konektoru:	N - Female - zlacený kontakt
Rozměr:	380 mm
Parabola:	hliníková slitina s vypalovanou barvou
Radom (kryt):	UV stabilizované ABS, zdarma ke každé anténě
Průměr držáku:	32 až 74 mm
Hmotnost:	3,5 kg

Jak vysílací anténa v obci Veselá, tak přijímací anténa v Trnavě jsou připojeny k RouterBoardu Mikrotik RB532.

RB532 je hardware sloužící jako směrovač, který disponuje procesorem s instrukční sadou MIPS o frekvenci 266 Mhz, dále pamětí 32 MB DDR RAM, 128 MB pamětí NAND, třemi porty LAN, dvěma MiniPCI sloty a operačním systémem Router OS L4. Více o jeho popisu a nastavení bude uvedeno v kapitole o páteřní síti.

Obr. 21. RB532

Nesmí být také opomenut **RB502** daughterboard 2 x miniPCI, což je rozšiřující deska pro RouterBoard 532, která umožňuje připojení dalších 2 miniPCI karet.

Obr. 22. RB532 rozšířený o RB502

Anténa s RB532 musí být spojena koaxiálním kabelem (pigtailem).

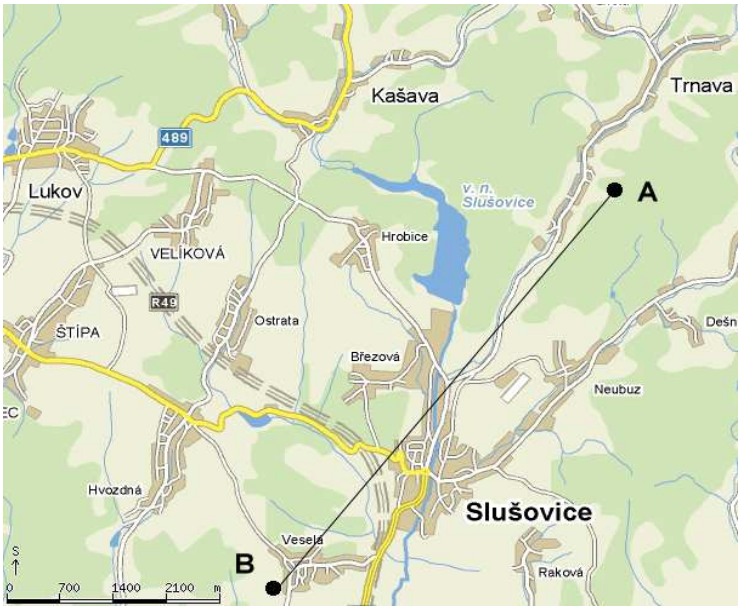
Obr. 23. Koaxiální kabel (pigtail)

Tento koaxiální anténní kabel mívá nejčastěji konektory RSMA-M a N-Male. Maximální délka by měla být okolo 5m. Útlum je 0,54dB/m v pásmu 2,4GHz a 0,67dB/m v pásmu 5GHz.

Další neuvedený hardware je popsán v kapitole o páteřní síti.

4.2.2 Provedení

Přesné nastavení parabol je velmi důležité pro získání dobrého signálu. Toho lze docílit tak, že z místa A je vysílán signál a v místě B je nastavována druhá anténa v režimu přijímací antény. Seřizuje se přesná poloha tak, aby byl signál co nejsilnější. Totéž musí být provedeno i naopak – tedy nechá se vysílat signál z místa B a bude seřízena parabola v místě A. Hlavní spoj používá přenosovou frekvenci 5GHz (5520MHz) a horizontální polarizaci. Toto pásmo bylo zvoleno i pro většinu páteřní sítě aby byla minimalizována možnost rušení s řadou jiných zařízení.



Obr. 24. Hlavní spoj

V obci Trnava byla přijímací anténa umístěna na bývalý obecní televizní vysílač zhruba do výšky 10 metrů. Aby nedocházelo ke ztrátě signálu, byly použity co nejkratší koaxiální kabely (pigtaily) spojující RouterBoard s anténami. Proto musí být RB532 až ve výšce antény a jeho napájení je tedy řešeno síťovým kabelem pomocí POE (Power Over Ethernet). Což je pasivní adaptér, který slučuje napájecí vedení do nevyužitých párů na UTP kabelu, takže po jednom kabelu mohou jít jak data tak napájení. Lze jej použít se zařízeními RouterBOARD nebo WRAP.

Obr. 25. POE

Fotografie, jak vše vypadá v praxi, jsou uvedeny v přílohách.

4.3 Páteřní síť

Celá páteřní síť je tvořena celkem sedmi převaděči. Tento vysoký počet je poněkud neobvyklý, ale vzhledem k obrovské délce pokryté oblasti a složitému reliéfu nemůže existovat jiné řešení. Do budoucna navíc přibudou další tři až čtyři vysílače. Větší část páteře je vedená na pásmu 5GHz a zbytek na frekvenci 2,4GHz. Technologie založené na

5GHz jsou poněkud dražší a protože je téměř vyloučeno, že zde bude konkurovat další poskytovatel wi-fi, mohla být pro část páteřní sítě použita zařízení s frekvencí 2,4 GHz.

4.3.1 Hardware

Panelová anténa PAN10 - 10 dBi (2,4 GHz)

Jedná se o lehkou a jednoduchou anténu pro pásmo 2,4 GHz. Její hmotnost je pouze 170g a proto je vhodná i pro umístění na okení tabulku. S touto anténou lze běžně dosáhnout spoje na vzdálenost 0,5 - 1,5 km.

Tabulka XII. Specifikace PAN10

Zisk:	10 dBi
Frekvenční pásmo:	2400 - 2500 MHz
Polarizace:	H/V
PSV:	<1,5
Maximální výkon:	10 W
Vyzař. úhel - H.:	60°
Vyzař. úhel - V.:	60°
Typ konektoru:	N female
Impedance:	50 Ohm
Rozměry:	130 x 130 x 25 mm
Hmotnost:	0,17 kg

Panelová anténa TA PAN-14 PRO (2,4 GHz)

PAN14 PRO je oblíbená sektorové anténa s vyzařovacím úhlem 28 nebo 39 stupňů v závislosti na polarizaci. Anténa je dodávána automaticky včetně stožárové příchytky. Je vhodná pro spoje do vzdálenosti cca 1 km.

Tabulka XIII. Specifikace PAN14

Zisk:	13,5 (+-0,5) dBi
Frekvenční pásmo:	2400 - 2500 MHz
Polarizace:	H/V
PSV:	<2
Maximální výkon:	10 W
Vyzař. úhel - H.:	39°
Vyzař. úhel - V.:	38°
Typ konektoru:	N female
Impedance:	50 Ohm
Rozměry:	160 x 160 x 30 mm
Hmotnost:	0,4 kg
Provozní teploty:	-40°C až +60°C

Všesměrová anténa OMNI8 8 dBi (2,4 GHz)

Jedná se o levnou a jednoduchou všesměrovou anténu s vertikální polarizací se ziskem 8 dBi. I přes svou nízkou cenu anténa zaujme precizním zpracováním. Lze ji připevnit dvěma šrouby nebo stahovacími pásy, které nejsou součástí dodávky.

Tabulka XIV. Specifikace OMNI8

Zisk:	8 dBi
Frekvenční pásmo:	2400 - 2500 MHz
Polarizace:	vertikální
PSV:	<1,5
Maximální výkon:	5 W
Vyzař. úhel - H.:	360°
Vyzař. úhel - V.:	8°
Typ konektoru:	N female
Impedance:	50 Ohm
Rozměry:	500 x 20 mm
Hmotnost:	0,2 kg
Teplotní rozsah:	-30 až +50°C
Odolnost proti větru:	do 120 km/h

Panelová anténa **TA 19 dBi PRO** (5 GHz)

Precizně zpracovaná panelová anténa od firmy Elboxrf s upevňovací polohovatelnou sadou a polarizací H/V dle natočení.

Tabulka XV. Specifikace PAN19

Zisk:	19 dBi
Frekvenční pásmo:	5.1 GHz - 5.9 GHz
Polarizace:	H / V
PSV:	<1,5
Maximální výkon:	10 W
Vyzař. úhel - H.:	20°
Vyzař. úhel - V.:	20°
Typ konektoru:	N female
Impedance:	50 Ohm
Rozměry:	160 x 160 x 30 mm
Hmotnost:	0,45 kg

Mikrotik RouterBoard RB532 popsaný v předchozí kapitole.

Mikrotik RouterBoard RB112 je levnější a méně výkonná varianta výše zmiňovaného modelu RB532. Disponuje procesorem s instrukční sadou MIPS o frekvenci 175 Mhz, dále

pamětí 16 MB SD RAM, 64 MB pamětí NAND, pouze jedním Ethernet 10/100Mbit portem, dvěma MiniPCI sloty a operačním systémem Router OS L4.

Obr. 26. RB112

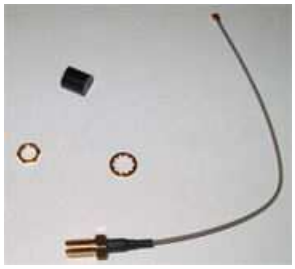
Další důležitou součástí jsou bezdrátové karty **WNC CM9 MiniPCI 802.11a/b/ g.** Jde o skvělou 2,4 GHz a 5 GHz wireless Mini-PCI kartu postavenou na AR5213 Multiprotocol MAC/baseband processoru a Atheros eXtended Range (XR) technology, která nabízí skvělé parametry. Nabízí mimo jiné i výstup na externí anténu a v kombinaci s redukcí MiniPCI do PCI slotu + Pigtail RP SMA se stává řešením pro nasazení i v běžných PC či serverech, které Mini-PCI slot nemají. Je to také ideální řešení pro bezproblémový roaming mezi jakoukoliv 802.11 sítí. Pro zabezpečení sítě je možné použít WEP, WPA, AES a TKIP.

Tabulka XVI. Parametry CM9

Operační mód	AP, Client, Ad-HOC
Frekvence:	2.4, 5 GHz
Přenosová rychlost:	11, 54 Mbps
Výstup na ext. anténu:	2 x U-FL male
Max. výstupní výkon:	18 dBm
Citlivost:	max. a:- 88 dBm, b: -95dBm, g: -90 dBm
Shoda:	FCC, CE
Spotřeba:	40 až 430 mW
Provozní teplota:	0 - 70 °C

Obr. 27. CM9

Další důležitou součástí je Pigtail U-FL/RSMA female pro CM9. Ten umožňuje k miniPCI kartě CM9 připojit externí anténu. Pigtail končí klasickým rev. SMA male konektorem stejně jako většina aktivních Wi-Fi prvků.



Obr. 28. Pigtail pro CM9

4.3.2 Typy převaděčů

V páteřní síti se nachází dva typy převaděčů. První je založen na RB532 rozšířeném o RB502 a se třemi kartami CM9. Tento Převaděč přijímá signál o frekvenci 5GHz a zároveň jej vysílá dále. Mimo to třetí wi-fi karta slouží k vykrytí oblasti - tedy připojení klientských stanic, ale to již na frekvenci 2,4 GHz.

Druhý typ je poněkud levnější variantou prvního, ale splňuje ty samé účely. Je založen na RB112 se dvěma kartami CM9. První anténa slouží jako přijímací (na frekvenci 2,4 GHz) a druhá jako vysílací a zároveň vykrývací.

Převaděč založený na RB532

Kompletace je poměrně jednoduchá. Bylo nutné zakoupit RB532 (3800 Kč), RB502 (650 Kč), kryt pro RB532+daughterboard (750 Kč), 3x kartu CM9 (2550 Kč), 3x pigtail pro CM9 (300 Kč), 3x pigtail pro antény (600 Kč), 2x panelová anténa TA 19 dBi PRO (2200 Kč). Jako vykrývací anténa byla vždy použita buď panelová anténa PAN10 - 10 dBi (500 Kč), nebo všesměrová anténa OMNI8 8 dBi (800 Kč).

Celková cena je tedy zhruba 11 000 Kč. Nastavení a zprovoznění převaděče je popsáno v kapitole o konfiguraci RouterBoardu Mikrotik.

Převaděč založený na RB112

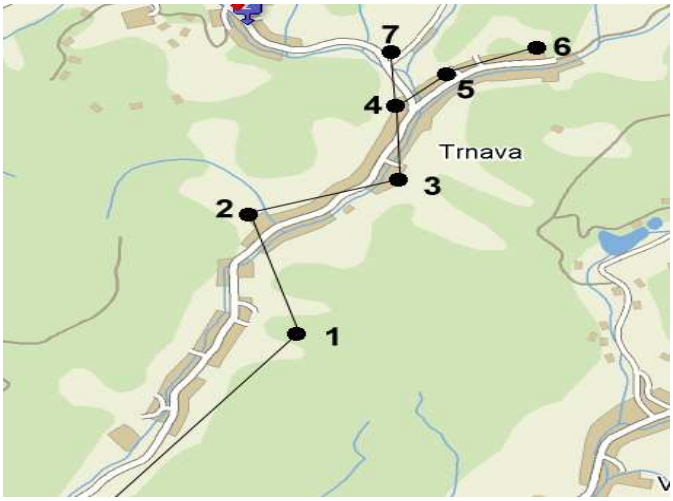
Jak již bylo zmíněno, jedná se o jednodušší a levnější variantu výše uvedeného typu. Pro jeho účely bylo nutné zakoupit RB112 (2000 Kč), kryt pro RB112 (400 Kč), 2x kartu CM9 (1700 Kč), 2x pigtail pro CM9 (200 Kč), 2x pigtail pro antény (400 Kč), 2x pigtail pro CM9 (200 Kč), 1x panelová anténa TA PAN-14 PRO (800 Kč). Jako vykrývací anténa byla vždy použita všesměrová anténa OMNI8 8 dBi (800 Kč).

Celková náklady tedy činí zhruba 6 300 Kč. Jak lze vidět, je to značný rozdíl v ceně a proto tato levnější variante byla využita pro vykrytí oblastí, kde se již nepočítá do budoucna s dalšími převaděči, tedy prodlužováním páteřní sítě.

4.3.3 Struktura páteřní sítě

Celá páteřní síť je tvořena celkem sedmi převaděči, z čehož jsou u čtyř použity RouterBoardy 532 a u tří RouterBoardy 112. Páteř tvoří velmi dlouhou linii kromě jednoho rozvětvení. Jiné řešení bohužel nebylo technicky možné.

Hlavní signál je přiveden hned na začátek páteřní sítě - je to tedy značná nevýhoda oproti tomu, kdyby byl signál Internetu směřován například doprostřed celé páteře. Dojde-li tedy ať už výpadkem proudu či jinou závadou k poruše hned na druhém převaděči, zůstává celý zbytek sítě bez spojení. Proto budou do budoucna všechny spoje vybaveny záložními zdroji UPS. Pro lepší představivost je uvedeno celkové schéma páteřní sítě.



Obr. 29. Páteřní síť

Dále jsou popsány jednotlivé spoje:

1 – převaděč s RouterBoardem 532 propojeným s přijímací anténou PAR24 – PRO, vysílací anténou TA 19 dBi PRO (5 GHz) a vykrývací panelovou anténou PAN10 - 10 dBi (2,4 GHz). Pro připojení klientských stanic byla použita pouze 10 dBi anténa z jediného prostého důvodu a tím je větší vyzařovací úhel, který v tomto místě bylo potřeba pro vykrytí širší oblasti. Všechny tři antény jsou nastaveny na horizontální polarizaci. Provedení v praxi lze vidět na následujícím obrázku (zleva PAR24 – PRO, PAN10 - 10 dBi (2,4 GHz), TA 19 dBi PRO (5 GHz). IP adresa převaděče je 10.3.30.1.

Obr. 30. První převaděč

2 – převaděč na stejném principu s RB532 používající pro přijímání a vysílání signálu o frekvenci 5 GHz dvě antény typu TA 19 dBi PRO (5 GHz). K pokrytí oblasti slouží panelová anténa PAN10 - 10 dBi (2,4 GHz) opět kvůli většímu vyzařovacímu úhlu. Přijímací anténa má logicky horizontální polarizaci stejně jako vykrývací, ale vysílací anténa je nastavena již vertikálně. IP adresa převaděče je 10.3.31.1.

3 – znovu převaděč na podobném principu s RB532. Jediným rozdílem je vykrývací všesměrová anténa OMNI8 8 dBi (2,4 GHz). Vysílací anténa páteřní sítě je nastavena pro změnu na horizontální polarizaci. Je to zároveň poslední spoj vedený na frekvenci 5GHz k převaděči číslo 5. IP adresa převaděče je 10.3.32.1.

4 – poslední prevaděč využívající RouterBoard 532. Od předchozích se ale liší tím, že má nainstalovány pouze dvě karty CM9 a tudíž používá jen dvě antény. Těmi jsou přijímací anténa 5Hz signálu TA 19 dBi PRO a vykrývací všesměrová anténa OMNI8 8 dBi (2,4 GHz). Samozřejmě by k tomuto účelu postačil i RB112, ale počítá se s tím, že trasa

vysílaná na kmitočtu 5GHz bude někdy prodloužena. Proto byl použit právě RB532, aby v budoucnu nemuselo dojít k celé výměně zařízení. IP adresa převaděče je 10.3.34.1.

5,6,7 – všechny tři téměř totožné převaděče s RouterBoardem RB112. Přijímají signál o kmitočtu 2,4 GHz pomocí panelové antény TA PAN-14 PRO (2,4 GHz). Jako vysílací a zároveň vykrývací slouží všesměrová anténa OMNI8 8 dBi (2,4 GHz). Pouze u převaděče č.6 je pro vykrytí oblasti použita PAN10 - 10 dBi (2,4 GHz). IP adresy převaděčů jsou 10.3.35.1, 10.3.36.1 a 10.3.37.1.

4.3.4 Zarušení a průchodnost

Zarušení v oblasti je velmi malé, protože se zde nevyskytuje žádný jiný poskytovatel. Snahou bylo střídat polarizaci u antén a nastavovat odlišné kanály. Jakékoliv nepříznivé vlivy na ostatní obyvatele a zařízení touto sítí nebyly zatím zjištěny.

Průchodnost sítě je zatím dostačující a má i dostatečné rezervy. Pro současné rychlosti uživatelů stačí přivádět 4 garantované Megabity. Páteřní síť při použití současných zařízení je schopna přenést zhruba dvounásobek při zachování stejné stability. To je zatím postačující okolnost i pro chystané zvýšení rychlosti Internetu všem uživatelům na dvojnásobek při zachování cen.

4.3.5 Pokrytí oblasti signálem

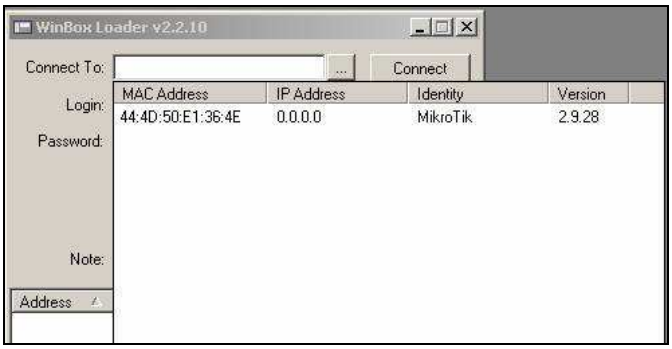
I přes značně složitý terén a vegetaci je pokrytí celé oblasti značně vysoké. Navíc je do budoucna v plánu situaci ještě vylepšit, aby mohli být připojeni i klienti, kteří se nachází v oblasti bez pokrytí. Údaje o vyzařovacích úhlech antén, které výrobci uvádějí, jsou značně zavádějící. Signál lze v mnoha případech bez problémů zachytit i mimo tyto zóny.

4.3.6 Konfigurace zařízení Mikrotik

RouterBoard Mikrotik je v oboru bezdrátových produktů velmi respektován a to zejména pro rozsáhlou funkcionalitu a to za velmi dobrou cenu. Veškeré nastavení se provádí pomocí jiného počítače, nebo nejlépe notebooku, který se připojí pomocí síťového kabelu do Ethernet portu. Ke konfiguraci směrovače lze využít program winbox.exe Program je možné stáhnout volně na URL *http://www.wirelessdrivers.net/download.php?view.221*. Po stažení se již může spustit samotný program *winbox.exe* a bude zobrazeno následující menu:

Obr. 31. Přihlašovací menu

Následně je nutné stisknout tlačítko  vlevo od tlačítka *Connect*. Dále se vybere řádek s nabízenou MAC adresou a tím se tato MAC adresa přenese do řádku *Connect To***:**



Obr. 32. Načtení MAC adresy

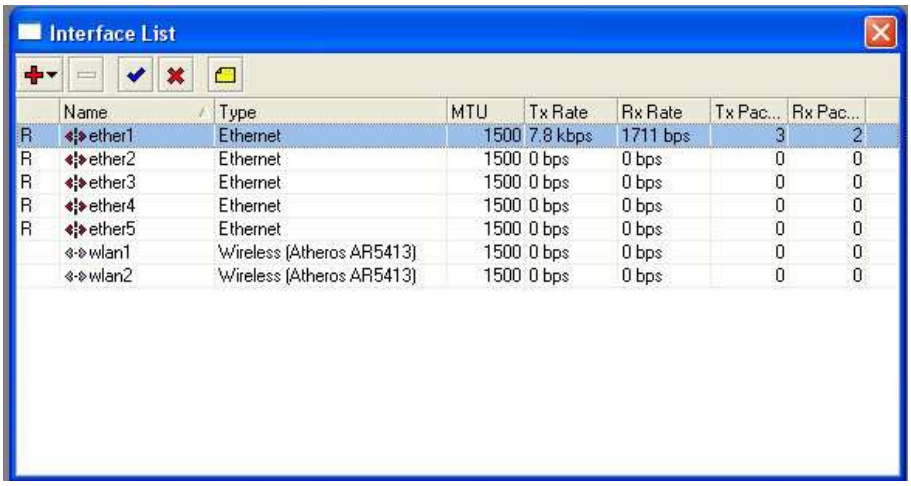
Následně se do okénka ***Login:*** napíše login *admin*

Obr. 33. Login

a po stisknutí tlačítka *Connect* dojde ke spojení s routerem a zobrazí se následující menu:

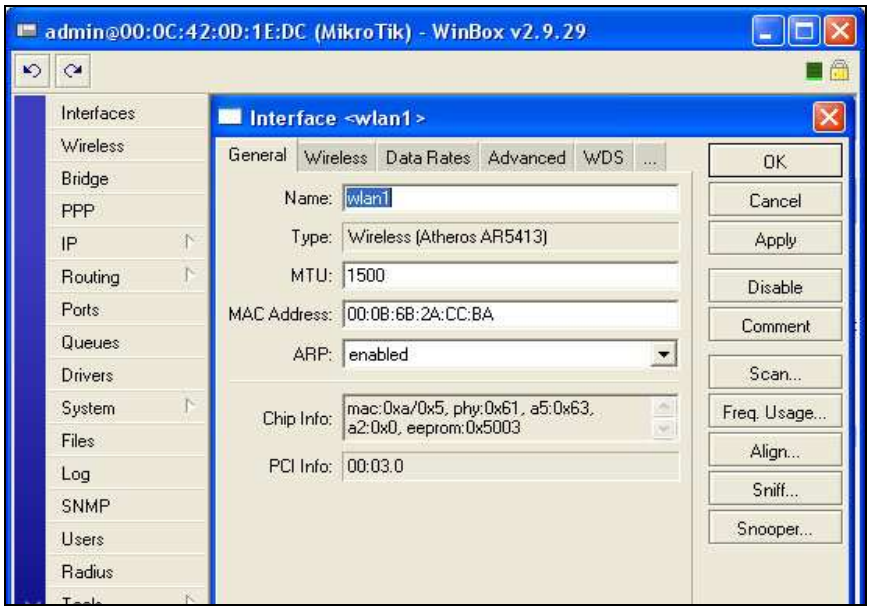
Obr. 34. Menu routeru Mikrotik

Jestliže jsou všechny karty správně připojeny, zobrazí se v menu *interfaces.* Na následujícím obrázku je routerboard s pěti porty ethernet a dvěmi připojenými kartami CM9.



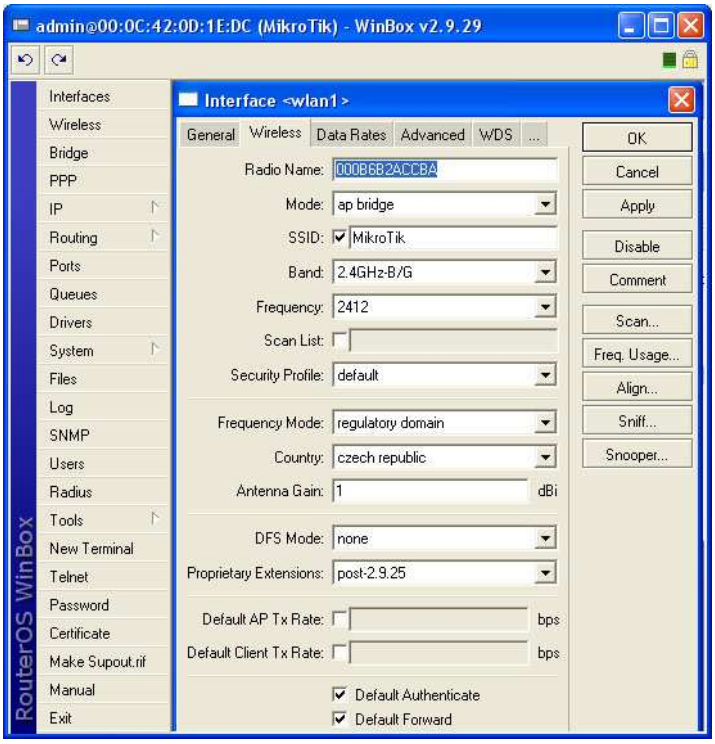
Obr. 35. Menu Interfaces

V menu *Interfaces* je doporučeno pojmenovat pro lepší přehled jednotlivé karty. To lze učinit dvojím kliknutím na příslušnou kartu a poté se objeví následující menu se záložkami.



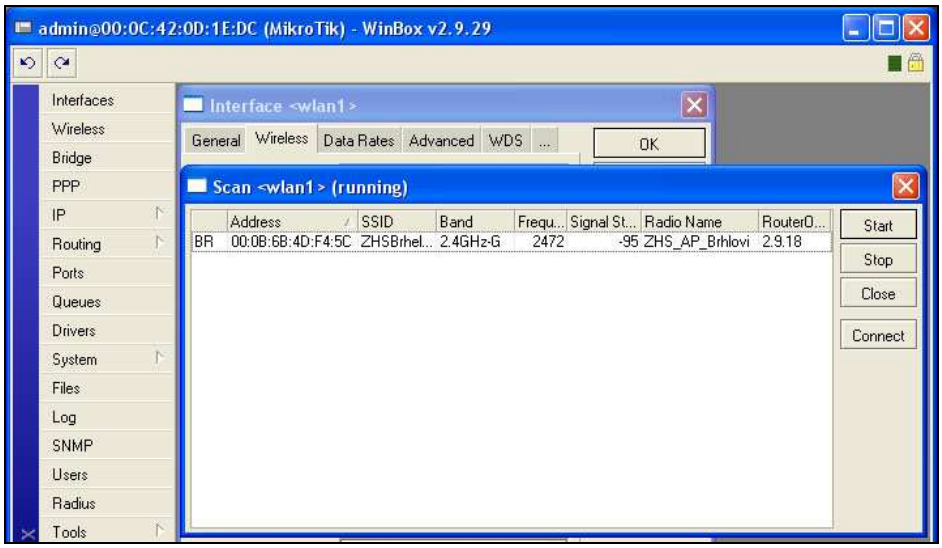
Obr. 36. Záložka General

V záložce *General* lze tedy přiřadit název kartě a v následující záložce *Wireless* se nastaví mód, ve kterém karta bude pracovat, dále pásmo, frekvence a země.



Obr. 37. Záložka Wireless

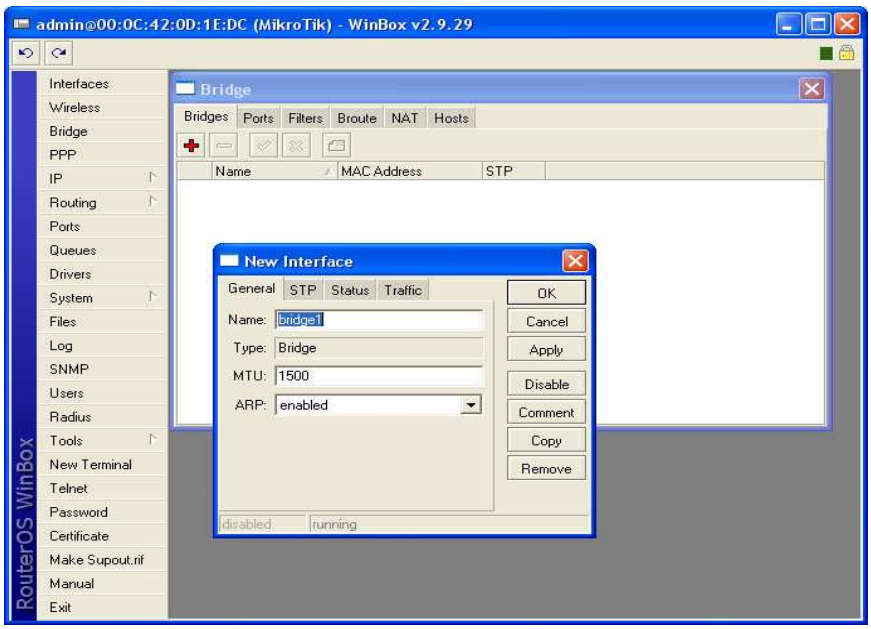
Jedna karta tedy bude nastavena do režimu stanice a druhá AP(acces point). U karty, která je v režimu stanice můžeme tlačítkem *Scan* vyhledat dostupné sítě a poté se k nim připojit tlačítkem *Connect*.



Obr. 38. Záložka Scan

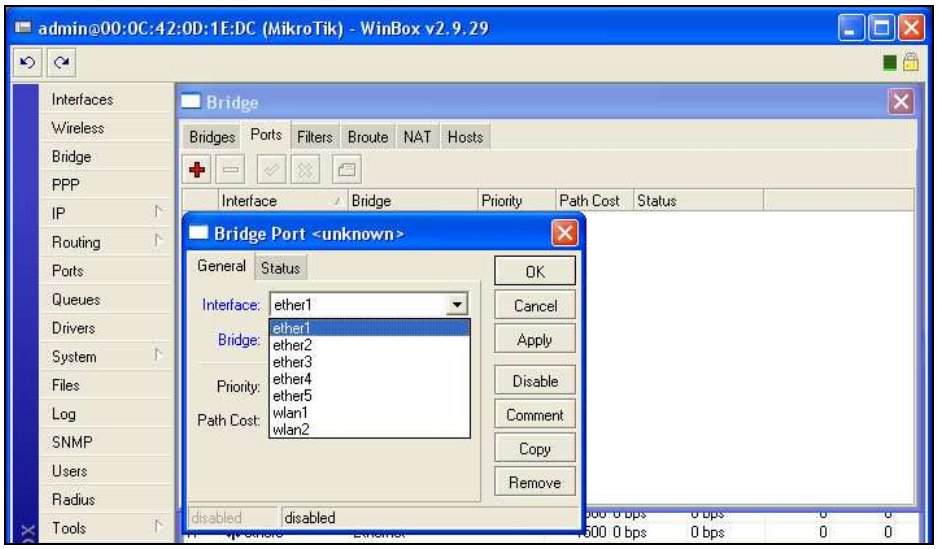
Velmi důležitým krokem, je rozdělení všech rozhraní na dvě části - na klient a bridge. Klientskou částí bude tedy jen jedna bezdrátová karta, která bude přijímat signál v režimu stanice. Do bridge se musí přidat všechny porty ethernet spolu s kartami, které budou v režimu AP (access point). Jak klient, tak bridge, budou mít svoji IP adresu, přičemž adresa bridge je zároveň IP adresou celého routerboardu.

Pro vytvoření bridge je nutné zvolit menu *Bridge* a zde nejprve záložku Bridges. Zde pak tlačítkem + *(add)* můžeme přidat nové rozhraní.



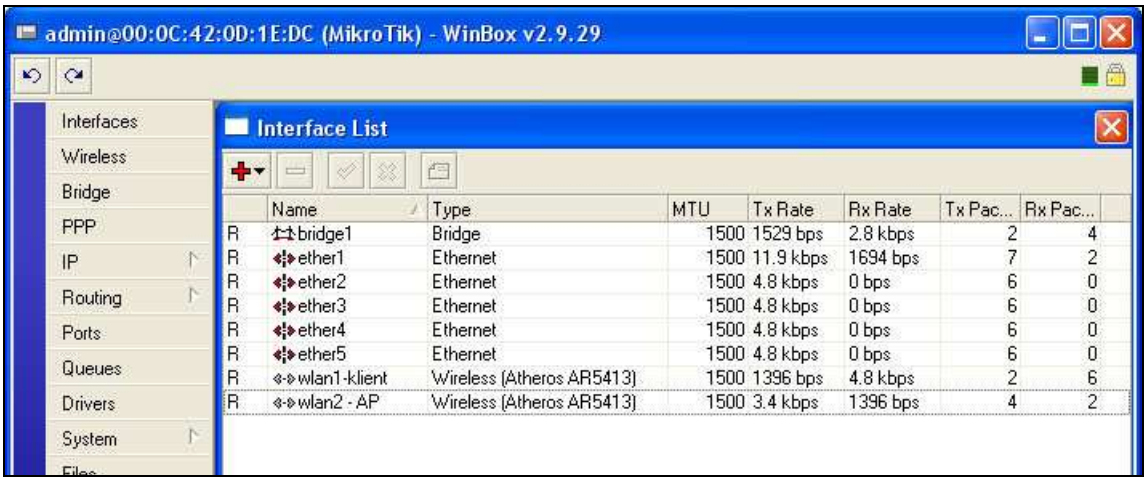
Obr. 39. Menu Bridge

Objeví se okno *New interface*, kde lze bridge pojmenovat. Po uložení změn se dále přejde do záložky *Ports*, kde se opět tlačítkem + *(add)* přidají postupně všechny ethernet porty a karty, které budou vysílat signál.



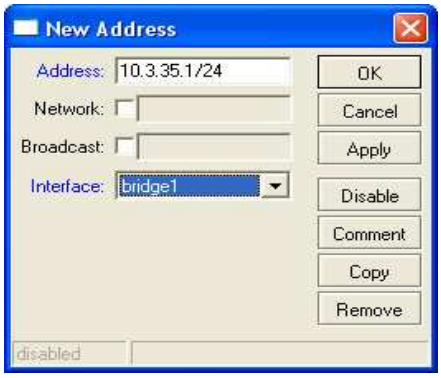
Obr. 40. Záložka Ports

Nyní se již v menu *Interfaces* objeví také vytvořený bridge.

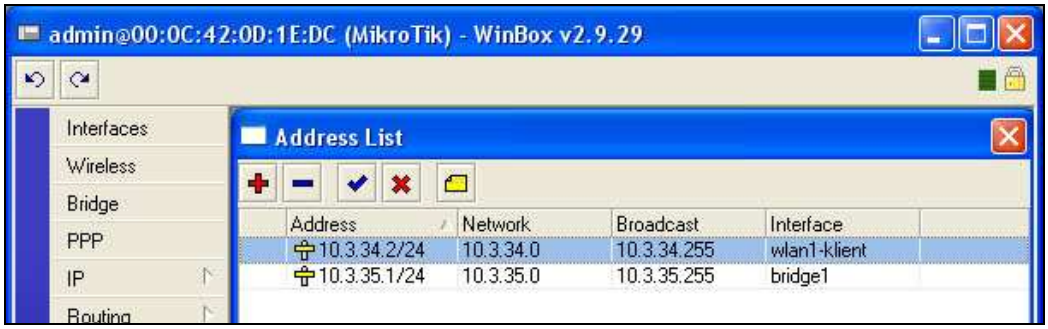


Obr. 41. Menu Interfaces

Dalším důležitým krokem je přiřazení IP adres. To lze provést v menu *IP – Addresses* znovu použitím tlačítka + *(add)*. Je-li adresa předchozího převaděče 10.3.34.1 a nastavujeme převaděč následující, je nutné bridgi přiřadit IP adresu například 10.3.35.1 a bezdrátové kartě, která přijímá signál adresu 10.3.34.2. V praxi to tedy vypadá následovně:



Obr. 42. Přiřazení IP adresy bridgi

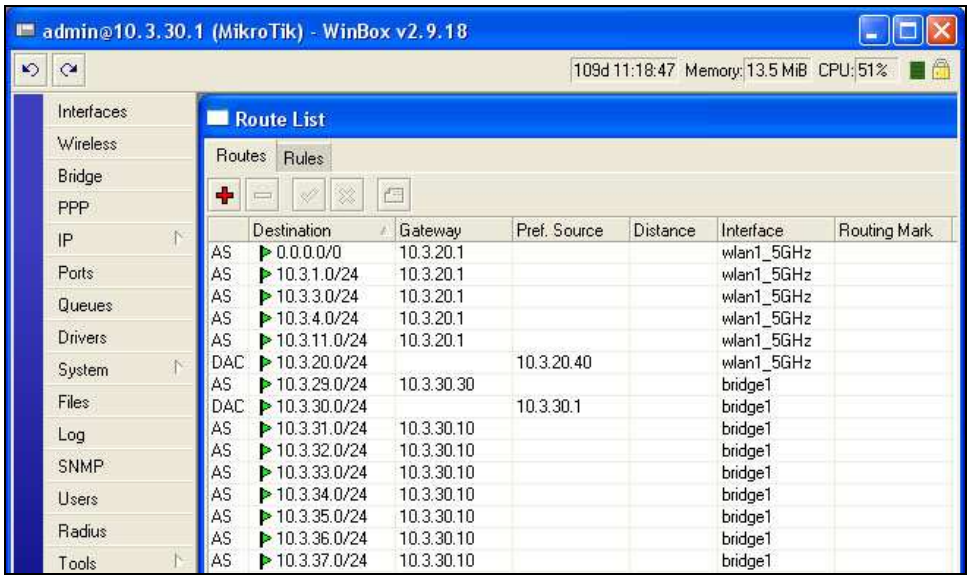


Obr. 43. Menu Address List

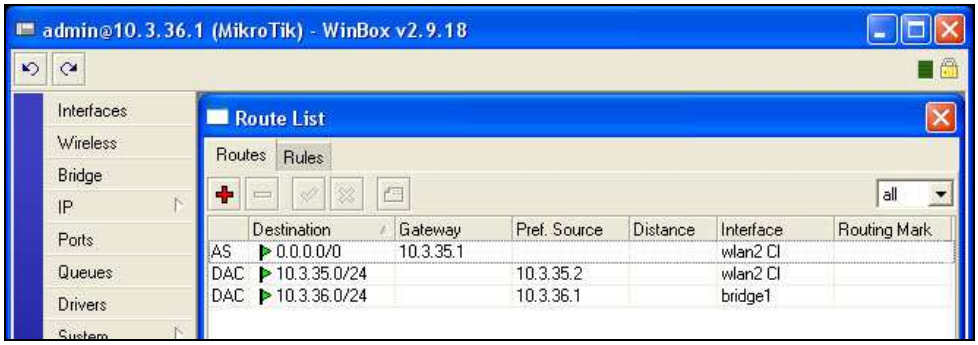
Jak je patrné, routerboard je nastaven jako směrovač. Je tedy nutné nastavit na každém z nich směrovací tabulky. V případě většího počtu převaděčů, jako tomu je v tomto případě, je na prvním z nich směrovací tabulka nejobsáhlejší a na posledním naopak nejstručnější. Na prvním z nich se totiž musí nastavit všechny cesty na další převaděče.

Pro názornost je uveden příklad.

Je nastavován převaděč s adresou 10.3.34.1. Směřuje-li paket na adresu 10.3.35.1, musí jít přes 10.3.34.2. Směřuje-li další paket na adresu 10.3.36.1, musí jít přes 10.3.34.2 atd. Zároveň se musí nastavit výchozí brána a tou je adresa předchozího převaděče 10.3.33.1. Jak vypadá směrovací tabulka v praxi na jednom z prvních a na jednom z posledních převaděčů lze vidět na následujících obrázcích.



Obr. 44. Směrovací tabulka1



Obr. 45. Směrovací tabulka 2

5 KLIENTSKÉ STANICE

Nejlevnějším řešením klientské stanice by samozřejmě bylo použití bezdrátové síťové karty s připojenou odpovídající anténou. Z důvodu lepší správy sítě a zjišťování závad bylo ale stanoveno, že každý přihlášený účastník si musí pořídit aktivní prvek. Byla vybrána zařízení s více porty LAN, aby nebyl problém s připojením více počítačů v domácnosti, například s dalším přikupováním zařízení (switch).

5.1 Hardware

Klientům tedy byly instalovány dva typy aktivních prvků:

OvisLink WL-5460AP

Je to bezdrátový prvek z rodiny OvisLink. Nástupce legendární jednotky WL-1120AP, zachovávající její funkce, rozšířené pro pásmo 802.11g s podporou 64/128 WEB a WPA. Chipset Realtec 8186.

Jednotka pracujíce v režimech:

- Access Point
- Client
- Repeater
- Bridge
- WISP

Dále umožňuje regulaci výstupního výkonu (max. 18 dBm) ve 4 krocích. Disponuje konektorem externí antény RSMA a dvojicí ethernet konektorů RJ-45. Rozšířená paměť (2MB Flash and 16MB SDRAM) je připravená pro další funkce, mezi nimi v základu nechybí WatchDog.

Obr. 46. OvisLink WL – 5460AP

Tabulka XVII. Parametry OvisLinku WL – 5460AP

Datová propustnost:	54, 48, 36, 24, 18,11, 5.5, 2, 1 Mbps
Firewall:	Ne
Konektor:	RSMA male
LAN:	2
Norma IEEE:	802.11 b/g
Překlad:	Ano
Regulace výstupního výkonu:	Ano
Výstupní výkon:	18 dB
Zabezpečení:	WEP/WPA/WPA2
Anténa:	2dBi odjímatelná dipólová anténa
Frekvenční pásmo:	USA (FCC) 11 kanálů: 2.412GHz - 2.462GHz Evropa (ETSI) 13 kanálů: 2.412GHz - 2.472GHz Japan (Telec) 14 kanálů: 2.412GHz - 2.483GHz
Provozní hodnoty:	provozní teplota 0~60°C skladovací teplota -20~65°C
Napájení:	DC12V, 800mA
Rozměry:	135 x 100 x 26mm
Váha:	180g

Druhým typem zařízení je **Straightcore WRT311.**

Bezdrátový router s možností klientského režimu WRT-311 je kompletně v českém jazyce, včetně obalové krabice a manuálu.

Toto výjimečné zařízení je založené na chipsetu Realtek 8186, pracuje tedy dle norem 802.11b/g a je radiově shodné například s Ovislinkem WL-5460AP. Zde však podobnost s ostatními zařízeními tohoto typu končí. Zvláštností této jednotky je totiž 5 ethernetových portů na zadní straně. Jednotka obsahuje 3 logické interface: 1 bezdrátový a dva ethernetové. Navíc jedno ethernetové rozhraní je rozšířeno na čtyřportový switch., lze tedy Jednotku lze nakonfigurovat jako:

-bridge (stejná funkce jako u Ovislink WL5460AP+4 port switch)

-drátový směrovač (ether1 je WAN, 4x LAN+WiFi je LAN)

-bezdrátový směrovač (WiFi je WAN, 4x LAN + jedním portem DMZ)

Celkem je k dispozici 6 operačních módů:

- Access Point
- Client
- Repeater
- Bridge

- NAT Router
- Wifi Router

Lze regulovat výstupní výkon po 1 dB v rozmezí 8-20 dB. Dále je zde možnost vypnout NAT a routing provádět bez překladu adres. Disponuje také hardwarovým a softwarovým watchdogem, který zajistí automatický restart v případě problému. Dalšími zajimavými vlastnostmi je například DDNS dynamické DNS nebo QoS řízení rychlosti na WAN port v krocích od 64kbit -4Mbit.

Obr. 47. Straightcore WRT - 311

Tabulka XVIII. Parametry WRT-311

Datová propustnost:	54/48/36/24/12/11/5,5/2/1 Mbps s automatickým snižováním v zarušeném prostředí
Standardy:	802.11b/g bezdrátová část, IEEE 802.3 LAN část
typ antény:	odpojitelný dipól 2dB (konektor RP-SMA)
Frekvence	2,4 - 2,4835 Ghz
Porty	1xWAN, 4xLAN 10/100 Mbit/sec.
výstupní výkon:	8-20 dB
ostatní parametry:	podpora šifrování:WEP64/128,WPA,WPA2
Diagnostické LED	Napájení, WAN, 4x LAN, Wifi
Napájecí adaptér	12V/0,5A
Provozní teplota	0 - 55°C
Rozměry	30x127x96 mm

Dalším hardwarem jsou samozřejmě antény. Jsou použity výše zmiňované typy PAN10 - 10 dBi (2,4 GHz), TA PAN-14 PRO (2,4 GHz) a v některých případech přímo dipól 2dBi.

5.2 Připojení klientských stanic

Kompletní sada pro připojení tedy obsahuje anténu, konzoli, pigtail, přijímač (OvisLink 5460 nebo WRT311), UTP kabel a koncovky RJ-45. Pigtail je omezen Délkou 5m, kdežto UTP kabel může být dlouhý i 100 metrů. Z toho vyplývá, že přijímač bude umístěn nejdále 5 metrů od antény a zároveň je vhodné, aby se nacházel ve vnitřních prostorách. Dále je nutné přivést k počítači síťový kabel. Konkrétní délku je třeba vyrobit a proto je potřeba krimpovacích kleští k adjustáži koncovek.

5.2.1 Zhotovení kabelu s koncovkami RJ-45

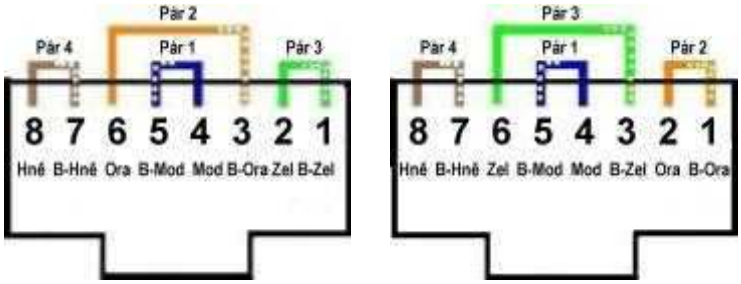
Strukturovaná kabeláž používá čtyřpárové kroucené "twistované" kabely. Existují dva typy UTP, jeden používá kabelů z drátků a u druhého jsou zhotovovány z lanek. Podle příslušného provedení kabelu je nutno vybírat i příslušné provedení konektorů (drát, lanko). Jednotlivé páry v kabelu jsou označeny barevně (modrá, oranžová, zelená, hnědá).

Obr. 48. Páry UTP kabelu

Vždy jeden z vodičů v páru má příslušnou barvu a druhý do páru je buď bílý, nebo různě proužkovaný v kombinaci bílá/příslušná barva. Pro připojení jednotlivých drátů ke kontaktům konektoru existují dva standardy **T568A a T568B.**

Tabulka XIX. Rozdíl mezi standardy T568A a T568B

T568A	T568B
1 - Bílá / Zelená	1 - Bílá / Oranžová
2 - Zelená	2 - Oranžová
3 - Bílá / Oranžová	3 - Bílá / Zelená
4 - Modrá	4 - Modrá
5 - Bílá / Modrá	5 - Bílá / Modrá
6 - Oranžová	6 - Zelená
7 - Bílá / Hnědá	7 - Bílá / Hnědá
8 - Hnědá	8 - Hnědá



Obr. 49. Pohled zepředu na zástrčky (T568A, T568B)

Pokud je snaha propojit pouze 2 počítače (síťové karty) mezi sebou, není potřeba switche či jiného dalšího aktivního prvku. Stačí pouze křížový propojovací kabel. Stejný kabel je nutno používat i pro propojení dvou hubů či jiných aktivních prvků v případě, že použitý prvek nemá možnost prohození vývodů TD a RX.

V našem případě je ale potřeba propojit počítač s aktivním prvkem a k tomuto účelu stačí nekřížený síťový kabel. Je nutné seřadit barvy tak, jak jsou uvedeny v následující tabulce a nacvaknout koncovku.

Tabulka XX. Barvy obou koncovek kabelu podle T568B

Bílá / Oranžová	**Bílá / Oranžová**
Oranžová	**Oranžová**
Bílá / Zelená	**Bílá / Zelená**
Modrá	**Modrá**
Bílá / Modrá	**Bílá / Modrá**
Zelená	**Zelená**
Bílá / Hnědá	**Bílá / Hnědá**
Hnědá	**Hnědá**

Pro zhotovení kříženého kabelu by byl pro jednu koncovku použit standard T568A a pro druhou T568B.

5.2.2 Napájení aktivního prvku

Použité aktivní prvky mají ve výbavě síťový adaptér. Ve většině případů musí být ale zařízení umístěno na místo, kde není přivedena elektrická síť. Standart 10BaseT / 100BaseT používá pro komunikaci pouze dva páry, pár 2 (oranžová) a 3 (zelená). Zbývající páry 1 (modrá) a 4 (hnědá) neslouží v tomto případě pro komunikaci a je možno je použít právě pro napájení tak, že se kabel síťového adaptéru rozstřihne a konec se zástrčkou se napojí na straně u počítače a druhý na straně u přijímače. Toto řešení je velmi jednoduché a nevyžaduje žádné další finanční náklady.

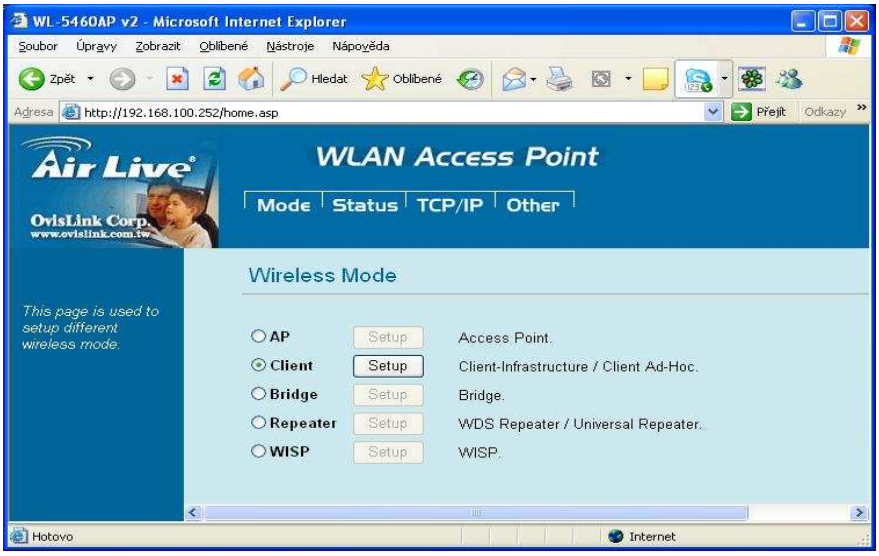
Je-li aktivní prvek připojen k počítači a zároveň i do elektrické sítě, může nastat jeho konfigurace.

5.2.3 Nastavení Ovislink 5460AP

Zařízení bylo nastavováno ve dvou režimech:

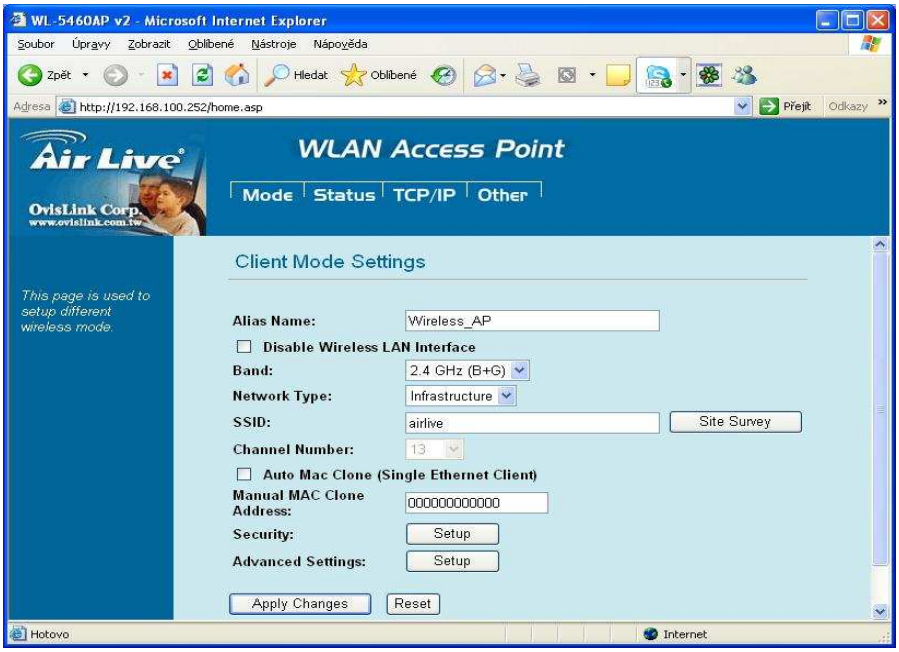
Klient se statickou IP adresou

Po zadání adresy *192.168.100.252* do okna internetového prohlížeče se následně objeví menu.



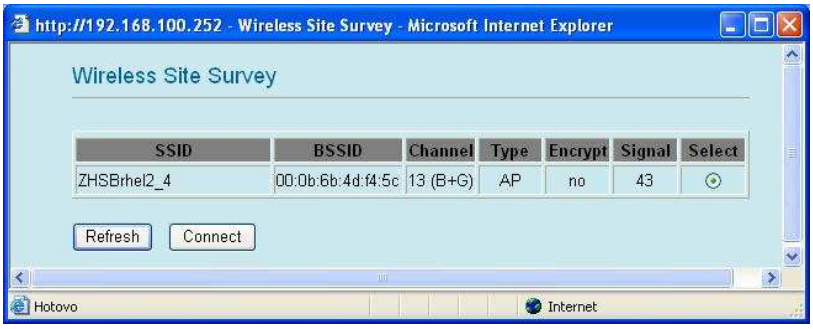
Obr. 50. Výběr režimu

V záložce *Mode* je nutno nastavit režim *Client* a dále kliknout na tlačítko *setup*. Objeví se následující tabulka, kde je potřeba vyplnit základní údaje jako například jméno klienta, pásmo, typ sítě apod. Po změně jména se můžou všechny položky nechat ve výchozím nastavení. Ostatní položky jsou pro tento režim nepodstatné. V *advanced settings* je možné ještě nastavit watchdog.



Obr. 51. Úvodní nastavení

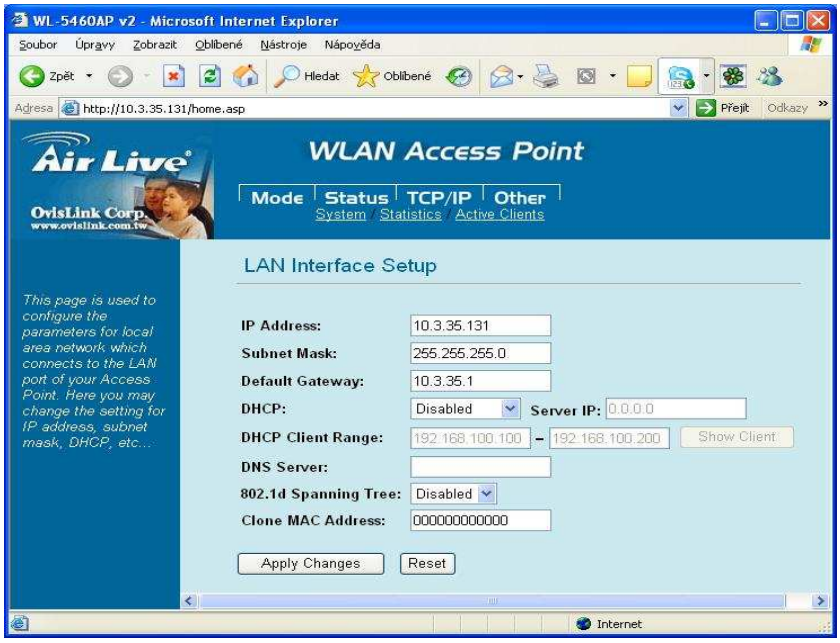
Po uložení změn stisknutím tlačítka *apply changes* následuje přechod do okna pro vyhledání dostupné sítě tlačítkem *site survey*.



Obr. 52. Vyhledání dostupné sítě

Po kliknutí na tlačítko *Refresh* dojde k zobrazení nalezené sítě, síle signálu a dalších parametrů. Po označení příslušné sítě pod nápisem *Select* může tedy dojít k připojení pomocí *Connect*. Následně se objeví se zpráva o úspěšném připojení.

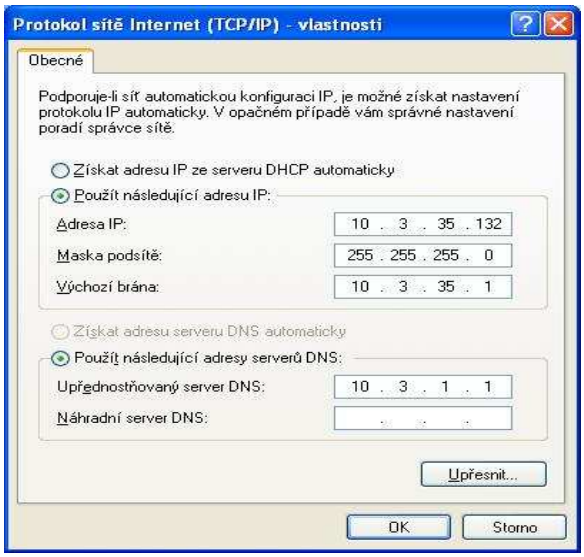
V záložce *TCP/IP* je nutné přiřadit IP adresu samotnému zařízení, vyplnit masku podsítě a bránu. DHCP se v tomto případě nenastavuje.



Obr. 53. Nastavení TCP/IP

IP adresa musí být v podsíti daného vysílače a bránou je adresa samotného převaděče.

Po uložení změn je nastavení přijímače kompletní a stačí jen nastavit IP adresu příslušnému počítači. To lze učinit ve vlastnostech TCP/IP protokolu.



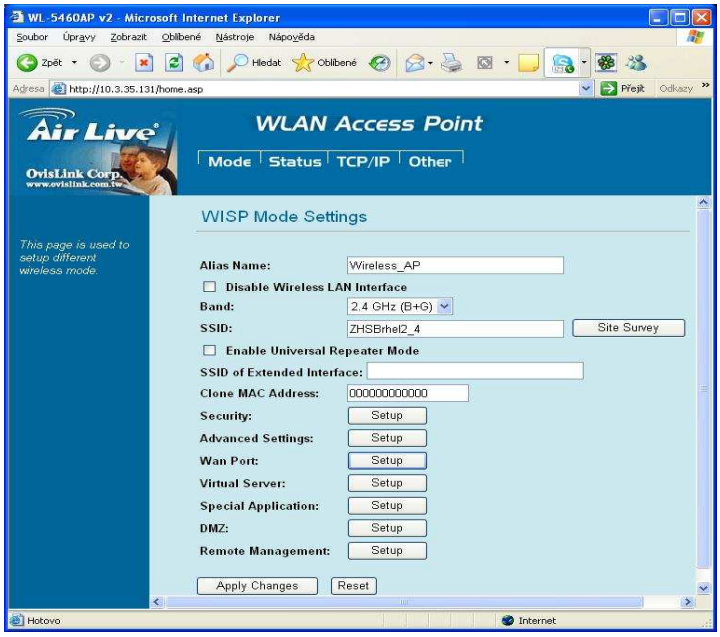
Obr. 54. Nastavení TCP/IP

Mimo IP adresy je nutné vyplnit také masku podsítě, výchozí bránu a DNS server. Po stisknutí tlačítka *OK* je již samotný počítač připojen k internetu.

Nevýhodou tohoto nastavení je nutnost po každé přeinstalaci operačního systému nastavovat IP adresy ručně. Další nevýhodou je spotřeba IP adres v případě většího počtu PC připojených k OvisLinku.

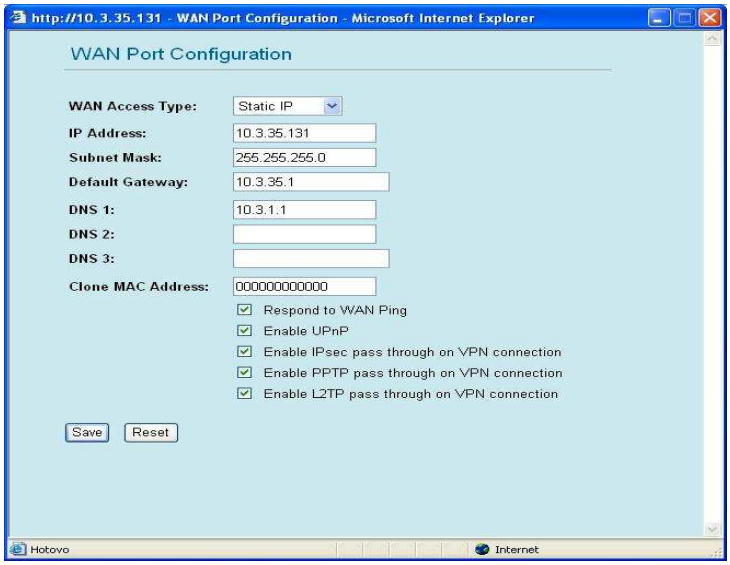
Klient s dynamickým přidělením IP adresy

V úvodním menu v záložce *MODE* je nutné zvolit režim *WISP*. Zobrazí se znovu úvodní nastavení s drobnými rozdíly oproti předchozímu případu.



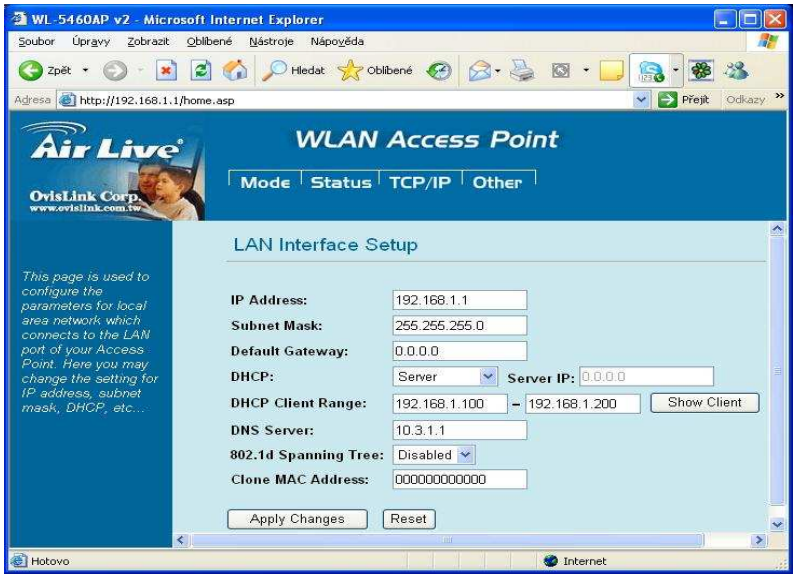
Obr. 55. WISP nastavení

Velmi důležitá položka je *Wan Port*.



Obr. 56. WAN nastavení

Zde je nutné nastavit typ přístupu WAN na *static IP* a dále nastavit IP adresu zařízení, masku podsítě, výchozí bránu a DNS server. Všechny ostatní položky zůstávají opět ve výchozím nastavení. Po uložení změn zbývá nastavit záložku *TCP/IP*.



Obr. 57. Nastavení DHCP

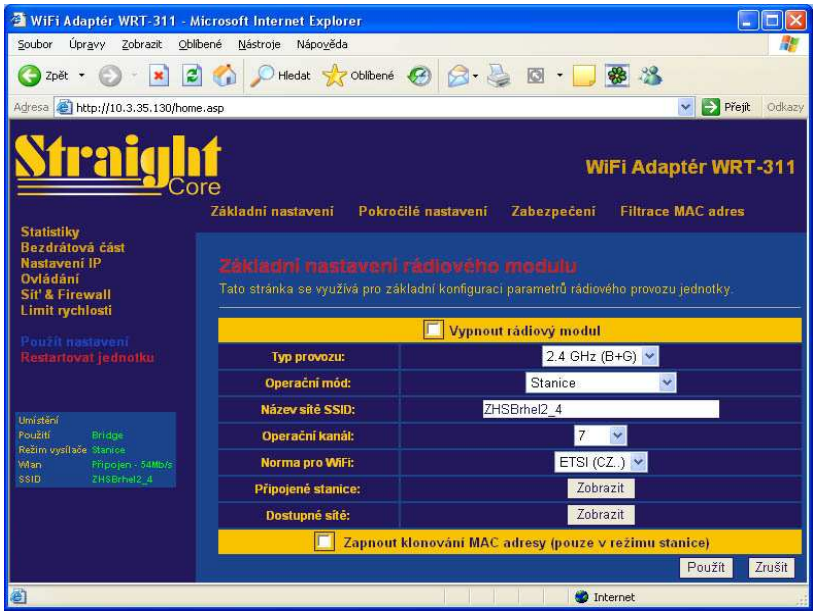
Zde se nastavuje adresa zařízení pro přístup z vnitřní sítě. Adresa může být zvolena z privátních rozsahů libovolně, například *192.168.1.1*. DHCP je nutné nastavit do režimu *Server* a dále určit rozsah adres přidělovaných počítačům za směrovačem (v tomto případě 192.168.1.100-192.168.1.200). Na PC se již nemusí nic nastavovat, po uložení změn je přístup k Internetu zprovozněn.

Výhodou tohoto nastavení je, že Internet běží ihned po zapojení síťového kabelu do počítače a není potřeba nastavovat IP adresy ručně. Další výhodou je šetření IP adresasmi. Nevýhodou je to, že software typu HAMACHI nedokáže spojit dva klienty takto skryté za směrovačem.

5.2.4 Nastavení WRT311

Klient se statickou IP adresou

Nastavení je velmi podobné jako u předchozího zařízení s tím rozdílem, že vše je v českém jazyce. Pro přístup do menu se ale musí v internetovém prohlížeči zadat IP adresa *192.168.1.1*, která je oproti továrnímu nastavení Ovislinku 5460AP odlišná. V záložce *Bezdrátová část* je nutné nastavit pásmo *2,4 GHz (B+G)*, operační mód *stanice* a také normu pro Wi-Fi na *ETSI(CZ..)*.

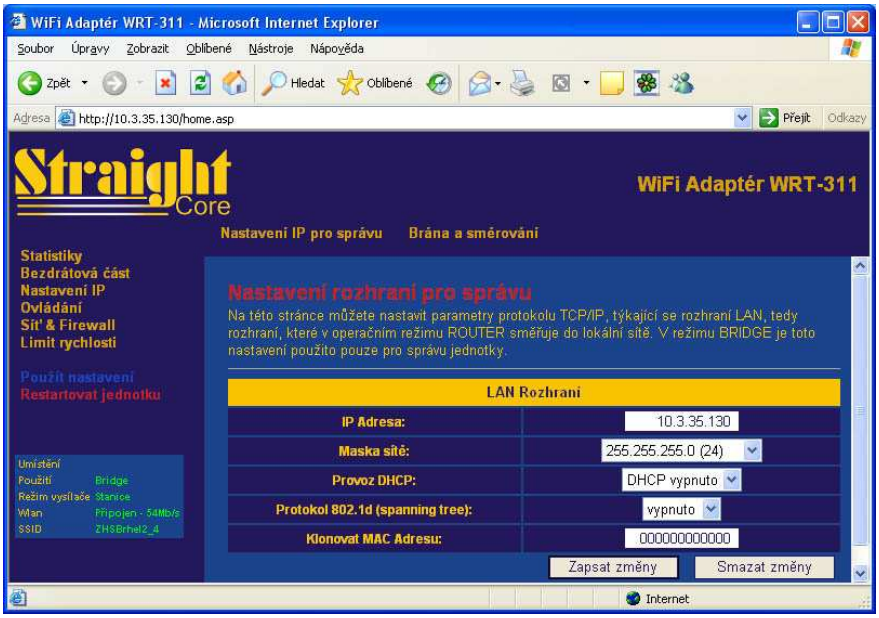


Obr. 58. Základní nastavení WRT311

Kliknutím na tlačítko *Zobrazit* u dostupných sítí se objeví tabulka, kde jsou zobrazeny všechny nalezené sítě a může dojít k připojení k některé z nich. Na následujícím obrázku lze vidět, že přijímač detekoval mimo vysílače, na který bude připojen i vysílač předchozí (ZHSAPVranik). Rozdíl v signálu je ale značný.

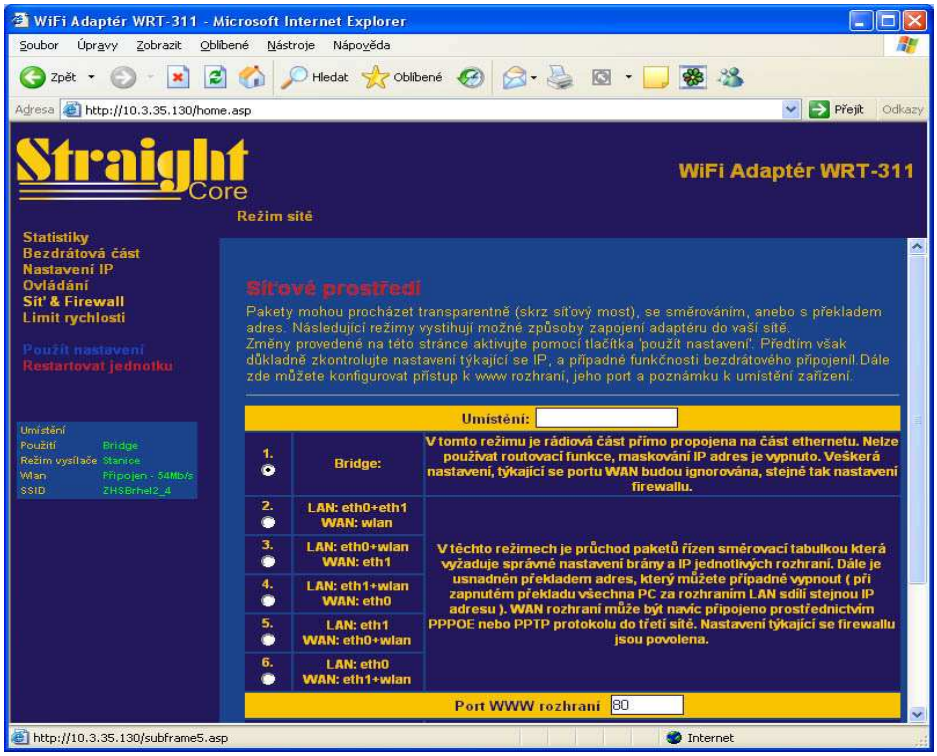
Obr. 59. Dostupné sítě

V nastavení IP se přiřadí adresa Wi-Fi adaptéru a nastaví se maska. DHCP v tomto případě zůstává vypnuto. Dále v záložce *Brána a směrování* je nutné nastavit IP adresu výchozí brány.



Obr. 60. Nastavení IP

V záložce *Síť & firewall* musí být nastaven režim bridge, protože bude mít počítač staticky přidělenou adresu. Poslední záložka *limit rychlosti* se nenastavuje. Veškerá omezení se jsou nastavena přímo v Mikrotiku.



Obr. 61. Síť a firewall

Po nastavení správné IP adresy, masky, brány a DNS serveru v počítači je připojení k Internetu aktivní.

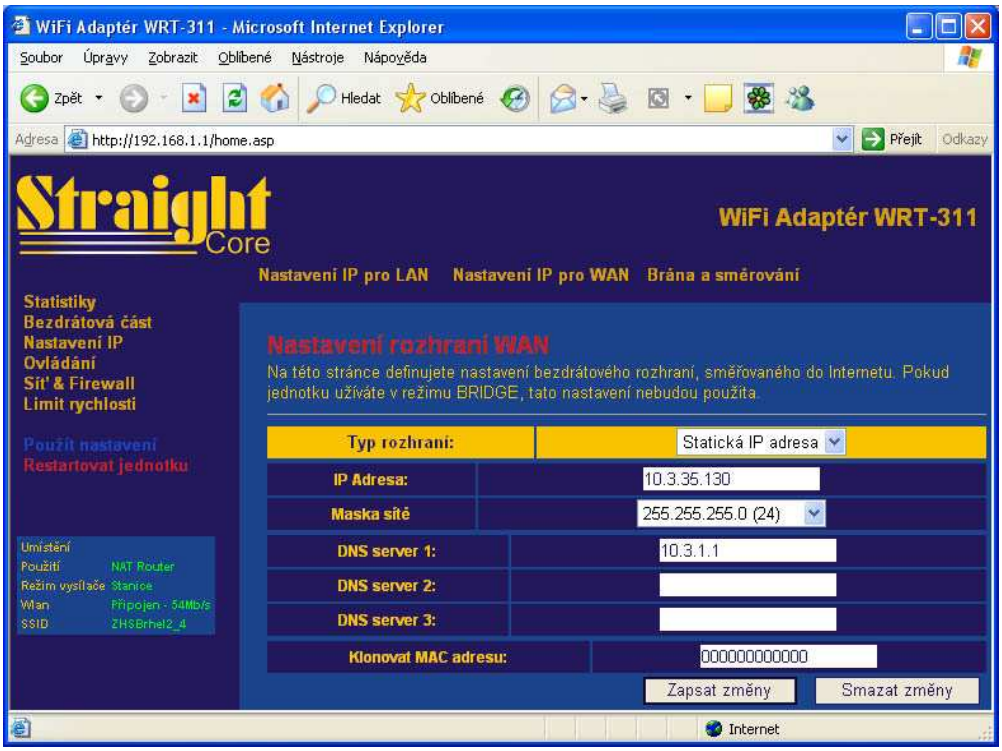
Klient s dynamickým přidělením IP adresy

V záložce *Bezdrátová část* zůstává vše stejně jako v předchozím případě. Tedy operační mód je *stanice*, typ provozu je nastaven na *2,4HZ (B+G)* a norma pro Wi-Fi je zvolena *ETSI(CZ..)*.

Pro zprovoznění DHCP je ale důležitá záložka *Síť a firewall*, kde pro tento účel máme k dispozici tři režimy (*2*,*5* a *6* viz obr. 48.).

V režimu číslo 2 slouží pro WAN bezdrátová karta wlan a pro lokální síť je určeno rozhraní eth0 + eth1. V režimu číslo 5 je WAN rozhraním eth0 + wlan a pro účely místní sítě slouží eth1. Podobné je to u režimu číslo 6, kde je WAN rozhraním eth1 + wlan a pro lokální síť eth0.

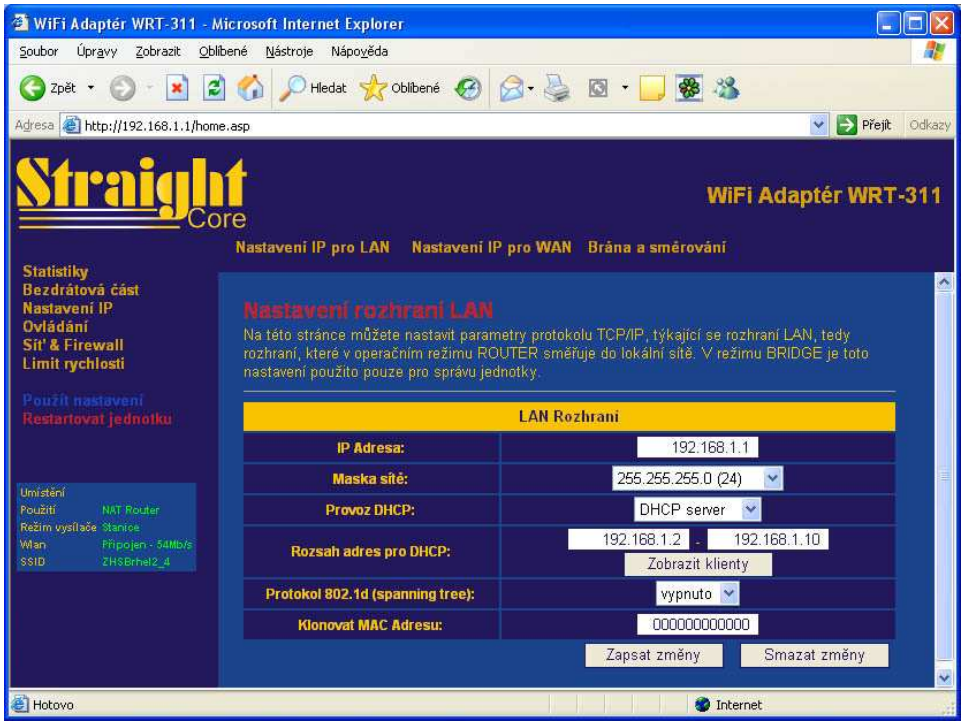
Protože je Internetový signál přijímán pouze bezdrátově, je nejvhodnější nastavit režim číslo 2, aby bylo možné všechny ostatní porty použít pro počítače. Po uložení změn se již může přejít do záložky *Nastavení IP*, která v tomto případě je oproti předchozímu případu pozměněna.



Obr. 62. Nastavení WAN

V *Nastavení rozhraní WAN* je určen typ rozhraní na statickou IP adresu, dále je nutné vyplnit IP adresu přidělenou správcem sítě, masku podsítě a DNS server.

V *Nastavení rozhraní LAN* se přidělí zařízení IP adresa pro přístup z vnitřní sítě, maska sítě a *Provoz DHCP* se nastaví na *DHCP server*. Dále musí být určen příslušný rozsah adres pro DHCP, které budou přidělovány počítačům.

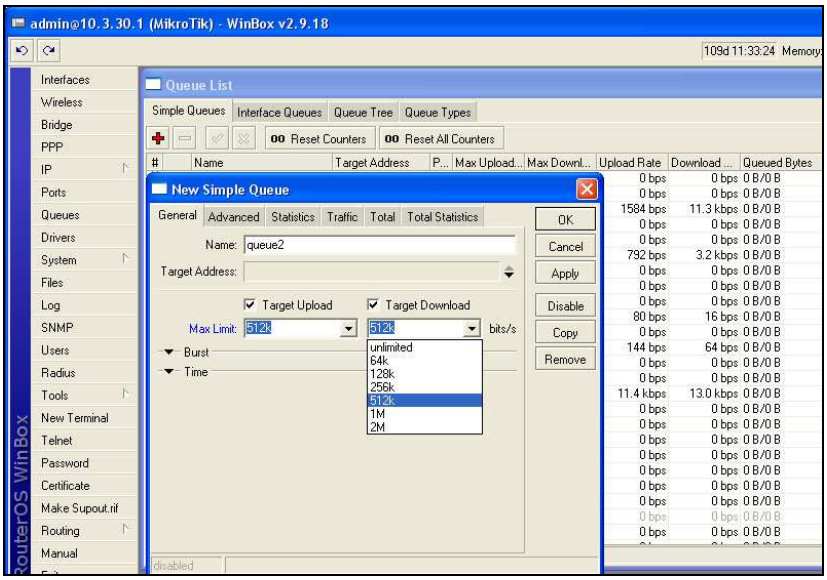


Obr. 63. Nastavení LAN

V poslední záložce *Brána a směrování* se již nastavuje pouze výchozí brána. Po uložení nastavení je již možné na připojených PC bez jakéhokoliv nastavování IP adres přijímat internetový signál.

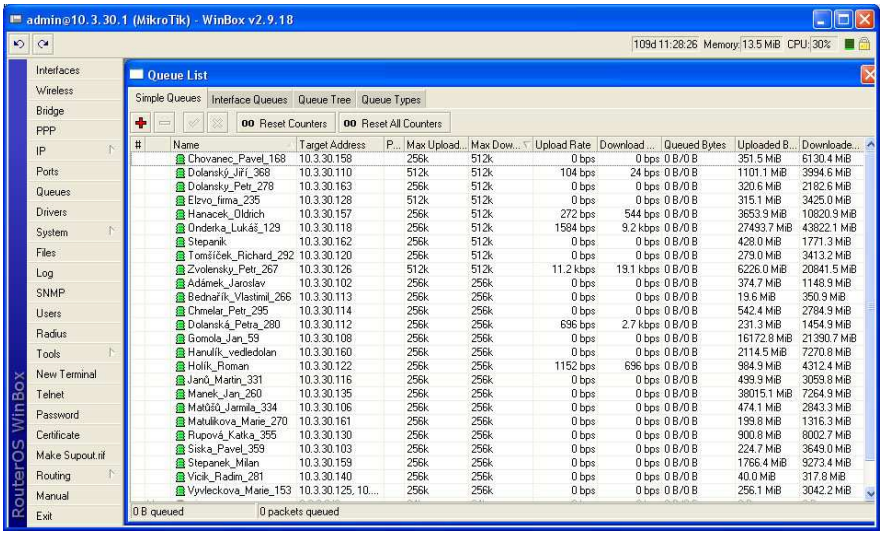
5.3 Nastavení rychlosti Internetu u klientů

Klientům byly nabídnuty pro začátek dva typy rychlostí - 512kbps a 256 kbps. Tato rychlost je stejná jak pro download tak i pro upload. Z důvodu konkurence ADSL nebyla nastavena žádná datová omezení. Rychlosti uživatelů jsou nastaveny opět přímo v Mikrotik OS. Pro tento účel slouží menu *Queues*, kde opět tlačítkem + *(add)* lze přidat uživatele.



Obr. 64. Přidání uživatele

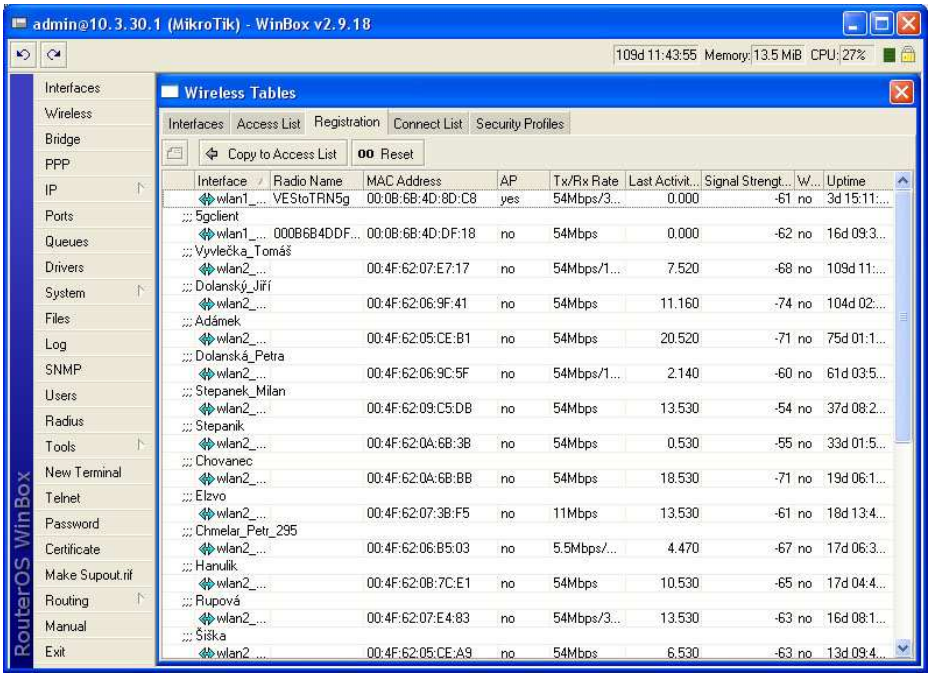
V záložce *General* se nastavuje jméno uživatele, IP adresa a přidělené rychlosti směrem k uživateli a od uživatele. V záložce *Advanced* lze potom nastavit datová omezení, což v tomto případě nebylo třeba. V praxi vypadá queue list uživatelů připojených na jeden převaděč následovně:



Obr. 65. Qeue list

V tabulce je také vidět, jak uživatelé právě využívají svou rychlost připojení a celková data přenesená směrem od nich i směrem k nim za určité období.

V menu Wireless lze sledovat, jaký mají uživatelé signál a jakou dobu jsou připojeni.



Obr. 66. Menu Wireless

6 EKONOMICKÉ HODNOCENÍ, KONKURENCE A BUDOUCNOST

6.1 Ekonomické hodnocení

Z důvodu utajení dohodnutých cen s poskytovatelem budou uvedeny jen přibližné částky. Celkové náklady na projekt byly poměrně vysoké. Jak již bylo zmíněno, důvodem byla neobvyklá délka páteřní sítě. Klientské zařízení a antény byly ale zaplaceny samotnými uživateli.

Cena na vybudování celé páteřní sítě činí tedy zhruba 70 000 Kč.

Cena za konektivitu je přibližně 1 500 Kč měsíčně za 1 garantovaný Mbit. Zatím jsou přivedeny celkově 4 Mbity, což je 6 000 Kč měsíčně.

Měsíční příjem plateb od uživatelů činí zhruba 30 000 Kč.

Provozní náklady jsou velmi nízké, protože všechna zařízení jsou v záruce a pronájmy ploch jsou řešeny bezplatným poskytnutím Internetu vlastníkům.

Měsíční zisk projektu je tedy přes 20 000 Kč měsíčně.

Z uvedených částek lze určit celková doba návratnosti, která při současných podmínkách činí tři a půl měsíce.

6.2 Konkurence a budoucnost projektu

Vzhledem k tomu, že v této oblasti nikdo nechtěl podobný projekt kvůli obtížnému provedení realizovat, je velmi malá pravděpodobnost, že se zde do budoucna objeví další poskytovatel Wi-Fi. Proto také ceny za internet jsou stanoveny tak, aby konkurovaly pouze ceně za ADSL a nemusí být brán ohled na ceny bezdrátového připojení v ostatních obcích a městech.

Projekt má velmi dobré vyhlídky do budoucnosti, protože za první půlrok existence se neodhlásil ani jeden z uživatelů pro nespokojenost, naopak stále se objevují noví zájemci. Je počítáno s tím, že se bude ještě postupně rozšiřovat páteřní síť a modernizovat hardware, protože nároky na rychlost budou stále větší a dosavadní zařízení nemusí v budoucnu stačit.

ZÁVĚR

Cílem diplomové práce bylo navrhnout a realizovat bezdrátovou síť připojenou do Internetu v obci Trnava a vyřešit tak krizovou situaci ohledně vysokorychlostního internetu v této oblasti. Snahou bylo vytvořit takový projekt, který bude uspokojovat všechny jeho uživatele a bude mít dobré vyhlídky do budoucna. Při obtížném navrhování a budování projektu bylo potřeba překonat značné množství překážek (jednání s majiteli pozemků ohledně umístění převaděčů, získání povolení pro kácení stromů atd.).

V teoretické části jsou popsány základy počítačových sítí a také bezdrátové Wi-Fi sítě. V praktické části je popsána páteřní síť a její struktura a také samotné připojování klientských stanic.

Závěrem lze říci, že projekt předčil všechna očekávání, jak po stránce ekonomické, tak po stránce poruchovosti. Ta je totiž poměrně malá a do budoucna bude ještě minimalizována umístěním zařízení UPS na všechny převaděče signálu. Projekt je sám o sobě dostatečně výdělečný, takže v případě potřeby modernizace bude dostatek finančních prostředků na všechna zařízení.

ZÁVĚR V ANGLIČTINĚ

The goal of this thesis was propose and realize wireless network connected to Internet in municipality Trnava and solve that critical situation regarding high-speed Internet in this area. There was endeavour to create project which will content every users and also will have good expectations into the future. During complicated proposing and construction of project was necessity to overcome considerable of obstacles (dealing with landowners concerning location of transmitters, obtaining leave for tree felling etc.).

In the theoretic part are described principles of computer networks and also wireless Wi-Fi networks. In the practical part are described backbone net and it's structure and connecting of client stations.

In fine can be stated, that project outdid every ecpectation concerning economics and also failure rate, which is relatively small and will be still minor in the future, because every transmitters of signal will have UPS back-up power supply. Project is well moneymaking, that in the case of need new equipment will be enough financial resources.

SEZNAM POUŽITÉ LITERATURY

[1] Základy počítačových sítí [online]. [cit. 2007-4-10]. Dostupné z URL: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=21

[2] Harold Davis, Wi-Fi Bezdrátové sítě, Grada 2006. [cit. 2007-4-15]

[3] Miroslav Matýsek: Prezentace Počítačové sítě. [cit. 2007-4-15]

[4] Jak na Wi-Fi [online]. [cit. 2007-4-15]. Dostupné z URL: http://www.bezdratovepripojeni.cz/wi-fi/

[5] Wikipedie – otevřená encyklopedie: Ethernet [online]. [cit. 2007-4-16]. Dostupné z URL: http://cs.wikipedia.org/wiki/Ethernet

[6] Zandl P.: Bezdrátové sítě WiFi: Praktický průvodce. Computer Press 2003.

[7] Barken L.: Wi-Fi: Jak zabezpečit bezdrátovou síť. Computer Press 2004.

[8] Fiedler P.; Bradáč Z.: Zabezpečení bezdrátových sítí WiFi (IEEE 802.11b, g), 7.10.2004 [online]. Dostupné z URL: http://www.odbornecasopisy.cz/automa/2004/au100426.htm

[9] Podrobné informave k provozu bezdrátových sítí v pásmech 5 GHz, 17.11.2004 [online]. Dostupné z URL: http://www.i4shop.net/cz/iObchod/Webinfo.asp?Id=136

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Wi-Fi	Wireless Fidenlity (bezdrátová věrnost) – organizace označující určitý bezdrátový standard neboli protokol používaný k bezdrátové komunikaci
PCI	Peripheral Component Interconnect - slot pro rozšiřující karty, např. síťové apod.
PCMCIA	Personal Computer Memory Card International Association – slot pro pro přídavné karty převážně u notebooků.
USB	Universal Serial Bus – rozhraní pro připojení různých periferních zařízení
LAN	Local Area Network – lokální síť
FDDI	Fiber Distributed Data Interface – lokální síť tvořící okruh propojený převážně optickým vláknem
ATM	Asynchronous Transfer Mode - transparentní přenosové prostředí, kombinující výhody switchovaných okruhů a flexibilitu okruhů na bázi přenosu paketů
UTP	Unshelded Twisted Pair – kroucená dvojlinka
MAN	Metropolitan Area Network – metropolitní síť
WAN	Widea Area Network – rozsáhlá síť
ISO	International Organization for Standardization – Mezinárodní organizace pro normalizaci
OSI	Open Systems Interconnection - propojení otevřených systémů
TCP/IP	Transmission Control Protocol/Internet Protocol - standardní soubor protokolů používající se po celé síti Internet
MAC	Media Access Control - jedinečný identifikátor síťového zařízení
UDP	User Datagram Protocol – nespojový protokol
CSMA	Carrier Sense Multiple Access - metoda náhodného přístupu
CD	Collision Detection – detekce kolizí
ARPANET	Advanced Research Project Agency´s NET – síť amerického minist. obrany

STP	Spanning Tree Protocol – mechanismus pro zabránění nekonečného přeposílání paketů
IPX/SPX	Internet Packet Exchange/Sequenced Packet Exchange - síťový protokol používající se v operačním systému Novell NetWare
ARP	Address Resolution Protocol - Internetový protokol, který dynamicky mapuje internetové síťové IP adresy do fyzických MAC adres
UPS	Uninterruptible Power Supply – záložní zdroj
WDS	Wireless Distribution System - je nadstavba nad původní normu 802.11, která umožňuje bezdrátové propojení dvou access pointů
WEP	Wired Equivalent Privacy – šifrovací protokol
WPA	Wi-Fi Protected Access - bezpečnostní mechanismus schválený Wi-Fi Aliancí
CRC	Cyclic Redundancy Check – kontrolní součet
ACK	Acknowledgment - kód pro indikaci korektního příjmu zprávy
ČTÚ	Český telekomunikační úřad
ADSL	Asymmetric Digital Subscriber Line - jedna ze čtyř technologií typu DSL s větší přenosovou šířkou pásma směrem k uživateli než od něj
POE	Power Over Ethernet – pasivní adaptér, který slučuje napájecí vedení do nevyužitých párů na UTP kabelu
DNS	Domain Name System – systém překladu doménových jmen na IP adresy
DHCP	Dynamic Host Configuration Protocol - Mechanismus pro dynamické přidělování IP adres jednotlivým uzlům sítě

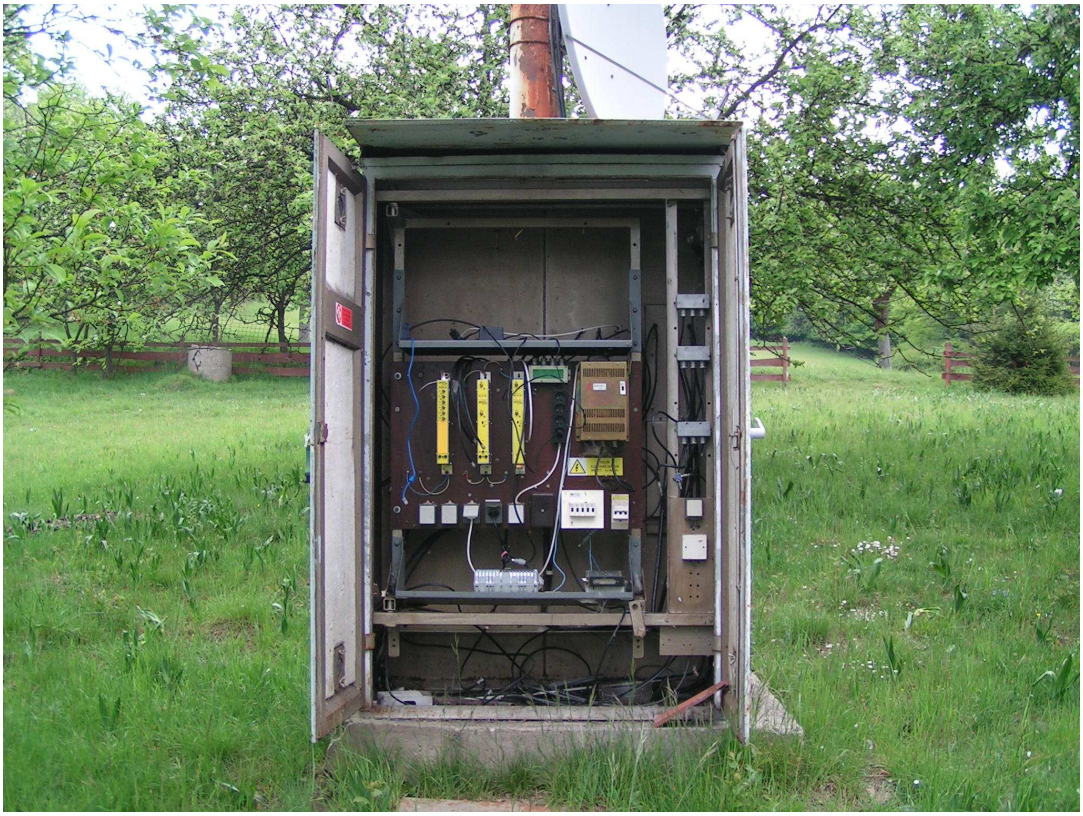
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

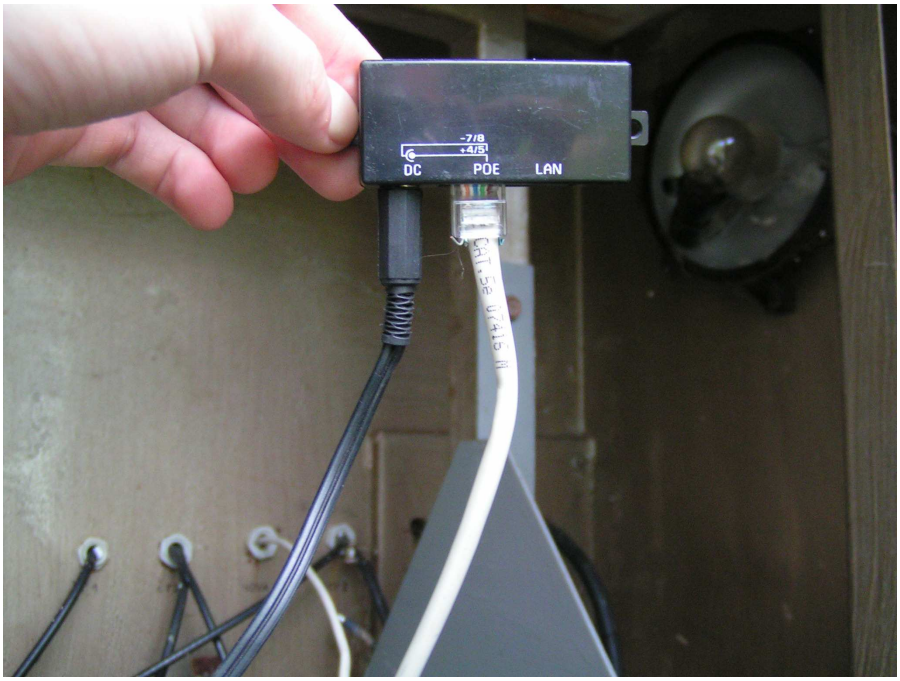
SEZNAM PŘÍLOH

PŘÍLOHA P I: FOTOGRAFIE OBECNÍHO STOŽÁRU S PRVNÍM PŘEVADĚČEM

PŘÍLOHA P II: FOTOGRAFIE SKŘÍNĚ ELEKTRICKÉHO NAPĚTÍ U PRVNÍHO PŘEVADĚČE



PŘÍLOHA P III: NÁHLED NA ŘEŠENÍ NAPÁJENÍ PRVNÍHO PŘEVADĚČE POMOCÍ POE



PŘÍLOHA P IV: FOTOGRAFIE PŘÍMÉ VIDITELNOST HLAVNÍHO SPOJE S POUŽITÍM PŘIBLÍŽENÍ (10X ZOOM)

PŘÍLOHA P V: FOTOGRAFIE PŘÍMÉ VIDITELNOST HLAVNÍHO SPOJE BEZ POUŽITÍ PŘIBLÍŽENÍ