Návrh a realizace metropolitní sítě v Pardubicích pro připojení klientů k bezdrátovému Internetu

Bc. Milan Velich

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Bc. Milan Velich**
Osobní číslo:	**A12354**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh a realizace metropolitní sítě v Pardubicích pro připojení klientů k bezdrátovému Internetu**
Téma anglicky:	**The Design and Implementation of a Metropolitan Network in Pardubice for Connecting Clients to the Wireless Internet**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Navrhněte metropolitní síť s využitím bezdrátových pojítek a prvků optických sítí.**
3. **Realizujte metropolitní síť pro připojení klientů k Internetu.**
4. **Navrhněte a realizujte místní sítě s využitím metalického vedení.**
5. **Navrhněte vhodné nástroje pro řešení dohledu a databázi klientů.**
6. **Navrhněte zabezpečení sítě z hlediska poskytovatele internetových služeb.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. 1. vyd. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.**
2. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. 1. vyd. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.**
3. **ROHLÍK, Matěj a Pavel LAFATA. Bezpečnostní rizika v současné generaci pasivních optických přístupových sítí. Electrorevue [online]. 2010, roč. 12, č. 3 [cit. 2013-12-5]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/download/bezpecnostni-rizika-v-soucasne-generaci-pasivnich-optickych-pristupovych-siti/**
4. **Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: 127/2005. 2005, č. 127, 43/2005. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&nr=127 2F2005&rpp=15local-content**
5. **STALLINGS, William. Local and metropolitan area networks. 6. ed. Upper Saddle River: Prentice Hall, 2000, 478 p. ISBN 9780130129390.**
6. **MAIER, Martin. Optical switching networks. Cambridge: Cambridge University Press, 2008, 324 p. ISBN 0-521-86800-9.**

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

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 14.5.2014

…….
podpis diplomanta

ABSTRAKT

Tato práce obsahuje popis výstavby metropolitní sítě pro komerční připojení klientů k Internetu. Místem realizace je město Pardubice. Práce je rozdělena do dvou základních částí. V první části, teoretické, jsou popsány základní prvky pro výstavbu bezdrátových, optických a místních sítí. Pozornost je věnována také zabezpečení těchto prvků. Poslední kapitola teoretické části seznamuje s právními aspekty výstavby a provozu sítí.

Praktická část popisuje vlastní návrh, výstavbu a modernizaci metropolitní sítě tak, jak k ní postupně během několika let stále dochází. Největší pozornost je věnována rozmístění páteřních prvků a uzlových bodů. Samostatně je uveden návrh sítí LAN. Další kapitola popisuje navržené a instalované řešení dohledového systému a klientské databáze. Posledním bodem je návrh a realizace bezpečnostních opatření v síti.

Klíčová slova: MAN, Internet, ISP, optické sítě, LAN, bezpečnost

ABSTRACT

This thesis describes building a metropolitan area network by a commercial service provider, using Pardubice metropolitan network as a case study. The paper is divided into two parts. The first, theoretical part looks at the basic components required to build wireless, optical and local networks, paying particular attention to security of the elements. The final chapter of this part studies the legal aspects of building and operating networks.

The practical part describes the design of the metropolitan area network itself, its building and modernization development over the last few years, with a special focus placed on the location of backbone elements and nodes. The local network design is listed separately. The next chapter concentrates on the design and installation of the monitoring system and the client database. The paper concludes with the design and implementation of the network security measures.

Keywords: MAN, Internet, ISP, optical networks, LAN, security measures

PODĚKOVÁNÍ

Na tomto místě bych chtěl poděkovat vedoucímu práce Ing. Miroslavu Matýskovi, Ph.D. za cenné připomínky ke zpracování. Dále společníkům a zaměstnancům firmy KVE s.r.o. Pardubice za jejich nasazení při realizaci výstavby metropolitní sítě. V neposlední řadě děkuji Bc. Lence Havranové za pomoc s korekturami textu.

OBSAH

ÚVOD

V posledních letech dochází ke značnému rozvoji využívání Internetu. V začátcích většina domácností využívala vytáčené připojení pomocí pevné linky. Takové připojení bylo účtováno na základě minutové tarifikace. Nevýhodou tohoto řešení bylo, mimo jiné, nutnost platit paušální poplatek za pevnou linku. Po technické stránce často docházelo k velmi zdlouhavým opakovaným pokusům o připojení a pádům spojení během komunikace.

Se vzrůstající poptávkou domácností i podniků po řešení připojení k Internetu začaly vznikat regionální firmy zabývající se poskytováním datových služeb. Základní myšlenkou bylo nakoupení konektivity a její distribuce uživatelům v bytových a rodinných domech. To se poměrně snadno realizovalo pomocí bezdrátových pojítek provozovaných v nelicencovaných pásmech. Bylo tak možné nabídnout rychlejší přístup do Internetu za paušální poplatek. Uživatel se tedy mohl připojit kdykoliv bez nutnosti navazovat zdlouhavá spojení a bez nutnosti využívání uživatelských účtů. Takové služby byly ve městech poskytovány za paušál okolo 300,- Kč měsíčně. Rychlosti připojení po roce 2000 se pohybovaly od 128 kb/s s agregací cca 1:30. Rychlosti se postupně navyšovaly, mnohdy i několinásobně během jednoho roku, za stejných cenových podmínek.

Postupem času začalo docházet k zahlcení pásma 2,4 GHz z důvodu velkého počtu poskytovatelů. Dalším důvodem bylo připojování stále většího počtu objektů, přičemž počet využitelných kanálů je omezený. Docházelo k častému rušení mezi instalovanými zařízeními a služby se stávaly nespolehlivými. Bylo nutné hledat jiná řešení. Tím mohla být instalace spojů pracujících v licencovaném pásmu alespoň na důležitých páteřních trasách. Cenová nedostupnost byla mnohdy řešena formou pronájmu zařízení od jiné společnosti. Druhou možností v této situaci bylo využití bezdrátových optických sítí, které nabízely vyšší přenosovou rychlost, nízkou odezvu, nízkou ztrátovost a byly finančně dostupné. Zařízení však pracovala pouze do vzdálenosti zhruba jednoho kilometru a měla nízkou spolehlivost při zhoršených klimatických podmínkách.

Další rozvoj přinesla lepší cenová dostupnost pojítek v nelicencovaném pásmu 5 GHz. Částečně se tak uvolnilo přehlcené a zarušené pásmo 2,4 GHz. S dalším širším nasazením těchto pojítek se situace do značné míry opakovala. Dále se instalovaly spoje v nelicencovaném pásmu 10 GHz a opět spoje v pásmu licencovaném jako páteřní trasy k zajištění dostatečné kvality služeb.

V současnosti dochází k neustálému navyšování rychlostí a požadavků klientů. Lokální poskytovatelé služeb jsou nuceni držet krok s konkurencí, tedy firmami nabízejícími služby v rámci celé ČR založené na DSL, s mobilními operátory, poskytovateli kabelové TV a v neposlední řadě s konkurencí lokálního charakteru. Řešením této situace je především výstavba vlastních optických sítí a provozování služeb na této technologii. Způsob, jakým lze k výstavbě takové metropolitní sítě v krajském městě nahlížet, je předmětem této práce.

I. TEORETICKÁ ČÁST

1 BEZDRÁTOVÉ SÍTĚ

1.1 Prvky bezdrátových sítí

Každá bezdrátová síť se skládá z několika základních prvků. Jedná se o vlastní aktivní prvek například v režimu směrovače, přístupového bodu, přemostění. Podmínkou funkce je zajištění napájení odpovídajícím zdrojem a v případě nutnosti zajištění provozní spolehlivosti také doplněním o záložní zdroj. Prvky jsou dále vybaveny anténami a propojeny odpovídající kabeláží.

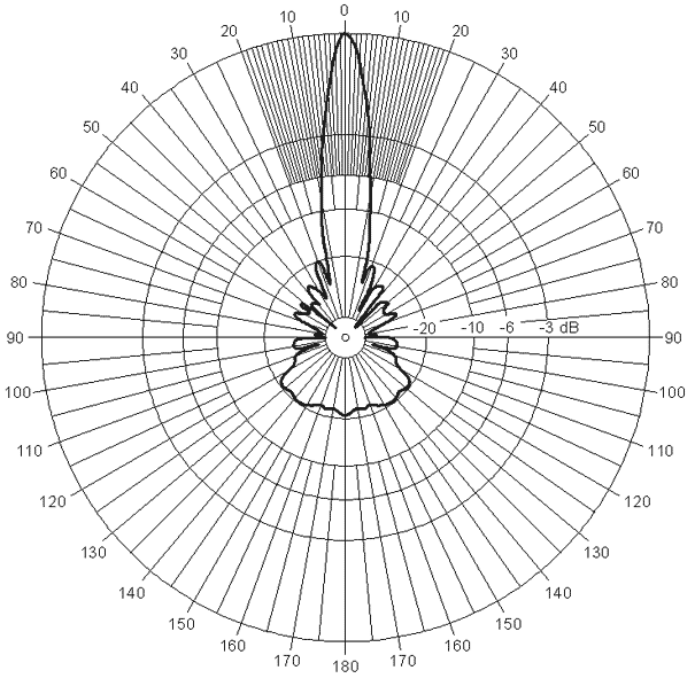
1.1.1 Antény, kabeláž, konektory

Antény můžeme dělit z několika hledisek (jedno z možných nekonvenčních dělení z pohledu poskytovatele datových služeb):

- Typ konstrukce, rozsah frekvenčního pásma.
- Podle zisku - ziskem antény se rozumí zesílení výkonu, které měříme v dBi, v dB (Decibel) vztažených k izotropnímu zářiči ve všech směrech [2].
- Podle charakteru vyzařování (vyzařovacího úhlu): udává tvar vyzařovacího diagramu. Může být trojrozměrný, tedy s vertikální i horizontální rovinou [2].

Rozsah frekvenčního pásma je vybírán s ohledem na použití konkrétního aktivního prvku. Z hlediska charakteru vyzařování pak využíváme antény všesměrové, směrové a sektorové. Všesměrové antény naleznou využití především u malých domácích směrovačů, přípojných bodů v rámci vnitřních prostor komerčních objektů, k pokrytí prostor hotelů, zahrádek restaurací apod. Ke kvalitnímu pokrytí signálem pro několik vzdálených objektů se všesměrové antény nevyužívají. Důvodem je nízká úroveň získaného signálu, která souvisí také s předepsaným omezením maximálního vysílaného výkonu připojených prvků. V městské zástavbě dále není vhodné využívat všesměrové antény z důvodu zbytečného zahlcení kanálů, jichž je omezený počet.

Sektorové antény se s oblibou používají právě k pokrytí určité lokality nebo části ulice, tedy sektoru, ve kterém se nacházejí klienti. Výrobci u těchto antén udávají vyzařovací úhel, podle kterého můžeme výrobek v konkrétních podmínkách využít. Anténa směrová najde uplatnění především u spojů typu bod-bod, kde potřebujeme dosáhnout vyšší úrovně signálu mezi dvěma, mnohdy více vzdálenými, objekty. Výhodou je, že opět nedochází k nežádoucímu zahlcení kanálu ve velkém prostoru (úhlu).



Obr. 1. Vyzařovací diagram [9].

1.1.2 Napájené prvky

Jedná se o zařízení bezdrátových sítí pracující v režimu přístupových bodů, klientských stanic, nebo přemostění. V současnosti provozovatelé datových služeb využívají především zařízení, která jsou integrována v boxu uzpůsobeném pro venkovní prostředí. Tento box zároveň obsahuje anténu. Takové řešení je vhodné zejména pro realizaci koncové přípojky. Ta může být určena pro jednoho klienta v rodinném domě, nebo se může jednat o koncovou přípojku pro celý objekt, např. panelový dům na sídlišti.

Obr. 2. Outdoor box 19 dBi [10].

Výhodou takového řešení je vedení pouze datového kabelu z místní domovní sítě k anténě. Nemusí se tak řešit problematické vedení koaxiálního kabelu, na kterém vždy vzniká nechtěný útlum. Výhodou této instalace v bytových domech je také skutečnost, že nevznikají nároky na umístění technologií ve společných částech domu a zařízení jsou tak lépe chráněna proti odcizení, nebo vandalismu. K výše popsaným účelům se používá zařízení známé jako RouterBOARD v licenci MikroTik v různých modifikacích.

Obr. 3. RouterBOARD 433 v licenci MikroTik [11].

1.1.3 Směrovače pro domácnosti a kanceláře

Koncovou klientskou přípojku je možné dovybavit malým směrovačem. Výhodou takového řešení je pokrytí celého bytu, podlaží rodinného domu, nebo kanceláře bezdrátovým signálem. K těmto zařízením se mohou připojovat především notebooky, chytré mobilní telefony, tablety apod. Bezdrátovým rozhraním lze vybavit i pevný počítač pomocí adaptéru do slotu PCI (Peripheral Component Interconnect), případně adaptérem přes USB (Universal Serial Bus) rozhraní.

Tyto směrovače pracují většinou na frekvencích v nelicencovaném pásmu 2,4 GHz (Gigahertz) a 5 GHz podle standardu 802.11. Jsou vybaveny všesměrovými anténami se ziskem zpravidla okolo 5 dBi. V provedení s jednou anténou umožňují dosáhnout podle použité normy teoreticky rychlost až 150 Mb/s (Megabit za sekundu). V případě nutnosti pokrytí komerčních prostor, jako jsou provozy restaurací, kaváren apod., kde dochází k připojování více klientů, je vhodnější použít jiná zařízení [5].

Obr. 4. Směrovač Tenda W311 R+ [12].

1.1.4 Napájecí zdroje, PoE prvky, zálohování

Bezdrátové aktivní jednotky je třeba napájet vhodnými zdroji elektrické energie. Většina používaných zařízení je konstruována na malé stejnosměrné napětí (běžně hodnoty cca 12-24 V). Pro koncové přípojky je vhodné použití tzv. PoE (Power over Ethernet) napájecích zdrojů. Výhodou tohoto řešení je využití jediného kabelu pro data a současně pro napájení. To je realizováno tak, že je běžný UTP (Unshielded Twisted Pair) kabel se čtyřmi páry vodičů „rozdělen“ na dvě části. Po dvou párech je realizována datová komunikace, jeden pár pak slouží pro kladné a druhý pro záporné napětí. Značná část prodávaných aktivních prvků je PoE rozhraním vybavena. Jedná se o konektor RJ-45 s tímto označením a příslušným přizpůsobením hardware výrobce. Samotný zdroj je pak vybaven dvěma shodnými konektory. Jedním pro ethernetový kabel označeným LAN a druhým pro připojení aktivního prvku označeným PoE.

Obr. 5. Napájecí zdroj PoE 48 V [13].

Na uzlových bodech je nutné zálohování pro případ výpadků elektrické energie. Využívají se k tomu speciálně určené záložní zdroje. Výhodou jsou poměrně kompaktní rozměry a

přijatelná cena. Mezi hlavní nevýhody, především levnějších výrobků, patří omezená doba napájení ze záložní baterie, která bývá nastavena výrobcem na konkrétní délku. Takový záložní zdroj pak pracuje například pouze deset minut, i když ještě nebylo využito veškeré dostupné kapacity připojeného akumulátoru. Nepomůže ani možnost kalibrace.

Vhodnějším řešením pak je využití měniče napětí a připojení akumulátoru libovolné kapacity. To je realizováno propojením měniče stejnosměrného napětí 12 V na napětí střídavé 230 V a bezúdržbových akumulátorů s požadovanou kapacitou. Takto lze zálohovat uzlové body na dobu dlouhou v řádu několika hodin. Při provozování rozsáhlé sítě, nebo významného uzlového bodu s umístěním serverů, či jiných strategicky důležitých zařízení, je vhodné zajistit možnost nasazení agregátu, který musí být konstruován s ohledem na požadavky těchto zařízení. V opačném případě by mohlo docházet k výpadkům za provozu, nebo dokonce k poškození zařízení.

Obr. 6. Měnič 12/230V [14].

1.2 Spoje v nelicencovaném pásmu

Zde se jedná o bezdrátová zařízení provozovaná na základě generální licence ČTÚ (Český Telekomunikační Úřad). Tyto prvky pak může provozovat každý, kdo splní podmínky této generální licence. V podmínkách nalezneme především specifikaci použitelných zařízení, přehled (frekvencí) kanálů, maximální vysílací výkony apod. Výhodou je skutečnost, že za provozování takových zařízení se neplatí žádný poplatek. Nevýhodou je především to, že na stejné frekvenci (stejném kanále) může vysílat kdokoliv jiný a naši komunikaci tím může rušit, nebo zcela potlačit. Z pohledu poskytovatelů datových služeb jsou nejvýznamnější prvky pracující v pásmech 2,4 GHz a 5 GHz, dle standardu 802.11.

1.2.1 Standard 802.11

Specifikace standardu 802.11 byla přijata v roce 1997. Bylo počítáno s přenosovou rychlostí 1, nebo 2 Mb/s. Protokol pracoval s fyzickou a linkovou vrstvou modelu OSI (Open Systems Interconnection) [1].

Jak uvádí Barken [1], na úrovni druhé vrstvy definoval standard 802.11 následující služby:

- Autentizace a deautentizace.
- Asociace, disasociace a reasociace.
- Privátnost (WEP).
- Doručování MSDU (Mac Service Data Unit).

Na vrstvě fyzické byly dle Barkena [1] definovány tyto tři metody:

- DSSS (Direct Sequence Spread Spectrum).
- FHSS (Freguency Hopping Spread Spectrum).
- Infračervený přenos.

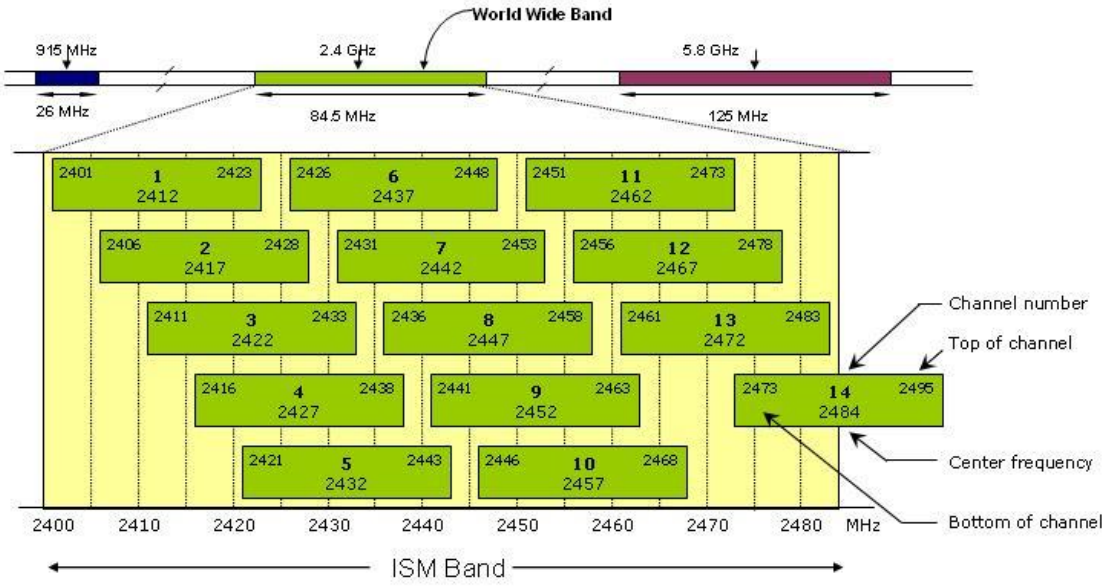
V roce 1999 byly vydány dva doplňky 802.11a a 802.11b, v roce 2003 pak 802.11g. Základní parametry jednotlivých protokolů jsou shrnuty v následující tabulce:

Tabulka 1. přehled parametrů jednotlivých protokolů 802.11 [2].

Protokol	Rok vydání	Max. rychlost	Frekvence	Modulace	Šířka kanálu
802.11a	1999	54 Mb/s	5 GHz	64 QAM	20 MHz
802.11b	1999	11 Mb/s	2,4 GHz	11 CCK	20 MHz
802.11g	2003	54 Mb/s	2,4 GHz	64 QAM	20 MHz
802.11n	2009	65-600 Mb/s	2,4 nebo 5 GHz	64 QAM	20 a 40 MHz
802.11ac	2012	78 Mb/s - 3,2 Gb/s	5 GHz	256 QAM	20, 40, 80 a 160 MHz

1.2.2 Technologie DSSS

Tato technologie podporuje vyšší přenosové rychlosti, než jak je tomu u FHSS. Obě technologie využívají rozprostřené spektrum. To spočívá v tom, že se přenášený signál „rozprostře“ do několika přenosových frekvencí (frekvenčního spektra). Díky tomuto řešení se zvyšuje odolnost k rušení. Problémem se může zdát skutečnost, že dochází k neefektivnímu využívání kmitočtů. Rozložení třinácti kanálů používaných v Evropě, včetně uvedení střední frekvence, je patrné z následujícího obrázku [1].



Obr. 7. Rozložení kanálů v pásmu 2,4 GHz [15].

1.3 Spoje v licencovaném pásmu

Jedná se o bezdrátové spoje, k jejichž provozu je potřeba získat licenci od ČTÚ. Jedná se o přidělení kmitočtu pro konkrétní zařízení, které plánuje poskytovatel datových služeb provozovat. Povolení se váže vždy k lokalitě uvedené v žádosti, aby bylo zajištěno nerušené využití kmitočtu držitelem licence. Jiný zájemce tak nemůže logicky obdržet licenci se shodnými parametry. Licence se přiděluje za určitý paušální (zpravidla měsíční) poplatek. Příkladem spojů v licencovaných pásmech jsou zařízení pracující na těchto kmitočtech: 3,5; 7; 11; 13; 15; 18; 23 GHz atd.

1.4 Bezpečnost bezdrátových sítí

Bezdrátovou síť poskytovatele datových služeb je nutné vhodným způsobem chránit proti neoprávněnému přístupu. Do sítě by se mohly připojovat subjekty, které za danou službu nemají zaplaceno a vznikala by tak škoda poskytovateli připojení. Dále je toto opatření potřebné z hlediska zabránění narušení bezpečnosti soukromí při přenášení dat od jednotlivých uživatelů v síti. Požadavků na zabezpečení bezdrátových sítí ze strany klientů neustále přibývá, neboť dříve běžné pevné drátové připojení do místních LAN (Local Area Network) sítí je z velké části nahrazeno používáním Wi-Fi směrovačů v domácnostech a v kancelářích.

Naopak páteřní spoje poskytovatelů internetových služeb byly z velké části tvořeny bezdrátovými pojítky v licencovaných nebo nelicencovaných pásmech. V dnešní době je zájem nahrazovat tato spojení optickými vlákny, kde je zabezpečení poněkud jednodušší.

Donedávna bylo nejběžnějším způsobem zabezpečení metodou WEP, později WPA a v současnosti se využívá zabezpečení WPA2. V dalším textu budou jednotlivé druhy zabezpečení a útoků podrobně popsány.

1.4.1 SSID

Jedná se o označení – identifikaci sítě (Service Set IDentifier). Klient se může připojit pouze k síti, jejíž SSID zná. SSID se používá pro identifikaci všech prvků. Každý takový prvek vysílá informace o svém identifikátoru v určitých časových intervalech v otevřené formě. Aktivní prvky ve svém managementu sice nabízejí možnost skrytí SSID, ale jedná se o opatření, které lze poměrně snadno obejít. Narušitel pošle falešný požadavek na odpojení skutečné aktivní stanice, ta se pak musí znovu připojit pomocí provozních dotazů probe a associate, ze kterých lze SSID zjistit [2].

1.4.2 WEP

Jde o dnes již nevhodné zabezpečení bezdrátové sítě (Wired Equivalent Privacy), které bylo vytvořeno a standardizováno v roce 1997. Tento druh zabezpečení byl však v roce 2001 prolomen z důvodu neúplnosti standardu a bylo nutné využít jiné typy. Z hlediska modelu OSI pracuje WEP na linkové vrstvě. Šifrovány jsou jednotlivé přenášené rámce. Využívá se přitom proudová šifra RC4. Výhodou je, že není nutné měnit stávající aplikace a přenosové protokoly [1], [2].

Je zde používán 40 bitový klíč spolu se 24 bitovým inicializačním vektorem. Celkově tak tvoří 64 bitový klíč. Je možné se také setkat se 128 a 256 bitovým klíčem. Byly také snahy nahradit WEP, respektive jej zdokonalit. Jedná se o zabezpečení WEPplus (WEP+) a WEP2. Nevýhodou WEPplus je, že pokud není využíván všemi zúčastněnými uživateli, nepřináší žádnou výhodu oproti klasickému WEP [1], [2].

1.4.3 WPA

V roce 2001, kdy byl prolomen WEP, bylo nutné najít jiné řešení. Popsáno bylo v roce 2002 jako WPA (Wi-Fi Protected Access). Hlavní podmínkou bylo, aby byl stávající hardware

použitelný i s novým typem zabezpečení. Aby byla odstraněna slabá místa dřívějších inicializačních vektorů používaných u WEP, došlo k vývoji protokolu TKIP (Temporal Key Integrity Protocol). Byla zavedena dynamická správa šifrovacích klíčů. Data byla přenášena zabezpečeně nejen na začátku, ale i během komunikace [1], [2].

U starších bezdrátových karet bylo nutné nainstalovat v operačním systému nové aktualizace ovladačů, případně aktualizovat firmware. Autentizace probíhá pomocí PSK (Pre-shared Key), případně je prováděna samostatným serverem - většinou v případě podnikových informačních systémů. Šifrování u WPA probíhá za pomoci 128 bitového klíče spolu se 48 bitovým inicializačním vektorem. U tohoto druhu zabezpečení je také lépe zvládnuta kontrola integrity dat. Využívá se k tomu metoda MIC (Message Integrity Code). Při používání metody WPA současně s TKIP není velkým problémem zabezpečení prolomit [1], [2].

1.4.4 WPA2

Pro zajištění ještě vyšší bezpečnosti bylo přistoupeno k vytvoření této metody. WPA2 muselo integrovat veškeré povinné součásti vycházející ze standardu IEEE 802.11i. To je docíleno tím, že k výše popsanému protokolu TKIP a MIC přidává algoritmus CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Ten využívá symetrickou blokovou šifru AES (Advanced Encryption Standard). V dnešní době je WPA2 povinné pro všechna vyráběná Wi-Fi zařízení) [1], [2].

1.4.5 Útok man-in-the-middle

Narušitel využívá tento typ útoku pro odcizení části komunikace a vložení vlastního obsahu. Toho může docílit pomocí škodlivého software (malware). Jak napovídá název, útočník se „postaví“ mezi klienta a přístupový bod. Pomocí odposlechu jejich komunikace zjistí Mac adresy. Dále může s těmito falešně získanými adresami komunikovat. Útočník pak vypadá pro přístupový bod jako korektní klient a naopak [2].

Tento typ útoku se provádí na fyzické nebo spojové vrstvě WLAN (Wirelles LAN). V případě fyzické vrstvy jde o zarušení konkrétního kanálu, případně zahlcení přístupového bodu jiným provozem. V tomto případě se jedná o tzv. jamming. Útok na druhé vrstvě je založen na falešném odhlášení ze sítě [2].

1.4.6 Útok typu DoS

K útoku vedoucímu k odepření služby jsou bezdrátové radiové sítě z principu poměrně dosti náchylné. Omezení služeb může být částečné, nebo v horším případě úplné. Proti tomuto typu útoku (s ohledem na návrh 802.11) neexistuje dostatečné opatření k zabezpečení na fyzické a v některých případech ani na spojové vrstvě [2].

Jak uvádí Pužmanová [2], k běžným útokům tohoto charakteru patří:

- Jamming.
- Záplava rámců pro odpojení ze sítě.
- Falešné chybové autentizační rámce.
- Chybějící šifrování a ochrana integrity pro rámce managementu.
- Přeplnění bufferu AP (přetečení vyrovnávací paměti a pád běhu AP).
- Útoky s ohledem na specifická nastavení WLAN (rámce pro spící klienty).

1.4.7 Vyhodnocení zabezpečení bezdrátových sítí.

Na základě výše uvedených charakteristik je v případě bezdrátového zabezpečení možné doporučit pouze metodu WPA2, která dostatečně chrání bezpečnost přenášených dat a samotný přístup do bezdrátové sítě. Výhodou je, že současné operační systémy jsou kompatibilní právě s tímto druhem zabezpečení. Stejně tak bezdrátová zařízení jsou dodávána s podporou tohoto standardu. Odpadají tak případné náklady a komplikace spojené s vlastními řešeními různých výrobců, jak tomu bývá u jiných zařízení v informačních systémech.

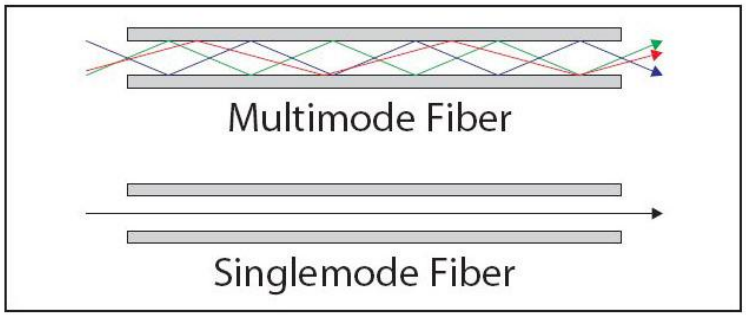
2 OPTICKÉ SÍTĚ

Použití optických sítí je mezi poskytovateli datových služeb stále častější. Hlavní výhodou je možnost přenosu signálu na delší vzdálenosti díky nízkému útlumu. Lze realizovat přenos větších objemů dat s vysokou rychlostí - až jednotky Tb/s (Terabit za sekundu). Výhodou je také úplná odolnost optických vláken k elektromagnetickému rušení. Z pohledu instalace je optické vlákno vhodné pro nízkou hmotnost a malé rozměry (průměr vodiče). Základním modelem optické sítě jsou tři prvky. Jedná se o vysílač – zdroj signálu, přenosové medium, tedy optické vlákno a přijímač signálů - detektor [6].

2.1 Prvky optických sítí

2.1.1 Základní princip optického vlákna

Prostředí optického vlákna je v principu dielektrikum a signál se šíří prostřednictvím vidů. Počet vidů závisí na průměru jádra vlákna a na vlnové délce záření. Podle počtu vidů rozlišujeme vlákna jednovidová (vláknem se šíří pouze jeden vid) a vlákna mnohavidová (vláknem se šíří stovky až tisíce vidů). Optická vlákna dále můžeme dělit podle materiálu použitého k jejich výrobě na skleněná z materiálu SiO_2, která mají skleněné jádro i plášť. Dále plastová - s plastovým jádrem i pláštěm a hybridní se skleněným jádrem a plastovým pláštěm [6].



Obr. 8. Šíření vidů ve dvou typech vláken [16].

2.1.2 Optické vlákno jednovidové

Jednovidové optické vlákno SM (Singlemode) bylo využíváno především k přenosům na delší vzdálenosti. Nyní jsou tato vlákna využívána i v metropolitních sítích, případně ke kratším spojům. Jedná se o kvalitativně lepší produkt oproti vláknům mnohavidovým.

2.1.3 Optické vlákno mnohavidové

Jedná se o vlákna vyrobená ze skla, nebo plastu, jejichž prostřednictvím je vedeno světlo přenášející potřebné signály. Vlákna mnohavidová MM (Multimode) se obecně používají na kratší vzdálenosti, tedy na propojení v rámci objektu, případně na propojení budov v areálu apod. Tato vlákna jsou zpravidla cenově dostupnější.

2.1.4 Spojování optických vláken

Optická vlákna lze spojovat pomocí konektorů, svařováním, nebo opatřit mechanickou spojkou. Nejčastějším způsobem spojování je svařování pomocí svářečky optických vláken. Před vlastním svářením je nutné zbavit optický kabel primární ochrany i sekundární izolace na jednotlivých vláknech. Dalším krokem je precizní očištění vláken a přesné seříznutí pomocí zalamovačky.

Obr. 9. Zalamovačka optických vláken [17].

Dva takto upravené konce je možné vložit do svářečky, která se postará (dle výbavy) o přesné vycentrování vláken proti sobě a provede vlastní svár. Na displeji svářečky se objeví hodnota dosaženého útlumu sváru a provede se zkouška pevnosti v tahu. Posledním krokem je opatření nově vzniklého sváru ochranou proti mechanickému poškození. Ochrana v podobě plastové trubičky je zatavena na svár pomocí pícky, která bývá součástí svářečky.

Obr. 10. 3D svářečka optických kabelů [18].

Optická vlákna se také opatřují konektory. Při zapojování je nutné precizní vyleštění dosedacích plošek konektorů. Mezi nejběžněji používané typy patří konektory označované jako LC, SC, FC, ST u skleněných vláken a SC, SMA u vláken plastových [6].

2.1.5 Mechanická ochrana optických kabelů

Při ukládání optických vláken do volného terénu (při výkopových pracích) je nutné kabeláž vhodným způsobem chránit proti mechanickému poškození. K tomu se využívají chráničky optických kabelů. Jedná se o silnostěnné, většinou plastové trubky různých průměrů. V rámci objektů a na menší vzdálenosti se využívají také tzv. mikrotrubičky. Ty mohou být silnostěnné i tenkostěnné. Běžně se setkáme například s údajem 12/8 tedy s označením vnějšího a vnitřního průměru v milimetrech.

Vnitřní povrch bývá přizpůsoben tak, aby umožnil snadnější umístění optického vlákna do této chráničky. To se provádí zafukováním, kdy je do chráničky vháněn pomocí kompresoru vzduch a současně je vtlačováno optické vlákno. Díky vháněnému vzduchu dochází k menšímu tření mezi vláknem a vnitřním povrchem chráničky a je tak možno zafukovat kabely na poměrně velkou vzdálenost.

2.1.6 Optické přepínače

Přepínače v optických sítích můžeme rozdělit podle toho, zda pracují s čistě optickým signálem, nebo převádějí optický signál na elektrický, který pak zpracovávají. Nejběžnější je využívání právě přepínačů typu OEO (Optical-Electrical-Optical). Je snaha vyvíjet celoop-

tické přepínače typu OOO (Optical-Optical-Optical), čímž by se předešlo zpoždění ve zpracování signálu z důvodu zařazení prvku OEO. Prvky OOO zatím nejsou cenově příliš dostupné pro běžné nasazení [6].

V praxi se běžně používají moduly k převodu optického signálu na elektrický. Nejčastěji v provedení s označením GbIC (Gigabit Interface Converter). Jde o malý modul, který je možné vložit do běžného přepínače pro metalickou síť, pokud je k tomu uzpůsoben. Do tohoto modulu je pak možné připojit optické vlákno pomocí konektoru. Dalším řešením je použití media konvertoru. Jedná se o modul vybavený rozhraním RJ-45 a rozhraním pro připojení optického vedení.

Obr. 11. Media konvertor optika/RJ-45 [19].

2.2 Pasivní optické sítě

V současné době dochází k rozvoji využívání pasivních optických sítí PON (Passive Optical Network) jako prvku poslední míle. Jde tedy například o využití optického vlákna k připojování jednotlivých klientů v rámci bytového domu. Toto řešení bývá označováno jako FTTH (Fiber To The Home). Název pasivní optická síť vychází z toho, že mezi zařízeními poskytovatele v jeho síti a koncovým rozhraním klienta není využito aktivních prvků. Přepínače jsou v tomto případě tedy plně pasivním, elektricky nenapájeným zařízením [6].

PON se skládá vždy z několika prvků. Jedná se o zakončení optického vedení - OLT (Optical Line Termination) na straně ústředny. K těmto zakončením jsou připojovány optické přepínače, ke kterým můžeme dále připojovat koncové uživatele až do vzdálenosti několika desítek kilometrů. Koncová jednotka je nazývána jako ONU (Optical Network Unit). Koncová jednotka ONU může přizpůsobit optické vedení na elektrický signál (například pro rozhraní

Ethernet). Obdobným způsobem se připojují také jednotky ONT (Optical Network Termination) [6].

Z pohledu poskytovatele datových služeb přijdeme nejčastěji do styku se sítěmi založenými na časovém dělení multiplexu – TDM (Time Division Multiplex). Pak rozlišujeme několik typů PON [6]:

- APON
- GPON
- EPON
- Další varianty (10G-EPON, 10G-PON, XG-PON).

2.3 Aktivní optické sítě

Sítě AON (Active Optical Network) využívají mezi prvky OLT a ONU/ONT aktivní zařízení. Jedná se o elektricky napájené přepínače. Z tohoto faktu vyplývá určitá nevýhoda těchto sítí, tedy nutnost elektrického napájení zařízení, která jsou umístěna na trase mezi koncovým klientem a technologií poskytovatele služeb. Výhodou AON je lepší možnost zabezpečení [6].

2.4 Bezdrátové optické sítě

Jedná se o bezdrátové sítě založené na FSO (Free Space Optic). Využívají se v metropolitních sítích k propojení objektů vzdálených do jednoho kilometru. Podmínkou jejich nasazení je přímá viditelnost mezi přípojnými body. Nevýhodou je především nefunkčnost při zhoršených klimatických podmínkách, tedy v situacích kdy dojde k narušení přímé viditelnosti (mlha, sníh, hustý déšť). Výhodou je vysoká odolnost k bezpečnostním hrozbám, nízká odezva a nízká ztrátovost [2].

Bezdrátové optické sítě byly nasazovány v některých městech především v období, kdy většina poskytovatelů datových služeb využívala spoje v pásmu 2,4 GHz. Využití FSO představovalo konkurenční výhodu, neboť bylo možné nabídnout o řád vyšší rychlost. Vhodné bylo spoje FSO zálohovat bezdrátovými pojítky s ohledem na zmíněné nedostatky. S dalším rozvojem bezdrátových i optických sítí a jejich cenové dostupnosti se technologie FSO příliš neuplatňuje.

2.5 Bezpečnost PON

Jak bylo uvedeno výše, v současnosti je u poskytovatelů datových služeb tendence k nahrazování bezdrátových radiových pojítek optickými vlákny. Jednou z výhod tohoto řešení je lepší možnost zabezpečení a eliminace odposlechu na takových sítích. Z hlediska bezpečnosti je vhodné optické sítě rozdělit na dvě skupiny. První z nich jsou PON a druhou AON. Při zabezpečení narážíme na více specifických problémů v první skupině, tedy u sítí pasivních. Následující text tak bude zaměřen především na tuto skupinu.

V minulosti bylo již celkem běžné propojit nejdůležitější páteřní spoje poskytovatelů služeb optickými vlákny. Jednalo se především o propojení mezi aglomeracemi a vybudování několika přípojek v rámci metropolitní sítě, například přivedení optického vlákna na každé sídliště ve větším městě. Zde pak byly služby distribuovány bezdrátově.

Naproti tomu v současnosti se připojují už i jednotlivé bytové domy, nebo dokonce jednotlivé domácnosti a kanceláře za pomoci optických technologií. Tím se dostává otázka bezpečnosti těchto sítí do popředí zájmu poskytovatelů i klientů. Samotná bezpečnost uživatelů na síti je již uspokojivě vyřešena pomocí zabezpečených přenosů typu SSL (Secure Socket Layer) apod [6].

Problémem pro poskytovatele služeb zůstává například možnost odposlechu na síti a podvržení vlastního obsahu přenášených dat. U optické sítě odpadá možnost pasivního odposlechu, jako je to možné provádět u metalických vedení. Stejně tak odpadají rizika známá u nezabezpečených, nebo nevhodně chráněných bezdrátových sítí, jak již bylo zmíněno.

Jak uvádí Rohlík a Lafata [3]: *"Nejzávažnější problém představuje samotná architektura sítě, kdy všechny optické síťové jednotky či zakončení ONU/ONT (Optical Network Unit/Termination) sdílejí navzájem část optické distribuční sítě ODN (Optical Distribution Network)."*

Kapacita pro oba směry pro přenos dat je sdílena pomocí časově sdíleného přístupu. Do veškerých koncových zařízení jsou multirámce v sestupném směru distribuovány pasivními optickými prvky – přepínači. Koncové zařízení si pak převezme pouze tu část rámce, která je určena pro něj samotné. Toto je zařízeno informací o konkrétních koncových jednotkách, která je obsažena v záhlaví všech datových skupin. Tyto informace jsou v sestupném směru vždy šifrovány (například již uváděným standardem AES) [3].

Ve směru od koncových zařízení k přepínači a dále například k serveru, tedy ve směru vzestupném, je nutné zabezpečit, aby nedocházelo ke kolizím mezi koncovými prvky. Fyzický přístup k serveru daného poskytovatele služeb bývá znemožněn jejich bezpečným umístěním na chráněném místě. U optických síťových jednotek však tato výhoda „zabezpečení umístěním“ odpadá. Z hlediska poskytovatele je koncový bod u zákazníka volně přístupným místem a kdokoliv může provést případný útok. Stejně tak tomu je v případě volných a nezakončených optických výstupů přepínačů ve společných prostorách domů apod [3].

2.5.1 Nejčastější bezpečnostní hrozby

Přehled nejčastějších bezpečnostních hrozeb [3]:

• Útok odepření služby DoS (Denial of Service).

• Odposlech (odposlech služebních zpráv, odposlech uživatelských dat v obou směrech).

• Maskování (spoofing, masquerading).

2.5.2 Útok typu DoS

Při tomto útoku nedochází k odcizení nebo pozměňování dat jako v ostatních případech. Útok je zaměřen na odepření služby. Snahou útočníka je tedy znemožnit funkčnost služby, nebo celé sítě poskytovatele konečnému zákazníkovi. Toho je možné docílit právě připojením z koncového bodu, kdy je narušen časový rámec, který byl danému zařízení přidělen a dochází tak ke vzniku kolizí, případně k úplné nefunkčnosti sítě. Takový bod je v síti obtížně dohledatelný a musí se přistoupit k odpojování jednotlivých okruhů od větších uzlů po koncové přípojky [3].

Odpojování těchto úseků je možné provést pomocí speciálních spojek. Nevýhodou využívání těchto spojek je, že musí být po použití opět zprůchodněny manuálně obsluhou přímo v místě instalace. Aktivace spojky naproti tomu proběhne automaticky. Z hlediska provozních nákladů je výhodné toto zařízení využívat, neboť je pasivní a nepotřebuje napájecí zdroj [3].

2.5.3 Odposlech služebních zpráv

Při komunikaci mezi prvky v pasivní optické síti jsou šifrována pouze uživatelská data. Záhlaví, které obsahuje služební a řídící zprávy již nikoliv. U dříve popsaného řešení optických sítí mají veškerá koncová zařízení přístup ke všem přenášeným datům. Koncové zařízení vybírá na základě služebních dat pouze ty segmenty, které jsou mu určeny. Toto lze obejít a

získat na koncovém zařízení veškerá data. Útočník tak může získat veškerá data uživatelská v šifrované podobě a nešifrované služební zprávy. Data je pak možno analyzovat na vyšších vrstvách modelu OSI. Analýzou služebních zpráv může útočník získat cenné informace o provozních zvyklostech na části i na celé optické pasivní síti. Má totiž v tomto okamžiku přehled o každém aktivním zařízení, především o jeho identifikátoru a informace o časovém rámci určeném k vysílání konkrétní jednotky. Útočník nyní může vydávat svou nelegálně připojenou jednotku za tu, jejíž identifikační údaje popsaným způsobem získal. Tomuto nelegálnímu chování v síti se říká maskování (masquerading) [3].

2.5.4 Odposlech odchozích dat uživatelů

Pasivní optická síť je navržena tak, aby byly veškeré informace ve směru od koncové k centrální jednotce šířeny pouze mezi těmito dvěma zařízeními. Nemělo by tak docházet k situaci, kdy k uvedeným datům mají přístup také ostatní koncová zařízení. Nedokonalostmi při návrhu a výstavbě pasivní optické sítě může dojít k situaci, kdy vznikají odrazy. Vzniklý odraz se pak šíří sestupným směrem ke všem jednotkám a na všechna zakončení, což přináší již uvedená rizika odposlechu. Tyto odrazy nelze analyzovat běžnou jednotkou, která pracuje na jiných vlnových délkách. Většina odrazů nemá dostatečnou úroveň k tomu, aby mohly být správně vyhodnoceny, přesto je nutné se touto možností odposlechu důsledně zabývat při realizaci a provozu sítě [3].

Zásadní nebezpečí je v tom, že data odesílaná od koncové jednotky k serveru nejsou nijak šifrována a fakt, že pasivní odposlech není možné nijak detekovat [3].

2.5.5 Odposlech příchozích dat uživatelů

Odposlech v tomto směru je možné provádět opět pasivně přes připojenou koncovou jednotku, která nelegálně získala cizí identifikátor. Samotnou část rámce s datovým souborem není možné dešifrovat. Data jsou zabezpečena pomocí AES, jež není možné v této době prolomit. Řešením je získání klíče při odposlechu dat odchozích. Pak lze i příchozí data dešifrovat [3].

2.5.6 Vyhodnocení bezpečnostních rizik v síti PON

V předešlých odstavcích byly popsány nejčastější bezpečnostní hrozby u pasivních optických sítí. Ty jsou dány především topologií a funkcí této sítě, kdy jsou veškerá data ve směru

od serveru ke koncovým uživatelům odesílána ke všem jednotkám celou sítí. V těchto rámcích jsou šifrována pouze data uživatelská a nikoliv provozní. Ve směru od koncových jednotek k serveru pak data nejsou šifrována vůbec.

Z těchto skutečností vyplývá nutnost pro všechny poskytovatele služeb se důsledně zabývat všemi bezpečnostními hrozbami při návrhu pasivní optické sítě, při její realizaci i při samotném provozu. Je však především nutné zvážit, zda optickou síť vůbec realizovat tímto způsobem s ohledem na uvedené hrozby. Z hlediska bezpečnostního není možné tuto realizaci doporučit jako nejvhodnější. Při rozhodování se poskytovatelé zabývají mimo jiné technickou a ekonomickou stránkou, kde mají pasivní optické sítě své výhody.

3 SÍTĚ LAN

Domovní sítě LAN stavěné za účelem poskytování datových služeb se realizují nejčastěji pomocí metalického vedení. Jako vodič se používá kabel UTP.

3.1 Síťové prvky

3.1.1 Kabeláž, konektory, spojky

Vedení jsou realizována pomocí kabelu označovaného jako UTP, který se skládá z osmi vodičů kroucených do čtyř párů. Kabely jsou označovány číslem kategorie. Nyní se nejčastěji používá UTP kategorie 5e a vyšší. Pro instalace ve společných prostorách domu a svislé rozvody je předepsáno provedení, ve kterém je vodičem měděný drát. Plášť tohoto kabelu musí vyhovovat protipožárním předpisům. Má být tedy v nehořlavém provedení. V rámci bytu lze od účastnické zásuvky, případně od domácího přepínače, nebo směrovače použít kabel, kde je vodičem lanko [5], [7].

Celková délka kabelu od koncového zařízení k aktivnímu prvku by neměla přesáhnout 100 m. V místech, kde je to nutné, lze použít stíněný kabel. Pro připojení místní sítě k bezdrátovému aktivnímu prvku na střeše objektu se využívá kabel se zvýšenou ochranou pro venkovní povětrnostní podmínky, tedy především s úpravou proti UV záření [7].

Category	Type	Frequency Bandwidth	Applications & Notes
Cat 1		0.4 MHz	Telephone and modem lines (not described in EIA/TIA recommendations and not suitable for modern systems).
Cat 2			Older Terminal Systems (not described in EIA/TIA recommendations and not suitable for modern systems).
Cat 3	UTP	16 MHz	10BASE-T & 100BASE-T4 Ethernet (Described in EIA/TIA-568. Not suitable for speeds > 16 Mbps. Commonly used for telephone cables).
Cat 4	UTP	20 MHz	16 Mbps Token Ring (Not commonly used these days)
Cat 5	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet (Commonly found in most of the LAN implementations)
Cat 5e	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet (Cat5 Enhanced. Same structure as Cat 5, but with better testing standards)
Cat 6	UTP	250 MHz	1000BASE-T Ethernet (SFS-EN 50173-1)
Cat 6e		250 MHz (500 MHz in some cases)	Not a standard; its a proprietary of cable manufacturers
Cat 6a		500 MHz	10GBASE-T Ethernet (ISO/IEC 11181:2002 Amendment 2)
Cat 7	S/FTP	600 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet. (Contains Four pairs, S/FTP : Shielded pairs, Braid-screened cable. ISO/IEC 11801 2nd Ed.)
Cat 7a		1000 MHz	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet. (Contains Four pairs, S/FTP : Shielded pairs, Braid-screened cable. ISO/IEC 11801 2nd Ed. Amendment 2)
Cat 8		1200 MHz	Under Development. (Four pairs, S/FTP: Shielded pairs, braid-screened cable. its a standard under development)

Obr. 12. Přehled kategorií UTP kabeláže [20].

Zakončení kabelů se provádí pomocí konektorů RJ-45. Je možné dvojí provedení zapojení vodičů do konektoru podle barevného schématu A nebo B. K některým koncovým zařízením bylo nutné dodávat křížené kabely. V současnosti je většina zařízení vybavena funkcí Auto MDI/MDI-X a nutnost použití křížených kabelů odpadá. Ukončení v jednotlivých bytech se realizuje pomocí zásuvky s RJ-45 konektorem [7].

3.1.2 Napájené prvky

Při výstavbě místních sítí se využívají přepínače. Můžeme je rozdělovat podle několika kritérií:

- Podle počtu portů – vyrábí se přepínače s počtem 5,8,16,24… portů.
- Podle provedení – desktop, rackmount.
- Podle napájení – 12 V, 230 V…
- Podle rychlosti – 100 Mb/s, 1000 Mb/s…

Desktopové přepínače jsou určeny především do domácností a menších kanceláří, tomu odpovídá počet portů, který se pohybuje nejčastěji v rozmezí 5-16. Napájení je realizováno pomocí adaptéru. Provedení normované k umístění do racku je vhodné pro realizaci místních domovních sítí a pro rozsáhlejší firemní sítě. Počet portů se pohybuje v rozmezí 16-48, nejčastěji 24. Tyto přepínače bývají vybaveny webovým rozhraním pro jejich správu, kde je možné sledovat základní provoz, odpojovat porty apod. Napájení je přímo ze sítě 230 V. Metalické vedení bývá na straně klienta zakončeno zpravidla konektorem RJ-45. Síťové karty s tímto rozhraním jsou dnes již běžně součástí prodávaných počítačů [7], [8].

3.2 Základní vlastnosti

Mezi poskytovateli datových služeb je v současnosti nejvíce rozšířena hvězdicová topologie. Případně se lze ještě setkat s kombinacemi, kde například bytový dům s několika vchody má v každém z nich umístěný přepínač. Ty jsou propojeny do kaskády za sebou, případně propojeny hvězdicově s jiným přepínačem. Výhodou takového řešení je mnohdy značná úspora na kabeláži, nevýhodou je ztráta přenosové rychlosti způsobená „přeskokem“ přes několik prvků a dělením jejich kapacity. Z hlediska síťového provozu se při poskytování datových služeb jedná o komunikaci typu client-server.

3.3 Bezpečnost LAN

Bezpečnost místních síti je třeba hodnotit ze dvou základních hledisek. Prvním pohledem je eliminace rizik spojených s provozem lokální sítě jako takové. V druhém případě se musíme zabývat bezpečností vyplývající z propojení domácí nebo firemní sítě s Internetem.

Při návrhu zabezpečení místní domovní sítě, která není propojena s jinými sítěmi, jsou bezpečnostní rizika celkem dobře předvídatelná a lze jim poměrně snadno předcházet. Obsahem takových opatření bude zamezení fyzického přístupu k prvkům sítě, což většinou vyplývá z podstaty umístění těchto zařízení uvnitř budovy. V případě podniků je situace o něco složitější. Útočník se může pohybovat uvnitř budovy, může jím být třeba i samotný zaměstnanec. Síť je chráněna také pomocí bezpečnostní politiky firmy (oprávnění v síti, fyzický přístup, autentizace uživatelů) [5], [8].

Největší rizika přináší propojení místních sítí do celosvětové sítě Internet. Musíme zde vhodným způsobem ochránit přenášený obsah proti odposlechu paketů. Dále se objevují pakety s podvrženým obsahem. Známé jsou také nejrůznější útoky na hesla. Obecně známým doporučením je instalace speciálního software – Firewallu. Jeho hlavní funkcí je zabránit nechtěnému přístupu zvenčí. Dále zde lze zakazovat určitý typ komunikace např. omezení přístupu k serverům s nelegálním obsahem, případně s obsahem, který nesouvisí s pracovní činností apod.

3.3.1 Síť VPN

Zaměstnanci některých firem se často setkají s potřebou bezpečné komunikace s podnikem prostřednictvím Internetu. Jedná se o situaci, kdy potřebujeme přistupovat k datům na firemním serveru z „venkovní“ sítě jiného poskytovatele. Tyto služby využívají zaměstnanci na služebních cestách, obchodní zástupci, lidé pracující v domácnosti apod. Nastavení firemní sítě by s ohledem na bezpečnostní politiku nemělo umožnit přímé připojení „zvenku“. Za tím účelem je vhodné využít tzv. virtuální privátní síť (Vitual Private Network - VPN). To nám umožní komunikovat prostřednictvím jakékoliv nezabezpečené, tedy nedůvěryhodné veřejné sítě tak, že veškerá komunikace mezi naším PC a firemním serverem je šifrována [5], [8].

4 PRÁVNÍ ASPEKTY VÝSTAVBY A PROVOZU SÍTÍ

4.1 Oprávnění k výstavbě sítí

Oprávnění budovat telekomunikační sítě je třeba rozebrat v několika rovinách. Prvním předpokladem je způsobilost firmy – podnikatele z hlediska živnostenského zákona. Nelze opomenout ani obecně platné právní předpisy, normy apod. Dodržení některých norem může být také vyhrazeno smlouvou s koncovým zákazníkem – klientem.

Druhým bodem je dodržení povinností vyplývajících z telekomunikačního zákona, kde se musí podnikatel zaměřit na využívání pouze schválených zařízení, zorientovat se v možnostech využívání licencovaných a nelicencovaných pásem. Také je nutné omezit v souladu s předpisy maximální výkony zařízení apod.

V další rovině se musí zájemce o výstavbu telekomunikační sítě obrátit se svým záměrem na vlastníky dotčených objektů a pozemků. Patří sem jednání o podmínkách umístění zařízení (přístup, nájemní smlouva, úhrada za spotřebovanou energii…). Taková jednání probíhají nejčastěji s představiteli samospráv, stavebními a bytovými družstvy a s pracovníky úřadů místní samosprávy.

4.2 Provozování telekomunikačních sítí

Fyzická nebo právnická osoba, která měla zájem poskytovat datové služby, byla do dubna roku 2005 povinna zřídit si vázanou živnost „poskytování telekomunikačních služeb“. Spolu s nabytím platnosti zákona č. 127/2005 Sb. o elektronických komunikacích není poskytování těchto služeb v režimu živnostenského zákona. Od 1.5.2005 je osoba podnikající v elektronických komunikacích povinna provést registraci prostřednictvím formuláře na ČTÚ. Při registraci se uvádí údaje o podnikateli a především se definuje rozsah nabízených služeb. Tedy zda se bude jednat o síť veřejnou, nebo privátní. Dále zda budou nabízeny hlasové, datové služby, nebo jejich kombinace, zda budou nabízeny prostřednictvím pevných sítí apod [4].

Jednou z povinností podnikatele poskytujícího telekomunikační služby je vyplňování výkazů souvisejících s jeho podnikáním. Jedná se o záznamy o počtech připojených klientů, tržby za určená období, přehled o investicích do sítí [4].

Další povinností podnikatele zajišťujícího veřejnou telekomunikační síť je oznámení typu rozhraní, která využívá pro připojení zařízení. V případě realizované sítě se jedná o rozhraní

10Base-T, 100Base-Tx a 1000Base-Tx, vždy podle doporučení IEEE 802.3 s využitím konektoru RJ-45. Oznámení musí být provedeno tak, aby umožnilo vzdálený přístup. Optimální je využití webových stránek podnikatele [4].

4.2.1 Záznamy o provozu na telekomunikační síti

Od roku 2005 je dána v ČR v souvislosti s platností zákona č. 127/2005 Sb. o elektronických komunikacích povinnost poskytovatelům služeb elektronických komunikací sledovat, ukládat a uchovávat data o provozu uživatelů jejich služeb. Z hlediska poskytovatele služeb má zásadní význam §97, který mimo jiné doslovně definuje [4]:

„(1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna na náklady žadatele zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv a to Policii ČR, BIS a Vojenskému zpravodajství.“

„(3) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací.“

Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout: orgánům činným v trestním řízení, Polici ČR, BIS, Vojenskému zpravodajství a ČNB. Všem těmto orgánům a institucím pouze pro účely a za podmínek v zákoně dále specifikovaných [4].

Problémem pro poskytovatele služeb byla poměrně neurčitá specifikace toho, co všechno se rozumí pod pojmem „provozní a lokalizační údaje“. Konkrétnější byl prováděcí předpis - vyhláška č. 485/2005 Sb. Zde je pro poskytovatele datových služeb důležitá definice pro sítě s přepojováním paketů. Tuto informaci lze nalézt ve vyhlášce - Rozsah uchovávání provozních a lokalizačních údajů. Důležitý je bod první [4]:

„a) u služeb přístupu k síti s uvedením typu připojení, identifikátoru uživatelského účtu, identifikátoru zařízení uživatele služby, data a času zahájení připojení, data a času ukončení připojení, zájmových identifikátorů (například IP adresa, číslo portu), statusu události (například úspěch, neúspěch, řádné nebo mimořádné ukončení připojení), množství přenesených dat (v příchozím směru/v odchozím směru).“

Zákon byl novelizován, neboť vznikaly nejasnosti. Například nebylo jasné, jak dlouho data uchovávat a jak s nimi naložit po této době. *„Doba uchovávání těchto provozních a lokalizačních údajů nesmí být kratší než 6 měsíců a delší než 12 měsíců. Po uplynutí této doby je osoba, která údaje podle věty první a druhé uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního předpisu nebo tento zákon nestanoví jinak (§ 90)“* [4]

4.2.2 Dopady zákona č. 127/2005 Sb. na poskytovatele datových služeb

Výše uvedený zákon s sebou přináší nemalé povinnosti pro poskytovatele a nutnost technických opatření k jejich bezproblémovému zajištění. V současné době se ještě využívají veřejné adresy IPv4 (Internet Protocol version 4) , kterých je celkově nedostatečné množství a každý poskytovatel má přidělený pouze určitý segment, který je nižší než počet aktivních prvků a koncových uživatelů v jeho síti. Situace bývá řešena službou NAT (Network Adress Translation), kdy za jednou veřejnou IP adresou je překládáno několik adres vnitřní sítě poskytovatele, respektive několik uživatelů.

V případě, kdy by došlo k vyžádání údajů o provozu na některé veřejné adrese ze strany oprávněného orgánu, tedy byl by například položen dotaz typu: *„Komu byla přidělena IP adresa: , dne 1.1.2014 v čase 15:37, ze které přistupoval na webovou stránku http://www.seznam.cz?“*, by poskytovatel služeb dle svých běžných záznamů určil pouze okruh klientů. Ten může představovat například obyvatele a uživatele jednoho bytového domu, sídliště, obce, ale také všechny uživatele jeho služeb. Dle zákonných povinností se však s takovou odpovědí nelze spokojit a je nutné identifikovat konkrétního uživatele. Za tímto účelem se většinou instalují servery se speciálně vyvinutými aplikacemi.

4.2.3 Ochrana osobních údajů

Podnikatel se může například v souvislosti s vedením databáze klientů využívajících jeho služby setkat se shromažďováním osobních údajů. Každý zpracovatel je povinen, dle platného zákona (mimo stanovených výjimek), provést registraci prostřednictvím Úřadu pro ochranu osobních údajů (ÚOOÚ). Zde se uvede důvod k uchovávání, charakter osobních údajů, způsob uchování, zabezpečení a případné předávání třetím stranám.

II. PRAKTICKÁ ČÁST

5 NÁVRH A REALIZACE METROPOLITNÍ SÍTĚ

Při návrhu a realizaci sítě bylo třeba zohlednit dva základní aspekty důležité pro další rozhodování o výstavbě. Prvním aspektem k řešení byla otázka rozsahu poskytovaných služeb a jejich předpokládané kvality. Dále bylo potřebné zohlednit charakter celé lokality, ve které má k vybudování sítě dojít. Na základě těchto podkladů bylo přistoupeno k výběru konkrétních technických prostředků, které tvoří celou síť.

5.1 Rozsah a parametry poskytovaných služeb

Parametry poskytovaných služeb lze rozdělit do několika bodů:

- Rychlost připojení.
- Kvalita připojení (dostupnost, odezva).
- Servis (čas obnovení provozu).
- Cena (realizace přípojky a měsíční paušál).

V prvním bodě byla řešena otázka rychlosti připojení. Při návrhu bylo uvažováno o rychlosti cca 8 Mb/s v případě objektů připojených bezdrátovým pojítkem a o rychlostí 33 Mb/s pro objekty připojené do optické sítě poskytovatele. Pro samostatné přípojky v rodinných domech, případně v malých provozech bylo kalkulováno s rychlostí 6 Mb/s. Předpokládána byla agregace 1:20 u všech služeb. Veškerá koncová zařízení byla vybírána tak, aby zde byla jistá rezerva pro případné navýšení rychlostí. To bylo důležité zejména u bezdrátových pojítek, kde je omezení největší. Optické trasy většinou umožňují poskytování rychlostí i několinásobně vyšších oproti těm současně nabízeným.

Úvahy o kvalitě poskytovaných služeb směřovaly především k dostupnosti. Uvažováno bylo o celkové dostupnosti služeb ve výši cca 99,5 % z celkového času. Na optických sítích byl předpoklad vyšší (až 99,9 % z celkového času). Tato čísla byla důležitá s ohledem na výběr služeb poskytovaných třetími stranami (garance časů servisních zásahů třetích stran). Další nutností bylo splnění podmínky dostatečně nízké odezvy a to především přípojek realizovaných na bezdrátových sítích.

Garantované obnovení provozu při výpadku způsobeném na straně poskytovatele služeb je ukotveno smluvně na 48 hodin v pracovních dnech. U tohoto typu služby je však obecně předpokládáno rychlejší obnovení provozu. Většina poruch je řešena okamžitě po jejich zjiš-

tění a bývá vyřešena nejpozději do několika hodin v pracovní den. V případě nočních výpadků, kdy je nutné zpřístupnění uzavřených prostor třetími stranami, dochází k obnovení následující den.

Pro výběr konkrétních používaných zařízení je neméně důležitým kritériem cena služeb. Cena použitých zařízení musí být úměrná ceně služby, respektive tržbám z paušálů na konkrétních lokalitách. Téma ekonomické rozvahy celého projektu není součástí této práce. Výše měsíčního paušálu je stanovena v rozpětí 292-333 Kč (v závislosti na frekvenci plateb – měsíční nebo roční zvýhodněný paušál). Tržby za realizaci přípojky v bytovém domě nebyly uvažovány (předpokládalo se využití delšího smluvního závazku, který zcela eliminoval aktivační poplatek).

5.2 Popis lokality pro realizaci

Metropolitní síť byla navrhována a realizována ve městě Pardubice. Jedná se o krajské město s necelými sto tisíci obyvateli. Město se rozprostírá v polabské nížině, bez významnějšího převýšení terénu v rámci celé zástavby. To bylo určitou výhodou při realizaci a provozu bezdrátových pojítek. Samotná zástavba sestává z několika městských částí. V této práci jsou rozděleny podle přípojných uzlových bodů, nikoliv striktně podle hranic městských obvodů nebo sídlišť. Centrální technologie a přívod konektivity je na sídlišti Závodu Míru. Odtud jsou páteřními spoji služby dále distribuovány do několika částí, na kterých jsou vybudované uzlové body v druhé úrovni.

Na pravém břehu Labe se jedná o dvojici sídlišť – Polabiny a Cihelna. Na druhé straně pak sídliště Dukla, Karlovina a Višňovka. Nejvzdálenější je pak trasa na sídliště Dubina. Na většinu z těchto přístupových uzlů je zároveň připojen jeden nebo více spojů tvořící další nižší úroveň přístupového bodu. V průběhu výstavby sítě byly veškeré body, byť přechodně, připojeny pomocí bezdrátových pojítek. Z toho důvodu byly přípojné body ve všech úrovních vybírány tak, aby byla zajištěna přímá viditelnost na uzlový bod vyšší úrovně.

5.3 Hlavní prvky použité pro realizaci

Celá metropolitní síť sestává z několika základních prvků, jejichž použití se v různých částech opakuje. Jedná se především o bezdrátové okruhy v licencovaných pásmech v případě páteřních tras a o bezdrátové spoje v pásmu 5 GHz v nejnižší úrovni (poslední míli). Druhou skupinou pak jsou optické sítě. Realizovaná síť se skládá z okruhů vlastních optických tras a dále jsou využívána pronajatá vlákna od jiných společností.

5.3.1 Pronajaté bezdrátové okruhy

Při realizaci sítě bylo využito několik spojů pracujících v licencovaném pásmu, které nejsou vlastnictvím investora. Jedná se o spoje značky Ceragon pracující v pásmu 23 GHz. Zařízení byla pronajata na dobu určitou. Výhodou tohoto řešení je omezení investičních nákladů, vzhledem k omezenosti vlastních zdrojů. Smlouva s poskytovatelem této služby musela být koncipována tak, aby bylo vyhověno požadavkům uvedeným v kapitole 5.1. Dodavatel tedy musí nabízet především rychlé obnovení služeb při výpadku. Tyto okruhy byly použity jako páteřní spoje pro uzlové body v nejvyšší úrovni (spojení z centrálního bodu na jednotlivá sídliště – lokality).

5.3.2 Pronajaté optické okruhy

Dalším zásadním prvkem jsou pronajaté optické okruhy. Při realizaci byly využity tam, kde nebylo možné umístit vlastní optické trasy, nebo tam, kde by takové řešení bylo technicky, nebo finančně příliš náročné. Tento typ propojení je využíván opět pro zajištění páteřních tras. V menší míře jsou tímto způsobem připojeny také koncové objekty (především domy s vysokým počtem klientů).

5.3.3 Vlastní optické okruhy

Jedná se optické trasy řešené v zásadě dvěma způsoby:

- Uložení chrániček v tepelných sítích místní elektrárny.
- Samonosné optické kabely mezi objekty.

V prvním případě ukládá chráničky optických vláken naše společnost do tepelných sítí místní elektrárny na základě nájemní smlouvy. Chráničky jsou takto umísťovány v podzemí v betonových kanálech spolu s potrubím. Položení chráničky probíhá vzhledem ke stísněným podmínkám v kanálech pomocí dálkově ovládaného pásového zařízení s kamerou a přenosem v reálném čase, ke kterému je připevněna plastová struna. Za tu se pak zavlékne samotná chránička, kterou je možno projetým úsekem protáhnout. Chránička je instalována do jednotlivých objektů v místě přivedení tepelných trubek do bytového domu (společné prostory v přízemí). Zde dochází k napojení do sítě LAN. Takové připojení je využito pro páteřní spoje i koncové objekty. Tímto způsobem je připojena zhruba polovina klientů celé společnosti. K realizaci se využívá silnostěnná chránička o celkovém průměru 40 mm a dále malé chráničky silnostěnné o venkovním průměru 12 mm. V rámci objektu jsou instalovány tenkostěnné chráničky o celkovém průměru 10 mm. Dodavatelem je firma Dura-Line

CT s.r.o., z Tlumačova. Veškerá instalovaná optická vlákna (kabely) jsou jednovidová s různým počtem vláken. Pocházejí od různých výrobců. Kabely byly do chrániček zafukovány přímo naší společností.

Druhý způsob řešení vlastních optických sítí představuje použití samonosného optického kabelu Samsung s různým počtem vláken, který je zavěšen pomocí speciálních kotev mezi dva objekty. Výhodou je rychlá instalace s minimálními náklady. Kabel také nenarušuje svým vzhledem okolní prostředí díky svému malému průměru a nenápadné barvě slonové kosti. Toto řešení je využito k propojení dvou sousedních objektů v několika případech. Řešení pomocí vlastních výkopů zatím není realizováno s ohledem na administrativní překážky a vysoké vstupní náklady. Předpokládá se však i nasazení této varianty.

5.3.4 Ostatní spoje a spoje v pásmu 5 GHz

Na trasách, kde není možné využití optických okruhů, jsou nasazena pojítka v pásmu 5 GHz. Jde v naprosté většině případů o zařízení RouterBOARD Mikrotik v různých verzích. Pro koncová zařízení jsou využívány venkovní plastové boxy, které přímo obsahují 19 dBi anténu. K těmto je přiveden kabel UTP uzpůsobený pro venkovní prostředí zn. Signamax.

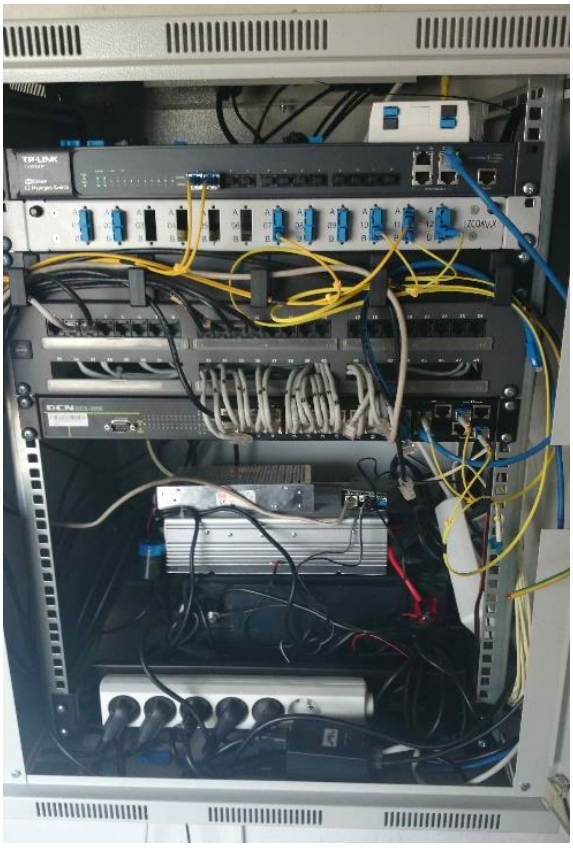
Jako přístupové body jsou využity kovové boxy zn. Signamax s integrovanou anténou. V některých případech nastala nutnost pokrytí více oblastí z jednoho přístupového bodu. Ty však někdy ležely mimo úhel integrované antény. Řešením byla instalace dalších sektorových antén připojených do téhož boxu, který byl vybaven zařízením s více bezdrátovými kartami (moduly). K těmto kartám jsou pak pomocí pig-tailů jednotlivé antény připojeny.

Obr. 13. Signamax box.

Spoje, které překonávají delší vzdálenosti (do několika kilometrů) jsou vybaveny směrovými anténami.

Napájení je realizováno pomocí PoE zdrojů odpovídajícího napětí. U koncových prvků se jedná o adaptér do zásuvky se dvěma výstupy RJ-45. Jeden je označen PoE, tedy s napájením, druhý slouží pro připojení k síti LAN, směrovači, nebo přímo PC. Zařízení na uzlových bodech jsou napájena pomocí přizpůsobeného patch panelu umístěného v racku.

V tomto případě je napájení zálohováno pro případ výpadku v elektrické rozvodné síti. To je realizováno pomocí bezúdržbové baterie a měniče napětí 12/230 V.



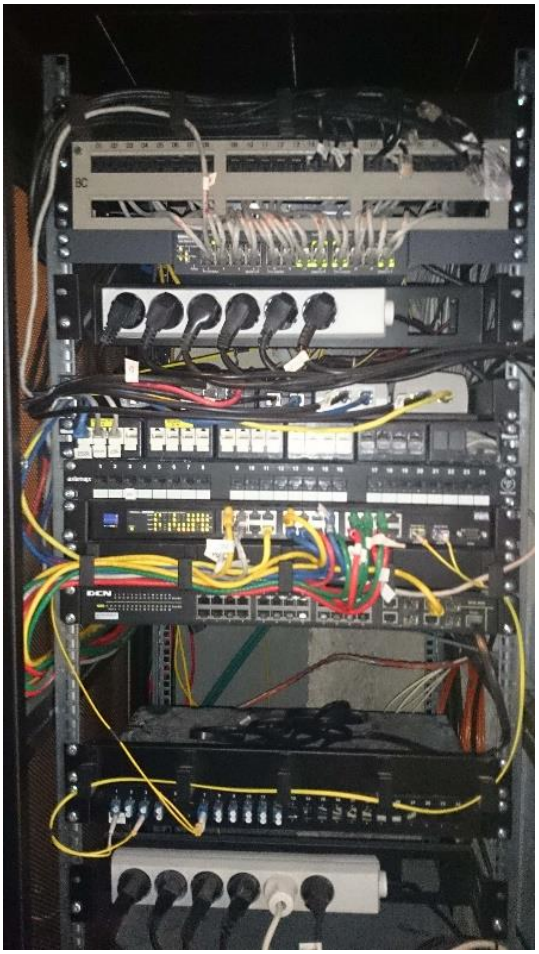
Obr. 14. Měnič 12/230 V v racku.

5.4 Centrální část s umístěním serverů

Pro umístění hlavního uzlového bodu byla vybrána lokalita na sídlišti Závodu Míru. Hlavním důvodem je skutečnost, že většina dodavatelů konektivity je schopna předat své služby na optické lince právě na této adrese bez nutnosti budování radiových „přeskoků“, které by mohly vést ke zhoršení kvality dále poskytovaných služeb na místní úrovni. Tato lokalita má určitou výhodu danou geograficky a to tím, že se nachází ve střední části území realizované metropolitní sítě.

5.4.1 Konektivita

Pro zajištění požadovaného rozsahu služeb je nutné si pronajímat odpovídající konektivitu. Ta je v současné době ve výši 1 Gb/s. Konektivita je do objektu přivedena na optické síti a předávána pomocí dvou 1 Gb/s portů do hlavního přepínače naší společnosti. Ten je umístěn ve stojanovém racku ve střešní místnosti (výtahové nástavbě). Odtud je vedena kabeláž pro připojení sítě LAN a kabeláž pro připojení páteřních spojů z ostatních lokalit. Na střeše je také vybudován přístupový bod pro připojení objektů v ulici nábř. Závodu Míru.



Obr. 15. Hlavní rack.

5.4.2 Servery

V témže racku jsou umístěny dva hlavní servery společnosti. Na nich probíhají především tyto služby:

- Rozdělování konektivity.
- Funkce mail serveru.
- Klientská databáze.
- Dohledový systém (částečně).
- Ukládání dat o provozu (data retention).

Veškerá zařízení jsou zálohována na dobu cca 12 h s možností připojení agregátu při déle trvajících odstávkách nebo poruchách elektrické sítě.

5.4.3 Anténní systém

Na střeše objektu jsou instalovány čtyři anténní stožáry pro umístění páteřních spojů. Rozmístění stožárů bylo zvoleno tak, aby byla možnost umístění spojů s otevřeným výhledem do všech potřebných směrů. Stožáry jsou uzemněny a připojeny k hromosvodné síti, dle příslušných předpisů.

Obr. 16. Stožár Závodu Míru.

5.4.4 Připojení lokality Závodu Míru z centrálního uzlu

Objekt sloužil pro připojení asi deseti koncových zařízení – bytových domů pomocí bezdrátových pojítek v pásmu 5 GHz. V současnosti již byla většina těchto přípojek realizována pomocí vlastní optické sítě. Na objekt je dále napojeno několik koncových klientů v rodinných domech nebo menších komerčních provozech.

5.5 Hlavní přístupové body

Z hlavního uzlového bodu v lokalitě Závodu Míru je vybudováno celkem šest hlavních páteřních tras. Jedná se o dvě trasy optické na sídliště Polabiny a Dubina. Ostatní čtyři lokality jsou prozatím připojeny prostřednictvím bezdrátových spojů v licencovaných pásmech a po-

stupně bude docházet k jejich nahrazování optickými trasami. Rozmístění jednotlivých lokalit je patrné z následujícího obrázku, kde jsou značeny optické spoje červenou a bezdrátové spoje modrou barvou. Uvedené lokality budou dále podrobněji popsány.

Obr. 17. Mapa páteřní sítě - červeně optické trasy, modře bezdrátové spoje (mapový podklad ČÚZK).

5.5.1 Připojení sídliště Polabiny

Přívod konektivity pro další distribuci na sídlišti Polabiny je řešen spojením objektů Závodu Míru a Valčíkova. Vzdušná vzdálenost mezi těmito domy je bezmála jeden kilometr. V minulosti bylo spojení realizováno pronajatým bezdrátovým spojem. Nyní je tento okruh propojen pomocí optické trasy. Technologie je umístěna ve střešní výtahové nástavbě prostředního vchodu v racku. Veškeré antény jsou umístěny na jednom stožáru. Z lokality Valčíkova pokračují tři páteřní spoje pro tři uzlové body další nižší úrovně. Jedná se o lokality Sluneční, Trnová a Kpt. Bartoše. Na objektu jsou dále instalovány 4 přístupové body pro připojení přilehlých bytových domů a rodinných domků v lokalitě Rosice nad Labem a Kréta. Celkem je k tomuto uzlu připojeno cca 20 koncových přípojek na bezdrátové technologii i na optických linkách.

Obr. 18. Anténní stožár Polabiny.

Napájení je zálohováno pro případ výpadku na cca 10 hodin. V samotném objektu byla realizována síť LAN pro připojení obyvatel domu. Služby v tomto domě využívá asi 100 klientů.

5.5.2 Připojení sídliště Dubina

Uzlový bod Dubina je nevzdálenějším (téměř 4 km) a zároveň nejvíce vytíženým. Zhruba 30-40 % veškerého toku celé sítě jde přes tento uzel. Také z toho důvodu je připojení této lokality realizováno prostřednictvím optických tras. Technologie je umístěna v racku ve střešní výtahové nástavbě čtrnáctipodlažního domu v ulici Bartoňova.

Obr. 19. Rack Dubina a rack sítě LAN.

V domě byla realizována síť FTTH, metalická síť, dále kabelové rozvody pro distribuci televizního signálu z pozemního vysílaní a satelitu.

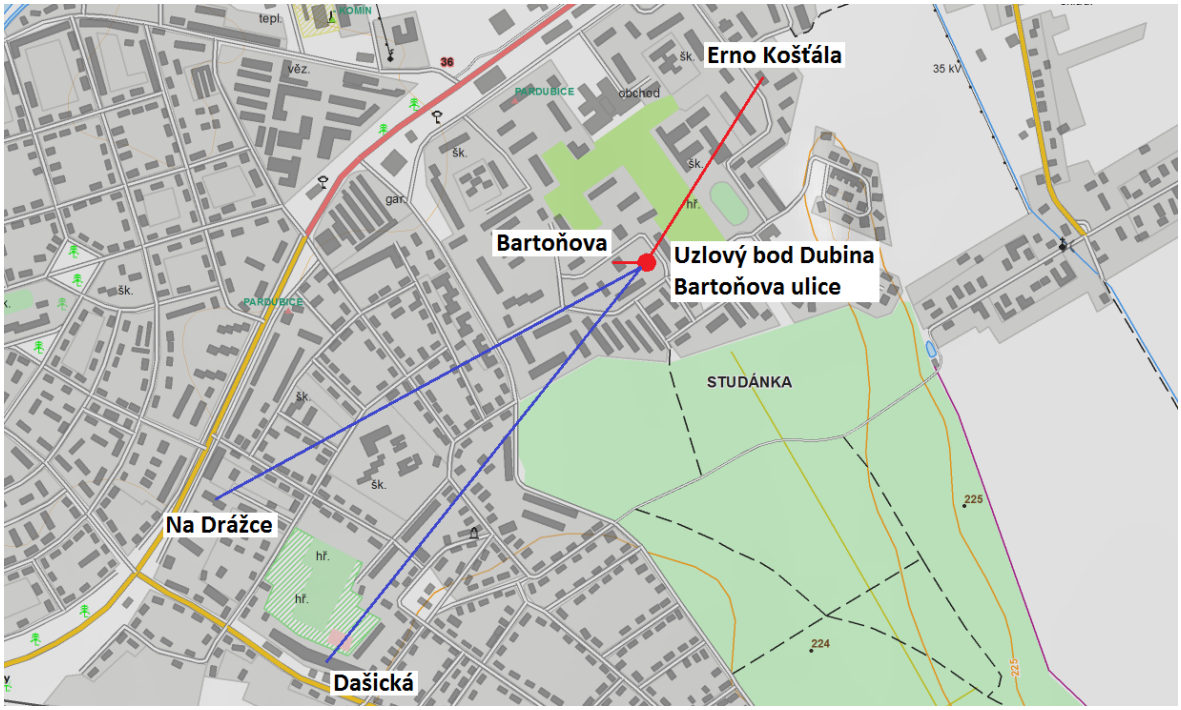
Obr. 20. Realizace antén pro TV.

Na celkem třech stožárech je umístěno několik přístupových bodů a dalších antén pro připojení okolních objektů. V minulosti tak byla realizována většina spojení. Postupně byla tato zařízení nahrazena připojením pomocí vlastních optických tras. Většina objektů je připojena tímto způsobem a přístupové body tak slouží pouze pro připojení rodinných domů v místní části Spojil. Technologie jsou zálohovány pro případ výpadku elektrické energie na dobu asi 20 hodin.

Obr. 21. Anténní stožár Dubina.

Z tohoto uzlu dále pokračují páteřní spoje na tyto čtyři lokality (v závorce uvedeno pokrytí hlavních ulic z daného uzlového bodu):

- Erno Košťála (Erno Košťála, Dubinská)
- Bartoňova (Bartoňova, L. Malé, Blahoutova)
- Na Drážce (Na Drážce, severozápadní část Dašické)
- Dašická (Pardubičky, jihovýchodní část Dašické)



Obr. 22. Mapa uzlových bodů Dubina (mapový podklad ČÚZK).

Jak je patrné z uvedeného obrázku, dva uzly jsou připojeny bezdrátově a dva pomocí optické trasy. Uzel Erno Košťála slouží především k propojení optických tras vedených z okolních objektů.

5.5.3 Připojení lokality Karlovina

Jedná se o přístupový bod pro centrální část města, který je vzdálen asi 1,5 km. Je realizován prostřednictvím bezdrátového spoje v licencovaném pásmu. Technologie je umístěna ve výtahové nástavbě čtrnáctipodlažního domu v ulici Karla IV. Zařízení jsou umístěna v racku a zdroje jsou zálohovány pro případ výpadku. V domě je také vybudována síť LAN pomocí metalického vedení pro připojení klientů k Internetu.

Obr. 23. Rack Karlovina.

Z objektu je prostřednictvím přístupových bodů na dvou anténních stožárech připojeno několik okolních bytových domů v ulicích Anenská, Jiráskova, Karla IV, Sladkovského, Polská a Na Třísle. Dále je sem připojeno několik menších domů, ležících především v historickém centru na Pernštýnském náměstí a v jeho okolí. Jedná se zejména o restaurace, kde byly zároveň realizovány přístupy pro hosty v těchto zařízeních a na předzahrádkách.

Obr. 24. Oblast historické zástavby Pardubic pokrytá anténním systémem Karlovina.

Z tohoto uzlu je realizován pouze jeden „přeskok“ na ulici Jindřišská prostřednictvím bezdrátového spoje. Na jednom ze stožárů je umístěna webová kamera, která snímá nepřetržitě centrum města, a tyto záběry jsou součástí webové prezentace firmy.

5.5.4 Připojení sídliště Dukla

Sídliště Dukla je poněkud specifické oproti ostatním lokalitám svou zástavbou. Na místě někdejší polní nemocnice z počátku minulého století, která byla největší svého druhu ve střední Evropě, vzniklo v padesátých letech dvacátého století zcela nové sídliště ve stylu socialistického realismu. Jedná se většinou o tří až pětipodlažní bytové domy tvořené zpravidla třemi a více vchody, vždy se sedlovou střechou. Jeden z těchto domů v centrální části sídliště v Jilemnického ulici byl vybrán pro umístění uzlového bodu. Veškerá technologie je umístěna na půdě objektu v racku. Anténní stožár je využíván pouze jeden, společný pro televizní antény a jiné technologie, které zde mají umístěné vlastníci bytů. Na tomto stožáru bylo instalováno několik sektorových antén pro připojení dalších objektů v ulicích Jilemnického, Artura Krause, Gorkého a Wolkerova. V domě je vybudována metalická síť pro připojení zdejších obyvatel.

Obr. 25. Stožár Dukla.

Současně musely být instalovány dva spoje pro uzlové body nižší úrovně. Problémem nebyla vzdálenost, ale omezená viditelnost mezi objekty. Ta byla dána dvěma faktory. Prvním je poměrně velké množství zeleně převyšující střechy domů a druhým je fakt, že některé domy jsou „schovány“ mezi ostatními vícepodlažními objekty. Situace je patrná z následujícího obrázku, kde je červeně označen místní uzel, modře trasy k přístupovým bodům nižší úrovně a oranžově ostatní objekty, které jsou do sítě připojeny.

Obr. 26. Sídliště Dukla s vyznačením uzlových a připojených objektů (mapový podklad ČÚZK).

5.5.5 Připojení sídliště Cihelna

Sídliště Cihelna je tvořeno novější panelovou zástavbou několika domů a dále objekty Univerzity Pardubice. Technologie je umístěna v racku ve výtahové nástavbě nad posledním podlažím domu v ulici Kunětická, který je vzdálen od centrálního prvku vzdušnou čarou necelé dva kilometry.

Obr. 27. Pokrytí přístupového bodu Cihelna a vyznačení uzlového bodu Závodu Míru.

Na dvou anténních stožárech je umístěno několik přístupových bodů především pro firemní klienty v oblastech Fáblovka a Polabiny I. Veškeré přilehlé bytové domy, kde jsou poskytovány datové služby naší společností, jsou připojeny pomocí vlastní optické sítě. Jedná se o ulice Kunětická, K Rozvodně a U Josefa. Z tohoto bodu nepokračuje žádný další spoj pro připojení uzlového bodu nižší úrovně. Výjimku tvoří přípojka pro koupaliště Cihelna, kde je signál dále distribuován do dalších provozních částí, jiným subjektům i návštěvníkům tohoto zařízení. Technologie instalovaná naší firmou je však vlastnictvím provozovatele koupaliště.

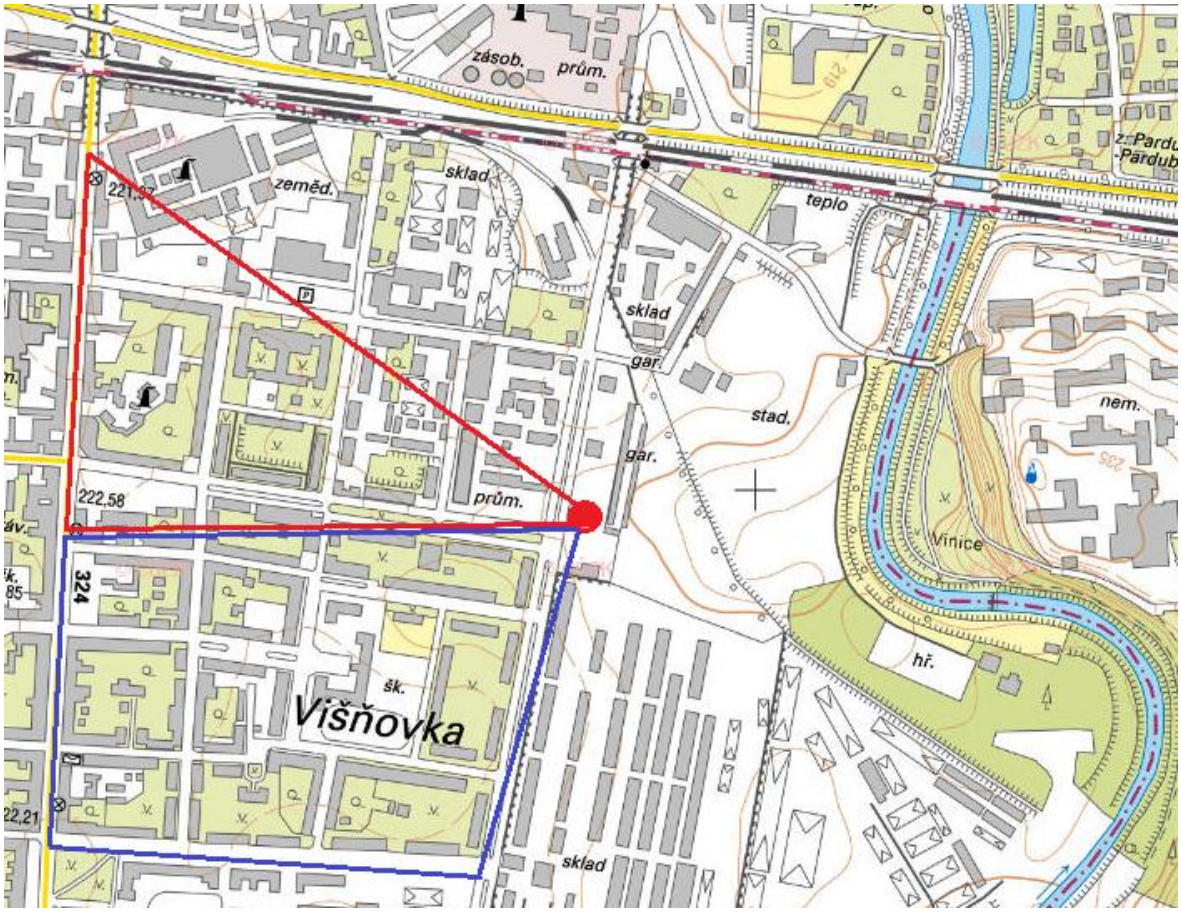
Obr. 28. Rack Cihelna.

5.5.6 Připojení lokality Višňovka

Lokalita Višňovka je pomyslně ohraničena řekou Chrudimkou, železničním koridorem vedoucím přes město, ulicí Jana Palacha a ulicí Pod Břízkami. Zástavba je tvořena obdobnými objekty jako sídliště Dukla spolu s novějšími zděnými domy ležícími v okolí ulice S. K. Neumanna. Pro umístění uzlového bodu byl vybrán desetipodlažní dům v ulici S. K. Neumanna, který výrazně převyšuje okolní zástavbu a je z něj potřebný přímý výhled na všechny připojené bytové i rodinné domy.

Obr. 29. Stožár Višňovka.

Přívodní trasa je realizována vlastním spojem v nelicencovaném pásmu 10 GHz s dostatečnou propustností. Vlastní technologie je umístěna v racku ve společných prostorách domu na chodbě v posledním patře. Zařízení jsou zálohována pro případ výpadku elektrické energie. Na jednom stožáru jsou instalovány dva přístupové body, které pokrývají celou zájmovou lokalitu pomocí sektorových antén. Zájmové území pomyslně rozdělené těmito sektory je patrné na následujícím obrázku.



Obr. 30. Zájmové území rozdělené na dva sektory (mapový podklad ČÚZK).

Obr. 31. Fotografie shodné lokality z místa stožáru Višňovka.

6 NÁVRH A REALIZACE SÍTÍ LAN

Při realizaci metropolitní sítě byly současně navrženy a realizovány domovní sítě LAN. Ty mohou být realizovány pomocí metalického nebo optického vedení. Většina sítí je metalických, proto je tato kapitola zaměřena na ně. Je zde řešena otázka použitých aktivních prvků, kabeláže, konektorů, elektrického napájení atd.

Každá z vybudovaných cca 140 sítí LAN je v podstatě originálem. Existují však určité styčné prvky, které každá z nich obsahuje. Lze tedy předložit jakýsi návrh vzorové sítě, který bude tyto společné vlastnosti naplňovat. Výjimku tvoří vždy určité odlišnosti vyplývající z charakteru připojeného bytového domu:

- Panelový bytový dům s jedním vchodem.
- Panelový bytový dům se dvěma a více vchody.
- Zděné (cihlové) většinou starší domy, zpravidla s půdou.

Nejjednodušší situace je v prvním případě. V panelovém domě je většinou dostatečný prostor pro svislé rozvody kabeláže. Ty jsou realizovány v ohebných plastových trubkách umístěných v rozvaděči společně s rozvody elektřiny, domovních telefonů, zvonků apod. Případně jsou tyto trubky samostatně ve zdi ukončené rozvodnými krabičkami v každém patře.

Ve vodorovném směru po chodbách je pak vždy umístěna tenká plastová PVC lišta, do které je kabel pro koncového klienta vložen. Samotný přepínač je umístěn do společných prostor do racku, nebo do plastové skříně odpovídajících rozměrů. Zpočátku byla většina přepínačů umístěna v nejvyšších patrech objektů. Bylo to v době, kdy se umísťovaly do společné skříně s bezdrátovou technologií a bylo nutné dodržet co nejkratší svod od antény z důvodu útlumu na kabelu vedoucímu k anténě. S nahrazením „klasických“ antén venkovními boxy s integrovanou anténou tento problém odpadl.

Umístění přepínačů v nejvyšším patře přináší určité problémy při nahrazování bezdrátových spojů optickými vlákny. Optická vlákna jsou přiváděna přesně opačně, tedy z přízemí, nebo suterénu domu a je nutné je dotáhnout v chráničce až do horních pater a připojit ke stávající síti. To bývá problematické vzhledem k omezeným průměrům trubek v rozvodech objektů. Nově navrhované sítě počítají s umístěním přepínače právě v přízemí.

Druhým typem objektu je panelový dům s více vchody. Tam je situace obdobná jako v předchozím případě. Pouze nastává otázka, jak vyřešit propojení vchodů mezi sebou. To lze realizovat tak, že se veškerá kabeláž ze všech vchodů táhne do jednoho rozvaděče do vchodu

umístěného nejvíce ke středu. Nevýhodou je značný průměr celého svazku kabelů, které je nutno táhnout mezi jednotlivými vchody, dále vyšší náklady na kabeláž a u vyšších objektů s velkým počtem vchodů snadné překročení maximální délky kabelu 100 m. Druhým řešením je umístění přepínače do každého vchodu a jejich propojení. Nevýhodou je kaskádování sítě a nutnost vybudování napájení pro každý přepínač (lze vyřešit pomocí PoE).

Posledním typem objektu, ve kterém došlo k instalaci sítí LAN je zděný dům se sedlovou střechou. Jedná se především o starší zástavbu v centrálních částech města v lokalitě Višňovka a na sídlišti Dukla. Jde většinou o tří až pětipodlažní objekty se třemi vchody. V těchto objektech byly určité problémy s instalací rozvodů k jednotlivým klientům. Většinou zde nejsou žádné rezervní ohebné plastové trubky jako v předchozích případech. K rozvodům je tak nutné využívat staré nepotřebné komíny nebo světlíky. Komíny jsou mnohdy zasypané a je nutné je před samotnou instalací řádně vyčistit. Řešení v podobě průrazů přes jednotlivá patra většinou nepřicházelo v úvahu s ohledem na přání majitelů domů. V několika případech bylo k instalaci využito šachty s rozvody plynového potrubí, se schválením a stanovením zvláštních podmínek revizním technikem.

6.1 Právní podklady

Před vlastní výstavbou je nutné shromáždit příslušná potřebná povolení. Jedná se především o souhlas vlastníka dotčeného objektu s instalací a provozováním sítě. S každým vlastníkem bytového domu je zpravidla sepsána smlouva o umístění zařízení, nebo je alespoň vydán písemný souhlas, kde se stanoví konkrétní podmínky. Jedná se ustanovení v těchto oblastech:

- Nájemné za umístění technologií poskytovatele (bezúplatně/nájemné).
- Podmínky při výstavbě (odkaz na ČSN, BOZP, protipožární předpisy…).
- Odpovědnost poskytovatele služeb za škody.
- Zpřístupnění prostor (vydání kopií klíčů za účelem servisních návštěv).
- Technická dokumentace (před výstavbou, dále po ukončení výkaz změn).
- Způsob odběru elektrické energie (vlastní měřicí přístroj, podružné měření, paušál).

Bez těchto dokumentů by nebylo možné k instalaci sítě přistoupit. Při větších zásazích v objektu může být vyžadováno některé z opatření vyplývajících ze stavebního zákona (územní souhlas, ohlášení stavby, stavební povolení…).

6.2 Použité prvky a struktura sítě

Veškeré instalované sítě byly realizovány za použití v zásadě shodných prvků. Jednotlivá použitá zařízení budou dále podrobněji rozebrána.

6.2.1 Kabeláž

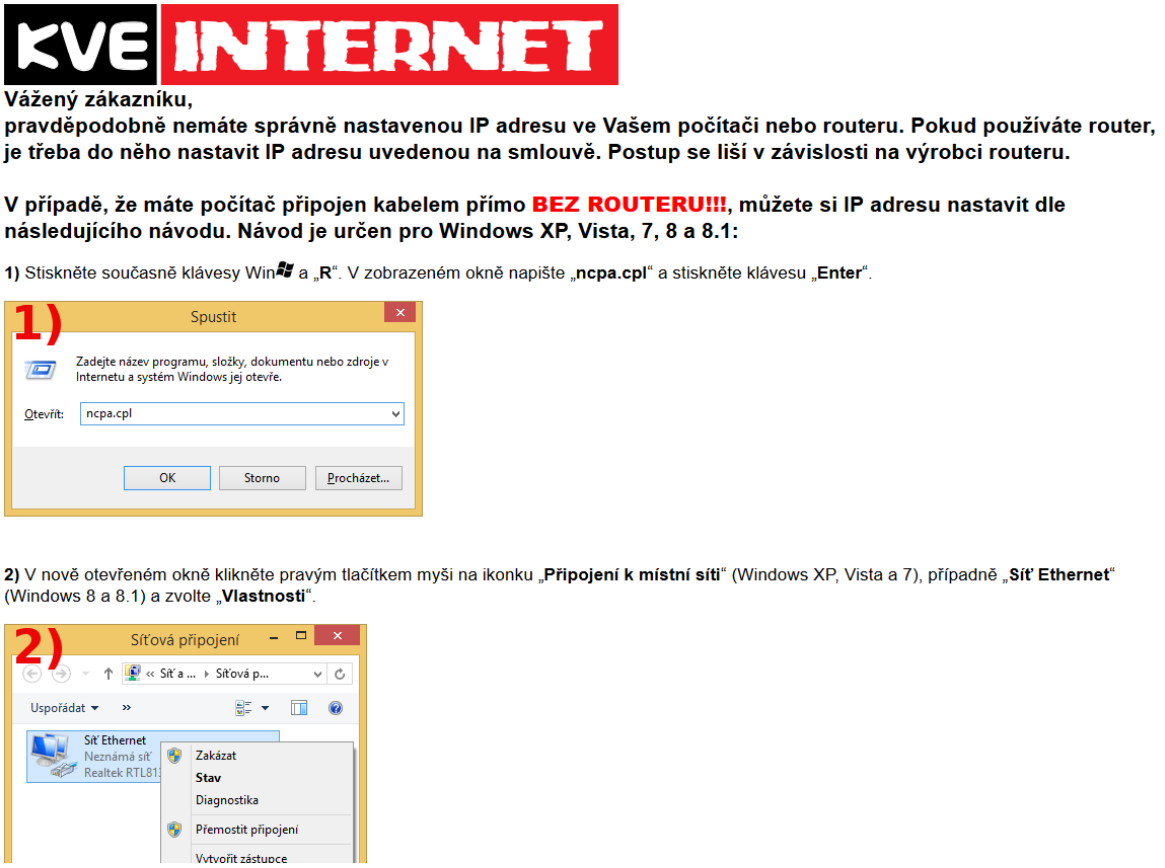
K veškerým rozvodům ve společných prostorách domu byl použit kabel UTP, kde vodičem byl drát. Na většině míst byl použit kabel Signamax kategorie 5e, případně vyšší, vždy v provedení s nehořlavým pláštěm LS0H (Low Smoke Zero Halogen) . Kabely byly od jednotlivých klientů přivedeny vždy do jednoho racku nebo plastového rozvaděče a ukončeny konektorem RJ-45 podle barevného schématu A.

6.2.2 Aktivní prvky

Jako aktivní prvky byly využity stolní přepínače s rychlostí 100 Mb/s značky Edimax, případně Signamax. Využity byly přepínače s pěti porty, ale nejčastěji s osmi nebo šestnácti. Tyto prvky byly umístěny do plastových skříní ve společných prostorách domů. V současné době jsou postupně nahrazovány přepínači v provedení do racku. Jedná se o přepínače různých značek s přizpůsobením na optickou síť. Tyto prvky lze spravovat pomocí webového rozhraní dálkovým přístupem.

6.2.3 Koncové přípojky

Účastnické přípojky byly zakončeny prostým opatřením konců kabelů konektorem RJ-45, případně byly instalovány zásuvky s RJ-45. V případě zájmu klienta byla přípojka opatřena domácím bezdrátovým směrovačem Tenda W311R+, který umožňuje současné připojení více PC, chytrých telefonů apod. Podmínkou správné funkce koncového zařízení klienta je nastavení platných údajů dle smlouvy (IP adresa, maska, brána, DNS servery). V případě chybného výchozího nastavení zařízení ze strany klienta (zaškrtnutá volba automatického přidělování údajů) je poskytovatelem automaticky zobrazen návod pro bezchybné nastavení.



Obr. 32. Automaticky zobrazovaný návod v případě chybného nastavení (část okna).

6.2.4 Napájení sítě

K napájení sítí LAN bylo využito PoE zdrojů, které ve vlastní úpravě zajišťují jak napájení síťových prvků, tak bezdrátového zařízení na střeše objektu. V případě využití optické přípojky také napájení souvisejících zařízení. Veškerá zařízení v koncových domech, které nejsou uzlovým bodem, nejsou zálohována pro případ výpadku elektrické energie. Předpokládalo se, že při výpadku energie v celém domě nebude nikdo z klientů využívat Internet, i když by to bylo teoreticky možné například při použití notebooku na baterii.

7 NÁVRH ŘEŠENÍ DOHLEDU SÍTĚ A DATABÁZE KLIENTŮ

K bezproblémovému provozu sítě bylo nutné zajistit kvalitní systém pro dohlížení nad jednotlivými prvky. Instalované řešení bude popsáno v následujících odstavcích. Pro správu smluvních údajů a řešení plateb klientů byla použita databáze, která bude také předmětem podrobnějšího seznámení.

7.1 Dohled nad provozem sítě

Na dohledový systém společnosti bylo před vlastní realizací kladeno několik základních požadavků, které měl splňovat:

- Dohled síťových prvků v reálném čase.
- Webové rozhraní s dálkovým přístupem.
- Nezávislost funkce na vlastní síti.
- Zasílání některých stavových informací prostřednictvím SMS.
- Uchování historie provozu.

Dohledový systém společnosti sleduje provoz veškerých registrovaných prvků a při výpadku konkrétního zařízení nebo části sítě okamžitě informuje technickou podporu o nastalé situaci. Hlášení probíhá pomocí krátké textové zprávy odeslané na mobilní telefon. Ta obsahuje předem nastavené pojmenování prvku s popisem nastalého problému. Většinou se jedná o název objektu (dle ulice a čísla popisného) s uvedením ztrátovosti na daném prvku, kde 100 % ztrátovost odpovídá úplnému výpadku a jiná procentuální hodnota poukazuje na zarušení, problémy s anténou apod.

Jednotlivým prvkům je přiřazena vždy určitá priorita, podle které je o jejich stavu technická podpora informována. Nejvyšší prioritu mají páteřní spoje, prvky centrálního uzlu, dále koncové objekty. O problémech na těchto zařízení jsou informace posílány formou SMS okamžitě. Další skupinou jsou prvky nižší úrovně, tedy například domácí bezdrátové směrovače na koncových přípojkách. To je užitečné při výpadku části sítě LAN, kdy sledované zařízení vyšší úrovně je v pořádku, ale přepínač v síti LAN je vadný. Běžně použité přepínače nelze sledovat přímo.

Pro snadné přidávání prvků a pro přehlednost je dohledový systém vybaven webovým rozhraním. Přes něj je možné přidávat jednotlivá zařízení podle použité IP adresy, přidělovat priority a nastavovat zobrazování požadovaných údajů. Po přihlášení obsluhy (zabezpeče-

ným způsobem) je úvodní obrazovka rozdělena na dvě části. Vlevo je v úzkém pruhu zobrazena stromová struktura veškerých přiřazených prvků dle jejich skutečného zapojení v síti. Nad ní je ještě pole vyhledávání pro snadnější výběr prvku. Vpravo je přehled aktuálně problematických prvků s uvedením názvu, IP adresy, ztrátovosti v % a délky výpadku. Po výběru konkrétního prvku z levého sloupce se zobrazí podrobné údaje o něm. Jde především o název, IP adresu, celkovou dobu běhu, celkovou dostupnost v %, celková doba výpadků, aktuální stav atd. V dalším okně je historie několika posledních výpadků s uvedením data a času, kdy došlo k výpadku a čas, kdy byl provoz obnoven. Náhled, jak informace o takovém prvku vypadají, je na následujícím obrázku.

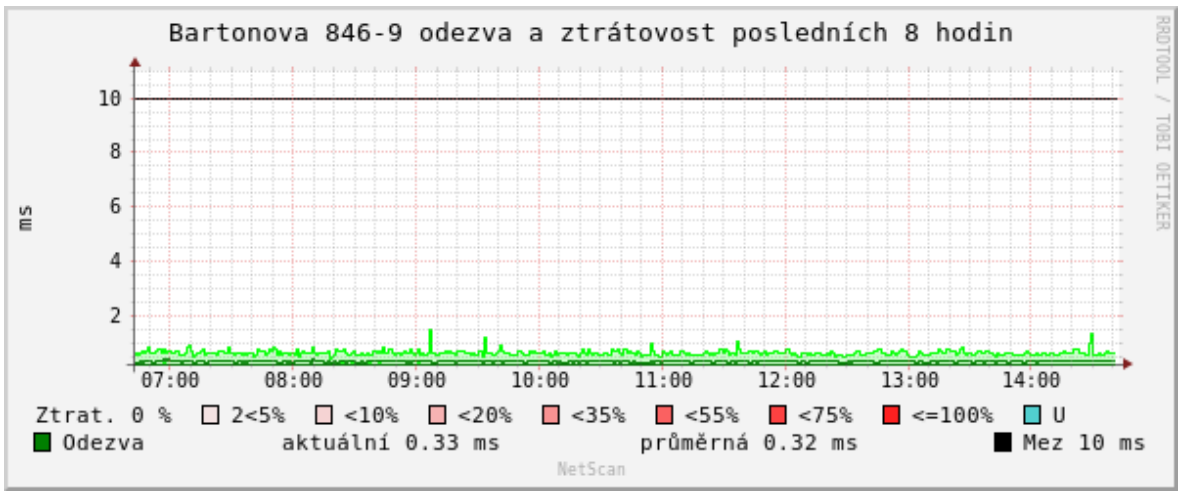
Přehled | 8 hodin den týden měsíc rok | Menu prvku

Název:	Bartonova 846-9 (611)	**Objekt:**	Bartoňova undefined 849
IP:	10.10.5.51		
Typ:	Router	**Stav:**	OK
Běh celkem:	979 dní 6 h 7 min	**Výpadky celkem:**	15 h 5 min
Dostupnost:	99.936%	**Tento měsíc:**	100.000%
Akt. odezva:	0.322 ms	**Akt. ztrátovost:**	0 %
Poznámka:			

Od	Délka výpadku:	Čas náběhu:
2013-11-07 02:11:32	5 min. 19 s	2013-11-07 02:16:51
2013-10-24 04:09:17	4 min. 51 s	2013-10-24 04:14:08
2013-08-12 07:31:25	3 min. 55 s	2013-08-12 07:35:20
2013-07-31 04:54:59	3 min. 54 s	2013-07-31 04:58:53
2013-07-29 18:37:47	59 min. 47 s	2013-07-29 19:37:34
2013-07-29 08:37:45	45 min. 59 s	2013-07-29 09:23:44
2013-07-26 05:08:57	6 min. 19 s	2013-07-26 05:15:16

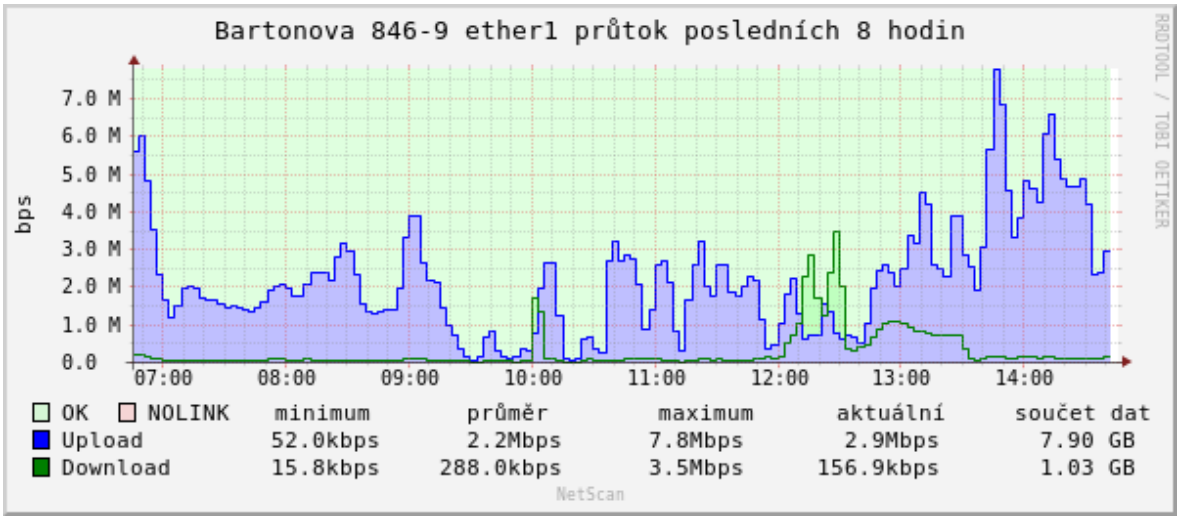
Obr. 33. Dohled - souhrnné informace o stavu prvku.

Zbylá část okna je věnována třem grafům. První zobrazuje průběh odezvy v milisekundách a ztrátovost v procentech.



Obr. 34. Dohled - graf odezvy a ztrátovosti.

Druhý uvádí vytížení procesoru daného prvku. Poslední zobrazuje průtok dat a to zvlášť pro stahovaná a zvlášť odesílaná data (pakety).



Obr. 35. Dohled - graf toku dat přes prvek.

Grafy lze zobrazovat za různá časová období. Pro zajištění bezproblémového běhu při výpadku celé vlastní sítě je část dohledového systému instalována na zařízeních, která nejsou umístěna v této síti.

7.2 Databáze klientů

S komerčním provozem sítě pro připojení klientů k Internetu je spojena nutnost vedení potřebných záznamů. Za tímto účelem jsou tvořeny různé klientské databáze. Základní seznámení s jedním možným řešením, které bylo navrženo a realizováno pro potřeby této sítě, je popsáno v následujících podkapitolách. Základními požadavky je možnost dálkového přístupu (webové rozhraní) a rychlé automatické spárování přijatých plateb.

Základní funkce klientské databáze lze rozdělit do dvou částí:

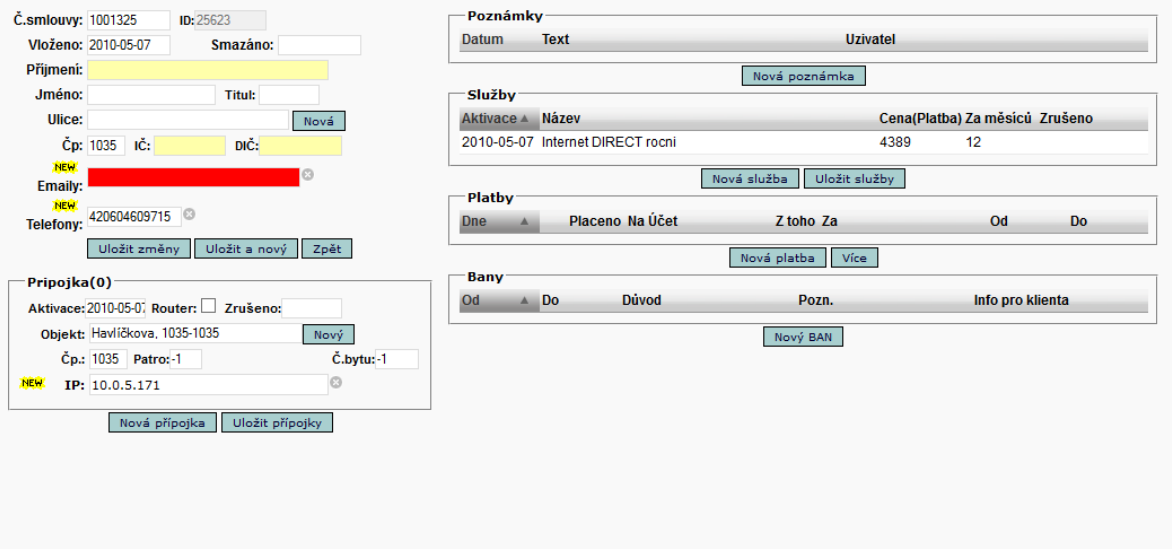
- Vedení a správa osobních údajů.
- Přehled a správa plateb.

7.2.1 Vedení a správa osobních údajů

Pro účely plnění smluvních závazků ze strany poskytovatele služeb je nutné shromažďování základních údajů o jednotlivých klientech. V tomto směru databáze umožňuje vkládání nových a editaci stávajících záznamů, dále vyhledávání podle jednotlivých atributů a vyhledávání pomocí složených dotazů. Evidována jsou tato data:

- Osobní údaje (jméno, příjmení, adresa trvalého bydliště, kontaktní údaje)
- Údaje o službě (číslo smlouvy, adresa místa odběru, IP adresa)

Dvě uvedené kategorie bylo nutné od sebe oddělit, protože běžně dochází k situaci, kdy má jeden klient více přípojek (smluvních vztahů) v rámci metropolitní sítě. Při ukončení odběru služeb na jedné adrese pak může zůstat klient aktivním zákazníkem s jinou přípojkou. Pro veškeré vkládané údaje jsou aplikována požadovaná integritní omezení. V samostatném rámu části okna je prostor pro zápis poznámek.



Obr. 36. Klientská databáze - základní okno webového rozhraní.

Zpracování osobních údajů bylo v souladu se zákonem nahlášeno prostřednictvím webového formuláře ÚOOÚ (Úřadu pro ochranu osobních údajů).

7.2.2 Přijaté platby a neplatiči

Druhou základní funkcí databáze je řešení plateb klientů. V této části je vždy uveden název tarifu, datum aktivace a cena služby, která má být v daném období uhrazena. Jedná se většinou o paušální částku s uvedením období (v měsících) na které má klient předplaceno. V příkladu na obrázku se jedná o částku 4389,- Kč, která je předplatným na dvanáct měsíců.

V dalším rámu je přehled přijatých plateb. Zde se přiřadí platba přijatá prostřednictvím některého ze dvou bankovních účtu, případně platba přijatá v hotovosti přes pokladnu. Rám obsahuje datum připsání platby, účet, účel a v případě paušálního poplatku datum od/do kdy je platba použita jako předplatné.

V posledním rámu je možnost omezení služeb zákazníkům. Jedná se o několik základních možností, kdy může k omezení dojít:

- Nezaplacené služby.
- Přerušení služeb.
- Ukončení služby (dočasné).
- Způsobování problémů v síti ze strany klienta (viry).

Před aplikací úplného omezení služeb z důvodu neplacení se využívá částečné omezení služeb, kdy musí zákazník potvrdit automatické okno ve webovém prohlížeči se zobrazením podrobností o výši dluhu a údajů pro platbu. Potvrzení je vyžadováno každé tři hodiny a počet potvrzení ze strany klienta se ukládá pro případné pozdější použití. Marným uplynutím stanovené lhůty pro úhradu dlužné částky (většinou 1-2 měsíce) jsou služby zcela omezeny.

Další omezení služeb je přerušení. To se děje na základě písemné žádosti klienta, kdy poskytovatel umožní přerušení služeb na určité časové období, případně na dobu neurčitou (vždy na celé měsíce). Této možnosti využívají studenti v pronájmu v době prázdnin, chalupáři v letních měsících apod.

Databáze je provázána se dvěma bankovními účty poskytovatele služeb. Z těchto účtů jsou veškeré platby importovány a na základě uvedeného variabilního symbolu automaticky přiřazovány k jednotlivým klientům. V případě, kdy není možné platbu automaticky přiřadit, je tato zařazena do nespárových a musí být přiřazena „ručně“ obsluhou aplikace. Jedná se o případy, kdy není uveden variabilní symbol, nebo je nekompletní. Také může dojít k zaslání jiné než smluvené částky a v tom případě je opět nutná manuální kontrola obsluhou. To jsou další důvody, proč před úplným omezením služeb dochází k upomínání klientů prostřednictvím automatické hlášky.

Obr. 37. Klientská databáze - okno omezení přístupu.

Přiřazování plateb probíhalo vždy na začátku dalšího měsíce spolu s vygenerováním elektronických výpisů z bankovních účtů. Docházelo však k situacím, kdy byl klient na začátku měsíce upozorněn na neuhrazený paušál a poté okamžitě tento stav napravil. Pokud však na tuto skutečnost poskytovatele neupozornil, byla mu hláška nadále zobrazována celý měsíc až do připsání platby dle elektronického výpisu. Takové řešení se ukázalo jako nevhodné a zbytečně matoucí. Nyní jsou tedy platby přiřazovány automaticky denně po ukončení daného bankovního dne.

8 BEZPEČNOST METROPOLITNÍ SÍTĚ

V souvislosti s provozem metropolitní sítě je nutné navrhnout a zrealizovat účinná preventivní opatření pro zamezení škod vzniklých jejich podceněním. Základní hrozby a jejich možné řešení byly popsány v teoretické části práce. Opatření v konkrétních situacích budou v následujícím textu jen velmi stručně popsána. Důvodem je skutečnost, že se jedná o vůbec nejcitlivější oblast podniku. V průběhu provozu sítě došlo k útokům s cílem zamezení funkčnosti, které byly velmi závažného charakteru, avšak byly dostatečným ponaučením pro přijetí účinnějších opatření.

8.1 Návrh konkrétních opatření

Zabezpečení metropolitní sítě je možné rozdělit do několika oblastí:

- Zabezpečení aktivních prvků.
- Zabezpečení serverů.
- Bezpečnostní opatření ve vztahu k zaměstnancům.

V případě zabezpečení aktivních prvků je situace do značné míry ovlivněna výrobcem konkrétního zařízení. Konfigurace zařízení probíhala tak, aby nebyl v budoucnu umožněn přístup k administraci prostřednictvím nevhodných služeb. Například je nežádoucí používat k přístupu k prvkům Mikrotik službu Telnet, neboť taková komunikace není nijak dodatečně zabezpečena. Obecným předpokladem zabezpečení bylo dále použití silného hesla pro každý prvek zvlášť. Také bylo využito možnosti omezit administraci prvků pouze z určitého rozsahu konkrétních IP adres. Zvláštní pozornost bylo nutné věnovat možnosti přístupu k aktivním prvkům, zejména přepínačům s rozšířenou funkcionalitou. Některé umožňují snadný přístup k administraci prostřednictvím továrně nastaveného „servisního účtu“, který lze při provádění prvotní konfigurace snadno přehlédnout.

Zabezpečení hlavních serverů má obdobné rysy jako opatření u aktivních prvků. Vhodné by bylo i zabezpečení fyzické, umístěním zařízení na bezpečném nepřístupném místě. Toho však nebylo možné docílit, neboť daný nebytový prostor sdílí několik poskytovatelů současně. Zavedeno bylo zrcadlení obsahu serveru na jiný, vzdálený server, umístěný v nezávislé síti. Bylo také zajištěno ukládání informací o veškerých přístupech na hlavní server (samozřejmě včetně neúspěšných pokusů).

Ve vztahu k zaměstnancům bylo nutné provést příslušné proškolení, jehož předmětem byly informace o bezpečnostních opatřeních. Bylo například stanoveno, jakým způsobem mají

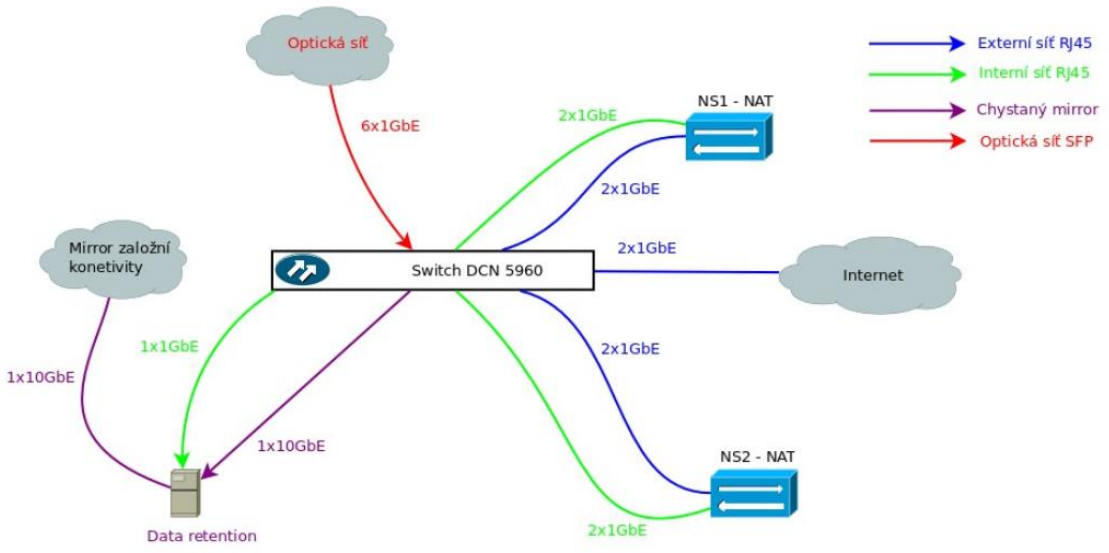
servisní technici nakládat s hesly, jak je uchovávat. Bylo určeno, jak lze nakládat s firemní technikou, se kterou se přistupuje do administrátorského rozhraní, tedy o zákazu instalace firmou neschváleného software do notebooků apod.

8.2 Zajištění ukládání dat o provozu na síti

Za účelem vyhovění zákonu o elektronických komunikací podle § 97 odst. 3 a prováděcí vyhlášce 357/2012 (§ 2 odst. 3 písmena a) a f) byl navržen projekt pro zaznamenávání uskutečněného provozu na síti poskytovatele. Projekt byl předložen Polici ČR ke schválení, neboť bude z její strany docházet k pravidelné úhradě nákladu spojených se zřízením a údržbou systému k popsanému účelu. Při návrhu bylo stanoveno několik základních požadavků:

- Vytváření záznamů o provedených spojeních.
- Pokrytí všech hraničních a páteřních linek.
- Systém nesmí negativně ovlivnit poskytované služby.
- Zajištění všech požadavků jmenovaného zákona.
- Podpora IPv4 (včetně NAT) a IPv6
- Možnost rozšíření systému o funkci datového odposlechu.

Pro realizaci systému bylo použito dvou síťových prvků. Prvním je síťový přepínač, který zajišťuje koncentraci datových toků z jednotlivých lokalit sítě, jak je znázorněno na obrázku. Druhým je server, který zajišťuje analýzu, agregaci a ukládání záznamů o prováděných spojeních.



Obr. 38. Schéma zapojení prvků pro data retention.

8.2.1 Přepínač

Pro koncentraci datových toků před/za NAT bude použit přepínač DCS-5960 firmy DCN dodávaný společností Alternetivo s.r.o. Tento přepínač disponuje 10 GbE (Gigabit Ethernet) portem, do kterého budou zrcadleny datové toky před/za NAT (Network Adress Translation) obou serverů. Každý ze serverů je před i za NAT připojen dvěma 1 GbE a servery jsou v redundantním zapojení. Vzhledem k minimálnímu potřebnému počtu 10 portů 1GbE, byl zvolen 24 portový přepínač. Aby bylo možné zaznamenávat všechny datové toky, je nutné koncentrovat zrcadlený datový tok do jednoho portu, což je v současné době možné pouze na technologii 10 GbE. Vzhledem k těmto požadavkům byl vybrán výše zmíněný typ přepínače. Navíc přepínač disponuje dostatečným výkonem i pro další předpokládané navyšování rychlosti sítě, a to až na 10 Gb/s.

8.2.2 Server

Pro vlastní analýzu a agregaci datových toků byl vybrán server PCS S2420Q-M5+ SYS dodávaný společností ABACUS ELECTRIC spol. s r. o. Server disponuje dvěma 10GbE z nichž jeden bude využit pro zrcadlený datový tok z přepínače. Na serveru bude provozován operační systém Linux a námi vyvíjený nástroj pro analýzu, agregaci a uchovávání záznamů o spojení. Systém umožňuje výstup dat požadovaných dle aktuální prováděcí vyhlášky 357/2012 Sb. ve formátu CSV (Comma Separated Values). Navíc systém provádí pasivní ověřování hardwarových adres (MAC Media Access Control).

Server disponuje dostatečným výkonem a pamětí pro zajištění logování datových toků i v plné rychlosti rozhraní, tedy 10GbE. Veškerý celkový agregovaný tok v síti KVE s.r.o. je aktuálně cca 1210 Mb/s. Redukce uchovávaných dat se předpokládá cca 400:1. Je tedy nutné zaznamenávat cca 3,025 Mb/s, což je 32,67 Gb statistik denně. Zákonem požadovaných 6 měsíců pak znamená zajistit úložiště minimálně 5,96 TB. Vzhledem k předpokládanému růstu toku v síti podle trendu předešlých let, bylo zvoleno úložiště o velikosti 9 TB realizované pěti pevnými disky v zapojení RAID6 tak, aby se zmírnil dopad případné závady na pevných discích.

ZÁVĚR

Cílem této práce bylo navrhnout a zrealizovat metropolitní síť pro komerční připojení klientů k Internetu v krajském městě Pardubice. Bylo navrženo umístění páteřních spojů a uzlových bodů pro další distribuci služeb. Konkrétně se jedná o připojení šesti hlavních lokalit. Dále bylo navrženo řešení připojení koncových bytových domů včetně sítí LAN. Záměr byl úspěšně realizován a služby v současné době využívá asi 2800 domácností připojených ve zhruba 140 bytových domech. Více než polovina domácností byla připojena pomocí optických sítí. V takto připojených objektech využívá většina uživatelů Internetu služeb této společnosti. V menší míře byly připojeny také samostatné firmy a zákazníci v rodinných domech.

Připojení do této metropolitní sítě představuje zajímavou alternativu ke službám, které nabízejí firmy s působností v rámci celé ČR a mobilní operátoři. Přínosem zrealizovaného záměru je vznik několika pracovních pozic v administrativním a především technickém zázemí poskytovatele služeb. Realizace se zúčastnilo také několik studentů střední průmyslové školy elektrotechnické Pardubice v rámci odborné praxe.

Pro účely správy údajů o klientech této poměrně rozsáhlé sítě byly navrženy základní parametry a požadavky na klientskou databázi. Podobně byly navrženy základní funkce dohledového systému. Současně s výstavbou a provozem sítě bylo nutné zohlednit související právní aspekty. V poslední kapitole byly navrženy prvky a vlastnosti systému pro povinné ukládání dat o provozu na síti.

Realizace této metropolitní sítě není definitivním řešením. Neustále dochází k dalšímu rozvoji nových technologií a nabídce nových relevantních výrobků pro výstavbu sítí. Klienti požadují stále kvalitnější služby a rozšiřování nabídky společně s tlakem na cenu. V odvětví je silná konkurence na místní i celostátní úrovni. Předpokladem úspěchu i v dalším období je neustálé sledování nových trendů v oboru a nasazování perspektivních zařízení do sítě. Nyní se jedná především o připojování dalších objektů prostřednictvím optických sítí v maximální možné míře. Bude tak možné nabídnout rychlejší a bezpečnější služby, případně rozšíření o IPTV apod.

Poskytování telekomunikačních služeb je zajímavým a rychle se rozvíjejícím odvětvím informatiky. Lze očekávat další zvyšování zájmu o tyto služby.

SEZNAM POUŽITÉ LITERATURY

[1] BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť.* 1. vyd. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

[2] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G.* 1. vyd. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[3] ROHLÍK, Matěj a Pavel LAFATA. *Bezpečnostní rizika v současné generaci pasivních optických přístupových sítí.* Electrorevue [online]. 2010, roč. 12, č. 3 [cit. 2013-12-5]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/download/bezpecnostni-rizika-v-soucasne-generaci-pasivnich-optickych-pristupovych-siti/

[4] *Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).* In: 127/2005. 2005, č. 127, 43/2005. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&nr=127~2F2005&rpp=15#local-content

[5] STALLINGS, William. *Local and metropolitan area networks.* 6. ed. Upper Saddle River: Prentice Hall, 2000, 478 p. ISBN 9780130129390.

[6] MAIER, Martin. *Optical switching networks.* Cambridge: Cambridge University Press, 2008, 324 p. ISBN 0-521-86800-9.

[7] TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení.* 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

[8] DOSTÁLEK, Libor a Alena KABELOVÁ. *Velký průvodce protokoly TCP/IP a systémem DNS: hardware, instalace a zapojení.* 5. aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

[9] Vyzařovací diagram. In: *Digizone.cz* [online]. © 2005 – 2014 Internet Info, s.r.o. [cit. 12.4.2014]. Dostupné z: http://www.digizone.cz/clanky/existuje-antena-ktera-by-byla-nejlepsi-2/

[10] Outdoor box 19 dBi. In: *TomiCzech* [online]. © 2014 Tomi czech s.r.o. [cit. 15.03.2014]. Dostupné z: http://www.t-cz.com/outdoor-box-19dbi-pro-rb133v_ie136.jpg

[11] Mikrotik RB 433. In: *TomiCzech* [online]. © 2014 Tomi czech s.r.o. [cit. 15.03.2014]. Dostupné z: http://www.t-cz.com/mikrotik-rb433-level4-3x-minipci-3x-lan-64mb-atheros300_ie3470.jpg

[12] Router Tenda W311R+. In: *TomiCzech* [online]. © 2014 Tomi czech s.r.o. [cit. 16.03.2014]. Dostupné z: http://www.t-cz.com/tenda-w311r-wireless-n-router-802-11b-g-n-150-mb-s-1x-wan-4x-lan-1x-ext-ant-_ie48089.jpg

[13] PoE zdroj. In: *100Mega* [online]. © 2014 100MEGA Distribution [cit. 13.04.2014]. Dostupné z: http://eshop.100mega.cz/airlive-poe-48pb-v2-napajeci-zdroj-s-injektorem-48v-802-3af_d96776.html

[14] Měnič 12/230V. In: *100Mega* [online]. © 2014 100MEGA Distribution [cit. 13.04.2014]. Dostupné z: http://eshop.100mega.cz/whitenergy-menic-napeti-dc-ac-12v-230v-400w-usb_i116428.jpg

[15] 2,4 GHz channels. In: *Moonblinkwifi* [online]. © 2014 Moonblink Communications [cit. 14.04.2014]. Dostupné z: http://www.moonblinkwifi.com/2point4freq.cfm

[16] Fiber Optic. In: *ProSoundWeb* [online]. © 2014 © Copyright 2014 ProSoundWeb.com [cit. 16.04.2014]. Dostupné z: http://www.prosoundweb.com/images/uploads/FiberOpticsGraphic1.jpg

[17] Zalamovačka INNO VF-78B. In: *Wifishop.cz* [online]. © 2014 CyberSoft s.r.o. [cit. 16.04.2014]. Dostupné z: http://www.wifi-shop.cz/img.asp?attid=82204

[18] Svářečka Ilsintech. In: *Ipmedia.cz* [online]. © 2014 CyberSoft s.r.o. [cit. 16.04.2014]. Dostupné z: http://www.ipmedia.cz/img.asp?attid=21408

[19] Media konvertor TP-link. In: *Alternetivo.cz* [online]. © 1996-2013 Alternetivo [cit. 16.04.2014]. Dostupné z: http://www.alternetivo.cz/media-konvertor-10-100base-tx-fx-rady-mc-singlemode-20km-sc-duplex-tx1310nm-rx1310nm-neriditelny-9v_ies40877.jpg

[20] UTP categories. In: *Nbiton.info* [online]. © 2014 Nbiton Solutions Pvt. Ltd. [cit. 10.04.2014]. Dostupné z: http://www.nbiton.info/uploads/8/8/6/9/8869636/9303242_orig.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
AON	Active Optical Network
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CSV	Comma Separated Values
ČTÚ	Český telekomunikační úřad
ČÚZK	Český úřad zeměměřický a katastrální
dB	Decibel
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
FHSS	Freguency Hopping Spread Spectrum
FSO	Free Space Optic
FTTH	Fiber To The Home
GBE	Giga Byte Ethernet
GbIC	Gigabit interface converter
GHz	Giga Hertz
IPv4	Internet Protocol version 4
LAN	Local Area Network
LS0H	Low Smoke Zero Halogen
MAC	Media Access Control
MAN	Metropolitan Area Network
Mb/s	Megabit za sekundu
MIC	Message Integrity Code
MM	Multimode
MSDU	Mac Service Data Unit

NAT	Network Adress Translation
ODN	Optical Distribution Network
OEO	Optical-Electrical-Optical
OLT	Optical Line Termination
ONT	Optical Network Termination
ONU	Optical Network Unit
OOO	Optical-Optical-Optical
OSI	Open Systems Interconnection
PCI	Peripheral Component Interconnect
PoE	Power over Ethernet
PON	Passive Optical Network
PSK	Pre-shared Key
SM	Singlemode
SSID	Service Set Identifier
SSL	Secure Socket Layer
TB/s	TeraByte za sekundu
TDM	Time Division Multiplex
TKIP	Temporal Key Integrity Protocol
ÚOOÚ	Úřad pro ochranu osobních údajů
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VPN	Vitual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK