

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Diplomová práce

Zabezpečení a monitoring bezdrátové sítě pro poskytovatele internetu

Bc. Miroslav Šůch

© 2012 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Šůch Miroslav

Veřejná správa a regionální rozvoj nav.- Klatovy

Název práce

Zabezpečení a monitoring bezdrátové sítě pro poskytovatele internetu - rezervováno Šůch

Anglický název

Security and monitoring wi-fi network for internet service provider

Cíle práce

Cílem práce je popsat a analyzovat současnou počítačovou bezdrátovou síť poskytovatele internetu, popsat základní komponenty, softwarové vybavení a funkčnost celé této sítě. Na základě této analýzy pak navrhnout monitoring i zabezpečení sítě tak, aby došlo ke správnému a bezpečnému chodu počítačové sítě a k rychlému sběru potřebných dat o skutečném a aktuálním stavu takové sítě, a tedy k rychlé reakci poskytovatele na odstraňování síťových potíží, což povede nejen k usnadnění práce poskytovatele, ale především ke zvýšení spokojenosti zákazníků.

Metodika

Analýza současné počítačové sítě bude provedena metodou skutečného fyzického zjištění stavu jednotlivých přístupových bodů, jejich kontrolou, zhodnocením a popsáním jednotlivých hardwarových komponentů, dále monitorováním těchto přístupových bodů pomocí softwaru Winbox a pochopitelně i studiem odborných informačních zdrojů. Praktická část je zaměřena na vytvoření administrativní aplikace, která bude klíčová pro monitoring celé internetové sítě poskytovatele, a která bude výsledkem pro reálné využití v této síti a povede k naplnění cíle této práce.

Harmonogram zpracování

- 1) Studie odborných informačních zdrojů: do 6/2011
- 2) Fyzická kontrola a analýza současné počítačové sítě a její popsání: 7/2011-10/2011
- 3) Navržení a vytvoření aplikace pro monitoring sítě: 11/2011-1/2012
- 4) Vytvoření finálního dokumentu diplomové práce: 3/2012
- 5) Odevzdání diplomové práce a téze: 3/2012

Rozsah textové části

60 - 80 stran

Klíčová slova

Síť, Wi-fi, routerboard, Winbox, acces point, topologie,

Doporučené zdroje informací

1. SOSINSKY Barrie. Mistrovství počítačové sítě. Vydání 1. Nakladatelství Brno: Computer Press 2010. ISBN 978-80-251-3363-7
2. A. DONAHUE Gary. Kompletní průvodce síťového experta. Vydání 1. Nakladatelství Brno: Computer Press 2009. ISBN 978-80-251-2247-1
3. PUŽMANOVÁ, Rita. TCP/IP v kostce. Vydání 1. Nakladatelství České Budějovice: KNOPP 2004. ISBN 80-7232-236-2.
4. HORÁK, Jaroslav.; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. Vydání 4. Nakladatelství Brno: Computer Press 2008. ISBN 978-80-251-2073-6.
5. ZANDL, Patrik. Bezdrátové sítě WIFI – Praktický průvodce. Dotisk prvního vydání. Nakladatelství Brno: Computer Press 2006. ISBN 80-7226-632-2.

Vedoucí práce

Vasilenko Alexandr, Ing.

Termín odevzdání

duben 2012

doc. Ing. Zdeněk Havlíček, CSc.

Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr.h.c.

Děkan fakulty

V Praze dne 21.5.2011

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Zabezpečení a monitoring bezdrátové sítě pro poskytovatele internetu“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v seznamu literatury na konci této práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 20. 3. 2012

.....

vlastnoruční podpis

Poděkování

Rád bych touto cestou poděkoval především vedoucímu práce p. Ing. Alexandru Vasilenkovi za přínosné konzultace, odborné rady a poznatky, které byly využity při sepsání této práce, a které jsou v současné době aplikovány na bezdrátové síti poskytovatele internetu firmy Sky-Soft s. r. o. v Blovicích. Poděkování patří i této firmě, která mi umožnila několika-měsíční sledování a přístup k její síti a po vypracování této práce a několika konzultací souhlasila s její realizací a aplikací do její stávající sítě. Nemalé poděkování patří také firmě K2Computer se sídlem v Nepomuku, okr. Plzeň-jih, kde jsem získal při provádění praxe důležité poznatky týkající se nejen síťové technologie.

Zabezpečení a monitoring bezdrátové sítě pro poskytovatele internetu

Security and monitoring wi-fi network for internet service provider

Souhrn:

Diplomová práce stručně popisuje vývoj bezdrátové technologie, její komponenty a funkčnost a charakterizuje současný stav bezdrátové sítě poskytovatele internetu v obci Blovice, okr. Plzeň-jih a jeho blízkém okolí. Analyzuje monitoring i zabezpečení sítě, popisuje podrobně její komponenty a hledá rizika v souvislosti s funkčností celé sítě, možných výpadků jednotlivých přístupových bodů, ale i samotné konektivity internetu. V diplomové práci je rovněž proveden výzkum týkající se spokojenosti stávajících zákazníků této sítě a zodpovězení základních otázek jako je funkčnost a spolehlivost připojení, četnost a doby jednotlivých výpadků internetu a dalších důležitých otázek, které jsou podstatné pro charakteristiku celé sítě. Diplomová práce na základě této analýzy navrhuje konkrétní řešení vedoucí k vylepšení této sítě, a to především v zabezpečení a monitoringu, jelikož právě tyto aspekty jsou jedny z nejdůležitějších pro zaručení správného chodu celé sítě.

Summary:

This thesis briefly describes the development of wireless technology, its components and functionality. It characterizes the current status of wireless network in the town Blovice, Pilsner-south region and its surroundings. It analyzes monitoring and network security and describes its components in details. It also looks for risks related to network functionality, possible downtime caused by individual access codes as well as Internet connectivity itself. A research is also done in the thesis. It relates to the existing customers' satisfaction who use this network. It also brings their answers to basic questions such as functionality and reliability of connection, frequency and duration of individual outages of the Internet and other important questions which are essential to characterize the whole network. On the basis of this analysis the thesis proposes a specific solution leading to improvements of this network, mainly in getting its security and monitoring. The reason is that these aspects are just some of the most important ones to guarantee the correct operation of the whole network..

Klíčová slova:

ISP (Poskytovatel internetových služeb), síť, wifi, topologie, přístupový bod, směrovač, blok dat, síťový počítač.

Keywords:

ISP (Internet service provider), network, wi-fi, topology, access point, router, paket, server.

OBSAH

1	ÚVOD.....	9
2	CÍL PRÁCE A METODIKA	11
3	POČÍTAČOVÁ SÍŤ A KOMPONENTY	12
3.1	VŠEOBECNÁ DEFINICE POČÍTAČOVÉ SÍŤE	12
3.2	TYPY SÍŤÍ.....	12
3.2.1	PAN (Personal Area Network).....	12
3.2.2	LAN (Local Area Network).....	13
3.2.3	WAN (Wide Area Network).....	14
3.3	TOPOLOGIE SÍŤE.....	14
3.3.1	Fyzická topologie.....	14
3.3.2	Logická topologie.....	15
3.4	SÍŤOVÉ MODELY	15
3.5	SÍŤOVÝ HARDWARE	19
3.5.1	Server	19
3.5.2	Rack.....	20
3.5.3	Síťové rozhraní.....	20
3.5.4	Přenosová média	21
3.5.5	Aktivní prvky síťe.....	23
3.6	WI-FI (BEZDRÁTOVÉ SÍŤE).....	26
3.6.1	Typy bezdrátových síťí.....	26
3.6.2	Standardy IEEE 802.11	27
3.7	SÍŤOVÉ OPERAČNÍ SYSTÉMY.....	28
3.7.1	Free BSD.....	29
4	POČÍTAČOVÁ SÍŤ POSKYTOVATELE INTERNETU (ISP) SKY-SOFT S.R.O.....	30
4.1	KONEKTIVITA INTERNETU.....	30
4.2	HARDWAROVÉ KOMPONENTY PŘÍSTUPOVÝCH BODŮ.....	31
4.2.1	Konzole a místo pro umístění technologie.....	33
4.2.2	Mikrotik.....	34
4.2.3	MiniPCI karta CM9 a kabeláž k anténě	35

4.2.4	Antény	35
4.3	PROPOJENÍ PŘÍSTUPOVÉHO BODU HASIČSKÉ ZBROJNICE	37
4.3.1	technologie v pásmu 2,4 GHz	38
4.3.2	Technologie v pásmu 5 GHz	39
4.3.3	Způsob připojení zákazníků	40
4.4	SOUČASNÝ STAV ZABEZPEČENÍ A MONITORING SÍTĚ FIRMY SKY-SOFT	41
4.5	VÝZKUM SPOKOJENOSTI ZÁKAZNÍKŮ	44
4.5.1	Počet zákazníků	44
4.5.2	Dotazník	45
4.5.3	Výsledek dotazníkového šetření	45
4.6	VÝSLEDEK ZJIŠTĚNÉHO STAVU POČÍTAČOVÉ SÍTĚ ISP	46
5	VYTVOŘENÍ NOVÉHO ZABEZPEČENÍ A MONITORINGU POČÍTAČOVÉ SÍTĚ	48
5.1	ZABEZPEČENÍ SÍTĚ ISP	48
5.1.1	Záložní zdroje přístupových bodů	48
5.1.2	Zabezpečení přístupových bodů	50
5.2	MONITORING SÍTĚ ISP	52
5.3	ADMINISTRAČNÍ APLIKACE SERVERU	52
5.3.1	Tabulka databáze ADMIN	54
5.3.2	Tabulka databáze Access pointy	58
5.3.3	Tabulka databáze zákazníci	67
5.3.4	Grafy zatížení	73
6	EKONOMICKÝ DOPAD	75
7	ZÁVĚR	77
8	SEZNAM OBRÁZKŮ	78
9	SEZNAM POUŽITÝCH ZDROJŮ	79
10	PŘÍLOHY:	81
10.1	PŘÍLOHA Č. 1 – UKÁZKA SOFTWARE WINBOX	81
10.2	PŘÍLOHA Č. 2 – DOTAZNÍK	82
10.3	PŘÍLOHA Č. 3 – VÝSLEDKY DOTAZNÍKŮ	84
10.4	PŘÍLOHA Č. 4 – ZNÁZORNĚNÍ KONFIGURACE MIKROTIKU PRO UPS	86
10.5	PŘÍLOHA Č. 5 – WEBOVÁ STRÁNKA – GRAFY	87

1 ÚVOD

Počítačové sítě jsou velmi rozsáhlým tématem a zasahují v podstatě do všech aspektů počítačových technologií. Existují i takové názory, že samotný počítač je vlastně síť a počítač bez sítě není počítačem. Ke vzniku těchto počítačových sítí pomohl především rozkvět osobních počítačů v osmdesátých a devadesátých letech dvacátého století. Vznikaly celé řady různých síťových technologií a vznikly i dnes nejmodernější síť TCP/IP a především internet. Společně s těmito technologiemi vzniká celá řada síťových prvků od různých výrobců a pochopitelně i různé softwary, které jsou dnes dostupné v podstatě všem. Jelikož za posledních několik let je poptávka po připojení počítačů do internetu velmi vysoká, vzniká celá řada velkých i malých firem, které se snaží svým zákazníkům nabídnout právě připojení do sítě internetu a to za různé měsíční poplatky a při různých rychlostech připojení. A právě jednou takovou malou firmou poskytující internetové připojení se zabývá tato práce.

Práce je rozdělena do tří hlavních částí. První teoretická část definuje obecně počítačovou síť se zaměřením na síť Wi-fi, přehled typů sítí, možné topologie, hardwarové komponenty jako jsou servery, síťové rozhraní, přenosová média a další.

Druhá, praktická část popisuje konkrétní počítačovou síť firmy Sky-Soft s. r. o., analyzuje její hardwarové komponenty, konektivitu internetu, architekturu sítě, i konfiguraci jednotlivých přístupových bodů doplněné grafickým znázorněním a pochopitelně i softwarové vybavení a funkčnost a to vše se souhlasem této firmy. Rovněž je zde proveden výzkum spokojenosti stávajících zákazníků s připojením do sítě internetu a tato část se snaží nalézt chyby a problémy, které se v síti vyskytují.

Třetí, praktická a stěžejní část této práce se zabývá vytvořením nového způsobu monitoringu a zabezpečení počítačové sítě poskytovatele a vytvořením aplikace, která bude nainstalována na základním serveru počítačové sítě, a na kterou bude možný přístup odkudkoliv z této sítě. Hlavním úkolem aplikace je neustálý monitoring všech přístupových bodů a to z hlediska funkčnosti přenosu dat a napájení. Veškeré tyto výpadky budou formou sms zpráv předávány na příslušná telefonní čísla pracovníků poskytovatele, kteří budou moci ihned řešit tyto síťové problémy. Další částí bude zabezpečit celou počítačovou síť tak, aby nebyla v žádném jejím místě volně přístupná neoprávněným osobám a v síti byly pouze zákazníci firmy Sky-Soft s. r. o.

Zhotovení této práce je zaměřeno na bezdrátovou síť v obci Blovice, okr. Plzeň-jih a její blízké okolí, která čítá celkem 23 vysílačů (přístupových bodů), a na které je v současné době připojeno celkem 147 zákazníků. Práce hodnotí rovněž ekonomický dopad na vytvoření takové administrace a veškeré změny s tím spojeny, které povedou k vylepšení chodu celé této sítě.

Tato práce se snaží popsat uvedenou problematiku v co možná nejjednodušší a nejsrozumitelnější podobě tak, aby byla pochopitelná nejen pro odborníky z řad IT, ale především pro laickou veřejnost a naplnila tak očekávané pochopení všem čtenářům. Z tohoto důvodu práce nepopisuje přesný krok za krokem všechny jednotlivé konfigurační příkazy a programování celkového systému, i když jsou nedílnou součástí takového nastavení, ale snaží se popsat toto nastavení co možná nejjednodušeji a s co možná nejméně použitými cizími termíny.

2 CÍL PRÁCE A METODIKA

Cílem této diplomové práce je na základě provedené analýzy současné počítačové sítě ISP vytvořit nový a funkční monitoring a kvalitnější zabezpečení této počítačové sítě. Výchozím problémem je popsání a analyzování současného stavu počítačové bezdrátové sítě poskytovatele firmy Sky-soft s. r. o. v Blovicích, okr. Plzeň-jih, zjištění a popsání základních komponentů, softwarového vybavení a celkové funkčnosti celé sítě. Na základě této analýzy je klíčové navrhnout a vytvořit monitoring i zabezpečení této sítě tak, aby došlo ke správnému a bezpečnému chodu, k rychlému sběru potřebných dat o skutečném a aktuálním stavu takové sítě, a tedy k rychlé reakci poskytovatele na odstraňování síťových potíží, což povede nejen k usnadnění práce poskytovatele, ale především ke zvýšení spokojenosti zákazníků.

Analýza počítačové sítě bude metodicky prováděna skutečnou fyzickou kontrolou všech přístupových bodů, zjišťováním funkčního stavu podle použitých hardwarových komponentů, dále pomocí příkazu PING a také prostřednictvím softwaru Winbox. Rovněž bude touto metodou provedena kontrola a způsob zabezpečení počítačové sítě proti možným výpadkům a proti možnému napadení cizích osob. Jako doplněk této analýzy, bude provedeno šetření mezi připojenými zákazníky za účelem zjištění spokojenosti těchto osob s poskytovatelem ISP. Toto šetření bude provedeno dotazníkovou metodou. Stěžejní část této práce je zaměřena na vytvoření nového a funkčního monitoringu, který bude implementován do současného systému a dále na vylepšení zabezpečení celé sítě, která bude spočívat nejen ve změně konfigurace, ale i v hardwarové změně některých přístupových bodů.

V konečné části bude zhodnocen ekonomický dopad na vytvoření této administrační aplikace a nového zabezpečení.

3 POČÍTAČOVÁ SÍŤ A KOMPONENTY

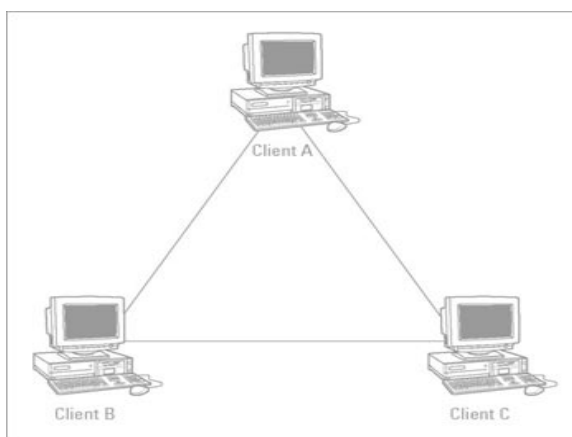
3.1 VŠEOBECNÁ DEFINICE POČÍTAČOVÉ SÍŤE

Počítačová síť znamená propojení dvou, nebo více počítačů mezi sebou za účelem vzájemné výměny dat. Takové síť se skládají z různých hardwarových komponentů, jako jsou počítače, přepínače, kabeláže, antény a podobně, a dále z propojovacích softwarů, které umožňují komunikaci mezi těmito počítači. Na základě těchto různých forem použití hardwaru, uspořádání, architektury a různým velikostem těchto sítí je můžeme rozdělit na různé typy s různou topologií.

3.2 TYPY SÍŤÍ

3.2.1 PAN (PERSONAL AREA NETWORK)

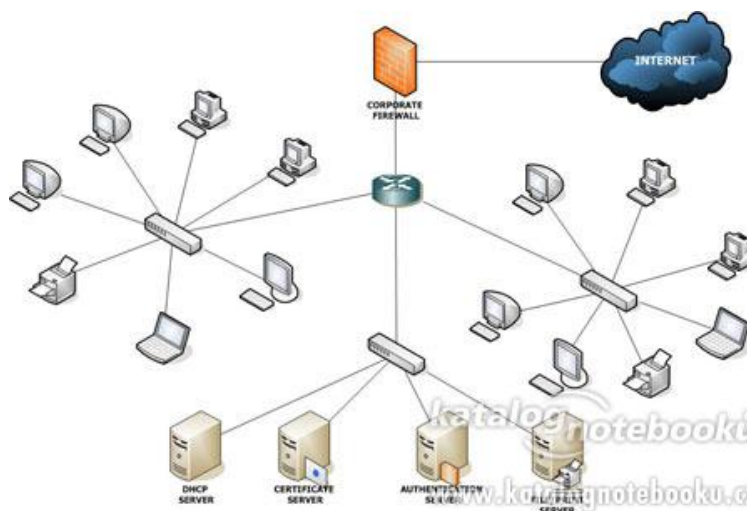
Počítačovou síť může tvořit jediný kabel propojující dva počítače. Takovéto propojení nazýváme sítí typu peer-to-peer ve které nejsou žádné jiné komponenty, které by zprostředkovali komunikaci. V této síti si jsou počítače rovnocenné. Jedná se tedy o nejmenší síť nazývající se personální síť LAN, tedy pLAN. Pokud by tímto způsobem byly počítače propojeny bezdrátovým přenosem, tak takovou síť nazýváme sítí Ad-hoc. Síť Ad-hoc se používají jen zřídka a využití si najdou jen tam, kde je propojeno malé množství počítačů na krátkou vzdálenost. Další uplatnění je například u typického spojení technologie Bluetooth různých elektronických zařízení jako je PDA, mobilní telefony, nebo i bezdrátová sluchátka.



Obrázek 1 - Schéma zapojení Peer to Peer. Dostupný na WWW: <http://pocitacovesite.blog.cz/>

3.2.2 LAN (LOCAL AREA NETWORK)

Jedná se o lokální, nebo také místní síť. Samotný pojem místní síť je však velmi subjektivní. Obecně můžeme za LAN síť požadovat propojení určitého množství počítačů v jedné místnosti, nebo na jednom patře budovy, či také celé jedné budovy nebo areálu budov určité firmy. Na druhou stranu může být taková síť tvořena jen malým počtem počítačů a jedním rozbočovačem¹. Asi základním rozdělením sítě LAN je různá adresace jednotlivých zařízení. Pokud v síti narazíme na zařízení, které je přemostovacím prvkem a rozděluje nám adresací počítačovou síť, můžeme hovořit o dvou LAN sítích, které spojuje právě tento síťový prvek. Pokud uvažujeme například o soustavě počítačů, které jsou ve stejné podsíti v rozsahu adres 192.168.250.100 až 192.168.250.200 a jsou umístěny v celém areálu jedné firmy, tak se jedná o jednu síť LAN, která poté vstupuje do sítě internetu s jiným rozsahem pomocí inteligentního zařízení, kterým může být například modem od firmy O2. Pokud však budeme uvažovat o stejné firmě, která má v jedné budově síť s adresací v rozsahu 192.168.250.100 až 192.168.250.200 a v druhé budově rozsah 192.168.1.100 až 192.168.1.200, můžeme hovořit o dvou sítích LAN, které jsou navzájem propojeny inteligentním síťovým zařízením a společně poté obě tyto LAN sítě vstupují prostřednictvím uvedeného modemu do sítě internetu.

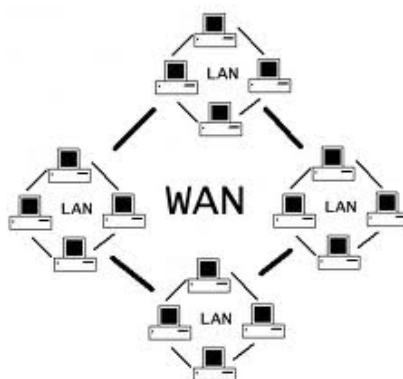


Obrázek 2 - Síť LAN. Dostupný na WWW: <http://clanky.katalognotebooku.cz/notebooky-clanky/co-je-lan/>

¹ Rozbočovač je síťové zařízení, které je podrobněji vysvětleno v kapitole 3.5. Hardware

3.2.3 WAN (WIDE AREA NETWORK)

Jedná se o rozsáhlou velkou síť propojující více sítí LAN. Klasickým příkladem takové sítě je samotný internet. Takové sítě se budují pro jednotlivé společnosti a jsou soukromé, ale budují je i jednotlivé malé firmy poskytující internet, jako je i firma Sky-Soft s. r. o., která je klasickým providerem, nebo také ISP². U těchto rozsáhlých sítí můžeme hovořit i o jiných menších sítích s názvem jako je MAN či CAN. MAN (Metropolitan Area Network) je označení pro síť v určitém městě a CAN (Campus Area Network) je označení pro síť o určitém počtu, či skupině budov. Vždy se jedná stejně jako u sítě LAN o subjektivní posouzení.



Obrázek 3 - Síť WAN. Dostupný na WWW: <http://www.networkingtipsblog.com/networking/wan-computer-networks/>

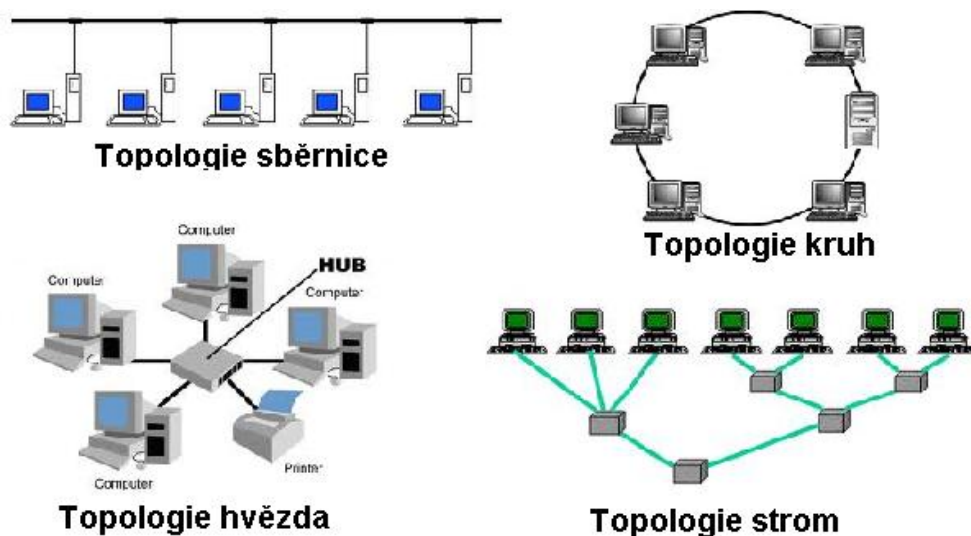
3.3 TOPOLOGIE SÍTĚ

Jedná se o jiný způsob klasifikace počítačových sítí. V zásadě topologii můžeme rozdělit na dvě hlediska a to topologii fyzickou a topologii logickou.

3.3.1 FYZICKÁ TOPOLOGIE

Fyzická topologie popisuje vztah mezi jednotlivými zařízeními, které tvoří síť. Takovými zařízeními mohou být koncové prvky sítě, uzly či spoje a kabeláže. Existuje několik typů fyzické topologie. Mezi nejpoužívanější patří Bus (Sběrnice), Star (Hvězda), Ring (Kruh) a Tree (Strom). V praktickém provedení sítí se však tyto typy kombinují a mají tedy různé provedení.

² ISP –Internet service provider – poskytovatel internetových služeb



Obrázek 4 - Druhy fyzické topologie. Dostupný na WWW: <http://euler.fd.cvut.cz/predmety/UP1/up1-3.html>, http://www.brainbell.com/tutorials/Networking/Ring_Topology.html, <http://ictsmksh.blogspot.com/>, <http://ct.upce.cz/machalik/puitk-stare/site/prvni.htm>

3.3.2 LOGICKÁ TOPOLOGIE

Základním principem logické topologie je mapování trasy, kterou prochází pakety³ od jednoho zařízení k druhému. Aby mohla být logická topologie funkční, musí být v síti dostupné uzly prostřednictvím potřebných protokolů, které se používají pro výměnu dat. Každé zařízení v síti musí být tedy nějak identifikovatelná. Základním identifikátorem každého síťového zařízení je jeho MAC adresa (Media Access Control adresa). Toto číslo je každému zařízení přiřazováno při jeho výrobě a někdy se mu také říká fyzická adresa. Pokud do sítě tedy zapojíme nějaký logický prvek, jako je přepínač, můžeme tento nakonfigurovat a tím změnit celou logiku topologie. Mezi logické topologie patří například logický řetěz a hvězda. Z toho také vyplývá, že logická topologie nemusí nutně kopírovat topologii fyzickou.

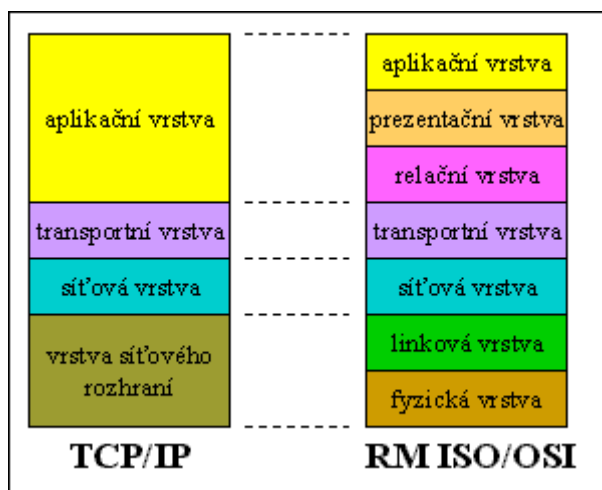
3.4 SÍŤOVÉ MODEL Y

Pro pochopení a funkčnost celé komunikace v síti je potřeba vysvětlit síťový model, který zajišťuje přenos dat mezi dvěma počítačovými systémy. Existují dva nejdůležitější modely a to ISO/OSI a TCP/IP. Každý je trochu odlišný a rozděluje zařízení,

³ Paket – blok dat, který je přenášen v počítačové síti a lze jej považovat za spolehlivý přenos dat

služby i software na skupiny vrstev dle architektury. OSI (Open Systems Interconnection od organizace ISO⁴ je model rozdělující komunikaci do sedmi vrstev. Každá vrstva, která přijme určitá data, obaluje tyto data dalšími informacemi a předává následující vrstvě. Mezi tyto vrstvy patří fyzická, linková, síťová, transportní, relační, prezentační a aplikační vrstva. Druhý model, kterým se budeme zabývat více je TCP/IP (Transmission Control Protocol/Internet Protocol). Tento model rozeznává ve své komunikaci jen čtyři vrstvy. Jedná se o vrstvu síťového rozhraní, síťovou, transportní a aplikační vrstvu.

Modely můžeme tedy definovat jako architekturu sítí, jejichž pomocí je možné popisovat počítačové sítě a zařízení. Vrstvy tvoří síťový zásobník, který na svém vrcholu operuje již s aplikacemi a s různým softwarem. Uprostřed modelu dochází k formátování dat a spodní vrstvu můžeme charakterizovat jako hardwarové komponenty. Při komunikaci musí data projít celým zásobníkem. V praxi to vypadá tak, že určitá aplikace vyšle data, které projdou zásobníkem tohoto vysílacího systému od shora dolů, dále prochází sítí až k přijímacímu systému a zde opět prochází od spodní vrstvy celým zásobníkem směrem nahoru. Modely jsou zobrazeny na následujícím obrázku.



Obrázek 5 - Model ISO/OSI a TCP/IP. Dostupný na WWW:
<http://www.earchiv.cz/anovinky/ai1592.php3>

⁴ ISO – Mezinárodní organizace pro normalizaci (International Organization for Standardization)

VRSTVA SÍŤOVÉHO ROZHRAŇÍ

Tato vrstva odpovídá dvěma spodním vrstvám v rámci modelu ISO/OSI. Umožňuje přístup k fyzickému přenosovému médiu a je zodpovědná za přístup k síti. Protokoly na této vrstvě umožňují systému doručit data jiných systémů, které jsou přímo propojené v síti.

SÍŤOVÁ VRSTVA

Síťová vrstva zajišťuje logickou, síťovou adresaci, směrování a předávání dat přes komunikační podsíť. Rovněž tato vrstva zajišťuje segmentaci a znovusestavování datagramů⁵ do nižších i vyšších vrstev. Mezi protokoly této vrstvy patří např. IP (Internet protokol), ARP (Address resolution protocol).

TRANSPORTNÍ VRSTVA

Tato vrstva nabízí mechanismus pro koncový přenos dat mezi dvěma stanicemi. Transportní služby jsou nabízeny se spojením, nebo bez spojením. Z toho také vycházejí dva nejnámější protokoly této vrstvy a to TCP a UDP.

TCP (Transmission Control Protocol) – je spolehlivý transportní protokol, který poskytuje transportní službu se spojením.

UDP (User Datagram Protocol) – je nespolehlivý transportní protokol a transportní službu poskytuje bez spojením.

Rozdíl mezi spolehlivým a nespolehlivým přenosem dat spočívá v tom, že pokud nastane při přenosu dat v síti chyba, při spolehlivém přenosu o tom odesílatel dostane zprávu, ale při nespolehlivém přenosu zprávu nedostane. Oba tyto protokoly tedy používají pakety, ale v případě UDP paketů se tyto označují jako datagramy.

APLIKAČNÍ VRSTVA

Je nejvyšší vrstvou v síťové architektuře a obsahuje všechny protokoly, které poskytují uživatelům konkrétní aplikace.

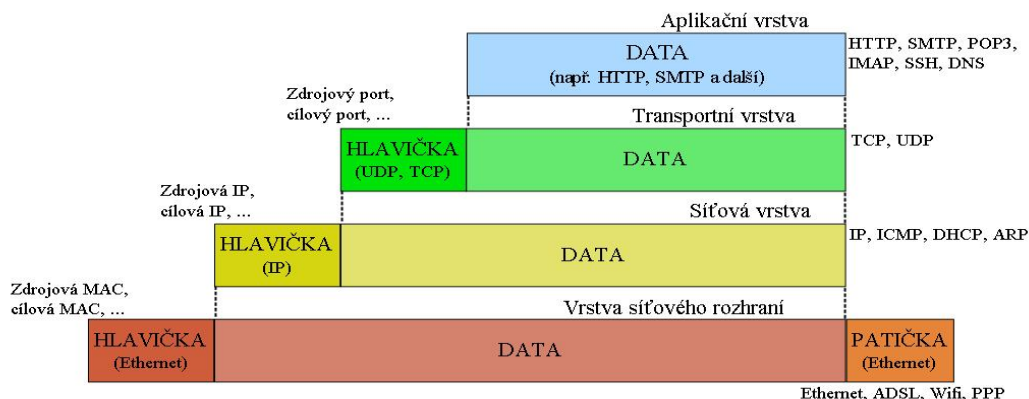
⁵ Datagram – základní jednotka přepravovaná v počítačové síti. Datagram lze chápat obdobně jako Paket, ale rozdíl je v tom, že datagram označuje službu nespolehlivého přenosu dat. Viz Transportní vrstva

Aplikační vrstvu můžeme charakterizovat i jako programy či procesy, které využívají uživatelé k přenosu dat po síti. Mezi takové protokoly patří například:

- FTP (File Transfer Protocol) – jedná se o protokol k přenosu souborů mezi počítači za pomoci počítačové sítě
- HTTP (Hypertext Transfer Protocol) – jedná se o internetový protokol, který je určen pro výměnu dokumentů ve formátu HTML (HyperText Markup Language – značkovací jazyk pro vytváření stránek v systému World Wide Web – www, umožňující publikovat různé dokumenty prostřednictvím internetu)
- DHCP (Dynamic Host Configuration Protocol) – protokol pro automatickou konfiguraci počítačů v síti. DHCP server přiděluje jednotlivým počítačům ve své síti potřebné konfigurační nastavení. Mezi takové patří IP adresa, maska podsítě, brána a DNS servery (viz. níže).
- DNS (Domain Name System) – jedná se o systém doménových jmen. Tento je realizován servery DNS. Hlavním úkolem tohoto protokolu je převod doménových jmen na IP adresy a obráceně.
- SNMP (Simple Network Monagement Protocol) – slouží ke správě počítačových sítí. Tento protokol sbírá průběžně různé data ze sítě a následně je vyhodnocuje. Proto je tento protokol základem pro různé aplikace pro správu sítě.
- POP3 (Post Office Protocol version3) – je to protokol, který se používá pro stahování emailových zpráv ze serveru do počítače.
- SMTP (Simple Mail Transfer Protocol) – Na rozdíl od protokolu POP3 se jedná také o protokol pro emailové zprávy, ovšem SMTP je určen pro odesílané elektronické zprávy. Zpráva se odesílá do schránky adresáta a z této si jej může adresát pomocí POP3 vyzvednout.

Zapouzdření dat v síti TCP/IP je znázorněno na následujícím obrázku.

ZAPOUZDŘENÍ DAT V SÍTI TCP/IP



Obrázek 6 - Síťové vrstvy TCP/IP. Dostupný na WWW:

<http://home.zcu.cz/~tody/kiv-zps/tcp-ip.html>

3.5 SÍŤOVÝ HARDWARE

Hardware jako takový vychází z anglického významu „železářské zboží“. Lze jej charakterizovat jako veškeré fyzicky existující technické vybavení počítače. Stejně tak u síťového hardwaru je to fyzické zařízení, které se používá pro samotnou počítačovou síť. Můžeme pochopitelně konstatovat, že i samotný počítač je síťový hardware, jelikož je s touto sítí propojen. Toto tvrzení lze chápat také jako správné, ale v této části se budeme zabývat pouze nejpoužívanějšími a nejrozšířenějšími prvky počítačových sítí a prvky, které jsou použity v síti internetového poskytovatele Sky-Soft s. r. o.

3.5.1 SERVER

Server můžeme definovat různými způsoby. V podstatě je to počítač, který je základním prvkem celé určité sítě, a který poskytuje určité služby jiným počítačům zapojeným v této síti. Jinak můžeme ovšem také říci, že server je software, neboli program, který poskytuje tyto služby jiným počítačům v síti. Samotné slovo server je tedy v informatice dosti volný termín. My jej však pro naše potřeby a vysvětlení budeme chápat jako počítač, na kterém je nainstalován speciální síťový operační systém. Ve spojení

s tímto systémem se tedy jedná o server, který poskytuje jiným počítačům v síti určité služby.

Servery jsou označovány podle své aplikační funkce. Nejčasněji rozeznáváme:

- Aplikační servery – Jedná se o databázové servery, e-mailové servery, webové servery a další. Pokud bychom za server považovali software, tak velmi často se používá pro tento název serveru název výrobce. Například Apache server
- Síťové servery – přesná definice není stanovena, ale takovýmto serverem se rozumí server zajišťující služby směrování, identifikace a další. Mezi servery patří například DNS a DHCP server
- Tiskové servery – jedná se o zařízení poskytující propojení tiskárny do sítě a tím umožňuje všem počítačům v této síti tisknout na jednu tiskárnu
- Zálohovací servery – servery, které ukládají a zálohují data

3.5.2 RACK

Jedná se o standardizované zařízení pro montáž různých síťových prvků či serverů, pro propojování těchto komponentů a k vyústění kabelových rozvodů pro další využití. Rack lze také popsat jako kovový rám s plechovými stěnami a kolejnicemi pro umístění různých switchů, UPS, serverů a dalších síťových zařízeních. Takový rack bývá často chlazen pomocí soustavy několika větráků. Toto zařízení často využívají poskytovatelé internetů k umístění své základní technologie.

3.5.3 SÍŤOVÉ ROZHRAŇÍ

Síťové rozhraní lze definovat jako hranici mezi různými médii, nebo také jako hranici mezi fyzickou komunikační vrstvou (rádiové vlny, dráty) a aplikačními vrstvami. Pojmům síťového rozhraní uvádí odborná literatura mnoho definic a vysvětlení. Asi nejjednodušším pro pochopení však síťové rozhraní můžeme definovat jako bod setkání různých sítí, který je však adresovatelný. Takovým bodem je především síťová karta, která přijímá a vysílá síťová data.

Karta síťového rozhraní je zařízením fungující na první síťové vrstvě TCP/IP, a proto ji lze chápat jako fyzické síťové rozhraní. Toto rozhraní je v síti adresovatelné,

a proto jej můžeme jmenovat partnerem komunikace. Adresaci lze rozdělit na adresaci fyzickou a logickou.

Fyzickou adresací je jedinečné 48bitové číslo zvané MAC adresa (Media Access Control). Tato adresa je obsažena v každé síťové kartě při její výrobě a je jedinečná. Logická adresace znamená, že se k fyzickému rozhraní připojí další identifikátor. Jedná se o číslo logické jednotky, jinak řečeno LUN (Logical Unit Number). Takovéto logické rozhraní může být nakonfigurováno pro více IP adres. Proto se také jediný počítač může v síti jevit jako by se jednalo o více různých systémů.

3.5.4 PŘENOSOVÁ MÉDIA

O přenosových médiích můžeme říci, že se vyskytují ve fyzické vrstvě a slouží k přenosu signálů od jednoho zařízení k druhému. Tyto média můžeme rozdělit na tři základní části. Metalické kabely, optické kabely a bezdrátové spoje.

METALICKÉ KABELY

Metalické kabely jsou nejpoužívanějšími a nejlevnějšími přenosovými médii v sítích. Na druhou stranu jsou však také nejméně výkonné. Mezi takové patří nejpoužívanější kroucený kabel, někdy také UTP kabel (Unshielded twisted pair). Jedná se o kabel, který je odvozen od telefonního kabelu a používá se především v sítích LAN. Vodič tvoří celkem osm vodičů, které jsou krouceny do čtyř párů a tyto páry jsou dále krouceny do jednoho celku kabele. Kroucení vodiče je provedeno z důvodu odbourání možného rušení a dosažení tak kvalitního přenosu. Na konci takového kabele je použit konektor RJ45. Tyto kabely se vyrábí i ve stíněném provedení, které jsou pochopitelně odolnější proti možnému rušení jako je magnetické pole, indukované napětí apod. Kabel se stíněním má označení STP (Shielded twisted pair)

Mezi další metalické kabely můžeme zařadit koaxiální kabel. Tento kabel tvoří dva vodiče, kdy vnější obaluje vnitřní, a po tomto vnitřním se přenášejí signály. Mezi těmito vodiči je izolace, která je mezi sebou odděluje. Horní vodič má stínící funkci a tento je pochopitelně také kryt ochranným pouzdem. V použití síťových spojů existují dva druhy těchto kabelů a to silný a tenký. Silný koaxiální vodič je obklopen čtyřmi vrstvami izolačního a stínícího materiálu. Použití takového kabelu se může využít především

v páteřních sítích, jelikož je kvalitnější, i když je náročnější na instalaci. Tenký koaxiální vodič, který je obklopen jen jednou vrstvou izolace je levnější, pružnější a méně náročný na instalaci. Současné době se však používá jen zřídka.

OPTICKÉ KABELY

Optické kabely, někdy také zvané jako světlovody jsou nejnovějšími přenosovými médii, které se používají v komunikačních sítích. Signál se zde šíří v podobě světla na rozdíl od metalických kabelů, kde se šíří v podobě elektrických impulzů. Světlo se pohybuje ve vlákne, které je izolováno sekundární ochranou. Tato ochrana zabraňuje ohybům kabelu a tím zabezpečuje průchod světelného paprsku. Na této sekundární ochraně je konstrukční vrstva a vnější obal. Zdrojem světla pro optické kabely jsou LED diody, nebo laserové diody, které jsou sice kvalitnější, ale podstatně dražší a také se méně využívají. Rozeznáváme dva typy optických kabelů, jednovidové a mnohovidové. Jednovidové kabely mají tenké vlákno a používají jako zdroj světla právě laser. Toto světlo má konstantní vlnovou délku a šíří se středem vlákna, aniž by se odráželo od hran izolace kabelu. Takové kabely se používají pro větší vzdálenosti, až několik desítek kilometrů. Mnohovidové kabely využívají jako zdroj světla světelnou diodu, která se skládá z více vlnových délek. Paprsek, který vniká do vlákna kabelu, se odráží od okrajů optického jádra a z tohoto důvodu je také dosahováno menších vzdáleností při přenosu.

BEZDRÁTOVÉ SPOJE

Bezdrátový spoj je tvořen vysílacím a přijímacím zařízením a představuje bezdrátovou síť. Bezdrátová síť je podrobněji rozebrána v bodě 3.6.

Mezi hlavní hardwarové komponenty pro bezdrátový přenos signálu patří antény. Antény mohou mít různé provedení i velikost, podle toho k jakému přenosu jsou určeny a na jakou vzdálenost mají data přenášet. Z těchto důvodů můžeme antény rozdělit na všesměrové, sektorové a směrové. Všesměrové antény šíří signál okolo sebe do všech stran, tedy pod úhlem 360 stupňů. Takové antény se používají tam, kde je potřeba souvislé pokrytí. Takové antény se používají například u malých wifi routerů pro použití v domácnostech, nebo je používají internetový poskytovatelé v malých obcích, či jednotlivých čtvrtí měst, kde je potřeba pokrýt signál plošně. Sektorové antény vyzařují

signál pod určitým úhlem, který může být různý. Takové antény se používají tam, kde je potřeba signálem vykrýt pouze určitou oblast. Umístění může být například na zdi budovy. Směrové antény jsou potom zvláštním druhem sektorových antén. Jedná se o parabolické antény ve tvaru síta, bubnu, nebo typu Yagi. Takové antény září pouze jedním směrem a jsou určeny především pro vytváření spojů na delší vzdálenosti. U antén je třeba zmínit, že nejdůležitějším parametrem je zisk. Tento zisk v podstatě uvádí výkon takové antény a udává se v dBi, neboli v decibelech na isotop. Laicky řečeno, čím větší bude zisk, tím vzdálenější signál může anténa zachytit. Dalším důležitým údajem pro antény je polarizace elektromagnetického vlnění. Pro bezdrátový přenos se používají polarizace lineární a kruhová. Lineární může být horizontální, nebo vertikální a kruhová polarizace může být pravotočivá, nebo levotočivá.

3.5.5 AKTIVNÍ PRVKY SÍŤE

Samotná síť, aby byla sítí, musí obsahovat aktivní propojovací prvky (zařízení), které vytváří nejen fyzickou síť, ale síť umožňující doručení dat na správná místa a ve správnou dobu. Data v síti můžeme označit tzv. pakety, které sítí prochází. Tyto pakety se přenáší kabely, nebo jinými přenosovými medii, ale výběr optimální trasy, kterou budou pakety procházet, nebo správnost těchto paketů, rozhodování kam paket má síť projít a kam ne a mnoho dalších úkolů musejí provádět další prvky, které jsou do sítě vloženy. Právě tyto prvky, které se aktivně podílejí na dění v síti označujeme aktivními prvky. Ostatní prvky jako např. kabeláž je prvkem pasivním.

Mezi takové aktivní prvky můžeme řadit rozbočovače, přepínače, směrovače, brány.

ROZBOČOVAČ (HUB):

Je velmi jednoduché zařízení, které propojuje síťové uzly⁶ ve stejném segmentu. Je podobný konektorům kabelů, avšak základem jeho funkce je rozvětvení. Jedinou vstupní linku dokáže propojit s několika dalšími spoji. Některé rozbočovače však dokáží tento procházející signál zesílit. V tom případě mluvíme o zesilovači, nebo také opakovači.

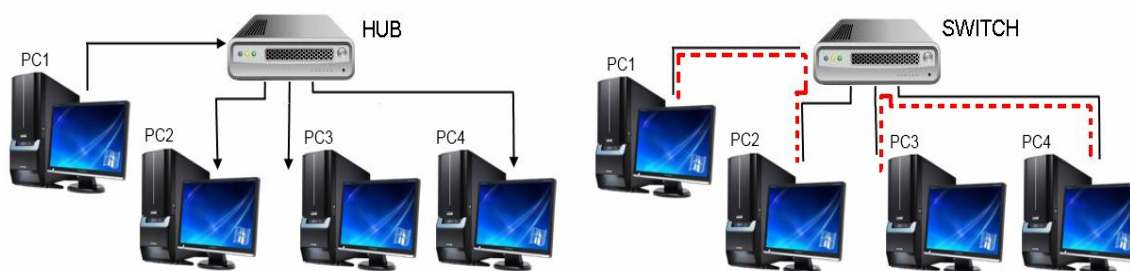
⁶ Síťový uzel lze definovat jako zařízení, které je připojeno do počítačové sítě. Takovým uzlem může být počítač, mobilní telefon, ale i další síťová zařízení jako switche, routery apod.

Rozbočovače však nejsou inteligentními prvky a nedají se administrovat. Každý paket, který do rozbočovače přijde je přeposlán všemi dalšími směry dále. Koncové zařízení, pro které je paket určen tento přijme, ostatní zařízení na jiných větvích tento nepřijmou. Nevýhodou takové komunikace je zahlcování cizími pakety a dochází ke zpomalování komunikace v síti.

PŘEPÍNAČ (SWITCH):

Skutečný název přepínač není nikde definován a neexistuje tedy žádná pevná definice přepínače. Často se tento termín používá třeba u rozbočovače, opakovače či mostu. Základním rozdílem od rozbočovače je však způsob přeposílání paketů. Přepínače dokáží budovat virtuální okruhy, které prochází skrze ně a vstupní pakety přeposílají těm uzlům pro které jsou určeny. Z toho důvodu je také přepínač inteligentnější zařízení než rozbočovač a nezahlučuje a nezpomaluje komunikaci v síti.

Rozdíl mezi Hubem a Switchem znázorňuje následující obrázek.



Obrázek 7 - Hub versus Switch. Dostupný na WWW:

http://kevincomputers.4fan.cz/?page_id=703

Pokud při propojení Hubem stanice PC1 pošle paket stanici PC2, tak tento paket prochází rozvětvením i k dalším zařízením v síti. Paket stanice PC2 přijme, ale ostatní stanice PC3 a PC4 tento nepřijmou, jelikož jim nepatří. Pokud však bude v síti Switch a stanice PC1 pošle paket stanici PC2, bude procházet pouze spojem pro stanici PC2 a ostatní stanice v síti nebudou tímto signálem zahlušeny. Stejně tak, pokud mezi sebou budou komunikovat i stanice PC3 a PC4, nebudou ovlivňovat a zpomalovat stanice PC1 a PC2.

SMĚROVAČ (ROUTER)

Patří mezi nejinteligentnější síťové aktivní prvky, které jsou administrovatelné. Dokáže pakety filtrovat a inteligentně je směruje. Sbírá informace o připojených sítích a vybírá nejvhodnější cestu, kterým paket pošle. Používá se pro rozdělení dvou rozdílných sítí. Mezi neznámější firmu zabývající se vývojem směrovačů patří firma CISCO⁷.

BRÁNA (GATEWAY)

Je zařízení, nebo software, který umožňuje vzájemnou komunikaci mezi rozdílnými sítěmi. Brány dokáží překládat síťové adresy, protokoly i samotná data. Bránu můžeme chápat i jako nižší hardwarový prvek, kterým může být směrovač, jelikož i ten umí přeložit síťovou adresu a v určitém kontextu tak může být bránou. Co však skutečně odlišuje bránu od ostatních zařízení je její fungování na vyšších vrstvách modelu ISO/OSI. Brány někdy fungují na čtvrté vrstvě, někdy však až na poslední sedmé vrstvě. Některé směrovače však zasahují maximálně do čtvrté vrstvy a nikdy ne výše.

Následující tabulka popisuje síťové vrstvy, na kterých jednotlivé aktivní prvky fungují.

Aktivní prvek	Funkce	Vrstva ISO/OSI
Rozbočovač (Hub)	Rozvádí signál do dalších větví	Fyzická
Přepínač (Switch)	Filtruje pakety a propojí pouze ty stanice, které spolu komunikují	Linková
Směrovač	Směruje pakety	Síťová
Brána	Propojuje dvě různé sítě	Aplikační

Tabulka popisující síťové vrstvy a aktivní prvky, vlastní zdroj

⁷ Cisco je jedna z největších a dominujících počítačových firem, která se zabývá vývojem síťových prvků a softwaru. Název cisco je odvozeno od slova San Francisco, kde má firma centrálu

3.6 WI-FI (BEZDRÁTOVÉ SÍŤE)

Bezdrátová síť je taková síť, kde se jednotlivé síťové prvky nepropojují pomocí kabeláže, ale bezdrátovým médiem. Toto médium je vlastně rádiová frekvence pracující nejčastěji v pásmech 2,4 a 5 GHz. Šířka pásma je rozdělována na jednotlivé kanály.

Pro bezdrátové síť se používá název WiFi, neboli Wireless Fidelity. Podle klasifikace velikosti můžeme tyto síť rozdělit podobně jako kabelové na:

- Wireless Personal Area Network (WPAN)
- Wireless Local Area Network (WLAN)
- Wireless Wide Area Network (WWAN)

Bezdrátová síť lze budovat různými způsoby a to podle toho jakou má plnit funkci. Nejdůležitější roli v bezdrátové počítačové síti tvoří identifikátor SSID (Service Set Identifier). Jedná se v podstatě o název bezdrátové síť, která je svým způsobem i klíčem pro vzájemné spojení stanic. Pokud by se klíč klientské stanice neshodoval s klíčem přístupového bodu, není komunikace možná. Z tohoto důvodu lze tento parametr SSID považovat za první úroveň zabezpečení. Tento parametr se běžně nechává otevřený a všechny klientské zařízení jsou schopny tento název síť vidět. Avšak pro větší bezpečnost je možné SSID skrýt a tudíž se tento identifikátor klientům nezobrazuje, nebo se síť zobrazuje jako nepojmenovaná a tím se může zabránit připojením neoprávněných osob.

3.6.1 TYPY BEZDRÁTOVÝCH SÍŤÍ

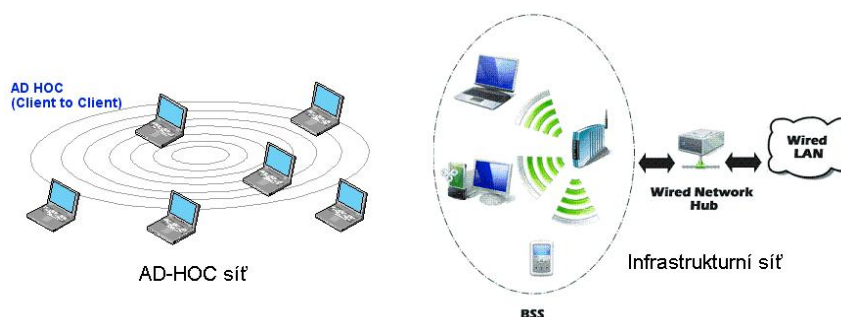
V bezdrátové síťové komunikaci existují dva typy architektury, kterými jsou **Ad-hoc** a **infrastrukturní režim**.

AD-HOC

je typická pro WPAN, což je obdoba peer-to-peer u kabelového propojení, ovšem přenosovým médiem zde není kabel, ale rádiová frekvence. Tímto způsobem mezi sebou počítače komunikují přímo bez jakéhokoliv dalšího zařízení a jedná se tedy o nejmenší bezdrátové počítačové síť, kterými si však více zabývat nebudeme.

INFRASTRUKTURNÍ SÍŤ

Základem infrastrukturní sítě je přístupový bod neboli access point (AP), jedná se o zařízení, které spojuje bezdrátovou část sítě s kabelovou částí a lze chápat podobně jako aktivní prvek v kabelové síti. Přístupový bod je schopen komunikovat s více než jen jednou stanicí a může tedy propojovat i jiné stanice nezávisle na tom, zda tyto stanice chtějí vstupovat do kabelového ethernetu, či nikoliv. Komunikace mezi jednotlivými stanicemi tedy neprobíhá přímo jako u Ad-hoc, ale prostřednictvím tohoto přístupového bodu.



Obrázek 8 - Ad-hoc versus Infrastrukturní síť. Dostupný na WWW: <http://images.yourdictionary.com/mobile-ad-hoc-network>, <http://www.djmichal.osoba.cz/informace-o-wifi>

3.6.2 STANDARDY IEEE 802.11

IEEE: „plný název Institute of Electrical and Electronics Engineers (česky „Institut pro elektrotechnické a elektronické inženýrství“) je mezinárodní nezisková profesní organizace usilující o vzestup technologie související s elektrotechnikou. Tento institut čítá nejvíce členů technické profese ve světě, a to přes 360 000 ve 175 zemích. Sídlo má v USA ve státě New Jersey“⁸.

IEEE 802 můžeme chápat jako standardy týkající se počítačových sítí. Mezi takové patří například 802.3 – Ethernet, 802.16 – bezdrátový přenos na vysokých frekvencích, nebo 802.11 – Wifi. A právě standard 802.11 - Wifi je důležitou součástí k pochopení přenosového média bezdrátové sítě. V současné době existují čtyři hlavní standardy IEEE

⁸ Citace: IEEE. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 18.1.2012 [cit. 2012-01-31]. Dostupné z: <http://cs.wikipedia.org/wiki/IEEE>

802.11, a to 802.11a, 802.11b, 802.11g, a 802.11n. Každý tento standard má svou přenosovou rychlost a frekvenci. Jasný rozdíl znázorňuje následující tabulka.

Dalším důležitým standardem pro bezdrátový přenos je standard 802.16 – Broadband Wireless Access. Jedná se o širokopásmový bezdrátový přenos, někdy označován jako IEEE 802.16 WirelessMAN. Tento standard využívá vysoké frekvence v rozmezí od 10 do 66 GHz. Tyto pásma jsou licencovaná, což znamená, že pro využití takové technologie musí mít firma licenci od národního regulátora, kterým je Český telekomunikační úřad.

Standard	Pásmo v GHz	Maximální rychlost v Mbit/s
802.11a	5	54
802.11b	2,4	11
802.11g	2,4	54
802.11n	2,4 nebo 5	600

Tabulka znázorňující Standardy IEEE 802.11

3.7 SÍŤOVÉ OPERAČNÍ SYSTÉMY

Síťový operační systém je systém poskytující síťové služby jiným systémům v síti. Musí poskytovat podporu hardwaru, spouštět protokoly a služby, a tyto služby poskytovat klientům v síti. Pochopitelně musí umožňovat správu, zálohování, zabezpečení, síťové směrování a další služby. Síťový systém, který nabízí takové široké spektrum funkcí se označuje jako platforma. Takovou platformou může být například UNIX, Linux, nebo Microsoft Windows. Některé síťové systémy jsou určeny pouze ke konkrétním účelům, jako například IOS (Internetwork Operating System), což je síťový systém od společnosti Cisco a který funguje právě na směrovačích a prepínačích Cisco.

Za prototyp operačního síťového systému lze považovat UNIX, který byl základem a ze kterého se vyvíjely další síťové systémy. Mezi takové lze uvést například Linux, Free BSD, Sun OS, Net BSD, Open Solaris a další.

Síťové operační systémy bývají nejčastěji nasazovány na serverovém hardwaru, který společně tvoří výkonný a základní síťový prvek typický pro poskytovatele internetu, jako je tomu i v případě firmy Sky-Soft s. r. o. Konkrétně firma Sky-Soft používá systém Free BSD.

3.7.1 FREE BSD

Jedná se o svobodný operační systém vycházející z UNIXU, který byl vyvinut na Kalifornské Univerzitě v Berkley. Pojem svobodný znamená volný, nebo také free software, který obsahuje i zdrojový kód a je s ním zaručeno právo jej používat, modifikovat a distribuovat. Tento software je vyvíjen jako kompletní operační systém společně s uživatelskými utility a to stejnou skupinou vývojářů, čímž se liší například od Linuxu, kde je každý program vyvíjen jinou skupinou a poté jako kompletní celek je vydán jinými vývojáři ve formě Linuxových distribucí. FreeBSD je všeobecně velmi používaný operační systém, který je pokládán za spolehlivý, stabilní a robustní.

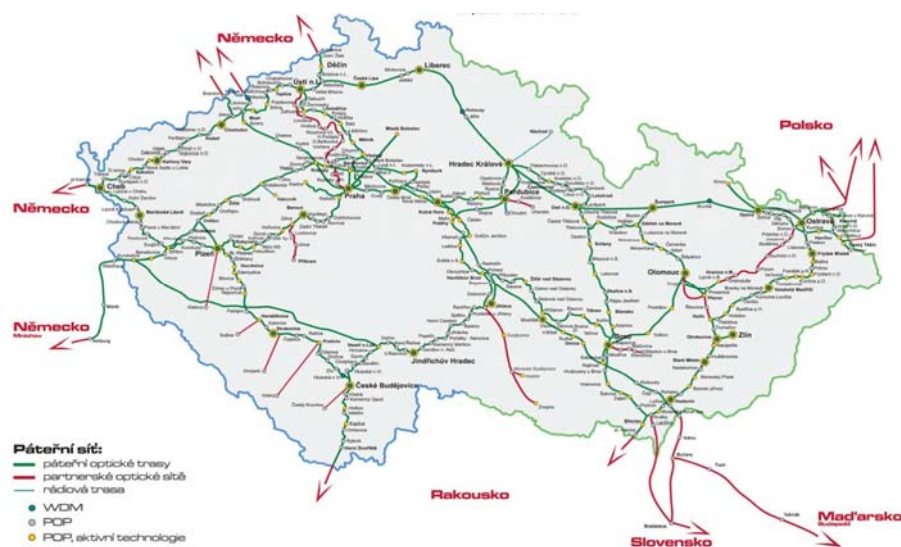
4 POČÍTAČOVÁ SÍŤ POSKYTOVATELE INTERNETU (ISP) SKY-SOFT S.R.O.

Tato praktická část popisuje skutečnou charakteristiku počítačové sítě poskytovatele internetu Sky-Soft v obci Blovice a jeho blízkém okolí. Metodický způsob zjištění tohoto stavu sítě byl proveden skutečnou fyzickou kontrolou všech těchto přístupových bodů, zdokumentováním jednotlivých hardwarových komponentů a rovněž softwarovou kontrolou pomocí příkazů ping a pomocí softwaru Winbox.

4.1 KONEKTIVITA INTERNETU

Konektivita internetu v podstatě znamená připojení veřejné sítě internetu na síť poskytovatele (ISP). S tím samozřejmě souvisí, způsob jakým je tato konektivita odebrána, místo, kde je toto spojení provedeno, rychlost připojení, která je poskytovateli prodávána a samozřejmě i cena za konektivitu.

Firma Sky-Soft kupuje konektivitu od firmy Sloane Park Property Trust, a.s. (dále jen Sloane Park). Sloane Park je firma, která má vlastní rozsáhlou optickou síť, a která se zaměřuje na velkoobchodní prodej konektivity a datových okruhů. Tato síť vznikala nejprve podél ropovodu Mero, a dále podél železničních tratí, stejně jako například síť ČD Telematiky. Síť je znázorněna na následujícím obrázku.



Obrázek 9 - Síť Sloane Park. Dostupný na WWW:

<http://www.lupa.cz/clanky/na-nakup-sloane-park-si-brousi-zuby-upc/>

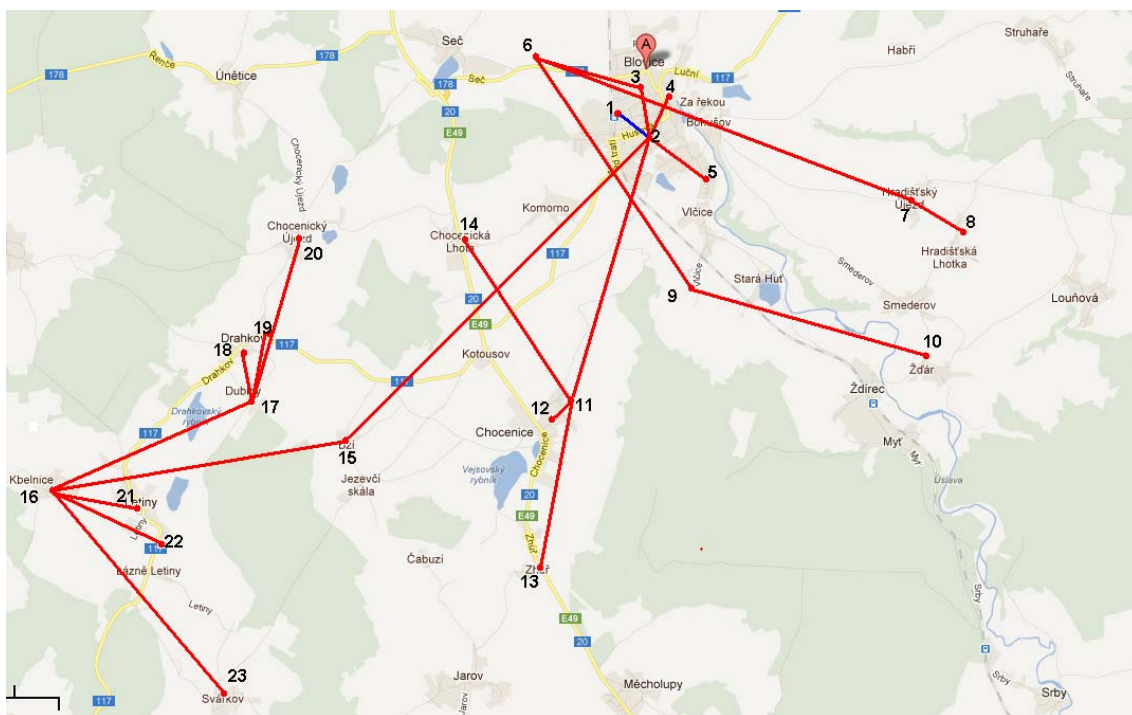
Konektivita je poskytována optickým mnohovidovým vláknem, které je přiveden do technické místnosti v budově Českých drah v Blovicích. Rychlost této konektivity je 44 Mbit/s a cena za uvedenou rychlost je 18.000,-Kč, kterou firma Sky-Soft měsíčně hradí na účet firmy Sloane Park.

Tato konektivita je dále přivedena do základního serveru celé této sítě, který je umístěn v rackové skříni v technické místnosti ČD Blovice. Server zde plní základní část celé této sítě. Z tohoto serveru je konektivita bezdrátově přenášena na první a základní přístupový bod budovy Hasičské zbrojnice Blovice. Tento spoj konektivity je proveden pomocí technologie 10 GHz anténou Alcoma. Na této budově je umístěno bezdrátové zařízení Mikrotik a několik antén poskytující samotnou konektivitu jak zákazníkům, tak dalším přístupovým bodům. Spojením těchto přístupových bodů vzniká síť poskytovatele, a na každém takovém bodě je několik antén poskytující konektivitu koncovým zákazníkům. Způsob propojení jednotlivých bodů, jejich umístění a technologie je znázorněna na obrázcích č. 10 a 11 a je označena čísly 1 až 23.

4.2 HARDWAROVÉ KOMPONENTY PŘÍSTUPOVÝCH BODŮ

Celou počítačovou síť tvoří celkem 23 přístupových bodů (vysílačů). Na každém takovém vysílači je soustava několika antén a základní zařízení Mikrotik, které řídí provoz takového vysílače. Základní technologie těchto bodů pracují na frekvencích 2,4 GHz, nebo 5 GHz, a tímto způsobem jsou připojeni do počítačové sítě i jednotliví zákazníci. Co se týče spojení mezi jednotlivými body, to je provedeno pomocí směrových, nebo sektorových antén a technologií 5 GHz, vyjma základního spoje mezi budovou ČD a hasičskou zbrojnicí, kde je využito spojení technologií 10 GHz. Každý přístupový bod má tedy jednu směrovou anténu, která signál přijímá od jiného vysílače a jednu vysílací na další přístupový bod, pokud ovšem není konečným vysílačem sítě, jako je například vysílač č. 10 v obci Žďár. Tato vysílací anténa je buď směrová, pokud je použita na delší vzdálenosti, nebo sektorová, pokud je použita na kratší vzdálenosti. V případě použití sektorové antény na kratší vzdálenosti se na takovou anténu nepřipojuje jen samotný další vysílač sítě, ale i zákazníci v jejím dosahu. Dále je na každém vysílači jedna, nebo více antén, které signál vysílají a pokrývají tak daný okruh, nebo místo pro který jsou určeny. Takové antény pracuje také v pásmu 2,4 GHz, nebo 5 GHz. Některé přístupové body mají

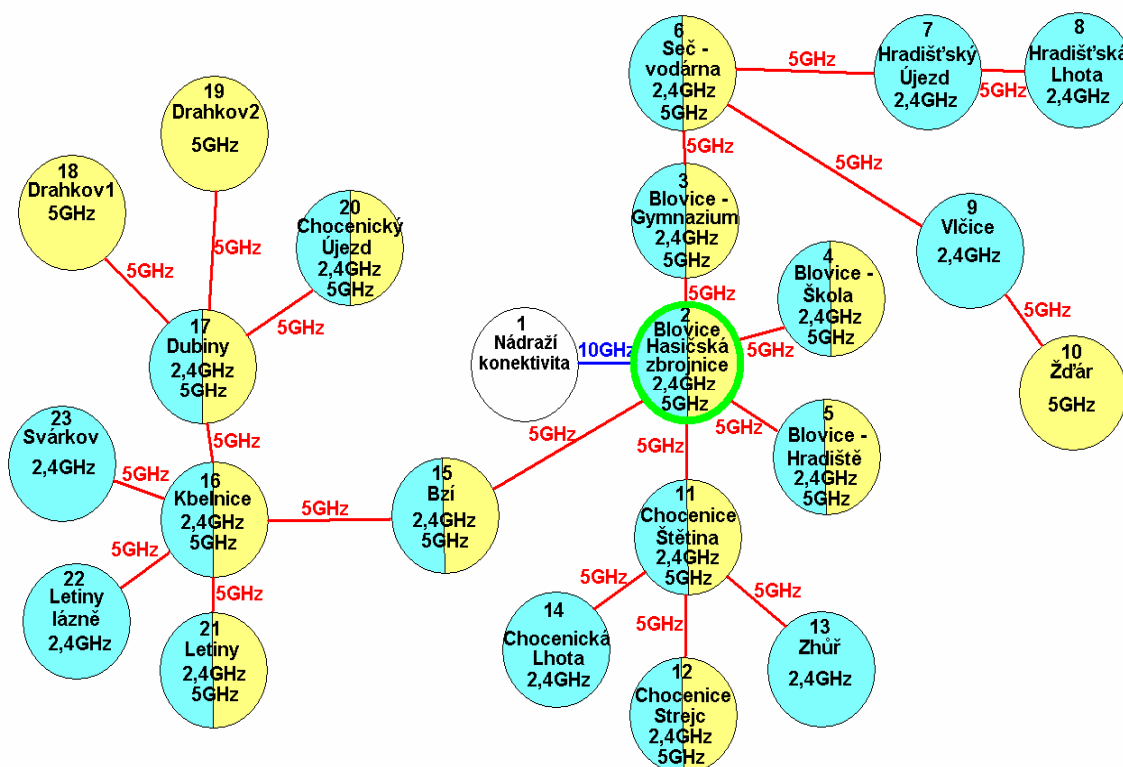
obě tyto technologie, tedy obě antény, jiné vysílače mají jen jednu anténu a to buď pracující v pásmu 2,4 GHz, nebo v pásmu 5 GHz. Vše je graficky znázorněno na obrázku č. 10 a 11, kde je znázorněna celá síť firmy Sky-Soft v obci Blovice a jeho okolí. Z těchto obrázků rovněž vyplývá fyzická architektura (topologie), kterou je topologií strom. Jelikož cílem práce není popsat do detailu všechny tyto přístupové body, ale především vysvětlit princip a způsobu propojení, je zde popsán jeden konkrétní vysílač a jeho komponenty. Jedná se o vysílač hasičské zbrojnice, kde je použita veškerá technologie, kterou lze v síti nalézt. Tento přístupový bod je na obrázku 11 označen v zeleném kroužku. Jelikož se jedná o největší vysílač v celé této síti a je zde použito větší množství antén, je to také jediný vysílač, kde jsou použity dva Mikrotiky, jelikož do jednoho nelze zapojit tak velké množství wifi miniPCI karet a tedy zapojit tolik antén.



Obrázek 10 - Mapa přístupových bodů, vlastní zdroj

Obrázek č. 10 znázorňuje geograficky skutečné umístění vysílačů v jednotlivých obcích a jejich vzájemné propojení. Na následujícím obrázku č. 11 je graf znázorňující tyto vysílače, jejich použitou technologii vysílajících frekvencí a pochopitelně jednotlivé propojení těchto vysílačů mezi sebou. Žlutou barvou jsou označeny vysílače, které vysílají

signál pro zákazníky v pásmu 5 GHz a modrou barvou vysílače, které poskytují signál v pásmu 2,4 GHz. Jednotlivé spoje jsou označeny barvou červenou pracující v pásmu 5 GHz a spoj Alcoma pracující v pásmu 10 GHz barvou tmavě modrou.



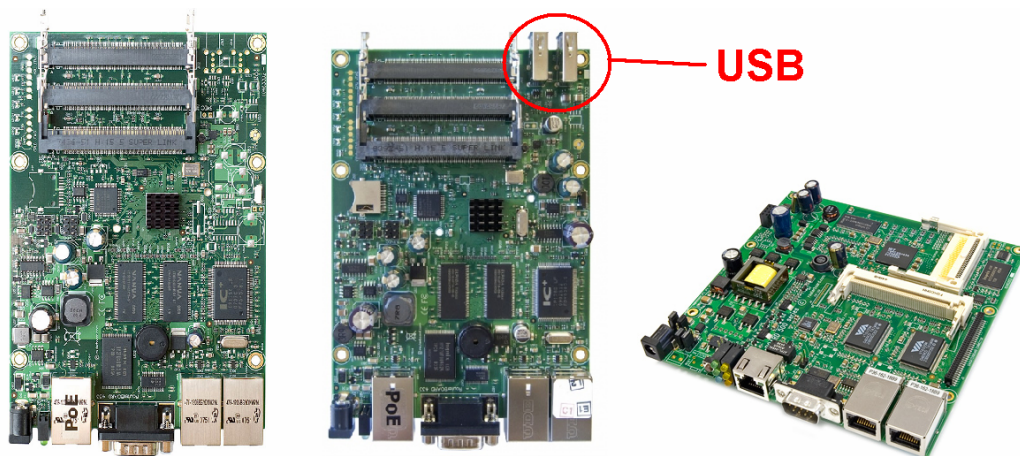
Obrázek 11 - Znázornění vysílačů a jejich vysílací frekvence, vlastní zdroj

4.2.1 KONZOLE A MÍSTO PRO UMÍSTĚNÍ TECHNOLOGIE

Základem každého přístupového bodu je jakási konstrukce (konzole) na které jsou jednotlivé antény usazovány, a dále vodotěsné a prachu-vzdorné místo, kde je umístěn základní prvek sítě, kterým je Mikrotik. Samotný Mikrotik je umístěn v plastové, vodotěsné bedně, a pokud je to možné je celá tato bedna ukryta na půdách domů, nebo v jiných blízkých a krytých místech samotné konstrukce pro antény. Antény se na konzole usazují tak, aby jedna nepřekrývala druhou a každá tak měla nejlepší možný vyzářovací úhel svého vysílání.

4.2.2 MIKROTIK

Mikrotik, někdy také RouterBoard (RB) patří mezi nejkvalitnější a v sítích ISP mezi nejpoužívanější routery. Jedná se o router v podobě desky, na kterém jsou osazeny sloty pro miniPCI karty, několik ethernetových portů pro konektory RJ45, konektor pro napájení, konektor RS232 pro konfiguraci a u některých Mikrotiků i USB konektor. Existuje celá řada těchto routerů a podle typu mají různý počet slotů pro miniPCI karty a různý počet ethernetových portů. V síti firmy Sky-Soft jsou použity routery RB433, RB 433UAH a RB532. Součástí RouterBoardu je dále RouterOS, což je operační program tohoto zařízení pracující na systému Linuxu a umožňující tak celkovou funkci takového Mikrotiku.



Obrázek 12 – Mikrotiky RB433, RB433UAH, RB532. Dostupný na WWW: http://mikrotik.tlupa.com/?page_id=150, http://mikrotik.tlupa.com/?page_id=167, http://infodepot.wikia.com/wiki/Mikrotik_Routerboard_RB-532_vA

Toto zařízení je konfigurováno pomocí softwarového programu Winbox, což je program pracující pod systémem Windows a souží ke správě všech těchto Mikrotiků v síti. Každý takový Mikrotik je nastaven tak, aby vyhovoval požadavkům v síti a plnil tak veškeré potřebné funkce sítě v daném přístupovém místě.

Na vysílači hasičské zbrojnice jsou použity dva Mikrotiky typu RB433UAH. První Mikrotik č. 1 ovládá dvě směrové antény pracující v pásmu 5 GHz a jednu všesměrovou anténu pracující v pásmu 2,4 GHz. Druhý Mikrotik č. 2 ovládá sadu tří sektorových antén pracující v pásmu 5 GHz.

V celé síti ISP je použito 7 Mikrotiků typu RB433UAH, které jsou na páteřních spojích vysílačů označených čísly 2, 3, 6, 11, 15, 16. Tyto routerboardy jsou navíc opatřeny konektory USB, jak ukazuje předchozí obrázek. Dále jsou v síti použity tři Mikrotiky typu RB433 a to na zbylých páteřních vysílačích označených čísly 7, 9 a 17. Ostatní vysílače, které jsou koncovými body v síti jsou opatřeny Mikrotiky typu RB532. V tomto případě se jedná o vysílače čísel 4, 5, 8, 10, 12, 13, 14, 18, 19, 20, 21, 22, 23.

4.2.3 MINIPCI KARTA CM9 A KABELÁŽ K ANTÉNĚ

MiniPCI je wifi karta, která je umístěna v jednom ze slotů Mikrotiku a která je dále pomocí pigtailu propojena s anténou. Karta má na sobě konektor UFL určený pro připojení pigtailu. Tato karta podporuje normy 802.11 a/b/g, je osazena výkonným čipem Atheros AR5213 a zaručuje maximální citlivost, spolehlivost a odolnost proti rušení. Karta se softwarově nastaví tak, aby vysílala buď v pásmu 2,4 GHz, nebo v pásmu 5 GHz podle potřeby. Tato karta je pomocí pigtailu a koaxiálního kabele propojena s patřičnou anténou. Pigtail je malý kabel o délce 20 cm, který je na jedné straně osazen konektorem UFL pro připojení do miniPCI karty a na druhé straně konektorem RSMA pro připojení koaxiálního kabele. Koaxiální kabel bývá různé délky a je propojen přímo s jednou anténou na vysílači. Je osazen konektory RSMA pro pigtail a konektorem N-Male pro anténu.



Obrázek 13 - Pigtail a koaxiální kabel. Dostupný na WWW:

<http://www.vseprowifi.cz/inshop/kabely/pigy-merene/>, <http://www.wifihw.cz/ufl-r-sma-f/>

4.2.4 ANTÉNY

Firma Sky-Soft používá pro pokrytí území a pro propojení jednotlivých vysílačů různé druhy antén. Jedná se o směrové, sektorové a všesměrové antény a to pracující v pásmu 2, 4, 5, ale i 10 GHz. Základní spoj z ČD na hasičskou zbrojnici je proveden pomocí technologie 10 GHz a to zařízením Alcoma.

ALCOMA A SMĚROVÉ ANTÉNY

Alcoma spol. s r.o. je ryze česká společnost, která vznikla v roce 1993 skupinou několika inženýrů, a která patří mezi špičkové a přední tuzemské výrobce radioreléových spojů. Firma Sky-Soft má pro tento spoj pronajatou od firmy Sloane Park jednu sadu antén typu Alcoma AL10D MP91. Jedná se o směrové antény.

Tento spoj je tvořen sadou dvou antén, který pracuje v kmitočtovém pásmu 10 GHz. Přenosová kapacita spoje je 44/66/88 Mbit/s. Vzhledem k tomu, že firma Sky-Soft v současné době kupuje konektivitu 44 Mbit/s je zde předpoklad do budoucnosti, že toto pojítko (sada antén) bude postačovat ještě několik let a kapacita rychlosti se bude moci zvyšovat bez toho, aniž by se muselo toto pojítko měnit. Elektronika tohoto spoje je v anténě zabudovaná do hliníkové slitiny, která splňuje nejvyšší nároky na klimatickou odolnost. Tento spoj patří mezi nejkvalitnější spoje a využívají je nejen někteří poskytovatelé internetu, ale i jiné firmy, které jsou pod dohledem Českého telekomunikačního úřadu. Vzhledem k cenové náročnosti takového spoje, který se pohybuje řádově kolem 80.000,- Kč patří tento spoj firmě Sloane Park a firma Sky-Soft jej má v pronájmu za cenu 1.500,- Kč měsíčně. Tato částka je zahrnuta v konektivě internetu, která, jak již bylo zmíněno činí 18.000,- Kč měsíčně. V případě výpadku či jiné nefunkčnosti tohoto spoje řeší tyto problémy samotná firma Sloane Park.

Mezi další směrové antény, které firma Sky-Soft používá pro svoje spoje mezi jednotlivými přístupovými body jsou antény typu síta a parabolických bubnů. Tyto antény pracují v pásmu 5 GHz a pomocí koaxiálních kabelů a pigtailů jsou propojeny s miniPCI kartou a Mikrotikem. Další specifickou anténou, která je v síti použita je anténa Airgrid M5 od firmy UBNT. Tato anténa je specifická tím, že má sama elektroniku – router zabudován přímo v hlavici antény a ke své činnosti tedy nepotřebuje jiné zařízení jako je Mikrotik, nebo jiný router. Sama je tedy nakonfigurovaná podle potřeby a lze ji také využít jako klientské zařízení zákazníků. Z této hlavice je zařízení propojeno do sítě kroucenou dvojlinkou (UTP kabelem). Na následujícím obrázku jsou zleva tyto antény: spoj Alcoma 10 GHz, síto 5 GHz, parabolický buben 5 GHz, Airgrid M5 - 5 GHz.



Obrázek 14 - Směrové antény. Dostupný na WWW: <http://avonet.cz/page/69021.alcoma-al10d-mp91/>, <http://www.i4wifi.eu/22-dbi-parabolic-antenna-grid-5-ghz-d919.html>, <http://www.az-pocitace.cz/z/acant1553/antena-5ghz-parabola-jrc-24-extrem-2xpack-antena-23dbi-s-licem-5-ghz>, <http://wifi.aspa.cz/ubnt-airgrid-m5-ant-23dbi-1xzaric-1xsito-mimo-5ghz-airmax-station-outdoor-klient-mimo-5ghz-z101920/>

Na samotném vysílači hasičské zbrojnice je použita anténa Alcoma pro spoj z nádraží a dále dvě směrové antény v podobě parabolického bubnu, které spojují vysílač Chocenice-Štětina a vysílač Bzí. Vše je znázorněno na obrázku č. 11.

SEKTOROVÉ ANTÉNY A VŠESMĚROVÉ ANTÉNY

Sektorové a všesměrové antény firma Sky-Soft využívá především pro připojení samotných zákazníků do své sítě. Způsob vysílání těchto antén je buď v pásmu 2,4 GHz, nebo 5 GHz. Sektorové antény vykrývají pásmo pokrytí pod určitým úhlem a všesměrové zabírají kolem sebe celé pásmo, tedy úhel 360 stupňů.

Konkrétně na vysílači hasičské zbrojnice jsou umístěny tři sektorové antény pracující v pásmu 5 GHz, a každá z nich vykrývá úhel 120 stupňů. Dohromady tak pokrývají celý prostor 360 stupňů kolem sebe a jsou dostatečně silné, aby na ně mohly být připojení jak zákazníci, tak i ostatní vysílače nacházející se také v obci Blovice. Konkrétně se jedná o vysílače Blovice-gymnázium, Blovice-škola a Blovice-Hradiště. Na vysílači je dále umístěna jedna všesměrová anténa pracující v pásmu 2,4 GHz a vykrývající také celý prostor 360 stupňů. Na této technologii jsou většinou připojeni zákazníci již několik let, kdy zde ještě technologie 5 GHz nebyla umístěna.

4.3 PROPOJENÍ PŘÍSTUPOVÉHO BODU HASIČSKÉ ZBROJNICE

Samotné komponenty vysílače hasičské zbrojnice byly popsány v předchozích kapitolách. Propojení těchto komponentů a prostup signálu je následující. Konektivita

je přivedena kroucenou dvojlinkou z pojiťka Alcomy do čtvrtého ethernetového portu Mikrotiku č. 1 označeného jako ether4 (viz. Příloha č. 1). Zde je signál rozdělen do tří miniPCI wifi karet a ethernetového portu č. 2. První wifi karta je určena pro všesměrovou anténu, která je nakonfigurována pro vysílání v pásmu 2,4 GHz a je určena pouze pro zákazníky. Druhá a třetí wifi karta propojuje dvě směrové antény pracující v pásmu 5 GHz a vysílající tento signál k dalším vysílačům v obci Chocenice a Bzí. Tyto jsou určeny tedy pouze pro spojení těchto vysílačů a zákazníci se na tyto antény nepřipojují. Signál je dále propouštěn do portu č. 2 Mikrotiku a z něj je konektivita vedena opět kroucenou dvojlinkou na první ethernetový port Mikrotiku č. 2. Tento druhý Mikrotik je osazen také třemi miniPCI Wifi kartami, které propojují již zmiňované tři sektorové antény pracující v pásmu 5 GHz, a které jsou určeny jak pro zákazníky, tak pro spojení vysílačů Blovice-gymnázium, Blovice-škola a Blovice-Hradiště.

4.3.1 TECHNOLOGIE V PÁSMU 2,4 GHz

Technologie 2,4 GHz je starším způsobem připojení, který je využíván poskytovatelem již několik let. V době, kdy firma Sky-Soft začínala nabízet tyto služby, byla tato technologie cenově nejdostupnější a splňovala veškeré požadavky, které měla síť plnit. Technologie byla funkční a hlavně cenově přijatelná, což mělo za následek rozvíjení této sítě a přibývání počtu přístupových bodů a tím i množství zákazníků. Ve stejném frekvenčním pásmu však pracují i jiné zařízení, jako jsou mikrovlnné trouby, bezdrátové telefony, Bluetooth, nebo třeba i různé hračky na bezdrátové ovládání, či chůvičky pro děti. Všechny tyto rozvíjející technologie společně s rozvíjejícím se počtem wifi připojení měli za následek vzájemné interference, a tím přibývání problémů v síti spojené nejen s rušením, ale někdy i s výpadky tohoto spojení. Postupem času a s vývojem nových technologií jako je pásmo 5GHz bylo, a v současné době ještě je, postupně přecházeno na toto nové pásmo, které má větší rozsah kanálů a není ovlivňováno uvedeným jiným zařízením.

Tato technologie je v současné době použita jen v místech, kde toto vzájemné rušení je minimální a to převážně v malých obcích, kde je menší počet lidí a kde není jiný poskytovatel internetu, který by svým vysíláním mohl také uvedené pásmo rušit.

Pro připojení zákazníků v tomto pásmu firma Sky-Soft využívá dva typy routerů a to WA2204 od firmy Zcomax a AirLive od firmy Ovislink, ke kterým je poté obdobně jako na vysílačích připojena pomocí koaxiálního kabelu anténa pro příjem takového signálu. Antény mohou být různé a liší se především svým výkonem a velikostí. Nečastěji jsou použity antény PAN10, nebo PAN14.



Obrázek 15 - Routery 2,4GHz - WA2204, Air-Live a anténa PAN10. Dostupný na WWW:
<http://www.i4wifi.cz/wa-2204a-54mbit-ap-kl-router-br-switch-2-4-ghz-d26.html>,
<http://cz.airlive.com/product/WL-5450AP>, <http://www.i4shop.net/cz/iObchod/WebInfo.asp?Id=185>

4.3.2 TECHNOLOGIE V PÁSMU 5 GHz

Tato technologie je oproti pásmu 2,4 GHz podstatě novější a je využívána pro připojení klientů od roku 2008. Technologie je méně náchylná na rušení okolních bezdrátových zařízení a rovněž dokáže přenést větší obsah dat za jednotku času, což přispívá ke zkvalitnění takového spojení.

Takovou technologii firma používá především v místech, kde je větší množství zákazníků a pochopitelně na své spojení mezi jednotlivými přístupovými body, což už bylo v předchozích odstavcích řečeno.

Mezi zařízení pracující v tomto pásmu, které firma využívá pro připojení svých zákazníků, patří především zařízení od firmy UBNT Nanostation M5, a Airgrid M5. Zvláštností těchto zařízení je to, že routery jsou zabudovány přímo v anténách, což vytváří toto zařízení multifunkčním a není potřeba zde zapojovat další prvky do sítě a rovněž odpadá koaxiální kabel, který je náchylný na ohyb. Manipulace s takovým zařízením je tak podstatně jednodušší a k takovému zařízení se připojuje kroucená dvojlinka pomocí konektoru RJ45.



Obrázek 16 - Nanostation M5 a AirGrid M5. Dostupný na WWW:
<http://www.streakwave.com/Itemdesc.asp?ic=NSM5>, <http://www.i4-wifi.com/?p=productsMore&iProduct=277&sName=ubnt-airgrid-m5-airmax-27-dbi>

4.3.3 ZPŮSOB PŘIPOJENÍ ZÁKAZNÍKŮ

Každému zákazníkovi je přidělena jedna IP adresa, což je číslo identifikující síťové rozhraní v počítačové síti. Tato IP adresa je nastavena na příjmové části každého zařízení (routeru), který zákazník při připojení obdrží. Tímto způsobem se stává zákazník, respektive jeho zařízení, jedinečným v síti poskytovatele a lze jej podle této IP adresy lehce dohledat. Taková IP adresa vypadá například následovně: 192.168.35.35

Zákazníkův router je nakonfigurován tak, aby poskytoval NAT (Network Address Translation), což znamená přeložení této adresy na jinou IP adresu a dále pomocí protokolu DHCP, který byl vysvětlen v aplikační vrstvě kapitoly 3.4 automaticky nakonfiguroval cílový počítač zákazníka. Router je schopný poskytnout řádově desítky různých IP adres v počítačové síti zákazníka a nakonfigurovat tak různý počet počítačů v jeho síti, které jsou připojeny na tento router. Cílové adresy jednotlivých počítačů mohou být například 192.168.250.1, 192.168.250.2, 192.168.250.3 atd. V praxi to znamená, že všechny tyto počítače zákazníka obdrží IP adresu ve stejném rozsahu, čímž je zabezpečena jejich vzájemná komunikace a přitom se navenek tváří pod jednou přeloženou IP adresou poskytnuto ISP. Tímto způsobem je uspokojen jak zákazník, který může mít v domácnosti připojeno více počítačů, aniž by musel řešit konfiguraci takového PC, tak i poskytovatel, který má spojenou se zákazníkem jedinečnou IP adresu a nemusí tak přidělovat více adres pod stejné jméno, což by mělo za následek nepřehlednost a složitost takového monitorování.

4.4 SOUČASNÝ STAV ZABEZPEČENÍ A MONITORING SÍTĚ FIRMY SKY-SOFT

Stejně jako každý router zákazníka, tak i každé zařízení v síti ISP je v síti identifikovatelné podle IP adresy. Toto zařízení (Mikrotik) má IP adresu v rozsahu 192.168.5.x a je z celé sítě poskytovatele přístupné právě pomocí této jeho IP adresy. Zabezpečení k přístupu je provedeno pomocí uživatelského jména a hesla, který znají pouze pracovníci firmy ISP a není tedy možné, aby se na tento přístupový bod připojila cizí osoba a nastavenou konfiguraci změnila.

Samotná konfigurace jednotlivých přístupových bodů je provedena tak, že každý vysílající signál v podobě SSID je zabezpečen WPA klíčem (Wi-Fi Protecte Access). Tento způsob využívá 128bitový šifrovací klíč a 48bitový inicializační vektor. Tímto je zabezpečeno, že se na vysílací signál poskytovatele může připojit jen takové zařízení, které toto zabezpečení zná a má tedy nakonfigurován tento bezpečnostní identifikátor.

Firma ISP nepoužívá žádnou aplikaci, která by kontrolovala on-line činnost těchto vysílacích bodů, ani funkci zařízení jednotlivých zákazníků. Jako svoji evidenci má firma vytvořenou pouze Excel tabulku, v níž je uvedeno jméno zákazníka, jeho bydliště, telefonní číslo, IP adresa, která mu byla přidělena, zařízení s MAC adresou, které má namontované pro připojení do sítě ISP a rychlost internetového připojení, které má k dispozici dle tarifu rychlostí podle stanoveného ceníku služeb. Ověření funkčnosti jakéhokoliv zařízení v síti, tedy Mikrotiků jednotlivých přístupových bodů i zařízení koncových zákazníků je prováděno náhodně a to pomocí příkazu PING, případně softwarem Winbox.

PING: „(anglicky Packet InterNet Grouper) umožňuje prověřit funkčnost spojení mezi dvěma síťovými rozhraními (počítače, síťová zařízení) v počítačové síti, která používá rodinu protokolu TCP/IP. Ping při své činnosti periodicky odesílá IP datagramy a očekává odezvu protistrany. Při úspěšném obdržení odpovědi vypíše délku zpoždění (latence) a na závěr zobrazí statistický souhrn“⁹.

Takový příkaz se provádí pomocí příkazového řádku Windows, kdy je potřeba vypsát příkaz ping a cílovou adresu, která se má v síti ověřit. Na následujícím obrázku

⁹ Citace: PING. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 26.12.2011 [cit. 2012-01-31]. Dostupné z: <http://cs.wikipedia.org/wiki/PING>

je provedena kontrola přístupového bodu hasičské zbrojnice s IP 192.168.5.250 a následně adresa jednoho vybraného zákazníka X ze Svárkova s IP adresou 192.168.70.70. Test byl proveden z PC připojeného na vysílač Vlčice.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.5.250 -t

Příkaz PING na 192.168.5.250 s délkou 32 bajtů:

Odpověď od 192.168.5.250: bajty=32 čas=6ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=5ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=4ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=5ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=2ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=7ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=2ms TTL=63
Odpověď od 192.168.5.250: bajty=32 čas=10ms TTL=63

Statistika ping pro 192.168.5.250:
Pakety: Odeslané = 8, Přijaté = 8, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
  Minimum = 2ms, Maximum = 10ms, Průměr = 5ms
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.70.70 -t

Příkaz PING na 192.168.70.70 s délkou 32 bajtů:

Odpověď od 192.168.70.70: bajty=32 čas=10ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=11ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=54ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=16ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=70ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=9ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=11ms TTL=253
Odpověď od 192.168.70.70: bajty=32 čas=9ms TTL=253

Statistika ping pro 192.168.70.70:
Pakety: Odeslané = 8, Přijaté = 8, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
  Minimum = 9ms, Maximum = 70ms, Průměr = 23ms

```

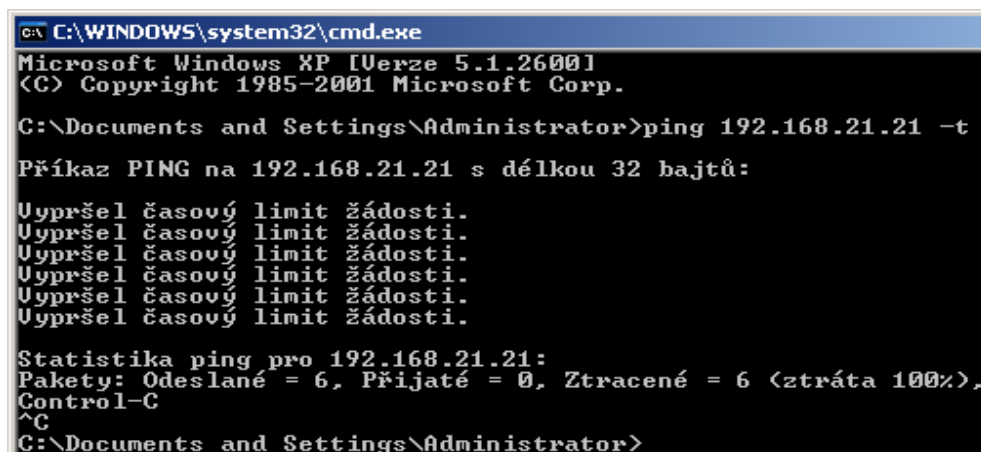
Obrázek 17 - Příkaz PING, vlastní zdroj

Příkaz na hasičskou zbrojnici byl vypsán, jak je vidět na třetím řádku tabulky, následovně: ping 192.168.5.250 -t. Atribut -t znamená, že příkaz bude prováděn neustále, dokud jej obsluha nezastaví stisknutím klávesy CTRL+C. Bez tohoto atributu by byly provedeny pouze tři testovací pingy (tedy proběhly by pouze tři zkušební řádky). Z výsledku testu je patrné, že došlo k nulové ztrátě paketů a odezva na Mikrotik hasičské zbrojnice je v průměru 5ms (milisekund), nejdelší doba byla naměřena 10ms a nejkratší doma 2ms. Jednotlivé časy každého takového pingu jsou znázorněny na předposledním sloupci čas=XXms. V případě проверки zákazníka X s IP 192.168.70.70 je zjištěno, že rovněž nedošlo ke ztrátě žádných paketů a průměrný naměřený čas je 23ms, nejdelší čas je 70ms a nejkratší 9ms.

Porovnáním těchto dvou jednoduchých testů je zjištěno, že čas datagramu s odezvou je u zákazníka X podstatně delší než u hasičské zbrojnice, což je dáno vzdáleností a počtem jednotlivých přístupových bodů. Patrné je to z obrázku č. 11, kdy z PC připojeného na vysílač č. 9 v obci Vlčice prochází datagram cestou přístupových bodů: Vlčice(9) – SečVodárna(6) – BloviceGymnazium(3) – Hasičská zbrojnice(2) a zpět, zatímco datagramu na zákazníka X prochází cestou přístupových bodů: Vlčice(9) – SečVodárna(6) – BloviceGymnazium(3) – Hasičská zbrojnice(2) – Bzí(15) – Kbelnice(16) – Svárkov(23) – PC zákazníka X a zpět.

Tímto jednoduchým testem byly rovněž otestovány všechny vypsané přístupové body, kterým datagram procházel. Kdyby byl totiž jeden z nich nefunkční, tak by datagram nemohl projít a test by byl neúspěšný.

V tomto případě by vypadal výsledek takového testu tak, jak znázorňuje obrázek č. 18. Z výsledku jasně vyplývá, že nebyla provedena ani jedna odpověď z IP adresy 192.168.21.21. Výsledkem tedy je, že bylo odesláno celkem šest paketů, přijaté nebyly žádné a ztráta se rovnala šesti, tedy sto procentům.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.21.21 -t

Příkaz PING na 192.168.21.21 s délkou 32 bajtů:

Upršel časový limit žádosti.
Upršel časový limit žádosti.
Upršel časový limit žádosti.
Upršel časový limit žádosti.
Upršel časový limit žádosti.
Upršel časový limit žádosti.

Statistika ping pro 192.168.21.21:
Pakety: Odeslané = 6, Přijaté = 0, Ztracené = 6 (ztráta 100%).
Control-C
^C
C:\Documents and Settings\Administrator>
```

Obrázek 18 - Neúspěšný ping, vlastní zdroj

Dalším způsobem, kterým lze zjistit funkčnost jednotlivých vysílačů je pomocí softwaru Winbox. Připojením tímto způsobem na Mikrotik lze zjistit nejen funkčnost samotného Mikrotiku, ale i funkčnost jednotlivých miniPCI wifi karet včetně vysílacích antén, jejich kvality spojení apod. Dle tohoto softwaru lze zjistit aktuální stav připojených

zákazníků na tento vysílač, vyčíst IP adresy, které jsou s vysílačem spojeny a jak dlouho, sílu signálu mezi vysílačem a zákazníkem, sílu signálu mezi jednotlivými vysílači a lze zjistit i množství dat, které vysílačem prostupují. Celou řadu těchto, ale i dalších informací nám Mikrotik poskytne a na základě toho můžou technici Mikrotik konfigurovat tak, aby byl vyladěn co možná nejefektivněji a byl plně funkční a spolehlivý.

Winbox lze také charakterizovat jako aplikaci pro konfiguraci routerů Mikrotik a to pomocí grafického rozhraní Windows. Ukázka tohoto softwaru je přílohou č. 1 této práce a jedná se o kontrolu mikrotiku na hasičské zbrojnici. Z této aplikace lze vidět levou postraní lištu s různými záložkami pod kterými se může provádět konfigurace samotného Mikrotiku. Je zde otevřena první záložka Interface a dále okno InterfaceList ve kterém jsou znázorněny rozhraní mikrotiku na hasičské zbrojnici. Základním rozhraním je ether 4, který označuje přívod konektivity do Mikrotiku. Jako další rozhraní jsou zde pro ukázkou otevřeny wlan1_SKYSOFT_stanice a wlan4_spoj_bzi. Z obrázku je patrné, že wlan1 je anténa vysílající na frekvenci 2,4GHz a jedná se tedy o zákaznickou anténu pracující v tomto pásmu pod SSID: SKYSOFT_stanice. Druhá anténa wlan4 pracuje na frekvenci 5 GHz a to pod SSID: spoj_bzi. Z toho vyplývá, že se jedná o směrovou anténu, která spojuje vysílač Bzi č. 15.

Kontrolou všech přístupových bodů tímto softwarem nebyly zjištěny žádné podstatné chyby, které by měly vliv na nekvalitní přenos dat v bezdrátových spojích. Signály mezi jednotlivými přístupovými body jsou plně dostačující.

Další kontrola byla tímto softwarem provedena za účelem zjištění připojeným MAC adres na jednotlivé přístupové body. Tyto MAC adresy byly porovnány s tabulkou zákazníků (Excel-tabulka), kterou firma používá jako svoji evidenci zákazníků. Výsledkem bylo zjištěno, že do počítačové sítě poskytovatele byly připojeny dvě MAC adresy, které neodpovídali seznamu zákazníků. Z toho se lze domnívat, že se jedná o dvě neoprávněné osoby, které se do sítě připojili například znalostí WPA hesla.

4.5 VÝZKUM SPOKOJENOSTI ZÁKAZNÍKŮ

4.5.1 POČET ZÁKAZNÍKŮ

Firma Sky-Soft má v současné době ve své počítačové síti připojeno celkem 147 zákazníků. Kontrolou již vytvořeného seznamu bylo zjištěno, že 87 zákazníků je do sítě

připojeno modernější technologií 5 GHz a 60 zákazníků starší technologií 2,4 GHz. Z těchto šedesáti lidí je 26 lidí připojeno v místech, kde firma nemá na svých vysílačích technologii 5 GHz, a proto není v současné době možné tyto lidi připojit jiným způsobem.

4.5.2 DOTAZNÍK

Pro zjištění spokojenosti zákazníků s internetovým připojením a službami s tím souvisejících byl k tomuto výzkumu vytvořen krátký dotazník, který je přílohou č. 2 této práce. Dotazník byl rozeslán prostřednictvím poštovních adres i prostřednictvím e-mailů všem 147mi zákazníkům. Dotazník byl anonymní a cílem bylo zjistit především takové skutečnosti, které by vedly ke zjištění nejčastějších problémů v síti a na základě toho se také zaměřit na patřičné změny, které povedou ke zlepšení chodu počítačové sítě a tím i k lepšímu zabezpečení a monitoringu takové sítě.

4.5.3 VÝSLEDEK DOTAZNÍKOVÉHO ŠETŘENÍ

Ze 147mi dotazníků, které byly rozeslány, bylo vyplněno a vráceno celkem 116 dotazníků, což odpovídá 79ti procentům všech zákazníků připojených do sítě poskytovatele. Ač byl dotazník anonymní téměř u všech těchto vyplněných dotazníků byly uvedeny podpisy zákazníků a to konkrétně ve 108mi případech. Z tohoto důvodu lze odpovědi dotazníku považovat za velmi přesné a odpovídající skutečnému stavu počítačové sítě.

Výsledky dotazníku uvádí tabulka a grafické vyjádření, které jsou přílohou č. 3 této práce. Výsledky jednotlivých odpovědí jsou uvedeny jak v číselných hodnotách, tak v procentech z celkového množství odpovědí. Výsledky uvádí především střední až velkou nespokojenost zákazníků s internetovým připojením. Celkovou úroveň služeb poskytovatele považuje 58,7 procent zákazníků za průměrnou a 26,7 procent za špatnou. Pouze 14,6 procent zákazníků považuje úroveň služeb za velmi dobrou. Rovněž větší procento zákazníků uvádí časté výpadky internetového připojení a firmu ISP by ve větší části nedoporučili jiným potenciálním zákazníkům.

4.6 VÝSLEDEK ZJIŠTĚNÉHO STAVU POČÍTAČOVÉ SÍTĚ ISP

Fyzickou kontrolou jednotlivých přístupových bodů poskytovatele, sledováním celé této sítě prostřednictvím příkazů ping i softwaru Winbox, konzultací s pracovníky firmy Sky-Soft a provedeným průzkumem u zákazníků lze konstatovat následující výsledky.

Žádný z vysílačů není opatřen záložním zdrojem elektrické energie, jako je UPS (Uninterruptible Power Supply – nepřetržitý zdroj energie), kromě samotného místa konektivity, kterým je nádraží ČD Blovice. Zde je umístěn záložní zdroj APC Smart-UPS 1000VA. Jedná se o velmi kvalitní záložní zdroj, který je majetkem firmy SloanePark a stejně jako základní spoj Alcoma je tento firmou Sky-Soft pronajat. Cena je zahrnuta do celkové ceny pronájmu základního spoje, jak už bylo uvedeno. Absence záložních zdrojů na ostatních vysílačích má za následek, že jakýkoliv výpadek elektrického proudu v místě přístupového bodu má vliv na jeho funkčnost a tím i funkčnost všech ostatních přístupových bodů, které jsou připojeny za ním. K tomu je potřeba také konstatovat, že výpadek elektrického proudu je poměrně častou záležitostí, i když doba výpadků většinou není dlouhá. Nejčastěji dochází k výpadkům v období bouřek a tehdy se doba výpadků rapidně zvyšuje. Přesto takové výpadky trvají přibližně jednu hodinu.

Neexistuje žádný způsob, který by automaticky sděloval pracovníkům firmy ISP výpadky této sítě. Tyto skutečnosti lze zjistit pouze náhodným kontrolováním sítě, jak již bylo popsáno v předchozích kapitolách. Takové kontroly se provádí přibližně jednu hodinu denně, většinou při začátku pracovní doby.

Vysílací frekvence všech přístupových bodů jsou zabezpečeny pouze WPA klíčem, který v současné době není nejlepším možným řešením a lze jej za určitých podmínek, jako jsou schopnosti a softwarového vybavení prolomit. Rovněž byly v síti nalezeny dvě MAC adresy, které byly připojeny neoprávněně.

Celá počítačová síť je sice funkční, ale je velmi náchylná na poruchy v podobě výpadků. Monitoring sítě lze hodnotit jako minimální a zabezpečení rovněž odpovídá spíše standardním a domácím způsobům ochrany, což u poskytovatele internetových služeb lze považovat spíše za nedostačující.

Rovněž spokojenost zákazníků s internetovým připojením je spíše průměrná až podprůměrná, což má negativní vliv na celkový pohled této firmy, její profesionalitu i kvalitu.

Výsledek tohoto šetření a zjištění skutečného stavu počítačové sítě ISP jasně ukazuje na nutnost vytvořit nový systém zabezpečení a monitoringu počítačové sítě tak, aby síť byla spolehlivější, kvalitnější, lépe zabezpečena a zákazníci byly spokojenější. Firma by se poté mohla pyšnit dlouhodobou profesionalitou, stabilitou a schopností rychle řešit servisní zásahy.

5 VYTVOŘENÍ NOVÉHO ZABEZPEČENÍ A MONITORINGU POČÍTAČOVÉ SÍTĚ

Na základě zjištění skutečného stavu počítačové sítě poskytovatele internetu, jeho způsobu zabezpečení a monitoringu celé sítě, a rovněž dle výsledku dotazníkového šetření u jednotlivých zákazníků, bylo nutné vypracovat a vytvořit takovou aplikaci a provést takové opatření, která povedou ke zkvalitnění nabízených internetových služeb a především ke zlepšení zabezpečení a monitoringu celé této sítě.

Na základě těchto závěrů byly vytvořeny změny v počítačové síti, které jsou postupně rozepsány v následujících bodech.

5.1 ZABEZPEČENÍ SÍTĚ ISP

5.1.1 ZÁLOŽNÍ ZDROJE PŘÍSTUPOVÝCH BODŮ

Pro správný chod sítě byly nejdůležitější přístupové body opatřeny záložními zdroji, které zabezpečí funkčnost vysílače i při výpadku elektrického napětí. Podle důležitosti těchto bodů byly použity dva typy záložních zdrojů. Nejsilnější záložní zdroj byl použit na budově hasičské zbrojnice, kde jsou umístěny dva Mikrotiky o celkové spotřebě 40W. Byl zde umístěn zdroj APC Power-Saving Back – UPS Pro 900, který při výpadku elektrického napětí je schopen napájet vysílač (tedy oba Mikrotiky) po dobu 155 minut. Jako druhý typ záložního zdroje byl použit APC Power-Saving Back – UPS Pro 550. Tento je schopen napájet jeden Mikrotik 137 minut. Těchto zdrojů bylo použito celkem devět a byly umístěny na všechny vysílače, které nejsou koncovými vysílači v síti. Konkrétně se jedná o vysílače čísel 2, 3, 6, 7, 9, 11, 15, 16 a 17 dle obrázku č. 11. Co se týče ostatních koncových vysílačů, zde záložní zdroje zatím nejsou umístěny vzhledem k tomu, že tyto zdroje vyžadují poměrně velké finanční náklady na pořízení. Těchto vysílačů je v počítačové síti celkem 13. Rovněž počet zákazníků na každém z těchto koncových přístupových bodů je poměrně nízký a výpadek proudu na takovém vysílači nepředstavuje zásadní problém. Přesto je doporučeno postupem času použít záložní zdroje na všech vysílačích v síti a to především na těch, kde se bude počet připojených zákazníků zvyšovat.



Obrázek 19 - 1) UPS Pro 550, 2) UPS Pro 900, 3) UPS SC620. Dostupný na WWW: <http://www.apc.com/site/products/index.cfm/homeoffice/>

Použitím těchto záložních zdrojů je tedy docíleno funkčnosti celé sítě i po výpadku elektrického napětí, která je schopna plné funkce více než dvě hodiny. Je to dostatečně dlouhá doba na to, aby pracovníci firmy mohli tyto závady výpadků elektrického proudu bez problémů řešit.

Nejdůležitější částí takového zabezpečení provozu je však včasná informace o výpadku proudu. Záložní zdroje sice převezmou funkci a dodávají elektrický proud Mikrotiku, čímž je zaručen jeho další provoz, ale je potřeba vytvořit systém, který danou informaci neprodleně předá technikům firmy. Proto je každý tento záložní zdroj připojen USB kabelem do USB portu Mikrotiku RB433UAH a ten sleduje funkčnost záložního zdroje.

Jelikož v síti páteřních vysílačů se nacházeli tři vysílače s Mikrotikem RB433, které nebyly osazeny porty USB potřebnými pro sledování stavu UPS, bylo potřeba tyto Mikrotiky nahradit typem RB433UAH. Konkrétně se jednalo o vysílače 7, 9, 17.

Poté co byly všechny páteřní vysílače osazeny Mikrotiky s konektory USB a byly zde všechny UPS záložní zdroje, došlo k nakonfigurování všech těchto Mikrotiků tak, aby v případě výpadku elektrického proudu a sepnutí záložního zdroje předali danou zprávu prostřednictvím e-mailu na příslušnou e-mailovou adresu. Tato konfigurace je vytvořena napsáním příslušného skriptu prostřednictvím softwaru Winbox do samotného systému Mikrotiku. Skript je napsán prostřednictvím záložky „Systém“ do oken ScriptList a UPS. Ukázka tohoto nastavení je přílohou č. 4 této práce. Z okna UPS je v záložce Status patrný stav záložního zdroje, který činí 100% a předpokládaná doba provozu po výpadku proudu. Ve skriptu jsou znázorněny e-mailové adresy na které bude zaslán

e-mail informující o výpadku elektrického proudu. Rovněž je zde e-mail mobilního operátora O2 s telefonním číslem. Zasláním zprávy na tento mail dojde ze strany operátora k přeoslání této zprávy na vybrané telefonní číslo. Tím je zajištěna okamžitá informovanost o tomto stavu konkrétnímu technikovi ISP.

5.1.2 ZABEZPEČENÍ PŘÍSTUPOVÝCH BODŮ

Zabezpečení přístupových bodů je základem bezpečné funkčnosti celé sítě ISP. Nejdůležitější je zabezpečit každý tento bod tak, aby se na něj nemohla připojit neoprávněná osoba a dále tak, aby osoba, která je přes tento bod připojena do sítě internetu (zákazník) nemohla ohrozit funkčnost tohoto bodu, jeho konfiguraci atd.

Aby byla síť zabezpečena proti přístupu neoprávněným osobám, bylo potřeba zvýšit způsob zabezpečení, kterým byl pouze WPA klíč. Tento klíč je do jisté míry bezpečný, avšak lze jej při jistých schopnostech a softwarového vybavení prolomit. Z tohoto důvodu byly na každém vysílači uzamčeny všechny MAC adresy routerů jednotlivých zákazníků. Toto uzamčení bylo provedeno na každém Mikrotiku pomocí softwaru Winbox v okně Wireless Tables a záložce Access List, jak je znázorněno na následujícím obrázku. Tímto došlo k povolení komunikace s vysílačem pouze takovému zákaznickému zařízení, které má svoji MAC adresu povolenou na daném vysílacím bodě. Jelikož MAC adresa každého síťového zařízení je jedinečná, není možné, aby se do tímto způsobem zabezpečené sítě neoprávněná osoba připojila. Pokud by se na ni někdo takový pokoušel připojit a znal by také WPA klíč, tak k připojení vzhledem nesprávné MAC adrese nedojde.

Obrázek ukazuje celkem 16 MAC adres, které jsou povoleny na Mikrotiku a jiné zařízení s tímto Mikrotikem komunikovat nemůžou. Pokud by došlo k poškození zákaznického zařízení (routerů) a bylo by potřeba takový router vyměnit, tak stará MAC adresa bude ze seznamu vymazána a bude nahrazena novou MAC adresou nového routeru. Z důvodu ochrany dat byly části těchto MAC adres na obrázku umazány.

#	MAC Address	Interface	Signal Str...	Authentication	Forwarding
0	00:0B:68:81:00:00	wlan2_spoj_5g	-120..120	yes	yes
1	00:21:00:1E:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
2	00:11:A3:00:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
3	00:02:72:60:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
4	00:21:00:1E:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
5	00:02:72:70:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
6	00:02:72:70:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
7	00:15:6D:A0:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
8	00:02:72:72:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
9	00:02:72:74:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
10	00:02:72:70:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
11	00:4F:62:11:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
12	00:02:72:7E:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
13	00:02:72:7E:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
14	00:02:72:7E:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
15	00:02:72:70:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes
16	00:02:72:60:00:00	wlan1_SKYSOFT_letiny	-120..120	yes	yes

Obrázek 20 - Zabezpečení MAC adres, vlastní zdroj

Aby nedošlo k ohrožení konfigurace nastaveného Mikrotiku, musí být i tento zabezpečen proti neoprávněnému přístupu nejen hackerů, ale i samotných zákazníků, kteří jsou pochopitelně k tomuto přístupovému bodu připojeni. Z tohoto důvodu byla vytvořena servisní IP adresa, která je jako jediná oprávněna přistupovat na jakýkoliv Mikrotik v síti ISP. Nastavení této IP je provedeno opět systémem Winbox cestou Systém/Users a editací příslušného účtu. V tomto účtu je nastavena tato IP a tudíž pouze s takovou lze na Mikrotik přistupovat. Tato IP adresa je povolena na všech Mikroticích v síti a s touto IP adresou je možno se na Mikrotik připojit, ovšem opět pouze s takovou MAC adresou, která je na Mikrotiku také povolena. Pokud by se tedy někdo, kdo je do sítě připojen (např. zákazník) chtěl připojit na administrační konzoly Mikrotiku, musí znát servisní IP adresu a tu nastavit ve svém routeru. Zákaznický router je však techniky při jeho konfiguraci zabezpečen vstupním heslem. Nastavit tak servisní IP do routeru je tedy bez znalosti hesla nemožná. Rovněž by musel být zákazník znalý v oboru a vědět jakým způsobem se takový router konfiguruje. Pokud by však bylo známo heslo a na routeru by byla nakonfigurována servisní IP, potom je možné se na zařízení Mikrotik přihlásit prostřednictvím webového rozhraní, nebo softwaru Winbox. Pro přihlášení je však opět potřeba znát IP adresu konkrétního vysílače a pochopitelně přístupové jméno i heslo. Pouze znalostí těchto všech IP adres i hesel je možné na Mikrotik přistoupit a konfigurovat jej. Z těchto důvodů je tento způsob zabezpečení Mikrotiků v síti plně postačující a bezpečný.

5.2 MONITORING SÍTĚ ISP

Jak už bylo řečeno zjištění funkčnosti jednotlivých přístupových bodů lze zjistit příkazem PING z jakéhokoliv místa v síti poskytovatele. Pro neustálý dohled je však potřeba vytvořit takovou aplikaci, která bude kontrolu funkčnosti provádět automaticky 24 hodin denně a v případě výpadku bude tato informace okamžitě předána na patřičná místa. Pro tento monitoring je vytvořena aplikace, která je podrobněji vysvětlena v následující kapitole. Aplikace se skládá ze tří hlavních částí, jejímž cílem je vytvoření seznamu uživatelů (zákazníků) s dalšími informacemi, jako je jejich místo připojení, IP adresa a telefonní kontakt. Dále seznamu přístupových bodů se znázorněním jejich místa umístění, IP adres a aktuální funkčnosti. Poslední částí je grafické znázornění vytížení konektivity linky.

5.3 ADMINISTRAČNÍ APLIKACE SERVERU

Pro vytvoření aplikace monitoringu počítačové sítě je potřeba tento nainstalovat na základní server počítačové sítě, který se nachází v budově ČD. Na serveru je již nainstalován operační systém FreeBSD verze 7.4. Z tohoto důvodu bude nová administrace přizpůsobena tomuto operačnímu systému. Aplikace, která bude představovat webové rozhraní bude vytvořena tak, aby k ní bylo možné přistupovat odkudkoliv, a byl tak zajištěn patřičný dohled z jakéhokoliv místa sítě. Aplikace je vytvořena pomocí programovacího jazyka PHP. Abychom mohli na serveru programovat pomocí tohoto jazyka je potřeba nejprve do systému nainstalovat modul Apache s podporou PHP. Rovněž tak je potřeba vytvořit na serveru systém databází, který bude poskytovat všechny informace, jak o jednotlivých vysílačích, tak o zákaznících. Toto zajistíme instalací databázového systému MySQL. Posledním softwarem, který na server nainstalujeme je Multi Router Traffic Grapher (MRTG), kterým zajistíme grafické znázornění toku dat na serveru.

Apache můžeme chápat jako programový server, který běží na hardwarovém zařízení připojeného do internetu a zajišťující obsluhu webových prohlížečů jednotlivých návštěvníků. Hlavní výhodou tohoto softwaru je jeho dostupnost pro všechny hlavní platformy jako je Windows, Linux a další, ale především fakt, že Apache je vyvíjen jako open source, což zajišťuje jeho bezplatnost. Stejně tak databázový systém MySQL

je bezplatný a volně šiřitelný software, který využívá jazyk SQL. Jedná se o relační databázový systém, který je oblíben především pro svou jednoduchost a výkon. Každá taková databáze je tvořena z jedné nebo více tabulek, které mají řádky a sloupce. Sloupce jsou pojmenovány a uvozují datový typ o jednotlivých záznamech a řádky tyto záznamy obsahují.

Multi Router Traffic Grapher (MRTG) je software, který pomocí protokolu SNMP provádí monitorování síťových zařízení. Tento software pracuje tak, že se periodicky dotazuje monitorovaných zařízení a následně od nich získává informace jako je zatížení procesoru, využití operační paměti, či se dotazuje na velikost síťového provozu. Z dat, která následně získá, generuje HTML stránky s grafy a tyto si ukládá do svého kořenového adresáře.

Po nainstalování těchto softwarů již můžeme začít s programováním a vytvořením konečné aplikace zajišťující všechny stanovené cíle. Samotné programování je dosti složitý proces skládající se z vytvoření několika souborů, které jsou napsány pomocí jednotlivých skriptů a uloženy do operačního systému FreeBSD. Výsledkem je hotová a funkční administrace. Jelikož není možné v této práci detailně popisovat všechny kroky tohoto programování a definovat jednotlivé příkazy daného skriptu, budou zde uvedeny jen ty nejzákladnější a zjednodušeně popsané postupy takového programování a instalace.

Nejprve je potřeba zajistit zabezpečený vstup do vytvářené aplikace. Tato bude zabezpečena jménem a heslem, které uložíme do databáze MySQL. Při vstupu na webovou stránku bude systém porovnávat vypsané jméno a heslo se jménem a heslem v databázi a v případě shody poté umožní vstup do vytvořené aplikace. K tomuto je potřeba uvést, že veškeré databázové příkazy budou prováděny pomocí příkazového řádku přímo na serveru.

Samotná vytvořená databáze bude obsahovat tři tabulky. První tabulka bude zajišťovat přihlášení do systému, a proto ji nazveme „ADMIN“, druhá tabulka bude obsahovat informace o jednotlivých access pointech (přístupových bodech), proto bude mít název „ACCESSPOINTY“ a třetí bude obsahovat informace o zákaznících s názvem „ZÁKAZNÍCI“

5.3.1 TABULKA DATABÁZE ADMIN

Nejprve provedeme navržení databázové struktury tabulky s názvem Admin, která bude obsahovat pořadové číslo (ID), přihlašovací jméno (Login), přihlašovací heslo (Heslo) a popis (Popis). Vytvoření takové struktury provedeme následujícím příkazem.

```
CREATE TABLE `admin`  
  `id` int(8) NOT NULL AUTO_INCREMENT,  
  `login` varchar(20) NOT NULL DEFAULT "",  
  `heslo` varchar(20) NOT NULL DEFAULT "",  
  `popis` varchar(30) NOT NULL,  
  KEY `id` (`id`);
```

Z tohoto příkazu je patrné, že vytváříme tabulku pod jménem Admin. Atribut Integer11 nám určuje, že záznam ID může obsahovat pouze číslice o velikosti maximálně 11 pozic a atribut Auto_increment udává, že čísla nebude vkládat uživatel, ale budou přiřazovány automaticky. Aby byl záznam správný nesmí mít nulovou hodnotu, jinak k uložení nedojde. Další řádky příkazů s atributem Varchar20 nám říkají, že hodnoty jednotlivých záznamů pro login, heslo a popis mohou být různé, tedy že mohou obsahovat nejen číslice a písmena, ale i jiné znaky, přičemž počet těchto znaků nesmí překročit hodnotu dvaceti pozic. Poslední řádka KEY uvádí, že záznam ID je hlavním identifikátorem pro mazání a editování příslušného řádku.

Dalším příkazem je třeba uvedenou tabulku naplnit informacemi o přihlašovacích údajích, podle kterých se vstup bude ověřovat.

```
INSERT INTO `admin` VALUES ('', 'mira', 'mira', 'Mira Such');
```

Příkaz lze přečíst následovně. Vkládám data do tabulky admin s těmito hodnotami (první hodnota ID automaticky spočtená, hodnota login zní Míra, hodnota heslo zní Míra, hodnota popis zní Mira Such) Prázdná hodnota uvádí hodnotu ID, která je automaticky spočtená. Těchto příkazů lze uložit více, podle toho kolik uživatelů bude mít oprávnění do databáze vstupovat.

Tímto způsobem jsme tedy vytvořili strukturu první tabulky databáze, která bude sloužit pro správné a ověřené přihlášení do vytvořené aplikace.

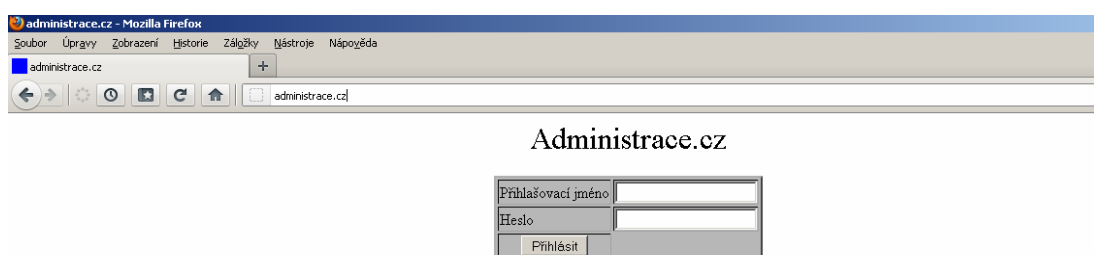
Dalším krokem je vytvoření webového zobrazení pro toto přihlášení. Jedná se o napsání skriptu, který je obdobný jako psaní klasických webových stránek. Skript je napsán v textovém editoru a následně uložen na serveru jako soubor pod názvem INDEX.PHP. Tento skript budeme pro další vysvětlení nazývat jako první skript a jeho obsah je následující:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1250">
<title>administrace.cz</title>
</head>
<body>
<?
require("config.inc.php");
?>
<div align="center">
<font size="6">Administrace.cz</font><br>
<br>
<form action="vstup.php" method="post">

<TABLE bgcolor="#b7b7b7" border="2" bordercolor="Black">
  <TR>
    <TD>Přihlašovací jméno</TD>
    <TD><INPUT maxLength=20 name="log_login" type="text"></TD>
  </TR>
  <TR>
    <TD>Heslo</TD>
    <TD><INPUT maxLength=20 name="log_heslo" type="password"></TD>
  </TR>
  <TR>
    <TD>
      <P align=center><INPUT type="submit" value="Přihlásit"></P></TD>
    </TR></TABLE>
      <input type="hidden">
</form>
</div>
</body>
</html>
```

Tento skript se skládá z hlavičky (HEAD) a těla (BODY). Hlavička popisuje způsob kódování, jazyk, kterým je napsán, přičemž se jedná o jazyk HTML a ukazuje styl rozvržení písma, kterým je windows 1250. Rovněž znázorňuje název (titulek) této hlavičky, kterým je administrace.cz. Tělo skriptu popisuje tabulku, která je důležitá pro přihlášení. Atribut Require znamená načtení konfiguračního souboru config.inc.php z databáze MySQL. Další atributy popisují zarovnání údajů na střed (div align), velikost

textu (font size), a tag br značí měkký enter, neboli vytvoření mezery mezi názvem Administrace a přihlašovací tabulkou. Atribut Form action představuje formulář, který se po stisknutí tlačítka „Přihlásit“ odešle na další souborový skript, kterým je VSTUP.PHP a který bude vysvětlen později. Atribut Table představuje přihlašovací tabulku s konkrétní barvou, okrajem a barvou okraje tabulky. Atributy TR představují řádky tabulky a atributy TD sloupce tabulky, přičemž je patrné, že první řádka představuje přihlašovací jméno, druhá řádka heslo a třetí řádka funkční tlačítko „Přihlásit“. Takový skript ve výsledku zobrazí webový prohlížeč způsobem, jak ukazuje následující obrázek.



Obrázek 21 - Přihlášení do administrace, vlastní zdroj

V prvním skriptu byla použita funkce require, která znamená načtení konfiguračního souboru CONFIG.INC.PHP z databáze MySQL. Tento soubor představuje správně nedefinované přihlášení do databáze. Lze jej definovat také jako konfigurační soubor, který navazuje spojení mezi softwarem Apache a databází MySQL a tím umožní vzájemnou spolupráci a znázorňování dat z databáze prostřednictvím webového prohlížeče. Samotná funkce require je vždy použita u všech skriptů, které slouží k navázání komunikace s databází. Skript souboru Config.inc.php je následující:

```
<?
$dtbserver      = "localhost";           //server, na kterem bezi databaze
$dtblogin       = "root";                //logovací jmeno pro databazi
$dtbheslo       = "heslo";               //heslo pro databazi
$dtb            = "mira";                //jmeno databaze

@$spojeni=MySQL_Connect($dtbserver,$dtblogin,$dtbheslo);
MySQL_Select_Db($dtb);
?>
```

Ze skriptu lze vyčíst, že navázání spojení softwarem Apache na databázi MySQL je provedeno na stejném zařízení (serveru), což představuje hodnota „localhost“, dále

je zde logovací jméno a heslo pro databázi a také název databáze. Tímto je tedy zabezpečen vstup do databáze pouze se znalostí přihlašovacího jména a hesla.

Dalším důležitým skriptem je skript, který porovnává přihlašovací údaje s údaji v databázi a tím umožní, nebo neumožní vstup do vytvořené aplikace. Tento skript, stejně jako předchozí patří mezi skripty, které se nezobrazují prostřednictvím webových stránek. Skript je uložen jako soubor pod názvem VSTUP.PHP a je následující:

```
<?
require("config.inc.php");

function authent($login,$heslo,$odkud)
{
//Test do databaze
@$test_v=MySQL_Query("SELECT * FROM $odkud WHERE login='$login'");
@$test=MySQL_Fetch_Array($test_v);

//Overeni autentifikace uzivatele
if (MD5($test["heslo"]) != $heslo or !$test):
    return 0;
else:
    return 1;
endif;
}
//pri spatnem heslu skok na prihlaseni
if (authent($log_login,MD5($log_heslo),"admin")==0):
    Header("Location:index.php");
    die;
endif;
$heslo=MD5($log_heslo);
$skam="accesspointy.php";
Header("Location:".$skam);
?>
```

Ze skriptu opět vyplývá, že dojde k navázání spojení mezi softwary Apache a MySQL. Funkce `authent` porovnává přihlašovací jméno a heslo s údaji v databázi. V případě, že jméno i heslo souhlasí bude přeskočen odstavec `If (authent....)`, a dojde ke spuštění aplikace, konkrétně k zobrazení webové stránky `accesspointy.cz`. Pokud by bylo jméno, nebo heslo nesprávné, odstavec `If (authent....)` znovu odkáže administrátora na přihlašovací stránku.

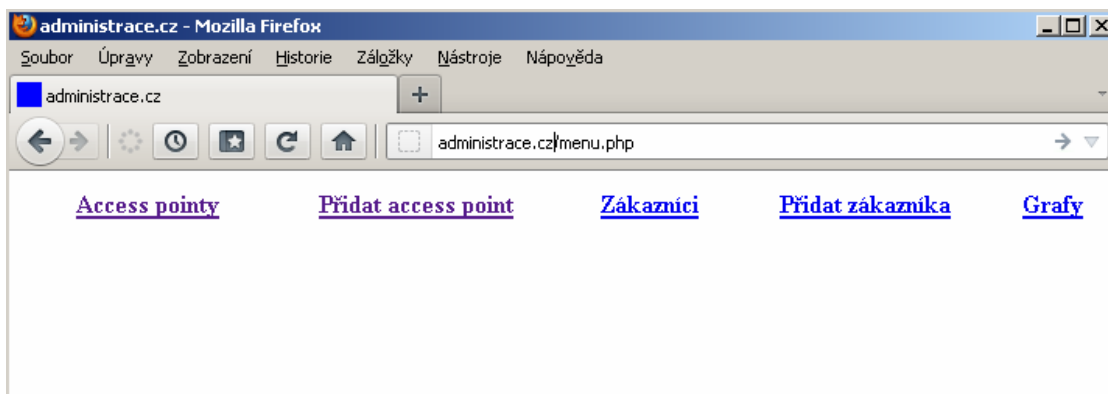
Další webová stránka, která bude znázorněna po přihlášení do systému je stránka samotné aplikace, která znázorňuje celkem pět následujících odkazů. `Access pointy`, `Přidat access point`, `Zákazníci`, `Přidat zákazníka`, `Grafy`. Způsob psaní těchto skriptů je stejný jako v předchozích případech. Skript., který je uložen v souboru pod názvem `MENU.PHP` a jeho výsledek zobrazení ve webovém prohlížeči je následující:

```

<html>
<head>
  <title>administrace.cz</title>
  <meta http-equiv="Content-Type" content="text/html; charset=windows-1250">
  <META http-equiv="Refresh" content="3600">
</head>
<div align="center">
<tr>
<!-- menu -->
<table width="100%">
<tr>
<td width="2"></td>
<td align="center"><b><a href="accesspointy.php">Access pointy</a></b></td>
<td align="center"><b><a href="accesspointyadd.php">Přidat access point</a></b></td>
<td align="center"><b><a href="zakaznici.php">Zákazníci</a></b></td>
<td align="center"><b><a href="zakazniciadd.php">Přidat zákazníka</a></b></td>
<td align="center"><b><a href="grafy.php">Grafy</a></b></td>
</tr>
</table>

</tr>
<tr>
<td>
<table width="100%" border="0" cellpadding="3" cellspacing="3">
<tr>
<td valign="top">

```



Obrázek 22 - Administrace – menu, vlastní zdroj

Tímto způsobem je tedy nastaveno základní přihlášení do administrační aplikace, která je zabezpečena proti neoprávněnému přístupu jménem a heslem. Následuje naprogramování dalších částí této aplikace.

5.3.2 TABULKA DATABÁZE ACCESS POINTY

Stejně jako při návrhu databázové struktury tabulky Admin vytvoříme i tabulku databáze s názvem Accesspointy. Její strukturu si navrhne tak, aby obsahovala ID číslo – číslo pořadí, Jméno – název vysílače, Adresu – místo kde se vysílač nachází, IP – adresa

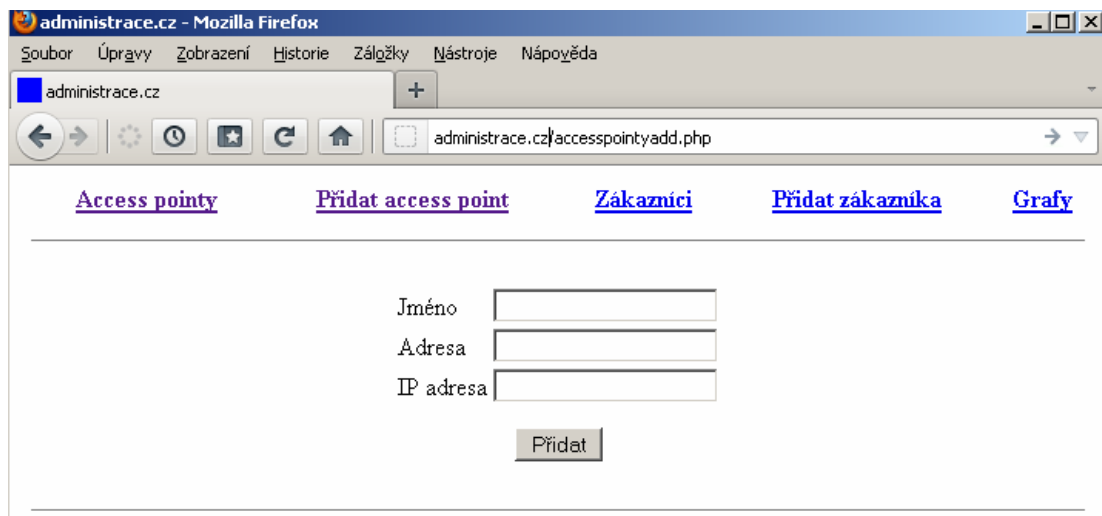
IP vysílače, UP – sloupec znázorňující zda je vysílač v provozu, AVG – průměrná doba odezvy (ping), OK – funkčnost vysílače, SMS_send – sloupec, který uvádí zda se má odeslat zpráva sms u konkrétního vysílače, SMS – informace zda již byla sms odeslána, Over_ok – pomocný řádek, který zajišťuje, aby byla zpráva sms odeslána pouze jednou. Příkaz vypadá následovně:

```
CREATE TABLE `accesspointy` (
  `id` int(8) NOT NULL AUTO_INCREMENT,
  `login` varchar(20) NOT NULL,
  `jmeno` varchar(30) NOT NULL,
  `ip` varchar(20) NOT NULL,
  `up` tinyint(1) DEFAULT NULL,
  `avg` varchar(10) DEFAULT NULL,
  `ok` tinyint(1) NOT NULL,
  `sms_send` int(1) NOT NULL,
  `sms` int(1) NOT NULL,
  `over_ok` int(1) DEFAULT NULL,
```

Tímto je vytvořena struktura tabulky s accesspointy a následuje vytvoření skriptů pro webové zobrazení, možnost vkládání, editování a mazání jednotlivých dat. Skript pro vyplňování nových accesspointů, který je uložen jako soubor pod názvem ACCESSPOINTYADD.PHP je následující:

```
<? require("config.inc.php");?>
<? require("menu.php"); ?>
<hr width="100%" size="1">
<br>
<div align="center">
<table>
<form action="/accesspointyadd2.php" method="post">
<tr>
<td>Jméno</td>
<td><input type="text" name="logina"></td></tr>
<tr>
<td>Adresa</td>
<td><input type="text" name="jmenoa"></td></tr>
<tr>
<td>IP adresa</td>
<td><input type="text" name="ipa"></td></tr>
<tr>
<td height="10" colspan="3"></td>
</tr>
<tr>
<td colspan="3" align="center"><input type="submit" name="sub" value="Přidat"></td>
</tr>
</form>
</table>
</div>
<? require("konecek.php"); ?>
```

Výsledek skriptu znázorňuje webový prohlížeč tímto způsobem:



Obrázek 23 - Administrace - přidání accesspointu, vlastní zdroj

Uvedený skript tedy umožní vypsát údaje o vysílačích. Dalším důležitým skriptem, který souvisí s přidáním Access pointů je skript uložený na serveru jako ACCESSPOINTYADD2.PHP a tento se spustí po stisknutí tlačítka „Přidat“, které je znázorněno na předchozím obrázku. Tímto příkazem dojde k uložení dat do tabulky databáze accesspointů a následně přepne webovou stránku na záložku Access pointy. Tento skript pro uložení do databáze se na webových stránkách nezobrazuje a jeho obsah je následující:

```
<?
require("../config.inc.php");

MySQL_Query("INSERT INTO accesspointy VALUES ('$logina','$jmeno','$ipa',' ',' ','1','')");

Header("Location: accesspointy.php");
die;
?>
```

Vytvořením těchto dvou skriptů je tedy možné naplnit databázi MySQL informacemi o všech přístupových bodech, které poskytovatel ISP používá. Po vypsání těchto informací a uložení dat do databáze budou naprogramovány další skripty, které budou zajišťovat zobrazování, editaci, případně mazání přístupových bodů. K zobrazení přístupových bodů je napsán skript uložený v souboru pod názvem ACCESSPOINTY.PHP. Skript je následující:

```

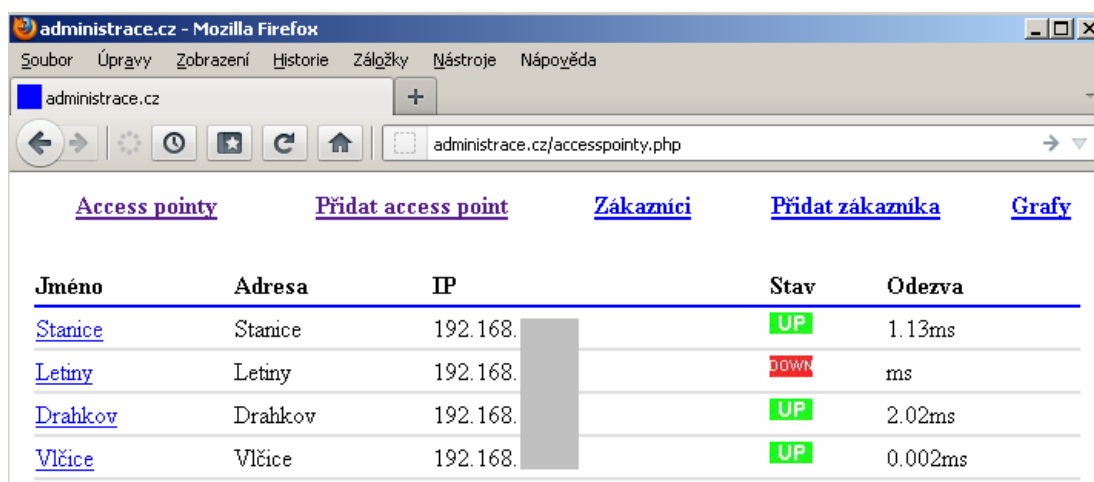
<?
require("config.inc.php");
require("menu.php");
?>
<br>
<? $data_v=MySQL_Query("SELECT * FROM accesspointy ORDER BY id"); ?>
<table width="100%"><tr>
    <td><b>Jméno</b></td>
    <td><b>Adresa</b></td>
    <td><b>IP</b></td>
    <td><b>Stav</b></td>
    <td><b>Odezva</b></td>
</tr>
<tr><td height="1" colspan="10" bgcolor="blue"></td></tr>
<?while($data=MySQL_Fetch_Array($data_v)):?>
<?
$stav=$data["up"];
$ok=$data["ok"];
if($stav==0){
$sup_i="";
$avg_i="";
}
else{
if($stav==1 and $ok==0){
$sup_i='';
$avg_i=$data["avg"]."ms";}
else{
$sup_i='';
$avg_i="";
}
};
?>
<tr>
    <td valign="top"><a href="accesspointy_edit.php?eid=? echo $data["id"] ?"><? echo
    $data["login"] ?></a></td>
    <td valign="top"><? echo $data["jmeno"]?></td>
    <td valign="top"><? echo $data["ip"]?></td>
    <td valign="top"><?echo $sup_i?></td>
    <td valign="top"><? echo $data["avg"]?>ms</td>
</tr>
<tr><td height="1" colspan="10" bgcolor="#DFDFDF"></td></tr>
<? endwhile; ?>
</table>

<? require("konecek.php"); ?>

```

Tento skript představuje navázání spojení mezi softwary Apache a MySQL, načtení skriptu MENU.PHP a dále načtení informací z databáze accesspointy a to pouze ty údaje, které chceme mít zobrazené. Konkrétně se jedná o sloupcové hodnoty Jméno, Adresa, IP, Stav a Odezva. Atribut td height znázorňuje modrou čáru oddělující názvy jednotlivých odstavců od konkrétních údajů v řádkách. Další atributy představují načítání informací o vysílačích z databáze a porovnávání funkčnosti. Funkční vysílač je příkazem označen obrázkem zelené barvy a názvem UP a nefunkční červeným obrázkem s názvem DOWN.

Rovněž je zde zobrazena průměrná hodnota odezvy v milisekundách, která je automaticky prováděna příkazem PING. Způsob této kontroly stavu a odezvy bude vysvětlen později. Následující obrázek znázorňuje malou část takové webové stránky ze které je jasně patrný stav uvedených vysílačů, přičemž vysílač pod názvem LETINY je jako jediný ve stavu nefunkčním. Adresy IP byly úmyslně umazány z důvodu ochrany dat uvedené sítě.



Jméno	Adresa	IP	Stav	Odezva
Stanice	Stanice	192.168. [redacted]	UP	1.13ms
Letiny	Letiny	192.168. [redacted]	DOWN	ms
Drahkov	Drahkov	192.168. [redacted]	UP	2.02ms
Vlčice	Vlčice	192.168. [redacted]	UP	0.002ms

Obrázek 24 - Administrace - seznam accesspointů, vlastní zdroj

Tímto jsme tedy naprogramovali další webovou stránku zobrazující všechny access pointy s patřičnými informacemi. Editace a mazání konkrétních vysílačů bude prováděna tak, že po kliknutí na název patřičného vysílače bude otevřena další stránka, kterou představuje obrázek č. 25. Zde jsou k dispozici funkční tlačítka, kterými mohou být údaje o vysílači změněny, nebo smazány. Zobrazení takové webové stránky zajistí následující skript uložený na serveru pod názvem ACCESSPOINTY_EIDT.PHP.

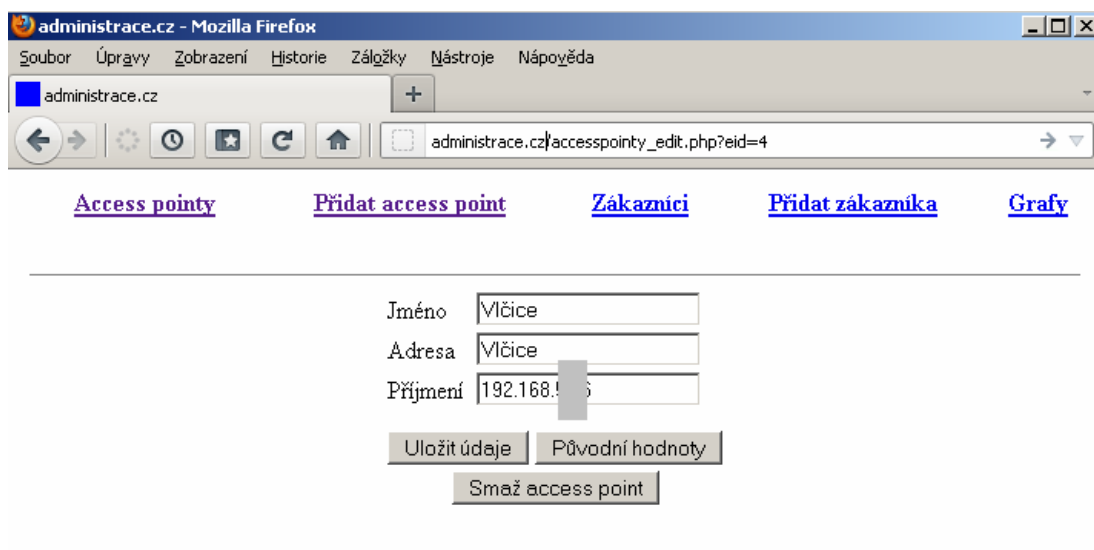
```
<?
require("config.inc.php");
require("menu.php");
$us_v=MySQL_Query("SELECT * FROM accesspointy WHERE id like '$eid'");
$us=MySQL_Fetch_Array($us_v);
?>
<br>
<hr width="100%" size="1">
<div align="center">
<table>
<form action="/accesspointy_edit2.php?fid=<?echo $eid?>" method="post">
<tr>
<td>Jméno</td>
<td><input type="text" name="logina" value="<? echo $us["login"] ?>"></td>
```

```

</tr>
<tr>
<td>Adresa</td>
<td><input type="text" name="jmeno" value="<? echo $us["jmeno"] ?>"></td>
</tr>
<tr>
<td>Příjmení</td>
<td><input type="text" name="ipa" value="<? echo $us["ip"] ?>"></td>
</tr>
<tr>
<td colspan="3" height="10"></td>
</tr>
<tr>
<td colspan="3" align="center"><input type="submit" name="sub" value="Uložit údaje"> <input
type="reset" name="reset" value="Původní hodnoty"></td>
</tr>
</form>
<form action="accesspointy_smaz.php?fid=<?echo $eid?>" method="post">
<td colspan="3" align="center"><input type="submit" name="sub" value="Smaž access point"></td>
</form>
</table>
</div>
<? require("konecek.php"); ?>

```

Výsledek tohoto skriptu zobrazí následující webovou stránku tímto způsobem:



Obrázek 25 - Administrace - editace accesspointu, vlastní zdroj

Tato stránka představuje editaci vysílače Vlčice. Z napsaného skriptu i zobrazené stránky jsou patrná funkční tlačítka, které se odkazují na další psané skripty zajišťující

provedení změny v databázi MySQL. Po provedené změně a uložení, nebo po smazání celého vysílače dojde k zobrazení výchozí webové stránky seznamu accesspointů.

K editaci, nebo smazání vysílače z databáze jsou napsány dva skripty, které příslušnou změnu v systému provedou. Tyto skripty jsou v systému uloženy, ale nemají žádný webový výstup a nejsou tedy obsluhou nijak znázorňovány. Skript pro editaci je uložen v souboru pod jménem ACCESSPOINTY_EIDT2.PHP a jeho obsah je následující:

```
<?
require("config.inc.php");
MySQL_Query("UPDATE accesspointy SET login='$logina' WHERE id like '$fid'");
MySQL_Query("UPDATE accesspointy SET jmeno='$jmeno' WHERE id like '$fid'");
MySQL_Query("UPDATE accesspointy SET ip='$ipa' WHERE id like '$fid'");
Header("Location: ./accesspointy.php");
die;
?>
```

Následující skript je určen pro smazání vysílače a tento je uložen v souboru ACCESSPOINTY_SMAZ.PHP:

```
<?
require("config.inc.php");
Mysql_Query("DELETE FROM accesspointy WHERE id=$fid");
Header("Location: accesspointy.php");
?>
```

Další nejdůležitější částí této administrace je monitoring spojení jednotlivých přístupových bodů. Nejjednodušším způsobem této kontroly je pomocí příkazu ping, o kterém již bylo hovořeno v kapitole 4.4.

Princip takové kontroly spočívá v opakovaném zasílání datagramu na všechny monitorované vysílače v síti (respektive jejich IP adresy) a to každou jednu minutu, přičemž je posláno celkem pět datagramů. Po vrácení odezvy těchto datagramu skript vyhodnotí, zdali je vysílač funkční, či nikoliv. V případě, že je v pořádku uloží do databáze dat k danému vysílači číslici 1, znamenající stav UP (funkční vysílač označen zeleně) a v případě, že datagramy nedostanou žádnou odezvu, uloží skript do databáze k danému vysílači číslici 0 znamenající stav DOWN (nefunkční vysílač označen červenou barvou). Dále dojde k uložení průměrné hodnoty pingu, který je na webové stránce zobrazen v sloupci Odezva. Skript pro uvedenou činnost kontroly je uložen v souboru pod názvem PING.PHP a je následující:


```

<?
$self = $PHP_SELF;
$system = ini_get('system');
$data_v=MySQL_Query("SELECT * FROM accesspointy WHERE up=1");
while($data=MySQL_Fetch_Array($data_v):
$ip = $data["ip"];
$ids= $data["id"];
$avg = system ("ping -c 3 -t 5 $ip | grep round | cut -d=' ' -f2 | cut -d/' ' -f1");
if($avg==""){
$over="1";
$avg="0";
$over1=$data["over_ok"];
        if ($over1=="1"){
            $oki="1";}
        else
        {
            $oki="0";}
    }
else{
$oki="0";
$over="0";}

        MySQL_Query("UPDATE accesspointy SET over_ok='$over' WHERE id='$ids'");
        MySQL_Query("UPDATE accesspointy SET avg='$avg' WHERE id='$ids'");
        MySQL_Query("UPDATE accesspointy SET ok='$oki' WHERE id='$ids'");
$sms_k=$data["ok"];
if($sms_k<>$oki){
        MySQL_Query("UPDATE accesspointy SET sms='0' WHERE id='$ids'");
    }
else{
$b="ok";
}
endwhile;
?>

```

Tento skript rovněž nemá žádný webový výstup, neboť provede pouze příkaz ping a uloží výsledek do databáze accesspointů. Tento výsledek je poté skriptem v souboru ACCESSPOINTY.PHP zobrazen do webového rozhraní, jak ukazuje obrázek č. 24.

Dalším krokem je vytvoření skriptu pro odesílání e-mailových zpráv o změně stavu funkčnosti jednotlivých vysílačů. Každá taková změna „UP“, nebo „DOWN“ je zaslána na stanovený e-mail a stejně jako u monitoringu UPS je na základě telefonního operátora tato informace předána na telefonní číslo technika firmy. Skript pro toto zasilání zpráv opět nemá žádný webový výstup a je uložen pod názvem SMS.PHP:

```

<?
$time=StrFTime("%d/%m/%Y %H:%M:%S", Time());
$predmet="predmet";
//UP
$data_v=MySQL_Query("SELECT * FROM accesspointy WHERE sms=0 and sms_send=1 and ok=0");
$up_pocet=MySQL_Num_Rows($data_v);
if($up_pocet=="0"){

```

```

}
else{
while($data=MySQL_Fetch_Array($data_v)):
Sids= $data["id"];
$smssendtext.=$data["hosts"].", ";
        MySQL_Query("UPDATE accesspointy SET sms='1' WHERE id='$sids'");
endwhile;
$times=$time." UP: ";
$sms_v1=MySQL_Query("SELECT * FROM sms_info WHERE aktiv=1 ORDER BY id");
While($sms1=MySQL_Fetch_Array($sms_v1)):
$smail=$sms1["email"];
//echo $smail;
Mail($smail,$times,$smssendtext,"From:<email@administrace.cz>");
Endwhile;

//DOWN
$data_v1=MySQL_Query("SELECT * FROM accesspointy WHERE sms=0 and sms_send=1 and ok=1");
$down_pocet=MySQL_Num_Rows($data_v1);
if($down_pocet=="0"){
}
else{
while($data1=MySQL_Fetch_Array($data_v1)):
Sids= $data1["id"];
$smssendtext1.=$data1["hosts"].", ";
        MySQL_Query("UPDATE accesspointy SET sms='1' WHERE id='$sids'");
endwhile;
$times2=$time." DOWN: ";
$sms_v2=MySQL_Query("SELECT * FROM sms_info WHERE aktiv=1 ORDER BY id");
While($sms2=MySQL_Fetch_Array($sms_v2)):
$smail2=$sms2["email"];
//echo $smail2;
Mail($smail2,$times2,$smssendtext1,"From:<email@administrace.cz>");
Endwhile;
?>

```

Ze skriptu lze vyčíst tyto základní údaje. Na prvním řádku je vygenerován čas, který se v e-mailu projeví a určí dobu, kdy došlo ke změně stavu funkčnosti vysílače. Dále je vyčten z databáze accesspointů současný stav daného vysílače a to s hodnotou 1=UP, nebo 0=DOWN a je porovnán s novou hodnotou 1=UP, nebo 0=DOWN. Pokud nedojde ke změně této hodnoty, skript neprovede žádnou operaci. V opačném případě odešle e-mail na stanovenou adresu, která je znázorněna na předposledním řádku skriptu.

Dále je zapotřebí, aby se oba skripty PING.PHP a SMS.PHP spouštěly každou minutu, což se docílí tím, že v systému FreeBSD využijeme softwarového démona Cron.

Cron: „je softwarový démon, který v operačních systémech automatizovaně spouští v určitý čas nějaký příkaz resp. proces (skript, program apod.). Jedná se vlastně o specializovaný systémový proces, který v operačním systému slouží jakožto plánovač

úloh, jenž umožňuje opakované spouštění periodicky se opakujících procesů (např. noční běhy dávkových úloh při hromadném zpracování dat) apod.¹⁰

Pro opakované spouštění obou uvedených skriptů je nutné nakonfigurovat tohoto démona následujícím příkazem.

```
#minute      hour  mday  month  wday  who   command
#Kontrola PING
*/1 * * * * root /usr/local/bin/lynx -dump http://administrace.cz/ping.php > /dev/null
2>&1
*/1 * * * * root /usr/local/bin/lynx -dump http://administrace.cz/email.php > /dev/null
2>&1
```

Z tohoto příkazu lze vyčíst, že každou jednu minutu po dobu každé hodiny, dne i měsíce se spustí skript PING.PHP a skript SMS.PHP. Výsledek funkčnosti je poté uložen v databázi accesspintů, který se projevuje ve webové zobrazení a zasíláním sms zpráv na příslušné telefonní číslo.

Tímto naprogramováním, nastavením systému serveru a napsáním příslušných skriptů jsme docílili vytvoření webové administrace sloužící k neustálému sledování všech přístupových bodů, které jsou každou minutu automaticky kontrolovány a výsledky zaznamenávány do databáze. Tyto jsou poté zobrazeny pomocí webové stránky, kde u každého vysílače je zobrazen jeho stav funkčnosti, odezva příkazu ping v milisekundách a v případě změny stavu různého vysílače zaslána zpráva sms.

5.3.3 TABULKA DATABÁZE ZÁKAZNÍCI

Pro vytvoření databáze zákazníků je opět potřeba vytvořit strukturu tabulky na serveru s názvem Zákazníci, která bude obsahovat patřičné sloupce pro ukládání konkrétních dat. Těmito sloupci jsme si zvolili pořadové číslo (ID), název (Login), jméno, příjmení, telefonní číslo, adresu, IP číslo zákazníka a popis. Takovou strukturu tabulky vytvoříme následujícím příkazem.

¹⁰ Citace: Cron. In *Wikipedie*: otevřená encyklopedie [online]. St.Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2011-11-01. [cit. 2012-01-31]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Cron>.

```
CREATE TABLE `zakaznici` (
  `id` int(8) NOT NULL AUTO_INCREMENT,
  `login` varchar(20) COLLATE utf8_bin DEFAULT NULL,
  `jmeno` varchar(30) COLLATE utf8_bin DEFAULT NULL,
  `prijmeni` varchar(30) COLLATE utf8_bin DEFAULT NULL,
  `telefon` varchar(13) COLLATE utf8_bin DEFAULT NULL,
  `adresa` varchar(50) COLLATE utf8_bin DEFAULT NULL,
  `ip` varchar(20) COLLATE utf8_bin DEFAULT NULL,
  `popis` text CHARACTER SET utf32 COLLATE utf32_czech_ci,
  UNIQUE KEY `id` (`id`),
```

Výslednou tabulku lze přečíst obdobně jako tabulku Admin, která již byla popsána v kapitole 5.3.1.

Tabulka je po napsání uložena na server a dalším krokem je vytvoření webových stránek zobrazujících veškeré informace o zákaznících, možnost jejich přidávání, editace a mazání. K tomu je opět potřeba napsat několik skriptů, které budou na server uloženy jako soubory XXX.PHP. Tři tyto skripty budou zobrazovány prostřednictvím webového prohlížeče a další tři budou provádět pouze určité operace a změny v databázi bez toho, aniž by byly nějak na webových stránkách zobrazeny. Mezi zobrazující stránky patří přidání zákazníka, seznam zákazníků a stránka na editaci zákazníka. Skripty a zobrazení těchto webových stránek jsou pak následující.

STRÁNKA PRO PŘIDÁNÍ ZÁKAZNÍKA:

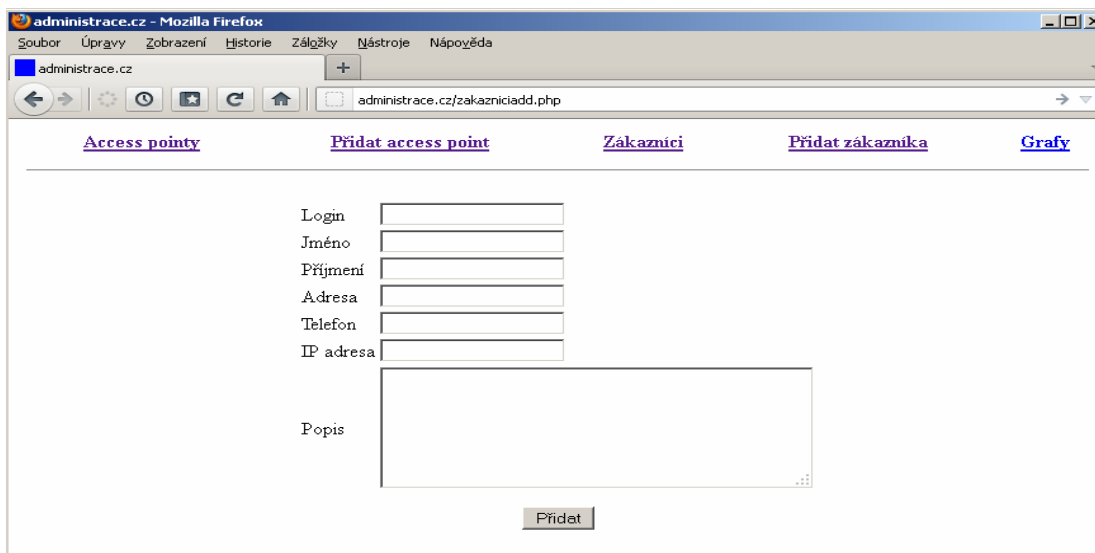
```
<? require("config.inc.php");?>
<? require("menu.php");
?>
<hr width="100%" size="1">
<br>
<div align="center">
<table>
<form action="/zakazniciadd2.php" method="post">
<tr>
<td>Login</td>
<td><input type="text" name="loginz"></td>
</tr>
<tr>
<td>Jméno</td>
<td><input type="text" name="jmenoz"></td>
</tr>
<tr>
<td>Příjmení</td>
<td><input type="text" name="prijmeniz"></td>
</tr>
<tr>
<td>Adresa</td>
<td><input type="text" name="adresaz"></td>
</tr>
<tr>
<td>Telefon</td>
<td><input type="text" name="telefonz"></td>
</tr>
<tr>
```

```

<td>IP adresa</td>
<td><input type="text" name="ipz"></td>
</tr>
<tr>
<td>Popis</td>
<td><textarea cols="40" rows="6" name="popisz"></textarea></td>
</tr>
<tr>
<td height="10" colspan="3"></td>
</tr>
<tr>
<td colspan="3" align="center"><input type="submit" name="sub" value="Přidat"></td>
</tr>
</form>
</table>
</div>
<? require("konecek.php"); ?>

```

Skript je uložen jako soubor ZAKZANICIADD.PHP a jeho webový výstup je následující:



Obrázek 26 - Administrace - přidání zákazníka, vlastní zdroj

STRÁNKA SEZNAMU ZÁKAZNÍKŮ:

```

<?
require("config.inc.php");
require("menu.php");
$data_v=MySQL_Query("SELECT * FROM zakaznici ORDER BY id");
?>
<div align="left">
<table width="100%">
<tr>
<td><b>Login</b></td>
<td><b>Jméno a Příjmení</b></td>
<td><b>Adresa</b></td>
<td><b>Telefon</b></td>
<td><b>IP adresa</b></td>
<td><b>Poznámka</b></td>

```

```

</tr>
<tr><td height="1" colspan="20" bgcolor="blue"></td></tr>
<?while($data=MySQL_Fetch_Array($data_v)):?>
<td valign="top"><a href="zakaznici_edit.php?eid=? echo $data["id"] ?"><? echo $data["login"] ?></a></td>
<td valign="top"><? echo $data["jmeno"] ?> <? echo $data["prijmeni"] ?></td>
<td valign="top"><? echo $data["adresa"] ?></td>
<td valign="top"><? echo $data["telefon"] ?></td>
<td valign="top"><? echo $data["ip"] ?></td>
<td valign="top"><? echo $data["popis"] ?></td>
</tr>
<tr><td height="1" colspan="20" bgcolor="#DFDFDF"></td></tr>
<? endwhile; ?>
<? require("konecek.php"); ?>

```

Skript je uložen jako soubor ZAKAZNICI.PHP a jeho webový výstup je následující:

Access pointy	Přidat access point	Zakaznici	Přidat zakaznika	Grafy	
Such-Vlcice	Mira Such	Vlcice	777 158 625	192.168.19.19	WA2204
Benes-Hradistska Lhota	Jan Beneš	602 35	Hradištský újezd 4	192.168.23.23	Nanostation2
Novotný-Blovica skola	Libor Novotný	723 23	Blovica 54	192.168.22.25	Nanostation2
Počátecký-Letiny	Petr Počátecký	603 67	Letiny 28	192.168.12.12	Nanostation2
Palacký-Drahkov	Jiří Palacký	602 12	Drahkov 30	192.168.51.51	Nanostation5
Srb-Blovica	Luboš Srb	732 56	Blovica 49	192.168.90.90	Nanostation5

Obrázek 27 - Administrace - seznam zákazníků, vlastní zdroj

STRÁNKA PRO EDITACI ZÁKAZNÍKA:

```

<?
require("config.inc.php");
require("menu.php");
$us_v=MySQL_Query("SELECT * FROM zakaznici WHERE id like '$eid'");
$us=MySQL_Fetch_Array($us_v);
?>
<br>
<hr width="100%" size="1">
<div align="center">
<table>
<form action="/zakaznici_edit2.php?fid=? echo $eid ?" method="post">
<tr>
<td>Login</td>
<td><input type="text" name="loginz" value=? echo $us["login"] ?></td> </tr>
<tr>
<td>Jméno</td>
<td><input type="text" name="jmenoz" value=? echo $us["jmeno"] ?></td> </tr>

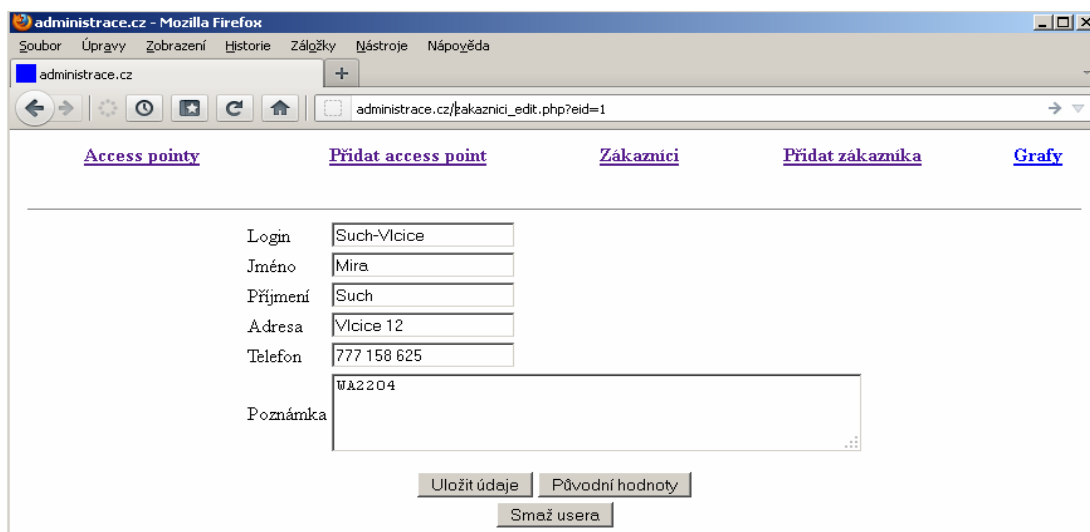
```

```

<tr>
<td>Příjmení</td>
<td><input type="text" name="prijmeniz" value="<? echo $us["prijmeni"] ?>"></td> </tr>
<tr>
<td>Adresa</td>
<td><input type="text" name="adresaz" value="<? echo $us["adresa"] ?>"></td> </tr>
<tr>
<td>Telefon</td>
<td><input type="text" name="telefonz" value="<? echo $us["telefon"] ?>"></td> </tr>
<tr>
<td>Poznámka</td>
<td><textarea cols="50" rows="3" name="popisz"><? echo $us["popis"] ?></textarea></td> </tr>
<tr>
<td height="10" colspan="3"></td> </tr>
<tr>
<td colspan="3" align="center"><input type="submit" name="sub" value="Uložit údaje"> <input type="reset"
name="reset" value="Původní hodnoty"></td> </tr>
</form>
<form action="zakaznici_smaz.php?fid=<?echo $eid?>" method="post">
<td colspan="3" align="center"><input type="submit" name="sub" value="Smaž usera"></td>
</form>
</table>
</div>
<? require("konecek.php"); ?>

```

Skript je uložen jako soubor ZAKAZNICI_EDIT.PHP a jeho webový výstup je následující:



Obrázek 28 - Administrace - editace zákazníka, vlastní zdroj

Další tři skripty nejsou výstupem webového zobrazení, ale pouze provedou operaci (změnu) v databázi zákazníků na serveru. Těmito skripty jsou:

- 1) Skript, který se spustí po stisknutí tlačítka „PŘIDAT“ na webové stránce přidání nového zákazníka (viz. obrázek č.26). Skript provede uložení nového zákazníka do databáze a následně zobrazí stránku

seznamu zákazníků (viz. obrázek č. 27), kde již bude nový zákazník zobrazen. Tento skript je uložen jako soubor ZAKAZNICIADD2.PHP.

- 2) Skript, který se spustí po stisknutí tlačítka „ULOŽIT ÚDAJE“, na webové stránce editace zákazníka (viz. obrázek č.28) . Skript opět uloží změny údajů v databázi konkrétního zákazníka a následně zobrazí stránku seznamu zákazníků (viz. obrázek č.27), kde již bude tato změna zobrazena. Skript je uložen jako soubor pod názvem ZAKAZNICI_EDIT2.PHP.
- 3) Skript, který se spustí po stisknutí tlačítka „SMAŽ USERA“ na webové stránce editace zákazníka (viz. obrázek č.28). Skript vymaže data z databáze tohoto zákazníka a zobrazí seznam zákazníků (viz. obrázek č. 27), kde již tento zákazník nebude uveden. Skript je na serveru uložen jako soubor ZAKAZNICI_SMAZ.PHP.

Tyto tři uvedené skripty jsou napsány následujícím způsobem:

ZAKAZNICIADD2.PHP

```
<?
require("./config.inc.php");
MySQL_Query("INSERT INTO zakaznici VALUES
('$loginz','$jmeno','$prijmeniz','$adresaz','$telefonz','$ipz','$popisz')");
Header("Location: zakaznici.php");
die;
?>
```

ZAKAZNICI_EDIT2.PHP

```
<?
require("config.inc.php");
MySQL_Query("UPDATE zakaznici SET login='$loginz' WHERE id like '$fid'");
MySQL_Query("UPDATE zakaznici SET jmeno='$jmeno' WHERE id like '$fid'");
MySQL_Query("UPDATE zakaznici SET prijmeni='$prijmeniz' WHERE id like '$fid'");
MySQL_Query("UPDATE zakaznici SET adresa='$adresaz' WHERE id like '$fid'");
MySQL_Query("UPDATE zakaznici SET telefon='$telefonz' WHERE id like '$fid'");
MySQL_Query("UPDATE zakaznici SET popis='$popisz' WHERE id like '$fid'");
Header("Location: ./zakaznici.php");
die;
?>
```

ZAKAZNICI_SMAZ.PHP

```
<?
require("config.inc.php");
Mysql_Query("DELETE FROM zakaznici WHERE id=$fid");
Header("Location: zakaznici.php");
?>
```


Tímto naprogramováním jsme tedy vytvořili webovou aplikaci seznamu všech zákazníků v síti poskytovatele ISP, který může tyto zákazníky prostřednictvím webových stránek přidávat, mazat, editovat a to z jakéhokoliv místa v síti. Tím má možnost získat okamžitě všechny potřebné informace o zákazníkovi a to především jeho IP adresu, případně zařízení, které má v síti nakonfigurované.

5.3.4 GRAFY ZATÍŽENÍ

Poslední část webové aplikace znázorňuje grafické zatížení datového přenosu (konektivity), který vstupuje do serveru. Pro toto znázornění jsme již nainstalovali do operačního systému FreeBSD serveru software Multi Router Traffic Grapher (MRTG).

Konfigurace tohoto softwaru MRTG je velmi jednoduchá a konfigurační soubor je následující.

```
WorkDir: /administrace.cz/mrtg/  
Language: czech  
Options[r10]: growright,bits  
Target[r10]: 1:public@127.0.0.1  
XSize[r10]: 600  
YSize[r10]: 200  
MaxBytes[r10]: 5500000  
Title[r10]: : Interface r10  
PageTop[r10]: <H2>Traffic Analysis for r10
```

Tento soubor je napsán v textovém editoru a uložen v adresáři Workdir tohoto programu pod názvem MRTG.cfc. Příkaz generuje na základě toku dat na serveru obrázky a ukládá je do svého adresáře pod příponou png. Výsledkem jsou obrázky (grafy) znázorňující tok dat. Název takového výsledku může být například mrtg/r10-day.png.

Pro spuštění softwaru MRTG s uvedeným konfiguračním souborem využijeme opět démona Cron napsáním příkazu:

```
#minute hour mday month wday who command  
*/5 * * * * root /usr/local/bin/mrtg /administrace.cz/mrtg.cfg > /dev/null  
2>&1
```

Z příkazu vyplývá, že každých 5 minut v každé hodině, dnu i měsíci se spustí program MRTG s uvedeným konfiguračním souborem. Výsledkem tohoto programu je vygenerování výsledků (grafů) na cestu uvedenou v konfiguračním souboru, což je adresář Workdir. Proto, aby tyto grafy byly znázorněny v administrační aplikaci

prostřednictvím webových stránek je potřeba vytvořit následující poslední skript. Skript je uložen pod názvem GRAFY.PHP.

```
<? require("./config.inc.php");  
require("menu.php");  
?>  
<table cellspacing="2" cellpadding="2" border="0">  
<div align="center">  
<tr>  
<td>  
<br>  
  
<br>  
  
<br>  
  
<br>  
  
<br>  
<br>  
</td>  
<td>  
</div>  
</table>  
<? require("konecek.php"); ?>
```

Výsledkem tohoto skriptu je zobrazení webové stránky s grafy, která je přílohou č. 5 této práce.

6 EKONOMICKÝ DOPAD

Pro provedení změn v síti ISP týkající se monitoringu a zabezpečení bylo nakoupeno celkem 9 UPS záložních zdrojů a tři Mikrotiky RB433UAH. Dále byla vytvořena aplikace, která byla nainstalována na základní server sítě, a také byly překonfigurovány všechny přístupové body v síti.

Instalace aplikace i konfigurace všech přístupových bodů si vyžádala celkový čas 61 hodin. Celkové náklady na změnu této sítě činí 52.302,- Kč a jsou podrobně zobrazeny v následující tabulce. Ceny za použité komponenty vycházejí z ceníků internetových prodejců, které jsou uvedeny v internetových zdrojích na konci této práce.

Komponenty:	Cena za jednotku:	Počet ks:	Celkem:
Záložní zdroj: Power-Saving Back – UPS Pro 550	3065	8	24520
Záložní zdroj: APC Power-Saving Back – UPS Pro 900	4598	1	4598
Mikrotik RB433UAH pro vysílače 7,9,17	2848	3	8544
	Celkem za komponenty v Kč:		37662
Software a instalace:	Cena na hodinu:	Počet hodin:	Celkem:
modul Apache			zdarma
databáze MySQL			zdarma
Multi Router Traffic Grapher			zdarma
Výměna tří kusů Mikrotiků a umístění všech záložních zdrojů na vysílače	240	12	2880
Konfigurace Mikrotiků všech přístupových bodů	240	23	5520
Instalace serveru a naprogramování nové administrace	240	26	6240
	Celkem za instalaci v Kč:		14640
	Celkem v Kč:		52302

Zdroj: Cena za komponenty dle ceníku dostupného na WWW: <http://www.apc.com/products/family/index.cfm?id=27>. Cena za práci na hodinu zjištěna dle interních předpisů firmy Sky-Soft s. r. o.

Samotná návratnost investice, která má za následek zjednodušení, zkvalitnění a zajištění lepší funkčnosti celé této sítě, a také pravděpodobné zvýšení spokojenosti zákazníků je nevyčíslitelná. Kvantitativně lze tyto náklady zahrnout pouze do pracovní doby, kterou jsou pracovní firmy nuceni denně provádět pro zjištění stavu počítačové sítě, a které jsou po zavedení aplikace do praxe zproštěny. Tím dochází každý den k ušetření nákladů jedné hodiny mzdy, což činí 240,- Kč. Pokud bychom tedy celkové náklady 52.302,- Kč vydělili ušetřenou hodinovou mzdou, dostaneme se k výsledku 218ti hodin, a tedy k 218ti pracovním dnům, za které se tyto náklady firmě skutečně navrátí. Těchto 218 dní představuje necelých 11 měsíců. Počínaje dvanáctým měsícem tedy dojde ke snížení nákladů o 240,- Kč denně, což činí 4.800,- Kč měsíčně. Tyto ušetřené finance poté může firma investovat do dalšího zkvalitňování a rozvoje své počítačové sítě.

7 ZÁVĚR

Cílem diplomové práce bylo na základě provedené analýzy počítačové sítě poskytovatele internetu firmy Sky-Soft v obci Blovice a jeho okolí, navrhnout a vytvořit nový způsob zabezpečení a monitoringu, který by vedl k celkovému zkvalitnění a zlepšení funkčnosti této počítačové sítě.

Byla provedena fyzická kontrola všech vysílačů v síti, zjištěna konektivita internetu, zkontrolovány jednotlivé hardwarové komponenty, zjištěny způsoby zabezpečení a celá síť byla monitorována pomocí softwaru Winbox a příkazů Ping. Bylo hovořeno s pracovníky firmy za účelem zjištění možných problémů a výpadků počítačové sítě, a také byl vytvořen a rozeslán dotazník s cílem zjistit spokojenost zákazníků s internetovými službami a zjistit četnost poruch a výpadků této sítě.

Po provedené analýze a zhodnocení závěrů o stavu funkčnosti, zabezpečení, i monitoringu této sítě byly provedeny některé hardwarové změny. Všechny důležité přístupové body byly opatřeny záložními zdroji a některé byly opatřeny novými komponenty tak, aby mohly být vzdáleně monitorovány. Tím došlo k zajištění těchto nejdůležitějších, páteřních přístupových bodů proti možným výpadkům elektrické energie. Dále byla vytvořena administrační aplikace, která byla nainstalována na základním serveru počítačové sítě, a která svou činností nepřetržitě sleduje provoz této sítě a jednotlivé výpadky oznamuje prostřednictvím e-mailů a SMS zpráv na příslušná telefonní čísla pracovníků firmy. Rovněž tato aplikace umožňuje vytváření seznamu nových přístupových bodů i zákazníků a dalších důležitých informací, které jsou pro poskytovatele internetu nezbytné.

Tyto provedené změny sítě si vyžádaly celkové náklady ve výši 52.302,- Kč. Návratnost nákladů činní necelých jedenáct měsíců od implementování těchto změn do počítačové sítě a dále se po této době předpokládá šetření dalších nákladů ve výši 4.800,- Kč měsíčně. Od 1. 1. 2012 je tato navržená síť uvedena do praxe a je plně funkční. Samotná administrační aplikace je navržena a zpracována tak, aby k ní byl možný přístup z jakéhokoliv místa počítačové sítě, a rovněž ji lze rozšiřovat o další informační moduly podle potřeb firmy.

8 SEZNAM OBRÁZKŮ

Obrázek 1 - Schéma zapojení peer to peer	12
Obrázek 2 - Síť LAN	13
Obrázek 3 - Síť WAN	14
Obrázek 4 - Druhy fyzické topologie	15
Obrázek 5 - Model ISO/OSI a TCP/IP	16
Obrázek 6 - Síťové vrstvy TCP/IP	19
Obrázek 7 - Hub versus Switch	24
Obrázek 8 - Ad-doc versus Infrastrukturní síť	27
Obrázek 9 - Síť Sloane Park	30
Obrázek 10 - Mapa přístupových bodů	32
Obrázek 11 - Znázornění vysílačů a jejich vysílací frekvence	33
Obrázek 12- Mikrotiky RB433, RB433UAH, RB532	34
Obrázek 13 - Pigtail a koaxiální kabel	35
Obrázek 14 - Směrové antény	37
Obrázek 15 - Routery 2,4GHz - WA2204, Air-Live a anténa PAN10	39
Obrázek 16 - Nanostation M5 a AirGrid M5	40
Obrázek 17 - Příkaz PING	42
Obrázek 18 - Neúspěšný ping	43
Obrázek 19 - 1)UPS Pro 550, 2) UPS Pro 900, 3) UPS SC620	49
Obrázek 20 - Zabezpečení MAC adres	51
Obrázek 21 - Přihlášení do administrace	56
Obrázek 22 - Administrace - menu	58
Obrázek 23 - Administrace - přidání accesspointu	60
Obrázek 24 - Administrace - seznam accesspointů	62
Obrázek 25 - Administrace - editace accesspointu	63
Obrázek 26 - Administrace - přidání zákazníka	69
Obrázek 27 - Administrace - seznam zákazníků	70
Obrázek 28 - Administrace - editace zákazníka	71

9 SEZNAM POUŽITÝCH ZDROJŮ

1. DONAHUE, Gary A. *Kompletní průvodce síťového experta*. Vyd. 1. Brno: Computer Press, 2009, 528 s. ISBN 978-802-5122-471.
2. HORÁK, Jaroslav. *Počítačové sítě pro začínající správce*. 4. aktualiz. a rozšíř. vyd. Praha: Computer Press, 2008, 327 s. ISBN 978-80-251-2073-6.
3. PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 1. vyd. České Budějovice: Kopp, 2004, 607 s. ISBN 80-723-2236-2.
4. SOSINSKY, Barrie. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-802-5133-637
5. ZANDL, Patrik. *Bezdrátové sítě WiFi: praktický průvodce*. Dotisk 1. vyd. Brno: Computer Press, 2006, 190 s. ISBN 80-722-6632-2..

Internetové zdroje:

1. IEEE. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2010-02-01 [cit. 2012-02-15]. Dostupné z: <http://cs.wikipedia.org/wiki/IEEE>.
2. Ping. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2012-02-19 [cit. 2012-02-21]. Dostupné z: <http://cs.wikipedia.org/wiki/PING>.
3. Cron. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2012-02-09. [cit. 2012-02-20]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Cron>.
4. Cisco. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2011-12-29. [cit. 2012-01-01]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Cisco>.
5. Wi-Fi. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2011-12-29. [cit. 2012-01-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Wifi>.
6. 802.11. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2012-02-12. [cit. 2012-02-16]. Dostupný z WWW: http://cs.wikipedia.org/wiki/IEEE_802.11.
7. MikroTik RouterBOARD. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2010-11-22. [cit. 2011-11-16]. Dostupný z WWW: http://cs.wikipedia.org/wiki/MikroTik_RouterBOARD.
8. MikroTik RouterOS. In: *Wikipedie: otevřená encyklopedie* [online]. St. Petersburg (Florida): Wikimedia Foundation, 2001-, strana naposledy edit. 2012-01-19. [cit. 2012-01-23]. Dostupný z WWW: http://cs.wikipedia.org/wiki/MikroTik_RouterOS.
9. Obrázek č.1: Schéma zapojení Peer to Peer. [cit. 2011-10-11]. Dostupný na WWW: <http://pocitacovesite.blog.cz/>.
10. Obrázek č.2: Síť LAN. [cit. 2011-10-11]. Dostupný na WWW: <http://clanky.katalognotebooku.cz/notebooky-clanky/co-je-lan/>.
11. Obrázek č. 3: Síť WAN. [cit. 2011-10-11]. Dostupný na WWW: <http://www.networkingtipsblog.com/networking/wan-computer-networks/>.

12. Obrázek č. 4: Druhy fyzické topologie. [cit. 2011-10-13]. Dostupný na WWW: <http://euler.fd.cvut.cz/predmety/UP1/up1-3.html>, http://www.brainbell.com/tutorials/Networking/Ring_Topology.html, <http://ictsmksh.blogspot.com/>, <http://ct.upce.cz/machalik/puitk-stare/site/prvni.htm>.
13. Obrázek č. 5: Model ISO/OSI a TCP/IP. [cit. 2011-10-13]. Dostupný na WWW: <http://www.earchiv.cz/anovinky/ai1592.php3>.
14. Obrázek č. 6: Síťové vrstvy TCP/IP. [cit. 2011-10-20]. Dostupný na WWW: <http://home.zcu.cz/~tody/kiv-zps/tcp-ip.html>.
15. Obrázek č. 7: Hub versus Switch. [cit. 2011-10-20]. Dostupný na WWW: http://kevincomputers.4fan.cz/?page_id=703.
16. Obrázek č. 8: Ad-hoc versus Infrastrukturní síť. [cit. 2011-10-20]. Dostupný na WWW: <http://images.yourdictionary.com/mobile-ad-hoc-network>, <http://www.djmichal.osoba.cz/informace-o-wifi>.
17. Obrázek č. 9: Síť Sloane Park. [cit. 2011-11-12]. Dostupný na WWW: <http://www.lupa.cz/clanky/na-nakup-sloane-park-si-brousi-zuby-upc/>.
18. Obrázek č. 10: Mapa přístupových bodů. [2011-12-20]. Vlastní zdroj vytvořen pomocí nástroje Malování - Windows na podkladě mapy získané ze zdroje WWW: <http://maps.google.cz/maps?hl=cs&tab=wl>.
19. Obrázek č. 12: Mikrotiky RB433, RB433UAH, RB532. [cit. 2011-12-21]. Dostupný na WWW: http://mikrotik.tlupa.com/?page_id=150, http://mikrotik.tlupa.com/?page_id=167, http://infodepot.wikia.com/wiki/Mikrotik_Routerboard_RB-532_vA.
20. Obrázek č. 13: Pigtail a koaxiální kabel. [cit. 2011-12-21]. Dostupný na WWW: <http://www.vseprowifi.cz/inshop/kabely/pigy-merene/>, <http://www.wifihw.cz/ufl-r-sma-f/>.
21. Obrázek č. 14: Směrové antény. [cit. 2011-12-21]. Dostupný na WWW: <http://avonet.cz/page/69021.alcoma-al10d-mp91/>, http://www.i4wifi.eu/22-dbi-parabolic-antenna-grid-5-ghz-_d919.html, <http://www.az-pocitace.cz/z/acant1553/antena-5ghz-parabola-jrc-24-extrem-2xpack-antena-23dbi-s-licem-5-ghz>, <http://wifi.aspa.cz/ubnt-airgrid-m5-ant-23dbi-1xzaric-1xsito-mimo-5ghz-airmax-station-outdoor-klient-mimo-5ghz-z101920/>.
22. Obrázek č. 15: Router 2,4GHz – WA2204, Air-Live a anténa PAN10. [cit. 2011-12-28]. Dostupný na WWW: http://www.i4wifi.cz/wa-2204a-54mbit-ap-kl-router-br-switch-2-4-ghz-_d26.html, <http://cz.airlive.com/product/WL-5450AP>, <http://www.i4shop.net/cz/iObchod/WebInfo.asp?Id=185>.
23. Obrázek č. 16: Nanostation M5 a AirGrid M5. [cit. 2012-01-06]. Dostupný na WWW: <http://www.streakwave.com/Itemdesc.asp?ic=NSM5>, <http://www.i4-wifi.com/?p=productsMore&iProduct=277&sName=ubnt-airgrid-m5-airmax-27-dbi>.
24. Obrázek č. 19: UPS Pro 550, UPS Pro 900, UPS SC620. [cit. 2012-01-06]. Dostupný na WWW: <http://www.apc.com/site/products/index.cfm/homeoffice/>?
25. Ceník použitých komponentů UPC. [cit. 2012-02-16]. Dostupný na WWW: <http://www.apc.com/products/family/index.cfm?id=27>.
26. Ceník použitých komponentů Mikrotik. [cit. 2012-02-16]. Dostupný na WWW: <http://www.alza.cz/mikrotik-rb433uah-d161038.htm>.

10 PRÍLOHY:

10.1 PRÍLOHA Č. 1 – UKÁZKA SOFTWARE WINBOX

The screenshot displays the RouterOS WinBox interface. At the top, the user is logged in as 'admin@192.168.5.250 (Stanice) - Winbox v5.0 on RB433C (mipsbe)'. The system status bar shows 'Uptime: 20d 03:07:41 | Memory: 237.0 MB | CPU: 8%' and 'Hide Passwords' is checked. The main menu on the left includes 'Interfaces', 'Wireless', 'Bridge', 'PPP', 'Switch', 'Mesh', 'IP', 'MPLS', 'Routing', 'System', 'Queues', 'Files', 'Log', 'Radius', 'Tools', 'New Terminal', 'MeterROUTER', 'Make Snapshot', 'Manual', and 'Exit'.

The 'Interface List' table shows the following configuration:

Interface	Type	MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors
R1-4-bridge1	Bridge	1524	102.3 kbps	8.9 kbps	10	13	0	0	0	0
R1-4-ethernet4	Ethernet	1524	304.3 kbps	5.9 Mbps	313	586	0	0	0	0

The configuration panels for two wireless interfaces are visible:

- Interface < wlan1_1 (SXS/OFT_stanice) >**:
 - Mode: ap bridge
 - Band: 2GHz-B
 - Channel Width: 20Mhz
 - Frequency: 2472 MHz
 - SSID: SXS/OFT_stanice
 - Scan List: 2412,2472
 - Wireless Protocol: unspecified
 - Security Profile: default
 - Antenna Mode: antenna a
 - Bridge Mode: enabled
 - Default AP Tx Rate: bps
 - Default Client Tx Rate: bps
- Interface < wlan4_spoil_bah >**:
 - Mode: ap bridge
 - Band: 5GHz-A
 - Channel Width: 20Mhz
 - Frequency: 5300 MHz
 - SSID: spoil_bah
 - Scan List: (empty)
 - Wireless Protocol: unspecified
 - Security Profile: default
 - Antenna Mode: antenna a
 - Bridge Mode: enabled
 - Default AP Tx Rate: bps
 - Default Client Tx Rate: bps

The bottom status bar shows system icons and the time '15:14'.

10.2 PŘÍLOHA Č. 2 – DOTAZNÍK

Vážený pane, Vážená paní,

Ve snaze poskytovat ty nejlepší služby a péči všem zákazníkům poskytovatele internetu, se na Vás obracím s laskavou žádostí o vyplnění tohoto krátkého dotazníku, který je anonymní a jeho vyplnění je dobrovolné.

Tento dotazník je zaměřen na kvalitu poskytovaných služeb internetového připojení firmou Sky-Soft s. r. o. a na Vaše přání a požadavky týkající se těchto služeb.

Budu velmi rád, pokud přijmete uvedenou nabídku ke spolupráci a věnujete svůj čas na vyplnění tohoto dotazníku.

Na otázky odpovídejte zaškrtnutím příslušné odpovědi, případně dopište podle Vašeho uvážení a názorů své odpovědi.

Pokud máte nějaké konkrétní přání, požadavek, nebo jste s něčím nespokojen/a, napište to prosím na závěr tohoto dotazníku.

Děkuji za Váš čas i ochotu věnovat se tomuto dotazníku a přeji Vám mnoho úspěchů ve Vašem životě.

Bc. Miroslav Šůch
za firmu Sky-Soft s. r. o.

Vyplněný dotazník můžete odeslat poštou na adresu firmy Sky-Soft s. r. o., ul. Husova č. 286, Nepomuk 335 01. Obálku označte „dotazník“.
Dotazník je rovněž možno vyplnit elektronicky a poslat na e-mail:
miroslav.such@skysoft.cz

Jak dlouho využíváte služeb Vašeho poskytovatele internetu?

- méně než rok
 jeden až tři roky
 tři až pět let
 více než pět let

Jak hodnotíte celkovou úroveň služeb Vašeho poskytovatele internetu?

- Velmi dobrá Průměrná Špatná

Jaké faktory nejvíce ovlivňují Váš názor na výběr poskytovatele internetu?

- Kvalita a spolehlivost
 Cena
 Reference
 Lokalita
 Jiné

V případě že jste odpověděl/a „jiné“ napište jaké:

Dochází k výpadkům internetového připojení?

- nikdy téměř nikdy občas často téměř pořád

Kolik hodin denně využíváte internet?

- méně než 1 hodinu 1-3 hodiny 3-6 hodin více než 6 hodin

Existuje nějaká činnost, nebo služba, kterou u svého poskytovatele internetu postrádáte?

- ano (jakou?)
 ne
 nedokážu posoudit

Uvažoval jste, nebo uvažujete o změně poskytovatele internetového připojení?

- ano ne

Které výhody by pro Vás byly zajímavé, kdybyste o změně poskytovatele uvažoval?

- levnější připojení
 navýšení rychlosti připojení za stejnou cenu
 lepší a rychlejší servisní služby
 jiné (napište):

Doporučil byste Vašeho internetového poskytovatele svým známým?

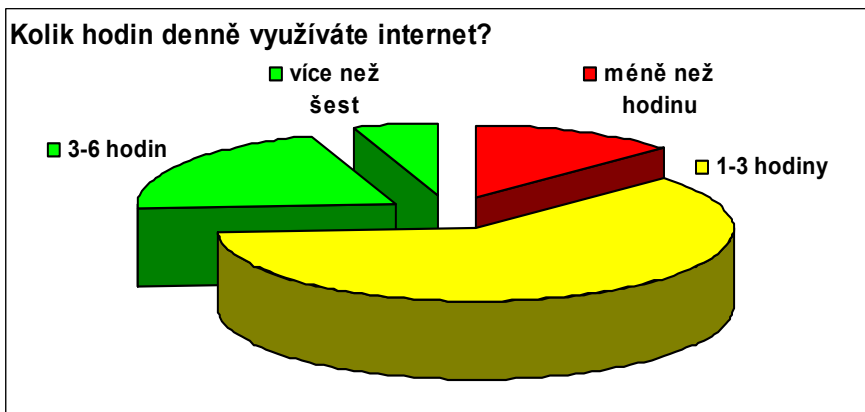
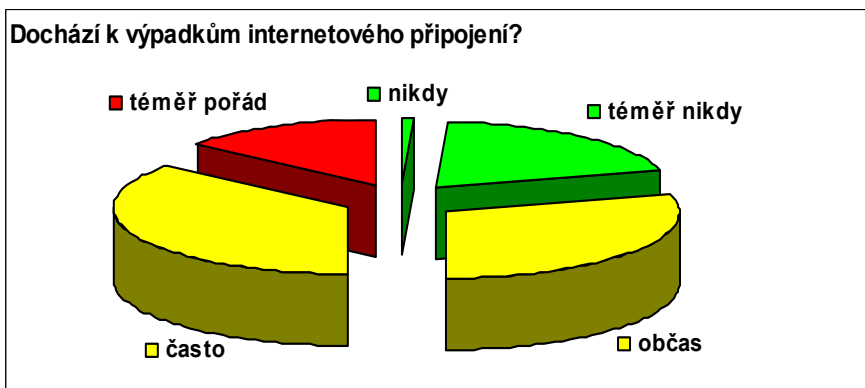
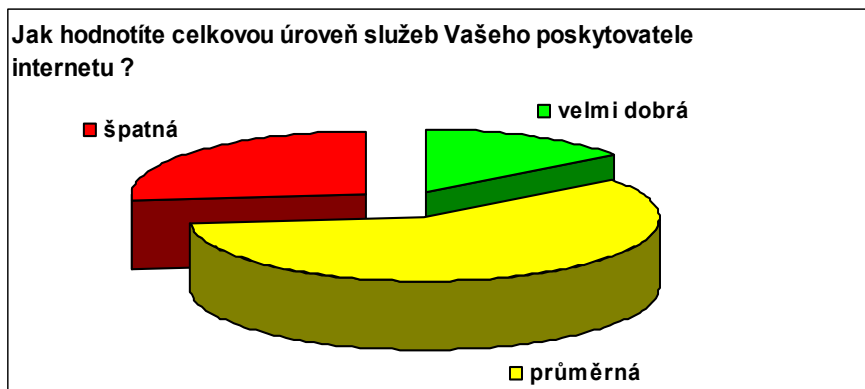
- ano ne

Konkrétní přání a požadavky:

10.3 PŘÍLOHA Č.3 – VÝSLEDKY DOTAZNÍKŮ

Otázky z dotazníku s nabídkou odpovědi:	Počet odpovědí:	Odpovědi v procentech:
Jak dlouho využíváte služeb Vašeho poskytovatele internetu?		
méně než rok	13	11,2
jeden až tři roky	34	29,3
tři až pět	58	50
více než pět	11	9,5
Jak hodnotíte celkovou úroveň služeb Vašeho poskytovatele internetu?		
velmi dobrá	17	14,6
průměrná	68	58,7
špatná	31	26,7
Jaké faktory nejvíce ovlivňují Váš názor na výběr poskytovatele internetu?		
Kvalita a spolehlivost	49	42,2
cena	39	33,7
reference	15	12,9
lokalita	11	9,5
jiné	2	1,7
Dochází k výpadkům internetového připojení?		
nikdy	1	0,9
téměř nikdy	23	19,8
občas	34	29,3
často	42	36,2
téměř pořád	16	13,8
Kolik hodin denně využíváte internet?		
méně než hodinu	15	12,9
1-3 hodiny	71	61,2
3-6 hodin	24	20,7
více než šest	6	5,2
Existuje nějaká činnost, nebo služba, kterou u svého poskytovatele internetu postrádáte?		
ano	18	15,5
ne	98	84,5
Uvažoval jste, nebo uvažujete o změně poskytovatele internetového připojení?		
ano	74	63,8
ne	42	36,2
Které výhody by pro Vás byly zajímavé, kdybyste o změně poskytovatele uvažoval?		
levnější připojení	29	25
navýšení rychlosti za stejnou cenu	41	35,3
lepší a rychlejší servisní služby	19	16,4
jiné	27	23,3
Doporučil byste Vašeho internetového poskytovatele svým známým?		
ano	51	44
ne	65	56

Nejdůležitější výsledky dotazníku v grafickém vyjádření:



10.4 PRÍLOHA Č. 4 – ZNÁZORNĚNÍ KONFIGURACE MIKROTIKU PRO UPS

The screenshot displays the RouterOS WinBox interface with the UPS configuration window open. The configuration is as follows:

- UPS <ups1>**
 - General: Name: ups1, Port: serial0, Model: Smart-UPS 420
 - Status: Transfer Cause: Unacceptable utility voltage rate of chan., Run Time Left: 02:20:00, Offline After: (empty)
 - Battery Charge: 100%
 - Battery Voltage: 13.77V
 - Line Voltage: 231.80V
 - Output Voltage: 231.80V
 - Load: 14%
 - Temperature: 0.00 C
 - Frequency: 50 Hz
 - On Line
 - On Battery
 - Replace Battery
 - Smart Boost
 - Smart Tim
 - Overload
 - Low Battery
- Script <ups>**
 - Name: ups
 - Owner: admin
 - Policy:
 - reboot
 - write
 - test
 - sniff
 - Last Time Started: Jan/19/2012
 - Run Count: 50094
- Script List**

Name	Owner	Last Time Started	Run Count
ups	admin	Jan/19/2012 20:27:28	50094
- Source:**

```

:local mailto1 "+420603904415@sms.cz o2.com";
:local mailto2 "heponuk@skysol.cz";
:local mailto3 "mla333@seznam.cz";
:local mailto4 "dohledstie@seznam.cz";
:local upstName "ups1";

#
# do NOT make changes below!
#
:global flagonbat;
:global flagbatlow;
:local batalarm 15;
:local batok 40;
:local curonbat;
:local curcharge;

:local sysname {/system identity get name};
:local datetime {/system clock get date};
:local datetime {/system clock get time};

# First run? If so, we need to initialize the global flags
if ([/typeof $flagonbat]=nothing) do={set flagonbat 0}

```

10.5 PŘÍLOHA Č.5 – WEBOVÁ STRÁNKA – GRAFY

Ukázka vygenerování grafického toku dat na serveru.

