Návrh a realizace lokální počítačové sítě ve střední firmě

The Design and Implementation of a LAN in a Medium-sized Company

Bc. Petr Haresta

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr HARESTA**
Osobní číslo:	**A10415**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh a realizace lokální počítačové sítě ve střední firmě**

Zásady pro vypracování:

1. **Analyzujte současný stav a požadavky firmy na počítačovou síť.**
2. **Proveďte návrh nové počítačové sítě.**
3. **Nakonfigurujte serverové služby (DHCP, DNS, pošta).**
4. **Zabezpečte síť pomocí firewallu a nakonfigurujte automatické zálohování.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KRČMÁŘ, Petr. Linux: postavte si počítačovou síť. 1. vyd. Praha: Grada, 2008, 182 s. ISBN 978-802-4712-901.**
2. **HUNT, Craig. Linux: síťové servery. Praha: SoftPress, c2003, 672 s. ISBN 80-864-9759-3.**
3. **SCHRODER, Carla. Linux: kuchařka administrátora sítě. Vyd. 1. Brno: Computer Press, 2009, 596 s. ISBN 978-802-5124-079.**
4. **TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-802-4720-982.**
5. **BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.**
6. **PURDY, Gregor N. Linux iptables: pocket reference. Sebastopol, CA: OReilly, c2004, 91 s. ISBN 05-960-0569-5.**
7. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-802-5122-365.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

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

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce zpracovává návrh a modernizaci stávající lokální počítačové sítě ve střední firmě. Teoretická část se zabývá informacemi o počítačových sítích, které jsou nutné pro navržení a správné řešení nové firemní sítě. Je zde popsán operační systém Linux, jeho instalace a nejpoužívanější příkazy. V teoretické části jsou uvedeny služby, které jsou konfigurovány v praktické části.

Praktická část se zabývá analýzou stávající sítě, návrhem nové sítě a konfigurací jednotlivých služeb. Obsahují konkrétní konfigurační soubory Samby, DHCP, DNS, OpenVPN, Postfixu a firewallu. V závěru jsou shrnuty požadavky firmy a návrh na jejich dosažení.

Klíčová slova: počítačová síť, Linux, firewall, Samba, DHCP, DNS, OpenVPN, Postfix

ABSTRACT

This thesis focuses on a local network and server services in a middle-size company. It contains a current-state evaluation and an improvement proposal. Theoretical part of the paper deals with computer networks in general and specific aspects which must be considered in order to develop the improvement proposal. Linux operating system, its installation and basic commands are described. The overview of the network services used in the company is presented.

The practical part of the thesis deals with the analysis of the current state of the network, the improvement proposal and its practical implementation. Specific configuration files of the network services described in previous part are presented. These services are: Samba, DHCP, DNS, OpenVPN, Postfix and firewall. In the end of the paper, the requirements of the company are summed and evaluated.

Keywords: Computer Network, Linux, firewall, Samba, DHCP, DNS, OpenVPN, Postfix

Poděkování, motto

Děkuji mému vedoucímu Ing. Jiřímu Korbelovi, Ph.D. za vedení a cenné připomínky při vypracování diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Správně navržená počítačová síť je základem úspěchu každé firmy. Bez výpočetní techniky se již nelze obejít. Nějakou dobu lze vzdorovat pokroku i se starými technologiemi. Nemá-li však firma stát na „hliněných nohách“, je nutností jí dát pevný základ „na skále“.

Obrovský důraz je kladen na vzájemnou komunikaci výpočetní techniky. Vznikají tak informační sítě, které přenáší stále více dat. Usnadňuje se vzájemná komunikace uživatelů. Historie počítačových sítí, její členění, standardy, normy, hardware, členění a dělení kabeláže jsou popsány v teoretické stati.

Praktická část je analýzou současného stavu (hliněných nohou), poukazuje na slabosti hardwaru i softwaru. Navrhuje postavit počítačovou síť na pevný „skalnatý“ základ operačního systému Linux, s důrazem na zálohování dat a zabezpečení celého systému. V neposlední řadě je možno najít i finanční kalkulaci.

I. TEORETICKÁ ČÁST

1 TEORETICKÉ ZÁKLADY

Kapitola popisuje teoretické základy týkající se počítačových sítí. Jsou zde nastíněny vlastnosti, dělení a topologie sítí. Je vysvětlen síťový hardware, přenosové média a jejich standardy. Je zmíněn model ISO/OSI, jenž je standardem počítačových sítí.

1.1 Počítačové sítě

V dnešní době obrovského množství počítačů je dobré jejich spojení v jeden celek. Počítačová síť je spojení nejméně dvou, ale převážně více počítačů prostřednictvím přenosového média v jeden celek. Toto spojení umožňuje udržovat počítačovou síť s aktuálními daty (sdílenými daty, databázemi), sdílení hardwaru (např. tiskárnou připojenou k jinému počítači) [1].

V počítačových sítích rozlišujeme dva typy počítačů. Počítač, který je připojený k síti a nabízí své prostředky, se nazývá server. Počítač, který k těmto prostředkům přistupuje, se nazývá klient/pracovní stanice. Stanice jsou většinou levné, málo výkonné. Oproti tomu servery jsou výkonné, optimalizované pro rychlé zpracování požadavků.

Pro přenos dat se využívá přenosové médium. Přenosové médium je buď vlnění, nebo fyzická přenosová jednotka jako je kabel. Přenosové médium slouží k přenosu analogových a digitálních dat. V počítačové síti se setkáváme s pojmem síťový segment. Síťový segment chápeme jako část počítačové sítě – např. rozdělení velké sítě na několik menších.

1.2 Rozdělení počítačových sítí

Sítě můžeme rozdělit podle:

- Velikosti – rozlehlosti
- Typu sítě
- Topologie
- Komunikace

1.2.1 Dělení podle velikosti

Sítě dle velikosti můžeme rozdělit následně:

- **sítě PAN** (Personal Area Network) – osobní síť. Její dosah je velmi malý. Maximálně několik metrů. Síť slouží především potřebám jednotlivce nebo velmi malé skupině uživatelů. Slouží uživateli především k připojení různých mobilních zařízení (mobilní telefony, tablety, PDA) a umožňuje jim komunikovat vzájemně mezi sebou. Pomocí technologií Bluetooth, Wifi, USB atd.
- **sítě LAN** (Local Area Network) – jedná se o lokální sítě omezené na malé geografické území (domácnost, malé firmy).
- **sítě MAN** (Metropolitan Area Network) – jedná se o rozlehlou počítačovou síť, kdy spojuje několik menších podsítí. Jejich využití lze nalézt především jako páteřní sítě velkých podniků a městských institucí. Mohou být veřejné i soukromé. Tvoří přechodovou hranici mezi sítěmi LAN a WAN. Mezi přenosová média vzhledem k vysokým přenosovým rychlostem se využívají optické kabely [1].
- **sítě WAN** (Wide Area Network) – jedná se o rozlehlé sítě. Tato síť se skládá z propojených více sítí. To je buď provedeno opticky, nebo bezdrátově. Rozsáhlost sítě může být různá od firemní sítě s více pobočkami až po tu největší síť internet.

Jak ale rozlišit, zdali se jedná ještě o síť LAN nebo už síť WAN? Pro síť LAN se používají kabely, oproti tomu WAN propojují sítě vzdálené desítky km. K tomu se nejčastěji používají optická média, telekomunikační linky atd.

1.2.2 Dělení podle typu sítě

Sítě lze rozdělit do dvou kategorií (peer to peer a klient/server). Toto rozdělení je důležité, protože obě kategorie se od sebe liší a nabízí uživatelům odlišné schopnosti [1].

- **síť peer to peer** (rovný s rovným) - tento typ sítě není v dnešní době obvyklý. Lze se s ní setkat u menších sítí s menším množstvím uživatelů. V této síti nenalezneme žádné vyhrazené servery. Všechny počítače v síti jsou si rovné a označují se peer (druzi). Každý počítač slouží jako klient i server. Uživatel každého počítače si stanoví, jaká data a jakým způsobem bude v síti sdílet. Velkou slabinou sítě je zabezpečení. Všichni uživatelé sítě si nastavují své vlastní zabezpečení pro sdílené

prostředky. Výhodou sítě je, že pro správu nejsou zapotřebí příliš velké znalosti a jsou levným řešením.

- **síť klient/server -** síť peer to peer není vhodná pro velké sítě. Síť typu klient/server je výkonnější. Uplatnění najde především v síti s větším počtem počítačů. Klient si žádá o služby serveru. Servery jsou optimalizovány pro rychlé zpracování požadavků od více síťových klientů. Výhody jsou především v bezpečnosti dat, přehlednosti a rychlosti. Na serveru je nainstalován síťový operační systém např. Microsoft Windows 2003/2008 Server, Novell Netvare nebo distribuce Linuxu (Red Hat, SuSE, CentOS). Nevýhody tohoto typu sítě jsou vysoké náklady na nákup serveru a nutnost mít zkušeného správce sítě.

1.2.3 Dělení podle topologie sítě

Topologií je označován způsob, jakým jsou počítače a další zařízení v síti propojeny. Topologii lze rozdělit na [2]:

- **fyzickou** - fyzická topologie udává, jak jsou jednotlivá zařízení mezi sebou zapojeny (pracovní stanice, servery atd.). Propojení je realizováno pomocí kabelů nebo bezdrátově.
- **logickou** - logická topologie definuje, jakým způsobem mezi sebou komunikují prvky v síti a jak se přenášejí data. Logická topologie nemusí být shodná s fyzickou.

1.2.3.1 Logická topologie

- **typ sběrnice** - informace je zasílána všem uzlům současně. Jednotlivé uzly obdrží každou informaci v přibližně stejný okamžik.
- **typ kruh** - informace je zaslána sekvenčně, podle předem daného pořadí, z jednoho uzlu na uzel následující.

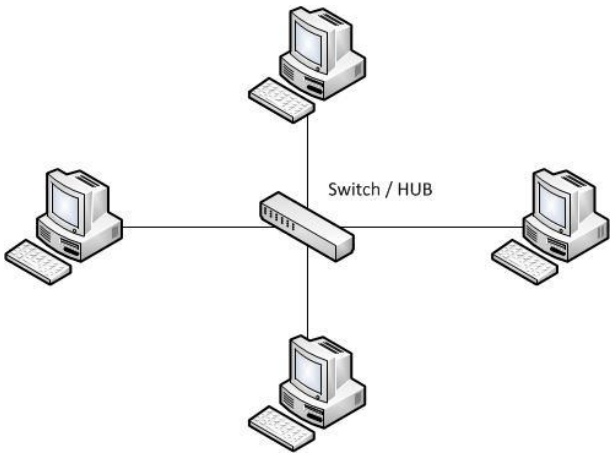
1.2.3.2 Fyzická topologie

- **Sběrnicová topologie (bus topology)**

Dříve běžně používaná topologie. V současné době nepoužívaná z důvodu vzniku kolizí na síti. K propojení využívala koaxiální kabel.

- **Hvězdicová topologie (star topology)**

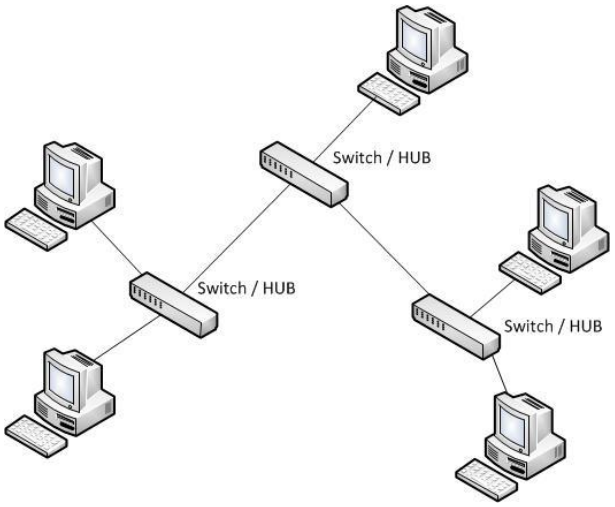
Topologie zapojením připomínající hvězdici. Každé zařízení je připojeno samostatným kabelem [2], v dnešní době nejčastěji kroucenou dvojlinkou k centrálnímu uzlu. Centrální uzel dříve tvořily huby, ale v dnešní době jsou to především switche (popsán v kapitole 1.7.1). Ve switchi se data nasměrují ke správnému a konkrétnímu příjemci – nedochází k přetížení sítě. Starý hub posílal data i k dalším stanicím, čímž docházelo k zatížení sítě. Síť je odolná proti výpadkům jednotlivých zařízení a linek. Lokalizace poruchy je snazší než u sběrnicové topologie. Síť je citlivá na poruchu centrálního uzlu [2]. Je dnes nejpoužívanější topologií v síti LAN.



Obr. 1. Hvězdicová topologie

- **Stromová topologie (tree topology)**

Topologie je složena z několika hvězdicových segmentů, které jsou v dnešní době převážně spojeny switchi. Tato topologie má stejné výhody a nevýhody jako hvězdicová a využívá se ve velkých firmách [2].



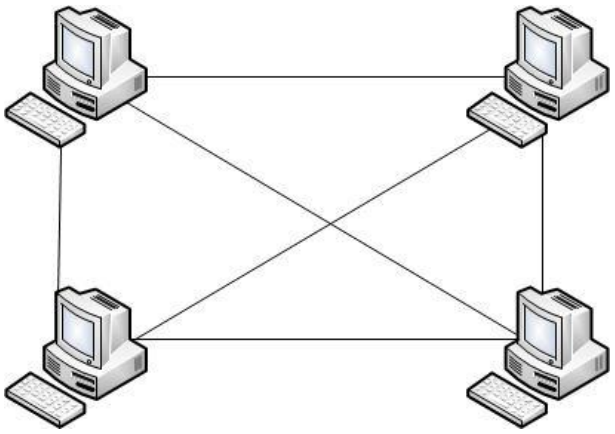
Obr. 2. Stromová topologie

- **Páteřní topologie (backbone)**

Jedná se o vedení, kterým jsou propojeny ostatní segmenty sítě. Veškerá komunikace stanic přesahující jeden síťový segment pak prochází právě tímto vedením. S topologií se můžeme hlavně setkat u sítí typu WAN. Hlavními požadavky na páteřní vedení je vysoká přenosová rychlost.

- **Mesh topologie**

Někdy také nazývána topologií úplnou. Jedná se o topologii, kde každé zařízení může být propojené s každým (úplný mesh) nebo může být použita alternativa, kde se některé spoje vynechají (částečný mesh). Výhodou topologie je velká spolehlivost [1]. V případě výpadku spoje si data najdou jinou cestu k cíli. Nevýhodou topologie je složité připojení nového zařízení. Uplatnění nachází spíše v bezdrátových sítích.



Obr. 3. Mesh topologie

1.3 Dělení podle komunikace

- **sítě spojované** - sítě s navazováním spojení. Dříve, nežli si obě koncové stanice vymění data, je nutné navázat spojení. Typicky se s tímto setkáme u telefonních sítí.
- **sítě nespojované** - sítě bez navazování spojení fungují na principu rozdělení dat na malé balíčky tzv. pakety. Ty putují sítí, dokud nedorazí do cíle [1]. Jednotlivé pakety jsou opatřeny cílovou adresou, podle které je jednotlivé uzly sítě směrují. Pakety mohou dorazit v nesprávném pořadí. Standardně se využívá přepojování paketů (packet switching), které jsou součástí aktivních prvků a pomocí nich jsou pakety filtrovány, usměrňovány.

1.4 Typy serverů

V dnešní době, kdy musí servery plnit více úkolů je dobré jejich rozdělení dle specifických prostředků a služeb, aby každý úkol byl proveden co nejefektivněji. Potom v určité síti může být několik serverů [1]:

- **souborové a tiskové servery** – jejich hlavním úkolem je zajišťovat přístup uživatele k souborům a k prostředkům pro tisk. Výhodou souborového serveru je centralizovaná správa a snadnější zálohování.
- **aplikační servery** – slouží ke správě obrovského množství dat a efektivnímu poskytování dat klientům.
- **databázové servery** – ve většině případů se používá systém správy na databázi založený na SQL (DBMS). Klientské stanice odešlou požadavky SQL serveru a ten přistoupí k databázi, aby daný požadavek zpracoval a vrátil výsledek klientské stanici. Software pro správu databází je např. Microsoft SQL Server.
- **webové servery –** jedná se o server, který je zodpovědný za vyřizování požadavků http od klientů. Klientovi webový server na základě požadavku odešle webovou stránku.
- **FTP servery** – servery FTP zajišťují přenos souborů mezi jednotlivými počítači. Obsahují prvky zabezpečení přenosu. Servery FTP využívají uspořádání klient/server. Servery FTP zajišťují zabezpečení přenosu, řízení souborů atd. Klient

zajišťuje příjem souborů a jejich uložení na disk, k tomu lze využít specializovaný software.

- **poštovní servery** – jedny z nejpoužívanějších typů serverů. Zajišťují nám e-mailovou komunikaci. Poštovní servery (Sendmail, Postfix, Microsoft Exchange) zpracovávají tok pošty mezi jednotlivými uživateli sítě.
- **firewall server** – firewall slouží jako obranná linie k neoprávněnému přístupu k nebo z privátní sítě LAN. Firewally máme hardwarové, softwarové a jejich kombinaci. Zabraňuje neoprávněným uživatelům z veřejné sítě (internetu) přistoupit do sítě soukromé (LAN). Veškerá komunikace směřující do nebo z privátní sítě prochází firewallem, který zprávu prohlédne a zablokuje ty, které nevyhovují požadovaným kritériím zabezpečení.

1.5 Model ISO/OSI

Vypracovala organizace ISO v roce 1984 za účelem sjednocení a především standardizaci počítačových sítí. Nastavuje principy sedmivrstvé síťové architektury. Vrstvy jsou oddělené a každá má svou specifickou funkci pro komunikaci. Každá vrstva využívá služby nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě. Model je důležitý především pro výrobce síťového hardwaru. Model ISO/OSI se velmi často rozděluje do dvou kategorií horních a spodních vrstev. Relační až aplikační vrstva patří do kategorie horních a obvykle souvisejí s aplikacemi. Dolní vrstvy fyzická až transportní souvisejí s přenosem informací v síti a jsou nejčastěji implementovány v hardwaru. Komunikace mezi stejnými vrstvami se nazývá interface, mezi různými protokoly [2].

- **Fyzická vrstva**

Podporuje fyzickou komunikaci. Popisuje mechanické, elektrické, funkční a další vlastnosti. Fyzické spojení může být dvoubodové (sériová linka) nebo mnohobodové (Ethernet). Popisuje, jak je reprezentována logická jednička, jak přijímací stanice rozezná začátek bitu apod.

- **Linková (spojová) vrstva**

Tato vrstva realizuje spojení mezi dvěma sousedními systémy. Přenáší datagramy po fyzickém médiu. Využívá k tomu fyzické adresy síťových karet tzv. MAC adresy. Seřazuje

přenášené rámce, stará se o nastavení parametrů přenosů linky, oznamuje neopravitelné chyby atd.

- **Síťová vrstva**

Tato vrstva se stará o směrování v sítí a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesouvisí [1]. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti přenosových sítí. Zajišťuje volbu trasy při spojení mezi uzly, tzv. routování.

- **Transportní vrstva**

Poskytuje spolehlivý, transparentní přenos dat s požadovanou kvalitou. Vyrovnává rozdílné kvality přenosových sítí. Setkáváme se s protokolem TCP (spolehlivý), UDP (nespolehlivý). Na téhle vrstvě se provádí řízení toku (k zachování integrity dat), zajištění bezchybného doručení dat na místo určení, segmentaci datagramů z horních vrstev atd.

Protokol TCP garantuje spolehlivé (spojované transportní služby) doručení dat a to ve správném pořadí. Umožňuje rozlišit data pro vícenásobné, současně běžící aplikace (např. ssh server a www server). Segment v protokolu TCP se skládá z 224 bitů obsahující zdrojový a cílový port, kontrolní součty, data atd.

Protokol UDP nezaručuje přenos všech datagramů v síti (nespojované transportní služby). Oproti protokolu TCP nezaručuje, zda se přenášený datagram neztratí, anebo nezmění-li se pořadí doručovaní datagramů v síti. Protokol UDP je vhodný pro nasazení, kde je potřeba jednoduchost a rychlost (DNS, multimedia, hry). Protokol UDP je bezstavový.

- **Relační vrstva**

Cílem této vrstvy je spravovat relace mezi spolupracujícími relačními vrstvami a řídit výměnu dat mezi nimi. Provádí ověřování uživatelů, zabezpečuje přístup k zařízením. Umožňuje vytvářet a ukončovat spojení mezi relačními spojeními.

- **Prezentační vrstva**

Funkcí této vrstvy je transformovat data do podoby, které používají aplikace. Formát datové struktury se může lišit na obou komunikačních systémech. Tato vrstva převádí kódy a abecedy, komprimuje, šifruje. Vrstva se zabývá jen strukturou dat, ale ne jejich významem. V praxi často splývá s vrstvou relační.

- **Aplikační vrstva**

Jedná se o vrstvu, která má nejblíže ke koncovému uživateli. Obstarává služby e-mailu, souborového přístupu, tiskové, databázové atd [2].

1.6 Členění síťových prvků

- síťové počítače (počítače pracující v síti)
- síťový hardware (přenosová media, aktivní/pasivní prvky, síťové karty)
- síťový software (síťový operační systém)

1.7 Síťový hardware

Hardwarové prvky sítí jsou nedílnou součástí počítačové sítě. Spojením těchto prvků jsou dosaženy různé topologie, standardy, vlastnosti. Patří sem tzv. pasivní a aktivní prvky. Síťový hardware má vliv především na rychlost a kvalitu přenosu [2].

- Aktivní prvky jsou takové, které určitým způsob aktivně se signálem pracují. Zesilují, vyhodnocují, směrují atd. Vyžadují napájení. Patří sem zařízení switch, router apod.
- Pasivní prvky sítí jsou zařízení, které nevyžadují napájení a na komunikaci se podílejí pouze pasivně (přenosová média).

1.7.1 Switch

Nahradil zastaralé huby, jejich funkcí bylo rozbočování signálu neboli větvení sítě. Switchem jsou jednoduše propojeny sítě v hvězdicové topologii. Patří do aktivních síťových prvků, skládající se z několika jednotek až případných stovek portů. Výhodou switche je, že odděluje komunikaci stanic od zbytku sítě. Nedochází tím ke zbytečnému zahlcování sítě provozem, který není nutný, jako tomu bylo u hubu. Zjednodušeně řečeno, posílá-li jedna stanice paket například stanici čtyři, tak hub pošle pakety všem stanicím připojených do sítě, ale pouze stanice čtyři paket přijme. Většina switchů pracuje na druhé vrstvě modelu ISO/OSI. V dnešní době se díky svému rozšíření začínají objevovat takzvané L3 switche. L3 označuje switche, které umějí pracovat na třetí

vrstvě modelu ISO/OSI. Tyto switche umí analyzovat protokol IP a fungovat jako router [1].

1.7.2 Směrovač (router)

Řadí se mezi nejinteligentnější síťové prvky. Pracuje na třetí vrstvě modelu ISO/OSI. Router inteligentně přeposílá datagramy směrem k cíli. Dále je doplněn o filtraci paketů. Rozdíl oproti switchi je v tom, že router spojuje dvě rozdílné sítě, zatímco switch spojuje počítače v místní síti. Routery bývají na hranicích sítě [2]. Router využívá routovací tabulku, která obsahuje nejlepší cesty k jistým cílům a routovací metriky.

1.7.3 Síťové karty (NIC)

Síťová karta (Network Interface Controller) slouží ke vzájemné komunikaci počítačů v počítačové síti. Karta je rozhraním mezi počítačem a sítí. Zprostředkovává komunikaci podle pravidel daných datovým protokolem. Síťové karty jsou v dnešní době integrovány téměř ve všech základních deskách. Každá síťová karta má od výrobce definovaný jedinečný 48-bitový identifikátor, nazývající se MAC adresa [2].

1.8 Přenosová média

Přenosová média jsou řazena do kategorie pasivních prvků. Jedná se o média, kterými jsou přenášena data. Přenosová média můžeme rozdělit na tři různé typy:

- **metalické kabely** – nejčastěji používaná přenosová media, založená na kovovém vodiči, který přenáší elektrický signál (koaxiální kabel, kroucená dvojlinka).
- **optické kabely** – přenášejí data světelnými impulsy ve světlovodivých vláknech.
- **vzduch** – vysokofrekvenční elektromagnetické vlnění

V dnešní době se používají převážně kroucené dvojlinky a optické kabely. Mezi zastaralá média patří koaxiální kabel. Přenosová média mají své parametry:

- **Přenosová rychlost**

Parametr udávající rychlost přenosu dat. Rychlost se uvádí nejčastěji v megabitech za sekundu (Mb/s), nové rychle se rozšiřující prvky 1 000 Mb/s tedy 1 Gb/s (gigabit za sekundu) [1].

- **Impedance**

Kabel představuje pro připojené zařízení určitý odpor (impedanci). Impedance kabelu a zařízení by měli být stejné. Velikost impedance se uvádí v Ω (ohmech).

- **Útlum**

Jedná se o úbytek v přenosovém médiu. Velikost útlumu se uvádí v dB (decibelech) a je přímo úměrná délce kabelu. Čím delší kabel, tím větší je útlum.

- **Zkreslení**

Jedná se o deformaci signálu, která vzniká při jeho přenosu. Opět platí, že čím delší je kabel, tím větší je zkreslení.

- **Odolnost proti vnějšímu elektromagnetickému vlnění**

Jde o rušení signálu z okolního vedení. Jednotkou je dB. Čím vyšší hodnota, tím je toto vzájemné rušení nižší.

1.8.1 Kroucená dvojlinka (twisted pair cable)

Jedná se o nejrozšířenější metalický vodič v sítích LAN, skládající se z 8 vodičů, tvořící 4 páry. Elektrické signály přenášené vodičem jsou náchylné na rušení, vznikající vzájemným působením vodičů. Rušení se předchází zkroucením vodičů tvořící jeden pár. Páry jsou také navzájem překrouceny. Jednotlivé páry jsou od sebe odlišeny barvou. Setkáme se s ní nejčastěji ve dvou variantách:

- **STP (Shielded Twisted Pair) – stíněná dvojlinka**

Má kovové opletení, zvyšující ochranu proti vnějšímu rušení. Jsou dražší než nestíněný kabel [2].

- **UTP (Unshielded Twisted Pair) – nestíněná dvojlinka**

Vyrábí se v různých kategoriích očíslovaných 1-7. Nejčastěji se setkáváme s kabely kategorie 5 nebo 5e. Kabel kategorie 5 se používá pro rychlost do 100 Mb/s, kategorie 5e je určena pro rychlost 1 Gb/s. Kabely kategorie 6 a 7 jsou určené pro nejrychlejší přenosy jednotky Gb/s a 10 Gb/s přenosy. Jednotlivé kategorie se od sebe liší vnitřní konstrukcí, která nám umožňuje zvětšit šířku pásma – vyšší rychlost přenosu dat [1]. Větší rychlosti dat dosáhneme pomocí většího počtu kroucení. K dosažení rychlosti musíme samozřejmě

použít aktivní prvky odpovídající kategorie. Impedance u všech typů je 100 ohmů, maximální délka kabelu pro síť Ethernet je 100 m. K zakončení kabelu se používá konektor RJ-45.

1.8.2 Optický kabel (fiber optic cable)

Signály jsou přenášeny pomocí světla. Princip přenosu dat je úplný odraz světla. Optický kabel se skládá z jádra, pláště světlovodu a plastového obalu. Základním prvkem kabelu je optické vlákno. Zároveň jich může mít optický kabel více. Optické kabely jsou schopny přenést data na velké vzdálenosti – řádově kilometry, s vysokou kapacitou přenášených dat. Výhodou oproti kroucené dvojlince je, že optický signál nelze snadno odposlouchávat. Používají se kvůli rychlosti především v páteřních sítích.

K optickým kabelům můžeme potřebovat převodník, abychom převedli elektrický signál na optický a opačně. Další možností je použít přímo síťovou kartu, ke které lze přímo připojit optický kabel. Zdrojem optického signálu je laser nebo LED dioda [2]. Přijímač se skládá z fotodetektoru. Optické kabely rozdělujeme na:

- **Jednovidé**

Mají velmi úzké jádro. Kabelem prochází jen jeden paprsek. Mají lepší optické vlastnosti (malý útlum) - vyšší přenosovou kapacitu. Dokážou přenést signál na delší vzdálenost než mnohovidové. Jsou oproti mnohovidovým kabelům dražší.

- **Mnohovidové**

Mají tlustší jádro. Paprsek se odráží od pláště vlákna. Vzhledem k tomu, že je jádro tlustší, může být generováno více paprsků současně (odborně se jim říká vidy). Každý vid vstupuje do kabelu pod jiným úhlem a odráží se také pod jiným úhlem. Paprsek tedy prochází optickým vláknem od generátoru až po detektor po jiné dráze než ostatní vidy. Detektor pak musí provést součet jednotlivých vidů. Kabel má horší optické vlastnosti a při práci je potřeba s ním opatrněji zacházet.

Kabel je ukončen normovanou koncovkou [2]. Převážně se používají dva typy zakončení:

- kulatý konektor ST
- hranatý konektor SC

1.9 Standardy síťového hardwaru

Jednotlivé prvky sítě lze spojovat. Jsou přitom využívány různé kabely, přístupové metody, topologie sítě a rozdílná rychlost sítě. Při spojování prvků sítě používáme různou rychlost sítě. Proto byly stanoveny standardy-normy, které definují požadavky na technické provedení sítí. Ethernet je nejrozšířenější technologií pro budování přístupových sítí typu LAN. Pracuje s ethernetovými rámci. Ethernet je technologií zajišťují skutečný přenos dat. V modelu ISO/OSI pokrývá fyzickou a linkovou vrstvu. Pro sítě typu LAN jsou důležité standardy [1]:

- IEEE 802.3 Standardy sítě Ethernet
- IEEE 802.4 Sběrnicové sítě s metodou přístupu token
- IEEE 802.5 Kruhové sítě s metodou přístupu token
- IEEE 802.11 Pro bezdrátové sítě

Z výše uvedeného vyplývá, že nás zajímají především vlastnosti:

- Topologie sítě (kruhová, stromová …)
- Rychlost přenosu dat
- Typ, zapojení a délka kabelu
- Přístupová metoda

1.9.1 Gigabitový Ethernet (rychlost 1 000 Mb/s)

Implementace Ethernetu, které dosahují přenosových rychlostí až 1 000 Mb/s. Standardizované pro optické kabely (802.3z) a kroucenou dvojlinku (802.3ab). Člení se na čtyři kategorie [2]:

- **1000Base-X** – navržen především pro optické kabely. Standard existuje ve dvou variantách, lišící se použitým světelným zdrojem.
- **1000Base-SX** – používá krátkovlnný světelný zdroj 850 nm. Světlo se přenáší levnými mnohovidovými optickými kabely. Vzdálenost přenosu je 220 m při průměru optického vlákna 62,5 μm a 500 m při průměru 50 μm.

- **1000Base-LX** – používá delší světelný zdroj 1 310 nm. Je možné použít dražší jednovidový optický kabel, jehož maximální délka segmentu je až 5 km nebo levnější mnohovidový, jehož vzdálenost přenosu je 550 m.
- **1000Base-T** – definuje použití Gigabit Ethernetu pomocí kroucené dvojlinky kategorie 5 a vyšší. Doporučuje se kabeláž kategorie 5e. Využívá všech 4 párů a tím lze dosáhnout rychlosti 1 000 Mb/s. Maximální délka segmentu je 100 m.

1.9.2 10 GB Ethernet (Standart 802.3ae)

Verze Ethernetu podporující přenosové rychlosti až do 10 Gb/s. Je vyvíjena nejen pro sítě LAN, ale také pro sítě MAN a WAN. Přenosová vzdálenost může být při použití jednovidého kabelu až 40 km. Vzhledem k vysokým frekvencím, kterými jsou data vysílána, je nutné použít jako zdroj světla laser nikoliv LED diodu. Existuje v několika variantách [2]:

- **10GBase-S (short)** – využívá laser s krátkou vlnovou délkou (850 nm) a je určena pro vícevidové kabely. Maximální délka optického kabelu je 300 m, ale při použití kvalitnějšího kabelu je možné propojení na větší vzdálenost.
- **10GBase-L (long)** – používá laser s dlouhou vlnovou délkou (1 310 nm) a je určena pro jednovidové optické kabely s maximální délkou 10 km.
- **10GBase-E (extended)** – používá laser s velmi dlouhou vlnovou délkou 1 550 nm. Určena pro jednovidové optické kabely, kdy maximální délka kabelu je 40 km.
- **10GBase – LX4** – používá laser o vlnové délce okolo 1 310 nm. Může používat jednovidové (max. délka 10 km) i vícevidové (max. délka 300 m) optické kabely.

2 LINUX

Kapitola se zabývá členěním linuxových distribucí, jejich dělením a vlastnostmi. Popisuje základní přikazy, které jsou nutné k administraci systému. V závěru je popsáno nastavení síťového rozhraní.

2.1 Linuxové distribuce

Dříve, než začneme s instalací linuxu, je nutné si zvolit vhodnou distribuci. Linuxových verzí existuje něco okolo tisíce. Zanalyzujeme si, pro jaké účely distribuci budeme využívat, jestli pro domácí stanici, server, mobilní telefon. Přehled všech distribucí najdeme na http://distrowatch.com/.

Distribuce lze rozdělit na komerční (RedHat, SuSE) a nezávislé distribuce (CentOS, Debian), které jsou zdarma. Dále člení na live a standardně instalované distribuce. Live distribuci si můžeme spustit bez instalace, stačí jen nabootovat s CD. Pokud budeme instalovat nějakou běžnou desktopovou distribuci, setkáme se nejčastěji se dvěma správci oken KDE a GNOME. Nelze říci, který správce oken je nejlepší, nicméně výše zmíněné se řadí mezi výkonově náročnější. Pokud toužíme po méně výkonné distribuci, je lepší nainstalovat správce oken Xfce [3].

Co to vůbec distribuce je? Základní součástí všech distribucí je tzv. jádro [3], které je rozšířeno o vhodný software. Tím se od sebe liší. Jsou vždy nějak pojmenovány, např. Fedora, Ubuntu a mají různé zaměření, např. pro desktop, vývoj, výuka atd. Můžeme si také vytvořit svou vlastní distribuci.

Samozřejmě jsme instalovali nějakou serverovou edici. Zde se většinou žádné grafické rozhraní neinstaluje, protože většina serverů nemá připojený ani monitor, klávesnici a k serverům se připojujeme vzdáleně a spravujeme je pomocí textové konzoly.

Dalším rozhodujícím faktorem je balíčkovací systém. Většina distribucí je rozšiřována, aktualizována pomocí tzv. balíčků. Mezi nejpoužívanější balíčky patří DEB a RPM.

Pro každého administrátora nebo uživatele jsou jiné rozhodující faktory. Pro někoho je rozhodují bezpečnost, pro někoho zase snadnost instalace.

Rozdíl mezi desktopovou a serverovou distribucí není nijak zásadní. Pro stavbu našeho serveru budeme vybírat nekomerční serverovou distribuci. Rozhodoval jsem se mezi těmito třemi:

- **Debian**

Distribuce Debian je spíše vhodnější pro zkušenější administrátory [3]. Je známá přehledným balíčkovacím systémem obsahujícím 29 000 balíčků. Debian v současné době využívá jádro linuxu, nicméně pokračují práce i pro jiná jádra (Hurd, FreeBSD…). Využívá balíčky deb. Vychází ve dvou verzích stable a testing. Stable je stabilní verze balíčků, které se mění poměrně za dlouhou dobu, tato verze je vhodná na server. Máme jistotu, že po aktualizaci systému budou všechny služby fungovat. Oproti tomu verze testing obsahuje neotestované balíky, které později mohou způsobit nefunkčnost některých služeb.

- **Gentoo**

Hlavní odlišností této distribuce je, že software se distribuuje pomocí zdrojových souborů, které si uživatel zkompiluje do spustitelných souborů. V dnešní době je kompilace řízena utilitami, které zvládne úplný začátečník. Výhodou zdrojových souborů je, že se dají upravovat dle vlastní potřeby [3]. Nevýhodou, že zdrojové soubory se musí kompilovat, pak je potřeba více procesorového času, což prodlužuje aktualizaci systému až na několik hodin.

- **CentOS**

Distribuce je odvozena od největší komerční distribuce RHEL (Red Hat Enterprise Linux). Je 100% binárně kompatibilní s RHEL. CentOS je k dispozici zcela zdarma a není spravován ani podporován firmou Red Hat. Rozdíly oproti RHEL jsou především v odstranění ochranných známek. Aktualizace jsou vydávány se zpožděním, po vydání zdrojových kódů RHEL.

Pro stavbu serveru jsem zvolil distribuci CentOS. Důvodem je, že je volně dostupná, velice stabilní a snadno se spravuje. Je pravidelně aktualizována, obsahuje všechny nástroje, které budeme potřebovat. Obsahuje staré, ale osvědčené verze softwaru, které nemají bezpečnostní díry atd.

2.2 Nejpoužívanější příkazy

- **Pro práci se soubory**

Tab. 1. Příkazy pro práci se soubory

Příkaz:	Popis příkazu:
pwd	Print work directory - vypíše adresář ve kterém se právě nacházíme
mkdir	(Make dir - vytvoř adresář) - vytvoří nový adresář zadaného jména
cd	Change directory - změň adresář
cd	Přesune se do domovského adresáře
cd /home/temp	Přesune se skrz adresář home do adresáře temp
cp	Copy - kopíruj
cp zdroj cíl	Zkopíruje soubor zdroj do souboru cíl. Původní soubor zůstává, jen je vytvořena nová kopie
mv	Move - přesuň, přesune soubor na jiné umístění nebo ho přejmenuje
mv zdroj cíl	Přejmenuje soubor zdroj na soubor cíl
mv zdroj /root	Přesune soubor zdroj do adresáře root, nepřejmenuje ho
rm	Odstraní zadaný soubor, tento příkaz nefunguje na neprázdných adresářích
rm -r	Smaže rekurzivně všechny soubory v adresářích a nakonec i samotný adresář
ls	(List - seznam) vypíše seznam souborů v daném adresáři
ls -a	Vypíše všechny soubory v adresáři včetně skrytých
ls -l	Podrobný výpis souborů (velikost souborů, čas vytvoření apod.)
find	Prohledává adresářovou strukturu
find . -name hledany.txt	Hledá soubor hledany.txt v aktuálním adresáři a podadresářích
locate	Vyhledávání souborů pomocí vzorků v pomocné databázi
locate smb.conf	Vyhledá soubor smb.conf
cat	Vypíše obsah souboru - cat /etc/dhcpd.conf
head	Vypíše začátek souboru - head /etc/dhcpd.conf
tail	Vypíše konec souboru - tail /etc/dhcpd.conf
man	Vypíše manuálovou stránku daného příkazu - man cd -> vypíše návod na použití příkazu cd

- **Příkazy pro zjištění systémových informací**

Tab. 2. Příkazy pro zjištění systémových informací

Příkaz:	Popis příkazu:
ipconfig	Vypíše informace o síťových rozhraních - IP adresu, masku atd.
route -n	Výpis routovací tabulky
iptables -L	Výpis nastavených pravidel firewallu
hostname	Zobrazí jméno počítače

- **Příkazy pro práci s uživatelskými účty a skupinami**

Tab. 3. Příkazy pro práci s uživatelskými účty

Příkaz:	Popis příkazu:
adduser	Vytvoří nového uživatele (adduser petr)
userdel	Vymaže uživatele (userdel petr)
passwd	Nastaví heslo uživatele (passwd petr)
addgroup	Vytvoří skupinu
groupdel	Vymaže skupinu
gpasswd	Nastavení hesla skupiny

Výše uvedené příklady patří mezi jedny z nejpoužívanějších. Příkazů existuje celá řada a v případě potřeby lze využít dokumentaci pomocí příkazu `man`.

2.3 Konfigurace síťových rozhraní

Připojení do sítě je nejčastěji realizováno ethernetovou kartou (může být také realizováno sériovou linkou). Síťová rozhraní v linuxu jsou označována eth0 až ethX, dle počtu síťových karet. Další přítomné rozhraní je loopback, označeno zkratkou lo. Má přidělenou IP adresu 127.0.0.1 a masku 255.0.0.0 [3].

Nastavení síťových rozhraní lze provést pomocí příkazu `ifconfig`. Zadáme-li příkaz `ifconfig` bez parametrů, vypíše přehled a nastavení všech rozhraní v počítači. Chceme-li například zobrazit nastavení adaptéru eth0, použijeme příkaz: `ifconfig eth0`

```
eth0          Link encap:Ethernet  HWaddr 00:E0:7D:F3:A2:0E
              inet addr:46.149.120.6  Bcast:46.149.120.7      Mask:255.255.255.252
              inet6 addr: fe80::2e0:7dff:fef3:a20e/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:307 errors:0 dropped:0 overruns:0 frame:0
              TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:49868 (48.6 KiB)  TX bytes:32191 (31.4 KiB)
```

Z výpisu vidíme celé rozhraní, a to postupně: Typ rozhraní, MAC adresa, IP adresa, broadcastová adresa, maska atd.

Příkaz `ifconfig` neslouží jen k zobrazení, ale i k nastavení vlastností adaptéru. Na adaptéru eth0 zadáváme veřejnou IP adresu tak, abychom mohli server připojit do internetu. Adaptér eth1 zařadíme do neveřejné sítě.

2.4 Routovací tabulka

Často nazývaná směrovací tabulkou. Umožňuje nám směrování mezi sítěmi. Jeden počítač je povýšen na tzv. bránu (Gateway). Jedná se nejčastěji o počítač nebo router, který má jedno rozhraní v naší síti a druhé mimo ni. Pak pomocí routovací tabulky směruje pakety správným směrem, co nejefektivnější cestou. Směrování zajišťuje síťová vrstva modelu ISO/OSI. Směrování je samozřejmě využíváno i ve vnitřních sítích. Záznamy v routovací tabulce mohou být statické (nemění se, jsou nastaveny pořád stejně, dokud někdo záznamy neupraví) nebo dynamické (reagují na změnu v síti) [2]. Routovací tabulka zpracovává IP datagramy, kde cílová adresa je porovnávána s hodnotami ve směrovací tabulce. Pokud je nalezena shoda, je datagram předán. V obráceném případě je paket předán nastavené bráně (Default Gateway). Nachází se většinou na posledním řádku a slouží ke směrování datagramů, pro které není uveden v tabulce záznam. Routovací tabulku vypíšeme pomocí příkazu `route`:

```
[root@gw ~]# route
Kernel IP routing table
Destination  Gateway Genmask     Flags   Metric Ref Use Iface
46.149.120.4    *  255.255.255.252 U      0      0   0    eth0
```

V linuxu jsou řádky seřazeny vždy podle délky síťové masky (na začátku je nejdelší síťová maska).

- **Destination (cíl)** – cílová podsíť, hodnotu default má implicitní brána. Slouží k porovnání s cílovou IP adresou z diagramu.
- **Genmask** – síťová maska

Vpravo je uvedeno síťové rozhraní. Příkaz pro přidání defaultní brány:

```
route add default gw 46.149.120.5 eth0
```

3 SLUŽBY

Ve stati jsou teoreticky rozebrány jednotlivé služby, které jsou v návrhu použity. Jde o služby pro automatické přidělování IP adres (DHCP), filtrování paketů (iptables), sdílení souborů (Samba), bezpečný přístup do sítě (VPN), překladu jmen na IP adresu a opačně (DNS). Nachází se zde poštovní služby, metody a možnosti zálohování dat.

3.1 DHCP

DHCP server slouží pro automatickou konfiguraci počítačů připojených do počítačové sítě. Dynamic Host Configuration Protocol je název síťového protokolu spadající do transportní vrstvy UDP na portu 67 a 68 [4]. Pracuje jak na koncových stanicích s Linuxem, tak i s Windows. V konfiguraci sítě v systému Windows je k tomuto účelu připravena volba získat adresu z DHCP serveru. Používá se především tam, kde je více počítačů, a v přidělených adresách by vznikaly nejasnosti. DHCP se dělí:

- server
- klienta

Pomocí protokolu DHCP se přiděluje:

- IP adresu
- maska sítě
- defaultní brána
- DNS server

Platnost přidělených dat je časově omezená a nastavuje se v konfiguraci DHCP serveru. Z toho důvodu na klientovi běží DHCP klient, který si vyžaduje nová data. DHCP je následníkem protokolu BOOTP, se kterým je zpětně kompatibilní. Přidělení IP adresy se provádí:

Ručně:

- **Ruční nastavení** - Administrátor nastaví pevně konfiguraci jednotlivých stanic. Nevyužívá se služeb DHCP. Využívá se především na serverech, kde by změna ohrozila chod služeb

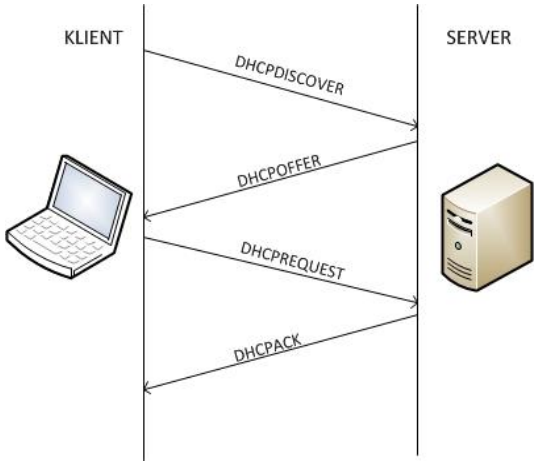
Pomocí DHCP:

- **Statická alokace** – DHCP server má v konfiguraci nastavené MAC adresy a k nim příslušné IP adresy. Pokud si zažádá o IP adresu stanice s uvedenou MAC adresou, dostane vždy definovanou IP adresu.
- **Dynamická alokace** – V konfiguraci DHCP serveru vymezí správce sítě pevně definovaný rozsah stanicím, které nejsou v konfiguraci DHCP serveru. Přidělují IP adresu jen na určitý časový úsek. To dovoluje DHCP serveru již nepoužívané IP adresy přiřadit jiným stanicím, serverům atd.

Komunikace mezi serverem a klientem probíhá pomocí DHCP zpráv, které si mezi sebou zasílají. Komunikace může mít 8 typů zpráv. Pět zpráv zasílá klient serveru (DHCPDISCOVER, DHCPREQUEST, DHCPRELEASE, DHCPDECLINE, DHCPINFORM) a tři zprávy posílá server klientovi (DHCPOFFER, DHCPACK, DHCPNAK). Celá komunikace se skládá ze čtyř kroků. Celkově se tedy vyšlou 4 zprávy - logicky vyšle 2 zprávy klient a 2 zprávy server [3].

1. Klient vyšle broadcastem (zprávu přijmou všechna připojená zařízení v síti) DHCPDICOVER. Zpráva může oslovit několik DHCP serverů.
2. Jakmile server přijme zprávu od klienta, pošle tzv. nabídku – paket DHCPOFFER. Obsahuje klientovu MAC adresu, nabízenou IP adresu, masku a časový interval, po který bude IP adresa platná.
3. Když klient přijme nabídku od serveru, potvrdí mu ji pomocí paketu DHCPREQUEST.
4. Následuje potvrzení serveru všech parametrů pomocí zprávy DHCPACK, obsahující konfigurační parametry.

Zbývající zprávy jsou spíše podpůrné, slouží např. pro zaslání zprávy, když server indikuje špatnou IP adresu apod.



Obr. 4. Komunikace mezi serverem a klientem

3.2 IPTABLES

Firewall je typ služby operačního systému, který slouží k oddělení dvou síťových rozhraní. Chrání tak počítačovou síť před nezvanými hosty. Iptables dovoluje postavení několika typů firewallů (transparentní, stavový …). Funkce iptables zajišťuje část linuxového jádra. Umožňuje řídit veškerou síťovou komunikaci. Lze realizovat jakoukoliv činnost s pakety.

Existuje celá řada nástrojů k zjednodušení práce s iptables. Například jednoduché konfigurátory, přednastavené speciální distribuce atd. Iptables udávají, jaký síťový provoz může být propouštěn a jaký blokován, případně odmítnut [5].

Iptables jsou součástí zdrojového balíku Netfilter. V linuxu se používá od jádra verze 2.4. Netfilter obecně udává, co se s paketem může stát. Může být akceptován (ACCEPT), zahozen (DROP), odmítnut (REJECT) nebo předán jinému řetězu [6]. Obecný princip, jak iptables pracují:

1. paket se zařadí do příslušného řetězce (chain)
2. paket postupně prochází pravidla od prvního po poslední
3. pokud vyhoví pravidlu, provede se akce pravidla
4. pokud nevyhoví ani jednomu pravidlu, provede se implicitní akce pro daný řetězec

3.2.1 Syntaxe iptables

Syntaxe zápisu vypadá následně:

iptables [tabulka] [akce] [chain] [ip_část] [match] [target] [target_info]

Iptables se skládají ze tří tabulek (poznají se podle parametru – t), které se skládají z řetězců:

- filter

- INPUT
- OUTPUT
- FORWARD

- nat

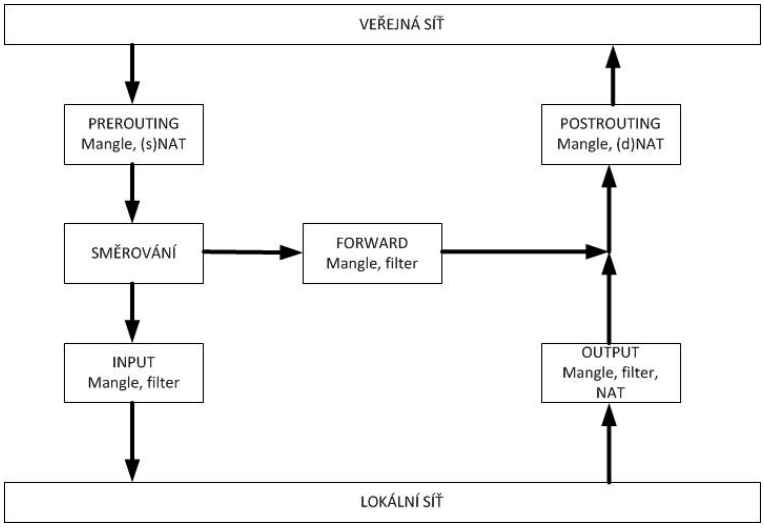
- PREROUTING
  - DNAT
- POSTROUTING
  - SNAT
- OUTPUT

- mangle

- INPUT
- OUTPUT
- FORWARD
- PREROUTING
- POSTROUTING

Tabulku si můžeme představit jako tři knihy, které mají své kapitoly – řetězce [3].

- **Filter** – jedná se o výchozí tabulku. To znamená, pokud se nepoužije žádná tabulka, užívá se výchozí. Řetězec INPUT je platný, pokud paket putuje dovnitř sítě, OUTPUT je pro odchozí pakety. FORWARD pro pakety, které se posílají mezi sítěmi. Pakety procházející přes FORWARD, neprochází pravidly INPUT ani OUTPUT.



Obr. 5. Procházení paketů firewallem

- **Nat** – tabulka má opět jen tři řetězce, viz výše. Slouží k překladu adres, tzv. maškarádu. PREROUTING je řetězec, který se aplikuje na příchozí pakety a jím modifikuje cílovou adresu tzv. Destination NAT (DNAT). Pomáhá forwardovat porty do místní vnitřní sítě. Opakem je POSTROUTING. Pomocí tohohle řetězce modifikujeme odchozí spokojení Source NAT (SNAT). SNAT se využívá nejčastěji, slouží k schování lokální sítě za jednu veřejnou adresu. OUTPUT je řetězec pravidel uplatňujících se před modifikací odchozích paketů [6].
- **Mangle** – je tabulka, která obsahuje všech pět řetězců a modifikuje hlavičky paketů. Modifikace TTL, značkování atd.

Akce:

Parametr udává, co se právě děje s pravidly. Existuje jich mnoho. Nejdůležitější a nejčastěji používané jsou:

-A, --append - přidání nového pravidla na konec řetězce.

-I, --insert – vytvořené nové pravidlo se přidá na začátek řetězce.

-D, --delete – smaže pravidlo. Pravidlo je definováno buď jeho původním zadáním nebo jeho číslem.

-F, --flush – vyprázdní daný řetězec. Všechna pravidla v řetězci budou smazána.

-L, --list – výpis všech pravidel v zadaném řetězci. Pokud nebyl řetězec definován, vypíšou se všechny.

-P, --policy – zadání hlavního pravidla, tzv. policy

Pomocí iptables lze vytvářet vlastní řetězce:

-N, --new-chain – založení nového řetězce

-X, --delete-chain – smazaní řetězce – nelze však smazat výchozí řetězce (INPUT, OUTPUT atd.)

-E, --rename-chain – přejmenování řetězce

Další parametry:

-s, --source – zdrojová IP adresa paketu

-d, --destination – cílová IP adresa paketu

-i, --in-interface – vstupní zařízení, kterým paket připutoval do počítače, např. eth1

-o, --out-interface – výstupní zařízení, kudy má paket odejít

--sport, --source-port – zdrojový port paketu, ze kterého paket přichází

--dport, --destination-port – cílový port, na který paket putuje

Posledním a prakticky nejpoužívanějším pravidlem je jump (-j). Obsahuje jej skoro každé pravidlo. Stanovuje cíl, jak s paketem naložit. Jedná se o tři hlavní pravidla:

ACCEPT – akceptuje pravidlo, pustí paket dále

DROP – neakceptuje paket, zdrojový počítač nebude informován o zahození paketu

DENY – neakceptuje paket, zdrojový počítač bude informován o zahození paketu

Ve většině distribucí jsou výchozí politiky (policy) nastaveny na ACCEPT. Tím, je povolená veškerá komunikace. Doporučené je pravidlo, co není povoleno, je zakázáno, např. zahození všech příchozích paketů [3]:

```
iptables –P INPUT DROP
```

3.3 Samba

Samba je open-source balík aplikací, které implementují protokol SMB (Server Message Block). Samba slouží především pro sdílení souborů v systému Microsoft Windows. Balík

se může používat na Linuxu, FreeBSD, Solaris a na dalších unixových systémech. Samba umožňuje [7]:

- sdílení souborů
- sdílení tiskáren
- autentizační služby
- automatické procházení stromu služeb

V současné verzi 3 poskytuje Samba integraci do domény Windows, např. jako primární doménový řadič. Samba je v CentOsu součástí instalace systému. Jen démoni Samby jsou zastaveni. Jedná se o démony:

- **smbd** – je démon, který zajišťuje autentizaci uživatelů, sdílení souborů a tiskáren
- **nmbd** – je druhý démon, který poskytuje překlad jmen (NetBIOS na IP adresu) a především zobrazení stromu služeb poskytovaných počítači v celé síti.

Balík obsahuje několik dalších užitečných utilit [7]:

smbclient – konzolový klient pro přístup ke sdíleným zdrojům

smbget – program pro stahování souborů ze serverů Samba

smbmount – program pro připojení sdílených svazků

smbumount – program pro odpojení svazků

smbpasswd – program sloužící ke správě hesel uživatelů Samby

smbstatus – zobrazuje stav serveru Samba

testparam – kontrola konfiguračních souborů Samby

3.4 Virtuální privátní síť

Anglicky virtual private network (VPN). Většina služeb, které síť nabízí, by neměla být dostupná z internetu. Snahou administrátorů je výstupy ze sítě minimalizovat (nezbytně nutné). Administrátor se snaží upravit služby tak, aby byly přístupné pokud možno jen z vnitřní sítě. VPN umožňuje zabezpečený přístup odkudkoliv ze světa, pokud má uživatel připojení k internetu. Zajišťuje tak uživateli přístup k datům a poště. VPN umožňuje propojit počítače rozeseté po celém světě do jedné virtuální sítě. K propojení jsou potřeba

dvě části, server a klient. Server musí mít veřejnou IP adresu, naslouchá a čeká na příchozí spojení klientů. Jeden server je schopen obsloužit větší množství klientů, záleží na jeho konfiguraci. Komunikaci lze popsat v pěti krocích [3]:

1. klient se připojí k určenému serveru
2. obě strany vytvoří šifrovaný kanál pro komunikaci
3. proběhne autentizace klienta
4. klient dostane IP adresu a stává se součástí sítě

Vzhledem k tomu, že počítač je součástí počítačové sítě, je potřeba dbát určité bezpečnosti. Implementací VPN existuje mnoho, komerčních, i nekomerčních. Byl vybrán produkt OpenVPN který je šířen pod licencí GNU/GPL (a je volně šiřitelný). Mezi jeho hlavní výhody patří [8]:

- silné šifrování (standardně blowfish, ale může použít libovolnou šifru podporovanou OpenSSL)
- jednoduchá konfigurace
- je multiplatformní (běží na systémech s Windows, OpenBSD, FreeBSD atd.)
- funguje i na horších linkách – 256 kb/s
- veškerá komunikace probíhá na jediném portu

OpenVPN pracuje na protokolu UDP nebo TCP. Slouží pro vytvoření jednoduchého tunelu mezi dvěma počítači (1:1) nebo k vytvoření virtuální sítě (1:N). Při autorizaci lze využít sdílený klíč (shared), i velmi bezpečné dynamické klíče. Tvorba sítě typu klient-server. Vznikne virtuální síť, v níž jeden server bude přijímat požadavky od několika klientů. Prověření klientů bude realizováno na úrovni certifikátů. K tomu abychom, mohli realizovat virtuální sít, potřebujeme server s veřejnou IP adresou a otevřeným portem UDP.

Virtuální LAN je realizována pomocí síťových adaptérů, označovaných jako TAP a TUN.

- **TAP** – vytvoří síťové zařízení pracující na druhé vrstvě modelu ISO/OSI (linková). Slouží k vytváření mostů.
- **TUN** – vytvoří síťové zařízení pracující na třetí vrstvě modelu ISO/OSI (síťová). Používá se k routování.

Důležitou fází při vytváření šifrovaného spojení mezi dvěma body je autentizace. Jsou možné dvě autentizace [9]:

- **Sdílený klíč (pre-shared key)** – velmi jednoduché generování. Obě strany (server, klient) mají stejný klíč. Klíč se skládá ze čtyř nezávislých klíčů (HMAC, send/recieve, šifrovací a dešifrovací klíč). Klíč musí být na obou stranách před vytvořením VPN tunelu. Nutno dbát na bezpečný přenos vygenerovaného klíče ke klientovi.
- **SSL/TLS** – využití asymetrické kryptografie. Využívá SSL/TLS a certifikátů pro autentizaci a výměnu klíčů. Metoda založena na ustanovení klíče pomocí Diffie-Hellmann protokolu. Pro konfiguraci OpenVPN je využito PKI (Public Key Infrastructure), který vychází z asymetrické kryptografie. Skládá se ze dvou částí:
  - veřejné klíče a soukromé klíče. Zvlášť pro každého klienta a server.
  - certifikační autority (CA), které podepisují jednotlivé certifikáty (klienta i serveru)

Princip autentizace je následující. OpenVPN využívá obousměrnou autentizaci. To znamená, že server musí autentizovat klientský certifikát a naopak klient musí autentizovat certifikát serveru. Důležitou součástí ověření je především zjištění, že zadaný certifikát byl podepsán certifikační autoritou (CA). Server akceptuje jen certifikáty, které byly podepsány certifikační autoritou. Certifikáty lze zneplatnit (revokovat). Vytvoření vlastní PKI lze provést [9]:

- ručně – pomocí OpenSSL.
- s využitím předefinovaných skriptů (easy-rsa), které jsou součástí OpenVPN

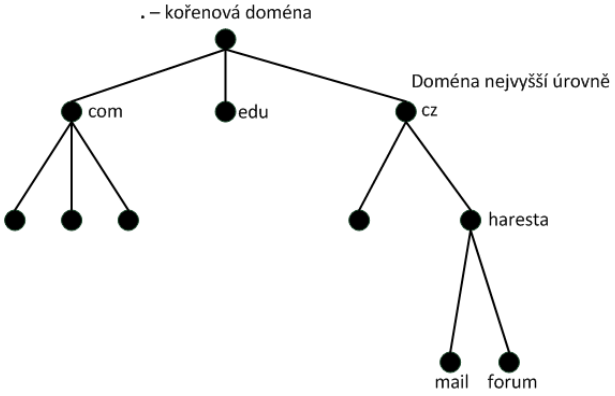
3.5 DNS

Je zkratka z anglického Domain Name System a označuje hierarchickou databázi doménových jmen. DNS převádí jména počítačů na IP adresy, které jsou přiřazeny počítačům v síti. Jeho základní funkcí jsou překlady doménových jmen na adresu a opačně. Například jméno počítače gw.haresta.cz je mapováno na IP adresu počítače 46.149.120.6 a opačně. Opačnému způsobu mapování se říká obrácené (reverzní) mapování [3]. Reverzní dotazy mají obrácené pořadí bajtů v adrese. K obrácené adrese pak přidá doménu

in-addr.arpa a výsledné doménové jméno pak vyhledává standardním způsobem. Tedy například při dotazu na jméno IP adresy 46.149.120.6 to bude 6.120.149.46.in-addr.arpa.

Důvodem vzniku DNS je, že se hůře uživatelům pamatují adresy ve tvaru 46.149.120.6. Proto vznikly adresy v tzv. doménovém tvaru. Adresa v doménovém tvaru se zapisuje jako několik slov oddělených tečkami. Tato struktura je hierarchicky členěna. Úplně na vrcholu stromu je tzv. kořenová doména, která se zapisuje jako samostatná tečka. Pod ní se hierarchicky nacházejí domény nejvyšší úrovně (Top-Level Domain, TLD), jako jsou například cz – pro Česko nebo edu - pro vzdělávání. Dále se nachází nižší domény. Vpravo se tedy nacházejí domény obecnější a směrem doleva se konkretizuje [3].

- nejvíce vpravo se nachází doména nejvyšší úrovně např. haresta.cz má TLD cz.
- jednotlivé sub-domény mohou mít až 63 znaků a mohou dosahovat celkové délky doménového jména až 255 znaků. Doména může mít až 127 znaků.



Obr. 6. Hierarchie DNS

Strom lze rozdělit do zón, které spravují jednotliví správci. Právě distribuovaná správa DNS tvoří klíčové vlastnosti. DNS servery se dělí [3]:

- **Primární server** – je autoritativním nositelem informace, zde se upravují záznamy DNS. Jakmile zde proběhnou nějaké změny v nastavení, sekundární servery si informace synchronizují. Informace na primárním a sekundárním serveru mají být stejné. Každá doména má právě jeden primární DNS server.
- **Sekundární server** – sekundární server si v pravidelných intervalech synchronizuje informace z primárního serveru. Slouží jako záloha primárního serveru v případě jeho výpadku. Dále pomáhá při rozkládání zátěže u frekventovaných domén.

- **Cachovací server** – slouží jako pomocný server, vyrovnávací paměť pro snížení zátěže a především pro zrychlení odezvy. Výsledky a mezivýsledky dotazů si uchovává ve své vyrovnávací paměti, dokud jim nevyprší platnost.

Autoritativní odpověď je odpověď přímo z primárního nebo sekundárního serveru – jedná se o ověřenou správnou informaci. Odpověď poskytnutá z vyrovnávací paměti není brána za autoritativní. Existují následující typy zón [3]:

- **master** – hlavní kopie zóny spravovaná primárním serverem
- **slave** – záložní kopie spravovaná sekundárním serverem
- **forward** – přesměrování
- **hint** – seznam všech kořenových serverů

3.5.1 Root servery

Kořenové jmenné servery (root name servers) představují zásadní část infrastruktury internetu. Závisí na nich funkčnost celého internetu. Tyto servery poskytují kořenový zónový soubor (root zone file) ostatním DNS serverům. Jedná se o distribuovanou databázi, která slouží k překladu unikátních doménových jmen na ostatní identifikátory. Kořenový soubor se často nemění. Soubor je vytvářen a měněn organizací IANA. Existuje 13 kořenových jmenných serverů nacházející se ve 34 zemích světa. Na více než 80 místech [4].

3.5.2 Řešení dotazů

Každý ový počítač má ve své konfiguraci obsaženou mimo jiné adresu lokálního DNS serveru, na nějž se počítač obrací s dotazy. V operačních systémech Unix/Linux najdeme konfiguraci v souboru /etc/resolv.conf v MS Windows ji nalezneme ve vlastnostech protokolu TCP/IP. Řešení dotazů probíhá takto [3]:

1. uživatel vloží do prohlížeče nějakou adresu
2. DNS klient se nejprve podívá do souboru /etc/hosts
3. v případě, že nenalezne patřičnou adresu, zašle dotaz lokálnímu DNS serveru (nejčastěji dle konfigurace /etc/resolv.conf)

4. lokální nameserver se nejdříve podívá do cache, pokud odpověď nenalezne, podívá se na nejpravější části adresy a pošle dotaz na root server
5. root server mu vrátí adresu autoritativního DNS serveru dané TLD (top level domain)
6. lokální name server pak na tento DNS server pošle dotaz na následující část jména (tj. doménu druhého řádu)
7. dotázaný DNS server TLD vrátí adresu autoritativního serveru dané domény
8. lokální name server zašle na daný server dotaz z následující subdoménou
9. dotázaný server vrátí buď adresu autoritativního serveru dané subdomény nebo konkrétního stroje
10. body 8 a 9 se iterativně opakují, dokud není zpracován celý doménový název a vrácena ip adresa požadovaného serveru

3.5.3 Typy DNS záznamů

- **A** – (adress record) – obsahuje IPv4 adresu přiřazenou danému jménu. Např. jménu gw.haresta.cz jemuž přísluší IP adresa 46.149.120.6.

```
gw    IN    A     46.149.120.6
```

- **AAAA** – (IPv6 adress record) obsahuje IPv6 adresu přiřazenou danému jménu. Např. gw.haresta.cz jemuž přísluší adresa 2001:718:1c01:1:02e0:7dff:fe96:daa8:

```
gw    IN    A     2001:718:1c01:1:02e0:7dff:fe96:daa8:
```

- **CNAME** – (canoncial name record) – je alias (jiné jméno pro jméno již zavedené), přiřazený již zavedenému záznamu. Např. alias ftp pro gw.haresta.cz:

```
ftp   IN    CNAME      gw
```

- **MX** – (mail exchange record) – má dva parametry. Priorita (přirozené číslo, čím nižší, tím vyšší priorita) a adresa pro příjem elektronické pošty na dané doméně. Např. MX záznam pro situaci, když poštu pro adresu gw.haresta.cz přijímá server mail.haresta.cz a v případě výpadku primárního serveru se bude pošta přesměrovávat na server zalozni.server.cz [4]:

```
gw    IN    MX    10 mail
```

```
        IN    MX    20 zalozni.server.cz.
```

- **NS** – (name server record) – oznamuje jméno autoritativního serveru pro danou doménu. Např. doména haresta.cz má mít poddoménu obchod.haresta.cz, jejíž autoritativní servery budou ns.haresta.cz (primární) a ns.jinde.cz (sekundární):

```
obchod    IN    NS    ns
          IN    NS    ns.jinde.cz.
```

- **PTR** – (pointer record) – je speciální typ záznamu alias (reverzní DNS záznam). Obsahuje na pravé straně jméno počítače, přidělené adrese na levé straně. Výše uvedený příklad pro záznam typu A by v souladu s ním (zónový soubor pro doménu 120.149.46.in-addr.arpa) měl obsahovat:

```
6       IN      PTR     gw.haresta.cz.
```

- **SOA** – (start of autority record) – jedná se o záznam zahajující zónový soubor. Obsahuje jméno primárního serveru, adresu elektronické pošty jejího správce (zavináč je v ní nahrazen tečkou) a další údaje [4]:

  Serial – sériové číslo, které je nutné zvýšit při každé změně záznamu. Podle něj sekundární server pozná, že došlo ke změně. Pro přehlednost se nejčastěji používá formát YYYYMMDDHH.

  Refresh – jak často má sekundární server kontrolovat verzi zóny.

  Retry - v jakých intervalech má sekundární server opakovat své pokusy, pokud se mu nedaří spojit s primárním serverem.

  Expire – čas, po kterém má sekundární server označit své záznamy jako neaktuální, v případě že se mu nedaří kontaktovat primární server.

  TTL – implicitní doba záznamu

3.6 Poštovní server - Postfix

Historie elektronické pošty (e-mailu) se začíná psát už v roce 1970. Jedná se o jednu z nejstarších služeb. K posílání prvních zpráv docházelo přes síť Arpanet. Mít ve firmě vlastní poštovní server má mnoho výhod (kontrola nad tím co přichází/odchází,

konfigurace serveru dle libosti, přímý přístup k poště atd.). Elektronická pošta má tyto zkratky:

- **MUA** – (mail user agent) jedná se o uživatelského správce pošty, který odeslanou poštu předá poštovnímu serveru, na kterém běží přenosový agent (Mail Transfer Agent – MTA). Mezi e-mailové klienty patří například Thunderbird, Outlook, The Bat! atd. Jsou instalovány na straně uživatele [10].
- **MTA** – (mail transport agent) jako je například Sendmail nebo Postfix. Starají se o přesun zprávy z jednoho systému na druhý. Při obdržení požadavku na příjem pošty stanoví agent MTA, zda má zprávu přijmout či nikoliv. Jakmile MTA zprávu přijme, musí se rozhodnout, co s ní udělá. Může ji odeslat nějakému svému uživateli, nebo ji předat jinému agentovi MTA. Nedokáže-li MTA zprávu doručit, odešle ji zpět uživateli. Jakmile zprávu obdrží koncový MTA a je-li zpráva určena uživateli systému, daný MTA zprávu předá MDA [10] [11].
- **MDA** – (message delivery agent) jedná se o program, který zpracuje a uloží poštu. MDA zprávu může uložit jako prostý soubor, uložit do databáze atd. Před uložením zprávy lze provést například antivirovou kontrolu. Patří mezi ně například Procmail nebo Maildrop [10] [11].

SMTP

Simple Mail Transfer Protocol. Jde o velmi jednoduchý protokol, sloužící k odeslání zpráv a jejich předávání mezi agenty MTA. Zjednodušeně řečeno slouží k přenosu zpráv z jednoho počítače na druhý. Jeho syntaxe je velmi prostá, k přenosu využívá čistý text. Klientský software (MUA) zná adresu SMTP serveru (MTA), kterou použije k odeslání. Připojí se k němu na port 25 a e-mail mu předá. Transakce se skládá z posloupnosti SMTP příkazů identifikující odesílatele a příjemce, a také i z těla samotného mailu. Na každý příkaz mu server odpoví OK nebo chybou [10].

Některé příkazy:

- EHLO – extended HeLO, identifikace klienta serveru
- MAIL – zahájení přenosu zprávy
- RECIPIENT – specifikace příjemce

- DATA – přenos obsahu zprávy. Ukončeno řádkem s tečkou („.“)
- RESET – zrušení aktuální transakce
- VERIFY – ověření existence e-mailové adresy
- HELP - vypíše užitečné informace
- QUIT - uzavře spojení

Příklad komunikace:

S : Server, C: Client

```
telnet mail.example.cz 25
S: 220mail.example.cz ESMTP Postfix
C: HELO example.cz
S: 250 Hello example.cz
C: MAIL FROM: <petr@example.cz>
S: 250 OK
C: RCPT TO: <pavel@seznam.cz>
S: 250 OK
C: DATA
S: 354 End data with .
C: Subject: Zprava
C: From: petr@example.cz
C: To: pavel@seznam.cz
C:
C: Ahoj, posilam tesovaci zpravu.
C: .
S: 250 Ok: queued as 12374
C: QUIT
S: 221 Bay
```

Všechny zprávy ze strany serveru jsou označeny kódem zprávy. Kódy jsou umístěny na začátku řádku, protože zjednodušují klientům identifikaci jednotlivých informací. Na začátku komunikace je identifikace obou stran. Dále klient oznámí serveru, že bude posílat zprávu od Petra pro Pavla. Následuje datová část, kdy server informuje klienta, že data musí být ukončena tečkou na prázdném řádku. Klient pak pošle tělo zprávy, zakončí jej tečkou. Server přijetí zprávy potvrdí a dojde k rozloučení a ukončení komunikace [11].

Pokud-li zpráva náleží pro danou doménu, kterou server obsluhuje, je zpráva předána MDA a uložena do schránky příslušného uživatele. Mnohem častěji se stává, že zpráva musí být doručena do jiné sítě úplně cizímu uživateli. V takovém případě se poštovní server dotáže DNS systému na tzv. MX záznam, který uvádí cizí server, který se o poštu stará. Server se pak k cizímu serveru připojí a použije výše zmínění protokol SMTP k předání zprávy [10].

Vyzvednutí pošty je pak možné přímo na serveru pomocí telnetu nebo SSH. V dnešní době málo využívaná možnost. Častěji využívá možnost přímo přes webové rozhraní (SquirrelMail, Horde) nebo přes klientský software na počítači uživatele.

Zpřístupnění pošty je možné obvykle pomocí dvou různých protokolů:

- POP3 (běžící na portu 110 nebo 995)
- IMAP4 (běžící na portu 143 nebo 993)

Protokoly umějí stahovat poštu ze serveru k uživateli, ale přitom je mezi nimi rozdíl.

- **POP3** (Post Office Protocol) – stahuje veškerou novou poštu, která je pak přístupná i pokud je uživatel offline. Zprávy nezůstavájí na serveru [10].
- **IMAP4** (Internet Message Access Protocol) – umožňuje práci s poštou přímo na serveru. Veškerá práce s poštou jako je přesouvání, třídění do složek a mazání je prováděna přímo na serveru. Pošta je stahována do počítače až na vyžádání uživatele. Je proto možné pracovat stále se stejným obsahem z různých stanic klientů. Při zobrazení složky se stáhne jen záhlaví zpráv. Obsah složky se stáhne jen v případě, že chce uživatel zprávu přečíst. Protokol umožňuje připojení více klientům současně [10].

Obě varianty je možné používat i v šifrované podobě (porty 993 a 995), kdy je použit bezpečný protokol SSL (Secure Sockets Layer). Komunikace je zabezpečena šifrováním, autentizací, čímž se zabrání sledování přenášených dat.

3.6.1 Postfix

Existuje celá řada kompletních poštovních serverů s různými možnostmi a modularitou. Známé jsou malé odlehčené poštovní servery nebo například standardní Sendmail. Zde je použit program Postfix z důvodu snadné konfigurace a modularitě.

Postfix je Mail Transfer Agent, tedy program zajišťující předávání e-mailových zpráv mezi servery. Nezajišťuje komunikaci POP3 ani IMAP. Jedná se o MTA, který pouze odesílá a přijímá zprávy elektronické pošty a to pomocí protokolu SMTP. Postfix napsal Wietse Venema v roce 1998 jako open-source software. Firma IBM Research sponzorovala původní uvedení a podporuje i jeho neustálý vývoj. Postfix nabízí mnoho podstatných výhod [10]:

- Bezpečnost – zavádí proti útočníkovi několik obranných vrstev. Funguje systém nejnižších oprávnění, každý proces běží izolovaně s nejnižší sadou oprávnění.
- Spolehlivost – efektivně pracuje při vysokém zatížení.
- Flexibilita – systém je složen z několika programů a systémů. Tím se stává pružným, flexibilním.
- Jednoduchá konfigurace.

3.6.2 SpamAssassin

S e-mailovou komunikací je úzce spojena problematika spamu. Jedná se o nevyžádané sdělení, nejčastěji reklamní, masivně se šířící internetem. Pro vyžádanou zprávu se používá termín ham.

SpamaAssassin je počítačový program, určený k filtrování spamu na základě analýzy obsahu zprávy. Využívá k tomu různé techniky detekce spamu na základě [12]:

- online databází
- blacklistů (seznamy IP adres, ze kterých bylo zaznamenáno rozesílání spamů)
- greylistingu (princip dočasného odmítnutí zprávy)
- Bayesovského filtru (na základě učení) atd.

SpamAssassin je možné integrovat do poštovního serveru tak, aby automaticky filtroval veškerou poštu. SpamAssassin je aplikace napsaná v Perlu a jeho velkou výhodou je široká konfigurovatelnost. Má v sobě několik pravidel, pomocí kterých určuje, zdali se jedná o spam nebo ne. Pravidla nejčastěji fungují na principu vyhodnocení regulárních výrazů, které kontrolují obsah těla, hlavičky atd. Každý z prováděných testů má bodové hodnocení, které se na konci sečte. Získané skóre může být pod definovanou hranicí (negativní), indikuje ham. Nad definovanou hranicí (pozitivní) indikují spam. E-mail považovaný za spam většinou splňuje více kriterií. Shoda s jedním testem obvykle není dostatečná, aby byl práh dosažen. Program umožňuje individuální nastavení pro jednotlivé uživatele. Lze měnit například skóre pro určitá pravidla, adresy, ze kterých nikdy nebudou považovány zprávy za spam atd.

3.7 Zálohování

Záloha je kopie dat uložená na jiném datovém nosiči (DVD, externí disk atd.). Data v dnešní době mají velkou hodnotu a jejich ztráta může způsobit velké finanční, časové a majetkové obtíže. Důvodem zálohování je tedy snaha ochránit data před jejich ztrátou. Příčiny ztráty mohou být různé:

- vnější hrozby (napadení počítače útočníkem)
- lidská chyba nebo úmysl
- selhání hardwaru
- přírodní katastrofy (požár, povodeň)
- poškození operačního systému
- a další …

Mezi vnější hrozby bezpochyby patří napadení počítače útočníkem. Lidská chyba se řadí mezi nejčastější příčinu ztráty dat, způsobených nechtěným smazáním nebo přepsáním [13].

Následuje příčina selhání hardwaru. Existují společnosti zabývající se obnovou dat z poškozených disků. Služba je drahá (řádově desítky tisíc korun) a ne vždy se podaří obnovit vše potřebné.

Přírodní katastrofy hrají značnou roli u velkých podniků, kdy data mají nevyčíslitelnou hodnotu. Zálohy a záložní servery se nachází mimo objekt firmy, v jiných městech nebo i na jiném kontinentu.

Poškození operačního systému, zde se doporučuje oddělovat data od systému. Důvodem je, že při poškození systému není potřeba při reinstalaci systému data zálohovat. K smazání dat dochází, když uživatel místo opravy systému zvolí novou instalaci.

Zálohují se data, která jsou pro uživatele nebo společnost cenná. Zálohu lze provádět pravidelně i nepravidelně. Nepravidelná záloha se provádí hlavně v domácnostech. Uživatel si připojí externí disk nebo vypálí zálohu na DVD. Pravidelná záloha probíhá především ve firmách, kdy dochází k automatickým zálohám podle sestavěného plánu. Zálohy můžeme rozdělit na:

- online
- offline

Online zálohování se provádí za běhu počítače. Offline zálohování se provádí mimo provoz počítače. Offline záloha se nejčastěji provádí pomocí bootovacích medií, které umí vytvořit např. image disku. Zálohy se dělí dle typu [13]:

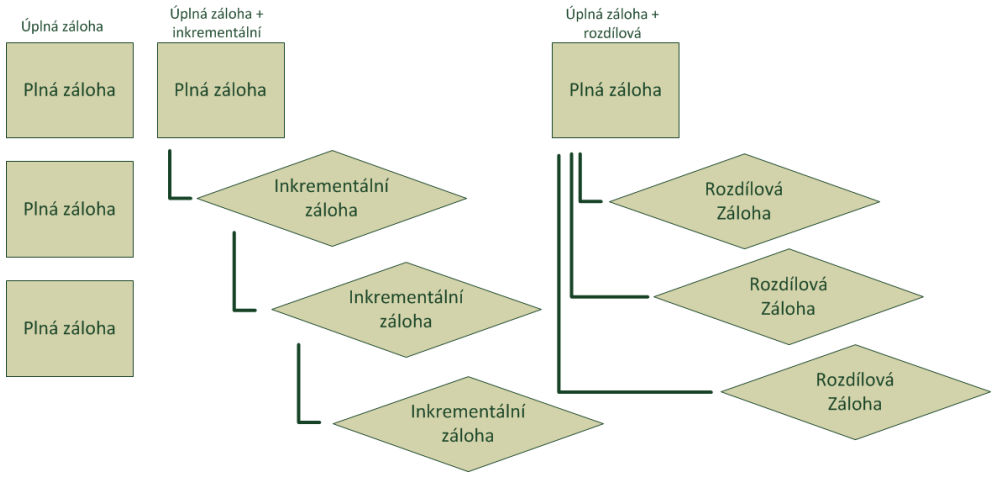
- úplná
- inkrementální
- rozdílová
- úplná záloha systému

Úplná záloha je záloha všech dat. Nevýhodou zálohy oproti inkrementální je časová zátěž a náročnost místa na ukládacím mediu. Výhodou je, že stačí uchovat poslední zálohu, protože pokrývá veškeré předchozí [14].

Inkrementální záloha se využívá při objemných zálohách. Provede se úplná záloha dat. S následnou inkrementální zálohou. To znamená, že se ukládají jen soubory, které se změnily od předešlé úplné nebo inkrementální zálohy. Výhodou je nižší časová zátěž a menší náročnost na místo na ukládacím mediu. Nevýhodou je nutnost pracovat s úplnou zálohou a následnými inkrementálními zálohami až k požadovanému okamžiku zálohy [13].

Rozdílová záloha má opět využití při vytváření více objemných záloh. Rozdíl oproti předchozí je, že se zálohují změny vždy oproti úplné záloze, i když jsou některé změny za-zálohovány v předchozí rozdílové záloze. Výhodou je jednoduchost obnovy dat, stačí jen 2 zálohy – úplná záloha a poslední rozdílová záloha [14].

Rozdíl mezi zálohami je patrný z obrázku 7.



Obr. 7. Rozdíl jednotlivých záloh

Úplná záloha systému je metoda, která vytváří kompletní zálohu dat, včetně operačního systému. Vytváří se tzv. obraz disku.

Mezi média pro ukládání dat patří NAS (Network Attached Storage), magnetické pásky a USB flash disky. NAS je síťové úložiště skládající se z jednoho nebo více pevných disků.

Zálohy lze zmenšit kompresí a zabezpečit šifrováním. Nevýhodou šifrování je zpomalení procesu zálohování.

3.7.1 Cron

Cron je linuxový démon, který spouští programy v předem definovanou dobu (podobné jako naplánované úlohy ve Windows). Cron je součástí každé linux/unix distribuce. Využívají ho převážně linux/unix administrátoři ke spouštění úloh operačního systému, uživatelských akcí [15].

Ke spouštění úlohy máme dvě možnosti. První skript/aplikaci se nakopíruje do adresáře `/etc/cron.daily`, `/etc/cron.hourly`, `/etc/cron.weekly` a `/etc/cron.monthly`. Z názvu je patrné, kdy se skripty budou spouštět [15].

Pokud je vyžadováno jiné, přesnější časování, používá se crontab. Edituje se pomocí příkazu: `crontab -e`

Otevře se přednastavený textový editor, v něm je seznam úloh. Záznam v crontabu se skládá z šesti parametrů oddělených mezerami nebo tabelátory [15].

1. minuta (0-59)

2. hodina (0-23)
3. den v měsíci (1-31)
4. měsíc (1-12)
5. den v týdnu (0=neděle, 1=pondělí ….)
6. cesta k programu, který má cron spustit

Každé pole může obsahovat hvězdičku znamenající, že se na danou hodnotu nebere ohled. Respektive se příkaz provádí vždy (např. hvězdička v položce minuty znamená, že se příkaz spouští každou minutu). Může obsahovat konkrétní číslo (9), seznamy oddělené čárkou (20,40) a v neposlední řadě rozsahy oddělené pomlčkou (15-20).

Např:

```
45 22 * * * /root/bin/backup
```

Příkaz spustí každý den v 22:45 skript backup.

II. PRAKTICKÁ ČÁST

4 NÁVRH SÍTĚ LAN

Tato ryze praktická kapitola se zabývá analýzou stávající počítačové sítě. Stanovuje její slabé a nedostačující stránky. Shrnuje požadavky investora. V kapitole 4.3 je návrh nové počítačové sítě.

Obsahuje konfiguraci jednotlivých služeb, vyplývající z představ investora a návrhu sítě. V neposlední řadě lze v příloze nalézt cenovou kalkulaci návrhu nové sítě.

4.1 Analýza současného stavu sítě

Firma má 83 zaměstnanců. Výpočetní techniku a síť využívá 69 uživatelů. Celkový počet stanic je 69. Z toho je 10 klasických počítačů typu tower, ostatní jsou notebooky. V síti je používáno 7 síťových tiskáren, z toho je jedna barevná.

Kabeláž

V současné době sídlí firma ve starých kancelářských prostorách. Datové rozvody nejsou optimálně řešené. Kabeláž je volně položena po kancelářích a rozdělena do hvězdy pomocí několika malých switchů, které nemají centrální správu. Strukturovaná kabeláž je realizována kategorií 5. Splňující standart 100 Base-T a maximální rychlost 100 Mb/s. Při analýze sítě LAN bylo zjištěno, že neexistuje žádná dokumentace nebo schéma sítě. Patch panel je nepopsaný, lze obtížně zjistit, kde je konkrétní zásuvka umístněna.

Klientské stanice

Konfigurace klientských stanic si jsou výkonem i softwarem velmi podobné. Z hlediska hardwaru jsou však rozdílné. To je nevhodné řešení pro administraci i opravy.

Na stanicích pracují uživatelé, kteří využívají především kancelářské aplikace, elektronickou poštu a kreslí technické výkresy. Jak se postupně rozšiřovala firma, nakupovala se technika a tím je každý počítač de facto originál. Operační systém tvoří z 65 % Windows XP Professional SP3, 10 % Windows Vista Business SP 2 a zbylých 25 % Windows 7 Professional SP1. Vzhledem k tomu, že firma nezaměstnává žádného správce IT a služby se provádí externě, je současný stav výpočetní techniky a sítě neudržitelný. Zásah ze strany správce není tak včasný, jak by si firma představovala.

Server

Servery jsou ve firmě dva. Velmi zastaralé, hardwarově nevyhovující. První je obyčejný kancelářský počítač, který má velkou kapacitu disku na ukládání dat (700 Gb). Instalován je operační systém Windows XP Professional SP3. Server slouží jako datové úložiště veškerých souborů. Druhý server má stejný systém a slouží jako rozšířené datové úložiště.

Servery jsou velmi zastaralé a nesplňují požadavky na síťové úložiště. Obsahují jen 100 Mb/s síťové karty a pevné disky s nízkými přístupovými dobami. Navíc nejsou zabezpečeny proti selhání – disky nejsou v RAIDu. Nemalým problémem je zabezpečení při sdílení souborů, kde chybí řízení přístupu.

Správa identit

V současné situaci nemá administrátor sítě kontrolu ani nad identitami. Na počítačích je každý administrátor, nejsou mu upravena práva a do některých stanic se lze přihlásit bez hesla.

Zabezpečení

Síť není chráněna centrálním firewallem. Na každé stanici je nainstalován produkt McAffe Endpoint security s centrální správou na jednom ze serverů (obsahuje moduly Anti-virus, Anti-spyware, Desktop firewall).

Služby

Poštovní server je hostován u firmy Bernátek a zároveň se firma Bernátek stará o celou počítačovou síť. S firmou je většina uživatelů nespokojená. Oprava poruch trvá dlouhou dobu.

Zálohování

Data nejsou žádným způsobem zálohována, existuje jen slabá forma zabezpečení a uživatelé nemají nastavena žádná práva.

Připojení k internetu

Připojení k internetu je od firmy O2, pomocí ADSL. Z důvodu malého uploadu je připojení zcela nevyhovující. Rychlost downloadu je 8 192 kb/s a uploadu 512 kb/s. Reálná změřená rychlost stahování byla okolo 5 000 kb/s. Agregace je 1:50.

4.2 Zhodnocení současného stavu

4.2.1 Slabé stránky

1. Kabeláž je volně položena, hrozí její poškození
2. Kabeláž je kategorie 5, maximální rychlost 100 Mb/s. Při přístupu více uživatelů k větším souborům dochází k snížení propustnosti sítě.
3. Mnoho malých switchů
4. Malý upload internetového připojení

4.2.2 Nevyhovující stránky

5. Neexistuje schéma sítě a není popsán patch panel
6. Nejsou definována uživatelská práva při sdílení souborů
7. Každý uživatel je na daném počítači administrátor
8. Data nejsou zálohovaná
9. Chybějící centrální firewall

4.2.3 Požadavky investora

10. Zajistit propustnost sítě v následujícím období, je očekáván nárůst počtu pracovních stanic
11. Zabezpečení počítačové sítě
12. Zabezpečení vzdáleného přístupu do sítě tzv. home office
13. Zabezpečení síťového úložiště (sdílení, zálohování)
14. Vlastní poštovní server

4.3 Návrh nové sítě

Prioritou firmy je zvýšit produktivitu, bezpečnost a komfort uživatelů. Cílem je inovovat hardwarově i softwarově servery i datové rozvody. Návrh obsahuje cenovou i materiálovou kalkulaci.

Kabely

Předpokládá se rozvoj firmy a současný stav je nedostačující. Navrhované řešení sítě bude obsahovat standard GigabitEthernet, jehož rychlost je 1 Gb/s (zajištěn bod č. 2 a č. 10 vyplívající z hodnocení současného stavu). Důvodem je přenos velkých souborů mezi jednotlivými kancelářemi a větší objem příloh elektronické komunikace.

Pro GigaBitový Ethernet využijeme kabel kategorie 6. Strukturovaná kabeláž tedy bude natažena kabely od firmy Schrack Technik a zakončena zásuvkami od stejné firmy (dle rozpočtu v příloze s označením PIV). Kabeláž bude vedena parapetním žlabem subdodávkou od firmy dodávající silnoproudé rozvody (vyřešen bod č. 1). Kabely budou odděleny odstíněnou přepážkou. Protože nové sídlo firmy bude rozděleno na dvě podlaží, je nutné propojení switchů optickým propojem osmi vláknovým kabelem s těsnou sekundární ochranou.

Značení kabelů

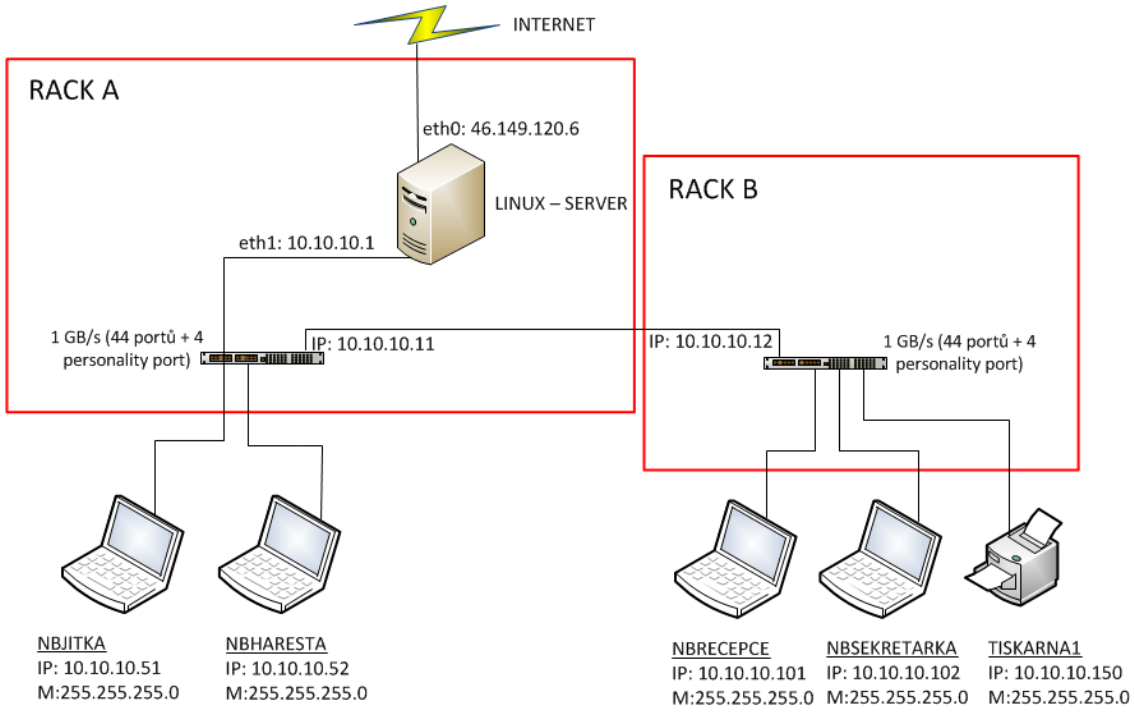
Pro označení datových zásuvek a datových kabelů bude v rozvaděči a na datových zásuvkách použit následující systém (vyřešen bod č. 5):

1.223 kde:

- 1 označení podlaží (1 nebo 2)
- 22 označení kanceláře
- 3 označení zásuvky (A až Z)

Rack

V druhém patře je stojanový rack (označení A) typ DS226080-A obsahující optickou vanu, dva modulární patch panely, čtyři vyvazovací panely, switch, server, záložní zdroj (viz příloha s označením PI). Vše podrobněji dokresluje logická mapa sítě (Obr. 8) a rozmístění datových zásuvek (příloha s označením PIII).



Obr. 8. Logická mapa sítě

V prvním patře se nachází menší nástěnný rack (označení B) typ DW186050 obsahující stejné vybavení jako rack A, jen neobsahuje server (viz příloha s ozančením PII).

Switch

Rack A i B obsahují switch od firmy HP s označením V1910-48G. Switch má 48 portů o rychlosti až 1 Gb/s (odstraněn bod č. 3). Dále má čtyři SFP porty. Do jednoho z nich je vložen optický přijímač typu LC, konkrétně HP X121 1G. Přijímače zajišťují přenos dat mezi patry. Důvodem volby switche byla jeho jednoduchá správa, široké možnosti nastavení a poměr cena-výkon. Switche jsou jištěny záložním zdrojem.

Záložní zdroje

Rack A je jištěn záložním zdrojem APC Smart-UPS 2200VA. Záložní zdroj má vyšší kapacitu, oproti záložnímu zdroji v Racku B. Výkon 2200 VA garantuje jištění serveru i switche. Pomocí propojovacího kabelu mezi serverem a UPS je záložní zdroj monitorován softwarem PowerChute, v případě výpadku elektrického napájení je server včas a bezpečně vypnut.

Rack B je zálohován menším zdrojem, konkrétně APC Smart-UPS SC 450VA.

Hardware pro server

Jeden server zjednodušuje administraci i údržbu. Hardwarová struktura pro navržený server je taková, aby dokázala pokrýt nároky na zpracování příchozí i odchozí e-mailové komunikace. Obsahuje kvalitní disky s krátkou přístupovou dobou (kvůli datovému úložišti). Byly zvoleny dva disky 1 TB WD RE4. Kapacita je dimenzována pro server s úložištěm dat. Má disky s tzv. RAID edice, které jsou konstruovány pro provoz v RAIDU. RAID je metoda zabezpečení dat proti selhání disku. Data jsou ukládána na více nezávislých discích a jsou zachována i při selhání některého z nich. Byl vybrán softwarový RAID konkrétně RAID 1. Zápis dat zajišťuje operační systém. RAID 1 je označován jako zrcadlení disků. Zápis dat je prováděn současně na oba disky. V případě výpadku jednoho disku (degradovaný stav) se pracuje s kopií dat, která je ihned k dispozici na druhém disku. Správce počítače disk později vymění a zařadí zpět do pole.

Na serveru bude provozován firewall (iptables) a je třeba, aby byl vybaven dvěma síťovými gigabitovými kartami tak, aby byla zaručena dostatečná rychlost přenosu dat (zajištěn bod č. 9).

Jako vhodný server byl zvolen HP DL360, obsahující redundantní napájecí zdroj. V případě výpadku jednoho záložního zdroje server běží dále. Dle cenové nabídky je možné si dokoupit záruky na 365 dní v roce, 24 hodin denně, případně servisní zásah na místě do 4 hodin viz příloha s označením PIV.

Správa identit

Uživatelům nastavena pouze uživatelská práva (pokryt požadavek č. 7).

Software

Levným řešením je distribuce CentOs, která je zároveň velice stabilní a snadno se udržuje. Je pravidelně aktualizována a obsahuje všechny potřebné nástroje. Obsahuje staré, ale osvědčené verze softwaru, které nemají bezpečnostní díry atd.

Na všech stanicích v kancelářích je nainstalován operační systém MS Windows. Síťové adresy stanic přiděluje dynamicky DHCP server (viz kapitola 4.5).

Na serveru bude nastaven firewall pomocí iptables (pokryt požadavek č. 11). Online služby budou vhodně ošetřeny firewallem (viz kapitola 4.6).

Do vnitřní sítě bude možný přístup odkudkoliv pomocí šifrovaného spojení a softwaru OpenVPN (zajištěn požadavek investora č. 12), na základě uživatelského certifikátu. (viz kapitola 4.8).

Jednotlivé stanice budou přistupovat dle pevně definovaných práv k souborům pomocí open-source Samba (pokryt požadavek č. 6 a č. 13) (viz kapitola 4.7).

Dále bude na serveru nakonfigurován Postfix (viz kapitola 4.10) používaný jako poštovní server (zajištěn požadavek č. 14). Důvodem volby Postfixu je jeho bezpečnost. Pro vzdálený bezpečný přístup k poště bude nakonfigurován software Dovecot (viz kapitola 4.10.1) a zabezpečen pomocí SSL (viz kapitola 4.10.2). K ochraně před nevyžádanou poštou slouží SpamAssassin (viz kapitola 4.10.3).

Bezpečnost dat je pojištěna pravidelnou automatickou zálohou serveru (pokryt bod č. 8 a č. 13). Každý den se budou provádět inkrementální zálohy souborového systému pomocí nástroje dump (viz kapitola 4.11.2). Navíc každou sobotu bude prováděno vytvoření image disku pomocí nástroje MondoRescue (viz kapitola 4.11.1).

Připojení k internetu

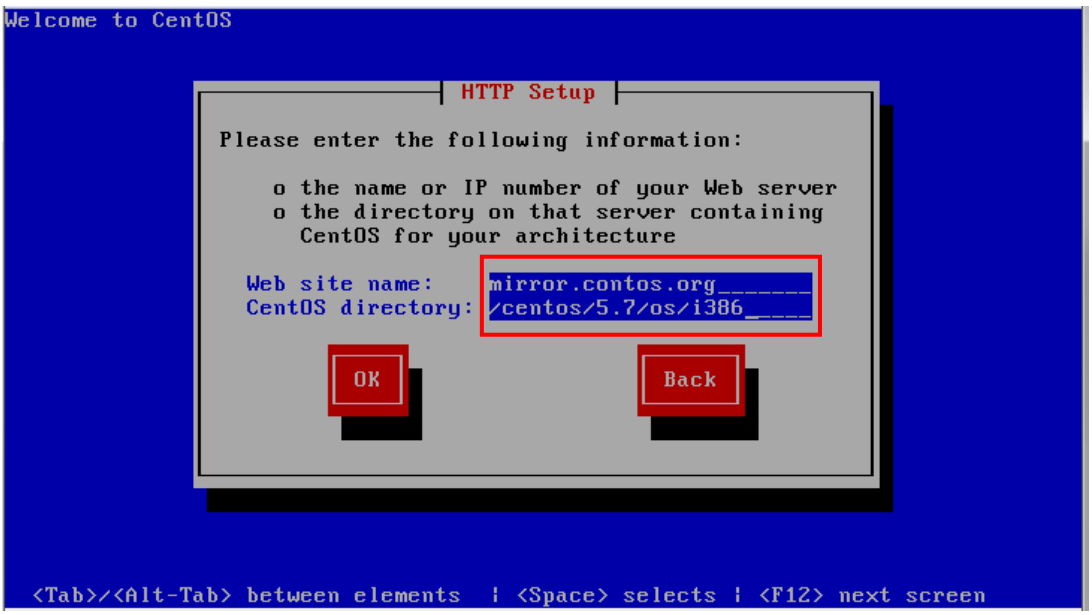
Stávající připojení bude nahrazeno optickým připojením od firmy Alfservis s.r.o. Firma Alfservis má optiku „zakruhovanou“. V případě výpadku jedné větve nedojde k výpadku internetu. Cena připojení je 4 200 Kč bez DPH za 8 Mbit/s symetricky (zajištěn bod č. 4). To znamená 8 Mbit/s upload a 8 Mbit/s download. V ceně jsou k dispozici dvě veřejné IP adresy.

4.4 Instalace CentOS

Pro server je zvolena distribuce CentOS. Instalace je velmi jednoduchá. Instalační soubor se stáhne ze stránek CentOSu: http://centos.org/. Je vybrána možnost netinstall. Nahrá se instalační iso soubor, který má velikost 12MB a vypálí se na CD jako obraz a nabootuje se z něj. Distribuci CentOS lze instalovat v textovém nebo grafickém režimu. Instalátor využívá systém Anaconda. Po nabootování následují kroky:

1. K instalaci v grafickém režimu, se stiskne pouze enter.
2. Určí se jazyk systému – English.
3. Zadá se rozložení klávesnice – us.

4. Zvolí se instalace balíčků z http.
5. Povolí se pouze verze IPv4.
6. Nakonfiguruje se cesta, odkud se stáhnou balíčky:

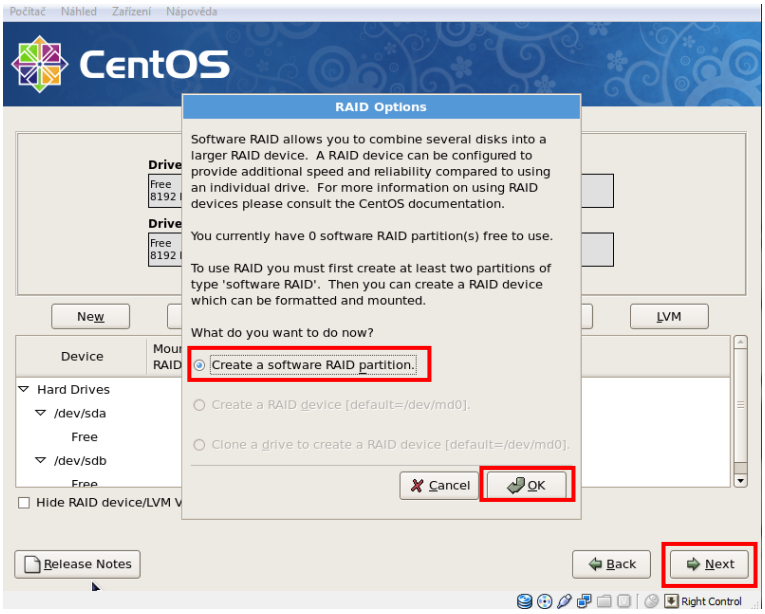


Obr. 9. Cesta odkud, se stahují balíčky

7. Následuje krok rozdělení disku. Zvolí se možnost, změnit rozdělení disků.

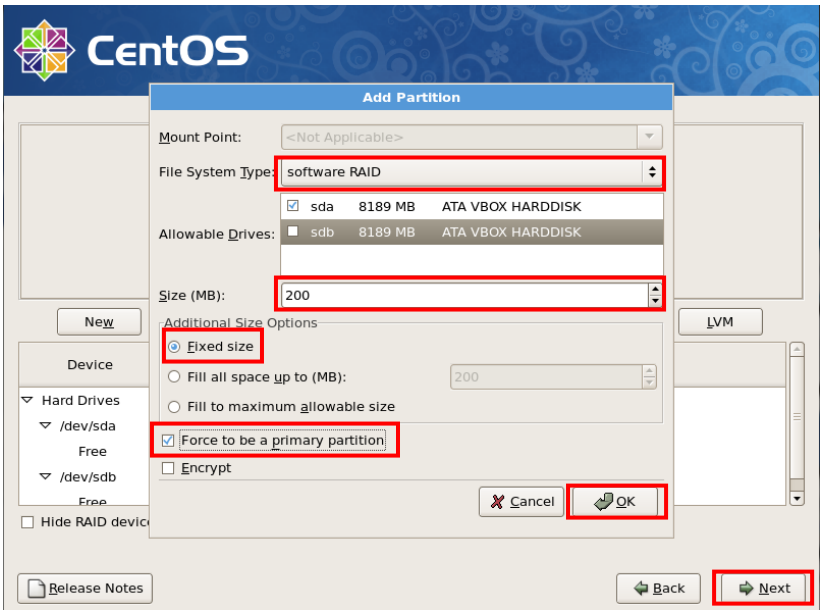
Obr. 10. Rozdělení disku

8. Stiskne se tlačítko reset. Tím se disky dají do stavu bez jakéhokoliv rozdělení.
9. Stiskne se tlačítko RAID, Create a software RAID.



Obr. 11. Vytvoření RAIDu

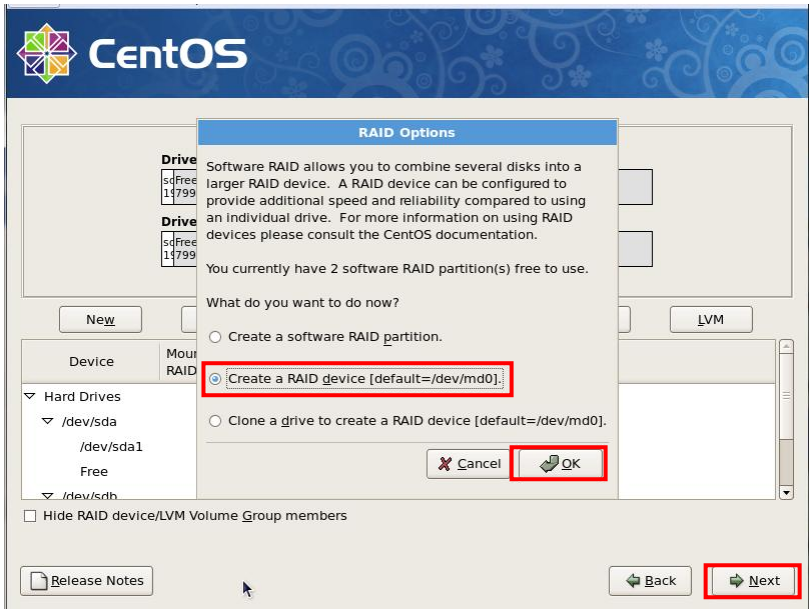
10. Nejdříve se vytvoří RAID partition pro oblast /boot. Vybere se disk sda a vyhradí se 200 MB a zvolí se možnost Force to be a primary partition.



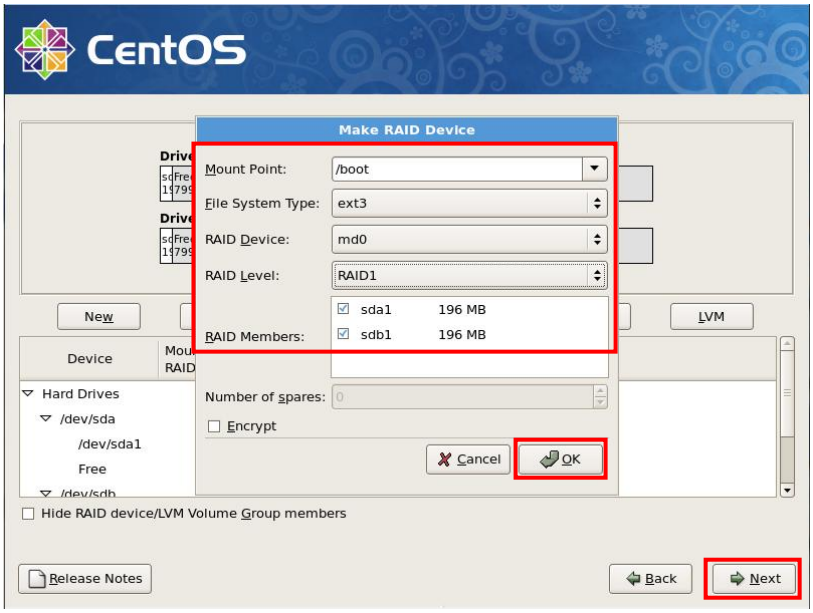
Obr. 12. Vytvoření oblasti pro /boot

11. Vše se zopakuje pro disk sdb.

12. Následuje vytvoření softwarového RAIDu pomocí tlačítka RAID, propojení do pole md0 (RAID 1) a vytvoření oddílu /boot.

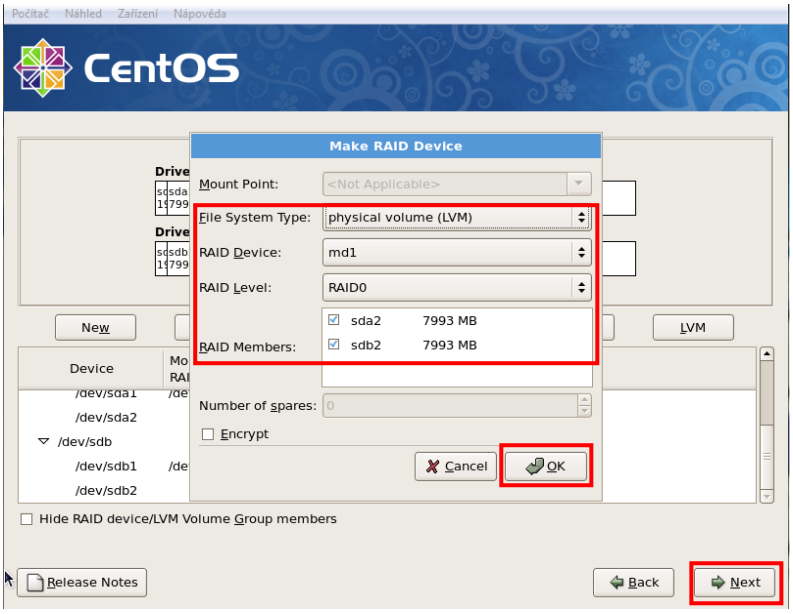


Obr. 13. Vytvoření RAIDu – md0



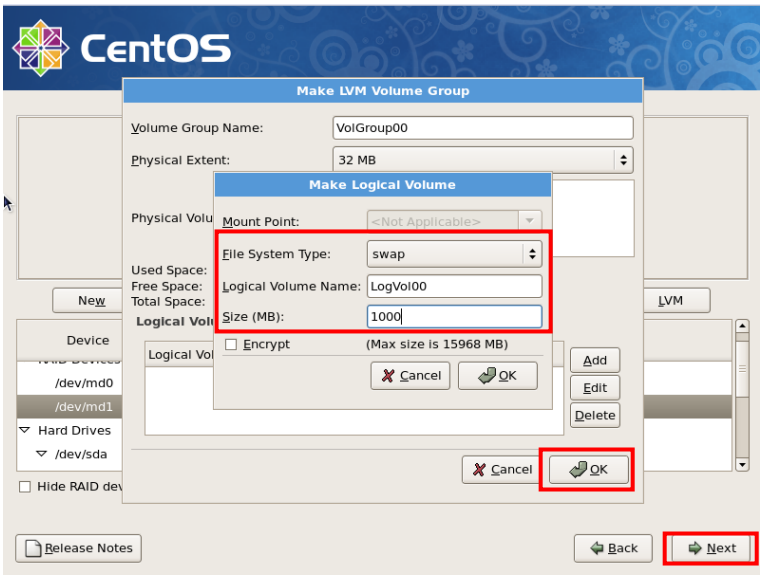
Obr. 14. Vytvoření oddílu /boot na md0

13. To samé platí pro zbytek disku. Zvolí se varianta, aby sda a následně sdb obsadilo maximálně volného místa (fill to maximum allowable size) a vytvoří se z nich pole md1. Filesystém je LVM.

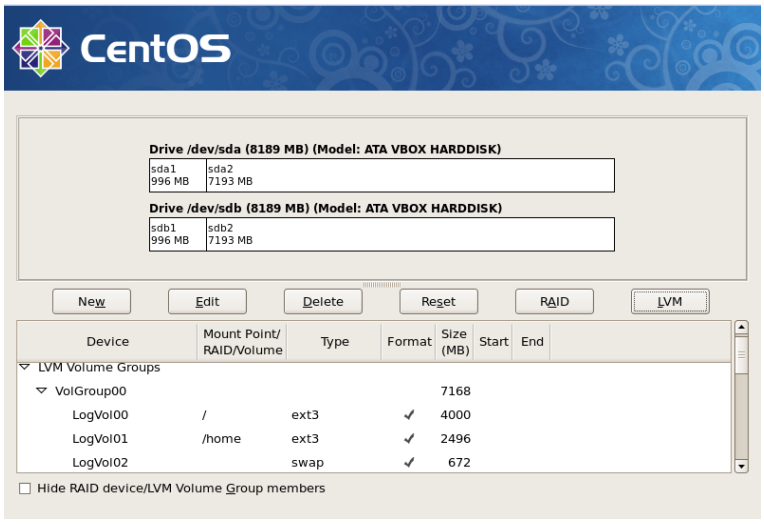


Obr. 15. Vytvoření filesystému LVM na md1

14. Zvolí se tlačítko LVM a vytvoří se jednotlivé oddíly pro swap, home a kořen.

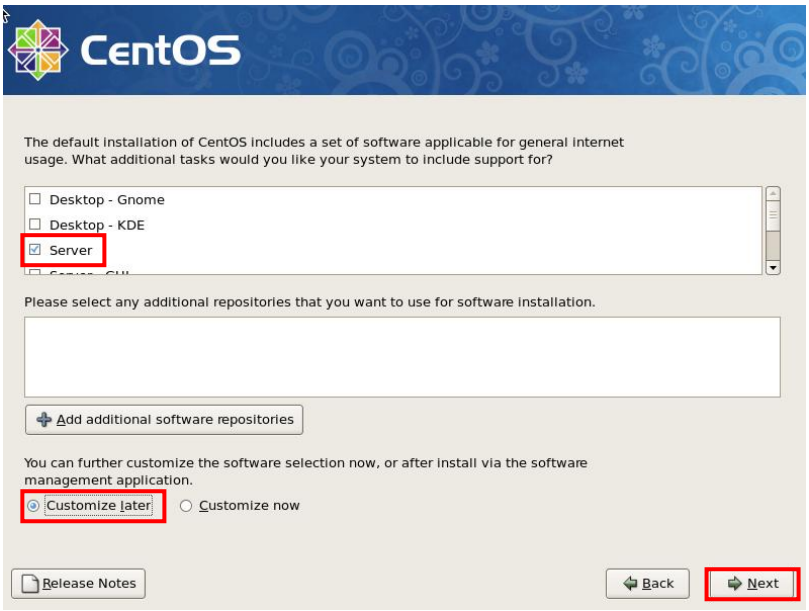


Obr. 16. Vytvoření jednotlivých oddílů swap, home a kořen



Obr. 17. Konečné rozdělení disků

15. Po vytvoření oblasti, se pokračuje pomocí tlačítka next.
16. Nastaví se IP adresy pro rozhraní eth0 a eth1.
17. Vybere se světová oblast.
18. Nastaví se heslo administrátora systému – root.
19. Následuje možnost volby aplikací. Na server nebude instalováno grafické rozhraní, proto se zvolí varianta server.



Obr. 18. Výběr aplikací

20. Po instalaci se vyjme instalační medium a provede se restart.

Po naběhnutí systému se provede aktualizace příkazem `yum update`.

4.5 Konfigurace DHCP serveru

Nejdříve je potřeba DHCP démona nainstalovat. Provádí se pomocí příkazu:

```
yum install dhcp
```

Konfigurační soubor DHCP démona se nachází v `/etc/dhcpd.conf`. Je dobré si konfigurační soubor preventivně zazálohovat:

```
cp /etc/dhcpd.conf /etc/dhcpd.conf.orig
```

Obsah konfiguračního souboru se prakticky dělí na dvě části (obecnou a konkrétní). V první části je uvedeno jméno sítě, maska, implicitní brána a parametry, chování serveru.

V druhé části se nastaví vlastnosti jednotlivých podsítí a klientů. Důležité je nezapomínat středník na koncích řádků.

Konfigurace DHCP serveru:

```
# Pokud je v siti vice DHCP serveru vybere si authoritative
authoritative;

# Synchronizace s domenou zakazana:
ddns-update-style none;

# Nazev domeny
option domain-name "haresta.cz";

# Adresa routeru-brany
option routers 10.10.10.1;

# Adresa DNS serveru
option domain-name-servers 10.100.160.1, 10.100.160.7;

# Maska site:
option subnet-mask 255.255.255.0;

# Adresa broadcastu
option broadcast-address 10.10.10.255;

# Standardni cas zapujceni IP adresy v sekundach
default-lease-time 3600;

# Nejdelsi cas zapujceni adresy v sekundach
max-lease-time 7200;

# Definovani podsite, ze ktere budou prirazovany adresy:
subnet 10.10.10.0 netmask 255.255.255.0 {

# Nadefinovani rozsahu adres, ktere se mohou pridelit tj. 10.10.10.51 az 10.10.10.150
       range 10.10.10.50 10.10.10.150;
}
# Definice jednotlivych klientu:

host NBJITKA {                                  // Nazev hosta
       hardware ethernet 00:16:36:52:35:49;     // Hardwarova adresa MAC
       fixed-address 10.10.10.51;               // Napevno pridelena IP adresa
       }

host NBHARESTA {
       hardware ethernet 00:26:b9:0a:93:b7;
       fixed-address 10.10.10.52;
       }
```

Ke konfiguraci DHCP serveru je třeba zjistit hardwarovou adresu síťové karty, aby byla vždy přiřazena stejná IP adresa. V linuxu lze zjistit hardwarovou IP adresu pomocí příkazu:

```
ifconfig | grep HWaddr
```

Výstup vypadá následovně:

```
eth0      Link encap:Ethernet  HWaddr 00:E0:7D:F3:A2:0E
```

V operačním systému Windows se zjistí hardwarová adresa pomocí příkazu:

```
ipconfig /all
```

Dále je potřeba upravit soubor `/etc/sysconfig/dhcpd` a to následně:

```
DHCPDARGS=eth1
```

Ve výpisu zařízení se najde položka fyzické adresy u adaptéru sítě Ethernet připojení k místní síti.

Tím je dáno DHCP démonovi na vědomí, že má naslouchat na rozhraní eth1.

Dále je nutné zajistit, aby DHCP démon startoval po spuštění systému. To se děje pomocí příkazu: `chkconfig --level 345 dhcpd on`

Pokud v `/etc/dhcpd.conf` úprava, je potřeba provést restart služby:

```
/etc/init.d dhcpd restart
```

V případě potíží je potřeba sledovat log, který obsahuje chybová hlášení (např. chyby v syntaxi): `cat /var/log/messages | grep dhcpd`

DHCP server funguje, nicméně klienti nemohou přistoupit na internet. Příčinou je, nutnost zapnout ve firewallu v iptables NATování:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
$IPTABLES -A FORWARD -i eth1 -o eth0 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o eth0 -j SNAT --to 46.149.120.
```

Z hlediska bezpečnosti je podstatné zamezit pomocí firewallu propagaci broadcast IP adresy do vnější sítě. Přes iptables se zakáže přístup na porty DHCP serveru zvenčí tak, aby někdo nepoužil všechny IP adresy a tím neodstavil část klientů. Přidělené IP adresy jsou ukládány do souboru `dhcp.leases`. Zde se dá přesně zjistit, jaké IP adresy byly přiděleny stanicím [3].

4.6 Konfigurace firewallu

Konkrétní nastavení softwarového firewallu se nachází v příloze (příloha PV). Příkazy jsou popsány vysvětlivkami.

4.7 Konfigurace Samba serveru

Správa uživatelů:

Správa uživatelů se provádí programem smbpasswd. Program nám umožňuje přidávat, editovat a odebírat jednotlivé účty.

- vytvoření nového uživatele: `smbpasswd –a honza`
- změna hesla uživatele: `smbpasswd honza`
- smazaní uživatele: smbpasswd –x honza

Konfigurace Samba serveru:

```
# Globalni nastaveni serveru Samba
[global]

# Nastaveni jmena pracovni skupiny
workgroup = TEST

# Popis serveru
server string = Samba Server Version %v

# Omezeni pristupu podle rozhrani
interfaces = lo eth1 10.10.10.0/24

# Adresy pomoci niz lze k serveru pristupovat
hosts allow = 127. 10.10.10.

# Kam se ma logovat, rozdeleni (%m) podle nazvu pocitace
log file = /var/log/samba/%m.log

# Maximalni velikost logu 50 KB, pak rotace
max log size = 50

# Mapovani uzivatelu systemu na uzivatele Samby
username map = /etc/samba/smbusers

# Soubor s hesly uzivatelu Samby
smb passwd file = /etc/samba/smbpasswd

# Hesla budou sifrovana
encrypt passwords = yes

# Synchronizovat z hesel Samby a systemu
unix password sync = yes
passwd program = /usr/bin/passwd %u

# Server bude zajistovat prochazeni site
local master = yes

# Nastaveni kodovani
dos charset = cp852
unix charset = utf-8
display charset = utf-8

# Mapovani uctu hosta
guest account = nobody
```

```
# v pripadne zadneho nebo spatneho loginu lze mapovat uzivatele automaticky na guest
# account:
map to guest = bad user

[homes]
# Komentar k dane sekci
comment = Domovske adresare

# Urcuje zda slozka bude soucasti verejneho seznamu, sdilena slozka neni viditelna pri
# prochazeni
browseable = no

# Zapisovani povoleno
writable = yes

# Nove vytvorene soubory dostanou zde nastavena prava. Vse se ridi stejnymi pravi jako
# linuxova prava.
create mask = 0775

# Nastaveni prav k adresarum, opravneni uzivatel muze cist, zapisovat a spoustet. Ostatni
# uzivatele jen cist a zapisovat.
directory mask = 0775

[vyroba]
comment = vyrobni data

# Uplna cesta k adresari
path = /home/harri/vyroba

# Pristup jen pro opravnene uzivatele
public = no

# Jmena uzivatelu, kteri mohou adresar sdilet
writable = yes
valid users = harri
create mask = 0775
directory mask = 0775

[public]
comment = public
path = /tmp/public
writable = yes
guest ok = yes
public = yes
writable = yes
browsable = yes
```

K tomu, aby byla Samba funkční, se spustí dva procesy: smbd a nmbd. Lze provést: ručně, automaticky během startu systému nebo pomocí služby xinetd. Je zvolena možnost automaticky během startu systému:

```
/etc/init.d/smbd start
```

```
/etc/init.d/nmbd start
```

Automaticky po startu systému:

```
chkconfig --level 345 smbd on
```

```
chkconfig --level 345 nmbd on
```

4.8 Konfigurace OpenVPN

Instalace OpenVPN: `yum install openvpn`

Nakopírování skriptů (easy-rsa), pro vytvoření vlastní PKI:

`cp -R /usr/share/doc/openvpn-2.2.0/easy-rsa/ /etc/openvpn/`

Přejití do daného adresáře: `cd /etc/openvpn/easy-rsa/2.0/`

Upraví se práva tak, aby šlo zapisovat, číst, spouštět: `chmod +rwx *`

Nadefinují se základní parametry PKI, nacházející se v souboru vars, konkrétně následující proměnné:

```
export KEY_COUNTRY="CZ"                          // zeme
export KEY_PROVINCE="Czech Republic"             // mesto
export KEY_CITY="Blansko"                        // mesto
export KEY_ORG="HARESTA"                         // organizace
export KEY_EMAIL=harri@haresta.cz                // e-mail
```

Provede se úvodní inicializace a vytvoření certifikační autority (CA).

```
source ./vars         // zvoli se zdrojovy soubor zakladních parametrů PKI
./clean-all           // vycisti se adresar
./build-ca            // vygeneruje se certifikacni autorita
```

Při generování certifikátu je nutná interakce (zadání požadovaných údajů):

```
./build-ca
Generating a 1024 bit RSA private key
.....................................................................++++++
..................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CZ]:CZ
State or Province Name (full name) [Czech Republic]:Czech Republic
Locality Name (eg, city) [Blansko]:Blansko
Organization Name (eg, company) [HARESTA]:HARESTA
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [HARESTA CA]:Petr Haresta
Name []:
Email Address [harri@haresta.cz]:harri@haresta.cz
```

Díky před-vyplněným údajům lze údaje jen potvrdit. Po příkazu dojde k vytvoření souborů `ca.crt` (certifikát) a `ca.key` (privátní klíč). Soubory jsou defaultně uloženy ve složce keys. Složku lze upravit editací souboru vars. Platnost certifikátu je defaultně nastavena na 10 let. Je důležité udržet soubor `ca.key` v bezpečí, jinak dojde k poškození důvěry certifikační autority. Jak je psáno výše, OpenVPN využívá obousměrnou autentizaci, proto je nutné ještě vygenerovat certifikát serveru a klienta. Generování certifikátu a privátního klíče pro server provedeme příkazem: `./build-key-server server`

Výstup příkazu je obdobný výstup jako u certifikační autority. Nyní máme soubory `server.crt`, `server.key`.

Zbývá vygenerovat certifikát klienta: `./build-key honza`

Příkaz nezabezpečí přístup k certifikátu heslem. Proto se využívá příkazu:

`./build-key-pass honza`

Výstup je opět obdobný. V úvodu generování certifikátu je nutné zadat heslo. Mohlo by se zdát, že je vše připraveno, ale není tomu tak. Je ještě potřeba vygenerovat Diffie-Hellman parametry. Protokol slouží k bezpečné výměně klíčů přes nezabezpečené médium. Generování parametrů se provádí pomocí skriptu: `./build-dh`

Nyní je v podadresáři keys vše připraveno.

Konfigurace serveru (/etc/openvpn/server.conf):

```
# OpenVPN pobezi v rezimu server a bude se chovat jako TLS server
mode server
tls-server

# Pobezi na portu 1194 (nutno povolit ve firewallu) a protokolu UDP
port 1194
proto udp

# Virtualni adapter tun0, umoznuje routovani
dev tun0

# Jednotlive certifikaty (certifikacni autorita, certifikat serveru a privatni klic
# serveru)
ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key

#  Diffie-Hellman parametry
dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem

# Definice IP adresy serveru
server 10.10.11.0 255.255.255.0

#  Routa pro pristup do eth1
push "route 10.10.10.0 255.255.255.0"

# Keepalive zpravy kazdych 10 sekund, po 120 sekundach je zrejme, ze klient je nedostupny
keepalive 10 120

# Nastaveni logovani
log-append /var/log/openvpn.log

# Komprese cele komunikace
comp-lzo

# Pro vyssi bezpecnost bezi demon OpenVPN pod neprivilegovanym  opravnenim uzivatel
# openvpn, skupina openvpn
user openvpn
group openvpn

# Direktivy zajistuji udrzeni zdroju (klice, adapter) v pripade restartu
persist-key
persist-tun

# Konfigurace statickych adres pro klienty v adresari ccd
client-config-dir ccd
```

To je celá konfigurace serveru. Zbývá nastavit konfiguraci klientů na serveru v adresáři ccd:

```
cat /etc/openvpn/ccd/harri
ifconfig-push 10.10.11.21 10.10.11.22
```

To znamená, že uživatel harri dostane vždy IP adresu 10.10.11.21.

Konfigurace klienta:

Vzhledem k tomu, že jsou všichni klienti na operačním systému Windows, je popis instalace na tomto systému. Aplikace pro Windows se stahují ze stránek http://openvpn.se/. Instalace je velmi jednoduchá a jednotlivé body instalace potvrzují stisknutím tlačítka next. Program se standardně nainstaluje do adresáře: `c:\Program Files\OpenVpn\`. Do adresáře `config` do soboru `gw.haresta.ovpn` se umístní konfigurační parametry uvedené níže. Nastaví se bezpečně přenesená certifikační autorita, certifikát klienta a privátní klíč klienta. Vše přenést do adresáře `c:\Program Files\OpenVPN\config\haresta` (uvedeno v konfiguračním souboru).

```
# OpenVPN bezi v rezimu klienta a bude se chovat jako TLS client
client
tls-client

# Vyuziva se adapter tun0
tun0

# Jmeno/IP adresa a port serveru na ktery se vzdalene pripojuji
remote gw.haresta.cz 1194

# Direktivy zajistuji udrzeni zdroju (klice, adapter) v pripade restartu
persist-key
persist-tun


# Jednotlive certifikaty (certifikacni autorita, certifikát klienta a privatni klic
# klienta)
ca "C:\\Program Files\\OpenVPN\\config\\haresta\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\haresta\\harri.crt"
key "C:\\Program Files\\OpenVPN\\config\\haresta\\harri.key"

# Komprese cele komunikace
comp-lzo

# Nastaveni urovne logovani
verb 3
```

4.9 Konfigurace DNS serveru

Bind je jeden z nejpoužívanějších multiplatformních DNS serverů. Bind je součástí CentOS. Konfigurační soubor se nachází v `/etc/named.conf`:

```
options {

        directory "/var/named";      // adresar ve ktere BIND hleda sve konfiguracni
                                     // soubory
        auth-nxdomain no;            // DNS server neposkytuje informace o siti
        query-source port 53;        // Pro komunikaci s ostatnimi dns servery se pouzije
                                     // port 53
```

```
 # Pokud DNS server nezna odpoved, zepta se serveru uvedenych ve forwarders
 forward first;
  forwarders {
        46.149.113.2;
        46.149.114.2;
  };

# Adresy, kde nas DNS server posloucha
    listen-on {
          127.0.0.1;
          46.149.120.6;
   };
  };

#Informace o korenovych DNS serverech nachazejicich se v souboru named.ca
 zone "." IN {
         type hint;
         file "named.ca";
 };

# Reverzni zona
zone "0.0.127.in-addr.arpa" IN {
          type master;
          file "named.local";
          allow-update { none; };
}

# Nastaveni primarniho serveru
 zone "haresta.cz" IN {
         type master;
         file "haresta.cz.zone";
         allow-update { none; };
     allow-transfer { // Informace se poskytuje jen sekundarnim serverum
       89.187.142.9;
       46.149.113.151;
       193.179.195.121;
    };
 };
```

Konfigurace kořenových DNS serverů se nachází ve `/var/named/named.ca` (příloha PII).

Konfigurace reverzní zóny vyskytující se ve `/var/named/named.local:`

```
$TTL 86400
  @       IN SOA gw.haresta.cz. harri.haresta.cz. (
                  2011120902 ;       // Serial
                  43200 ;            // Refresh
                  3600 ;             // Retry
                  1209600 ;          // Expire
                  3600 ;             // Minimum
                  )
          NS gw.haresta.cz.
 1       PTR localhost.
```

Konfigurace DNS záznamu pro doménu haresta.cz, vyskytující se ve /var/named/haresta.cz.zone:

```
$TTL 86400
  @       IN SOA gw.haresta.cz. harri.haresta.cz. (
                  2011121201 ;       // Serial
                  43200 ;            // Refresh
                  3600 ;             // Retry
                  1209600 ;          // Expire
                  3600 ;             // Minimum
                  )

          IN NS gw.haresta.cz.       // primarni server
          IN NS ns.gosw.cz.          // sekundarni server
          IN MX 10 gw.haresta.cz.    // MX zaznam pro postovni s.

  gw IN A 46.149.120.6               // gw.haresta.cz prislusi IP 46.149.120.6
```

```
mail IN CNAME gw.haresta.cz.       // nameserver bude zaroven i postovnim serverem
ftp IN CNAME gw.haresta.cz.        // zaroven bude ftp serverem
```

Spuštění démona named se provede pomocí příkazu: `/etc/init.d/named start`

Trvalé spuštění se provádí pomocí příkazu:

```
chkconfig --level 345 named on
```

K ověření nastavení lze použít například resolver dig: `dig gw.haresta.cz`

4.10 Konfigurace poštovního serveru – Postfix

Postfix není součástí distribuce CentOS. Naopak součástí distribuce je MTA Sendmail. Ten je potřeba deaktivovat. Zastaví služba Sendmail a zajistí se, aby se nespustila při restartu serveru:

```
/etc/init.d/sendmail stop
```

```
chkconfig sendmail off
```

Instalaci Postfixu se spustí:

```
yum install postfix
```

Změní se defaultní MTA, aktuálně je defaultní Sendmail, pomocí stisku klávesy 2. se přepne na Postfix:

```
alternatives –config mta
There are 2 programs which provide 'mta'.
Selection      Command
-----------------------------------------------
*+ 1  /usr/sbin/sendmail.sendmail
2  /usr/sbin/sendmail.postfix
Enter to keep the current selection[+], or type selection number: 2
```

Konfigurační soubory se nachází v adresáři `/etc/postfix/`. Hlavním konfiguračním souborem je soubor `main.cf`. Dalším pak `master.cf`, který se upravuje zřídka. Pracuje se s ním jen, když se přidává nebo odebírá nějaká služba.

Konfigurace main.cf:

```
# Definice jmene adresy adresy serveru (plne DNS jmeno)
myhostname = gw.haresta.cz

# DNS jmeno domeny
mydomain = haresta.cz

# Prepsani adresy u odesilanych e-mailu – vzdy bude haresta.cz
myorigin = $mydomain

# Z vnitrniho rozhrani je prijimana veskera posta
```

```
inet_interfaces = all

# Pro jake destinace bude Postfix prijimat postu
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

# Z duvodu zabezpeceni Postfixu je povolen pristup klientum jen z urcitych adres
mynetworks = 10.10.10.0/24, 127.0.0.0/8

# Kam se maji ukladat e-maily
home_mailbox = Maildir/
```

Zdá se, že je vše nastaveno, ale opak je pravdou. Server by se choval jako open-relay. To znamená, že vezme k poslání jakoukoliv zprávu bez ohledu na odesílatele nebo adresáta. Server umožňuje přijetí zprávy odkudkoliv a dopravit ji kamkoliv. Přes server tak může odejít mnoho SPAMů. SMTP server by měl být nastaven tak, aby nepřebíral zprávy, které přichází z vnějšku a nemají adresáta uvnitř domény. To se provede následujícími pravidly:

```
#  Helo restriction – aplikuje se v SMTP protokolu HELO/EHLO
# Pozaduje se, aby klient navazoval komunikaci SMTP prikazem v HELO/EHLO
smtpd_helo_required = yes

smtpd_helo_restrictions =
# Povoli se pokud adresa klienta odpovida adresam uvedenych v mynetworks
       permit_mynetworks,

# Odmitne se pokud HELO/EHLO hostname neni v plne kvalifikovane domenove forme
reject_non_fqdn_helo_hostname,

# Odmitne se pokud HELO/EHLO hostname ma spatnou syntaxi
reject_invalid_helo_hostname,
       permit

# Sender restrictions - aplikuje se v SMTP protokolu v MAIL FROM:
smtpd_sender_restrictions =

# Povolime se pokud adresa klienta odpovida adresam uvedenych v mynetworks
permit_mynetworks,

# Odmitne pozadavek pokud adresa v prikazu MAIL FROM není v plne kvalifikovane domenove
# forme jak vyzaduje RFC
reject_non_fqdn_sender,

# Odmitne pozadavek pokud nazev domeny adresy zadane v prikazu MAIL FROM nema A nebo MX
# zaznam
reject_unknown_sender_domain,
       permit

# Recipient restrictions – aplikuje se v SMTP protokolu v RCPT TO:
smtpd_recipient_restrictions =

# Odmitne pozadavek pokud je posta dorucovana hromadne pomoci odeslani vice prikazu
# najednou.
reject_unauth_pipelining,

# Odmitne pozadavek pokud adresa v prikazu RCPT TO neni v plne kvalifikovane forme, jak
# vyzaduje RFC
reject_non_fqdn_recipient,

# Odmitne pozadavek pokud nazev domeny adresy zadane v prikazu RCPT TO nema zaznam DNS a
# nebo MX
reject_unknown_recipient_domain,

# Povoli se pokud adresa klienta odpovida adresam uvedenych v mynetworks
permit_mynetworks,

# Odmitne pozadavek pokud server neni cilovym mistem nebo predavajicim serverem pro cilove
# misto. Cilova mista jsou uvedena v parametrech mydestination inet_interfaces
reject_unauth_destination,
```

```
# Kontroluje zadane e-mailove adresy v souboru /etc/postfix/sender_access dle toho, co je v
# souboru uvedeno. Muze postu prijmout (OK), odmitnout (REJECT,)umisti zpravu do fronty
# (HOLD)
check_sender_access
              hash:/etc/postfix/sender_access,

# Omezeni pro cerne listiny zjistuje, ze klient je uveden v sluzbe DNSBL
reject_rbl_client sbl.spamhaus.org,
       reject_rbl_client bl.spamcop.net,
       permit
```

Spuštění démona postfix se provede pomocí příkazu: `/etc/init.d/postfix start`

Trvalé spuštění se provádí pomocí příkazu:

```
chkconfig --level 345 postfix on
```

4.10.1 Dovecot

Aby bylo možné ke schránkám přistupovat vzdáleně (mimo program, který se spouští přímo na serveru), pomocí protokolu POP3/POP3S, IMAP/IMAPS slouží software Dovecot. Konfigurační soubor se nachází v `/etc/dovecot.conf`:

```
# Podporovane protkoly
protocols = imap pop3 imaps pop3s

# Nastaveni lokace ulozenych e-mailu
mail_location = maildir:~/Maildir
```

Spuštění démona dovecot se provede pomocí příkazu:

```
/etc/init.d/dovecot start
```

Trvalé spuštění se aktivuje příkazem:

```
chkconfig --level 345 dovecot on
```

4.10.2 SSL

Dalším požadavkem firmy bylo zabezpečit e-mailovou komunikaci proti odposlechnutí. K tomu je třeba vygenerovat soukromý a veřejný klíč, na základě asymetrické kryptografie. Komunikace mezi serverem a klientem je šifrovaná. Generování certifikátu je popsáno v kapitole OpenVPN (kapitola 4.8).

Zedituje se konfigurační soubor `/etc/postfix/main.cf`:

```
# Aktivace TLS
smtp_use_tls = yes
smtpd_use_tls = yes

# Cesta k serverovemu certfikatu
smtpd_tls_cert_file = /etc/pki/tls/certs/server.crt

# Cesta k soukromemu klici
smtpd_tls_key_file = /etc/pki/tls/certs/server.key
```

```
# Debugovaci level 1 = informace o spusteni a o certfikatech
smtpd_tls_loglevel = 1

# Zasobnik na klice, aby nebyl zbytecne pretezovan server
# Expirace klicu v databazi je 1. hodina = 3600 sekund
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:/var/spool/postfix/smtpd_tls_cache

# Napoji se Postfix na generator nahodnych cisel
tls_random_source = dev:/dev/urandom
```

Následně je třeba editovat konfigurační soubor: `/etc/postfix/master.cf:`

```
smtps     inet  n       -       n       -       -       smtpd -o smtpd_tls_wrappermode=yes
```

V předposledním kroku se zedituje konfigurační soubor: `/etc/dovecot.conf:`

```
# Zapne se podpora SSL
ssl_disable = no

# Cesta k servrovemu certfikatu
ssl_cert_file = /etc/pki/tls/certs/server.crt

# Cesta k soukromemu klici
ssl_key_file = /etc/pki/tls/certs/server.key
```

Nakonec je potřeba služby restartovat:

```
/etc/init.d/postfix restart

/etc/init.d/dovecot restart
```

4.10.3 SpamAssassin

Instalace se provede pomocí příkazu: `yum install spamassassin`

Provede se aktualizace: `sa-update`

Upraví se konfigurační soubor `/etc/master.cf:`

```
smtp      inet  n       -             n       -       -       smtpd -o
content_filter=spamassassin

spamassassin   unix   -      n      n      -      -      pipe   user=nobody
argv=/usr/bin/spamc -f -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

A konfigurační soubor `/etc/mail/local.cf:`

```
# Presahne-li hranici 5 bodu bude predmet zpravy oznacen jako  [SPAM]
required_hits 5

#Nebude se menit telo e-mailu
report_safe 0
rewrite_header Subject [SPAM]
```

Spustí se SpamAssassina: `/etc/init.d/spamassassin start`

Trvalé spuštění SpamAssassina se provede příkazem:

```
chkconfig --level 345 spamassassin on
```

Vzhledem k tomu, že byl upraven konfigurační soubor Postfixu, je nutné provést jeho restart: `/etc/init.d/postfix restart`

Test SpamAssassina se provede příkazem:

```
spamassassin < /usr/share/doc/spamassassin-3.3.1/sample-spam.txt
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on gw.haresta.cz
X-Spam-Flag: YES
X-Spam-Level: **************************************************
X-Spam-Status: Yes, score=1000.0 required=5.0 tests=GTUBE,NO_RECEIVED,
        NO_RELAYS autolearn=no version=3.3.1
X-Spam-Report:
        * -0.0 NO_RELAYS Informational: message was not relayed via SMTP
        * 1000 GTUBE BODY: Generic Test for Unsolicited Bulk Email
        * -0.0 NO_RECEIVED Informational: message has no Received headers
Subject: [SPAM] Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Spam-Prev-Subject: Test spam mail (GTUBE)
```

Z výstupu je vidět, že SpamAssassin správně vyhodnotil vzorek a ohodnotil jako spam (`X-Spam-Flag: YES`).

4.11 Zálohování

4.11.1 MondoRescue

Zálohovací nástroj byl vybrán, protože vytváří úplný image disku za běhu stroje, tzv. on-the-fly a umožňuje snadnou obnovu. Zálohuje MBR, rozdělení disků, GRUB atd.

Instalace:

Pro OS CentOs má MondoRescue vlastní repositář, proto je instalace trochu náročnější. Nejdříve je nutné nainstalovat repositář RPMforge. Stáhne se pomocí příkazu wget:

```
wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el5.rf.i386.rpm
```

Nainstaluje si DAG´s GPG key:

```
rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
```

Ověření staženého balíčku: `rpm -K rpmforge-release-0.5.2-2.el5.rf.*.rpm`

Nainstaluje se balíček: `rpm -i rpmforge-release-0.5.2-2.el5.rf.*.rpm`

Instalace Mondo Rescue: `yum install mondo`

MondoRescue se skládá ze dvou hlavních částí – mindi a mondo. Mindi vytváří zálohu běžícího jádra včetně potřebných modulů. Mondo je nástroj skládající se ze dvou programů mondoarchive a mondorestore. Mondorestore se využívá k obnově zálohy a prakticky se nikdy nespouští ručně, protože se spouští samostatně při nabootování ze záchranného CD/DVD.

Mondoarchive lze spustit bez parametrů a interaktivně nastavit vše potřebné. Cílem je automatické zálohování, proto je využit neinteraktivní režim, kdy lze skript spouštět třeba v noci, pomocí cronu. Jednotlivé použité parametry jsou uvedené v skriptu.

```
#!/bin/sh
# Skript pro zalohovani image serveru do iso souboru

# Promenne
DATUM=`date "+%Y-%m-%d %H:%M:%S"`
CIL="/mnt/backup_mondo/"
LOG="/var/log/backup.log"

echo "Zaloha image serveru: " $DATUM >> $LOG
echo -e "-------------------------------------------" >> $LOG

# Nejdrive se pripoji sitova jednotka
mount -t cifs //10.10.10.1/public /mnt/ -o guest
echo -e "Uspesne pripojeny disk" >> $LOG

# Samotne zalohovani
# -O ... chce zalohovat(existuje parametr -v, pro overeni zalohy)
# -i ... vystup do souboru
# 9 ... maximalni komrese (0-9)
# -d ... kam vysledny iso soubor ulozit
# -g ... spusti rozhrani gui pro prehlednejsi prubeh zalohovani
# -s ... velikost iso souboru napr. DVD 4200m

if [ -d /mnt/backup_mondo/ ]; then
        mondoarchive -Oi9 -d $CIL -g -s 4200m;
        #Odpojeni disku;
        umount.cifs /mnt/;
        echo -e "Zaloha probehla uspesne a podarilo se odpojit sitovy disk" >> $LOG
                echo -e "Zkontrolujte log less /var/log/mondoarchive.log" >> $LOG
        cat $LOG | mail -s "Zaloha Mondo Rescue uspesne ukoncena" haresta@gmail.com
        exit 0
else
        echo -e "Zaloha neprobehla usepsne - nepodarilo se pripojit sitovy disk" >> $log
        cat $log | mail -s "Zaloha Mondo Rescue obsahuje chybu" haresta@gmail.com
        exit 2
fi
```

Při úspěšném ukončení zálohy je vygenerována informace o pozitivním výsledku. Výsledný iso soubor pak je v adresáři `/mnt/backup_mondo/`. V skriptu je uložen výsledný *.iso soubor na filesystém Samby. Ve skriptu je test, zda-li se filesystém podaří připojit nebo ne.

4.11.2 Dump/restore

Jedná se o velmi často využívaný zálohovací software. Jeho uplatnění je především při zálohování celých diskových oddílů. Lze s ním zálohovat i jednotlivé adresáře, ale tam nelze uplatnit široké možnosti softwaru. K souborovému systému se nepřistupuje pomocí jádra, nýbrž pomocí vlastních knihoven. To s sebou nese spoustu výhod a nevýhod. Mezi nevýhody patří:

- může ho používat jen root
- inkrementální zálohování nefunguje při zálohování seznamu adresářů

Výhody:

- je velmi rychlý – zná dobře souborový systém
- podporuje přímo inkrementální zálohování
- podporuje interaktivní obnovu

Historii jednotlivých inkrementálních záloh je zaznamenána v souboru `/etc/dumpdates`.

```
/dev/mapper/VolGroup00-LogVol01  0  Wed  Feb  15  18:46:58  2012
+0100
/dev/mapper/VolGroup00-LogVol01  1  Sat  Feb  16  14:38:57  2012
+0100
```

V souboru jsou tři sloupce oddělené pomocí bílých znaků, ve kterých je postupně uvedeno:

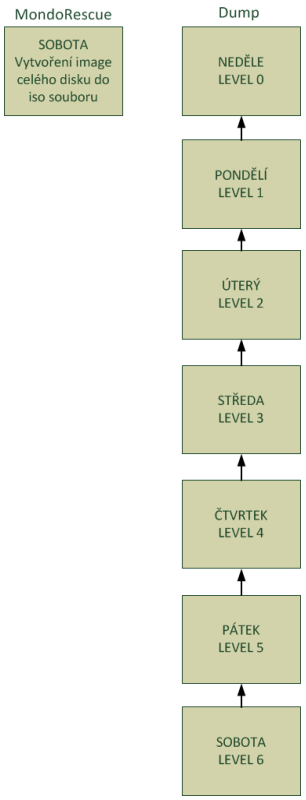
- jméno zařízení, na kterém je uložený souborový systém (/dev/mapper/VolGroup00-LogVol01)
- úroveň zálohy (0,1 …)
- datum, kdy byla provedena záloha

Výsledný skript vypadá následně:

```
#!/bin/sh
# Skript pro zalohovanou souboroveho systemu -> plne a inkrementalni zalohovani
#
# V nedeli se provadi plna zaloha, ostatni dny inkrementalni
#
# Naposledy upravil 11.2.2012

# Promene
DATUM=`date "+%Y-%m-%d %H:%M:%S"`
ZDROJ="/dev/mapper/VolGroup00-LogVol01"
```

```
KOMPRESE="gzip -c"
LOG="/var/log/backup_dump.log"
SERVER="ssh -c blowfish root@10.10.10.99"
ZALOHA=`date "+%a"`

echo -e "Zaloha pomoci nastroje dump $DATUM \n" >> $LOG
echo -e "-------------------------------------------\n" >> $LOG

case $ZALOHA in
    Sun) LEVEL=0;;
    Mon) LEVEL=1;;
    Tue) LEVEL=2;;
    Wed) LEVEL=4;;
    Thu) LEVEL=5;;
    Fri) LEVEL=6;;
    Sat) LEVEL=7;;
esac

# - level urcuje uroven inkrementalni zalohy, v pripade 0 provede celkovou zalohu
# -u bude aktualizovan soubor /etc/dumpdates
# -f cilove zarizeni
dump -${LEVEL}uaf - $ZDROJ 2>>$LOG | $KOMPRESE | $SERVER  "cat >
/tmp/backup/backup${LEVEL}.dump.gz"

echo -e "Zaloha probehla uspesne" >> $LOG

# Odeslani logovaciho souboru e-mailem
cat $LOG | mail -s "Zaloha dump uspesne ukoncena" haresta@gmail.com
exit 0
```

Skript pracuje dle zálohovacího plánu (obrázek 18). V neděli je prováděna úplná záloha a ostatní dny inkrementální. Do proměnné `ZALOHA` jsou vloženy jednotlivé dny a následně v podmínce `case` je určena úroveň zálohy. Parametry jsou opět popsány ve skriptu.



Obr. 19. Zálohovací plán

Ve skriptu je patrné, že záloha je provedena na vzdálený server pomocí ssh a využívá šifrování blowfish. V této podobě nebude skript fungovat autonomně. Při každém spuštění bude vyžadovat heslo k přístupu uživatele root na vzdálený server. Proto se vygeneruje klíč bez „passphrase“, aby nebylo nutno zadávat heslo pro přihlášení na zálohovací server.

Vygenerování klíče se uskuteční příkazem: `ssh-keygen -t rsa`

Klíč se uloží do souboru: `/.ssh/id_rsa.pub`

Nastaví se práva na adresář i na soubory:

```
chmod 700 ~/.ssh && chmod 600 ~/.ssh/*
```

Následně se nakopíruje veřejný klíč na druhou protistranu do souboru `authorized_keys` a to pomocí příkazu:

```
scp /root/.ssh/id_rsa.pub
root@10.0.0.99:/root/.ssh/authorized_keys
```

A opět se nakonfigurují práva na adresář a soubory. Firma vyžaduje automatické zálohování, k němuž je zapotřebí nástroje, který skript automaticky spustí. Mezi ně patří cron (kapitola 3.7.1). Aby docházelo ke spuštění zálohovacích skriptů automaticky, je cron následně upraven:

```
0 1 * * * /root/bin/backup_dump
0 3 * * 6 /root/bin/backup_mondo
```

ZÁVĚR

Při návrhu a modernizaci stávající sítě LAN se vycházelo především z požadavků managementu i zaměstnanců firmy. Diplomová práce popisuje současné provedení počítačové sítě a upozorňuje na její nedostatky.

Snaží se navrhnout jedno řešení, obsahující základní prvky počítačové sítě tak, aby splňovaly veškeré požadavky firmy. Studie doporučuje zjednodušení správy serverů centralizací do jednoho zařízení. Je doporučena výměna stávající kabeláže a aktivních prvků počítačové sítě. Po softwarové stránce je vybrán pro server operační systém Linux, jeho distribuce CentOS.

Firma chtěla provozovat svůj poštovní server a přitom bezpečně vzdáleně přistupovat do počítačové sítě. Požadavku je vyhověno instalací a konfigurací Postfixu pro poštovní server a pro jeho bezpečný přístup bylo zvoleno zabezpečení SSL. Aby uživatel nebyl obtěžován nevyžádanou poštou je nakonfigurován spamový filr SpamAssassin. Pro bezpečný vzdálený přístup je užito služby OpenVPN.

Mezi hlavní požadavky firmy patřilo bezpečné úložení dat. Dosaženo redundancí disku v serveru RAID a jeho monitoringem. Byla nainstalována a nakonfigurována Samba, která umožňuje nastavení přístupových práv k souborům. Data jsou zabezpečena pravidelnou denní zálohou.

Pro zajištění bezpečnosti sítě je nakonfigurován firwall iptables, pomocí kterého je zamezeno neoprávněnému přístupu do lokální sítě.

Z návrhu inovace jsou zřejmé výhody, které sebou nová změna přináší. Zrychlení a zefektivnění práce běžných uživatelů. Devizou budoucnosti je zabezpečení dat.

ZÁVĚR V ANGLIČTINĚ

The network improvement proposal was based mainly on the requirements of the company management and employees. The thesis focuses on the current state of the network and identifies it's weak points.

One possible solution was presented. It arranges basic elements of the network in the way which satisfies all the company requirements. The thesis proposes server administration simplification by the means of centralization of all the features in one device. Cabling restructuralization and active network devices usage is adviced. The centralized server is to be equipped with the Linux operating system (CentOS variant).

The main requirements of the company was to operate it's own mail server and to be able to access the local services remotely in a secure manner. This was satisfied with the Postfix mail server software and secure access by SSL protocol. To diminish the obtrusive emails volume, usage of the spam filterSpamAssassin was proposed. Secure remote access was implemented by OpenVPN service.

Another main requirement was a secure data storage. It was achieved by a disk redundancy (RAID) with appropriate monitoring. Data access management was implemented by Samba access rights. Daily backups ensure adequate protection against data loss risk.

To gain appropriate network security, iptables firewall was configured. By this way, any unauthorized access to network services is denied.

The proposed improvements of the network infrastructure and server services will bring effectivity, speed and comfort to the end users and also adequate protection of the data against standard risks.

SEZNAM POUŽITÉ LITERATURY

[1] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[2] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006, 211 s. ISBN 80-251-0892-9.

[3] KRČMÁŘ, Petr. *Linux*: *postavte si počítačovou síť*. 1. vyd. Praha: Grada, 2008, 182 s. ISBN 978-80-247-1290-1.

[4] HUNT, Craig. *Linux*: *síťové servery*. Praha: SoftPress, c2003, 672 s. ISBN 80-864-9759-3.

[5] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery*. Vyd. 1. Brno: Computer Press, 2003, 450 s. ISBN 80-722-6983-6.

[6] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[7] ECKSTEIN, Robert. *Samba*: *Linux jako server v sítích windows*. Vyd. 2. Brno: Computer Press, 2005, 525 s. ISBN 80-251-0649-7.

[8] LINUXEXPRES. [online]. © 2012 [cit. 2012-04-28]. Dostupné z: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-openvpn-server

[9] SCHRODER, Carla. *Linux*: *kuchařka administrátora sítě*. Vyd. 1. Brno: Computer Press, 2009, 596 s. ISBN 978-80-251-2407-9.

[10] DENT, Kyle D. *Postfix*: *kompletní průvodce*. 1. vyd. Praha: Grada, 2005, 237 s. ISBN 80-247-1029-3.

[11] HILDEBRANDT, Ralf a Patrick KOETTER. *Postfix*: *provozujeme poštovní server v Linuxu*. vyd. 1. Brno: Computer Press, 2006, 431 s. ISBN 80-251-1020-6.

[12] LINUXEXPRES. [online]. © 2012 [cit. 2012-04-28]. Dostupné z: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-agenti-e-mailu-metody-ochrany

[13] Zálohování. [online]. s. 36 [cit. 2012-05-01]. Dostupné z: http://www.cbvk.cz/files/regionfce/vzdelavani/zalohovani.pdf

[14] LINUXEXPRES. [online]. © 2012 [cit. 2012-04-28]. Dostupné z: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-uvod-do-zalohovani

[15] *Používáme Linux*: *podrobný průvodce Linuxem*. 3., aktualiz. vyd. Brno: Computer Press, 2003. ISBN 80-722-6698-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
Gbit/s	Gigabit za sekundu
IMAP	Internet Message Access Protocol
IP	Internet Protocol
LAN	Local Area Network
LVM	Logical Volume Management
MAC	Media Access Control
MAN	Metropolitan Area Network
Mbit/s	Megabit za sekundu
NAT	Network Adress Translation
PKI	Public Key Infrastructure
POP3	Post Office Protocol vision 3
RAID	Redundant Array of Inexpensive Disks
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
STP	Shielded Twisted Pair
TCP	Transimission Control Protocol
Tzv.	Tak zvaný
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair

VPN	Virtual Private Network
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

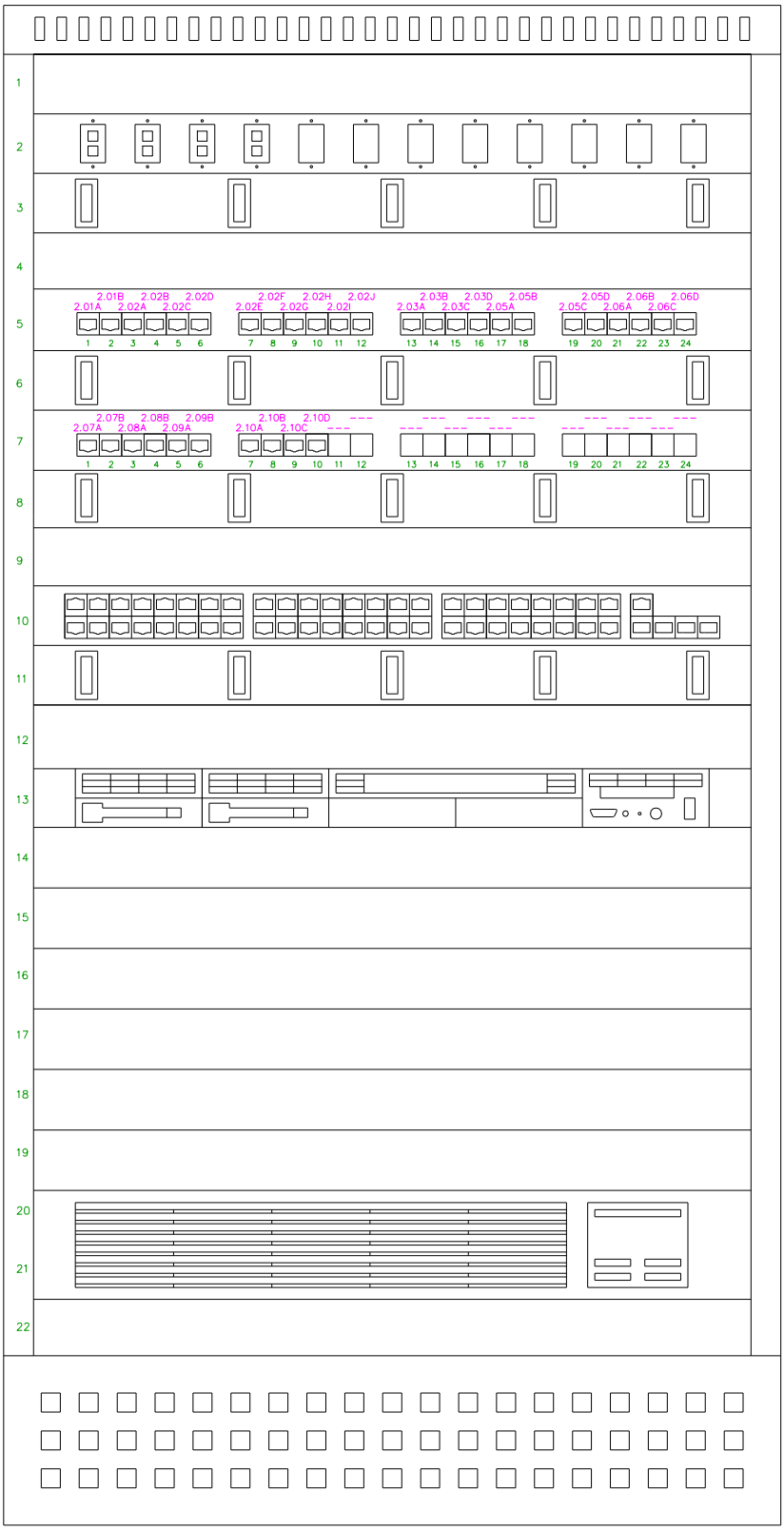
SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA PI: SCHÉMA RACKU A

RACK A:

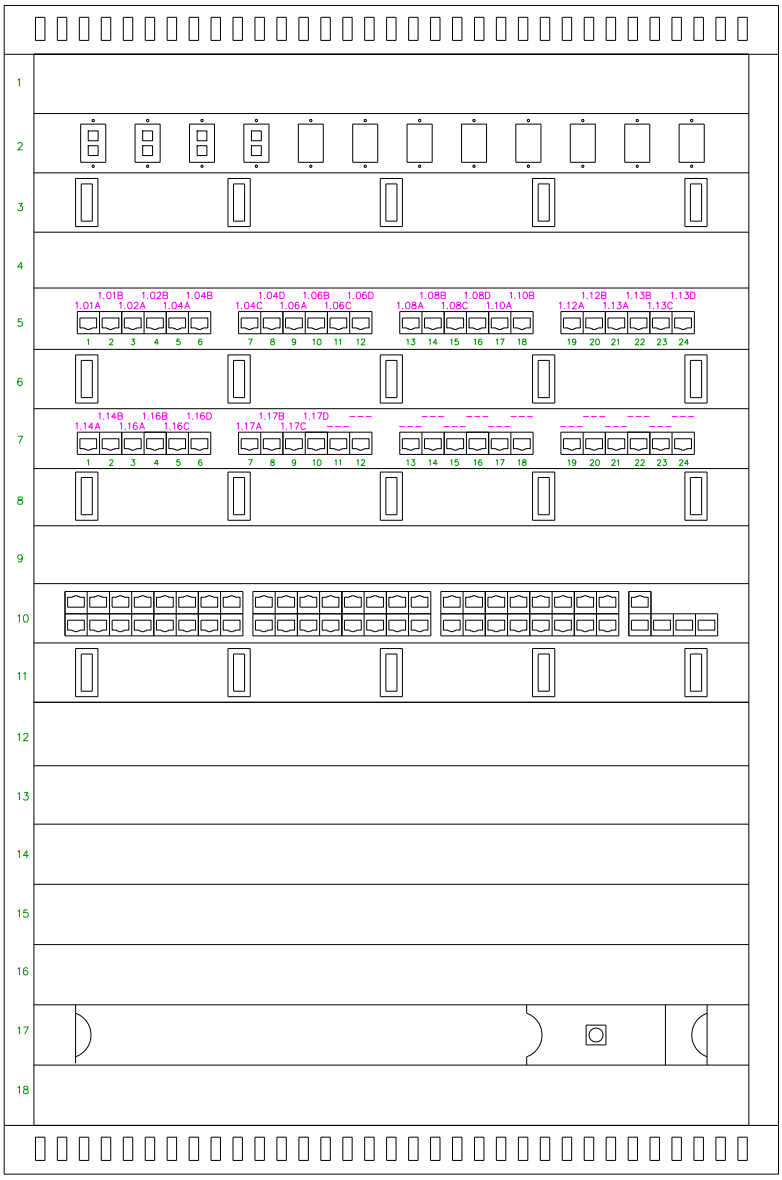
STOJANOVÝ DATOVÝ ROZVADĚČ 19", 22U, 600x1080x800 (šxvxh)



PŘÍLOHA PII: SCHÉMA RACKU B

RACK B:

NÁSTĚNNÝ DATOVÝ ROZVADĚČ 19", 18U, 600x900x495 (šxvxh)



Rezerva

Optická vana HSELS085LG – 8x vlákno MM, konektory LC

Vyvazovací panel
DBS14805

Rezerva

Modulární patch panel HSER0240GS
24x keystone RJ-45 UTP cat. 6 HSEMRJ6UWS

Vyvazovací panel
DBS14805

Modulární patch panel HSER0240GS
20x keystone RJ-45 UTP cat. 6 HSEMRJ6UWS

Vyvazovací panel
DBS14805

Rezerva

Aktivní prvek LAN
Switch HP V1910-48G

Vyvazovací panel
DBS14805

Rezerva

Rezerva

Rezerva

Rezerva

Rezerva

Záložní zdroj UPS
APC Smart-UPS SC 450VA

Rezerva

PŘÍLOHA PIII: SCHÉMA 1. A 2. POSCHODÍ

PŘÍLOHA PIV: CENOVÝ ROZPOČET

Návrh datové sítě firmy
VÝKAZ VÝMĚR

PČ	Specifikace položky	Typové označení	Dodavatel	počet	MJ	Materiál		Práce	
						Kč/MJ	Cena celkem	Kč/MJ	Cena celkem
Datové zásuvky									
	Keystone modul RJ-45 nestíněný, Cat.6 (třída E) 250 MHz	HSEMRJ6UWS	Schrack Technik	68	ks	92,00	6 256,00	120,00	8 160,00
	Datová zásuvka MOSAIK 45x22,5 mm, pro 1 modul, neosazená, RAL 91010	HSEMD01W1F	Schrack Technik	68	ks	17,20	1 169,60	20,00	1 360,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 1 m	H6ULG01K0G	Schrack Technik	20	ks	34,00	680,00	10,00	200,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 2 m	H6ULG02K0G	Schrack Technik	25	ks	45,50	1 137,50	10,00	250,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 3 m	H6ULG03K0G	Schrack Technik	23	ks	60,14	1 383,22	10,00	230,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 5 m	H6ULG05K0G	Schrack Technik	0	ks	81,00	-	10,00	-
Datový rozvaděč RACK A									
	Stojanový rozvaděč 22U, kompletní, RAL 7035, 600x1080x800 (šxvxh), 51 kg, prosklené dveře s bezpečnostním sklem	DS226080-A	Schrack Technik	1	ks	9 808,00	9 808,00	1 500,00	1 500,00
	Zámek FAB, systém EMKA, 1 klíč	DV900333	Schrack Technik	1	ks	244,00	244,00	50,00	50,00
	Náhradní klíč k zámku DV900333	DV900334	Schrack Technik	1	ks	45,50	45,50	-	-
	Modulární podstavec, boční panel (1 pár), hloubka 800 mm	DSOT1280	Schrack Technik	1	ks	771,00	771,00	200,00	200,00
	Modulární podstavec, přední / zadní panel, kabelový vstup s kartáčem, šířka 600 mm	DSOF1262	Schrack Technik	1	ks	266,00	266,00	100,00	100,00
	Modulární podstavec, přední / zadní panel, s protiprachovým filtrem, šířka 600 mm	DSOF1263	Schrack Technik	1	ks	361,50	361,50	100,00	100,00
	Háček 80 x 80 mm, kovový	DBKO8080	Schrack Technik	4	ks	70,00	280,00	25,00	100,00
	19" polička s perforací, pokládací, hloubka 450 mm, max. zatížení 80 kg	DFS14845-D	Schrack Technik	1	ks	443,00	443,00	120,00	120,00
	Ventilační jednotka horní / spodní, 2 ventilátory	DLT44802-A	Schrack Technik	1	ks	2 105,50	2 105,50	250,00	250,00
	19" vyvazovací panel výšky 1U, 5 x vyvazovací háček, barva světle šedá RAL 7035	DBS14805	Schrack Technik	4	ks	198,00	792,00	120,00	480,00
	19" optický rozvaděč kompletní, pro 8 vláken MM OM2, spojky LC, optická kazeta pro 12 vláken s integrovaným držákem pro uložení svárů, 8x pigtail LC OM2 2 m	HSELS085LG	Schrack Technik	1	ks	2 961,00	2 961,00	120,00	120,00
	Ochrana sváru, 60 mm	HCLSPHSCHR	Schrack Technik	8	ks	13,00	104,00	15,00	120,00
	Optický propojovací kabel duplexní OM2, LC / LC 2 m	HLP25LL02F	Schrack Technik	1	ks	461,00	461,00	10,00	10,00
	19" modulární patchpanel, prázdný, neosazený, pro max. 24 modulů	HSER0240GS	Schrack Technik	2	ks	510,50	1 021,00	120,00	240,00
	Keystone modul RJ-45 nestíněný, Cat.6 (třída E) 250 MHz	HSEMRJ6UWS	Schrack Technik	34	ks	92,00	3 128,00	120,00	4 080,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 1 m	H6ULG01K0G	Schrack Technik	34	ks	34,00	1 156,00	10,00	340,00
	Switch HP V1910-48G, 48 portů 10/100/1000 + 4 porty 10/100/1000 dual personality, kapacita přepínání: 104 Gbps, napájení 100-240V AC	JE009A	C System CZ	1	ks	17 429,00	17 429,00	120,00	120,00
	HP X121 1G SFP LC SX Transceiver	J4858C	C System CZ	1	ks	7 095,00	7 095,00	50,00	50,00
	HP DL360 G7 E5606 2.13GHz 4-core 1P 4GB-R								
	P410i/ZM 460W	633778-421	C System CZ	1	ks	57 198,00	57 198,00	600,00	600,00
	HP 460W CS HE Gold Pow er Supply	503296-B21	C System CZ	1	ks		-		-
	1TB 3G SATA 7.2k 2.5in MDL HDD	625609-B21	C System CZ	2	ks		-		-
	HP 3 year 4 hour 24x7 ProLiant DL36x p Collaborative Support		HP	1	kpl	26 345,00	26 345,00	-	-
	HP 3y Nbd CTR ProLiant DL360 HW Support		HP	1	kpl	11 952,00	11 952,00	-	-
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 2 m	H6ULG02K0G	Schrack Technik	1	ks	45,50	45,50	10,00	10,00
	Záložní zdroj 1980W, 2U Rack-mount, SmartSlot, USB+RS-232, černá	APC Smart-UPS 2200VA LCD RM	C System CZ	1	ks	20 199,00	20 199,00	250,00	250,00

Datový rozvaděč RACK B									
	Nástěnný jednodílný rozvaděč s odnímatelnými bočnicemi, 18U, 600x900x495 (šxvxh), 30,4 kg, celoskleněné dveře s bezpečnostním sklem	DW186050	Schrack Technik	1	ks	5 813,00	5 813,00	1 500,00	1 500,00
	19" napájecí panel AXON, 5 x 230 V, 3 m přívodní kabel, přepěťová ochrana	CSRAB-RPX2	Schrack Technik	0	ks	710,00	-	120,00	-
	19" vyvazovací panel výšky 1U, 5 x vyvazovací háček, barva světle šedá RAL 7035	DBS14805	Schrack Technik	4	ks	198,00	792,00	120,00	480,00
	19" optický rozvaděč kompletní, pro 8 vláken MM OM2, spojky LC, optická kazeta pro 12 vláken s integrovaným držákem pro uložení svárů, 8x pigtail LC OM2 2 m	HSELS085LG	Schrack Technik	1	ks	2 961,00	2 961,00	120,00	120,00
	Ochrana sváru, 60 mm	HCLSPHSCHR	Schrack Technik	8	ks	13,00	104,00	15,00	120,00
	Optický propojovací kabel duplexní OM2, LC / LC 2 m	HLP25LL02F	Schrack Technik	1	ks	461,00	461,00	10,00	10,00
	19" modulární patchpanel, prázdný, neosazený, pro max. 24 modulů	HSER0240GS	Schrack Technik	2	ks	510,50	1 021,00	120,00	240,00
	Keystone modul RJ-45 nestíněný, Cat.6 (třída E) 250 MHz	HSEMRJ6UWS	Schrack Technik	34	ks	92,00	3 128,00	120,00	4 080,00
	Propojovací kabel nestíněný, 2 x RJ-45, šedý, délka 1 m	H6ULG01K0G	Schrack Technik	34	ks	34,00	1 156,00	10,00	340,00
	Switch HP V1910-48G, 48 portů 10/100/1000 + 4 porty 10/100/1000 dual personality, kapacita přepínání: 104 Gbps, napájení 100-240V AC	JE009A	C System CZ	1	ks	17 429,00	17 429,00	120,00	120,00
	HP X121 1G SFP LC SX Transceiver	J4858C	C System CZ	1	ks	7 095,00	7 095,00	50,00	50,00
	Záložní zdroj 1U, RS-232, černá	APC Smart-UPS SC 450VA	C System CZ	1	ks	4 279,00	4 279,00	250,00	250,00
Instalační materiál									
	Univerzální optický kabel s těsnou sekundární ochranou – typ INTEX , 8 x 50/125	CSHGU8G50	Schrack Technik	15	m	38,00	570,00	25,00	375,00
	Kabel U/UTP, 4 x 2 x AWG 23, 250 MHz, PVC modrý plášť, 500 m	HSEKU423P1	Schrack Technik	3850	m	9,60	36 960,00	19,00	73 150,00
	Kabelové trasy - dodávka stavby dle realizační projektové dokumentace			1	kpl	-	-	-	-
							Materiál		**Práce**
							256 606,32 Kč		99 875,00 Kč
Ostatní									
	Svaření optického vlákna			16	ks		-	500,00	8 000,00
	Měření optického portu, tisk měřícího protokolu			8	ks			110,00	880,00
	Měření metalického portu, tisk měřícího protokolu			84	ks		-	105,00	8 820,00
	Zahoření serveru, instalace SW			1	kpl			500,00	1 500,00
	Nastavení síťových aktivních portů			1	kpl			500,00	1 500,00
	Projektová dokumentace			1	kpl		-	5 600,00	5 600,00
	VRN			1	kpl		-	9 400,00	9 400,00
									Ostatní
									35 700,00 Kč
	Celkem cena bez DPH								**392 181,32 Kč**
	DPH 20%								78 436,26 Kč
	Celkem cena včetně DPH								**470 617,58 Kč**

PŘÍLOHA PV: KONFIGURACE IPTABLES

```
#!/bin/bash

#--------------------------------------------------------------#
#     SCRIPT IPTABLES
#--------------------------------------------------------------#

#--------------------------------------------------------------#
#     Nastaveni rozhrani
#--------------------------------------------------------------#

IPTABLES=/sbin/iptables

#--------------------------------------------------------------#
#     Moduly
#--------------------------------------------------------------#

# Modul pro MASQUERADE
/sbin/modprobe ipt_MASQUERADE

# Modul pro FTP
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp

# Smazani vsech pravidel
$IPTABLES -F -t nat #smaze tabulku NAT
$IPTABLES -F #smaze vsechny pravidla
$IPTABLES -X #smaze vlastni retezce

echo "Uspesne nacteny moduly a smazany pravidla"

#--------------------------------------------------------------#
#     Nastaveni politik
#--------------------------------------------------------------#

# Co neni povoleno, je zakazano
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD DROP

echo "Uspesne nastaveni politiky"

#--------------------------------------------------------------#
#     Vlastni retezce
#--------------------------------------------------------------#

# Ochrana proti SYN-FLOOD - propusti pouze 5 SYN segmentu za 1 sec
$IPTABLES -N syn-flood #vytvori si novy retezec
$IPTABLES -A syn-flood -m limit --limit 1/s --limit-burst 5 -j RETURN #pokud je dodrzen
# limit spojeni vraceno do INPUT jinak zahodim
$IPTABLES -A syn-flood -j DROP #zahodime

echo "Uspesne vytvoreny retezce "

#--------------------------------------------------------------#
#     INPUT
#--------------------------------------------------------------#

# navazane spojeni z internetu akceptuje
$IPTABLES -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A INPUT -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

$IPTABLES -A INPUT -i tun0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# loopback neomuzeje
$IPTABLES -A INPUT -i lo -j ACCEPT

# Odfiltrovani pokusu o SYN flooding
$IPTABLES -A INPUT -i eth0 -p tcp --syn -j syn-flood

# Odfiltrovani pokusu o zahlceni ICMP
$IPTABLES -A INPUT -i eth0 -p icmp -j syn-flood

# Ochrana proti ping of death - max 5 pingu za sekundu
$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 5 -m limit --limit 1/s --limit-burst 5 -j
ACCEPT

# povoleni icmp paketu
```

```
# icmp(0) - echo replay - odpoved
$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 0 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p icmp --icmp-type 0 -j ACCEPT
$IPTABLES -A INPUT -i tun0 -p icmp --icmp-type 0 -j ACCEPT

# icmp(3) - destination unreable - nedorucitelny datagram
$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 3 -j ACCEPT

# icmp(8) - echo request - zadost
$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 8 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p icmp --icmp-type 8 -j ACCEPT
$IPTABLES -A INPUT -i tun0 -p icmp --icmp-type 8 -j ACCEPT

# icmp(11) - time execeed - cas doby doruceni skoncil
$IPTABLES -A INPUT -i eth0 -p icmp --icmp-type 11 -j ACCEPT
#$IPTABLES -A INPUT -i tun0 -p icmp --icmp-type 11 -j ACCEPT

# zbytek icmp paketu se zahodi
$IPTABLES -A INPUT -p icmp -j DROP

# povolene sluzby

# OpenVPN
$IPTABLES -A INPUT -i tun0 -j ACCEPT

# SSH
$IPTABLES -A INPUT -i eth1 -p tcp --dport 2223 -j ACCEPT

# SSH zvenku jen na urcity port
$IPTABLES -A INPUT -i eth0 -p tcp --dport 2223 -j ACCEPT

# SMTP
$IPTABLES -A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 25 -j ACCEPT

# DNS - BIND
$IPTABLES -A INPUT -i eth1 -p udp --dport 53 -j ACCEPT
$IPTABLES -A INPUT -i eth0 -p tcp --dport 53 -j ACCEPT

# SAMBA
$IPTABLES -A INPUT -i eth1 -p tcp --dport 135 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p udp --dport 137:138 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 139 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 445 -j ACCEPT

# IMAP
$IPTABLES -A INPUT -i eth1 -p tcp --dport 143 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 465 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 993 -j ACCEPT


# HTTPS
$IPTABLES -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT
#$IPTABLES -A INPUT -i eth1 -p tcp --dport 10000 -j ACCEPT
$IPTABLES -A INPUT -i eth1 -p tcp --dport 443 -j ACCEPT

# OpenVPN
$IPTABLES -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT

# Zbytek paketu se loguje
$IPTABLES -A INPUT -i eth0 -j LOG --log-prefix "DROP: INPUT eth0: "
$IPTABLES -A INPUT -i eth1 -j LOG --log-prefix "DROP: INPUT eth1: "
echo "INPUT OK"

#------------------------------------------------------------#
#     OUTPUT
#------------------------------------------------------------#

echo "OUPUT OK"

#------------------------------------------------------------#
#     FORWARD
#------------------------------------------------------------#

# Povoleni navazaneho spojeni, jiz existujiciho
$IPTABLES -A FORWARD -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Odfiltrovani pokusu o zahlceni ICMP
$IPTABLES -A FORWARD -i eth0 -p tcp --syn -j syn-flood
```

```
# Povoleni NAT-maskarady v jadre
echo "1" > /proc/sys/net/ipv4/ip_forward
$IPTABLES -A FORWARD -i eth1 -o eth0 -j ACCEPT
$IPTABLES -t nat -A POSTROUTING -o eth0 -j SNAT --to 46.149.120.6

# OpenVPN
$IPTABLES -A FORWARD -s 10.10.10.0/24 -d 10.10.11.0/24 -j ACCEPT
$IPTABLES -A FORWARD -s 10.10.11.0/24 -d 10.10.10.0/24 -j ACCEPT

# Zbytek se loguje
$IPTABLES -A FORWARD -i eth0 -j LOG --log-prefix "DROP: FORWARD eth0: "
$IPTABLES -A FORWARD -i eth1 -j LOG --log-prefix "DROP: FORWARD eth1: "

echo "FORWARD OK"

# Ulozeni pravidel
/sbin/service iptables save
echo "SAVE OK"
```

PŘÍLOHA PVI: KONFIGURACE KOŘENOVÝCH DNS SERVERŮ

```
$TTL 86400
@       IN SOA gw.haresta.cz. harri.haresta.cz. (
                2011120902 ;  // seriove cislo
                43200 ;       // refersh
                3600 ;        // retry
                1209600 ;     // expire
                3600 ;        // TTL
                )
 .                      6D  IN      NS      A.ROOT-SERVERS.NET.
 .                      6D  IN      NS      B.ROOT-SERVERS.NET.
 .                      6D  IN      NS      C.ROOT-SERVERS.NET.
 .                      6D  IN      NS      D.ROOT-SERVERS.NET.
 .                      6D  IN      NS      E.ROOT-SERVERS.NET.
 .                      6D  IN      NS      F.ROOT-SERVERS.NET.
 .                      6D  IN      NS      G.ROOT-SERVERS.NET.
 .                      6D  IN      NS      H.ROOT-SERVERS.NET.
 .                      6D  IN      NS      I.ROOT-SERVERS.NET.
 .                      6D  IN      NS      J.ROOT-SERVERS.NET.
 .                      6D  IN      NS      K.ROOT-SERVERS.NET.
 .                      6D  IN      NS      L.ROOT-SERVERS.NET.
 .                      6D  IN      NS      M.ROOT-SERVERS.NET.
 A.ROOT-SERVERS.NET.    6D  IN      A       198.41.0.4
 B.ROOT-SERVERS.NET.    6D  IN      A       128.9.0.107
 C.ROOT-SERVERS.NET.    6D  IN      A       192.33.4.12
 D.ROOT-SERVERS.NET.    6D  IN      A       128.8.10.90
 E.ROOT-SERVERS.NET.    6D  IN      A       192.203.230.10
 F.ROOT-SERVERS.NET.    6D  IN      A       192.5.5.241
 G.ROOT-SERVERS.NET.    6D  IN      A       192.112.36.4
 H.ROOT-SERVERS.NET.    6D  IN      A       128.63.2.53
 I.ROOT-SERVERS.NET.    6D  IN      A       192.36.148.17
 J.ROOT-SERVERS.NET.    6D  IN      A       198.41.0.10
 K.ROOT-SERVERS.NET.    6D  IN      A       193.0.14.129
 L.ROOT-SERVERS.NET.    6D  IN      A       198.32.64.12
 M.ROOT-SERVERS.NET.    6D  IN      A       202.12.27.33
```