UNIVERZITA PALACKÉHO V OLOMOUCI

Pedagogická fakulta

Katedra technické a informační výchovy

Diplomová práce

ZDENĚK KONFRŠT

OLOMOUC 2010

UNIVERZITA PALACKÉHO V OLOMOUCI

Pedagogická fakulta

Katedra technické a informační výchovy

INFORMAČNÍ SYSTÉM ŠKOLY POSTAVENÝ NA VYUŽITÍ SLUŽEB PLATFORMY LINUX

Diplomová práce

ZDENĚK KONFRŠT

Obor: Učitelství pro 2. stupeň ZŠ,

kombinace matematika – technická a informační výchova

Vedoucí práce: PhDr. Milan Klement, Ph.D.

OLOMOUC 2010

Prohlášení:

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a použil jen uvedených pramenů a literatury. Dále jsem využil poznatky získané v průběhu svého studia na UP a vlastní zkušenosti nabyté při práci s operačním systémem Linux.

V Olomouci dne Zdeněk Konfršt

Poděkování:

Rád bych poděkoval PhDr. Milanu Klementovi, Ph.D za odborné vedení při vypracování diplomové práce.

OBSAH

Úvod

Technický pokrok jde v dnešní době obrovským tempem dopředu, počet počítačů ve světě strmě stoupá. Téměř v každé rodině u nás i ve světě se dnes osobní počítač objevuje a je považován za zcela běžnou součást vybavení domácnosti. Běžné jsou i případy, kdy je v domácnosti více než jeden počítač. S větším počtem počítačů v jedné domácnosti proto vyvstává otázka jejich vzájemného spojování, tedy tvorby menší počítačové sítě - LAN. Vytvořit si v dnešní době takovouto malou domácí síť není z hlediska dostupnosti a ceny potřebného technického vybavení prakticky žádný problém. Počet počítačů roste nejen v domácnostech, počty počítačů se raketovým tempem zvětšují snad v každé organizaci na světě. Logicky se tedy dnes žádná škola, jakožto příspěvková organizace, neobejde bez většího počtu počítačů. Počítače slouží jak administrativním pracovníkům, kteří zajišťují celkový chod školy, tak i pro pedagogy ke zkvalitnění jejich výuky, ale dnes také samotným žákům těchto škol. V dnešní době není žádnou výjimkou, aby se na jedné škole nacházelo i několik desítek počítačů, které jsou podle možností koncentrovány především ve specializovaných a k tomu určených učebnách, kabinetech nebo kancelářích pedagogických pracovníků.

Se zvětšujícím se počtem počítačů ve školách roste i potřeba tyto počítače spojovat a využívat je tak ne pouze jako samostatné pracovní jednotky, ale především využít jejich vzájemnou komunikaci a možnost výměny dat k celkovému zkvalitnění výuky a fungování školy. Vzniká tedy první podnět k tvorbě školní počítačové sítě. Jelikož je návrh školní počítačové sítě velice rozsáhlý, komplikovaný a finančně náročný projekt, je vhodné, aby při jeho realizaci spolupracoval ICT koordinátor školy a zároveň kvalifikovaní odborníci z oboru IT. Díky této spolupráci budou v návrhu zohledněny jak požadavky pedagogů, tak i současné trendy v IT.

Tuto skutečnost si uvědomilo i Ministerstvo školství, mládeže a tělovýchovy a na základě toho vznikl projekt INDOŠ. Tento projekt "Internet do škol" přinesl do několika tisíc českých škol možnosti elektronické komunikace. Ministerstvo školství, mládeže a tělovýchovy tak prostřednictvím generálního dodavatele, nyní provozovatele, zavedlo do počítačově nevybavených českých škol počítače, periferie, internetové připojení a související internetové i intranetové služby.

Jako provozovatel a zřizovatel byla vybrána firma AutoCont CZ a.s., která zajišťovala vybavení škol jak potřebným hardwarem, tak i kvalifikovanými externisty. ICT koordinátoři škol figurovali v mnoha případech pouze jako prostředníci mezi školou a zřizovatelskou firmou, než jako plnohodnotní partneři projektu a na běhu a správě celé sítě se podíleli jen velmi omezeně. Proto si myslím, že by se na některých školách v budoucnosti mohla objevit potřeba vytvoření vlastního serveru, který by plně přebral funkci serverů dodávaných v rámci projektu INDOŠ a umožnil tak snadnější správu sítě.

Cílem mé diplomové práce je navržení jednoduchého manuálu, který by pomohl ICT koordinátorům škol při tvorbě serveru, jenž by byl zcela pod jejich kontrolou a umožňoval tak lepší fungování celé sítě. Server by byl postavený na využití služeb platformy Linux, která je podle mého názoru a dosavadních zkušeností (Od roku 2007 vytvářím a administruji free.net síť se servery postavenými na operačním systému Linux Debian.) pro tyto účely nejvhodnější. V úvodní části předložené diplomové práce bude čtenář seznámen s teorií fungování počítačové sítě, protože praxe vždy vychází z teoretických poznatků. Celá práce je rozčleněna do jednotlivých kapitol, ve kterých postupně seznámím se všemi aspekty, ke kterým je třeba přihlédnout, abychom mohli vytvořit a administrovat takovýto server. Zároveň v této práci bude zmíněna historie systému Unix a nastíněn vývoj operačního systému Linux. Rád bych také stručně charakterizoval několik vývojových větví tohoto systému. (Debian, Mandrake apod.). V této práci se budeme zabývat především sítěmi typu Ethernet, protože tato forma spojení počítačů je na školách nejběžnější. O dnes velmi rozšířených a oblíbených sítích typu Wi-Fi se zmíním pouze okrajově, i když se již tato forma spojení začíná ve školách pozvolna také nasazovat.

Diplomová práce je psána v období přelomu roků 2009 a 2010. Proto bych chtěl čtenáře předem upozornit, že všechny odkazy na použitý software jsou platné k tomuto datu a není proto možné zaručit jejich dlouhodobou dostupnost.

Celá moje práce je koncipována jako návod, jak vytvořit novou nebo vylepšit stávající školní počítačovou síť a jak navrhnout a realizovat vlastní server, který nebude finančně náročný, ale bude plnit všechny nezbytné funkce. Je plně v kompetenci tvůrce serveru, jak si tuto práci upraví nebo rozšíří. Upozorňuji však čtenáře, že se při hlubším zájmu o danou problematiku budou muset seznámit s množstvím další doplňkové literatury.

2. Konkrétní případ pro základní školu

2.1. Počítač a informační systém školy

Téma informačních systémů škol představuje relativně nové téma jak v mezinárodním kontextu, tak zejména v České republice. Informační systémy škol představují specifickou oblast využití manažerských informačních systémů. Informační systémy škol jsou využívány pro řízení činnosti škol a umožňují komunikaci nejen uvnitř školy, ale i navenek. Tyto systémy jsou používány na základních, středních i vysokých školách [1].

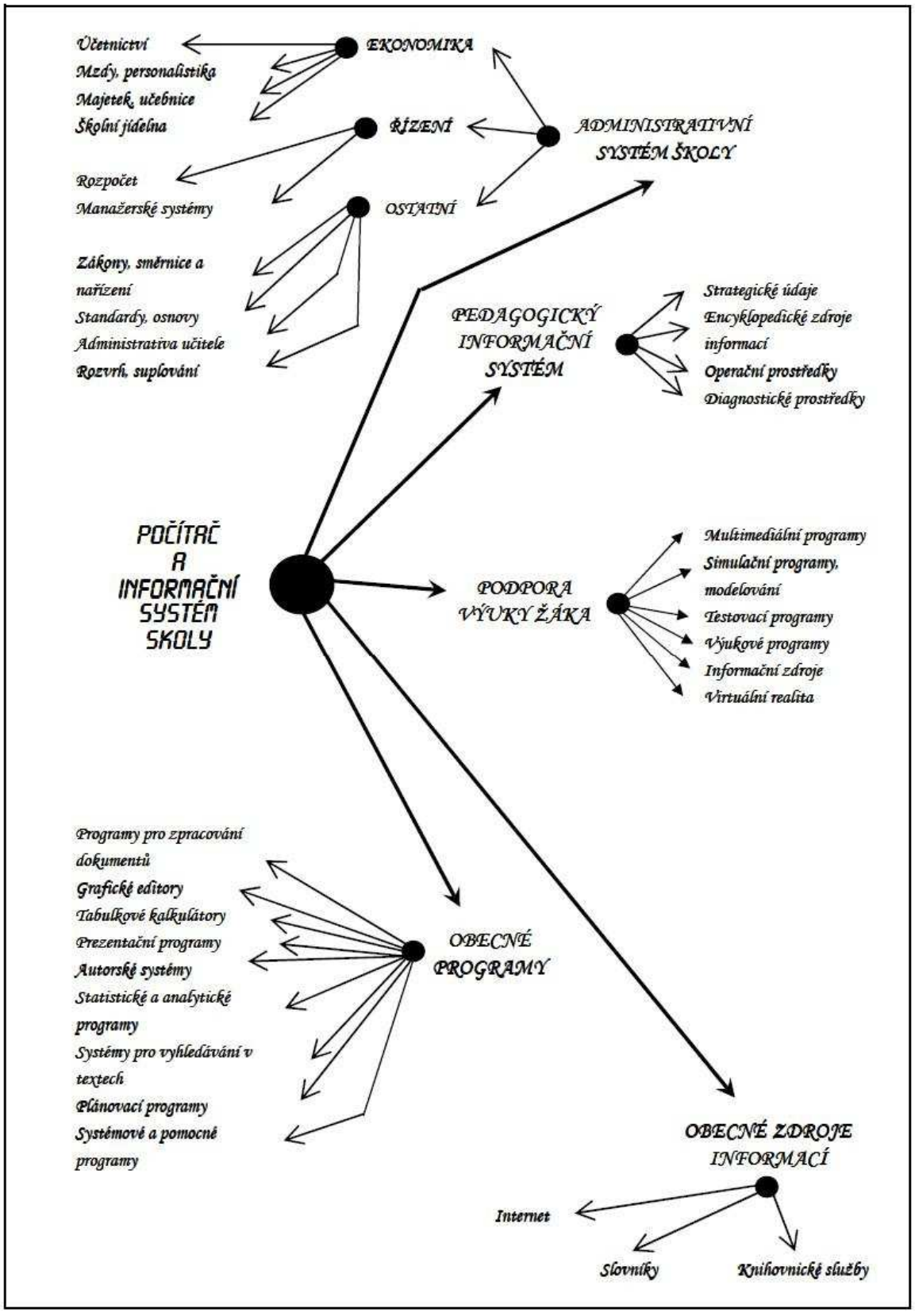
Tento celek se skládá z několika malých částí a v různých formách a v různém stupni funkčnosti se vyskytuje na každé škole. Tyto malé části jsou vzájemně propojeny a spolupracují. Jejich propojení je ve většině případů realizováno za pomoci školní počítačové sítě. Na správném fungování tohoto celku se tedy podílí především sám ICT koordinátor školy případně ICT koordinátor školy, ve spolupráci s kvalifikovaným externím poradcem z oboru IT.

S ohledem na uvedený kontext je možné tvrdit, že výhodu budou mít ty školy, které budou schopny „těžit“ z používání informačního systému školy. Prostřednictvím informačního systému školy je například možné analyzovat výsledky žáků, lze sledovat množství absencí, vést evidenci majetku, vytvářet plány rozvoje školy a sledovat jejich plnění, apod. Většinou je součástí tohoto systému i modul, který umožňuje vést evidenci žáků a učitelů. Souhrnně lze říci, že díky informačnímu systému školy je možné provádět činnosti, které přispějí k usnadnění a urychlení rozhodování managementu školy a zvýší efektivitu jeho práce [1].

Není-li informační systém školy funkční, případně je-li neúplný, nebo málo efektivní, vznikají informační problémy. Proto by každá škola měla pečlivě dbát na dostatečnou účinnost svého informačního systému [2].

Pro snadnější pochopení co to informační systém školy vlastně je, může posloužit následující schéma. Je třeba podotknout, že i přes tento název se nejedná o model, který je uplatňován pouze ve školách, ale s různými obměnami se vyskytuje takřka v každé organizaci nebo firmě.

Obrázek č. 1 – Informační systém školy



2.1.1 Administrativní systém školy

Oblast administrativního systému školy lze ještě pro větší přehlednost rozčlenit na 3 subkategorie - ekonomika, řízení a ostatní. Celkově vzato celá tato oblast slouží především k zajištění ekonomického zázemí školy, k řízení chodu celé instituce a tvorbu kutikulárních dokumentů [2].

2.1.2 Pedagogický informační systém

Činnosti, které spadají do oblasti pedagogického informačního systému, slouží především učitelům a dalším pedagogickým pracovníkům pro všestranné zajištění výuky [2].

2.1.3 Podpora výuky žáků

Tato oblast nachází využití především ze strany žáků. Do této oblasti spadají všechny programy, s kterými pracují především žáci a to jak samostatně, tak i ve spolupráci s učitelem nebo ostatními spolužáky [2].

2.1.4 Obecné programy

Využití této oblasti nelze striktně definovat, jedná se především o činnosti a aktivity jak ze strany učitelů, tak žáků i ostatních pedagogických pracovníků, které nelze zařadit do jiných kategorií. Jinými slovy lze říct, že se jedná o všechny typy programů a činností, které mají obecnější využití [2].

2.1.5 Obecné zdroje informací

Do této kategorie spadají především informační zdroje a systémy, které slouží k podpoře výuky a umožňují žákům srovnávat vědomosti získané při výuce s celosvětově platnými vědeckými trendy a názory [2].

3. Počítačová síť

3.1 Co je to počítačová síť

Při vyslovení pojmu počítačová síť si většina lidí představí několik vzájemně propojených počítačů, které mohou sdílet své technické prostředky a to jak hardwarové, tak i softwarové. Díky tomuto propojení lze dosáhnout mnohem vyššího výpočetního výkonu při nižších celkových nákladech. Toto je víceméně intuitivní představa o počítačové síti, ale pokud bychom chtěli počítačovou síť nějak terminologicky vymezit, tak jako vhodná se mně jeví následující definice:

„Počítačové sítě jsou sítě tvořené skupinou výpočetních systémů propojených přenosovými a spojovacími prostředky za účelem vzájemné komunikace [3]*.“*

3.2 Dělení sítí podle rozlehlosti

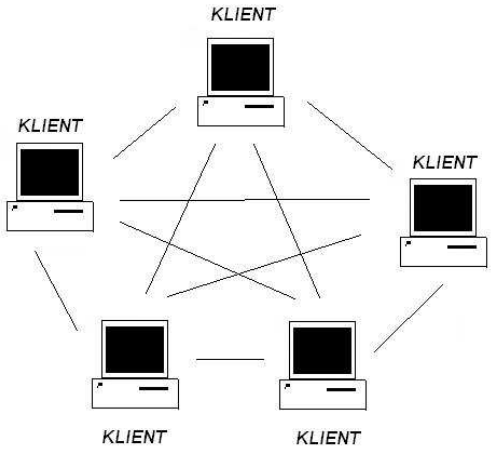
Protože existuje velké množství nejrůznějších typů sítí, bylo nutné zavést jejich kategorizaci. Počítačové sítě je možné dělit podle mnoha hledisek. Nejčastěji se dnes sítě dělí podle rozlehlosti, topologie a použité technologie. V této kapitole budu na počítačové sítě nahlížet z prvního hlediska – rozlehlosti. Protože je ve světě obrovské množství nejrůznějších sítí, kde každá z nich může obsahovat od několika desítek počítačů až po stovky nebo tisíce samostatných strojů, bylo potřeba zavést nějaký druh kategorizace sítí podle velikosti. Jako nejvhodnější rozdělení byly nakonec stanoveny 3 kategorie – LAN, MAN a WAN [4].

LAN – Lokální počítačová síť. Jedná se o první druh počítačových sítí, které byly ve světě realizovány. V počátcích se jednalo o malé sítě, které se sestávaly pouze z několika desítek počítačů a vznikaly především proto, že začala vznikat nutnost vysokorychlostního propojení sálových počítačů. Na začátku existovalo mnoho nejrůznějších technologií, které se ke spojení používaly. Bohužel tyto technologie nebyly vzájemně slučitelné. Až později s nástupem osobních počítačů IBM se do popředí dostal standart Ethernet, který je dnes nejpoužívanější při tvorbě LAN sítí. Později byly do sítě začleňovány další komponenty jako například tiskárna nebo CD-Rom mechanika. Velikost těchto sítí byla v počátku omezena dostupnou

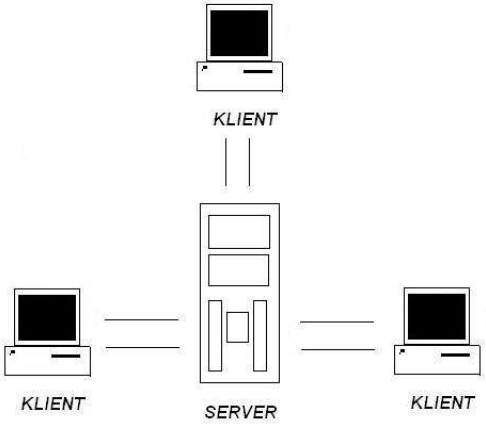
technologií na několik desítek samostatných zařízení, ale dnes již technologie pokročila natolik, že můžeme dosáhnout zapojení nesrovnatelně vyššího počtu počítačů. Hlavní charakteristikou těchto sítí je jejich vazba na nějaký prostor, typicky na jedno podlaží nebo jednu budovu. I když jsou sítě LAN prostorově omezeny na oblast několika desítek, maximálně stovek metrů čtverečních neznamená to, že nemohou být vzájemně propojeny do rozsáhlejších datových sítí. Obecně lze tedy říct, že LAN sítě jsou pouze dílčí části nějaké větších sítí a jejichž vzájemné propojení je realizováno nejčastěji pomocí tzv. vstupních bran, které přenášejí data a zároveň je mění podle protokolů používaných v síti příjemce a umožňují tak i spojení několika nesourodých sítí. Většina dnešních LAN umožňuje připojení množství počítačů a dalšího síťového zařízení. Jediné „omezení“ spočívá v tom, že si tato zařízení musí vzájemně „rozumět“, tzn. všechna zařízení musí používat stejnou sadu pravidel pro komunikaci – komunikační protokol [5].

Tyto sítě můžeme ještě rozdělit podle vzájemného vztahu propojených počítačů na sítě typu peer-to-peer a klient-server. Hlavní charakteristikou sítí typu peer-to-peer je, že všechny zapojené počítače jsou si navzájem rovny a nejsou vzájemně v žádném vztahu podřízenosti a podle požadavků pak nabízejí svoje prostředky ke sdílení sítě. Tento typ propojení je používán zpravidla v jednodušších sítích, u nichž není třeba dbát na bezpečnost. Často se jedná o sítě sestavené jen na určitou předem stanovenou dobu. Naopak sítě typu klient-server jsou vzhledem k bezpečnosti spolehlivější a lépe zabezpečené proti neoprávněnému vniknutí. Takto zapojené sítě jsou přímo postaveny na vzájemném vztahu podřízenosti, kde jeden nebo více počítačů má speciální vyhrazenou funkci. Tyto počítače se nazývají servery, je na nich nainstalovaný specifický druh síťového operačního systému, a tyto servery poskytují svoje služby ostatním počítačům v síti. Prostřednictvím serverů je celá síť spravována. Zbylé počítače jsou těmto serverům podřízeny a nazývají se pracovní stanice. Pracovní stanice neposkytují žádné prostředky ke sdílení, ale pouze využívají prostředků nabízených servery [5].

Obrázek č. 2 – Síť typu peer-to-peer



Obrázek č. 3 – Síť typu klient-server

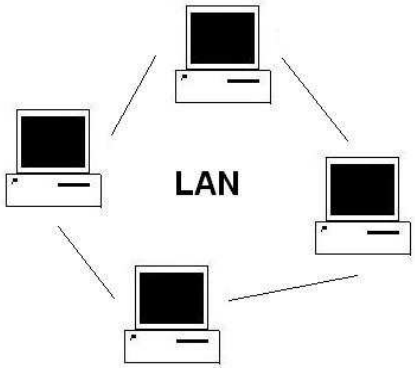


MAN – Metropolitní počítačová síť. Tuto síť si lze představit jako spojovací článek mezi sítěmi LAN a WAN. Nejčastěji je MAN ohraničena velikostí jednoho města, ale je schopna přenášet data na vzdálenost několika desítek kilometrů, a proto jsou tyto sítě používány jako spojovací články LAN sítí.

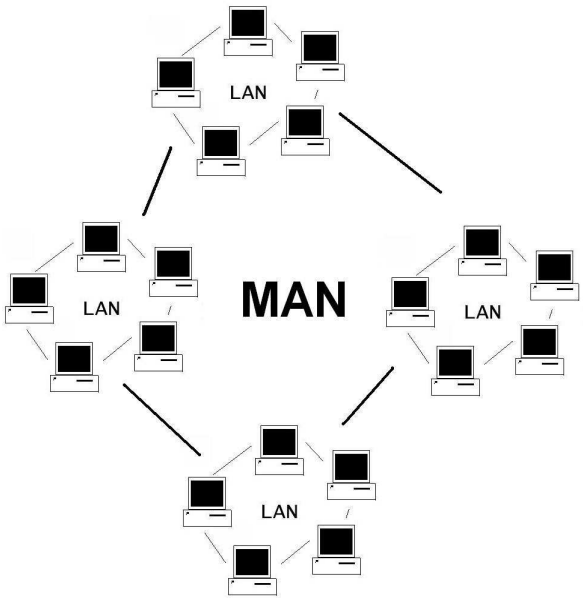
WAN – Rozlehlá počítačová síť. S růstem geografického dosahu sítí, připojováním uživatelů v různých městech nebo zemích přerůstají sítě LAN a MAN do tzv. sítě WAN. Tyto sítě slouží především pro přenosy a propojení na vzdálenosti několika stovek až tisíců kilometrů. Obecně lze tedy o síti typu WAN mluvit jako o prostředku pro spojení několika LAN, MAN nebo dalších typů sítí a to tak, aby uživatelé z různých míst mohli spolu vzájemně a bezproblémově komunikovat.

Do této kategorie spadá celá řada sítí, které svojí rozlohou pokrývají takřka celý svět. Není možné všechny tyto sítě vyjmenovat, ale asi každý z nás si vybaví nejznámější, nejkomplikovanější a nejrozsáhlejší síť typu WAN a tou je síť Internet.

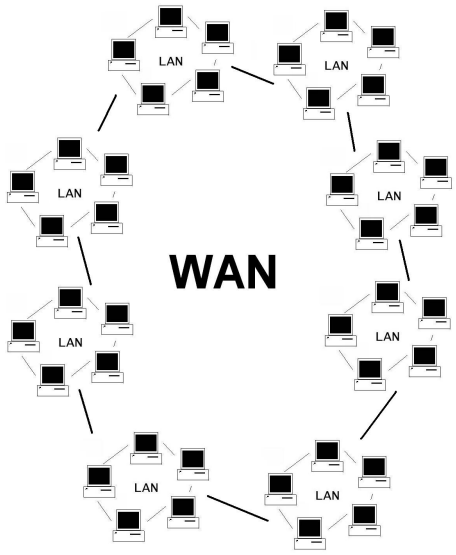
Obrázek č. 4 – Lokální počítačová síť



Obrázek č. 5 – Metropolitní počítačová síť



Obrázek č. 6 – Rozlehlá počítačová síť



3.3 Dělení sítí podle topologie

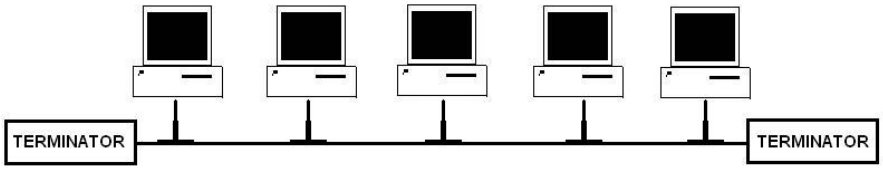
Další možností, jak lze počítačové sítě rozdělit, je jejich rozdělení podle fyzického uspořádání. Toto fyzické uspořádání se nazývá topologie, a proto se následující rozdělení nazývá rozdělování sítí podle topologie. Při nahlížení na sítě z hlediska topologie zcela ignorujeme, na jakém prostoru se sítě rozkládají, ale zajímá nás pouze způsob, jímž jsou jednotlivé části sítě vzájemně propojeny. Zajímá nás tedy plošná případně prostorová struktura sítě.

Z tohoto hlediska rozlišujeme celkem 3 základní druhy topologií – *sběrnicová, kruhová a hvězdicová*. Kombinací těchto základních druhů pak lze vytvořit další typy topologií [6].

Topologie sběrnicová – někdy též nazývaná lineární. Jedná se o první a nejjednodušší způsob, kterým byly vzájemně propojovány počítače, aby vytvořily počítačovou síť. I když je tato metoda nejjednodušší, patřila mezi nejvíce užívané a to především díky své jednoduchosti. V praxi se v podstatě jedná o jediný, dlouhý, celistvý kabel nazývaný hlavní kabel nebo též páteř, který je na obou stranách zakončen tzv. terminátorem. K tomuto kabelu jsou pak vhodným způsobem připojeny všechny počítače v síti. K připojení počítačů se nejčastěji používá tzv. T-spojek. Komunikace v síti je realizována pomocí elektrických signálů a to tak, že data jsou

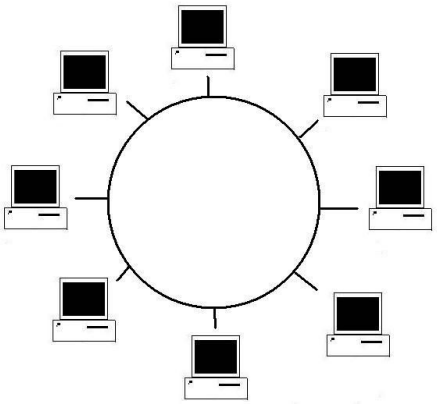
odvysílána všem počítačům, které jsou v síti připojené, nicméně informaci přijme pouze ten počítač, jehož adresa odpovídá adrese zakódované v počátečním signálu. Z toho vyplývá, že v daný okamžik může zprávy odesílat vždy pouze jeden počítač a ostatní musí čekat. Protože data neboli elektrický signál, jsou posílána po celé síti, cestují z jednoho konce kabelu na druhý. Kdyby mohl signál pokračovat bez přerušení, neustále by se vracel tam a zpět podél kabelu a zabránil by tak ostatním počítačům v odesílání jejich signálů. Proto je potřeba signál, který měl možnost dosáhnout cílové adresy, zastavit. Z toho důvodu je v síti umístěn terminátor, což je vlastně odpor s hodnotou odpovídající charakteristické impedanci vedení, který volné signály pohlcuje, linku čistí a umožňuje tak komunikaci dalším strojům [6].

Obrázek č. 7 – Sběrnicová topologie



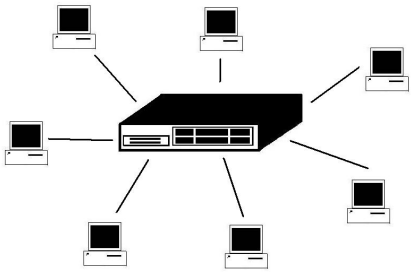
Topologie kruhová – někdy též nazývaná prstencová. Jedná se o další druh topologie, která v podstatě vznikne z topologie sběrnicové tím způsobem, že se spojí volné konce hlavního kabelu a vznikne tak pomyslný kruh. V praxi to znamená, že prstencová topologie propojuje počítače pomocí jediného kabelu do jediného okruhu a to tak, že každý počítač připojený do této sítě je přímo spojen s předchozím a následujícím počítačem. V síti neexistuje žádné zakončení, jako je tomu u sběrnicové topologie. Komunikace v síti probíhá tak, že pokud nějaký počítač začne vysílat a odešle zprávu, tato zpráva je pak zpracovávána každým počítačem v kruhu. Pokud počítač, který aktuálně vysílání zpracovává, není adresátem zprávy, předá ji dalšímu uzlu, až zpráva doputuje ke svému adresátovi. Vysílání se může v kruhové topologii šířit pouze jedním směrem a na rozdíl od sběrnicové topologie, kde se zpráva při průchodu uzlem nijak nemění, dochází zde k tomu, že každý uzel funguje zároveň jako zesilovač. Proto se tato topologie někdy označuje jako aktivní a topologie sběrnicová se označuje jako pasivní [6].

Obrázek č. 8 – Kruhová topologie



Hvězdicová topologie – jedná se dnes o nejpoužívanější a zároveň vývojově nejmladší topologii, kdy vzájemné propojení počítačů tvarem připomíná hvězdu. V praxi je síť sestavená pomocí této topologie realizována tak, že v celé síti existuje jeden centrální prvek, který se nazývá hub nebo switch. K tomuto prvku jsou pak nejčastěji pomocí strukturované kabeláže připojeny všechny pracovní stanice, servery a další síťová zařízení tak, že mezi dvěma prvky sítě existuje vždy jen jedna cesta. Komunikace v síti probíhá tak, že pokud kterýkoliv připojený počítač začne vysílat, tak se jeho vysílání přenáší přes centrální prvek sítě do všech ostatních připojených zařízení. V danou chvíli může vysílat několik počítačů zároveň, což klade velké nároky na centrální prvek a je nutné ho vhodně dimenzovat [6].

Obrázek č. 9 – Hvězdicová topologie



3.4 Dělení sítí podle použité technologie

Posledním rozdělením sítí, o kterém se ve své práci budu zmiňovat, je rozdělení sítí podle technologie, která je při jejím budování použita. Díky tomuto náhledu lze rozlišit dva typy sítí. Prvním typem jsou sítě rádiové, druhým typem jsou sítě metalické.

Pod souhrnným názvem rádiové sítě se skrývá množství technologií, které přenáší data bezdrátovou formou. Jednou, z nich dnes nejznámější je technologie Wi-Fi. Samotný pojem Wi-Fi poprvé zavedla skupina WECA, která se v roce 2000 přejmenovala na WiFi alianci. Tato organizace se starala a neustále stará o testování kompatibility jednotlivých zařízení. Při schválení zařízení je mu touto skupinou propůjčeno logo Wi-Fi a je možné jej provozovat. Pod pojmem Wi-Fi se tedy skrývá bezdrátová komunikace v licencovaném nebo bezlicenčním pásmu. Tato technologie nabízí řadu výhod, ale i několik nevýhod. Největší z pozitiv je možnost snadno a rychle vytvořit síť bez nutnosti pokládání kabeláže. Největší z negativ je fakt, že přenosová rychlost je nižší a zároveň dochází ke vzájemnému rušení blízkých bezdrátových sítí [7].

Druhým typem jsou sítě metalické. Tento druh sítí je v podstatě protikladem k sítím rádiovým. Jedná se o vývojově starší druh datových sítí. Tento typ sítí je stále velmi rozšířený, protože se stále jedná o nejvýhodnější poměr cena a přenosová rychlost. Nejznámějším typem těchto sítí jsou sítě typu Ethernet. Ethernet vznikl v roce 1973 ve výzkumném ústavu PARC společnosti Xerox s počáteční přenosovou rychlostí 2,94 Mb/s. Od doby zrodu však prošel Ethernet bouřlivým vývojem. Dnes se odhaduje, že více než 80 % sítí LAN je vybudováno na tomto typu sítě. V současnosti se však Ethernet uplatňuje i na poli metropolitních sítí. Je standardizován skupinou standardů IEEE 802.3*, kde * rozlišuje specifikace pro různé rychlosti. Existuje široká škála standardů pro různé rychlosti a určité typy vedení. Mezi hlavní výhody Ethernetu se řadí široká podpora od výrobců, nízká cena zařízení, snadné nasazení sítě a její údržba, snadná konfigurovatelnost [3].

Protože ne vždy je možné vytvořit celou síť pouze použitím jediné technologie, je výhodné obě technologie v sítí kombinovat.

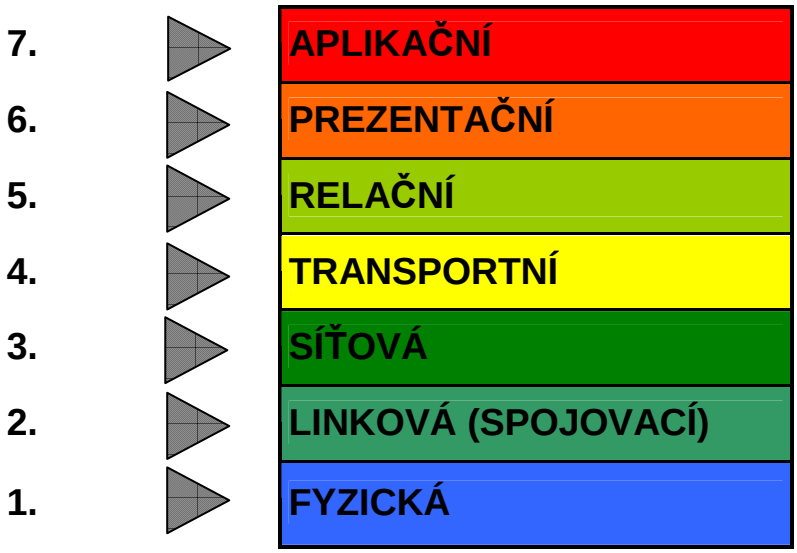
3.5 Model ISO/OSI

Při stavbě počítačové sítě se velmi často pracuje s pojmem *„Referenční model ISO/OSI“*, proto je nutné si tento pojem charakterizovat.

V každé počítačové síti probíhá mezi propojenými uzly určitá vzájemná datová komunikace. Při této datové komunikaci si však všechna hovořící zařízení musí vzájemně „rozumět“ a musí se shodnout na nějaké společné sadě pravidel při komunikaci tzv. protokolu a ten pak dodržovat. Díky tomuto protokolu je pak možné zprávy v sítí odesílat i přijímat. A právě z těchto důvodů byl stanoven referenční model OSI. Referenční model ISO/OSI vypracovala organizace ISO jako hlavní část snahy o standardizaci počítačových sítí a v roce 1984 ho přijala jako mezinárodní normu ISO 7498. Základním účelem tohoto modelu je definovat a seskupit logické funkce informačního toku. Tyto funkce byly seskupeny do sedmi vrstev. Každá vrstva tedy zastupuje skupinu souvisejících logických funkcí. Model definuje celkovou funkci každé vrstvy a její vztah s vyššími a nižšími vrstvami. Tento model vytváří strukturu, ale nedefinuje metody komunikace. Ty obstarávají komunikační protokoly, které definují pravidla, podle nichž se informace v síťových systémech vyměňují [6].

Celý tento model je pak možné reprezentovat pomocí následujícího diagramu:

Obrázek č. 10 – Referenční model ISO/OSI



Celý model ISO/OSI má celkem sedm vrstev. V této části práce si ve stručnosti popíšeme funkce každé z nich.

3.5.1 Fyzická vrstva

Fyzická vrstva je nejnižší vrstvou modelu a zabývá se tedy vlastním přenosem informace prostřednictvím elektromagnetického signálu. Je to vlastně fyzické rozhraní mezi všemi zařízeními v datové síti. Důležité parametry této vrstvy, které je nutné sledovat, jsou především parametry mechanické, elektrické a funkční [3].

3.5.2 Linková vrstva

Tato vrstva je v modelu ISO/OSI nadřazena pouze vrstvě fyzické, jejíchž služeb také využívá. Vrstva zajišťuje síťové služby, které jsou nezbytné pro komunikaci několika sousedních uzlů datové sítě. Přenášená data pak řadí do větších celků, které nazýváme rámce. Tato vrstva nijak nerozlišuje jednotlivé bity přenášené informace, stará se pouze o vlastní přenos. O další rozlišení se pak starají až další vrstvy [3].

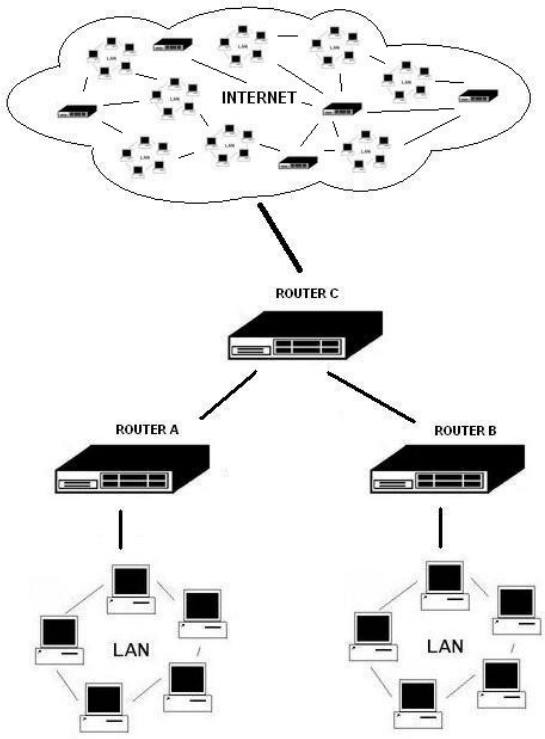
3.5.3 Síťová vrstva

Třetí vrstvou modelu je vrstva síťová. Hlavním úkolem této vrstvy je za využití svých podřazených vrstev umožnit přenos dat i mezi uzly, které spolu přímo nesousedí. Jinými slovy lze říct, že se tato vrstva stará o směrování dat v sítích. Protože vrstva má na starost směrování, je nutné, aby síťová vrstva měla alespoň základní informace o topologii celé sítě, aby mohla zvolit správný „směr“ pro odesílané pakety. Základní informace, které mají zařízení pracující na síťové vrstvě, se nazývají směrovací tabulky. Směrování v síti může být dvojího druhu - statické a dynamické [3].

Směrování statické. Při tomto směrování zůstává směrovací tabulka po celou dobu beze změny, je pevně dána konfigurací počítače nebo jiného síťového zařízení. Pokud chceme záznamy ve směrovací tabulce nějakým způsobem modifikovat, je nutné to vždy provést ručně. Ve staticky dané směrovací tabulce se zpravidla nacházejí pouze dva záznamy. Prvním záznamem je adresa brány sítě a druhý záznam je informace o tom, jak doručovat data pro uzly ze stejné podsítě. Tyto

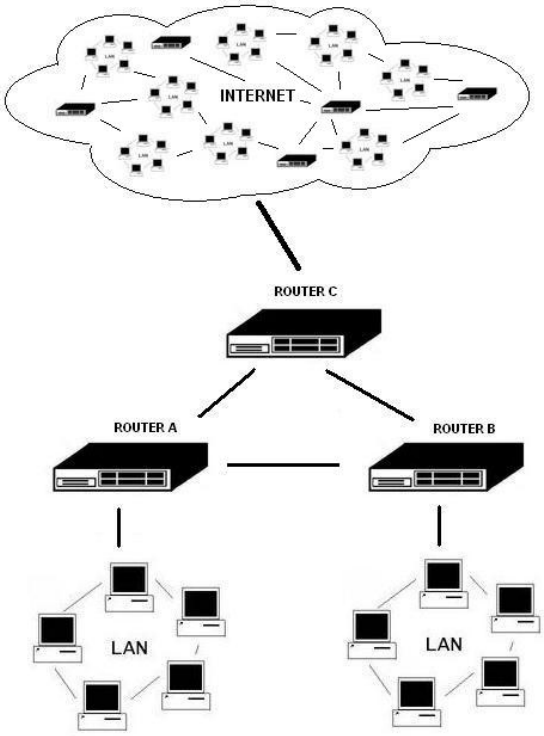
informace se nastavují buď manuálně, nebo automaticky přes tzv. DHCP server. Pokud nedojde k významné modifikaci topologie sítě, není nutné tyto záznamy po celou dobu provozu uzlu nijak upravovat [8].

Obrázek č. 11 – Statické směrování v sítích



Dynamické směrování. Jedná se o druhý typ směrování, který tato vrstva může realizovat. Tento druh směrování se někdy také nazývá adaptivní a to proto, že směrovací tabulky připojených uzlů sítě dokáží měnit své záznamy a tím pádem dokáží dynamicky reagovat na změny provedené v topologii sítě. Dynamické směrování se zpravidla používá pro rozlehlé sítě, v nichž si směrovací uzly pravidelně vyměňují směrovací informace. Na základě této pravidelné komunikaci a výměně informací mezi uzly pak dochází k aktualizaci směrovacích tabulek u směrovacích uzlů a díky tomu získávají uzly přehled o celkové topologii sítě. To jim pak umožňuje vybrat nejvhodnější cestu, přes kterou odešlou data. Tato vzájemná komunikace směrovacích uzlů sice nepatrně zatěžuje celou síť, ale výhody z toho plynoucí dalekosáhle předčí tuto skutečnost. Dynamické směrování zajišťují tzv. směrovací protokoly. Mezi nejznámější a nejpoužívanější protokoly patří především: OSPF, BGP, RIP, apod. [8].

Obrázek č. 12 – Dynamické směrování v sítích



V předcházejících odstavcích jsem nastínil základní rozdělení směrování v sítích a podrobněji se mu již nebudu věnovat. Bližší informace o této problematice lze pak najít na webu a specializované literatuře.

Dalším úkolem této vrstvy ještě je zajištění předávání paketů až do koncového uzlu. Tato vrstva koncové uzly identifikuje jako celky na základě tzv. IP adresy. V souvislosti s tím tak ještě vrstva plní úkoly, které mají předejít zahlcení jedné části sítě a umožňují co nejrovnoměrnější využívání všech přenosových kapacit sítě [3].

3.5.4 Transportní vrstva

Transportní vrstva je v modelu ISO/OSI zařazena jako čtvrtá. Díky jejímu zařazení ji můžeme považovat za jakousi vyvažovací a přizpůsobovací vrstvu mezi třemi nižšími vrstvami, které jsou orientovány na přenos dat a mezi třemi vrstvami vyššími, které jsou orientovány větší měrou na aplikace a jejich podporu. Další funkcí této vrstvy je zabezpečení bezchybnosti a úplnosti přenosu zprávy. Výše uvedený údaj však není jediné specifikum této vrstvy. Další důležitá změna proti nižším vrstvám je ta, že tato vrstva již na přenášená data nenahlíží jako na dále nedělitelný

ucelený blok, ale v rámci uzlu již rozlišuje jednotlivé procesy. Toto rozlišení se děje na základě tzv. portů, kdy většina služeb má svůj standardní, vyhrazený port [9].

Na závěr předkládám výčet několika málo síťových služeb a typických portů, na nichž jsou tyto služby provozovány. Kompletní přehled o všech portech lze najít na adrese http://www.iana.org/assignments/port-numbers.

Obrázek č. 13 – Síťové služby a jejich porty

Název síťové služby	Číslo přiřazeného portu
FTP	***20 nebo 21***
SSH	***22***
Telnet	***23***
SMTP	***25***
DNS	***53***
HTTP	***80***
NTP	***123***
HTTPS	***443***
SIP	***5060***

3.5.5 Relační vrstva

Jedná se o pátou vrstvu celkového modelu. Ostatní čtyři nižší vrstvy modelu jsou zaměřeny především na vlastní přenos dat mezi jednotlivými uzly sítě, ale tato vrstva řeší hlavně problémy spojené se zajištěním správného vedení dialogů komunikujících aplikační procesů. Vrstva realizuje navazování, udržování a rušení relací. Definuje typ komunikace a zavádí synchronizační body do přenášené zprávy pro možné pokračování v přenosu v případě rozpadu a obnovy spojení [3].

3.5.6 Prezentační vrstva

Pět nejnižších vrstev referenčního modelu ISO/OSI dělá vše pro to, aby přenášená data vždy dorazila ke svému koncovému příjemci přesně v takové

podobě, v jaké byla vyslána. Stejná "podoba" však ještě nezaručuje, že pro příjemce nebudou jedna a tatáž data představovat něco jiného, než pro jejich odesilatele [9].

Tato vrstva tedy slouží k tomu, aby upravila přenášená data do tvaru, který je srozumitelný oběma komunikujícím stranám.

3.5.7 Aplikační vrstva

Poslední, nejvyšší vrstvou modelu ISO/OSI je vrstva aplikační. Úkolem této vrstvy je implementovat protokoly tvořící základ konkrétních aplikací. Definuje způsob, jakým komunikují se sítí různé aplikace. Používá služby nižších vrstev a díky tomu je izolována od problémů síťových technických prostředků [9].

3.6 Model TCP/IP

Z ISO/OSI vychází i rodina protokolů TCP/IP. Tento protokol původně vznikl jako komunikační protokol ministerstva obrany USA pro sjednocení komunikace vládních počítačů v počítačové síti ARPANET. Slouží ke komunikaci především v heterogenních sítích a je součástí prakticky všech operačních systémů. Používá se i pro komunikaci v síti Internet. Proto jeho význam neustále stoupá [10].

Model TCP/IP je zcela nezávislý na přenosovém médiu a je uplatňován jak v LAN, tak i ve WAN. Jeho filozofie se liší od modelu ISO/OSI. Tento rozdíl plyne především z rozdílných výchozích předpokladů a postojů jeho tvůrců. Tvůrci totiž vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků nikoliv celé sítě. Díky této myšlence se ušetří část přenosové kapacity v síti a tuto naspořenou část pak bude možné využít pro vlastní datový přenos [10].

Rodina protokolů TCP/IP předpokládá existenci čtyř vrstev: aplikační, transportní, síťové a vrstvy síťového rozhraní.

3.6.1 Vrstva síťového rozhraní

Jedná se o nejnižší vrstvu modelu. Tato vrstva zajišťuje vysílání a příjem paketů, které buď ze sítě odchází, nebo do ní vstupují. Tato vrstva je závislá pouze na přenosovém médiu [9].

3.6.2 Síťová vrstva

V modelu TCP/IP je tato vrstva zařazena jako druhá nejnižší. Její úkol je stejný jako v modelu ISO/OSI. Jejím hlavním úkolem je totiž zajistit, aby se pakety dostaly od odesílatele až ke skutečnému příjemci, i přes případné směrovače [9].

3.6.3 Transportní vrstva

Úkolem této v pořadí třetí vrstvy je zajištění přenosu mezi dvěma koncovými účastníky. V případě TCP/IP jsou těmito účastníky přímo programy. Podle nároků a potřeb těchto programů pak tato vrstva může regulovat tok dat v síti. Dále tato vrstva řeší zajištění spolehlivosti celého přenosu [9].

3.6.4 Aplikační vrstva

Nejvyšším bodem modelu je právě tato vrstva. Jejími entitami jsou jednotlivé aplikační programy. Tyto programy přímo komunikují s transportní vrstvou. Další prezentační a relační služby, které jsou v modelu ISO/OSI zajišťovány samostatnými vrstvami, si zde musí jednotlivé aplikace zajistit v případě nutnosti sami [10].

4. Síťový hardware

Každá počítačová síť se skládá z nějakých částí. Každá z těchto částí má v sítí svůj úkol. Některé části sítě data pouze přenáší, ale nijak je nemění. Těmto součástkám se říká pasivní části sítí. V praxi se jedná především o síťovou kabeláž. Jiné části sítě s daty aktivně pracují, mění je a směrují. Tyto součástky se hromadně označují pojmem aktivní části sítě. V praxi jsou to především huby, switche nebo routery.

4.1 Aktivní prvky

Na úvod této kapitoly je třeba si nejdříve definovat pojem aktivní prvek počítačové sítě: *„Aktivní prvek lokální počítačové sítě je zařízení, které vzájemně propojuje všechny komponenty počítačové sítě uvnitř budovy nebo areálu, jako jsou počítače, servery, tiskárny, IP telefony apod.“* [11].

Jako jedna z nejdůležitějších, ne-li vůbec nejdůležitější část každé počítačové sítě jsou aktivní prvky. Jejich výběr musí splňovat velké množství kritérií. Jedná se především o kritéria, jejichž splnění umožňuje to, aby budovaná síť byla schopna plnit všechny požadované služby a funkce, které její tvůrce zamýšlí v budoucnu provozovat. Mezi tato kritéria řadíme zejména požadavky na dostatečnou propustnost sítě, vhodně zvolenou síťovou topologii a dostatečnou rychlost komunikace uvnitř celé sítě. S těmito požadavky jde ruku v ruce i požadavek na její odolnost proti výpadkům a poruchám.

Správný návrh počítačové sítě musí zohledňovat všechna tato kritéria a teprve po jejich zvážení lze rozhodnout jaké konkrétní aktivní prvky v síti použít. Cenové hledisko se dnes samozřejmě zohledňuje, ale nemůže být hlavním kritériem pro správný výběr a návrh. V dnešní době je k odstání velké množství nejrůznějších aktivních prvků od mnoha výrobců, které lze podle jejich funkce rozdělit do třech kategorií – rozbočovače, přepínače a směrovače. Všechna tato zařízení je nutné aktivně napájet z elektrické sítě.

4.1.1 Rozbočovače

Rozbočovače, někdy také označovány jako Ethernetové Huby, případně pouze Huby, se používají v sítích, které nejsou příliš rozsáhlé nebo tam, kde je třeba

rozšířit stávající možný počet připojených pracovních stanic. Jednotlivé počítače se připojují na rozbočovač pomocí kabelu typu Ethernet a data, která se odesílají z jednoho počítače do druhého, procházejí přes rozbočovač. Rozbočovač však neumí identifikovat zdroj nebo určený cíl těchto dat, proto je rozešle všem připojeným počítačům včetně toho, který informace odeslal. Rozbočovač může odesílat a přijímat informace, ale nemůže dělat oboje zároveň. V jednom okamžiku je přenos signálu zprostředkován pouze pro jeden počítač vysílající a jeden přijímající. Ostatní stanice proto musejí čekat na uvolnění přenosového kanálu. Průměrná průchodnost informací přes rozbočovač je tedy dána rychlostí přenosu dělenému počtem připojených stanic. Vzhledem ke zmíněným poznatkům je jasné, že rozbočovače naleznou uplatnění především v sítích, kde nedochází příliš často k jejímu velkému zatížení. Tomu odpovídá i cena, která je velmi nízká [12].

Celkově lze rozbočovače popsat jako nejpomalejší, nejjednodušší a nejlevnější z aktivních prvků.

4.1.2 Přepínače

Přepínače, někdy také označovány jako Ethernetové Switche případně pouze Switche, se používají tam, kde je již nasazení hubů nedostačující. Jedná se hlavně o místa, ve kterých dochází k vysokému zatížení sítě. Přepínače pracují stejným způsobem jako rozbočovače, ovšem jejich podstatné vylepšení spočívá v tom, že umí identifikovat určený cíl přijatých dat. Díky tomu odesílají informace pouze počítačům, které je mají přijmout. Tím nedochází ke zbytečnému zatížení ostatních portů přepínače. Díky tomu jsou tyto porty volné pro současnou komunikaci jiných dvou uzlů sítě. Dalším podstatným vylepšením oproti hubům je fakt, že přepínače jsou schopny odesílat a přijímat data zároveň [12].

Souhrnně lze přepínače označit jako technologicky vylepšené nástupce zastaralých hubů. V poslední době nacházejí stále vyšší uplatnění zařízení, které v sobě slučují funkci přepínačů a směrovačů.

4.1.3 Směrovače

Směrovače, jinými slovy též Ethernetové Routery nebo pouze Routery, pracují podobně jako přepínače. Základem jejich činnosti je schopnost identifikovat příjemce dat a tato data mu posléze přímo odeslat. Rozdíl je v tom, že identifikování se neděje

pouze v rámci jedné sítě, ale dochází ke směrování dat mezi různými sítěmi. Směrovače tedy slouží jako vstupní brány do sítí a zároveň mezi nimi tvoří určité rozhraní. Směrovače mohou být jak kabelové, tak i bezdrátové. Typickým příkladem je směrování dat mezi domácí LAN sítí a sítí Internet [12].

Souhrnně lze tedy říct, že směrovače se co do funkčnosti řadí na přední místa mezi aktivními síťovými prvky a to především proto, že v sobě kombinují několik funkcí. Směrovače jsou cenově nejdražší ze zmiňovaných síťových prvků, ale jejich nasazení je nejuniverzálnější.

4.2 Pasivní prvky

Vzájemně izolované aktivní prvky by počítačovou síť nemohly vytvořit. Z tohoto důvodu se do sítí musí začlenit pasivní síťové prvky, které plní především funkci spojovací a přenosovou. Tím doplňují huby, switche, routery a spolu s nimi tvoří jeden celek s názvem počítačová síť. Jsou to prvky, které data pouze přenáší, ale nemění je. Také umožňují připojení aktivních prvků. Z předchozího odstavce vyplývá, že se jedná především o kabely a přípojná místa aktivních prvků nebo klientských stanic. Žádnou z těchto komponent není nutné připojovat k elektrické síti.

Obrázek č. 14 – Druhy síťových kabelů [13]

- koaxiální kabel

- tenký koaxiální kabel

- tlustý koaxiální kabel

- kroucená dvoulinka

- stíněná

- nestíněná

- optické kabely

- jednovidové

- mnohovidové

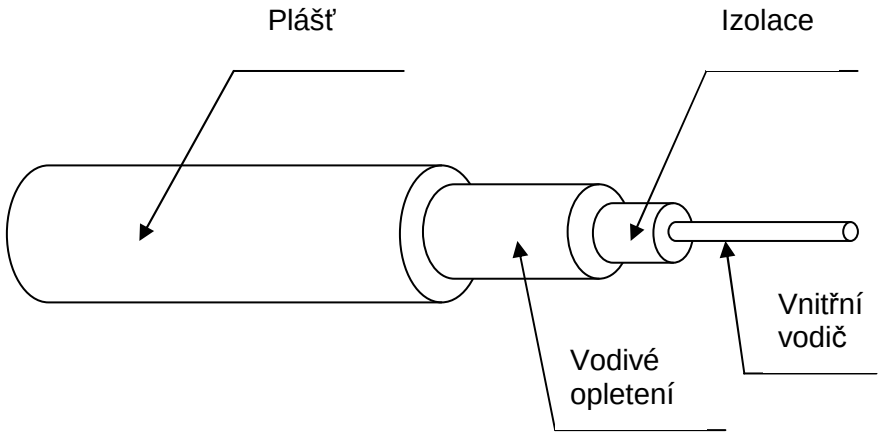
V předchozí tabulce jsem uceleně sepsal všechny doposud používané propojovací kabely datových sítí. Pro výstavby moderních počítačových sítí se dnes využívají převážně kroucené dvoulinky (UTP) nebo optické kabely.

4.2.1 Koaxiální kabel

Koaxiální kabely byly první hromadně využívané kabely, které velkou měrou přispěly k rozvoji počítačových sítí, především pak Ethernetu. Koaxiální kabely patří do kategorie přenosových médií drátového typu. Toto označení získaly díky svému konstrukčnímu provedení. Tento kabel totiž přenáší elektrické signály pomocí dvojice vodičů. Každý vodič z této dvojice plní speciální funkci. První z dvojice je tvořen silným, nejčastěji měděným drátem a je veden středem celého kabelu. Druhý vodič je tvořen složitou, vodivou sítí, která je vedena okolo prostředního vodiče a zajišťuje odolnost kabelu vůči vnějšímu rušení. Samotný přenášený signál je přitom reprezentován napětím mezi oběma vodiči. Důležitým parametrem každého koaxiálního kabelu, která vyjadřuje jak velký odpor klade kabel procházejícímu proudu. Ve světě počítačů se používají nejčastěji koaxiální kabely s impedancí 50 Ohmů. Postupným vývojem vznikly dva druhy koaxiálních kabelů, které se označují jako „tlustý" a „tenký". Tyto kabely se liší pouze ve svém průměru [13].

Koaxiální kabely sehrály velmi významnou roli při budování počítačových sítí, zejména těch lokálních. Byly relativně levné, vcelku nenáročné na manipulaci, a také dosti odolné. V praxi je stále možné se s těmito kabely setkat, a to především ve starších, doposud provozovaných sítích. Pro budování nových lokálních sítí se však koaxiální kabely používají již jen zcela výjimečně - dnes jednoznačně převládá tzv. kroucená dvoulinka [9].

Obrázek č. 15 – Struktura koaxiálního kabelu



4.2.2 Kroucená dvoulinka

Kroucená dvoulinka spolu s optickým vláknem zaujímají čelní příčky při budování počítačových sítí. V rámci LAN stále převažuje využití kroucené dvoulinky. Označení tohoto kabelu je odvozeno od jeho struktury. Tato struktura je tvořena dvojicemi vodičů, které jsou po celé své délce pravidelně zakrouceny. Nakonec jsou do sebe zakrouceny i tyto dvojice. Každý z dvojice vodičů má prakticky rovnocenné postavení [14].

Kroucená dvoulinka se vyrábí ve dvou provedeních. Prvním z nich je tzv. stíněné provedení. V tom provedení jsou všechny vodiče opatřeny ještě vodivým obalem, který slouží k dokonalejšímu odizolování kabelu od možného okolního elektromagnetického rušení. Druhým typem je tzv. nestíněné provedení, které plní stejnou funkci jako stíněné. Rozdíl je v tom, že u tohoto provedení neexistuje žádný vodivý obal. Stíněný kabel je primárně určen do míst, kde je nutná vysoká odolnost. Nestíněný kabel je určen pro nenáročnější instalace, a to především uvnitř budov [15].

Díky tomu, že jsou obě provedení konstrukčně odlišná, je odlišná i jejich cena. UTP provedení je levnější, a proto je i více rozšířené. V běžném prostředí se používá téměř výlučně, zatímco s dražší stíněnou dvoulinkou se lze setkat spíše výjimečně a to především tam, kde je velmi silné či velmi citlivé „elektromagnetické okolí", velmi přísné hygienické předpisy apod.

Kromě rozdílu v existenci či neexistenci stínění se oba druhy kroucené dvojlinky liší i v tom, jak rychlý přenos dat jsou schopny realizovat. Dříve se používalo takové provedení kroucené dvoulinky, které „sneslo" přenosy dat rychlostí 10 megabitů za sekundu. Dnes se tento druh kroucené dvoulinky označuje jako „kategorie 3", ale v běžné praxi se již používá téměř výlučně dvoulinka kategorie 5. Tato kategorie totiž „snáší" přenosy rychlostí 100 Mbps, které jsou potřebné pro dnešní vysokorychlostní přenosové technologie.

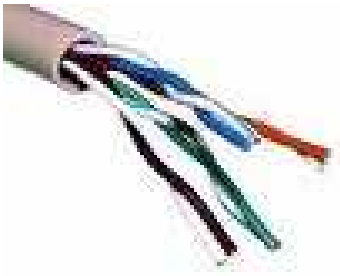
Dříve se používala hlavně topologie sběrnicová, ale s nástupem kroucené dvoulinky se to změnilo. Na rozdíl od koaxiálního kabelu totiž není možné na kroucené lince jednoduše udělat odbočku. Kroucená dvoulinka se totiž výhradně využívá pro vytváření spojů typu bod – bod o maximální vzdálenosti mezi koncovými uzly 100 m. Tento vzniklý problém byl nakonec vyřešen pomocí elektronického přídavného zařízení zvaného rozbočovač. Díky tomuto zařízení se doposud

využívaná sběrnicová topologie plynule změnila na dnes nejrozšířenější hvězdicovou topologii. S postupným vývojem počítačových sítí docházelo i k postupnému vývoji a vylepšování přenosových kabelů. V následující tabulce jsou uvedeny jednotlivé typy kroucené dvoulinky:

Obrázek č. 16 – Kategorie kroucené dvoulinky [16]

Kategorie 1: *Tento typ není určen k datovým přenosům. Používá se pouze k telefonním rozvodům. Jeho přenosová rychlost je maximálně do 1 Mbit/s* [16].
Kategorie 2: *Určen pro přenos dat, s maximální šířkou pásma 1,5 MHz. Používá se pro digitální přenos zvuku. Jeho přenosová rychlost je přibližně 4 Mbit/s* [16].
Kategorie 3: *Tato kategorie je určena pro přenos dat a hlasu s šířkou pásma 16 MHz. Její přenosová rychlost je do 10 Mbit/s* [16].
Kategorie 4: *Tato kategorie je určen pro přenos dat s šířkou pásma 20 MHz. Její přenosová rychlostí je do 16 Mbit/s* [16].
Kategorie 5: *Pracuje v šířce pásma do 100 MHz. Používá se pro počítačové sítě s přenosovou rychlostí 100 Mbit/s nebo 1 Gbit/s v případě využití všech 8 vláken. V současné době je nahrazena standardem kategorie 5E* [16].
Kategorie 5E: *Pracuje rovněž v šířce pásma do 100 MHz. Cílem této kategorie je dosáhnout přenosové rychlosti 1 Gbit/s* [16].
Kategorie 6: *Pracuje s šířkou pásma 250 MHz. Využívá se pro ultrarychlé páteřní aplikace v oblasti lokálních sítí* [16].

Obrázek č. 17 – Kroucená dvoulinka [16]



4.2.3 Optický kabel

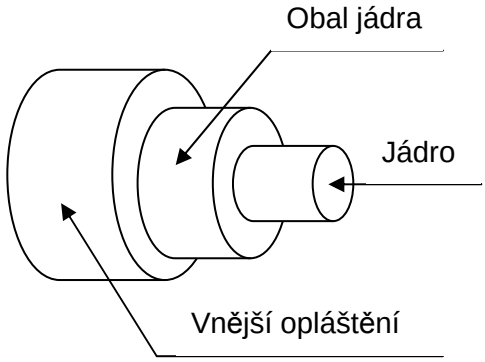
Posledním a nejmodernějším typem kabeláže je využití optických kabelů. Tato technologie se využívá především při budování MAN nebo WAN. Při tvorbě LAN stále převažuje využívání kroucené dvoulinky.

Pod pojmem optický kabel se skrývá skleněný nebo také plastový kabel, který je schopen přenášet data za pomoci světelného paprsku v něm šířeného. Pomocí této technologie je možné přenášet velké objemy dat velkou rychlostí a v relativně krátkém časovém úseku. Při přenosu dat nedochází prakticky k žádným ztrátám. Díky tomu je možné přenášet signály na větší vzdálenosti. Další výhodou tohoto druhu přenosu je vysoká odolnost vůči okolnímu elektromagnetickému rušení [17].

Princip, na kterém je tato technologie založena, je následující: Na začátku každého optického kabelu je umístěn tzv. generátor - zdroj světla. Tímto generátorem může být buď obyčejná elektroluminiscenční dioda (LED), nebo laserová dioda. Tyto diody vytvářejí světelné pulzy. Tyto pulzy vznikají na základě přivedeného elektrického proudu a šíří se kabelem. Na konci kabelu je umístěn tzv. detektor světla, který tyto signály zachytává a převádí je zpět na elektrické signály. Tyto elektrické signály jsou určené k dalšímu šíření. Jako detektor se nejčastěji používá fotodioda. Mezi generátorem a detektorem je vedeno vlastní přenosové médium – optické vlákno. Signál se optickým vláknem šíří díky jeho fyzikálním vlastnostem. Nejdůležitější je jeho odraz. Při odrazu se využívá fyzikálního zákona: *"Dopadá-li světelný paprsek na rozhraní dvou prostředí s různými optickými vlastnostmi (např. na rozhraní mezi jádrem a pláštěm), v obecném případě se část tohoto paprsku odráží zpět do původního prostředí, a část prostupuje do druhého prostředí. Záleží však na úhlu, pod jakým paprsek dopadá na rozhraní (dáno též optickými vlastnostmi obou prostředí). Je-li tento úhel větší než určitý mezní úhel, dochází k úplnému odrazu paprsku zpět do původního prostředí"* [18].

Optické vlákno musí být tomuto zákonu celé uzpůsobeno. Proto je složeno ze tří základních součástí – jádro (Core), obal jádra (Cladding) a vnější opláštění (Buffer) [19].

Obrázek č. 18 – Struktura optického vlákna

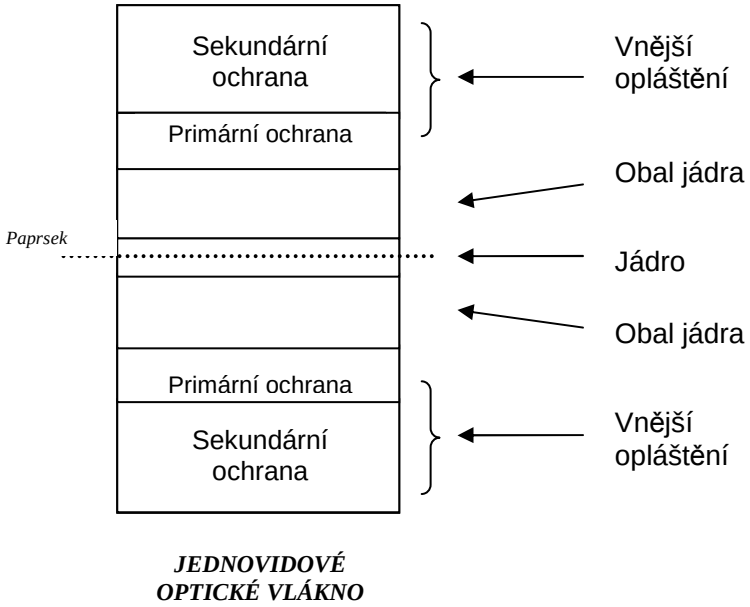


a) Jádro je nejdůležitější prvek celého optického kabelu a je určeno pro vlastní přenos dat. Jádro má průměr v řádu několika mikrometrů a je nejčastěji vyrobeno ze skla nebo z plastu. *b) Obal jádra* je v kabelu přítomen z důvodu zpevnění kabelu a poskytuje také ochranu pro jádro. *c) Vnější opláštění* slouží k prvotní ochraně optického kabelu, a to především od nepříznivých účinků okolního prostředí. Vrstva je nejčastěji tvořena tvrzeným akrylátovým lakem [19].

4.2.3.1 Jednovidové optické kabely

Jednovidové optické vlákno je z pohledu přenosu signálů kvalitnější. Tento typ kabelů bývá nasazen převážně tam, kde je nutné překonat velké vzdálenosti. Kabel je konstrukčně tvořen pouze jediným videm. Díky tomu je dosaženo velkého úhlu odrazu paprsku v jádře, minimalizuje se prodloužení dráhy paprsku a přenos je kvalitnější a rychlost vyšší. Dosáhnout toho, aby v jádře mohl být pouze jeden vid, je možné díky tomu, že jádro má velice malý průměr. S tím jsou spojeny vyšší nároky na výrobu, což se promítá v koncové ceně, která je vyšší než u mnohovidových kabelů [18].

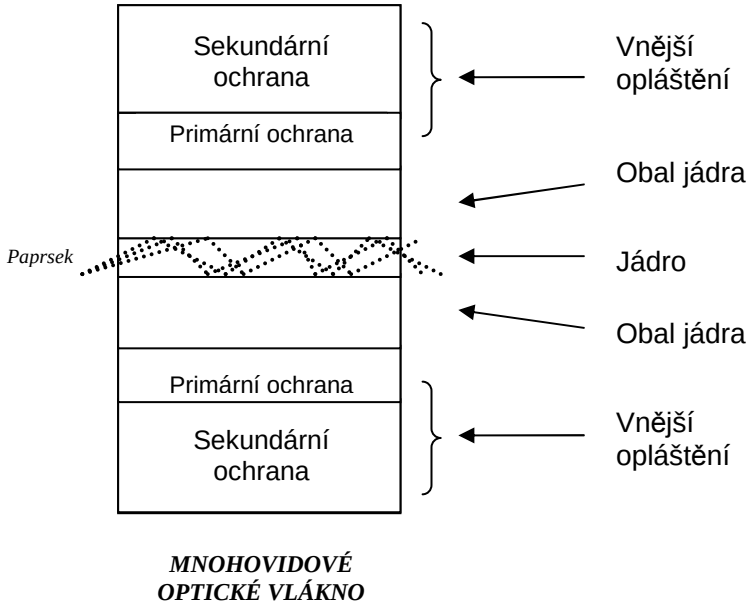
Obrázek č. 19 – Princip přenosu v jednovidovém optickém vlákně



3.2.3.2 Mnohovidové optické kabely

Mnohovidové optické vlákno je z pohledu přenosu signálu méně kvalitní. Využívá se proto tam, kde není požadována tak vysoká spolehlivost. Kabel není tvořen pouze jediným videm, ale několika vidy. Každý z těchto vidů přitom vstupuje do optického vlákna pod jiným úhlem, pod jiným úhlem se odráží a v důsledku toho prochází celým optickým vláknem od generátoru až k detektoru po jinak dlouhé dráze než ostatní vidy, a to i přesto, že byly všechny vygenerovány společně v rámci jediného světelného impulsu. Jelikož jsou jednotlivé vidy rozptýleny, dochází ke zkreslení přijímaného signálu. Proto jsou tato vlákna délkově omezena a nacházejí uplatnění především při budování malých sítí [18].

Obrázek č. 20 – Princip přenosu v mnohovidovém optickém vlákně



MNOHOVIDOVÉ OPTICKÉ VLÁKNO

Při tvorbě školní počítačové sítě prozatím převládá využívání strukturované kabeláže, protože tato kabeláž je cenově dostupnější než optická vlákna. V podmínkách školy je tato technologie prozatím plně dostačující. Věřím, že v budoucnu však bude nutné sáhnout ke kvalitnější kabeláži a postupně optická vlákna začít nasazovat.

5. Systém Unix

Systémy z rodiny Unix se dnes řadí mezi širokou škálu operačních systému, které se využívají při tvorbě a instalaci síťových serverů.

5.1 Historie

Historie operačního systému Unix, předchůdce dnešního Linux, se začala psát v roce 1965. V této době spolupracovali společnosti Bell Telephone Laboratories a General Electric na projektu „MAC of MIT“, jehož cílem bylo vytvořit operační systém Multics. Později se tato spolupráce rozpadla, když se společnost Bell Telephone Laboratories rozhodla od ní odstoupit. V důsledku toho neměla k dispozici kvalitní operační systém. Proto se zaměstnanci Bell Telephone Laboratories Ken Thompson a Dennis Ritchie rozhodli navrhnout vlastní operační systém. Díky jejich spolupráci vznikl operační systém, který byl pojmenován Unix. Původní Unix byl napsán v programovacím jazyce Asembler. Až později, v roce 1977, po vytvoření a zveřejnění programovacího jazyka C, byl celý Unix v tomto jazyce přepsán. V těchto letech nedošlo pouze k přepsání Unixu, ale došlo i k tomu, že licence na tento systém byla převedena na půdu několika univerzit. Unix se díky tomu stal populárním především v akademických kruzích, avšak postupem času se začal prosazovat i v komerční sféře. Po jeho rozšíření začalo vznikat nepřeberné množství klonů. Nejznámějšími klony jsou v dnešní době především BSD, Irix nebo Solaris. Poté vývoj Unixu na několik let ustal, až na počátku 90. let došlo k jeho opětovnému vzkříšení. V této době totiž nastal velký rozmachu Internetu, mnoho lidí potřebovalo na svém počítači, potažmo serveru, kvalitní operační systém. Těmto požadavků Unix dokonale vyhovoval. Ovšem jeho obrovskou nevýhodou byla cena. Proto vzniklo několik skupin programátorů snažících se vyvinout nový operační systém, který by byl zdarma. Mezi takto vzniklé operační systémy se řadí právě i Linux, který je dnes asi nejznámější. Duchovním otcem nově vznikajícího operačního systému Linux je finský programátor Linus Torvalds. Programátor Tornvalds je autorem prvotní verze - jádra operačního systému. Jeho původní verze však byla v průběhu následujícího desetiletí zdokonalována bezpočtem lidí na celém světě až do dnešní podoby. Vývoj systému Linux neustal ani dnes. Stále dochází k jeho zdokonalování a inovování. Snahou všech lidí, kteří se na vývoji podílejí, je přetvořit jej do podoby, v níž bude

schopný plnohodnotně konkurovat ostatním operačním systémům na trhu. Na operační systém Linux se vztahují licenční podmínky GPL (GNU General Public Licence). Tato licence se vztahuje na veškeré programové vybavení produkované nadací Free Software Foundation a jejím cílem je zabránit komukoliv omezovat distribuční práva ostatních. Jinými slovy, podle licenčních podmínek GPL si může každý účtovat za distribuci programového vybavení GNU kolik chce, ale nesmí nikomu nařizovat, za jaký poplatek je má distribuovat dál. Dále musí každý vývojář zpřístupnit zdrojové kódy vytvořených programů. Tento fakt je velmi užitečný pro ostatní vývojáře. Pak si totiž každý může modifikovat operační systém Linux podle svých potřeb a dále distribuovat tuto modifikovanou verzi – opět za předpokladu, že ji bude distribuovat podle licenčních podmínek GPL [20].

5.2 Výhody a nevýhody systému

Stejně jako každý jiný operační systém i systém Linux v sobě skrývá velké množství kladů, výhod a vylepšení, ale i několik záporů a nevýhod. Kouzlo tohoto operačního systému však spočívá v tom, že klady jednoznačně převažují nad zápory. A takto by to mělo všech dobrých operačních systémů, mezi které se Linux jednoznačně řadí, být. Mezi klady lze zařadit především jeho cenu. Pouze tato skutečnost by z něho ale nedělala to, čím je dnes. Další jeho předností je bezpečnost a stabilita při běhu. Tyto dvě vlastnosti uživatel ocení především při instalaci systému na síťový server. Díky vysoké bezpečnosti a bezproblémovosti serverového operačního systému se zvýší i bezpečnost a bezchybný chod celé sítě. Další nespornou výhodou je fakt, že Linux je možné provozovat prakticky na jakékoliv hardwarové konfiguraci počítače od nejstarších strojů až po nejvýkonnější počítače a servery dneška. Poslední vlastností, která v tomto výčtu stojí za zmínku je tzv. „programátorské uspořádání systému“. Pod tímto pojmem se skrývá skutečnost, že v Linux není žádné centrální konfigurační úložiště tzv. register, ale každý program má svůj vlastní konfigurační soubor. Někomu může toto uspořádání připadat jako nevýhoda, ale podle mého názoru je to efektivnější řešení než u jiných systémů. Stejně tak jako obdobné operační systémy, má i Linux několik záporů. Není jich však mnoho. Jako první negativum je možné zmínit absenci registru. Někteří uživatelé, kteří byli zvyklí na jiný operační systém, kde se registr nachází, s tím mohou mít ze začátku obtíže. Ruku v ruce s tímto „problémem“ jde i skutečnost, že Linux není

vyvíjen jednou osobou nebo firmou, ale širokou škálou různě smýšlejících osob. Díky tomu dochází při vývoji ke větvení a odchylkám, vzniká množství různorodého softwaru. Někteří méně zkušení nebo začínající uživatelé tím pak mohou být zmateni a zaskočeni. Jako poslední a nejvýraznější chybu bych označil neochotu některých firem a jedinců poskytnout zdrojové kódy ostatním vývojářům, což je v přímém rozporu s filozofií celého Linux.

5.3 Síťové servery

Pojmem síťový server (zkráceně server) je v informatice označován počítač, který poskytuje svoje služby jiným počítačům v síti. Nabízené služby jsou realizovány díky na serveru běžícím programům. Tyto programy jsou na různých platformách označovány různě. V Linux jsou tyto programy označovány jako démoni (anglicky daemons) [14].

Servery jako takové můžou být umístěny buď ve specializované, často klimatizované místnosti tzv. serverově, nebo mohou být umístěny volně. Umístění v serverově je po všech stránkách výhodnějším řešením, především pak u výkonných serverů. Tyto výkonné servery se nejčastěji umisťují do speciálních skříní, tzv. racků, a to především kvůli úspoře místa a také lepšímu chlazení při provozu. Podstatou každé sítě jsou služby, které tato síť svým uživatelům poskytuje. Nabízené služby jsou ve většině případů realizovány díky síťovým serverům. Správné fungování těchto služeb je tedy přímo závislé na těchto zařízeních, proto je u nich požadována vysoká spolehlivost a výkon. V důsledku těchto požadavků a stále se zvyšujícím nárokům na tato zařízení je nutné používat jak spolehlivý a dostatečně výkonný hardware, ale také vhodný software, zejména operační systém.

5.3.1 Hardware

Pojmem hardware se v informatice obecně označuje veškeré fyzicky existující technické vybavení počítače. Hardware jsou součástky počítače, bez nichž by nebyl schopen pracovat. Jsou to elektronické součástky, které jsou umístěny na základové jednotce někdy nazývané základová deska, motherboard nebo mainboard [14].

Při stavbě serveru je třeba brát na zřetel to, že když dojde k výpadku serveru, znamená to obvykle výpadek celé sítě, která je na něj napojená. Proto je vhodné při

návrhu a stavbě síťového serveru tuto skutečnost zohlednit. V praxi by ideálním řešením bylo vytvoření několika identických serverů, které by se svojí činností doplňovaly, a tím se zmenšila šance na výpadek. Toto řešení je bohužel ve většině případů nerealizovatelné, zvláště ve školním prostředí. Ve školách je ve velké většině případů nasazen pouze jediný server, který sám poskytuje všechny služby. Jelikož nejsou všechny služby stejně náročné, je nutné vybrat tu, která bude server zatěžovat nejvíce a podle ní jej pak dimenzovat. V reálném provozu několika tisíc počítačů by toto řešení bylo naprosto nevyhovující. Jelikož bude mnou navrhovaný server sloužit pouze na jedné škole a pouze pro několik desítek až stovek uživatelů, je toto řešení myslím dostačující. Je samozřejmě dobré, aby si ICT koordinátor zajistil dostatečné finanční prostředky pro stavbu více serverů a vylepšil tak chod celé sítě.

5.3.1.1 Router/firewall

Pojmem router je v informatice označováno aktivní zařízení, které procesem zvaným routování posílá data směrem k jejich cíli [14].

Pojmem firewall je v informatice označováno aktivní zařízení, které slouží k zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říci, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje [14].

Pokud tedy oba dva pojmy složíme dohromady, vznikne nám pojem router/firewall. Vždy záleží na konkrétní situaci, do níž budeme toto zařízení nasazovat. V případě sítě s několika tisíci uživateli je nutností, aby byl router/firewall dostatečně výkonný a konfigurovatelný. Je proto vhodné použít pro tento účel speciálně navržené zařízení. Toto zařízení se označuje pojmem hardwarový firewall. Pokud není možné takovéto zařízení do sítě začlenit, nabízí se možnost vytvoření dostatečně odolného firewallu pomocí speciálních programů. Tím nám vznikne druhý typ firewallu, který se označuje jako softwarový firewall. Jelikož my tvoříme server, který bude obsluhovat pouze menší množství klientů jedné školy, zvolíme při tvorbě firewallu druhou možnost. Tato možnost bude v konkrétní situaci zcela dostačující a zároveň ušetříme nemalé finanční prostředky, které bude možné využít v jiné oblasti. V našem případě bude firewall provozován na samostatném počítači. Zmenší se tím šance na průnik dovnitř sítě a zvýší se její odolnost, protože ostatní služby bude poskytovat jiné zařízení. V případě školy a předpokladu, že tento server bude

sloužit výhradně jako brána/firewall, postačí k jeho vytvoření jakékoliv starší PC, do kterého bude možné osadit minimálně dvě síťové karty.

5.3.1.2 Hlavní server

V případě hlavního serveru je situace výrazně odlišná. Tento server nebude plnit pouze jednu dedikovanou funkci, ale bude na něm spuštěno velké množství různých služeb, které bude využívat mnoho uživatelů. Proto je nutné, aby tento server byl mnohonásobně výkonnější. Při stavbě serveru si zvolíme počítač, který bude konstrukčně podobný uživatelské pracovní stanici. Při jeho sestavování budeme sledovat odlišné parametry než je tomu u obyčejné pracovní stanice. Základem serveru bude kvalitní základní deska nejlépe formátu ATX. Deska by měla umožňovat osazení množstvím nejrůznějších dodatečných komponent jako je například dostatečně kvalitní a rychlá síťová karta. V praxi bude dostačovat karta standardu 100Mbit, protože na školách se ve většině případů rychlejší sítě nevyskytují. Server bude osazen celkem dvěma síťovými kartami, které budou tvořit vstupní a výstupní rozhraní. V návrhu není nutné počítat s výkonnou grafickou kartou, ale bude dostačovat libovolná grafická karta, protože na serveru nebudou provozovány žádné graficky náročné aplikace. Rovněž zvuková karta není nutná. Výkon procesoru není na serveru rozhodujícím faktorem, proto bude postačovat libovolný starší procesor. Jako vhodný se jeví procesor Intel Pentium 3 o taktu 1Ghz. Namísto výkonného procesoru je nutné pořídit co největší množství operační paměti, protože lze říct, že výkon serveru je přímo úměrný množství operační paměti v něm nainstalované. Server bude osazen kvalitními harddisky s vysokou kapacitou. Tyto disky budou zdvojeny, aby se předešlo ztrátám dat na nich uložených. Je vhodné využívat disky s nízkou spotřebou. Celý server by měl být uložen v dostatečně prostorné a větrané skříni. Konfiguraci serveru je vhodné zálohovat. Proto je vhodné, aby na serveru byla nainstalována zálohovací mechanika. Optická nebo FDD mechanika je nutná pouze pro instalaci serveru, při provozu je možné ji ze serveru odstranit.

5.3.2 Software

Pod pojmem software se v informatice obecně označuje sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Software lze dále rozdělit na systémový software, který zajišťuje chod samotného počítače a jeho styk s okolím a na aplikační software, se kterým buď pracuje uživatel počítače, nebo zajišťuje řízení nějakého stroje [14].

Jelikož bude navrhovaný server vytvořen z „klasického“ stolního počítače, bude hlavní rozdíl spočívat v jeho programovém vybavení. Programy nainstalované na serveru budou sloužit pro desítky uživatelů a budou zaměřeny na to, aby nabízely a plnily požadované síťové služby a tím zajišťovaly bezproblémový chod sítě. V dnešní době jsou na poli síťových operačních systémů zastoupeny největší měrou dvě linie. Tyto linie se liší především z obchodního hlediska. První linií jsou produkty společnosti Microsoft, které jsou chráněny mezinárodními licenčními ujednáními a jejich užívání je vázáno zakoupením licence. Druhá významná linie je tvořena tzv. open-source softwarem. Hlavními zástupci této kategorie jsou operační systémy z rodiny Unix. Všechny tyto programy jsou šířeny nekomerčně, s využitím licence GNU/GPL a jsou tedy zdarma.

5.3.2.1 Zvolená linuxová distribuce

Při stavbě serveru se setkáváme s mnoha úskalími. Jedním z nich je i výběr vhodné distribuce, kterou budeme na serveru provozovat. Distribuce začaly vznikat na počátku 90. let a to především pro zvýšení komfortu pro uživatele. Jednotlivé distribuce totiž přinášejí vše potřebné v jedné, ucelené podobě. Pojem distribuce je v podstatě označení souboru nástrojů a programů, které jsou spolu s Linuxem dodávaný jako celek. Distribuce můžeme dělit podle několika hledisek – binární/zdrojové, komerční/nekomerční případně serverové/desktopové. Jednotlivé distribuce se výrazně neliší, protože všechny vychází z jednoho prapůvodního zdroje – Unixu. Jediná výraznější odlišnost spočívá ve skladbě a množství dalších dodatečných programů. Dnes tedy existuje celá řada na kancelářských stanicích a serverech, využitelných distribucí OS Linuxu, jako například:

- *Debian GNU/Linux*
- *Ubuntu GNU/Linux*
- *Fedora GNU/Linux*
- *Mandriva GNU/Linux*

Debian GNU/Linux

Projekt Debian je sdružení dobrovolníků, kteří sdílejí myšlenku na vytvoření svobodného operačního systému. Tento systém se nazývá Debian GNU/Linux, nebo krátce Debian. V jeho středu je systémové jádro, které je nejzákladnějším programem a zajišťuje všechny základní služby včetně spouštění dalších programů. Debian momentálně používá jádro Linux, které je podporováno více než tisíci programátory z celého světa. Velká část základních nástrojů, které spolu s jádrem vytvářejí použitelný operační systém, pochází z projektu GNU. Poslední verzí této distribuce je Debian GNU/Linux 5.0. Tato verze vyšla v únoru roku 2009 a obsahuje zhruba 22349 dalších programů svobodného softwaru. Tento software je k dispozici pro všechny podporované architektury. Systém Debian se ve své společenské smlouvě zavázal, že bude založen na svobodném softwaru a sám vždy svobodným softwarem zůstane. To je velmi podstatný rys této distribuce. Znamená to významnou záruku pro její uživatele – mohou se pro Debian rozhodnout a začít na něm stavět s jistotou, že základní komponenta bude vždy uživateli poskytovat jeho svobody [21].

Především díky této záruce a mojí osobní zkušenosti jsem se rozhodl pro nasazení této konkrétní distribuce na budovaném serveru.

Ubuntu GNU/Linux

Ubuntu je komunitně vyvíjený operační systém, který je možné nasadit na laptopy, osobní počítače a server jak v domácnostech, tak i v kancelářích. Ubuntu je a vždy bude zdarma, a proto si jej můžete legálně stáhnout, používat a sdílet. Nová verze systému je vydávána pravidelně každých šest měsíců. Ubuntu se zakládá na Linuxovém jádře a je od základu navrženo s ohledem na bezpečnost, díky čemuž se minimalizuje riziko zavirování nebo jiného narušení počítače [22].

Fedora GNU/Linux

Fedora je kompletní operační systém Linux, jenž vznikl jako nekomerční odnož Red Hat Linuxu. Vyvíjí ho komunita vývojářů za podpory firmy Red Hat. Na základě Fedory pak Red Hat připravuje své komerční distribuce Red Hat Enterprise Linux. Fedora je známa svou pokrokovostí a zpravidla přináší v každé verzi několik zásadních novinek. Distribuce je značně univerzální, se znatelným zaměřením na použití na osobních počítačích [23].

Mandriva GNU/Linux (dříve Mandrake)

Mandriva Linux (dříve Mandrake Linux) je kompletní operační systém vybavený stovkami aplikací pro každodenní použití. Jednou z jeho hlavních výhod je velmi rychlá instalace a snadné základní nastavení. Mandriva Linux je nejsnazší na použití pro Linuxové začátečníky. Je nasazován především na pracovních stanicích, ale začíná být oblíben i jako serverová distribuce. Velký podíl na jeho oblíbenosti mají výborné konfigurační nástroje, které umožňují snadné a efektivní nastavení počítače. Instalace je rychlá a snadná. Díky tomu se jedná o výkonný, stabilní a bezpečný operační systém bez virů [24].

Obrázek č. 21 – Loga operačních systémů Linux

5.3.2.2 Instalační média

Operační systém Linux lze instalovat téměř z každého média. Mezi nejběžnější způsoby instalace se řadí instalace pomocí instalačního média, naklonováním již nainstalovaného systému a instalace po síti. Při zvolení prvního způsobu se využívá především instalace za pomoci dodávaných CD nebo DVD médií, někdy i FDD média. Výhodou je, že při instalaci není nutné připojení

k internetu. Druhým způsobem je klonování celého systému z jednoho serveru na druhý. Výhodou tohoto způsobu je především jeho rychlost, po instalaci není nutné nastavovat žádné služby, vše se přenese z původního systému. Posledním způsobem je využít instalaci takzvaně „po síti“. Pod tímto pojmem se skrývá instalace systému přes veřejně dostupné FTP nebo NFS. Výhodou posledního jmenovaného způsobu je především to, že při instalaci ze síťového úložiště se vždy nainstalují aktuální verze všech programů. Jaký způsob instalace zvolit záleží na zkušenostech správce systému a technickém vybavení. Jako nejvýhodnější se podle mého názoru nabízí kombinovaná instalace za pomoci jak dodávaného instalačního média, tak instalace z FTP nebo NFS.

5.3.2.3 Serverové služby

Server je svou podstatou předurčen k tomu, že bude plnit požadavky klientů k němu připojených. Tyto požadavky budou plnit programy na serveru nainstalované. Při vysokém síťovém provozu je vhodné, aby každá služba měla vyhrazený svůj vlastní síťový server. Jednak je každá z nabízených služeb jinak hardwarově náročná a hlavně se díky rozložení služeb na více serverů předejde větším výpadkům služeb v síti. Pokud bude nasazeno množství serverů, z nichž každý bude plnit svoji vlastní roli, a u jednoho z nich dojde k výpadku, nebudou důsledky tak rozsáhlé. Dojde pouze k omezení jedné nebo několika služeb a funkčnost sítě zůstane zachována. Pokud by se v síti vyskytoval pouze jeden server, který by sám zajišťoval všechny služby pro klienty, a došlo by k jeho výpadku, znamenalo by to s největší pravděpodobností poruchu celé sítě. Další nevýhodou tohoto řešení je fakt, že při jakékoliv úpravě serveru jej bude nutné na určitou dobu odstavit. Tím dojde k narušení provozu celé sítě. V případě, že bychom jednotlivé služby rozložily na více serverů, nedocházelo by při jejich úpravě k úplnému přerušení provozu, ale pouze k částečnému omezení.

Ve velmi vytížených počítačových sítích jsou služby takto rozděleny. Díky tomu jsou ovšem náklady na návrh a stavbu serverů mnohonásobně vyšší. Můj navrhovaný server bude fungovat ve škole a rozpočet většiny škol je velice napnutý. Těžko se shání finanční prostředky, a proto jsem se rozhodl, že i přes všechna rizika s tím spojená, budu navrhovat server, na němž budou běžet všechny služby najednou. Jedinou výjimkou bude speciální server, který bude sloužit jako firewall.

Postupem času si každý ICT koordinátor sám ověří, jestli je vhodné server takto provozovat nebo jestli je třeba nějakým službám vyčlenit vlastní, speciální server. Při instalaci serveru je důležité si dopředu naplánovat, jaké služby bude tento server v síti poskytovat. Při instalaci je nutné zahrnout všechna hlediska a na základě toho pak vybrat a instalovat příslušné programy. My si na serveru do začátku vytvoříme jednoduchý firewall, DHCP a DNS serveru, WWW serveru a E-MAIL server. Jako další službu bude server plnit úlohu centralizovaného datového úložiště pro studenty i učitele. Ve výše uvedeném přehledu jsou vyjmenovány všechny služby, které budou dostupné všem uživatelům. Nicméně na serveru je také nutné provozovat služby, které slouží k jeho správě a údržbě. Jedná se o služby SSH a VPN serveru. Tyto služby bude využívat pouze ICT koordinátor nebo správce server. Pro běžného uživatele nebudou dostupné.

Základní zabezpečení serveru i celé sítě bude realizováno pomocí vhodně nastaveného firewallu. Jako nejvhodnější se nabízí možnost vytvoření firewallu pomocí tzv. IPtables. Tento program je standardní součástí většiny distribucí Linux. Z pohledu bezpečnosti není vždy vhodné na síti provozovat DHCP server. Je nutné si promyslet, jak velkou kontrolu nad sítí bude správce mít. Jelikož bude tato síť vytvořená a provozovaná v jedné budově je vhodné DHCP server nastavit a provozovat. Nejrozšířenějším a nejlepším programem pro tento účel je Dhcp3-server. Tento program použijeme i v naší implementaci. Spolu s DHCP server je vhodné provozovat i DNS server. Nejlépe hodnoceným, nejbezpečnějším, nejrozšířenějším a nejpoužívanějším programem je Bind9. I na našem serveru bude tento program využit. Další službou bude služba WWW, na serveru tedy poběží vhodný webový server. Ze všech dostupných programů je nejvýhodnější využít program Apache2, jenž je součástí většiny distribucí. Proto bude využitý i na našem serveru. Ruku v ruce se službou WWW jde i využití e-mailu pro komunikaci. Na našem serveru bude tato služba zastoupena hned několika běžně dostupnými programy. Jedná se především o programy Exim4, Dovecot a Squirrelmail. Poslední službou, která bude určena pro uživatele, je využití serveru jako datového úložiště. Tuto funkci budou plnit především programy Samba a Proftpd. Jako další služba, kterou bude server nabízet, je zajištění vzdáleného přístupu do sítě. Tato možnost nebude dostupná pro běžného uživatele, ale pouze pro správce systému nebo ICT koordinátora a to proto, aby bylo možné zajistit bezproblémový chod a fungování celé

sítě bez nutnosti fyzické přítomnosti u serveru. Všechny plánované služby jsme si stručně popsali a nyní se již pustíme do detailnější konfigurace.

6 Hlavní serverové služby

Podstatou serveru je poskytování služeb klientům. Server poskytuje množství různých služeb. Většina z těchto služeb bude bez omezení sloužit pro všechny klienty, ale budou zde i služby, k nimž bude přístup omezen. Toto omezení bude zajištěno buď přímo v jejich konfiguračních souborech, nebo filtrovacím pravidlem ve firewallu. Pojmem hlavní serverové služby budeme označovat všechny služby, ať už jsou omezeny nebo ne.

6.1 Firewall a NAT

Z logiky věci vyplývá, že je vždy potřeba mít celou síť perfektně zabezpečenou. V systému Linux se nabízí hned několik variant. Je možné využít speciálně navržených a přednastavených programů, které se budou o bezpečnost sítě starat. Tyto programy jsou již předkonfigurovány a není možné je detailně nastavovat, můžeme provádět pouze nepatrné úpravy. Druhou možností je stejně jako v prvním případě také využití speciálních programů, které jsou však na rozdíl od prvního způsobu plně konfigurovatelné, tzn. že veškerá bezpečnostní pravidla je možné detailně přidávat, rušit a upravovat. Poslední možností je kombinace obou způsobů. V našem případě zvolíme způsob číslo dvě a využijeme sadu programů pod názvem IPtables.

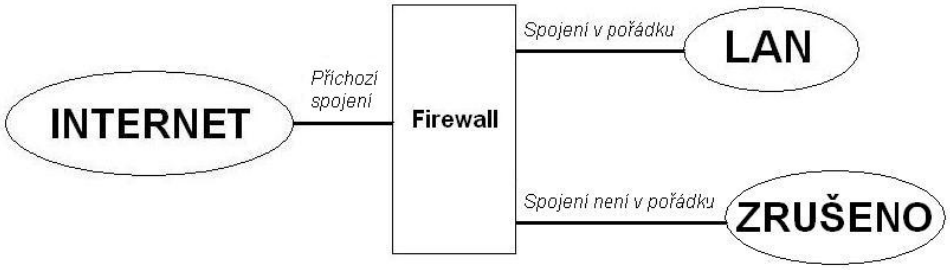
IPtables je velmi silný nástroj, který umožňuje regulovat a řídit veškerou síťovou komunikaci protékající přes server [25].

Tato sada programů umožňuje vytvoření obou dnes využívaných druhů firewallu – stavového i transparentního. Zároveň nám tyto programy umožní sdílení připojení. Toto sdílení připojení se nazývá Network Address Translation – NAT a slouží k tomu, abychom mohli připojit více počítačů na jednu veřejnou IP adresu, což nám vyřeší nedostatek přidělených veřejných adres a zároveň se zvýší odolnost sítě vůči možnému průniku. Kombinace firewallu a NATu tak vytvoří z našeho serveru perfektně fungující, síťovou dopravní křižovatku.

Konfigurace takovéhoto firewallu se provádí za pomoci editace jediného souboru. Do tohoto souboru se zapisují příslušná filtrovací pravidla. Tato pravidla se

automaticky nastaví při startu serveru a jsou po celou dobu běhu server aplikována na síťový provoz. Jeho příklad je uveden v pozdější části mé práce.

Obrázek č. 22 – Funkce firewallu



6.2 Systém DNS

Systém DNS se začal rozvíjet velice brzy po vzniku samotného internetu a to především kvůli usnadnění práce pro koncového uživatele. Tento systém slouží k tomu, aby bylo možné provádět vzájemné převody doménových jmen a IP adres. Pro každou IP adresu máme zavedeno doménové jméno. Toto doménové jméno dokáže plně nahradit IP adresu, a to ve všech směrech. Jedna IP adresa může mít přiřazeno více doménových jmen. Hlavním důvodem vzniku je především fakt, že člověk si snadněji zapamatuje název než poměrně složitou číselnou adresu. Vztah mezi IP adresou a doménovým jménem je uložen v databázi jmenného serveru. Původně tuto funkci plnil pouze jeden soubor, ale s velkým tempem rozvoje celosvětové sítě přestal tento způsob dostačovat a začalo se pro tento účel využívat speciálně navržených programů. Protože je Internet obrovským „prostorem“, který obsahuje nepřeberné množství komunikačních uzlů, a tím pádem i doménových jmen nebylo by možné, aby se o všechny DNS dotazy staral pouze jediný server. Proto existuje množství vzájemně nezávislých jmenných serverů, které jsou kvůli správné funkčnosti hierarchicky uspořádané, a každý z nich obsluhuje určitou část Internetu, která se nazývá zóna. Z hlediska klienta není důležité, jaký typ jmenného serveru mu poskytne překlad, všechny mají z pohledu klienta stejnou váhu. Rozlišujeme
4 základní druhy jmenných serverů – primární, sekundární, caching only a root name server. Na primárním serveru jsou uložena všechna data pro příslušnou zónu. Při úpravě libovolného záznamu v zóně, je tato úprava prováděna právě zde. Sekundární server slouží jako záloha při výpadku primárního serveru. Tento sekundární server si v pravidelných intervalech kopíruje údaje o zóně ze serveru

primárního, aby v případě výpadku dokázal tento server plnohodnotně nahradit. Caching only server je v podstatě pouze pomocný, vyvažovací server pro jednotlivé zóny. Nad všemi těmito servery je potom nadřazený root name server, který obsluhuje root doménu [26].

Stejně jako ve většině případů, existuje v systému Linux množství takto zaměřených programů. My budeme pro tento účel využívat celosvětově nejrozšířenější a nejpoužívanější program Bind9. Jeho konfigurační soubory jsou celkem dva. Jeden slouží pro překlad doménového jména uzlu na IP adresu a druhý plní opačnou funkci. Konkrétní příklad konfigurace bude uveden v další části mojí práce.

Obrázek č. 23 – Funkce DNS serveru

6.2.1 Struktura systému DNS

Celý Internet je pomocí systému DNS rozčleněn na skupiny jmen – domény. Tyto domény jsou logicky uspořádány a to tak, že jejich struktura připomíná hierarchické uspořádání do tvaru stromu. Na nejvyšším patře jsou tzv. hlavní domény, někdy nazývané též domény root. Přímými podřízenými těchto domén jsou pak domény, které se označují jako domény nejvyššího řádu neboli Top Level Domains (TLD). V systému DNS rozlišujeme dva základní druhy TLD. Prvním druhem jsou domény konkrétního státu. Pro Českou republiku je rezervována doména .CZ. Druhým jsou pak domény, které neoznačují konkrétní územní celek (stát apod.), ale označují subjekty, které mají určité společné rysy. Nejznámějším příkladem je doména .ORG, která byla původně určena pouze pro nevýdělečné organizace. Jako další příklady lze jmenovat .EDU, která označuje vzdělávací

zařízení nebo .MIL, jenž je určena pro vojenské subjekty. Tyto TLD se ještě rozčleňují na tzv. subdomény, které označují jednotlivé organizace. Podle velikosti dané organizace je pak ještě možné tyto domény dále členit (např. jednotlivé pobočky apod.) na menší celky. Nejmenším objektem v systému DNS je uživatelská stanice. I přes to, že komunikace mezi jednotlivými uzly sítě Internet probíhá pouze za pomoci IP adres, nikoliv doménových jmen, vyžadují některé aplikace pro svoje fungování skutečnost, aby bylo možné k doménovému jménu přiřadit IP adresu. Tento proces přiřazování se nazývá zpětný neboli reverzním překladem. K běžným doménám tedy vznikají domény reverzní, které jsou také uloženy a obsluhovány DNS servery a stejně jako běžné domény jsou stromově uspořádány [26].

6.2.2 Struktura doménového jména

Doménový název neboli jméno je uváděno v tzv. tečkové notaci, která má obecnou strukturu danou následující syntaxí: *řetěz.řetěz. …. řetěz.*

Prvním řetězem ve jméně je vždy doménový název uživatelského počítače, tento název je následován jménem nejnižší subdomény. Následuje jméno domény vyšší apod. Posledním řetězcem je pak název root domény, která je reprezentován pouze tečkou. Doménové jméno může v součtu všech řetězců čítat maximálně 255 znaků a každý z řetězců pak může mít délku maximálně 63 znaků. Jednotlivé řetězce je možné skládat z číslic, písmen a pomlčky, ale při jejich tvorbě musíme zachovat platné normy, tzn. na začátku ani na konci řetězce se nesmí vyskytovat tečka. V řetězcích se pro jednoduchost nerozlišují velká a malá písmena – jsou považována za jeden znak [26].

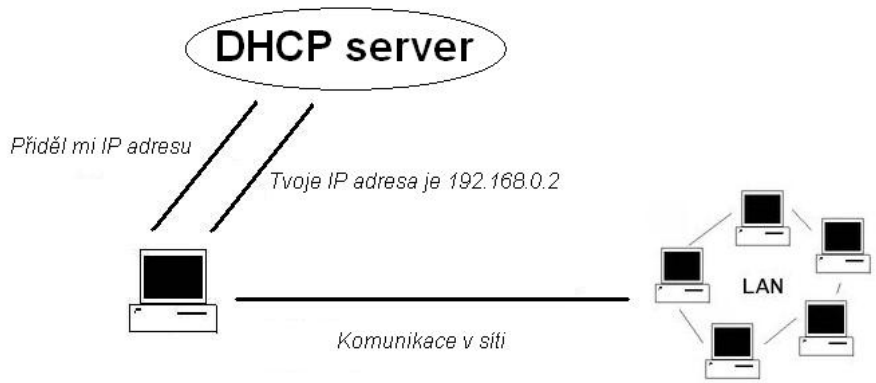
6.3 DHCP server

Systém DHCP se stejně jako systém DNS začal vyvíjet brzy po vzniku Internetu. Tento systém se používá k tomu, aby bylo možné koncovým uživatelským stanicím přidělit všechny potřebné informace, které jim umožní plnohodnotné fungování v síti. Parametry, které se přidělují pomocí systému DHCP, lze rozdělit na dvě kategorie. První kategorií jsou parametry nutné pro začlenění počítače do sítě. Mezi tyto parametry se řadí především adresa IP, maska sítě, výchozí brána a IP adresa jmenných serverů. Druhá kategorie jsou parametry tzv. doplňkové. Pokud by tyto parametry nebyly koncovému počítači známy, neovlivnilo by to jeho začlenění do

sítě. Tyto parametry tedy pouze „vylepšují“ integraci počítače v síti. Mezi tyto parametry se řadí například IP adresa časového serveru, IP adresa WINS serveru apod. Oba dva druhy parametrů, které DHCP server svým klientům distribuuje, lze přidělovat dvěma způsoby. Údaje je možné jednotlivým klientům dodávat zcela náhodně, tzn. při každém připojení stanice do sítě je jí přidělena jiná sada informací (IP adresa a další údaje), které po uplynutí určitého časového údaje opět vrátí a dostane přidělenu odlišnou sadu informací. Druhým způsobem je přidělování těchto informací tzv. staticky, tzn. při každém připojení do sítě je počítači vždy přidělena stejná sada informací (IP adresa apod.), která je po uplynutí stanovené doby opět obnovena v nezměněné podobě. Statické přidělování adres se zajistí v konfiguraci serveru tak, že se spojí MAC adresa příslušného počítače a přidělená IP adresa. Správně nastavený a zabezpečený systém DHCP velmi zjednodušuje správu jednotlivých počítačů i celé sítě a umožňuje ekonomicky hospodařit s vyhrazeným adresním prostorem, což jsou z pohledu správce velice výhodné a požadované vlastnosti [27].

V Linux se pro tento účel jako nejvhodnější nabízí program Dhcp3-server, který budeme využívat i v naší implementaci.

Obrázek č. 24 – Funkce DHCP serveru



6.4 Proxy server

Tato služba, pokud je na serveru provozována, funguje jako spojovací článek mezi klientskou stanicí a příslušným webovým serverem v Internetu. Při komunikaci bez použití proxy serveru jsou požadavky klienta a odpovědi serveru předávány

přímo přes bránu. Pokud je v síti zařazen proxy server, probíhá komunikace odlišně. V tomto případě nejsou požadavky a odpovědi předávány přímo mezi komunikujícím klientem a odpovídajícím serverem, ale do této trasy je začleněn ještě jeden prvek - proxy server. Ten funguje jako prostředník mezi klientem a cílovým serverem. Proxy server si klientské požadavky uloží do své vyrovnávací paměti a předá je následně dále příslušnému serveru. Vůči tomuto serveru pak figuruje sám jako klient. Přijatou odpověď následně opět uloží a odešle zpět ke správnému klientovi. Pokud se jiný klient ze sítě bude dotazovat na stejnou informaci, nebude už nutné znovu navazovat spojení s příslušným serverem, ale klientovi bude poskytnuta odpověď, která je uložena ve vyrovnávací paměti proxy serveru. Celá komunikace se pak omezí pouze na to, že si proxy server ověří, jestli je informace na něm uložená dostatečně aktuální. Pokud ano, poskytne ji klientovi, pokud ne, naváže se spojení se serverem v Internetu a celý proces se opakuje. Díky tomu celá komunikace proběhne rychleji a sníží se tím i vytížení přípojné linky do Internetu. Server si ukládá vždy nejaktuálnější informace, které si vždy při vhodných příležitostech aktualizuje, a proto nemůže dojít k situaci, že by klientovi byla poskytnuta zastaralá informace. Tato činnost poskytování informací může probíhat dvěma způsoby. Prvním z nich je tzv. transparentní, tzn. proxy server v síti funguje, aniž je nutné klienty na tuto skutečnost speciálně konfigurovat. Každý klient na síti pak tuto službu využívá. Druhou možností je proxy server, který je klienty využíván pouze v případě, že je na tuto skutečnost speciálně nakonfigurujeme. Znamená to, že ne každý klient v síti musí tuto službu využívat. Činnost proxy serveru může zajišťovat buď speciálně navržený kus hardware, nebo vhodný software provozovaný na obyčejném počítači [25].

V systému Linux existuje několik programů, které se k tomuto účelu dají použít. Nejznámějším a nejrozšířenějším je program Squid, který využijeme i v našem případě.

6.5 Samba a FTP server

Protokol SMB a jeho implementace Samba se využívají především k vzdálenému přístupu k souborům. Počátky vývoje tohoto programu jsou datovány do roku 1992 a s jeho vývojem začala firma IBM, od které jej následně převzal Microsoft a upravil pro svoje účely a integroval do systému Windows. Původní komunikace programu neprobíhala za pomoci protokolů TCP/IP, ale postupem času

se ukázalo, že je vhodnější upravit sambu pro použití s rodinou protokolů TCP/IP. Jedná se o velice užitečný nástroj pro každého správce, kterému v síti figurují buď pracovní stanice se systémem Windows, nebo pracovní stanice se systémem Linux, případně kombinace obou systémů. Tento protokol však umožňuje nejen vzdálený přístup k souborům, ale je vhodný i k tomu, aby zpřístupnil vzdálené tiskárny a umožnil tak jejich sdílení v síti. Samba server bychom tedy mohli považovat za velmi zvláštní a zároveň užitečný program, který může být provozován jak platformě Windows, tak i Linux. Je to program, který se snaží spojit dva rozdílné světy - svět Linux a svět Windows [28].

I když by se mohlo někomu zdát, že v prostředí sítě, kde se vyskytují pracovní stanice s operačním systémem Windows, by bylo vhodnější použít ke sdílení souborů a tiskáren Windows server, je zde řada důvodů, které to vyvracejí. Především Samba je šířena pod licencí GNU/GPL a těší se velkému zájmu vývojářů a programátorů. Lze tedy říci, že po čtrnácti letech existence je Samba vyspělý produkt, který umožňuje sdílení souborů, tiskáren a autentizaci uživatelů. Správce sítě tak může využít výhod unixové správy uživatelů a přitom nemusí běžné uživatele nutit do Linuxu [29].

Díky všem těmto vlastnostem bude i na náš server implementován program Samba, který bude na rozdíl od protokolu FTP využíván všemi uživateli v podobě sdíleného adresáře nebo adresářů.

Současně bude na serveru provozován i FTP server. Protokol FTP pochází také již z počátků vývoje Internetu. Protokol ke své činnosti využívá portů číslo 20 a 21 a komunikuje výhradně přes TCP. Forma komunikace je stanovena do vztahu server – klient, kdy FTP server poskytuje své služby pro klientské stanice. Klient pak využije nabízených služeb a může na serveru provádět definované operace. Na celý tento proces je dohlíženo ze serveru, který tuto činnost za pomoci sady příkazů řídí a reguluje. Dnes již není tento protokol považován za bezpečný, proto není vhodné jej využívat při citlivé komunikaci. Tento nedostatek je dnes vyřešen pomocí různých nadstaveb – například FTPS, který již využívá šifrovaného spojení [30].

FTP server je možné provozovat téměř na všech platformách, na nichž existuje mnoho programů a to jak volně dostupných, tak i licencovaných. My tento server budeme využívat především pro aktualizaci a údržbu webových stránek, nebude využíván běžnými uživateli pro přístup k jejich soukromým adresářům.

V systému Linux je možné vybírat z několika volně dostupných aplikací, které umožňují server vytvořit. Naší volbou bude volně dostupný program ProFTPD.

6.6 Webový server

HTTP je významnou součástí Internetu. Originálně byl určen pro výměnu dokumentů vytvořených ve formátu HTML. Tento protokol při komunikaci využívá portu číslo 80 a komunikuje výhradně přes TCP. Tento protokol byl v kombinaci s protokolem elektronické pošty jednou z hlavních příčin, díky nimž došlo k tak masovému rozšíření Internetu. Dnes již tento protokol není využíván pouze pro přenos souborů HTML, ale lze jím přenášet i jiné informace, a to především díky různým nadstavbám. Stejně jako protokol FTP není ani protokol HTTP považován za bezpečný, a proto není vhodné jej využívat při citlivé komunikaci. Tento nedostatek je dnes vyřešen pomocí různých nadstaveb. Díky tomu vznikla speciální, bezpečnější varianta tzv. HTTPS, která umožňuje přenášet data šifrovanou formou, a tím je chránit před případným zneužitím. Celý protokol funguje způsobem klient – server. Klient odešle svůj požadavek na server, ten jej zpracuje a vrátí zpět příslušnou odpověď.

Program Apache představuje serverovou implementaci protokolu HTTP. Jeho vývoj začal v roce 1993 ve Spojených státech amerických na akademické půdě univerzity v Illinoi. V současnosti je tento webový server jedním z nejpopulárnějších webových serverů a je provozován na více než 50 % serverů na světě. Při instalaci Apache na server je velmi vhodné připojit k němu i nadstavbu určenou pro provoz a tvorbu www stránek v programovacím jazyce PHP a samozřejmě i vhodnou databázi, která bude se serverem spolupracovat. Nejvhodnější databází je program Mysql. Tato trojkombinace se v některých případech souhrnně označuje zkratkou LAMP – Linux, Apache Mysql, Php. Prohlížeče jako například Internet Explorer, Opera apod. jsou klientskou implementací tohoto protokolu. Rozdíl v těchto prohlížečích je pak především v jejich pořizovací ceně, stabilitě a flexibilitě [31].

6.7 E-mailový server

Při tvorbě školního serveru – brány se jistě nespokojíme pouze s nainstalováním výše uvedených služeb, ale především pro zlepšení komunikace mezi učiteli a žáky nebo mezi žáky navzájem je výhodné instalovat e-mailový server.

Otázkou ovšem je, jaký emailový server zvolit. Protože celý server bude založený na využívání služeb systému Linux, budeme při volbě vhodného programu vybírat mezi programy, kterých je v Linux celá řada. Než vybereme vhodný program, je třeba zvážit, co vše by měl tento program umět. Nabízí se hned několik variant, podle jejichž vzoru je možné server vystavět.

První variantou je možnost, že na našem serveru bude provozován pouze server, který je určený pro odesílání pošty. Tento server se nazývá SMTP. Situace by poté vypadala tak, že každý uživatel by byl nucen pro komunikaci využívat specializovaného poštovního klienta a svoji e-mailovou schránku by měl vytvořenu na nějakém „externím“ serveru. Výhodou tohoto řešení je především jeho jednoduchost a nenáročnost na údržbu, ovšem nevýhodou je fakt, že každý uživatel bude mít jiný tvar e-mailové schránky a bude využívat jiný e-mailový klient, díky tomu by pak mohla vznikat různá nedorozumění, a to jak při komunikaci, tak i při práci s těmito klienty.

Druhou variantou je možnost, že na našem serveru bude provozován nejen server pro odchozí poštu, ale také server, jenž bude určen pro přijetí e-mailových zpráv. Tento server pro příchozí poštu se nazývá POP3 nebo IMAP. Situace by poté vypadala tak, že by každý z uživatelů byl opět nucen využívat pro komunikaci specializovaný e-mailový klient, ale na rozdíl od prvního případu by měl každý uživatel svoji schránku umístěnu na lokálním serveru – bráně. Díky tomu by bylo možné každému uživateli přidělit e-mailovou schránku ve stejném formátu.

Protože by tvary e-mailových schránek byly jednotné, nedocházelo by díky tomu k nesrovnalostem v komunikaci a celý systém e-mailové komunikace by působil jednotně a uceleně, což by byla výhoda. Přetrvávající nevýhodou by byl fakt, že by nezmizely problémy, spojené s obsluhou e-mailových klientů. Navíc by přibyl ještě problém správci systému - jelikož je tento systém e-mailového serveru komplikovanější než předchozí varianta, byla by náročnější také jeho obsluha a údržba.

Třetí, poslední, nejlepší, a nejkomplikovanější variantou je pak možnost, že na našem serveru budou provozovány nejen servery pro odchozí a příchozí poštu, ale i specializovaný server určený pro tzv. webový přístup do schránky. Pod tímto pojmem se skrývá speciální program, který spolupracuje s POP3/IMAP serverem, a to tak, že umožní uživateli, aby do své e-mailové schránky vstoupil nejen přes speciální e-mailový klient, ale také „přímo“ přes webovou schránku.

Všechny tyto programy a jejich řešení využívají protokolů SMTP, POP3 nebo IMAP.

První z protokolů – SMTP – je určený pro odesílání pošty mezi e-mailovými servery. Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. Všechny zprávy jsou doručovány do poštovních schránek, z nichž si je pak uživatel vyzvedne za pomoci protokolu POP3 nebo SMTP. Tento systém pracuje s protokolem TCP/IP a využívá port číslo 25 [14].

Druhý z protokolů – POP3 – je určený pro výběr e-mailových zpráv ze vzdálených nebo lokálních schránek. Tento systém pracuje s protokolem TCP/IP a ke svému fungování využívá port číslo 110. Tento protokol umožňuje si zprávy ze svého účtu stáhnout a následně s nimi pracovat i bez přímého připojení k Internetu. Proces stahování zpráv probíhá ve třech krocích. V první fázi klient otevře spojení na server a ten mu odpoví, v druhém kroku jsou serverem požadovány autorizační údaje od klienta. V poslední fázi, poté, co jsou oba předchozí kroky úspěšně dokončeny, je možné začít se zprávami pracovat [14].

Poslední z protokolů – IMAP – je také určený pro výběr e-mailových zpráv ze vzdálených nebo lokálních schránek. Tento protokol vyžaduje trvalé připojení k Internetu, potažmo e-mailové schránce. Díky tomu je možné s celou poštovní schránkou plně pracovat z libovolného místa. Všechny zprávy a složky jsou uloženy na poštovním serveru a na počítač se stahují jen nezbytné informace. Takže při zobrazení složky se stáhnou jen záhlaví zpráv a jejich obsah až v případě, že zprávu chce uživatel přečíst. U jednotlivých zpráv se uchovává jejich stav, uživatel může se zprávami libovolně pracovat [14].

V systému Linux existuje nepřeberné množství programů, které plní jednotlivé funkce celého serveru. Na našem serveru budeme používat kombinaci programů Postfix, Dovecot a Squirrel.

6.8 Správa uživatelů a skupin

I když se to nemusí mnohým uživatelům zdát, je správa uživatelských kont a uživatelských skupin na serverech velice důležitou činností. Jelikož celý server bude sloužit především pro lidi, tedy žáky a učitele, je nutné si předem stanovit vhodnou strategii, podle níž budeme uživatele rozčleňovat a řadit. Bez ohledu na velikost školy, v níž bude server provozován, je nutné, aby všichni uživatelé byli

rozděleni do příslušných skupin. Důvodů pro to je spousta, mezi hlavními bych jmenoval snadnější manipulaci s účty jednotlivých uživatelů, správa a ochrana uživatelských dat a především bezpečnost. Při vytvoření uživatelského účtu v systému Linux se běžně vytvoří i skupina, do níž je tento účet přiřazen. Při použití systému Debian Linux se pro každého uživatele vytvoří stejnojmenná skupina a uživatelský účet se do ní automaticky přiřadí. Správa takto rozděleného systému by ovšem byla velice obtížná, proto je nutné zvolit jiné rozdělení. Protože je škola rozdělena na jednotlivé ročníky a třídy, kdy každá ze tříd má svého třídního učitele, nabízí se hned tři možná rozdělení uživatelských účtů.

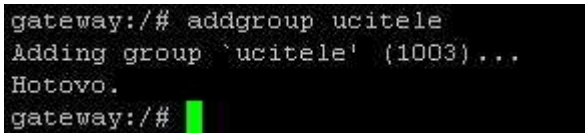
Prvním možným dělením je rozčlenit všechny dostupné účty žáků do ročníků a tříd. Výhodou je fakt, že by nebylo možné zaměnit dvě skupiny mezi sebou – název třídy je vždy unikátní. Nevýhodou tohoto řešení je fakt, že by jednou za rok bylo nutné tato rozdělení aktualizovat.

Druhý možný způsob dělení je rozdělovat jednotlivé uživatelské účty podle jména třídního učitele. Výhodou tohoto způsobu dělení je především fakt, že jméno třídního učitele se při normální situaci změní za celou dobu školní docházky pouze jedenkrát – při přechodu žáka z prvního na druhý stupeň. Drobnou nevýhodou pak může být fakt, že na škole mohou pracovat dva učitelé se shodným jménem. Tato možnost je ovšem velice nepravděpodobná, ale její řešení je poměrně jednoduché.

Jako třetí možný způsob rozčlenění účtů do skupin se nabízí členění účtů na základě data, kdy žák nastoupil povinnou školní docházku. Výhodou je zde fakt, že by nebylo nutné za celou dobu školní docházky nijak upravovat příslušnost účtu ve skupině.

Jako nejvhodnější řešení je podle mého názoru kombinace druhého a třetího způsobu. Na našem serveru jej proto budeme využívat. V předchozí části jsem zvolil strategii, kterou při návrhu serveru budu používat. Prvním krokem je vytvoření příslušných pracovních skupin, do nichž jsou uživatelé zařazováni. Pro vytváření skupin je v systému Linux speciální příkaz. Tento příkaz má název addgroup. Tento příkaz umožňuje provádět množství nejrůznějších, přídavných nastavení skupin. V mém případě toto není nutné. Pouze provedu tento příkaz bez přídavných nastavení. V následujícím příkazu uvádím vytvoření skupiny, do níž jsem zařadil učitele.

Obrázek číslo 25 – Vytvoření skupiny



Stejným způsobem by se vytvořily i všechny ostatní skupiny. Rozdíl by byl pouze v tom, že by se měnily jejich názvy. Po vytvoření všech požadovaných skupin, je nutné do těchto skupin uživatele rozdělit. Toto rozdělení jsem zajistil přímo při vytváření uživatelských účtů. Tento způsob je podle mého názoru nejjednodušší a nejrychlejší. Nový uživatel se vytvoří podle následujícího příkladu. V tomto příkladu jsem využil několik přepínačů. První přepínač –g se stará o to, aby byl účet zařazený do správné skupiny. Název skupiny se uvádí za tímto přepínačem. Druhý přepínač –d zajišťuje vytvoření domovského adresáře pro nového uživatele. Za tímto přepínačem se uvádí cesta, kde na pevném disku se má adresář vytvořit. Přepínač –c slouží k vytvoření komentáře pro daný účet. Poslední částí příkazu je název uživatelského účtu.

Obrázek číslo 26 – Vytvoření uživatelského účtu

Tvorba všech ostatních uživatelských účtů se provádí stejným příkazem. Jediný rozdíl spočívá v tom, že se postupně mění název účtu, umístění domovského adresáře uživatele a název skupin, do které je účet zařazen.

6.9 Diskové kvóty

Při tvorbě školního serveru je nutností vytvořit na něm diskové kvóty a tyto následně aplikovat na uživatelská konta. I když v dnešní době se ceny velkokapacitních disků snižují, je velice problematické ve školství potřebné částky získat. Proto je každému správci jasné, že neustálé nakupování dalších a dalších disků není ideální řešení. Vzhledem k tomu jsou správně nastavené diskové kvóty perfektním řešením. Diskové kvóty jsou velice jednoduchý způsob, jak omezit diskový prostor pro uživatele serveru. Tyto kvóty výborně spolupracují s různými programy, mimo jiné i programem Samba, což je velice výhodné. Po správné

konfiguraci jsou uživatelé omezování ve svém užívání, a to hned několika způsoby [27].

Prvním ze způsobů je možnost omezit uživateli jeho přidělený diskový prostor a to bez ohledu na počet jeho uložených souborů. Tato úprava je v konfiguraci zajištěna dvěma parametry – hard limit a soft limit. Hard limit je pevná hranice a uživateli se nikdy nepodaří na disk uložit více dat, než je uvedeno v tomto parametru. Soft limit je hranice, při jejímž překročení je uživatel o této skutečnosti varován, ale po určitou předem stanovenou dobu je možné ji překročit. Tato předem stanovená doba se v konfiguraci nastavuje pomocí parametru grace period a pokud neprovedeme její změnu, je defaultně nastavena na dobu 1 týden.

Druhou možností je neomezovat uživateli celkový diskový prostor, ale omezit mu počet možných, uložených souborů na sdíleném disku. Toto omezení se provádí vhodným nastavením parametrů při konfiguraci systému. Stejně jako v prvním případě se i zde uplatňuje parametr grace period.

Poslední, nejlepší možností je omezit uživateli jak celkový diskový prostor, tak i počet možných uložených souborů a zkrátit dobu grace period na 1 den. Při konfiguraci diskových kvót serveru je vždy důležité porovnat, jak velký sdílený disk bude v serveru nainstalován a počet uživatelů využívajících tento server. Těmto dvěma podmínkám je posléze nutné přizpůsobit velikost diskového prostoru vyhrazeného každému z uživatelů. V mém návrhu jsem se rozhodl využít primárního disku o kapacitě 80Gb. Tento disk je určen výhradně pro instalaci systému a všech nutných podpůrných aplikací. Sdílení dat z tohoto disku není v mém návrhu žádoucí. Kvůli sdílení dat jsem do serveru zařadil dva pevné disky každý o kapacitě 1TB. Tyto disky jsem sestavil do diskového pole typu Raid1. Tento typ se nazývá zrcadlení. Rozhodl jsem se tak proto, aby se vylepšila ochrana dat na serveru uložených. Na tomto diskovém poli jsou umístěny všechny sdílené adresáře a jsou na něm aplikovány diskové kvóty. Aby bylo možné používat tyto kvóty je nejdříve nutné, aby se upravilo jádro operačního systému. Tato úprava spočívá v tom, že se do jeho konfigurace přidá software, který kvóty obsluhuje.

Obrázek číslo 27 – Úprava jádra pro využití kvót

```
[*] Quota support
[ ]   Report quota messages through netlink interface
[*]   Print quota warnings to console (OBSOLETE)
<M>   Old quota format support
<M>   Quota format v2 support
```

Při přípravě systému na využití kvót je v dalším kroku nutné, aby se označily disky, na nichž se mají kvóty používat. Toto označení jsem provedl úpravou konfiguračního souboru, který se stará o správu disků. Tento soubor se nazývá fstab a je umístěn v adresáři /etc. Jeho úprava spočívá v tom, že se do příslušného řádku v tomto souboru přidá označení kvót.

Obrázek číslo 28 – Úprava souboru fstab.

```
Soubor: fstab          Sloupec 0          514 bytů
# /etc/fstab: static file system information.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
/dev/hda1       /               ext3    defaults,errors=remount-ro 0       1
/dev/hda5       none            swap    sw              0       0
/dev/hdc        /media/cdrom0   udf,iso9660 user,noauto     0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto  0       0
/dev/md1        /media/raid1    ext3    defaults,usrquota       0       0
```

V posledním kroku je ještě nutné nainstalovat obslužný software. Jedná se o dva programy. První z nich se nazývá quota, druhý quotatool. Po těchto třech úpravách je systém připraven pro užití kvót. Aby se kvóty aktivovaly je v posledním kroku nutné celý systém restartovat. Při jeho opětovném startu jsou již kvóty automaticky aktivovány. Nyní přistoupíme k omezování diskového prostoru uživatelů. Na tomto serveru je k dispozici disk o kapacitě 1TB. Tento disk bude využívat přibližně 450 uživatelů. Vzhledem k tomu jsem se rozhodl, že každému žáku vyhradím diskový prostor o kapacitě 750MB, u učitelů pak 1,5Gb. Díky tomuto nastavení bude uživateli zabráno z celkové kapacity disku 345Gb. Zbylý diskový prostor je určený pro instalaci síťových výukových programů, pro provoz FTP a WWW serveru školy. Celkovou koncepci jsem si připravil, nyní předvedu, jak ji realizovat. Omezování prostoru je nutné nastavit pro každého uživatele jednotlivě. V tomto případě by se jednalo o velice zdlouhavý proces. Protože je systém Linux

geniální, umožňuje tuto činnost značně zrychlit. Toto zrychlení spočívá v tom, že se diskové kvóty detailně nastaví pro jednoho uživatele. Nastavení tohoto uživatele se potom pouze okopíruje pro všechny ostatní. V tomto návrhu předvedu, jak nastavit kvóty pro všechny učitele. Žákovské kvóty se nastavují stejně, pouze s tím rozdílem, že se změní velikost hodnoty přiděleného diskového prostoru.

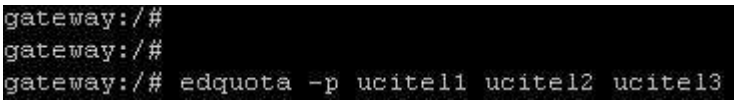
Obrázek číslo 29 – Nastavení vzorového uživatele

Syntaxe příkazu je následující. Přepínač –u označuje uživatele, pro kterého vše nastavujeme. První číslo značí tzv. soft limit, druhé číslo tzv. hard limit. Další dvě čísla značí soft a hard limit pro množství uložených souborů. Přepínač –a jsem zde umístil proto, abych tyto kvóty aktivoval na všech připravených discích. Dalším krokem je zkrácení tzv. grace periody na dobu 1 dne.

Obrázek číslo 30 – Nastavení vzorového uživatele

Tento příkaz je velice jednoduchý. Jeho aplikací se zkrátí doba grace period na 1 den, a to u všech uživatelů najednou. Není proto nutné toto nastavení provádět pro jednotlivé uživatele. Posledním krokem je „okopírování“ tohoto nastavení pro zbylé učitele. To se provede za pomoci následujícího příkazu.

Obrázek číslo 31 – Nastavení zbylých uživatelů



Syntaxe příkazů zřejmá. Přepínač –p označuje to, že první z vyjmenovaných uživatelů slouží jako vzor pro všechny další vyjmenované uživatele. Tímto je ukázka konfigurace dokončena.

6.10 Vzdálená správa

Při návrhu a stavbě nového serveru se pravděpodobně každý jeho tvůrce nebo administrátor bude muset rozhodnout, jaký způsob vzdálené správy bude využívat. Důvod je zřejmý – ne vždy je možné, aby se administrátor fyzicky nacházel u serveru v případě, když se vyskytne problém. K dispozici je hned několik řešení vzdálené správy. Každý ze způsobů s sebou přináší nejen výhody, ale zároveň i nevýhody a možná bezpečnostní rizika. V systému Linux se nabízejí dvě varianty vzdáleného připojení k serveru. Prvním ze způsobů je připojení k serveru pouze přes textové rozhraní. V tomto případě je řešení velice jednoduché a snadno najdeme vhodný nástroj. Tímto nástrojem je program OpenSSH. Druhou možností připojení k serveru je využít tzv. grafického klienta. Z tohoto pohledu není řešení vůbec složitější a snadno najdeme vhodný nástroj. Tímto programem je OpenVPN.

OpenSSH je balík počítačových programů, které ke své činnosti využívají šifrovaného spojení založené na využití protokolu SSH. Tento program má dvě části – SSH klient, který je vzdáleně spouštěn a je určen k připojení serveru. Druhá část je SSH server, který je permanentně spuštěn na serveru a naslouchá příchozím žádostem o komunikaci [28].

OpenVPN je jednoduše použitelná, robustní a velmi dobře konfigurovatelná implementace protokolu VPN umožňující bezpečně propojit dvě nebo více sítí. Celá uskutečněná komunikace je šifrována. Výhodou programu je, že je šířený pod licencí GNU/GPL a zároveň je multiplatformní. Tento program má dvě části – VPN klient, který je vzdáleně spouštěn a je určen k připojení serveru. Druhá část je VPN server, který je permanentně spuštěn na serveru a naslouchá příchozím žádostem o komunikaci [32].

Na většině serverů, které jsou zaměřeny podobně jako je tento právě budovaný, se využívá kombinace obou způsobů vzdálené správy. I v našem případě budeme tento server takto nastavovat.

7 Konkrétní případ pro ZŠ Buttulova, Chotěboř

V předešlé části textu byla vyjmenována různá fakta a teoretické poznatky, které se týkají stavby a provozu počítačové sítě. V této části mojí práce se budeme věnovat jejich praktické realizaci. Popíšeme jak navrhnout, sestavit, nainstalovat a provozovat síťový server ve škole. Dále navrhneme a popíšeme konfigurace jednotlivých síťových služeb ze serveru.

Před tím, než se pustíme do samotné stavby serveru je nutné, abychom si vše dopředu naplánovali. Můj navrhovaný server bude provozován na základní škole. Tuto školu v současné době navštěvuje přibližně 400 žáků a pracuje zde 40 pedagogů. Server bude tedy poskytovat služby přibližně 450 uživatelům. Z množství uživatelů a počtu nabízených služeb vyplývá i jeho hardwarová konfigurace.

V nedávné době na této škole došlo k modernizaci počítačové učebny. Díky tomu se z provozu vyřadilo několik starších uživatelských stanic. Protože je mým cílem vytvořit co nejlevnější a zároveň plně funkční server, využijeme k jeho stavbě jednu z těchto stanic. Její konfiguraci podle potřeby upravíme a budeme využívat jako síťový server. Po hardwarové stránce má upravená pracovní stanice tuto konfiguraci. Jedná se o PC Intel Pentium 3 o taktu 500Mhz. Tento server v sobě ukrývá základní desku od společnosti MSI s označením 694T Pro. Tato deska nabízí celkem 5 PCI slotů, po jednom slotu AGP a ISA. Ve slotu AGP je umístěna grafická karta S3. Ve slotech PCI jsou umístěny síťové karty 3Com a dále také řadič diskových jednotek typu SATA. Součástí základní desky je integrovaná zvuková karta, která je ovšem pro běh systému zcela zbytečná. Proto jsem tuto kartu v systému BIOS zakázal. Dále jsou na desce umístěny tři banky na operační paměť. Každý tento bank je schopen pojmout operační paměť typu DIMM PC 133Mhz o maximální velikosti modulu 512Mb. Celková maximální kapacita operační paměti serveru je 1,5Gb. Pro osazení procesorem je na desce umístěn Socket typu 370, který umožňuje osazení procesory Celeron/Pentium 3 o maximálním taktu 1,2Ghz. Deska umožňuje připojení pouze starších pevných disků typu IDE. Proto jako primární disk bude použit Disk Western Digital o kapacitě 80Gb. Jako další přídavné disky budou v serveru umístěny 2 pevné disky každý o velikosti 1TB. Tyto dva disky budou společně zapojeny do diskového pole typu Raid 1. Toto zapojení se označuje jako zrcadlení, tzn. data uložena na server jsou uložena na obou discích ve stejné

podobě. Díky tomu jsou data zálohována, proto nedojde k jejich ztrátě ani při výpadku jednoho z disků. Připojení těchto disků je realizováno přídavným řadičem SATA firmy Kouwell umístěným ve slotu PCI. Tento řadič je plně podporován v systému Linux. V serveru je použit procesor Pentium 3. Tento procesor má takt 500Mhz. Procesor je z výkonnostního hlediska pro naše účely zcela dostačující. Server jsem osadil třemi kusy operační pamětí typu DIMM PC 133Mhz. Díky těmto třem modulům disponuje server operační pamětí o celkové kapacitě 1,5GB. Tato velikost je zároveň maximální možná velikost operační paměti, která je podporovaná základní deskou. Do serveru jsem umístil 2 síťové karty 3Com o rychlosti 100Mbit. Tyto karty jsou k tomuto účelu vhodnější než běžné síťové karty s chipem REALTEK, protože jsou schopny spolehlivě pracovat i při vysokém zatížení. Karty 3Com mají také plnou softwarovou podporu operačního systému Linux. Server je osazen jednou optickou mechanikou. Jedná se o mechaniku CD-Rom. V zásadě je možné využít mechaniku od jakéhokoliv výrobce. Celý server je uzavřen v počítačové skříni ATX se zdrojem 300W. Tato skříň je dostatečně prostorná a umožňuje umístění veškerých součástí. Dále tato skříň umožňuje dobrou cirkulaci vzduchu a v případě potřeby je možné ji osadit přídavnými větráčky. Celkově bych shrnul konfiguraci mnou navrženého serveru do následující tabulky.

Název komponentu	**Popis komponentu**	**Obrázek komponentu**
Základní deska (MB)	1 x Základní deska MSI 694T Pro, societ 370, chipset Via, 5 x PCI, 1 x AGP, 1 x ISA, 3 x DIMM, 2 x IDE, 1 x FDD	
Procesor (CPU)	1 x Intel Pentium 3 500Mhz, societ 370, aktivní chlazení	
Operační paměť (RAM)	3 x 512 Mb Sdram PC 133 Mhz	
Pevný disk (HDD) - primární	1 x Western Digital, WD 800BB, 80Gb	

Pevný disk (HDD) - sekundární	2 x Western digital, WD Caviar Green, 1TB.	
Přídavné karty – řadič SATA	1 x Kouwell KW-571S - SATA	
Přídavné karty – síťová karta 3Com	2 x PCI síťová karta 3C905CX-TX-M, rychlost 100Mbit.	
Přídavné karty – Grafická karta	1 x AGP grafická karta S3 Trio64V+ 1MB	
Optická mechanika	1 x CD-Rom mechanika TEAC CD-540E	
Počítačová Skříň	1 x Case ATX, pozice 2 x 5,25“, 3 x 3,5“, Zdroj 300W	

Obrázek č. 32 – Server postavený na systému Linux

7.1. Počítač a informační systém školy

Na této základní škole, stejně na jakékoliv jiné, je několik samostatných celků, které spolu vzájemně spolupracují. Prvním z těchto celků je ředitelství školy, které ředitelka školy a jejího zástupce. Obě tyto osoby mají pro svoji potřebu k dispozici

pracovní stanici. Obě jejich stanice jsou zapojeny do počítačové sítě a využívají především síťových služeb určených pro sdílení dat v síti, dále serveru DNS pro přístup k Internetu, e-mailového serveru a místního webového serveru. O správný chod těchto stanic se stará zástupce ředitele, který je zároveň IC koordinátorem školy. Druhým celkem je sekretariát školy. V tomto celku figurují celkově dvě osoby. První z nich je mzdová účetní a druhou je sekretářka. Jejich náplně práce se částečně překrývají. Co je ale mnohem důležitější je fakt, že obě dvě osoby mají opět k dispozici vlastní pracovní stanice. Tyto stanice využívají podobné síťové služby v prvním případě. Dalším subjektem na této škole jsou kabinety pedagogů prvního a druhého stupně. V části kabinetů jsou také umístěny pracovní stanice, ale v části kabinetů tyto stanice stále chybí. Stanic v kabinetech pedagogů je přibližně 10. Ostatní učitelé, kteří nemají přímo v kabinetu k dispozici vlastní PC, využívají dvou pro ně volně přístupných pracovních stanic ve sborovně. Na této škole se nachází jedna počítačová učebna se 17 pracovními stanicemi. Přes tyto stanice přistupují k síti především žáci. Při svém přístupu využívají nabízených síťových služeb. Posledním celkem jsou učebny vybavené projektorem a stolním počítačem nebo laptopem. Na škole se nachází přibližně 10 takto vybavených učeben.

7.2 Výhody školní počítačové sítě

Všechny vyjmenované celky jsou přes LAN vzájemně propojeny. Díky tomuto spojení spolu mohou pracovní stanice libovolně komunikovat. Rychlost vystavěné sítě je 100mbit. Toto je na školách běžná praxe, která je po všech stránkách dostačující. Server samotný je umístěn v počítačové učebně a přes LAN poskytuje svoje služby. Nejvyužívanější službou je sdílení dat po síti. Toto sdílení umožňuje učiteli snadnější manipulaci s připravenými výukovými materiály. Protože jsou počítače vzájemně přístupné, odpadá nutnost přenášení materiálů na discích CD-rom, DVD-Rom nebo pamětech Flash. Učitel si přes síť jednoduše otevře potřebný soubor přímo ze svého počítače a za pomoci projektoru s ním pracuje. Další možností je poskytnout tento soubor přímo žákovi pro jeho domácí přípravu. Sdílení dat využívají i žáci. Z jejich strany tato činnost probíhá poněkud odlišně. Žáci nemají svůj osobní počítač, ale mají svůj osobní adresář. Tento adresář je také přístupný z jakéhokoliv místa sítě. Díky tomu jej může žák používat buď pro ukládání důležitých souborů, nebo pro jejich spouštění například při prezentaci referátu. Další

z výhod zapojení v sítí je možnost přístupu k Internetu z jakéhokoliv počítače. Toto lze využít ve výuce nebo pro zábavu. Spojení počítačů do jednoho celku zároveň šetří čas i finanční prostředky, protože předávání dat elektronickou formou je velice rychlé a levné.

7.2.1 Administrativní systém školy

Následující oblast se dělí na tři podkategorie. První z nich je ekonomika. V této oblasti se využívá hlavně těch služeb serveru, které umožňují fungování ekonomických, účetních programů. Jedná se především o službu sdílení dat. Dále je zde využito předávání zpráv ze sekretariátu na ředitelství a naopak. K tomu je možné využít opět sdílení dat nebo též e-mailovou komunikaci. Vše je zajištěno serverem. Druhou podoblastí je řízení školy. Do této oblasti částečně spadají již zmíněné účetní programy, ale především manažerské systémy, u nichž se opět využívá služby sdílení dat. Tyto systémy umožňují vytvoření a správu nejrůznějších druhů databází od evidence žáků, pedagogických pracovníků, až po evidenci majetku. Díky tomu, že jsou tyto soupisy umístěny v databázi, dochází ke značnému zrychlení při práci s nimi. A protože je databáze umístěna na serveru je zároveň možné s těmito seznamy pracovat z libovolného počítače umístěného v síti. Díky tomu opět dochází ke zkvalitnění správy celé organizace. Poslední kategorií je využívání síťového serveru jako elektronické nástěnky nebo rozcestníku. K tomuto účelu je vhodné využít webového serveru. Na tomto serveru se vytvoří jedna nebo více speciálních sekcí. Do těchto sekcí se pak nahrají všechny zákony, směrnice, nařízení, standardy a osnovy. Tyto pak budou každému uživateli podle potřeby libovolně přístupné. Zároveň je možné do této sekce nahrát i rozvrhy jednotlivých tříd, plány suplování na jednotlivé dny apod. Díky tomu, že budou tyto dokumenty zveřejněny online, dojde ke zlepšení informovanosti žáků i jejich rodičů.

7.2.2 Pedagogický informační systém

Tuto oblast využívají jak pedagogové, kteří při své výuce využívají předem připravených elektronických výukových materiálů nebo zdrojů z Internetu, tak
i ostatní učitelé, kteří využívají jinou strategii výuky. Učitelé mohou díky počítačové síti při tvorbě materiálů spolupracovat, data si jednoduše vyměňovat a vzájemně kontrolovat. Dále je učitelům umožněno využívat veškeré výukové programy.

Dokonale funkční počítačová síť a síťový server umožňují učiteli mít svoje data vždy přístupná. O chod serveru a jeho služeb se stará správce. Vzájemnou komunikací správce a „běžného učitele“ dojde k dokonalé spolupráci a zkvalitnění výuky.

7.2.3 Podpora výuky žáků

Další oblastí, v níž se budou síťové služby serveru využívat, je podpora výuky žáků. Tato podpora se zajišťuje součinností učitele, serveru a jeho správce. Učitel zde figuruje v roli koordinátora a tvůrce vyučovací jednotky. Server má roli pasivní a pouze umožňuje plnění požadovaných operací. Mezi tyto operace se řadí sdílení dat a využívání výukových programů, vzájemnou komunikaci a výměnu dat mezi uživateli a použití nejrůznějších testovacích programů pro ověření dosažených kompetencí. Posledním článkem je správce serveru, který se stará o instalaci požadovaných programů, jejich správnou funkčnost a aktuálnost.

7.2.4 Obecné programy

Stejně jako v ostatních blocích se i zde využívá síťových služeb poskytnutých lokálním nebo internetovým serverem. Jak je z názvu patrné, nelze striktně vymezit působnost této oblasti. Do této kategorie se řadí jak síťové programy, tak i programy instalované na lokálních pracovních stanicích. Z lokálních programů se jedná především o programy, které umožňují tvorbu a editaci textových a grafických dokumentů. Dále sem spadá využití síťových programů, a to především autorských systémů, statistických, analytických, plánovacích a jiných programů. Jinými slovy lze říct, že se jedná o všechny typy programů a činností, které mají obecnější využití.

7.2.5 Obecné zdroje informací

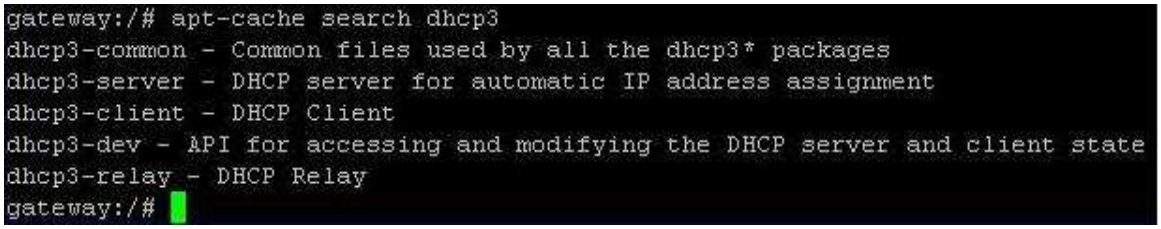
V této kategorii je server využit spíše jako prostředník mezi místní sítí a jejími zdroji a zdroji veřejně dostupnými na celosvětové síti Internet. Server prostřednictvím svých služeb umožňuje přístup k online informačním zdrojům jako jsou encyklopedie, slovníky, překladače apod.. Protože jsou na serveru nainstalované nejrůznější výukové programy, může server samotný také sloužit jako zdroj informací. Záleží pouze na ochotě správce, jaké množství programů uživatelům zpřístupní.

7.3 Konfigurace síťových služeb

V mém návrhu jsem se rozhodl nechat běžet všechny síťové služby s výjimkou firewallu pouze na jednom jediném síťovém server. Toto řešení není ideální, ale vzhledem k omezeným možnostem finančním a vzhledem k umístění serveru v poměrně malé organizaci, je podle mého názoru a dosavadním zkušenostem můj návrh zcela dostačující. Pro každou službu jsem použil jiný program. Každý z těchto programů je po jeho instalaci vždy nutné správně nakonfigurovat. Konfigurace velké většiny programů v Linux se provádí editací jediného souboru. Název tohoto souboru je nejčastěji ve tvaru **.conf*. Tento přístup je značně odlišný než v systému Windows. Bývá pravidlem, že součástí tohoto souboru je také návod, jak s konfigurací začít. Někdy je tento soubor již částečně předkonfigurován. V takovémto případě se pak již pouze doplní požadované funkce. V konfiguračním souboru je možné uvádět tzv. komentáře. Tyto se zapisují ve speciálním tvaru *# komentář* nebo *// komentář* a umožňují nám si v tomto souboru zapisovat případné poznámky nebo upřesnění konfigurace. Správnou úpravou tohoto souboru pak dosáhneme požadovaných vlastností programu a tím i správné funkčnosti celého serveru. Jak jsem ve své práci proklamoval, bude na jednom serveru spuštěno množství různých služeb. V této části mojí práce si detailně popíšeme konkrétní konfigurační soubory většiny z nich. Jedinou službu, kterou jsem se rozhodl detailně nepopisovat, je služba e-mailového serveru, jelikož tato problematika je velice rozsáhlá a komplikovaná.

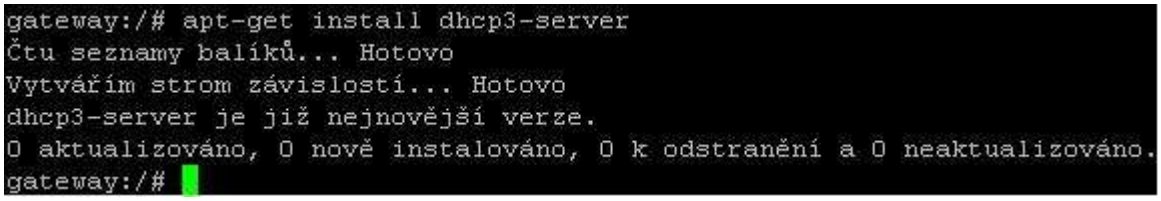
Každou službu je před jejím nastavováním nutné na server umístit. Toto umístění se provede nainstalováním příslušného programu, který je k tomu určený. Ve většině případů nabízí Linux několik programů se stejným zaměřením. Záleží pouze na vkusu a zkušenostech správce serveru, který program zvolí. Instalace programu se v operačním systému Linux Debian provádí za pomoci sady příkazů. Prvním z nich je příkaz, který nalezne vhodný program. Tento příkaz se zadává z příkazové řádky a má tvar: *apt-cache search název_programu_nebo_jeho_části*.

Obrázek č. 32 – Použití příkazu apt-cache search dhcp3



V případě úspěšného nalezení jednoho nebo několika programů se využije druhý příkaz, který příslušný program již nainstaluje. Příkaz se zadává ve tvaru *apt-get install název_programu*.

Obrázek č. 33 – Použití příkazu apt-get install dhcp3



První běžící služba se týká zabezpečení a nazývá se firewall. Pro realizaci firewallu jsem se rozhodl nasadit sadu programů pod názvem IPtables. Tato sada programů a jejich funkce je detailněji popsána v kapitole 6.1. Tyto programy umožňují relativně širokou škálu nejrůznějších nastavení. Na mnou navrhovaném serveru bude firewall vypadat následovně.

```
#-------------------------------------------------------------------------------#
############        ZAČÁTEK SKRIPTU        ############
#-------------------------------------------------------------------------------#
```

#! /bin/sh

Nejdříve je vhodné si popsat situaci, v níž je firewall nasazen. Server bude osazen
dvěma síťovými kartami. První nese označení eth0 a je směrována do Internetu.
Druhá je pojmenována jako eth1 a je směrována do LAN. Přístupová linka školy do
sítě Internet má kapacitu 2Mbit/512 kbit.
V prvním kroku jsem provedl nastavení NAT. Toto se provádí následující sérií
příkazů.

iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE

echo "1" > /proc/sys/net/ipv4/ip_forward

V další části jsem nadefinoval řetězce, které budu dále ve zbytku konfigurace
využívat. Díky tomu si ušetřím spoustu zbytečné práce. Prvním z nich je řetězec,
který zajišťuje ochranu před podvržením zdrojové IP adresy. Druhým z nich je
řetězec, který zvyšuje odolnost firewallu proti DoS útokům. V posledním řetězci
jsou definovány třídy IP adres, které se nesmí na rozhraní vedoucím do Internetu
objevit.
iptables -N spoofing
iptables -A spoofing -m limit --limit 5/h --limit-burst 3 -j LOG --log-prefix "Rezervovana adresa:"
iptables -A spoofing -j DROP
#
iptables -N syn_flood
iptables -A syn_flood -m limit --limit 1/s --limit-burst 4 -j RETURN
iptables -A syn_flood -j DROP
#
iptables -N nesmyslna_IP
iptables -A nesmyslna_IP -s 192.168.0.0/16 -j spoofing
iptables -A nesmyslna_IP -s 172.16.0.0/12 -j spoofing
iptables -A nesmyslna_IP -s 10.0.0.0/8 -j spoofing
iptables -A nesmyslna_IP -s 127.0.0.0/8 -j spoofing
Aby mohl správce systému vzdáleně operovat s FTP serverem, je nutné k tomu
firewall přizpůsobit. Toto přizpůsobení se realizuje tím, že se do něj zahrnou
speciální, k tomu určené moduly. Ty už se samy postarají o zbytek
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp
Protože je tento firewall předřazený hlavnímu serveru, je nutné, aby byla zajištěna
jeho průchodnost pro některé služby. Těmito službami jsou především vzdálená
správa, WWW server, mailový a FTP server. Tato průchodnost se zajišťuje ve
firewallu tak, že se do něho přidá vhodná sada pravidel. Tato pravidla vypadají
následovně.
průchodnost pro FTP server
eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány
iptables -t nat -A PREROUTING -p tcp --dport 20 -j DNAT --to 192.168.1.2:20
iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to 192.168.1.2:21

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

průchodnost pro WWW server

eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány

iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to 192.168.1.2:80

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 80 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

průchodnost pro VPN server

eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány

iptables -t nat -A PREROUTING -p tcp --dport 1194 -j DNAT --to 192.168.1.2:1194

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 1194 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

průchodnost pro SSH server

eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány

iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to 192.168.1.2:22

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

průchodnost pro SMTP server

eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány

iptables -t nat -A PREROUTING -p tcp --dport 25 -j DNAT --to 192.168.1.2:25

iptables -A FORWARD -i eth0 -o br0 -p tcp -d 192.168.1.2 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

průchodnost pro SMTP server

eth0 = Internetové rozhraní, eth1 = LAN rozhraní, 192.168.1.2 = IP adresa brány

iptables -t nat -A PREROUTING -p tcp --dport 110 -j DNAT --to 192.168.1.2:110

iptables -A FORWARD -i eth0 -o eth1 -p tcp -d 192.168.1.2 --dport 110 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

Jako jednu ze služeb jsem se rozhodl na serveru zprovoznit tzv. cachovací server.

Pro toto řešení jsem se rozhodl hlavně z toho důvodu, že je škola do Internetu

připojena velmi pomalou linkou. Tato služba mi umožnila tento nedostatek

částečně vykompenzovat. Služba bude nastavena jako „neviditelná“ pro všechny

klienty. Proto je nutné na tuto službu za pomoci firewallu klienty přesměrovat. To
nám umožní následující příkaz.
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128
Nejdůležitější částí firewallu jsou pravidla, která definují jak zacházet s příchozími
daty. Jsou to především následující pravidla. První z nich je nastavení defaultní
politiky. My požadujeme, aby se vše příchozí zahodilo a povolily se jen
vyjmenované výjimky. To nám zajistí toto pravidlo.
iptables -P INPUT DROP
Nyní následují pravidla pro výjimky. Prvním z nich je povoleni ICMP zpráv.
iptables -A INPUT -p ICMP --icmp-type 0 -j ACCEPT # Echo Reply
iptables -A INPUT -p ICMP --icmp-type 3 -j ACCEPT # Echo Request - ping
iptables -A INPUT -p ICMP --icmp-type 8 -j ACCEPT # Destination Unreachable
iptables -A INPUT -p ICMP --icmp-type 11 -j ACCEPT # Time Exceeded
Ochrana pred SYN flooding.
iptables -A INPUT -i eth0 -p tcp --syn -j syn_flood
Ochrana pred SYN flooding pres icmp pakety.
iptables -A INPUT -i eth0 -p icmp -j syn_flood
Zákaz rezervovaných IP adres na Internetovém rozhraní.
iptables -A INPUT -i eth0 -j nesmyslna_IP
Ochrana pred Ping of death.
iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -m limit --limit 10/s --limit-burst 20 -j ACCEPT
Ochrana před portscanem s nastavenym SYN,FIN.
iptables -A INPUT -i eth0 -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
Blokování sluzby AUTH.
iptables -A INPUT -i eth0 -p TCP --destination-port 113 -j REJECT --reject-with tcp-reset
Pakety, které jsou označené jako NEW, ale nemají nastavený SYN flag do sítě
nepatří.
iptables -A INPUT -i eth0 -p tcp ! --syn -m state --state NEW -j DROP
Rozhraní loopback povolím bez omezení.
iptables -A INPUT -i lo -p ALL -j ACCEPT
Pakety, které jsou součástí již navázaných spojení, do sítě pustíme.

iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Seznam všech povolených služeb.

iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT # SSH z Internetu

iptables -A INPUT -i eth1 -p tcp --dport 22 -j ACCEPT # SSH z Vnitřní sítě

iptables -A INPUT -p udp --dport 53 -j ACCEPT # DNS Server UDP

iptables -A INPUT -p tcp --dport 53 -j ACCEPT # DNS Server TCP

iptables -A INPUT -p tcp --dport 1194 -j ACCEPT # VPN Server

iptables -A INPUT -p tcp --dport 20 -j ACCEPT # FTP Server

iptables -A INPUT -p tcp --dport 21 -j ACCEPT # FTP Server

Další důležitou sekcí firewallu je sekce, která určuje, jak se bude zacházet s daty,
která se předávají z jednoho síťového rozhraní na druhé. Pro účely školy jsem se
rozhodl povolit vše a až v případě potřeby tuto defaultní politiku upravit.

iptables -P FORWARD ACCEPT

Poslední částí firewallu je sekce, která určuje, jak se má zacházet s daty, která
opouští síťové rozhraní. Pro školní účely jsem opět nastavil defaultní politiku tak, že
jsou všechna data propuštěna. V případě nutnosti je opět možné toto pravidlo
zpřísnit.

iptables -P OUTPUT ACCEPT

#----------#

########## ***KONEC SKRIPTU*** ##########

#----------#

Druhá služba jejíž konfiguraci jsem se rozhodl detailněji popsat je služba DHCP serveru. Pro implementaci této služby jsem zvolil program Dhcp3-server. Tento program je běžnou součástí operačního systému Linux Debian. Popis služby DHCP, její výhody i nevýhody, jsem uvedl v kapitole číslo 6.3. Mnou navržený konfigurační soubor vypadá následujícím způsobem. Samozřejmě není nejmenší problém mnou navrhovanou konfiguraci upravit potřebám jakékoliv jiné školy.

#--#

########## ***ZAČÁTEK SKRIPTU*** ##########

#--#

Celý konfigurační soubor jsem rozdělil na dvě části. V této první části jsou všechna
nastavení, která jsou platná pro jakýkoliv připojený počítač sítě. Zahrnul jsem sem
parametry jak povinné, tak i doplňkové. Nyní podrobněji popíšu každý z nich.
První parametr jsem zde umístil proto, abych zvýšil odolnost sítě proti případnému
útočníkovi. Parametr zajišťuje to, že se IP adresa a další údaje přidělí pouze
důvěryhodným klientům. Tito důvěryhodní klienti jsou vyjmenováni v další části
konfigurace.

boot-unknown-clients true;

Tento parametr zajišťuje, aby byla každému klientovi přidělena pouze jedna IP
adresa.

one-lease-per-client true;

I když to není tento případ, může se v síti vyskytovat více DHCP serverů. Jeden
z nich je vždy hlavní. Tento fakt, aby byl server hlavní autoritou DHCP v síti, se
zajišťuje následujícím parametrem.

authoritative;

DHCP server svoje údaje klientským stanicím propůjčuje na určitou dobu. Tato
doba se počítá v sekundách. Následující dva řádky určují standardní dobu
zapůjčení a maximální dobu zapůjčení údajů.

default-lease-time 7200;

max-lease-time 14400;

Každý počítač v síti musí znát IP adresu jmenného serveru. Vždy je pro případ
výpadku vhodné použít minimálně 2 různé jmenné servery. V mém nastavení
prozatím použiji pouze jeden server.

option domain-name-servers 192.168.2.1;

DHCP server je schopný klientům delegovat název domény do níž jsou připojeni.
Tuto doménu jsem nazval *zakladni.skola*. Její přidělení je zajištěno tímto
parametrem.

option domain-name "zakladni.skola";

Následující parametr určuje hodnostu síťové masky.

option subnet-mask 255.255.255.0;

Posledním parametrem této části se klientům sděluje IP adresa tzv. WINS serveru.
Tento server jsem zde implementoval za použití programu Samba. Tento server je
na síti nejvyšší autoritou co se týká vzájemného sdílení dat mezi propojenými
stanicemi.
option netbios-name-servers 192.168.2.1;
V tuto chvíli je ukončeno všeobecné nastavování hodnot přidělovaných serverem.
Proto přejdu ke druhé části. V této části jsem provedl nastavení rozsahu, z něhož
se budou klientům přidělovat IP adresy, nastavení IP adresy výchozí brány
a nastavení tzv. všesměrového vysílání. Veškerá tato nastavení jsou zajištěna
následující sadou instrukcí.
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.2.2 192.168.2.254;
  option routers 192.168.2.1;
  option broadcast-address 192.168.2.255;
V další části této sekce jsem vyjmenoval důvěryhodné klienty, o nichž jsem se
zmínil v předchozí části. Rozhodl jsem se, že nakonfiguruji server tak, že bude
využívat tzv. statické přidělování adres. To v praxi znamená, že každý přidělený
klient vždy obdrží stejnou sadu instrukcí. Díky tomu se zlepší přehled správce
o celé síti. Navíc, pokud to bude nutné, toto nastavení umožní zablokování
komunikace z konkrétního počítače. Tím se zamezí šíření virů, spamů a dalších
nežádoucích věcí.
group {
        use-host-decl-names true;
Doménový název hostitele.
        host reditelka {
Fyzická adresa síťového rozhraní hostitele.
                hardware ethernet 00:80:48:60:9F:BA;
Přidělená IP adresa pro konkrétní fyzickou adresu.
                fixed-address 192.168.2.2;
            }
Všechny ostatní uzly jsou vždy pojmenovávány ve stejném tvaru. Liší se pouze
v přiděleném doménovém názvu a IP adrese. Pro příklad uvedu pouze několik
z nich. Přidání libovolného počtu dalších uzlů není sebemenší problém.
Příklad konfigurace počítače umístěného ve sborovně.

```
        host sborovna_PC-1 {
                hardware ethernet 00:4F:62:13:21:89;
                fixed-address 192.168.2.4;
           }
# Příklad konfigurace počítače umístěného v kabinetu.
        host kabinet-první_stupen {
                hardware ethernet 00:04:75:AC:54:9D;
                fixed-address 192.168.2.5;
           }
# Příklad konfigurace počítače umístěného v počítačové učebně.
        host ucebna_PC-1 {
                hardware ethernet 00:04:75:F0:56:EE;
                fixed-address 192.168.2.6;
           }
        }
}
                #-------------------------------------------------------------------------#
                ############        KONEC SKRIPTU        ############
                #-------------------------------------------------------------------------#
```

Další provozovanou službou je služba jmenného serveru. Tuto službu jsem implementoval za pomoci programu Bind9. Jeho konfigurace se skládá z celkem třech souborů. V prvním souboru se vymezí jméno zóny a její působnost. Druhý soubor je určený pro překlad doménového jména určitého uzlu na IP adresu. Poslední z trojice souborů slouží k překladu IP adresy zpět na doménové jméno. V následujícím příkladě předvedu po řadě ukázky všech těchto souborů. Nebudu zde uvádět celý soubor, ale pouze nastavení, která jsem v něm provedl. Tato nastavení detailněji popíšu.

#--#

############ ***ZAČÁTEK SKRIPTŮ*** ############

#--#

Soubor číslo 1 – nastavení působnosti domény:

Konfigurace zóny a název školní domény.

zone "zakladni.skola" {

Tento parametr určuje, že se jedná o primární zónu.

type master;

Konfigurace této zóny je uložena v samostatném souboru. Tento parametr určuje,

kde na disku se tento soubor nachází a jak se jmenuje.

file "/etc/bind/192.168.tam";

};

Konfigurace reverzní zóny

zone "168.192.in-addr.arpa" {

Tento parametr určuje, že se jedná o primární zónu.

type master;

Konfigurace této zóny je uložena v samostatném souboru. Tento parametr určuje,

kde na disku se tento soubor nachází.

file "/etc/bind/192.168.zpet";

};

Soubor číslo 2 – vlastní nastavení zóny:

V tomto souboru se provádí nezbytná nastavení, která souvisí s překladem

doménového jména uzlu na jeho IP adresu. I zde jsem se rozhodl, že předvedu

pouze ukázku pro několik málo uzlů sítě. Rozšířit konfiguraci o další uzly už potom

nepředstavuje žádný problém. Následujících několik řádků za začátku konfigurace

se týká nastavení vzájemné komunikace mezi jmennými servery primárními

a sekundárními. Jediný parametr, který považuji za nutné detailněji popsat, je

parametr serial.

$TTL 604800

@ IN SOA gateway.zakladni.skola. root.gateway.zakladni.skola. (

Tento parametr je v podstatě počítadlo jakékoliv změny v konfiguraci provedené.

Při dopsání, smazání nebo jakékoliv úpravě konfiguračního souboru je nutné toto

sériové číslo změnit. Jeho nejobvyklejší syntaxe je založena na datu. Má tvar

rok-měsíc-den-počet_pokusů

2010010101 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

Dále je do konfigurace začleněno nastavení jmenného a e-mailového serveru.

@ IN NS gateway.mujnet.doma.

@ IN MX 30 server.mujnet.doma.

V poslední částí jsou již vyjmenovány konkrétní uzly sítě. Každý z těchto uzlů má
svůj doménový název, který je v celé síti unikátní. Konfiguraci této části je možné
doplnit o tzv. CNAME záznamy. Tyto záznamy umožňují pojmenovat jeden uzel
několika jmény. To je užitečné především v případech, kdy jeden uzel slouží pro
více účelů. V mém konkrétním příkladě uplatním tuto vlastnost u vstupní brány,
protože ta poskytuje více služeb.

gateway IN A 192.168.2.1

www CNAME gateway

mail CNAME gateway

ftp CNAME gateway

Příklad konfigurace počítačů v ředitelně.

reditelka IN A 192.168.2.2

zastupce IN A 192.168.2.3

Příklad konfigurace počítače umístěného ve sborovně.

Sborovna-PC_1 IN A 192.168.2.4

Příklad konfigurace počítače umístěného v kabinetu.

kabinet-první_stupen IN A 192.168.2.5

Příklad konfigurace počítače umístěného v počítačové učebně.

ucebna_PC-1 IN A 192.168.2.6

<u>Soubor číslo 3 – vlastní nastavení reverzní zóny:</u>

V tomto souboru se provádí nezbytná nastavení, která souvisí reverzním
překladem. I zde jsem se rozhodl, že předvedu pouze ukázku pro několik málo uzlů
sítě. Rozšířit konfiguraci o další uzly už potom nepředstavuje žádný problém.
Následujících několik řádků za začátku konfigurace se týká nastavení vzájemné

komunikace mezi jmennými servery primárními a sekundárními. Jediný parametr,
který považuji za nutné detailněji popsat je parametr serial.

$TTL 604800

@ IN SOA 168.192.in-addr.arpa. gateway.zakladni.skola. (

Tento parametr je v podstatě počítadlo jakékoliv změny v konfiguraci provedené.
Při dopsání, smazání nebo jakékoliv úpravě konfiguračního souboru je nutné toto
sériové číslo změnit. Jeho nejobvyklejší syntaxe je založena na datu. Má tvar
rok-měsíc-den-počet_pokusů

2010010101 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL

V další části jsem opět provedl nastavení jmenného server.

@ IN NS gateway.mujnet.doma.

V poslední částí jsou již vyjmenovány konkrétní uzly sítě. Každý z těchto uzlů má
svůj doménový název, který je v celé síti unikátní.

1.2 IN PTR gateway.zakladni.skola.

Příklad konfigurace počítačů v ředitelně.

2.2 IN PTR reditelka.zakladni.skola.
3.2 IN PTR zastupce.zakladni.skola.

Příklad konfigurace počítače umístěného ve sborovně.

4.2 IN PTR sborovna_PC-1.zakladni.skola.

Příklad konfigurace počítače umístěného v kabinetu.

5.2 IN PTR kabinet-první_stupen.zakladni.skola.

Příklad konfigurace počítače umístěného v počítačové učebně.

6.2 IN PTR ucebna-PC_1.zakladni.skola.

#----------#

########## ***KONEC SKRIPTŮ*** ##########

#----------#

Další službou, kterou jsem se rozhodl umístit na server je služba PROXY. Důvod, proč jsem se k tomu rozhodl je ten, že tato škola je do Internetu připojena ne příliš rychlou linkou. Proxy server mně umožní docílit toho, aby kleslo vytížení této linky. Druhou důležitou vlastností je fakt, že díky proxy serveru je možné odfiltrovat nežádoucí webový provoz. Docílíme tak toho, že si žáci ve škole nebudou moci prohlížet stránky s nevhodným obsahem. Jako softwarovou implementaci jsem se rozhodl použít program Squid. Konfigurační soubor tohoto programu je velice rozsáhlý. Ve většině případů je možné jej ponechat bez změny, pouze upravit dvě sekce týkající se „odlehčení“ linky a filtrace provozu. Tyto sekce zde budu prezentovat. Jejich konkrétní podoba vypadá následovně.

#--#
########## ***ZAČÁTEK SKRIPTU*** ##########
#--#

Zde je ukázka konfigurace první části. Tato první část určuje, že se proxy server
bude chovat tzv. transparentně. V praxi to znamená, že všechna data klientů
budou protékat skrz tento server a klienty na tuto situaci nebude nutné žádným
způsobem speciálně nastavovat.

httpd_accel_host proxy
httpd_accel_port 80
httpd_accel_single_host off
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
httpd_accel_no_pmtu_disc off

Filtrování nevhodného obsahu je možné provádět několika způsoby. Jejich
podrobný popis je možné najít na webových stránkách projektu. Já budu na tomto
serveru používat kombinaci filtrování celých nevhodných domén spolu s filtrováním
stránek, které obsahují nevhodná klíčová slova. Tato kombinace je podle mého
názoru nejefektivnější.
V prvním kroku jsem definoval název pravidla a zařadil do něj nevhodné domény.
Toto nastavení je možné podle potřeby libovolně upravovat, stačí pouze dopsat na
konec níže uvedeného příkazu další domény podle potřeby.

acl nevhodne_domeny dstdomain facebook.com lide.cz

V druhém kroku jsem definoval název pravidla, které slouží k tomu, aby bylo možné
odfiltrovat všechny stránky, které obsahují nevhodné výrazy. Tuto skutečnost
zajišťuje následující pravidlo. Opět je možné jej libovolně upravovat, stačí pouze na
konec příkazu dopsat další klíčová slova.

acl nevhodne_vyrazy url_regex –i sex xxx porno

V posledním kroku uvedeme tato pravidla do činnosti.

http_access deny nevhodne_domeny

#----------#
########## ***KONEC SKRIPTU*** ##########
#----------#

V mém návrhu jsou začleněny i služby, které umožňují uživatelům vzájemně sdílet data. Jednou z těchto služeb je právě FTP server. Tento server není přímo určený pro výměnu dat, ale umístil jsem jej sem proto, že skrz něj bude možné efektivně aktualizovat webové stránky školy. Softwarově bude tuto funkci plnit program ProFTPD. Jeho konfigurační možnosti jsou obrovské. Jejich kompletní výčet je opět možno najít na webových stránkách. Já jsem se rozhodl pro následující konfiguraci. Ta je pro můj účel zcela dostačující.

#----------#
########## ***ZAČÁTEK SKRIPTU*** ##########
#----------#

Toto nastavení aktivuje přídavné moduly, které jsou nutné pro správnou funkčnost.

Include /etc/proftpd/modules.conf

Server je nakonfigurován pouze pro používání protokolu IPv4.

UseIPv6 off

Název FTP serveru

ServerName "Skolni FTP Server"

Následujících několik nastavení je nutných pro správnou funkčnost celého serveru.
Podle mého názoru není nutné k těmto nastavením uvádět podrobné komentáře.
Pokud by někdo chtěl podrobněji zjistit, co které nastavení provádí, může tak učinit
na webových stránkách projektu.

ServerType standalone

MultilineRFC2228 on

DefaultServer on

ShowSymlinks on

TimeoutNoTransfer 600

TimeoutStalled 600

TimeoutIdle 1200

DisplayLogin welcome.msg

DisplayFirstChdir .message

ListOptions "-l"

DenyFilter *.*/

DefaultRoot /var/www/stranky

RootLogin off

Toto nastavení určuje číslo portu, který se používá pro běh serveru. Standardně se
používá port číslo 21 a ve většině případů jej není nutné měnit.

Port 21

Tato dvě nastavení určují uživatele, s jehož oprávněními server běží.

User proftpd

Group nogroup

Toto nastavení určuje, že je možné soubory na serveru přepisovat.

AllowOverwrite on

Provoz serveru je vhodné zaznamenávat. Toto zaznamenávání je užitečné hlavně
pro ladění serveru. Záznamy se ukládají do souborů. Tyto dva řádky určují, kde se
na disku záznamy nachází.

TransferLog /var/log/proftpd/xferlog

SystemLog /var/log/proftpd/proftpd.log

Server je možné nastavit buď tak, že se na něj může přihlásit každý uživatel nebo
je vyžadováno přihlašovací jméno a heslo. Tato varianta je bezpečnější. Já jsem
tento server nastavil druhým způsobem. V této části jsou vyjmenovaní uživatelé,
kteří se mohou na server přihlásit.

<Limit LOGIN>

Order allow,deny

AllowUser ftp administrator

DenyAll

</Limit>

#--#

########## ***KONEC SKRIPTU*** ##########

#--#

V souvislosti se sdílením dat jsem na server nasadil program Samba. Tento program umožňuje sdílení dat v sítí běžnými uživateli. Pro školu je vhodné vytvořit několik síťových sdílených adresářů, z nichž každý bude mít vlastní bezpečnostní politiku – některé budou přístupné bez omezení, přístup k jiným bude omezen. Konfigurační soubor programu je rozčleněný do několika oddílů. Prvním z nich je sekce s názvem *GLOBAL*. Jak už název napovídá, všechny uvedené parametry v této sekci slouží jako globální nastavení celého programu a ovlivňují nejen správný chod samotného serveru, ale částečně i chod celé sítě. Druhou sekcí je sekce s názvem *HOMES*. V této sekci budu ovlivňovat domovské adresáře uživatelů. Následuje sekce *PRINTERS*. Zde se nastavují případné síťové, sdílené tiskárny připojené k serveru. Jelikož je na škole provozována samostatná síťová tiskárna, nebudu v této sekci nic nastavovat a ponechám defaultní nastavení. Poslední sekcí je pak sekce s názvem USERSHARES. V této sekci budou definovány všechny další sdílené adresáře, a to jak veřejně přístupné, tak i soukromé. V našem případě pak bude konfigurační soubor vypadat následovně.

#--#

########## ***ZAČÁTEK SKRIPTU*** ##########

#--#

První sekce - GLOBAL

Následující tři řádky určují po řadě název zavedení pracovní skupiny, název
serveru zanesený v doménových záznamech a přívlastek jenž se objeví v okolních
počítačích u jména serveru.

workgroup = ŠKOLA

netbios name = Brana

server string = Samba_server

Tyto dva řádky zabezpečují správné zobrazování českých znaků ve sdílených.
adresářích a souborech.

unix charset = ISO8859-2

dos charset = 852

Tyto tři řádky definují způsob, jakým bude program zaznamenávat svoji činnost.
log file = /var/log/samba/log.%m
log level = 2
max log size = 500
V programu Samba lze definovat několik způsobů přístupu k jednotlivým sdíleným
adresářům. Následujících šest řádků určuje, že se ke sdíleným adresářům bude
přistupovat za pomoci kombinace uživatelské_jméno a heslo.
security = user
username map = /etc/samba/smbpasswd
invalid users = root
unix password sync = yes
encrypt passwords = yes
passwd program = /usr/bin/passwd %u
Následující čtyři řádky doplňují bezpečnostní nastavení. Po řadě definují z jakým
podsítí je možné k serveru přistoupit, na jakých síťových rozhraních server
naslouchá, chování serveru v případě anonymního přihlašování a chování serveru
v případě ilegálního přihlašování.
hosts allow = 192.168.1. 10.8.0. 127.0.0.1
interfaces = eth0 tap0 lo
guest account = nobody
map to guest = bad user
Následujících pět řádků určuje, že server bude hlavní autoritou pro řízení sdílení na
síti.
os level = 255
wins support = yes
preferred master = yes
local master = yes
domain master = yes
Další dodatečná nastavení určená ke zlepšení chodu serveru.
usershare allow guests = yes
name resolve order = wins lmhosts hosts bcast
dns proxy = yes
bind interfaces only = yes
deadtime = 10

debug level = 3

socket options = TCP_NODELAY

Tato část určuje chování případné sdílené síťové tiskárny.

load printers = yes

printing = bsd

printcap = /var/spool/samba

Druhá sekce - PRINTERS

Celá tato sekce určuje chování případné sdílené síťové tiskárny. Jelikož k serveru
není žádná tiskárna připojena, ponechám ji bez změny v defaultním nastavení.

comment = Tiskárny

path = /var/spool/samba

printable = yes

public = no

browseable = no

writable = no

printer admin = @administratori

create mode = 0700

Třetí sekce - HOMES

Celá následující sekce je určena k nastavení sdílení domovských adresářů pro
jednotlivé uživatele, a to jak žáky tak i učitele. Já popíšu nastavení jednoho
sdíleného adresáře. Ostatní sdílení se nastavují identicky, pouze dochází ke
změnám názvů jednotlivých adresářů a změnám v bezpečnostní politice adresáře.
Název sdílené složky, který se objeví v okolních počítačích.

[učitelé]

Stručný popis komu je složka určena. Slouží administrátorovi pro lepší orientaci.
Jedná se o nepovinný parametr.

comment = Společný_adresář_pedagogického_sboru

Stručný popis komu je složka určena. Objeví se v okolních počítačích. Jedná se
o nepovinný parametr.

volume = ucitele

Všechna sdílení jsou uložena na pevném disku serveru. Tato položka určuje, kde
přesně je možné všechny sdílení najít. Vhodne rozčlenění pak velice

usnadňuje práci správce.

path = /samba/ucitele

Tyto položky určují, jestli bude sdílený adresář automaticky viditelný v okolních
počítačích nebo jestli jej bude nutné manuálně připojovat. V našem případě je
zvolena manuální metoda.

public = no

browseable = no

Tyto položky určují míru zabezpečení adresáře. První a druhá určují, že do
adresáře bude možné zapisovat. Třetí položka určuje, kdo bude mít do adresáře
přístup. Čtvrtá položka určuje, že uživatelé bez platného uživatelského jména
a hesla se do složky nedostanou.

read only = no

writable = yes

valid users = učitel1 učitel2 učitel3 …

guest ok = no

Vzhledem k nastavení složky pouze pro čtení je tento parametr poměrně důležitý.
Určuje totiž uživatele, kteří budou moci do složky zapisovat. V našem případě to
jsou všichni uživatelé, kteří jsou členy skupiny „administratori”.

write list = @administratori

Tyto dvě položky určují, jaká práva budou mít nově vytvořené soubory a složky ve
sdíleném adresáři. Práva ve tvaru 0777 znamenají, že každý uživatel bude se
souborem nebo adresářem moci manipulovat bez omezení.

create mask = 0777

directory mask = 0777

Čtvrtá sekce - USERSHARES

Celá následující sekce je určena k nastavení dalších sdílených adresářů na síti.
Tyto adresáře budou využívány jak pro výuku, tak i pro další účely. (Například pro
ukládání hotových cvičení při výuce ICT.) Já popíšu nastavení jednoho
sdíleného adresáře. Ostatní sdílení se nastavují identicky, pouze dochází ke
změnám názvů jednotlivých adresářů a změnám v bezpečnostní politice adresáře.
Název sdílené složky, který se objeví v okolních počítačích.

[Vyukove_programy]

Stručný popis komu je složka určena. Slouží administrátorovi pro lepší orientaci.

Jedná se o nepovinný parametr.

comment = Nase_vyukove_programy

Stručný popis komu je složka určena. Objeví se v okolních počítačích. Jedná se
o nepovinný parametr.

volume = vyukove_programy

Všechna sdílení jsou uložena na pevném disku serveru. Tato položka určuje, kde
přesně je možné všechny sdílení najít. Vhodné rozčlenění pak velice usnadňuje
práci správce.

path = /samba/programy/vyukove

Tyto položky určují, jestli bude sdílený adresář automaticky viditelný v okolních
počítačích nebo jestli jej bude nutné manuálně připojovat. V našem případě je
zvolena manuální metoda.

public = yes

writable = yes

Tyto položky určují míru zabezpečení adresáře. První a druhá určují, že do
adresáře nebude možné zapisovat. Třetí a čtvrtá položka určují, že uživatelé bez
platného uživatelského jména a hesla budou tuto složku moci využívat.

read only = yes

writeable = no

guest ok = yes

guest only = yes

Tyto dvě položky určují, jaká práva budou mít nově vytvořené soubory a složky ve
sdíleném adresáři. Práva ve tvaru 0777 znamenají, že každý uživatel bude se
souborem nebo adresářem moci manipulovat bez omezení.

directory mask = 0777

create mask = 0777

Tato položka určuje kolik uživatelů najednou bude moct využívat tuto složku. Je
vhodné omezit počet, aby nedocházelo k přetížení nebo pádům serveru. Omezení
je nastaveno na 75 uživatelů.

max connections = 75

#----------#

########## ***KONEC SKRIPTU*** ##########

#----------#

Především pro potřeby komunikace a snadného přístupu žáků a jejich rodičů k informacím, jsem ve své implementaci nasadil WWW server. Tento server jsem zrealizoval za pomoc programu Apache2. Nastavení tohoto programu je nutné provést ve dvou souborech. V prvním souboru se provádí nastavení vlastního serveru. Ve druhém souboru se určují parametry pro webový přístup k němu a pro služby, které bude poskytovat. Jedná se o široce konfigurovatelný server. V tomto případě jsem provedl následující úpravu prvního konfiguračního souboru.

```
#--------------------------------------------------------------------------#
############        ZAČÁTEK SKRIPTŮ        ############
#--------------------------------------------------------------------------#
# První sekce slouží ke globálnímu nastavení serveru. Je zde zahrnuta většina
# náležitostí, které jsou potřeba pro běh samotného serveru. Tyto nastavení se
# nemění, a proto není nutné je detailněji popisovat.
ServerRoot "/etc/apache2"
LockFile /var/lock/apache2/accept.lock
PidFile /var/run/apache2.pid
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
<IfModule mpm_prefork_module>
    StartServers          5
    MinSpareServers       5
    MaxSpareServers      10
    MaxClients          150
    MaxRequestsPerChild   0
</IfModule>
<IfModule mpm_worker_module>
    StartServers          2
    MaxClients          150
    MinSpareThreads      25
    MaxSpareThreads      75
    ThreadsPerChild      25
```

```
   MaxRequestsPerChild   0
</IfModule>
# Tato dvě nastavení určují uživatele, s jehož oprávněními server běží.
User www-data
Group www-data
# Následující blok příkazů je zde proto, aby se zajistila bezpečnost serveru.
AccessFileName .htaccess
<Files ~ "^\.ht">
   Order allow,deny
   Deny from all
</Files>
TypesConfig /etc/mime.types
# Toto nastavení určuje, jak se má pracovat s HTML dokumenty uloženými na
# serveru. Toto nastavení je pro školu vhodné, protože na serveru budou uloženy
# převážně textové soubory.
DefaultType text/plain
# Následující sekce příkazů určuje jakým způsobem bude server zaznamenávat svoji
# činnost.
HostnameLookups Off
ErrorLog /var/log/apache2/error.log
LogLevel warn
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
# Tento příkaz určuje, jaké informace o sobě server na požádání poskytne.
ServerTokens Full
# Tento blok příkazů určuje, jak se bude zacházet s komprimovanými soubory, jaký
# je standardní jazyk HTML dokumentů. Dále jsou vyjmenovány další použitelné
# jazyky a pořadí jejich nasazení.
<IfModule mod_mime.c>
   AddType application/x-compress .Z
   AddType application/x-gzip .gz .tgz
```

DefaultLanguage cs

AddLanguage ca .ca

AddLanguage cs .cz .cs

AddLanguage da .dk

AddLanguage de .de

AddLanguage el .el

AddLanguage en .en

AddLanguage eo .eo

AddLanguage es .es

AddLanguage et .et

AddLanguage fr .fr

AddLanguage he .he

AddLanguage hr .hr

AddLanguage it .it

AddLanguage ja .ja

AddLanguage ko .ko

AddLanguage ltz .ltz

AddLanguage nl .nl

AddLanguage nn .nn

AddLanguage no .no

AddLanguage pl .po

AddLanguage pt .pt

AddLanguage pt-BR .pt-br

AddLanguage ru .ru

AddLanguage sv .sv

AddLanguage zh-CN .zh-cn

AddLanguage zh-TW .zh-tw

</IfModule>

<IfModule mod_negotiation.c>

LanguagePriority cs en ca da de el eo es et fr he hr it ja ko ltz nl nn no pl pt pt-BR ru sv zh-CN zh-TW

</IfModule>

Tato sekce udává hlavní a ostatní typy jazykového kódování.

<IfModule mod_mime.c>

AddDefaultCharset WINDOWS-1250

AddCharset us-ascii .ascii .us-ascii

AddCharset ISO-8859-1 .iso8859-1 .latin1

AddCharset ISO-8859-2 .iso8859-2 .latin2 .cen

AddCharset ISO-8859-3 .iso8859-3 .latin3

AddCharset ISO-8859-4 .iso8859-4 .latin4

AddCharset ISO-8859-5 .iso8859-5 .cyr .iso-ru

AddCharset ISO-8859-6 .iso8859-6 .arb .arabic

AddCharset ISO-8859-7 .iso8859-7 .grk .greek

AddCharset ISO-8859-8 .iso8859-8 .heb .hebrew

AddCharset ISO-8859-9 .iso8859-9 .latin5 .trk

AddCharset ISO-8859-10 .iso8859-10 .latin6

AddCharset ISO-8859-13 .iso8859-13

AddCharset ISO-8859-14 .iso8859-14 .latin8

AddCharset ISO-8859-15 .iso8859-15 .latin9

AddCharset ISO-8859-16 .iso8859-16 .latin10

AddCharset ISO-2022-JP .iso2022-jp .jis

AddCharset ISO-2022-KR .iso2022-kr .kis

AddCharset ISO-2022-CN .iso2022-cn .cis

AddCharset Big5 .Big5 .big5 .b5

AddCharset cn-Big5 .cn-big5

AddCharset WINDOWS-1251 .cp-1251 .win-1251

AddCharset CP866 .cp866

AddCharset KOI8 .koi8

AddCharset KOI8-E .koi8-e

AddCharset KOI8-r .koi8-r .koi8-ru

AddCharset KOI8-U .koi8-u

AddCharset KOI8-ru .koi8-uk .ua

AddCharset ISO-10646-UCS-2 .ucs2

AddCharset ISO-10646-UCS-4 .ucs4

AddCharset UTF-7 .utf7

AddCharset UTF-8 .utf8

AddCharset UTF-16 .utf16

AddCharset UTF-16BE .utf16be

AddCharset UTF-16LE .utf16le

AddCharset UTF-32 .utf32

AddCharset UTF-32BE .utf32be

AddCharset UTF-32LE .utf32le

AddCharset euc-cn .euc-cn

AddCharset euc-gb .euc-gb

AddCharset euc-jp .euc-jp

AddCharset euc-kr .euc-kr

AddCharset EUC-TW .euc-tw

AddCharset gb2312 .gb2312 .gb

AddCharset iso-10646-ucs-2 .ucs-2 .iso-10646-ucs-2

AddCharset iso-10646-ucs-4 .ucs-4 .iso-10646-ucs-4

AddCharset shift_jis .shift_jis .sjis

AddHandler type-map var

AddType text/html .shtml

AddOutputFilter INCLUDES .shtml

</IfModule>

Tyto sekce řeší známé problémy s HTTP požadavky v různých klientech.

<IfModule mod_setenvif.c>

BrowserMatch "Mozilla/2" nokeepalive

BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0

BrowserMatch "RealPlayer 4\.0" force-response-1.0

BrowserMatch "Java/1\.0" force-response-1.0

BrowserMatch "JDK/1\.0" force-response-1.0

BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully

BrowserMatch "MS FrontPage" redirect-carefully

BrowserMatch "^WebDrive" redirect-carefully

BrowserMatch "^WebDAVFS/1.[012]" redirect-carefully

BrowserMatch "^gnome-vfs/1.0" redirect-carefully

BrowserMatch "^XML Spy" redirect-carefully

BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully

</IfModule>

Pro správnou funkčnost je nutné do konfigurace přidat několik dalších souborů.

Poslední z těchto souborů slouží pro nastavení, která se týkají webového přístupu
k serveru.
Include /etc/apache2/mods-enabled/*.load
Include /etc/apache2/mods-enabled/*.conf
Include /etc/apache2/httpd.conf
Include /etc/apache2/ports.conf
Include /etc/apache2/conf.d/
Include /etc/apache2/sites-enabled/

Ve druhém konfiguračním souboru se určuje, jak bude server reagovat na webový
přístup, kde na pevném disku budou uloženy jeho soubory, jaká bude www adresa
apod.
NameVirtualHost *:80
<VirtualHost *:80>
Servername www.zakladni.skola
ServerAdmin administrator@zakladni.skola
DocumentRoot /var/www/stranky
<Directory /var/www/stranky>
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/stranky>
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order deny,allow
Allow from All
Deny from All
</Directory>
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
AllowOverride None
Options ExecCGI -MultiViews +SymLinksIfOwnerMatch
Order allow,deny
Allow from all

</Directory>

ErrorLog /var/log/apache2/intranet.log

</VirtualHost>

#----------#

########## ***KONEC SKRIPTŮ*** ##########

#----------#

Poslední službou, kterou jsem se rozhodl detailněji popsat je služba pro vzdálený přístup do sítě. Tato služba je realizována ve dvou variantách. První variantou je přístup přes textovou konzoli. Tento přístup je implementován programem Openssh-server. Po instalaci tohoto programu není nutné jeho připravenou konfiguraci vůbec měnit. Proto nebudu detailněji popisovat jeho konfigurační soubor. Druhou variantou přístup přes grafickou konzoli. Tento přístup je zajištěn instalací programu Openvpn. Nastavení jeho konfiguračního souboru je nutné upravit. Já jsem ho k tomuto účelu upravil tímto způsobem.

#----------#

########## ***ZAČÁTEK SKRIPTŮ*** ##########

#----------#

Tento program je univerzální a je možné ho nastavit do role klienta i serveru. Já
požaduji, aby program sloužil jako server. Toto jsem zajistil následující dvojicí
příkazů.

mode server

tls-server

Tímto jsem určil, jaké číslo portu bude program při své činnosti používat. Port 1194
je standardní a ve většině případů jej není nutné měnit.

port 1194

Tento server může při své činnosti využívat spojení přes TCP i přes UDP. Já jsem
ho nastavil pro využití TCP.

proto tcp-server

Pro svoji činnost vyžaduje server vytvoření virtuálního síťového rozhraní. Zde jsem
určil název tohoto rozhraní.

dev tap0

Spojení realizované po VPN je zabezpečeno šifrováním. Tyto parametry určují, kde
na pevném disku se tyto soubory nachází a jak silné šifrování je použito.
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
dh dh1024.pem
tls-auth ta.key 0
persist-key
persist-tun
Jelikož si server vytvořil vlastní virtuální rozhraní, je nezbytné mu přidělit IP adresu.
Tato IP adresa musí být odlišná od té, kterou má přidělenu jakákoliv síťová karta.
server 10.8.0.0 255.255.255.0
Pomocí direktivity PUSH se připojujícím se klientům přiřazují nezbytné údaje.
Jedná se o podobnou funkci, kterou plní v síti DHCP server. Postupně dojde
k delegaci podsítě virtuálního rozhraní, podsítě fyzického rozhraní, adresy
jmenného serveru, název domény a adresu serveru, který řídí sdílení dat na síti.
push "route 10.8.0.0 255.255.255.0"
push "route 192.168.2.0 255.255.255.0"
push "dhcp-option DNS 192.168.2.1"
push "dhcp-options DOMAIN zakladni.skola"
push "dhcp-option WINS 192.168.2.1"
K serveru se může v jeden okamžik připojit několik klientů. Aby spolu mohli tito
klienti komunikovat, je nutné to v nastavení serveru zahrnout. To se provede za
pomoci tohoto příkazu.
client-to-client
Při přístupu více klientů by měl každý z nich využívat vlastní přístupový klíč. Jelikož
se na tento server vzdáleně bude hlásit pouze omezený počet osob – správců,
povolil jsem to, aby mohli všichni používat stejný přístupový klíč.
duplicate-cn
Tato direktiva se stará o to, aby spojení mezi klientem a serverem bylo stále
aktivní.
keepalive 10 120
Tímto jsem omezil počet najednou připojených klientů na 10.
max-clients 10

Tato dvě nastavení určují uživatele, s jehož oprávněními server běží.

user nobody

group nogroup

Následující sekce příkazů určuje jakým způsobem bude server zaznamenávat svoji
činnost.

status /var/log/openvpn-status.log

log-append /var/log/openvpn.log

verb 4

mute 20

#----------#

########## ***KONEC SKRIPTU*** ##########

#----------#

Závěr

Cílem mé diplomové práce bylo zpracovat návrh školního síťového serveru, který by plnohodnotně nahradil stávající servery ve školách umístěné. V první části diplomové práce byly stručně zmíněny teorie fungování počítačových sítí. V další části byly popsány vybrané druhy počítačových sítí a byla nastíněna hlediska, podle nichž lze sítě kategorizovat. Dále byl nastíněn princip komunikace v datových sítích. Diplomová práce je zaměřena k využití na základních školách, proto byla největší pozornost věnována tvorbě LAN. Poté následovala stručná historie operačního systému Linux.

Poslední část diplomové práce je věnována praktickým ukázkám konkrétních konfiguračních souborů. V úvodu byla popsána hardwarová konfigurace serveru a dále byly vyjmenovány softwarové nástroje použité při jeho tvorbě. Aby měl přechod na tento server smysl, je nutné, abychom si uvědomili výhody, které z toho plynou. Hlavní výhoda, která z návrhu vyplývá, je celková pořizovací cena. Server je navržen tak, aby se minimalizovala počáteční investice. Proto je k tvorbě využita vyřazená pracovní stanice z počítačové učebny. Protože pracovní stanice a síťový server plní odlišné funkce, je nutné tento počítač k tomuto účelu náležitě upravit. Vzhledem k provozovaným službám, bylo nutné zvětšit velikost operační paměti a úložné diskové kapacity. Celkové náklady na tuto úpravu se pohybovaly v řádu několika málo tisíc korun. Jako síťový software jsem použil volně dostupný operační systém Linux, konkrétně distribuci Debian. Tato distribuce je šířena nekomerčně a její nasazení proto nezvyšuje celkové pořizovací náklady na tvorbu serveru.

V diplomové práci byly uvedeny ukázky konfiguračních souborů jednotlivých služeb. Protože nejsou všechny školy stejné, byly uvedeny pouze některé možnosti konfigurace. Každý, kdo bude tento návrh využívat, si jak doufám tyto nastavení přizpůsobí pro svoji konkrétní situaci.

Tento konkrétní server byl po dobu jednoho měsíce testován ve školním provozu. Při tomto testovacím provozu server obsluhoval v normálním provozu 20 – 25 pracovních stanic. Na serveru byly po tuto dobu instalovány výukové programy firmy Terasoft. Celkově se jednalo o 10 výukových titulů. Celková disková kapacita byla využita z 10 %. Množství přenesených dat se v průměru pohybovalo v rozmezí 5 – 6 Gb za den. Při tomto testu zatížení serveru nepřesáhlo průměrnou hodnotu 10 %. I přesto, že se jedná o krátký časový úsek, jsem dospěl k závěru, že bude takto

dimenzovaný server pro tuto školu plně dostačovat a bude možné jej využít jako náhradu za stávající server, který byl do školy dodán spolu s projektem INDOŠ.

Tato diplomová práce naznačuje pouze některé ze široké škály možností, jak ve školním prostředí vytvořit a navrhnout vlastní server. Nejedná se o podrobně zpracovaný návod. I přesto doufám, že bude tato diplomová práce přínosem pro všechny učitele, ICT koordinátory a počítačové nadšence, kteří budují nebo spravují počítačovou síť a mají zájem ji neustále rozšiřovat, vylepšovat a optimalizovat.

Literatura

1. BASL, J. *Informační systém škol – specifická oblast využití manažerských informačních systémů* [online]. [cit 2010-06-16]. Dostupné na WWW: http://www.ikaros.cz/node/3736/.

2. KROPÁČ, J., KUBÍČEK, Z., CHRÁSKA, M., HAVELKA, M. *Didaktika technických předmětů vybrané kapitoly.* 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2004. 223 s. ISBN 80-244-0848-1.

3. NOVOTNÝ, V. *Architektura sítí*. 1. vyd. Brno: Vysoké Učení Technické, 2002. 136 s.

4. REYNDERS, D., WRIGHT, E. *Practical TCP/IP and ethernet networking.* 1. vyd. Oxford: Linacre House, Jordan Hill, 2003. 306 s. ISBN 07506 58061.

5. *Maturitní otázky z informatiky* [online]. [cit. 2010-06-17]. Dostupné na WWW: http://www.cihak.com/michal/maturita/maturitni_otazky.htm/.

6. *Počítačové sítě* [online]. [cit. 2009-02-20]. Dostupné na WWW: http://site.the.cz/.

7. ZANDL, P. *Wifi Praktický Průvodce.* 1. vyd. Brno: Computer Press, 2003. 217 s. ISBN 80-7226-632-2.

8. *Směrování v síti – statické směrování* [online]. [cit. 2009-03-20]. Dostupné na WWW: http://owebu.bloger.cz/PC-site/Smerovani-v-siti-staticke-smerovani-2-dil.

9. *PETERKA, J. E-archiv* [online]. 2010 [cit. 2010-01-20]. Dostupné na WWW: http://www.earchiv.cz.

10. *Počítačové sítě* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://pc-site.owebu.cz/.

11. *Aktivní prvky* [online]. 2009 [cit. 2009-03-20]. Dostupné z WWW: http://www.gity.cz/cs/art/1113-aktivni-prvky.

12. *Jak se liší směšovače, rozbočovače, přístupové body a směrovače* [online]. 2009 [cit. 2009-03-20]. Dostupné z WWW: http://windows.microsoft.com/cs-CZ/windows-vista/How-do-hubs-switches-routers-and-access-points-differ.

13. *Chapter 4: Cabling* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://fcit.usf.edu/network/chap4/chap4.htm.

14. Wikipedie, otevřená encyklopedie. [cit. 2010-06-16]. Dostupné z WWW: http://cs.wikipedia.org/wiki/Hlavní_strana.

15. Kroucená dvoulinka / Slovníček pojmů [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://www.pripojeno.cz/cd/slovnicek_pojmu/kroucena_dvoulinka.htm.

16. *sec – Kroucená dvojlinka* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://budnet.eu/sec/?p=135.

17. *Možnosti optických vláken* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://www.ofacom.cz/index.php?option=com_content&view=article&id=129:moznosti-optickych-vlaken&catid=80:ofs-v-&Itemid=96.

18. *Co je to v IT > Optické vlákno a kabely* [online]. 2010 [cit. 25.2.2010] Dostupné z WWW: http://hps.mallat.cz/view.php?cisloclanku=2003090203.

19. *Technologie přenosu dat přes optická vlákna* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://pctuning.tyden.cz/hardware/site-a-internet/9994-technologie_prenosu_dat_pres_opticka_vlakna.

20. KOLEKTIV AUTORŮ *Linux - Dokumentační projekt*. 3. vyd. Brno: Computer Press, 2003. 1001 s. ISBN 80-7226-761-2.

21. *Debian.cz – o Debianu* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://debian.cz/info/about.php.

22. *Ubutu – Linux pro lidi* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://www.ubuntu.cz/produkty/cojeubuntu.

23. *Fcz:o_fedore [FedoraWiki]* [online]. 2010 [cit. 2010-06-17]. Dostupné z WWW: http://wiki.fedora.cz/doku.php?id=fcz:o_fedore.

24. *Základní informace o Mandriva Linux* [online]. [cit. 2010-06-17]. Dostupné z WWW: http://www.mandrivalinux.cz/o-mandriva-linuxu.

25. *Root.cz – informace nejen ze světa Linuxu* [online]. 2010 [cit 2010-06-17]. Dostupné z WWW: http://www.root.cz/.

26. DOSTÁLEK, L. - KABELOVÁ, A. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. vyd. Brno: Computer Press, 2000. 435 s. ISBN 80-7226-323-4.

27. *AbcLinuxu.cz – Linux na stříbrném* podnose [online]. [cit. 30.5.2010]. Dostupné z: http://www.abclinuxu.cz/.

28. Linux EXPRESS [online]. [cit. 5.6.2010]. Dostupné z WWW: http://www.linuxexpres.cz/.

29. JAY, TS. – ECKSTEIN, R. – COLLIER-BROWN, D. Using samba. 2. vyd. O'Reilly, 2003. 622 s. ISBN 0-596-00256-4.

30. Shah, S. – GRAHAM, S. Administrace systému LINUX, 3. vyd. Praha: Grada Publishing, 2002. 552 s. ISBN 80-247-0641-5.

31. MOHAMMED J. KABIR Apache server 2 bible. New York: Hungry Minds, Inc., 2002. 793 s. ISBN 0-7645-4821-2.

32. *OpenVPN* [online]. [cit. 10.6.2010]. Dostupné z: http://www.openvpn.net/.

ANOTACE

Jméno a příjmení:	Zdeněk Konfršt
Katedra nebo ústav:	Katedra technické a informační výchovy
Vedoucí práce:	PhDr. Milan Klement, Ph.D.
Rok obhajoby:	2010

Název práce:	Informační systém školy postavený na využití služeb platformy Linux.
Název v angličtině:	School information system based on Linux-platform services.
Anotace práce:	Práce je zaměřena na návrh a realizaci školního počítačového serveru, podává přehled o počítačových sítích, operačním systému Linux a síťových zařízeních.
Klíčová slova:	Linux, server, škola, informační systém, konfigurační soubor, služba
Anotace v angličtině:	This works reports on project and implementation Linux-platform server, it presents a review of computer network, operation system Linux and hardware.
Klíčová slova v angličtině:	Linux, server, school, information system, configuration file, service
Přílohy vázané v práci:	-
Rozsah práce:	103
Jazyk práce:	čeština